IBM

eserver

iSeries

iSeries 보안을 위한 추가 정보 및 툴

버전 5

SA30-0525-07

IBM

@server

iSeries

iSeries 보안을 위한 추가 정보 및 툴

버전 5

SA30-0525-07

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 185 페이지의 『주의사항』의 정보를 읽으십시오.

제 8 판(2004년 4월)

| 이 개정판은 새 개정판에 별도로 명시하지 않는 한, IBM Operating System/400(제품 번호 5722-SS1)의 버전 5, 릴리스 3, 수정 0 | 및 모든 후속 릴리스와 수정판에 적용됩니다. 이 버전은 모든 축약 명령어 세트 컴퓨터(RISC) 모델 및 CISC 모델에서 실행되지 않 | 습니다.

이 개정판은 SA30-0525-06을 대체합니다.

목차

그림

표

iSeries 보안을 위한 팁 및 도구(SA30-0525-07)

조직에서 컴퓨터가 담당하는 역할이 빠르게 변화하므로 컴퓨터 관리자, 소프트웨어 제공자, 보안 관리자 및 감사자는 과거에 당연한 것으로 여겨졌던 많은 분야를 재검토해야만 합니다. iSeries 보안도 여기에 해당됩니다.

이전의 계정 어플리케이션과는 매우 다른 새로운 기능이 많이 제공되고 있습니다. 사용자들은 새로운 방법으로 시스템에 접속합니다. 즉, LAN, 교환 회선(전화 접속), 무선, 모든 유형의 네트워크를 통해 시스템에 접속합니다. 사용자가 사인 온 화면을 전혀 볼 수 없을 때도 있습니다. 많은 조직이 독점 네트워크나 인터넷을 사용하여 『확장 기업』이 되기 위해 노력하고 있습니다.

갑자기 시스템에 전혀 새로운 출입구들이 생긴 것처럼 보입니다. 당연히 시스템 관리자와 보안 관리자는 이렇게 빠른 속도로 변화하는 환경에서 정보 자산을 보호하기 위한 방법에 대해 관심을 가지게 됩니다.

이 정보는 iSeries의 보안 피처 사용 및 보안 인식 조작 프로시듀어 설정에 대한 실제 제안들을 제공합니다. 이 정보의 권장사항은 평균적인 보안 요구사항 및 노출을 사용하는 설치에 적용됩니다. 이 정보에서는 iSeries에서 사용할 수 있는 보안 피처들을 자세히 설명하지 않습니다. 추가 옵션에 대해 읽고자 하거나 더 자세한 백그라운드 정보가 필요하면 181 페이지의 제 17 장 『관련 정보』에 설명된 서적을 참조하십시오.

또한 이 정보에서는 OS/400의 일부인 보안 툴을 설정하고 사용하는 방법을 설명합니다. 31 페이지의 제 4 장 『iSeries를 구성하여 보안 툴 사용』 및 32 페이지의 『보안 명령에 대한 명령 및 메뉴』에 보안 툴에 관한 참조 정보가 제공됩니다. 이 정보는 툴 사용을 위한 예를 제공합니다.

이 책의 사용자

보안 담당자 또는 **보안 관리자**가 시스템 보안을 책임집니다. 그 책임에는 대개 다음 타스크가 포함됩니다.

- 사용자 프로파일 설정 및 관리
- 보안에 영향을 주는 시스템 공통값 설정
- 오브젝트에 대한 권한 관리
- 보안 방침 실행 및 모니터

이 정보는 하나 이상의 iSeries 시스템의 보안 관리 책임을 맡고 있는 사용자에게 이상적입니다. 이 정보의 지침은 다음 사항을 가정한 것입니다.

- 사용자가 사인 온 및 명령 사용과 같은 기본적인 iSeries 조작 프로시듀어에 익숙합니다
- 사용자가 iSeries 보안의 기본 요소, 즉 보안 레벨, 보안 시스템 값, 사용자 프로파일 및 오브젝트 보안에 익숙합니다.

  주: 3 페이지의 제 1 장 『iSeries 보안의 기본 요소』에서 이들 요소에 대한 내용을 제공합니다. 이 기본 요소들이 사용자에게 새로운 것이면 iSeries Information Center에 나오는 *기본 보안 및 계획* 주제를 읽어보십시오. 자세한 내용은 『요구사항 및 관련 정보』를 참조하십시오.
- QSECURITY(보안 레벨) 시스템 값을 적어도 30으로 설정하여 시스템 보안을 가동했습니다.

IBM®에서는 계속해서 iSeries의 보안 기능을 향상시킵니다. 이러한 확장 기능을 활용하려면, 현재 릴리스에서 사용할 수 있는 누적 수정 패키지를 정기적으로 평가해야 합니다. 보안과 관련된 수정이 들어 있는지 확인하십시오.

정보 사용법

시스템에서 보안 툴을 사용하도록 설정하지 않았거나 이전 릴리스의 Security ToolKit for OS/400을 설치한 경우, 다음을 수행하십시오.

1. 11 페이지의 제 2 장 『iSeries 보안 마법사 및 eServer 보안 플래너』로 시작하십시오. 권장되는 보안 툴을 선택하기 위해 이 피처를 사용하는 방법과 그 시작 방법이 설명됩니다.
2. 기본 보안 정보는 iSeries™ Information Center에서 온라인 상태에 있는 보안 참조 정보를 검토할 수 있습니다.

> **주**
>
> 이 정보에는 iSeries을 보호하기 위한 많은 추가 정보가 있습니다. 사용자 시스템은 일부 영역에서만 보호가 필요할 수 있습니다. 가능한 보안 노출과 그 해결 방법을 배우려면 이 정보를 사용하십시오. 그런 다음 시스템의 가장 중요한 부분에 초점을 맞추십시오.

요구사항 및 관련 정보

iSeries Information Center를 iSeries 기술 정보를 찾기 위한 출발점으로 사용하십시오.

다음 두 방법으로 Information Center에 액세스할 수 있습니다.

- 다음 웹 사이트로부터:

http://www.ibm.com/eserver/iseries/infocenter

- 이 *iSeries Information Center*, SK3T-4091-04 CD-ROM으로부터. 이 CD-ROM은 새 iSeries 하드웨어 또는 IBM Operating System/400 소프트웨어 업그레이드 주문 시 제공됩니다. 다음 IBM 서적 센터에서 CD-ROM을 주문할 수도 있습니다.

  http://www.ibm.com/shop/publications/order

iSeries Information Center에는 소프트웨어 및 하드웨어 설치, Linux, WebSphere®, Java™, 고가용성, 데이터베이스, 논리 파티션, CL 명령 및 시스템 어플리케이션 프로그래밍 인터페이스(API)와 같은 갱신된 새로운 iSeries 정보가 있습니다. iSeries 하드웨어 및 소프트웨어의 계획, 문제 해결 및 구성을 지원하기 위해 어드바이저와 파인더도 제공합니다.

새 하드웨어를 주문하면 다음 CD-ROM이 제공됩니다. *iSeries 설정 및 조작 CD-ROM*, SK3T-4098-02. 이 CD-ROM에는 IBM **@server** Windows용 IBM e(logo)server iSeries Access 및 EZ-Setup 마법사가 있습니다. iSeries Access 제품군클라이언트는 PC를 iSeries 서버에 연결하기 위한 강력한 클라이언트 및 서버 기능 세트를 제공합니다. EZ-Setup 마법사는 많은 iSeries 설치 타스크를 자동화합니다.

고객 의견서를 보내는 방법

고객 여러분의 의견은 정확하고 우수한 품질의 정보를 제공하는 데 있어서 매우 중요합니다. 이 책이나 기타 iSeries 책에 관해 의견이 있으시면 전자우편 또는 아래의 전화번호로 보내주십시오.

- 전자우편: ibmkspoe@kr.ibm.com
- 한국 아이.비.엠 고객만족센터: 02-3781-7114

의견을 보내실 때에는 반드시 다음 항목을 기록해 주십시오.

- 이 책의 이름 또는 iSeries Information Center 주제명
- 책의 주문 번호
- 의견에 해당되는 책의 페이지 번호 또는 주제

제 1 부 기본 iSeries 보안

제 1 장 iSeries 보안의 기본 요소

여기에서는 iSeries 보안을 제공하기 위해 함께 작업되는 기본 요소들을 간단히 알아봅니다. 이 책의 다른 부분에서는 조직의 필요에 맞게 다음 보안 요소들을 사용할 수 있는 초보 단계 이상의 추가 정보를 제공합니다.

보안 레벨

보안 레벨(QSECURITY) 시스템 값을 설정하여 시스템이 수행할 보안 정도를 선택할 수 있습니다. 시스템은 5개의 보안 레벨을 제공합니다.

레벨 10:

보안이 수행되지 않고 있습니다. 암호가 필요하지 않습니다. 사인 온시 지정된 사용자 프로파일이 시스템에 없으면 사용자 프로파일이 하나 작성됩니다.

주의:

V4R3부터는 QSECURITY 시스템 값을 10으로 설정할 수 없습니다. 시스템의 현재 보안 레벨이 10이면, 버전 4 릴리스 3을 설치할 때 레벨 10으로 유지됩니다. 보안 레벨을 다른 값으로 변경하면 다시 레벨 10으로 변경할 수 없습니다. 레벨 10이 어떠한 보안 보호도 제공하지 않으므로 IBM은 보안 레벨 10을 권장하지 않습니다. **IBM은 상위 보안 레벨에서도 문제가 발생할 것 같지 않으면, 보안 레벨 10에서 발생하는 문제에 대해서는 지원하지 않습니다.**

레벨 20:

사인 온하려면 사용자 ID와 암호가 필요합니다. 보안 레벨 20은 **사인 온 보안**이라고도 합니다. 디폴트로, 모든 사용자가 *ALLOBJ 특수 권한이 있으므로 모든 사용자는 모든 오브젝트에 액세스할 수 있습니다.

레벨 30:

사인 온하려면 사용자 ID와 암호가 필요합니다. 디폴트로 사용자에게 어떠한 권한도 부여하지 않으므로, 사용자는 오브젝트를 사용할 수 있는 권한이 있어야 합니다. 이것을 **자원 보안**이라고 합니다.

레벨 40:

사인 온하려면 사용자 ID와 암호가 필요합니다. 시스템은 자원 보안 외에 **무결성 보호** 기능도 제공합니다. 오퍼레이팅 시스템의 인터페이스에 대한 매개변수의 유효성과 같은 무결성 보호 기능은 숙련된 시스템 사용자가 시스템 및 시스템의 오브젝트를 함부로 고치는 것으로부터 보호하기 위한 것입니다. 레벨 40

은 대부분의 설치에서 권장되는 보안 레벨입니다. V4R5 또는 그 이후 릴리스의 새 iSeries 시스템을 받으면 보안 레벨이 40으로 설정됩니다.

레벨 50:

사인 온하려면 사용자 ID와 암호가 필요합니다. 시스템이 레벨 40의 자원 보안 및 무결성 보호를 강제로 수행하지만 시스템 상태 프로그램 및 사용자 상태 프로그램 간 메시지 처리의 제한사항과 같은 **향상된 무결성 보호**를 제공합니다. 보안 레벨 50은 높은 레벨의 보안이 요구되는 iSeries 시스템을 위한 것입니다.

주: 레벨 50은 C2 인증(및 FIPS-140 인증)을 위한 필수 레벨입니다.

*iSeries 보안 참조서*의 제 2 장은 보안 레벨에 대한 자세한 내용 및 보안 레벨 사이의 이동 방법을 설명합니다.

글로벌 설정

시스템에는 작업을 시스템에 입력하는 방법과 다른 시스템 사용자에게 시스템을 나타내는 방법에 영향을 주는 글로벌 설정이 있습니다. 이 설정에는 아래와 같은 것들이 포함됩니다.

보안 시스템 값:

보안 시스템 값은 시스템에서 보안을 제어하기 위해 사용됩니다. 이 값은 다음과 같은 네 개의 그룹으로 나누어집니다.

- 일반 보안 시스템 값
- 보안과 관련된 기타 시스템 값
- 암호를 제어하는 시스템 값
- 감사를 제어하는 시스템 값

이 책의 몇몇 주제에서 특정 시스템 값을 내포하는 보안에 대하여 다룹니다. *iSeries 보안 참조서*의 제 3 장은 모든 보안 관련 시스템 값에 대해 설명합니다.

네트워크 속성:

네트워크 속성은 시스템이 다른 시스템과 네트워크에 관여(또는 관여하지 않도록 선택)하는 방법을 제어합니다. 네트워크 속성에 대한 자세한 내용은 *작업 관리* 책을 참조하십시오.

서브시스템 설명 및 기타 작업 관리 요소:

작업 관리 요소는 작업이 시스템에 입력되는 방법 및 작업이 실행되는 환경을 판별합니다. 이 정보의 몇몇 주제에서 일부 작업 관리 값을 내포하는 보안에 대하여 다룹니다. *작업 관리* 책에 자세한 정보가 들어 있습니다.

통신 구성:

또한 통신 구성 작업이 사용자의 시스템에 입력되는 방법에 영향을 줍니다. 이 정보의 몇몇 주제에서 네트워크에 관여할 때 시스템을 보호하기 위한 제안사항이 제공됩니다.

사용자 프로파일

각 시스템 사용자에게는 **반드시** 사용자 프로파일이 있어야 합니다. 사용자가 사인 온 하기 전에 사용자 프로파일을 작성해야 합니다. 사용자 프로파일을 사용하여 DASD 및 주 기억장치 덤프와 같은 서비스 툴에 대한 액세스를 제어할 수도 있습니다. 자세한 내용은 68 페이지의 『서비스 툴 관리』를 참조하십시오.

사용자 프로파일은 강력하고 융통성있는 툴입니다. 사용자가 수행할 수 있는 사항을 제어하고 시스템이 사용자에게 표시하는 방법을 사용자 정의합니다. *iSeries 보안 참조서* 책은 사용자 프로파일에 있는 모든 매개변수를 설명합니다.

그룹 프로파일

그룹 프로파일은 사용자 프로파일의 특수 유형입니다. 그룹 프로파일을 사용하여 각 사용자 개인에게 권한을 부여하는 대신 사용자 그룹에 대한 권한을 정의할 수 있습니다. 또한 프로파일 복사 기능을 사용하여 개별 사용자 프로파일을 작성할 때 하나의 패턴으로 그룹 프로파일을 사용하거나 iSeries Navigator를 사용할 경우, 사용자 권한을 편집하기 위해 보안 정책 메뉴를 사용할 수 있습니다.

*iSeries 보안 참조서*의 제 5 장 및 제 7 장은 그룹 프로파일 계획 및 사용에 대한 자세한 내용을 제공합니다.

자원 보안

시스템의 자원 보안을 사용하여 오브젝트 사용자 및 해당 오브젝트 사용법을 정의할 수 있습니다. 오브젝트에 액세스할 수 있는 기능을 **권한**이라고 합니다. 오브젝트 권한을 설정할 때에는 사용자들에게 시스템을 검색하고 변경할 수 있는 권한을 부여하지 않고서도 사용자들이 작업하기에 충분한 권한을 부여해야 합니다. 오브젝트 권한은 사용자에게 특정 오브젝트를 위한 권한을 부여하고 오브젝트에 대해 사용자에게 허용되는 작업을 지정합니다. 오브젝트 자원은 레코드 추가나 레코드 변경과 같이 특정의 상세한 사용자 권한을 통해 제한시킬 수 있습니다. 시스템 자원은 특정의 시스템 정의 서브세트 권한(*ALL, *CHANGE, *USE, *EXCLUDE)에 사용자 액세스를 부여하기 위해 사용될 수 있습니다.

파일, 프로그램, 라이브러리 및 디렉토리는 자원 보안 보호를 필요로 하는 가장 일반적인 시스템 오브젝트이지만 시스템의 어느 오브젝트에 대해서나 권한을 지정할 수 있습니다.

제 5 장 『오브젝트 권한을 사용하여 정보 자산 보호』은 시스템의 오브젝트 권한 설정에 대한 중요성을 다룹니다. *iSeries 보안 참조서*의 제 5 장은 자원 보안을 설정하기 위한 옵션에 대해 설명합니다.

프로그램 기능에 대한 액세스 제한

프로그램 기능에 대한 제한 액세스는 프로그램 보안을 담당할 iSeries 오브젝트가 없을 때 프로그램에 보안을 제공할 수 있도록 해줍니다. 프로그램 기능에 대한 지정 액세스 지원이 V4R3에 추가되기 전에, 권한 부여 리스트나 기타 오브젝트를 작성하고, 오브젝트에 대한 권한 부여를 검사하여 프로그램 기능에 대한 액세스를 제어할 수 있습니다. 이제 프로그램 기능에 대한 액세스를 제한하여 어플리케이션, 어플리케이션의 일부 또는 프로그램 안의 기능을 보다 쉽게 제어할 수 있습니다.

iSeries Navigator를 통해 어플리케이션 기능에 대한 사용자 액세스를 관리할 수 있는 두 가지 방법이 있습니다. 첫 번째 방법은 관리 지원을 사용하는 것입니다.

1. 변경하려는 설정에 액세스하는 기능이 들어 있는 시스템을 마우스 오른쪽 버튼으로 클릭하십시오.
2. **어플리케이션 관리**를 선택하십시오.
3. 관리 시스템이 작동되면 **로컬 설정**을 선택하십시오. 그렇지 않으면, 다음 단계를 계속하십시오.
4. 관리 가능한 기능을 선택하십시오.
5. 적용 가능한 경우, **디폴트 액세스**를 선택하십시오. 이렇게 하면 모든 사용자가 디폴트로 해당 기능에 액세스할 수 있습니다.
6. 적용 가능한 경우, **모든 오브젝트 액세스**를 선택하십시오. 이렇게 하면 모든 오브젝트 시스템 권한이 있는 모든 사용자가 해당 기능에 액세스할 수 있습니다.
7. 적용 가능한 경우, **사용자 정의**를 선택하십시오. **사용자 정의 액세스** 대화 상자에서 **추가** 및 **제거** 버튼을 사용하여 **허용된 액세스** 및 **거부된 액세스** 리스트에서 사용자 또는 그룹을 추가하거나 제거하십시오.
8. 적용 가능한 경우, **사용자 정의 제거**를 선택하십시오. 이렇게 하여 선택된 기능의 사용자 정의된 액세스를 삭제합니다.
9. **확인**을 클릭하여 **어플리케이션 관리** 대화 상자를 닫으십시오.

사용자 액세스를 관리하는 두 번째 방법은 iSeries Navigator의 사용자 및 그룹 지원입니다.

1. iSeries Navigator에서 **사용자 및 그룹**을 펼치십시오.
2. **모든 사용자**, **그룹** 또는 **그룹에 없는 사용자**를 선택하여 사용자 및 그룹 리스트를 표시하십시오.
3. 사용자 또는 그룹을 마우스 오른쪽으로 클릭한 후 **등록 정보**를 선택하십시오.

4. **기능**을 클릭하십시오.
5. **어플리케이션** 탭을 클릭하십시오.
6. 해당 페이지를 사용하여 사용자 또는 그룹의 액세스 설정을 변경하십시오.
7. **확인**을 두 번 클릭하여 **등록 정보** 대화상자를 닫으십시오.

iSeries Navigator 보안 문제에 대한 자세한 내용은 171 페이지의 『iSeries Navigator 보안』을 참조하십시오.

어플리케이션 작성자인 경우 프로그램 기능 API에 대한 제한 액세스를 사용하여 다음을 수행할 수 있습니다.

- 기능 등록
- 기능에 대한 정보 검색
- 기능 사용자 및 사용할 수 없는 사용자 정의
- 기능을 사용할 수 있도록 허용된 사용자인지 검사

주: 이 지원은 자원 보안에 대한 대체가 **아닙니다**. 프로그램 기능에 대한 액세스 제한으로 사용자가 다른 인터페이스로부터 자원(파일 또는 프로그램과 같은)을 액세스할 수 없게 합니다.

어플리케이션에서 이 지원을 사용하려면 어플리케이션 제공자가 어플리케이션을 설치할 때 기능을 등록해야 합니다. 등록된 기능은 어플리케이션의 특정 기능에 대한 코드 블록과 대응합니다. 사용자가 어플리케이션을 실행할 경우, 어플리케이션이 코드 블록을 호출하기 전에 API를 호출합니다. API는 기능 사용이 허용된 사용자인지 확인하기 위하여 API 사용 검사를 호출합니다. 등록된 기능을 사용할 수 있는 사용자일 경우, 코드 블록이 실행됩니다. 기능 사용이 허용되지 않은 사용자일 경우, 사용자는 코드 블록을 실행할 수 없습니다.

주: API는 등록 데이터베이스(WRKREGINF)에 30자 기능 ID를 등록하는 것과 관련이 있습니다. 기능 API에 대한 제한 액세스가 사용하는 기능 ID와 관련된 종료점이 없는 경우에도 종료점이 필요합니다. 레지스트리에 무언가를 등록하려면 **반드시** 종료점 형식의 이름을 제공해야 합니다. 이렇게 하기 위해 레지스터 기능 API가 더미 형식 이름을 작성하고 등록되는 모든 기능의 더미 형식 이름을 사용합니다. 그 이유는 이것이 더미 형식명이므로 어떤 종료점 프로그램도 호출되지 않기 때문입니다.

시스템 관리자는 기능에 대해 액세스하도록 허용 또는 거부된 사용자를 지정합니다. 관리자는 API를 사용하여 프로그램 기능에 대한 액세스를 관리하거나 iSeries Navigator 어플리케이션 관리 GUI를 사용할 수 있습니다. *iSeries 서버 API 참조서* 책은 프로그램 기능 API에 대한 제한 액세스에 대한 정보를 제공합니다. 기능 액세스 제어에 대한 자세한 내용은 171 페이지의 『iSeries Navigator 보안』을 참조하십시오.

보안 감사

시스템 보안을 감사하는 이유는 다음과 같습니다.

- 보안 계획이 완벽한지 여부를 평가하기 위해.
- 계획된 보안 제어가 제 자리를 잡고 작동 중인지 확인하기 위해. 이런 유형의 감사는 대개 일일 보안 관리의 일부로서 보안 담당자에 의해 수행됩니다. 또한 때로는 더 자세하게 내부 또는 외부 감사자에 의해 주기적인 보안 검토의 일부로서 수행됩니다.
- 시스템 보안이 시스템 환경의 변화에 따라가고 있는지를 확인하기 위해. 보안에 영향을 주는 변경의 몇 가지 예는 다음과 같습니다.
  - 시스템 사용자가 작성한 새 오브젝트
  - 시스템에 들어온 새로운 사용자
  - 오브젝트 소유권의 변경(권한 부여는 조정되지 않음)
  - 책임 변경(사용자 그룹 변경)
  - 임시 권한(시기 적절하게 철회되지 않음)
  - 설치된 새 제품
- 새 어플리케이션 설치, 상위 보안 레벨로의 이동 또는 통신 네트워크 설정과 같은 장차 발생할 수 있는 이벤트에 준비하기 위해.

여기에서는 이러한 모든 상황에 적합한 기술이 설명됩니다. 사용자가 감사하는 대상과 빈도는 조직의 규모와 보안 수요에 따라 다릅니다.

보안 감사에는 시스템에 대한 명령 사용 및 기록부 및 저널 정보 액세스가 포함됩니다. 시스템의 보안 감사를 수행할 사람이 사용할 특수 프로파일을 작성할 수 있습니다. 감사자 프로파일에는 시스템에 대한 감사 특성을 변경하기 위한 *AUDIT 특수 권한이 필요합니다. 이 장에서 제안되는 감사 타스크의 일부는 *ALLOBJ 및 *SECADM 특수 권한을 갖는 사용자 프로파일이 필요합니다. 감사 기간이 종료했을 때 반드시 감사자 프로파일에 대한 암호를 *NONE으로 설정하십시오.

보안 감사에 대한 자세한 내용은 *보안 참조서* 책의 제 9 장을 참조하십시오.

예: 시스템 보안 속성 보고서

9 페이지의 그림 1은 PRTSYSSECA(시스템 보안 속성 인쇄) 명령 출력의 한 예를 보여줍니다. 보고서는 정상적인 보안 요구사항을 갖는 시스템에 대해 권장되는 보안 관련 시스템 값 및 네트워크 속성에 대한 설정을 표시합니다. 또한 사용자 시스템의 현재 설정을 표시합니다.

주: 보고서의 *현재 값* 열은 시스템의 현재 설정을 표시합니다. 이 값을 권장 값과 비교하여 보안 노출 가능성이 있는지 확인하십시오.

시스템 보안 속성

```
시스템 값
이름            현재 값              권장 값
QALWOBJRST      *NONE                *NONE
QALWUSRDMN      *ALL                 QTEMP
QATNPGM         QEZMAIN   QSYS       *NONE
QAUDENDACN      *NOTIFY              *NOTIFY
QAUDFRCLVL      *SYS                 *SYS
QAUDCTL         *AUDLVL              *AUDLVL   *OBJAUD
QAUDLVL         *SECURITY            *AUTFAIL  *CREATE
                                     *DELETE   *SECURITY
                                     *SAVRST   *NOQTEMP
```

그림 1. 시스템 보안 속성 보고서-예 (1/4)

```
QAUTOCFG        0                    0
QAUTORMT        1                    0
QAUTOVRT        9999                 0
QCMNRCYLMT      0 0                  0 0
QCRTAUT         *CHANGE              Control at library level.
QCRTOBJAUD      *NONE                Control at library level.
QDEVRCYACN      *DSCMSG              *DSCMSG
QDSCJOBITV      120                  120
QDSPSGNINF      1                    1
QINACTITV       60                   60
QINACTMSGQ      *ENDJOB              *ENDJOB
QLMTDEVSSN      0                    1
QLMTSECOFR      0                    1
QMAXSGNACN      2                    3
QMAXSIGN        3                    3
```

그림 1. 시스템 보안 속성 보고서-예 (2/4)

```
QPWDEXPITV      60                   60
QPWDLMTAJC      1                    1
QPWDLMTCHR      *NONE                AEIOU@$#
QPWDLMTREP      1                    2
QPWDLVL         0
QPWDMAXLEN      8                    8
QPWDMINLEN      6                    6
QPWDPOSDIF      1                    1
QPWDRQDDGT      1                    1
QPWDRQDDIF      0                    1
QPWDVLDPGM      *NONE                *NONE
QRETSVRSEC      0                    0
QRMTIPL         0                    0
QRMTSIGN        *FRCSIGNON           *FRCSIGNON
QSECURITY       50                   50
QSHRMEMCTL      1                    0
QSRVDMP         *DMPUSRJOB           *NONE
QUSEADPAUT      *NONE                CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                     CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                     CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST      1                    3
```

그림 1. 시스템 보안 속성 보고서-예 (3/4)

시스템 보안 속성

네트워크 속성

이름	현재 값	권장 값
DDMACC	*OBJAUT	*REJECT
JOBACN	*FILE	*REJECT
PCSACC	*OBJAUT	*REJECT

그림 1. 시스템 보안 속성 보고서-예 (4/4)

제 2 장 iSeries 보안 마법사 및 eServer 보안 플래너

iSeries 서버 보안 마법사와 eServer 보안 플래너를 이용하여 iSeries 서버에 적용할 보안 값을 결정할 수 있습니다. iSeries Navigator에서 iSeries 서버 보안 마법사를 사용하여 선택한 응답을 기반으로 하는 사용자의 보안 요구를 반영한 보고서를 작성합니다. 그러고 나서 이 보고서를 사용하여 시스템 보안을 구성할 수 있습니다.

iSeries 서버의 기본 보안 정책을 계획하고 구현하는 데 도움이 되도록 iSeries 보안 마법사나 eServer 보안 플래너를 사용하십시오. 모든 툴의 목표는 사용자가 시스템에서 보안을 보다 쉽게 구현하고 관리하는 것입니다. OS/400®의 일부로 사용할 수 있는 마법사는 사용자의 응답을 기반으로 서버 환경에 대한 여러 상위 레벨 질문을 요청하고 해당 마법사가 사용자 시스템에 바로 적용할 수 있는 권장사항 세트를 제공합니다.

eServer 보안 플래너는 보안 마법사의 온라인 버전입니다. 이는 보안 요구를 기초로 선택사항을 선택하도록 한 다음, 사이트 보안에 필요한 피처를 제안하는 보고서를 제공합니다.

eServer 보안 플래너는 마법사의 웹 기반 버전입니다. 마법사가 하는 것처럼 시스템에서 보안 구현에 대한 권장사항을 제공합니다. 그러나 어드바이저는 권장사항을 적용할 수 없습니다. 오히려 어드바이저의 질문에 대한 응답을 기반으로 해당 시스템에 적용해야 하는 시스템 보안 값 및 다른 속성 리스트를 출력합니다.

보안 마법사

비즈니스에 사용해야 할 iSeries 보안 시스템 값 결정은 복잡할 수 있습니다. iSeries 서버에서 보안 구현을 처음 사용하거나 iSeries 서버를 실행시키는 환경이 최근에 변경된 경우, 보안 마법사가 결정에 도움을 줄 수 있습니다.

마법사란 무엇인가?

- 마법사는 시스템에 무언가를 설치하거나 구성해야 하는 초보 사용자가 실행할 수 있도록 설계된 툴입니다.
- 마법사는 질문을 통해 사용자에게 정보를 프롬트합니다. 각 질문에 대한 응답이 다음 질문 내용을 결정합니다.
- 마법사가 모든 질문을 완료하면 사용자에게 완료 패널을 표시합니다. 그러고 나서 사용자가 **완료** 버튼을 누르면 항목의 설치 및 구성이 이루어집니다.

보안 마법사의 목표

보안 마법사의 목적은 다음 항목에 대한 사용자 응답을 기초로 구성을 수행하는 것입니다.

- 보안 관련 시스템 값 및 네트워크 속성
- 시스템 모니터링을 위한 보안 관련 보고
- 관리자 정보 보고서 및 사용자 정보 보고서를 생성하려면 다음과 같이 하십시오.
  - 관리자 정보 보고서에는 수행하기 전에 따라야 할 권장 절차 및 보안 설정이 포함됩니다.
  - 사용자 정보 보고서에는 업무 보안 방침에 사용할 수 있는 정보가 포함됩니다. 예를 들면, 이 보고서에 암호 구성 규칙이 포함되어 있습니다.
- 시스템상의 다양한 보안 관련 항목에 대해 권장된 설정값을 제공하려면 다음과 같이 하십시오.

보안 마법사의 목표

- 보안 마법사의 목표는 다음과 같습니다.
  - 마법사의 질문에 대한 사용자 응답을 기초로 시스템 보안 설정을 판별한 다음 적절한 때에 설정을 실행합니다.
  - 마법사는 다음 항목을 포함하여 자세한 정보 보고서를 작성합니다.
    - 마법사의 권장사항을 설명하는 보고서
    - 실행 전에 따라야 하는 프로시듀어에 관한 자세한 보고서
    - 시스템 사용자에게 분배할 해당 정보를 나열한 보고서
- 이들 항목은 사용자 시스템상에서 기본적인 보안 방침이 구현되도록 합니다.
- 마법사는 감사 저널 보고서를 정기적으로 실행하도록 권장합니다. 정기 실행 스케줄을 작성할 경우, 보고서를 통해 다음과 같은 도움을 받을 수 있습니다.
  - 보안 방침을 따르게 됩니다.
  - 보안 방침은 사용자 승인이 있어야만 변경되도록 합니다.
  - 시스템상에서의 보안 관련 이벤트를 모니터하는 보고서를 스케줄합니다.
- 마법사는 권장사항을 저장하거나 시스템에 전체 권장사항 또는 그 일부를 적용할 수 있도록 해줍니다.

주: 보안 마법사는 같은 시스템에 여러 번 사용이 가능하므로 이전에 설치한 사용자들이 현재 보안을 검토할 수 있습니다. 보안 마법사는 V3R7 시스템(iSeries Navigator가 도입된 시기) 이상의 시스템에서 사용할 수 있습니다.

iSeries Navigator를 사용하려면 Windows®용 IBM iSeries Access가 Windows 95/NT PC에 설치되어 있고 iSeries 서버가 이 PC에 연결되어 있어야 합니다. 마법사의 사용자가 iSeries 서버에 연결되어야 합니다. 그리고 사용자에게 *ALLOBJ, *SECADM, *AUDIT, *IOSYSCFG 특수 권한의 사용자 ID가 반드시 있어야 합니다. Windows 95/NT PC를 iSeries 시스템에 연결할 때 도움을 받으려면, Information Center의 Windows용 IBM iSeries Access 주제를 참조하십시오(자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』 참조).

보안 마법사에 액세스하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 서버를 펼치십시오.

2. **보안**을 마우스 오른쪽으로 클릭한 후 **구성**을 선택하십시오.
   - 사용자가 iSeries Navigator의 **보안** 옵션을 시작할 때 사용자의 특수 권한을 검사하기 위한 요청이 iSeries 서버로 송신됩니다.
   - 사용자가 필요한 모든 특수 권한(*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM)이 없으면, **구성** 옵션이 표시되지 않으며 보안 마법사에 액세스할 수 없습니다.
3. 사용자에게 필수 권한이 있다고 가정하면,
   - 이전의 마법사 응답이 검색됩니다.
   - 현재 보안 설정이 검색됩니다.

보안 마법사는 세 가지 시작 화면 중 하나를 표시합니다. 나타나는 화면은 다음 중 어떤 상황인지에 따라 달라집니다.

- 마법사가 목표 iSeries 서버에 대해 실행된 적이 없습니다.
- 마법사가 이전에 실행되었고 보안 변경이 연기되었습니다.
- 마법사가 이전에 실행되었고 보안 변경이 수행되었습니다.

iSeries Navigator를 사용하지 않더라도 사용자의 보안 요구를 위한 계획 도움말을 구할 수 있습니다. eServer 보안 플래너는 보안 마법사의 온라인 버전으로 한 가지 차이점이 있습니다. 어드바이저는 시스템을 자동으로 구성하지 않습니다. 그러나 사용자 응답을 기초로 권장 보안 옵션의 보고서를 생성합니다. eServer 보안 플래너에 액세스하려면, 다음 eServer Information Center를 방문하십시오.

`http://publib.boulder.ibm.com/eserver/`

eServer 보안 플래너

eServer 보안 플래너는 보안 마법사의 온라인 버전입니다. 보안 어드바이저는 보안 마법사와 동일한 질문을 하고 사용자 응답을 기초로 동일한 권장사항을 제시합니다. 두 가지 툴간의 주된 차이점은 다음과 같습니다.

- eServer 보안 플래너는 다음을 수행하지 **않습니다**.
  - 보고서 생성
  - 현재 설정과 권장 설정의 비교
  - 시스템 값 자동 설정
- eServer 보안 플래너로부터 권장사항을 적용할 수 없습니다.

eServer 보안 플래너는 보안 구성 자동화에 사용하기 위해 잘라 붙이고 편집할 수 있는 CL 프로그램을 생성합니다. eServer 보안 플래너로부터 iSeries 서버 문서에 직접 연결할 수도 있습니다. 이 설정이 사용자 환경에 적절한지 판별할 수 있는 시스템 값 또는 보고서에 대한 정보를 제공합니다.

eServer 보안 플래너에 액세스하려면 인터넷 브라우저에서 다음 URL로 이동하십시오.

http://publib.boulder.ibm.com/eserver/

제 3 장 대화식 사인 온 제어

시스템에 대한 항목을 제한하려면 사인 온 화면에서 시작하십시오. 다음은 누군가가 사인 온 화면을 통해 시스템에 사인 온하는 것을 어렵게 하기 위한 옵션입니다.

암호 규칙 설정

시스템 사인 온을 보안하려면 다음과 같이 하십시오.

- 단순하지 않고 공유되지 않는 암호 방침을 설정하십시오.
- 시스템 값을 설정하십시오. 표 1은 권장 시스템 값 설정을 나타냅니다.

표 1의 값 조합은 매우 제한적이며 단순 암호와의 유사성을 줄이기 위한 것입니다. 그러나 사용자에게는 이러한 제한사항에 알맞는 암호를 선택하는 것이 매우 어려운 일입니다.

사용자에게 다음을 제공하는 것이 좋습니다.

1. 암호 기준 리스트
2. 유효 암호 및 유효하지 않은 암호의 예
3. 좋은 암호를 생각하는 방법에 대한 제안

CFGSYSSEC(시스템 보안 구성) 명령을 실행하여 다음 값을 설정하십시오. PRTSYSSECA(시스템 보안 속성 인쇄) 명령을 사용하여 이러한 시스템 값에 대한 현재 설정을 인쇄하십시오.

iSeries 보안 참조서 책의 제 3 장. 40 페이지의 『시스템 보안 구성 명령으로 설정된 값』에서 CFGSYSSEC 명령에 대한 추가 정보를 제공합니다.

표 1. 암호에 대한 시스템 값

시스템 값 이름	설명	권장값
QPWDEXPITV	시스템 사용자가 암호를 변경해야 하는 빈도. 사용자 프로파일의 개별 사용자에 대하여 다른 값을 지정할 수 있습니다.	60(일)
QPWDLMTAJC	동일 문자의 인접 금지 여부	1(예)
QPWDLMTCHR	암호에 사용될 수 없는 문자.[2]	AEIOU#$@
QPWDLMTREP	암호에 동일 문자를 두 번 이상 표시 금지 여부	2(연속 불가)
QPWDLVL	사용자 프로파일 암호가 10자 또는 최대값인 128자로 제한되는지 여부.	0[3]
QPWDMAXLEN	암호의 최대 문자 수	8
QPWDMINLEN	암호의 최소 문자 수	6
QPWDPOSDIF	암호의 각 문자가 이전 암호에서 같은 위치에 있는 문자와 달라야 하는지의 여부	1(예)
QPWDRQDDGT	암호에 최소한 한 개의 숫자가 포함되어야 하는지의 여부	1(예)
QPWDRQDDIF	동일한 암호를 다시 사용하기 위한 기간.[2]	5이하(만기 간격)[1]

표 1. 암호에 대한 시스템 값 (계속)

시스템 값 이름	설명	권장값
QPWDVLDPGM	새로 지정된 암호의 유효성을 검사하기 위하여 호출하는 나감 프로그램	*NONE

주:

1. QPWDEXPITV 시스템 값은 암호를 변경해야 하는 빈도(예: 60일마다)를 지정합니다. 이것이 **만기 간격**입니다. QPWDRQDDIF 시스템 값은 같은 암호를 다시 사용하기까지 경과해야 하는 만기 간격을 지정합니다. *iSeries 보안 참조서*의 제 3 장에서는 이러한 시스템 값으로 작업하는 방법에 대한 정보를 제공합니다.
2. QPWDLMTCHR은 암호 레벨 2 또는 3에서 강제되지 않습니다. 자세한 내용은 『암호 레벨』을 참조하십시오.
3. 사용자에게 꼭 맞는 암호 레벨을 판별하려면 17 페이지의 『암호 레벨 변경 계획』을 참조하십시오.

암호 레벨

오퍼레이팅 시스템의 V5R1을 시작하여 QPWDLVL 시스템 값이 증가된 암호 보안을 제공합니다. 이전 릴리스에서는 사용자들이 문자 범위의 제한으로부터 10자 이하의 암호로 제한되었습니다. 이제는 사용자들이 자신의 시스템이 설정되는 암호 레벨에 따라서 최대 128자까지의 암호(또는 passphrase)를 선택할 수 있습니다. 암호 레벨은 다음과 같습니다.

- **레벨 0:** 이 레벨에서 시스템이 출하됩니다. 레벨 0에서, 암호는 10자 이하이며 A - Z, 0 - 9, #, @, $ 및 _ 문자만을 포함합니다. 레벨 0의 암호는 상위 암호 레벨에 있는 암호보다 보안성이 낮습니다.
- **레벨 1:** 암호 레벨 0과 동일한 규칙을 갖지만 Windows Network Neighborhood의 iSeries 지원에 대한 암호(이후에 iSeries NetServer라고도 함)가 저징되지 않습니다.
- **레벨 2:** 이 레벨에서 암호를 보안합니다. 이 레벨은 테스트 목적으로 사용할 수 있습니다. 암호가 10자 이하이고 레벨 0 또는 1 암호의 문자 세트를 사용하는 경우 레벨 0 또는 1 암호에서 사용자에 대해 저장됩니다. 이 레벨에 있는 암호(또는 passphrases)는 다음 특성을 갖습니다.
  - 최대 128자까지 가능합니다.
  - 사용할 수 있는 모든 키보드 문자로 구성됩니다.
  - 공백만으로 구성될 수 없습니다. 공백은 암호의 끝에서 제거됩니다.
  - 대소문자를 구분합니다.
- **레벨 3:** 이 레벨의 암호는 가장 안전하며, 사용할 수 있는 가장 첨단의 암호화 알고리즘을 이용합니다. 이 레벨의 암호는 레벨 2의 암호와 동일한 특성을 갖습니다. iSeries NetServer에 대한 암호는 이 레벨에서 저장되지 않습니다.

네트워크에서 모든 시스템이 다음 기준과 일치하는 경우 암호 레벨 2와 3만 사용해야 합니다.

- 오퍼레이팅 시스템이 V5R1 이상

- 암호 레벨을 2 또는 3으로 설정

마찬가지로, 사용자들은 모두 동일한 암호 레벨을 사용하여 로그인해야 합니다. 암호 레벨은 글로벌입니다. 즉, 사용자가 자신의 암호를 보안하기 원하는 정도의 레벨을 선택할 수 없습니다.

암호 레벨 변경 계획

암호 레벨 변경은 주의해서 계획해야 합니다. 암호 레벨 변경을 충분히 계획하지 않으면 다른 시스템과의 조작이 실패하거나 사용자들이 시스템에 사인 온하지 못할 수 있습니다. QPWDLVL 시스템 값을 변경하기 전에, SAVSECDTA 또는 SAVSYS 명령을 사용하여 보안 자료를 저장하십시오. 현재 백업이 있으면, 하위 암호 레벨로 리턴해야 하는 경우 모든 사용자의 프로파일에 대한 암호를 재설정할 수 있습니다.

암호 레벨(QPWDLVL) 시스템 값이 2 또는 3으로 설정될 때 사용자가 시스템 및 시스템이 인터페이스하는 클라이언트에서 사용하는 제품에 문제가 있을 수 있습니다. 사용자가 사인 온 화면에 입력하는 명백한 텍스트가 아니라 암호화된 형식으로 시스템에 암호를 송신하는 모든 제품 또는 클라이언트가 QPWDLVL 2 또는 3에 대한 새 암호 암호화 규칙에 대해 작업하도록 업그레이드되어야 합니다. 암호화된 암호를 송신하는 것을 **암호 대체**라고 합니다.

암호 대체는 암호가 네트워크에서의 전송 중에 캡처되지 않도록 하는데 사용됩니다. 특정 문자가 올바른 경우에도 QPWDLVL 2 또는 3에 대한 새 알고리즘을 지원하지 않는 이전 클라이언트에 의해 생성되는 암호 대체는 허용되지 않습니다. 이것은 또한 한 시스템에서 다른 시스템을 인증하기 위해 암호화된 값을 이용하는 모든 iSeries 대 iSeries 대등 액세스에도 적용됩니다.

일부 영향을 받는 제품(Java Toolbox와 같은)이 미들웨어로 제공된다는 사실로 인해 문제가 발생됩니다. 이들 제품 중 하나의 이전 버전과 협동하는 다른 회사 제품은 갱신된 미들웨어 버전을 사용하여 리빌드될 때까지 올바르게 작동하지 않을 것입니다.

이 시나리오와 다른 시나리오에서, QPWDLVL 시스템 값을 변경하기 전에 주의깊은 계획 수립이 필요한 이유는 명백합니다.

0에서 1로 QPWDLVL 변경에 대한 고려사항

암호 레벨 1은 Windows 95/98/ME AS/400® Client Support for Windows Network Neighborhood(iSeries NetServer) 제품과 통신할 필요가 없는 시스템이 시스템에서 iSeries NetServer 암호를 제거할 수 있게 합니다. 시스템에서 불필요한 암호화된 암호를 제거하면 시스템의 전체적인 보안이 증가됩니다.

QPWDLVL 1에서, 현재의 모든 V5R1 이전 암호 대체 및 암호 인증 메카니즘이 계속 작동합니다. iSeries NetServer 암호가 필요한 기능 및 서비스를 제외하고는 침입의 가능성이 거의 없습니다.

0 또는 1에서 2로 QPWDLVL 변경에 대한 고려사항

암호 레벨 2는 최고 128자의 대소문자 구분 암호(passphrase라고도 함)의 사용을 도입하며 QPWDLVL 0 또는 1로 복귀하는 최대 능력을 제공합니다.

시스템의 암호 레벨과 상관없이, 암호 레벨 2 및 3 암호는 암호가 변경되거나 사용자가 시스템에 사인 온할 때마다 작성됩니다. 시스템이 여전히 암호 레벨 0 또는 1에 있는 동안 레벨 2 및 3 암호가 작성되도록 하면 암호 레벨을 2 또는 3으로 변경하기 위한 준비에 도움이 됩니다.

QPWDLVL을 2로 변경하기 전에, DSPAUTUSR 또는 PRTUSRPRF TYPE(*PWDINFO) 명령을 사용하여 암호 레벨 2에서 사용할 수 있는 암호가 없는 모든 사용자 프로파일을 찾아야 합니다. 이들 명령이 위치한 프로파일에 따라, 다음 메카니즘 중 하나를 사용하여 암호 레벨 2 및 3이 프로파일에 추가되도록 할 수 있습니다.

- CHGUSRPRF 또는 CHGPWD CL 명령 또는 QSYCHGPW API를 사용하여 사용자 프로파일에 대한 암호를 변경하십시오. 이것은 시스템이 암호 레벨 0과 1에서 사용할 수 있는 암호를 변경하도록 만듭니다. 또한 시스템은 암호 레벨 2와 3에서 사용할 수 있는 두 개의 동등한 대소문자 구분 암호를 작성합니다. 암호의 모두 대문자 및 모두 소문자 버전이 암호 레벨 2 또는 3에서 사용하기 위해 작성됩니다.

  예를 들어, 암호를 C4D2RB4Y로 변경하면 시스템이 C4D2RB4Y 및 c4d2rb4y 암호 레벨 2 암호를 생성합니다.
- 텍스트로 암호를 제공하는(암호 대체를 사용하지 않는) 메카니즘을 통해 시스템에 사인 온하십시오. 암호가 유효하고 사용자 프로파일이 암호 레벨 2와 3에서 사용할 수 있는 암호를 갖지 않는 경우, 시스템은 암호 레벨 2와 3에서 사용할 수 있는 두 개의 동등한 대소문자 구분 암호를 작성합니다. 암호의 모두 대문자 및 모두 소문자 버전이 암호 레벨 2 또는 3에서 사용하기 위해 작성됩니다.

암호 레벨 2 또는 3에서 사용할 수 있는 암호가 없는 것은 사용자 프로파일도 암호 레벨 0과 1에서 사용할 수 있는 암호가 없을 때마다 또는 사용자가 암호 대체를 사용하는 제품을 통해 사인 온하려고 시도할 때 문제가 될 수 있습니다. 이러한 경우에, 암호 레벨이 2로 변경될 때 사용자가 사인 온할 수 없게 됩니다.

사용자 프로파일에 암호 레벨 2와 3에서 사용할 수 있는 암호가 없고, 사용자 프로파일이 암호 레벨 0과 1에서 사용할 수 있는 암호를 갖고 사용자가 투명한 텍스트 암호를 송신하는 제품을 통해 사인 온하는 경우, 시스템은 암호 레벨 0 암호에 대해 사용자를 유효성 확인하고 해당 사용자 프로파일에 대해 두 개의 암호 레벨 2 암호(위에서 설명한 것처럼)를 작성합니다. 후속 사인 온은 암호 레벨 2 암호에 대해 유효성 확인됩니다.

암호 대체를 사용하는 모든 클라이언트/서비스는 해당 클라이언트/서비스가 새 암호(passphrase) 대체 체계를 사용하도록 갱신되지 않은 경우 QPWDLVL 2에서 올바르게 작동하지 않습니다. 관리자는 새 암호 대체 체계로 갱신되지 않은 클라이언트/서비스가 필요한지 여부를 검사해야 합니다.

암호 대체를 사용하는 클라이언트/서비스에는 다음이 포함됩니다.

- TELNET
- iSeries Access
- iSeries 호스트 서버
- QFileSrv.400
- iSeries NetServer 인쇄 지원
- DDM
- DRDA®
- SNA LU6.2

QPWDLVL 2로 변경하기 전에 보안 자료를 저장할 것을 강력하게 권장합니다. 이렇게 하면 QPWDLVL 0 또는 1로의 역방향 변환이 필요하게 되는 경우 변환을 더 쉽게 만드는데 도움이 됩니다.

QPWDLVL 2에서의 일부 테스트가 발생한 이후까지는 QPWDMINLEN 및 QPWDMAXLEN과 같이 다른 암호 시스템 값이 변경되지 않는 것이 좋습니다. 이것은 필요한 경우 QPWDLVL 1 또는 0으로의 역방향 변환을 더 쉽게 만듭니다. 그러나 QPWDVLDPGM 시스템 값은 시스템이 QPWDLVL이 2로 변경되도록 허용하기 전에 *REGFAC 또는 *NONE을 지정해야 합니다. 따라서 암호 유효성 프로그램을 사용하는 경우, ADDEXITPGM 명령을 사용하여 QIBM_QSY_VLD_PASSWRD 종료점에 대해 등록될 수 있는 새 프로그램을 작성하기 원할 것입니다.

iSeries NetServer 암호가 QPWDLVL 2에서 여전히 지원되므로, iSeries NetServer 암호가 필요한 모든 기능/서비스는 여전히 올바르게 기능해야 합니다.

관리자가 QPWDLVL 2에서 시스템을 실행하는 데 익숙해지면, 더 긴 암호를 전개하기 위해 암호 시스템 값을 변경하기 시작할 수 있습니다. 그러나, 관리자는 더 긴 암호가 다음과 같은 영향을 미친다는 점을 유의해야 합니다.

- 10자 이상의 암호가 지정되면, 암호 레벨 0 및 1 암호가 지워집니다. 시스템이 암호 레벨 0 또는 1로 리턴하는 경우 이 사용자 프로파일은 사인 온할 수 없습니다.
- 암호에 특수 문자가 들어 있거나 단순 오브젝트명(대소문자 구분 제외)에 대한 조합 규칙을 따르지 않는 경우, 암호 레벨 0 및 1 암호가 지워집니다.
- 15자 이상의 암호가 지정되는 경우, 사용자 프로파일에 대한 iSeries NetServer 암호가 지워집니다.

- 암호 시스템 값은 새 암호 레벨 2 값에만 적용되며 시스템이 생성하는 암호 레벨 0 과 1 암호 또는 iSeries NetServer 암호 값(생성되는 경우)에는 적용되지 않습니다.

2에서 3으로 QPWDLVL 변경에 대한 고려사항

얼마 동안 QPWDLVL 2에서 시스템을 실행한 후, 관리자는 암호 보안 보호를 극대화하기 위해 QPWDLVL 3으로의 이동을 고려할 수 있습니다.

QPWDLVL 3에서, 모든 iSeries NetServer 암호가 지워지므로 시스템은 iSeries NetServer 암호를 사용할 필요가 없을 때까지 QPWDLVL 3으로 이동하지 말아야 합니다.

QPWDLVL 3에서, 모든 암호 레벨 0 및 1 암호는 지워집니다. 관리자는 DSPAUTUSR 또는 PRTUSRPRF 명령을 사용하여 암호 레벨 2 또는 3 암호가 연관되지 않은 사용자 프로파일을 찾을 수 있습니다.

하위 암호 레벨로의 변경

가능한 경우 하위 QPWDLVL 값으로 리턴하는 것이 쉬운 것은 아닙니다. 일반적으로, 하위 QPWDLVL 값에서 상위 QPWDLVL 값으로 바꾼 경우 복귀는 거의 불가능합니다. 그러나, 하위 QPWDLVL 값이 복귀되어야 하는 경우가 있을 수 있습니다.

다음 섹션은 각각 하위 암호 레벨로 되돌아가는데 필요한 작업을 설명합니다.

QPWDLVL 3에서 2로의 변경에 대한 고려사항: 이 변경은 상대적으로 쉽습니다. QPWDLVL이 2로 설정되면, 관리자는 iSeries NetServer 암호 또는 암호 레벨 0 또는 1 암호를 포함해야 하는 사용자 프로파일이 있는지를 판별해야 하며, 그 경우 사용자 프로파일의 암호를 허용 가능한 값으로 변경해야 합니다.

또한, 암호 시스템 값이 iSeries NetServer 및 암호 레벨 0 또는 1 암호와 호환되는 값으로 다시 변경되어야 할 것입니다(그런 암호가 필요한 경우).

QPWDLVL 3에서 1 또는 0으로의 변경에 대한 고려사항: 시스템에 대한 문제(모든 암호 레벨 0 및 1 암호가 지워졌기 때문에 누구도 사인 온할 수 없는 경우와 같이)를 유발할 가능성이 아주 크기 때문에, 이 변경은 직접 지원되지 않습니다. QPWDLVL 3에서 QPWDLVL 1 또는 0으로 변경하려면, 시스템이 먼저 QPWDLVL 2로의 중간 변경을 수행해야 합니다.

QPWDLVL 2에서 1로의 변경에 대한 고려사항: QPWDLVL을 1로 변경하기 전에, 관리자는 DSPAUTUSR 또는 PRTUSRPRF TYPE(*PWDINFO) 명령을 사용하여 암호 레벨 0 또는 1 암호가 없는 모든 사용자 프로파일을 찾아야 합니다. QPWDLVL이 변경된 후에 사용자 프로파일에 암호가 필요할 경우, 관리자는 다음 메카니즘 중 하나를 사용하여 해당 프로파일에 대한 암호 레벨 0 및 1 암호가 작성되도록 해야 합니다.

- CHGUSRPRF 또는 CHGPWD CL 명령 또는 QSYCHGPW API를 사용하여 사용자 프로파일에 대한 암호를 변경하십시오. 이것은 시스템이 암호 레벨 2과 3에서 사용할 수 있는 암호를 변경하도록 만듭니다. 또한 시스템은 암호 레벨 0와 1에서 사용할 수 있는 동등한 대문자 암호를 작성합니다. 다음 조건이 만족되는 경우에만 시스템은 암호 레벨 0 및 1 암호를 작성할 수 있습니다.
  - 암호가 10자 이하입니다.
  - 암호가 대문자 EBCDIC 문자 A - Z, 0 - 9, @, #, $ 및 밑줄로 변환될 수 있습니다.
  - 암호가 숫자 또는 밑줄 문자로 시작하지 않습니다.

  예를 들어, 암호를 RainyDay의 값으로 변경하면 시스템은 RAINYDAY라는 암호 레벨 0 및 1 암호를 생성합니다. 그러나 Rainy Days In April에 대한 암호 값을 변경하면 시스템은 암호 레벨 0 및 1 암호를 지웁니다(암호가 너무 길고 공백을 포함하기 때문입니다).

  암호 레벨 0 또는 1 암호가 작성될 수 없는 경우 메세지나 표시가 생성되지 않습니다.
- 텍스트로 암호를 제공하는(암호 대체를 사용하지 않는) 메카니즘을 통해 시스템에 사인 온하십시오. 암호가 유효하고 사용자 프로파일에 암호 레벨 0과 1에서 사용할 수 있는 암호가 없는 경우, 시스템은 암호 레벨 0와 1에서 사용할 수 있는 동등한 대문자 암호를 작성합니다. 위에서 나열된 조건이 만족되는 경우에만 시스템은 암호 레벨 0 및 1 암호를 작성할 수 있습니다.

그런 다음 관리자는 QPWDLVL을 1로 변경할 수 있습니다. iSeries QPWDLVL 1로의 변경이 효력을 가질 때(다음 IPL) 모든 NetServer 암호가 지워집니다.

QPWDLVL 2에서 0으로의 변경에 대한 고려사항: 변경이 효력을 가질 때 모든 iSeries NetServer 암호가 보유된다는 점을 제외하면 고려사항은 QPWDLVL 2에서 1로 변경하는 것과 같습니다.

QPWDLVL 1에서 0으로의 변경에 대한 고려사항: QPWDLVL을 0으로 변경한 후, 관리자는 DSPAUTUSR 또는 PRTUSRPRF 명령을 사용하여 iSeries NetServer 암호가 없는 모든 사용자 프로파일을 찾아야 합니다. 사용자 프로파일에 iSeries NetServer 암호가 필요한 경우, 사용자의 암호를 변경하거나 암호 대체를 사용하지 않고 텍스트로 암호를 제공하는 메카니즘을 통해 사인 온하여 암호를 작성할 수 있습니다.

그런 다음 관리자는 QPWDLVL을 0으로 변경할 수 있습니다.

알려진 암호 변경

다음을 수행하여 시스템에 잘 알려진 iSeries 서버 통로를 닫으십시오.

__ 단계 1. 사용자 프로파일에 디폴트 암호(사용자 프로파일명과 동일한)가 없도록 하십시오. ANZDFTPWD(디폴트 암호 분석) 명령을 사용할 수 있습니다(27 페이지의 『디폴트 암호 방지』를 참조하십시오).

__ 단계 2. 표 2에 표시된 사용자 프로파일과 암호 조합으로 시스템을 사인 온해 보십시오. 이러한 암호는 널리 알려져 있으므로 시스템 침입자가 가장 먼저 이러한 암호를 선택합니다. 사용자가 사인 온할 경우, CHGUSRPRF(사용자 프로파일 변경) 명령을 사용하여 암호를 권장 값으로 변경하십시오.

__ 단계 3. DST(전용 서비스 툴)를 시작하여 표 2에 표시된 암호로 사인 온을 시도하십시오. iSeries Information Center --> 보안 --> 서비스 툴을 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

__ 단계 4. 이들 암호 중 하나로 DST에서 사인 온할 경우, 암호를 변경해야 합니다. iSeries Information Center --> 보안 --> 서비스 툴은 서비스 툴 사용자 ID 및 암호를 변경하는 방법에 대한 자세한 지침을 제공합니다. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

__ 단계 5. 마지막으로, 사용자 ID 및 암호를 입력하지 않고, 사인 온 화면에서 Enter 키만 눌러 사인 온할 수 있는지 확인하십시오. 다른 여러 화면에서 사용해 보십시오. 사인 온 화면에 정보를 입력하지 않고 사인 온하려면 다음을 수행하십시오.

- 보안 레벨 40 또는 50(QSECURITY 시스템 값)으로 변경하십시오.

  주: 보안 레벨을 40 또는 50으로 변경하면 어플리케이션이 다르게 실행될 수 있습니다.

- USER(*RQD)를 지정한 작업 설명을 가리키도록 대화식 서브시스템에 대한 모든 워크스테이션 항목을 변경하십시오.

표 2. IBM 제공 프로파일에 대한 암호

사용자 ID	암호	권장값
QSECOFR	QSECOFR[1]	보안 관리자에게만 알려진 단순하지 않은 값. **선택한 암호를 기록하여 안전한 장소에 저장하십시오.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

표 2. IBM 제공 프로파일에 대한 암호 (계속)

사용자 ID	암호	권장값

주:

1. *YES로 설정된 QSECOFR에 대한 *암호가 만기로 설정* 값에 도달합니다. 처음 새 시스템에서 사인 온할 경우, QSECOFR 암호를 변경해야 합니다.
2. 시스템 기능에 이러한 사용자 프로파일이 필요하지만, 이 프로파일을 사용하여 사용자가 사인 온할 수 있도록 허용해서는 안 됩니다. V3R1 또는 이후 릴리스가 새 시스템에 설치된 경우, 암호는 *NONE으로 제공됩니다.

   CFGSYSSEC 명령을 실행할 경우, 시스템은 이들 암호를 *NONE으로 설정합니다.
3. TCP/IP를 사용하여 Windows용 iSeries Access를 실행하려면, QUSER 사용자 프로파일을 사용할 수 있어야 합니다.

표 3. 전용 서비스 툴에 대한 암호

DST 레벨	사용자 ID[1]	암호	권장값
기본 기능	11111111	11111111	보안 관리자에게만 알려진 단순하지 않은 값[2]
전체 기능	22222222	22222222[3]	보안 관리자에게만 알려진 단순하지 않은 값[2]
보안 기능	QSECOFR	QSECOFR[3]	보안 관리자에게만 알려진 단순하지 않은 값[2]
서비스 기능	QSRV	QSRV[3]	보안 관리자에게만 알려진 단순하지 않은 값[2]

주:

1. 사용자 ID는 오퍼레이팅 시스템의 PowerPC® AS(RISC) 릴리스에만 필요합니다.
2. 하드웨어 서비스 담당자가 이 사용자 ID 및 암호로 사인 온할 경우, 하드웨어 서비스 담당자가 사용한 후 암호를 새 값으로 변경하십시오.
3. 서비스 툴 사용자 프로파일은 처음으로 사용되자마자 만기됩니다.

주: 인증된 장치만이 DST 암호를 변경할 수 있습니다. 이것은 모든 암호 및 동일한 대응하는 사용자 ID의 경우에도 마찬가지입니다. 인증된 장치에 대한 자세한 정보는 iSeries Information Center에 있는 콘솔 조작 설정 정보를 참조하십시오.

사인 온 값 설정

24 페이지의 표 4에서는 권한 없는 사용자가 시스템을 사인 온하기 힘든 몇 가지 값을 보여줍니다. CFGSYSSEC 명령을 실행할 경우, 시스템 값이 권장값으로 설정됩니다. *iSeries 보안 참조서*의 제 3 장에서 시스템 값에 대한 자세한 내용을 참조할 수 있습니다.

표 4. 사인 온 시스템 값

시스템 값 이름	설명	권장 설정
QAUTOCFG	시스템이 자동으로 새 장치를 구성할지 여부	0(아니오)
QAUTOVRT	사용할 수 있는 장치가 없는 경우, 시스템이 자동으로 작성하는 가상 장치 설명의 수	0
QDEVRCYACN	오류 후 장치가 재연결될 때의 시스템 수행사항[1]	*DSCMSG
QDSCJOBITV	단절된 작업을 종료하기 전에 시스템이 대기하는 시간	120
QDSPSGNINF	사용자가 시작할 때 이전 사인 온 활동에 대한 정보를 표시할지의 여부	1(예)
QINACTITV	대화식 작업이 비활동일 경우, 조치를 취하기 전에 대기하는 시간	60
QINACTMSGQ	QINACTITV 시간에 도달했을 때 시스템이 수행하는 활동	*ENDJOB
QLMTDEVSSN	사용자가 동시에 둘 이상의 워크스테이션에서 사인 온할 수 없도록 금지할지의 여부	1(예)
QLMTSECOFR	*ALLOBJ 또는 *SERVICE 특수 권한이 있는 사용자가 특정 워크스테이션에서만 사인 온할 수 있는지 여부	1(예)[2]
QMAXSIGN	연속적으로 틀린 사인 온 시도 최대 수(사용자 프로파일 또는 암호가 틀림)	3
QMAXSGNACN	QMAXSIGN 한계에 도달했을 때 시스템이 수행하는 활동	3(사용자 프로파일 및 장치 모두 작동불가)

주:

1. 세션에 대한 장치 설명이 명시적으로 지정되면, 시스템이 TELNET 세션을 단절한 다음 다시 연결할 수 있습니다.
2. 시스템 값을 1(예)로 설정할 경우, 명시적으로 장치에 대해 *ALLOBJ 또는 *SERVICE 특수 권한으로 사용자에게 권한을 부여해야 합니다. 가장 간단한 방법은 QSECOFR 사용자 프로파일에 특정 장치에 대한 *CHANGE 권한을 부여하는 것입니다.

사인 온 오류 메세지 변경

해커들은 시스템에 침입하려는 때를 알려고 합니다. 사인 온 화면의 오류 메세지에 암호가 틀림이라고 표시될 경우, 해커는 사용자 ID가 맞다고 가정합니다. CHGMSGD(메세지 설명 변경) 명령으로 두 개의 사인 온 오류 메세지에 대한 텍스트를 변경하여 해커를 오판하도록 할 수 있습니다. 표 5에 권장 텍스트가 표시됩니다.

표 5. 사인 온 오류 메세지

메세지 ID	제공 텍스트	권장 텍스트
CPF1107	CPF1107 - 사용자 프로파일에 대한 암호가 올바르지 않음.	사인 온 정보가 올바르지 않습니다. **주:** 메세지 텍스트에 메세지 ID를 포함하지 마십시오.
CPF1120	CPF1120 - 사용자 XXXXX가 없습니다.	사인 온 정보가 올바르지 않습니다. **주:** 메세지 텍스트에 메세지 ID를 포함하지 마십시오.

사용자 프로파일의 스케줄 가용성

하루의 특정 시간 동안 또는 한 주의 특정 일에만 일부 사용자 프로파일을 사인 온에 사용할 수 있게 할 수 있습니다. 예를 들면, 보안 감사자를 위해 설정한 프로파일이 있으면 감사자가 근무할 시간에만 해당 사용자 프로파일을 작동가능하게 할 수 있습니다. 또한, 비번 일 동안(QSECOFR 사용자 프로파일을 포함하여) *ALLOBJ 특수 권한이 있는 사용자 프로파일을 작동불가능하게 할 수 있습니다.

CHGACTSCDE(활동 스케줄 항목 변경) 명령을 사용하여 사용자 프로파일을 자동으로 작동가능 및 작동불가능으로 설정할 수 있습니다. 스케줄하려는 각 사용자 프로파일에 대하여 사용자 프로파일의 스케줄을 정의하는 항목을 작성합니다.

예를 들면, QSECOFR 프로파일을 아침 7시에서 저녁 10시까지만 사용할 수 있게 하려면, CHGACTSCDE 화면에 다음과 같이 입력하십시오.

```
                          활성 스케줄 항목 변경(CHGACTSCDE)

선택사항을 입력한 후 Enter 키를 누르십시오.


사용자 프로파일  . . . . . > QSECOFR       이름
작동 시간  . . . . . > '7:00'        시간, *NONE
작동불가 시간  . . . . . > '22:00'       시간, *NONE
요일 . . . . . > *MON         *ALL, *MON, *TUE, *WED...
                             > *TUE
                             > *WED
                             > *THU
            추가하려면 + 입력  > *FRI
```

그림 2. 프로파일 활성화 스케줄 화면-샘플

사실 매일 아주 제한된 시간 동안만 QSECOFR 프로파일 사용이 가능하게 됩니다. *SECOFR 클래스의 다른 사용자 프로파일을 사용하여 대부분의 시스템 기능을 수행할 수 있습니다. 따라서 잘 알려진 사용자 프로파일은 해킹 시도에 노출되지 않도록 해야 합니다.

DSPAUDJRNE(감사 저널 항목 표시) 명령을 주기적으로 사용하여 CP(프로파일 변경) 감사 저널 항목을 인쇄할 수 있습니다. 이러한 항목을 사용하여 계획된 스케줄에 따라 사용자 프로파일을 작동가능 또는 불가능한지를 검증하십시오.

사용자 프로파일이 계획된 스케줄에 따라 작동불가능으로 지정되도록 점검하기 위한 또 다른 방법은 PRTUSRPRF(사용자 프로파일 인쇄) 명령을 사용하는 것입니다. 보고 유형에 *PWDINFO를 지정하면, 보고서에 선택된 각 사용자 프로파일의 상태가 포함됩니다. 예를 들면, *ALLOBJ 특수 권한이 있는 모든 사용자 프로파일을 정기적으로 사용하지 못하게 할 경우, 프로파일을 중지한 후, 다음 명령을 스케줄링하여 즉시 실행하도록 할 수 있습니다.

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

비활동 사용자 프로파일 제거

시스템에 필요한 사용자 프로파일만 있어야 합니다. 사용자가 퇴사했거나 조직 안의 다른 작업을 수행하여 더이상 사용자 프로파일이 필요하지 않을 경우, 사용자 프로파일을 제거하십시오. 장기간 조직을 떠나 있을 경우, 해당 사용자의 프로파일을 작동할 수 없게(비활성화) 하십시오. 불필요한 사용자 프로파일은 시스템에 권한이 없는 입력을 제공할 수 있습니다.

자동으로 사용자 프로파일 작동 불가능

ANZPRFACT(프로파일 활동 분석) 명령을 사용하여 지정된 일 수 동안 활동하지 않았던 사용자 프로파일을 작동할 수 없게 할 수 있습니다. 일단 ANZPRFACT 명령을 사용할 경우, 시스템이 찾는 비활동 일 수를 지정할 수 있습니다. 시스템은 최종 사용 날짜, 복원 날짜 및 사용자 프로파일의 작성 날짜를 살펴봅니다.

일단 ANZPRFACT 명령에 값을 지정하면(사용자가 처음 값을 지정한 다음 날부터) 매주 오전 1시에 작업을 실행하도록 스케줄됩니다. 작업은 모든 프로파일을 검토하여 비활동 프로파일을 작동불가능하게 합니다. 비활동 일 수를 변경하지 않는 한, ANZPRFACT 명령을 사용할 필요가 없습니다.

CHGACTPRFL(활동 프로파일 리스트 변경) 명령을 사용하여 일부 프로파일을 ANZPRFACT 처리에서 제외시킬 수 있습니다. CHGACTPRFL 명령은 해당 프로파일의 비활동 기간에 상관없이 ANZPRFACT 명령이 작동가능으로 지정한 프로파일 리스트를 작성합니다.

시스템이 ANZPRFACT 명령을 실행할 경우, 작동불가능으로 지정된 각 사용자 프로파일의 감사 저널에 CP 항목을 기록합니다. DSPAUDJRNE 명령을 사용하여 새로 작동불가능으로 지정된 사용자 프로파일을 나열할 수 있습니다.

주: QAUDCTL 값이 *AUDLVL을 지정하고 QAUDLVL 시스템 값이 *SECURITY를 지정할 경우에만 감사 항목이 기록됩니다.

사용자 프로파일이 계획된 스케줄에 따라 작동불가능으로 지정되도록 점검하기 위한 또 다른 방법은 PRTUSRPRF(사용자 프로파일 인쇄) 명령을 사용하는 것입니다. 보고 유형에 *PWDINFO를 지정하면, 보고서에 선택된 각 사용자 프로파일의 상태가 포함됩니다.

자동으로 사용자 프로파일 제거

CHGEXPSCDE(만기 스케줄 항목 변경) 명령을 사용하여 사용자 프로파일의 제거 또는 작동불가능을 관리할 수 있습니다. 사용자가 장기간 자리를 비울 경우, 사용자 프로파일을 제거하거나 작동불가능으로 지정하도록 스케줄할 수 있습니다.

처음 CHGEXPSCDE 명령을 사용할 경우, 매일 자정 1분 후에 실행되는 작업 스케줄 항목을 작성합니다. 작업은 QASECEXP 파일을 점검하여 사용자 프로파일이 해당 일에 제거되도록 스케줄링되었는지 판별합니다.

CHGEXPSCDE 명령으로 사용자 프로파일을 작동불가능으로 지정하거나 삭제할 수 있습니다. 사용자 프로파일을 삭제하도록 선택할 경우, 시스템이 사용자의 오브젝트에 대하여 수행할 작업을 지정해야 합니다. 사용자 프로파일의 삭제를 스케줄링하기 전에 사용자의 오브젝트를 조사해야 합니다. 예를 들면, 사용자가 권한을 허용하는 프로그램을 소유한 경우, 이 프로그램이 새 소유자의 소유권도 허용하겠습니까? 또는 새 소유자가 (특수 권한과 같은) 필요 이상의 권한이 있습니까? 그렇지 않다면, 특수 권한을 갖는 새 사용자 프로파일을 작성하여 권한 허용이 필요한 프로그램을 구비해야 합니다.

또한 사용자 프로파일을 삭제할 경우, 어플리케이션 문제가 발생할지 여부를 조사해야 합니다. 예를 들면, 작업 설명에서 사용자 프로파일을 디폴트 사용자로서 지정합니까?

DSPEXPSCD(만기 스케줄 표시) 명령을 사용하여 작동불가능 또는 제거되도록 스케줄된 프로파일 리스트를 표시할 수 있습니다.

DSPAUTUSR(권한 부여된 사용자 표시) 명령을 사용하여 시스템의 모든 사용자 프로파일을 나열할 수 있습니다. DLTUSRPRF(사용자 프로파일 삭제) 명령을 사용하여 날짜가 지나 사용할 수 없는 프로파일을 삭제하십시오.

보안 주:: 사용자 프로파일의 상태를 *DISABLED로 설정하여 사용자 프로파일을 작동불가능으로 지정할 수 있습니다. 사용자 프로파일을 작동불가능으로 지정할 경우, 대화식 사용에 사용할 수 없게 합니다. 작동불가능하게 된 사용자 프로파일로는 사인 온할 수 없거나 작업을 변경할 수 없습니다. 일괄처리 작업은 작동불가능으로 지정된 사용자 프로파일로 실행할 수 있습니다.

디폴트 암호 방지

새 사용자 프로파일을 작성할 때 디폴트는 암호를 사용자 프로파일 이름과 같게 지정하는 것입니다. 누군가가 프로파일명 지정 방침을 알아내어 새로운 사용자가 조직에 참여할 경우, 시스템에 침입할 수 있는 기회를 제공하는 것입니다.

새 사용자 프로파일을 작성할 때 디폴트 암호를 사용하는 대신 고유하고 단순하지 않은 암호 지정을 고려하십시오. 보안 방침을 대략 설명해 놓은『환영 인사』와 같은 내용으로 비밀리에 새 사용자에게 암호를 알리십시오. 사용자 프로파일을 PWDEXP(*YES)로 설정하여 처음 시작할 때 사용자가 암호를 변경해야 합니다.

ANZDFTPWD(디폴트 암호 분석) 명령을 사용하여 시스템의 모든 사용자 프로파일의 디폴트 암호를 검사할 수 있습니다. 보고서를 인쇄할 경우, 암호가 사용자 프로파일명

과 같으면(사용자 프로파일에 작동불가능과 같이) 시스템이 조치를 취하도록 지정하는 옵션이 있습니다. ANZDFTPWD 명령은 찾은 프로파일과 취한 조치 리스트를 인쇄합니다.

주: 암호는 일방적 암호화 형식으로 시스템에 저장됩니다. 암호가 해독될 수 없습니다. 시스템은 지정된 암호를 암호화하여 시스템을 사인 온할 때 암호를 검사하는 것처럼 저장된 암호와 비교합니다. *AUTFAIL(권한 실패)을 감사할 경우, 시스템은 (V4R1 또는 이전 릴리스 실행 시스템에 대하여) 디폴트 암호가 없는 각 사용자 프로파일에 대해 PW 감사 저널 항목을 기록합니다. V4R2 시작시 시스템은 ANZDFTPWD 명령을 실행할 때 PW 감사 저널 항목을 기록하지 않습니다.

사인 온 및 암호 활동 모니터

권한을 부여받지 않고 시스템에 침입한 시도에 대해 PRTUSRPRF 명령을 사용하여 사인 온 및 암호 활동을 모니터할 수 있습니다.

다음은 이 보고서 사용에 대한 몇 가지 제안사항입니다.

- 일부 사용자 프로파일에 대한 암호 만기 간격이 시스템 값보다 더 긴지와 더 긴 만기 간격이 합당한지의 여부를 판별하십시오. 예를 들어, 보고서에서 USERY는 암호 만기 간격이 120일입니다.
- 보고서를 정기적으로 실행하여 실패한 사인 온 시도를 모니터하십시오. 시스템 침입자는 시도를 실패한 후 시스템에서는 조치를 취한다는 사실을 알게 될 것입니다. 매일 밤 침입자는 시도에 대한 경보를 피하기 위하여 QMAXSIGN 값보다 적게 시도할 것입니다. 그러나 매일 아침 일찍 이 보고서를 실행하여 특정 프로파일에서 사인 온 시도가 자주 성공하지 못한다는 사실을 알게 되면 문제가 있다고 의심할 수 있습니다.
- 오랫동안 사용하지 않은 사용자 프로파일이나 오랫동안 암호가 변경되지 않은 프로파일을 식별하십시오.

암호 정보 저장

일부 네트워크 기능 및 통신 요구사항을 지원하기 위해 iSeries 서버에서는 해독할 수 있는 암호 저장을 위한 보안 방법을 제공합니다. 예를 들어, 다른 시스템과의 SLIP 연결을 설정할 때, 시스템에서 이 암호를 사용합니다(141 페이지의 『보안 및 다이얼 아웃 세션』에는 저장된 암호의 사용법이 설명되어 있습니다).

iSeries 서버는 사용자 프로그램 또는 인터페이스에서 액세스할 수 없는 보안 지역에 이러한 특수 암호를 저장합니다. 명시적으로 권한을 부여받은 시스템 기능만이 이러한 암호를 설정하여 검색할 수 있습니다.

예를 들면, 다이얼 아웃 SLIP 연결에 저장된 암호를 사용할 경우, 구성 프로파일을 작성하는 시스템 명령인 WRKTCPPTP로 암호를 설정하십시오. 이 명령을 사용하려면 *IOSYSCFG가 있어야 합니다. 특수 코드화 연결 스크립트가 다이얼 아웃 프로시듀어 중에 암호를 검색한 후 해독합니다. 해독된 암호는 사용자 또는 작업 기록부에서 볼 수 없습니다.

보안 관리자로서 해독할 수 있는 암호를 시스템에 저장할 것인지를 결정해야 합니다. 이를 지정하려면 QRETSVRSEC(서버 보안 자료 보유) 시스템 값을 사용하십시오. 디폴트는 0(아니오)이므로, 이 시스템 값을 명시적으로 설정하지 않을 경우, 시스템에서는 해독할 수 있는 암호를 저장하지 않습니다.

저장된 암호에 대한 네트워크 또는 통신 요구사항이 있는 경우, 적합한 방침을 설정하고 통신 상대의 방침 및 관행을 알아야 합니다. 예를 들면, SLIP를 사용하여 다른 iSeries 서버와 통신할 때, 두 시스템 모두 세션 설정을 위한 특수 사용자 프로파일 설정을 고려해야 합니다. 특수 프로파일은 시스템에서 제한된 권한을 가져야 합니다. 이것은 저장된 암호를 절충할 경우, 시스템에 대한 영향을 줄일 수 있습니다.

제 4 장 iSeries를 구성하여 보안 툴 사용

이 정보는 OS/400의 일부인 보안 툴을 사용하기 위해 시스템을 설정하는 방법에 대해 설명합니다. OS/400을 설치하면 보안 툴을 사용할 수 있습니다. 다음 주제는 보안 툴을 사용한 조작 프로시듀어의 제안사항입니다.

안전하게 보안 툴 조작

OS/400을 설치하면 보안 툴과 연관된 오브젝트가 보안됩니다. 보안 툴을 안전하게 조작하려면 보안 툴 오브젝트에 대한 권한을 변경하지 마십시오.

다음은 보안 툴 오브젝트에 대한 보안 설정 및 요구사항입니다.

- 보안 툴 프로그램 및 명령이 QSYS 제품 라이브러리에 있습니다. 명령 및 프로그램이 *EXCLUDE 공용 권한과 함께 제공됩니다. 많은 보안 툴 명령이 QUSRSYS 라이브러리에서 파일을 작성합니다. 이러한 파일이 작성될 경우, 파일에 대한 공용 권한은 *EXCLUDE입니다.

  변경된 보고서 생성에 대한 정보가 들어 있는 파일명은 QSEC로 시작됩니다. 사용자 프로파일 관리에 대한 정보가 들어 있는 파일명은 QASEC로 시작됩니다. 이러한 파일에는 시스템에 관한 기밀 정보가 들어 있습니다. 따라서 파일에 대한 공용 권한을 변경해서는 안 됩니다.
- 보안 툴은 정상 시스템 설정을 사용하여 인쇄 출력을 보냅니다. 이러한 보고서에는 시스템에 관한 기밀 정보가 들어 있습니다. 출력을 보호 출력 대기행렬로 보내려면, 보안 툴을 실행할 사용자 프로파일 또는 작업 설명을 적절히 변경하십시오.
- 이 보안 기능과 이 기능이 시스템의 많은 오브젝트에 액세스하므로 보안 툴 명령에는 *ALLOBJ 특수 권한이 필요합니다. 일부 명령에도 *SECADM, *AUDIT 또는 *IOSYSCFG 특수 권한이 필요합니다. 명령을 정상적으로 실행하려면 보안 툴을 사용할 경우, 보안 담당자로 사인 온해야 합니다. 따라서, 보안 툴 명령에 개인 권한을 부여할 필요는 없습니다.

파일 충돌 방지

많은 보안 툴 보고서 명령은 변경된 보고서 버전을 인쇄하기 위해 사용할 수 있는 데이터베이스 파일을 작성합니다. 32 페이지의 『보안 명령에 대한 명령 및 메뉴』는 한번에 하나의 작업에서 하나의 명령만 수행할 수 있습니다. 이제 대부분의 명령은 이와 같이 되었는지 검사합니다. 아직 다른 작업 실행이 완료되지 않았는데 명령을 실행할 경우 오류 메세지가 나타납니다.

많은 인쇄 작업이 장기 실행 작업입니다. 보고서를 일괄처리로 제출하거나 작업 스케줄러에 추가할 경우, 파일 충돌을 피하도록 주의해야 합니다. 예를 들면, 두 개의 PRTUSRPRF 보고서 버전을 다른 선택 범주로 인쇄하려 할 수 있습니다. 보고서를 일괄처리로 제출하려면, 한 번에 하나의 작업만 실행하는 작업 대기행렬을 사용하여 보고서 작업을 순차적으로 실행해야 합니다.

작업 스케줄러를 사용하려면, 첫 번째 버전이 완료되고 두 번째 작업을 시작할 정도로 두 작업 사이에 시간을 충분히 두고 계획해야 합니다.

보안 툴 저장

SAVSYS(시스템 저장) 명령 또는 SAVSYS 명령을 실행하는 저장 메뉴의 옵션을 실행할 때마다 보안 툴 프로그램이 저장됩니다.

보안 툴 파일은 QUSRSYS 라이브러리에 있습니다. 정상 조작 프로시듀어의 일부로 이 라이브러리를 이미 저장하고 있어야 합니다. QUSRSYS 라이브러리에는 시스템의 많은 사용권 프로그램에 대한 자료가 들어 있습니다. QUSRSYS 라이브러리를 저장하는 명령 및 옵션에 대한 자세한 내용은 Information Center를 참조하십시오.

보안 명령에 대한 명령 및 메뉴

이 섹션에서는 보안 툴에 대한 명령 및 메뉴에 대해 설명합니다. 이 정보에는 명령 사용법에 대한 예가 있습니다.

보안 툴에 대해 두 가지 메뉴를 사용할 수 있습니다.

- 대화식으로 명령을 실행하기 위한 SECTOOLS(보안 툴) 메뉴
- 일괄처리로 보고서 명령을 실행하는 SECBATCH(일괄처리로 보안 보고서 제출 또는 스케줄) 메뉴. SECBATCH 메뉴는 두 부분으로 되어 있습니다. 메뉴의 첫 번째 부분은 SBMJOB(작업 제출) 명령을 사용하여 즉시 처리할 보고서를 일괄처리로 제출합니다.

  메뉴의 두 번째 부분은 ADDJOBSCDE(작업 스케줄 항목 추가) 명령을 사용하여 지정된 날짜와 시간에 보안 보고서가 정기적으로 실행되도록 스케줄합니다.

보안 툴 메뉴 옵션

표 6은 이들 메뉴 옵션 및 관련 명령에 대해 설명합니다.

표 6. 사용자 프로파일의 툴 명령

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
1	ANZDFTPWD	디폴트 암호 분석 명령을 사용하여 암호가 사용자 프로파일명과 동일한 사용자 프로파일에 대해 보고하고 조치를 취합니다.	QASECPWD[2]

표 6. 사용자 프로파일의 툴 명령 (계속)

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
2	DSPACTPRFL	활동 프로파일 리스트 표시 명령을 사용하여 ANZPRFACT 처리에서 면제된 사용자 프로파일 리스트를 표시 또는 인쇄합니다.	QASECIDL[2]
3	CHGACTPRFL	활동 프로파일 리스트 변경 명령을 사용하여 ANZPRFACT 명령의 면제 리스트에서 프로파일을 추가 및 제거합니다. 활동 프로파일 리스트에 있는 사용자 프로파일은 리스트에서 프로파일을 제거할 때까지 영구적으로 활동합니다. ANZPRFACT 명령은 프로파일의 비활동 기간에 상관없이 활동 프로파일 리스트에 있는 프로파일을 사용할 수 있도록 합니다.	QASECIDL[2]
4	ANZPRFACT	프로파일 활동 분석 명령을 사용하여 지정된 일 수 동안 사용되지 않은 사용자 프로파일을 사용할 수 없게 합니다. ANZPRFACT 명령을 사용한 후에 일 수를 지정하면, 매일 밤 ANZPRFACT 작업이 실행됩니다. CHGACTPRFL 명령을 사용하여 사용자 프로파일이 사용불가에서 면제되도록 할 수 있습니다.	QASECIDL[2]
5	DSPACTSCD	프로파일 활동 스케줄 표시 명령을 사용하여 특정한 사용자 프로파일 사용가능 또는 사용불가능 스케줄에 관한 정보를 표시 또는 인쇄합니다. CHGACTSCDE 명령으로 스케줄을 작성합니다.	QASECACT[2]
6	CHGACTSCDE	활성화 스케줄 항목 변경 명령을 사용하여 사용자 프로파일을 하루 또는 일주일 동안 일정 횟수만 사인온할 수 있도록 합니다. 예정된 각 사용자 프로파일에 대하여 사용가능 및 불가능 횟수에 대한 작업 스케줄 항목이 작성됩니다.	QASECACT[2]
7	DSPEXPSCD	만기 스케줄 표시 명령을 사용하여 이후에 시스템에서 사용불가 또는 제거되도록 예정된 사용자 프로파일 리스트를 표시 또는 인쇄합니다. CHGEXPSCDE 명령을 사용하여 만기될 사용자 프로파일을 설정할 수 있습니다.	QASECEXP[2]
8	CHGEXPSCDE	만기 스케줄 항목 변경 명령을 사용하여 제거할 사용자 프로파일을 계획합니다. 사용할 수 없게 하여 임시 제거하거나, 시스템에서 삭제할 수 있습니다. 이 명령은 자정 1분 후인 00:01에 매일 실행하는 작업 스케줄 항목을 사용합니다. 작업은 QASECEXP 파일을 점검하여 사용자 프로파일이 해당 일에 만기되도록 설정되었는지 판별합니다. DSPEXPSCD 명령을 사용하여 만기되도록 스케줄된 사용자 프로파일을 표시합니다.	QASECEXP[2]
9	PRTPRFINT	프로파일 내부 인쇄 명령을 사용하여 사용자 프로파일의 항목 수에 대한 정보가 들어 있는 보고서를 인쇄합니다. 항목 수로 사용자 프로파일의 크기를 판별합니다.	

표 6. 사용자 프로파일의 툴 명령 (계속)

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
주: 1. 옵션은 SECTOOLS 메뉴에 있습니다. 2. 이 파일은 QUSRSYS 라이브러리에 있습니다.			

메뉴상에서 다음 페이지로 이동하면 추가 옵션을 볼 수 있습니다. 표 7은 보안 감사에 대한 메뉴 옵션 및 관련 명령에 대해 설명합니다.

표 7. 보안 감사의 툴 명령

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
10	CHGSECAUD	보안 감사 변경 명령을 사용하여 보안 감사를 설정하고 보안 감사를 제어하는 시스템 값을 변경합니다. CHGSECAUD 명령을 실행할 경우, QAUDJRN(보안 감사) 저널이 없으면 작성됩니다. CHGSECAUD 명령은 QAUDLVL(감사 레벨) 시스템 값을 더 간단하게 설정할 수 있는 옵션을 제공합니다. *ALL을 지정하여 모든 가능한 감사 레벨을 활성화할 수 있습니다. 또는 *DFTSET를 지정하여 가장 일반적으로 사용되는 설정(*AUTFAIL, *CREATE, *DELETE, *SECURITY 및 *SAVRST)을 활성화할 수 있습니다. **주:** 보안 툴을 사용하여 감사를 설정하면 반드시 감사 저널 리시버의 관리를 계획하십시오. 그렇지 않으면, 금방 디스크 이용에 문제가 발생할 수 있습니다.	
11	DSPSECAUD	보안 감사 표시 명령을 사용하여 보안 감사 저널과 보안 감사를 제어하는 시스템 값에 대한 정보를 표시합니다.	
주: 1. 옵션은 SECTOOLS 메뉴에 있습니다.			

보안 일괄처리 메뉴 사용

다음은 SECBATCH 메뉴의 첫 번째 부분입니다.

```
SECBATCH         보안 보고서를 일괄처리로 제출 또는 스케줄
                                                          시스템:
다음 중 하나를 선택하십시오.


  보고서를 일괄처리로 제출
    1. 허용 오브젝트
    2. 저널 항목 감사
    3. 권한 부여 리스트 권한
    4. 명령 권한
    5. 명령 개인 권한
    6. 통신 보안
    7. 디렉토리 권한
    8. 디렉토리 개인 권한
    9. 문서 권한
   10. 문서 개인 권한
   11. 파일 권한
   12. 파일 개인 권한
   13. 폴더 권한
```

이 메뉴에서 옵션을 선택할 경우, SBMJOB(작업 제출) 화면이 표시됩니다. 명령에 대한 디폴트 옵션을 변경하려면, *실행 명령* 행에서 F4(프롬트) 키를 누르십시오.

스케줄 일괄처리 보고서를 보려면 SECBATCH 메뉴에서 다음 페이지로 가십시오. 예를 들면, 이 부분의 메뉴에 있는 옵션을 사용하여 변경된 보고서 버전을 정기적으로 실행하도록 설정할 수 있습니다. 추가 메뉴 옵션을 보기 위해 다음 페이지로 갈 수 있습니다. 메뉴에서 옵션을 선택하면, ADDJOBSCDE(작업 스케줄 항목 추가) 화면이 표시됩니다.

실행 명령 행에 커서를 놓고 F4(프롬트) 키를 눌러 보고서에 대한 다른 설정을 선택할 수 있습니다. 작업 스케줄 항목을 표시할 경우, 항목을 인식할 수 있도록 의미있는 작업명을 할당해야 합니다.

보안 일괄처리 메뉴 옵션

36 페이지의 표 8은 보안 보고서에 대한 메뉴 옵션과 관련 명령에 대해 설명합니다.

보안 보고서를 실행할 경우, 지정한 선택 기준과 툴에 대한 선택 기준 모두에 알맞는 정보만 인쇄됩니다. 예를 들면, 사용자 프로파일명을 지정하는 작업 설명은 보안에 관련됩니다. 따라서 PRTJOBDAUT(작업 설명) 보고서는 작업 설명에 대한 공용 권한이 *EXCLUDE가 아닙니다. *그리고*, 작업 설명에서 USER 매개변수에 사용자 프로파일명을 지정할 경우에만 지정된 라이브러리의 작업 설명을 인쇄합니다.

마찬가지로 서브시스템 정보(PRTSBSDAUT 명령)를 인쇄할 경우, 서브시스템 설명에 사용자 프로파일을 지정하는 통신 항목이 있을 경우에만 서브시스템에 대한 정보가 인쇄됩니다.

특정 보고서에 예상보다 적은 정보가 인쇄되면 온라인 도움말 정보에 문의하여 보고서의 선택 기준을 알아보십시오.

표 8. 보안 보고서에 대한 명령

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
1, 40	PRTADPOBJ	허용 오브젝트 인쇄 명령을 사용하여 지정된 사용자 프로파일의 권한을 허용하는 오브젝트 리스트를 인쇄합니다. 단일 프로파일, 총칭 프로파일명(Q로 시작하는 모든 프로파일과 같은) 또는 시스템상의 모든 사용자 프로파일을 지정할 수 있습니다. 이 보고서에는 두 가지 버전이 있습니다. 전체 보고서는 선택 기준에 알맞는 허용된 오브젝트를 모두 나열합니다. 변경 보고서는 현재 시스템에 있는 허용된 오브젝트와 마지막으로 보고서를 실행했을 때 시스템에 있던 허용된 오브젝트 사이의 차이를 나열합니다.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	감사 저널 항목 표시 명령을 사용하여 보안 감사 저널에 있는 항목에 대한 정보를 표시 또는 인쇄합니다. 특정 항목 유형, 특정 사용자 및 시간을 선택할 수 있습니다.	QASYxxJ4[3]
3, 42	PRTPVTAUT *AUTL	*AUTL 오브젝트에 대해 개인 권한 인쇄 명령을 사용할 경우, 시스템의 모든 권한 부여 리스트 중 하나를 수신합니다. 보고서에는 각 리스트에 대해 권한이 부여된 사용자와 리스트에 대한 사용자의 권한이 포함됩니다. 이 정보를 사용하여 시스템의 오브젝트 권한 소스를 분석할 수 있습니다. 이 보고서에는 세 가지 버전이 있습니다. 전체 보고서는 시스템의 모든 권한 부여 리스트를 나열합니다. 변경 보고서는 보고서를 마지막으로 실행한 이후 권한 부여에 추가 및 변경한 사항을 나열합니다. 삭제 보고서는 보고서를 마지막으로 실행한 이후 권한 부여 리스트에 대한 권한이 삭제된 사용자를 나열합니다. 전체 보고서를 인쇄할 경우, 각 권한 부여 리스트가 보안하는 오브젝트 리스트를 인쇄하는 옵션이 있습니다. 시스템은 각 권한 부여 리스트에 대한 별도의 보고서를 작성합니다.	QSECATLOLD[2]
6, 45	PRTCMNSEC	통신 보안 인쇄 명령을 사용하여 시스템의 통신에 영향을 주는 오브젝트의 보안 관련 설정을 인쇄합니다. 이러한 설정은 사용자 및 작업이 시스템에 입력되는 방법에 영향을 줍니다. 이 명령으로 시스템의 구성 리스트에 대한 설정을 표시하는 보고서 및 행 설명, 제어기 및 장치 설명에 대한 보안 관련 매개변수를 나열하는 보고서 두 가지가 생성됩니다. 이러한 각각의 보고서에는 전체 버전 및 변경된 버전이 있습니다.	QSECCMNOLD[2]

표 8. 보안 보고서에 대한 명령 (계속)

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
15, 54	PRTJOBDAUT	작업 설명 권한 인쇄 명령을 사용하여 사용자 프로파일을 지정하고 *EXCLUDE가 아닌 공용 권한을 갖는 작업 설명 리스트를 인쇄합니다. 보고서는 작업 설명에 지정된 사용자 프로파일에 대한 특수 권한을 표시합니다. 이 보고서에는 두 가지 버전이 있습니다. 전체 보고서는 선택 기준에 알맞는 모든 작업 설명 오브젝트를 나열합니다. 변경 보고서는 현재 시스템에 있는 작업 설명 오브젝트와 마지막으로 보고서를 실행했을 때 시스템에 있던 작업 설명 오브젝트 사이의 차이를 나열합니다.	QSECJBDOLD[2]
주 4 참조	PRTPUBAUT	공용 권한 부여 오브젝트 인쇄 명령을 사용하여 공용 권한이 *EXCLUDE가 아닌 오브젝트 리스트를 인쇄합니다. 명령을 실행할 경우, 오브젝트 유형 및 보고서의 라이브러리를 지정할 수 있습니다. PRTPUBAUT 명령을 사용하여 시스템의 모든 사용자가 액세스할 수 있는 오브젝트에 대한 정보를 인쇄합니다. 이 보고서에는 두 가지 버전이 있습니다. 전체 보고서는 선택 기준에 알맞는 모든 오브젝트를 나열합니다. 변경 보고서는 현재 시스템에 있는 오브젝트와 마지막으로 보고서를 실행했을 때 시스템에 있던(동일 라이브러리에 있는 같은 유형의) 오브젝트 사이의 차이를 나열합니다.	QPBxxxxxx[5]
주 5 참조	PRTPVTAUT	개인 권한 인쇄 명령을 사용하여 지정된 라이브러리에 있는 지정된 유형의 오브젝트에 대한 개인 권한 리스트를 인쇄합니다. 이 보고서를 사용하여 오브젝트에 대한 권한의 소스를 판별할 수 있습니다. 이 보고서에는 세 가지 버전이 있습니다. 전체 보고서는 선택 기준에 알맞는 모든 오브젝트를 나열합니다. 변경 보고서는 현재 시스템에 있는 오브젝트와 마지막으로 보고서를 실행했을 때 시스템에 있던(동일 라이브러리에 있는 같은 유형의) 오브젝트 사이의 차이를 나열합니다. 삭제 보고서는 보고서를 마지막으로 인쇄한 이후 오브젝트에 대한 권한이 삭제된 사용자를 나열합니다.	QPVxxxxxx[5]
24, 63	PRTQAUT	대기행렬 보고서 인쇄를 사용하여 시스템의 출력 대기행렬 및 작업 대기행렬에 대한 보안 설정을 인쇄합니다. 이러한 설정은 출력 대기행렬 또는 작업 대기행렬에 있는 항목을 열람하고 변경할 수 있는 사용자를 제어합니다. 이 보고서에는 두 가지 버전이 있습니다. 전체 보고서는 선택 기준에 알맞는 모든 출력 대기행렬 및 작업 대기행렬 오브젝트를 나열합니다. 변경 보고서는 현재 시스템에 있는 출력 대기행렬 및 작업 대기행렬 오브젝트와 마지막으로 보고서를 실행했을 때 시스템에 있던 출력 대기행렬 및 작업 대기행렬 오브젝트 사이의 차이를 나열합니다.	QSECQOLD[2]

표 8. 보안 보고서에 대한 명령 (계속)

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
25, 64	PRTSBSDAUT	서브시스템 설명 인쇄 명령을 사용하여 시스템의 서브시스템 설명에 대한 보안 관련 통신 항목을 인쇄합니다. 이러한 설정은 작업을 시스템에 입력하는 방법 및 작업 실행 방법을 제어합니다. 보고서는 사용자 프로파일명을 지정하는 통신 항목이 있을 경우에만 서브시스템 설명을 인쇄합니다. 이 보고서에는 두 가지 버전이 있습니다. 전체 보고서는 선택 기준에 알맞는 모든 서브시스템 설명 오브젝트를 나열합니다. 변경 보고서는 현재 시스템에 있는 서브시스템 설명 오브젝트와 마지막으로 보고서를 실행했을 때 시스템에 있던 서브시스템 설명 오브젝트 사이의 차이를 나열합니다.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	시스템 보안 속성 인쇄 명령을 사용하여 보안 관련 시스템 값과 네트워크 속성의 리스트를 인쇄합니다. 보고서에는 현재값과 권장값이 표시됩니다.	
27, 66	PRTTRGPGM	트리거 프로그램 인쇄 명령을 사용하여 시스템의 데이터베이스 파일과 연관된 트리거 프로그램의 리스트를 인쇄합니다. 이 보고서에는 두 가지 버전이 있습니다. 전체 보고서는 할당되어 선택 기준에 알맞는 모든 트리거 프로그램을 나열합니다. 변경 보고서는 마지막으로 보고서를 실행한 이후에 할당된 트리거 프로그램을 나열합니다.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	사용자 오브젝트 인쇄 명령을 사용하여 라이브러리에 있는 사용자 오브젝트(IBM에서 제공하지 않는 오브젝트)의 리스트를 인쇄합니다. 이 보고서를 사용하여 라이브러리 리스트의 시스템 부분에 있는(QSYS와 같은) 라이브러리의 사용자 오브젝트 리스트를 인쇄합니다. 이 보고서에는 두 가지 버전이 있습니다. 전체 보고서는 선택 기준에 알맞는 모든 사용자 오브젝트를 나열합니다. 변경 보고서는 현재 시스템에 있는 사용자 오브젝트와 마지막으로 보고서를 실행했을 때 시스템에 있던 사용자 오브젝트 사이의 차이를 나열합니다.	QSECPUOLD[2]
29, 68	PRTUSRPRF	사용자 프로파일 인쇄 명령을 사용하여 지정된 기준에 알맞는 사용자 프로파일을 분석합니다. 특수 권한, 사용자 클래스 또는 특수 권한과 사용자 클래스 사이의 불일치에 따라 사용자 프로파일을 선택할 수 있습니다. 권한 정보, 환경 정보, 암호 정보 또는 암호 레벨 정보를 인쇄할 수 있습니다.	
30, 69	PRTPRFINT	프로파일 내부 인쇄 명령을 사용하여 항목 수에 대한 내부 정보 보고서를 인쇄합니다.	

표 8. 보안 보고서에 대한 명령 (계속)

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
31, 70	CHKOBJITG	오브젝트 무결성 검사 명령을 사용하여 프로그램과 같은 조작가능한 오브젝트가 컴파일러를 사용하지 않고 변경되었는지 판별합니다. 이 명령으로 시스템에 바이러스 프로그램을 도입하려는 시도 또는 권한이 없는 명령어를 수행하는 프로그램을 변경하려는 시도를 감지할 수 있습니다. *iSeries 보안 참조서* 책은 CHKOBJITG 명령에 대한 자세한 정보를 제공합니다.	

주:

1. 옵션은 SECBATCH 메뉴에 있습니다.
2. 이 파일은 QUSRSYS 라이브러리에 있습니다.
3. xx는 두 문자 저널 항목 유형입니다. 예를 들면, AE 저널 항목에 대한 모델 출력 파일은 QSYS/QASYAEJ4입니다. 모델 출력 파일은 *iSeries 보안 참조서* 책의 부록 F에서 설명합니다.
4. SECBATCH 메뉴에는 보안 관리자의 일반적 관심의 대상인 오브젝트 유형에 대한 옵션이 있습니다. 예를 들어, *FILE 오브젝트에 대해 PRTPUBAUT 명령을 실행하려면, 옵션 11 또는 50을 사용하십시오. 오브젝트 유형을 지정하려면 일반 옵션 18 및 57을 사용하십시오.
5. SECBATCH 메뉴에는 보안 관리자의 일반적 관심의 대상인 오브젝트 유형에 대한 옵션이 있습니다. 예를 들면, 옵션 12 또는 51은 *FILE 오브젝트에 대해 PRTPVTAUT 명령을 실행합니다. 오브젝트 유형을 지정하려면 일반 옵션 19 및 58을 사용하십시오.
6. 파일명의 xxxxxx는 오브젝트 유형입니다. 예를 들면, 프로그램 오브젝트에 대한 파일은 공용 권한에 대해서는 QPBPGM, 개인 권한에 대해서는 QPVPGM이라고 합니다. 해당 파일은 QUSRSYS 라이브러리에 있습니다.

   파일에는 보고서를 인쇄한 각 라이브러리에 대한 멤버가 들어 있습니다. 멤버명은 라이브러리명과 같습니다.

보안 사용자 정의 명령

표 9는 시스템의 보안을 사용자 정의하기 위해 사용할 수 있는 명령에 대해 설명합니다. 이러한 명령은 SECTOOLS 메뉴에 있습니다.

표 9. 시스템을 사용자 정의하기 위한 명령

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
60	CFGSYSSEC	시스템 보안 구성 명령을 사용하여 보안 관련 시스템 값을 권장 설정으로 설정합니다. 또한 명령은 시스템에 보안 감사도 설정합니다. 40 페이지의 『시스템 보안 구성 명령으로 설정된 값』에서는 명령 수행사항에 대해 설명합니다. **주:** 사용자 상황에 맞는 보안 권장사항을 보려면, 이 명령을 실행하는 대신 iSeries 보안 마법사나 iSeries 보안 어드바이저를 실행하십시오. 이들 툴에 대해서는 11 페이지의 제 2 장 『iSeries 보안 마법사 및 eServer 보안 플래너』를 보십시오.	
61	RVKPUBAUT	공용 권한 취소 명령을 사용하여 시스템의 보안 감지 명령 세트에 대해 공용 권한을 *EXCLUDE로 설정합니다. 42 페이지의 『공용 권한 취소 명령의 기능』에서는 RVKPUBAUT 명령을 수행하는 조치가 나열됩니다.	

표 9. 시스템을 사용자 정의하기 위한 명령 (계속)

메뉴[1] 옵션	명령어	설명	사용되는 데이터베이스 파일
주:			
1. 옵션은 SECTOOLS 메뉴에 있습니다.			

시스템 보안 구성 명령으로 설정된 값

표 10은 CFGSYSSEC 명령을 실행할 때 설정되는 시스템 값을 나열합니다. CFGSYSSEC 명령은 QSYS/QSECCFGS라는 프로그램을 실행합니다.

표 10. CFGSYSSEC 명령으로 설정된 값

시스템 값 이름	설정	시스템 값 설명
QALWOBJRST	*NONE	시스템 상태 프로그램 및 권한을 허용하는 프로그램을 복원할 수 있는지의 여부
QAUTOCFG	0(아니오)	새 장치 자동 구성
QAUTOVRT	0	사용할 수 있는 장치가 없는 경우, 시스템이 자동으로 작성하는 가상 장치 설명의 수
QDEVRCYACN	*DSCMSG(메세지와 단절)	통신이 재설정되었을 때의 시스템 조치
QDSCJOBITV	120	단절된 작업에서 시스템이 조치를 취하기 전의 시간
QDSPSGNINF	1(예)	사용자에게 사인 온 정보 화면이 표시되는지의 여부
QINACTITV	60	비활동 대화식 작업에서 시스템이 조치를 취하기 전의 시간
QINACTMSGQ	*ENDJOB	시스템이 비활동 작업에 취하는 조치
QLMTDEVSSN	1(예)	사용자가 한번에 한 장치에서 사인 온하도록 제한되는지의 여부
QLMTSECOFR	1(예)	*ALLOBJ 및 *SERVICE 사용자가 특정 장치로 제한되는지의 여부
QMAXSIGN	3	허용될 수 있는 연속해서 성공하지 못한 사인 온 시도 수
QMAXSGNACN	3(둘다)	QMAXSIGN 한계에 도달했을 때 시스템이 워크스테이션을 작동불능으로 하는지 또는 사용자 프로파일을 작동불능으로 하는지의 여부
QRMTSIGN	*FRCSIGNON	시스템이 리모트(passthru 또는 TELNET) 사인 온 시도를 처리하는 방법
QRMTSVRATR	0(오프)	시스템을 리모트로 분석하도록 허용
QSECURITY 41 페이지의 1	50	시행되는 보안 레벨
QVFYOBJRST	3(복원시 서명 검증)	복원시 오브젝트 검증
QPWDEXPITV	60	사용자가 암호를 변경해야 하는 빈도
QPWDMINLEN	6	암호의 최소 길이
QPWDMAXLEN	8	암호의 최대 길이
QPWDPOSDIF	1(예)	새 암호의 모든 위치가 최종 암호의 위치와 동일한지의 여부
QPWDLMTCHR	주 41 페이지의 2 참조	암호에 허용되지 않은 문자
QPWDLMTAJC	1(예)	인접 숫자가 암호에서 금지되는지의 여부
QPWDLMTREP	2(연속적으로 반복할 수 없음)	반복 문자가 암호에서 금지되는지의 여부
QPWDRQDDGT	1(예)	암호에 최소 하나의 숫자가 있어야 하는지의 여부
QPWDRQDDIF	1(32개의 고유 암호)	한 암호를 반복하기 전에 필요한 고유 암호의 수

표 10. CFGSYSSEC 명령으로 설정된 값 (계속)

시스템 값 이름	설정	시스템 값 설명
QPWDVLDPGM	*NONE	암호의 유효성을 검사하기 위해 시스템에서 호출하는 사용자 나감 프로그램

주:

1. 현재 40 이하의 QSECURITY 값으로 실행중인 경우, 더 높은 보안 레벨로 변경하기 전에 *iSeries 보안 참조서* 제 2 장에 있는 내용을 검토하십시오.
2. 제한된 문자는 메세지 파일 QSYS/QCPFMSG의 메세지 ID CPXB302에 저장되어 있습니다. 이 문자들은 AEIOU@$#로 제공됩니다. CHGMSGD(메세지 설명 변경) 명령을 사용하여 제한 문자를 변경할 수 있습니다. QPWDLMTCHR 시스템 값은 암호 레벨 2 또는 3에서 시행되지 않습니다.

CFGSYSSEC 명령은 또한 다음과 같은 IBM 제공 사용자 프로파일에 대해 암호를 *NONE으로 설정합니다.

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

마지막으로 CFGSYSSEC 명령은 CHGSECAUD(보안 감사 변경) 명령을 사용하여 보안 감사를 설정합니다. CFGSYSSEC 명령은 조치 및 오브젝트 감사를 켜고, CHGSECAUD 명령에서 감사할 디폴트 조치 세트를 지정합니다.

프로그램 사용자 정의

이러한 설정 중 일부가 설치에 적합하지 않은 경우, 명령을 처리할 자체의 프로그램 버전을 작성할 수 있습니다. 다음을 수행하십시오.

__ 단계 1. RTVCLSRC(CL 소스 검색) 명령을 사용하여 CFGSYSSEC 명령을 사용할 때 실행되는 프로그램에 대한 소스를 복사하십시오. 검색할 프로그램은 QSYS/QSECCFGS입니다. 검색할 때 이 프로그램에 *다른 이름*을 제공하십시오.

__ 단계 2. 프로그램을 편집하여 변경하십시오. 그런 다음 컴파일하십시오. 컴파일할 때 IBM 제공 QSYS/QSECCFGS 프로그램을 대체하지 *마십시오*. 프로그램은 다른 이름이어야 합니다.

__ 단계 3. CHGCMD(명령 변경) 명령을 사용하여 CFGSYSSEC 명령에 대한 명령(PGM) 매개변수를 처리할 프로그램을 변경하십시오. PGM 값을 프로그램 명으로 설정하십시오. 예를 들면, QGPL 라이브러리에 MYSECCFG라는 프로그램을 작성하려면 다음과 같이 입력하십시오.

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

주: QSYS/QSECCFGS 프로그램을 변경하는 경우, IBM은 이 프로그램의 신뢰성, 서비스 가능성, 성능 또는 기능을 보증할 수 없습니다. 특정 목적을 위한 판매 가능성 및 적합성에 대한 암시적 보증에 대한 권리는 포기합니다.

공용 권한 취소 명령의 기능

RVKPUBAUT(공용 권한 취소) 명령을 사용하여 명령 및 프로그램에 대해 공용 권한을 *EXCLUDE로 설정할 수 있습니다. RVKPUBAUT 명령은 QSYS/QSECRVKP라는 프로그램을 실행합니다. QSECRVKP는 제공된 경우, 표 11 및 표 12에 나열된 어플리케이션 프로그래밍 인터페이스(API)에 대해 공용 권한을 *EXCLUDE로 설정하여 공용 권한을 취소합니다. 시스템이 도착하면 이러한 명령 및 API는 공용 권한을 *USE로 설정합니다.

표 11 및 표 12에 나열된 API 시스템 모두에서 손해가 생길 수 있는 기회를 제공하는 기능을 수행합니다. 보안 관리자로서 모든 시스템 사용자가 이러한 명령 및 프로그램을 사용할 수 있도록 하는 대신, 그 명령 및 프로그램을 실행하도록 사용자에게 명시적으로 권한을 부여해야 합니다.

RVKPUBAUT 명령을 실행할 때 명령이 들어 있는 라이브러리를 지정하십시오. 디폴트는 QSYS 라이브러리입니다. 시스템에서 둘 이상의 자국어를 사용할 경우, 각 QSYSxxx 라이브러리에 대해 명령을 실행해야 합니다.

표 11. RVKPUBAUT 명령으로 공용 권한이 설정되는 명령

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

표 12의 모든 API는 QSYS 라이브러리에 있습니다.

표 12. RVKPUBAUT 명령으로 공용 권한이 설정되는 프로그램

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

RVKPUBAUT 명령을 실행하면, 시스템은 루트 디렉토리에 대한 공용 권한(이미 *USE 이하가 아닌 경우)을 *USE로 설정합니다.

프로그램 사용자 정의

이러한 설정 중 일부가 설치에 적합하지 않은 경우, 명령을 처리할 자체의 프로그램 버전을 작성할 수 있습니다. 다음을 수행하십시오.

__ 단계 1. RTVCLSRC(CL 소스 검색) 명령을 사용하여 RVKPUBAUT 명령을 사용할 때 실행되는 프로그램에 대한 소스를 복사하십시오. 검색할 프로그램은 QSYS/QSECRVKP입니다. 검색할 때 이 프로그램에 *다른 이름*을 제공하십시오.

__ 단계 2. 프로그램을 편집하여 변경하십시오. 그런 다음 컴파일하십시오. 컴파일할 때 IBM 제공 QSYS/QSECCFGS 프로그램을 대체하지 *마십시오*. 프로그램은 다른 이름이어야 합니다.

__ 단계 3. CHGCMD(명령 변경) 명령을 사용하여 RVKPUBAUT 명령에 대한 명령(PGM) 매개변수를 처리할 프로그램을 변경하십시오. PGM 값을 프로그램 명으로 설정하십시오. 예를 들면, QGPL 라이브러리에 MYRVKPGM이라는 프로그램을 작성하려면 다음과 같이 입력하십시오.

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

주: QSYS/QSECRVKP 프로그램을 변경하는 경우, IBM은 이 프로그램의 신뢰성, 서비스 가능성, 성능 또는 기능을 보증할 수 없습니다. 특정 목적을 위한 판매 가능성 및 적합성에 대한 암시적 보증에 대한 권리는 포기합니다.

제 2 부 고급 iSeries 보안

제 5 장 오브젝트 권한을 사용하여 정보 자산 보호

보안 관리자로서의 임무는 시스템 사용자에게 불편을 주지 않으면서 조직의 정보 자산을 보호하는 것입니다. 사용자가 그들의 작업을 수행하는 데에는 충분한 권한을 부여하면서도, 시스템 전체 열람 및 권한이 없는 변경을 수행하는 것을 방지하도록 해야 합니다.

보안 추가 정보

너무 엄격한 권한은 예상에 어긋난 결과를 초래할 수 있습니다. 사용자들은 때로 권한이 너무 엄격하게 제한될 경우 서로 암호를 공유하는 등의 부작용을 야기할 수 있습니다.

OS/400 오퍼레이팅 시스템은 통합 오브젝트 보안을 제공합니다. 사용자는 시스템에서 오브젝트 액세스를 위해 제공하는 인터페이스를 사용해야 합니다. 예를 들어, 데이터베이스 파일에 액세스하려면 데이터베이스 파일 액세스용 명령 또는 프로그램을 사용해야 합니다. 메세지 대기행렬 또는 작업 기록부용 명령은 사용할 수 없습니다.

오브젝트에 액세스하기 위해 시스템 인터페이스를 사용할 때마다, 시스템은 사용자에게 해당 인터페이스에 필요한 오브젝트 권한이 있는지 검증합니다. 오브젝트 권한은 시스템의 자산 보호를 위한 강력하고 융통성 있는 툴입니다. 보안 관리자로서 과제는 관리 및 유지보수할 수 있는 효율적인 오브젝트 보안 체계를 설정하는 것입니다.

오브젝트 권한 강행

오브젝트 액세스를 시도할 때마다 오퍼레이팅 시스템에서 해당 오브젝트에 대한 사용자의 권한을 검사합니다. 그러나 시스템의 보안 레벨(QSECURITY 시스템 값)이 10 또는 20으로 설정된 경우, 모든 사용자 프로파일에 *ALLOBJ 특수 권한이 있으므로 모든 사용자는 자동으로 모든 오브젝트에 대한 액세스 권한을 갖습니다.

오브젝트 권한 추가 정보: 오브젝트 보안을 사용하고 있는지 알 수 없을 경우, QSECURITY(보안 레벨) 시스템 값을 검사하십시오. QSECURITY가 10 또는 20인 경우에는 오브젝트 보안을 사용하고 있지 않습니다.

보안 레벨을 30 이상으로 변경하기 전에 먼저 계획 및 준비를 해야 합니다. 그렇지 않을 경우, 사용자가 필요한 정보를 액세스하는 것이 불가능할 수 있습니다.

Information Center의 **기본적인 시스템 보안 및 계획** 주제에서 어플리케이션 분석 및 오브젝트 보안 설정 방법을 결정하기 위한 방법을 제공합니다. 아직 오브젝트 보안을 사용하지 않고 있거나 오브젝트 보안 체계가 오래된 복잡한 것이면 이 장을 읽고 시작하는 것이 좋습니다.

메뉴 보안

iSeries 서버는 원래 S/36 및 S/38의 후속 제품으로 설계되었습니다. 이전에는 여러 iSeries 서버 설치가 S/36 설치 또는 S/38 설치였습니다. 이러한 이전 시스템의 보안 관리자는 사용자가 수행할 수 있는 사항을 제어하기 위해 대체로 **메뉴 보안** 또는 **메뉴 액세스 제어**라는 기법을 사용했습니다.

메뉴 액세스 제어의 의미는 사용자가 사인 온할 때 사용자는 메뉴를 보게 됩니다. 사용자는 메뉴에 있는 기능만 수행할 수 있습니다. 사용자는 메뉴에 없는 기능을 수행하기 위해 시스템의 명령 행으로 갈 수 없습니다. 이론적으로는 메뉴 및 프로그램에서 사용자가 수행할 수 있는 사항을 제어하므로, 보안 관리자가 오브젝트 권한에 대해 우려할 필요는 없습니다.

iSeries 서버에서는 메뉴 액세스 제어를 지원하기 위한 여러 가지 사용자 프로파일 옵션을 제공합니다.

- 사용자가 사인 온한 후 맨 처음 보게 되는 메뉴를 제어하는 **초기 메뉴**(INLMNU) 매개변수.
- 사용자가 메뉴를 보기 전에 설정 프로그램을 실행하는 **초기 프로그램**(INLPGM) 매개변수. 또는 INLPGM 매개변수를 사용하여 하나의 프로그램만 실행되도록 사용자를 제한할 수 있습니다.
- 사용자를 제한된 명령 세트로 제한하는 **능력 제한**(LMTCPB) 매개변수. 또한, 이 매개변수를 사용하면 사인 온 화면에서 사용자가 다른 초기 프로그램 또는 메뉴를 지정할 수 없습니다(LMTCPB 매개변수는 명령 행에서 입력된 명령만 제한합니다).

메뉴 액세스 제어 제한사항

지난 몇 년 동안 컴퓨터 및 컴퓨터 사용자에게 커다란 변화가 있었습니다. 사용자가 일부 자체 프로그래밍을 수행하여 IS 부서를 오프로드할 수 있도록 조회 프로그램 및 스프레드쉬트와 같은 여러 가지 툴을 사용할 수 있습니다. SQL 또는 ODBC와 같은 일부 툴은 정보를 열람할 수 있는 기능 및 정보를 변경할 수 있는 기능을 제공합니다. 메뉴 구조에서 이러한 툴이 작동할 수 있도록 하기란 매우 어려운 일입니다.

PC 및 컴퓨터간 네트워크가 고정 기능(『녹색 화면』) 워크스테이션을 빠른 속도로 대체하고 있습니다. 시스템이 네트워크에 참여하는 경우, 사용자는 사인 온 화면 또는 메뉴를 보지 않고도 시스템에 들어갈 수 있습니다.

메뉴 액세스 제어를 수행하는 보안 관리자에게는 다음과 같은 두 가지 기본 문제점이 있습니다.

- 사용자를 메뉴로 제한할 경우, 최신 툴을 사용하는 능력이 제한되므로, 사용자에게 불만이 있을 수 있습니다.
- 사용자를 제한하지 못할 경우, 메뉴 액세스 제어가 보호해야 할 중대한 기밀 정보에 위험이 생길 수 있습니다. 시스템이 네트워크에 참여할 경우, 메뉴 액세스 제어를 강행하는 능력이 줄어듭니다. 예를 들면, LMTCPB 매개변수는 대화식 세션의 명령 행에서 입력한 명령에만 적용됩니다. LMTCPB 매개변수 PC 파일 전송, FTP 또는 리모트 명령과 같은 통신 세션의 요구에 아무런 영향도 주지 않습니다.

오브젝트 보안을 사용하여 메뉴 액세스 제어 향상

시스템 연결시 사용할 수 있는 모든 새로운 옵션들 때문에 앞으로의 실용적인 측면에서 iSeries 서버 보안 체계는 메뉴 액세스 제어에만 의존할 수 없습니다. 여기서는 메뉴 액세스 제어를 보충하기 위해 오브젝트 보안 환경으로 이동하기 위한 제안사항을 제공합니다.

Information Center의 *기본적인 시스템 보안 및 계획* 주제에서는 현재 어플리케이션을 실행하기 위해 사용자가 오브젝트에 대해 가져야 하는 권한을 분석하는 방법을 설명합니다. 분석을 마친 후 사용자를 그룹에 할당하고 그룹에 적합한 권한을 부여할 수 있습니다. 이러한 접근 방법은 타당하고 논리적인 방법입니다. 그러나 시스템이 작동한 지 오래되어 많은 어플리케이션을 가지고 있을 경우, 어플리케이션을 분석하고 오브젝트 권한을 설정하는 타스크가 무리일 수 있습니다.

오브젝트 권한 추가 정보: 프로그램 소유자 권한을 허용하는 프로그램과 결합된 현재의 메뉴에서 메뉴 액세스 제어 이상의 전환을 제공합니다. 권한을 허용하는 프로그램과 프로그램을 소유하는 사용자 프로파일 모두 보호해야 합니다.

어플리케이션 및 오브젝트를 점차적으로 분석하는 반면에 현재의 메뉴를 사용하여 전환 환경 설정에 도움을 줄 수 있습니다. 다음은 OEMENU(주문 입력) 메뉴와 관련 파일 및 프로그램을 사용하는 예입니다.

예: 전환 환경 설정

이 예는 다음과 같은 가정 및 요구사항으로 시작합니다.

- 모든 파일이 라이브러리 ORDERLIB에 있습니다.
- 파일명을 전혀 알지 못합니다. 다른 파일에 대하여 메뉴 옵션에 필요한 권한도 알 수 없습니다.
- 메뉴 및 해당 메뉴가 호출하는 모든 프로그램이 ORDERPGM이라는 라이브러리에 있습니다.
- 시스템에서 사인 온할 수 있는 모든 사용자는 조회 또는 스프레드쉬트를 사용하여 모든 주문 파일, 고객 파일 및 항목 파일 정보를 열람할 수 있기를 원합니다.
- 현재의 사인 온 메뉴가 OEMENU인 사용자만 파일을 변경할 수 있습니다. 또한 변경하려면 사용자가 메뉴에 있는 프로그램을 사용해야 합니다.

- 보안 관리자 이외의 시스템 사용자에게는 *ALLOBJ 또는 *SECADM 특수 권한이 없습니다.

이 메뉴 액세스 제어 환경을 변경하여 조회에 필요한 사항을 충족시키려면 다음 단계를 수행하십시오.

__ 단계 1. 초기 메뉴가 OEMENU인 사용자 리스트를 작성하십시오.

PRTUSRPRF *ENVINFO(사용자 프로파일 인쇄) 명령을 사용하여 시스템의 모든 사용자 프로파일에 대한 환경을 나열할 수 있습니다. 이 보고서에는 초기 메뉴, 초기 프로그램 및 현재 라이브러리가 포함됩니다. 67 페이지의 그림 7은 이러한 보고서의 예를 나타냅니다.

__ 단계 2. 사인 온에 사용되지 않은 사용자 프로파일에서 OEMENU 오브젝트(*PGM 오브젝트 또는 *MENU 오브젝트)를 소유하도록 하십시오. 사용자 프로파일을 작동불가능하게 하거나 암호 *NONE을 갖도록 해야 합니다. 이 예의 경우, OEOWNER에서 OEMENU 프로그램 오브젝트를 소유한다고 가정하십시오.

__ 단계 3. OEMENU 프로그램 오브젝트를 소유하는 사용자 프로파일은 그룹 프로파일이 아니어야 합니다. 다음과 같은 명령을 사용할 수 있습니다.

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ 단계 4. OEMENU 프로그램을 변경하여 OEOWNER 사용자 프로파일 권한을 허용하십시오(CHGPGM 명령을 사용하여 USRPRF 매개변수를 *OWNER로 변경하십시오).

주: *MENU 오브젝트는 권한을 허용할 수 없습니다. OEMENU가 *MENU 오브젝트이면 다음 중 하나를 수행하여 이 예를 적용시킬 수 있습니다.

- 메뉴를 표시할 프로그램을 작성하십시오.
- 사용자가 OEMENU 메뉴에서 옵션을 선택할 때 실행되는 프로그램에 허용한 권한을 사용하십시오.

__ 단계 5. 다음 두 가지 명령을 입력하여 ORDERLIB의 모든 파일에 대한 공용 권한을 *USE로 설정하십시오.

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
   AUT(*USE)
```

*USE 권한을 선택할 경우, 사용자는 PC 파일 전송 또는 FTP를 사용하여 파일을 복사할 수 있습니다.

__ 단계 6. 다음을 입력하여 메뉴 프로그램을 소유하는 프로파일에 대한 *ALL 권한을 부여하십시오.

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

대부분 어플리케이션의 경우, 파일에 대한 *CHANGE 권한으로 충분합니다. 그러나 사용자의 어플리케이션에서 *CHANGE 이상의 권한이 필요한 기능(예를 들어, 실제 파일 멤버 비우기)을 수행할 수도 있습니다. 결국 어플리케이션을 분석하여 어플리케이션에 필요한 최소 권한만 제공해야 합니다. 그러나 전환 기간중에 *ALL 권한을 허용하여 권한 부족으로 야기될 수 있는 어플리케이션 실패를 방지합니다.

__ 단계 7. 다음을 입력하여 주문 라이브러리에 있는 프로그램에 대한 권한을 제한하십시오.

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

__ 단계 8. 다음을 입력하여 라이브러리에 있는 프로그램에 OEOWNER 프로파일 권한을 부여하십시오.

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
   AUT(*USE)
```

__ 단계 9. 각 사용자에 대해 다음을 입력하여 단계 1에서 식별한 사용자에게 메뉴 프로그램에 대한 권한을 부여하십시오.

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(user-profile-name) AUT(*USE)
```

이들 단계를 완료하면 명시적으로 제외되지 않은 모든 시스템 사용자는 ORDERLIB 라이브러리에 있는 파일을 액세스할 수는 있으나 변경할 수는 없습니다. OEMENU 프로그램에 대한 권한이 있는 사용자는 메뉴에 있는 프로그램을 사용하여 ORDERLIB 라이브러리에 있는 파일을 갱신할 수 있습니다. 이제 OEMENU 프로그램에 대한 권한이 있는 사용자만 이 라이브러리에 있는 파일을 변경할 수 있습니다. 오브젝트 보안과 메뉴 액세스 제어를 조합하여 파일을 보호합니다.

사용자 자료를 포함하고 있는 모든 라이브러리에 대해 비슷한 단계를 완료하면 데이터베이스 갱신 제어를 위한 간단한 체계가 작성됩니다. 이러한 방법은 승인된 메뉴 및 프로그램을 사용할 때를 제외하고 시스템 사용자가 데이터베이스 파일을 갱신할 수 없도록 합니다. 동시에 의사 결정 지원 툴 또는 다른 시스템이나 PC의 링크를 사용하여 보기, 분석 및 복사에 데이터베이스 파일을 사용할 수 있게 됩니다.

오브젝트 권한 추가 정보: 시스템이 네트워크에 참여할 경우, *USE 권한이 기대 이상의 권한을 제공할 수도 있습니다. 예를 들어, FTP를 사용하면 파일에 대해 *USE 권한이 있을 경우 파일을 다른 시스템(PC 포함)에 복사할 수 있습니다.

라이브러리 보안을 사용하여 메뉴 보안 보충

라이브러리의 오브젝트에 액세스하려면 오브젝트와 라이브러리 모두에 대한 권한이 있어야 합니다. 대부분의 조작에는 라이브러리에 대한 *EXECUTE 권한 또는 *USE 권한이 필요합니다.

상황에 따라서 라이브러리 권한을 오브젝트 보안을 위한 간단한 방법으로 사용할 수 있습니다. 예를 들면, 주문 입력 메뉴의 예에서 주문 입력 메뉴에 대한 권한이 있는 ORDERPGM 라이브러리에 있는 모든 프로그램을 사용할 수 있다고 가정하십시오. 개별 프로그램을 보안하기보다는 ORDERPGM 라이브러리에 대한 공용 권한을 *EXCLUDE로 설정할 수 있습니다. 그런 다음 라이브러리에 대한 *USE 권한을 특정 사용자 프로파일에 부여할 수 있으므로 라이브러리의 프로그램을 사용할 수 있습니다 (이 경우 프로그램에 대한 공용 권한이 *USE 이상이라고 가정합니다).

라이브러리 권한은 오브젝트 권한 관리를 위한 간편하고 효율적인 방법이 될 수 있습니다. 그러나 오브젝트에 대해 의도하지 않은 액세스를 제공하지 않도록 보안하려는 라이브러리의 내용을 잘 알고 있어야 합니다.

오브젝트 소유권 구성

시스템에 있는 오브젝트 소유권은 오브젝트 권한 체계에서 중요한 부분입니다. 디폴트로, 오브젝트 소유자는 오브젝트에 대해 *ALL 권한을 가집니다. *iSeries 보안 참조서* 책의 제 5 장은 오브젝트 소유권 계획에 대한 권장사항 및 예를 제공합니다. 몇 가지 추가 정보는 다음과 같습니다.

- 일반적으로 그룹 프로파일은 오브젝트를 소유할 수 없습니다. 그룹 프로파일이 오브젝트를 소유할 경우, 해당 그룹 멤버가 명시적으로 제외되지 않는 한 모든 그룹 멤버는 오브젝트에 대해 *ALL 권한을 가집니다.
- 허용한 권한을 사용할 경우, 프로그램을 소유하는 사용자 프로파일이 파일과 같은 어플리케이션 오브젝트도 소유해야 하는지 고려하십시오. 권한을 허용하는 프로그램 실행 사용자가 파일에 대해 *ALL 권한을 갖지 않기를 원합니다.

iSeries Navigator를 사용 중인 경우, 보안 **정책** 기능을 사용하여 변경을 완료할 수 있습니다. 추가 정보는 iSeries Information Center를 참조하십시오(세부사항은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오).

시스템 명령 및 프로그램에 대한 오브젝트 권한

다음의 권한은 IBM 제공 오브젝트로 제한할 경우의 몇 가지 제안사항입니다.

- 시스템에서 둘 이상의 자국어를 사용할 경우, 시스템에는 둘 이상의 시스템(QSYS) 라이브러리가 있게 됩니다. 시스템에는 시스템의 각 자국어에 대해 QSYSxxxx 라이브러리가 있습니다. 시스템 명령에 대한 액세스 제어를 위해 오브젝트 권한을 사용하는 경우, 시스템의 QSYS 라이브러리 및 모든 QSYSxxx 라이브러리에 있는 명령을 반드시 보안해야 합니다.
- System/38™ 라이브러리에서는 때로 제한하려는 명령과 동등한 기능을 갖는 명령을 제공합니다. QSYS38 라이브러리에 있는 동등한 명령을 반드시 제한하십시오.

- System/36™ 환경에 있는 경우, 추가 프로그램을 제한해야 합니다. 예를 들어 QY2FTML 프로그램은 System/36 파일 전송을 제공합니다.

보안 기능 감사

이 장은 시스템에 대한 보안의 효율성 감사 기술을 설명합니다. 시스템 보안을 감사하는 이유는 다음과 같습니다.

- 보안 계획이 완벽한지 여부를 평가하기 위해.
- 계획된 보안 제어가 제 자리를 잡고 작동 중인지 확인하기 위해. 이런 유형의 감사는 대개 일일 보안 관리의 일부로서 보안 담당자에 의해 수행됩니다. 또한 때로는 더 자세하게 내부 또는 외부 감사자에 의해 주기적인 보안 검토의 일부로서 수행됩니다.
- 시스템 보안이 시스템 환경의 변화에 따라가고 있는지를 확인하기 위해. 보안에 영향을 주는 변경의 몇 가지 예는 다음과 같습니다.
  - 시스템 사용자가 작성한 새 오브젝트
  - 시스템에 들어온 새로운 사용자
  - 오브젝트 소유권의 변경(권한 부여는 조정되지 않음)
  - 책임 변경(사용자 그룹 변경)
  - 임시 권한(시기 적절하게 철회되지 않음)
  - 설치된 새 제품
- 새 어플리케이션 설치, 상위 보안 레벨로의 이동 또는 통신 네트워크 설정과 같은 장차 발생할 수 있는 이벤트에 준비하기 위해.

이 장에서 설명하는 기술은 이러한 모든 상황에 적합합니다. 사용자가 감사하는 대상과 빈도는 조직의 규모와 보안 수요에 따라 다릅니다. 이 장의 목적은 감사 빈도에 대한 지침을 제공하기 보다는 사용할 수 있는 정보, 정보를 얻는 방법 및 필요한 이유를 설명하는 것입니다.

이 정보는 다음 세 부분으로 구성됩니다.

- 계획하고 감사할 수 있는 보안 항목의 체크 리스트.
- 시스템이 제공하는 감사 저널의 설정 및 사용에 대한 정보.
- 시스템에 대한 보안 정보를 수집하기 위해 사용할 수 있는 다른 기술.

보안 감사에는 iSeries 시스템에 대한 명령 사용 및 시스템의 기록부 및 저널 정보 액세스가 포함됩니다. 시스템의 보안 감사를 수행할 사람이 사용할 특수 프로파일을 작성할 수 있습니다. 감사자 프로파일은 시스템의 감사 특성을 변경할 수 있도록 *AUDIT 특수 권한이 필요합니다. 이 장에서 제안되는 감사 타스크의 일부는 *ALLOBJ 및 *SECADM 특수 권한을 갖는 사용자 프로파일이 필요합니다. 감사 기간이 종료했을 때 반드시 감사자 프로파일에 대한 암호를 *NONE으로 설정해야 합니다.

보안 감사에 대한 자세한 내용은 *보안 참조서* 책의 제 9 장을 참조하십시오.

사용자 프로파일 분석

DSPAUTUSR(권한이 있는 사용자 표시) 명령으로 시스템에 있는 모든 사용자의 전체 리스트를 표시하거나 인쇄할 수 있습니다. 리스트는 프로파일명 또는 그룹 프로파일명 별로 순서지정될 수 있습니다. 다음은 그룹 프로파일 순서의 한 예입니다.

```
                          권한이 있는 사용자 표시

                                 암호
그룹             사용자          최종          암호
프로파일         프로파일        변경일        없음      텍스트
DPTSM
                 ANDERSOR        08/04/0x                Roger Anders
                 VINCENTM        09/15/0x                Mark Vincent
DPTWH
                 ANDERSOR        08/04/0x                Roger Anders
                 WAGNERR         09/06/0x                Rose Wagner
QSECOFR
                 JONESS          09/20/0x                Sharon Jones
                 HARRISOK        08/29/0x                Ken Harrison
*NO GROUP
                 DPTSM           09/05/0x    X           Sales and Marketing
                 DPTWH           08/13/0x    X           Warehouse
                 RICHARDS        09/05/0x                Janet Richards
                 SMITHJ          09/18/0x                John Smith
```

선택된 사용자 프로파일 인쇄

DSPUSRPRF(사용자 프로파일 표시) 명령을 사용하여 조회 툴을 사용하여 처리할 수 있는 출력 파일을 작성할 수 있습니다.

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

조회 툴을 사용하여 다음과 같이 출력 파일의 다양한 분석 보고서를 작성할 수 있습니다.

- *ALLOBJ 및 *SPLCTL 특수 권한을 모두 갖는 모든 사용자 리스트.
- 초기 프로그램 또는 사용자 등급과 같은 사용자 프로파일 필드에 의해 순서가 지정된 모든 사용자 리스트.

조회 프로그램을 작성하여 출력 파일로부터 여러 가지 보고서를 생성할 수 있습니다. 예를 들면, 다음과 같습니다.

- UPSPAU 필드가 *NONE이 아닌 레코드를 선택하여 임의의 특수 권한을 갖는 모든 사용자 프로파일을 나열합니다.
- *기능 제한* 필드(모델 데이터베이스 출력파일에서 UPLTCP라고 부름)가 *NO 또는 *PARTIAL이 아닌 레코드를 선택하여 명령을 입력할 수 있는 모든 사용자를 나열합니다.
- 특정 초기 메뉴 또는 초기 프로그램을 갖는 모든 사용자를 나열합니다.
- 최종 사인 온 날짜 필드를 찾아서 비활동 사용자를 나열합니다.

큰 사용자 프로파일 검사

시스템의 대부분에 무작위로 퍼져 있는 것으로 나타나고 많은 수의 권한을 갖는 사용자 프로파일은 보안 계획의 약점을 반영할 수 있습니다. 다음은 큰 사용자 프로파일을 찾아서 평가하는 한 가지 방법입니다.

1. 시스템의 모든 사용자 프로파일에 대한 정보가 들어 있는 출력 파일을 작성하려면 DSPOBJD(오브젝트 설명 표시) 명령을 사용하십시오.

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. 각 사용자 프로파일의 이름과 *크기*를 *크기*별로 내림차순으로 나열하려면 조회 프로그램을 작성하십시오.
3. 가장 큰 사용자 프로파일에 대한 상세 정보를 인쇄하고 권한 및 소유 오브젝트를 평가하여 적절한지 확인하십시오.

   ```
   DSPUSRPRF USRPRF(user-profile-name) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(user-profile-name) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   일부 IBM 제공 사용자 프로파일은 프로파일이 소유하는 오브젝트 수 때문에 매우 큽니다. 이 프로파일을 나열하고 분석하는 것은 대개 불필요합니다. 그러나, QSECOFR 및 QSYS와 같이 *ALLOBJ 특수 권한을 갖는 IBM 제공 사용자 프로파일의 권한을 허용하는 프로그램은 점검해야 합니다.

보안 감사에 대한 자세한 내용은 *보안 참조서* 책의 제 9 장을 참조하십시오.

오브젝트 권한 분석

다음 방법을 사용하여 시스템의 라이브러리에 대한 권한을 갖는 사람을 판별할 수 있습니다.

1. DSPOBJD 명령을 사용하여 시스템의 모든 라이브러리를 나열합니다.

   ```
   DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
   ```

   주: 사용이 불가능한 상태인 독립 보조 기억장치 풀의 라이브러리는 이 명령에 의해 표시되지 않습니다.

2. DSPOBJAUT(오브젝트 권한 표시) 명령을 사용하여 특정 라이브러리에 대한 권한을 나열합니다.

   ```
   DSPOBJAUT OBJ(QSYS/library-name) OBJTYPE(*LIB) +
             ASPDEV(asp-device-name) OUTPUT(*PRINT)
   ```

3. DSPLIB(라이브러리 표시) 명령을 사용하여 라이브러리의 오브젝트를 나열합니다.

   ```
   DSPLIB LIB(QSYS/library-name) ASPDEV(asp-device-name) OUTPUT(*PRINT)
   ```

이들 보고서를 사용하여 라이브러리에 무엇이 있고 누가 라이브러리에 액세스하는지 판별할 수 있습니다. 필요한 경우, DSPOBJAUT 명령을 사용하여 라이브러리에 있는 선택된 오브젝트에 대한 권한을 볼 수도 있습니다.

수정된 오브젝트 검사

CHKOBJITG(오브젝트 무결성 검사) 명령을 사용하여 수정된 오브젝트를 찾을 수 있습니다. 수정된 오브젝트는 대개 누군가가 사용자 시스템을 침입하려고 시도 중임을 표시합니다. 다음을 수행한 후 이 명령을 실행할 수 있습니다.

- 시스템에 프로그램을 저장
- 전용 서비스 툴(DST) 사용

명령을 실행할 때, 시스템은 모든 잠재적인 무결성 문제점에 대한 정보가 들어 있는 데이터베이스 파일을 작성합니다. 한 프로파일, 여러 다른 프로파일 또는 모든 프로파일이 소유하는 오브젝트를 검사할 수 있습니다. 정의역이 수정된 오브젝트를 찾을 수 있습니다. 또한 프로그램 유효성 검사 값을 다시 계산하여 *PGM, *SRVPGM, *MODULE 및 *SQLPKG 유형을 갖고 수정된 오브젝트를 찾을 수도 있습니다.

CHKOBJITG 프로그램을 실행하려면 *AUDIT 특수 권한이 필요합니다. 명령이 수행하는 스캔 및 계산 때문에 명령이 실행하는 데 긴 시간이 소요될 수 있습니다. 시스템이 바쁘지 않을 때 이 명령을 실행해야 합니다.

주: 많은 개인 권한을 갖는 많은 오브젝트를 소유하는 프로파일은 매우 커질 수 있습니다. 소유자 프로파일 크기는 소유된 오브젝트에 대한 권한에 대해 작업하고 표시할 때와 프로파일을 저장하거나 복원할 때 성능에 영향을 줍니다. 시스템 조작도 영향을 받을 수 있습니다. 성능이나 시스템 조작에 대한 영향을 막기 위해, 오브젝트 소유권을 복수 프로파일에 분산하십시오. **단 하나의 소유자 프로파일에 모든(또는 거의 모든) 오브젝트를 지정하지 마십시오.**

허용된 권한 분석 프로그램

*ALLOBJ 특수 권한을 갖는 사용자의 권한을 허용하는 프로그램은 보안 노출을 의미합니다. 다음 방법을 사용하여 이들 프로그램을 찾고 검사할 수 있습니다.

1. *ALLOBJ 특수 권한을 갖는 각 사용자에 대해, DSPPGMADP(허용한 프로그램 표시) 명령을 사용하여 해당 사용자의 권한을 허용한 프로그램을 나열합니다.

```
DSPPGMADP USRPRF(user-profile-name) +
          OUTPUT(*PRINT)
```

주: 54 페이지의 『선택된 사용자 프로파일 인쇄』 주제는 *ALLOBJ 권한을 갖는 사용자를 나열하는 방법을 표시합니다.

2. DSPOBJAUT 명령을 사용하여 각 허용 프로그램을 사용할 권한이 있는 사람과 해당 프로그램에 대한 공용 권한이 무엇인지를 판별합니다.

```
DSPOBJAUT OBJ(library-name/program-name) +
          OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
          OUTPUT(*PRINT)
```

3. 소스 코드 및 프로그램 설명을 조사하여 다음을 평가합니다.
   - 프로그램의 사용자가 허용된 프로파일에서 실행하는 동안 명령행 사용과 같은 액세스 기능이 금지되는지 여부.
   - 프로그램이 의도한 기능에 필요한 최소 권한 레벨을 허용하는지 여부. 프로그램 실패를 사용하는 어플리케이션은 오브젝트 및 프로그램의 동일한 소유자 프로파일을 사용하여 설계될 수 있습니다. 프로그램 소유자의 권한이 허용될 때, 사용자는 어플리케이션 오브젝트에 대해 *ALL 권한을 갖습니다. 많은 경우에, 소유자 프로파일에는 특수 권한이 필요없습니다.
4. DSPOBJD 명령을 사용하여 프로그램이 최종 변경된 시기를 확인합니다.

```
DSPOBJD OBJ(library-name/program-name) +
        OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
        DETAIL(*FULL)
```

감사 저널 및 저널 리시버 관리

감사 저널인 QSYS/QAUDJRN은 단지 보안 감사를 위한 것입니다. 오브젝트를 감사 저널에 저널해서는 안됩니다. 확약 제어가 감사 저널을 사용해서는 안됩니다. 사용자 항목이 SNDJRNE(저널 항목 송신) 명령이나 QJOSJRNE(저널 항목 송신) API를 사용하여 이 저널에 송신되지 않아야 합니다.

시스템이 감사 저널에 감사 항목을 기록할 수 있도록 보장하기 위해 특수 잠금 보호가 사용됩니다. 감사가 활동할 때(QAUDCTL 시스템 값이 *NONE이 아닐 때), 시스템 조정자 작업(QSYSARB)이 QSYS/QAUDJRN 저널에 대한 잠금을 보유합니다. 감사가 활동할 때는 감사 저널에 다음과 같은 조작을 수행할 수 없습니다.

- DLTJRN 명령
- ENDJRNxxx 명령
- APYJRNCHG 명령
- RMVJRNCHG 명령
- DMPOBJ 또는 DMPSYSOBJ 명령
- 저널 이동
- 저널 복원

- GRTOBJAUT 명령과 같이 권한에 대해 작업하는 조작
- WRKJRN 명령

보안 저널 항목에 기록되는 정보는 *보안 참조서* 책에 설명되어 있습니다. 감사 저널의 모든 보안 항목은 저널 코드 T를 갖습니다. 보안 항목에 추가하여 시스템 항목도 저널 QAUDJRN에 나타납니다. 이들은 저널 코드 J를 갖는 항목이며, 초기 프로그램 로드 (IPL) 및 저널 리시버에 대해 수행되는 일반 조작(예를 들면, 리시버 저장)과 관련됩니다.

저널이나 현재 리시버에 손상이 발생하여 감사 항목이 저널될 수 없는 경우, QAUDENDACN 시스템 값에 의해 시스템이 취하는 조치가 판별됩니다. 손상된 저널 또는 저널 리시버로부터의 회복은 다른 저널의 경우와 같습니다.

시스템이 저널 리시버의 변경을 관리할 수도 있습니다. QAUDJRN 저널을 작성할 때 MNGRCV(*SYSTEM)을 지정하거나, 저널을 해당 값으로 변경하십시오. MNGRCV(*SYSTEM)을 지정하면, 리시버가 임계 크기에 도달할 때 자동으로 리시버를 분리하고 새 저널 리시버를 작성하여 접속합니다. 이를 **시스템 변경 저널 관리**라고 합니다. 자세한 내용은 iSeries Information Center --> 시스템 관리 --> 저널 관리 --> 로컬 저널 관리 --> 관리 저널을 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

제 6 장 권한 관리

시스템에서 권한이 설정되는 방법을 추적하기 위해 보안 보고서 세트를 사용할 수 있습니다. 이러한 보고서를 초기에 실행하면 모든 사항(예: 모든 파일 또는 모든 프로그램에 대한 권한)을 인쇄할 수 있습니다.

정보의 기초를 설정한 후, 변경된 버전의 보고서를 정기적으로 실행할 수 있습니다. 변경된 버전으로 시스템에서 주의를 요하는 보안 관련 변경사항을 식별할 수 있습니다. 예를 들면, 파일에 대한 공용 권한을 나타내는 보고서를 매주 실행할 수 있습니다. 변경된 버전의 보고서만 요구할 수 있습니다. 이 보고서는 시스템에서 모든 사용자가 사용할 수 있는 새 파일과 최종 보고서 이후 공용 권한이 변경된 기존 파일을 나타냅니다.

보안 툴을 실행하려는 경우, 다음 두 가지 메뉴를 사용할 수 있습니다.

- 프로그램을 대화식으로 실행하려면 SECTOOLS 메뉴를 사용하십시오.
- 프로그램 일괄처리로 실행하려면 SECBATCH 메뉴를 사용하십시오. SECBATCH 메뉴는 두 부분으로 되어 있는데, 하나는 작업을 작업 대기행렬에 즉시 제출하기 위한 것이고 다른 하나는 작업을 작업 스케줄러에 배치하기 위한 것입니다.

iSeries Navigator를 사용하는 경우, 다음 단계를 따라 보안 툴을 실행하십시오.

1. iSeries Navigator에서 서버 --> **보안**을 펼치십시오.
2. **정책**을 마우스 오른쪽 버튼으로 클릭하고 **탐색**을 선택하여 작성 및 관리할 수 있는 정책 리스트를 표시하십시오.

오브젝트에 대한 공용 권한 모니터

편리한 사용과 성능 향상을 위해 대부분 시스템이 사용자가 오브젝트를 사용할 수 있도록 설정됩니다. 사용자들에게 모든 오브젝트를 사용하도록 명시적으로 권한이 부여되기보다는 일부 기밀의 보안에 민감한 오브젝트에 대한 액세스가 명시적으로 거부됩니다. 보안 요구사항이 높은 소수의 시스템은 정반대의 접근 방식을 취하며 알아야 할 기준으로 오브젝트에 대한 권한을 부여합니다. 그러한 시스템에서 대부분의 오브젝트가 공용 권한을 *EXCLUDE로 설정하여 작성됩니다.

iSeries은 여러 가지 유형의 오브젝트가 있는 오브젝트 기반 시스템입니다. 대부분의 오브젝트 유형에는 민감한 정보가 들어 있지 않으며, 보안 관련 기능을 수행하지 않습니다. 일반 보안 요구사항을 가진 iSeries 시스템의 보안 관리자로서 데이터베이스 파일 및 프로그램과 같이 보호가 필요한 오브젝트에 주의를 기울일 수 있습니다. 다른 오브젝트 유형에 대해서는 어플리케이션에 충분한 공용 권한을 설정하기만 하면 되는데, 대부분의 오브젝트 유형에 대한 권한은 *USE 권한입니다.

PRTPUBAUT(공용 권한 인쇄) 명령을 사용하여 공용 사용자가 액세스할 수 있는 오브젝트에 대한 정보를 인쇄할 수 있습니다(**공용 사용자**는 오브젝트에 대한 명시적인 권한 없이 사인 온 권한을 가진 사용자를 말합니다). PRTPUBAUT 명령을 사용하면 검토하려는 오브젝트 유형 및 라이브러리 또는 디렉토리를 지정할 수 있습니다. 가장 공통적으로 보안 관련사항이 들어 있는 오브젝트 유형에 대한 공용 권한 부여 오브젝트 보고서를 인쇄하기 위해 SECBATCH 및 SECTOOLS 메뉴에서 옵션을 사용할 수 있습니다. 이 보고서의 변경된 버전을 정기적으로 인쇄하여 주의를 요하는 오브젝트를 알아볼 수 있습니다.

신규 오브젝트에 대한 권한 관리

OS/400은 시스템의 새 오브젝트에 대한 권한 및 소유권 관리에 도움이 되는 기능을 제공합니다. 사용자가 새 오브젝트를 작성하면 시스템에서 다음 사항을 판별합니다.

- 오브젝트 소유자
- 오브젝트에 대한 공용 권한
- 오브젝트에 개인 권한이 있는지 여부
- 오브젝트의 위치(라이브러리 또는 디렉토리)
- 오브젝트에 대한 액세스 감사 여부

시스템은 이러한 결정을 하기 위해 시스템 값, 라이브러리 매개변수 및 사용자 프로파일 매개변수를 사용합니다. *iSeries 보안 참조서* 제 5 장의 『새 오브젝트 권한 및 소유권 지정』에서 사용할 수 있는 옵션에 대한 몇 가지 예를 제공합니다.

PRTUSRPRF 명령을 사용하여 새 오브젝트에 대한 소유권과 권한에 영향을 주는 사용자 프로파일 매개변수를 인쇄할 수 있습니다. 66 페이지의 그림 5는 이러한 보고서의 예를 나타냅니다.

권한 부여 리스트 모니터

권한 부여 리스트를 사용하여 유사한 보안 요구사항이 있는 오브젝트를 그룹화할 수 있습니다. 개념상으로 권한 부여 리스트에 사용자 리스트 및 리스트에 의해 보안되는 오브젝트에 대한 사용자의 권한이 포함됩니다. 권한 부여 리스트는 시스템에 있는 유사한 오브젝트 권한을 관리할 수 있는 효율적인 방법을 제공합니다. 그러나 일부의 경우 오브젝트에 대한 권한 추적을 어렵게 할 수 있습니다.

PRTPVTAUT(개인 권한 인쇄) 명령을 사용하여 권한 부여 리스트 권한에 대한 정보를 인쇄할 수 있습니다. 61 페이지의 그림 3은 샘플 보고서를 나타냅니다.

개인 권한(전체 보고서)

SYSTEM4

권한 부여 리스트	소유자	1차 그룹	사용자	권한	리스트 Mgt	리스트 Opr	오브젝트 Mgt	오브젝트 있음	오브젝트 변경	오브젝트 Ref	자료 읽기	자료 추가	자료 갱신	자료 삭제	자료 실행
LIST1	QSECOFR	*NONE	*PUBLIC	*EXCLUDE											
LIST2	BUDNIKR	*NONE	BUDNIKR	*ALL	X	X	X	X	X	X	X	X	X	X	X
			*PUBLIC	*CHANGE		X					X	X	X	X	X
LIST3	QSECOFR	*NONE	*PUBLIC	*EXCLUDE											
LIST4	CJWLDR	*NONE	CJWLDR	*ALL	X	X	X	X	X	X	X	X	X	X	X
			GROUP1	*ALL		X	X	X	X	X	X	X	X	X	X
			*PUBLIC	*EXCLUDE											

그림 3. 권한 부여 리스트에 대한 개인 권한 보고서

이 보고서는 EDTAUTL(권한 부여 리스트 편집) 화면에 표시된 것과 동일한 정보를 나타냅니다. 이 보고서의 장점은 모든 권한 부여 리스트에 관한 정보를 한 곳에 제공한다는 것입니다. 예를 들어, 새 오브젝트 그룹에 대해 보안을 설정하는 경우, 보고서를 신속히 스캔하여 기존의 권한 부여 리스트가 그 오브젝트에 대한 사용자의 요구에 맞는지 확인할 수 있습니다.

보고서의 변경된 버전을 인쇄하여 새 권한 부여 리스트 또는 보고서를 마지막으로 인쇄한 이후의 권한 변경사항이 있는 권한 부여 리스트를 볼 수 있습니다. 또한, 각 권한 부여 리스트에 의해 보안되는 오브젝트 리스트를 인쇄할 수 있는 옵션도 있습니다. 그림 4에서 권한 부여 리스트에 대한 보고서의 예를 나타냅니다.

권한 부여 리스트 오브젝트 표시

```
권한 부여 리스트  . . . . . :   CUSTAUTL
라이브러리 . . . . . :     QSYS
소유자 . . . . . :   AROWNER
1차 그룹 . . . . . :   *NONE
```

오브젝트	라이브러리	유형	소유자	1차 그룹	텍스트
CUSTMAS	CUSTLIB	*FILE	AROWNER	*NONE	
CUSTORD	CUSTORD	*FILE	OEOWNER	*NONE	

그림 4. 권한 부여 리스트 오브젝트 보고서 표시 화면

예를 들면, 이 보고서를 사용하여 새 사용자를 권한 부여 리스트(사용자가 수신하게 될 권한)에 추가한 결과를 알 수 있습니다.

권한 부여 리스트 사용

iSeries Navigator는 보안 계획 및 정책 개발을 지원하고 회사에서 필요로 하는 사항을 만족시키는 시스템을 구성하기 위해 설계된 보안 피처를 제공합니다. 사용할 수 있는 기능 중 하나는 권한 부여 리스트를 사용하는 기능입니다.

권한 부여 리스트에는 다음과 같은 피처가 있습니다.

- 권한 부여 리스트는 비슷한 보안 요구사항을 갖는 오브젝트를 그룹화합니다.

- 권한 부여 리스트는 개념상으로 사용자 리스트 및 리스트에 의해 보안되는 오브젝트에 대한 사용자의 권한을 포함합니다.
- 각 사용자와 그룹은 리스트가 보안하는 오브젝트 세트에 대해 서로 다른 권한을 가질 수 있습니다.
- 개별 사용자 및 그룹이 아닌 리스트를 통해 권한을 부여할 수 있습니다.

권한 부여 리스트를 사용하여 수행할 수 있는 타스크에는 다음이 포함됩니다.

- 권한 부여 리스트 작성
- 권한 부여 리스트 변경
- 사용자 및 그룹 추가
- 사용자 허가 변경
- 보안 오브젝트 표시

이 기능을 사용하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 서버 --> 보안을 펼치십시오. **권한 부여 리스트** 및 **정책**이 표시됩니다.
2. **권한 부여 리스트**를 마우스 오른쪽을 클릭한 후 **새 권한 부여 리스트**를 선택하십시오. **새 권한 부여 리스트** 창을 사용하여 다음을 수행할 수 있습니다.
   - **사용:** 오브젝트 속성에 대한 액세스와 오브젝트 사용을 허용합니다. 공개하게 되면 오브젝트를 열람할 수 있지만 변경할 수는 없습니다.
   - **변경:** 오브젝트 내용을 변경할 수 있습니다(일부 제외).
   - **모두:** 소유자로 제한되는 것을 제외한 모든 조작을 오브젝트에 수행할 수 있습니다. 사용자 또는 그룹은 오브젝트의 존재를 제어하고, 오브젝트에 대한 보안을 지정하고, 오브젝트를 변경하고 오브젝트에 대해 기본 기능을 수행할 수 있습니다. 사용자 또는 그룹은 오브젝트의 소유권을 변경할 수도 있습니다.
   - **제외:** 오브젝트에 대한 모든 조작이 금지됩니다. 이 권한을 갖는 사용자 및 그룹에 대한 오브젝트에 대한 액세스 또는 조작은 허용되지 않습니다. 공개하게 되면 오브젝트를 사용할 수 없도록 지정합니다.

권한 부여 리스트에 대해 작업할 때 오브젝트와 자료 모두에 대해 권한을 부여하기 원할 것입니다. 사용자가 선택할 수 있는 오브젝트 권한이 아래에 나열됩니다.

- **조작:** 오브젝트의 설명을 보고 사용자 또는 그룹이 오브젝트에 대해 갖는 자료 권한에 의해 판별되는 대로 오브젝트를 사용할 권한을 제공합니다.
- **관리:** 오브젝트에 대한 보안을 지정하고 오브젝트를 이동 또는 이름 변경하고 데이터베이스 파일에 멤버를 추가하는 권한을 제공합니다.
- **존재:** 오브젝트의 존재와 소유권을 제어하는 권한을 제공합니다. 사용자 또는 그룹은 오브젝트를 삭제하고, 오브젝트의 기억장치를 사용할 수 있게 하고, 오브젝트에 대한 저장 및 복원 작업을 수행하고, 오브젝트 소유권을 전송할 수 있습니다. 사용자 또는 그룹이 특수 저장 권한을 갖는 경우, 사용자 또는 그룹은 오브젝트 존재 권한이 필요없습니다.

- **수정**(데이터베이스 파일 및 SQL 패키지에만 사용됨): 오브젝트의 속성을 수정하는 데 필요한 권한을 제공합니다. 사용자 또는 그룹이 데이터베이스 파일에 대해 이 권한을 갖는 경우, 사용자 또는 그룹은 트리거를 추가 및 제거하고, 참조 및 고유 제한사항을 추가 및 제거하고, 데이터베이스 파일의 속성을 변경할 수 있습니다. 사용자 또는 그룹이 SQL 패키지에 대해 이 권한을 갖는 경우, 사용자 또는 그룹은 SQL 패키지의 속성을 변경할 수 있습니다. 이 권한은 현재 데이터베이스 파일 및 SQL 패키지에만 사용됩니다.
- **참조**(데이터베이스 파일 및 SQL 패키지에만 사용됨): 해당 오브젝트에 대한 조작이 다른 오브젝트에 의해 제한될 수 있도록 다른 오브젝트에서 오브젝트를 참조하는 데 필요한 권한을 제공합니다. 사용자 또는 그룹이 실제 파일(PF)에 대해 이 권한을 갖는 경우, 사용자 또는 그룹은 실제 파일이 상위인 참조 제한사항을 추가할 수 있습니다. 이 권한은 현재 데이터베이스 파일에만 사용됩니다.

사용자가 선택할 수 있는 자료 권한이 아래에 나열됩니다.

- **읽기:** 파일에 있는 레코드 보기와 같이 오브젝트의 내용을 입수하고 표시하는 데 필요한 권한을 제공합니다.
- **추가:** 메세지 대기행렬에 메세지 추가 또는 파일에 레코드 추가와 같이 오브젝트에 항목을 추가하는 권한을 제공합니다.
- **갱신:** 파일의 레코드 변경과 같이 오브젝트의 항목을 변경하는 권한을 제공합니다.
- **삭제:** 메세지 대기행렬에서 메세지 제거 또는 파일에서 레코드 제거와 같이 오브젝트에서 항목을 제거하는 권한을 제공합니다.
- **실행:** 프로그램, 서비스 프로그램 또는 SQL 패키지을 실행하는 데 필요한 권한을 제공합니다. 사용자는 또한 라이브러리나 디렉토리에서 오브젝트를 찾을 수 있습니다.

권한 부여 리스트를 작성 또는 편집할 때의 각 프로세스에 대한 추가 정보는 iSeries Navigator에 있는 사용 가능한 온라인 도움말을 사용하십시오.

iSeries Navigator에서 정책 액세스

iSeries Navigator를 사용하여 iSeries 서버의 정책을 보고 관리할 수 있습니다. iSeries Navigator에는 5개의 정책 영역이 있습니다.

- **감사 정책**
  이렇게 하면 특정 조치에 대한 모니터링을 설정하고 사용자 시스템에서 특정 자원에 액세스할 수 있습니다.
- **보안 정책**
  이렇게 하면 시스템 보안에 관련된 보안 레벨 및 추가 옵션을 지정할 수 있습니다.
- **암호 정책**
  이렇게 하면 해당 시스템의 암호 레벨을 지정할 수 있습니다.
- **복원 정책**
  이렇게 하면 특정 오브젝트를 해당 시스템에서 복원하는 방법을 지정할 수 있습니다.

- **사인 온 정책**
  이렇게 하면 사용자가 해당 시스템에 사인 온할 수 있는 방법을 지정할 수 있습니다.

iSeries Navigator를 사용하여 정책을 보거나 변경하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> **보안**을 펼치십시오.
2. **정책**을 마우스 오른쪽 버튼으로 클릭하고 **탐색**을 선택하여 작성 및 관리할 수 있는 정책 리스트를 표시하십시오. 이러한 정책에 대한 특정 사항은 iSeries Navigator 도움말을 참조하십시오.

오브젝트에 대한 개인 권한 모니터

SECBATCH 메뉴 옵션

12 *즉시 제출* **41** *작업 스케줄러 사용*

PRTPVTAUT(개인 권한 인쇄) 명령으로 사용자는 지정된 라이브러리에 있는 유형의 오브젝트에 대한 모든 개인 권한의 보고서를 인쇄할 수 있습니다.

이 보고서를 사용하여 오브젝트에 대한 새 권한을 감지할 수 있습니다. 또한, 개인 권한 체제가 얽혀서 관리할 수 없는 상태가 되지 않도록 할 수 있습니다.

출력 및 작업 대기행렬에 대한 액세스 모니터

때로는 보안 관리자가 파일에 대한 액세스 보안에만 신경쓴 나머지 파일 내용이 인쇄될 때 발생하는 사항에 대해 잊어버릴 수 있습니다. iSeries 서버는 사용자가 민감한 출력 대기행렬 및 작업 대기행렬을 보호할 수 있는 기능을 제공합니다. 예를 들어, 권한이 없는 사용자가 인쇄 대기중인 기밀 스풀 파일을 열람하거나 복사할 수 없도록 출력 대기행렬을 보호합니다. 권한이 없는 사용자가 기밀 작업을 비기밀 출력 대기행렬로 재지정하지 않거나 작업을 완전히 취소할 수 없도록 작업 대기행렬을 보호합니다.

SECBATCH 메뉴 옵션

24 즉시 제출 63 *작업 스케줄러 사용*

Information Center의 *기본적인 시스템 보안 및 계획* 및 *iSeries 보안 참조서* 책에서 출력 대기행렬 및 작업 대기행렬 보호 방법을 설명합니다.

PRTQAUT(대기행렬 권한 인쇄) 명령을 사용하여 시스템에 있는 작업 대기행렬 및 출력 대기행렬에 대한 보안 설정을 인쇄할 수 있습니다. 그런 다음, 기밀 정보를 인쇄하는 인쇄 작업을 평가하여 보호되는 출력 대기행렬 및 작업 대기행렬로 가게 할 수 있습니다.

보안에 민감하다고 생각되는 출력 대기행렬 및 작업 대기행렬에 대한 보안 설정을 *iSeries 보안 참조서* 부록 D에 있는 내용과 비교할 수 있습니다. 부록 D의 표는 여러 가지 출력 대기행렬 및 작업 대기행렬 기능을 수행하는 데 필요한 설정에 대해 설명합니다.

특수 권한 모니터

시스템의 사용자가 필요하지 않은 특수 권한이 있을 경우, 오브젝트 권한 체계 개발 노력이 무의미하게 될 수 있습니다. 사용자 프로파일이 *ALLOBJ 특수 권한이 있는 경우, 오브젝트 권한은 의미가 없습니다. *SPLCTL 특수 권한이 있는 사용자는 출력 대기행렬을 보안하기 위한 노력에 관계없이 시스템에서 스풀 파일을 볼 수 있습니다. *JOBCTL 특수 권한이 있는 사용자는 시스템 조작에 영향을 주고 작업을 재지정할 수 있습니다. *SERVICE 특수 권한이 있는 사용자는 서비스 툴을 사용하여 오퍼레이팅 시스템을 통하지 않고도 자료에 액세스할 수도 있습니다.

SECBATCH 메뉴 옵션

29 즉시 제출 68 *작업 스케줄러 사용*

PRTUSRPRF(사용자 프로파일 인쇄) 명령을 사용하여 시스템에 있는 사용자 프로파일의 특수 권한 및 사용자 클래스에 대한 내용을 인쇄할 수 있습니다. 보고서를 실행할 경우, 다음과 같은 몇 가지 옵션이 있습니다.

- 모든 사용자 프로파일
- 특정한 특수 권한이 있는 사용자 프로파일
- 특정 사용자 클래스가 있는 사용자 프로파일
- 사용자 클래스와 특수 권한 사이에 불일치가 있는 사용자 프로파일

그림 5는 모든 사용자 프로파일에 대한 특수 권한을 표시하는 보고서의 예를 보여줍니다.

```
                                                                사용자 프로파일 정보
  보고서 유형  . . . . . . . . . . :   *AUTINFO
  선택 기준  . . . . . . . . . . . :   *SPCAUT
  특수 권한  . . . . . . . . . . . :   *ALL
                    ---------------  특수 권한  ----------------
                                 *IO                                                                  그룹
사용자     그룹      *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL   사용자                 그룹       권한          제한
프로파일   프로파일   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL   클래스     소유자      권한       유형          기능
USERA      *NONE      X     X     X     X     X     X     X     X    *SECOFR    *USRPRF    *NONE      *PRIVATE      *NO
USERB      *NONE                        X     X                       *PGMR      *USRPRF    *NONE      *PRIVATE      *NO
USERC      *NONE      X     X     X     X     X     X     X     X    *SECOFR    *USRPRF    *NONE      *PRIVATE      *NO
USERD      *NONE                                                      *USER      *USRPRF    *NONE      *PRIVATE      *NO
```

그림 5. 사용자 정보 보고서: 예 1

보고서는 특수 권한 외에도 다음과 같은 사항이 있습니다.

- 사용자 프로파일에 제한된 기능이 있는지 여부
- 사용자 또는 사용자의 그룹이 사용자가 작성하는 새 오브젝트를 소요하는지 여부
- 사용자의 그룹이 사용자가 작성하는 새 오브젝트에 대해 자동으로 수신하는 권한

그림 6은 불일치 특수 권한 및 사용자 클래스에 대한 보고서의 예를 보여줍니다.

```
                                                  사용자 프로파일 정보
보고서 유형  . . . . . . . . . . :   *AUTINFO
선택 기준  . . . . . . . . . . . :   *MISMATCH
                    ---------------  특수 권한  ----------------
                                 *IO                                                                  그룹
사용자     그룹      *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL   사용자                 그룹       권한          제한
프로파일   프로파일   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL   클래스     소유자      권한       유형          기능
USERX      *NONE      X                 X     X                 X    *SYSOPR    *USRPRF    *NONE      *PRIVATE      *NO
USERY      *NONE                                    X                 *USER      *USRPRF    *NONE      *PRIVATE      *NO
USERZ                                               X                 *USER      *USRPRF    *NONE      *PRIVATE      *NO
           QPGMR                        X     X
```

그림 6. 사용자 정보 보고서: 예 2

그림 6에서 다음 사항에 유의하십시오.

- USERX에는 시스템 오퍼레이터(*SYSOPR) 사용자 클래스가 있지만 *ALLOBJ 및 *SPLCTL 특수 권한도 있습니다.
- USERY에 사용자(*USER) 사용자 클래스가 있지만 *SECADM 특수 권한이 있어야 합니다.
- USERZ 또한 사용자(*USER) 클래스 및 *SECADM 특수 권한이 있습니다. 또한, USERZ는 QPGMR 그룹의 멤버이며, 이 그룹은 *JOBCTL 및 *SAVSYS 특수 권한이 있음을 알 수 있습니다.

이 보고서를 정기적으로 실행하여 사용자 프로파일 관리를 모니터할 수 있습니다.

사용자 환경 모니터

사용자 프로파일의 한 가지 역할은 출력 대기행렬, 초기 메뉴 및 작업 설명을 포함하는 사용자 환경을 정의하는 것입니다. 사용자 환경은 사용자가 시스템을 보는 방법, 범위, 사용자가 수행할 수 있는 사항에 영향을 줍니다. 사용자는 사용자 프로파일에 지정된 오브젝트에 대한 권한이 있어야 합니다. 그러나 권한 체계가 아직 진행중이거나 그다지 제한적이지 않을 경우, 사용자 프로파일에 정의된 사용자 환경으로 인해 의도하지 않은 결과가 생길 수 있습니다. 다음은 몇 가지 예입니다.

SECBATCH 메뉴 옵션

29 *즉시 제출* **68** *작업 스케줄러 사용*

- 사용자의 작업 설명은 사용자보다 많은 권한을 가진 사용자 프로파일을 지정할 수 있습니다.
- 사용자의 초기 메뉴에는 명령 행이 없을 수 있습니다. 그러나 사용자의 주의 키 처리 프로그램에서 명령 행을 제공할 수도 있습니다.
- 사용자에게 기밀 보고서를 실행할 권한이 부여될 수 있습니다. 그러나 사용자의 출력은 보고서를 볼 수 없는 사용자가 사용할 수 있는 출력 대기행렬로 지정될 수도 있습니다.

PRTUSRPRF(사용자 프로파일 인쇄) 명령의 *ENVINFO 옵션을 사용하여 시스템 사용자에 대해 정의된 환경을 모니터할 수 있습니다. 그림 7은 이러한 보고서의 예를 나타냅니다.

```
                                                                  사용자 프로파일 정보
  보고서 유형  . . . . . :   *ENVINFO
  선택 기준  . . . . . :   *USRCLS
                          초기          초기          작업          메세지        출력          주의
사용자          현재      메뉴/         프로그램/     설명/         대기행렬/     대기행렬/     프로그램/
프로파일        라이브러리  라이브러리    라이브러리    라이브러리    라이브러리    라이브러리    라이브러리
AUDSECOFR       AUDITOR   MAIN          *NONE         QDFTJOBD      QSYSOPR       *WRKSTN       *SYSVAL
                          *LIBL                       QGPL           QSYS
USERA           *CRTDFT   OEMENU        *NONE         QDFTJOBD      USERA         *WRKSTN       *SYSVAL
                          *LIBL                       QGPL           QUSRSYS
USERB           *CRTDFT   INVMENU       *NONE         QDFTJOBD      USERB         *WRKSTN       *SYSVAL
                          *LIBL                       QGPL           QUSRSYS
USERC           *CRTDFT   PAYROLL       *NONE         QDFTJOBD      USERC         PAYROLL       *SYSVAL
                          *LIBL                       QGPL           QUSRSYS        PRPGMLIB
```

그림 7. 사용자 프로파일-사용자 환경 예 인쇄

서비스 툴 관리

사용자 서버를 구성, 관리 및 제공하는 데 서비스 툴을 사용합니다. 전용 서비스 툴(DST) 또는 시스템 서비스 툴(SST)에서 서비스 툴을 액세스할 수 있습니다. DST 및 SST에 액세스하고 논리 파티션의 iSeries Navigator 기능(LPAR) 관리 및 디스크 장치 관리를 사용하는 데 서비스 툴 사용자 ID가 있어야 합니다.

OS/400이 로드되지 않는 경우에도 사용권 내부 코드를 시작할 때 DST를 사용할 수 있습니다. SST는 OS/400에서 사용할 수 있습니다. 다음 표에서 DST 및 SST 간 기본 차이점을 간단하게 설명합니다.

특성	DST	SST
액세스 방법	수동 IPL 중 콘솔을 통해 또는 제어판에서 옵션 21을 선택하여 실제로 액세스.	QSRV로 사인 온하는 기능의 대화식 작업 또는 다음 권한을 통해 액세스. • STRSST(SST 시작) CL 명령에 대한 권한. • 서비스 특수 권한(*SERVICE) 또는 모든 오브젝트 특수 권한(*ALLOBJ). • SST 사용에 대한 기능적 권한.
사용 가능한 시기	서버가 기능을 제한할 때에도 사용 가능. OS/400이 DST에 액세스할 필요 없음.	OS/400이 시작되었을 때 사용 가능. OS/400이 SST에 액세스해야 함.
인증 방법	서비스 툴 사용자 ID 및 암호 필수.	서비스 툴 사용자 ID 및 암호 필수.

서비스 툴을 사용하여 다음 타스크를 수행하는 데 대한 내용은 iSeries Information Center --> 보안 --> 서비스 툴을 참조하십시오.

- DST를 사용한 서비스 툴 액세스
- SST를 사용한 서비스 툴 액세스
- iSeries Navigator를 사용한 서비스 툴 액세스
- 서비스 툴 사용자 ID 작성
- 서비스 툴 사용자 ID의 기능적 권한 변경
- 서비스 툴 사용자 ID의 설명 변경
- 서비스 툴 사용자 ID 표시
- 서비스 툴 사용자 ID 작동 가능 또는 불가능
- 서비스 툴 사용자 ID 삭제
- SST 또는 DST를 사용하여 서비스 툴 사용자 ID 및 암호 변경
- STRSST를 사용하여 서비스 툴 사용자 ID 암호 변경
- 서비스 툴 사용자 ID 및 암호 변경
- 서비스 툴 사용자 ID(QSYCHGDS) API 변경

- QSECOFR OS/400 사용자 프로파일 암호 재설정
- QSECOFR 서비스 툴 사용자 ID 및 암호 재설정
- 서비스 툴 보안 자료 저장 및 서비스 툴 보안 자료 복원
- QSECOFR 서비스 툴 사용자 ID의 버전 작성
- DST에 대해 서비스 툴 서버 구성
- OS/400에 대해 서비스 툴 서버 구성
- DST를 통해 모니터 서비스 기능 사용
- OS/400 보안 감사 로그를 통해 모니터 서비스 툴 사용

iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

제 7 장 논리 파티션 보안(LPAR) 사용

다음 시나리오에서 단일 iSeries 서버에 복수 논리 파티션을 갖는 것이 유익하다는 것을 알 수 있습니다.

- **독립 시스템 유지보수**: 자원(디스크 기억 장치, 프로세서, 메모리 및 I/O 장치)의 일부를 한 파티션에 대해서만 할당하면 소프트웨어의 논리적 분리가 이루어집니다. 논리 파티션은 또한 적절하게 구성되는 경우 어느 정도의 하드웨어 결함 허용 한계를 갖습니다. 단일 기계에서 함께 잘 실행하지 않을 수 있는 대화식 및 일괄처리 작업 부하가 별도의 파티션에 분리되어 효율적으로 실행할 수 있습니다.
- **통합**: 논리 파티션된 시스템은 기업망 내에서 필요한 iSeries 서버 시스템 수를 줄일 수 있습니다. 논리적으로 분할된 단일 파티션 시스템으로 여러 시스템을 통합할 수 있습니다. 이것으로 추가 장치가 필요없고 그에 따른 비용도 들어가지 않게됩니다. 필요사항이 변경되면 한 논리 파티션에서 다른 파티션으로 자원을 이동할 수 있습니다.
- **혼합 생산 및 테스트 환경 작성:** 혼합 생산 및 테스트 환경을 작성할 수 있습니다. 1차 파티션에 단일 생산 파티션을 작성할 수 있습니다. 복수 생산 파티션의 경우, 아래의 *복수 생산 파티션 환경 작성*을 참조하십시오.

  한 논리 파티션은 테스트 또는 생산 파티션입니다. 생산 파티션은 기본 비지니스 어플리케이션을 실행합니다. 생산 파티션이 실패하면 비지니스 조작이 많이 지연되고 시간과 비용이 들게 됩니다. 테스트 파티션은 소프트웨어를 테스트합니다. 테스트 파티션의 실패는, 계획할 필요는 없지만, 정상적인 비지니스 조작을 손상시키지 않습니다.
- **복수 생산 파티션 환경 작성:** 2차 파티션에만 복수 생산 파티션을 작성해야 합니다. 이 경우, 1차 파티션은 파티션 관리 전용으로 사용합니다.
- **핫 백업:** 2차 파티션이 동일 시스템 내의 다른 논리 파티션으로 복제될 때, 파티션 실패 중에 백업으로 교환하면 불편함을 최소화할 수 있습니다. 이 구성은 또한 긴 저장 창의 효과를 최소화합니다. 다른 논리 파티션이 계속 생산 작업을 수행하는 동안 백업 파티션을 오프라인으로 만들고 저장할 수 있습니다. 이 핫 백업 전략을 사용하려면 특별한 소프트웨어가 필요합니다.
- **통합 클러스터:** OptiConnect/400과 고가용성 어플리케이션 소프트웨어를 사용하여, 파티션 시스템이 통합 클러스터로서 실행할 수 있습니다. 통합 클러스터를 사용하여 2차 파티션 내의 대부분의 예약되지 않은 실패로부터 시스템을 보호할 수 있습니다.

주: 2차 파티션을 설정할 때, 카드 위치에 대해 추가로 고려해야 합니다. 콘솔에 대해 선택한 입/출력 프로세서(IOP)가 LAN 카드도 갖고 있고 LAN 카드가 Operations Console에 사용할 의도가 아닌 경우, 해당 카드가 콘솔이 사용하도록 활성화되고 사용자는 의도한 목적으로 LAN 카드를 사용할 수 없을 것입니다. Operations Console에 대한 작업에 대해 자세히 알려면, 75 페이지의 제 8 장 『iSeries Operations Console』을 참조하십시오.

이 주제에 대한 자세한 내용은 iSeries Information Center의 ″논리 파티션″을 참조하십시오.

논리 파티션에 대한 보안 관리

논리 파티션에 대해 수행하는 보안 관련 타스크는 논리 파티션이 없는 시스템에 대한 것과 동일합니다. 그러나, 논리 파티션을 작성할 때, 둘 이상의 독립 시스템에 대해 작업합니다. 따라서 논리 파티션이 없는 시스템에서 한 번만 수행하는 대신 각 논리 파티션에 동일한 작업을 수행해야 합니다.

다음은 논리 파티션에 대한 보안을 다룰 때 기억해야 하는 몇 가지 기본 규칙입니다.

- 한 번에 한 논리 파티션씩 시스템에 사용자를 추가합니다. 사용자가 액세스하기 원하는 각 논리 파티션에 사용자를 추가해야 합니다.
- 1차 파티션에서 SST(시스템 서비스 툴) 또는 DST(전용 서비스 툴)에 가는 권한을 가진 사용자 수를 제한하십시오. DST 및 SST에 대한 자세한 내용은 iSeries Information Center의 ″iSeries Navigator, DST 및 SST를 사용하여 논리 파티션 관리″ 주제를 참조하십시오. 서비스 툴 사용자 프로파일을 사용한 파티션 활동에 대한 액세스 제어에 대한 정보는 68 페이지의 『서비스 툴 관리』를 참조하십시오.

  주: iSeries Navigator를 사용하여 LPAR 기능에 액세스하기 전에 서비스 툴 서버(STS)를 초기화해야 합니다. 자세한 정보는 iSeries Information Center --> 보안 --> 서비스 툴을 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.
- 2차 파티션은 다른 논리 파티션의 주 기억장치 및 디스크 장치를 보거나 사용할 수 없습니다.
- 2차 파티션은 자신의 하드웨어 자원만을 볼 수 있습니다.
- 1차 파티션은 DST 및 SST의 시스템 파티션에 대한 작업 화면에서 모든 시스템 하드웨어 자원을 볼 수 있습니다.
- 1차 파티션 오퍼레이팅 시스템은 여전히 그의 자원만을 사용할 수 있는 것으로 봅니다.
- 시스템 제어판이 1차 파티션을 제어합니다. 패널 모드를 보안으로 설정할 때, SST로부터 파티션 상태에 대한 작업 화면에 어떤 조치도 수행할 수 없습니다. 시스템 제어판에서 DST를 강제하려면, 모드를 수동으로 변경해야 합니다.
- 2차 파티션의 작동 모드를 보안으로 설정할 때, 다음 방법으로 파티션 상태에 대한 작업의 사용이 제한됩니다.
  - 파티션 상태를 변경하기 위해 2차 파티션에서 DST만을 사용할 수 있습니다. SST를 사용하여 파티션 상태를 변경할 수 없습니다.
  - 1차 파티션 파티션 상태에 대한 작업 화면에서 DST 또는 SST를 사용하여 2차 파티션에서 DST만을 강제할 수 있습니다.

– 1차 파티션에서 DST만을 사용하여 2차 파티션 모드를 보안에서 다른 값으로 변경할 수 있습니다.

일단 2차 파티션 모드가 더 이상 보안 상태가 아니면, 2차 파티션에서 DST와 SST를 둘다 사용하여 파티션 상태를 변경할 수 있습니다.

iSeries 서버 보안 관련 정보는 보안 참조서 및 iSeries Information Center의 기본 시스템 보안 및 계획 페이지를 참조하십시오.

제 8 장 iSeries Operations Console

Operations Console은 사용자가 PC를 사용하여 iSeries 서버에 액세스하고 제어할 수 있도록 합니다. Operations Console은 iSeries가 콘솔 장치를 사용하지 않고 제공하는 리모트 PC 다이얼 인을 지원하고, 리모트 PC가 해당 콘솔이 되게 합니다. Operations Console을 사용할 때 다음을 주의하십시오.

- Operations Console으로부터 일반적인 콘솔에서 수행할 수 있는 모든 타스크를 수행할 수 있습니다. 예를 들어, *SERVICE 또는 *ALLOBJ 특수 권한이 있는 사용자 프로파일은 Operations Console 세션이 작동 불가능한 경우에도 이 세션에 사인온할 수 있습니다.
- Operations Console은 서비스 툴 사용자 프로파일 및 암호를 사용하여 iSeries 서버에 대한 연결을 작동할 수 있게 합니다. 이것은 서비스 툴 사용자 프로파일 및 암호를 변경하는 것을 특히 중요하게 만듭니다. 해커들은 기본 서비스 툴 사용자 프로파일 사용자 ID와 암호에 친숙한 경향이 있으며 이들을 사용하여 사용자의 iSeries 서버에 리모트 콘솔 세션을 시도할 수 있습니다. 암호에 대한 추가 정보는 22 페이지의 『알려진 암호 변경』 및 27 페이지의 『디폴트 암호 방지』를 참조하십시오.
- 리모트 콘솔을 사용할 때 사용자 정보를 보호하기 위해, Windows 전화 접속 네트워킹의 뒤로 호출 옵션을 사용하십시오.
- 2차 파티션을 설정할 때, 카드 위치에 대해 추가로 고려해야 합니다. 콘솔에 대해 선택한 입/출력 프로세서(IOP)가 LAN 카드도 갖고 있고 LAN 카드가 Operations Console에 사용할 의도가 아닌 경우, 해당 카드가 콘솔이 사용하도록 활성화되고 사용자는 의도한 목적으로 LAN 카드를 사용할 수 없을 것입니다.

V5R1에서, Operations Console은 콘솔 활동이 근거리 통신망(LAN)을 통해 수행될 수 있도록 향상되었습니다. 향상된 인증 및 자료 암호화는 콘솔 프로시듀어에 대한 네트워크 보안을 제공합니다. LAN 연결을 갖는 Operations Console을 사용하려면, 다음 제품을 설치할 것을 강력하게 권장합니다.

- 사용자 iSeries 서버에 Cryptographic Access Provider, 5722-AC2 또는 5722-AC3
- 사용자의 Operations Console PC에 Client Encryption, 5722-CE2 또는 5722-CE3

콘솔 자료가 암호화되기 위해서, iSeries 서버에 Cryptographic Access Provider 제품 중 하나가 설치되고 **또한** PC에 Client Encryption 제품 중 하나가 설치되어야 합니다.

주: 암호 제품이 설치되지 않은 경우, 자료는 암호화되지 않습니다.

아래 표는 사용할 수 있는 제품의 암호화 결과를 요약합니다.

표 13. 암호화 결과

사용자 **iSeries** 서버에 **Cryptographic Access Provider**	사용자의 **Operations Console PC**의 **Client Encryption**	결과 자료 암호화
없음	없음	없음
5722-AC2	5722-CE2	56비트
5722-AC2	5722-CE3	56비트
5722-AC3	5722-CE2	56비트
5722-AC3	5722-CE3	128비트

iSeries Operations Console 설정 및 관리에 대한 추가 정보는 iSeries Information Center를 참조하십시오.

Operations Console 보안 개요

Operations Console 보안은 다음으로 이루어집니다.

- 콘솔 장치 인증
- 사용자 인증
- 자료 프라이버시
- 자료 무결성

직접 연결되는 Operations Console은 해당 지점간 연결로 인해 내재적인 장치 인증, 자료 프라이버시 및 자료 무결성을 갖습니다. 사용자 인증 보안은 콘솔 표시장치에 사인 온해야 합니다.

콘솔 장치 인증

콘솔 장치 인증은 어떤 실제 장치가 콘솔인지를 보장합니다. 직접 연결되는 Operations Console은 쌍축 콘솔과 비슷한 실제 연결을 사용합니다. 직접 연결을 사용하는 Operations Console은 실제 콘솔 장치에 대한 액세스를 제어하기 위한 쌍축 연결과 비슷하게 물리적으로 보안될 수 있습니다.

LAN 연결을 갖는 Operations Console은 장치 및 사용자 인증을 지원하지만 인증서를 사용하지 않는 SSL(보안 소켓층) 버전을 사용합니다. 이 형태의 연결의 경우, 장치 인증은 서비스 툴 장치 프로파일을 기본으로 합니다. 자세한 내용은 77 페이지를 참조하십시오.

사용자 인증

사용자 인증은 콘솔 장치를 사용하고 있는 사용자에 관한 보장을 제공합니다. 사용자 인증과 관련된 모든 문제는 콘솔 유형과 무관하게 동일합니다.

자료 개인보호정책

자료 개인보호정책은 콘솔 자료를 의도된 수신자만이 읽을 수 있는 확신을 제공합니다. 직접 연결성을 갖는 Operations Console은 콘솔 자료를 보호하기 위해 LAN 연결을 위한 쌍축 콘솔 또는 보안 네트워크 연결과 비슷한 물리적 연결을 사용합니다. 직접 연결을 사용하는 Operations Console은 쌍축 연결의 동일한 자료 개인보호정책을 갖습니다. 실제 접속이 안전한 경우, 콘솔 자료는 계속 보호됩니다.

적절한 암호 제품이 설치되는 경우(ACx 및 CEx) LAN 연결을 갖는 Operations Console은 보안 네트워크 연결을 사용합니다. 콘솔 세션은 iSeries 서버 및 Operations Console을 실행하는 PC에 설치된 암호 제품에 따라서 가능한 가장 강력한 암호화를 사용합니다.

주: 암호 제품이 설치되지 않은 경우, 어떤 자료 암호화도 없습니다.

자료 무결성

자료 무결성은 콘솔 자료가 수신자로의 라우트를 변경하지 않았다는 확신을 제공합니다. 직접 연결성을 갖는 Operations Console은 콘솔 자료를 보호하기 위해 LAN 연결을 위한 쌍축 콘솔 또는 보안 네트워크 연결과 비슷한 물리적 연결을 사용합니다. 직접 연결을 사용하는 Operations Console은 쌍축 연결의 동일한 자료 무결성을 갖습니다. 실제 접속이 안전한 경우, 콘솔 자료는 계속 보호됩니다.

적절한 암호 제품이 설치되는 경우(ACx 및 CEx) LAN 연결을 갖는 Operations Console은 보안 네트워크 연결을 사용합니다. 콘솔 세션은 iSeries 서버 및 Operations Console을 실행하는 PC에 설치된 암호 제품에 따라서 가능한 가장 강력한 암호화를 사용합니다.

주: 암호 제품이 설치되지 않은 경우, 어떤 자료 암호화도 없습니다.

LAN 연결을 갖는 Operations Console 사용

주: 모든 Operations Console 장치가 콘솔이 될 수 있지만, LAN 기반 구성만이 서비스 툴 사용자 프로파일을 사용합니다.

iSeries 서버는 디폴트 암호 QCONSOLE을 갖는 디폴트 서비스 툴 장치 프로파일 QCONSOLE과 함께 출하됩니다. LAN 연결을 갖는 Operations Console은 성공적인 각 연결 동안 이 암호를 변경합니다. 자세한 내용은 78 페이지의 『Operations Console 설치 마법사 사용』을 참조하십시오.

iSeries LAN 연결을 갖는 Operations Console에 대한 추가 정보는 Information Center에 있는 LAN 연결을 갖는 Operations Console 구성 주제를 참조하십시오.

LAN 연결을 갖는 Operations Console 보호

LAN 연결을 갖는 Operations Console을 사용할 때, 아래 항목들이 권장됩니다.

- 콘솔 속성을 갖는 다른 서비스 툴 장치 프로파일을 작성하고 프로파일 정보를 안전한 장소에 보관하십시오.
- iSeries 서버에 Cryptographic Access Provider, 5722-AC2 또는 5722-AC3을 설치하고 Operations Console PC에 Client Encryption, 5722-CE2 또는 5722-CE3을 설치하십시오.
- 평범하지 않은 서비스 장치 정보 암호를 선택하십시오.
- 쌍축 콘솔이나 직접 연결을 갖는 Operations Console을 보호하는 것과 같은 방식으로 Operations Console PC를 보호하십시오.

Operations Console 설치 마법사 사용

설치 마법사는 LAN 연결을 갖는 Operations Console을 사용할 때 PC에 필요한 정보를 추가합니다. 설치 마법사는 서비스 툴 장치 프로파일, 서비스 툴 장치 프로파일 암호 및 서비스 툴 장치 프로파일 정보를 보호하기 위한 암호를 묻습니다.

주: 서비스 툴 장치 프로파일 정보 암호는 PC의 서비스 툴 장치 프로파일 정보(서비스 툴 장치 프로파일 및 암호)를 풀고 잠그는데 사용됩니다.

네트워크 연결을 설정할 때, Operations Console 설치 마법사가 암호화된 서비스 툴 장치 프로파일 및 암호에 액세스하기 위해 서비스 장치 정보 암호를 사용자에게 프롬트할 것입니다. 또한 유효한 서비스 툴 사용자 식별 및 암호도 프롬트될 것입니다.

제 9 장 의심이 가는 프로그램 감지

최근에는 컴퓨터 시스템에 신뢰할 수 없는 소스 프로그램 또는 알려지지 않은 기능을 수행하는 프로그램이 있을 가능성이 높아졌습니다. 그 예는 다음과 같습니다.

- 퍼스널 컴퓨터 사용자가 때로 다른 PC 사용자로부터 프로그램을 얻습니다. PC가 iSeries 시스템에 접속된 경우, 해당 프로그램이 iSeries 서버에 영향을 줄 수 있습니다.
- 예를 들면, 네트워크에 연결하는 사용자가 게시판에서 프로그램을 얻을 수도 있습니다.
- 해커의 활동이 더욱 왕성해지고 유명해졌습니다. 해커는 해킹 방법과 그 결과를 출판하기도 합니다. 따라서 정상적으로 법을 준수하던 프로그래머도 모방하려고 할 수 있습니다.

이러한 경향으로 인해 컴퓨터 보안에 있어서 **컴퓨터 바이러스**라는 새로운 문제가 대두되었습니다. 바이러스는 자체의 사본을 포함하도록 다른 프로그램을 변경하는 프로그램입니다. 이때 나머지 프로그램들이 바이러스에 감염되었다고 할 수 있습니다. 또한 바이러스는 시스템 자원을 소모하거나 자료를 파손할 수 있는 다른 조작을 수행할 수 있습니다.

iSeries 서버의 구조는 컴퓨터 바이러스의 감염으로부터 시스템을 보호합니다. 80 페이지의 『컴퓨터 바이러스에 대한 보호』에서 이를 설명합니다. iSeries 서버 보안 관리자는 권한이 없는 기능을 수행하는 프로그램에 더욱 관심을 가져야 합니다. 이 장의 나머지 주제는 나쁜 의도를 가진 사용자가 시스템에 실행할 지도 모르는 해로운 프로그램을 설정하는 방법에 대해 설명하고 있습니다. 이러한 주제는 프로그램이 권한이 없는 기능을 수행하지 않도록 추가 정보를 제공합니다.

보안 추가 정보

오브젝트 권한이 항상 첫 번째 방어선입니다. 오브젝트 보호를 위한 마땅한 계획이 없으면, 시스템은 무방비 상태입니다. 이 정보는 권한을 부여받은 사용자가 오브젝트 권한 체제에서 허점(loop-hole)을 이용하는 방법에 대해 다룹니다.

컴퓨터 바이러스에 대한 보호

바이러스에 감염된 컴퓨터에는 다른 프로그램을 변경할 수 있는 프로그램이 있습니다. iSeries의 오브젝트 기반 구조는 다른 컴퓨터 구조보다 이러한 유형의 바이러스를 생성해서 퍼뜨리는 일이 더욱 어렵습니다. iSeries 서버에서는 특정 명령 및 지침을 사용하여 각 유형의 오브젝트에 대해 작업합니다. 실행가능한 프로그램 오브젝트를 변경하기 위해 파일 지침을 사용할 수는 없습니다(대부분의 바이러스 작성자가 이를 수행합니다). 또한 다른 프로그램 오브젝트를 변경하는 프로그램도 쉽게 작성할 수 없습니다. 이를 수행하려면 상당한 시간과 노력 및 전문 기술이 필요하며, 일반적으로 사용할 수 없는 툴과 문서에 대한 액세스가 필요합니다.

그러나 새로운 iSeries 서버 기능이 열린 시스템 환경에 참여할 수 있게 되면서 iSeries 서버의 일부 오브젝트 기반 보호 기능을 더이상 적용할 수 없게 되었습니다. 예를 들면, 통합 파일 시스템 서버를 사용하여 사용자는 스트림 파일과 같은 디렉토리에 있는 일부 오브젝트를 직접 조작할 수 있습니다.

또한, iSeries 서버 구조로 인해 바이러스가 iSeries 서버프로그램에 퍼지는 것이 어렵기는 하지만, iSeries 서버가 바이러스에 감염되는 것을 막을 수는 없습니다. 파일 서버로서 iSeries 서버는 많은 PC 사용자가 공유하는 프로그램을 저장할 수 있습니다. 이들 프로그램 모두에는 iSeries 서버가 감지하지 못하는 바이러스가 들어 있을 수 있습니다. 이러한 유형의 바이러스가 iSeries 서버에 접속된 PC를 감염시킬 수 없게 하려면, PC 바이러스 스캔 소프트웨어를 사용해야 합니다.

iSeries 서버에는 실행 가능한 오브젝트 프로그램을 변경하는 포인터 기능으로 저급 언어를 사용하지 못하게 하는 몇 가지 기능이 있습니다.

- 시스템이 보안 레벨 40 이상에서 실행하는 경우, 무결성 보호에는 프로그램 오브젝트 변경에 대한 보호가 포함됩니다. 예를 들면, 블록화된(보호된) 기계 명령어가 들어 있는 프로그램을 정상적으로 실행할 수 없습니다.
- 프로그램 유효성 검사값을 사용하여 다른 시스템에서 저장된(잠재적으로 변경되기도 한) 프로그램을 복원할 경우, 사용자를 보호할 수도 있습니다. 제 2 장, *iSeries 보안 참조서*에서는 프로그램 유효성 검사값을 포함하여 보안 레벨 40 이상에 대한 무결성 보호 기능을 설명합니다.

  주: 프로그램 유효성 검사값은 안전하지 않으며, 시스템에 복원된 프로그램 평가시 경계 대체물도 아닙니다.

시스템에 변경된 프로그램이 들어오는 것을 감지하는 데 사용할 수 있는 다음과 같은 몇 가지 툴이 있습니다.

- CHKOBJITG(오브젝트 무결성 검사) 명령을 사용하여 탐색값에 알맞는 오브젝트(실행가능한 오브젝트)를 스캔해서 그러한 오브젝트가 변경되었는지 확인할 수 있습니다. 이는 바이러스 스캔 기능과 유사합니다.

- 보안 감사 기능을 사용하여 변경 또는 복원된 프로그램을 모니터할 수 있습니다. 권한 레벨 시스템 값의 *PGMFAIL, *SAVRST 및 *SECURITY 값은 바이러스 유형의 프로그램을 시스템에 도입하려는 시도를 감지하는 데 도움이 될 수 있는 감사 레코드를 제공합니다. 제 9 장, *iSeries 보안 참조서* 및 부록 F에서 감사값 및 감사 저널 항목에 대한 자세한 내용을 제공합니다.
- CHGPGM(프로그램 변경) 명령의 FRCCRT(강제 작성) 매개변수를 사용하여 시스템에 복원된 모든 프로그램을 재작성할 수 있습니다. 이 시스템은 프로그램 템플리트를 사용하여 이 프로그램을 다시 작성합니다. 프로그램 오브젝트가 컴파일된 후 변경되었으면, 시스템은 변경된 오브젝트를 재작성한 후 이를 대체합니다. 프로그램 템플리트에 블록화된(보호된) 명령어가 있을 경우, 시스템은 프로그램을 정상적으로 재작성하지 못합니다.
- 해당 시스템으로 복원할 때 QFRCCVNRST(복원시 강제 변환) 시스템 값을 사용하여 프로그램을 다시 작성할 수 있습니다. 이 시스템은 프로그램 템플리트를 사용하여 프로그램을 다시 작성합니다. 이 시스템 값은 다시 작성할 프로그램에 대한 여러 선택사항을 제공합니다.
- QVFYOBJRST(복원시 오브젝트 검증) 시스템 값을 사용하여 디지털 서명이 없거나 유효한 디지털 서명을 갖지 않는 프로그램의 복원을 막을 수 있습니다. 디지털 서명이 유효하지 않을 때, 이것은 프로그램이 개발자에 의해 서명된 이후에 변경되었음을 의미합니다. 사용자가 자신의 프로그램, 저장 파일 및 스트림 파일을 서명할 수 있는 API들이 있습니다.

서명 및 서명을 사용하여 공격으로부터 시스템을 보호할 수 있는 방법에 대한 자세한 정보는 94 페이지의 『오브젝트 서명』을 참조하십시오.

허용된 권한의 사용 모니터

iSeries 서버에서 프로그램 소유자의 권한을 허용하는 프로그램을 작성할 수 있습니다. 이것은 프로그램을 실행하는 모든 사용자가 프로그램을 소유하는 사용자 프로파일과 동일한 권한(개인 권한 및 특수 권한)이 있음을 의미합니다.

허용된 권한을 올바르게 사용할 경우에는 귀중한 보안 툴입니다. 예를 들면, 49 페이지의 『오브젝트 보안을 사용하여 메뉴 액세스 제어 향상』에서 메뉴 액세스 제어 이상으로 확장하도록 허용된 권한과 메뉴를 결합하는 방법에 대해 설명합니다. 허용된 권한을 사용하면 사용자가 여전히 파일에 대한 조회를 허용하는 반면, 중요한 파일이 승인된 어플리케이션 프로그램 외부에서 변경되지 않도록 보호할 수 있습니다.

보안 관리자로서 허용된 권한이 올바르게 사용되도록 확인해야 합니다.

- 프로그램은 권한을 과소하게 주지 않고 필요한 기능 수행에 충분한 권한만 갖도록 사용자 프로파일의 권한을 허용해야 합니다. *ALLOBJ 특수 권한이 있거나 중요한 오브젝트를 소유하는 사용자 프로파일의 권한을 허용하는 프로그램을 특히 주의해야 합니다.
- 권한을 허용하는 프로그램에는 특정의 제한된 기능이 있어야 하고 명령 입력 기능을 제공할 수 없습니다.
- 권한을 허용하는 프로그램은 적절하게 보안되어야 합니다.
- 허용된 권한을 지나치게 사용하면 시스템 성능에 부정적인 영향을 줄 수 있습니다. 성능상의 문제점을 방지하려면 제 5 장, *iSeries 보안 참조서*에 있는 허용된 권한 사용에 대한 권한 검사 흐름도 및 제안사항을 검토하십시오.

SECBATCH 메뉴 옵션

1 *즉시 제출* **40 작업 스케줄러 사용**

PRTADPOBJ(허용 오브젝트 인쇄) 명령(SECTOOLS 메뉴의 옵션 21)을 사용하여 시스템에서 허용된 권한 사용을 모니터할 수 있습니다.

해당 보고서는 지정된 사용자 프로파일의 특수 권한, 사용자 프로파일의 권한을 허용하는 프로그램 및 프로파일의 권한을 사용하는 ASP 장치를 표시합니다. 정보의 기준을 설정한 후 허용한 오브젝트의 변경된 버전 보고서를 정기적으로 인쇄할 수 있습니다. 이 보고서는 보고서를 마지막으로 실행한 이후 권한을 허용하도록 변경된 프로그램 및 권한을 허용하는 새 프로그램을 나열합니다.

허용된 권한이 시스템에서 오용된다고 의심될 경우, *PGMADP를 포함하도록 QAUDLVL 시스템 값을 설정할 수 있습니다. 이 값이 활동중일 경우, 시스템은 권한을 허용하는 프로그램을 시작 또는 종료할 때마다 감사 저널 항목을 작성합니다. 이 항목에는 프로그램을 시작한 사용자명과 프로그램명이 포함됩니다.

허용된 권한의 사용 한계

iSeries 프로그램이 실행할 때 프로그램은 허용된 권한을 사용하여 다음 두 가지 방법으로 오브젝트에 액세스할 수 있습니다.

- 프로그램 자체에서 소유자의 권한을 허용할 수 있습니다. 이것은 프로그램 또는 서비스 프로그램의 USRPRF(사용자 프로파일) 매개변수에 지정됩니다.
- 프로그램은 아직 작업의 호출 스택에 있는 이전 프로그램에서 허용한 권한을 사용(상속)할 수 있습니다. 프로그램은 프로그램 자체에서 권한을 허용하지 않을 때에도 이전 프로그램에서 허용한 권한을 상속할 수 있습니다. 프로그램 또는 서비스 프로

그램의 USEADPAUT(허용된 권한 사용) 매개변수는 프로그램이 프로그램 스택에 있는 이전 프로그램에서 허용된 권한을 상속하는지 여부를 제어합니다.

다음은 이전 프로그램에서 허용된 권한 사용법의 한 예입니다.

ICOWNER 사용자 프로파일이 ITEM 파일에 대해 *CHANGE 권한이 있으며, ITEM 파일에 대한 공용 권한은 *USE라고 가정하십시오. 다른 사용자 프로파일은 ITEM 파일에 대해 명시적으로 정의된 권한을 갖지 않습니다. 표 14에서는 ITEM 파일을 사용하는 세 가지 프로그램의 속성을 보여줍니다.

표 14. 허용된 권한 사용(USEADPAUT) 예

프로그램명	프로그램 소유자	USRPRF 값	USEADPAUT 값
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

예 1-권한 허용:

1. USERA는 PGMA 프로그램을 실행합니다.
2. PGMA 프로그램이 갱신 가능으로 ITEM 파일을 열려고 합니다.

결과: 시도가 성공했습니다. PGMA가 ICOWNER의 권한을 허용하기 때문에 USERA가 ITEM 파일에 대한 *CHANGE 액세스를 갖습니다.

예 2-허용된 권한 사용:

1. USERA는 PGMA 프로그램을 실행합니다.
2. PGMA 프로그램은 PGMB 프로그램을 호출합니다.
3. PGMB 프로그램이 갱신 가능으로 ITEM 파일을 열려고 합니다.

결과: 시도가 성공했습니다. PGMB 프로그램이 권한(*USRPRF가 *USER임)을 허용하지 않더라도, 이 프로그램은 이전에 허용한 권한(*USEADPAUT가 *YES임) 사용을 허용합니다. PGMA 프로그램은 계속 프로그램 스택에 있습니다. 따라서, PGMA가 ICOWNER의 권한을 허용하므로 USERA는 ITEM 파일에 대한 *CHANGE 액세스를 갖습니다.

예 3-허용된 권한을 사용하지 않음:

1. USERA는 PGMA 프로그램을 실행합니다.
2. PGMA 프로그램은 PGMC 프로그램을 호출합니다.
3. PGMC 프로그램이 갱신 가능으로 ITEM 파일을 열려고 합니다.

결과: 권한 실패. PGMC 프로그램이 권한을 허용하지 않습니다. PGMC 프로그램은 또한 이전 프로그램에서 허용한 권한 사용도 허용하지 않습니다. PGMA가 아직 호출 스택에 있지만 허용된 권한은 사용되지 않습니다.

새 프로그램이 허용된 권한을 사용하지 못하게 함

채택된 권한을 스택에 있는 이후의 프로그램에 전달하면, 시스템을 잘 아는 프로그래머가 트로이의 목마 프로그램을 작성할 수 있는 기회를 제공합니다. 트로이의 목마 프로그램은 스택에 있는 이전 프로그램에 근거하여 손해를 입힌 정도의 권한을 얻을 수 있습니다. 이를 방지하기 위해 이전 프로그램의 허용된 권한을 사용하는 프로그램을 작성할 수 있는 사용자를 제한할 수 있습니다.

새로운 프로그램을 작성하면 시스템은 자동으로 USEADPAUT 매개변수를 *YES로 설정합니다. 프로그램이 허용한 권한을 상속하지 않도록 하려면, CHGPGM(프로그램 변경) 명령 또는 CHGSRVPGM(서비스 프로그램 변경) 명령을 사용하여 USEADPAUT 매개변수를 *NO로 설정해야 합니다.

권한 부여 리스트 및 QUSEADPAUT(허용된 권한 사용) 시스템 값을 사용하여 허용 권한을 상속하는 프로그램 작성자를 제어할 수 있습니다. QUSEADPAUT 시스템 값에 권한 부여 리스트명을 지정하면, 시스템은 이 권한 부여 리스트를 사용하여 새 프로그램 작성 방법을 판별합니다.

사용자가 프로그램 또는 서비스 프로그램을 작성하면, 시스템은 권한 부여 리스트에 대한 사용자의 권한을 검사합니다. 사용자에게 *USE 권한이 있으면, 새 프로그램의 USEADPAUT 매개변수가 *YES로 설정됩니다. 사용자에게 *USE 권한이 없으면, USEADPAUT 매개변수는 *NO로 설정됩니다. 권한 부여 리스트에 대한 사용자의 권한은 허용된 권한에서 올 수 없습니다.

QUSEADPAUT 시스템 값에 지정하는 권한 부여 리스트는 또한 사용자가 CHGxxx 명령을 사용하여 프로그램 또는 서비스 프로그램에 대한 USEADPAUT 값을 설정할 수 있는지를 제어합니다.

주:

1. 권한 부여 리스트 QUESADPAUT를 호출할 필요는 없습니다. 다른 이름을 갖는 권한 리스트를 작성할 수 있습니다. 그런 다음, QUSEADPAUT 시스템 값에 그 권한 부여 리스트를 지정하십시오. 이 예의 명령에서 권한 부여 리스트명을 대체하십시오.
2. QUSEADPAUT 시스템 값은 시스템에 있는 기존 프로그램에 영향을 주지 않습니다. CGHPGM 명령 또는 CHGSRVPGM 명령을 사용하여 기존 프로그램에 대한 USEADPAUT 매개변수를 설정하십시오.

강화된 제한적인 환경: 대부분의 사용자가 USEADPAUT 매개변수가 *NO로 설정된 새로운 프로그램을 작성하도록 하려면 다음을 수행하십시오.

1. 권한 부여 리스트의 공용 권한을 *EXCLUDE로 설정하려면 다음과 같이 입력하십시오.

```
CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

2. 이전 프로그램의 허용 권한을 사용하는 프로그램을 작성할 수 있도록 특정 사용자를 설정하려면, 다음과 같이 입력하십시오.

```
ADDAUTLE AUTL(QUSEADPAUT) USER(user-name)
   AUT(*USE)
```

완화된 제한적인 환경: 대부분의 사용자가 USEADPAUT 매개변수를 *YES로 설정하여 새 프로그램을 작성할 수 있도록 하려면, 다음을 수행하십시오.

1. *USE로 설정된 권한 부여 리스트의 공용 권한을 그대로 두십시오.
2. 특정 사용자가 이전 프로그램의 허용 권한을 사용하는 프로그램을 작성하지 못하게 하려면, 다음과 같이 입력하십시오.

```
ADDAUTLE AUTL(QUSEADPAUT)
   USER(user-name) AUT(*EXCLUDE)
```

트리거 프로그램의 사용 모니터

DB2® UDB는 트리거 프로그램을 데이터베이스 파일과 연관시키는 기능을 제공합니다. 트리거 프로그램 기능은 고기능 데이터베이스 관리자용 산업에서 일반적입니다.

트리거 프로그램을 데이터베이스 파일과 연관시킬 때 트리거 프로그램을 실행할 시기를 지정합니다. 예를 들면, 새 레코드가 파일에 추가될 때마다 트리거 프로그램은 실행하도록 고객 주문 파일을 설정할 수 있습니다. 고객의 미결재 잔액이 신용한도를 초과하면, 트리거 프로그램이 고객에게 경고문을 인쇄하고 신용 관리자에게 메세지를 송신할 수 있습니다.

트리거 프로그램은 어플리케이션 기능을 제공하고 정보를 관리하는 생산적인 방법입니다. 트리거 프로그램은 또한 나쁜 의도를 가진 사용자가 시스템에 『트로이의 목마』를 작성할 수 있는 기능도 제공합니다. 시스템의 데이터베이스 파일에 어떤 이벤트가 발생하면 실행하기 위해 파괴적인 프로그램이 안착하여 대기하고 있을 수 있습니다.

주: 트로이의 목마는 역사적으로 그리스 병사들이 숨어 있던 커다란 목마입니다. 이 목마를 트로이의 성벽 안으로 들여온 후 병사들이 목마에서 나와 트로이를 물리쳤습니다. 컴퓨터 세계에서는 파괴적인 기능을 숨기고 있는 프로그램을 트로이의 목마라고 합니다.

SECBATCH 메뉴 옵션

27 *즉시 제출* **66** *작업 스케줄러 사용*

시스템에 제공될 때 트리거 프로그램을 데이터베이스 파일에 추가하는 기능이 제한됩니다. 오브젝트 권한을 주의깊게 관리할 경우, 일반 사용자에게는 트리거 프로그램을 데이터베이스 파일에 추가할 수 있는 충분한 권한이 없습니다(*iSeries 보안 참조서* 부록 D는 ADDPFTRG(실제 파일 트리거 추가) 명령을 포함하여 필요한 명령 또는 모든 명령을 알려줍니다).

PRTTRGPGM(트리거 프로그램 인쇄) 명령을 사용하여 특정 라이브러리 또는 모든 라이브러리에 있는 모든 트리거 프로그램 리스트를 인쇄할 수 있습니다.

초기 보고서를 바탕으로 이미 시스템에 있는 트리거 프로그램을 평가할 수 있습니다. 그런 다음, 변경된 보고서를 정기적으로 인쇄하여 새 트리거 프로그램이 시스템에 추가되었는지 여부를 알아볼 수 있습니다.

트리거 프로그램을 평가할 경우, 다음 사항을 고려하십시오.

- 누가 트리거 프로그램을 작성했습니까? DSPOBJD(오브젝트 설명 표시) 명령을 사용하여 이를 판별할 수 있습니다.
- 프로그램이 무엇을 수행합니까? 소스 프로그램을 참조하거나 프로그램 작성자에게 이를 판별하도록 요청해야 합니다. 예를 들면, 트리거 프로그램이 사용자가 누구인지를 알아보기 위해 검사합니까? 트리거 프로그램은 시스템 자원에 액세스하기 위해 특정 사용자(QSECOFR)를 기다리고 있습니다.

정보의 기준을 설정한 후 변경된 보고서를 정기적으로 인쇄하여 시스템에 추가된 새 트리거 프로그램을 모니터할 수 있습니다.

숨겨진 프로그램 검사

트리거 프로그램이 트로이의 목마를 시스템에 도입할 수 있는 유일한 방법은 아닙니다. 트리거 프로그램은 **나감 프로그램**의 한 예입니다. 트리거 프로그램의 경우, 파일 갱신과 같은 특정 이벤트가 발생하면 시스템은 해당 이벤트와 연관된 나감 프로그램을 실행합니다.

87 페이지의 표 15는 시스템에 있는 나감 프로그램의 다른 예를 설명합니다. 트리거 프로그램에 사용하는 이러한 나감 프로그램의 사용 및 내용을 평가하는 데에 동일한 방법을 사용해야 합니다.

주: 87 페이지의 표 15는 사용가능한 나감 프로그램의 전체 리스트가 아닙니다.

.

표 15. 시스템 제공 나감 프로그램

프로그램명	프로그램이 실행할 때
DDMACC 네트워크 속성의 사용자 지정명	사용자가 시스템에서 DDM 파일을 열려고 하거나 DRDA 연결을 만들 때
PCSACC 네트워크 속성의 사용자 지정명	사용자가 시스템의 오브젝트에 액세스하기 위해 원래 클라이언트를 사용하여 Client Access™ 기능을 사용하려고 할 때.
QPWDVLDPGM 시스템 값의 사용자 지정명	사용자가 암호 변경 기능을 실행할 때
QRMTSIGN 시스템 값의 사용자 지정명	사용자가 리모트 시스템에서 대화식으로 사인 온할 때
QSYS/QEZUSRCLNP	자동 클린업 기능을 실행할 때
CHGBCKUP 명령의 EXITPGM 매개변수의 사용자 지정명	Operation Assistant 백업 기능을 사용할 때
CRTPRDLOD 명령의 사용자 지정명	명령으로 작성한 제품을 저장, 복원 또는 삭제하기 전후
CHGMSGD 명령의 DFTPGM 매개변수의 사용자 지정명	메세지에 디폴트 프로그램이 지정되면, 시스템은 메세지가 발행될 때 프로그램을 실행합니다. 일반 시스템에는 메세지 설명이 많이 있으므로 디폴트 프로그램을 사용하면 모니터가 어렵습니다. 공용 사용자가 메세지에 대한 디폴트 프로그램을 추가하지 못하게 하려면, 메제지 파일(*MSGF 오브젝트)에 대한 공용 권한을 *USE로 설정하십시오.
STREML3270 명령의 FKEYPGM 매개변수의 사용자 지정명	사용자가 3270 장치 에뮬레이션 세션중에 기능 키를 누를 때. 시스템은 나감 프로그램이 종료할 때 3270 장치 에뮬레이션 세션에 대한 제어를 리턴합니다.
성능 모니터 명령의 EXITPGM 매개변수의 사용자 지정명	STRPFRMON, ENDPFRMON, ADDPFRCOL 및 CHGPFRCOL 명령으로 수집한 자료 처리. 프로그램은 자료 콜렉션이 종료할 때 실행됩니다.
RCVJRNE 명령의 EXITPGM 매개변수의 사용자 지정명	지정된 저널 및 저널 리시버로부터 읽는 각 저널 항목 또는 저널 항목 그룹에 대해.
QTNADDCR API의 사용자 지정명	COMMIT 또는 ROLLBACK 조작 동안에
QHFRGFS API의 사용자 지정명	파일 시스템 기능 수행
인쇄 장치 설명의 SEPPGM 매개변수의 사용자 지정명	스풀 파일 또는 인쇄 작업 전후에 분리 페이지에서 인쇄할 사항 판별
QGPL/QUSCLSXT	파일 사용 정보 캡처를 허용하기 위해 데이터베이스 파일을 닫을 때
논리 파일의 FMTSLR 매개변수의 사용자 지정명	레코드가 데이터베이스 파일에 기록되고 레코드 형식명이 고급 언어 프로그램에 포함되지 않을 때. 선택기 프로그램은 레코드를 입력으로 수신하며, 사용된 레코드 형식을 판별하고 이를 데이터베이스에 리턴합니다.
QATNPGM 시스템 값, 사용자 프로파일의 ATNPGM 매개변수 또는 SETATNPGM 명령의 PGM 매개변수에 지정된 사용자 지정명	사용자가 주의 키를 누를 때
TRCJOB 명령의 EXITPGM 매개변수의 사용자 지정명	작업 추적 프로시듀어를 시작하기 전

나감 프로그램을 지정할 수 있는 명령에 대해 나감 프로그램 지정을 위한 명령 디폴트가 변경되었는지 확인해야 합니다. 또한, 이러한 명령의 공용 권한이 명령 디폴트 변경에 충분한지도 확인해야 합니다. CHGCMDDFT 명령에는 명령에 대한 *OBJMGT 권한이 필요합니다. 명령 실행에 *OBJMGT 권한은 필요하지 않습니다.

등록된 나감 프로그램 평가

시스템 등록 기능을 사용하여 특정 이벤트가 발생할 때 실행해야 할 나감 프로그램을 등록할 수 있습니다. 시스템의 등록 정보를 나열하려면 WRKREGINF OUTPUT(*PRINT)를 입력하십시오. 그림 8은 이러한 보고서의 예를 보여줍니다.

```
                          등록 정보에 대한 작업
종료점 . . . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
종료점 형식  . . . . . . . . . . . . . . :   NJE00100
종료점 등록  . . . . . . . . . . . . . . :   *YES
등록 취소 허용 . . . . . . . . . . . . . :   *YES
최대 나감 프로그램 수  . . . . . . . . . :   *NOMAX
현재 나감 프로그램 수  . . . . . . . . . :   0
추가 사전처리  . . . . . . . . . . . . . :   *NONE
  라이브러리 . . . . . . . . . . . . . . :
  형식 . . . . . . . . . . . . . . . . . :
제거 사전처리  . . . . . . . . . . . . . :   *NONE
  라이브러리 . . . . . . . . . . . . . . :
  형식 . . . . . . . . . . . . . . . . . :
검색 사전 처리 . . . . . . . . . . . . . :   *NONE
  라이브러리 . . . . . . . . . . . . . . :
```

그림 8. 등록 정보에 대한 작업 - 예

시스템의 각 종료점에 대한 보고서는 현재 등록된 나감 프로그램이 있는지를 보여줍니다. 종료점에 현재 등록된 프로그램이 있으면 WRKREGINF 버전 표시에서 옵션 8(프로그램 표시)을 선택하여 프로그램에 관한 정보를 표시할 수 있습니다.

```
                          등록 정보에 대한 작업

옵션을 입력한 후 Enter 키를 누르십시오.
5=종료점 표시   8=나감 프로그램에 대한 작업


                          종료점
Opt  종료점                형식          등록     텍스트
     QIBM_QGW_NJEOUTBOUND  NJE00100     *YES     네트워크 작업 항목 아웃바운드 예
8    QIBM_QHQ_DTAQ         DTAQ0100     *YES     원래의 자료 대기행렬 서버
     QIBM_QLZP_LICENSE     LICM0100     *YES     원래의 사용권 관리 서버
     QIBM_QMF_MESSAGE      MESS0100     *YES     원래의 메세지 서버
     QIBM_QNPS_ENTRY       ENTR0100     *YES     네트워크 인쇄 서버 - 항목
     QIBM_QNPS_SPLF        SPLF0100     *YES     네트워크 인쇄 서버 - 스풀
     QIBM_QNS_CRADDACT     ADDA0100     *YES     CRQ 설명 활동 추가
     QIBM_QNS_CRCHGACT     CHGA0100     *YES     CRQ 설명 활동 변경
```

다른 나감 프로그램과 트리거 프로그램에서 사용하는 것과 동일한 방법을 이러한 나감 프로그램 평가에 사용하십시오.

스케줄된 프로그램 검사

iSeries는 작업 스케줄러를 포함하여 나중에 실행하도록 작업을 스케줄하는 여러 가지 방법을 제공합니다. 일반적으로 이러한 방법은 작업을 스케줄하는 사용자가 작업을 일괄처리로 제출하는 데 필요한 것과 동일한 권한을 가져야 하기 때문에 보안 노출을 나타내지는 않습니다.

그러나 나중에 스케줄된 작업을 정기적으로 검사해야 합니다. 조직에서 더 이상 근무하지 않는 불만을 가진 사용자가 이 방법을 사용하여 불행한 사태를 스케줄할 수도 있습니다.

저장 및 복원 기능 제한

대부분의 사용자는 시스템에서 오브젝트를 저장 및 복원하지 않아도 됩니다. 저장 명령이 조직의 중요한 자산을 매체 또는 다른 시스템에 복사할 수 있는 가능성을 제공합니다. 대부분의 저장 명령은 매체 또는 저장/복원 장치에 대한 액세스 없이 다른 시스템(SNDNETF 파일 명령 사용)에 송신할 수 있는 저장 파일을 지원합니다.

복원 명령은 프로그램, 명령 및 파일과 같은 권한이 없는 오브젝트를 시스템에 복원할 수 있는 기회를 제공합니다. 또한, 저장 파일을 사용해서 매체 또는 저장/복원 장치에 대한 액세스 없이 정보를 복원할 수 있습니다. 저장 파일은 SNDNETF 명령을 사용하거나 FTP 기능을 사용하여 다른 시스템으로부터 송신할 수 있습니다.

다음은 시스템에서 저장 및 복원 조작을 제한하기 위한 제안사항입니다.

- *SAVSYS 특수 권한을 갖는 사용자를 제어하십시오. *SAVSYS 특수 권한을 사용하면 사용자가 오브젝트에 대한 필수 권한이 없을 경우에도 오브젝트를 저장하고 복원할 수 있습니다.
- 장치를 저장 및 복원하기 위한 실제 액세스를 제어하십시오.
- 저장 및 복원 명령에 대한 액세스를 제한하십시오. OS/400 사용권 프로그램을 설치할 때, RSTxxx 명령에 대한 공용 권한은 *EXCLUDE입니다. SAVxxx 명령의 공용 권한은 *USE입니다. SAVxxx 명령의 공용 권한을 *EXCLUDE로 변경하십시오. RSTxxx 명령에 대한 권한을 부여받을 사용자를 주의해서 제한하십시오.
- QALWOBJRST 시스템 값을 사용하여 시스템 상태 프로그램, 권한을 채택하는 프로그램 및 유효성 오류가 있는 오브젝트의 복원을 제한하십시오.
- 사용자 시스템에 부호화된 오브젝트 복원을 제어하려면 QVFYOBJRST 시스템 값을 사용하십시오.
- QFRCCVNRST 시스템 값을 사용하여 해당 시스템에서 복원 중인 특정 오브젝트의 다시 작성을 제어하십시오.

- 보안 감사를 사용하여 복원 조작을 모니터하십시오. QAUDLVL 시스템 값에 *SAVRST를 포함시키고 복원 조작으로 작성된 감사 레코드를 정기적으로 인쇄하십시오(제 9 장, *iSeries 보안 참조서* 및 부록 F에서는 항목 감사 작업에 대한 자세한 내용을 제공합니다).

보호된 라이브러리에서 사용자의 오브젝트 검사

모든 iSeries 서버 작업에는 라이브러리 리스트가 있습니다. 오브젝트명과 함께 라이브러리명이 지정되지 않으면, 라이브러리 리스트에서 시스템이 오브젝트를 탐색하는 순서를 판별합니다. 예를 들어, 프로그램의 위치를 지정하지 않고 프로그램을 호출하면, 시스템이 라이브러리 리스트를 순서대로 탐색하여 찾은 첫 번째 프로그램 사본을 실행합니다.

*iSeries 보안 참조서*는 라이브러리 리스트의 보안 노출 및 라이브러리명 없이 프로그램 호출하기(**비규정화 호출**이라고 함)에 대한 자세한 내용을 제공합니다. 또한, 라이브러리 리스트의 내용 및 시스템 라이브러리 리스트 변경 기능 제어에 대한 제안사항도 제공합니다.

시스템이 제대로 실행되려면 QSYS 및 QGPL과 같은 일부 시스템 라이브러리가 모든 작업의 라이브러리 리스트에 있어야 합니다. 이러한 라이브러리에 프로그램을 추가할 수 있는 사용자를 제어하려면 오브젝트 권한을 사용해야 합니다. 그러면 나중에 라이브러리 리스트에 있는 라이브러리에 나타나는 프로그램과 같은 이름을 가진 이러한 라이브러리 중 하나에 사칭 프로그램을 배치할 수 없습니다.

또한, CHGSYSLIBL 명령에 대해 권한을 가진 사용자를 평가하고 보안 감사 저널에서 SV 레코드를 모니터해야 합니다. 나쁜 의도를 가진 사용자가 라이브러리를 라이브러리 리스트에서 QSYS 앞에 배치하여 다른 사용자가 IBM 제공 명령과 동일한 이름으로 권한이 없는 명령을 실행할 수 있습니다.

SECBATCH 메뉴 옵션

28 *즉시 제출* **67** *작업 스케줄러 사용*

PRTUSROBJ(사용자 오브젝트 인쇄) 명령을 사용하여 지정된 라이브러리에 있는 사용자 오브젝트(IBM에서 작성하지 않은 오브젝트) 리스트를 인쇄할 수 있습니다. 그런 다음, 리스트의 프로그램을 평가하여 프로그램 작성자 및 프로그램이 수행하는 기능을 판별할 수 있습니다.

프로그램 이외의 사용자 오브젝트도 시스템 라이브러리에 있을 때 보안 노출을 나타낼 수 있습니다. 예를 들면, 프로그램이 이름이 규정되지 않은 파일에 기밀 자료를 기록할 경우, 해당 프로그램은 시스템 라이브러리에서 해당 파일의 가짜 버전을 열게 될 수도 있습니다.

제 10 장 도용 시도 방지 및 감지

이 정보에는 잠재적인 보안 노출 및 도용자를 감시하는 데 도움이 되는 기타 추가 정보가 나옵니다.

실제 보안

시스템 장치는 중요한 업무 자산 및 시스템으로 들어가는 잠재적인 문을 나타냅니다. 시스템 내부의 일부 시스템 구성요소는 작지만 귀중한 것입니다. 시스템 장치를 제어된 위치에 두어 귀중한 시스템 구성요소를 제거할 수 없게 해야 합니다.

시스템 장치에는 워크스테이션 없이 기본 기능을 수행할 수 있는 능력을 제공하는 제어판이 있습니다. 예를 들면, 제어판을 사용하여 다음을 수행할 수 있습니다.

- 시스템 중단
- 시스템 시작
- 오퍼레이팅 시스템 로드
- 서비스 기능 시작

이러한 모든 활동이 시스템 사용자를 방해할 수 있습니다. 또한, 이러한 활동은 시스템에 대한 잠재적 보안 노출을 나타냅니다. 시스템에 제공되는 키잠금을 사용하여 이러한 활동의 허용 시기를 제어할 수 있습니다. 제어판 사용을 방지하려면, 키잠금을 보안 위치에 놓고 키를 제거한 후 안전한 장소에 저장하십시오.

주:

1. 시스템에서 리모트 IPL을 수행하거나 리모트 진단을 수행해야 하는 경우, 키잠금에 다른 설정을 선택해야 할 수도 있습니다. iSeries Information Center에 있는 시작하기 주제에 키잠금 설정에 대한 자세한 정보가 제공됩니다(세부사항은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오).
2. 모든 시스템 모델에 표준 피처로서 키잠금이 제공되지는 않습니다.

사용자 프로파일 활동 모니터

사용자 프로파일에는 시스템에 대한 항목이 있습니다. 사용자 프로파일의 매개변수가 사용자 환경 및 사용자 보안 특성을 판별합니다. 보안 관리자는 시스템의 사용자 프로파일에 발생하는 변경사항을 제어하고 감시해야 합니다.

사용자 프로파일에 변경 레코드를 기록할 수 있도록 보안 감사를 설정할 수 있습니다. DSPAUDJRNE 명령을 사용하여 해당 변경에 대한 보고서를 인쇄할 수 있습니다.

나감 프로그램을 작성하여 사용자 프로파일에 대해 요구한 조치를 평가할 수 있습니다. 표 16은 사용자 프로파일 명령에서 사용할 수 있는 종료점을 표시합니다.

표 16. 사용자 프로파일 활동에 대한 종료점

사용자 프로파일 명령	종료점 이름
CRTUSRPRF(사용자 프로파일 작성)	QIBM_QSY_CRT_PROFILE
CHGUSRPRF(사용자 프로파일 변경)	QIBM_QSY_CHG_PROFILE
DLTUSRPRF(사용자 프로파일 삭제)	QIBM_QSY_DLT_PROFILE
RSTUSRPRF(사용자 프로파일 복원)	QIBM_QSY_RST_PROFILE

예를 들어, 나감 프로그램에서 사용자가 권한이 없는 프로그램의 버전을 실행할 수 있는 변경사항을 찾을 수 있습니다. 이러한 변경사항은 다른 작업 설명 또는 새로운 현재 라이브러리를 할당하고 있을 수 있습니다. 나감 프로그램은 나감 프로그램이 수신한 정보에 따라 메세지 대기행렬에 통지하거나 조치(사용자 프로파일의 변경 또는 사용불가)를 취합니다.

*iSeries 보안 참조서*에서는 사용자 프로파일 활동에 나감 프로그램의 자세한 내용을 제공합니다.

오브젝트 서명

누군가가 사용자 시스템에 조작된 자료를 도입하여 사용자가 취하는 모든 보안 주의사항을 바이패스하는 경우 보안은 의미가 없습니다. iSeries 서버에는 조작된 소프트웨어가 시스템에 로드되는 것을 막고 이미 존재하는 그런 소프트웨어를 감지하는 데 사용할 수 있는 많은 내장 피처가 있습니다. V5R1에 추가된 기술 중 하나가 오브젝트 서명입니다.

오브젝트 서명은 ″디지털 서명″으로 알려진 암호 개념의 iSeries 서버 구현입니다. 아이디어는 상대적으로 단순합니다. 즉, 소프트웨어 작성자가 소프트웨어를 고객에게 제공할 준비가 되면, 작성자는 소프트웨어에 ″서명″합니다. 이 서명은 소프트웨어가 특정 기능을 수행할 것을 보증하지 않습니다. 그러나, 소프트웨어가 서명한 작성자로부터 유래한 것이며 소프트웨어가 생산되어 서명된 이후 변경되지 않았음을 증명하는 하나의 방법을 제공합니다. 이것은 특히 소프트웨어가 인터넷을 통해 전송되거나 사용자가 수정되었다고 느낄 수 있는 매체에 저장된 경우에 중요합니다.

디지털 서명 사용은 사용자 시스템에 로드될 수 있는 소프트웨어에 대한 더 큰 제어를 제공하고 사용자에게 소프트웨어가 로드된 후의 변경을 감지하는 더 많은 능력을 제공합니다. 새로운 시스템 값인 QVFYOBJRST(오브젝트 복원 검증)가 시스템에 로드되는 모든 소프트웨어가 알려진 소프트웨어 소스에 의해 서명되도록 하는 제한적 정책을 설정하는 메카니즘을 제공합니다. 또한 보다 개방적인 정책을 선택하고 단순히 서명(있는 경우)을 검증할 수도 있습니다.

옵션 소프트웨어와 iSeries 서버 사용권 프로그램뿐 아니라 모든 OS/400 소프트웨어가 시스템을 신뢰할 수 있는 소스에 의해 서명되었습니다. 이 서명은 시스템의 무결성을 보호하는 데 도움이 되며, 수정 프로그램이 시스템을 신뢰할 수 있는 소스로부터 나온 것이고 전송 중에 변경되지 않았음을 확인하기 위해 수정 프로그램을 시스템에 적용할 때 서명이 검사됩니다. 이들 서명은 또한 일단 소프트웨어가 시스템에 있으면 검사할 수 있습니다. CHKOBJITG(오브젝트 무결성 검사) 명령이 시스템에 있는 오브젝트의 다른 무결성 피처에 추가하여 서명을 검사하도록 확장되었습니다. 또한, 디지털 인증 관리자에 오퍼레이팅 시스템에 있는 오브젝트를 포함하여 오브젝트의 서명을 검사하는 데 사용할 수 있는 패널이 있습니다.

오퍼레이팅 시스템이 서명된 것처럼, 디지털 서명을 사용하여 비지니스에 중요한 소프트웨어의 무결성을 보호할 수 있습니다. 소프트웨어 제공자가 서명한 소프트웨어를 구매하거나 사용자가 구매하거나 작성한 소프트웨어를 서명할 수 있습니다. 그런 다음 보안 정책의 일부가 주기적으로 CHKOBJITG 또는 디지털 인증 관리자를 사용하여 해당 소프트웨어의 서명이 여전히 유효한지, 즉 오브젝트가 서명된 이후 변경되지 않았는지를 검증할 수 있습니다. 시스템에 복원되는 모든 소프트웨어가 사용자 또는 알려진 소스에 의해 서명되도록 추가로 요구할 수 있습니다. 그러나, IBM이 생산하지 않는 대부분의 iSeries 서버 소프트웨어가 현재 서명되지 않으므로 이것은 시스템에 대한 제한일 수도 있습니다. 새로운 디지털 서명 지원은 소프트웨어 무결성을 얼마나 보호할 것인지를 결정하는 유연성을 제공합니다.

소프트웨어를 보호하는 디지털 서명은 단지 디지털 인증의 한 가지 사용법입니다. 디지털 인증 관리에 대한 추가 정보를 Information Center에 있는 디지털 인증 관리 주제에서 찾을 수 있습니다(세부사항은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오).

서브시스템 설명 모니터

iSeries 서버에서 서브시스템을 시작하면 시스템은 작업이 시스템에 들어가서 실행할 수 있는 환경을 작성합니다. 서브시스템 설명은 그 환경이 어떤 것인지를 정의합니다. 따라서, 서브시스템은 그릇된 사용자에게 기회를 제공합니다. 나쁜 의도를 가진 사용자가 서브시스템 설명을 사용하여 프로그램을 자동으로 시작하거나 사용자 프로파일 없이 사인 온할 수 있습니다.

RVKPUBAUT(공용 권한 취소) 명령을 실행할 때, 시스템에서는 서브시스템 설명 명령에 대한 공용 권한을 *EXCLUDE로 설정합니다. 이로써 구체적으로 권한을 부여받지 않은 사용자(및 *ALLOBJ 특수 권한이 없는 사용자)가 서브시스템 설명을 변경 또는 작성할 수 없습니다.

다음 주제는 현재 시스템에 있는 서브시스템 설명을 검토하기 위한 제안사항을 제공합니다. WRKSBSD(서브시스템 설명에 대한 작업) 명령을 사용하여 모든 서브시스템 설

명 리스트를 작성할 수 있습니다. 리스트에서 5(표시)를 선택하면, 선택한 시스템 설명에 대한 메뉴가 표시됩니다. 이 메뉴는 서브시스템 환경의 부분 리스트에서 보여줍니다.

옵션을 선택하여 부분에 대한 세부사항을 참조하십시오. 메뉴의 처음 두 항목을 변경하려면 CHGSBSD(서브시스템 설명 변경) 명령을 사용하십시오. 다른 항목을 변경하려면 항목 유형에 적합한 추가, 제거 또는 변경 명령을 사용하십시오. 예를 들어, 워크스테이션 항목을 변경하려면 CHGWSE(워크스테이션 항목 변경) 명령을 사용하십시오.

*작업 관리*에서는 서브시스템 설명의 작업에 대해 자세한 내용을 제공합니다. 또한 IBM 제공 서브시스템 설명에 제공된 값도 나열합니다.

자동시작 작업 항목

자동시작 작업 항목은 작업 설명 이름을 포함합니다. 작업 설명에는 프로그램 또는 명령을 실행시키는 RQSDTA(요구 자료)가 포함될 수 있습니다. 예를 들면, RQSDTA는 `CALL LIB1/PROGRAM1`일 수 있습니다. 서브시스템이 시작될 때마다 시스템은 라이브러리 LIB1에서 프로그램 PROGRAM1을 실행합니다.

자동시작 작업 항목 및 연관 작업 설명을 참조하십시오. 서브시스템이 시작할 때 자동으로 실행되는 프로그램의 기능을 잘 알고 있어야 합니다.

워크스테이션 이름 및 워크스테이션 유형

서브시스템이 시작하면, 서브시스템은 워크스테이션명 및 유형에 대한 항목에(상세하게 또는 총칭적으로) 나열된 할당되지 않은 모든 워크스테이션을 할당합니다. 사용자가 시작하면, 사용자는 워크스테이션을 할당한 서브시스템으로 사인 온하게 됩니다.

워크스테이션 항목은 작업이 해당 워크스테이션에서 시작할 때 어느 작업 설명을 사용할 것인지를 알려 줍니다. 작업 설명에는 프로그램 또는 명령을 실행시키는 요구 자료가 포함될 수 있습니다. 예를 들면, RQSDTA 매개변수는 `CALL LIB1/PROGRAM1`일 수 있습니다. 사용자가 해당 서브시스템에 있는 워크스테이션을 시작할 때마다 시스템은 LIB1에서 PROGRAM1을 실행합니다.

워크스테이션 항목 및 연관 작업 설명을 참조하십시오. 사용자가 알지 못하는 프로그램을 실행하기 위해 아무도 항목을 추가 또는 갱신한 적이 없는지 확인하십시오.

워크스테이션 항목은 디폴트 사용자 프로파일을 지정할 수도 있습니다. 일부 서브시스템 구성의 경우, 이 지정은 누군가가 단지 Enter 키를 눌러서 사인 온할 수 있게 합니다. 시스템의 보안 레벨(QSECURITY 시스템 값)이 40 미만이면, 디폴트 사용자에 대한 워크스테이션 항목을 검토해야 합니다.

작업 대기행렬 항목

서브시스템이 시작하면, 서브시스템은 서브시스템 설명에 나열된 할당되지 않은 모든 작업 대기행렬을 할당합니다. 작업 대기행렬 항목은 직접적인 보안 노출을 제공하지 않습니다. 그러나 작업을 무인 환경에서 실행하도록 함으로써, 시스템 성능을 바꿀 수 있는 기회를 제공할 수 있습니다.

서브시스템 설명에 있는 작업 대기행렬 항목을 정기적으로 검토하여 일괄처리 작업이 원하는 위치에서 실행되는지를 확인해야 합니다.

라우팅 항목

라우팅 항목은 서브시스템에 들어간 후 작업이 수행하는 일을 정의합니다. 서브시스템은 일괄처리, 대화식 및 통신 작업 등 모든 작업 유형에 라우팅 항목을 사용합니다. 라우팅 항목은 다음을 지정합니다.

- 작업에 대한 클래스. 작업 대기행렬 항목과 같이 작업과 연관된 클래스는 그 성능에 영향을 줄 수 있지만, 보안 노출을 나타내지는 않습니다.
- 작업이 시작할 때 실행하는 프로그램. 라우팅 항목을 참조하여 사용자가 알지 못하는 프로그램을 실행하기 위해 아무도 항목을 추가 또는 갱신한 적이 없는지 확인하십시오.

통신 항목 및 리모트 위치명

통신 작업이 시스템에 입력되면, 시스템은 활동중인 서브시스템에서 통신 항목 및 리모트 위치명 항목을 사용하여 통신 작업의 실행 방법을 판별합니다. 이러한 항목에 대해 다음 사항을 참조하십시오.

- 모든 서브시스템은 통신 작업을 실행할 수 있습니다. 통신에 사용할 서브시스템이 활동중이 아니면, 시스템에 들어오려는 작업이 다른 서브시스템 설명에서 요구를 충족시키는 항목을 찾을 수 있습니다. 따라서, 모든 서브시스템 설명에 있는 항목을 참조해야 합니다.
- 통신 항목은 작업 설명을 포함합니다. 작업 설명에는 프로그램 또는 명령을 실행시키는 요구 자료가 포함될 수 있습니다. 통신 항목 및 연관 작업 설명을 참조하여 작업의 시작 방법을 알아두십시오.
- 통신 항목은 또한 시스템이 일부 상황에서 사용하는 디폴트 사용자 프로파일을 지정합니다. 디폴트 프로파일의 역할을 알아두십시오. 시스템에 디폴트 프로파일이 있는 경우, 최소의 권한을 가진 프로파일인지 확인하십시오. 디폴트 사용자 프로파일에 대한 자세한 내용은 제 12 장『APPC 통신 보안』을 참조하십시오.

  PRTSBSDAUT(서브시스템 설명 인쇄) 명령을 사용하여 사용자 프로파일명을 지정하여 통신 항목을 식별할 수 있습니다.

사전시작 작업 항목

사전시작 작업 항목을 사용하여 작업이 보다 빨리 시작하도록 일부 종류의 작업에 대해 서브시스템을 준비시킬 수 있습니다. 사전시작 작업은 서브시스템이 시작할 때 또는 필요할 때 시작할 수 있습니다. 사전시작 작업 항목은 다음을 지정합니다.

실행할 프로그램

디폴트 사용자 프로파일

작업 설명

위의 사항 모두 잠재적인 보안 노출을 제공합니다. 사전시작 작업 항목이 권한을 부여받은 의도한 기능만 수행하도록 확인해야 합니다.

작업 및 작업 설명

작업 설명은 해당 작업 설명을 사용할 때 특정 프로그램을 실행시키는 요구 자료 및 라우팅 자료를 포함합니다. 작업 설명이 요구 자료 매개변수에 프로그램을 지정하면 시스템은 그 프로그램을 실행합니다. 작업 설명이 라우팅 자료를 지정하면, 시스템은 라우팅 자료와 일치하는 라우팅 항목에 지정된 프로그램을 실행합니다.

시스템은 대화식 및 일괄처리 작업 모두에 작업 설명을 사용합니다. 대화식 작업에 대해 워크스테이션 항목은 작업 설명을 지정합니다. 일반적으로 워크스테이션 항목값은 *USRPRF이므로, 시스템은 사용자 프로파일에 지정된 작업 설명을 사용합니다. 일괄처리 작업에 대해서는 작업을 제출할 때 작업 설명을 지정하십시오.

작업 설명을 정기적으로 검토하여 의도하지 않은 프로그램을 실행하지 않도록 하십시오. 또한, 오브젝트 권한을 사용하여 작업 설명에 대한 변경을 방지해야 합니다. 작업 설명이 있는 작업 실행에는 *USE 권한으로 충분합니다. 일반 사용자는 작업 설명에 대한 *CHANGE 권한이 필요하지 않습니다.

SECBATCH 메뉴 옵션

15 *즉시 제출* **54** *작업 스케줄러 사용*

작업 설명은 또한 어떤 사용자 프로파일에서 작업을 실행해야 하는지를 지정할 수 있습니다. 보안 레벨이 40 이상이면, 작업 설명 및 작업 설명에 지정된 사용자 프로파일에 대한 *USE 권한이 있어야 합니다. 보안 레벨이 40 미만인 경우, 작업 설명에 대해서만 *USE 권한이 있어야 합니다.

PRTJOBDAUT(작업 설명 권한 인쇄) 명령을 사용하여 사용자 프로파일을 지정하고, 공용 권한 *USE를 갖는 작업 설명 리스트를 인쇄할 수 있습니다.

위 보고서는 작업 설명에 지정된 사용자 프로파일의 특수 권한을 보여줍니다. 보고서에는 사용자 프로파일이 가지고 있는 그룹 프로파일의 특수 권한이 포함됩니다. 다음 명령을 사용하여 사용자 프로파일의 개인 권한을 표시할 수 있습니다.

```
DSPUSRPRF USRPRF(profile-name) TYPE(*OBJAUT)
```

작업 설명은 작업 실행시 작업이 사용하는 라이브러리 리스트를 지정합니다. 사용자의 라이브러리 리스트를 변경할 수 있는 사용자는 다른 라이브러리에서 무인 버전 프로그램을 실행할 수도 있습니다. 시스템의 작업 설명에 지정된 라이브러리 리스트를 정기적으로 검토해야 합니다.

마지막으로 무인 작업 설명을 가리키기 위해 SBMJOB(작업 제출) 명령과 CRTUSRPRF(사용자 프로파일 작성) 명령의 디폴트 값을 변경했는지 확인해야 합니다.

구조 트랜잭션 프로그램명

일부 통신 요구는 시스템에 특정 유형의 신호를 송신합니다. 트랜잭션 프로그램명이 시스템의 APPC 구조의 부분이므로, 이 요구를 **구조 트랜잭션 프로그램명(TPN)**이라고 합니다. 표시장치 pass-through 요구가 TPN 구조의 한 예입니다. 구조 TPN은 통신이 기능할 수 있는 정상적인 방법이며, 반드시 보안 노출을 표시하지는 않습니다. 그러나 구조 TPN은 시스템으로의 예기치 않은 진입을 제공할 수 있습니다.

일부 TPN은 요구시 프로파일을 전달하지 않습니다. 디폴트 사용자가 *SYS인 통신 항목과 연관되면, 해당 요구가 시스템에서 시작될 수 있습니다. 그러나 *SYS 프로파일은 시스템 기능만 실행할 수 있으며 사용자 어플리케이션은 실행하지 못합니다.

구조 TPN이 디폴트 프로파일을 사용하여 실행되지 않게 하려면, 통신 항목에서 디폴트 사용자를 *SYS에서 *NONE으로 변경할 수 있습니다. 100 페이지의 『구조화된 TPN 요구』는 구조 TPN 및 연관 사용자 프로파일을 나열합니다.

특정 TPN이 시스템에서 전혀 실행되지 못하게 하려면 다음을 수행하십시오.

1. 몇 가지 매개변수를 승인하는 CL 프로그램을 작성하십시오. 프로그램은 기능을 수행해서는 안 됩니다. 단지 매개변수에 대한 DCL(Declare)문만 가져야 하며, 그런 다음 종료해야 합니다.
2. 통신 항목 또는 리모트 위치명 항목을 갖는 각 서브시스템에 TPN에 대한 라우팅 항목을 추가하십시오. 라우팅 항목은 다음 사항을 지정해야 합니다.
   - 시작 위치가 37인 TPN(구조화된 TPN 요구 참조)에 대한 프로그램명과 동일한 *값 비교*(CMPVAL) 값.
   - 1단계에서 작성한 프로그램명과 일치하는 PGM(*호출할 프로그램*) 값. 이렇게 하면 TPN이 *ANY와 같은 다른 라우팅 항목을 찾을 수 없습니다.

여러 TPN이 이미 QCMN 서브시스템에 자체의 라우팅 항목을 가지고 있습니다. 성능상의 이유로 이들 TPN이 추가되었습니다.

구조화된 TPN 요구

표 17. TPN 요구를 위한 프로그램 및 사용자

TPN 요구	프로그램	사용자 프로파일	설명
X'30F0F8F1'	AMQCRC6A	*NONE	메세지 대기행렬화
X'06F3F0F1'	QACSOTP	QUSER	APPC 사인 온 트랜잭션 프로그램
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC 구성
X'30F0F1F9'	QCNPCSUP	*NONE	공유 폴더
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	리모트 SQL-DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX-PC 리시버
X'30F0F1F3'	QDXPSEND	QUSER	DSNX-PC 송신자
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 서버
X'30F0F6F0'	QHQTRGT	*NONE	PC 자료 대기행렬
X'30F0F8F0'	QLZPSERV	*NONE	Client Access 사용권 관리자
X'30F0F1F7'	QMFRCVR	*NONE	PC 메세지 수신자
X'30F0F1F8'	QMFSNDR	*NONE	PC 메세지 송신자
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 워크스테이션 제어기
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	시스템 관리 유틸리티
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I 네트워크 인쇄 서버
X'30F0F7F9'	QOCEVOKE	*NONE	상호 시스템 캘린더
X'30F0F6F1'	QOKCSUP	QDOC	디렉토리 새도우 처리
X'20F0F0F7'	QOQSESRV	QUSER	DIA 버전 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA 버전 2

표 17. TPN 요구를 위한 프로그램 및 사용자 (계속)

TPN 요구	프로그램	사용자 프로파일	설명
X'30F0F5F1'	QOQSESRV	QUSER	DIA 버전 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA 버전 1
X'30F0F0F5'	QPAPAST2	QUSER	S/36--S/38 passthru
X'30F0F0F9'	QPAPAST2	QUSER	프린터 pass-through
X'30F0F4F6'	QPWFSTP0	*NONE	공유 폴더 유형 2
X'30F0F2C8'	QPWFSTP1	*NONE	Client Access 파일 서버
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** Client Access 파일 서버
X'30F0F6F9'	QRQSRVX	*NONE	리모트 SQL 수렴 서버
X'30F0F6F5'	QRQSRV0	*NONE	확약 없는 리모트 SQL
X'30F0F6F4'	QRQSRV1	*NONE	확약 없는 리모트 SQL
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 수신자
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 송신자
X'30F0F1F6'	QTFDWNLD	*NONE	PC 전송 기능
X'30F0F2F4'	QTIHNPCS	QUSER	TIE 기능
X'30F0F1F5'	QVPPRINT	*NONE	PC 가상 인쇄
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 서버
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I 자료 액세스 서버
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS 수신자
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS 송신자
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I 자료 대기행렬 서버
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I 리모트 명령 서버
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I 중앙 서버

보안 이벤트를 모니터하기 위한 방법

보안 설정은 한번에 시도되지 않습니다. 시스템에서의 변경사항과 보안 실패를 계속해서 평가해야 합니다. 그런 다음, 보안 환경을 조정하여 발견한 사항에 대응하십시오.

보안 보고서를 사용하면 시스템에서 발생하는 보안 관련 변경사항을 모니터할 수 있습니다. 다음은 보안 실패 또는 노출을 감지하기 위해 사용할 수 있는 기타 시스템 기능입니다.

- 보안 감사는 시스템에서 발생하는 여러 유형의 보안 관련 이벤트를 관찰할 때 사용할 수 있는 강력한 툴입니다. 예를 들면, 사용자가 갱신을 위해 특정 데이터베이스 파일을 열 때마다 감사 레코드를 기록하도록 시스템을 설정할 수 있습니다. 시스템 값에 대한 모든 변경사항을 감사할 수 있습니다. 사용자가 오브젝트를 복원할 때 발생하는 조치를 감사할 수 있습니다.

  iSeries 보안 참조서 책의 제 9 장은 보안 감사 기능에 관한 자세한 내용을 제공합니다. CHGSECAUD(보안 감사 변경) 명령을 사용하여 시스템에 보안 감사를 설정

할 수 있습니다. 또한, DSPAUDJRNE(감사 저널 항목 표시) 명령을 사용하여 보안 감사 저널에서 선택한 정보를 인쇄할 수 있습니다.

- QSYSMSG 메세지 대기행렬을 작성하여 중대한 시스템 오퍼레이터 메세지를 캡처할 수 있습니다. QSYSOPR 메세지 대기행렬은 일반 업무일에 다양한 정도의 중요성을 지니는 여러 메세지를 수신합니다. QSYSOPR 메세지 대기행렬의 중요성이 덜한 메세지 볼륨으로 인해 중대한, 보안 관련 메세지가 간과될 수 있습니다.

  QSYSMSG 메세지 대기행렬을 시스템의 QSYS 라이브러리를 작성하는 경우, 시스템은 자동으로 일부 중대한 메세지를 QSYSOPR 메세지 대기행렬 대신 QSYSMSG 메세지 대기행렬로 방향지정합니다.

  프로그램을 작성하여 QSYSMSG 메세지 대기행렬을 모니터하거나 구분 모드로 사용자 자신 또는 다른 신뢰할 수 있는 사용자에게 할당할 수 있습니다.

제 3 부 어플리케이션 및 네트워크 통신

제 11 장 보안된 파일에 통합 파일 시스템 사용

통합 파일 시스템은 iSeries 서버에 정보를 저장하고 열람할 수 있는 여러 가지 방법을 제공합니다. 통합 파일 시스템은 스트림 입출력 조작을 지원하는 OS/400 오퍼레이팅 시스템의 일부입니다. 퍼스널 컴퓨터 오퍼레이팅 시스템 및 UNIX® 오퍼레이팅 시스템과 유사하고(호환될 수 있는) 기억장치 관리 방법을 제공합니다.

통합 파일 시스템의 경우, 시스템의 모든 오브젝트는 계층적 디렉토리 구조에서 열람할 수 있습니다. 그러나 대부분의 경우 사용자는 특정 파일 시스템에 대하여 가장 공통적인 방법으로 오브젝트를 열람합니다. 예를 들어, ″기존″ iSeries 오브젝트는 QSYS.LIB 파일 시스템에 있습니다. 일반적으로 사용자는 라이브러리의 관점에서 이러한 오브젝트를 열람합니다. 사용자들은 폴더 내에 문서의 관점에서 QDLS 파일 시스템에 있는 오브젝트를 열람합니다. 루트(/)인 QOpenSys 및 사용자 정의 파일 시스템은 계층(내포) 디렉토리의 구조를 나타냅니다.

보안 관리자로서 다음 사항을 알아야 합니다.

- 시스템에서 사용되는 파일 시스템
- 각 파일 시스템의 고유 보안 특성

다음 주제는 통합 파일 시스템의 보안에 대한 일부 일반 고려사항을 제공합니다.

통합 파일 시스템 보안 접근

루트 파일 시스템은 iSeries 서버에 있는 다른 모든 파일 시스템에 대하여 포괄적(또는 토대)으로 작용합니다. 상위 단계에서 루트 파일 시스템은 시스템의 모든 오브젝트의 통합 보기를 제공합니다. iSeries 서버에 존재할 수 있는 다른 파일 시스템은 기반이 되는 각 파일 시스템의 목적에 따라 오브젝트 관리 및 통합으로 다양한 접근을 제공합니다. 예를 들어, QOPT(광) 파일 시스템으로 iSeries 어플리케이션 및 서버(Windows용 iSeries Access 파일 서버 포함)가 iSeries 서버의 CD-ROM 드라이브를 액세스할 수 있습니다. 마찬가지로, QFileSvr.400 파일 시스템은 어플리케이션이 리모트 iSeries 서버의 통합 파일 시스템 자료에 액세스할 수 있게 합니다. QLANSrv 파일 서버는 네트워크에 있는 iSeries용 통합 xSeries 서버 또는 다른 연결 서버에 저장된 파일에 대한 액세스를 허용합니다.

각 파일 시스템에 대한 보안 접근은 파일 시스템이 사용할 수 있는 자료에 따라 다릅니다. 예를 들어, QOPT 파일 시스템은 권한 정보를 CD-ROM에 기록할 수 있는 기술이 없으므로, 오브젝트 레벨 보안을 제공하지 않습니다. QFileSvr.400 파일 시스템의 경우, 액세스 제어는 파일이 실제 저장 및 관리되는 리모트 시스템에서 발생합니다. QLANSrv와 같은 파일 시스템의 경우, iSeries용 통합 xSeries 서버는 액세스 제어를

제공합니다. 다른 보안 모델에도 불구하고 많은 파일 시스템은 CHGAUT(권한 변경) 및 CHGOWN(소유자 변경)과 같은 통합 파일 시스템 명령을 통한 액세스 제어의 일관성 있는 관리를 지원합니다.

다음은 통합 파일 시스템 보안의 헛점과 관련된 일부 추가 정보입니다. 통합 파일 시스템은 최대한으로 POSIX 표준에 따라 설계되었습니다. 이것은 결국 iSeries 권한과 POSIX 권한이 ″혼합된″ 곳에서 관심있는 일부 작동을 가져옵니다.

1. 사용자가 공용 권한, 그룹 또는 권한 부여 리스트를 통해 권한을 부여받더라도 그 사용자가 소유한 디렉토리에 대해 사용자의 개인 권한을 제거하지 마십시오. 표준 iSeries 서버 보안 모델 안의 라이브러리나 폴더에 대해 작업할 때, 소유자의 개인 권한을 제거하는 것은 사용자 프로파일에 저장된 권한 정보의 양을 감소시키며 다른 조작에 영향을 주지 않습니다. 그러나 POSIX 표준이 디렉토리에 대한 권한 상속을 정의하는 방식으로 인해 새로 작성된 디렉토리의 소유자가 상위 디렉토리에 대해 다른 개인 권한을 갖더라도, 상위 디렉토리의 소유자가 상위 디렉토리에 대해 가진 것과 동일한 오브젝트 권한을 새로 작성된 디렉토리의 소유자가 그 디렉토리를 갖습니다. 이것을 이해하는 것은 쉽지 않으므로 한 가지 예를 들어보겠습니다. USERA가 /DIRA 디렉토리를 소유하지만 USERA의 개인 권한은 제거되지 않았습니다. USERB에는 /DIRA에 대한 개인 권한이 있습니다. USERB가 /DIRA/DIRB 디렉토리를 작성합니다. USERA가 /DIRA에 대해 오브젝트 권한이 없으므로 USERB가 /DIRA/DIRB에 대해 오브젝트 권한을 갖지 않습니다. USERB가 USERB의 오브젝트 권한을 변경하는 데 있어서 더 이상의 조치 없이는 /DIRA/DIRB를 삭제하거나 이름을 변경할 수 없습니다. 이것은 O_INHERITMODE 플래그를 사용하는 open() API와 함께 파일을 작성할 때에도 해당합니다. USERB가 /DIRA/FILEB 파일을 작성한 경우에는 USERB에 어떤 오브젝트 권한 AND도 없으면 어떤 자료 권한도 없습니다. USERB가 신규 파일로 기록할 수 없습니다.
2. 허용된 권한은 대부분의 실제 파일(PF) 시스템이 무시합니다. 여기에는 루트(/), QOpenSys, QDLS 및 사용자 정의 파일 시스템이 포함됩니다.
3. 사용자 프로파일의 OWNER 필드가 *GRPPRF로 설정된 경우에도 오브젝트는 오브젝트를 작성한 사용자 프로파일이 소유합니다.
4. 많은 파일 시스템 조작들이 루트(/) 디렉토리를 포함하여 경로의 각 구성요소에 대해 *RX 자료 권한을 필요로 합니다. 권한 문제가 발생할 때에는 루트 자체에 대한 사용자의 권한을 검사해 보십시오.
5. 현재 작업 디렉토리를 표시하거나 검색하려면(DSPCURDIR, getcwd() 등) 경로의 각 구성요소에 대해 *RX 자료 권한이 필요합니다. 그러나 현재 작업 디렉토리를 변경하는 것은(CD, chdir() 등) 각 구성요소에 대해 *X 자료 권한만을 필요로 합니다. 따라서 사용자가 현재 작업 디렉토리를 특정 경로로 변경한 다음 그 경로를 표시하는 것은 불가능합니다.
6. COPY 명령의 목적은 오브젝트를 복제하는 것입니다. 신규 파일에 대한 권한 설정은 소유자를 제외하고 원래의 것과 같습니다. 그러나 CPYTOSTMF 명령의 목적

은 단순히 자료를 복제하는 것입니다. 신규 파일에 대한 권한 설정은 사용자가 제어할 수 없습니다. 작성자/소유자가 *RWX 자료 권한을 갖지만 그룹 및 공용 권한이 *EXCLUDE입니다. 원하는 권한을 할당하려면 반드시 다른 방법(CHGAUT, chmod()을 사용해야 합니다.

7. 오브젝트에 관한 권한 정보를 검색하려면 사용자가 반드시 소유자이거나 오브젝트에 대해 *OBJMGT 오브젝트 권한이 있어야 합니다. 이것은 COPY와 같이 목표 오브젝트에 동등한 권한을 설정하기 위해 소스 오브젝트에서 권한 정보를 반드시 검색해야 하는 일부 예상하지 못한 경우에서 발생합니다.
8. 오브젝트의 소유자나 그룹을 변경할 때에는 사용자에게 오브젝트에 대한 적절한 권한을 포함하여 신규 소유자/그룹 사용자 프로파일에 대한 *ADD 자료 권한과 이전 소유자/그룹 프로파일에 대한 *DELETE 자료 권한이 반드시 있어야 합니다. 이 자료 권한들은 파일 시스템 자료 권한과 관련이 없습니다. 이 자료 권한들은 DSPOBJAUT 명령으로 표시하고 EDTOBJAUT 명령으로 변경할 수 있습니다. 또한 신규 오브젝트를 위해 그룹 ID를 설정하려 할 때 예상 밖으로 COPY에서 발생하기도 합니다.
9. MOV 명령은 특히 하나의 실제 파일 시스템으로부터 다른 실제 파일 시스템으로 이동하거나 자료 변환을 수행할 때 권한 오류를 발생시키는 경향이 있습니다. 이와 같은 경우, 실제로는 이동이 복사 및 삭제 조작이 됩니다. 따라서 MOV 명령이 기타 특정 MOV 고려사항에 더하여 COPY 명령(위의 7과 8 참조) 및 RMVLNK 명령과 동일한 모든 권한 고려사항에 영향을 받습니다.

다음 절에서는 여러 가지 대표적인 파일 시스템에 대한 고려사항을 제공합니다. iSeries 서버에 특정 파일 시스템에 대한 자세한 정보는 파일 시스템을 사용하는 사용권 프로그램에 대한 문서를 참조할 필요가 있습니다.

루트(/), QOpenSys 및 사용자 정의 파일 시스템

다음은 루트, QOpenSys 및 사용자 정의 파일 시스템에 대한 보안 고려사항입니다.

권한 작동 방식

루트, QOpenSys 및 사용자 정의 파일 시스템은 오브젝트 관리 및 보안 둘다에 대한 iSeries 서버, PC 및 UNIX**의 혼합 기능을 제공합니다. iSeries 서버 세션(WRKAUT 및 CHGAUT)에서 통합 파일 시스템 명령을 사용할 때, 사용자는 모든 정상 iSeries 서버 오브젝트 권한을 설정할 수 있습니다. 여기에는 (UNIX 유형의 오퍼레이팅 시스템) 스펙 1170과 호환되는 *R, *W, *X 권한이 포함됩니다.

주: 루트, QOpenSys 및 사용자 정의 파일 시스템은 기능적으로 동등합니다. QOpenSys 파일 시스템은 대소문자를 구분합니다. 루트 파일 시스템은 대소문자를 구분하지 않

습니다. 사용자 정의 파일 시스템은 대소문자를 구분하여 정의될 수 있습니다. 두 파일 시스템이 같은 보안 특성을 가지므로, 다음에서는 두 파일명이 서로 바뀌어 사용됩니다.

PC 세션으로부터 관리자로서 루트 파일 시스템에 액세스할 때, PC가 특정 액세스 유형을 제한하는 데 사용하는 오브젝트 속성을 설정할 수 있습니다.

- 시스템
- 숨김
- 아카이브
- 읽기 전용

PC 속성은 iSeries 서버 오브젝트 권한값을 대체하는 것이 아니라 추가하는 것입니다.

루트 파일 시스템에 있는 오브젝트에 액세스를 시도할 때, OS/400은 해당 권한이 사용자의 인터페이스에서 ″가시적″인지에 관계없이 모든 오브젝트 권한값과 오브젝트에 대한 속성을 강제합니다. 예를 들면, 오브젝트에 대한 읽기 전용 속성이 on으로 설정되었다고 가정합니다. PC 사용자는 iSeries Access 인터페이스를 통해 오브젝트를 삭제할 수 없습니다. 고정 기능 워크스테이션을 갖는 iSeries 서버 사용자는 iSeries 서버 사용자가 *ALLOBJ 특수 권한을 갖더라도 오브젝트를 삭제할 수 없습니다. 오브젝트가 삭제되기 전에 권한을 부여받은 사용자는 PC 기능을 사용하여 읽기 전용값을 `off`로 재설정해야 합니다. 이와 같이 PC 사용자는 오브젝트의 PC 관련 보안 속성을 변경할 정도의 충분한 OS/400 권한을 갖고 있지 않습니다.

iSeries 서버에서 실행하는 API(어플리케이션 프로그래밍 인터페이스)와 UNIX 유형 어플리케이션 프로그래밍 인터페이스를 사용하여 루트 파일 시스템에 있는 자료로 액세스할 수 있습니다. UNIX 유형 API의 경우, 어플리케이션은 다음 보안 정보를 인식하고 유지보수할 수 있습니다.

- 오브젝트 소유자
- 그룹 소유자(iSeries 서버 1차 그룹 권한)
- 읽기(파일)
- 쓰기(내용 변경)
- 실행(프로그램 실행 또는 디렉토리 탐색)

시스템은 기존 iSeries 서버 오브젝트와 자료 권한에 대하여 이들 자료 권한을 맵핑합니다.

- 읽기(*R) = *OBJOPR 및 *READ
- 쓰기(*W) = *OBJOPR, *ADD, *UPD, *DLT
- 실행(*X) = *OBJOPR 및 *EXECUTE

다른 오브젝트 권한(*OBJMGT, *OBJEXIST, *OBJALTER 및 *OBJREF)에 대한 개념은 UNIX 유형 환경에 존재하지 않습니다.

그러나 이들 오브젝트 권한이 루트 파일 시스템의 모든 오브젝트에 대해 존재하는 것은 아닙니다. UNIX와 같은 API를 사용하여 오브젝트를 작성할 때 그 오브젝트는 상위 디렉토리로부터 이들 권한을 물려받습니다. 그 결과는 다음과 같습니다.

- 새로운 오브젝트의 소유자는 상위 디렉토리 소유자와 같은 오브젝트 권한을 가집니다.
- 새로운 오브젝트의 1차 그룹은 상위 디렉토리의 1차 그룹과 같은 오브젝트 권한을 가집니다.
- 새로운 오브젝트의 공용은 상위 디렉토리의 공용과 같은 오브젝트 권한을 가집니다.

소유자, 1차 그룹 및 공용에 대한 새로운 오브젝트의 자료 권한은 모드 매개변수와 함께 API에서 지정됩니다. 모든 오브젝트 권한이 작동(on)되면 UNIX 유형 환경에서와 같은 권한 작동이 이루어집니다. POSIX와 같은 작동을 원하지 않는 한 '작동(on)'된 채로 두는 것이 가장 좋습니다.

UNIX 유형 API를 사용하는 어플리케이션을 실행할 때, 시스템은 UNIX 유형 어플리케이션에 대하여 "가시적"인지 여부에 관계없이 모든 오브젝트 권한을 강제합니다. 예를 들면, 시스템은 권한 부여 리스트의 개념이 UNIX 유형 오퍼레이팅 시스템에 존재하지 않더라도 권한 부여 리스트의 권한을 강제합니다.

혼합 어플리케이션 환경인 경우, 어떤 특정 환경에서 권한을 변경하면, 다른 환경에서 사용자의 어플리케이션을 침입할 권한을 변경하지 말아야 합니다.

루트(/), QOpenSys 및 사용자 정의 파일 시스템에 대한 보안 작업

통합 파일 시스템을 도입하는 경우, iSeries 서버에는 다중 파일 시스템에서 오브젝트 작업에 대한 명령의 새로운 세트가 제공됩니다. 이 명령 세트는 다음 보안 작업에 대한 명령을 포함합니다.

- CHGAUD(감사 변경)
- CHGAUT(권한 변경)
- CHGOWN(소유자 변경)
- CHGPGP(1차 그룹 변경)
- DSPAUT(권한 표시)
- WRKAUT(권한에 대한 작업)

이러한 명령은 기본 자료 및 오브젝트 권한을 UNIX 유형 권한 서브세트로 그룹화합니다.

***RWX** 읽기/쓰기/실행
***RW** 읽기/쓰기
***R** 읽기
***WX** 쓰기/실행
***W** 쓰기
***X** 실행

또한 UNIX 유형의 API는 보안에 대한 작업에 사용할 수 있습니다.

루트 디렉토리에 대한 공용 권한

시스템에 제공될 때, 루트 디렉토리에 대한 공용 권한은 *ALL(모든 오브젝트 권한 및 모든 자료 권한)입니다. 이 설정은 UNIX 유형 어플리케이션이 기대하는 것과 일반 iSeries 서버 사용자가 기대하는 것을 모두 충족시키는 적응성과 호환성을 제공합니다. iSeries 서버 사용자는 간단히 CRTLIB 명령을 사용하여 QSYS.LIB 파일 시스템에 새로운 라이브러리를 작성할 수 있습니다. 보통 전형적인 iSeries 서버에 대한 권한은 이를 허용합니다. 이와 같이 루트 파일 시스템에 대하여 제공된 설정의 경우, 일반적인 사용자는 PC에 새 디렉토리를 작성할 수 있듯이 루트 파일 시스템에 새 디렉토리를 작성할 수 있습니다.

보안 관리자로서 작성한 오브젝트를 적절하게 보호하는 방법을 사용자들에게 가르쳐야 합니다. 사용자가 라이브러리를 작성할 때 라이브러리에 대한 공용 권한이 *CHANGE(디폴트)이면 안 됩니다. 사용자는 공용 권한을 라이브러리의 내용에 따라 *USE 또는 *EXCLUDE로 설정해야 합니다.

사용자가 루트(/), QOpenSys 또는 사용자 정의 파일 시스템에 새 디렉토리를 작성할 필요가 있는 경우, 다음과 같이 여러 보안 옵션이 있습니다.

- 사용자가 새 디렉토리를 작성할 때 디폴트 권한을 대체하도록 학습할 수 있습니다. 디폴트는 즉시 상위 디렉토리로부터 권한 상속되는 것입니다. 루트 디렉토리에서 새로 작성된 디렉토리의 경우, 디폴트로 공용 권한은 *ALL이 됩니다.
- 루트 디렉토리 아래 ″마스터″ 서브디렉토리를 작성할 수 있습니다. 해당 마스터 디렉토리에 대한 공용 권한을 사용자의 구성 설정에 적절하게 설정하십시오. 그런 다음, 사용자에게 마스터 서브디렉토리에 새 개인용 디렉토리를 작성할 것을 지시합니다. 새로운 디렉토리는 해당 권한을 상속합니다.
- 루트 디렉토리에 대한 공용 권한을 변경하여 해당 디렉토리에 오브젝트를 작성할 수 없도록 할 수 있습니다(*W, *OBJEXIST, *OBJALTER, *OBJREF 및 *OBJMGT 권한을 제거하십시오). 그러나 이 변경이 어플리케이션에 어떤 문제를 발생시킬지 평가해야 합니다. 예를 들어, 루트 디렉토리로부터 오브젝트를 삭제하기를 기대하는 UNIX 유형 어플리케이션을 가질 수 있습니다.

개인 권한 오브젝트 인쇄(PRTPVTAUT) 명령

PRTPVTAUT(개인 권한 인쇄) 명령으로 사용자는 지정된 라이브러리, 폴더 또는 디렉토리에 지정된 유형의 오브젝트에 대한 모든 개인 권한의 보고서를 인쇄할 수 있습니다. 보고서는 지정된 모든 유형의 오브젝트와 오브젝트에 대하여 권한 부여된 사용자를 나열합니다. 이것은 오브젝트에 대한 권한의 다른 소스를 검사하는 방법입니다.

이 명령은 선택한 오브젝트에 대하여 세 가지 보고서를 인쇄합니다. 첫 번째 보고서(전체 보고서)에는 선택한 오브젝트 각각에 대한 모든 개인 권한을 포함합니다. 두 번째

보고서(변경 보고서)에는 PRTPVTAUT 명령이 지정된 라이브러리, 폴더 또는 디렉토리에서 지정된 오브젝트가 이전에 실행되었을 경우, 선택한 오브젝트의 개인 권한에 대한 추가 및 변경사항을 포함합니다. 선택한 유형의 새 오브젝트, 기존 오브젝트에 대한 새 권한 또는 기존 오브젝트에 대한 기존 권한의 변경사항이 '변경 보고서'에 나열됩니다. PRTPVTAUT 명령이 지정된 라이브러리, 폴더 또는 디렉토리에서 지정된 오브젝트가 이전에 실행되지 않은 경우 '변경 보고서'는 없습니다. 명령이 이전에 실행되었으나 오브젝트의 권한에 대한 변경사항이 없을 경우, '변경 보고서'가 인쇄되지만 나열된 오브젝트는 없습니다.

세 번째(삭제 보고서)에는 PRTPVTAUT 명령이 이전에 실행된 이후 지정된 오브젝트로부터 삭제된 개인 권한 사용자가 포함됩니다. 개인 권한을 부여받은 사용자로서 삭제 또는 제거된 오브젝트는 '삭제 보고서'에 나열됩니다. PRTPVTAUT 명령이 이전에 실행되지 않은 경우 '삭제 보고서'는 없습니다. 명령이 이전에 실행되었으나 오브젝트의 권한에 대한 삭제 작업이 없을 경우, '삭제 보고서'가 인쇄되지만 나열된 오브젝트는 없습니다.

제한: 이 명령을 사용하려면 *ALLOBJ 특수 권한이 있어야 합니다.

예:

이 명령은 PAYROLLLIB에서 모든 파일 오브젝트에 대한 전체 보고서, 변경된 보고서 및 삭제된 보고서를 작성합니다.

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

이 명령은 디렉토리 garry에 있는 모든 스트림 파일 오브젝트에 대해 전체 보고서, 변경된 보고서 및 삭제된 보고서를 작성합니다.

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

이 명령은 디렉토리 garry에서 시작하는 서브디렉토리 구조에 있는 모든 스트림 파일 오브젝트에 대한 전체 보고서, 변경된 보고서 및 삭제된 보고서를 작성합니다.

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

공용 권한 부여 오브젝트 인쇄(PRTPUBAUT) 명령

PRTPUBAUT(공용 권한 부여 오브젝트 인쇄) 명령으로 *EXCLUDE인 공용 권한이 없는 지정된 오브젝트의 보고서를 인쇄할 수 있습니다. *PGM 오브젝트의 경우, 사용자가 호출할 수 있는(프로그램이 사용자 정의역 또는 시스템 보안 레벨(QSECURITY 시스템 값)이 30 이하인) *EXCLUDE인 공용 권한이 없는 프로그램만이 보고서에 포함됩니다. 이는 시스템의 모든 사용자가 액세스 권한 부여된 오브젝트에 검사하는 방법입니다.

이 명령은 두 가지 보고서를 인쇄합니다. 첫 번째 보고서(전체 보고서)는 *EXCLUDE의 공용 권한이 없는 지정된 모든 오브젝트를 포함합니다. 두 번째 보고서(변경 보고서)는 PRTPUBAUT 명령이 이전에 실행되었을 때 *EXCLUDE의 공용 권한을 소유했거나 하지 않은 현재 *EXCLUDE의 공용 권한이 없는 오브젝트를 포함합니다. PRTPUBAUT 명령이 지정된 라이브러리, 폴더 또는 디렉토리에서 지정된 오브젝트에 대하여 이전에 실행되지 않은 경우 '변경 보고서'는 없습니다. 명령이 이전에 실행되었으나 오브젝트의 *EXCLUDE 공용 권한에 대한 변경사항이 없을 경우, '변경 보고서'가 인쇄되지만 나열된 오브젝트는 없습니다.

제한: 이 명령을 사용하려면 *ALLOBJ 특수 권한이 있어야 합니다.

예:

이 명령은 *EXCLUDE의 공용 권한이 없는 라이브러리 GARRY에 있는 모든 파일 오브젝트에 대한 전체 보고서 및 변경된 보고서를 작성합니다.

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

이 명령은 *EXCLUDE의 공용 권한이 없는 디렉토리 garry에서 시작하는 서브디렉토리 구조에 있는 모든 스트림 파일 오브젝트에 대한 전체 보고서, 변경된 보고서 및 삭제된 보고서를 작성합니다.

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

QSYS.LIB 파일 시스템으로 액세스 제한

루트 파일 시스템이 우산 파일 시스템이므로, QSYS.LIB 파일 시스템은 루트 디렉토리 내에서 서브디렉토리로서 나타납니다. 그러므로, 사용자 iSeries 서버로 액세스하는 PC 사용자는 일반 PC 명령 및 활동으로 iSeries 서버 라이브러리(QSYS.LIB 파일 시스템)에 저장된 오브젝트를 조작할 수 있습니다. 예를 들어, PC 사용자는 중요한 자료 파일에 대한 라이브러리와 같은 QSYS.LIB 오브젝트를 휴지통으로 끌기할 수 있습니다.

107 페이지의 『루트(/), QOpenSys 및 사용자 정의 파일 시스템』에서 언급했듯이 시스템은 모든 오브젝트 권한에 인터페이스로 가시화할지의 여부를 강요합니다. 그러므로, 사용자가 오브젝트에 대한 *OBJEXIST 권한이 없는 경우, 사용자는 오브젝트를 절단(삭제)할 수 없습니다. 그러나 사용자의 iSeries가 오브젝트 보안이 아닌 메뉴 액세스 보안에 따라 다른 경우, PC 사용자는 절단할 수 있는 QSYS.LIB 파일 시스템의 오브젝트를 쉽게 발견할 것입니다.

시스템의 사용 및 제공하는 다른 액세스 방법을 확장할 때, 사용자는 곧바로 메뉴 액세스 보안이 충분하지 않다는 것을 발견할 것입니다. 47 페이지의 제 5 장 『오브젝트 권한을 사용하여 정보 자산 보호』에서는 오브젝트 보안에 대한 메뉴 액세스 제어 보충에 대한 전략을 논의합니다. 그러나 iSeries 서버는 또한 루트 파일 시스템 디렉토리 구

조를 통해 QSYS.LIB 파일 시스템으로 액세스를 방지하는 간단한 방법을 제공합니다. QPWFSERVER 권한 부여 리스트를 사용하여 루트 디렉토리를 통해 QSYS.LIB 파일 시스템에 액세스할 수 있는 사용자를 제어합니다.

QPWFSERVER 권한 부여 리스트에 대한 사용자의 권한이 *EXCLUDE일 때, 사용자는 루트 디렉토리 구조에서 QSYS.LIB 디렉토리를 입력할 수 없습니다. 사용자의 권한이 *USE일 때 사용자는 디렉토리를 입력할 수 있습니다. 일단 사용자가 디렉토리에 입력할 권한이 있는 경우, 일반 오브젝트 권한은 사용자가 QSYS.LIB 파일 시스템 내에 오브젝트에 수행하려는 활동에 적용됩니다. 즉, QPWFSERVER 권한 부여 리스트에 대한 권한은 전체 QSYS.LIB 파일 시스템으로 가는 문과 같은 역할을 합니다. *EXCLUDE 권한에 대한 사용자의 경우는 문이 잠겨져 있습니다. *USE 권한(또는 더 큰 권한)에 대한 사용자의 경우 문은 열려 있습니다.

대부분의 경우, 사용자는 QSYS.LIB 파일 시스템에 있는 오브젝트에 액세스하기 위하여 디렉토리 인터페이스를 사용할 필요가 없습니다. 공용 권한을 *EXCLUDE에 대한 QPWFSERVER 권한 부여 리스트로 설정하기를 원할 수 있습니다. 권한 부여 리스트에 대한 권한이 사용자 라이브러리를 포함하여 QSYS.LIB 파일 시스템 내에 있는 모든 라이브러리의 문을 열거나 닫는다는 것을 기억하십시오. 제외에 대하여 이의를 제기하는 사용자가 생기면 개인 기준에 대한 요구사항을 평가할 수 있습니다. 적절한 경우, 개인 사용자에게 권한 부여 리스트에 대한 권한을 명시적으로 부여할 수 있습니다. 그러나 사용자가 QSYS.LIB 파일 시스템 내 오브젝트에 대한 적절한 권한이 있는지 확인해야 합니다. 그렇지 않으면, 사용자는 오브젝트 또는 전체 라이브러리를 무심코 삭제할 수 있습니다.

주:

1. 시스템에 제공될 때 QPWFSERVER 권한 부여 리스트에 대한 공용 권한은 *USE입니다.
2. 개별 사용자에게 명시적으로 권한을 부여하면 권한 부여 리스트가 iSeries Access 파일 서비스, NetServer 파일 서비스 및 iSeries 서버간 파일 서비스에 대해서만 액세스를 제어합니다. 이것은 FTP, ODBC 및 기타 네트워크를 통해 같은 디렉토리로 액세스하는 것을 방지하지 않습니다.

보안 디렉토리

루트 파일 시스템 내의 오브젝트에 액세스하려면 해당 오브젝트의 전체 경로를 읽어야 합니다. 디렉토리를 탐색하려면 해당 디렉토리에 대한 *X(*OBJOPR 및 *EXECUTE) 권한이 있어야 합니다. 예를 들어, 다음 오브젝트에 액세스한다고 가정합니다.

```
/companya/customers/custfile.dat
```

companya 디렉토리 및 customers 디렉토리에 대한 *X 권한이 있어야 합니다.

루트 파일 시스템의 경우, 사용자는 오브젝트로 심볼 링크를 작성할 수 있습니다. 개념적으로 심볼 링크는 경로명에 대한 별명입니다. 보통 별명은 전체 경로명보다 더 짧고 기억하기 용이합니다. 그러나 심볼 링크는 오브젝트에 대한 실제 경로를 작성합니다. 사용자는 여전히 오브젝트에 대한 실제 경로에 있는 모든 디렉토리와 서브디렉토리에 대하여 *X 권한을 필요로 합니다.

루트 파일 시스템에 있는 오브젝트의 경우, QSYS.LIB 파일 시스템에 라이브러리 보안을 사용하듯이 디렉토리 보안을 사용할 수 있습니다. 예를 들어, 공용 사용자가 해당 트리 내의 오브젝트에 액세스하지 못하도록 방지하려면 디렉토리의 공용 권한을 *EXCLUDE로 설정할 수 있습니다.

신규 오브젝트에 대한 보안

루트 파일 시스템에 새로운 오브젝트를 작성할 때 작성시 사용하는 인터페이스가 권한을 결정합니다. 예를 들어, CRTDIR 명령 및 디폴트를 사용하면 새로운 디렉토리는 개인 권한, 1차 그룹 권한, 권한 부여 리스트 연관을 포함한 상위 디렉토리의 모든 권한 특성을 상속합니다. 다음 섹션에서는 각 인터페이스 유형에 대해 권한이 결정되는 방식에 대해 설명합니다.

권한은 트리에 있는 더 상위에 있는 디렉토리가 아닌 바로 상위 디렉토리에서 옵니다. 그러므로, 보안 관리자의 두 가지 관점에서 계층의 디렉토리에 대하여 할당한 권한을 열람할 필요가 있습니다.

- 권한(라이브러리 권한 길이)이 트리에 있는 오브젝트로 액세스하는 데 영향을 주는 방법
- 권한(라이브러리에 대한 CRTAUT 값과 같은)이 새로 작성된 오브젝트에 영향을 주는 방법

권장사항: 통합 파일 시스템에서 작업하는 사용자에게 홈 디렉토리(예: /home/usrxxx)를 부여하려면, PUBLIC *EXCLUDE와 같은 보안을 적절히 설정하십시오. 그러면 홈 디렉토리에 작성한 디렉토리는 권한을 상속합니다.

다음은 다른 인터페이스에 대한 권한 상속에 대한 설명입니다.

디렉토리 작성 명령 사용

CRTDIR 명령을 사용하여 새 서브디렉토리를 작성할 때 지정하는 권한에 대한 두 가지 옵션이 있습니다.

- 공용 권한(자료 권한, 오브젝트 권한 또는 둘다)을 지정할 수 있습니다.
- 자료 권한, 오브젝트 권한 또는 둘다에 대하여 *INDIR을 지정할 수 있습니다. 자료 권한 및 오브젝트 권한에 대하여 *INDIR을 지정할 때 시스템은 권한 부여 리스트, 1차 그룹, 공용 권한 및 개인 권한을 포함하여 상위 디렉토리에서 새 오브젝트로 모

든 권한 정보를 정확히 복사합니다(시스템은 QSYS 프로파일 또는 QSECOFR 프로파일이 오브젝트에 대하여 갖는 개인 권한을 복사하지 않습니다).

API를 사용하여 디렉토리 작성

mkdir() API를 사용하여 디렉토리를 작성할 때 소유자, 1차 그룹 및 공용(*R, *W 및 *X의 권한 맵핑 사용)에 대한 자료 권한을 지정할 수 있습니다. 시스템은 상위 디렉토리의 정보를 사용하여 소유자, 1차 그룹 및 공용에 대한 오브젝트 권한을 설정하십시오.

UNIX 유형 오퍼레이팅 시스템에 오브젝트 권한에 대한 개념이 없으므로, mkdir() API는 지정하는 오브젝트 권한을 지원하지 않습니다. 다른 오브젝트 권한을 원할 경우, iSeries 서버 명령(CHGAUT)을 사용할 수 있습니다. 그러나 일부 오브젝트 권한을 제거할 때, UNIX 유형 어플리케이션은 사용자가 작업하기를 기대할 때 작업하지 않을 것입니다.

open() 또는 creat() API를 사용하여 스트림 파일 작성

creat() API를 사용하여 스트림 파일을 작성할 때, 소유자, 1차 그룹 및 공용(*R, *W, *X의 UNIX와 같은 권한 사용)에 대한 자료 권한을 지정할 수 있습니다. 시스템은 상위 디렉토리의 정보를 사용하여 소유자, 1차 그룹 및 공용에 대한 오브젝트 권한을 설정하십시오.

open() API를 사용하여 스트림 파일을 작성할 때 이 권한을 지정할 수도 있습니다. 또한, open() API를 사용할 때 오브젝트가 상위 디렉토리로부터 모든 권한을 물려받도록 지정할 수 있습니다. 이를 상속 모드라고 합니다. 상속 모드를 지정할 때 시스템은 권한 부여 리스트, 1차 그룹, 공용 권한 및 개인 권한을 포함하여 상위 권한에 대하여 완전 대응을 작성합니다. 이 옵션은 CRTDIR 명령에 대해 *INDIR을 지정하는 것과 같이 작업합니다.

PC 인터페이스를 사용하여 오브젝트 작성

PC 어플리케이션을 사용하여 루트 파일 시스템에 오브젝트를 작성할 때, 시스템은 상위 디렉토리로부터 모든 권한을 자동 상속합니다. 이것은 권한 부여 리스트, 1차 그룹, 공용 권한 및 개인 권한을 포함합니다. 오브젝트를 작성할 때 PC 어플리케이션은 권한을 지정하는 것과 같지 않습니다.

QFileSvr.400 파일 시스템

QFileSvr.400 파일 시스템의 경우, 한 iSeries 시스템(SYSTEMA)의 사용자(USERX)가 연결된 다른 iSeries 시스템(SYSTEMB)의 자료에 액세스할 수 있습니다. USERX는 Client Access 인터페이스와 같은 인터페이스를 갖습니다. 리모트 iSeries(SYSTEMB) 서버는 서브디렉토리와 같은 모든 파일 시스템을 갖는 디렉토리를 나타냅니다.

USERX가 이 인터페이스를 사용하여 SYSTEMB로 액세스하고자 할 때, SYSTEMA는 USERX의 사용자 프로파일명 및 암호화된 암호를 SYSTEMB로 송신합니다. 같은 사용자 프로파일 및 암호는 SYSTEMB에 존재하거나 SYSTEMB가 요구를 거부합니다.

SYSTEMB가 요구를 허용할 경우, USERX는 Client Access 사용자와 같이 SYSTEMB로 표시합니다. 같은 권한 검사 규칙이 USERX가 시도하려는 활동에 적용됩니다.

보안 관리자로서 사용자는 QFileSvr.400 파일 시스템은 다른 가능한 사용자 시스템의 문으로 표시됨을 알아야 합니다. 표시장치 passthrough로 대화식 사인 온에 대하여 리모트 사용자를 제한하려고 한다고 가정할 수 없습니다. QSERVER 서브시스템을 실행하고 사용자의 시스템이 다른 iSeries 시스템에 연결된다면, 리모트 사용자는 로컬 PC에 Client Access를 실행하는 것처럼 시스템을 액세스할 수 있습니다. 더구나 시스템은 QSERVER 서브시스템을 실행하는 연결을 갖게 됩니다. 이것이 좋은 오브젝트 권한 구조가 필수적인 또다른 이유입니다.

네트워크 파일 시스템

NFS(네트워크 파일 시스템)는 NFS가 실행하는 시스템으로부터 액세스하여 해당 시스템까지 액세스를 제공합니다. NFS는 네트워크된 시스템상의 사용자들이 정보를 공유할 수 있는 산업 표준 방식입니다. (PC 오퍼레이팅 시스템을 포함하여) 대부분 주요 오퍼레이팅 시스템은 NFS를 제공합니다. UNIX 시스템의 경우, NFS가 자료 액세스를 위한 1차 방법입니다. iSeries 서버는 NFS 클라이언트 및 NFS 서버로서의 역할을 합니다.

NFS 서버로서 작용하는 iSeries 시스템의 보안 관리자일 때, NFS의 보안적 측면을 이해하고 관리해야 합니다. 다음은 제안 및 고려사항입니다.

- STRNFSSVR 명령을 사용하여 NFS 서버 기능을 명시적으로 시작해야 합니다. 이 명령을 사용할 권한을 갖는 사용자를 제어하십시오.
- 내보내기를 이용하여 NFS 클라이언트에 대하여 사용할 수 있는 디렉토리 또는 오브젝트를 만듭니다. 그러면, 네트워크에 NFS 클라이언트에 대하여 사용할 수 있는 시스템의 부분을 매우 특별하게 제어합니다.
- 내보내기할 때 오브젝트로 액세스하는 클라이언트를 지정할 수 있습니다. 시스템명 또는 IP 주소에 의하여 클라이언트를 식별할 수 있습니다. 클라이언트는 개별 PC, 전체 iSeries 서버 또는 UNIX 시스템일 수 있습니다. NFS 용어에서 클라이언트(IP 주소)는 기계라고 합니다.
- 내보내기할 때 내보내기된 디렉토리 또는 오브젝트에 액세스하는 각 기계에 대하여 읽기 전용 액세스 또는 읽기/쓰기 액세스를 지정할 수 있습니다. 대부분의 경우, 읽기 전용 액세스를 제공하려 할 것입니다.

- NFS는 암호 보호를 제공하지 않습니다. 시스템이 신뢰할 수 있는 공동체 내에서 자료를 공유하려는 의도에서 설계되었습니다. 사용자가 액세스를 요구할 때 서버는 사용자의 uid를 수신합니다. 다음은 일부 uid 고려사항입니다.
  - iSeries 서버는 같은 uid를 갖는 사용자 프로파일의 위치를 찾아내려 합니다. 대응하는 uid를 발견할 경우, 사용자 프로파일에 대한 증명서를 사용합니다. 증명서는 사용자의 권한을 사용하여 설명하는 NFS 용어입니다. 이것은 다른 iSeries 서버 어플리케이션에서 프로파일 스왑핑과 유사합니다.
  - 디렉토리 또는 오브젝트를 내보내기할 때 루트 권한을 갖는 프로파일에 의해 액세스를 허용할지를 지정할 수 있습니다. iSeries 서버상의 NFS 서버는 루트 권한을 *ALLOBJ 특수 권한과 동일하게 합니다. 루트 권한을 허용하지 않을 것을 지정하면, *ALLOBJ 특수 권한을 갖는 사용자 프로파일로 맵핑하는 uid가 있는 NFS 사용자는 그 프로파일하의 오브젝트에 액세스할 수 없게 됩니다. 대신, 익명의 액세스가 허용되면 리퀘스터는 익명의 프로파일로 맵핑됩니다.
  - 디렉토리 또는 오브젝트를 내보내기할 때 익명 요구를 허용할 것을 지정할 수 있습니다. 익명 요구는 시스템상의 uid와 일치하지 않는 uid를 갖는 요구입니다. 익명 요구를 허용할 것을 선택한다면, 시스템은 익명의 사용자를 IBM 제공 QNFSANON 사용자 프로파일로 맵핑합니다. 이 사용자 프로파일은 특수 권한 또는 명시적 권한이 없습니다(원하는 경우, 내보내기시 익명 사용자의 요구에 대하여 다른 사용자 프로파일을 지정할 수 있습니다).
- 사용자의 iSeries 서버가 NFS 네트워크(또는 uid에 의존하는 UNIX 시스템이 있는 임의의 네트워크)에 참여할 때, 시스템이 자동으로 할당하게 하는 대신 자체 uid를 직접 관리해야 합니다. 네트워크에서 다른 시스템이 있는 uid를 조정해야 합니다.

  네트워크에 있는 다른 시스템과의 호환성을 갖도록 uid(IBM 제공 사용자 프로파일 조차도)를 변경해야 함을 알 수 있습니다. 이 프로그램은 사용자 프로파일에 대한 uid를 보다 간단하게 변경할 수 있도록 합니다. (사용자 프로파일에 대하여 uid를 변경할 때, 루트 디렉토리 또는 QOpenSrv 디렉토리에 프로파일이 소유하는 모든 오브젝트에 대하여 uid를 변경해야 합니다.) QSYCHGID 프로그램은 사용자 프로파일 및 모든 소유 오브젝트에서 uid를 자동 변경합니다. 이 프로그램의 사용법에 관한 정보는 *iSeries 시스템 API 참조서*를 참조하십시오.

제 12 장 APPC 통신 보안

시스템이 다른 시스템과의 네트워크에 참여할 경우, 시스템의 새로운 문과 창 세트가 사용가능합니다. 보안 관리자로서 APPC 환경에서 시스템에 대한 진입을 제어하기 위해 사용할 수 있는 옵션을 알아야 합니다.

APPC는 퍼스널 컴퓨터를 포함하여, 컴퓨터들이 서로 통신하는 방법을 말합니다. 표시 장치 passthru, 분산 자료 관리(DDM), Windows용 iSeries Access는 모두 APPC 통신을 사용합니다.

다음 주제는 APPC 통신 작업 방법 및 적합한 보안을 설정할 수 있는 방법에 대해 기본적인 정보를 제공합니다. 이 주제는 APPC 구성의 보안 관련 요소를 집중적으로 다룹니다. 이 예를 사용자 상황에 맞게 조정하려면 통신 네트워크를 관리하는 사용자 및 어플리케이션 제공자와 함께 작업해야 합니다. 보안 문제 및 APPC에서 사용할 수 있는 옵션을 이해하려면, 이 정보를 기초로 사용하십시오.

보안은 상당히 『어려운』 문제입니다. 네트워크 보안을 쉽게 유지할 수 있는 일부 제안 사항은 네트워크 관리를 더욱 어렵게 만들 수 있습니다. 예를 들어, APPN® 없이 보안을 이해하고 관리하는 것이 더 쉬우므로, 이 정보는 APPN(대등 시스템간 통신 기능®)을 강조하지 않습니다. 그러나 APPN이 없으면, APPN이 자동으로 작성하는 구성 정보를 네트워크 관리자가 수작업으로 작성해야 합니다.

PC도 통신을 사용함

iSeries 서버에 PC를 연결하는 많은 방법은 APPC 또는 TCP/IP와 같은 통신에 따라 다릅니다. 다음 주제를 읽을 때 다른 시스템 및 PC 둘다의 연결에 대한 보안 문제를 고려하십시오. 네트워크 보호를 계획할 경우, 시스템에 접속된 PC에 악영향을 미치지 않게 하십시오.

APPC 용어

APPC는 한 시스템의 사용자가 다른 시스템에서 작업을 수행할 수 있는 기능을 제공합니다. 요구가 시작되는 시스템을 다음과 같이 부릅니다.

- **소스 시스템**
- **로컬 시스템**
- **클라이언트**

요구를 수신하는 시스템은 다음과 같이 부릅니다.

- **목표 시스템**
- **리모트 시스템**
- **서버**

APPC 통신의 기본 요소

보안 관리자의 관점에서 한 시스템(SYSTEMA) 사용자가 다른 시스템(SYSTEMB)에서 중요한 작업을 수행하기 전에 다음을 준비해야 합니다.

- 소스 시스템(SYSTEMA)은 목표 시스템(SYSTEMB)에 대한 경로를 제공해야 합니다. 이 경로를 **APPC 세션**이라고 합니다.
- 목표 시스템은 사용자를 식별하고 사용자 프로파일과 연관시켜야 합니다. 목표 시스템은 소스 시스템의 암호화 알고리즘을 지원해야 합니다(자세한 내용은 16 페이지의 『암호 레벨』을 참조하십시오).
- 목표 시스템은 적절한 환경(작업 관리값)의 사용자에 대해 작업을 시작해야 합니다.

다음 주제는 이러한 요소 및 보안과 연관되는 방법에 대하여 다룹니다. 목표 시스템의 보안 관리자에게 APPC 사용자가 보안을 위반하지 않도록 보증하는 1차 책임이 있습니다. 그러나 양쪽 시스템의 보안 관리자가 함께 작업할 경우, APPC 보안 관리 작업은 훨씬 용이합니다.

예: 기본 APPC 세션

APPC 환경에서 한 시스템 사용자 또는 어플리케이션이 다른 시스템에 대한 액세스를 요구할 경우, 두 시스템이 하나의 세션을 설정합니다. 세션을 설정하려면 대응하는 두 개의 APPC 장치 설명을 연결해야 합니다. SYSTEMA 장치 설명의 리모트 위치명(RMTLOCNAME) 매개변수는 SYSTEMB 장치 설명의 로컬 위치명(LCLLOCNAME) 매개변수와 일치해야 하고, 그 반대의 경우도 마찬가지입니다.

두 시스템이 하나의 APPC 세션을 설정하려면, SYSTEMA 및 SYSTEMB에 있는 APPC 장치 설명의 위치 암호가 동일해야 합니다. 둘다 *NONE을 지정하거나 둘다 같은 값을 지정해야 합니다.

암호가 *NONE 이외의 값일 경우, 암호는 암호화된 형식으로 저장되어 전송됩니다. 암호가 일치하면 세션이 설정됩니다. 암호가 일치하지 않으면 사용자의 요구가 거부됩니다. 위치 암호를 지정하여 세션을 설정할 경우, 이를 **보안 바인드**라고 합니다.

주: 모든 컴퓨터 시스템이 보안 바인드 기능에 대한 지원을 제공하지는 않습니다.

APPC 세션 제한

소스 시스템의 보안 관리자로서 오브젝트 권한을 사용하여 다른 시스템에 액세스할 수 있는 사용자를 제어할 수 있습니다. APPC 장치 설명에 대한 공용 권한을 *EXCLUDE

로 설정하고 특정 사용자에게 *CHANGE 권한을 부여하십시오. QLMTSECOFR 시스템 값을 사용하여 *ALLOBJ 특수 권한이 있는 사용자가 APPC 통신을 사용할 수 없도록 하십시오.

목표 시스템의 보안 관리자로서, APPC 장치에 대한 권한을 사용하여 사용자가 시스템에서 APPC 세션을 시작하지 못하게 할 수도 있습니다. 그러나 APPC 장치 설명에 액세스하려는 사용자 ID를 알아야 합니다. 『목표 시스템에 대한 APPC 사용자 액세스』는 iSeries 서버가 사용자 ID를 APPC 세션에 대한 요구와 연관시키는 방법에 대해 설명합니다.

주: PRTPUBAUT *DEVD(공용 권한 부여 오브젝트 인쇄) 명령 및 PRTPVTAUT *DEVD(개인 권한 인쇄) 명령을 사용하여 시스템의 장치 설명에 대한 권한이 있는 사용자를 찾을 수 있습니다.

시스템에서 APPN을 사용할 경우, 시스템이 선택한 라우트에 기존 장치를 사용할 수 없으면 새 APPC 장치를 자동으로 작성합니다. APPN을 사용하는 시스템에서 APPC 장치에 대한 액세스를 제한하는 한 가지 방법은 권한 부여 리스트를 작성하는 것입니다. 권한 부여 리스트에는 APPC 장치에 대하여 권한을 부여받아야 할 사용자의 리스트가 들어 있습니다. 그러면 CHGCMDDFT(명령 디폴트 변경) 명령을 사용하여 CRTDEVAPPC 명령을 변경하십시오. CRTDEVAPPC 명령의 AUT(권한) 매개변수는 작성된 권한 부여 리스트로 디폴트 값을 설정하십시오.

주: 시스템에 영어가 아닌 언어가 있을 경우, 시스템에 있는 QSYSxxxx 라이브러리에서 명령 디폴트를 변경해야 합니다.

APPC 장치 설명의 LOCPWD(위치 암호) 매개변수를 사용하여 시스템(사용자 또는 어플리케이션 대신)의 세션을 요구하는 다른 시스템의 ID에 대해 유효성 검사를 합니다. 위치 암호는 불량 시스템을 감지하는 데 도움이 될 수 있습니다.

위치 암호를 사용할 경우, 네트워크의 다른 시스템에 대한 보안 관리자와 조정해야 합니다. APPC 장치 설명 및 구성 리스트를 작성 또는 변경할 수 있는 사용자도 제어해야 합니다. APPC 장치 및 구성 리스트에 대하여 작업하는 명령을 사용하려면 시스템에 *IOSYSCFG 특수 권한이 있어야 합니다.

주: APPN을 사용할 경우, 위치 암호가 장치 설명이 아닌 QAPPNRMT 구성 리스트에 저장됩니다.

목표 시스템에 대한 APPC 사용자 액세스

APPC 세션을 설정할 때 요구한 사용자가 목표 시스템의 문으로 들어갈 수 있는 경로가 작성됩니다. 사용자가 다른 시스템에 들어가기 위한 여러 가지 다른 요소가 수행해야 할 활동이 판별됩니다.

다음 주제는 APPC 사용자가 목표 시스템에 들어갈 수 있는 방법을 결정하는 요소에 대해 설명합니다.

사용자에 대한 정보를 송신하는 시스템 방법

APPC 구조는 소스 시스템에서 목표 시스템으로 사용자에 대한 보안 정보를 송신할 수 있는 세 가지 방법을 제공합니다. 이러한 방법들은 **구조화된 보안값**으로 언급됩니다. 표 18은 이들 방법을 나타냅니다.

주: *APPC Programming* 책은 구조화된 보안값에 대한 자세한 내용을 제공합니다.

표 18. APPC 구조의 보안값

구조화된 보안값	목표 시스템에 송신된 사용자 ID	목표 시스템에 송신된 암호
없음	아니오	아니오
같음	예[1]	주 2 참조
프로그램	예	예[3]

주:

1. 목표 시스템에 SECURELOC(*YES) 또는 SECURELOC(*VFYENCPWD)가 지정될 경우, 소스 시스템에서 사용자 ID를 송신합니다.
2. 사용자는 암호가 이미 소스 시스템에서 검증되었으므로 요구할 때 암호를 입력하지 않습니다. SECURELOC(*YES) 및 SECURELOC(*NO)의 경우, 소스 시스템에서 암호를 송신하지 않습니다. SECURELOC(*VFYENCPWD)의 경우, 소스 시스템이 저장, 암호화된 암호를 검색한 다음 (암호화된 형식으로) 송신합니다.
3. 이 시스템은 소스 및 목표 시스템이 암호의 암호화를 지원할 경우, 암호화된 형식으로 암호를 송신합니다. 그렇지 않으면, 암호가 암호화되지 않습니다.

사용자가 요구하는 어플리케이션이 구조화된 보안값을 판별합니다. 예를 들면, SNADS는 항상 SECURITY(NONE)를 사용합니다. DDM은 SECURITY(SAME)를 사용합니다. 표시장치 passthru의 경우, 사용자는 STRPASTHR 명령의 매개변수를 사용하여 보안값을 지정합니다.

모든 경우 목표 시스템이 소스 시스템에 지정된 보안값으로 요구를 허용할지 여부를 선택합니다. 어떤 상황에서는 목표 시스템이 요구를 완전히 거부할 수 있습니다. 또다른 상황에서는 목표 시스템이 다른 보안값을 강요할 수 있습니다. 예를 들면, 사용자가 STRPASTHR 명령에 사용자 ID 및 암호를 둘다 지정할 경우, 요구에 SECURITY(PGM)가 사용됩니다. 그러나 QRMTSIGN 시스템 값이 목표 시스템에서 *FRCSIGNON일 경우, 여전히 사인 온 화면이 표시됩니다. *FRCSIGNON이 설정되면 시스템은 항상 사용자가 STRPASTHR 명령에 사용자 ID 및 암호를 입력하지 않는 것과 같은 SECURITY(NONE)를 사용합니다.

주:

1. 소스 및 목표 시스템은 자료를 송신하기 전에 보안값을 협상합니다. 예를 들면, 목표 시스템이 SECURELOC(*NO)를 지정하고 요구가 SECURITY(SAME)인 경우, 목표 시스템은 소스 시스템이 SECURITY(NONE)를 사용하도록 지시합니다. 소스 시스템은 사용자 ID를 송신하지 않습니다.
2. 목표 시스템은 목표 시스템의 사용자 암호가 만기되면 세션 요구를 거부합니다. 다음을 포함하여 암호를 송신하는 연결 요구에만 적용됩니다.
   - 유형 SECURITY(PROGRAM)의 세션 요구
   - SECURELOC 값이 *VFYENCPWD일 경우, 유형이 SECURITY(SAME)인 세션 요구

네트워크 보안 의무 나누기 옵션

사용자 시스템이 네트워크에 참여할 경우, 사용자의 시스템에 들어오려는 사용자의 ID를 유효성 검사를 하는 다른 시스템을 신뢰할지 여부를 판별해야 합니다. USERA가 정말 USERA(또는 QSECOFR이 정말 QSECOFR)인지를 확인하는 SYSTEMA를 신뢰합니까? 아니면 사용자 ID 및 암호를 다시 제공하도록 요구합니까?

목표 시스템의 APPC 장치 설명에 있는 SECURELOC(보안 위치) 매개변수가 소스 시스템이 보안(신뢰) 위치인지를 지정합니다.

두 시스템 모두 *VFYENCPWD를 지원하는 릴리스를 실행할 경우, 어플리케이션에서 SECURITY(SAME)를 사용하면 SECURELOC(*VFYENCPWD)가 추가 보호를 제공합니다. 리퀘스터가 요구할 때 암호를 입력하지 않더라도 소스 시스템이 사용자의 암호를 검색하고 요구와 함께 송신합니다. 요구를 정상적으로 완료하려면, 사용자는 양쪽 시스템에 동일한 사용자 ID 및 암호를 가져야 합니다.

목표 시스템이 SECURELOC(*VFYENCPWD)를 지정하고 소스 시스템이 이 값을 지원하지 않을 경우, 목표 시스템은 요구를 SECURITY(NONE)로 처리합니다.

표 19는 다음과 같이 구조화된 보안값과 SECURELOC 값이 함께 작업하는 방법을 나타냅니다.

표 19. APPC 보안값과 SECURELOC 값이 함께 작업하는 방법

소스 시스템	**목표 시스템**	
구조화된 보안값	**SECURELOC 값**	**작업에 대한 사용자 프로파일**
없음	있음	디폴트 사용자[1]
같음	*NO	디폴트 사용자[1]
	*YES	소스 시스템의 리퀘스터와 동일한 사용자 프로파일명
	*VFYENCPWD	소스 시스템의 리퀘스터와 동일한 사용자 프로파일명. 사용자는 양쪽 시스템에 같은 암호를 가져야 합니다.

표 19. APPC 보안값과 SECURELOC 값이 함께 작업하는 방법 (계속)

소스 시스템	목표 시스템	
구조화된 보안값	**SECURELOC 값**	**작업에 대한 사용자 프로파일**
프로그램	있음	소스 시스템의 요구에 지정된 사용자 프로파일

주:

1. 디폴트 사용자는 서브시스템 설명의 통신 항목에서 판별합니다. 『작업에 대한 사용자 프로파일의 목표 시스템 지정』에서 이에 대하여 설명합니다.

작업에 대한 사용자 프로파일의 목표 시스템 지정

사용자가 다른 시스템에서 APPC 작업을 요구할 경우, 요구에 이와 연관된 모드명이 있습니다. 모드명은 사용자의 요구에서 나오거나 소스 시스템의 네트워크 속성에 있는 디폴트 값입니다.

목표 시스템은 모드명과 APPC 장치명을 사용하여 작업 실행 방법을 판별합니다. 목표 시스템은 APPC 장치명과 모드명에 가장 적합한 통신 항목을 활동 서브시스템에서 탐색합니다.

통신 항목은 시스템이 SECURITY(NONE) 요구에 사용하는 사용자 프로파일을 지정합니다. 다음은 서브시스템 설명에 있는 통신 항목의 예입니다.

```
                          통신 항목 표시

서브시스템 설명:   QCMN                    상태:   ACTIVE

                                                    디폴트
장치          모드        작업 설명      라이브러리   사용자        최대 활동
*ALL          *ANY        *USRPRF                    *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                    *NONE         *NOMAX
```

표 20은 통신 항목의 디폴트 사용자 매개변수에 가능한 값을 나타냅니다.

표 20. 디폴트 사용자 매개변수에 가능한 값

값	결과
***NONE**	디폴트 사용자를 사용할 수 없습니다. 소스 시스템이 요구할 때 사용자 ID를 제공하지 않을 경우, 작업이 실행되지 않습니다.
***SYS**	IBM 제공 프로그램(시스템 작업)만 실행됩니다. 사용자 어플리케이션은 실행되지 않습니다.
user-name	소스 시스템이 사용자 ID를 송신하지 않으면 작업이 이 사용자 프로파일하에서 실행됩니다.

PRTSBSDAUT(서브시스템 설명 인쇄) 명령을 사용하여 통신 항목이 디폴트 사용자 프로파일인 모든 서브시스템의 리스트를 인쇄할 수 있습니다.

표시장치 passthru 옵션

표시장치 passthru는 APPC 통신을 사용하는 어플리케이션의 한 예입니다. 표시장치 passthru를 사용하여 네트워크를 통해 사용자 시스템에 연결된 다른 시스템을 사인 온 할 수 있습니다.

표 21에는 passthru 요구(STRPASTHR 명령)의 예와 목표 시스템이 요구를 처리하는 방법이 나와 있습니다. 표시장치 passthru의 경우, 시스템은 APPC 통신의 기본 요소 및 리모트 사인 온(QRMTSIGN) 시스템 값을 사용합니다.

주: 표시장치 passthru 요구는 QCMN 또는 QBASE 서브시스템을 통해 라우팅되지 않습니다. V4R1부터는 QSYSWRK 서브시스템을 통해 라우팅됩니다. V4R1 이전 버전에서는 QCMD 또는 QBASE 서브시스템이 시작되지 않아 표시장치 passthru가 작동되지 않습니다. 그러나 이후 버전에서는 그렇지 않습니다. QPASTHRSVR 시스템 값을 0으로 변경하여 표시장치 passthru가 QCMN(활동중인 경우에는 QBASE)을 강제로 통과하도록 할 수 있습니다.

표 21. passthru 사인 온 요구 샘플

STRPASTHR 명령에 대한 값		**목표 시스템**		
사용자 ID	**암호**	**SECURELOC 값**	**QRMTSIGN 값**	**결과**
*NONE	*NONE	있음	있음	사용자는 목표 시스템에서 사인 온해야 합니다.
사용자 프로파일명	입력되지 않음	있음	있음	요구가 실패함
*CURRENT	입력되지 않음	*NO	있음	요구가 실패함
		*YES	*SAMEPRF	소스 시스템의 사용자 프로파일과 같은 사용자 프로파일명을 갖는 대화식 작업이 시작합니다.리모트 시스템에 암호가 전달되지 않습니다.사용자 프로파일명은 목표 시스템에 있어야 합니다.
			*VERIFY	
			*FRCSIGNON	사용자는 목표 시스템에서 사인 온해야 합니다.
		*VFYENCPWD	*SAMEPRF	소스 시스템의 사용자 프로파일과 같은 사용자 프로파일명을 갖는 대화식 작업이 시작합니다.소스 시스템은 사용자 암호를 검색한 후, 이를 리모트 시스템으로 보냅니다.사용자 프로파일명은 목표 시스템에 있어야 합니다.
			*VERIFY	
			*FRCSIGNON	사용자는 목표 시스템에서 사인 온해야 합니다.

표 21. passthru 사인 온 요구 샘플 (계속)

STRPASTHR 명령에 대한 값		**목표 시스템**		
사용자 ID	**암호**	**SECURELOC 값**	**QRMTSIGN 값**	**결과**
*CURRENT(또는 작업에 대한 현재 사용자 프로파일명)	입력되지 않음	있음	*SAMEPRF	소스 시스템의 사용자 프로파일과 같은 사용자 프로파일명을 갖는 대화식 작업이 시작합니다.리모트 시스템에 암호가 송신됩니다. 사용자 프로파일명은 목표 시스템에 있어야 합니다.
			*VERIFY	
			*FRCSIGNON	사용자는 목표 시스템에서 사인 온해야 합니다.
사용자 프로파일명(작업에 대한 현재 사용자 프로파일과 다른 이름)	입력되지 않음	있음	*SAMEPRF	요구가 실패함
			*VERIFY	소스 시스템의 사용자 프로파일과 같은 사용자 프로파일명을 갖는 대화식 작업이 시작합니다.리모트 시스템에 암호가 송신됩니다. 사용자 프로파일명은 목표 시스템에 있어야 합니다.
			*FRCSIGNON	대화식 작업은 지정된 사용자 프로파일명으로 시작됩니다. 암호가 목표 시스템으로 전송됩니다. 사용자 프로파일명은 목표 시스템에 있어야 합니다.

예상치 못한 장치 지정 방지

활동중인 장치가 실패하면 시스템이 회복을 시도합니다. 어떤 경우 연결이 단절되면 다른 사용자가 실패한 세션을 무심코 재설정할 수 있습니다. 예를 들면, USERA가 사인 오프하지 않고 워크스테이션 전원을 차단했다고 가정하십시오. USERB가 워크스테이션 전원을 공급하고 사인 온하지 않은 채 USERA의 세션을 재시작할 수 있습니다.

이러한 가능성을 방지하려면 QDEVRCYACN(장치 I/O 오류 활동) 시스템 값을 *DSCMSG로 설정하십시오. 장치가 실패한 경우 사용자 작업이 종료됩니다.

리모트 명령 및 일괄처리 작업 제어

다음을 포함하여 시스템에서 실행될 수 있는 리모트 명령 및 작업을 제어하는 데 도움이 되는 몇 가지 옵션을 사용할 수 있습니다.

- 시스템에서 DDM을 사용할 경우, 다른 시스템에서 SBMRMTCMD(리모트 명령 제출)를 사용할 수 없도록 DDM 파일에 액세스를 제한할 수 있습니다. SBMRMTCMD를 사용하려면 사용자가 DDM 파일을 열 수 있어야 합니다. DDM 파일을 작성하는 기능도 제한해야 합니다.
- DDMACC(DDM 요구 액세스) 시스템 값에 나감 프로그램을 지정할 수 있습니다. 나감 프로그램에서 허용하기 전에 모든 DDM 요구를 평가할 수 있습니다.

- JOBACN(네트워크 작업 활동) 네트워크 속성을 사용하여 네트워크 작업이 제출되지 않거나 자동으로 실행되지 않게 할 수 있습니다.
- 서브시스템 설명에서 PGMEVOKE 라우팅 항목을 제거하여 통신 환경에서 실행할 수 있는 프로그램 요구를 명시적으로 지정할 수 있습니다. 리퀘스터가 PGMEVOKE 라우팅 항목을 사용하여 실행되는 프로그램을 지정할 수 있습니다. QCMN 서브시스템 설명과 같은 서브시스템 설명에서 이 라우팅 항목을 제거할 경우, 정상적으로 실행해야 하는 통신 요구의 라우팅 항목을 추가해야 합니다.

  100 페이지의 『구조화된 TPN 요구』는 IBM 제공 어플리케이션의 통신 요구에 대한 프로그램명을 나열합니다. 허용하려는 각 요구에 대하여 비교값과 프로그램명이 둘 다 프로그램명과 같은 라우팅 항목을 추가할 수 있습니다.

  이 방법을 사용할 경우, 시스템의 작업 관리 환경 및 시스템에서 발생하는 통신 요구의 유형을 알아야 합니다. 가능하면 라우팅 항목을 변경한 후 제대로 작업할 수 있도록 모든 유형의 통신 요구를 테스트해야 합니다. 통신 요구가 사용가능한 라우팅 항목을 찾지 못하면 CPF1269 메세지가 수신됩니다. 다른 대안(오류가 적은 경향이 있으나 다소 비효율적인)은 시스템에서 실행하기를 원하지 않는 트랜잭션 프로그램에 대하여 공용 권한을 *EXCLUDE로 설정하는 것입니다.

  주: *작업 관리* 책은 라우팅 항목과 시스템이 프로그램 시작 요구를 처리하는 방법에 대한 자세한 정보를 제공합니다.

APPC 구성 평가

PRTCMNSEC(통신 보안 인쇄) 명령 또는 메뉴 옵션을 사용하여 APPC 구성에 있는 보안 관련 값을 인쇄할 수 있습니다. 다음 주제는 보고서에 관한 정보를 설명합니다.

APPC 장치에 대한 관련 매개변수

그림 9에서는 장치 설명에 대한 통신 정보 보고서의 예를 보여줍니다. 128 페이지의 그림 10에서는 구성 리스트에 대한 보고서의 예를 보여줍니다. 보고서 다음에는 보고서 필드에 관한 설명이 있습니다.

```
                    통신 정보(전체 보고서)
                                        SYSTEM4
오브젝트 유형  . . . . . . . . . :   *DEVD
                                                                      Pre            SNUF
오브젝트      오브젝트      장치          보안      위치      APPN      단일      설정              프로그램
 이름           유형        범주          위치      암호      가능      세션      세션                시작

CDMDEV1       *DEVD         *APPC         *NO       *NO       *NO       *YES      *NO
CDMDEV2       *DEVD         *APPC         *NO       *NO       *NO       *YES      *NO
```

그림 9. APPC 장치 설명 - 샘플 보고서

```
                        구성 리스트 표시                              1 페이지
                              SYSTEM4  12/17/95  07:24:36
구성 리스트  . . . . . . . . . . . :   QAPPNRMT
구성 리스트 유형  . . . . . . . . :   *APPNRMT
텍스트 . . . . . . . . . . . . . . :
------------------ APPN 리모트 위치 ------------------
          리모트
리모트    네트워크  로컬      리모트    제어점     보안
위치      ID        위치      제어점    Net ID     Loc
SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN       *NO
SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN       *NO
SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN       *YES
SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN       *NO
SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN       *NO
---------------------------- APPN 리모트 위치 ----------------------------
          리모트                                                    사전
리모트    네트워크  로컬       단일              대화     로컬      설정
위치      ID        위치       세션               수     제어점     세션
SYSTEM36  APPN      SYSTEM4    *NO               10      *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO               10      *NO        *NO
```

그림 10. 구성 리스트 보고서 - 예

보안 위치 필드

SECURELOC(보안 위치) 필드는 로컬 시스템이 리모트 시스템을 신뢰해서 로컬 시스템을 대신해 암호 검증을 수행하는지를 지정합니다. SECURELOC 필드는 DDM 및 CPI 통신 API를 사용하는 어플리케이션과 같이 SECURITY(SAME) 값을 사용하는 어플리케이션에만 적용됩니다.

SECURELOC(*YES)를 지정하면 로컬 시스템이 리모트 시스템의 취약한 영향을 받을 수 있습니다. 양쪽 시스템에 있는 모든 사용자는 로컬 시스템에서 프로그램을 호출할 수 있습니다. 이것은 QSECOFR(보안 담당자) 사용자 프로파일이 모든 iSeries 시스템에 있으며 *ALLOBJ 특수 권한이 있으므로 특히 위험합니다. 네트워크의 시스템이 QSECOFR 암호 보호를 제대로 수행하지 않으면, 그 시스템을 보안 위치로 사용하는 다른 시스템이 위험합니다.

SECURELOC(*VFYENCPWD)를 사용할 경우, 시스템은 암호를 제대로 보호하지 않는 다른 시스템의 영향을 덜 받습니다. SECURITY(SAME)을 사용하는 어플리케이션을 요구하는 사용자는 두 시스템에서 같은 사용자 ID 및 암호를 가져야 합니다. SECURELOC(*VFYENCPWD)는 사용자가 모든 시스템에서 같은 암호를 갖도록 네트워크에서 암호 관리 방침을 요구합니다.

주: SECURELOC(*VFYENCPWD)는 V3R2, V3R7 또는 V4R1을 실행하는 시스템 사이에서만 지원됩니다. 목표 시스템이 SECURELOC(*VFYENCPWD)를 지정하지만 소스 시스템이 이 기능을 지원하지 않을 경우, 해당 요구는 SECURITY (NONE)로 취급됩니다.

시스템이 SECURELOC(*NO)를 지정하면, SECURITY(SAME)을 사용하는 어플리케이션에 프로그램을 실행할 디폴트 사용자가 필요합니다. 디폴트 사용자는 장치 설명 및 요구와 연관된 모드에 따라 다릅니다(124 페이지의 『작업에 대한 사용자 프로파일의 목표 시스템 지정』을 참조하십시오).

위치 암호 필드

위치 암호 필드는 두 시스템이 암호를 교환하여 요구 시스템이 사이비 시스템이 아닌지 검증할지를 판별합니다. 120 페이지의 『예: 기본 APPC 세션』에서는 위치 암호에 대한 자세한 내용을 제공합니다.

APPN 가능 필드

APPN 가능(APPN) 필드는 리모트 시스템이 확장 네트워크 기능을 지원할 수 있는지 또는 단일 홉 연결로 제한되는지를 지정합니다. APPN(*YES)의 의미는 다음과 같습니다.

- 리모트 시스템이 네트워크 노드이면, 리모트 시스템은 로컬 시스템을 다른 시스템에 연결할 수 있습니다. 이것을 **중간 노드 라우팅**이라고 합니다. 시스템의 사용자가 리모트 시스템을 큰 규모의 네트워트에 대한 라우트로 사용할 수 있음을 의미합니다.
- 로컬 시스템이 네트워트 노드이면, 리모트 시스템은 로컬 시스템을 다른 시스템에 연결할 수 있습니다. 리모트 시스템의 사용자가 시스템을 큰 규모의 네트워크에 대한 라우트로 사용할 수 있습니다.

  주: DSPNETA 명령을 사용하여 시스템이 네트워크 노드인지 또는 끝 노드인지 판별할 수 있습니다.

단일 세션 필드

SNGSSN(단일 세션) 필드는 리모트 시스템이 동일한 APPC 장치 설명을 사용하여 한 번에 둘 이상의 세션을 실행할 수 있는지를 지정합니다. SNGSSN(*NO)은 리모트 시스템에 대해 여러 개의 장치 설명을 작성할 필요가 없으므로 일반적으로 사용됩니다. 예를 들면, PC 사용자는 종종 둘 이상의 5250 에뮬레이션 세션과 파일 서버 및 인쇄 서버 기능에 대한 세션이 필요합니다. SNGSSN(*NO)를 지정하면, iSeries 시스템의 PC에 대해 하나의 장치 설명으로 이 기능을 제공할 수 있습니다.

SNGSSN(*NO)은 사용자가 PC 사용자 및 다른 APPC 사용자의 보안 의식 오퍼레이팅 프로시듀어에 의존해야 한다는 것을 뜻합니다. 시스템은 리모트 시스템에서 기존 세션과 동일한 장치 설명을 사용하는 권한이 없는 세션을 시작하는 사용자의 영향을 받기가 쉽습니다(이것을 때로는 **피기백(piggy-backing)**이라고 합니다).

사전 설정 세션 필드

단일 세션 장치의 PREESTSSN(사전 설정) 세션 필드는 리모트 시스템이 처음 로컬 시스템과 접촉할 때 로컬 시스템에서 리모트 시스템으로 세션을 시작하는지를 제어합니다. PREESTSSN(*NO)은 어플리케이션이 시스템으로 세션을 요구할 때까지 로컬 시스템

에서 세션 시작을 기다린다는 의미입니다. PREESTSSN(*YES)은 어플리케이션 프로그램이 연결을 완료하기 위해 걸리는 시간을 최소화하는 데 유용합니다.

PREESTSSN(*YES)을 지정하면 시스템이 더 이상 사용되지 않는 교환(전화 접속) 회선을 단절하지 못합니다. 어플리케이션 또는 사용자가 회선을 명시적으로 단절변환해야 합니다. PREESTSSN(*YES)을 지정하면 로컬 시스템이 세션에서 피기백의 영향을 받는 시간이 길어질 수 있습니다.

SNUF 프로그램 시작 필드

SNUF 프로그램 시작 필드는 리모트 시스템이 로컬 시스템에 있는 프로그램을 시작할 수 있는지를 지정합니다. *YES는 리모트 시스템의 사용자가 로컬 시스템에서 작업을 시작하고 프로그램을 실행할 때, 로컬 시스템의 오브젝트 권한 체제가 오브젝트 보호에 적절해야 한다는 의미입니다.

APPC 제어기 매개변수

그림 11은 제어기 설명에 대한 통신 정보 보고서의 예를 보여줍니다. 보고서 다음에 보고서 필드에 관한 설명을 볼 수 있습니다.

```
                          통신 정보(전체 보고서)
                                                              SYSTEM4
오브젝트 유형  . . . . . :  *CTLD

오브젝트  오브젝트  제어기      자동      교환      호출      APPN      CP        단절      삭제  장치
이름      유형      범주        작성      제어기    방향      가능      세션      타이머    초    이름
CTL01     *CTLD     *APPC       *YES      *YES      *DIAL     *YES      *YES        0       1440  AARON
CTL02     *CTLD     *APPC       *YES      *YES      *DIAL     *YES      *YES        0       1440  BASIC
CTL03     *CTLD     *APPC       *YES      *YES      *DIAL     *YES      *YES        0       1440  *NONE
```

그림 11. APPC 제어기 설명 - 샘플 보고서

자동 작성 필드

회선 설명에서 AUTOCRTCTL(자동 작성) 필드는 수신 요구가 일치하는 제어기 설명을 찾을 수 없을 때 로컬 시스템에서 자동으로 제어기 설명을 작성하는지를 지정합니다. 제어기 설명에서 AUTOCRTDEV(자동 작성) 필드는 수신 요구가 일치하는 장치 설명을 찾을 수 없을 때 로컬 시스템에서 자동으로 장치 설명을 작성하는지를 지정합니다.

APPN 가능 제어기의 경우, 자동 작성 필드는 효력이 없습니다. 시스템은 자동 작성 필드 설정에 관계없이 필요시에 자동으로 장치 설명을 작성합니다.

회선 설명에 *YES를 지정하면, 회선에 액세스할 수 있는 모든 사용자가 시스템에 연결할 수 있습니다. 여기에는 브리지 및 라우터가 연결하는 사이트가 포함됩니다.

제어점 세션 필드

APPN 가능 제어기의 경우, CPSSN(제어점 세션) 필드는 시스템이 리모트 시스템과 자동으로 APPC 연결을 설정하는지를 제어합니다. 시스템은 CP 세션을 사용하여 리모트 시스템과 네트워크 정보 및 상태를 교환합니다. APPN 네트워크 노드 사이의 최신 정보 교환은 네트워크가 순조롭게 기능하도록 하는 데 특히 중요합니다.

*YES를 지정하면 유휴 교환 회선은 자동으로 단절되지 않습니다. 이로써 시스템이 더욱 피기백 세션의 영향을 받습니다.

단절 타이머 필드

APPC 제어기의 경우, 단절 타이머 필드는 시스템이 리모트 시스템에 대한 회선을 단절하기 전에 제어기가 사용되지 않는(활동 세션이 없음) 기간을 지정합니다. 이 필드는 두 가지 값을 갖습니다. 첫 번째 값은 처음 접촉된 시간부터 제어기가 활동 상태로 있게 될 시간을 지정합니다. 두 번째 값은 시스템이 회선을 제거하기 전에 최종 세션이 제어기에서 종료된 후 시스템이 대기하는 시간을 판별합니다.

시스템은 SWTDSC(교환 단절) 필드가 *YES일 때에만 단절 타이머를 사용합니다.

큰 값을 지정하면 시스템이 피기백 세션의 영향을 받기가 더욱 쉽습니다.

회선 설명 매개변수

그림 12에서는 회선 설명에 대한 통신 정보 보고서의 예를 보여줍니다. 보고서 다음에 보고서 필드에 관한 설명을 볼 수 있습니다.

통신 정보(전체 보고서)

```
오브젝트 유형  . . . . . :   *LIND
자동
오브젝트        오브젝트        회선          자동          삭제        자동        자동
이름              유형          범주          작성          초          응답        다이얼
LINE01          *LIND         *SDLC         *NO            0          *NO         *NO
LINE02          *LIND         *SDLC         *NO            0          *YES        *NO
LINE03          *LIND         *SDLC         *NO            0          *NO         *NO
LINE04          *LIND         *SDLC         *NO            0          *YES        *NO
```

그림 12. APPC 회선 설명 - 샘플 보고서

자동 응답 필드

AUTOANS(자동 응답) 필드는 교환 회선이 오퍼레이터의 간섭 없이 수신 호출을 승인하는지를 지정합니다.

*YES를 지정하면 시스템에 더 쉽게 액세스할 수 있으므로 보안이 덜 됩니다. *YES를 지정할 때의 보안 노출을 최소화하려면, 사용하지 않을 경우에는 회선을 단절변환해야 합니다.

자동 다이얼 필드

AUTODIAL(자동 다이얼) 필드는 교환 회선이 오퍼레이터의 간섭 없이 수신 호출을 승인하는지를 지정합니다. *YES를 지정하면, 통신 회선 및 모뎀에 대한 실제 액세스가 없는 사용자가 다른 시스템에 연결할 수 있습니다.

제 13 장 TCP/IP 통신 보안

TCP/IP(Transmission Control Protocol/Internet Protocol)는 모든 유형의 컴퓨터가 서로 통신하는 공통 방법입니다. TCP/IP 어플리케이션은 잘 알려져 있고 『정보 고속도로』를 통해 널리 사용됩니다.

이 장에서는 다음 사항에 대한 추가 정보를 제공합니다.

- TCP/IP 어플리케이션이 시스템에서 실행되지 않도록 방지
- TCP/IP 어플리케이션이 시스템에서 실행될 수 있을 때 시스템 자원 보호

iSeries Information Center --> 네트워킹 --> TCP/IP 웹 사이트는 모든 TCP/IP 어플리케이션 정보에 대한 완벽한 소스입니다. *SecureWay®: iSeries 및 인터넷*(iSeries Information Center --> 보안 --> SecureWay)은 인터넷(대형 TCP/IP 네트워크) 또는 인트라넷에 iSeries 서버를 연결할 때의 보안 고려사항을 설명합니다. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

iSeries 서버가 가능한 많은 TCP/IP 어플리케이션을 지원한다는 것을 명심하십시오. 시스템에서 하나의 TCP/IP 어플리케이션을 허용하도록 결정하면 다른 TCP/IP 어플리케이션도 작동가능하게 할 수 있습니다. 보안 관리자로서 TCP/IP 어플리케이션의 범위 및 이들 어플리케이션의 보안 관련사항을 알아야 합니다.

TCP/IP 처리 방지

TCP/IP 서버 작업은 QSYSWRK 서브시스템에서 실행합니다. TCP/IP 시작(STRTCP) 명령을 사용하여 시스템에서 TCP/IP를 시작합니다. TCP/IP 처리 또는 어플리케이션 실행을 원하지 않는 경우, STRTCP 명령을 사용하지 마십시오. 시스템에는 STRTCP 명령에 대한 공용 권한이 *EXCLUDE로 설정되어 제공됩니다.

명령에 액세스할 수 있는 사용자가 TCP/IP를 시작한다고 의심될 경우(예를 들어, 비근무 시간) STRTCP 명령에 대해 오브젝트 감사를 설정할 수 있습니다. 사용자가 명령을 실행할 때마다 시스템이 감사 저널 항목을 기록합니다.

TCP/IP 보안 구성요소

네트워크 보안을 향상시키고 유연성을 추가하기 위해 여러 가지 TCP/IP 보안 구성요소 기능을 이용할 수 있습니다. 이러한 기술 중 일부를 방화벽 제품에서도 찾을 수 있지만, OS/400에 대한 이러한 TCP/IP 보안 구성요소는 방화벽으로 사용될 목적은 아닙니다. 그러나, 별도의 방화벽 제품에 대한 필요를 제거한 일부 인스턴스에서 이러한

피처의 일부를 사용할 수 있습니다. 또한 TCP/IP 피처를 사용하여 이미 방화벽을 사용한 환경에서 추가 보안을 제공할 수 있습니다.

다음 구성요소를 이용하여 TCP/IP 보안을 향상시킬 수 있습니다.

- 패킷 규칙
- HTTP 프록시 서버
- VPN(가상 사설망)
- SSL(보안 소켓층)

패킷 규칙을 사용하여 TCP/IP 통신 보안

IP 필터링 및 네트워크 주소 변환(NAT)의 조합인 패킷 규칙은 허용되지 않은 사용자가 내부 네트워크를 사용하지 못하도록 방화벽처럼 작동합니다. IP 필터링은 사용자 네트워크로 또는 이 네트워크에서 허용하는 IP 통신을 제어할 수 있게 합니다. 기본적으로 정의하는 규칙에 따라 패킷을 필터링하여 네트워크를 보호합니다. 한편 NAT는 사용자가 등록된 IP 주소 세트 뒤에 등록되지 않은 개인 IP 주소를 숨길 수 있게 합니다. 이렇게 하여 외부 네트워크에서 내부 네트워크를 보호할 수 있습니다. 또한 NAT는 IP 주소 소멸 문제를 완화시키므로 많은 개인 주소를 등록된 작은 주소 세트로 나타낼 수 있습니다. 자세한 내용은 iSeries Information Center를 참조하십시오.

HTTP 프록시 서버

HTTP 프록시 서버는 iSeries 서버용 IBM HTTP Server와 함께 제공됩니다. HTTP 서버는 OS/400의 일부입니다. 프록시 서버는 웹 브라우저에서 HTTP 요구를 수신하고 웹 서버로 재전송합니다. 요구를 수신하는 웹 서버는 프록시 서버의 IP 주소만 인지하고 요구가 시작된 PC의 이름 및 주소는 판별할 수 없습니다. 프록시 서버는 HTTP, FTP, Gopher 및 WAIS에 대한 URL 요구를 처리할 수 있습니다.

프록시 서버는 모든 프록시 서버 사용자의 요구에서 리턴된 웹 페이지를 캐시하였습니다. 따라서, 사용자가 페이지를 요구하면 프록시 서버는 페이지가 캐시에 있는지 여부를 검사합니다. 만약 있을 경우, 프록시 서버가 캐시된 페이지를 리턴합니다. 캐시된 페이지를 사용하면 프록시 서버가 웹 페이지를 더 빨리 제공할 수 있어 시간이 소요될 수 있는 웹 서버에 대한 요구를 제거합니다.

또한, 프록시 서버는 추적 목적으로 모든 URL 요구를 기록할 수도 있습니다. 그러면 네트워크 자원의 사용과 오용을 모니터하기 위해 기록부를 검토할 수 있습니다.

IBM HTTP Server에서 HTTP 프록시 지원을 사용하여 웹 액세스를 강화할 수 있습니다. PC 클라이언트의 주소는 액세스하는 웹 서버에서 숨기므로 프록시 서버의 IP 주소만 알려집니다. 웹 페이지 캐시가 통신 대역폭(bandwidth) 요구사항 및 방화벽 작업 부하를 줄일 수도 있습니다. 자세한 정보는 iSeries용 IBM HTTP Server 홈 페이지 http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html에서 참조하십시오.

VPN(가상 사설망)

VPN(가상 사설망)은 각 회사에서 인터넷과 같은 공용 네트워크의 기존 구조에서 개인 인트라넷을 안전하게 확장할 수 있게 합니다. VPN을 사용하면 해당 회사에서 인증 및 자료 프라이버시와 같은 중요한 보안 기능을 제공하는 중 네트워크 통신을 제어할 수 있습니다.

OS/400 VPN은 iSeries Navigator 중 선택적으로 설치할 수 있는 OS/400용 그래픽 사용자 인터페이스(GUI) 구성요소입니다. 호스트 및 게이트웨이의 조합 사이에 보안 단말 경로를 작성할 수 있습니다. OS/400 VPN은 인증 메소드, 암호화 알고리즘 및 기타 예방책을 사용하여 해당 연결의 두 끝점 간 자료 송신을 안전하게 보호합니다.

VPN은 TCP/IP 계층 통신 스택 모델의 네트워크 계층에서 실행됩니다. 특히 VPN은 IPSec(IP Security Architecture) 개방형 구조를 사용합니다. IPSec는 견고하고 안전한 VPN(가상 사설망)을 작성할 수 있는 융통성 있는 빌딩 블록을 제공할 뿐만 아니라 인터넷에 기본 보안 기능을 제공합니다.

또한 VPN은 L2TP(layer 2 Tunnel Protocol) VPN 솔루션을 제공합니다. 가상 회선이라고도 하는 L2TP 연결은 공동 네트워크 서버에서 리모트 사용자에게 할당된 IP 주소를 관리할 수 있게 하여 리모트 사용자의 비용효율적인 액세스를 제공합니다. 또한 L2TP 연결을 IPSec에서 사용하지 못하게 할 때 해당 시스템 또는 네트워크에 보안 액세스를 제공합니다.

VPN이 전체 네트워크에 미치는 영향을 이해하는 것이 중요합니다. 성공하려면 적절하게 계획하고 구현해야 합니다. VPN가 작업하는 방법 및 사용자가 이 VPN을 사용할 수 있는 방법을 아는지 확인하려면 iSeries Information Center의 VPN 주제를 검토해야 합니다. 자세한 내용은 iSeries Information Center --> 보안 --> VPN(가상 사설망)을 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

SSL(보안 소켓층)

SSL이 인터넷과 같은 보호되지 않은 네트워크에서 안전한 통신 세션을 위한 어플리케이션을 작성할 수 있게 하는 산업 표준이 되었습니다. SSL 프로토콜은 클라이언트와 서버 어플리케이션 사이에 통신 세션의 하나 또는 양끝점에 대한 인증을 제공하는 보안 연결을 설정합니다. 또한 SSL은 클라이언트 및 서버 어플리케이션이 교환하는 자료의 프라이버시 및 무결성을 제공합니다. 자세한 내용은 iSeries Information Center --> 보안 --> SSL(보안 소켓층)을 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

TCP/IP 환경 보안

여기에서는 시스템의 TCP/IP 환경에서 보안 노출을 줄이기 위해 취할 수 있는 단계에 대한 일반적인 제안사항을 제공합니다. 이러한 추가 정보는 뒤에 나오는 주제에서 논의되는 특정 어플리케이션보다는 전체 TCP/IP 환경에 적용됩니다.

- TCP/IP 포트에 대한 어플리케이션을 작성할 경우, 어플리케이션이 적절하게 보안되도록 하십시오. 외부인이 해당 포트를 통해 해당 어플리케이션을 액세스할 수 있다는 것을 가정해야 합니다. 시스템을 잘 아는 외부인이 해당 어플리케이션에 대해 TELNET을 시도할 수도 있습니다.
- 시스템에서의 TCP/IP 포트 사용을 모니터하십시오. TCP/IP 포트와 연관된 사용자 어플리케이션은 사용자 ID 또는 암호 없이 시스템에 『백도어(back-door)』 항목을 제공할 수 있습니다. 시스템에서 충분한 권한을 가진 사용자가 어플리케이션을 TCP 또는 UDP 포트와 연관시킬 수 있습니다.
- 보안 관리자로서 해커가 사용하는 *IP 위장(spoofing)*이라는 기법을 알고 있어야 합니다. TCP/IP 네트워크의 모든 시스템은 IP 주소를 갖습니다. IP 위장 사용자는 기존 IP 주소 또는 신뢰할 수 있는 IP 주소로 보이도록 시스템(일반적으로 PC)을 설정합니다. 사칭자는 이렇게 관리자가 일반적으로 연결하는 시스템인 것처럼 보임으로써 시스템과의 연결을 설정합니다.

  시스템에서 TCP/IP를 실행하고 시스템이 실제적으로 보호되지 않는 네트워크에 참여하는 경우(모든 비교환 회선 및 사전정의된 링크), IP 위장을 당하기 쉽습니다. 시스템을 『사기꾼』의 손상으로부터 보호하려면, 이 장에 있는 사인 온 보호 및 오브젝트 보안과 같은 제안사항으로 시작하십시오. 또한 시스템에 적절한 보조 기억장치 한계가 설정되었는지도 확인해야 합니다. 이렇게 하면, 사기꾼이 넘치도록 많은 메일 또는 스풀 파일을 보내 시스템이 작동하지 못하도록 할 수 없습니다.

  또한, 시스템에서의 TCP/IP 활동을 정기적으로 모니터해야 합니다. IP 위장을 감지한 경우, TCP/IP 설정에서 약점을 찾아내어 조정할 수 있습니다.
- 인트라넷(외부에 직접 연결할 필요가 없는 시스템의 네트워크)에 대해 재사용할 수 있는 IP 주소를 사용하십시오. 재사용할 수 있는 주소는 사설망 내부용입니다. 인터넷 백본(backbone)은 재사용할 수 있는 IP 주소를 갖는 패킷의 라우트를 지정하지 않습니다. 따라서 재사용할 수 있는 주소는 방화벽 내부에서 추가의 보호층을 제공합니다.

  iSeries Information Center --> 네트워킹 --> TCP/IP 웹 사이트에서는 TCP/IP에 대한 보안 정보를 비롯하여, IP 주소 지정 방법 및 IP 주소 범위에 대한 자세한 정보를 제공합니다.
- 사용자 시스템을 인터넷 또는 인트라넷에 연결할 경우, *SecureWay: iSeries 및 인터넷*(iSeries Information Center --> 보안 --> SecureWay)에서 보안 정보를 검토하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

자동으로 시작하는 TCP/IP 서버 제어

보안 관리자로는 TCP/IP를 시작할 때 자동으로 시작하는 TCP/IP 어플리케이션을 제어해야 합니다. TCP/IP를 시작할 때 다음 두 가지 명령을 사용할 수 있습니다. 각 명령에 대해 시스템은 어느 어플리케이션(서버)을 시작할지를 판별할 때 서로 다른 방법을 사용합니다.

표 22는 두 가지 명령과 명령에 대한 보안 권장사항을 보여줍니다. 표 23은 서버에 대한 디폴트 자동 시작 값을 보여줍니다. 서버에 대한 자동 시작 값을 변경하려면, 서버에 대해 CHGxxxA(xxx 속성 변경) 명령을 사용하십시오. 예를 들면, TELNET에 대한 명령은 CHGTELNA입니다.

표 22. TCP/IP 명령을 시작할 서버의 판별 방법

명령	시작할 서버	보안 권장사항
STRTCP(TCP/IP 시작)	시스템은 AUTOSTART(*YES)를 지정하는 모든 서버를 시작합니다. 표 23은 각 TCP/IP 서버에 제공된 값을 보여줍니다.	• 자동 시작 설정을 변경할 수 있는 사용자를 제어하려면 *IOSYSCFG 특수 권한을 주의하여 지정하십시오. • STRTCP 명령 사용 권한이 있는 사용자를 주의하여 제어하십시오. 이 명령의 디폴트 공용 권한은 *EXCLUDE입니다. • *서버명* 속성 변경 명령(예: CHGTELNA)에 대해 오브젝트 감사를 설정하여 서버에 대한 AUTOSTART 값을 변경하려는 사용자를 모니터하십시오.
STRTCPSVR (TCP/IP 서버 시작)	시작할 서버를 지정하려면 매개변수를 사용하십시오. 이 명령이 제공하는 디폴트는 모든 서버를 시작하는 것입니다.	• CHGCMDDFT(명령 디폴트 변경) 명령을 사용하여 특정 서버만 시작하도록 STRTCPSVR 명령을 설정하십시오. 이 경우에도 사용자는 다른 서버를 시작할 수 있습니다. 그러나 명령 디폴트를 변경하면 사용자가 부주의로 모든 서버를 시작할 가능성이 적어집니다. 예를 들면, 다음 명령을 사용하여 TELNET 서버만 시작하도록 디폴트를 설정하십시오. `CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **주:** 디폴트 값을 변경하면 하나의 서버만 지정할 수 있습니다. 정기적으로 사용하는 서버를 선택하거나 보안 노출을 초래할 가능성이 가장 적은 서버(예: TFTP)를 선택하십시오. • STRTCPSVR 명령 사용 권한이 있는 사용자를 주의하여 제어하십시오. 이 명령의 디폴트 공용 권한은 *EXCLUDE입니다.

다음 테이블에는 TCP/IP 서버의 자동시작 값이 들어 있습니다. 이들 서버 각각에 대한 정보는 iSeries Information Center(**네트워킹 --> TCP/IP**)를 참조하십시오. iSeries Information Center 액세스에 대한 자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

표 23. TCP/IP 서버의 자동시작 값

서버	디폴트 값	사용자 값
TELNET	AUTOSTART(*YES)	
FTP(file transfer protocol)	AUTOSTART(*YES)	

표 23. TCP/IP 서버의 자동시작 값 (계속)

서버	디폴트 값	사용자 값
BOOTP(Bootstrap Protocol)	AUTOSTART(*NO)	
TFTP(trivial file transfer protocol)	AUTOSTART(*NO)	
REXEC(Remote EXECution 서버)	AUTOSTART(*NO)	
RouteD(RouteD(Route Daemon))	AUTOSTART(*NO)	
SMTP(simple mail transfer protocol)	AUTOSTART(*YES)	
POP(Post Office Protocol)	AUTOSTART(*NO)	
HTTP(Hypertext Transfer Protocol)[1]	AUTOSTART(*NO)	
ICS(인터넷 연결 서버)[1]	AUTOSTART(*NO)	
LPD(line printer daemon)	AUTOSTART(*YES)	
SNMP(SNMP(Simple Network Management Protocol))	AUTOSTART(*YES)	
DNS(domain name system)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP(dynamic host configuration protocol)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

주:

1. iSeries서버용 IBM HTTP 서버가 있을 경우, AUTOSTART 값을 설정하기 위해 CHGHTTPA 명령을 사용합니다.

SLIP 사용에 대한 보안 고려사항

iSeries 서버 TCP/IP 지원은 SLIP(Serial Interface Line Protocol)을 포함합니다. SLIP는 저비용 지점간 연결을 제공합니다. SLIP 사용자는 LAN 또는 WAN의 일부인 시스템과의 지점간 연결을 설정하여 LAN 또는 WAN에 연결할 수 있습니다.

SLIP는 비동기 연결시 실행됩니다. iSeries 서버와의 전화 접속 연결에 SLIP를 사용할 수 있습니다. 예를 들면, PC에서 iSeries 시스템으로 다이얼 인할 때 SLIP를 사용할 수 있습니다. 연결된 후에 PC에서 TELNET 어플리케이션을 사용하여 iSeries TELNET 서버에 연결할 수 있습니다. 또는 FTP 어플리케이션을 사용하여 두 시스템간에 파일을 전송할 수 있습니다.

시스템 제공시 SLIP는 구성되어 있지 않습니다. 따라서 시스템에서 SLIP(및 전화 접속 TCP/IP)를 실행하지 않으려면, SLIP에 대한 구성 프로파일을 구성하지 마십시오. WRKTCPPTP(TCP/IP 지점간에 대한 작업) 명령을 사용하여 SLIP 구성을 작성하십시오. WRKTCPPTP 명령을 사용하려면 *IOSYSCFG 특수 권한이 있어야 합니다.

시스템에서 SLIP를 실행하려면 하나 이상의 SLIP(지점간) 구성 프로파일을 작성하십시오. 다음 조작 모드로 구성 프로파일을 작성할 수 있습니다.

- 다이얼 인(*ANS)

• 다이얼 아웃(*DIAL)

다음 주제는 SLIP 구성 프로파일의 보안 설정 방법을 다루고 있습니다.

주: **사용자 프로파일**은 사인 온을 허용하는 iSeries 서버 오브젝트입니다. 모든 iSeries 서버 작업에는 실행할 사용자 프로파일이 있어야 합니다. **구성 프로파일**은 iSeries 시스템과의 SLIP 연결 설정에 사용되는 정보를 저장합니다. iSeries 서버에 대한 SLIP 연결을 시작할 때 간단히 링크를 설정하게 됩니다. 아직 iSeries 서버 작업을 사인 온 또는 시작하지 않았습니다. 따라서 iSeries 서버에 대한 SLIP 연결을 시작할 때 사용자 프로파일이 꼭 필요한 것은 아닙니다. 그러나 앞으로의 논의에서 보듯이 연결할 것인지를 판별할 때 SLIP 구성 프로파일에 사용자 프로파일이 필요할 수 있습니다.

다이얼 인 SLIP 연결 제어

다른 사용자가 SLIP를 사용하여 시스템에 다이얼 인 연결을 설정하기 전에 SLIP *ANS 구성 프로파일을 시작해야 합니다. SLIP 구성 프로파일을 작성 또는 변경하려면, WRKTCPPTP(TCP/IP 지점간에 대한 작업) 명령을 사용하십시오. 구성 프로파일을 시작하려면 STRTCPPTP(TCP/IP 지점간 시작) 명령을 사용하거나 WRKTCPPTP 화면에서 옵션을 사용하십시오. 시스템이 제공될 때 STRTCPPTP 및 ENDTCPPTP 명령의 공용 권한은 *EXCLUDE입니다. *IOSYSCFG 특수 권한이 있을 때에만 SLIP 구성 프로파일 추가, 변경 및 삭제 옵션을 사용할 수 있습니다. 보안 관리자로서 명령 권한과 특수 권한을 모두 사용하여 다이얼 인 연결을 허용하도록 시스템을 설정할 수 있는 사용자를 판별할 수 있습니다.

다이얼 인 SLIP 연결 보안

시스템에 다이얼 인하는 시스템의 유효성을 검사하려면 요구 시스템에서 사용자 ID와 암호를 송신하도록 해야 합니다. 이때 시스템에서 사용자 ID와 암호를 검증할 수 있습니다. 사용자 ID와 암호가 유효하지 않으면, 시스템은 세션 요구를 거부할 수 있습니다.

다이얼 인 유효성 검사를 설정하려면 다음을 수행하십시오.

__ 단계 1. 요구 시스템이 연결 설정에 사용할 수 있는 사용자 프로파일을 작성하십시오. 리퀘스터가 송신하는 사용자 ID와 암호가 이 사용자 프로파일명 또는 암호와 일치해야 합니다.

주: 시스템에서 암호 유효성 검사를 수행하려면 QSECURITY 시스템 값을 20 이상으로 설정해야 합니다.

추가 보호로서 구체적으로 SLIP 연결 설정을 위한 사용자 프로파일을 작성할 수도 있습니다. 사용자 프로파일은 시스템에서 제한된 권한을 가져야 합니다. SLIP 연결 설정을 제외한 기능에 대해서 사용자 프로파일을 사용하지 않으려면, 사용자 프로파일에 다음 값을 설정할 수 있습니다.

- *SIGNOFF의 초기 메뉴(INLMNU)
- *NONE의 초기 프로그램(INLPGM)
- *YES의 능력 제한(LMTCPB)

이러한 값은 사용자 프로파일과 대화식으로 사인 온할 수 없도록 합니다.

__ 단계 2. 리퀘스터가 SLIP 연결 설정을 시도할 때 시스템이 검사할 권한 부여 리스트를 작성하십시오.

주: SLIP 프로파일을 작성 또는 변경할 때 이 권한 부여 리스트를 *시스템 액세스 권한 부여 리스트* 필드에 지정하십시오(단계 4 참조).

__ 단계 3. ADDAUTLE(권한 부여 항목 추가) 명령을 사용하여 단계 1에서 작성한 사용자 프로파일을 권한 부여 리스트에 추가하십시오. 각 지점간 구성 프로파일에 대해 고유한 권한 부여 리스트를 작성하거나 몇 개의 구성 프로파일이 공유하는 권한 부여 리스트를 작성할 수 있습니다.

__ 단계 4. WRKTCPPTP 명령을 사용하여 다음과 같은 특성을 갖는 TCP/IP 지점간 *ANS 프로파일을 설정하십시오.

- 구성 프로파일은 사용자 유효성 검사 기능을 포함하는 연결 대화 스크립트를 사용해야 합니다. 사용자 유효성 검사에는 리퀘스터로부터 사용자 ID와 암호를 수신하여 유효성을 검사하는 일이 포함됩니다. 시스템에는 이러한 기능을 제공하는 몇 가지 샘플 대화 스크립트가 제공됩니다.
- 구성 프로파일은 단계 2에서 작성한 권한 부여 리스트명을 지정해야 합니다. 연결 대화 스크립트가 수신하는 사용자 ID는 권한 부여 리스트에 있어야 합니다.

다이얼 인 보안 설정값은 다이얼 인하는 시스템의 보안 관행 및 기능의 영향을 받는다는 점에 유의하십시오. 사용자 ID와 암호를 요구할 경우, 요구 시스템의 연결 대화 스크립트에서 사용자 ID와 암호를 송신해야 합니다. iSeries 서버와 같은 일부 시스템은 사용자 ID와 암호 저장을 위한 보안 방법을 제공합니다. (141 페이지의 『보안 및 다이얼 아웃 세션』에서 방법을 설명합니다.) 다른 시스템은 시스템에서 스크립트를 찾을 수 있는 장소를 알고 있는 모든 사용자가 액세스할 수 있는 스크립트에 사용자 ID와 암호를 저장합니다.

통신 상대방의 다른 보안 관행 및 기능으로 인해 요구 환경에 대한 다른 구성 프로파일을 작성하려 할 수 있습니다. STRTCPPTP 명령을 사용하여 특정 구성 프로파일에 대한 세션을 승인하도록 시스템을 설정하십시오. 예를 들면, 하루 중 특정 시간에만 일부 구성 프로파일에 대한 세션을 시작할 수 있습니다. 보안 감사를 사용하여 연관된 사용자 프로파일에 대한 활동을 기록할 수 있습니다.

다이얼 인 사용자의 다른 시스템 액세스 금지

시스템 및 네트워크 구성에 따라 SLIP 연결을 시작하는 사용자가 시스템에 사인 온하지 않고서 네트워크에 있는 다른 시스템에 액세스할 수 있습니다. 예를 들면, 사용자는 시스템에 SLIP 연결을 설정한 후 네트워크에서 다이얼 인을 허용하지 않는 다른 시스템에 FTP 연결을 설정할 수 있습니다.

구성 프로파일의 *IP 데이터그램 전송 허용* 필드에 N(아니오)을 지정하여 SLIP 사용자가 네트워크에 있는 다른 시스템에 액세스하지 못하도록 할 수 있습니다. 이렇게 하면, 사용자가 시스템에 로그온하기 전에는 네트워크에 액세스하지 못하게 할 수 있습니다. 그러나 사용자가 시스템에 로그온한 후에는 데이터그램 전송값은 효력이 없어집니다. 이로 인해 사용자가 iSeries 시스템에서 TCP/IP 어플리케이션(예: FTP 또는 TELNET)을 사용하는 능력과 네트워크에 있는 다른 시스템과의 연결을 설정하는 능력이 제한되지는 않습니다.

다이얼 아웃 세션 제어

시스템에서 다른 사용자가 SLIP를 사용하여 다이얼 아웃 연결을 설정하기 전에 먼저 SLIP *DIAL 구성 프로파일을 시작해야 합니다. SLIP 구성 프로파일을 작성 또는 변경하려면 WRKTCPPTP 명령을 사용하십시오. 구성 프로파일을 시작하려면 STRTCPPTP(TCP/IP 지점간 시작) 명령을 사용하거나 WRKTCPPTP 화면에서 옵션을 사용하십시오. 시스템이 제공될 때 STRTCPPTP 및 ENDTCPPTP 명령의 공용 권한은 *EXCLUDE입니다. *IOSYSCFG 특수 권한이 있을 때에만 SLIP 구성 프로파일 추가, 변경 및 삭제 옵션을 사용할 수 있습니다. 보안 관리자로서 명령 권한과 특수 권한을 모두 사용하여 다이얼 아웃 연결을 허용하도록 시스템을 설정할 수 있는 사용자를 판별할 수 있습니다.

보안 및 다이얼 아웃 세션

iSeries 시스템의 사용자가 사용자 유효성 검사가 필요한 다이얼 아웃 연결을 설정하려 할 수 있습니다. iSeries 서버의 연결 대화 스크립트에서 리모트 시스템에 사용자 ID와 암호를 송신해야 합니다. iSeries 서버는 그 암호를 저장하기 위한 보안 방법을 제공합니다. 암호를 연결 대화 스크립트에 저장할 필요는 없습니다.

주:

1. 시스템이 연결 암호를 암호화된 양식으로 저장하기는 하지만, 시스템은 암호를 해독한 후 송신합니다. FTP 및 TELNET 암호와 마찬가지로 SLIP 암호는 암호화되지 않은 채(『현상태대로』) 송신됩니다. 그러나 FTP 및 TELNET과는 달리 SLIP 암호는 시스템이 TCP/IP 모드를 설정하기 전에 송신됩니다.

   SLIP는 지점간 연결을 비동기식 모드로 사용하므로, 암호화되지 않은 암호를 송신할 때의 보안 노출은 FTP 및 TELNET 암호의 노출과는 다릅니다. 암호화되지 않은 FTP 및 TELNET 암호는 네트워크에서 IP 통신량으로 송신될 수 있으므로, 전자 탐지될 가능성이 큽니다. SLIP 암호 전송은 두 시스템간의 전화 연결만큼 보안됩니다.

2. SLIP 연결 대화 스크립트 저장을 위한 디폴트 파일은 QUSRSYS/QATOCPPSCR 입니다. 이 파일의 공용 권한은 *USE이므로 공용 사용자가 디폴트 연결 대화 스크립트를 변경할 수 없습니다.

유효성 검사가 필요한 리모트 세션에 대한 연결 프로파일을 작성할 경우, 다음을 수행하십시오.

__ 단계 1. QRETSVRSEC(서버 보안 자료 보유) 시스템 값을 1(예)로 하십시오. 이 시스템 값은 해독할 수 있는 암호를 시스템의 보호된 영역에 저장하도록 할 것인지 판별합니다.

__ 단계 2. WRKTCPPTP 명령을 사용하여 다음과 같은 특성을 갖는 구성 프로파일을 작성하십시오.

- 구성 프로파일 모드에 대해 *DIAL을 지정하십시오.
- *리모트 서비스 액세스명*에서 리모트 시스템에 필요한 사용자 ID를 지정하십시오. 예를 들면, 다른 iSeries 서버에 연결하려는 경우, 그 iSeries 서버에 사용자 프로파일명을 지정하십시오.
- *리모트 서비스 액세스 암호*에서 이 사용자 ID에 대해 리모트 시스템에서 요구하는 암호를 지정하십시오. iSeries 서버에서 암호는 해독할 수 있는 양식으로 보호 영역에 저장됩니다. 구성 프로파일에 할당하는 이름과 암호는 QTCP 사용자 프로파일과 연관됩니다. 사용자 명령 또는 인터페이스로 이 이름과 암호에 액세스할 수 없습니다. 등록된 시스템 프로그램만 이 암호 정보에 액세스할 수 있습니다.

  주: 연결 프로파일의 암호는 TCP/IP 구성 파일 저장시 저장되지 않는다는 점에 유의하십시오. SLIP 암호를 저장하려면 SAVSECDTA(보안 자료 저장) 명령을 사용하여 QTCP 사용자 프로파일을 저장해야 합니다.
- 연결 대화 스크립트에 대해 사용자 ID와 암호를 송신하는 스크립트를 지정하십시오. 시스템에는 이러한 기능을 제공하는 몇 가지 샘플 대화 스크립트가 제공됩니다. 시스템이 스크립트를 실행할 때, 시스템은 암호를 검색해서 해독한 후 이를 리모트 시스템에 송신합니다.

지점 간 프로토콜에 대한 보안 고려사항

PPP(지점 간 프로토콜)를 TCP/IP의 일부로 사용할 수 있습니다. PPP는 SLIP와 함께 사용할 수 있는 사항에 대해 추가의 기능을 제공하는 지점간 연결에 대한 산업 표준입니다.

PPP를 사용하여 iSeries 서버는 인터넷 서비스 제공자나 인트라넷 또는 엑스트라넷의 다른 시스템에 고속으로 연결할 수 있습니다. 리모트 LAN은 실제로 iSeries 서버에 다이얼 인 연결을 할 수 있습니다.

PPP도 SLIP와 같이 iSeries 서버에 대한 네트워크 연결을 제공한다는 점을 기억하십시오. PPP 연결은 본질적으로 리퀘스터를 시스템 문앞까지 오도록 합니다. 여전히 리퀘스터는 사용자 ID와 암호가 있어야 시스템에 들어가 TELNET 또는 FTP와 같이 TCP/IP 서버에 연결할 수 있습니다. 다음은 이러한 새 연결 기능에서의 보안 고려사항입니다.

주: Windows용 IBM iSeries Access 워크스테이션에서 iSeries Navigator를 사용하여 PPP를 구성합니다.

- PPP는 전용 연결을 할 수 있는 기능을 제공합니다(여기서 동일한 사용자 항상 동일한 IP 주소를 갖습니다). 전용 주소가 있는 경우, IP 위장 가능성이 있습니다(알려져 있는 IP 주소가 있는 신뢰할 수 있는 시스템처럼 꾸미는 사칭 시스템). 그러나 PPP가 제공하는 향상된 인증 기능으로 IP 위장으로부터 보호할 수 있습니다.
- PPP를 사용하여 SLIP를 사용할 때와 같이 사용자명과 연관 암호를 가지는 연결 프로파일을 작성하십시오. 그러나 SLIP와는 달리 사용자가 유효한 사용자 프로파일 및 암호가 없어도 됩니다. 사용자명 및 암호는 사용자 프로파일과 연결되어 있지 않습니다. 대신, PPP 권한 부여시 유효성 검사가 사용됩니다. 또한, PPP에는 연결 스크립트가 필요없습니다. 인증(사용자명 및 암호 교환)은 PPP 구조의 일부이며, SLIP의 보다 낮은 레벨에서 발생합니다.
- PPP를 사용할 경우, CHAP를 사용할 수 있는 옵션이 있습니다. CHAP에서 사용자명과 암호를 암호화하므로 암호 도청(sniffing)에 대해 더 이상 걱정하지 않아도 됩니다.

  PPP 연결은 양측 모두에 CHAP 지원이 있을 때에만 CHAP를 사용합니다. 두 모뎀 사이의 통신 설정을 위해서 신호를 교환하는 중에 두 시스템이 절충합니다. 예를 들면, SYSTEMA에서는 CHAP를 지원하고 SYSTEMB에서는 지원하지 않을 경우, SYSTEMA는 세션을 거부하거나 암호화되지 않은 사용자명과 암호를 사용하기로 동의할 수 있습니다. 암호화되지 않은 사용자명과 암호를 사용하기로 동의하는 것을 절충(negotiating down)이라고 합니다. 절충 결정은 구성 옵션입니다. 예를 들면, 모든 시스템이 CHAP 기능이 있는 인트라넷에서는 절충하지 않도록 연결 프로파일을 구성해야 합니다. 시스템이 다이얼 아웃하는 공용 연결시에는 절충해도 좋습니다.

  PPP에 대한 연결 프로파일은 유효한 IP 주소 지정 기능을 제공합니다. 예를 들면, 특정 사용자에 대해 특정 주소 또는 주소 범위가 필요하다고 표시할 수 있습니다. 이 기능은 암호화된 암호에 대한 기능과 함께 위장(spoofing)에 대해 추가의 보호를 제공합니다.

  활동 세션중의 위장 또는 피기백(piggy-backing)에 대한 추가 보호로서 PPP를 구성하여 지정된 간격으로 다시 시도할 수 있습니다. 예를 들면, PPP 세션이 활동 중인 동안 iSeries 서버가 다른 시스템에게 사용자 및 암호를 물을 수 있습니다. 같은 연결 프로파일인지를 확인하기 위해 매 15분마다 이를 수행합니다(일반 사용자는 이러한 재시도 활동을 알 수 없습니다. 시스템이 일반 사용자가 볼 수 있는 레벨 미만에서 이름과 암호를 교환합니다).

PPP를 사용할 경우, 리모트 LAN이 iSeries 서버와 확장 네트워크에 대해 다이얼인 연결을 설정하는 일이 현실성을 갖습니다. 이 환경에서는 IP 전송을 켜는 것이 하나의 요구사항이 될 수 있습니다. IP 전송은 침입자가 네트워크를 마음대로 둘러볼 수 있는 가능성을 제공합니다. 그러나 PPP에는 더 강력한 보호(예를 들어, 암호 및 IP 주소 암호화의 유효성 검사)가 있습니다. 이로 인해 무엇보다도 침입자가 네트워크 연결을 설정할 수 있는 가능성이 줄어듭니다.

PPP에 대한 자세한 내용은 iSeries Information Center를 참조하십시오.

Bootstrap Protocol 서버 사용에 대한 보안 고려사항

BOOTP(Bootstrap Protocol)는 워크스테이션을 서버와 연관시키고, 워크스테이션 IP 주소 및 초기 프로그램 로드(IPL) 소스를 지정하기 위한 동적 방법을 제공합니다.

BOOTP는 무매체 워크스테이션(클라이언트)에서 네트워크에 있는 서버의 초기 코드가 들어 있는 파일을 요구하기 위해 사용되는 TCP/IP 프로토콜입니다. BOOTP 서버는 잘 알려진 BOOTP 서버 포트 67에서 청취합니다. 클라이언트 요구가 수신되면, 서버는 해당 클라이언트에 대해 정의된 IP 주소를 찾아 클라이언트에게 클라이언트의 IP 주소 및 로드 파일명을 갖는 응답을 리턴합니다. 그런 다음, 클라이언트는 로드 파일에 대한 서버에 대해 TFTP 요구를 시작합니다. 클라이언트는 하드웨어 주소와 IP 주소 사이의 맵핑은 iSeries 서버의 BOOTP 표에 보유됩니다.

BOOTP 액세스 방지

사용자 네트워크에 접속된 thin 클라이언트가 없을 경우, 시스템에서 BOOTP 서버를 실행할 필요가 없습니다. 다른 장치에 사용할 수 있지만 이들 장치의 경우, DHCP를 사용하는 것이 좋습니다. BOOTP 서버가 실행되지 않게 하려면, 다음을 수행하십시오.

__ 단계 1. TCP/IP를 시작할 때 BOOTP 서버 작업이 자동으로 시작되지 않게 하려면, 다음을 입력하십시오.

```
CHGBPA AUTOSTART(*NO)
```

주:

a. AUTOSTART(*NO)가 디폴트 값입니다.

b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

__ 단계 2. 소켓 어플리케이션과 같은 사용자 어플리케이션을 시스템에서 BOOTP에 대해 일반적으로 사용하는 포트와 연결하지 못하게 하려면, 다음을 수행하십시오.

주: DHCP 및 BOOTP가 동일한 포트 번호를 사용하므로, DHCP가 사용하는 포트도 금지됩니다. DHCP를 사용하려면 포트를 제한하지 마십시오.

__ 단계 a. GO CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

__ 단계 b. 옵션 4(TCP/IP 포트 제한에 대한 작업)를 선택하십시오.

__ 단계 c. TCP/IP 포트 제한에 대한 작업 화면에서 옵션 1(추가)을 지정하십시오.

__ 단계 d. 하위 포트 범위에 67을 지정하십시오.

__ 단계 e. 상위 포트 범위에 *ONLY를 지정하십시오.

주:

1) 포트 제한은 다음에 TCP/IP를 시작할 때 효력을 발생합니다. 포트 제한을 설정할 때 TCP/IP가 활동중인 경우, TCP/IP를 종료하고 다시 시작해야 합니다.

2) RFC1700은 공통 포트 번호 할당에 대한 정보를 제공합니다.

__ 단계 f. 프로토콜에 *UDP를 지정하십시오.

__ 단계 g. 사용자 프로파일 필드의 경우, 시스템에서 보호되는 사용자 프로파일명을 지정하십시오(보호되는 사용자 프로파일은 권한을 허용하는 프로그램이 아니며 다른 사용자가 알고 있는 암호를 갖지 않는 사용자 프로파일입니다). 포트를 특정 사용자에게 제한하면 다른 모든 사용자는 자동으로 제외됩니다.

BOOTP 서버 보안

BOOTP 서버는 iSeries 시스템에 대한 직접적인 액세스를 제공하지 않으므로 제한된 보안 노출을 표시합니다. 보안 관리자로서의 1차적인 관심은 올바른 정보가 올바른 thin 클라이언트와 연관되도록 하는 것입니다. 다시 말하면 나쁜 의도를 가진 사용자가 BOOTP 표를 변경하여 thin 클라이언트가 잘못 작동하거나 작동하지 못하게 할 수 있습니다.

BOOTP 서버와 BOOTP 표를 관리하려면 *IOSYSCFG 특수 권한이 있어야 합니다. 시스템에서 *IOSYSCFG 특수 권한이 있는 사용자 프로파일을 주의하며 제어해야 합니다.

DHCP 서버 사용에 대한 보안 고려사항

DHCP(Dynamic host configuration protocol)는 구성 정보를 TCP/IP 네트워크의 호스트로 전달하기 위한 구조를 제공합니다. 클라이언트 워크스테이션에 대해 DHCP는 자동 구성과 유사한 기능을 제공할 수 있습니다. 클라이언트 워크스테이션의 DHCP 가능 프로그램은 구성 정보에 관한 요구를 브로드캐스트합니다. DHCP 서버가 iSeries 서버에서 실행 중인 경우, 서버는 TCP/IP를 올바로 구성하기 위해 클라이언트 워크스테이션에 필요한 정보를 송신하여 요구에 응답합니다.

DHCP를 사용하면 사용자가 iSeries 서버에 처음으로 연결할 때 더욱 간편하게 할 수 있습니다. 사용자가 TCP/IP 구성 정보를 입력할 필요가 없기 때문입니다. 또한 DHCP를 사용하여 서브네트워크에서 필요한 내부 TCP/IP 주소의 수를 줄일 수 있습니다. DHCP 서버는 IP 주소 풀에서부터 IP 주소를 활동 사용자에게 임시로 할당할 수 있습니다.

thin 클라이언트의 경우, BOOTP 대신 DHCP를 사용할 수 있습니다. DHCP는 BOOTP보다 많은 기능을 제공하며, thin 클라이언트와 PC의 동적 구성을 지원합니다.

DHCP 액세스 방지

시스템의 DHCP 서버를 아무도 사용할 수 *없게* 하려면 다음을 수행하십시오.

1. TCP/IP를 시작할 때 DHCP 서버 작업이 자동으로 시작되지 않게 하려면 다음을 입력하십시오.

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   주:

   a. AUTOSTART(*NO)가 디폴트 값입니다.

   b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

2. 사용자가 소켓 어플리케이션과 같은 사용자 어플리케이션을 시스템이 DHCP에 대해 일반적으로 사용하는 포트와 연결하지 못하게 하려면, 다음을 수행하십시오.

   a. GO CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

   b. 옵션 4(TCP/IP 포트 제한에 대한 작업)를 선택하십시오.

   c. TCP/IP 포트 제한에 대한 작업 화면에서 옵션 1(추가)을 지정하십시오.

   d. 하위 포트 범위에 67을 지정하십시오.

   e. 상위 포트 범위에 68을 지정하십시오.

      주:

      1) 포트 제한은 다음에 TCP/IP를 시작할 때 효력을 발생합니다. 포트 제한을 설정할 때 TCP/IP가 활동중인 경우, TCP/IP를 종료하고 다시 시작해야 합니다.

      2) RFC1700은 공통 포트 번호 할당에 대한 정보를 제공합니다.

   f. 프로토콜에 *UDP를 지정하십시오.

   g. 사용자 프로파일 필드의 경우, 시스템에서 보호되는 사용자 프로파일명을 지정하십시오(보호되는 사용자 프로파일은 권한을 허용하는 프로그램이 아니며 다른 사용자가 알고 있는 암호를 갖지 않는 사용자 프로파일입니다). 포트를 특정 사용자에게 제한하면 다른 모든 사용자는 자동으로 제외됩니다.

DHCP 서버 보안

다음은 iSeries 시스템에서 DHCP를 실행할 때의 보안 고려사항입니다.

- DHCP 관리 권한이 있는 사용자 수를 제한하십시오. DHCP를 관리하려면 다음과 같은 권한이 필요합니다.
  - *IOSYSCFG 특수 권한
  - 아래 파일에 대한 *RW 권한

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- LAN에 실제 액세스할 수 있는 정도를 평가하십시오. 외부인이 랩탑으로 해당 위치에 쉽게 들어가서 이를 LAN에 실제적으로 연결할 수 있습니까? 이것이 노출에 해당하는 경우, DHCP는 DHCP 서버가 구성할 클라이언트(하드웨어 주소) 리스트 작성 기능을 제공합니다. 이 피처를 사용할 경우, DHCP에서 네트워크 관리자에게 제공하는 일부 생산성 혜택이 제거됩니다. 그러나 시스템에 통보되지 않은 워크스테이션을 구성하지 못하게 됩니다.
- 가능하다면 재사용할 수 있는(인터넷용 구조가 아닌) IP 주소 풀을 사용하십시오. 이렇게 하면 네트워크 외부의 워크스테이션이 서버로부터 사용가능한 구성 정보를 얻을 수 없습니다.
- 추가의 보안 보호가 필요하면 DHCP 종료점을 사용하십시오. 다음은 종료점 및 그 기능에 대한 개요입니다. *iSeries 시스템 API 참조서*는 이들 종료점의 사용법을 설명합니다.

  포트 항목

  시스템은 포트 67(DHCP 포트)에서 자료 패킷을 읽을 때마다 나감 프로그램을 호출합니다. 나감 프로그램은 전체 자료 패킷을 수신합니다. 나감 프로그램은 시스템이 해당 패킷을 처리해야 하는지 또는 삭제해야 하는지를 결정합니다. 기존의 DHCP 스크린 피처가 필요사항에 충분하지 않은 경우, 이 종료점을 사용할 수 있습니다.

  주소 할당

  시스템은 DHCP에서 공식적으로 클라이언트에 주소를 할당할 때마다 나감 프로그램을 호출합니다.

  주소 해제

  시스템은 DHCP에서 공식적으로 주소를 해제한 뒤 해당 주소를 다시 주소 풀에 놓을 때마다 나감 프로그램을 호출합니다.

TFTP 서버 사용에 대한 보안 고려사항

TFTP(Trivial file transfer protocol)는 사용자 인증 없이 기본적인 파일 전송을 제공합니다. TFTP는 Bootstrap Protocol(BOOTP) 또는 DHCP(DHCP)와 함께 작용합니다.

클라이언트는 초기에 BOOTP 서버 또는 DHCP 서버에 연결합니다. BOOTP 또는 DHCP 서버는 클라이언트의 IP 주소와 로드 파일명으로 응답합니다. 그런 다음, 클라이언트는 로드 파일에 대한 서버에 대해 TFTP 요구를 시작합니다. 클라이언트가 로드 파일의 다운로드를 완료하면 TFTP 세션을 종료합니다.

TFTP 액세스 방지

사용자 네트워크에 접속된 thin 클라이언트가 없을 경우, 시스템에서 TFTP 서버를 실행할 필요가 없을 것입니다. TFTP 서버가 실행되지 않게 하려면 다음을 수행하십시오.

__ 단계 1. TCP/IP를 시작할 때 TFTP 서버 작업이 자동으로 시작되지 않게 하려면 다음을 입력하십시오.

```
CHGTFTPA AUTOSTART(*NO)
```

주:

a. AUTOSTART(*NO)가 디폴트 값입니다.

b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

__ 단계 2. 사용자가 소켓 어플리케이션과 같은 사용자 어플리케이션을 시스템이 TFTP에 대해 일반적으로 사용하는 포트와 연결하지 못하게 하려면, 다음을 수행하십시오.

__ 단계 a. GO CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

__ 단계 b. 옵션 4(TCP/IP 포트 제한에 대한 작업)를 선택하십시오.

__ 단계 c. TCP/IP 포트 제한에 대한 작업 화면에서 옵션 1(추가)을 지정하십시오.

__ 단계 d. 하위 포트 범위에 69를 지정하십시오.

__ 단계 e. 상위 포트 범위에 *ONLY를 지정하십시오.

주:

1) 포트 제한은 다음에 TCP/IP를 시작할 때 효력을 발생합니다. 포트 제한을 설정할 때 TCP/IP가 활동중인 경우, TCP/IP를 종료하고 다시 시작해야 합니다.

2) RFC1700은 공통 포트 번호 할당에 대한 정보를 제공합니다.

__ 단계 f. 프로토콜에 *UDP를 지정하십시오.

__ 단계 g. 사용자 프로파일 필드의 경우, 시스템에서 보호되는 사용자 프로파일명을 지정하십시오(보호되는 사용자 프로파일은 권한을 허용하는 프로그램이 아니며 다른 사용자가 알고 있는 암호를 갖지 않는 사용자 프로파일입니다). 포트를 특정 사용자에게 제한하면 다른 모든 사용자는 자동으로 제외됩니다.

TFTP 서버 보안

TFTP 서버는 iSeries 시스템에 대한 매우 제한된 액세스를 디폴트로 제공합니다. 이것은 구체적으로 thin 클라이언트에 대한 초기 코드를 제공하도록 구성되었습니다. 보안 관리자는 다음과 같은 TFTP 서버의 특성을 알고 있어야 합니다.

- TFTP 서버에는 인증(사용자 ID 및 암호)이 필요하지 않습니다. 모든 TFTP 작업은 QTFTP 사용자 프로파일하에서 실행됩니다. QTFTP 사용자 프로파일에는 암호가 없습니다. 따라서 대화식 사인 온에 사용할 수 없습니다. QTFTP 사용자 프로파일에는 어떠한 특수 권한도 없으며, 명시적으로 부여된 시스템 자원에 대한 권한도 없습니다. 이 사용자 프로파일은 thin 클라이언트에 필요한 자원에 액세스하기 위해 공용 권한을 사용합니다.
- TFTP 서버가 도착하면, thin 클라이언트 정보가 들어 있는 디렉토리를 액세스하도록 구성됩니다. *PUBLIC 또는 QTFTP에 해당 디렉토리에 쓰거나 읽을 권한이 있어야 합니다. 디렉토리에 기록하려면 CHGTFTPA 명령의 ″파일 쓰기 허용″ 매개변수에 *CREATE를 지정해야 합니다. 기존 파일에 기록하려면 CHGTFTPA의 ″파일 쓰기 허용″ 매개변수에 *REPLACE를 지정해야 합니다. *CREATE를 사용하여 기존 파일을 대체하거나 신규 파일을 작성할 수 있습니다. *REPLACE는 기존 파일을 대체하기 위해서만 사용할 수 있습니다.

  TFTP 클라이언트는 CHGTFTPA(TFTP 속성 변경) 명령으로 디렉토리를 명시적으로 정의하지 않을 경우, 다른 디렉토리를 액세스할 수 없습니다. 그러므로, 로컬 또는 리모트 사용자가 시스템에 TFTP 세션을 시작하려 할 경우, 사용자가 정보를 액세스하거나 손상을 초래할 수 있는 가능성이 극히 제한됩니다.
- TFTP 서버를 구성하여 thin 클라이언트 처리 이외의 다른 서비스를 제공하려는 경우, 나감 프로그램을 정의하여 모든 TFTP 요구를 평가하여 권한을 부여할 수 있습니다. TFTP 서버는 FTP 서버에 사용할 수 있는 나감과 유사한 요구 유효성 검사 나감을 제공합니다. 자세한 정보는 iSeries Information Center --> 네트워킹 --> TCP/IP --> TFTP를 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

REXEC 서버 사용에 대한 보안 고려사항

REXEC(Remote EXECution 서버)는 REXEC 클라이언트로부터 명령을 수신하여 실행합니다. REXEC 클라이언트는 일반적으로 REXEC 명령 송신을 지원하는 PC 또는 UNIX 어플리케이션입니다. 이 서버가 제공하는 지원은 FTP 서버에 대해 RCMD(리모트 명령) 부속명령을 사용할 때 사용할 수 있는 기능과 유사합니다.

REXEC 액세스 방지

iSeries 서버에서 REXEC 클라이언트의 명령을 승인하지 않게 하려면, 다음을 수행하여 REXEC 서버가 실행되지 않도록 하십시오.

__ 단계 1. TCP/IP를 시작할 때 REXEC 서버 작업이 자동으로 시작되지 않게 하려면, 다음을 입력하십시오.

```
CHGRXCA AUTOSTART(*NO)
```

주:

a. AUTOSTART(*NO)가 디폴트 값입니다.

b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

__ 단계 2. 일반적으로 시스템이 REXEC에 사용하는 포트에 소켓 어플리케이션과 같은 사용자 어플리케이션을 다른 사람이 연결시키지 못하도록 하려면, 다음을 수행하십시오.

__ 단계 a. GO CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

__ 단계 b. 옵션 4(TCP/IP 포트 제한에 대한 작업)를 선택하십시오.

__ 단계 c. TCP/IP 포트 제한에 대한 작업 화면에서 옵션 1(추가)을 지정하십시오.

__ 단계 d. 하위 포트 범위에 512를 지정하십시오.

__ 단계 e. 상위 포트 범위에 *ONLY를 지정하십시오.

__ 단계 f. 프로토콜에 *TCP를 지정하십시오.

__ 단계 g. 사용자 프로파일 필드의 경우, 시스템에서 보호되는 사용자 프로파일명을 지정하십시오(보호되는 사용자 프로파일은 권한을 허용하는 프로그램이 아니며 다른 사용자가 알고 있는 암호를 갖지 않는 사용자 프로파일입니다). 포트를 특정 사용자에게 제한하면 다른 모든 사용자는 자동으로 제외됩니다.

주:

a. 포트 제한은 다음에 TCP/IP를 시작할 때 효력을 발생합니다. 포트 제한을 설정할 때 TCP/IP가 활동중인 경우, TCP/IP를 종료하고 다시 시작해야 합니다.

b. RFC1700은 공통 포트 번호 할당에 대한 정보를 제공합니다.

REXEC 서버 보안

시스템에서 Remote EXECution 서버를 실행할 때의 고려사항은 다음과 같습니다.

- REXCD 요구에는 사용자 ID, 암호 및 실행할 명령이 포함됩니다. 다음과 같은 일반적인 iSeries 서버 인증 및 권한 검사가 적용됩니다.
  - 사용자 프로파일 및 암호 조합이 유효해야 합니다.
  - 시스템이 사용자 프로파일에 대해 *기능 제한*(LMTCPB) 값을 시행합니다.
  - 사용자는 명령 및 그 명령이 사용하는 모든 자원에 대한 권한이 있어야 합니다.

- REXEC 서버는 FTP 서버에 사용할 수 있는 종료점과 유사한 종료점을 제공합니다. 유효성 검사 종료점을 사용하여 명령을 평가하고 명령 허용 여부를 결정할 수 있습니다. 자세한 정보는 iSeries Information Center --> 네트워킹 --> TCP/IP --> REXEC를 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.
- REXEC 서버를 실행하려는 경우, 시스템에 있는 메뉴 액세스 제어 외부에서 실행하게 됩니다. 오브젝트 권한 체계가 자원 보호에 적합한지 확인해야 합니다.

RouteD 사용에 대한 보안 고려사항

RouteD(Route Daemon)(RouteD) 서버는 iSeries 서버에서 RIP(라우팅 정보 프로토콜)에 대한 지원을 제공합니다. RIP는 가장 광범위하게 사용되는 라우팅 프로토콜입니다. 이것은 자율적인 시스템 내의 IP 패킷 라우팅에서 TCP/IP를 지원하는 내부 게이트웨이 프로토콜입니다.

RouteD는 신뢰할 수 있는 네트워크의 시스템이 현재 라우트 정보로 서로를 갱신할 수 있도록 함으로써 네트워크 통신량의 효율을 높이기 위한 것입니다. RouteD를 실행할 때 시스템은 다른 참여 시스템으로부터 전송(패킷) 라우트 방법에 관한 갱신사항을 수신할 수 있습니다. 따라서 해커가 RouteD 서버를 액세스할 수 있을 경우, 해커는 패킷을 도청 또는 수정할 수 있는 시스템을 통해 패킷의 경로를 재지정할 수 있습니다. RouteD 보안에 관한 제안사항은 다음과 같습니다.

- iSeries 서버는 라우터 인증에 관한 어떠한 방법도 제공하지 않는 RIPv1을 사용합니다. 이것은 신뢰할 수 있는 네트워크 내부용입니다. 시스템이 ″신뢰″하지 않는 다른 시스템과의 네트워크에 있는 경우, RouteD 서버를 실행해서는 안 됩니다. RouteD 서버가 자동으로 시작되지 않게 하려면 다음을 입력하십시오.

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  주:

  1. AUTOSTART(*NO)가 디폴트 값입니다.
  2. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.
- RouteD 구성을 변경할 수 있는 사용자를 제어하십시오. 여기에는 *IOSYSCFG 특수 권한이 필요합니다.
- 시스템이 둘 이상의 네트워크(예: 인트라넷 및 인터넷)에 참여하는 경우, RouteD 서버를 구성하여 보안 네트워크와의 갱신사항만 송신 및 승인할 수 있습니다.

DNS 서버 사용에 대한 보안 고려사항

DNS(DNS) 서버는 호스트명에서 IP 주소로의 변환 및 역변환을 제공합니다. iSeries 서버에서 DNS 서버는 내부, 보안 네트워크(인트라넷)에 대한 주소 변환을 제공합니다.

DNS 액세스 방지

시스템의 DNS 서버를 아무도 사용할 수 *없게* 하려면 다음을 수행하십시오.

1. TCP/IP를 시작할 때 DNS 서버 작업이 자동으로 시작되지 않게 하려면 다음을 입력하십시오.

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   주:

   a. AUTOSTART(*NO)가 디폴트 값입니다.

   b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

2. 소켓 어플리케이션과 같은 사용자 어플리케이션을 시스템에서 DNS에 대해 일반적으로 사용하는 포트와 연결하지 못하게 하려면, 다음을 수행하십시오.

   a. GO CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

   b. 옵션 4(TCP/IP 포트 제한에 대한 작업)를 선택하십시오.

   c. TCP/IP 포트 제한에 대한 작업 화면에서 옵션 1(추가)을 지정하십시오.

   d. 하위 포트 범위에 53을 지정하십시오.

   e. 상위 포트 범위에 *ONLY를 지정하십시오.

      주:

      1) 포트 제한은 다음에 TCP/IP를 시작할 때 효력을 발생합니다. 포트 제한을 설정할 때 TCP/IP가 활동중인 경우, TCP/IP를 종료하고 다시 시작해야 합니다.

      2) RFC1700은 공통 포트 번호 할당에 대한 정보를 제공합니다.

   f. 프로토콜에 *TCP를 지정하십시오.

   g. 사용자 프로파일 필드의 경우, 시스템에서 보호되는 사용자 프로파일명을 지정하십시오(보호되는 사용자 프로파일은 권한을 허용하는 프로그램이 아니며 다른 사용자가 알고 있는 암호를 갖지 않는 사용자 프로파일입니다). 포트를 특정 사용자에게 제한하면 다른 모든 사용자는 자동으로 제외됩니다.

   h. *UDP(사용자 데이터그램) 프로토콜에 2c - 2g단계를 반복하십시오.

DNS 서버 보안

다음은 iSeries 시스템에서 DNS를 실행할 때의 보안 고려사항입니다.

- DNS 서버에서 제공하는 기능은 IP 주소 변환 및 이름 변환입니다. iSeries 시스템의 오브젝트에 대한 액세스는 제공하지 않습니다. 외부인이 DNS 서버에 액세스할 때의 위험은 서버에서 네트워크의 토폴로지를 쉽게 열람할 수 있는 방법을 제공한다는 점입니다. DNS로 인해 해커가 잠재적 목표 주소를 판별하는 수고를 덜 수도 있습니다. 그러나 DNS에서는 그러한 목표 시스템에 침입하는 데 도움이 될 수 있는 정보는 제공하지 않습니다.

- 일반적으로는 인트라넷용으로 iSeries DNS 서버를 사용합니다. 그러므로 DNS 조회 능력을 제한할 필요는 없을 것입니다. 예를 들면, 인트라넷 내에 여러 서브네트워크가 있을 수 있습니다. 다른 서브네트워크의 사용자가 iSeries 서버의 DNS를 조회하지 못하게 할 수 있습니다. DNS의 보안 옵션을 사용하여 1차 정의역에 대한 액세스를 제한할 수 있습니다. iSeries Navigator를 사용하여 DNS 서버가 응답해야 하는 IP 주소를 지정하십시오.

  또 다른 보안 옵션을 사용하여 1차 DNS 서버에서 정보를 복사할 수 있는 2차 서버를 지정할 수 있습니다. 이 옵션을 사용하면 서버는 명시적으로 나열되는 2차 서버로부터의 존(zone) 전송 요구(정보 복사 요구)만 승인합니다.
- DNS 서버에 대한 구성 파일 변경 능력을 제한할 때 주의하십시오. 예를 들면, 나쁜 의도를 가진 사용자가 DNS 파일을 변경하여 네트워크 외부의 IP 주소를 지시할 수 있습니다. 네트워크에서 서버를 시뮬레이트하여 서버를 방문하는 사용자의 기밀 정보에 액세스할 수도 있습니다.

iSeries용 HTTP 서버 사용에 대한 보안 고려사항

HTTP Server는 WWW 브라우저 클라이언트에 HTML(Hypertext Markup Language) 문서와 같은 iSeries 서버 멀티미디어 오브젝트에 대한 액세스를 제공합니다. 또한 *CGI(공통 게이트웨이 인터페이스)* 스펙을 지원합니다. 어플리케이션 프로그래머는 CGI 프로그램을 작성하여 서버 기능을 확장할 수 있습니다.

관리자는 인터넷 연결 서버나 iSeries용 IBM HTTP Server를 사용하여 같은 iSeries 서버에서 여러 서버를 동시에 실행시킬 수 있습니다. 실행되는 각 서버를 **서버 인스턴스**라고 합니다. 각 서버 인스턴스는 고유명을 갖습니다. 관리자는 시작할 인스턴스와 각 인스턴스가 수행할 수 있는 사항을 제어합니다.

주: 다음 사항을 구성하거나 관리하기 위해 웹 브라우저를 사용할 경우, HTTP Server의 *ADMIN 인스턴스를 실행해야 합니다.

- iSeries용 방화벽
- 인터넷 연결 서버
- 인터넷 연결 보안 서버
- iSeries용 IBM HTTP Server

사용자(웹 사이트 방문객)에게는 iSeries 서버 사인 온 화면이 표시되지 않습니다. 그러나 iSeries 서버 관리자는 HTTP 지시문을 통해 모든 HTML 문서 및 CGI 프로그램에 명시적으로 권한을 부여해야 합니다. 또한 관리자는 일부 또는 모든 요구에 대해 자원 보안 및 사용자 인증(사용자 ID 및 암호)을 설정할 수 있습니다.

해커의 침입으로 사용자 웹 서버에 대한 서비스가 거부될 수도 있습니다. 사용자 서버는 특정 클라이언트의 요구 시간종료를 측정해서 서비스 거부 침입을 감지합니다. 서버가 클라이언트로부터 요구를 받지 못하면 사용자 서버는 서비스 거부 침입이 진행되고

있다고 판별합니다. 이는 처음에 클라이언트가 사용자 서버로 연결한 후에 발생합니다. 서버는 기본적으로 침입을 감지하면 처벌을 수행합니다.

HTTP 액세스 방지

시스템에 액세스하기 위해 프로그램을 사용하는 사용자가 *없게* 하려면, HTTP Server가 실행하지 못하도록 해야 합니다. 다음을 수행하십시오.

__ 단계 1. TCP/IP를 시작할 때 HTTP Server 작업이 자동으로 시작되지 않게 하려면 다음을 입력하십시오.

```
CHGHTTPA AUTOSTART(*NO)
```

주:

a. AUTOSTART(*NO)가 디폴트 값입니다.

b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

__ 단계 2. HTTP Server 작업은 QTMHHTTP 사용자 프로파일을 사용합니다. HTTP Server가 시작되지 않게 하려면, QTMHHTTP 사용자 프로파일의 상태를 *DISABLED로 설정하십시오.

HTTP 서버에 대한 액세스 제어

HTTP Server의 1차 목적은 iSeries 시스템의 웹 사이트 방문객에게 액세스를 제공하는 것입니다. 웹 사이트를 방문하는 사용자를 무역 잡지의 광고를 열람하는 사람으로 생각해도 좋습니다. 방문객은 사용하고 있는 서버 유형, 서버의 실제 위치와 같이 웹 사이트를 실행하는 하드웨어 및 소프트웨어에 대해 알지 못합니다. 또한, 사용자는 잠재적 방문객과 웹 사이트 사이에 어떠한 장벽(예: 사인 온 화면)도 두고 싶지 않을 것입니다. 그러나 웹 사이트가 제공하는 일부 문서 또는 CGI 프로그램에 대한 액세스를 제한하려 할 수도 있습니다.

또한 하나의 iSeries 시스템이 다중의 논리 웹 사이트를 제공하게 할 수도 있습니다. 예를 들면, iSeries 시스템은 다른 고객 집합을 가진 다른 사업 지점을 지원할 수 있습니다. 이러한 각 사업 지점에 대해 방문객에게 완전히 독립적으로 보이는 고유 웹 사이트가 필요합니다. 또한 업무에 관한 기밀 정보가 있는 내부 웹 사이트(인트라넷)를 제공하려 할 수도 있습니다.

보안 관리자로서 웹 사이트의 내용을 보호해야 하는 한편, 동시에 보안 실천사항이 웹 사이트의 유용성에 부정적 영향을 끼치지 않도록 해야 합니다. 또한 HTTP 활동이 시스템 또는 네트워크의 무결성에 피해되지 않도록 해야 합니다. 다음 주제는 프로그램을 사용할 때의 보안 제안사항을 제공합니다.

관리 고려사항

다음은 인터넷 서버 관리를 위한 몇 가지 보안 고려사항입니다.

- 웹 브라우저 및 *ADMIN 인스턴스를 사용하여 설정 및 구성을 할 수 있습니다. 서버에서의 추가 인스턴스 작성과 같은 일부 기능에 대해서는 *ADMIN 서버를 *반드시* 사용해야 합니다.
- 관리 홈 페이지(*ADMIN 서버의 홈 페이지)의 디폴트 URL은 브라우저 관리 기능을 제공하는 제품 문서에 제공됩니다. 따라서 디폴트 URL은 IBM 제공 사용자 프로파일이 알려져 공개된 것처럼, 해커에게 알려져 해커 포럼에 공개될 수 있습니다. 다음과 같은 몇 가지 방법으로 노출로부터 스스로를 보호할 수 있습니다.
  - 관리 기능을 수행해야 할 경우, HTTP Server의 *ADMIN 인스턴스만 수행하십시오. *ADMIN 인스턴스가 항상 실행되지 않게 하십시오.
  - *ADMIN 인스턴스에 대해 SSL 지원을 활성화하십시오(디지털 인증 관리자 사용). *ADMIN 인스턴스는 사용자 ID와 암호를 확보하기 위해 HTTP 보호 지시문을 사용합니다. SSL을 사용할 경우, 사용자 ID 및 암호가(관리 양식에 나타나는 구성에 대한 다른 모든 정보와 함께) 암호화됩니다.
  - 인터넷에서 *ADMIN 서버에 대한 액세스를 방지하고, 시스템과 URL의 일부인 정의역명을 숨기려면 방화벽을 사용하십시오.
- 관리 기능을 수행할 때는 *IOSYSCFG 특수 권한이 있는 사용자 프로파일로 사인온해야 합니다. 또한 시스템에서 다음과 같은 특정 오브젝트에 대한 권한이 필요할 수도 있습니다.
  - HTML 문서 및 CGI 프로그램을 포함하는 라이브러리 또는 디렉토리
  - 서버에 대한 지시문 내에서 스왑할 계획인 모든 사용자 프로파일
  - 지시문이 사용하는 모든 디렉토리에 대한 액세스 제어 리스트(ACL)
  - 사용자 ID 및 암호 작성 및 유지보수를 위한 유효성 검사 리스트 오브젝트.

  *ADMIN 서버와 TELNET이 있으면 인터넷 연결에서 관리 기능을 리모트 실행하는 기능을 수행할 수 있습니다. 공용 링크(인터넷)에서 관리 기능을 수행할 경우, 중요한 사용자 ID 및 암호가 도청될 수 있다는 점을 유의하십시오. "도청자"가 이 사용자 ID와 암호를 사용하여 예를 들면, TELNET 또는 FTP를 사용해서 시스템에 액세스를 시도할 수 있습니다.

  주:

  1. TELNET을 사용하면 사인 온 화면이 다른 화면과 똑같이 취급됩니다. 암호를 입력할 때 암호가 표시되지는 않지만, 시스템은 암호화되거나 코드화되지 않은 채 암호를 전송합니다.
  2. *ADMIN 서버를 사용하면 암호가 암호화되지 않고 코드화됩니다. 코드화 체계는 산업 표준을 따르며 해커 집단에게 널리 알려져 있습니다. 우발적인 "도청자"는 코드화 체계를 쉽게 파악할 수 없지만, 익숙한 도청자는 암호 해독을 위한 툴을 가지고 있을 수 있습니다.

보안 추가 정보

인터넷에서 리모트 관리를 수행할 경우, 전송이 암호화되도록 SSL이 있는 *ADMIN 인스턴스를 사용해야 합니다. TELNET의 V4R4 이전 버전과 같은 비보안 어플리케이션은 사용하지 마십시오(TELNET은 V4R4에서부터 SSL을 지원합니다). *신뢰할 수 있는* 사용자의 인트라넷에서 *ADMIN 서버를 사용하는 경우, 이 서버를 안전하게 관리하며 사용할 수 있습니다.

- HTTP 지시문은 시스템에서의 모든 활동에 대한 토대를 제공합니다. 제공된 구성은 디폴트 환영 페이지에 적합한 기능을 제공합니다. 클라이언트는 서버 관리자가 서버에 대한 지시문을 정의할 때까지 환영 페이지를 제외한 어떤 문서도 열람할 수 없습니다. 지시문을 정의하려면 WRKHTTPCFG(HTTP 구성에 대한 작업) 명령 또는 *ADMIN 서버 및 웹 브라우저를 사용하십시오. 두 방법 모두 *IOSYSCFG 특수 권한이 필요합니다. iSeries 서버를 인터넷에 연결할 때 조직에서 *IOSYSCFG 특수 권한을 갖는 사용자 수를 평가 및 제어하는 것이 더욱 중요합니다.

자원 보호

iSeries용 IBM HTTP Server에는 서버가 사용하는 정보 자산에 대해 자세한 제어를 제공하는 HTTP 지시문이 포함되어 있습니다. 지시문을 사용하여 웹 서버가 HTML 파일 및 CGI 프로그램 모두의 URL을 제공하는 디렉토리를 제어하고, 다른 사용자 프로파일로 스왑하고, 일부 자원에 대한 인증을 요구할 수 있습니다.

주: Information Center의 ″웹 서빙″ 아래의 문서에서는 사용할 수 있는 HTTP 지시문의 전체 설명과 그 사용법이 제공됩니다. 다음은 이 지원 사용을 위한 몇 가지 제한사항 및 고려사항입니다.

- HTTP Server는 ″명시적인 권한″을 토대로 시작합니다. HTTP Server는 요구가 지시문에 명시적으로 정의되어 있지 않은 경우에는 해당 요구를 승인하지 않습니다. 다시 말해 서버는 URL이 지시문에(이름별로 또는 총칭적으로) 정의되어 있지 않은 경우, 해당 URL에 대한 요구를 즉시 거부합니다.
- 사용자 자원 전체 또는 일부에 대한 요구를 승인하기 전에 보호 지시문을 사용하여 사용자 ID 및 암호를 요구할 수 있습니다.
  - 사용자(클라이언트)가 보호된 자원을 요구하면, 서버는 브라우저에 사용자 ID 및 암호를 요구합니다. 브라우저는 사용자 ID와 암호를 입력하도록 사용자에게 프롬트한 후 해당 정보를 서버에 송신합니다. 일부 브라우저는 사용자 ID와 암호를 저장한 후, 후속 요구가 있을 때 자동으로 송신합니다. 이렇게 할 경우, 사용자가 각 요구 때마다 같은 사용자 ID와 암호를 반복해서 입력하지 않아도 됩니다.

일부 브라우저에서는 사용자 ID와 암호를 저장하므로, 사용자가 iSeries 서버 사인 온 화면이나 라우터를 통해 시스템에 들어갈 때와 동일한 사용자 교육 타스크가 있습니다. 무인 브라우저 세션은 잠재적인 보안 노출을 갖습니다.

– 시스템의 사용자 ID 및 암호(보호 지시문에 지정됨) 처리 방법에 대해 다음 세 가지 옵션이 있습니다.

  1. 일반 iSeries 서버 사용자 프로파일 및 암호 유효성 검사를 할 수 있습니다. 이 방법은 인트라넷(보안 네트워크)에서 자원 보호에 가장 일반적으로 사용됩니다.
  2. 유효성을 확인할 수 있지만 iSeries 서버에 사용자 프로파일이 없는 사용자, 즉 ″인터넷 사용자″를 작성할 수 있습니다. 인터넷 사용자는 ″유효성 검사 리스트″라는 iSeries 서버 오브젝트를 통해 구현됩니다. 유효성 검사 리스트 오브젝트에는 특정 어플리케이션에서 사용되도록 지정된 암호 및 사용자 리스트가 포함되어 있습니다.

     인터넷 사용자 관리 방법 뿐만 아니라 인터넷 사용자 ID 및 암호가 제공되는 방식(예. 전자 우편 요구에 대한 응답으로 관리자나 어플리케이션이 제공)을 결정합니다. HTTP Server의 브라우저 기반 인터페이스를 사용하여 이를 설정하십시오.

     비보안 네트워크(인터넷)의 경우, 인터넷 사용자를 사용하면 일반 사용자 프로파일 및 암호를 사용할 때보다 전반적으로 보호 기능이 향상됩니다. 고유한 사용자 ID 및 암호 세트는 사용자가 수행할 수 있는 사항에 대한 한계가 내장되어 있습니다. 이러한 사용자 ID와 암호는(TELNET 또는 FTP) 일반 사인 온에 사용할 수 없습니다. 또한 일반 사용자 ID와 암호를 도청되지 않게 합니다.
  3. LDAP(Lightweight directory access protocol)는 TCP(전송 제어 프로토콜)를 통해 디렉토리에 대한 액세스를 제공하는 디렉토리 서비스 프로토콜입니다. 이 프로토콜을 사용하여 해당 디렉토리 서비스에 정보를 저장하고 조회할 수 있습니다. 이제 LDAP는 사용자 인증에 대한 선택으로서 지원됩니다.

주:

1. 브라우저가(사용자 프로파일 또는 인터넷 사용자에 대한) 사용자 ID 및 암호를 송신할 때 정보는 암호화되지 않고 코드화됩니다. 코드화 체계는 산업 표준을 따르며 해커 집단에게 널리 알려져 있습니다. 우발적인 ″도청자″는 코드화 체계를 쉽게 파악할 수 없지만, 익숙한 도청자는 암호 해독을 위한 툴을 가지고 있을 수 있습니다.
2. iSeries 서버는 유효성 검사 오브젝트를 보호된 시스템 영역에 저장합니다. 정의된 시스템 인터페이스(API)나 적합한 권한이 있어야만 액세스할 수 있습니다.

- 디지털 인증 관리자(DCM)를 사용하면 사용자가 자체 인트라넷 인증 기관(CA)을 작성할 수 있습니다. 디지털 인증은 인증을 소유자의 사용자 프로파일과 자동으로 연관시킵니다. 인증은 연관된 프로파일과 동일한 권한 및 허가를 갖습니다.

- 서버가 요구를 승인할 때 일반 iSeries 서버 자원 보안이 발생합니다. 자원을 요구하는 사용자 프로파일은 자원(예: HTML 문서를 포함하는 폴더 또는 소스 실제 파일)에 대한 권한이 있어야 합니다. 작업은 QTMHHTTP 사용자 프로파일 아래서 디폴트로 실행합니다. 지시문을 사용하여 다른 사용자 프로파일로 교체할 수 있습니다. 이때 시스템에서는 오브젝트에 액세스하기 위해 해당 사용자 프로파일의 권한을 사용합니다. 다음은 이 지원에 대한 일부 고려사항입니다.
  - 사용자 프로파일 스와핑은 서버에서 둘 이상의 논리 웹 사이트를 제공할 때 특히 유용합니다. 다른 사용자 프로파일을 각 웹 사이트에 대한 지시문과 연관시켜서 각 사이트에 대한 문서를 보호하기 위해 일반 iSeries 서버 자원 보안을 사용할 수 있습니다.
  - 사용자 프로파일 스왑 기능을 유효성 검사 오브젝트와 함께 사용할 수 있습니다. 서버는 고유한 사용자 ID와 암호(일반 사용자 ID 및 암호와는 별개임)를 사용하여 초기 요구를 평가합니다. 서버가 사용자를 인증한 후, 시스템은 다른 사용자 프로파일로 스왑하여 자원 보안을 이용합니다. 따라서, 사용자는 진짜 사용자 프로파일명을 알지 못하므로, 다른 방법(예: FTP)으로 이를 사용할 수 없습니다.

- 일부 HTTP Server 요구는 HTTP Server에서 프로그램을 수행해야 합니다. 예를 들어, 프로그램은 사용자 시스템의 자료에 액세스할 수 있습니다. 프로그램을 실행하기 전에 서버 관리자는 먼저 요구(URL)를 CGI 사용자 인터페이스 표준을 따르는 특정 사용자 정의 프로그램에 맵핑해야 합니다. CGI 프로그램에 관한 일부 고려사항은 다음과 같습니다.
  - HTML 문서와 같이 CGI 프로그램에 대해 보호 지시문을 사용할 수 있습니다. 따라서 프로그램을 실행하기 전에 사용자 ID와 암호를 요구할 수 있습니다.
  - CGI 프로그램은 QTMHHTP1 사용자 프로파일하에서 디폴트로 실행합니다. 프로그램을 실행하기 전에 다른 사용자 프로파일로 스왑할 수 있습니다. 그러므로, CGI 프로그램이 액세스하는 자원에 대해 일반 iSeries 서버 자원 보안을 설정할 수 있습니다.
  - 보안 관리자는 시스템에 CGI 프로그램 사용 권한을 부여하기 전에 보안 검토를 수행해야 합니다. 프로그램이 어디에서 왔는지, CGI 프로그램이 어떤 기능을 수행하는지를 알아야 합니다. 또한 CGI 프로그램을 실행할 사용자 프로파일의 기능을 모니터해야 하며, 명령 행에 대한 액세스를 확보할 수 있는지를 판별하기 위해 CGI 프로그램에 대한 테스트를 수행해야 합니다. 권한을 허용하는 프로그램을 다룰 때와 똑같은 주의를 기울여 CGI 프로그램을 다루십시오.
  - 또한 부적절한 공용 권한을 가진 민감한 오브젝트를 평가해야 합니다. 드문 경우, 제대로 설계되지 않은 CGI 프로그램으로 인해 시스템을 잘 아는 나쁜 의도를 가진 사용자가 시스템을 검색할 수 있습니다.

– 모든 CGI 프로그램을 보유하려면 CGILIB와 같은 특정 사용자 라이브러리를 사용하십시오. 오브젝트 권한을 사용하여 이 라이브러리에 새 오브젝트를 둘 수 있는 사용자와 이 라이브러리에서 프로그램을 실행할 수 있는 사용자를 제어하십시오. 지시문을 사용하여 HTTP Server를 이 라이브러리에서 실행중인 CGI 프로그램으로 제한하십시오.

주: 서버에서 다중의 논리 웹 사이트를 제공하는 경우, 각 사이트에 대해 CGI 프로그램에 별개의 라이브러리를 설정하려 할 수 있습니다.

기타 보안 고려사항

다음은 추가적인 보안 고려사항입니다.

- HTTP는 iSeries 시스템에 대한 읽기 전용 액세스를 제공합니다. HTTP Server 요구는 시스템의 자료를 갱신 또는 삭제할 수 없습니다. 그러나 자료를 갱신하는 CGI 프로그램을 가질 수 있습니다. 또한, Net.Data® CGI 프로그램이 사용자의 iSeries 서버 데이터베이스에 액세스하게 만들 수 있습니다. 시스템은 스크립트(나감 프로그램과 유사)를 사용하여 Net.Data 프로그램에 대한 요청을 평가합니다. 따라서, 시스템 관리자는 Net.Data 프로그램이 취할 수 있는 조치를 제어할 수 있습니다.
- HTTP Server는 서버를 통한 액세스 및 시도된 액세스를 모니터할 때 사용할 수 있는 액세스 기록부를 제공합니다.

iSeries용 IBM HTTP Server와 함께 SSL을 사용하기 위한 보안 고려사항

iSeries용 IBM HTTP Server는 iSeries 서버에 보안 웹 연결을 제공할 수 있습니다. **보안 웹 사이트**는 클라이언트와 서버 사이의(양방향) 전송이 암호화된다는 것을 의미합니다. 이러한 암호화 전송은 도청자의 조사 및 전송을 잡아내거나 변경하려는 사용자들로부터 안전합니다.

주: 보안 웹 사이트는 클라이언트와 서버 사이에서 전달되는 정보 보안에 엄격하게 적용된다는 점을 명심하십시오. 그 목적은 해커에 대한 서버의 약점을 줄이기 위한 것이 아닙니다. 그러나 앞으로 있을 수 있는 해커의 도청을 통해 해커가 쉽게 얻을 수 있는 정보를 상당히 제한합니다.

Information Center에 나오는 SSL 및 Webserving(HTTP) 관련 주제에서 암호화 프로세스를 설치, 구성, 관리하기 위한 모든 정보를 제공합니다. 이 주제에서는 서버 피처 개요 및 서버 사용에 관한 몇 가지 고려사항을 알아봅니다.

인터넷 연결 서버에서는 다음 사용권 프로그램 중 하나가 설치될 때 HTTP 및 HTTPS 지원이 제공됩니다.

- 5722-NC1
- 5722-NCE

이들 옵션이 설치되었을 때 이 제품을 인터넷 연결 보안 서버라고 합니다.

iSeries용 IBM HTTP Server(5722-DG1)는 http 및 https 지원을 모두 제공합니다. SSL을 작동시키려면 다음 암호화 제품 중 하나를 설치해야 합니다.

- 5722-AC2
- 5722-AC3

암호화에 의존하는 보안에는 다음과 같은 몇 가지 요구사항이 있습니다.

- 송신자와 수신자(서버와 클라이언트) 모두 암호화 메커니즘을 "숙지해야" 하며, 암호화 및 해독을 수행할 수 있어야 합니다. HTTP Server에는 SSL 작동가능 클라이언트가 필요합니다(대부분의 일반적인 웹 브라우저는 SSL 작동가능합니다). iSeries 암호화 사용권 프로그램은 몇 가지 산업 표준 암호화 방법을 지원합니다. 클라이언트가 보안 세션 설정을 시도하면, 서버와 클라이언트는 양쪽 모두가 지원하는 가장 안전한 암호화 방법을 찾기 위해 절충합니다.
- 전송은 도청자에 의한 암호 해독이 불가능해야 합니다. 따라서 암호화 방법은 서버와 클라이언트 모두 알고 있는 암호화/해독 **개인용 키**를 가지도록 요구합니다. 안전한 *외부* 웹 사이트를 가지려면, 독립적인 인증 기관(CA)을 사용하여 사용자 및 서버에 대한 디지털 인증을 작성 및 발행해야 합니다. 인증 기관은 신뢰할 수 있는 상대방으로 알려져 있습니다.

암호화는 전송된 정보의 기밀성을 보호합니다. 그러나 재무 정보와 같은 민감한 정보의 경우, 기밀성 외에 무결성 및 인증성이 필요할 수 있습니다. 다시 말해 클라이언트와 (선택적으로) 서버는 (독립적인 참조를 통해) 상대방을 신뢰해야 하며, 반드시 전송이 변경되지 않도록 해야 합니다. 인증 기관(CA)이 제공하는 디지털 서명은 이러한 인증성 및 무결성에 대한 확신을 제공합니다. SSL 프로토콜은 서버의 인증(클라이언트의 인증은 선택) 디지털 서명을 확인하여 인증을 합니다.

암호화 및 해독에는 처리 시간이 필요하며 전송 성능에 영향을 줍니다. 따라서 iSeries 서버에서는 동시에 보안 및 비보안 기능을 위한 두 프로그램을 실행하는 기능이 제공됩니다. 비보안 HTTP Server를 사용하여 제품 카탈로그와 같이 보안이 필요없는 문서를 제공할 수 있습니다. 이러한 문서는 `http://`로 시작하는 URL을 갖습니다. 고객이 신용카드 정보를 입력하는 양식과 같이, 민감한 정보에 보안 HTTP Server를 사용할 수 있습니다. 이 프로그램은 URL이 `http://` 또는 `https://`로 시작하는 문서를 제공할 수 있습니다.

통지

클라이언트로의 전송이 언제 보안 또는 보안되지 않는지, 특히 웹 사이트에서 일부 문서에 대해서만 보안 서버를 사용할 때를 통지하는 것이 인터넷상의 예의입니다.

암호화에는 보안 클라이언트와 보안 서버 둘다 필요하다는 점을 기억하십시오. 보안 브라우저(HTTP 클라이언트)는 상당히 일반화되었습니다.

LDAP에 대한 보안 고려사항

LDAP(Lightweight Directory Access Protocol) 보안 피처에는 SSL(보안 소켓층), 액세스 제어 리스트 및 CRAM-MD5 암호 암호화가 포함됩니다. V5R1에서, LDAP 보안을 향상시키기 위해 Kerberos 연결 및 보안 감사 지원도 추가되었습니다.

이들 주제에 대한 자세한 내용은 iSeries Information Center --> 네트워킹 --> TCP/IP --> 디렉토리 서비스(LDAP)를 참조하십시오. iSeries Information Center 액세스에 대한 정보는 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

LPD에 대한 보안 고려사항

LPD(line printer daemon)는 프린터 출력을 시스템에 분배하는 기능을 제공합니다. 시스템에서는 LPD에 대해 사인 온 처리를 수행하지 않습니다.

LPD 액세스 방지

시스템에 액세스하기 위해 LPD를 사용하는 사용자가 *없게* 하려면, LPD 서버가 실행하지 못하도록 해야 합니다. 다음을 수행하십시오.

__ 단계 1. TCP/IP를 시작할 때 LPD 서버 작업이 자동으로 시작되지 않게 하려면 다음을 입력하십시오.

```
CHGLPDA AUTOSTART(*NO)
```

주:

a. AUTOSTART(*YES)가 디폴트 값입니다.

b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

__ 단계 2. 소켓 어플리케이션과 같은 사용자 어플리케이션을 시스템에서 LPD에 대해 일반적으로 사용하는 포트와 연결하지 못하게 하려면, 다음을 수행하십시오.

__ 단계 a. GO CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

__ 단계 b. 옵션 4(TCP/IP 포트 제한에 대한 작업)를 선택하십시오.

__ 단계 c. TCP/IP 포트 제한에 대한 작업 화면에서 옵션 1(추가)을 지정하십시오.

__ 단계 d. 하위 포트 범위에 515를 지정하십시오.

__ 단계 e. 상위 포트 범위에 *ONLY를 지정하십시오.

주:

1) 포트 제한은 다음에 TCP/IP를 시작할 때 효력을 발생합니다. 포트 제한을 설정할 때 TCP/IP가 활동중인 경우, TCP/IP를 종료하고 다시 시작해야 합니다.

2) RFC1700은 공통 포트 번호 할당에 대한 정보를 제공합니다.

__ 단계 f. 프로토콜에 *TCP를 지정하십시오.

__ 단계 g. 사용자 프로파일 필드의 경우, 시스템에서 보호되는 사용자 프로파일명을 지정하십시오(보호되는 사용자 프로파일은 권한을 허용하는 프로그램이 아니며 다른 사용자가 알고 있는 암호를 갖지 않는 사용자 프로파일입니다). 포트를 특정 사용자에게 제한하면 다른 모든 사용자는 자동으로 제외됩니다.

__ 단계 h. *UDP 프로토콜에 대해 단계 2c - 2g를 반복하십시오.

LPD 액세스 제어

LPD 클라이언트가 시스템에 액세스할 수 있게 하려면, 다음과 같은 보안사항을 알아야 합니다.

- 사용자가 불필요한 오브젝트로 시스템을 채우지 못하도록 하려면, ASP(보조 기억장치 풀)에 대해 적합한 임계값 한계를 설정했는지 확인하십시오. SST(시스템 서비스 툴) 또는 DST(전용 서비스 툴)를 사용하여 ASP에 대한 임계값을 표시 및 설정할 수 있습니다. *백업 및 회복*에서는 ASP 임계값에 대한 자세한 내용을 제공합니다.
- 출력 대기행렬에 대한 권한을 사용하여 시스템에 스풀 파일을 송신할 수 있는 사용자를 제한할 수 있습니다. 사용자 ID가 없는 LPD 사용자는 QTMPLPD 사용자 프로파일을 사용합니다. 이러한 사용자 프로파일에는 소수의 출력 대기행렬에 대한 액세스만 부여할 수 있습니다.

SNMP에 대한 보안 고려사항

iSeries 서버는 단순 네트워크 관리 프로토콜(SNMP) 에이전트의 역할을 수행할 수 있습니다. SNMP는 네트워크 환경에서 게이트웨이, 라우터 및 호스트를 관리하기 위한 방법을 제공합니다. SNMP 에이전트는 시스템에 관한 정보를 수집하고 리모트 SNMP 네트워크 관리자가 요구하는 기능을 수행합니다.

SNMP 액세스 방지

시스템에 액세스하기 위해 SNMP를 사용하는 사용자가 *없게* 하려면, SNMP 서버가 실행하지 못하도록 해야 합니다. 다음을 수행하십시오.

__ 단계 1. TCP/IP를 시작할 때 SNMP 서버 작업이 자동으로 시작되지 않게 하려면 다음을 입력하십시오.

CHGSNMPA AUTOSTART(*NO)

주:

a. AUTOSTART(*YES)가 디폴트 값입니다.

b. 137 페이지의 『자동으로 시작하는 TCP/IP 서버 제어』에서는 자동으로 시작하는 TCP/IP 서버 제어에 대한 자세한 내용을 제공합니다.

__ 단계 2. 사용자가 소켓 어플리케이션과 같은 사용자 어플리케이션을 시스템이 SNMP에 대해 일반적으로 사용하는 포트와 연관시키지 못하게 하려면, 다음을 수행하십시오.

__ 단계 a. GO CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

__ 단계 b. 옵션 4(TCP/IP 포트 제한에 대한 작업)를 선택하십시오.

__ 단계 c. TCP/IP 포트 제한에 대한 작업 화면에서 옵션 1(추가)을 지정하십시오.

__ 단계 d. 하위 포트 범위에 161을 지정하십시오.

__ 단계 e. 상위 포트 범위에 *ONLY를 지정하십시오.

주:

1) 포트 제한은 다음에 TCP/IP를 시작할 때 효력을 발생합니다. 포트 제한을 설정할 때 TCP/IP가 활동중인 경우, TCP/IP를 종료하고 다시 시작해야 합니다.

2) RFC1700은 공통 포트 번호 할당에 대한 정보를 제공합니다.

__ 단계 f. 프로토콜에 *TCP를 지정하십시오.

__ 단계 g. 사용자 프로파일 필드의 경우, 시스템에서 보호되는 사용자 프로파일명을 지정하십시오(보호되는 사용자 프로파일은 권한을 허용하는 프로그램이 아니며 다른 사용자가 알고 있는 암호를 갖지 않는 사용자 프로파일입니다). 포트를 특정 사용자에게 제한하면 다른 모든 사용자는 자동으로 제외됩니다.

__ 단계 h. *UDP 프로토콜에 대해 단계 2c - 2g를 반복하십시오.

SNMP 액세스 제어

SNMP 관리자가 시스템에 액세스하는 것을 허용하려는 경우, 다음과 같은 보안 관련 문제에 유의해야 합니다.

- SNMP로 네트워크를 액세스할 수 있는 사용자는 네트워크에 관한 정보를 수집할 수 있습니다. 별명과 정의역명 서버를 사용하여 숨긴 정보를 앞으로 있을 침입자가 SNMP를 통해 사용할 수 있게 됩니다. 또한, 침입자가 SNMP를 사용하여 네트워크 구성을 변경하여 통신을 방해할 수 있습니다.

- SNMP는 액세스를 위한 공동체명에 의존합니다. 개념상 공동체명은 암호와 유사합니다. 공동체명은 암호화되지 않기 때문에 탐지하기가 쉽습니다. SNMP를 위한 커뮤니티 추가(ADDCOMSNMP) 명령을 사용하여 *ANY 대신 하나 이상의 특정 IP 주소로 관리자 인터넷 주소(INTNETADR) 매개변수를 설정하십시오.
  ADDCOMSNMP 또는 CHGCOMSNMP 명령의 OBJACC 매개변수를 *NONE으로 설정하여 공동체 내의 관리자들이 MIB 오브젝트에 액세스하는 것을 방지할 수도 있습니다. 이는 공동체 자체를 제거하지 않고, 공동체 내의 관리자에 대한 액세스를 거부하기 위해 일시적으로 수행할 때 필요합니다.

INETD 서버에 대한 보안 고려사항

대부분의 TCP/IP 서버와 달리 INETD 서버는 하나의 단일 서비스를 클라이언트에 제공하지 않습니다. 대신, 관리자가 조정할 수 있는 다양한 여러 서비스를 제공합니다. 그런 이유로 INETD 서버를 ″수퍼 서버″라고도 합니다. INETD 서버에는 다음과 같은 서비스가 내장되어 있습니다.

- time
- daytime
- echo
- discard
- changed

이러한 서비스는 TCP와 UDP 모두에 대해 지원됩니다. UDP의 경우, echo, time, daytime, changed 서비스가 UDP 패킷을 수신하고 나면 원래 송신자(originator)에게 다시 전송됩니다. echo 서버는 수신한 패킷을 다시 에코하고, time 및 daytime 서버는 특정 형식으로 시간을 생성하고 나서 이를 다시 송신하고, changed 서버는 인쇄 가능한 ASCII 문자 패킷을 생성하고 나서 이를 다시 송신합니다.

이러한 UDP 서비스의 특성으로 인해 시스템은 서비스 침입을 거부함에 있어서 약점을 나타냅니다. 예를 들어, SYSTEMA 및 SYSTEMB라는 두 iSeries 시스템이 있다고 가정하십시오. 악의있는 프로그래머라면 time 서버의 UDP 포트 번호 및 SYSTEMA의 소스 주소로 IP 헤더 및 UDP 헤더를 위조할 수 있을 것입니다. 그런 후 이 패킷을 SYSTEMB의 time 서버로 보내고, time은 다시 SYSTEMA로, SYSTEMA는 다시 SYSTEMB에 응답하는 식으로, 계속적인 루프를 생성하므로, 네트워크 광역폭 뿐만 아니라 두 시스템 모두의 CPU 자원을 소비하게 됩니다.

따라서 iSeries 시스템에 이러한 공격의 위험이 있음에 유의하고, 보안 네트워크에서만 이들 서비스를 실행시켜야 합니다. INETD 서버는 TCP/IP를 시작할 때 자동 시작되지 않도록 되어 있습니다. INETD가 시작될 때 서비스를 시작할 것인지 여부를 구성할 수 있습니다. 기본적으로 TCP 및 UDP time 서버 및 daytime 서버 모두, INETD 서버를 시작할 때 시작됩니다.

INETD 서버에 대해 다음과 같은 두 개의 구성 파일이 있습니다.

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

이들 파일은 INETD 서버가 시작될 때 어떤 프로그램이 시작될 것인지를 결정합니다. 또한 INETD가 프로그램을 시작할 때 어떤 사용자 프로파일을 실행할 것인지도 결정합니다.

주: proddata 안의 구성 파일을 변경해서는 안 됩니다. 이 파일은 시스템이 다시 로드될 때마다 대체됩니다. 고객 구성 변경사항은 userdata 디렉토리 트리 안의 파일에만 위치시킬 수 있는데 그것은 이 파일이 릴리스 업그레이드중에는 변경되지 **않기** 때문입니다.

악의있는 프로그래머가 이들 파일에 액세스하면 INETD가 시작될 때 어떤 프로그램이라도 시작되도록 구성할 수 있을 것입니다. 따라서 이들 파일을 보호하는 것은 매우 중요합니다. 디폴트로 변경을 하려면 QSECOFR 권한이 필요합니다. 액세스하기 위해 필요한 권한을 줄여서는 안 됩니다.

주: ProdData 디렉토리에 있는 구성 파일을 수정하지 마십시오. 이 파일은 시스템이 재로드될 때마다 대체됩니다. 고객 구성 변경사항은 UserData 디렉토리 트리에 있는 파일에만 둘 수 있습니다. 이 파일은 릴리스 업그레이드중에는 갱신되지 않기 때문입니다.

제한된 TCP/IP 로밍에 대한 고려사항

시스템이 네트워크에 연결되어 있는 상태에서, 네트워크상에서 이러 저리 둘러보는 사용자를 TCP/IP 어플리케이션으로 제한하려 할 수 있습니다. 이를 수행하기 위한 한 가지 방법은 다음과 같은 클라이언트 TCP/IP 명령에 대한 액세스를 제한하는 것입니다.

주: 이러한 명령은 시스템의 여러 라이브러리에 있을 수 있습니다. 최소한 QSYS 라이브러리와 QTCP 라이브러리에 있습니다. 생성되는 모든 사항에 대해 찾고 보안을 조치해야 합니다.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD(REXEC 클라이언트)

사용자의 가능한 목적지는 다음 사항으로 판별할 수 있습니다.

- TCP/IP 호스트 표의 항목

- TCP/IP 라우트 표의 *DFTROUTE 항목. 이를 사용하여 사용자는 목적지가 알려지지 않은 네트워크인 경우, 다음 홉 시스템의 IP 주소를 입력할 수 있습니다. 사용자는 디폴트 라우트를 사용하여 리모트 네트워크에 도달하거나 연결할 수 있습니다.
- 리모트명 서버 구성. 이 지원으로 네트워크의 다른 서버가 사용자의 호스트명을 찾을 수 있습니다.
- 리모트 시스템 표

이 표에 항목을 추가하고 구성을 변경할 수 있는 사용자를 제어해야 합니다. 또한 표 항목 및 구성 관련사항을 알아야 합니다.

ILE C 컴파일러에 대해 액세스할 수 있는 시스템을 잘 알고 있는 사용자가 TCP 또는 UDP 포트에 접속할 수 있는 소켓 프로그램을 작성할 수 있음에 유의하십시오. QSYSINC 라이브러리에 있는 다음과 같은 소켓 인터페이스 파일에 대한 액세스를 제한하면 이를 더욱 어렵게 할 수 있습니다.

- SYS
- NETINET
- H
- ARPA
- 소켓 및 SSL

서비스 프로그램의 경우, 아래의 서비스 프로그램의 사용을 제한하여 소켓과 SSL 어플리케이션 이미 컴파일된 사용을 제한할 수 있습니다.

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

서비스 프로그램에는 공용 권한 *USE가 제공되지만, 그 권한을 *EXCLUDE(또는 필요한 다른 값)로 변경할 수 있습니다.

제 14 장 보안 워크스테이션 액세스

많은 시스템 사용자들이 워크스테이션으로 퍼스널 컴퓨터(PC)를 가지고 있습니다. 사용자들은 PC에서 실행하는 툴을 사용하며 PC를 사용하여 iSeries 서버에 연결합니다.

iSeries 서버로 PC를 연결하는 대부분의 방법은 워크스테이션 에뮬레이션보다 더 많은 기능을 제공합니다. PC가 iSeries의 화면과 같이 보이며, 사용자에게 대화식 사인 온 세션을 제공합니다. 또한, PC는 iSeries 서버에 또다른 컴퓨터처럼 보이며 파일 전송 및 리모트 프로시듀어 호출과 같은 기능을 제공합니다.

iSeries 서버 보안 관리자는 다음 사항을 알고 있어야 합니다.

- 시스템에 연결한 PC 사용자가 사용할 수 있는 기능
- PC 사용자가 액세스할 수 있는 iSeries 서버 자원

iSeries 서버 보안 체계가 확장 PC 기능에 대하여 아직 준비되어 있지 않으면(파일 전송 및 리모트 프로시듀어 호출과 같은) 확장 PC 기능을 방지하려 할 수 있습니다. 아마도 장기적 목표는 시스템의 정보를 보호하는 동안 확장 PC 기능을 허용하는 것입니다. 다음 주제는 PC 액세스와 연관된 일부 보안 문제에 대해 논의합니다.

워크스테이션 바이러스 방지

이 정보는 보안 관리자가 PC 바이러스에 대해 보호할 수 있는 방법을 제안합니다.

보안 워크스테이션 자료 액세스

일부 PC 클라이언트 소프트웨어는 서버에 정보를 저장하기 위하여 공유 폴더를 사용합니다. iSeries 데이터베이스 파일에 액세스하기 위한 PC 사용자에게 제한되고 잘 정의된 인터페이스 세트가 있습니다. 대부분의 클라이언트/서버 소프트웨어의 파일 전송 기능을 사용하여 PC 사용자가 서버와 PC 사이에서 파일을 복사할 수 있습니다. DDM 파일, 리모트 SQL 또는 ODBC 드라이버와 같은 데이터베이스 액세스 기능을 사용하여 PC 사용자가 서버의 자료에 액세스할 수 있습니다.

이 환경에서 서버 자원에 액세스하는 PC 사용자의 요구를 평가하는 프로그램을 작성할 수 있습니다. 요구에서 DDM 파일을 사용할 경우, DDMACC(분산 자료 관리 액세스) 네트워크 속성에 나감 프로그램을 지정합니다. 일부 PC 파일 전송 방법의 경우, PCSACC(클라이언트 요구 액세스) 네트워크 속성에 나감 프로그램을 지정합니다. 또는 PCSACC(*REGFAC)를 지정하여 등록 기능을 사용할 수도 있습니다. 요구가 다른 서버 기능을 사용하여 자료에 액세스할 경우, WRKREGINF 명령을 사용하여 해당 서버 기능에 나감 프로그램을 등록할 수 있습니다.

그러나 나감 프로그램은 설계하기가 어렵습니다. 나감 프로그램은 오브젝트 권한에 대한 대체가 아니며, 모든 소스의 권한 없는 액세스로부터 오브젝트를 보호하기 위하여 설계됩니다.

Windows용 IBM iSeries Access와 같은 일부 클라이언트 소프트웨어는 통합 파일 시스템을 사용하여 iSeries 서버에 자료를 저장하고 액세스합니다. 통합 파일 시스템을 통하여 PC 사용자가 전체 서버를 더욱 쉽게 사용할 수 있게 됩니다. 오브젝트 권한은 더욱 필요하게 됩니다. 충분한 권한을 가진 사용자는 통합 파일 시스템을 통하여 서버 라이브러리를 PC 디렉토리인 것처럼 열람할 수 있습니다. 간단한 이동 및 복사 명령은 iSeries 서버 라이브러리에서 PC 디렉토리로 자료를 즉시 이동할 수 있고, 그 반대도 마찬가지입니다. 시스템은 자동으로 자료의 형식을 적절히 변경합니다.

주:

1. 권한 부여 리스트를 사용하여 QSYS.LIB 파일 시스템의 오브젝트 사용을 제어할 수 있습니다. 자세한 내용은 112 페이지의 『QSYS.LIB 파일 시스템으로 액세스 제한』을 참조하십시오.
2. 105 페이지의 제 11 장 『보안된 파일에 통합 파일 시스템 사용』에서는 통합 파일 시스템의 보안 문제에 대한 자세한 내용을 제공합니다.

통합 파일 시스템의 장점은 사용자와 개발자들을 위한 단순성입니다. 사용자는 단일 인터페이스로 여러 환경에서 오브젝트에 대해 작업할 수 있습니다. PC 사용자는 오브젝트 액세스에 특수 소프트웨어 또는 API가 필요하지 않습니다. 대신 PC 사용자는 익숙한 PC 명령을 사용하거나 『지정 및 클릭』하여 오브젝트에 대해 직접 작업할 수 있습니다.

PC가 접속된 모든 시스템의 경우, 특히 통합 파일 시스템을 사용하는 클라이언트 소프트웨어가 있는 시스템의 경우, 좋은 오브젝트 권한 체계가 중요합니다. 보안이 OS/400 제품으로 통합되므로, 자료를 액세스하는 요청은 권한 검사 프로세스를 통과해야 합니다. 권한 검사는 소스에서 특정 방법을 사용하는 자료 액세스까지의 요구에 적용됩니다.

워크스테이션 액세스의 오브젝트 권한

오브젝트에 대한 권한을 설정하려면 해당 권한이 PC 사용자에게 제공되는 것을 평가해야 합니다. 예를 들면, 사용자가 파일에 대하여 *USE 권한을 가지면 파일의 자료를 열람하거나 인쇄할 수 있습니다. 파일의 정보를 변경하거나 파일을 삭제할 수 없습니다. PC 사용자의 경우, 보기는 『읽기』와 같으며, 사용자가 PC의 파일을 복사할 만큼 충분한 권한이 제공됩니다. 이것은 사용자의 의도가 아닐 수 있습니다.

일부 중요한 파일의 경우, 다운로드를 방지하기 위하여 공용 권한을 *EXCLUDE로 설정해야 할 수 있습니다. 그런 다음, 권한을 허용하는 메뉴 및 프로그램을 사용하는 것과 같이 서버의 파일을 『열람』하는 다른 방법을 제공할 수 있습니다.

다운로드를 방지하는 또다른 옵션은 PC 사용자가 (대화식 사인 온이 아닌) 서버 기능을 시작할 때마다 실행되는 나감 프로그램을 사용하는 것입니다. CHGNETA(네트워크 속성 변경) 명령을 사용하여 PCSACC 네트워크 속성에서 나감 프로그램을 지정할 수 있습니다. 또는 WRKREGINF(등록 정보에 대한 작업) 명령을 사용하여 나감 프로그램을 등록할 수 있습니다. 사용하는 방법은 PC가 사용하는 클라이언트 프로그램에 따라 다릅니다. 나감 프로그램(QIBM_QPWFS_FILE_SERV)은 IFS에 대한 iSeries Access 및 Net Server 액세스에 적용됩니다. FTP 또는 ODBC와 같이 메커니즘이 다른 PC의 액세스는 방지하지 않습니다.

PC 소프트웨어는 일반적으로 PC에서 서버 데이터베이스 파일로 자료를 복사할 수 있도록 업로드 기능도 제공합니다. 사용자의 권한 체계를 올바르게 설정하지 않을 경우, PC 사용자가 파일의 모든 자료를 PC의 자료와 오버레이시킬 수 있습니다. *CHANGE 권한을 조심스럽게 할당해야 합니다. 파일 조작에 필요한 권한을 알려면 *iSeries 보안 참조서* 책의 부록 D를 검토하십시오.

iSeries Information Center에서는 PC 기능에 대한 권한 및 나감 프로그램 사용에 대한 자세한 내용을 제공합니다. 자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

어플리케이션 관리

어플리케이션 관리는 iSeries Navigator 중 옵션으로 설치할 수 있는 iSeries 서버용 그래픽 사용자 인터페이스(GUI) 구성요소입니다. 어플리케이션 관리는 특정 서버에서 사용자와 그룹이 사용하는 기능이나 어플리케이션을 시스템 관리자가 제어할 수 있도록 해줍니다. 여기에는 사용자들이 클라이언트를 통해 서버에 액세스하기 위해 사용하는 기능들을 제어하는 것이 포함됩니다. 여기에서 서버를 Windows 클라이언트로부터 액세스하는 경우, Windows 사용자가 아닌 iSeries 서버 사용자가 관리에 사용할 수 있는 기능을 판별한다는 점에 주의하는 것이 중요합니다.

iSeries Navigator 어플리케이션 관리에 대한 모든 문서는 iSeries Information Center --> iSeries 연결 --> 연결 대상 --> iSeries Navigator(../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm)를 참조하십시오.

정책 관리

정책은 관리자들이 클라이언트 PC에 소프트웨어를 구성할 때 사용하는 하나의 툴입니다. 정책을 통해 사용자들이 PC에서 액세스를 갖는 기능 및 어플리케이션을 제한할 수 있습니다. 또한 정책을 통해 특정 사용자나 PC가 사용하는 구성을 제안 또는 강제할 수 있습니다.

주: 정책은 서버 자원에 대한 제어를 제공하지 않습니다. 정책은 서버 보안의 대체 기능이 아닙니다. 정책은 특정 사용자들에 의한 특정 PC로부터 iSeries Access를 서버에 액세스하는 방식에 영향을 주기 위해 사용됩니다. 그러나 다른 메커니즘을 통한 서버 자원의 액세스 방식은 변경하지 않습니다.

정책은 파일 서버에 저장되어 있습니다. 사용자가 자신의 Windows 워크스테이션에 사인 온할 때마다 그 Windows 사용자에게 적용되는 정책이 파일 서버로부터 다운로드됩니다. 정책은 사용자가 워크스테이션에서 작업을 수행하기 전에 레지스트리에 적용됩니다.

Microsoft® 정책 대 어플리케이션 관리

iSeries Access Express는 네트워크에서 관리 제어를 구현하기 위해 Microsoft 시스템 정책과 iSeries Navigator 어플리케이션 관리라는 두 가지 다른 전략을 지원합니다. 다음 요소를 고려하여 사용자에게 가장 적합한 전략이 어느 것인지 결정하십시오.

Microsoft 시스템 정책

정책은 특정 OS/400 릴리스와 관계없이 PC 주도로 이루어집니다. 정책은 Windows 사용자뿐 아니라 PC에도 적용됩니다. 이것은 사용자들이 서버 사용자 프로파일이 아닌 Windows 사용자 프로파일을 참조한다는 것을 의미합니다. 정책들은 제한은 물론 ″구성″을 위해서도 사용됩니다. 일반적으로 정책은 어플리케이션 관리보다 더 많은 세분성 및 더 넓은 기능을 제공합니다. 이것은 사용자가 기능을 수행할 수 있는지의 여부를 판별하는 데 있어서 서버와의 연결이 필요하지 않기 때문입니다. 정책을 다운로드하기 위해서는 Microsoft 시스템 정책 편집기를 반드시 사용해야 하고 PC를 개별적으로 구성해야 하므로 정책을 실행하는 것이 어플리케이션 관리를 실행하는 것보다 훨씬 더 복잡합니다.

iSeries Navigator 어플리케이션 관리

어플리케이션 관리는 자료를 Microsoft 시스템 정책이 연관시키는 Windows 프로파일 대신 사용자 프로파일과 연관시킵니다. 어플리케이션 관리를 사용하기 위해 iSeries 서버가 V4R3 이상의 OS/400 제품을 실행 중인 반면, 일부 기능들은 V4R4 이상에서만 사용할 수 있습니다. 어플리케이션 관리는 관리에 있어서 정책 편집기보다 사용이 훨씬 쉬운 iSeries Navigator의 그래픽 사용자 인터페이스를 사용합니다. 어플리케이션 관리 정보는 PC를 사인 온했는지와 관계없이 사용자에게 적용됩니다. iSeries Navigator 안의 특정 기능들은 제한시킬 수 있습니다. 제한하려는 모든 기능들이 어플리케이션 관리 작동가능 기능이며, 사용되는 OS/400 버전이 어플리케이션 관리를 지원할 경우에는 어플리케이션 관리를 사용하는 것이 좋습니다.

Windows용 iSeries Access와 함께 SSL 사용

SSL과 함께 iSeries Access Express를 사용하는 것에 대한 자세한 정보는 iSeries Information Center 주제 *SSL(Secure Sockets Layer) 관리, iSeries Access Express 및 iSeries Navigator, iSeries Developer Kit for Java 및 Java 기본 주제 아래의 iSeries Java Toolbox*를 참조하십시오. 시스템과 함께 제공되는 CD에 있는 이들 정보를 검토할 수도 있습니다.

iSeries Navigator 보안

iSeries Navigator는 iSeries Access가 있는 사용자가 간편하게 서버에 사용할 수 있는 인터페이스를 제공합니다. OS/400 제품의 각 새로운 릴리스를 사용하면 더 많은 서버 기능을 iSeries Navigator를 통하여 사용할 수 있습니다. 사용하기 쉬운 인터페이스는 경감된 기술 지원 비용 및 향상된 시스템 이미지를 포함하는 많은 이익을 제공합니다. 또한 보안에 대해 이의를 제기하기도 합니다.

보안 관리자는 자원의 보호를 위해 사용자가 시스템에 무지하기만을 바랄 수는 없습니다. iSeries Navigator로 사용자가 많은 기능을 쉽게 사용하고 볼 수 있게 되었습니다. 사용자의 보안 요구에 부합하기 위하여 사용자 프로파일 및 오브젝트 보안에 대한 보안 방침을 확실하게 설계하고 수행해야 합니다.

Windows용 IBM e(logo)server iSeries Access V4R4 이후의 버전에서는 다음과 같은 메소드를 제공하여 사용자가 iSeries Navigator를 이용하여 수행할 수 있는 기능들을 제어할 수 있도록 합니다.

- 선택 설치
- 어플리케이션 관리
- Windows NT® 시스템 정책 지원

iSeries Navigator는 별도로 설치할 수 있는 다중 구성요소로 구성되어 있습니다. 이것을 사용하면 사용자가 필요한 기능만 설치할 수 있습니다. 어플리케이션 관리 기능을 이용하여 관리자는 사용자나 그룹이 iSeries Navigator를 통해 액세스할 수 있는 기능을 제어할 수 있습니다. 어플리케이션 관리 기능은 어플리케이션을 다음과 같은 범주로 분류합니다.

iSeries Navigator
: iSeries Navigator와 기타 플러그인이 포함됩니다.

클라이언트 어플리케이션
: iSeries Access를 포함하여 어플리케이션 관리를 통해 관리되는 클라이언트상에서 기능을 제공하는 다른 모든 클라이언트 어플리케이션이 포함됩니다.

호스트 어플리케이션
: 전적으로 서버에 상주하고 어플리케이션 관리 기능을 통해 관리되는 기능을 제공하는 모든 어플리케이션이 포함됩니다.

선택 설치 및 어플리케이션 관리, 정책을 사용하여 사용자가 액세스할 수 있는 iSeries Navigator 기능을 제한할 수 있습니다. 그러나 이 중 어느 것도 자원 보안에 사용해서는 안 됩니다.

V4R4에서부터 Windows용 IBM e(logo)server iSeries Access는 Windows NT 시스템 정책 편집기 사용도 지원함으로써, 누가 PC를 사용하고 있는지에 관계없이 특정 PC 클라이언트로부터 수행할 수 있는 기능을 제어할 수 있게 되었습니다.

선택 설치, 어플리케이션 관리 및 정책 관리에 대한 추가 정보에 대해서는 iSeries Information Center를 참조하십시오. 이 책 6 페이지의 『프로그램 기능에 대한 액세스 제한』 섹션에는 어플리케이션 관리에 대한 일부 논의도 포함되어 있습니다.

ODBC 액세스 방지

ODBC(개방 데이터베이스 연결)은 PC 어플리케이션에서 iSeries 자료를 PC 자료인 것처럼 액세스할 때 사용할 수 있는 툴입니다. ODBC 프로그래머는 자료의 실제 위치를 PC 어플리케이션 사용자에게 투명하게 할 수 있습니다. ODBC 보안 고려사항에 대한 자세한 정보는 iSeries Information Center에 있는 ″Windows용 iSeries Access ODBC 보안″ 정보(/rzaii/rzaiiodbc09.HTM)를 참조하십시오.

워크스테이션 세션 암호에 대한 보안 고려사항

일반적으로 PC 사용자가 iSeries Access와 같은 연결 소프트웨어를 시작하면 사용자가 서버에 대한 사용자 ID 및 암호를 한 번 입력합니다. 암호는 암호화되어 PC 메모리에 저장됩니다. 사용자가 같은 서버에 새 세션을 설정할 때마다 PC에서 사용자 ID 및 암호를 자동으로 송신합니다.

일부 클라이언트/서버 소프트웨어도 대화식 세션에 대한 사인 온 화면을 바이패스하는 옵션을 제공합니다. 사용자가 대화식(5250 에뮬레이션) 세션을 시작할 경우, 소프트웨어가 사용자 ID 및 암호화된 암호를 송신합니다. 이 옵션을 지원하려면 서버의 QRMTSIGN 시스템 값이 *VERIFY로 설정되어야 합니다.

사인 온 화면의 바이패스를 허용하도록 선택할 경우, 보안 교환을 고려해야 합니다.

보안 노출: 5250 에뮬레이션 또는 다른 유형의 대화식 세션일 경우, 사인 온 화면은 다른 화면과 같습니다. 암호가 입력될 때 화면에 표시되지 않더라도 암호는 다른 자료 필드와 마찬가지로 암호화되지 않은 형식으로 링크에 송신됩니다. 이런 경우, 암호를 일부 감지할 수 있는 좋은 기회를 제공할 수 있습니다. 전자 장비를 사용한 링크 모니터링을 **도청**이라고 합니다. V4R4부터 시작하여 보안 소켓층(SSL)을 시용해서 iSeries Access와 iSeries 서버간 통신을 암호화할 수 있습니다. 이렇게 함으로써 암호와 같은 사용자 자료가 도청되는 것을 방지할 수 있습니다.

사인 온 화면을 바이패스하는 옵션을 선택할 경우, PC는 암호를 송신하기 전에 이를 암호화합니다. 암호화는 도청에 의한 암호의 도난 가능성을 방지합니다. 그러나 PC 사용자가 조작 보안을 실행해야 합니다. iSeries 시스템에 대해 활동중인 세션이 있는 무인 PC는 누군가가 사용자 ID 및 암호를 몰라도 다른 세션을 시작하는 기회를 제공합니다. 오랜 기간 동안 시스템이 활동하지 않을 경우, PC가 잠기도록 설정하고, 세션을 재개하려면 암호가 필요합니다.

사인 온 화면을 바이패스하도록 선택하지 않더라도 비활동 세션이 있는 무인 PC에서는 보안이 노출될 수 있습니다. PC 소프트웨어를 사용하면 사용자 ID와 암호를 모르더라도 다시 서버 세션을 시작하고 자료에 액세스할 수 있습니다. 세션을 시작하고 자료를 액세스하는 것이 보다 적은 지식을 필요로 하기 때문에 5250 에뮬레이션의 노출이 좀 더 심합니다.

또한 iSeries Access 세션의 연결 중단 영향에 대해 사용자를 교육시킬 필요도 있습니다. 많은 사용자들이 단절 옵션이 서버와의 연결을 완전히 중단할 것이라고 (논리적이지만 정확하지 않은) 생각합니다. 사실 사용자가 단절 옵션을 선택하면, 서버가 사용자의 세션(사용권)을 다른 사용자가 사용할 수 있도록 합니다. 그러나 서버에 대한 클라이언트의 연결은 여전히 열려 있습니다. 다른 사용자가 비보호 PC에 접근하여 사용자 ID 및 암호를 입력하지 않고도 서버 자원에 액세스할 수 있습니다.

세션을 단절해야 하는 사용자를 위해 다음 두 가지 옵션을 제안할 수 있습니다.

- PC에 암호를 요구하는 잠금 기능이 있는지 확인하십시오. 암호를 모르는 사용자가 무인 PC를 사용할 수 없게 합니다.
- 세션을 완전히 단절하려면 Windows를 로그오프하거나 PC를 재시작하십시오. 그러면 iSeries에 대한 세션이 종료됩니다.

또한, Windows용 iSeries Access를 사용할 경우, 가능한 보안 노출에 대하여 사용자를 교육해야 합니다. UNC(universal naming convention)를 지정하여 iSeries 자원을 식별할 경우, Win95 또는 NT 클라이언트는 서버에 링크하기 위해 네트워크 연결을 빌드합니다. 사용자는 UNC를 지정하므로, 이를 맵핑된 네트워크 드라이브로 볼 수 없습니다. 때로는 사용자가 네트워크 연결의 존재조차 알지 못합니다. 그러나 서버가 PC의 디렉토리 트리에 표시되므로, 이 네트워크 연결은 무인 PC에 보안 노출을 표시합니다. 사용자의 세션에 강력한 사용자 프로파일이 있으면, 서버 자원은 무인 PC에 노출될 수 있습니다. 이전 예에서와 같이 해결책은 반드시 사용자가 노출에 대하여 알고 PC 잠금 기능을 사용하는 것입니다.

리모트 명령 및 프로시듀어에서 서버 보호

iSeries Access와 같은 소프트웨어를 가진 지식있는 PC 사용자는 사인 온 화면을 거치지 않고도 서버에서 명령을 실행할 수 있습니다. 다음은 PC 사용자가 서버 명령을 실행할 수 있게 하는 여러 가지 방법입니다. 사용자의 클라이언트/서버 소프트웨어는 PC 사용자가 사용가능하게 할 수 있는 방법인지 판별합니다.

- 사용자는 DDM 파일을 열고 리모트 명령 기능을 사용하여 명령을 실행할 수 있습니다.
- iSeries Access 최적화 클라이언트와 같은 일부 소프트웨어는 DDM을 사용하지 않고 DPC(분산 프로그램 호출) API를 통해 리모트 명령 기능을 제공합니다.

- 리모트 SQL 및 ODBC와 같은 일부 소프트웨어는 DDM 또는 DPC가 없어도 리모트 명령 기능을 제공합니다.

리모트 명령 지원에 DDM을 사용하는 클라이언트/서버 소프트웨어의 경우, DDMACC 네트워크 속성을 사용하여 리모트 명령을 완전히 방지할 수 있습니다. 다른 서버 지원을 사용하는 클라이언트/서버 소프트웨어의 경우, 서버에 대하여 나감 프로그램을 등록할 수 있습니다. 리모트 명령을 허용하려면 사용자의 오브젝트 권한 체계가 자료를 적절히 보호하도록 해야 합니다. 리모트 명령 기능은 사용자에게 명령 행을 제공하는 것과 같습니다. 또한, iSeries가 DDM을 통해 리모트 명령을 수신하면, 시스템은 사용자 프로파일에 LMTCPB(제한된 기능) 설정을 강행하지 않습니다.

리모트 명령 및 프로시듀어에서 워크스테이션 보호

Windows용 IBM iSeries Access는 PC에서 리모트 명령을 수신하는 기능을 제공합니다. 서버에서 RUNRMTCMD(리모트 명령 실행) 명령을 사용하여 접속된 PC에서 프로시듀어를 실행할 수 있습니다. RUNRMTCMD 기능은 시스템 관리자 및 도움말 데스크 요원에게 중요한 툴입니다. 그러나 이것도 고의적 또는 우발적으로 PC 자료를 손상시킬 기회를 제공합니다.

PC에는 iSeries 서버와 같은 오브젝트 권한 기능이 없습니다. RUNRMTCMD 명령의 문제에 대한 최대 보호는 명령에 액세스할 수 있는 시스템 사용자를 조심스럽게 제한하는 것입니다. Windows용 IBM iSeries Access는 사용자가 특정 PC에서 리모트 명령을 실행할 수 있는 사용자를 등록하는 기능을 제공합니다. 연결이 TCP/IP를 통해 이루어질 경우, 클라이언트의 특성 제어판을 사용하여 리모트 명령 액세스를 제어할 수 있습니다. 사용자 ID 또는 리모트 시스템명으로 사용자에게 권한을 부여할 수 있습니다. 연결이 SNA를 통해 이루어질 경우, 일부 클라이언트 소프트웨어에서 대화에 대한 보안 설정 기능을 제공합니다. 다른 클라이언트 소프트웨어의 경우, 수신되는 명령 기능의 설정 여부만 선택합니다.

클라이언트 소프트웨어 및(TCP/IP 또는 SNA와 같은) 연결 유형의 각 조합일 경우, 접속한 PC에 수신되는 명령에 대한 가능성을 검토해야 합니다. 『수신 명령』 또는 『RUNRMTCMD』에 대하여 탐색하여 클라이언트 문서를 참조하십시오. PC 사용자 및 네트워크 관리자에게 클라이언트를 구성하는 기능을 허용 또는 방지하는 올바른(안전한) 방법에 대한 조언을 준비하십시오.

게이트웨이 서버

시스템이 iSeries 시스템 및 PC 사이의 중간 또는 게이트웨이 서버를 사용하여 네트워크에 참여할 수 있습니다. 예를 들면, iSeries 시스템은 PC 서버에 접속할 PC가 있는 PC 서버와 함께 LAN에 접속할 수 있습니다. 이런 상황에서 보안 문제는 게이트웨이 서버에서 실행중인 소프트웨어의 기능에 따라 다릅니다. 그림 13은 게이트웨이 서버 구성의 예를 보여줍니다.

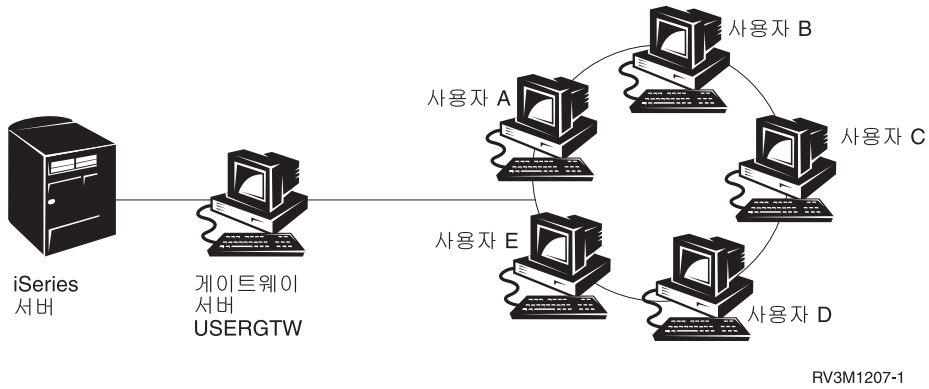

그림 13. 게이트웨이 서버의 iSeries 시스템

일부 소프트웨어의 경우, iSeries 시스템은 게이트웨이 서버에서 아래로 흐르는(USERA 또는 USERC와 같은) 사용자에 대하여 모릅니다. 서버는 단일 사용자(USERGTW)로서 시스템에서 사인 온합니다. USERGTW 사용자 ID를 사용하여 정방향 사용자에서 모든 요구를 처리합니다. USERA의 요구는 사용자 USERGTW의 요구와 같이 서버에 표시됩니다.

이러한 경우 보안 강행에 대하여 게이트웨이 서버에 의존해야 합니다. 게이트웨이 서버의 보안 기능을 알고 관리해야 합니다. iSeries 서버의 관점에서 모든 사용자에게 게이트웨이 서버가 세션을 시작하기 위하여 사용하는 사용자 ID와 같은 권한이 있습니다. 사용자는 권한을 허용하고 명령 행을 제공하는 프로그램 실행과 같게 생각할 것입니다.

다른 소프트웨어의 경우, 게이트웨이 서버는 개별 사용자에서 iSeries 서버로 요구를 전달합니다. iSeries 서버는 USERA가 특정 오브젝트에 대한 액세스를 요구하고 있다는 것을 인식합니다. 게이트웨이는 서버에서 볼 때 거의 투명합니다.

시스템이 게이트웨이 서버가 있는 네트워크에 있으면 게이트웨이 서버에서 사용하는 사용자 ID로 제공되는 권한의 정도를 평가해야 합니다. 또한 다음 사항을 알고 있어야 합니다.

- 게이트웨이 서버가 강행하는 보안 메커니즘
- 정방향 사용자가 사용자의 iSeries 시스템에 나타나는 방법

무선 LAN 통신

일부 클라이언트는 시스템과 무선으로 통신하기 위해 iSeries 무선 LAN을 사용할 수 있습니다. iSeries 무선 LAN은 무선 주파수 통신 기술을 사용합니다. 보안 관리자는 iSeries 무선 LAN 제품의 다음과 같은 보안 특성을 알고 있어야 합니다.

- 이러한 무선 LAN 제품은 스프레드 스펙트럼 기술을 사용합니다. 이와 동일한 기술을 무선 전송 보안을 위해 과거에 정부에서 사용한 바 있습니다. 자료 전송에 대해 전자적으로 모니터하려는 사용자에게는 전송이 실제 전송이 아니라 소음으로 나타납니다.
- 무선 연결에는 다음과 같은 세 가지의 보안 관련 구성 매개변수가 있습니다.
  - 자료 전송률(두 가지의 사용가능한 자료 전송률)
  - 주파수(5가지의 사용가능한 주파수)
  - 시스템 ID(8백만개의 사용가능한 ID)

  이러한 구성 요소가 결합하여 8천만개의 사용가능한 구성을 제공하므로, 해커가 올바른 구성을 알아낼 가능성은 매우 희박합니다.
- 다른 통신 방법과 같이 무선 통신 보안은 클라이언트 장치 보안의 영향을 받습니다. 시스템 ID 정보 및 기타 구성 매개변수는 클라이언트 장치의 파일에 있으며 보호되어야 합니다.
- 무선 장치가 유실되거나 도난당한 경우, 사인 온 암호 및 오브젝트 보안과 같은 일반 서버 보안 조치가 권한이 없는 사용자가 시스템에 액세스하기 위해 유실 또는 도난된 장치를 사용하려 할 때 보호를 제공합니다.
- 무선 클라이언트 장치가 유실 또는 도난된 경우, 모든 사용자, 액세스 지점 및 시스템에 대한 시스템 ID 정보 변경을 고려해야 합니다. 이를 열쇠를 도난당했을 때 문의 자물쇠를 바꾸는 것으로 생각하십시오.
- 서버를 고유 시스템 ID를 갖는 클라이언트 그룹으로 분할하려 할 수 있습니다. 이렇게 하여 장치가 유실 또는 도난되었을 때의 영향을 제한할 수 있습니다. 이 방법은 사용자 그룹을 특정 설치 부분으로 제한할 수 있을 경우에만 효력을 가질 수 있습니다.
- 유선 LAN 기술과는 달리 무선 LAN 기술은 소유권을 갖습니다. 따라서, 이러한 무선 LAN 제품에는 공식적으로 전자 탐지장치를 사용할 수 없습니다. 탐지 장치는 전송에 대해 권한이 없는 모니터링을 수행하는 전자 장치입니다.

제 15 장 보안 나감 프로그램

일부 iSeries 서버 기능은 시스템에서 사용자 작성 프로그램을 실행하여 추가 검사 및 유효성 검사를 수행할 수 있도록 나감을 제공합니다. 예를 들면, 시스템에서 분산 자료 관리(DDM) 파일을 열려는 사용자가 있을 때마다 나감 프로그램을 실행하도록 시스템을 설정할 수 있습니다. 등록 기능을 사용하여 특정 조건에서 실행되는 나감 프로그램을 지정할 수 있습니다.

일부 iSeries 책에는 보안 기능을 수행하는 나감 프로그램의 예제가 들어 있습니다. 표 24는 이러한 나감 프로그램의 리스트와 예제 프로그램의 소스를 제공합니다.

표 24. 나감 프로그램 샘플의 소스

나감 프로그램 유형	목적	예를 찾을 수 있는 위치
암호 유효성 검사	QPWDVLDPGM 시스템 값은 프로그램명을 지정하거나 QIBM_QSY_VLD_PASSWRD 종료점에 대해 등록된 유효성 프로그램이 QPWDxxx 시스템 값에 의해 처리되지 않는 추가 요구사항에 대해 새 암호를 점검하는 데 사용되도록 표시할 수 있습니다. 암호화되지 않은 암호를 수신하므로, 이 프로그램의 사용을 주의깊게 모니터해야 합니다. 이 프로그램은 파일에 암호를 저장하거나 암호를 다른 프로그램에 전달해서는 **안됩니다**.	• *An Implementation Guide for iSeries Security and Auditing, GG24-4200* • *iSeries 보안 참조서*, SC41-5302-07
PC Support/400 또는 Client Access 액세스[1]	이 프로그램명을 네트워크 속성의 PCSACC(클라이언트 요구 액세스) 매개변수에 지정하여 다음과 같은 기능을 제어할 수 있습니다. • 가상 프린터 기능 • 파일 전송 기능 • 공유 폴더 유형 2 기능 • Client access 메세지 기능 • 자료 대기행렬 • 리모트 SQL 기능	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
분산 자료 관리(DDM) 액세스	이 프로그램명을 네트워크 속성의 DDMACC(DDM 요구 액세스) 매개변수에 지정하여 다음과 같은 기능을 제어할 수 있습니다. • 공유 폴더 유형 0 및 1 기능 • 리모트 명령 제출 기능	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
리모트 사인 온	QRMTSIGN 시스템 값에 프로그램을 지정하여 어느 위치(passthru)에서 어느 사용자가 자동으로 사인 온할 수 있는지를 제어할 수 있습니다.	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*

표 24. 나감 프로그램 샘플의 소스 (계속)

나감 프로그램 유형	목적	예를 찾을 수 있는 위치
iSeries Access를 사용한 ODBC(개방 데이터베이스 연결성)[1]	ODBC의 다음 기능을 제어하십시오. • ODBC가 허용되는지의 여부 • iSeries 데이터베이스 파일에 허용되는 기능 • 허용되는 SQL문 • 데이터베이스 서버 오브젝트에 대해 검색할 수 있는 정보 • 허용되는 SQL 카탈로그 기능	사용 불가능
QSYSMSG 구분 처리 프로그램	QSYSMSG 메세지 대기행렬을 모니터할 프로그램을 작성하여 메세지 유형에 따라 적절한 조치(예를 들면, 보안 관리자에게 통지)를 취할 수 있습니다.	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
TCP/IP	일부 TCP/IP 서버(예: FTP, TFTP, TELNET 및 REXEC)는 종료점을 제공합니다. 나감 프로그램을 추가하여 로그온을 처리하고, 특정 파일 확보 또는 기록 요구와 같은 사용자 요구의 유효성을 검사할 수 있습니다. 또한 이러한 나감을 사용하여 시스템에 익명의 FTP를 제공할 수 있습니다.	『*iSeries 시스템 API 참조서* 책에 있는 TCP/IP User Exits』
사용자 프로파일 변경사항	다음 사용자 프로파일 명령에 대해 나감 프로그램을 작성할 수 있습니다. CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries 보안 참조서*, SC41-5302-07 • 『*iSeries 시스템 API 참조서* 책에 있는 TCP/IP User Exits』

주:

1. 이 주제에 대한 추가 정보는 iSeries Information Center에서 찾을 수 있습니다. 자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.

제 16 장 인터넷 브라우저에 대한 보안 고려사항

조직 내의 여러 PC 사용자는 워크스테이션에 브라우저를 갖습니다. 그들은 인터넷에 접속할 수 있습니다. 또한 사용자의 서버에도 접속할 수 있습니다. PC 및 서버에 대한 일부 보안 고려사항은 다음과 같습니다.

위험: 워크스테이션 손상

사용자가 방문하는 웹 페이지에는 Java 애플릿, Active-X 제어 또는 일부 다른 유형의 플러그 인과 같은 연관 "프로그램"이 있을 수 있습니다. 드물기는 하지만 이러한 유형의 "프로그램"은 PC에서 실행될 때 PC의 정보를 손상시킬 잠재적인 위험성을 지닙니다. 보안 관리자는 조직 내의 PC 보호를 위해 다음 사항을 고려하십시오.

- 사용자들이 가지고 있는 여러 브라우저의 보안 옵션을 이해해야 합니다. 예를 들어, 일부 브라우저를 사용하여 Java 애플릿이 브라우저 외부에서 갖는 액세스를 제어할 수 있습니다(Java의 제한된 운영 환경을 *sandbox*라고 합니다). 이로써 애플릿이 PC 자료를 손상시키지 않도록 할 수 있습니다.

  주: sandbox 개념 및 관련 보안 제한사항은 Active-X 및 다른 플러그 인에는 없습니다.
- 사용자에게 브라우저 설정에 대한 권장사항을 작성해 주십시오. 사용자들이 권장사항을 따르는지 확인할 시간이나 자원이 없을 수 있습니다. 따라서 적절하지 못한 설정으로 생길 수 있는 잠재적인 위험에 대해 사용자를 교육해야 합니다.
- 필요한 보안 옵션을 제공하는 웹 브라우저에 관한 표준화를 고려하십시오.
- 특정 웹 사이트와 연관될 수 있는 의심되는 작동 또는 징후를 알리도록 사용자에게 지시하십시오.

위험: 맵핑된 드라이브를 통한 iSeries 디렉토리 액세스

PC가 Windows용 IBM iSeries Access 세션으로 서버에 연결된다고 가정하십시오. 이 세션은 맵핑된 드라이브가 iSeries 통합 파일 시스템에 링크되도록 설정합니다. 예를 들어, PC의 **G** 드라이브는 네트워크에 있는 SYSTEM1 서버의 통합 파일 시스템에 맵핑될 수 있습니다.

이제 동일한 PC 사용자에게 브라우저가 있어서 인터넷에 액세스할 수 있다고 가정하십시오. 사용자가 Java 애플릿 또는 Active-X 제어와 같은 유해한 "프로그램"을 실행하는 웹 페이지를 요구합니다. 예상할 수 있듯이 이 프로그램은 PC의 G 드라이브에 있는 모든 것을 삭제하려 할 수 있습니다.

맵핑된 드라이브에 대한 손상에 대해 다음과 같은 보호 조치를 할 수 있습니다.

- 가장 중요한 보호는 서버상의 자원 보안입니다. Java 애플릿 또는 Active-X 제어는 PC 세션을 설정한 사용자와 같은 방식으로 서버를 취급합니다. PC 사용자가 서버에서 수행하도록 권한을 부여받는 사항을 주의깊게 관리해야 합니다.
- PC 사용자에게 맵핑된 드라이브에 액세스하지 않게 브라우저를 설정하도록 충고하십시오. 이것은 Java 애플릿에는 효력이 있으나 sandbox 개념이 없는 Active-X 제어에서는 작용하지 않습니다.
- 동일 세션에서 서버와 인터넷에 접속할 때의 위험에 관해 사용자를 교육하십시오. 또한, PC 사용자(예를 들어, Windows 95 클라이언트를 갖는 사용자)가 iSeries Access 세션이 종료된 것으로 보일 때에도 드라이브는 여전히 맵핑된 상태임을 이해하도록 하십시오.

위험: 신뢰할 수 있는 부호화 애플릿

사용자가 충고를 받아들여 애플릿이 PC 드라이브에 기록되지 못하도록 브라우저를 설정했을 수 있습니다. 그러나 PC 사용자는 *부호화 애플릿*이 브라우저에 대한 설정을 대체할 수 있다는 것을 알아야 합니다.

부호화 애플릿은 인증 설정을 위한 관련 디지털 서명을 갖습니다. 사용자가 부호화 애플릿이 있는 웹 페이지를 액세스하면 사용자에게 메세지가 표시됩니다. 이 메세지는 애플릿의 서명(부호화한 사용자와 부호화 시간)을 표시합니다. 사용자가 애플릿을 승인할 경우, 사용자는 애플릿에 브라우저에 대한 보안 설정을 대체할 권한을 부여하게 됩니다. 부호화 애플릿은 브라우저에 대한 디폴트 설정이 금지하는 경우에도 PC의 로컬 드라이브에 기록할 수 있습니다. 부호화 애플릿은 또한 서버의 맵핑된 드라이브가 PC에서 로컬 드라이브로 나타나기 때문에 맵핑된 드라이브에도 기록할 수 있습니다.

서버에서 제공되는 사용자 자신의 Java 애플릿의 경우, 부호화 애플릿을 사용할 필요가 있습니다. 그러나 사용자들에게 일반적으로 알 수 없는 소스에서 부호화 애플릿을 허용하지 않도록 지시해야 합니다.

제 17 장 관련 정보

매뉴얼

- *APPC Programming*, SC41-5443-00은 iSeries 시스템의 APPC(시스템간 프로그램 연결 통신) 지원에 대해 설명합니다. 이 책은 APPC를 사용하는 어플리케이션 프로그램 개발과 APPC 통신에 대한 통신 환경 정의를 안내합니다. 어플리케이션 프로그램 고려사항, 구성 요구사항과 명령, APPC에 대한 문제점 관리 및 일반 네트워크 고려사항 등이 포함되어 있습니다. iSeries Information Center CD-ROM을 참조하십시오.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet* 레드북, SG24-4929에서는 iSeries을 인터넷에 연결하는 것과 연관된 보안 문제 및 위험에 대해 다룹니다. 또한 TCP/IP 어플리케이션에 대한 예제, 권장사항, 추가 정보 및 기술도 제공합니다.
- *백업 및 회복*, SC41-5304-07은 백업 및 회복 전략 계획, 사용자 시스템의 정보 저장 및 이 시스템 회복에 대한 정보를 제공합니다. iSeries Information Center를 참조하십시오. 이들 주제 대한 추가 정보를 iSeries Information Center에서 찾을 수 있습니다. 자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.
- *CL 프로그래밍*, SC41-5721-06에서는 외부적으로 설명할 수 있는 파일의 DDS(자료 서술 스펙) 코드화에 대하여 자세히 설명합니다. 이러한 파일은 실제, 논리, 화면, 인쇄 및 ICF(시스템간 통신 기능) 파일입니다. iSeries Information Center를 참조하십시오.
- Information Center의 CL 주제(자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』 참조)에서 모든 iSeries 제어 언어(CL) 및 해당 OS/400 명령에 대한 설명을 다룹니다. OS/400 명령은 Operating System/400® (5722-SS1) 사용권 프로그램의 기능을 요청하는 데 사용됩니다. 다양한 모든 언어와 유틸리티를 포함하여 다른 사용권 프로그램과 연관된 OS/400 CL이 아닌 모든 명령은 해당 사용권 프로그램을 지원하는 다른 책에서 설명합니다.
- Wayne Madden과 Carol Woodbury가 작성한 *Implementing iSeries Security, 3rd Edition*. Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. iSeries 보안 계획, 설정 및 관리에 대한 지침과 실제 제안사항을 제공합니다.

  ISBN 주문 번호:

  1-882419-78-2
- HTTP 서버에 해당하는 자세한 정보는 다음 URL을 참조하십시오.

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`

- *iSeries 보안 참조서*, SC41-5302-07에서는 보안 시스템 값, 사용자 프로파일, 자원 보안 및 보안 감사에 대해 자세히 설명합니다. 이 안내서는 특정 사용권 프로그램, 언어 및 유틸리티에 대한 보안은 설명하지 않습니다. iSeries Information Center를 참조하십시오.
- Information Center의 "기본 시스템 조작" 주제에서 iSeries 기본 조작에 필요한 일부 핵심 개념과 타스크에 대한 정보를 제공합니다. 자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.
- Information Center는 TCP/IP와 FTP, SMTP 및 TELNET과 같은 여러 TCP/IP 어플리케이션을 사용하고 구성하는 방법을 설명합니다. 자세한 내용은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오.
- *OS/400용 TCP/IP 파일 서버 지원 Installation and User's Guide*, SC41-0125는 파일 서버 지원 사용권 프로그램 제공에 대한 소개 정보, 설치 지침 및 설정 프로시듀어를 제공합니다. 이 책은 제품에서 사용할 수 있는 기능을 설명하고 다른 시스템에서 사용하는 예와 요령도 설명합니다.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD는 컴퓨터 시스템에 대한 신뢰 레벨의 기준을 설명합니다. TCSEC는 미정부에서 발간한 책입니다. 이 책에는 정보 자원 리스트와 유용한 방문 사이트의 색인이 포함되어 있습니다.

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- Information Center에서 시스템 관리 및 작업 관리에 관련하여 iSeries에 대한 여러 가지 주제를 다룹니다. 이러한 일부 주제에 성능 자료 콜렉션, 시스템 값 관리 및 기억장치 관리가 들어 있습니다. Information Center 액세스에 대한 세부사항은 xii 페이지의 『요구사항 및 관련 정보』를 참조하십시오. 작업 관리 SC41-5306-03은 작업 관리 환경을 작성하고 변경하는 방법에 대한 정보를 제공합니다. iSeries Information Center를 참조하십시오.

이러한 Information Center 주제 및 보충 설명서뿐만 아니라 다음 보조 자원을 사용할 수 있습니다.

- **IBM SecureWay**
  IBM SecureWay는 고객의 정보 기술 보안에 도움이 되는 하드웨어, 소프트웨어, 상담 및 서비스와 같은 IBM의 광범위한 보안 제품 포트폴리오에 대하여 공통 상표를 제공합니다. 개별 요구를 다루거나 전사적 솔루션을 작성하든, IBM SecureWay는 비즈니스를 위한 보안 솔루션을 계획, 설계, 구현 및 작동하는 데 필요한 전문 지식을 제공합니다. IBM SecureWay 제안사항에 대한 자세한 정보를 보려면 다음 IBM SecureWay 홈 페이지를 방문하십시오.

http://www.ibm.com/secureway

- **서비스 제안사항**

  새 하드웨어 또는 소프트웨어를 설치하면 궁극적으로 사용자의 효율성 및 비즈니스 조작을 향상시킬 수 있습니다. 그러나 업무상의 혼란이나 작동 중단으로 인해 사용자가 불필요하게 내부 자원을 사용할 수 있습니다. IBM 글로벌 서비스는 iSeries 보안 관련 서비스를 제공합니다. 다음 웹 사이트에서 사용자가 iSeries의 모든 서비스 리스팅을 탐색할 수 있습니다.

  http://www.as.ibm.com/asus

주의사항

이 정보는 미국에서 제공되는 제품과 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급하는 것이 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 사용권까지 부여하는 것은 아닙니다. 사용권에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

2바이트(DBCS) 정보에 관한 사용권 문의는 한국 IBM 고객만족센터에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다. IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증없이 이 책을 현상태대로 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 이 변경사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통고없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(1) 독립적으로 생성된 프로그램이나 기타 프로그램(본 프로그램 포함)간의 정보 교환 및 (2) 교환된 정보의 상호 이용을 목적으로 정보를 원하는 프로그램 라이센스 사용자는 다음 주소로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

이러한 정보는 해당 조항 및 조건에 따라(예를 들면, 사용료 지불 포함) 사용할 수 있습니다.

이 정보에 기술된 라이센스가 있는 프로그램 및 이 프로그램에 대해 사용 가능한 모든 라이센스가 있는 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 레벨 상태의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한, 일부 성능은 추정치일 수도 있으므로 실제 결과는 다를 수 있습니다. 이 문서의 사용자는 해당 데이터를 사용자의 특정 환경에서 검증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 다른 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 배상 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM의 향후 방향 또는 의도에 관한 언급은 별도의 통지없이 변경될 수 있습니다.

이 정보는 계획 수립 목적으로만 사용됩니다. 이 책에 나오는 정보는 기술된 제품이 GA(General Availability)되기 전에 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및

제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

저작권:

이 정보에는 여러 운영 플랫폼에서의 프로그래밍 기법을 보여주는 원어로 된 샘플 응용프로그램이 들어 있습니다. 귀하는 이러한 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 추가 비용없이 이들 샘플 프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다. 이러한 샘플 프로그램은 모든 조건하에서 완전히 테스트된 것은 아닙니다. 따라서 IBM은 이들 샘플 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증하거나 암시하지 않습니다. 귀하는 IBM의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 추가 비용없이 이러한 샘플 응용프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다.

이 정보를 소프트카피로 보는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 등록상표입니다.

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e(로고)
IBM iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium 및 ProShare는 미국 또는 기타 국가에서 사용되는 Intel Corporation의 상표 또는 등록상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

Java 및 모든 Java 기반 상표는 미국 또는 기타 국가에서 사용되는 Sun Microsystems, Inc.의 상표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 Open Group의 등록상표입니다.

기타 회사, 제품 또는 서비스 이름은 해당 회사의 상표 또는 서비스표입니다.

색인

[가]

[나]

[다]

[라]

[마]

[바]

[사]

[아]

[자]

[차]

[카]

[타]

[파]

[하]

[숫자]

A

B

C

D

E

F

I

J

L

M

O

P

Q

R

S

T

U

W

[특수 문자]

IBM 한글 지원에 관한 설문

iSeries
iSeries 보안을 위한 추가 정보 및 툴
버전 5

SA30-0525-07

FAX : (02) 3787-0123

보내 주시는 의견은 더 나은 고객 지원 체제를 위한 귀중한 자료가 됩니다. 독자 여러분의 좋은 의견을 기다립니다.

성 명		직위/담당업무	
회 사 명		부 서 명	
주 소			
전화번호		팩스번호	
전자우편 주소			
사용중인 시스템	o 중대형 서버 o UNIX 서버 o PC 및 PC 서버		

1. IBM에서 제공하는 한글 책자와 영문 책자 중 어느 것을 더 좋아하십니까?
   그 이유는 무엇입니까?
   ☐ 한글 책자 ☐ 영문 책자
   (이유:)

2. 본 책자와 해당 소프트웨어에서 사용된 한글 용어에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

3. 본 책자와 해당 소프트웨어에서 번역 품질에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

4. 본 책자의 인쇄 상태에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

5. 한글 소프트웨어 및 책자가 지원되는 분야에 대해 귀하는 어떻게 생각하십니까?
   ☐ 한글 책자를 늘려야 함 ☐ 현재 수준으로 만족
   ☐ 그다지 필요성을 느끼지 않음

6. IBM은 인쇄물 형식(hardcopy)과 화면 형식(softcopy)의 두 종류로 책자를 제공합니다.
   어느 형식을 더 좋아하십니까?
   ☐ 인쇄물 형식(hardcopy) ☐ 화면 형식(softcopy) ☐ 둘 다

IBM 한글 지원 서비스에 대해 기타 제안사항이 있으시면 적어주십시오.

☺ 설문에 답해 주셔서 감사합니다.
귀하의 의견은 저희에게 매우 소중한 것이며, 고객 여러분들께 보다 좋은 제품을 제공해 드리기 위해 최선을 다하겠습니다.

SA30-0525-07