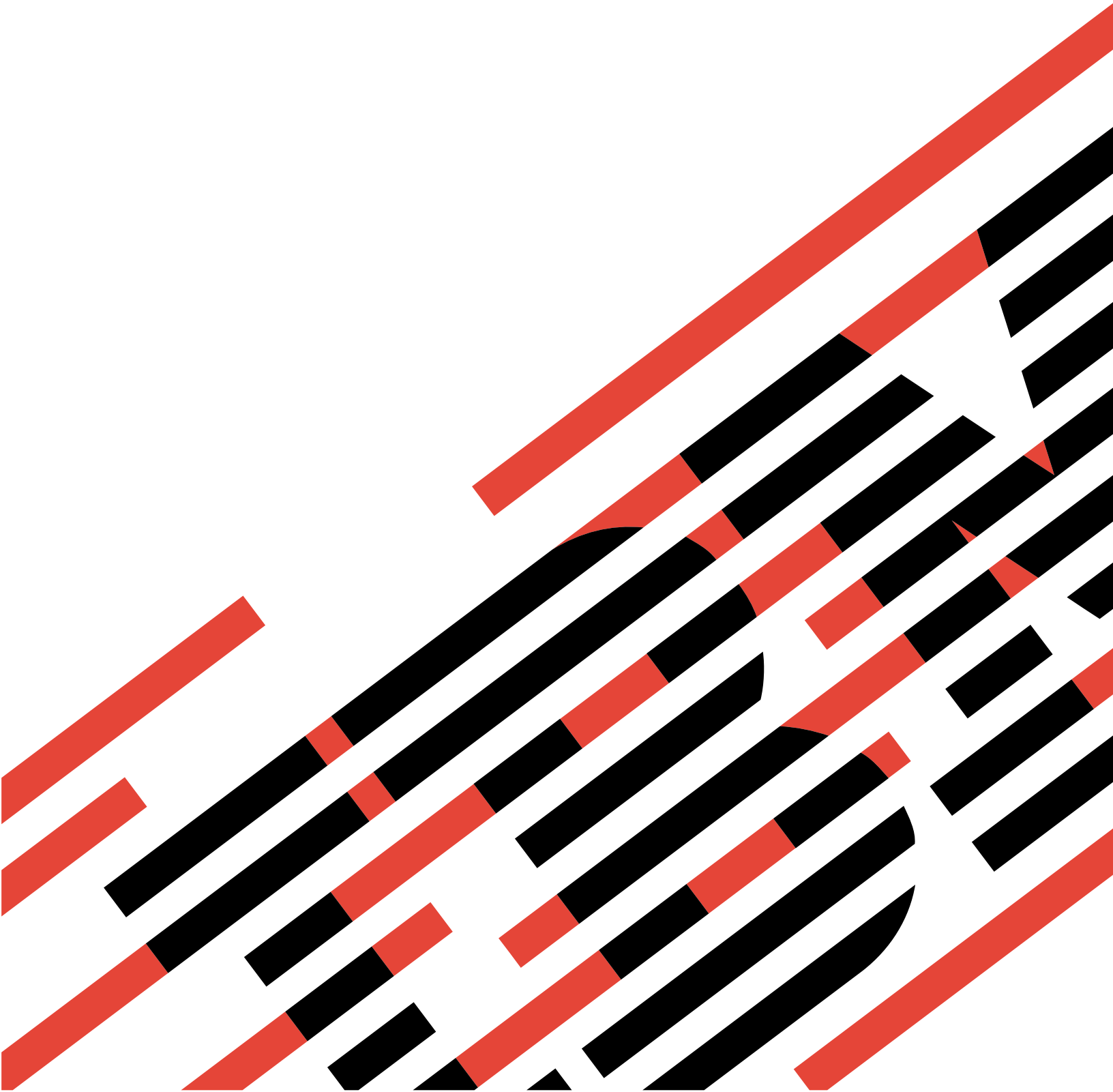
IBM

eserver

iSeries

기본 시스템 보안 및 계획



IBM

@server

iSeries

기본 시스템 보안 및 계획

목차

제 1 부 기본 시스템 보안 및 계획

기본 시스템 보안 및 계획은 iSeries 보안을 계획하고 설정하기 위한 자세한 정보를 제공합니다. 이 주제에서는 계획을 중점적으로 설명하며 보안 결정사항을 계획하고 기록할 때 사용할 수 있는 양식을 제공합니다. 또한 기본 시스템 보안을 위한 단계별 설정 지침을 제공합니다. 이 주제가 갖는 워크북으로서의 특성 때문에 내용을 인쇄하여 더 자세히 검토할 수도 있습니다.

iSeries를 위한 보안 설정은 크게 계획 타스크와 구성 타스크로 나누어집니다. 회사의 요구에 맞게 보안을 설정하기 위해서는 다음에 나오는 계획 주제를 잘 검토해야 합니다.

- 기본 시스템 보안 시작하기는 일반적인 보안 개념의 개요와 기본 시스템 보안에 관한 질의 응답을 제공합니다.
- 사용자 보안 계획은 시스템의 사용자에게 영향을 미치는 보안을 어떻게 계획할 것인지에 관한 정보를 제공합니다. 이와 같은 정보에는 물리적 보안, 어플리케이션 보안, 보안을 위한 종합적인 전략 그리고 시스템의 사용자 프로파일이 포함됩니다.
- 자원 보안 계획은 라이브러리와 라이브러리내의 오브젝트, 프린터, 프린터 출력, 워크스테이션을 포함하여 시스템의 오브젝트 보안 계획 방법에 관한 정보를 제공합니다.

계획 활동을 완료했으면 시스템의 보안 설정에 도움을 주는 다음 주제를 검토할 수 있습니다.

- 사용자 보안 설정은 사용자 및 그룹 보안을 설정하기 위한 세부사항을 제공합니다.
- 자원 보안 설정은 오브젝트에 대한 소유권, 오브젝트에 대한 공용 및 특정 권한 그리고 프린터 및 워크스테이션의 보안 설정 방법에 관한 정보를 제공합니다.
- 보안 테스트는 보안 테스트에 관한 정보를 제공합니다.
- 보안 정보 변경은 사용자 및 그룹 프로파일 그리고 자원 보안에 대한 갱신 및 수정에 관한 정보를 제공합니다.
- 보안 정보 저장은 보안 정보를 백업하는 것에 관한 정보를 제공합니다.
- 보안 모니터링은 보안 감사에 관한 정보 및 보안 추적을 위한 체크 리스트를 제공합니다.

위에 나열한 주제와 함께 전략 및 보안 결정사항을 계획할 때 계획 양식을 사용하십시오.

제 1 장 새로운 사항

V5R1에서 기본 시스템 보안 및 계획을 Information Center에 신규로 추가했습니다. 원래 이 정보는 *보안-기본*(SA30-0236-00) 책에 나오는 것입니다. 이 책을 V5R1 시스템의 보안을 설정하는 것과 관련된 현재 정보를 반영시켜서 갱신한 것입니다.

제 2 장 이 주제 인쇄

이 문서의 PDF 버전을 보거나 다운로드할 수 있습니다. PDF 파일을 보려면 Adobe® Acrobat® Reader가 설치되어 있어야 합니다. Adobe 홈 페이지  에서 사본을 다운로드 받을 수 있습니다.

PDF 버전을 보거나 다운로드하려면 기본 시스템 보안 및 계획(950KB 또는 164 페이지)을 선택하십시오.

워크스테이션에 PDF를 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 여십시오(위의 링크를 클릭하십시오).
2. 브라우저 메뉴에서 **파일**을 클릭하십시오.
3. **다른 이름으로 저장...**을 클릭하십시오.
4. PDF를 저장할 디렉토리로 이동하십시오.
5. **저장**을 클릭하십시오.

제 3 장 기본 시스템 보안 시작하기

시스템 관리자로부터 일반 사용자에 이르기까지 모두가 보안과 연관되어 있습니다. 시스템 보안은 고의로 또는 실수로 발생하는 모든 보안 침해로부터 iSeries400 및 업무상 민감한 정보를 보호합니다.

보안 환경 및 필요에 맞게 시스템 보안을 정의할 수 있습니다.

보안을 시스템을 들어가는 문으로 생각하십시오. 권한 없이 정보를 사용하는 경우가 발생하지 않도록 정보를 **잠금 처리**하거나 보호할 수 있습니다.

또한 시스템의 유연성을 **해제**시켜서 각 사용자에 맞게 정의할 수도 있습니다.

훌륭한 보안 계획이 시스템을 보호할 수는 있지만 장비나 정보의 보안을 보장할 수는 없습니다. 시스템 책임을 여러 직원들에게 분담시킴으로써 한 사람이 시스템에 대한 독점적 제어를 갖지 못하도록 해야 합니다.

기본 시스템 보안 및 계획은 기본 시스템 보안을 계획하고 설정하기 위한 단계별 접근 방식을 제공합니다. 이 주제는 시스템 보안 계획의 중요성을 강조하고 보안 결정사항을 기록할 때 사용하는 계획 양식을 제공합니다. 보안과 관련하여 결정을 내릴 때 참조할 수 있도록 이 주제에는 보안을 계획하는 한 회사의 예가 나옵니다.

시스템 보안을 성공적으로 완료하기 위해서는 신중하고 철저한 계획이 필수적입니다. 기본 보안의 필요성 및 보안 계획의 중요성에 대해 알아보려면 다음 주제를 검토하십시오.

- 기본 시스템 보안과 관련하여 자주 묻는 질문
- 기본 시스템 보안 개요
- 기본 시스템 보안 계획 방법

시스템의 모든 정보를 백업하고 회복하기 위한 훌륭한 계획도 필요합니다. 또한 재해가 발생할 경우에 대비하여 사용 중인 장비를 대체하기 위한 계획도 세워야 합니다. 훌륭한 백업 계획을 설계하기 위한 자세한 정보는 Information Center에서 백업 및 회복 주제를 참조하십시오.

사용자 보안에 관한 세부 계획 정보

다음 주제는 사용자 보안을 계획하는 방법을 제공합니다.

- 어플리케이션 보안 계획
- 보안 전략 계획
- 사용자 그룹 계획

- 개별 사용자 프로파일 계획

자원 보안에 관한 세부 계획 정보

다음 주제는 사용자를 위한 자원 보안을 계획할 때의 체계적인 접근방식을 제공합니다.

- 권한 유형 이해
- 어플리케이션 라이브러리 보안 계획
- 라이브러리 및 오브젝트 소유권 판별
- 오브젝트 그룹화
- 프린터 출력 보호
- 워크스테이션 보호
- 어플리케이션 설치 계획

인쇄 가능한 계획 양식

기본 시스템 보안 및 계획은 보안 결정사항 모두를 기록할 수 있는 인쇄 가능한 계획 양식을 제공합니다. 브라우저의 인쇄 버튼을 사용하여 전체 주제를 PDF로 인쇄하거나 개별 계획 양식을 인쇄할 수 있습니다.

기본 시스템 보안을 위한 단계별 설정 지침

이 주제는 보안 계획을 완료한 후 보안 계획을 적용하기 위한 단계를 제공합니다. 다음 주제는 시스템 보안을 설정할 때 도움을 줍니다.

- 사용자 보안 설정
- 자원 보안 설정

기본 시스템 보안에 관해 자주 묻는 질문

보안에 관해 자주 묻는 질문에 나오는 응답을 검토해보면 시스템 보안의 중요성을 잘 이해할 수 있습니다.

보안은 왜 중요한가?

시스템에 저장된 정보는 가장 중요한 업무 자산 중 하나입니다. 정보 자산을 보호하는 방법에 대해 생각할 때 다음의 세 가지 중요한 목적을 명심하십시오.

- **기밀성:** 훌륭한 보안 조치는 사용자들이 기밀 정보를 보거나 유출시키지 못하게 할 수 있습니다.
- **무결성:** 잘 설계된 보안 시스템은 컴퓨터에 있는 정보의 정확성을 어느 정도 보장할 수 있습니다. 권한 보안을 이용하여 권한이 없이는 자료를 변경하거나 삭제하지 못하게 할 수 있습니다.

- **가용성:** 누군가 실수로 또는 고의로 시스템의 자료를 손상시킨 경우 자료가 회복되기까지는 해당 자원에 액세스할 수 없습니다. 훌륭한 보안 시스템은 이러한 유형의 손상을 방지할 수 있습니다.

사람들이 시스템 보안에 대해 생각할 때 보통은 회사 외부(예: 경쟁사)로부터 시스템을 보호하는 것을 생각합니다. 실제로는 적절한 사용자의 호기심이나 시스템 사고로부터 보호하는 것이 잘 설계된 보안 시스템의 가장 큰 장점입니다. 훌륭한 보안 기능이 없는 시스템에서는 중요한 파일을 무심코 삭제할 수 있습니다. 잘 설계된 보안 시스템이라면 이와 같은 유형의 사고를 방지하는 데 도움이 됩니다.

시스템을 어느 정도로 보안시켜야 할지를 판별할 때 스스로에게 다음 질문을 해보십시오.

- 컴퓨터(및 컴퓨터에 저장한 자료)가 내 업무에 얼마나 중요한가?
- 일정한 보안 수준을 필요로 하는 회사 정책이 있는가?
- 감사자가 컴퓨터에 저장된 정보의 보안 레벨을 요구하는가?
- 가까운 장래에 일정 수준의 보안이 필요한가?

왜 시스템을 사용자 정의하는가?

iSeries는 광범위한 사용자를 수용합니다. 소형 시스템에는 소수의 어플리케이션을 실행하는 3-5명의 사용자가 있을 수 있습니다. 대형 시스템에는 많은 어플리케이션을 실행하는 대규모의 통신 네트워크에 수천명의 사용자가 있을 수 있습니다.

iSeries 설계는 광범위한 사용자 및 상황들을 수용할 수 있는 유연성을 제공합니다. 시스템이 사용자에게 어떻게 보이는지 그리고 시스템이 어떻게 수행되는지에 관한 많은 것을 변경할 기회가 있습니다.

시스템을 처음 받았을 경우 아마도 사용자 정의가 필요가 없거나 많은 부분을 정의하지는 않을 것입니다. IBM은 다양한 옵션에 대해 **디폴트**라는 초기 설정으로 시스템을 공급합니다. 보통 이 디폴트는 신규 설치에 있어서 최적의 작업을 위한 선택입니다.

주: 모든 신규 시스템들은 **40**의 디폴트 보안 레벨로 제공됩니다. 이 보안 레벨은 정의된 사용자만 시스템을 사용할 수 있는 레벨입니다. 이것은 또한 보안을 피해갈 수 있는 프로그램으로부터의 잠재적인 무결성이나 보안상의 위협을 방지하기도 합니다.

그러나 약간의 사용자 정의를 통해 시스템을 사용자를 위한 더 간단하고 효과적인 툴로 만들 수 있습니다. 한 예로 사용자가 사인 온할 때 항상 올바른 메뉴를 사용하도록 만들 수 있습니다. 각 사용자의 보고서를 올바른 프린터로 보낼 수 있습니다. 약간의 사용자 정의를 통해 시스템이 사용자 자신의 시스템인 것처럼 보고 느끼게 할 수 있다면 사용자들이 시스템에 대해 더욱 확신을 가질 것입니다.

책임자는 누구인가?

회사마다 보안에 대해 서로 다른 접근방식을 사용할 수 있습니다. 경우에 따라서는 프로그래머들이 모든 보안 요소에 대해 책임을 지는 경우가 있습니다. 또는 시스템을 관리하는 사람이 보안을 담당하기도 합니다. 어떻게 책임을 지정해야 할지 확신이 없는 사람들을 위해 한 가지 제안을 합니다.

- 자원 보안 계획 방법은 자사에서 어플리케이션을 개발하는지 아니면 외주를 주는지에 따라 다릅니다. 자체적으로 어플리케이션을 개발할 경우에는 개발 프로세스 내내 자원 보안 요구를 전달하십시오. 외주를 줄 경우에는 어플리케이션 설계자와 함께 작업하십시오. 어느 경우에서나 어플리케이션을 설계하는 사람들이 보안을 설계의 일부로 고려해야 합니다.
- 보안 설정은 보안 담당자의 책임입니다. 보안 담당자가 시스템 사용자 및 그 시스템에 대한 사용자 액세스를 정의합니다. 보안 담당자가 시스템의 기타 요소(예: 정보 백업 및 회복)에 대한 책임도 지는 경우가 많습니다.
- 시스템 사용자 정의에 있어서 많은 보안 요소들이 중요한 역할을 하므로 보안 담당자가 시스템도 사용자 정의해야 합니다.

보안 책임을 지정할 때 사용하는 방법이 어떤 것이든 **보안 정책을 알리십시오.** 회사의 최고 책임자가 모든 사람에게 컴퓨터에 저장된 정보가 회사의 중요한 자산임을 알려야 합니다(가능하면 서면으로). 다른 회사 자산과 마찬가지로 그 정보를 보호해야 합니다. 보안 정책의 예는 ″예: JKL Toy사의 보안 정책″을 참조하십시오.

시스템에 보안이 필요한 이유를 이해했으므로 이제 시스템 보안 고려사항의 개요를 검토하겠습니다.

기본 시스템 보안 개요

효과적으로 계획하기 위해서는 달성하려는 것의 목적이 시스템에서 제공하는 툴과 어떻게 관련되어 있는지를 이해해야 합니다. 또한 목적을 달성하기 위해서는 사용자와 시스템 피처가 어떻게 공동으로 작업하는지를 알아야 합니다.

다음 주제에서는 보안 및 사용자 정의에 관한 중요한 정보와 이들이 함께 어떻게 맞물려 있는지에 관해 알아봅니다. 다음 주제들은 계획을 세우기 전에 개요를 제공하기 위한 것입니다. 계획 프로세스에서 필요에 따라 여기에 나오는 모든 개념들을 더 자세히 설명합니다.

- 내장형 시스템 보안
- 기본 용어
- 사용자 관점에서의 보안
- 보안 및 사용자 정의를 위한 시스템 툴

내장형 시스템 보안

시스템쪽의 모든 보안 요소들은 시스템에 빌드되어 있습니다. 따라서 별도로 구매하지 않아도 됩니다. 이와 같은 통합 접근방식에는 몇 가지 장점이 있습니다.

- 보안은 나머지 오퍼레이팅 시스템과 일관성이 있습니다. 즉, 같은 화면, 명령, 용어를 사용합니다.
- 보안이 분리되어 있는 소프트웨어가 아니기 때문에 바이패스할 수 없습니다.
- 적절하게 설계된 보안은 성능에 거의 영향을 주지 않습니다.
- 보안이 항상 신규 소프트웨어 개발과 보조를 맞춥니다. 즉, 새로운 기능을 사용할 수 있을 때 그 기능에 대한 보안도 사용할 수 있습니다.

iSeries에서는 권한이 없으면 시스템을 시작할 수 없게 만드는 보안 레벨 40을 제공합니다. 이것은 보안을 피해가면서 접근할 수 있는 프로그램으로부터 무결성이나 보안 위험의 노출 가능성을 방지합니다. 그러나 특정 보안 설정값을 조정하거나 보안 레벨을 변경할 수 있습니다. 보안 레벨에 대한 설명은 "보안 레벨 선택" 주제를 참조하십시오.

지금까지 내장형 보안의 작업 방식에 관해 설명했으며 계속해서 일반적인 iSeries 용어에 관해 알아보겠습니다.

기본 용어

이 일반적인 용어 세트는 iSeries 보안을 이해하는 데 매우 중요합니다.

오브젝트

오브젝트는 시스템에 명명된 하나의 공간으로서 조작이 가능합니다. 가장 일반적인 오브젝트의 예로는 파일과 프로그램이 있습니다. 기타 오브젝트 유형으로는 명령, 대기행렬, 라이브러리, 폴더가 있습니다. 시스템에서 오브젝트는 오브젝트명, 오브젝트 유형, 오브젝트가 상주하는 라이브러리로 식별됩니다. 시스템의 각 오브젝트를 보안시킬 수 있습니다.

라이브러리

라이브러리는 기타 오브젝트들을 그룹화하는 데 사용되는 특별한 오브젝트 유형입니다. 시스템에 있는 많은 오브젝트들이 라이브러리에 상주합니다.

디렉토리

디렉토리는 시스템의 오브젝트를 그룹화하는 또 하나의 방법입니다. 여러 오브젝트가 하나의 디렉토리에 상주할 수 있습니다. 하나의 디렉토리가 하나의 계층 구조를 형성하면서 또 다른 디렉토리에 상주할 수 있습니다.

지금까지 일반적인 iSeries 보안 용어에 관해 설명했으며 계속해서 사용자 관점의 보안에 관해 알아보겠습니다.

사용자 관점에서의 보안

사용자 관점에서 보안은 시스템에서 타스크를 사용하고 완료하는 방법에 영향을 미칩니다. 또한 보안에는 그와 같은 타스크를 완료하기 위해 사용자들이 시스템과 대화하는 방법이 포함되어 있습니다. 사용자 관점의 보안을 고려하는 것은 중요합니다. 예를 들어, 암호 만기일을 5일로 설정하면 사용자들이 작업을 완료하는 것을 방해하거나 당황스럽게 만들 수 있습니다. 반면에 암호 정책이 너무 느슨하면 보안 문제를 발생시킬 수 있습니다.

시스템에 맞는 보안을 제공하기 위해서는 보안을 계획, 관리, 모니터할 수 있는 특정 부분으로 세분화시켜야 합니다. 사용자 관점에서 시스템 보안을 다음과 같이 여러 부분으로 나눌 수 있습니다.

시스템에 대한 물리적 액세스

물리적 보안은 시스템 장치, 모든 시스템 장치, 백업 기억장치 매체(예: 디스켓, 테이프 또는 CD)가 실수로나 아니면 고의로 유실 또는 손상되지 않도록 보호합니다.

시스템의 물리적 보안을 위해 취하는 대부분의 조치는 시스템 외부에서 이루어집니다. 또한 권한이 없이는 시스템 장치의 기능을 사용하지 못하도록 키 잠금 장치나 전자 키 스틱과 함께 시스템을 제공합니다.

″물리적 보안 계획″ 주제에 시스템의 물리적 보안 계획에 도움이 되는 자세한 정보가 나옵니다.

사용자의 사인 온 방법

사인 온 보안은 시스템에서 식별할 수 없는 사용자들은 사인 온하지 못하게 해줍니다. 사인 온하기 위해서는 개개인이 유효한 사용자 ID와 암호를 반드시 입력해야 합니다.

사인 온 보안을 위반하지 않도록 하기 위해 시스템 값과 개별 사용자 프로파일 모두를 사용할 수 있습니다. 예를 들어, 암호를 정기적으로 변경하도록 할 수 있습니다. 또한 추측하기 쉬운 암호는 사용하지 못하도록 할 수 있습니다.

사용자가 수행할 수 있는 작업

보안 및 시스템 사용자 정의에 있어서 중요한 역할은 사용자가 수행할 수 있는 것을 정의하는 것입니다. 보안 관점에서 볼 때 이것은 사용자들이 특정 정보를 보지 못하도록 기능을 **제한**하는 것입니다. 시스템 사용자 정의 관점에서 볼 때 이것은 **권한을 부여하는** 기능입니다. 올바로 사용자 정의가 이루어진 시스템은 불필요한 타스크와 정보를 제거하여 사람들이 작업을 잘 수행할 수 있게 해줍니다.

사용자들이 수행할 수 있는 작업을 정의하기 위한 몇 가지 방법들은 보안 담당자에게 해당하는 하는 것인 반면에 다른 방법들은 프로그래머의 책임입니다. 이 정보는 주로

보안 담당자가 일반적으로 수행하는 방법에 촛점을 맞추었습니다. *보안 참조서* (SA30-0237)의 3장, ″보안 시스템 값″에서 모든 시스템 값의 설명을 볼 수 있습니다.

개별 사용자 프로파일, 작업 설명, 클래스에 나오는 매개변수를 사용하여 사용자가 시스템에서 수행할 수 있는 작업을 제어할 수 있습니다. 아래 리스트는 사용할 수 있는 기법을 간략히 설명한 것입니다.

사용자를 몇 가지 기능으로 제한

사용자 프로파일을 기초로 사용자들을 특정 프로그램, 메뉴 또는 메뉴 세트, 몇 가지 시스템 명령으로 제한할 수 있습니다. 보통은 보안 담당자가 사용자 프로파일을 작성하고 제어합니다.

시스템 기능 제한

시스템 기능은 정보를 저장 및 복원하고 프린터 출력을 관리하며 신규 시스템 사용자를 설정할 수 있게 해줍니다. 각 사용자 프로파일이 그 사용자가 수행할 수 있는 가장 일반적인 시스템 기능 중 하나를 지정합니다.

iSeries 시스템에서는 제어 언어(CL) 명령과 어플리케이션 프로그래밍 인터페이스(API)를 사용하여 시스템 기능을 수행할 수 있습니다. 각각의 명령과 API가 하나의 오브젝트이므로 오브젝트 권한을 사용하여 시스템 기능을 사용하고 완료할 수 있는 사용자를 제어할 수 있습니다.

파일 및 프로그램 사용자 판별

자원 보안은 시스템에서 각 오브젝트의 사용을 제어하는 기능을 제공합니다. 어느 오브젝트에 대해서나 오브젝트 사용자 및 그 사용 방법을 지정할 수 있습니다. 예를 들면, 한 사용자는 파일의 정보를 보기만 할 수 있고 또 다른 사용자는 파일의 자료를 변경할 수 있으며 세 번째 사용자는 파일을 변경하거나 전체 파일을 삭제할 수 있도록 지정할 수 있습니다.

시스템 자원 남용 방지

시스템에서의 처리 능력은 시스템에 저장하는 자료 만큼 업무에 중요할 수 있습니다. 보안 담당자는 사용자들이 높은 우선순위의 작업을 실행하고, 보고서를 먼저 인쇄하게 하거나 디스크 기억장치를 너무 많이 사용하여 시스템 자원을 남용하지 않도록 도와줍니다.

시스템이 다른 컴퓨터와 통신하는 방법

시스템이 다른 컴퓨터나 프로그래밍 가능 워크스테이션과 통신하면 추가적인 보안 조치가 필요합니다. 적절한 보안 제어가 없으면 네트워크의 다른 컴퓨터에서 누군가가 사인온 프로세스를 거치지 않고 컴퓨터에 있는 정보에 액세스하거나 작업을 시작할 수 있습니다.

시스템 값과 네트워크 속성 모두를 사용하여 시스템에서 리모트 작업, 리모트 자료 액세스 또는 리모트 PC 액세스를 허용하는지의 여부를 제어할 수 있습니다. 리모트 액세

스를 허용할 경우 시행할 보안을 지정할 수 있습니다. *보안 참조서*(SA30-0237)의 3장, ″보안 시스템 값″에서 모든 시스템 값의 설명을 볼 수 있습니다.

보안 정보 저장 방법

시스템의 정보는 정기적으로 백업시켜야 합니다. 시스템의 자료를 저장하는 것 외에도 보안 정보를 저장해야 합니다. 재해가 발생할 경우 시스템 사용자, 권한 부여 정보에 관한 정보, 정보 자체를 회복시킬 수 있어야 합니다.

″보안 정보 저장″ 주제에서 보안 정보 저장 방법을 설명합니다. Information Center의 백업 및 회복 주제에서 보안 자료 백업 및 회복에 대한 자세한 정보를 제공합니다.

보안 계획 모니터 방법

시스템에서 보안 효율성을 모니터하기 위한 몇 가지 툴을 제공합니다.

- 특정 보안 위반이 발생할 때 시스템 오퍼레이터에게 메세지를 송신합니다.
- 다양한 보안 관련 트랜잭션을 특별한 감사 저널에 기록합니다.

″보안 모니터링″ 주제는 이 툴의 사용법을 일반적인 용어로 설명합니다. *보안 참조서* (SA30-0237)의 9장, ″시스템상의 보안 감사″에서 보안 감사에 관한 자세한 설명을 볼 수 있습니다.

시스템 사용자 정의 방법을 잘 이해하려면 사용자 관점에 나오는 사용자 정의를 잘 알아야 합니다.

사용자 관점의 시스템 사용자 정의

사용자가 일일 작업을 완료하는 데 도움이 되도록 시스템을 사용자 정의할 수 있습니다. 사용자에게 맞도록 시스템을 사용자 정의하기 위해서는 성공적인 작업을 위해 필요한 것이 무엇인지를 생각하여야 합니다. 여러 가지 방법으로 메뉴와 어플리케이션을 표시하도록 시스템을 사용자 정의할 수 있습니다.

사용자들이 원하는 것을 표시

대부분의 사람들은 자신이 가장 필요로 하는 것에 쉽게 접근할 수 있도록 책상이나 사무실을 배열합니다. 시스템 액세스도 같은 방식으로 고려하십시오. 시스템에 사인 온했으면 자신이 가장 많이 사용하는 메뉴나 화면을 처음에 볼 수 있어야 합니다. 이와 같이 할 수 있도록 사용자 프로파일을 쉽게 설계할 수 있습니다.

불필요한 것 제거

대부분의 시스템에는 서로 다른 여러 어플리케이션들이 있습니다. 그러나 대부분의 사용자들은 작업에 필요한 것만 보기를 원합니다. 사용자를 시스템의 몇 가지 기능으로 제한하면 작업이 훨씬 수월해집니다. 사용자 프로파일, 작업 설명, 적절한 메뉴로 각 사용자에게 시스템에 대한 특정 보기를 제공할 수 있습니다.

적합한 장소로 송신

사용자들이 자신의 보고서를 올바른 프린터로 보내기 위한 방법이나 일괄처리 작업을 실행하는 방법에 관해 걱정해서는 안됩니다. 시스템 값, 사용자 프로파일, 작업 설명이 이와 같은 일을 합니다.

지원 제공

시스템 사용자 정의가 올바로 이루어졌더라도 사용자들이 여전히 ″내 보고서가 어디로 갔지?″ 또는 ″내 작업이 벌써 끝났을까?″라고 궁금해 할 수 있습니다. **운영 지원** 화면에서 시스템 기능에 대한 단순한 인터페이스를 제공함으로써 이와 같은 의문사항들을 해결해줍니다. **지원 레벨**이라고 하는 여러 버전의 시스템 화면들을 통해 기술적 경험이 서로 다른 사용자들에게 도움을 제공합니다. 시스템을 받는 즉시 모든 사용자들이 자동으로 운영 지원 화면을 사용할 수 있습니다. 그러나 어플리케이션 설계상 사용자가 운영 지원 메뉴에 액세스하는 방법을 변경해야 할 수도 있습니다.

iSeries에서는 사용자들이 자원에 액세스하는 동안 시스템 보안을 사용자 정의하여 자원을 보호할 수 있는 시스템 툴을 제공합니다.

보안 및 사용자 정의를 위한 시스템 툴

효율적으로 계획하기 위해서는 사용자 관점의 보안 목적이 시스템이 제공하는 툴과 어떻게 관련되어 있는지를 이해해야 합니다. 이 시스템 툴을 사용하여 시스템에 보안을 사용자 정의할 수 있습니다.

보안 레벨

IBM은 모든 신규 iSeries에 보안 레벨 40을 제공합니다. 보안 레벨 40은 암호 및 자원 보안 그리고 시스템 무결성을 제공합니다. 시스템에서 활동 보안 레벨을 변경하기 위해 QSECURITY 시스템 값을 변경할 수 있습니다. 그러나 IBM에서는 보안 레벨을 40으로 설정할 것을 강력히 권장합니다. 보안 레벨을 변경하기 위해서는 사용자에게 *SECOFR 사용자 클래스나 *ALLOBJ 및 *SECADM 특수 권한이 필요합니다.

시스템은 아래 표에서와 같이 네 개의 보안 레벨을 제공합니다.

표 1. 시스템에서 사용할 수 있는 보안 레벨

보안 레벨	설명
보안 레벨 20	암호 보안만 제공
보안 레벨 30	암호 및 자원 보안 제공
보안 레벨 40	암호 및 자원 보안, 무결성 보안 제공
보안 레벨 50	암호 및 자원 보안, 향상된 무결성 보호 제공

″보안 레벨 선택″ 주제에서는 사용자 요구에 적합한 최적의 보안 레벨을 판별하는 방법에 관해 자세히 설명합니다.

시스템 값

오퍼레이팅 시스템의 특정 피처가 iSeries에서 작동하는 특정 피처를 제어하기 위한 시스템 값을 설정할 수 있습니다. 시스템 값을 회사 정책으로 생각하십시오. 시스템 값은 보다 세부적인 요소(예: 사용자 프로파일)가 시스템 값을 대체하지 않는 한 시스템을 사용하는 모든 사람에게 적용됩니다.

시스템 값은 기본 프린터, 시스템이 날짜를 표시하는 방법, 암호를 변경해야 하는 빈도 수 등을 판별합니다.

네트워크 속성

네트워크 속성은 시스템이 퍼스널 컴퓨터를 포함하여 다른 컴퓨터들과 어떻게 통신하는지에 관한 몇 가지 특성을 정의합니다. 네트워크 속성은 전체 시스템에 적용됩니다.

그룹 프로파일

그룹 프로파일이 사용자 그룹을 정의합니다. 그룹 프로파일을 부서의 정책으로 생각하십시오. 그룹 프로파일을 개별 사용자 프로파일을 작성하기 위한 하나의 패턴으로 사용할 수 있습니다. 또한 그룹 프로파일을 사용하여 그룹 멤버들이 시스템의 오브젝트에 액세스할 수 있는 방법을 정의할 수도 있습니다. 그룹 프로파일에 대한 자세한 정보는 ″사용자 그룹 계획″ 주제를 참조하십시오.

사용자 프로파일

사용자 프로파일은 시스템에서 가장 강력하고 그 용도가 다양한 오브젝트 중 하나입니다. 사용자 프로파일에는 암호 그리고 사용자가 사인 온한 후 보게 되는 메뉴 등이 들어 있습니다. 사용자 프로파일이 시스템에서 할 수 있는 일과 할 수 없는 일을 정의합니다. 즉 시스템에 대한 사용자 고유의 보기를 결정합니다. ″사용자 보안 계획″ 주제에서 사용자 프로파일 계획을 위한 추가 정보를 설명합니다.

작업 설명

작업 설명은 시스템이 사용자의 작업을 처리하는 방법을 결정하기 위해 시스템 값과 사용자 프로파일을 이용하여 작업합니다. 작업 설명이 사용자의 초기 라이브러리 리스트를 설정하며 그 초기 라이브러리 리스트가 사용자가 사인 온한 후 자동으로 액세스할 수 있는 라이브러리를 결정합니다.

자원 보안

보안 담당자는 자원 사용 권한을 가진 사용자와 그 사용자가 이 오브젝트(자원)에 액세스 하는 방법을 판별함으로써 시스템의 자원(오브젝트)을 보호합니다. 보안 담당자가 개별 오브젝트나 오브젝트 그룹(권한 부여 리스트)에 대해 오브젝트 권한을 설정할 수

있습니다. 파일, 프로그램, 라이브러리는 보호가 필요한 가장 일반적인 오브젝트이지만 사용자가 시스템 보안을 이용하여 시스템의 임의 오브젝트에 대해 오브젝트 권한을 설정할 수 있습니다.

일반적이면서 복잡하지 않은 접근방식을 사전에 계획하여 자원 보안을 간단하고 효과적으로 관리할 수 있습니다. 사전 계획없이 작성된 자원 보안 체계는 복잡하고 비효과적일 수 있습니다. ″자원 보안 계획″ 주제에서 자원 보안 계획 방법을 설명합니다.

시스템에서 복잡하지 않은 자원 보안 체계를 계획을 설계할 때 도움이 되는 몇 가지 툴을 제공합니다.

- **그룹 프로파일:** 하나의 그룹 프로파일하에 유사한 사용자들을 그룹화할 수 있습니다. 이 경우 사용자 그룹이 오브젝트에 대해 모두 같은 권한을 공유할 수 있습니다.
- **권한 부여 리스트:** 하나의 리스트에 유사한 보안 요구를 가진 오브젝트를 그룹화할 수 있습니다. 이 경우 개별 오브젝트가 아닌 그 리스트에 권한을 부여할 수 있습니다.
- **오브젝트 소유권:** 시스템의 모든 오브젝트에는 소유자가 있습니다. 그룹 프로파일 또는 개별 사용자가 오브젝트를 소유할 수 있습니다. 오브젝트 소유권을 적절히 할당하면 (1)어플리케이션을 관리하고 (2)정보 보안 책임을 위임할 때 도움이 됩니다.
- **1차 그룹:** 한 오브젝트에 1차 그룹 권한을 지정할 수 있습니다. 시스템은 그 오브젝트와 함께 1차 그룹 권한을 저장합니다. 1차 그룹 권한을 사용하면 권한 관리를 단순화하고 권한 검사 성능을 향상시킬 수 있습니다.
- **라이브러리 권한:** 보호가 필요한 파일과 프로그램을 라이브러리에 넣고 그 라이브러리에 대한 액세스를 제한할 수 있습니다. 이것이 각각의 개별 오브젝트에 대해 액세스를 제한하는 것보다 훨씬 간단할 수 있습니다. 중요한 오브젝트를 보호하기 위해서 오브젝트와 라이브러리 모두를 보안시킬 수도 있습니다.
- **오브젝트 권한:** 라이브러리에 대해 액세스를 제한하지 않는 상태에서 라이브러리에 대한 액세스를 충분히 세분화하지 않은 경우 개별 오브젝트(예: 파일)에 대한 권한을 제한할 수 있습니다.
- **공용 권한:** 각 오브젝트의 경우 그 오브젝트에 대해 다른 특별한 권한이 없는 시스템 사용자가 이용할 수 있는 액세스 종류를 정의할 수 있습니다. 공용 권한은 기밀사항이 아닌 오브젝트를 보안하기 위한 효과적인 방법으로서 시스템 성능을 향상시킵니다.
- **디렉토리 권한:** 라이브러리 권한을 사용하는 것과 같은 방법으로 디렉토리 권한을 사용할 수 있습니다. 디렉토리 안의 오브젝트들을 그룹화할 수 있으며 개별 오브젝트가 아닌 디렉토리를 보안할 수 있습니다.
- **권한 홀더:** 오브젝트를 삭제할 때 해당 오브젝트에 대한 권한 정보도 삭제하십시오. 권한 홀더가 어플리케이션을 삭제한 후 재작성한 프로그램 정의 파일의 권한 정보를 유지보수합니다. System/36으로부터의 마이그레이션을 지원하는 권한 홀더를 사용할 수 있습니다.

보안 툴

iSeries의 보안 환경을 관리하고 모니터하는 것을 도와주는 보안 툴을 사용할 수 있습니다. 다음은 사용자 프로파일 툴을 사용하여 할 수 있는 작업입니다.

- 디폴트 암호를 가진 사용자 프로파일을 찾습니다.
- 특정 시간이나 요일에 사용할 수 없도록 사용자 프로파일을 스케줄링합니다.
- 직원이 퇴사할 때 사용자 프로파일이 제거되도록 스케줄링합니다.
- 특수 권한이 있는 사용자 프로파일을 찾습니다.
- 시스템에서 오브젝트에 대한 권한이 허용되는 사용자를 찾습니다.

오브젝트 보안 툴을 사용하여 기밀 오브젝트와 연관된 공용 권한 및 개인 권한을 추적할 수 있습니다. 또한 다음과 같은 보고서를 정기적으로(예: 월간) 인쇄하여 보안 처리의 초점을 현재 문제에 맞출 수 있습니다. 마지막으로 실행한 이후의 변경사항만 표시하도록 보고서를 실행할 수도 있습니다.

다음은 기타 툴에서 제공하는 모니터 기능입니다.

- 트리거 프로그램
- 통신 항목, 서브시스템 설명, 출력 대기행렬, 작업 대기행렬, 작업 설명에 나오는 보안 관련 값
- 변경되거나 손상된 프로그램

지금까지 시스템 보안의 중요성을 설명했습니다. 다음에는 이 주제에서 예로 사용하는 계획 방법에 관해 설명하겠습니다.

기본 시스템 보안 계획 방법

보안 설계는 외부에서 내부로, 일반 범주에서 특정 범주로 이동해 나가면서 계획하십시오. 예를 들어, 프로파일을 계획할 경우 우선 사용자가 보아야 할 것(외부)을 생각하십시오. 그런 다음 볼 수 있는 방법(내부)을 결정해야 합니다.

먼저 시스템 값 및 그룹 프로파일(일반)을 계획한 후 개별 사용자에 대한 예외(특정) 조건을 결정하십시오.

"사용자 보안 계획"에 나오는 타스크를 순서대로 완료하십시오. 이 계획 단계에서는 시스템 사용 계획을 어떻게 세워야 하는지 그리고 어떻게 보안하고 조정할 것인지를 설명하기 위한 논리적인 처리 방식을 제공합니다. 이 주제에서는 보안 결정사항 및 이행 기록을 제공하는 계획 작업용지를 사용하십시오. 이 작업용지를 안전한 곳에 보관하십시오. 나중에 보안을 설정할 때 각 주제별로 작업용지에 수집했던 정보가 도움이 됩니다.

시스템 보안을 계획하고 설계할 경우 가장 기본적인 것에서부터 시작하십시오. 가장 기본적인 보안 형태에서 시작하여 더 복잡한 보안 문제를 해결하십시오. 사용 중인 시스

템의 물리적인 보안을 시작으로 어플리케이션과 시스템 값을 설명하는 방식으로 진행하십시오. 마지막으로, 시스템의 모든 사용자와 오브젝트에 대한 보안을 고려해야 합니다.

계획 주제를 검색하는 동안 이와 같은 접근 방식을 사용하는 JKL Toy사의 예를 볼 수 있을 것입니다. 물론 이 회사는 가상의 회사이지만 실제로 존재하는 많은 회사들과 유사합니다. ″예: JKL Toy사 소개″에서 이 회사에 관해 설명합니다.

예: JKL Toy사 소개

예를 보면 쉽게 이해할 수 있을 것입니다. 이 점을 기억하고, 이 주제에서는 JKL Toy사를 예로 사용합니다. 작지만 급속히 확장 중에 있는 JKL Toy사는 iSeries 시스템에 보안을 설정하기를 원합니다. John Smith 사장은 신규 iSeries 시스템이 JKL Toy사의 폭발적인 성장으로 인한 부담을 해결해 주기를 원하고 있습니다.

John은 회계 관리자인 Sharon Jones에게 시스템 관리자 및 보안 담당자의 책임을 부여했습니다. Sharon Jones는 보안을 포함하여 전체적인 설치를 무리없이 완료시켜야 합니다. Sharon은 계획이 얼마나 중요한지를 잘 알고 있습니다. 현재 이 회사는 규모가 작아 직원 대부분이 거의 모든 정보에 액세스합니다. 그러나 Sharon은 회사가 성장함에 따라 상황이 변할 것이라는 점을 알고 있습니다. 따라서 처음부터 모든 것이 올바로 처리되기를 원합니다.

처음에 JKL Toy사는 시스템에서 고객 주문 관리, 재고 관리, 계약 및 가격 관리, 미수금 관리와 같은 어플리케이션을 실행하기로 계획합니다. 그러나 계획 주제를 읽어가면서 JKL Toy사가 보안을 어떻게 처리하는지에 관해 더 많은 것을 알게 될 것입니다.

″계획 처리의 각 단계″ 주제에서는 시스템 보안을 계획할 때 따라야 할 각 단계를 설명합니다.

보안 계획 프로세스의 각 단계

다음 도표에서는 계획 프로세스의 각 단계를 설명하고 그 단계와 프로세스의 나머지 단계가 어떤 관계에 있는지를 설명합니다.

표 2. 보안 계획 프로세스의 각 단계

단계	이 단계에서 수행할 일	이 단계에서 서로 관련된 방식
물리적 보안 계획	시스템 장치, 각 장치, 백업 매체의 보호 계획 방법을 설명하십시오.	이 정보의 대부분은 나머지 프로세스와 무관합니다. 물리적 보안 계획 정보를 시스템에 입력할 필요는 없으나 시스템 값 및 자원 보안을 계획할 때 이 정보 중 일부가 필요합니다.
어플리케이션 계획	모든 어플리케이션의 목적, 기본 메뉴, 라이브러리를 설명하십시오.	나머지 계획 프로세스 및 다른 보안 결정사항을 위한 기초를 제공합니다. 이 정보는 시스템에 입력하지 않아도 됩니다.

표 2. 보안 계획 프로세스의 각 단계 (계속)

단계	이 단계에서 수행할 일	이 단계에서 서로 관련된 방식
종합적인 접근 계획	보안에 대한 종합적인 접근방식을 결정하십시오. 그 접근방식을 지원하는 시스템 값을 선택하십시오.	종합적인 접근방식을 결정할 경우 어플리케이션 계획 정보를 참조하십시오. 선택한 시스템 값이 사용자 및 그룹 프로파일 계획 방법에 영향을 미칩니다.
사용자 그룹 계획	사용자를 그룹으로 나눌 방법을 결정하십시오. 각 그룹의 특성을 결정하고 시스템에 특성을 정의하는 방법을 결정하십시오.	시스템의 그룹을 판별하려면 어플리케이션 설명을 사용하십시오. 정의한 사용자 그룹이 시스템에서 개별 사용자를 계획하는 방법에 영향을 미칩니다.
개별 사용자 프로파일 계획	하나의 그룹에 각 시스템 사용자를 지정하십시오. 그룹의 나머지 사용자와 다른 특성을 포함하여 각 사용자를 정의하십시오. 예를 들어 그룹의 나머지 사용자와는 다른 어플리케이션 또는 라이브러리에 액세스해야 할 사용자가 있습니다.	개별 사용자를 정의하려면 어플리케이션 계획 및 사용자 그룹 계획 정보를 사용하십시오.
자원 보안 계획	시스템에서 모두가 사용해야 하는 어플리케이션을 결정하십시오. 특정 어플리케이션을 제한해야 할 경우에는 어느 사용자나 그룹에게 그 어플리케이션을 사용하도록 허용할 것인지 결정하십시오.	자원 보안을 계획하려면 어플리케이션 계획 및 그룹 프로파일 계획 정보를 사용하십시오.
어플리케이션 설치 계획	어플리케이션 라이브러리의 소유권 및 공용 권한을 설정하기 위한 방법을 결정하십시오.	어플리케이션 설치를 계획하려면 자원 보안 계획 정보를 사용하십시오.

사용자 보안 계획으로 보안 계획 프로세스를 시작하십시오.

제 4 장 사용자 보안 계획

사용자 보안 계획에는 보안으로 인해 시스템의 사용자들이 영향을 받는 모든 영역에 대한 계획이 포함됩니다. 반드시 다음 영역을 설명해야 합니다.

물리적 보안

물리적 보안에는 사용 중인 iSeries 시스템을 고의적(또는 실수로) 손상 및 절도로부터 보호하는 것이 포함됩니다. 또한, 워크스테이션, 프린터, 기억장치 매체 모두에 대한 보호도 포함합니다. "물리적 보안 계획"에는 물리적 보안 계획, 위험 관리, IBM 권장사항에 대한 자세한 정보가 들어갑니다.

어플리케이션 보안

어플리케이션 보안은 시스템에 저장할 어플리케이션을 결정하고 여러 사용자가 그 어플리케이션에 동시에 액세스할 수 있도록 허용하는 반면에 그 어플리케이션을 어떻게 보호할 것인지에 관한 내용을 처리합니다. "어플리케이션 보안 계획"에서는 어플리케이션과 어플리케이션 명명 규칙을 설명하는 세부사항을 제공합니다.

종합적인 보안 전략

종합적인 보안 계획에는 비지니스의 현재 상태와 향후 추진 방향 모두를 고려하여 보안 계획을 개발하는 것이 포함됩니다. "종합적인 보안 전략 계획"에서는 보안 정책, 보안 레벨, 암호 고려사항, 시스템 값 판별에 관한 자세한 정보를 제공합니다.

사용자 그룹 보안

사용자 그룹은 같은 방식으로 같은 어플리케이션을 사용하는 사용자들의 그룹입니다. 사용자 그룹 보안 계획에는 시스템을 사용할 작업 그룹과 그 그룹이 필요로 하는 어플리케이션을 판별하는 것이 포함됩니다. "사용자 그룹 계획"에서는 사용자 그룹 식별, 그룹 프로파일 계획, 시스템 값 선택, 사용자 환경 판별에 관한 자세한 정보를 제공합니다.

개별 사용자 보안

필요한 사용자 그룹을 판별했으면 필요한 개별 사용자 프로파일을 계획할 수 있습니다. "개별 사용자 프로파일 계획"에서는 시스템 사용자 명명, 개별 사용자의 책임 판별, 시스템 값 선택에 관한 자세한 정보를 제공합니다.

이 계획 주제에는 계획 결정사항을 기록할 때 사용할 수 있는 계획 양식의 링크가 나옵니다.

물리적 보안 계획

iSeries 시스템 설치를 준비할 경우 다음 질문을 통해 물리적인 보안 계획을 작성하십시오.

- 시스템 장치를 어디에 설치할 것인가?
- 각 표시장치를 어디에 설치할 것인가?
- 프린터는 어디에 설치할 것인가?
- 필요한 추가 장비(예: 배선, 전화선, 가구, 창고)는 무엇인가?
- 화재나 전기 공급 중단과 같은 비상사태로부터 시스템을 보호하기 위해 어떤 조치를 취할 것인가?

물리적 보안은 종합적인 보안 계획의 일부이어야 합니다. 시스템과 그 장치를 설치한 곳에 따라 특별한 보호 조치가 필요할 수 있습니다.

물리적 보안 계획 양식을 사용하여 시스템의 물리적 보안에 관한 결정사항을 기록할 수 있습니다. 물리적 보안에 관한 모든 요소는 다음 주제를 검토하십시오.

- 시스템 장치의 물리적 보안에서는 시스템 자체를 보안하는 것에 관한 세부사항을 제공합니다.
- 시스템 문서 및 기억장치 매체의 물리적 보안에는 시스템 문서 및 기억장치 매체를 보안하는 것에 관한 정보가 들어 있습니다.
- 워크스테이션의 물리적 보안에서는 워크스테이션을 보안하기 위한 방법을 설명합니다.
- 프린터 및 프린터 출력의 물리적 보안에서는 프린터 및 그 출력을 물리적으로 보호하는 것에 관한 세부사항을 제공합니다.
- 보안 정책 계획에서는 사용자 지침 및 보안 정책을 준비하는 방법에 관해 설명합니다.

각 시스템 장치에는 기계를 수리하거나 특별한 시스템 조작(예: 시스템 켜기/끄기)을 위한 제어판이 있습니다. 권한이 없는 사람이 이러한 시스템 조작을 하지 못하도록 각 시스템 장치에는 키잠금 스위치 또는 전자 키스틱이 있습니다. 이와 같은 방법으로 시스템 장치를 일부 보호할 수는 있으나 키잠금 스위치나 전자 키스틱이 적절한 물리적 보안을 대체하지는 못합니다.

시스템 장치의 물리적 보안

iSeries 시스템에는 특별한 환경적 제어가 가능한 컴퓨터 룸이 필요 없습니다. 많은 사람들이 액세스할 수 있는 사무실 중간에 시스템 장치가 있는 것을 흔히 보게 됩니다. 사용자는 유지보수가 쉬운 소규모의 iSeries 시스템을 선호합니다. 그러나 이런 경우에는 보안상 노출의 위험이 있습니다. 예를 들면, 어떤 사람이 쉽게 시스템 장치를 훔치거나 시스템 장치에서 귀중한 부품을 꺼내 갈 수 있습니다.

시스템이 설치된 장소를 안전한 곳으로 만들기 위한 조치를 취해야 합니다. 최적의 장소는 잠글 수 있는 전용 룸입니다. 적어도 정규 업무 시간 이외에는 잠글 수 있는 곳에 시스템 장치를 설치해야 합니다.

시스템 장치에 대한 위험

시스템 장치나 그 부품을 도난당하는 것 외에도 부적절한 물리적 보안으로 인해 다른 위험에 노출될 수 있습니다.

우발적인 시스템 작동 방해

많은 보안 문제들이 권한을 가진 시스템 사용자로부터 발생합니다. 시스템의 표시장치 중 하나가 잠겨 있다고 가정하십시오. 시스템 오퍼레이터는 회의로 인해 자리에 없습니다. 실망한 표시장치 사용자는 시스템 장치로 가서 "내가 이 버튼을 누르면 제대로 될꺼야."라고 생각합니다. 그러나 그 버튼은 많은 작업이 실행되는 동안 시스템을 *끄*거나 재로드시키는 버튼일지 모릅니다. 이 경우 부분적으로 갱신된 파일을 회복하기 위해서는 몇 시간이 걸릴 수 있습니다. 이와 같은 일이 발생하지 않도록 하기 위해 시스템 장치 키잠금 스위치를 사용할 수 있습니다.

보안을 피해가기 위한 DST(전용 서비스 툴) 기능 사용

보안은 시스템이 수행하는 서비스 기능을 제어하지 않습니다. 이 기능이 필요한 경우 시스템 소프트웨어가 제대로 작동하지 않을 수 있기 때문입니다. 서비스 툴 사용자 ID와 암호를 알거나 추측할 수 있는 사람이면 시스템에 상당한 손상을 입힐 수 있습니다. 서비스 툴에 대해 자세히 알려면, Information Center의 서비스 툴 주제를 참조하십시오.

권장사항

- 시스템 장치는 잠긴 룸에 설치하는 것이 이상적입니다. 그렇게 할 수 없다면 외부인이 액세스할 수 없는 곳에 장치를 설치하십시오. 또한 책임자가 시스템 장치를 모니터할 수 있는 장소를 선택하십시오. 다음은 우발적인 또는 고의적인 손상으로부터 시스템을 보호할 때 도움을 주는 물리적 보안 피처입니다.
- 전자 키스틱 또는 키잠금을 사용하십시오.
  - 키를 사용하지 않고 시스템을 시작하려면 운영 모드를 정상으로 설정하십시오.
  - 시스템을 시작하고 중단할 때 자동 전원 공급/중단 기능을 사용하면 작동 모드를 자동으로 설정하십시오.
  - 키를 꺼내서 안전한 장소에 보관하십시오.
- 시스템을 설치하고 서비스 요원이 시스템을 사용한 직후 서비스 툴(DST) 사용자 ID와 암호를 변경하십시오. Information Center의 서비스 툴 주제에서는 이를 수행하는 방법에 대해 자세히 설명합니다.

시스템 문서 및 기억장치 매체의 물리적 보안을 계획하기 전에 JKL Toy사의 장치 보안 계획 예를 볼 수 있습니다.

예: JKL Toy사의 물리적 보안 계획 양식 -- 시스템 장치 부분

다음은 Sharon Jones가 시스템에 사용한 물리적 보안 계획 양식의 시스템 장치 부분의 예입니다.

표 3. JKL Toy사의 물리적 보안 계획 양식: 시스템 장치의 예

물리적 보안 계획 양식	
작성자: Sharon Jones	날짜: 1999년 9월 2일
시스템 장치:	
시스템 장치(잠겨 있는 방과 같은)를 보호하기 위한 보안 조치를 서술하십시오.	시스템 장치는 회계 부서에 설치되어 있습니다. 낮에는 회계 부서 직원들이 항상 있으므로 시스템 장치를 지켜볼 수 있습니다. 회계 부서 직원들은 소액의 현금 처리 및 중요한 레코드에 대한 책임도 있습니다. 정기적인 근무 시간 이외에는 그 지역을 잠궈 놓습니다.
일반적으로 사용하는 키 잠금 위치는 무엇입니까?	정상
키를 보관하는 곳은 어디입니까?	Sharon의 사무실에 있는 작은 금고
시스템 장치와 관련된 기타 주석:	시스템 장치를 쉽게 액세스할 수 있습니다. 회계 부서 직원들에게 시스템 장치를 함부로 조작하지 않도록 주지시키십시오.

시스템 장치의 물리적 보안을 계획했으면 시스템 문서 및 기억장치 매체의 물리적 보안을 계획할 수 있습니다.

시스템 문서 및 기억장치 매체의 물리적 보안

물리적 보안 계획에 있어서 또 하나의 요소로서 중요한 시스템 문서와 기억장치 매체를 저장하는 것이 있습니다. 시스템 문서에는 IBM®이 시스템과 함께 제공하는 정보, 암호 정보, 계획 양식, 시스템이 생성한 보고서 등이 포함됩니다.

시스템에 따라 백업 매체에는 테이프, CD-ROM, 디스켓 또는 DVD 기억장치가 포함됩니다. 시스템 문서 및 백업 매체 둘다 멀리 떨어진 다른 장소는 물론 업무를 수행하는 현장에 저장하고 있어야 합니다. 재해가 발생할 경우 시스템을 회복시켜야 할 때 이 정보가 필요합니다. 다음은 시스템 문서 및 기억장치 매체를 저장하기 위한 한 가지 방식입니다. 사용 방식을 결정했으면 그 내용을 물리적 보안 계획 양식의 백업 매체 및 문서 섹션에 기록하십시오.

시스템 문서의 안전한 저장

서비스 툴 및 보안 담당자 암호는 시스템 운영에 있어서 중요합니다. 이 암호를 기록하여 안전하고 은밀한 장소에 저장하십시오. 또한 재해가 발생했을 때 회복시킬 수 있도록 오프사이트에 이 암호의 사본을 보관하십시오.

재해가 발생했을 때 회복시킬 수 있도록 현장과 멀리 떨어진 곳에 구성 설정값 및 기본 어플리케이션 라이브러리 등 중요한 시스템 문서를 저장하도록 하십시오.

기억장치 매체의 안전한 저장

시스템을 설치할 때 테이프나 다른 기억장치 매체로 시스템의 모든 정보를 정기적으로 저장하는 계획을 수립하십시오. 필요 시 이 백업으로 시스템을 회복시킬 수 있습니다. 이 백업을 안전한 장소의 오프사이트에도 보관시켜야 합니다.

위험

- 백업 매체 손상: 재해나 파괴로 인해 시스템 백업 매체가 손상된 경우에는 인쇄된 보고서를 제외하고 시스템에 있었던 정보를 회복하는 것이 불가능합니다.
- 백업 매체 또는 암호 도난: 업무상 기밀 정보를 백업 매체에 저장할 때가 있습니다. 이 경우 시스템을 잘 아는 사용자라면 그 정보를 다른 컴퓨터에 복원하여 인쇄하거나 처리할 수 있습니다.

권장사항

- 모든 암호와 백업 매체를 잠글 수 있는 내화성 캐비넷에 저장하십시오.
- 정기적으로(예: 최소 일주일에 한 번) 백업 매체 사본을 작성하여 안전한 오프사이트에 보관하십시오.

워크스테이션의 물리적 보안을 계획하기 전에 JKL Toy사의 시스템 문서 저장 계획 예를 검토하십시오.

예: JKL Toy사의 물리적 보안 계획 양식 -- 백업 매체 및 문서 부분

JKL Toy사의 Sharon Jones가 아래 표에 나오는 것처럼 물리적 보안 계획 양식의 백업 매체 및 문서 섹션을 완료했습니다.

표 4. JKL Toy사의 물리적 보안 계획 양식: 백업 매체 및 문서의 예

물리적 보안 계획 양식	
작성자: Sharon Jones	날짜: 1999년 9월 2일
백업 매체 및 문서:	
사무실의 어느 곳에 백업 테이프를 저장합니까?	대형 내화성 금고
사무실과 떨어진 어느 곳에 백업 테이프를 저장합니까?	회사의 회계사 사무실에 있는 내화성 금고
보안 담당자, 서비스, DST 암호를 어디에 보관합니까?	John Smith 사무실의 금고
일련 번호나 구성과 같은 중요한 시스템 문서를 어디에 보관합니까?	회사 외부의 대형 금고 및 회계사의 사무실

저장 및 문서 보안을 계획했으면 워크스테이션을 위한 물리적 보안을 계획할 수 있습니다.

워크스테이션의 물리적 보안 계획

보통은 모든 사용자가 워크스테이션에 사인 온하여 권한이 있는 모든 기능을 수행합니다. 그러나 공적이거나 사적인 용도의 워크스테이션이 있다면 특별한 사전처리가 필요할 수 있습니다. 예를 들어, 키스트로크를 저장하는 표시장치와 특별한 퍼스널 컴퓨터

에는 특별한 고려사항이 요구됩니다. 물리적 보안 계획 양식의 파트 2(워크스테이션 및 프린터의 물리적 보안)를 완료하려면 다음을 참조하십시오.

워크스테이션과 연관된 위험

허가되지 않은 용도로 공개 장소에서 워크스테이션 사용

외부인이 쉽게 접근할 수 있는 장소인 경우 기밀 정보를 볼 가능성이 있습니다. 시스템 사용자가 워크스테이션을 사인 온 상태로 방치할 경우 외부인이 다가와서 기밀 정보에 액세스할 수 있습니다.

허가되지 않은 용도로 사적인 장소에서 워크스테이션 사용

사적인 장소의 워크스테이션은 침입자에게 감시를 당하지 않고 오랜 시간 동안 보안 조치를 피하기 위해 시도할 수 있는 기회를 제공합니다.

보안 조치를 피해가기 위해 표시장치에서 재생 기능 또는 PC 사인 온 프로그램을 사용

많은 표시장치에는 레코드 및 재생 기능이 있어서 사용자가 자주 사용하는 키스트로크를 저장하고 키 하나를 눌러 이를 반복할 수 있습니다. iSeries 시스템에서 워크스테이션으로 퍼스널 컴퓨터를 사용할 경우 사인 온 프로세스를 자동화하는 프로그램을 작성할 수 있습니다. 사용자들이 사인 온 프로세스를 빈번히 사용하기 때문에 사용자 ID와 암호를 사인 온할 때마다 매번 입력하는 대신 저장하기로 결정할 수 있습니다.

권장사항

다음은 워크스테이션에 물리적 보안을 설정할 때 고려해야 할 권장사항입니다.

- 가능하면, 공개적인 장소나 사적인 장소에 워크스테이션을 설치하지 마십시오.
- 시스템 사용자에게 워크스테이션을 떠나기 전에 사인 오프해야 하는 것이 얼마나 중요한지를 강조하십시오. 보안 정책에 사인 오프 프로시듀어를 포함시켜야 합니다.
- 표시장치나 PC 프로그램에 암호를 기록하는 것은 시스템 보안에 위배된다는 점을 강조하십시오. 보안 정책에 암호 정보를 기록하는 것을 포함시켜야 합니다.
- 비활동 타이머 시스템 값(QINACTITV 및 QINACTMSGQ)을 사용하여 사용자가 시스템을 사인 오프하지 않고 공개적인 장소의 워크스테이션을 방치하지 않도록 조치를 취하십시오.
- 제한된 권한을 가진 사용자에게만 해당 워크스테이션에 대한 권한을 부여하여 사용자가 공용 워크스테이션에서 수행할 수 있는 기능을 제한하십시오.
- 보안 또는 서비스 권한을 가진 사용자들은 사적인 워크스테이션에서 사인 온하지 못하게 하십시오. 사용자들이 이 권한으로 사인 온하는 위치를 제어하려면 QLMTSECOFR 시스템 값을 사용하십시오.
- 사용자들이 동시에 하나 이상의 워크스테이션에서 사인 온하지 못하게 하십시오. 장치 세션을 제한하는 시스템 값(QLMTDEVSSN)을 사용하여 사용자가 사인 온하는 위치를 제어할 수 있습니다.

이 권장사항들을 적용시키려면 "사인 온에 영향을 주는 시스템 값 선택" 및 "워크스테이션에 대한 자원 보안 계획" 주제에서 세부사항을 참조하십시오.

물리적 보안 계획 양식의 경우 물리적 위치로 인해 위험을 초래할 수 있는 워크스테이션을 식별해야 합니다. Sharon Jones가 JKL Toy사의 워크스테이션에 대해 물리적 보안을 계획한 예를 검토하십시오.

워크스테이션 보안을 계획했으면 프린터 및 프린터 출력의 물리적 보안을 계획할 수 있습니다.

프린터 및 프린터 출력의 물리적 보안

일단 인쇄가 시작되면 시스템 보안은 누가 그 출력물을 보는지를 제어할 수 없습니다. 누군가 민감한 업무 정보를 볼 수 있는 위험을 최소화하기 위해서는 프린터 및 프린터 출력을 보안시켜야 합니다. 기밀 업무 정보를 인쇄하는 것과 관련된 정책도 작성해야 합니다.

프린터 및 프린터 출력과 연관된 위험

업무 상황에 따라서는 다음과 같은 위험이 내재할 수 있습니다. 다음의 위험 상황은 프린터 및 프린터 출력과 연관된 가장 일반적인 보안 노출 상황입니다. 그러나 특정 업무 상황별로 또 다른 위험도 조사해야 합니다.

- 공개적인 장소에 설치한 프린터는 권한이 없는 사용자가 기밀 정보에 액세스할 수 있는 기회를 제공합니다.
- 책상 위에 놓인 프린터 출력물은 정보를 유출시킬 수 있습니다.
- 시스템에 프린터를 한 대나 두 대만 설치했을 수 있습니다. 이 경우 귀중한 정보나 기밀 정보(예: 급여)를 인쇄하여 회사 직원들이 그 정보를 볼 수 있습니다.

권장사항

다음은 프린터 및 프린터 출력과 연관된 보안 위험을 줄이기 위한 권장사항입니다.

- 시스템 사용자에게 기밀 정보의 프린터 출력을 보호하는 것이 얼나마 중요한지를 강조하십시오. 보안 정책에 프린터와 관련된 물리적 보안 결정사항을 포함시키십시오.
- 공개적인 장소에 프린터를 설치하지 마십시오.
- 기밀 정보를 인쇄하기 위한 일정을 세우고 인쇄 중에는 권한을 가진 사용자가 프린터 옆에서 대기하십시오.

"프린터 및 프린터 출력에 대한 보안 계획"에서는 기밀 정보의 프린터 출력을 처리하기 위한 제안사항을 설명합니다.

보안 정책 계획 수립을 시작하기 전에 JKL Toy사의 프린터 보안 계획 예를 볼 수 있습니다.

예: JKL Toy사의 물리적 보안 계획 양식 -- 워크스테이션 및 프린터 부분

아래는 Sharon Jones가 JKL Toy사에 사용한 물리적 보안 계획의 두 번째 부분에 관한 예입니다.

표 5. JKL Toy사의 물리적 보안 계획 양식: 워크스테이션 및 프린터의 예

물리적 보안 계획 양식			파트 2의 2
워크스테이션 및 프린터의 물리적 보안			
워크스테이션 또는 프린터 이름	위치 또는 설명	보안 노출	적용시킬 보호 조치
DSP06	출고지	너무 공개되어 있음	자동 사인 오프. 워크스테이션에서 완료할 수 있는 기능을 제한하십시오.
DSP09	고객 서비스 데스크	너무 공개되어 있음	자동 사인 오프. 워크스테이션에서 완료할 수 있는 기능을 제한하십시오.
RMT12	영업지사	너무 개인적임	보안 담당자가 그곳에서 사인 온할 수 없게 하십시오.
PRT02	시스템 장치 근처의 회계 부서	가격 리스트와 같은 민감한 정보가 노출될 수 있음	프린터 출력을 모니터할 사람을 지정하십시오.

물리적 보안 계획 양식을 완료했으면 "보안 정책 계획"을 검토하십시오.

보안 정책 계획

직원 모두에게 보안 지침을 전달하여 물리적 보안 및 시스템 보안과 관련된 보안 정책을 강조하는 것이 좋습니다. 나중에 시스템에 추가되는 신규 사용자들에게도 같은 지침을 제공할 수 있습니다.

이 지침에는 시스템 보안 보호 방법(예: 워크스테이션 사인 오프하기 및 암호 공유하지 않기)에 대한 몇 가지 일반적인 지침을 포함시켜야 합니다. 또한 특정 보안 결정사항에 대한 내용도 포함시켜야 합니다.

이 계획 정보를 검토해 나가면서 자신의 보안 정보에 포함시켜야 할 것들을 기록하십시오. 또한 자신의 보안 정책에 관한 아이디어도 메모할 수 있습니다.

예를 들어, JKL Toy사의 Sharon Jones는 시스템의 물리적 보안을 계획할 때 자신의 보안 지침에 대해 기록했습니다.

출고지(loading dock), 고객 서비스, 영업 지사에 대해 사인 오프의 중요성을 강조하십시오. 회계원이 시스템 장치를 감시할 것입니다.

물리적 보안 계획 양식을 완료했으면 어플리케이션에 대한 보안 계획을 수립할 준비가 된 것입니다.

어플리케이션 보안 계획

어플리케이션에 적절한 보안을 계획하려면 다음을 알아야 합니다.

- 시스템에 저장하려는 정보는 무엇인가?
- 그 정보에 액세스해야 할 사람은 누구인가?
- 필요한 액세스 유형은 무엇인가? 사람들이 정보를 변경해야 하는가 아니면 단지 보기만 하면 되는가?

어플리케이션 계획 주제를 읽어나가면서 시스템에 저장하려는 정보에 대한 첫 번째 질문에 답하십시오. 다음 주제에서 해당 정보를 필요로 하는 사람과 필요로 하는 액세스 유형을 결정하십시오. 어플리케이션 계획 정보는 시스템에 입력하지 마십시오. 그러나 사용자와 자원 보안을 설정할 때 이 정보가 필요합니다.

어플리케이션이란?

어플리케이션 보안을 위한 첫 번째 계획 단계에서는 시스템에서 실행할 어플리케이션을 설명해야 합니다. 어플리케이션은 논리적으로 함께 속하는 하나의 기능 그룹입니다. 예를 들어 JKL Toy사에 있어서 주문 입력, 주문 선적, 송장 인쇄는 모두 주문 처리라는 하나의 어플리케이션을 구성합니다.

보통 두 개의 서로 다른 어플리케이션 유형을 iSeries 시스템에서 실행할 수 있습니다.

- **업무 어플리케이션**: 특정 업무 기능(예: 주문 처리 또는 명세 관리)을 수행하기 위해 구매하거나 개발한 어플리케이션.
- **특수 어플리케이션**: 업무 처리를 위한 것이 아닌 다양한 활동을 수행하기 위해 회사 전체에서 사용되는 어플리케이션.

필요한 양식은?

어플리케이션 보안을 계획할 경우 다음 양식을 사용하십시오.

- 어플리케이션 설명 양식
- 라이브러리 설명 양식
- 명명 규칙 양식

이 양식을 인쇄하려면 링크를 클릭하고 오른쪽 프레임을 선택한 후 브라우저에서 **인쇄** 아이콘을 클릭하십시오.

계획 양식을 완료하려면 다음 정보를 참조하십시오.

- 어플리케이션 설명
- 명명 규칙 설명
- 라이브러리 정보 설명
- 어플리케이션 다이어그램 그리기

어플리케이션 설명

이제 각 업무 어플리케이션에 대한 몇 가지 일반 정보를 수집해야 합니다. 어플리케이션에 대한 정보를 아래 설명한 어플리케이션 설명 양식의 해당 필드에 추가하십시오. 나중에 이 정보를 사용하여 사용자 그룹 및 어플리케이션 보안을 계획할 때 도움을 받을 수 있습니다.

어플리케이션 이름 및 약어

단축명과 함께 양식에서 약어로 사용할 수 있으며 어플리케이션이 사용하는 오브젝트를 명명하기 위해 사용할 수 있는 약어를 어플리케이션에 제공합니다.

설명 정보

어플리케이션이 하는 일을 간략히 설명합니다.

1차 메뉴 및 라이브러리

어플리케이션에 액세스하기 위한 1차 메뉴를 식별합니다. 메뉴가 있는 라이브러리를 표시합니다. 보통 1차 메뉴는 특정 어플리케이션 기능을 가진 다른 메뉴로 안내합니다. 일반적으로 사용자들은 시스템에 사인 온한 직후 기본 어플리케이션의 1차 메뉴를 보고 싶어합니다.

초기 프로그램 및 라이브러리

때로는 어플리케이션이 사용자에 대한 백그라운드 정보를 설정하거나 보안 검사를 수행하는 초기 프로그램을 실행하는 경우가 있습니다. 어플리케이션에 초기 프로그램 또는 설정 프로그램이 있으면 양식에 기록하십시오.

어플리케이션 라이브러리

보통은 각 어플리케이션에 그 파일을 위한 기본 라이브러리가 있습니다. 프로그램 라이브러리 및 다른 어플리케이션이 소유하는 라이브러리를 포함하여 어플리케이션이 사용하는 모든 라이브러리를 포함시키십시오. 예를 들어 JKL Toy 사의 고객 주문 관리 어플리케이션은 재고 관리 라이브러리를 사용하여 항목의 잔고 및 설명을 확보합니다.

라이브러리와 어플리케이션간의 관계를 사용하여 각 라이브러리에 액세스해야 하는 사용자를 판별할 수 있습니다.

어플리케이션에 관한 정보 찾기

어플리케이션에 관해 필요한 정보를 아직 모르면 프로그래머나 어플리케이션 제공자에게 문의하십시오.

다음은 시스템에서 실행되는 어플리케이션에 관해 이 정보에 액세스 권한이 없을 때 스스로 정보를 수집하기 위한 방법입니다.

- 어플리케이션 사용자가 1차 메뉴 및 라이브러리명을 알려주거나 그들이 시스템에 사인 온하는 것을 주시할 수 있습니다.

- 사용자들이 사인 온한 직후 어플리케이션을 볼 경우 그 사용자 프로파일의 **초기 프로그램** 필드를 보십시오. 이 필드에 어플리케이션에 대한 초기 프로그램이 들어 있습니다. DSPUSRPRF 명령을 사용하여 초기 프로그램을 볼 수 있습니다.
- 시스템의 라이브러리 모두에 대한 이름 및 설명을 나열할 수 있습니다. DSPOBJD *ALL *LIB를 사용하십시오. 이것은 시스템의 라이브러리를 모두 표시합니다.
- 사용자들이 어플리케이션을 실행하는 동안 활동 작업을 관찰할 수 있습니다. 대화식 작업에 관한 자세한 정보를 구하려면 활동 작업에 대한 작업(WRKACTJOB) 명령을 중간 지원 레벨과 함께 사용하십시오. 사용 중인 라이브러리를 찾으려면 작업을 표시하고 라이브러리 리스트와 그 오브젝트 잠금 둘다 보십시오.
- 사용자 작업에 대한 작업(WRKUSRJOB) 명령을 사용하여 어플리케이션 안의 일괄처리 작업을 표시할 수 있습니다.

어플리케이션 보안을 계획하는 데 필요한 모든 정보를 수집하려면 계속하기 전에 다음 타스크를 완료해야 합니다.

- 각 업무 어플리케이션에 대해 어플리케이션 설명 양식을 완료하십시오. 보안 요구사항 섹션을 제외한 전체 양식을 채우십시오. ″자원 보안 계획″ 주제에서 설명한대로 해당 섹션을 사용하여 어플리케이션에 대한 자원 보안을 계획할 것입니다.
- 적용되는 경우 어플리케이션별로 어플리케이션 설명 양식을 준비하십시오. 이 양식은 어플리케이션에 액세스를 제공하는 방법을 결정할 때 도움이 됩니다.

주: IBM Query for iSeries와 같은 특별한 IBM 어플리케이션 설명 양식을 준비하는 것은 사용자의 선택사항입니다. 이 어플리케이션이 사용하는 라이브러리 액세스를 위해서는 특별한 계획이 필요 없습니다. 그러나 정보를 수집하고 양식을 준비하는 것이 유용하다는 것을 알 수 있을 것입니다.

명명 규칙 설명으로 이동하기 전에 JKL Toy사의 어플리케이션 설명에 대한 양식 예를 볼 수 있습니다.

예: JKL Toy사의 어플리케이션 설명 양식

Sharon Jones가 어플리케이션 설명 양식에 있는 약어로 회사의 모든 어플리케이션을 나열했습니다. Sharon은 또한 사용자들이 이 어플리케이션으로 어떻게 작업하는지에 관해 간단히 기술했습니다.

고객 주문 관리(CO)

주문을 입력, 추적, 출고합니다. 송장을 인쇄합니다.

제고 관리(IC)

완성품 및 자재에 관한 재고 수준을 관리합니다. 모든 재고의 추이를 처리합니다.

계약 및 가격 관리(CP)

고객과의 특별가 책정 및 계약을 관리합니다.

미수금 관리(AC)

현재 잔고를 추적합니다. 월별 대차 대조표를 인쇄합니다.

아래 표에는 고객 주문 관리 어플리케이션에 대한 Sharon Jones의 설명이 나옵니다. Sharon은 하나의 어플리케이션에서 시작하여 나머지를 설명하는 방식으로 체계적으로 양식을 준비했습니다.

표 6. JKL Toy사의 어플리케이션 설명 양식: 예

어플리케이션 설명 양식	
작성자: Sharon Jones	날짜: 1999년 9월 3일
어플리케이션 이름: 고객 주문 관리	약어: CO
어플리케이션에 대한 간단한 설명:	고객 주문을 입력하고 출고 전에 주문을 추적하며, 주문을 선적하고, 선적 서류 및 송장을 인쇄합니다.
1차 메뉴 이름: COMAIN	라이브러리: COPGMLIB
초기 프로그램 이름: NA	라이브러리: NA
파일 및 프로그램 모두에 어플리케이션이 사용하는 라이브러리를 나열합니다. • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
어느 정보가 기밀 정보인지와 같은, 어플리케이션에 대한 보안 목적을 정의하십시오.	

고객 주문 관리 어플리케이션에 추가하여 Sharon Jones는 JKL Toy사의 시스템에 이 어플리케이션을 위한 어플리케이션 설명 양식을 준비했습니다.

- 제고 관리
- 계약 및 가격 관리
- 미수금 관리

이제 시스템의 오브젝트에 대한 명명 규칙을 설명할 수 있습니다.

명명 규칙 설명

시스템이 오브젝트를 명명하는 방법을 알면 보안을 계획 및 모니터하고 문제점을 해결하여 백업 및 회복을 계획할 수 있습니다. 대부분의 어플리케이션에는 오브젝트(예: 라이브러리, 파일, 프로그램)에 이름을 할당하는 규칙이 있습니다. 어플리케이션이 서로 다른 소스에서 나오는 경우 각각 고유한 명명 시스템을 가질 것입니다.

반드시 명명 규칙 양식에 모든 어플리케이션 및 오브젝트 명명 규칙을 기록하십시오. 명명 규칙 양식에 라이브러리와 파일을 명명할 때 어플리케이션이 사용하는 규칙을 나열하십시오. 다른 명명 규칙(예: 프로그램 및 메뉴)에 대해 공백 행을 사용하려는 경우가 있을 것입니다. 어플리케이션이 서로 다른 소스에서 나오는 경우 각각 고유한 명명 시

스템을 가질 것입니다. 각 어플리케이션에 대해 명명 규칙을 설명하십시오. 두 개 이상의 명명 규칙 양식을 준비해야 할 것입니다.

라이브러리 정보 설명으로 이동하기 전에 Sharon이 JKL Toy사의 시스템 오브젝트에 대해 사용한 예를 볼 수 있습니다.

예: JKL Toy사의 명명 규칙 양식

아래 표는 라이브러리 및 파일에만 사용되는 명명 규칙을 보여줍니다. 시스템에 있는 다른 유형의 오브젝트를 위한 명명 규칙도 설명해야 합니다. 명명 규칙 양식에는 여러 가지 공통 오브젝트가 포함되어 있으나 그 외에도 준비해야 할 다른 오브젝트가 있을 수 있습니다.

표 7. JKL Toy사의 명명 규칙 양식: 예

명명 규칙 양식	
작성자: Sharon Jones	날짜: 1999년 9월 3일
오브젝트 유형	**명명 규칙**
라이브러리	파일을 포함하고 있는 라이브러리에는 CONTRACTS 또는 ITEMLIB처럼 의미를 가진 이름이 있습니다. 프로그램 라이브러리는 ICPGMLIB와 같이 PGMLIB가 뒤에 나오는 어플리케이션 약어를 사용합니다.
파일	CUSTMAST는 고객 마스터 파일(Customer Master file)의 이름, ITEMMAST는 품목 마스터 파일(Item Master file)의 이름을 나타내는 것처럼 주요 파일에는 의미를 가진 이름이 사용됩니다. 다른 어플리케이션 파일들은(프로그래머만을 위해 사용되는) ICFILE14와 같이 FILE 및 숫자가 뒤에 나오는 어플리케이션 약어로 명명됩니다.

명명 규칙 양식을 완료했으면 라이브러리 정보 설명을 시작할 수 있습니다.

라이브러리 정보 설명

명명 규칙을 설명했으면 시스템의 라이브러리를 설명해야 합니다. 라이브러리는 시스템의 오브젝트를 식별하고 체계화합니다. 유사한 파일들을 하나의 라이브러리에 함께 위치시키면 중요한 어플리케이션과 파일에 쉽게 액세스할 수 있습니다. 또한 일부 라이브러리에는 액세스할 수 있으나 다른 라이브러리에는 액세스할 수 없도록 사용자 권한을 정의할 수도 있습니다. 시스템의 모든 라이브러리를 각 어플리케이션에 대해 설명하십시오. 두 개 이상의 라이브러리 설명 양식을 준비해야 할 수 있습니다.

주: 라이브러리에 관한 설명 정보만 채우십시오. 라이브러리에 대한 자원 보안을 계획할 때 나머지 라이브러리 설명 양식을 채울 것입니다. 나중에 라이브러리에 권한에 관한 정보를 추가해야 합니다. 라이브러리 설명 양식의 나머지 부분을 완료하는 것에 관한 세부사항은 "어플리케이션 라이브러리에 대한 보안 계획"을 참조하십시오.

계속하기 전에 반드시 다음을 완료하십시오.

- 명명 규칙 양식의 라이브러리 및 파일 부분을 채우십시오.
- 각 어플리케이션 라이브러리에 대해 라이브러리 설명 양식의 설명 정보를 채우십시오.

어플리케이션 다이어그램 그리기에 앞서 JKL Toy사의 Sharon이 라이브러리를 설명한 방법에 대한 예를 볼 수 있습니다.

예: JKL Toy사의 라이브러리 설명 양식

아래의 두 가지 표에는 고객 주문 관리 어플리케이션이 JKL Toy사에서 사용하는 두 개의 라이브러리가 나옵니다. 첫 번째 표는 파일이 포함된 라이브러리를 설명하며, 두 번째 표는 프로그램이 포함된 라이브러리를 설명합니다.

표 8. JKL Toy사의 라이브러리 설명 양식: 파일이 포함된 라이브러리의 예

라이브러리 설명 양식	
작성자: Sharon Jones	날짜: 1999년 9월 3일
라이브러리명: CUSTLIB	설명(텍스트): 고객 레코드 라이브러리
이 라이브러리의 기능을 간단히 서술하십시오.	주문 및 미수금 관리를 포함하여 모든 고객 파일을 보유합니다.

표 9. JKL Toy사의 라이브러리 설명 양식: 프로그램이 포함된 라이브러리의 예

라이브러리 설명 양식	
작성자: Sharon Jones	날짜: 1999년 9월 3일
라이브러리명: COPGMLIB	설명(텍스트): 고객 주문 관리 프로그램 라이브러리
이 라이브러리의 기능을 간단히 서술하십시오.	고객 주문 관리 어플리케이션을 위한 모든 프로그램을 보유합니다.

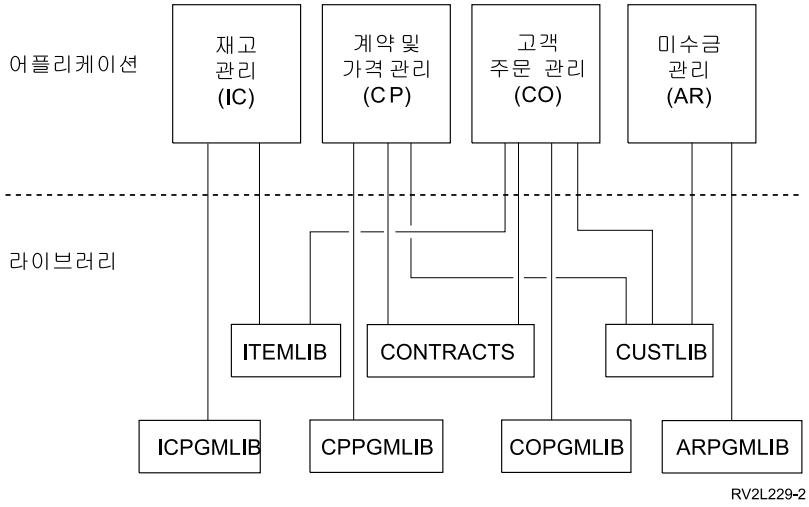
라이브러리를 설명했으면 시스템을 위한 어플리케이션 다이어그램 그리기를 시작하십시오.

어플리케이션 다이어그램 그리기

어플리케이션 설명 및 라이브러리 설명 양식을 준비할 때 어플리케이션과 라이브러리간의 관계를 표시하는 다이어그램을 그리는 것이 유용합니다. 다이어그램은 사용자 그룹과 자원 보안을 계획할 때 도움이 됩니다.

아래 그림은 JKL Toy사의 Sharon Jones가 어플리케이션 및 라이브러리를 그린 다이어그램입니다.

JKL Toy사의 어플리케이션 및 라이브러리 다이어그램



지금 어플리케이션 및 라이브러리에 대해 몇 가지 정보를 수집한 것이 보안 결정을 내릴 때 도움이 됩니다. 이것을 시스템과 어플리케이션에 대해 더 많이 알 수 있는 기회로 생각하십시오.

필요한 어플리케이션 정보를 수집했는지 확인하려면 다음과 같이 하십시오.

- 시스템의 각 업무 어플리케이션에 대해 어플리케이션 설명 양식을 완료하십시오.
- 선택적으로, 시스템에 있는 특별한 업무 어플리케이션에 대해 어플리케이션 설명 양식을 준비하십시오.
- 명명 규칙 양식의 라이브러리 및 파일 섹션을 채우십시오.
- 각 어플리케이션 라이브러리에 대해 라이브러리 설명 양식을 준비하십시오.
- 어플리케이션과 라이브러리간의 관계에 대한 다이어그램을 그리십시오.

이 양식을 완료했으면 종합적인 보안 전략 계획을 수립할 수 있습니다.

종합적인 보안 전략 계획

어플리케이션에 대한 보안 계획을 수립했으면 종합적인 보안 전략을 시작할 수 있습니다. 먼저, 시스템 보안에 대한 종합적인 접근방식을 결정해야 합니다. 결정을 내릴 때 회사의 현재 요구와 향후 요구에 있어서 균형을 맞추십시오.

이 정보는 계획 프로세스 전반에 걸쳐 보안 정책 및 목적을 결정할 때 이 정보를 사용하여 시스템의 모든 사용자에게 영향을 주는 기본 시스템 값을 선택할 수도 있습니다.

필요한 양식은?

어플리케이션 계획을 완료하려면 시스템 값 선택 양식을 사용하십시오.

이 주제를 검토하는 중에 이미 완료한 물리적 보안 계획 양식 및 어플리케이션 설명 양식을 사용하여 시스템 값에 대한 결정을 내려야 합니다.

보안 전략을 계획하려면 다음 주제를 검토하십시오.

- 보안 정책 작성
- 보안 레벨 선택
- 사인 온에 영향을 주는 시스템 값 선택
- 암호에 영향을 주는 시스템 값 선택
- 시스템 사용자 정의를 위해 시스템 값 사용

보안 정책 작성

계획하기 전에 시스템의 보안과 관련한 회사의 정책 발표문을 준비하십시오. 이 발표문은 사용자와 회사 최고 경영자간에 이루어지는 일종의 계약입니다. 이것이 결정을 내리고 중요한 내용을 결정할 때 도움이 될 것입니다. 보안 정책에는 종합적인 접근방식은 무엇이며 보호해야 하는 정보 자산에는 어떤 것이 있는지를 언급해야 합니다.

시스템마다 보안이 필요합니다. 다음 접근방식 중 하나를 보안에 적용할 수 있습니다.

- **고(strict)**: 이것을 필수 보안 계획으로 부르는 사람도 있습니다. 고(strict) 상태의 보안 환경에서는 작업을 수행할 때 필요한 정보 및 기능에만 액세스할 수 있는 권한을 사용자에게 부여하십시오. 다른 것들은 제외하십시오. 많은 감사자들이 고(strict) 상태의 접근방식을 권장합니다.
- **중(average)**: 중(average) 상태의 보안 접근방식은 사용자에게 할당한 권한을 근거로 오브젝트에 액세스할 권한을 부여합니다.
- **저(relax)**: 저(relax) 상태의 보안 환경에서는 권한이 있는 사용자가 시스템에 있는 대부분의 오브젝트에 액세스할 수 있도록 하십시오. 시스템에 저(relax) 상태의 접근방식을 사용하는 한 부서나 소규모 회사의 경우 중요한 자원이나 기밀 자원에 대해 액세스를 제한하십시오.

종합적인 접근방식은 특정 보안 요구에 관한 결정을 내릴 때 도움이 됩니다. 시스템에 대한 보안 접근방식이 회사 전체에 있어서 정보에 액세스하기 위한 철학과 일치해야 합니다. 어떤 접근방식을 사용해야 할지 확실하지 않으면 다음과 같이 하십시오.

- 완료한 어플리케이션 설명 양식을 사용하여 해당 어플리케이션에 액세스해야 할 사용자나 액세스해서는 안되는 사용자를 판별하십시오.
- 회사에서 사용하는 기법을 검토하십시오. 예를 들어, 시스템 또는 네트워크를 인터넷에 연결할 계획이면 인터넷 밖의 사용자로부터 시스템을 보호하기 위해 보다 제한적인 보안 환경을 원할 것입니다.
- 보안 요구를 더 잘 판별하려면 회사의 다른 직원(예: 보안 감사자)과 상의하십시오.

정책은 언제나 변경시킬 수 있다는 점을 기억하십시오. 대부분의 회사들은 회사 규모가 커짐에 따라 보다 엄격한 보안을 필요로 합니다. 이 정보는 많은 변경 없이 또는 모든 어플리케이션을 다시 테스트하지 않고도 나중에 보안을 더 추가할 수 있게 해 주는 보안 체계를 설정할 때 도움이 됩니다.

보안 대상

보안 정책에는 종합적인 보안 접근방식을 언급하는 것 외에도 회사의 중요한 정보 자산을 식별시켜야 합니다. 따라서 보안 시스템이 이와 같은 정보를 보호하도록 설계되어야 합니다. 다음은 중요한 자산을 판별하기 위해 사용할 수 있는 몇 가지 요구사항입니다.

- **기밀성**: 일반적으로 회사에서 사용자들이 사용할 수 없는 정보. 급여는 기밀 정보의 한 예입니다.
- **경쟁력**: 경쟁사에 비해 장점을 제공하는 정보(예: 제품 스펙 및 공식)
- **운영**: 일일 업무 운영에 필수적인 컴퓨터에 있는 정보(예: 고객 레코드 및 재고 잔고)

보안 담당자인 Sharon Jones와 사장인 John Smith가 공동으로 작업하여 보안 정책 발표문을 준비합니다. John Smith는 이 메모를 사용하여 JKL Toy사의 보안 정책 초안을 작성합니다. 여기에서 JKL Toy사가 보안을 계획하고 설정을 완료한 후 직원 모두에게 송신한 보안 정책을 검토할 수 있습니다. 이 계획 주제를 검토해 나가면서 보안 정책에 추가할 내용을 기록하는 것을 잊지 마십시오.

표 10. JKL Toy사의 보안 정책: 예

종합적인 접근방식 저(relax): 대부분의 사용자들이 거의 모든 정보에 액세스합니다. 중요한 정보 • 계약 및 특별가 관리 • 급여 관리 • 고객 관리 레코드 및 재고 관리 레코드는 회사 직원들만 사용할 수 있습니다. 일반 규칙 • 모든 시스템 사용자가 사용자 프로파일을 가집니다.사용자는 프로파일이나 암호를 공유할 수 없습니다. • 사용자는 60일 간격으로 암호를 변경해야 합니다.

보안 정책과 관련된 메모를 작성했으면 보안 레벨을 선택할 수 있습니다.

보안 레벨 선택

QSECURITY 시스템 값은 어느 정도의 보안을 시스템에 원하는지를 제어할 수 있게 해줍니다. 보안 레벨이 작동하는 방법을 이해하기 위해 시스템을 사람들이 들어가려고 하는 건물로 생각해 보십시오.

레벨 20: 암호 보안

레벨 20을 선택하면 약간의 보안 보호를 받습니다. 건물 입구에서 경비원이 신분과 암호를 확인합니다. 둘다 가지고 있는 사람만 건물에 들어갈 수 있습니다. 그러나 일단 안으로 들어가면 어디든지 갈 수 있으며 원하는 것을 마음대로 할 수 있습니다.

누군가 비밀 암호를 엿듣고 그 암호를 사용하여 입구의 경비원을 통과하면 더 이상의 보호를 받지 못합니다.

레벨 30: 암호 및 자원 보안

레벨 30은 레벨 20의 모든 보안에 추가하여 건물의 특정 구역으로 갈 수 있는 사람들을 제어하며 그 곳에 도착해서 할 수 있는 일을 제어합니다. 건물의 일부 구역은 공용으로 지정하고 다른 구역은 입구의 경비원이 제한하도록 지정할 수 있습니다.

제한된 구역에 액세스할 수 있는 사람들이 원하는 것을 할 수 있도록 허용하거나 권한이 있는 정보 요원(프로그램)에게 정보를 요구할 수 있습니다. 다른 사람의 암호를 사용하여 들어온 침입자가 보호 구역으로 들어 가기 위해서는 내부 경비원을 통과해야 합니다.

레벨 40: 무결성 보호

레벨 40에서는 레벨 30의 모든 보호와 함께 시스템이 사용자의 액세스를 확인합니다. 건물 내부의 출입문에 있는 경비원이 암호를 확인하여 방에 들어 가는 모든 사용자를 기록합니다.

레벨 50: 확장 무결성 보호

레벨 50에서는 경비원이 보다 엄격한 규칙을 시행하여 기록부에 사인하는 사람의 신원을 확인함으로써 특별한 지식을 가진 사용자가 제한 구역을 통과하지 못하게 합니다.

권장사항

보안 레벨 40을 갖춘 iSeries가 권장됩니다. 보안 레벨 40은 고(strict), 중(average), 저(relax)의 보안 정책을 채택하고 있는 어느 시스템에서나 최적의 선택입니다. 저(relax) 상태의 접근방식을 선택하면 시스템에 있는 대부분의 자원에 공용 액세스를 설정할 수 있습니다. 처음부터 보안 레벨 40을 사용하면 많은 변경을 하지 않고도 향후에 시스템 더 안전하게 만들 수 있는 유연성을 갖게 됩니다.

어플리케이션 프로그램을 구매할 경우 프로그램이 레벨 40에서 테스트를 완료한 것인지 어플리케이션 제공자에게 확인하십시오. 일부 어플리케이션은 보안 레벨 40에서 오

류를 일으키는 연산을 사용합니다. 어플리케이션이 레벨 40이나 50에서 테스트를 받지 않았으면 레벨 30으로 시작하십시오. 어플리케이션이 권한 실패를 기록하는지 확인하려면 감사 저널 기능을 사용하십시오. 기록하지 않으면 레벨 40이나 50으로 변경할 수 있습니다.

보안 레벨 50은 대부분의 시스템에서 보통 발생하지 않는 이벤트를 방지합니다. 프로그램이 시스템에서 실행될 때마다 시스템이 추가 검사를 합니다. 이 추가 검사로 인해 성능이 저하될 수 있습니다.

시스템 값 선택 양식에 보안 레벨에 대한 선택사항을 입력했으면 사인 온에 영향을 주는 시스템 값을 선택할 수 있습니다.

사인 온에 영향을 주는 시스템 값 선택

보안 레벨을 선택했으면 시스템 값을 사용하여 사용자들이 화면에서 보는 것을 사용자 정의하고 시스템과 대화하는 방법을 사용자 정의할 수 있습니다. 이 시스템 값을 계획하고 시스템 값 선택 양식을 사용하여 선택사항을 기록해야 합니다.

아래 표는 이 주제에서 사용하는 시스템 값을 설명한 것입니다.

표 11. iSeries 시스템 값 및 해당 설명

시스템 값	설명
QMAXSIGN	연속적인 사인 온 시도 횟수를 제한합니다.
QMAXSGNACN	연속적인 사인 온 시도 횟수에 도달했을 때 시스템이 취할 조치를 지정합니다.
QLMTDEVSSN	한 사용자가 동일한 사용자 프로파일로 두 개 이상의 워크스테이션에 사인 온할 수 있는지를 판별합니다.
QINACTITV	시스템이 비활동 작업에 대해 조치를 취하는 시기를 판별합니다.
QINACTMSGQ	대화식 작업이 QINACTITV 시스템 값으로 지정한 시간 동안 비활동 상태로 있을 때 시스템이 취할 조치를 판별합니다.
QDSCJOBITV	시스템이 일시적으로 단절된 작업을 종료하는지와 그 종료 시기를 제어합니다.
QLMTSECOFR	시스템의 모든 오브젝트에 대해 권한을 갖고 있는 보안 담당자를 특정 장치로 제한합니다.

사인 온 시도 횟수 제한(QMAXSIGN 및 QMAXSGNACN)

다음에 나오는 두 개의 시스템 값은 시스템에 사인 온을 시도할 수 있는 횟수와 한계에 도달할 때 시스템이 취할 조치를 판별합니다.

QMAXSIGN(최대 사인 온 시도 횟수) 시스템 값은 조치를 취하기 전에 시스템이 허용하는 올바르지 않은 연속적인 사인 온 시도 횟수를 제한합니다. 올바르지 않은 사인

온 시도 횟수는 누군가 워크스테이션에 유효하지 않은 암호나 부적절한 권한으로 특정 사용자의 프로파일을 사용하려고 했다는 것을 의미합니다.

최대 사인 온 조치(QMAXSGNACN) 시스템 값은 누군가 연속적으로 너무 많은 사인 온을 시도하는 경우 시스템이 어떻게 할 것인지를 지정합니다. 사용할 수 있는 값은 다음과 같습니다.

1 장치에 대한 더 이상의 사인 온 시도를 막습니다. 이것을 장치를 작동 불가능하게 한다라고 합니다. 이 경우 권한이 있는 사용자가 WRKCFGSTS 명령을 사용하여 장치를 변경할 때까지 누구도 그 장치에 사인 온할 수 없습니다. 일반적으로 이 옵션은 충분한 보호가 아니며, 특히 퍼스널 컴퓨터나 리모트 시스템에서 시스템에 사인 온을 시도할 때 발생합니다.

시스템 오퍼레이터나 장치에 대해 *USE 권한을 가진 사용자가 다시 장치를 사용할 수 있게 만들 수 있습니다.

2 사용자 프로파일에 대한 더 이상의 사인 온 시도를 막습니다. 이것을 사용자 프로파일을 작동 불가능하게 한다라고 합니다. 권한을 가진 사람이 CHGUSRPRF(사용자 프로파일 변경) 명령을 사용하여 사용자 프로파일을 다시 사용할 수 있게 만들 때까지 누구도 그 프로파일에 사인 온할 수 없습니다.

사용자 프로파일을 사용할 수 있게 만들려면(상태를 변경하려면) 사용자가 프로파일을 사용할 권한을 가진 보안 관리자이어야 합니다.

3 사용자 프로파일과 장치 모두를 작동 불가능하게 합니다.

위험 및 권장사항

문제를 일으키는 몇몇 사람들이 암호를 추측하여 시스템 안으로 침입하는 것을 즐깁니다. 이 경우 허용되는 사인 온 시도 횟수를 제한하여 추측을 위한 시도를 제한할 수 있습니다.

유효하지 않은 최대 사인 온 횟수(QMAXSIGN) 시스템 값은 허용되는 사인 온 시도 횟수를 판별합니다. 사용자들이 실망하지 않도록 높은 값을 설정하십시오. 그러나 부주의한 입력을 막고 침입자에게 추측할 수 있는 많은 기회를 제공하지 않도록 적당히 낮은 값을 설정해야 합니다. 최대 사인 온 횟수를 3-5로 설정하십시오.

사용자 프로파일을 포함하여 장치를 작동 불가능하게 할 경우 시스템 사용자에게 불편을 초래할 수 있으나 권장되는 QMAXSGNACN(최대 사인 온 조치)은 3입니다. 사적인 장소에 있는 워크스테이션은 침입자에게 서로 다른 사용자 프로파일 및 암호 조합을 시도할 수 있는 기회를 제공합니다. 장소로 인한 위험을 초래할 가능성이 있는 워크스테이션이 없으면 사용자 프로파일만 작동 불가능하게 만들어서 충분히 보호할 수 있습니다.

전에 완료한 물리적 보안 양식을 검사하십시오. 리모트 위치에 워크스테이션이 있거나 리모트 사용자(전화 회선 또는 VPN 연결을 통해 시스템에 액세스하는 사용자)가 있으

면 사인 온을 보다 엄격히 제한할 수 있습니다. 시스템 값 선택 양식의 파트 2에 QMAXSIGN 및 QMAXSGNACN에 대한 선택사항을 반드시 추가하십시오.

한 번에 하나의 워크스테이션으로 사용자를 제한하는 시스템 값을 선택하기 전에 이 시스템 값들이 사인 온 시도를 제한하기 위해 어떻게 함께 작업하는지를 보여주는 예를 검토하는 것이 유용합니다.

사인 온 시도 횟수 제한 예: Sharon Jones가 사인 온 시도 횟수를 3(QMAXSIGN이 3)으로 제한하고 제한을 초과할 경우(QMAXSGNACN이 3) 프로파일과 장치 모두를 작동 불가능 상태로 만들 것을 선택했습니다. 이 값에 도달하면 다음과 같은 일이 발생할 수 있습니다.

1. Roger가 정확하지 않은 암호를 두 번 입력합니다.
2. 두 번째 시도 후에도 Roger가 올바른 사인 온 시도를 하지 않으면 사용자 프로파일이 작동 불가능하게 된다는 것을 경고하는 메세지를 수신합니다.
3. Roger가 또 다시 올바르지 않은 암호를 입력합니다.
4. 시스템이 그의 프로파일을 작동 불가능으로 만들고 워크스테이션에는 더 이상 사인 온 화면이 나오지 않습니다. Roger가 다른 워크스테이션에서 사인 온을 시도하면 오류 메세지를 수신합니다.
5. 이제 Roger는 Sharon에게 프로파일을 재시도할 수 있게 조치해 줄 것을 요청해야 합니다. Sharon이나 시스템 운영자도 Roger의 워크스테이션을 사용할 수 있도록 조치해야 합니다. Roger가 암호를 잊은 경우 Sharon이 임시 암호를 부여할 수 있으나 Roser가 다시 사인 온할 때 암호를 변경해야 합니다.

다음에는 한 번에 하나의 워크스테이션으로 사용자를 제한하는 시스템 값을 검토할 수 있습니다.

한 번에 하나의 워크스테이션으로 사용자 제한

QLMTDEVSSN(장치 세션 제한) 시스템 값은 동일한 사용자가 동시에 두 개 이상의 워크스테이션에 사인 온할 수 있는지 여부를 판별합니다. 사용할 수 있는 값은 다음과 같습니다.

0 사용자 수에 제한 없이 동일한 사용자 프로파일로 동시에 시스템에 사인 온할 수 있도록 합니다.

1 한 번에 하나의 장치만 사용자 프로파일을 사용할 수 있습니다. 사용자가 동일한 장치에 두 개 이상의 세션을 가질 수 있습니다.

위험 및 권장사항

사용자가 한 번에 하나의 워크스테이션에만 사인 온할 수 있도록 하는 것이 좋은 보안 습관을 기르는 것입니다. 나태한 보안 습관은 보안 위험을 초래합니다.

- 사용자를 하나의 장치로 제한하면 사용자들이 ID와 암호를 공유하지 못합니다. 사람들이 사용자 ID를 공유하면 제어 및 책임 둘다 놓칠 수 있습니다. 실제로 시스템에서 누가 어떤 기능을 수행하는지 더 이상 알 수 없습니다.
- 다른 워크스테이션으로 이동하기 전에 한 워크스테이션을 사인 오프하는 것을 잊어서는 안됩니다. 사인 온 상태로 사용되지 않는 워크스테이션에는 보안 위험이 따릅니다.

시스템 값 QLMTDEVSSN에 권장되는 설정 값은 1이며 이 값은 사용자들을 하나의 장치로 제한합니다. 각 시스템 사용자에게 적절한 권한과 함께 고유 사용자 ID와 암호를 부여한 후 한 번에 하나의 워크스테이션을 사용하도록 제한하십시오. 시스템 값 선택 양식의 파트 2에 QLMTDEVSSN에 대한 선택사항을 반드시 추가하십시오.

다음으로 비활동 작업에 대한 시스템 값 계획을 수립할 수 있습니다.

비활동 작업에 대한 시스템 값 계획

다음에 나오는 세 개의 시스템 값은 사용자가 워크스테이션을 사인 오프하는 것을 잊었을 때 시스템이 취할 조치를 판별합니다.

비활동 작업 시간 종료 간격(QINACTITV)

QINACTITV 시스템 값은 표시장치를 사인 온했으나 지정 시간 동안 비활동 상태로 있을 때 시스템이 조치를 취하는지의 여부를 판별합니다.

주: **비활동** 상태는 사용자가 지정 시간 동안 Enter 키나 기능 키를 누르지 않았음을 의미합니다.

QINACTMSGQ(비활동 작업 메세지 대기행렬)

QINACTMSGQ 시스템 값에 대한 설정은 시스템 값 QINACTITV에서 지정하는 시간 제한이 만료할 때 시스템이 취할 조치를 판별합니다. ENDJOB을 선택하면 QINACTITV에 대해 사용자가 선택한 시간 종료 간격보다 더 오랜 시간 동안 비활동 상태로 있던 작업을 종료합니다. DSCJOB을 선택하면 시스템이 비활동 작업을 단절시킵니다. 메세지 대기행렬명을 지정하면 너무 오랜 동안 작업이 비활동 상태로 있을 때 시스템이 그 대기행렬로 경고 메세지를 보냅니다.

시스템이 워크스테이션에서 작업을 **단절**시키면 그 작업이 일시중단됩니다. 워크스테이션이 사인 온 화면으로 리턴합니다. 같은 사용자가 같은 워크스테이션에 다시 사인 온할 때 단절시켰던 작업이 재개됩니다.

QDSCJOBITV(단절된 작업 시간 종료 간격)

QDSCJOBITV 시스템 값은 시스템이 일시적으로 단절시킨 작업을 종료하는지 그리고 언제 종료하는지를 제어합니다. QINACTITV 및 QINACTMSGQ 시스템 값의 결과에 따라 시스템이 자동으로 작업을 단절시킬 수 있습니다. 또한 사용자들이 운영 지원 메뉴의 옵션이나 DSCJOB(작업 단절) 명령을 사용하여 작업이 일시적으로 사인 오프(단절)되도록 요구할 수 있습니다.

위험 및 권장사항

Sharon이 나가기 전에 워크스테이션을 사인 오프할 것을 잊은 경우 John이 워크스테이션으로 가서 Sharon에게 허용된 기능을 수행할 수 있습니다.

특히 다음의 두 경우 비활동 표시장치를 잘 관리해야 합니다.

- 시스템에 기밀 정보가 저장되어 있는 엄격한 보안 환경에 처해 있습니다.
- 회사 밖의 사용자들이 쉽게 액세스할 수 있는 장소에 워크스테이션이 있습니다.

때로는 정상적인 작업들이 워크스테이션의 사용자들을 인터럽트합니다. 다음에 나오는 세 개의 시스템 값은 정상적인 인터럽트를 허용하면서 계속해서 시스템 보안을 유지하기 위해 함께 작업하는 값입니다.

여러 가지 위험 요소를 없애기 위해 IBM에서는 QINACTITV, QINACTMSGQ, QDSCJOBITV 시스템 값을 함께 사용하여 정상적인 작업 인터럽트를 허용하고 시스템 보안을 유지할 것을 권장합니다.

QINACTITV(비활동 작업 시간 종료 간격): 워크스테이션을 무인 상태로 만들지 않되 사용자에게 불편을 초래하지 않을 정도의 짧은 간격을 설정하십시오. 권장 설정값은 30분입니다. 작업이 30분 동안 비활동 상태로 있으면 시스템이 비활동 작업 메세지 대기행렬에 지정된 조치를 취합니다.

QINACTMSGQ(비활동 작업 메세지 대기행렬): 작업 단절을 선택하십시오. 시스템이 비활동 작업 시간 종료 간격에 지정된 시간 동안 비활동 상태로 있던 작업을 단절시킵니다. 시스템이 작업을 일시중단하고 표시장치를 사인 오프합니다. 같은 사용자가 다시 사인 온할 경우 단절 위치에서부터 다시 작업이 계속됩니다.

이것은 시스템이 작업을 종료하지 않고 일시중단시키는 것이므로 사용자에게 더 편리합니다. 비활동 작업을 단절하는 것은 작업을 종료하는 것 만큼 시스템에 많은 보호를 제공합니다.

주: 일부 작업은 시스템이 단절시킬 수 없습니다. 그러나 시스템이 비활동 작업을 단절시킬 수 없으면 시스템이 그 작업들을 대신 종료합니다. 이 경우 정보을 유실할 수 있습니다. 시스템 오퍼레이터 메세지 대기행렬로 메세지를 송신하는 QINACTMSGQ를 설정할 것을 고려하십시오.

QDSCJOBITV(단절된 작업 시간 종료 간격): 시스템 사용자가 잠시 워크스테이션을 떠나 있어야 하거나 작업을 완료하고 장시간의 인터럽트를 위해 사인 오프시켜야 할 경우 일시적으로 시스템을 사인 오프시키는 것이 좋습니다.

시스템이 야간 처리(예: 자동 클린업)를 시작하기 전에 QDSCJOBITV를 사용하여 단절시켰던 작업을 종료하십시오. 워크스테이션으로 리턴하기 위해 업무 시간의 대부분을

사용자에게 부여할 정도로 길지만 야간 처리가 시작되기 전에 작업을 종료할 수 있을 정도의 짧은 값을 설정하십시오. 사용자의 작업을 방해하지 않고 야간 처리를 완료하기에 충분한 300분(5시간)을 선택하십시오.

주: 두 명의 사용자가 동시에 같은 정보를 변경하지 못하도록 하기 위해 시스템은 레코드를 갱신하기 전에 **잠급니다**. 자원에 대한 잠금 처리는 시스템이 사용자의 작업을 단절할 때에도 계속해서 유효합니다. 어플리케이션 설계 및 시스템 사용자 수에 따라서는 잠금 처리로 인해 시스템에 성능 문제가 발생할 수 있습니다. 프로그래머나 어플리케이션 제공자와 의논하여 잠금 처리가 성능에 영향을 미치는지 알아보십시오.

시스템에서 비활동 작업을 처리하기 위해 이 시스템 값이 어떻게 작업하는지에 관한 예를 검토할 수 있습니다.

시스템 값 선택 양식에 비활동 작업을 위한 결정사항을 기록했으면 보안 담당자가 사인 온할 수 있는 위치를 제한하기 위한 방법을 결정할 수 있습니다.

예: QINACTITV, QINACTMSGQ 및 QDSCJOBITV 시스템 값으로 비활동 작업 처리: 비활동 작업 시간 종료 간격(QINACTITV)을 30분으로 설정했다고 가정하십시오. 시스템이 비활동 작업(QINACTMSGQ가 DSCJOB임)을 단절시킵니다. 단절된 작업의 시간 종료 간격(QDSCJOBITV)은 300분(5시간)입니다. 예를 들어, Sharon이 오전 9시 30분에 사인 오프하는 것을 잊은 경우 시스템이 오전 10시 정각에 작업을 단절시키며 오후 3시에 작업을 종료시킵니다.

시스템 값 선택 양식의 파트 2에서 QINACTITV, QINACTMSGQ 및 QDSCJOBITV 시스템 값을 위한 선택사항을 추가하십시오.

시스템 값 선택 양식에 비활동 작업을 위한 결정사항을 기록했으면 보안 담당자가 사인 온할 수 있는 위치를 제한하는 방법을 결정할 수 있습니다.

보안 담당자가 사인 온할 수 있는 위치 제한

특정 워크스테이션에 대한 보안 및 제어 오브젝트를 변경할 수 있는 권한을 가진 사용자들을 제한할 경우가 있습니다. 이렇게 하면 사용자가 모르는 사이에 이 사람이 리모트 위치의 워크스테이션에 사인 온하지 못합니다. 시스템 값 QLMTSECOFR(보안 담당자 제한)을 사용하여 이와 같이 할 수 있습니다. QLMTSECOFR을 1로 설정하면 모든 오브젝트(*ALLOBJ) 또는 서비스(*SERVICE) 특수 권한을 가진 사용자들이 지정 콘솔이나 기타 워크스테이션에서만 사인 온할 수 있습니다.

QLMTSECOFR은 보안 담당자, 시스템의 모든 오브젝트에 대한 권한을 가진 사용자, 콘솔에 대한 서비스 요원을 제한합니다. GRTOBJAUT(오브젝트 권한 부여) 명령으로 이 사용자들이 다른 장치에 액세스하도록 할 수 있습니다.

주: QLMTSECOFR 시스템 값을 작동시키기 위해서는 시스템 보안 레벨이 30 이상이어야 합니다.

위험 및 권장사항

QLMTSECOFR 시스템 값은 1로 설정하십시오. 누군가가 보안 담당자 프로파일을 가진 사용자의 암호를 엿듣거나 추측할 경우 사인 온이 허용된 장치의 액세스도 얻을 수 있습니다.

시스템 값 선택 양식의 파트 2에 QLMTSECOFR에 대한 선택사항을 채웠으면 암호에 영향을 주는 시스템 값을 선택할 수 있습니다.

암호에 영향을 주는 시스템 값 선택

자신의 암호를 지정하는 것은 암호를 할당하는 보안 담당자가 아니라 사용자 자신이 할당할 수 있도록 해야 합니다. 사용자들이 자신의 암호를 작성할 경우 본인이 이 암호를 기록할 필요가 없습니다. 암호를 기록하게 되면 추측하기 쉬운 장소에 보관하는 경향이 있으므로 이로 인해 보안이 노출될 수 있습니다.

암호 작성을 위한 추가 정보

사용자들이 좋은 암호가 어떤 것인지를 생각하는 데 곤란을 겪을 수 있습니다. 그러나 기억하기 쉬운 문장을 사용하면 추측하기 어려운 암호를 작성할 수 있습니다. 예를 들어, 휴가를 마친 후라면 ″July 4th fishing was poor″라는 문장을 사용하여 J4FWP라는 암호를 작성할 수 있습니다.

일부 시스템 값이 암호를 조절합니다. 사용자들이 암호를 변경해야 하는 빈도를 제어할 수 있습니다. 또한 추측하기 쉬운 암호를 사용하지 못하도록 많은 규칙을 설정할 수도 있습니다. 이 시스템 값 중 다수가 대규모 조직체에서 중요합니다. 그 중에 일부는 모든 사람에게 중요합니다.

ASSIST 메뉴에서 옵션을 사용하거나 CHGPWD(암호 변경) 명령을 사용하여 사용자가 자신의 고유 암호를 할당할 수 있습니다. 사용자가 자신의 고유 암호를 변경할 때 시스템이 신규 암호를 암호 시스템 값과 비교하여 검사합니다. 사용자가 CHGUSRPRF 명령을 사용하여 암호를 변경하면 시스템이 신규 암호를 보안 시스템 값과 비교하여 검사하지 않습니다.

주: 암호 시스템 값을 설정한 경우에는 CHGUSRPRF 명령을 사용하여 암호를 설정하지 않는 한 시스템이 신규 암호가 사용자 프로파일명과 같아지는 것을 허용하지 않습니다.

아래 표는 암호 및 암호 정의에 영향을 주는 시스템 값을 표시한 것입니다.

표 12. iSeries 암호 관련 시스템 값

시스템 값	설명
QPWDEXPITV	지정된 기간이 경과하면 사용자가 암호를 변경해야 합니다.
QPWDMAXLEN	암호에 최대 문자 길이를 지정할 수 있도록 허용합니다.
QPWDMINLEN	암호에 최소 문자 길이를 지정할 수 있도록 허용합니다.
QPWDRQDDIF	사용자가 두 개의 다른 암호를 교대로 사용하지 못하게 합니다.

다음 주제는 암호와 관련된 시스템 값에 관해 자세한 정보를 제공합니다.

- 암호 기간 판별
- 암호 길이 판별
- 중복 암호 제한

CL 명령행에 WRKSYSVAL *SEC를 입력하고 문자 QPWD로 시작하는 시스템 값에 대한 온라인 정보를 보십시오.

암호 기간 판별

QPWDEXPITV 시스템 값은 사용자가 암호를 변경해야 하는 빈도를 판별합니다.

암호 만기일이 다가오면 시스템이 사용자에게 경고를 합니다. 암호가 만기되면 사용자가 다음 사인 온할 때 암호를 변경하도록 시스템이 프롬트를 제공합니다.

권장사항

사용자는 암호를 주기적으로 변경해야 합니다. 이렇게 하면 다른 시스템 사용자와 암호를 공유하기가 어렵습니다. 또한 권한이 없는 사용자가 누군가의 암호를 알게 되더라도 짧은 기간 동안만 그 암호를 사용할 수 있습니다. 사용자를 귀찮게 하지 않으면서 훌륭한 보안을 제공하는 정도의 짧은 암호 간격을 설정하십시오. 이와 같은 문제점을 피하려면 간격을 45 - 60일로 설정하십시오.

시스템 값 선택 양식의 파트 2에 QPWDEXPITV 시스템 값의 선택사항을 입력했으면 암호의 길이를 판별할 수 있습니다.

암호 길이 판별

일부 사용자들은 입력하는 것을 싫어합니다. 이와 같은 사용자들을 그대로 방치할 경우 한 자로 된 암호나 이름의 머릿글자를 암호로 선택할 것입니다. 불행하게도 짧은 암호는 침입자들이 추측하기가 쉽습니다. QPWDMINLEN 시스템 값은 시스템의 모든 암호에 대해 최소 길이를 설정하게 해줍니다.

사용 중인 시스템이 다른 시스템과 통신하면 사용자들이 두 컴퓨터간에 암호를 교환할 수 있습니다. 일부 통신 방법들은 암호를 최대 8자로 제한합니다. QPWDMAXLEN 시스템 값을 사용하여 최대 암호 길이를 지정할 수 있습니다.

권장사항

최소 암호 길이를 6으로 설정하십시오. 이렇게 하면 머릿글자를 사용하지 못하며 사용자들이 보다 독창적인 암호를 선택할 수 있습니다. 사용 중인 시스템이 다른 시스템과 통신하면 최대 암호 길이를 8로 설정하십시오.

시스템 값 선택 양식의 파트 2에 QPWDMINLEN 및 QPWDMAXLEN 시스템 값의 선택사항을 기록했으면 중복 암호를 제한하는 정도를 결정할 수 있습니다.

중복 암호 제한

CHGPWD(암호 변경) 명령은 신규 암호가 이전 암호와 다른 암호일 것을 요청합니다. 그러나 사용자가 QPWDRQDDIF 시스템 값을 사용하여 방지하지 않으면 두 개의 서로 다른 암호를 앞 뒤로 대체시킬 수 있습니다. 아래 표는 QPWDRQDDIF 시스템 값에 대한 선택사항을 표시합니다.

표 13. QPDRQDDIF 시스템 값에 대한 값

값	중복 확인되는 암호 수
0	0 중복 암호를 허용합니다.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

권장사항

1년 동안 암호를 고유하게 만들려면 암호 만기 간격 및 중복 암호 값을 사용하십시오. 예를 들어, 암호가 60일 후에 만기가 되면 QPWDRQDDIF 시스템 값을 7로 선택하십시오.

시스템 값 선택 양식의 파트 2에 QPWDRQDDIF 시스템 값의 선택사항을 기록했으면 시스템 값을 사용하여 시스템 사용자 정의를 수행하는 방법을 결정할 수 있습니다.

시스템 사용자 정의를 위해 시스템 값 사용

iSeries는 시스템 값 및 네트워크 속성을 사용하여 보안 이외에 많은 것을 제어합니다. 시스템 프로그래머와 어플리케이션 프로그래머들이 이 시스템 값 및 속성의 대부분을 사용합니다. 보안 담당자는 일부 시스템 값 및 네트워크 속성을 설정하여 시스템을 사용자 정의합니다.

시스템명 지정

SYSNAME 네트워크 속성을 사용하여 시스템에 이름을 할당하십시오. 시스템명은 사인 온 화면의 우측 상단과 시스템 보고서에 나옵니다. 또한 시스템명은 Windows용 iSeries Access를 사용하여 시스템이 다른 시스템이나 퍼스널 컴퓨터와 통신할 때 사용됩니다.

시스템이 다른 시스템이나 퍼스널 컴퓨터와 통신할 때 시스템명이 사용자의 시스템을 식별하여 네트워크의 다른 시스템과 구별합니다. 컴퓨터는 통신할 때마다 시스템명을 교환합니다. 일단 시스템명을 할당하면 시스템명을 변경할 경우 네트워크의 다른 시스템에 영향을 받을 수 있으므로 시스템명을 변경해서는 안됩니다.

권장사항

시스템에는 의미가 있는 고유한 이름을 선택하십시오. 다른 컴퓨터와 현재 통신하고 있지 않더라도 향후에 통신할 수 있습니다. 시스템이 네트워크의 한 부분이면 네트워크 관리자가 사용할 시스템명을 알려줄 것입니다.

예를 들어, JKL Toy사의 Sharon Jones는 시스템을 JKLTOY로 부르기로 했습니다.

시스템에 시간 및 날짜 표시

시스템이 날짜를 인쇄하거나 표시할 때 년, 월, 일이 표시되는 순서를 설정할 수 있습니다. 시스템이 년(Y), 월(M), 일(D)에 사용해야 하는 문자도 지정할 수 있습니다.

시스템 값 QDATFMT는 날짜 형식을 판별합니다. 다음 표는 시스템이 선택할 수 있는 형식으로 2000년 6월 16일을 인쇄하는 방법을 보여줍니다.

표 14. QDATFMT(시스템 날짜 형식)

사용자 선택사항	설명	결과
YMD	년, 월, 일	00/06/16
MDY	월, 일, 년	06/16/00
DMY	일, 월, 년	16/06/00
JUL	율리우스력 날짜	00/168

주: 이 예에서는 슬래시(/) 날짜 분리자를 사용합니다.

시스템 값 QDATSEP는 시스템이 년, 월, 일간에 사용하는 문자를 판별합니다. 아래 표는 선택사항을 표시합니다. 번호로 선택하십시오.

표 15. QDATSEP(시스템 날짜 분리자)

분리 문자	**QDATSEP 값**	결과
/(슬래시)	1	16/06/00
-(하이픈)	2	16-06-00
. (마침표)	3	16.06.00
,(쉼표)	4	16,06,00

표 15. QDATSEP(시스템 날짜 분리자) (계속)

분리 문자	**QDATSEP 값**	결과
(공백)	5	16 06 00

주: 위의 예에서는 DMY 형식을 사용합니다.

QTIMSEP 시스템 값은 시스템이 시간을 표시할 때 시, 분, 초를 분리하기 위해 사용하는 문자를 판별합니다. 숫자를 사용하여 선택하십시오. 아래 표는 각 값을 사용하여 오전 10:30을 형식화하는 방법을 표시합니다.

표 16. QTIMSEP(시스템 시간 분리자)

분리 문자	**QTIMSEP**	결과
:(콜론)	1	10:30:00
. (마침표)	2	10.30.00
,(쉼표)	3	10,30,00
(공백)	4	10 30 00

시스템 장치 명명 방법 결정

시스템이 자동으로 신규 표시장치와 접속 프린터를 구성합니다. 그리고나서 시스템이 각 신규 장치에 이름을 부여합니다. QDEVNAMING 시스템 값이 이름이 할당되는 방법을 판별합니다. 아래 표는 접속된 세 번째 표시장치와 두 번째 프린터를 시스템이 명명하는 방법을 표시합니다.

표 17. 시스템 장치 명명

사용자 선택사항	명명 형식	표시장치명	프린터명
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	장치 주소	DSP010003	PRT010002

주: 위의 예에서, 표시장치와 프린터는 첫 번째 케이블에 접속되어 있습니다.

권장사항

S/36 명명 처리가 필요한 소프트웨어를 실행하는 경우를 제외하고는 iSeries 명명 규칙을 사용하십시오. 표시장치 및 프린터에 있어서 iSeries 이름들이 장치 주소를 사용하는 이름보다 더 편리합니다. 표시장치명과 프린터명은 여러 운영 지원 화면에 나옵니다. 프린터 이름은 프린터 출력 관리에도 사용됩니다.

시스템이 신규 장치를 구성했으면 CHGDEVDSP(표시장치 변경) 명령이나 CHGDEVPRT(프린터 장치 변경) 명령을 사용하여 장치에 대해 의미있는 설명을 입력하십시오. 설명에 장치의 물리적 주소와 장치 위치(예: *John Smith의 사무실, 회선 1, 주소 6*) 모두를 포함시키십시오.

시스템 프린터 선택

QPRTDEV 시스템 값을 사용하여 시스템 프린터를 할당하십시오. 이 시스템 값, 사용자 프로파일, 작업 설명이 작업에 사용되는 프린터를 판별합니다. 사용자 프로파일이나 작업 설명이 다른 프린터를 지정하지 않는 한 작업에서 시스템 프린터를 사용합니다.

권장사항

보통은 시스템 프린터가 시스템에 있는 가장 빠른 프린터이어야 합니다. 긴 보고서 및 시스템 출력에는 시스템 프린터를 사용하십시오.

주: 시스템을 설치하여 구성할 때까지 프린터명을 알 수 없습니다. 현재 시스템 프린터의 위치를 적어두십시오. 나중에 프린터명을 채우십시오.

완료된 프린터 출력 표시 허용

시스템이 사용자가 프린터 출력을 찾을 수 있는 기능을 제공합니다. 프린터 출력에 대한 작업 화면에 현재 인쇄 중이거나 인쇄 대기 중인 모든 출력이 나옵니다. 또한 완료된 프린터 출력 리스트를 볼 수도 있습니다. 이 화면은 출력이 언제 인쇄되었는지 그리고 어떤 프린터에서 인쇄했는지를 표시합니다. 이것은 없어진 보고서를 찾을 때 유용합니다.

사용자가 작업 사용 통계 기능 및 QACGLVL 시스템 값을 사용하여 완료된 프린터 출력을 표시할 수 있습니다. QACGLVL 시스템 값에 *PRINT 옵션을 사용하면 완료된 프린터 출력에 관한 정보를 저장할 수 있습니다.

권장사항

완료된 프린터 출력에 관한 정보를 저장할 경우 시스템에서 일정 공간을 차지하게 됩니다. 많은 보고서를 사용자들이 인쇄할 것으로 생각되지 않으면 이 기능을 제공할 필요가 없습니다. 시스템 값 선택 양식에 NO를 입력하십시오. 이 값은 작업 사용 통계 레벨을 *NONE으로 설정합니다.

- Sharon Jones와 John Smith가 준비했던 JKL Toy사의 예와 유사한 회사 보안 정책 발표문을 작성했는지 확인하십시오.
- 시스템 값 선택 양식에 시스템 값에 대한 선택사항을 입력했는지 확인하십시오.
- 보안 메모에 포함시킬 내용을 기록하십시오.

시스템 값 선택 양식에 시스템 옵션 모두를 입력하고 보안 정책을 작성했으면 사용자 그룹 계획을 수립할 수 있습니다.

예: JKL Toy사의 보안 정책

아래의 메모는 JKL Toy사의 사장인 John Smith가 직원들에게 보내는 보안 정책을 설명한 것입니다. John은 이 보안 메모를 작성할 때 Sharon과 함께 기록했던 주를 사용합니다.

표 18. 예: JKL Toy사의 보안 메모

발신: John Smith, 사장

JKL Toy사

수신: JKL Toy사 전직원

제목: 신규 시스템 보안건

여러분 모두 새로 도입되는 시스템에 관한 정보 회의에 참석하셨습니다. 그 시스템을 사용하는 사람들은 소정의 교육을 마친 후 다음 주부터 고객 주문 처리를 시작할 것입니다. 새로 도입한 시스템이 우리의 사업을 성공으로 이끄는 중요한 역할을 할 수 있기를 기대합니다.

이제 보안 관련 결정사항 및 정책들을 검토하고 그것의 중요성을 강조하고자 합니다. 이 정책은 회사의 중요한 정보를 보호하기 위해 구상된 것입니다.

- Sharon Jones가 신규 시스템의 보안을 담당합니다. 그리고 Ken Harrison이 그녀를 보조할 것입니다. 질문 사항이나 보안 관련 문제가 발생할 경우 그들에게 문의하십시오.
- 시스템의 각 기능을 수행할 사람에 관한 결정사항은 정보와 관련하여 현재 우리의 정책에 기초하고 있습니다. 예를 들면, 다음과 같습니다.
  - 계약 및 특별가 책정 정보는 기밀로 간주합니다. 그와 같은 정보가 회사 외부인에게 알려져서는 안됩니다.
  - 회계 부서에서만 고객의 대변 한도를 설정하고 변경할 수 있습니다.
- 시스템을 사용해야 할 사람들에게는 사용자 ID와 암호를 발급할 것입니다. 처음에 시스템에 사인 온할 때 그리고 60일마다 암호를 변경하도록 요청받을 것입니다. 기억할 수 있는 암호를 선택하되 너무 쉬운 암호는 사용하지 마십시오. 사용자 ID와 함께 여러분이 받게 될 양식에 암호를 작성할 때의 몇 가지 제안사항이 있습니다.
- *다른 사람과 암호를 공유하지 마십시오.* 우리는 여러분의 업무에 필요한 모든 것이 시스템에서 가능하도록 배려했습니다. 정보에 액세스해야 할 경우 Sharon이나 Ken에게 문의하십시오. 또한 암호를 잊어버렸으면, Sharon 이나 Ken이 즉시 신규로 발급해줍니다. 다른 사용자의 ID와 암호로 사인 온해야 할 이유가 없습니다.
- 여러분 중에 대다수는 입력한 것을 저장하기 위해 워크스테이션의 레코드 및 재생 기능을 사용하는 방법에 관해 배웠을 것입니다. 그러나 암호 저장을 위해 이 기능을 절대로 사용하지 *마십시오.*
- 자리를 비울 때 사인 온 상태로 워크스테이션을 떠나지 마십시오. 교육을 통해 워크스테이션에서 일시적으로 사인 오프하는 방법을 배웠을 것입니다. 잠시 자리를 비울 경우에는 이 기능을 사용하십시오. 만약 오랜 시간 자리를 비워야 한다면 작업을 종료하고 정상적인 사인 오프를 사용하십시오.

  출고지, 고객 서비스 영역, 영업 지사와 같이 일반인들이 쉽게 접근할 수 있는 곳에서는 워크스테이션에서 자리를 비울 때 사인 오프를 하는 것이 특히 중요합니다.
- 시스템 장치가 단단한 것이기는 하지만, 시스템을 치거나 위에 물건을 올리는 일은 삼가하십시오. 장치의 제어판은 일반적으로 비활성화되어 있지만 손대지 마십시오. 회계 부서의 직원들에게는 사람들이 시스템 장치를 함부로 건드리지 못하게 할 책임이 있습니다.

신규 시스템은 우리의 모든 작업을 더 쉽게 만들어 주고 작업 능률을 향상시키기 위한 것임을 명심하십시오. 보안 정책은 여러분에게 도움을 주기 위한 것이며 방해하기 위한 것이 아닙니다. 이와 관련된 질문이 있으면 주저하지 말고 Sharon이나 Ken 또는 제게 문의하십시오.

보안 정책의 초안을 작성했으면 사용자 그룹 계획을 시작할 수 있습니다.

사용자 그룹 계획

보안 전략을 결정하는 계획 프로세스의 첫 번째 단계는 회사 정책을 결정하는 것과 유사합니다. 이제 사용자 그룹을 계획할 준비가 되었으며 이것은 부서 정책을 결정하는 것과 유사합니다.

사용자 그룹이란?

사용자 그룹은 이름이 암시하는 것과 똑같습니다. 즉, 같은 방법으로 같은 어플리케이션을 사용해야 하는 사용자들의 그룹입니다. 일반적으로 사용자 그룹은 같은 부서에서 일하는 사용자들로 이루어지며 비슷한 업무를 담당합니다. 그룹 프로파일을 작성하여 사용자 그룹을 정의하십시오.

그룹 프로파일이 하는 일은?

그룹 프로파일은 시스템에서 두 가지 목적으로 사용됩니다.

- **보안 툴:** 그룹 프로파일은 시스템에서 특정 오브젝트를 사용할 수 있는(오브젝트 권한) 사람들을 조직하는 간단한 방법을 제공합니다. 오브젝트 권한을 그룹의 개별 멤버 각각에 대해서가 아니라 전체 그룹에 대해 정의할 수 있습니다.
- **사용자 정의 툴:** 그룹 프로파일을 개별 사용자 프로파일을 작성하기 위한 하나의 패턴으로 사용할 수 있습니다. 같은 그룹에 속하는 대부분의 사용자가 같은 사용자 정의 요구(예: 초기 메뉴 및 디폴트 프린터)를 갖습니다. 이 요구를 그룹 프로파일에 정의하여 개별 사용자 프로파일로 복사할 수 있습니다.

그룹 프로파일을 사용하여 보안과 사용자 정의 모두에 대해 간단하고 일관된 계획을 보다 쉽게 유지보수할 수 있습니다.

필요한 양식은?

다음은 사용자 그룹을 계획할 때 필요한 양식입니다.

- 사용자 그룹 식별 양식
- 사용자 그룹 설명 양식

  주: 시스템에 놓일 각 사용자 그룹에 대해 하나의 사용자 그룹 설명 양식이 필요합니다.

이 양식을 완료하려면 다음 주제를 참조하십시오.

- 사용자 그룹 식별
- 그룹 프로파일 계획
- 사인 온에 영향을 주는 값 선택
- 사용자가 수행할 수 있는 작업을 제한하는 값 선택
- 사용자의 환경을 설정하는 값 선택

사용자 그룹 식별

사용자 그룹 계획을 수립하기 위해서는 먼저 시스템에서 사용자 그룹을 식별해야 합니다. 이것은 이 그룹이 필요로 하는 자원에 대한 액세스를 계획할 수 있게 해줍니다. 사용자 그룹을 식별할 때에는 간단한 방법을 사용하도록 하십시오. 시스템을 사용할 부서나 작업 그룹에 관해 생각해보십시오. 이전에 그린 어플리케이션 다이어그램을 보십시오. 작업 그룹과 어플리케이션간의 관계가 자연스러운지 확인하십시오.

- 각 작업 그룹에 대해 1차 어플리케이션을 식별할 수 있습니까?
- 각 그룹이 필요로 하는 어플리케이션을 알고 있습니까? 필요 없는 어플리케이션은 어느 것입니까?
- 각 어플리케이션 라이브러리에서 정보를 소유해야 하는 그룹을 알고 있습니까?

이 질문에 "예"라고 응답할 수 있다면 사용자 그룹 계획을 시작할 수 있습니다. 그러나 "경우에 따라서" 또는 "아마도"라고 응답했다면 체계적인 접근방식으로 사용자 그룹을 식별하는 것이 도움이 될 것입니다.

체계적인 접근방식으로 사용자 그룹을 식별하는 예를 검토하십시오.

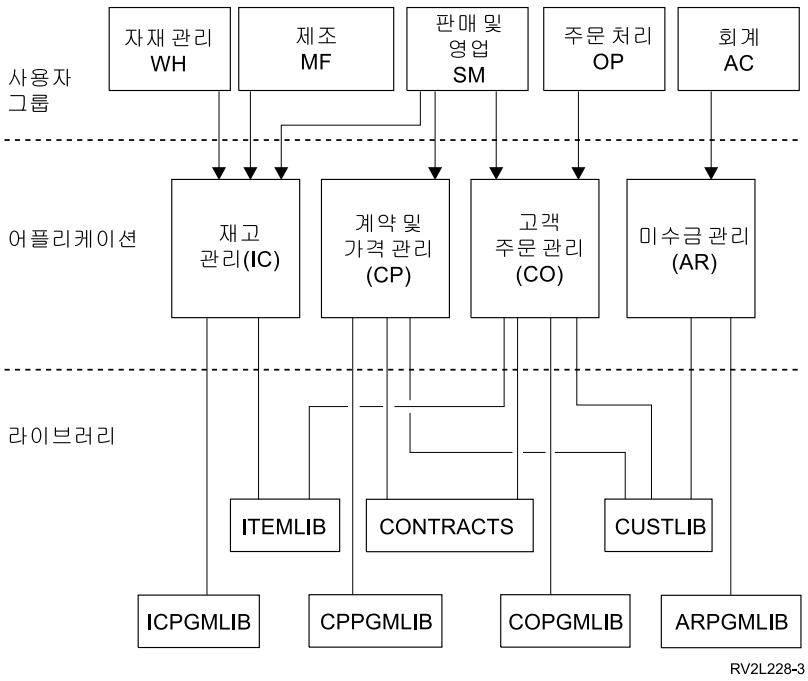
주: 사용자들을 한 그룹 프로파일만의 멤버로 만들면 보안 관리가 간단합니다. 그러나 사용자들을 두 개 이상의 그룹 프로파일에 속하도록 만드는 것이 더 좋을 경우가 있습니다.

사용자를 두 개 이상의 그룹 프로파일에 속하게 만드는 것이 개별 사용자 프로파일에 많은 개인 권한을 부여하는 것보다 관리가 쉽습니다.

예: 사용자 그룹 식별

작업 그룹과 어플리케이션간의 관계가 복잡하거나 모호한 경우 사용자 그룹 식별 양식과 같은 매트릭스 기법을 사용하여 명확하게 만들 수 있습니다. 시스템 사용자와 어플리케이션 요구를 매트릭스로 표시할 때 유사한 패턴을 알 수 있습니다. 사용자 그룹 식별 양식을 작성하는 것 외에 Sharon Jones는 어플리케이션 다이어그램을 사용하여 어플리케이션에 액세스가 필요한 사용자 그룹을 식별시켰습니다.

아래 그림은 JKL Toy사의 어플리케이션 다이어그램입니다.



보안 접근방식이 저(relax) 상태이면 X를 사용하여 어플리케이션이 필요한 사용자들을 나타내십시오. 보안 접근방식이 제한적이면 사용자들이 어플리케이션을 어떻게 사용하는지를 고려해야 합니다. 어플리케이션의 정보를 보기만 하면 되는 사용자에게는 매트릭스에 X 표시를 하지 말고 V(보기)를 사용하십시오. 정보를 변경시켜야 하는 사용자에게는 C(변경)를 사용하십시오. 정보에 대해 1차 책임이 있는 사용자에게는 O(소유자)를 사용하십시오.

예를 들어 JKL Toy사에서는 그룹마다 가격 및 계약 관리 어플리케이션을 필요로 합니다.

- 판매 및 마케팅 부서는 가격 및 고객 계약을 작성합니다. 이 부서에서는 가격 및 계약 관리 정보를 *소유*합니다.
- 고객 주문 관리 부서는 계약 정보를 간접적으로 변경합니다. 주문을 처리할 때 계약에 나오는 수량을 변경합니다. 이 부서에서는 가격 및 계약 관리 정보를 *변경*해야 합니다.
- 주문 처리 담당자들은 작업시 대변 한도 정보를 참조하되 변경할 수는 없습니다. 이 부서에서는 대변 한도 파일을 *보는 것*이 필요합니다.

표 19. JKL Toy사의 사용자 그룹 식별 양식: 예

사용자 그룹 식별 양식					
작성자: Sharon Jones		날짜: 1999년 9월 2일			
		어플리케이션에 필요한 액세스			
사용자 이름	부서	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	주문 처리(OP)	O	C	C	C

표 19. JKL Toy사의 사용자 그룹 식별 양식: 예 (계속)

Karen R.	주문 처리(OP)	O	C	C	C
Kris T.	회계(AC)	V		V	O
Sandy J.	회계(AC)	V	C	V	O
Peter D.	회계(AC)	C		V	O
Ray W.	재고 관리(WH)	V	O	V	
Rose Q.	재고 관리(WH)	V	O	V	
Roger T.	판매 및 마케팅(SM)	C	C	O	C
Sharon J.	관리자(MG)	C	C	C	C

주:

- 보안 환경이 *저(relax)* 상태이면 X를 사용하여 필요한 어플리케이션을 표시하십시오.
- 보안 환경이 *중(average)* 상태이면 A를 사용하여 어플리케이션에 권한이 필요한 사용자들을 표시하십시오.
- 보안 환경이 *고(strict)* 상태이면 C(변경), V(보기), O을 사용하여 어플리케이션이 사용되는 *방법*을 지정할 수 있습니다.

Sharon Jones는 매트릭스를 준비할 때 결정한 사항에 관해 몇 가지 메모를 했습니다.

- 주문 처리 및 회계 부서는 서로 백업을 제공합니다. 현재 두 부서에서는 유사한 어플리케이션들을 필요로 합니다. 그러나 더 많은 사람이 충원되면 향후 더 전문화시킬 것이므로 그룹을 분리시켜야 합니다.
- 주문 처리 부서에서 재고나 계약을 직접 변경할 수 있도록 허용하지 않더라도 주문을 작성하거나 이행할 때 항목 및 계약 잔고가 자동으로 변경됩니다. 이로 인해 나중에 보안 문제가 발생할 것인가?
- 판매 및 마케팅 부서 직원들은 업무의 각 부분과 모든 어플리케이션에 관련이 됩니다. 이 부서에서 항목 가격 및 설명을 설정합니다. 회계 부서에서 대변 한도를 설정하더라도 이 부서에서 신규 고객을 설정합니다. 이 부서가 모든 계약 조항 및 가격 설정을 담당합니다.

사용자 그룹을 어떻게 만들어야 하는지를 결정하십시오. 결정할 때 도움을 받기 위해 사용자 그룹 식별 양식이 필요한지를 사용자 그룹 식별 양식에 채우십시오.

사용자 그룹 식별 양식에 사용자를 추가했으면 그룹 프로파일 계획을 수립할 수 있습니다.

그룹 프로파일 계획

일단 사용자 그룹을 식별했으면 각 그룹에 대해 프로파일을 계획할 준비가 된 것입니다. 사용자가 결정한 많은 내용들이 보안과 사용자 정의 둘다에 영향을 줍니다. 예를 들어, 초기 메뉴를 지정할 때 사용자를 그 메뉴로만 제한할 수 있습니다. 그러나 일단 사용자가 사인 온한 후에는 올바른 메뉴를 볼 수 있도록 해야 합니다.

한 예로 하나의 사용자 그룹에 대해 사용자 그룹 설명 양식을 준비하십시오. 첫 번째 양식을 완료했으면 다시 돌아가서 필요한 다른 그룹에 대해 양식을 완료하십시오.

iSeries 시스템상의 보안 및 사용자 정의는 상당한 유연성을 제공할 수 있도록 설계되어 있습니다. 이 주제에 나오는 계획 수립 방법은 그룹 프로파일과 작업 설명을 설계하기 위한 훌륭한 방법을 제공하지만 프로그래머나 어플리케이션 제공자가 다른 방법을 추천할 수도 있습니다.

그룹 프로파일 명명

그룹 프로파일은 특별한 유형의 사용자 프로파일로 기능하기 때문에 리스트와 화면에서 그룹 프로파일을 쉽게 식별할 수 있습니다. 그룹 프로파일에는 특별한 이름을 할당해야 합니다. 리스트에 이름이 함께 나오게 하려면 그룹 프로파일을 같은 문자(예: GRP(그룹의 경우) 또는 DPT(부서의 경우))로 시작해야 합니다. 다음은 사용자 그룹의 이름을 지정할 때 사용할 수 있는 지침입니다.

- 사용자 그룹명에는 최대 10자를 사용할 수 있습니다.
- 이름에는 문자, 숫자, 특수 문자(예: 파운드(#), 달러($), 밑줄(_), at 부호(@) 등)를 포함시킬 수 있습니다.
- 이름은 숫자로 시작할 수 없습니다.

주: 각 그룹 프로파일의 경우 시스템이 그룹 식별 번호(*gid*)를 할당합니다. 보통은 시스템이 *gid*를 생성하게 만들 수 있습니다. 네트워크에서 시스템을 사용할 경우 그룹 프로파일에 특정 gid를 할당해야 합니다. 네트워크 관리자와 의논하여 gid를 할당해야 하는지를 확인하십시오.

명명 규칙 양식의 해당 필드에 그룹 프로파일을 위한 명명 시스템을 추가하십시오. 예를 들어, Sharon Jones는 그룹 프로파일에 대한 명명 규칙으로 DPT를 선택합니다. 그리고 명명 규칙 양식에 해당 섹션을 작성합니다.

표 20. JKL Toy사의 명명 규칙 양식: 그룹 프로파일의 예

오브젝트 유형	명명 규칙
그룹 프로파일	문자 DPT 뒤에는 부서 약어를 작성하십시오. 그룹 프로파일의 텍스트 설명이 부서명이어야 합니다.

사용자 그룹이 필요로 하는 어플리케이션 및 라이브러리 판별

아직 추가하지 않았으면 이전에 그린 어플리케이션 다이어그램과 라이브러리에 사용자 그룹을 추가하십시오. 이것을 각 그룹의 자원 및 어플리케이션 요구를 결정할 때 사용할 수 있습니다.

사용자 그룹 설명 양식의 파트 1에 가장 자주 사용하는 어플리케이션인 그룹의 1차 어플리케이션을 기록하십시오. 그리고 그룹에서 필요로 하는 다른 어플리케이션들도 나열하십시오.

각 그룹이 필요로 하는 라이브러리를 보려면 어플리케이션 설명 양식 및 어플리케이션 다이어그램을 보십시오. 프로그래머나 어플리케이션 제공자와 의논하여 이 라이브러리에 액세스를 제공하기 위한 최선의 방법을 찾으십시오. 대부분의 어플리케이션들이 다음 방법 중 하나를 사용합니다.

- 어플리케이션에 사용자의 초기 라이브러리 리스트에 있는 라이브러리를 포함시킵니다.
- 어플리케이션이 사용자의 라이브러리 리스트에 라이브러리를 위치시키는 설정 프로그램을 실행합니다.
- 라이브러리 리스트에는 라이브러리가 없어도 됩니다. 어플리케이션 프로그램이 항상 라이브러리를 지정합니다.

시스템은 라이브러리 리스트를 사용하여 어플리케이션을 실행할 때 필요한 파일 및 프로그램을 찾습니다. **라이브러리 리스트**는 사용자가 필요로 하는 오브젝트를 탐색할 때 시스템이 사용하는 라이브러리 리스트입니다. 이 리스트는 두 부분으로 되어 있습니다.

1. **시스템 부분**: QSYSLIBL 시스템에 지정되어 있는 값으로서 시스템 부분이 OS/400 라이브러리에 사용됩니다. 이 시스템 값의 디폴트 값은 변경할 필요가 없습니다.
2. **사용자 부분**: QUSRLIBL 시스템 값은 라이브러리 리스트의 사용자 부분을 제공합니다. 사용자의 작업 설명은 초기 라이브러리 리스트나 사용자가 사인 온한 후의 명령을 지정합니다. 초기 라이브러리 리스트가 있으면 이 리스트가 QUSRLIBL 시스템 값을 대체합니다. 어플리케이션 라이브러리를 라이브러리 리스트의 사용자 부분에 포함시키십시오.

작업 설명 사용

사용자가 시스템에 사인 온할 때 사용자의 작업 설명이 작업 인쇄 방법, 일괄처리 작업 실행 방법, 초기 라이브러리 리스트를 포함하여 많은 작업 특성을 정의합니다. 시스템에서 QDFTJOBD라는 작업 설명을 제공하며 그룹 프로파일을 작성할 때 이것을 사용할 수 있습니다. 그러나 QDFTJOBD는 QUSRLIBL 시스템 값을 초기 라이브러리 리스트로 지정합니다. 서로 다른 그룹의 사용자들이 사인 온할 때 서로 다른 라이브러리에 대해 액세스를 가질 수 있게 하려면 각 그룹에 대해 고유한 작업 설명을 작성해야 합니다.

사용자 그룹 설명 양식에 그룹이 필요로 하는 각 라이브러리를 나열하십시오. 라이브러리를 그룹의 작업 설명에 나오는 초기 라이브러리 리스트에 포함시켜야 할 경우 양식에 각 라이브러리명을 기록하십시오.

사인 온에 영향을 주는 값 선택을 시작하기 전에 Sharon Jones가 JKL Toy사의 사용자 그룹을 설명한 방법의 예를 검토하십시오.

예: JKL Toy사의 사용자 그룹 설명 양식

첫 번째 표는 Sharon Jones가 판매 및 마케팅 부서를 위해 준비한 사용자 그룹 설명 양식의 첫 번째 부분을 보여줍니다. 그룹의 초기 라이브러리 리스트에 Sharon이

CONTRACTS 및 CPPGMLIB 라이브러리를 포함시키지 않은 점에 주목하십시오. 어플리케이션이 이 라이브러리들을 DPTSM 초기 라이브러리 리스트에 포함시키지 않고 자동으로 라이브러리 리스트에 추가합니다. 사용자가 어플리케이션에서 나갈 때 시스템이 이 라이브러리들을 라이브러리 리스트에서 제거합니다. 어플리케이션 프로그램을 통해서만 이 라이브러리에 액세스할 수 있으므로 그와 같은 라이브러리에 대한 추가 보안을 제공하게 됩니다.

표 21. JKL Toy사의 사용자 그룹 설명 양식: 설명 정보의 예

사용자 그룹 설명 양식	파트 2의 1
작성자: Sharon Jones	날짜: 1999년 9월 5일
그룹 프로파일 이름: DPTSM 그룹 설명: 판매 및 마케팅 부서	
그룹을 위한 1차 어플리케이션: 계약 및 가격 관리 그룹에 필요한 기타 어플리케이션 나열: 재고 관리(항목 설명 및 가격을 입력하기 위한), 고객 주문 관리	
그룹에 필요한 각 라이브러리를 나열하십시오. 그룹을 위한 초기 라이브러리 리스트에 있어야 하는 각 라이브러리를 표시(✔)하십시오. • ✔CUSTLIB • ✔ITEMLIB • ✔COPGMLIB • ✔ICPGMLIB • CPPGMLIB • CONTRACTS	

또한 Sharon은 자재 관리 부서를 위한 사용자 그룹 설명을 시작했습니다.

표 22. 사용자 그룹 설명 양식: 설명 정보

사용자 그룹 설명 양식	파트 2의 1
작성자: Sharon Jones	날짜: 1999년 9월 5일
그룹 프로파일 이름: DPTWH 그룹 설명: 자재 관리 부서	
그룹을 위한 1차 어플리케이션: 재고 관리 그룹에 필요한 다른 어플리케이션 나열: 없음	
그룹에 필요한 각 라이브러리를 나열하십시오. 그룹을 위한 초기 라이브러리 리스트에 있어야 하는 각 라이브러리 앞에 체크 표시(✔)를 하십시오. • ✔ITEMLIB • ✔ICPGMLIB	

사용자 그룹 설명 양식의 파트 1을 완료했으면 사인 온에 영향을 미치는 값의 선택을 시작할 수 있습니다.

사인 온에 영향을 주는 값 선택

시스템에 대한 그룹 프로파일 계획을 수립했으면 사인 온에 영향을 주는 시스템 값을 선택해야 합니다. 사용자 그룹 설명 양식의 파트 2에 선택사항을 기록하십시오. 그룹 멤버를 위한 개별 프로파일을 작성하기 위해 복사할 값을 선택한다는 점을 명심하십시오. 선택한 그룹 프로파일명을 기록하고 그룹에 대해 간략한 설명(텍스트)을 기록하는 것으로 시작하십시오.

시스템을 올바로 사용자 정의하면 사인 온 화면에서 사용자 ID와 암호만 입력하면 됩니다. 사용자 프로파일이 기타 사인 온 값을 제공합니다.

암호

그룹 프로파일 암호를 *NONE으로 설정하십시오. 이렇게 하면 다른 사람들이 그룹 프로파일을 사용하여 사인 온하지 못합니다. 나중에 개별 사용자 프로파일을 작성하기 위해 그룹 프로파일을 복사할 때 각 사용자에 대해 암호를 설정하십시오.

초기 프로그램 및 초기 프로시듀어

사인 온 프로그램이라고도 하는 사용자의 초기 프로그램은 시스템이 첫 번째 메뉴를 표시하기 전에 실행됩니다. 라이브러리가 초기 라이브러리 리스트의 한 부분을 이루는 경우에도 프로그램명과 라이브러리 모두를 그룹 프로파일에 넣으십시오. 둘다 지정함으로써 시스템이 올바른 프로그램을 실행하게 만들 수 있으므로 라이브러리 리스트 변경에 관해 걱정할 필요가 없습니다.

초기 프로그램이나 프로시듀어는 다음 중 하나의 목적을 위해 사용합니다.

- 일부 어플리케이션이 어플리케이션 환경을 설정할 때 초기 프로그램을 사용합니다.
- 사용자가 한 개의 프로그램만 실행하고 메뉴를 볼 수 없도록 조치합니다. 예를 들어, JKL Toy사에서는 출고지(loadind dock)에 있는 워크스테이션을 사용하는 사람들만 물품을 수신하기 위한 프로그램을 실행시킬 수 있습니다. 이렇게 하면 공개 장소에 있는 워크스테이션에서의 보안 노출을 방지할 수 있습니다.

사용자에 대해 **기능 제한** 필드를 *YES나 *PARTIAL로 설정하면 사용자가 사인 온 화면에서 초기 프로그램을 변경하지 못합니다.

프로그래머와 의논하여 어플리케이션에 초기 프로그램이나 프로시듀어가 필요한지 알아보십시오.

초기 메뉴 및 초기 메뉴 라이브러리

첫 번째 메뉴라고도 하는 초기 메뉴는 사인 온 후 사용자가 보게 되는 첫 번째 메뉴입니다. 초기 프로그램은 초기 메뉴가 표시되기 전에 실행됩니다. 초기 프로그램이 화면을 표시하면 사용자는 시스템이 초기 메뉴를 표시하기 그 화면을 봅니다.

일반적으로 그룹에 대한 초기 메뉴는 그룹의 기본 어플리케이션의 1차 메뉴이어야 합니다. 메뉴명과 라이브러리 모두를 지정하십시오.

사용자에 대해 **기능 제한** 필드를 *YES로 설정하면 사용자가 사인 온 화면에서 초기 메뉴를 변경할 수 없습니다. 사용자에 대해 *기능 제한* 필드를 *PARTIAL로 설정하면 사용자가 사인 온 화면에서 초기 메뉴를 변경할 수 있습니다.

현재 라이브러리

현재 라이브러리를 **디폴트 라이브러리**라고도 합니다. 사용자에 대해 현재 라이브러리를 지정할 때 여러 가지 일들이 발생합니다.

- 사용자가 조회 프로그램과 같은 오브젝트를 작성할 경우 다른 라이브러리를 지정하지 않으면 시스템이 그 오브젝트를 현재 라이브러리에 넣습니다.
- 시스템이 자동으로 현재 라이브러리를 라이브러리 리스트의 사용자 부분에 추가합니다. 현재 라이브러리를 작업 설명의 초기 라이브러리 리스트에 포함시킬 수 있으나 반드시 그럴 필요는 없습니다.
- 현재 라이브러리가 라이브러리 리스트의 사용자 부분에서 첫 번째 라이브러리가 됩니다. 시스템은 사용자 라이브러리 리스트에서 라이브러리를 탐색하기 전에 현재 라이브러리에서 파일과 프로그램을 탐색합니다.
- 사용자에게 현재 라이브러리를 할당하지 않으면 시스템은 QGPL(범용) 라이브러리를 할당합니다.

권장사항

IBM Query for iSeries 사용권 프로그램이나 그와 유사한 다른 프로그램을 사용할 경우에는 현재 라이브러리가 특히 중요합니다. 다음 접근방식 중 하나를 사용하십시오.

- 그룹의 모든 사람이 공유할 수 있는 라이브러리를 작성하십시오. 그룹에 대한 모든 조회 프로그램과 파일들을 그 라이브러리에 넣으십시오. 그룹 프로파일과 같은 이름을 부여하고 그것을 그룹의 현재 라이브러리로 만드십시오.
- 조회를 사용할 각 사용자에게 개인용 라이브러리를 부여하십시오. 사용자 프로파일과 같은 이름을 라이브러리에 부여하십시오. 그 라이브러리를 그룹 프로파일이 아닌 그룹 멤버의 개별 프로파일에 현재 라이브러리로 지정하십시오.

사용자 설명 양식의 파트 2에 사인 온에 영향을 주는 필드에 대한 선택사항을 채우십시오.

사인 온에 영향을 주는 값을 선택했으면 사용자가 수행할 수 있는 작업을 제한하는 값을 선택 할 수 있습니다.

사용자가 수행할 수 있는 작업을 제한하는 값 선택

그룹 설명 양식의 파트 2에 사인 온에 영향을 주는 값에 대한 선택사항을 기록했으면 사용자가 시스템에서 수행할 수 있는 작업을 제한할 것을 고려해야 합니다. 다음과 같은 여러 가지 이유로 작업을 제한하려는 경우가 발생합니다.

- 사람들이 CL 명령을 사용하지 못하도록 하기 위해. 연습을 하려고 하거나 실수로 문제를 일으킬 있습니다.
- 사용자를 특정 어플리케이션이나 기능으로 제한하기 위해.
- 사용자들이 불필요한 선택으로 인해 혼란을 겪지 않도록 간단한 환경을 제공하기 위해.

사용자들이 얼마나 많은 일들을 할 수 있는지는 여러 요소에 의해 결정됩니다.

- 어플리케이션 설계
- 시스템 값
- 자원 보안
- 그룹 프로파일
- 사용자 프로파일
- 작업 설명

그룹 프로파일이나 사용자 프로파일에 있는 **기능 제한** 및 **사용자 클래스** 필드가 이미 정해진 결정사항을 사용자들이 얼마나 대체시킬 수 있는지를 결정합니다.

기능 제한

기능 제한 필드를 **제한된 명령행 사용**이라고 합니다. 사인 온 화면에서 값을 변경하거나 명령을 입력하거나 어텐션 키 처리 프로그램을 사용자들이 변경시킬 수 있는지를 제한할 수 있습니다. 고(strict) 제한(*YES), 중(average) 제한(*PARTIAL), 무제한(*NO)을 선택할 수 있습니다. 다음 표는 각각의 값이 무엇을 허용하는지를 보여줍니다.

표 23. 기능 제한 값별로 허용되는 기능

기능 제한 값	초기 프로그램 변경	초기 메뉴 변경	현재 라이브러리 변경	어텐션 프로그램 변경	명령 입력
*YES	아니오	아니오	아니오	아니오	몇 가지[1]
*PARTIAL	아니오	예	아니오	아니오	예
*NO	예	예	예	예	예

1 허용되는 명령은 SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, STRPCO입니다. 운영 지원 메뉴 또는 화면에서는 F9 키를 사용하여 명령행을 표시할 수 없습니다.

사용자 클래스

사용자 유형이라고도 하는 사용자 클래스가 사용자가 운영 지원 및 시스템 메뉴에서 보는 옵션을 결정합니다. **특수 권한** 필드에 권한을 나열하지 않는 한 사용자에게 허용되는 시스템 기능도 결정합니다.

제한된 기능 및 사용자 클래스 권장사항

대부분의 사용자들은 CL 명령이나 시스템 기능에 대한 액세스를 필요로 하지 않거나 원하지도 않습니다. 운영 지원 화면은 사용자들에게 자신의 작업 전반에 대한 정보 및 제어를 제공합니다. 다음 권장사항은 타스크를 완료해야 하는 해당 시스템 자원에만 사용자들이 액세스하게 해줍니다.

- 각 그룹 프로파일에서 **기능 제한** 필드를 *YES로 설정하십시오. *사용자 클래스* 필드를 *USER로 설정하십시오.
- 시스템 기능을 필요로 하는 개별 사용자별로 이 스펙을 대체하십시오.
- 어플리케이션간에서 사용자들이 이동을 해야 할 경우 메뉴에서 어플리케이션간에 이동할 수 있는 방법을 제공하는지 확인하십시오.

그룹 설명 양식의 파트 2에 사용자 클래스 및 기능 제한에 대해 선택사항을 입력했으면 사용자의 환경을 설정하는 값을 선택할 수 있습니다.

사용자의 환경을 설정하는 값 선택

사용자 그룹 설명 양식의 파트 2에 시스템에서 사용자가 수행할 수 있는 작업 제한에 대한 선택사항을 입력했으면 사용자의 운영 환경을 판별하는 값을 선택할 수 있습니다. 사용자 프로파일의 많은 필드들이 프린터, 메세지 송신 위치, 작업 우선순위 등 사용자의 작업 환경을 결정합니다. 이와 같은 대부분의 필드에 대해 디폴트 설정을 권장합니다. 몇몇 필드에 대해서는 다음 단락에서 설명합니다.

- **작업 설명 및 작업 설명 라이브러리**: 프로파일 안의 이 필드는 사용자가 사인 온할 때 어떤 작업 설명을 사용할 것인지를 시스템에 알려줍니다. 작업 설명에는 초기 라이브러리 리스트가 들어 있습니다. 각 사용자 그룹에는 그룹 프로파일과 같은 이름의 작업 설명이 있어야 합니다. 작업 설명은 보통 QGPL 라이브러리에 있습니다.
- **프린터 장치 및 출력 대기행렬**: 사용자가 작성한 프린터 출력은 특정 인쇄 작업이 출력을 다른 프린터로 송신하지 않는 한 프로파일에 나오는 프린터 장치로 갑니다. 사용자 그룹 멤버들은 보통 함께 위치하고 있으며 같은 프린터를 공유합니다. 그룹 프로파일에 그 프린터를 지정하여 각 개별 사용자 프로파일 안으로 복사할 수 있습니다. 사용자의 프린터 장치를 **디폴트 프린터**라고도 합니다.

  출력 대기행렬에는 인쇄 전의 프린터 출력이 들어 있습니다. 보통 각 프린터 장치에는 같은 이름의 자체 출력 대기행렬이 있습니다. 출력 대기행렬에 *DEV를 지정하여 시스템이 프린터 장치의 출력 대기행렬을 사용하도록 할 수 있습니다.

사용자 그룹 설명 양식의 작업 설명 이름 및 라이브러리, 디폴트 프린터, 출력 대기 행렬 필드를 채우십시오.

- **운영 지원 인터페이스 설정**: 시스템 출하시 운영 지원 메뉴는 모든 사용자를 위한 어텐션 키 처리 프로그램입니다. 어텐션 키를 누르면 사용자들이 운영 지원(ASSIST) 메뉴를 볼 수 있습니다. 어플리케이션 프로그램이 이미 다른 어텐션 키 처리 프로그램을 사용하고 있으면 사용자에게 운영 지원 메뉴에 도달할 수 있는 다른 방법을 제공해야 합니다.
  - GO ASSIST 또는 CALL QEZAST를 사용하여 기본 어플리케이션 메뉴에서 운영 지원 메뉴를 옵션으로 추가하십시오.
  - 사용자들이 명령행에서 GO ASSIST를 입력하게 만드십시오.

사용자 프로파일에서 **기능 제한** 필드를 *YES로 설정하면 사용자들이 GO 명령을 사용하여 메뉴를 표시할 수 없습니다. 운영 지원 사용자들이 ASSIST 메뉴에 액세스할 수 있는 방법을 제공해야 합니다.

JKL Toy사에서는 Sharon Jones가 사용자 그룹 설명 양식에 어떤 값을 선택했는지를 예에서 볼 수 있습니다.

이 계획 단계를 완료하려면 다음을 수행해야 합니다.

- 회사의 각 사용자 그룹에 대해 사용자 그룹 설명 양식을 완료하십시오.
- 명명 규칙 양식에 사용자 그룹을 명명하는 방법을 설명하십시오.
- 어플리케이션 다이어그램 및 라이브러리에 사용자 그룹을 추가하십시오.

이 타스크를 완료했으면 개별 사용자 프로파일 계획을 시작할 수 있습니다.

예: JKL Toy사의 사용자 그룹 설명 양식 -- 파트 2

Sharon Jones는 판매 및 마케팅 직원을 위해 사용자 그룹 설명 양식을 준비한 것처럼 판매 및 마케팅 그리고 자재 관리 부서에 관해서도 몇 가지 주를 작성했습니다.

- 판매 및 마케팅 직원은 IBM Query for iSeries의 주요 사용자가 됩니다. 각 사용자들이 개인적으로 라이브러리를 가지고 있어야 합니다. 자재 관리 부서가 하나의 그룹 라이브러리를 가질 수 있습니다.
- 출고지에서 근무하는 자재 관리 부서의 직원들은 초기 메뉴 대신에 초기 프로그램이 필요할 것입니다.

Sharon은 두 부서를 위해 사용자 그룹 설명 양식의 파트 2를 준비했습니다.

표 24. JKL Toy사의 사용자 그룹 설명 양식: 판매 및 마케팅 부서의 예

필드명	권장 값	사용자 선택사항
그룹 프로파일 이름(사용자)		DSTSM
암호	*NONE	*NONE
사용자 클래스(사용자 유형)	*USER	*USER

표 24. JKL Toy사의 사용자 그룹 설명 양식: 판매 및 마케팅 부서의 예 (계속)

필드명	권장 값	사용자 선택사항
현재 라이브러리(디폴트 라이브러리)	*그룹 프로파일 이름과 같음*	(그룹은 비워두고 개인 프로파일은 작성하십시오.)
호출할 초기 프로그램(사인 온 프로그램)		
초기 프로그램 라이브러리		
초기 메뉴(첫 번째 메뉴)		CPMAIN
초기 메뉴 라이브러리		CPMAINLIB
기능 제한(제한적인 명령행 사용)	*YES	*PARTIAL
텍스트(사용자 설명)		판매 및 마케팅
작업 설명	*그룹 프로파일 이름과 같음*	DPTSM
작업 설명 라이브러리		QGPL
그룹 프로파일 이름(사용자 그룹)	*NONE[1]	*NONE
인쇄 장치(디폴트 프린터)		PRT03
출력 대기행렬	*DEV	*DEV

표 25. JKL Toy사의 사용자 그룹 설명 양식: 재고 관리 부서의 예

필드명	권장 값	사용자 선택사항
그룹 프로파일 이름(사용자)		DPTWH
암호	*NONE	*NONE
사용자 클래스(사용자 유형)	*USER	*USER
특수 환경		
현재 라이브러리(디폴트 라이브러리)	*그룹 프로파일 이름과 같음*	DPTWH
호출할 초기 프로그램(사인 온 프로그램)		
초기 프로그램 라이브러리		
초기 메뉴(첫 번째 메뉴)		ICMAIN
초기 메뉴 라이브러리		ICPGMLIB
기능 제한(제한적인 명령행 사용)	*YES	*YES
텍스트(사용자 설명)		재고 관리 부서
작업 설명	*그룹 프로파일 이름과 같음*	DPTWH
작업 설명 라이브러리		QGPL
그룹 프로파일 이름(사용자 그룹)	*NONE[1]	*NONE
인쇄 장치(디폴트 프린터)		PRT04
출력 대기행렬	*DEV	*DEV

1 그룹 프로파일의 경우 그룹 프로파일의 이름은 반드시 *NONE이어야 합니다. 그룹 프로파일은 다른 그룹의 멤버가 될 수 없습니다.

이제 개별 사용자 프로파일 계획을 시작할 수 있습니다.

개별 사용자 프로파일 계획

종합적인 보안 전략을 결정하고 사용자 그룹을 계획했으므로 이제 개별 사용자 프로파일을 계획할 준비가 되었습니다.

필요한 양식?

다음 양식을 사용하여 개별 사용자 프로파일을 계획하십시오.

- 개별 사용자 프로파일 양식
- 시스템 책임 양식

다음 양식에 나오는 정보도 필요합니다.

- 사용자 그룹 정의 양식
- 명명 규칙 양식
- 어플리케이션 다이어그램

사용자 프로파일 명명

사용자 프로파일명은 사용자를 시스템에 식별시키는 방법입니다. 사인 온 화면의 **사용자 ID** 필드에 사용자 프로파일명을 입력하십시오. 수행하는 작업 및 작성하는 프린터 출력은 사용자 프로파일명과 연관이 있습니다.

사용자 프로파일명의 지정 방법을 결정할 때 다음을 고려하십시오.

- 사용자 프로파일명은 최대 10자까지 사용할 수 있습니다. 일부 통신 방식은 사용자 ID를 8자로 제한합니다.
- 사용자 프로파일명에는 문자, 숫자, 특수 문자(예: 파운드(#), 달러($), 밑줄(_), 부호(@) 등)를 포함시킬 수 있습니다. 그러나 숫자나 밑줄(_)로 시작할 수 없습니다.
- 시스템은 사용자 프로파일명에서 대소문자를 구별하지 않습니다. 영문 소문자를 입력하면 시스템이 대문자로 변환시킵니다.
- 사용자 프로파일 관리에 사용하는 화면 및 리스트에서는 사용자 프로파일명을 알파벳 순서로 표시합니다.
- 모든 IBM 제공 프로파일은 문자 Q로 시작합니다. 프로파일을 IBM 제공 프로파일과 별도로 보유하려면 문자 Q로 시작하는 사용자 프로파일명을 할당하지 마십시오.

권장사항

사용자 프로파일명을 할당하기 위한 한 가지 기법은 성의 처음 7자 다음에 이름의 첫 번째 문자가 오도록 하는 것입니다. 아래에 Sharon이 JKL Toy사의 사용자 프로파일에 사용한 명명 규칙이 나옵니다.

표 26. JKL Toy사의 명명 규칙 양식: 사용자 프로파일의 예

사용자 이름	사용자 프로파일명
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

이 방법을 사용하면 사용자 프로파일명을 기억하기는 것이 쉽습니다. 또한 리스트 및 화면은 성의 알파벳 순서로 되어 있습니다.

예를 들어, JKL Toy사의 Sharon Jones는 다음 명명 기법을 사용하기로 계획합니다. Sharon이 명명 규칙 양식의 해당 섹션을 채웠습니다.

표 27. JKL Toy사의 명명 규칙 양식: 사용자 프로파일의 예

오브젝트 유형	명명 규칙
사용자 프로파일	사용자 성의 처음 7자 다음에 사용자 이름의 첫 번째 문자가 오도록 하십시오. 사용자 프로파일에 대한 설명은 성, 이름입니다.

명명 규칙 양식에 사용자 프로파일명을 계획하는 방법을 설명했으면 시스템 기능 책임자 판별 및 각 사용자에 대한 값 선택을 수행할 수 있습니다.

시스템 기능 책임자 판별

개별 사용자 프로파일 계획을 수립할 경우 먼저 시스템에서 개별 사용자의 책임을 판별해야 합니다. 시스템을 효과적으로 운영하려면 다양한 관리 및 유지보수 기능을 정기적으로 수행할 사람들이 필요합니다. 이 타스크를 수행하는 사용자들에게 명령을 실행하고 시스템 기능을 수행할 권한이 필요합니다.

사용자가 수행할 수 있는 작업을 제한하는 값 선택에서 **사용자 클래스** 및 **기능 제한** 필드를 통해 사용자가 액세스할 수 있는 시스템 기능을 제어하는 방법을 설명했습니다. 보통은 대부분의 사용자들이 시스템 기능을 수행할 수 있도록 해서는 안됩니다(사용자 클래스를 *USER, 기능 제한을 *PARTIAL 또는 *YES로 설정하십시오). 그러나 시스템을 효과적으로 운영하기 위해 일부 사용자에게는 추가 권한이 필요합니다.

아래 표에는 몇 가지 중요한 시스템 관리 타스크가 나옵니다. 이 표에는 그와 같은 책임을 가진 사용자들에게 할당할 수 있는 사용자 클래스 및 특수 권한도 표시됩니다. 이 리스트는 시스템에서 특수 권한을 필요로 하는 사용자를 판별할 때 도움이 됩니다. 그러나 이것이 시스템 운영 및 유지보수를 위한 완벽한 계획 툴은 아닙니다. 이 표는 대부분의 시스템으로 작업하는 사용자 클래스 및 특수 권한을 제공합니다. 시스템에 따라 서로 다른 권한을 할당해야 할 경우도 있습니다.

프로파일에 *USER가 아닌 사용자 클래스를 할당하면 시스템 기능을 수행하기 위한 특수 권한 세트를 자동으로 수신합니다. 사용자 클래스 필드에 지정한 권한과 다른 사용자 특수 권한을 할당할 수 있으나 할당하는 것이 필요 없을 수 있습니다.

표 28. 시스템 책임, 사용자 클래스, 특수 권한

시스템 기능[1]	설명	필수 사용자 등급[2]	필수 특수 권한 [3]
시스템 작업	프린터 출력을 관리하고 시스템 메세지에 응답하고 정규 작업을 모니터하고 초기 프로그램 로드(IPL)를 수행합니다.	*SYSOPR	*JOBCTL
시스템 관리 (housekeeping)	시스템 관리(예: 자동 클린업 스케줄 설정 및 디스크 사용량 모니터링)를 수행합니다.	*SYSOPR	*JOBCTL
시스템 백업	정기적으로 어플리케이션 라이브러리, 시스템 라이브러리, 보안 정보를 저장합니다. 이 기능에 대한 세부사항은 Information Center의 백업 및 회복 주제를 참조하십시오.	*SYSOPR	*SAVSYS
프로파일 관리	신규 사용자 프로파일을 추가하고 기존 프로파일을 유지보수합니다.	*SECADM	*SECADM
자원 보안 관리	시스템의 오브젝트에 대한 권한을 유지보수합니다.	*SECOFR	*ALLOBJ
프로그램 유지보수	IBM 제공 라이브러리에 정기적인 프로그램 변경(PTF)을 적용합니다. 어플리케이션 라이브러리에 변경사항을 작성합니다.	*SECOFR	*ALLOBJ
보안 감사	보안 감사 기능을 설정합니다. 감사해야 하는 이벤트, 사용자, 오브젝트를 판별합니다.		*AUDIT [4]
시스템 구성	시스템에서 장치를 추가, 변경, 제거합니다.		*IOSYSCFG[5]

1 책임을 맡고 있는 사용자의 경우 기능 제한 필드를 *NO로 설정하십시오.

2 이것은 필요한 최소 사용자 클래스입니다. 사용자 클래스에서 기능을 수행할 때 필요한 명령 및 메뉴 옵션을 사용할 권한을 제공합니다. 자원 보안에 따라 추가 오브젝트 권한이 필요할 수 있습니다.

3 이 특수 권한은 작업 책임에 필요합니다. 사용자 클래스가 특수 권한을 추가로 부여할 수 있습니다.

4 *AUDIT 특수 권한에는 해당 사용자 클래스가 없습니다. *SECOFR 사용자 클래스에는 *AUDIT 특수 권한이 포함되어 있습니다. 그러나 감사자에게는 *SECOFR 사용자 클래스의 다른 기능이 필요 없습니다. 시스템에서 감사를 제어해야 하는 각 개별 사용자에 대해 *AUDIT 특수 권한을 지정하십시오.

5 *IOSYSCFG 특수 권한에는 해당 사용자 클래스가 없습니다. *SECOFR 사용자 클래스에는 *IOSYSCFG 특수 권한이 포함되어 있습니다. 시스템을 구성해야 하는 개별 사용자에 대해서만 *IOSYSCFG 특수 권한을 지정하십시오. 개개인이 회선, 제어기, 장치를 작성하거나 TCP/IP를 구성할 수 있습니다. 그러나 시스템을 구성하는 사용자에게는 *SECOFR 사용자 클래스의 다른 기능이 필요 없습니다.

권장사항

위의 표를 사용하여 누가 시스템 기능을 수행해야 하는지 계획하십시오. 최소한 시스템 보안 관리에 두 명을 할당하고 운영 및 백업 관리에 다른 두 명을 할당해야 합니다.

시스템 책임 양식을 시스템 관리 및 감사 툴로 사용하십시오. 시스템에서 특수 권한을 가진 모든 사람과 그 특수 권한이 필요한 이유를 추적하십시오.

각 사용자에 대한 값을 선택하기 전에 Sharon Jones가 사용자 책임을 판별한 방법의 예를 볼 수 있습니다.

예: JKL Toy사의 시스템 책임 양식

아래는 Sharon Jones가 완성한 시스템 책임 양식의 예입니다.

표 29. JKL Toy사의 시스템 책임 양식: 예

1차 보안 담당자는 누구입니까? Sharon Jones 백업 보안 담당자는 누구입니까? Ken Harrison			
프로파일 이름	사용자 이름	클래스	주석
JONESS	Sharon Jones	*SECOFR	Sharon은 1차 보안 담당자인 동시에 시스템 관리자입니다.
HARRISOK	Ken Harrison	*SECOFR	Ken은 전반적인 시스템 관리자로서 Sharon의 백업 관리자입니다.
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy는 시스템 운영 및 백업의 1차 책임을 담당합니다.
ROGERSK	Karen Rogers	*SYSOPR	Karen은 Sandy를 도와서 시스템 운영 및 백업을 담당합니다.
WILLISR	Rose Willis	*SYSOPR	Rose는 두 번째 업무 교대 중에 시스템을 운영합니다.

시스템 책임 양식을 완료했으면 각 사용자에 대한 값 선택을 시작할 수 있습니다.

각 사용자에 대한 값 선택

시스템에서 사용자의 책임을 판별했으면 각 사용자에 대한 값 선택을 시작할 수 있습니다. 그룹 프로파일을 개별 사용자 프로파일을 위한 패턴으로 계획하여 대부분의 작업을 완료했습니다. 개별 사용자 프로파일 양식을 사용하여 각 사용자에게 올바른 그룹을 할당하고 사용자가 그룹의 다른 사용자와 어떻게 다른지 정의하십시오. 예를 들어, 한 사용자 그룹에 대해 개별 사용자 프로파일 양식을 완료했으면 다시 돌아가서 추가 사용자 그룹에 대해 개별 사용자 프로파일 양식을 준비하십시오.

개별 사용자 프로파일 양식의 맨 위에 그룹 프로파일명 및 기타 설명 정보를 채우십시오.

예: JKL Toy사의 개별 사용자 프로파일 양식의 설명 정보

Sharon Jones는 다음과 같은 방법으로 개별 사용자 프로파일 양식의 맨 윗 부분을 채웠습니다.

표 30. JKL Toy사의 개별 사용자 프로파일 양식: 설명 정보의 예

개별 사용자 프로파일 양식	
작성자: Sharon Jones	날짜: 1999년 9월 5일
그룹 프로파일명: DPTOP	
작성된 오브젝트의 소유자:	작성된 오브젝트의 그룹 권한:
그룹 권한 유형:	

그룹 멤버에 대한 값 판별

개별 사용자 프로파일 양식에 그룹의 각 멤버의 프로파일명과 설명(사용자의 이름)을 기록하십시오. 아래 단락은 각 그룹 멤버에 대한 기타 값들을 판별하는 방법에 관해 설명합니다.

그룹 프로파일은 개별 사용자 프로파일을 위한 패턴이라는 점을 기억하십시오. 개별 사용자 프로파일 양식에서 그룹과 다른 것만 지정해야 합니다.

- **암호 할당**: 사용자에게 초기 암호를 할당하는 가장 쉬운 방법은 프로파일명과 같은 암호를 작성하는 것입니다. 그리고 나서 암호를 만기로 설정하여 사용자가 처음 사인 온할 때 암호를 변경해야 하도록 만들 수 있습니다. 암호를 만기로 설정 주제에서 그룹 프로파일을 복사할 때 자동으로 처리가 이루어지도록 하는 방법을 배울 수 있습니다. 이와 같이 할 경우 개별 사용자 프로파일 양식에 암호를 나열할 필요가 없습니다.
- **사용자 클래스 및 기능 제한**: **사용자 클래스** 및 **기능 제한** 필드에 서로 다른 값을 필요로 하는 각 그룹의 멤버들을 알아보려면 시스템 책임 양식을 보십시오. 그룹 프로파일이 아닌 다른 값이 필요로 하는 사용자의 경우 개별 사용자 프로파일 양식에 적절한 정보를 작성하십시오.
- **다른 값 지정**: 그룹에 대해 사용자 그룹 설명 양식에 지정한 값과 다른 값을 필요로 하는 사용자가 있는지 검사하십시오. 사용자 그룹 설명 양식에 **사용자 클래스** 및 **기능 제한** 필드가 맨 위에 나오는데 이것은 그룹의 일부 멤버에 대해 그 값이 다를 수 있기 때문입니다. 작업 중인 그룹의 멤버에 따라 달라지는 기타 필드를 나열하십시오.

이 계획 단계를 완료하려면 다음과 같이 하십시오.

- 시스템 값 선택 양식을 완료하십시오.
- 명명 규칙 양식에 사용자 프로파일 명명 계획 방법을 설명하십시오.
- 회사의 각 사용자 그룹에 대해 개별 사용자 프로파일 양식을 준비하십시오.

자원 보안 계획을 수립하기 전에 Sharon이 개별 사용자에 대해 사용했던 정보의 예를 검토할 수 있습니다.

예: JKL Toy사의 개인용 사용자 프로파일 양식

JKL Toy사에서는 출고지에서 근무하는 사용자의 경우 하나의 프로그램만 실행할 수 있습니다. Sharon은 일반인들이 쉽게 워크스테이션에 접근할 수 있는 장소에 출고지 직원들이 근무한다는 이유로 일부 기능만 사용할 수 있도록 제한시켰습니다. 즉, 자재 관리 부서 직원들의 경우 초기 프로그램은 가지고 있으나 초기 메뉴는 없습니다. 주문 처리 부서에는 로컬 프린터가 두 대 있으며 영업 지사에는 프린터가 한 대 있습니다. 따라서 그룹이 아닌 일부 사용자들에게는 다른 프린터를 할당했습니다.

아래는 Sharon Jones가 JKL Toy사의 자재 관리 및 주문 처리 부서를 위해 완료한 개별 사용자 프로파일 양식입니다. 필드가 그룹 프로파일에 설정되어 있는 값과 다른 경우에만 필드를 작성했다는 점에 주목하십시오.

표 31. JKL Toy사의 개인 사용자 프로파일 양식: 자재 관리 부서의 예

그룹 프로파일 이름: DPTWH					
그룹의 각 멤버를 위한 항목을 작성하십시오.					
사용자 프로파일	**텍스트(설명)**	**사용자 클래스**	**기능 제한**	**초기 프로그램/ 라이브러리**	**초기 메뉴/ 라이브러리**
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	없음
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	없음
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

표 32. 개인용 사용자 프로파일 양식: 주문 처리 부서의 예

그룹 프로파일 이름: DPTOP				
그룹의 각 멤버를 위한 항목을 작성하십시오.				
사용자 프로파일	**텍스트(설명)**	**사용자 클래스**	**기능 제한**	**인쇄 장치**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

이제 자원 보안 계획을 시작할 수 있습니다.

제 5 장 자원 보안 계획

시스템 사용자를 계획하기 위한 프로세스를 완료했으므로 시스템 오브젝트를 보호하기 위한 자원 보안을 계획할 수 있습니다. "자원 보안 설정"에서는 시스템 자원 보안 설정 방법을 알아봅니다.

시스템 값 및 사용자 프로파일은 시스템 액세스를 가진 사용자를 제어하여 권한이 없는 사용자가 사인 온하는 것을 방지합니다. 자원 보안은 권한을 가진 시스템 사용자가 성공적으로 사인 온을 마친 후 수행할 수 있는 조치를 제어합니다. 자원 보안은 시스템에서의 기본적인 보안 목표를 지원합니다.

- 정보의 기밀성 유지
- 권한이 없을 경우 변경하지 못하게 함으로써 정보의 정확성 유지
- 우발적이거나 고의적인 손상을 방지하기 위한 정보의 가용성 유지

회사에서 어플리케이션을 직접 개발하는지 아니면 외주를 주는지에 따라 자원 보안 계획을 달리 수립할 수 있습니다. 어플리케이션을 개발할 경우에는 어플리케이션 설계 프로세스 중에 프로그래머에게 정보 보안을 위한 요구사항을 전달해야 합니다. 외주를 줄 경우에는 보안 요구를 결정하여 외부 개발 업체가 어플리케이션을 설계 방식에 그와 같은 요구들을 일치시켜야 합니다. 여기에 나오는 방법은 두 경우 모두에 도움을 줍니다.

이 주제는 자원 보안 계획에 대한 기본적인 접근방식을 제공합니다. 기본적인 방법을 소개하고 그 사용 방법을 보여줍니다. 여기에 나오는 방법을 모든 회사와 모든 어플리케이션에 반드시 적용시켜야 하는 것은 아닙니다. 자원 보안을 계획할 경우 프로그래머나 어플리케이션 제공자와 상의하십시오.

자원 보안을 계획할 때 다음 주제를 검토하십시오.

- 자원 보안 목적 판별
- 권한 유형 이해
- 어플리케이션 라이브러리 보안 계획
- 라이브러리 및 오브젝트 소유권 판별
- 오브젝트 그룹화
- 프린터 출력 보호
- 워크스테이션 보호
- 자원 보안 권장사항 요약
- 어플리케이션 설치 계획

필요한 양식

다음 양식을 복사하여 이 주제를 읽어 나가면서 해당 양식을 채우십시오. 한 어플리케이션에 대해 전체 프로세스를 완료한 후 어플리케이션마다 프로세스를 반복하십시오.

표 33. 자원 보안 계획에 필요한 계획 양식

양식명	필요한 사본 수
권한 부여 리스트 양식	3-4부
프린터 출력 및 워크스테이션 보안 양식	1부

전에 작업한 양식을 사용하여 다음 양식에 정보를 추가하십시오.

표 34. 변경할 양식 계획

양식명	준비 위치
라이브러리 설명 양식	라이브러리 정보 설명
사용자 그룹 설명 양식	그룹 프로파일 계획

다음 양식(전에 준비했던)을 참조하십시오.

표 35. 완벽한 자원 보안에 필요한 계획 양식

양식명	준비 위치:
라이브러리 설명 양식	어플리케이션 다이어그램 그리기 및 사용자 그룹 식별
어플리케이션 설명 양식	어플리케이션 정보 설명
개별 사용자 프로파일 양식	각 사용자에 대한 값 선택
사용자 그룹 식별 양식	사용자 그룹 식별
시스템 책임 양식	시스템 기능 책임자 판별
물리적 보안 계획 양식	물리적 보안 계획

자원 보안 목적 판별

자원 보안 계획을 시작하려면 먼저 그 목적을 이해해야 합니다. iSeries는 유연성 있는 자원 보안 구현을 제공합니다. 사용자가 원하는 방식으로 중요한 자원을 보호할 수 있는 권한을 사용자에게 부여합니다. 그러나 자원 보안이 어플리케이션에 추가적인 오버헤드를 가져오기도 합니다. 한 예로 어플리케이션이 오브젝트를 필요로 할 때마다 시스템이 해당 오브젝트의 사용자 권한을 검사하는 경우입니다. 성능 비용을 고려하여 기밀성 요구와의 균형을 맞추어야 합니다. 자원 보안 결정을 내릴 때 비용과 대비하여 보안의 가치를 측정하십시오.

자원 보안으로 인해 어플리케이션 성능이 저하되는 것을 막으려면 다음 지침을 따르십시오.

- 자원 보안 체계를 단순화하십시오.
- 보안이 필요한 오브젝트만 보안하십시오.

- 정보를 보호하는 다른 툴을 대체하는 것이 아니라 보완하기 위한 수단으로 자원 보안을 사용하십시오.
  - 특정 메뉴 및 어플리케이션으로 사용자를 제한합니다.
  - 사용자들이 명령을 입력하지 못하게 합니다(사용자 프로파일에서 기능 제한).

목적을 정의하는 것에서부터 자원 보안 계획을 시작하십시오. 어플리케이션 설명 양식이나 라이브러리 설명 양식에 보안 목적을 정의할 수 있습니다.

사용하는 양식은 정보가 라이브러리에 구성되어 있는 방법에 따라 다릅니다.

자원 보안에 사용할 수 있는 권한 유형을 검토하기 전에 JKL Toy사의 보안 목적 예를 검토하십시오.

예: JKL Toy사의 보안 목적

JKL Toy사의 Sharon Jones는 고객 레코드 라이브러리(CUSTLIB)의 보안 요구사항을 설명하기 위해 라이브러리 설명 양식을 사용했습니다.

표 36. JKL Toy사의 라이브러리 설명 양식: 보안 목적의 예

라이브러리 설명 양식	파트 2의 1
라이브러리에 대한 보안 목적 정의(예: 기밀 정보 여부 판별):	현재로는 회사의 모든 사람들이 고객 정보와 고객 주문 정보를 볼 수 있습니다. 정보의 정확성을 보호하기 위해 정보를 변경할 사람들을 제어해야 합니다.

Sharon은 계약과 가격 관리 어플리케이션을 위한 설명 양식을 사용하여 보안 목적을 설명했습니다.

표 37. JKL Toy사의 어플리케이션 설명 양식: 보안 목적의 예

어플리케이션 설명 양식	파트 2의 1
라이브러리에 대한 보안 목적 정의(예: 기밀 정보 여부 판별):	계약 및 특별가 관리에 관한 정보는 기밀 사항입니다. 소수의 사람들만 검색하고 변경할 권한이 있습니다. • 판매 및 마케팅 직원 그리고 모든 관리자들이 계약을 작성, 변경, 분석할 수 있어야 합니다. 이들은 파일 및 프로그램 모두를 사용합니다. • 주문을 처리하는 직원들은 주문을 입력하고 선적할 때 간접적으로 계약을 변경하고 가격을 볼 수 있습니다. 주문을 입력하거나 변경할 때가 아니면 계약 및 가격을 볼 수 없습니다.

어플리케이션 설명 양식이나 라이브러리 설명 양식에 어플리케이션을 위한 보안 목적을 기록하십시오. 이제 자원 보안 계획에 사용할 수 있는 권한의 유형을 검토할 수 있습니다.

권한 유형 이해

자원 보안 목적을 판별하고 라이브러리 설명 양식에 결정사항을 기록했으면 권한 유형 계획을 시작할 수 있습니다. 자원 보안은 사용자가 시스템의 오브젝트에 액세스하는 방법을 정의합니다.

권한은 오브젝트를 사용할 수 있도록 인증하는 방법을 의미합니다. 예를 들어, 시스템의 정보를 보거나 변경할 권한을 가질 수 있습니다. 시스템은 서로 다른 여러 가지 권한 유형을 제공합니다. IBM에서는 이 권한 유형을 **시스템 정의 권한**이라는 범주로 그룹화하여 대부분의 사용자 요구를 충족시키고 있습니다. 아래 표는 각 범주를 나열하여 각각이 파일 및 프로그램 보안에 어떻게 적용되는지를 알려줍니다.

주: 권한을 계획할 때 아래 표를 참조하십시오.

표 38. 시스템 정의 권한

권한명	파일에 허용되는 조작	파일에 허용되지 않은 조작	프로그램에 허용되는 조작	프로그램에 허용되지 않은 조작
*USE	파일의 정보 보기.	파일의 정보 변경 또는 삭제. 파일 삭제.	프로그램 실행.	프로그램 변경 또는 삭제.
*CHANGE	파일의 레코드 보기, 변경, 삭제.	전체 파일 삭제 또는 지우기.	프로그램 설명 변경.	프로그램 변경 또는 삭제.
*ALL	파일 작성 및 삭제. 파일에 레코드 추가, 변경, 삭제. 다른 사용자에게 파일 사용 권한 부여.	없음	프로그램 작성, 변경, 삭제. 다른 사용자에게 프로그램 사용 권한 부여.	프로그램이 권한을 허용할 경우 프로그램 소유자 변경.
*EXCLUDE[1]	없음	파일 액세스.	없음	프로그램 액세스.
1 *EXCLUDE는 공용으로 부여하거나 그룹 프로파일을 통해 부여한 권한을 대체합니다.				

오브젝트 권한과 라이브러리 권한의 연관성 이해

단순한 자원 보안을 설계하려면 전체 라이브러리에 대한 보안을 계획하십시오. 이를 위해서는 시스템 정의 권한이 라이브러리에 어떻게 적용되는지를 이해해야 합니다. 아래 표를 참조하십시오.

표 39. 라이브러리에 대한 시스템 정의 권한

권한명	허용되는 조작	허용되지 않은 조작
*USE	• 라이브러리 오브젝트의 경우 오브젝트별로 권한이 허용하는 조작. • 라이브러리의 경우 설명 정보 보기.	• 라이브러리에 신규 오브젝트 추가. • 라이브러리 설명 변경. • 라이브러리 삭제.

표 39. 라이브러리에 대한 시스템 정의 권한 (계속)

권한명	허용되는 조작	허용되지 않은 조작
*CHANGE	• 라이브러리의 오브젝트의 경우 오브젝트별로 권한이 허용하는 조작. • 라이브러리에 신규 오브젝트 추가. • 라이브러리 설명 변경.	• 라이브러리 삭제.
*ALL	• 변경으로 허용되는 모든 것. • 라이브러리 삭제. • 다른 사용자에게 라이브러리에 대한 권한 부여.	• 없음

라이브러리와 오브젝트 권한이 어떻게 서로 연관되는지도 알아야 합니다. 아래 표에는 오브젝트와 라이브러리 모두에 필요한 권한의 예가 나옵니다.

표 40. 라이브러리 권한과 오브젝트 권한의 연관성

오브젝트 유형	조작	필요한 오브젝트 권한	필요한 라이브러리 권한
파일	자료 변경	*CHANGE	*USE
파일	파일 삭제	*ALL	*USE
파일	파일 작성	*ALL	*CHANGE
프로그램	프로그램 실행	*USE	*USE
프로그램	프로그램 변경(재컴파일)	*ALL	*CHANGE
프로그램	프로그램 삭제	*ALL	*USE

디렉토리 권한은 라이브러리 권한과 유사합니다. 오브젝트에 액세스하려면 오브젝트 경로명에 있는 디렉토리 모두에 대한 권한이 필요합니다.

이제 어플리케이션 라이브러리에 대한 보안 계획을 수립할 준비가 되었습니다.

어플리케이션 라이브러리 보안 계획

자원 보안 목적을 판별했으면 어플리케이션 라이브러리에 대한 보안 계획을 시작할 수 있습니다. 여기에 나오는 프로세스에 따라 작업할 어플리케이션 라이브러리 중 하나를 선택하십시오. 시스템이 별도 라이브러리에 파일과 프로그램을 저장하고 있으면 파일이 있는 라이브러리를 선택하십시오. 주제를 완료하면 나머지 어플리케이션 라이브러리에 대해서도 이 단계를 반복하십시오.

어플리케이션 및 라이브러리에 관해 수집한 정보를 검토하십시오.

- 어플리케이션 설명 양식
- 라이브러리 설명 양식

- 라이브러리가 필요한 임의 그룹에 대한 사용자 그룹 설명 양식
- 어플리케이션, 라이브러리, 사용자 그룹 다이어그램

라이브러리에서 정보가 필요한 그룹, 정보가 필요한 이유, 정보를 이용하여 처리할 작업에 대해 계획하십시오.

라이브러리 내용 판별

어플리케이션 라이브러리에는 중요한 어플리케이션 파일이 들어 있습니다. 기타 오브젝트도 들어 있을 수 있으며 그 가운데 대부분은 어플리케이션이 올바로 작업을 수행하기 위한 프로그래밍 툴로서 다음과 같은 항목들입니다.

- 작업 파일
- 자료 영역 및 메세지 대기행렬
- 프로그램
- 메세지 파일
- 명령
- 출력 대기행렬

파일 및 출력 대기행렬이 아닌 대부분의 오브젝트는 보안 노출을 나타내지 않습니다. 오브젝트에는 보통 적은 양의 어플리케이션 자료가 들어 있으며 프로그램 밖에서는 쉽게 이해하기 어려운 형식으로 되어 있습니다. 라이브러리 표시 명령을 사용하여 라이브러리에 있는 전체 오브젝트의 이름과 설명을 나열할 수 있습니다. 예를 들어 CONTRACTS 라이브러리 내용을 나열하려면 다음과 같이 입력하십시오.

```
DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)
```

그 다음 어플리케이션 라이브러리 및 프로그램 라이브러리에 필요한 공용 권한을 결정하십시오.

어플리케이션 라이브러리에 대한 공용 권한 결정

자원 보안 목적의 경우 **공용**은 시스템에 사인 온할 권한을 부여받은 임의의 사용자를 의미합니다. **공용 권한**은 특정 액세스가 없어도 사용자가 오브젝트에액세스할 수 있게 해줍니다. 이미 라이브러리에 있는 오브젝트에 대해 공용 권한을 결정하는 것 외에도 나중에 라이브러리에 추가시킨 신규 오브젝트에 대해 공용 권한을 지정할 수 있습니다. 이와 같이 하려면 **CRTAUT(작성 권한)** 매개변수를 사용하십시오. 일반적으로 라이브러리에 대한 공용 권한과 신규 오브젝트에 대한 라이브러리 작성 권한은 동일해야 합니다.

QCRTAUT(작성 권한) 시스템 값이 신규 오브젝트에 대한 시스템 전체의 공용 권한을 판별합니다. IBM은 QCRTAUT 시스템 값을 *CHANGE로 제공합니다. 많은 시스템

기능들이 QCRTAUT를 사용하므로 변경하지 마십시오. 어플리케이션 라이브러리의 CRTAUT(작성 권한)에 대해 *SYSVAL을 지정하면 QCRTAUT 시스템 값(*CHANGE)을 사용합니다.

단순화 및 높은 성능을 위해 가능하면 공용 권한을 사용하십시오. 라이브러리에 대한 공용 권한이 어떤 것이어야 하는지를 판별하려면 다음에 관해 알아보십시오.

- 회사 안의 모든 사용자들이 이 라이브러리에 있는 대부분의 정보에 액세스해야 하는가?
- 사람들이 이 라이브러리에 있는 대부분의 정보에 대해 어떤 유형의 액세스를 가져야 하는가?

대다수의 사람들과 정보를 중심으로 결정하십시오. 나중에 예외를 처리하는 방법에 관해 배웁니다. 때로는 자원 보안을 계획하는 것이 하나의 순환 프로세스입니다. 특정 오브젝트에 대한 요구사항을 고려한 후 공용 권한을 변경시켜야 한다는 것을 알 수 있을 것입니다. 보안 및 성능 요구에 맞는 권한을 선택하기 전에 오브젝트와 라이브러리 모두에 대한 공용 권한 및 개인 권한의 몇 가지 조합을 시도해 보십시오.

적절한 권한 보장

오브젝트에 *CHANGE 권한 그리고 라이브러리에 *USE 권한이면 대부분의 어플리케이션 기능에 적합합니다. 그러나 특정 어플리케이션 기능이 더 많은 권한을 요구하는지 알아보려면 프로그래머나 어플리케이션 제공자에게 다음에 관해 문의하십시오.

- 라이브러리 안의 파일이나 다른 오브젝트가 처리하는 중에 삭제되는가? 파일이 지워지는가? 파일에 멤버가 추가되는가? 오브젝트 삭제, 파일 지우기, 파일 멤버 추가를 위해서는 오브젝트에 *ALL 권한이 필요합니다.
- 라이브러리 안의 파일이나 다른 오브젝트가 처리하는 중에 작성되는가? 오브젝트를 작성하기 위해서는 라이브러리에 *CHANGE 권한이 필요합니다.

프로그램 라이브러리에 대한 공용 권한을 결정하기 전에 Sharon이 오브젝트 권한을 위해 선택한 예를 검토하십시오.

예: JKL Toy사의 라이브러리 설명 양식

Sharon Jones는 고객 정보를 사용하는 부서 및 어플리케이션에 관한 정보와 함께 고객 레코드 라이브러리를 위한 보안 목적을 검토했습니다. 그리고 나서 내린 결론은 다음과 같습니다.

- 자재 관리 및 생산 부서를 제외한 모든 부서가 고객 정보를 변경할 수 있어야 합니다.
- 자재 관리 및 생산 부서의 모든 사용자는 기능 제한(Yes) 상태의 사용자 프로파일을 가지며 특정 메뉴나 프로그램으로 사용이 제한됩니다. 메뉴를 통해 고객 정보를 볼 수 있으나 변경할 수는 없습니다.

- 고객 레코드 라이브러리에서 오브젝트를 위한 공용 권한을 *CHANGE로 설정할 수 있습니다. 메뉴 제한은 권한이 없는 사용자들이 고객 정보를 함부로 변경하지 못하게 합니다. 그러나 나중에 다른 부서를 시스템에 추가할 경우 그와 같은 제한은 다시 평가해야 합니다.

다음은 저(relaxed) 상태의 보안 접근방식으로 정보에 액세스하는 예입니다. 이 경우 권한 제한이 아닌 사용자 프로파일을 통해 예외를 처리합니다. Sharon이 고객 레코드 라이브러리(CUSTLIB)에 대한 라이브러리 설명 양식의 공용 권한 부분을 채워 넣었습니다.

표 41. JKL Toy사의 라이브러리 설명 양식 -- 파트 1: 고객 레코드의 예

라이브러리 이름: CUSTLIB	설명(텍스트): 고객 레코드
라이브러리의 공용 권한:	*USE
라이브러리내 오브젝트의 공용 권한:	*CHANGE
신규 오브젝트의 공용 권한(CRTAUT):	*CHANGE

Sharon Jones는 고객 레코드 라이브러리에서 일부 임시 파일이 미수금 관리 어플리케이션의 월말 처리 도중에 지워진 것을 발견했습니다. Sharon은 라이브러리에서 기타 오브젝트들이 사고로 지워질 수도 있는 위험을 감수하기보다는 그 파일에 대한 권한을 개별적으로 처리하기로 선택했습니다. 다른 모든 처리 활동에 대해서는 *CHANGE 권한으로 충분합니다.

비록 소수의 사람들만 월말 처리를 실행할지라도 Sharon은 임시 파일이 보안 노출의 위험을 내포하지 않는다고 생각했습니다. Sharon은 월말 처리를 실행하는 사람들에게만 권한을 부여하는 것이 아니라 위와 같은 파일에 대해서는 공용 *ALL 권한을 부여하기로 결정했습니다. 아래 표는 고객 레코드 라이브러리를 위한 라이브러리 설명 양식의 두 번째 부분을 보여줍니다.

표 42. JKL Toy사의 라이브러리 설명 양식 -- 파트 2: 고객 레코드의 예

라이브러리 오브젝트를 위한 특정 권한을 나열하십시오.				
그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

이제 원하는 프로그램 라이브러리에 대한 공용 권한을 결정할 수 있습니다.

프로그램 라이브러리에 대한 공용 권한 결정

때로는 어플리케이션 프로그램이 파일이나 기타 오브젝트와는 다른 별도 라이브러리에 보유됩니다. 어플리케이션에 별도 라이브러리를 사용해야 하는 것은 아니지만 많은 프로그래머들이 어플리케이션을 설계할 때 이 기법을 사용합니다. 어플리케이션에 별도의

프로그램 라이브러리가 있으면 그 라이브러리에 대해 공용 권한을 결정해야 합니다. 라이브러리와 라이브러리의 프로그램 모두에 *USE 권한을 사용하여 프로그램을 충분히 실행할 수 있지만 프로그램 라이브러리에 추가 권한이 필요한 다른 오브젝트가 있을 수 있습니다. 프로그래머에게 다음에 관해 알아보십시오.

- 어플리케이션이 프로그램간 통신을 위해 자료 영역이나 메세지 대기행렬을 사용하는가? 자료 영역이나 메세지 대기행렬이 프로그램 라이브러리에 있는가? 자료 영역 및 메세지 대기행렬을 처리하기 위해서는 오브젝트에 *CHANGE 권한이 필요합니다.
- 프로그램 라이브러리의 오브젝트(예: 자료 영역)가 처리 중에 삭제되는가? 오브젝트를 삭제하기 위해서는 오브젝트에 *ALL 권한이 필요합니다.
- 프로그램 라이브러리의 오브젝트(예: 자료 영역)가 처리 중에 작성됩니까? 라이브러리에 신규 오브젝트를 작성하기 위해서는 라이브러리에 *CHANGE 권한이 필요합니다.

라이브러리 소유자와 권한 부여 리스트 열을 제외하고 라이브러리 설명 양식의 자원 보안 정보 모두를 채우십시오. 그리고 나서 라이브러리 및 오브젝트 소유권을 판별할 수 있습니다.

Sharon Jones가 프로그램 라이브러리에 대한 권한을 판별한 두 가지 방법의 예를 검토할 수 있습니다. 첫 번째 예에서 Sharon은 고객 주문 관리 프로그램 라이브러리에 대해 제한 없는 접근방식이 적합한 것으로 결정했습니다. 두 번째 예에서는 Sharon이 미수 처리 프로그램 라이브러리에 대해 사용한 보다 제한적인 접근방식을 보여줍니다.

예: JKL Toy사의 라이브러리 설명 양식 -- 비제한적인 접근방식

Sharon Jones는 고객 주문 관리 프로그램 라이브러리를 조사한 후 다음과 같은 결론을 내렸습니다.

- 프로그램간의 통신에 COMSGQ01 메세지 대기행렬을 사용합니다.
- 메세지 대기행렬은 지워지지만 삭제되지는 않습니다. 메세지 대기행렬에는 *CHANGE 권한으로 충분합니다.

Sharon은 프로그램 라이브러리의 모든 오브젝트에 대해 *USE 권한을 부여하고 COMSGQ01 메세지 대기행렬을 별도로 정의했습니다. 아래의 두 가지 표는 COPGMLIB 라이브러리를 위한 라이브러리 설명 양식을 나타냅니다.

표 43. JKL Toy사의 라이브러리 설명 양식: 프로그램 라이브러리의 예

라이브러리 설명 양식	**파트 2의 1**
라이브러리 이름: COPGMLIB	설명(텍스트): 고객 주문 관리 프로그램 라이브러리
라이브러리의 공용 권한: *USE 라이브러리내 오브젝트의 공용 권한: *USE 신규 오브젝트의 공용 권한 (CRTAUT): *USE 라이브러리 소유자:	

표 44. JKL Toy사의 라이브러리 설명 양식: 프로그램 라이브러리의 예

라이브러리 설명 양식				**파트 2의 2**
라이브러리내 개별 오브젝트에 대한 권한을 나열하십시오.				
그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

액세스를 제어할 프로그램에 대한 권한 사용

JKL Toy사의 대다수 직원들이 고객 정보를 변경할 수 있으나 소수의 사람들만 고객의 대변 한도를 설정할 수 있습니다. 대변 한도는 고객 마스터 파일(CUSTMAS)에 저장이 되지만 ARPGMLIB에 있는 ARPGM12라는 별도의 프로그램으로 변경이 이루어집니다. Sharon은 권한이 없는 사람들이 대변 한도를 변경하는 것을 막기 위해 이 프로그램을 제한할 수 있습니다. 아래의 표는 ARPGMLIB을 위한 라이브러리 설명 양식을 보여줍니다.

표 45. JKL Toy사의 라이브러리 설명 양식: 개인 권한의 예

라이브러리 설명 양식	**파트 2의 1**
라이브러리 이름: ARPGMLIB	설명(텍스트): 미수금 관리 프로그램 라이브러리
라이브러리의 공용 권한: *USE 라이브러리내 오브젝트의 공용 권한: *USE 신규 오브젝트의 공용 권한 (CRTAUT): *USE 라이브러리 소유자:	

표 46. JKL Toy사의 라이브러리 설명 양식: 개인 권한의 예

라이브러리 설명 양식				**파트 2의 2**
라이브러리내 개별 오브젝트에 대한 권한을 나열하십시오.				
그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

라이브러리 및 오브젝트 소유권 판별을 시작하기 전에 허용된 권한을 사용하는 제한적인 예를 검토할 수 있습니다.

예: JKL Toy사의 라이브러리 설명 양식 -- 제한적인 접근방식

지금까지 나온 예들은 라이브러리에 있는 정보에 대해 대다수의 사람들이 액세스를 가지는 저(relaxed) 상태의 보안 접근 방식을 보여주는 것입니다. JKL Toy사에서는 계약 및 가격 관리 정보를 기밀 사항으로 간주하고 있으므로 제한적 접근 방식을 필요로

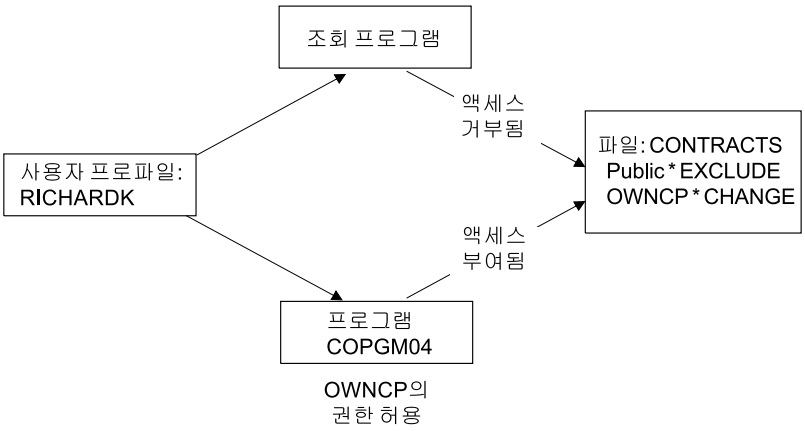
합니다. 다행스럽게도 이 모든 정보들은 별도의 라이브러리에 저장되어 있습니다. 계약 및 가격 관리 정보를 갱신하는 프로그램도 특별한 라이브러리에 있습니다.

Sharon은 계약 및 가격 관리 어플리케이션을 위한 보안 목적을 검토했습니다('자원 보안 목적 판별' 참조). Sharon은 또한 어플리케이션 설명 양식 및 라이브러리 설명 양식을 검토했습니다. Sharon은 어플리케이션의 보안 목적을 만족시키는 것이 어렵다고 생각하고 있습니다. 따라서 Sharon은 몇 가지 내용을 작성하여 어플리케이션 제공자와 논의하기로 했습니다.

- 판매 및 마케팅 직원 그리고 관리자들은 계약을 작성하고 변경할 수 있어야 합니다. 따라서 파일과 프로그램 둘다 사용해야 합니다.
- 주문을 처리하는 직원들은 주문을 입력하고 선적할 때 간접적으로 계약을 변경하거나 가격을 볼 수 있지만 다른 방법으로는 계약이나 가격을 볼 수 없습니다. 그러나 조회를 사용하여 고객 및 주문에 관한 자신만의 보고서를 작성할 수 있습니다. 계약 및 가격 관리 파일에 대한 권한이 있으면 조회 프로그램을 작성하여 그 파일들을 보거나 인쇄할 수 있습니다.

이 문제를 해결하기 위해 JKL Toy사에 어플리케이션을 제공자가 보안에 있어서 허용된 권한 피처를 사용할 것을 제안했습니다. **허용된 권한**은 프로그램이 실행되는 동안 사용자가 프로그램 소유자의 권한을 적용할 수 있게 해줍니다. 사용자에게 오브젝트에 대해 권한이 필요 없습니다.

아래의 다이어그램은 허용된 권한이 어떻게 작업하는지를 보여주는 예입니다. 주문 처리 부서의 Karen Richards(RICHARDK)에게는 정상적으로 계약 파일을 사용할 수 있는 권한이 없습니다. 그러나 주문을 입력할 때 계약의 잔고를 검사하고 갱신할 수 있어야 합니다. 계약의 잔고를 이용하여 작업하는 주문 입력 프로그램(COPGM04)이 OWNCP 프로파일 권한을 허용합니다. 따라서 COPGM04 프로그램을 실행하는 동안 Karen이 계약 관리 파일을 사용할 권한을 가질 수 있습니다.



오브젝트 소유권에 관한 자세한 설명은 ″오브젝트 및 라이브러리 소유권 판별″ 주제를 참조하십시오. 어플리케이션 제공자나 프로그래머가 프로그램을 작성(또는 컴파일)할 때 소유자 권한을 허용하도록 프로그램을 지정하거나 프로그래머가 CHGPGM(프로그램 변경) 명령을 이용하여 프로그램에 대해 허용된 권한을 지정할 수 있습니다. 이 방법을 사용하기 위해서는 먼저 프로그램의 모든 기능을 잘 알고 있어야 합니다.

Sharon은 판매 및 마케팅 부서 이외의 직원들에게 계약 및 가격 관리 파일에 대한 액세스를 부여하기 위해 허용된 권한 기능을 사용하기로 결정했습니다. Sharon은 또한 계약 및 가격 관리 어플리케이션이 사용되는 모든 오브젝트에는 *CHANGE 액세스로 충분하다고 결정했습니다. 아래 표는 계약 관리 라이브러리를 위한 라이브러리 설명 양식을 보여줍니다.

표 47. JKL Toy사의 라이브러리 설명 양식: 제한적 권한의 예

라이브러리 설명 양식		**파트 2의 1**
라이브러리 이름: CONTRACTS	설명(텍스트): 계약 및 가격 관리 라이브러리	
라이브러리 공용 권한: *EXCLUDE 라이브러리내 오브젝트의 공용 권한: *CHANGE 신규 오브젝트의 공용 권한(CRTAUT): *CHANGE 라이브러리 소유자:		

표 48. JKL Toy사의 라이브러리 설명 양식: 제한적 권한의 예

라이브러리 설명 양식				**파트 2의 2**
라이브러리내 개별 오브젝트에 대한 권한을 나열하십시오.				
그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

라이브러리 자체에 대해 액세스를 제한하기 때문에 라이브러리의 오브젝트에 대해 권한을 제한할 필요가 없습니다. 또한 Sharon은 관리자와 판매 및 마케팅 부서에 권한을 부여했습니다. Sharon은 부서의 각 개인들에게 권한을 부여하는 대신 그룹 권한을 부여했습니다.

주: 라이브러리에 대해 액세스를 가진 시스템 지식이 많은 프로그래머의 경우 라이브러리 권한을 취소시킨 이후에도 라이브러리의 오브젝트에 대한 액세스를 보유할 수 있습니다. 라이브러리에 상위 보안 요구사항을 가진 오브젝트가 있을 경우 완벽한 보호를 위해 오브젝트 및 라이브러리를 제한하십시오.

오브젝트 및 라이브러리 소유권의 판별을 시작하기 전에 공용 권한을 사용하는 비제한적 예를 검토할 수 있습니다.

라이브러리 및 오브젝트 소유권 판별

어플리케이션 라이브러리에 대한 보안 계획을 수립했으면 라이브러리 및 오브젝트 소유권을 결정할 수 있습니다. 각 오브젝트를 작성할 때 오브젝트마다 소유자가 할당됩니다. 오브젝트 소유자는 자동으로 오브젝트에 대한 모든 권한을 가지며 이 권한에는 다른 사용자가 오브젝트를 사용할 수 있도록 권한을 부여하고 오브젝트를 변경하며 오브젝트를 삭제하는 것이 포함됩니다. 보안 담당자가 시스템의 각 오브젝트에 대해 이 기능을 수행할 수 있습니다.

시스템이 오브젝트 소유자의 프로파일을 사용하여 오브젝트에 대한 권한을 가진 사용자를 추적합니다. 시스템은 이 기능을 내부적으로 완료합니다. 이것이 사용자 프로파일에 직접 영향을 주지 않을 수 있습니다. 그러나 오브젝트 소유권을 올바로 계획하지 않으면 일부 사용자 프로파일이 상당히 커질 수 있습니다.

시스템은 오브젝트를 저장할 때 소유 프로파일 이름 또한 저장합니다. 시스템은 오브젝트를 복원할 때 이 정보를 사용합니다. 복원시킨 오브젝트를 위한 소유 프로파일이 시스템에 없으면 시스템이 소유권을 QDFTOWN이라는 IBM 제공 프로파일로 전송합니다.

권장사항

다음에 나오는 권장사항은 여러 가지 상황에 적용되지만 모든 상황에 다 적용되는 것은 아닙니다. 권장사항을 검토한 후 프로그래머나 어플리케이션 제공자와 오브젝트 소유권에 대해 의견을 교환하십시오. 어플리케이션을 구매할 경우에는 프로파일이 어떤 라이브러리와 오브젝트를 소유하는지를 제어하지 못할 수 있습니다. 어플리케이션에 소유권 변경을 방지하는 설계가 사용되었을 수 있습니다.

- IBM 제공 프로파일(예: QSECOFR 또는 QPGMR)을 어플리케이션 소유자로 사용하지 마십시오. 이 프로파일은 IBM 제공 라이브러리 안에 많은 오브젝트를 가지고 있으므로 이미 상당히 큽니다.
- 일반적으로 그룹 프로파일은 어플리케이션을 소유할 수 없습니다. 특별히 하위 권한을 할당하지 않는 한 그룹의 모든 멤버가 그룹 프로파일과 동일한 권한을 가집니다. 실제로는 그 그룹의 모든 멤버에게 어플리케이션에 대한 모든 권한을 부여하게 됩니다.
- 여러 부서의 관리자에게 어플리케이션의 제어 책임을 위임하는 경우 그러한 관리자들은 모든 어플리케이션 오브젝트의 소유자가 될 수 있습니다. 그러나 어플리케이션 관리자가 책임을 변경시킬 수 있습니다. 이 경우 모든 어플리케이션 오브젝트의 소유권을 신규 관리자에게 전송할 수 있습니다.
- 많은 사람들이 *NONE으로 암호를 설정한 각 어플리케이션에 대해 특별한 소유자 프로파일을 작성하는 기술을 사용합니다. 시스템은 소유 프로파일을 사용하여 어플

리케이션에 대한 권한을 관리합니다. 보안 담당자(또는 해당 권한을 가진 사용자)는 어플리케이션을 실제로 관리하거나 특정 어플리케이션에 대해 *ALL 권한을 가진 관리자에게 위임됩니다.

어플리케이션을 소유해야 하는 프로파일을 결정하십시오. 각 라이브러리 설명 양식에 소유자 프로파일 정보를 기록하십시오.

사용자 라이브러리에 대한 소유권 및 액세스 결정을 시작하기 전에 JKL Toy사가 어플리케이션 소유권을 판별한 방법의 예를 검토하십시오.

예: JKL Toy사의 어플리케이션 소유권

Sharon Jones는 어플리케이션마다 특별한 소유자 프로파일을 작성하기로 결정했습니다. Sharon 및 백업 보안 담당자인 Ken Harrison이 어플리케이션 보안 관리 책임을 담당할 것입니다. 향후에 회사의 보안 요구사항이 더 복잡해지더라도 Sharon은 권한 관리를 위한 일부 권한을 부서 관리자에게 위임할 수 있습니다.

Sharon이 명명 규칙 양식에 신규 항목을 추가했습니다.

표 49. JKL Toy사의 명명 규칙 양식: 소유자 프로파일의 예

오브젝트 유형	명명 규칙
소유자 프로파일	각 어플리케이션별로 소유자 프로파일을 작성합니다. 소유자 프로파일이 내재되어 있는 모든 어플리케이션 라이브러리와 오브젝트를 소유합니다. 소유자 프로파일은 어플리케이션 약어를 덧붙여 OWN으로 명명합니다. 재고 관리 소유자 프로파일은 OWNIC입니다.

Sharon은 모든 소유자 프로파일이 화면과 리스트에 함께 나올 수 있도록 소유자 프로파일 이름을 OWN으로 시작하기로 결정했습니다.

Sharon이 소유자를 모든 어플리케이션 라이브러리에 할당하고 명명 규칙 양식에 그 정보를 입력했습니다. 둘 이상의 어플리케이션 소유자를 가질 가능성이 있는 유일한 라이브러리가 고객 레코드 라이브러리입니다. 미수금 관리 어플리케이션이 신규 고객을 작성하고 대변 한도를 설정하므로 Sharon은 이 어플리케이션이 고객 파일을 소유해야 한다고 결정했습니다. 다음은 Sharon이 할당한 소유자입니다.

라이브러리 이름	소유자 이름
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

이제 소유권 및 액세스를 결정할 수 있습니다.

사용자 라이브러리에 대한 소유권 및 액세스 결정

시스템에 IBM Query for iSeries 사용권 프로그램이나 다른 의사결정 지원 프로그램이 있으면 사용자들이 작성하는 조회 프로그램을 저장하기 위한 라이브러리가 필요합니다. 일반적으로 이 라이브러리는 사용자 프로파일에서 **현재 라이브러리**입니다. 각 사용자의 현재 라이브러리를 작성하는 것에 대한 자세한 정보는 "사인 온에 영향을 주는 값 선택"을 참조하십시오. Sharon Jones는 판매 및 마케팅 부서에 대해서는 현재 라이브러리를 사용하고 다른 부서에 대해서는 그룹 라이브러리를 사용하기로 계획합니다.

- 판매 및 마케팅 부서에서는 조회를 많이 합니다. 따라서 각 사용자에게 개인용 라이브러리가 있어야 합니다. 그렇지 않으면 자신의 조회를 어떻게 명명해야 할지에 대해 고민해야 하고 실수로 다른 사용자의 프로그램을 삭제할 수도 있습니다.
- 다른 부서들은 그룹 라이브러리를 사용할 것입니다. 많은 조회 프로그램을 작성할 경우에는 개별 라이브러리를 고려할 수 있습니다.

한 사용자가 하나의 그룹에 속하면 그 사용자 프로파일의 한 필드에 그 사용자가 작성한 오브젝트를 자신이 소유하는지 아니면 그룹이 소유하는지를 지정하십시오. 사용자가 오브젝트를 소유하면 그룹 멤버들이 그 오브젝트를 사용하기 위해 갖는 권한을 지정할 수 있습니다. 그룹의 권한이 1차 그룹 권한인지 아니면 개인 권한인지의 여부도 지정할 수 있습니다. 1차 그룹 권한이 더 좋은 시스템 성능을 제공할 수 있습니다. Sharon은 사용자 라이브러리에 관해 추가로 메모를 작성했습니다.

- 판매 및 마케팅 부서에서는 오브젝트를 소유한 그룹을 가지는 것이 아니라 자신이 작성한 오브젝트를 소유해야 합니다. 따라서 다른 사용자의 조회 프로그램을 변경할 필요가 없습니다.
- 그룹의 모든 사람은 다른 사람의 조회 프로그램을 실행할 수 있어야 하며 이것은 그 그룹이 그룹 멤버가 작성한 오브젝트에 대해 *USE 권한을 갖는다는 것을 의미합니다.
- 그룹의 권한은 1차 그룹 권한이어야 합니다.
- 일반 사람들은 이 라이브러리에 대한 액세스를 가질 수 없습니다. 판매 및 마케팅 부서에는 조회에서 나온 출력 파일이 있습니다. 그와 같은 파일에는 기밀 자료가 들어 있을 가능성이 있습니다.
- 다른 부서의 경우에는 그룹이 그룹 라이브러리와 라이브러리에 작성된 모든 것을 소유합니다. 이것은 그룹의 멤버가 라이브러리의 내용을 변경 또는 삭제할 수 있음을 의미합니다. 이로 인해 문제가 발생할 경우에는 다른 방법을 시도해야 합니다.

아래 표는 사용자가 소유한 오브젝트를 사용하는 판매 및 마케팅 부서의 개별 사용자 프로파일 양식을 보여줍니다.

표 50. JKL Toy사의 개별 사용자 프로파일 양식: 사용자가 소유하는 오브젝트의 예

그룹 프로파일명: DPTSM	
작성된 오브젝트의 소유자: *USRPRF	작성된 오브젝트에 대한 그룹 권한: *USE
그룹 권한 유형: *PGP	

아래 표는 그룹이 소유한 오브젝트를 사용하는 부서의 개별 사용자 프로파일 양식을 보여줍니다.

표 51. JKL Toy사의 개별 사용자 프로파일 양식: 그룹이 소유한 오브젝트의 예

그룹 프로파일명: DPTxx	
작성된 오브젝트의 소유자: *GRPPRF	작성된 오브젝트의 그룹 권한:

작성된 오브젝트에 대한 그룹 권한 필드는 작성된 오브젝트의 소유자가 그룹이면 사용되지 않습니다. 그룹 멤버들은 작성된 오브젝트에 대해 자동으로 *ALL 권한을 갖습니다.

사용자 라이브러리를 소유하고 액세스해야 하는 사용자를 결정하십시오. 개별 사용자 프로파일 양식의 **작성된 오브젝트 소유자** 및 **오브젝트에 대한 그룹 권한** 필드에 선택사항을 입력하십시오. 이제 오브젝트 그룹화를 시작할 준비가 되었습니다.

오브젝트 그룹화

라이브러리 및 오브젝트 소유권 판별을 수행했으면 시스템에서 오브젝트 그룹화를 시작할 수 있습니다. 관리 권한을 단순화하려면 권한 부여 리스트를 사용하여 같은 요구사항의 오브젝트들을 그룹화하십시오. 그리고 나서 리스트의 개별 오브젝트가 아닌 권한 부여 리스트에 공용 권한, 그룹 프로파일 권한, 사용자 프로파일 권한을 부여할 수 있습니다. 시스템은 권한 부여 리스트로 보안시킨 모든 오브젝트를 같은 것으로 처리하지만 서로 다른 사용자에게 전체 리스트의 서로 다른 권한을 부여할 수 있습니다.

권한 부여 리스트를 사용하면 오브젝트를 복원할 때 권한을 재설정하는 것이 더 쉽습니다. 권한 부여 리스트가 있는 오브젝트를 보안시키면 복원 프로세스가 그 오브젝트를 자동으로 리스트와 링크시킵니다.

그룹 또는 사용자에게 권한 부여 리스트 관리 권한(*AUTLMGT)을 부여할 수 있습니다. 권한 부여 리스트 관리는 사용자가 리스트에 다른 사용자들을 추가하거나 제거하여 그 사용자를 위한 권한을 변경할 수 있게 해줍니다.

권장사항

- 보안 보호가 필요하고 유사한 보안 요구사항을 가진 오브젝트에 권한 부여 리스트를 사용하십시오. 권한 부여 리스트를 사용하면 개별 권한이 아닌 권한 범주에 관해 생각하게 만듭니다. 권한 부여 리스트는 또한 시스템의 오브젝트 복원 및 권한 감사를 더 쉽게 만듭니다.

- 권한 부여 리스트, 그룹 권한, 개별 권한을 결합시킨 복잡한 구조는 피하십시오. 동시에 모든 방법을 사용하지 말고 요구사항에 가장 적합한 방법을 선택하십시오.

명명 규칙 양식에 권한 부여 리스트에 대한 명명 규칙도 추가해야 합니다.

일단 권한 부여 리스트 양식을 준비했으면 다시 돌아가서 라이브러리 설명 양식에 해당 정보를 추가하십시오. 프로그래머나 어플리케이션 제공자가 이미 권한 부여 리스트를 작성했을 수도 있습니다. 반드시 검사하십시오.

프린터 및 프린터 출력에 대한 보안 계획을 수립하기 전에 JKL Toy사의 Sharon Jones가 권한 부여 리스트를 계획한 방법의 예를 검토하십시오.

예: JKL Toy사의 권한 부여 리스트 양식

Sharon은 고객 레코드 라이브러리를 위한 라이브러리 설명을 검토하여 매월 말에 지워지는 파일에 대해 권한 부여 리스트를 작성하기로 결정했습니다. 비록 세 개의 파일만 지워지지만 Sharon은 권한 관리를 단순화시키기 위해 권한 부여 리스트를 사용하기로 결정했습니다. 나중에 월말 프로세스에 다른 파일을 추가할 경우 권한 부여 리스트를 통해 그 파일에 간단하게 보안을 설정할 수 있습니다. Sharon은 월말 처리에서 발생할 수 있는 예기치 못한 문제를 방지하기 위해 파일에서 공용 권한은 제외하기로 결정했습니다. Sharon은 처리를 실행하는 사용자에게만 *ALL 권한을 부여했습니다. 야간 근무 시스템 오퍼레이터인 Rose Willis는 월말 처리를 검사하기 위해 파일에 관한 정보를 볼 수 있어야 합니다. Rose Willis에게는 *USE 권한이 필요합니다.

아래 표는 Sharon이 권한 부여 리스트를 위해 사용한 명명 규칙을 보여줍니다.

표 52. JKL Toy사의 명명 규칙 양식: 권한 부여 리스트의 예

명명 규칙 양식	
작성자: Sharon Jones	날짜: 1999년 9월 5일
오브젝트 유형	**명명 규칙**
권한 부여 리스트	하나의 라이브러리에서 나온 오브젝트들을 보안하는 리스트의 경우 라이브러리명의 일부와 함께 LST 및 하나의 숫자를 사용하십시오. CUSTLIB의 오브젝트 리스트는 CUSTLST1이 될 것입니다. 두 개 이상의 라이브러리에서 나온 오브젝트를 보안하는 리스트의 경우 가능하면 ARLST1과 같은 어플리케이션 약어를 사용하십시오. 리스트가 여러 어플리케이션에 적용되면 의미있는 이름을 선택하십시오. 리스트의 설명은 기본 목적을 나타내는 것이어야 합니다.

아래 표는 CUSTLIB 라이브러리를 위한 권한 부여 리스트 양식을 보여줍니다. Sharon은 라이브러리 설명 양식에 있는 정보를 사용하여 이 양식을 준비했습니다.

표 53. JKL Toy사의 권한 부여 리스트 계획: 예

권한 부여 리스트 양식
권한 부여 리스트 이름: CUSTLST1
설명: 월말 처리 중 지워지는 파일.
리스트에서 보안시킨 오브젝트를 나열하십시오.

표 53. JKL Toy사의 권한 부여 리스트 계획: 예 (계속)

오브젝트 이름	오브젝트 유형	오브젝트 라이브러리	오브젝트 이름	오브젝트 유형	오브젝트 라이브러리
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
리스트에 대해 액세스를 가진 그룹 및 사용자를 나열하십시오.					
그룹 또는 사용자	허용되는 액세스 유형	리스트 관리?	그룹 또는 사용자	허용되는 액세스 유형	리스트 관리?
PUBLIC	*EXCLUDE	아니오	ROSSG	*ALL	아니오
SMITHJ	*ALL	아니오	JONESS	*ALL	예
WILLISR	*USE	아니오			

Sharon은 또한 CUSTLIB 라이브러리를 위한 라이브러리 설명 양식에 권한 부여 리스트 정보를 추가했습니다.

라이브러리 설명 양식				파트 2의 2
작성자: Sharon Jones			날짜: 1999년 9월 9일	
라이브러리 이름: CUSTLIB				
라이브러리 오브젝트를 위한 특정 권한을 나열하십시오.				
그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

공용 권한을 판별하기 위해 권한 부여 리스트를 사용하는 시스템의 경우 각 파일의 공용 권한을 *AUTL로 변경시켜야 하는 점에 주목하십시오.

라이브러리 설명 양식에서 그룹 및 개별 권한을 살펴보십시오. 권한 부여 리스트를 사용하는 것이 적절한 것인지 결정하십시오. 적절하다면 권한 부여 리스트 양식을 준비하고 권한 부여 리스트 정보와 함께 라이브러리 설명 양식을 갱신하십시오. 이제 프린터 및 프린터 출력의 보안을 계획할 수 있습니다.

프린터 및 프린터 출력에 대한 보안 계획

오브젝트를 그룹화했으면 프린터 출력을 보호하는 방법을 계획해야 합니다. 시스템에 저장된 정보를 보호하기 위한 계획을 완료했습니다. 이제 인쇄 중에 또는 인쇄를 기다리는 중에 기밀 정보를 보호하기 위한 계획이 필요합니다. 회사에서 기밀 출력에 사용하는 프린터의 물리적 보안 계획을 검사하십시오.

보고서를 인쇄하는 프로그램을 실행할 때 보통은 보고서가 프린터로 직접 가지 않습니다. 프로그램이 **스풀 파일** 또는 **프린터 출력**이라고 하는 보고서 사본을 작성합니다. 그리고 시스템이 프린터를 사용할 수 있을 때까지 **출력 대기행렬**이라는 오브젝트에 스풀

파일을 저장합니다. 출력 대기행렬에 프린터 출력이 있으면 워크스테이션에서 보고서를 볼 수 있습니다. 또한 프린터 출력을 보유시키거나 특정 프린터로 지정할 수 있습니다.

스풀링은 더 쉽게 인쇄 작업을 스케줄링하고 프린터를 공유할 수 있게 해줍니다. 스풀링은 또한 기밀 출력을 보호할 때 도움이 됩니다. 특수 출력 대기행렬을 하나 이상 작성하여 기밀 출력을 보유시키고 그 출력 대기행렬을 보거나 관리할 수 있는 사람들을 제한할 수 있습니다. 또한 기밀 출력을 대기행렬에서 프린터로 보내는 시기를 제어할 수도 있습니다.

이 주제를 통해 작업해 나가면서 프린터 출력 및 워크스테이션 보안 양식을 완료하십시오.

특수 출력 대기행렬을 작성할 때 보안과 관련된 여러 가지 매개변수를 지정할 수 있습니다.

- **DSPDTA(자료 표시) 매개변수**: 출력 대기행렬의 DSPDTA 매개변수는 한 사용자가 소유하고 있는 스풀 파일을 다른 사용자가 보거나 송신하거나 복사할 수 있는지를 판별합니다.
- **AUTCHK(검사 권한) 매개변수**: 출력 대기행렬의 AUTCHK 매개변수는 한 사용자가 소유하고 있는 스풀 파일을 다른 사용자가 변경하거나 삭제할 수 있는지를 판별합니다.
- **오퍼레이터 제어(OPRCTL) 매개변수**: 출력 대기행렬의 OPRCTL 매개변수는 *JOBCTL 특수 권한(또는 *SYSOPR 사용자 클래스)을 가진 사용자가 출력 대기행렬을 제어할 수 있는지를 판별합니다.

출력 대기행렬 매개변수, 출력 대기행렬에 대한 사용자의 권한, 사용자의 특수 권한은 사용자가 출력 대기행렬의 스풀 파일에서 수행할 수 있는 기능을 판별하기 위해 함께 작업합니다. 아래 표는 사용자들이 서로 다른 기능을 수행할 수 있게 해 주는 조합을 표시한 것입니다.

인쇄 기능	출력 대기행렬 매개변수			출력 대기행렬 권한	특수 권한
	DSPDTA	**AUTCHK**	**OPRCTL**		
스풀 파일을 대기행렬에 추가합니다.[1]	Any	Any	Any	*READ	없음
	Any	Any	*Yes	Any	*JOBCTL
스풀 파일 리스트를 봅니다 (WRKOUTQ 명령).[2]	Any	Any	Any	*READ	없음
	Any	Any	*Yes	Any	*JOBCTL
스풀 파일을 표시, 복사, 전송합니다(DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPLF).[2]	*YES	Any	Any	*READ	없음
	*NO	*DTAAUT	Any	*CHANGE	없음
	*NO	*OWNER	Any	Owner[3]	없음
	*YES	Any	*Yes	Any	*JOBCTL
	*NO	Any	*Yes	Any	*JOBCTL
	*OWNER[5]	Any	Any	Any	Any

스풀 파일을 변경, 삭제, 보류, 해제합니다(CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF).[2]	Any	*DTAAUT	Any	*CHANGE	없음
	Any	*OWNER	Any	Owner[3]	없음
출력 대기행렬을 변경, 지우기, 보류, 해제합니다(CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT).[2]	Any	*DTAAUT	Any	*CHANGE	없음
	Any	*OWNER	Any	Owner[3]	없음
	Any	Any	*YES	Any	*JOBCTL
대기행렬을 위해 출력기를 시작합니다(STRPRTWTR, STRRMTWTR). [2]	Any	*DTAAUT	*Any	*CHANGE[4]	없음
	Any	Any	*YES	Any[4]	*JOBCTL

1 이것은 출력을 출력 대기행렬로 지정하기 위한 필수 권한입니다.

2 이 명령이나 화면에서 이에 해당하는 옵션 사용

3 사용자가 출력 대기행렬의 소유자이어야 합니다.

4 프린터 장치 설명에 대한 *USE 권한도 필요합니다.

5 사용자가 스풀 파일의 소유자이거나 *SPLCTL 특수 권한을 가지고 있어야 합니다.

물리적 보안 계획의 프린터 부분을 검토하십시오. 주제를 통해 작업해 나가면서 프린터 출력 및 워크스테이션 보안 양식의 출력 대기행렬 섹션을 채우십시오.

워크스테이션에 대한 자원 보안 계획을 수립하기 전에 JKL Toy사의 Sharon Jones가 이 출력 대기행렬 매개변수를 판별한 방법의 예를 검토할 수 있습니다.

예: JKL Toy사의 출력 대기행렬 및 워크스테이션 보안 양식 -- 출력 대기행렬 부분

JKL Toy사의 판매 및 마케팅 부서에는 기밀 사항을 인쇄할 때 지켜야 하는 두 가지 요구사항이 있습니다.

- 임시 가격 리스트는 가격 변경이 예정되어 있을 때 인쇄하는 것입니다. 회사 관리자를 제외하고 판매 및 마케팅 부서 외부인은 절대로 이 정보를 볼 수 없습니다.
- 협상 중에는 계약이 기밀 사항입니다. 계약서의 초안은 계약을 협상 중인 당사자만 볼 수 있어야 하며 판매 및 마케팅 부서의 다른 사람들은 볼 수 없습니다.

Sharon은 두 가지의 특별한 출력 대기행렬을 작성하기로 결정했습니다.

PRICEQ

임시 가격 리스트에 사용합니다. 판매 및 마케팅 부서의 모든 사람들은 출력 대기행렬의 모든 기능을 수행할 수 있습니다. 시스템 오퍼레이터를 포함하여 판매 및 마케팅 부서 이외의 사람들은 출력 대기행렬을 사용할 수 없습니다. PRICEQ는 CONTRACTS 라이브러리에 있습니다.

NEWCP

협상 중인 계약을 인쇄할 때 사용합니다. 출력 대기행렬은 판매 및 마케팅 부

서가 공유하지만 출력 대기행렬의 스풀 파일을 작성한 사람만 파일을 제어할 수 있습니다. NEWCP는 CONTRACTS 라이브러리에 있습니다.

아래 표는 Sharon이 출력 대기행렬을 위해 준비한 출력 대기행렬 및 워크스테이션 보안 양식을 보여줍니다.

표 54. JKL Toy사의 출력 대기행렬 및 워크스테이션 보안 양식: 프린터 출력 대기행렬의 예

제한적인 출력 대기행렬의 매개변수를 나열하십시오.				
출력 대기행렬 이름	출력 대기행렬 라이브러리	모든 파일 표시 (DSPDTA)	검사 권한(AUTCHK)	오퍼레이터 제어 (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

프로그램 라이브러리에 대한 공용 권한 결정 주제에는 JKL Toy사의 CONTRACTS 라이브러리를 위한 권한을 보여주는 예가 나옵니다. 판매 및 마케팅 부서의 관리자와 직원들만 라이브러리에 액세스합니다. 라이브러리 오브젝트(출력 대기행렬을 포함하여)에 대한 공용 권한은 *CHANGE입니다.

NEWCP 출력 대기행렬의 AUTCHK 매개변수가 *OWNER이므로 스풀 파일의 소유자만 그 파일에 작업할 수 있습니다(위에 나오는 '인쇄 기능을 수행하는 데 필요한 권한' 표 참조). 이 기능은 판매 및 마케팅 부서의 직원들이 서로 다른 사람의 신규 계약을 인쇄하거나 출력 대기행렬에서 보지 못하도록 합니다.

프린터 출력 대기행렬 보안을 계획했으면 워크스테이션 보안을 계획할 수 있습니다.

워크스테이션에 대한 보안 계획

프린터 및 프린터 출력에 대한 자원 보안 계획을 수립했으면 워크스테이션 보안 계획을 시작할 수 있습니다. 물리적 보안 계획에서, 위치로 인해 보안 위험이 있는 워크스테이션을 나열했습니다. 이 정보를 사용하여 제한해야 하는 워크스테이션을 판별하십시오.

이 워크스테이션을 사용하는 사용자들이 특별히 보안에 유의하도록 할 수 있습니다. 워크스테이션을 떠날 때마다 사인 오프해야 합니다. 보안 정책에서 공격받기 쉬운 워크스테이션을 위해 사인 오프 프로시듀어에 대한 결정을 기록하고자 할 수 있습니다. 해당 워크스테이션에서 수행할 수 있는 기능을 제한하여 위험을 최소화할 수도 있습니다.

워크스테이션의 기능을 제한하는 가장 쉬운 방법은 제한된 기능으로 사용자 프로파일을 제한하는 것입니다. Sharon Jones는 JKL 장난감 회사의 재고 관리 부서에 위의 기법을 사용했습니다. Sharon은 로딩 도크에서 근무하는 Ray Wagner 및 Janice Ames에게 명세 수신 프로그램 실행만 허용했습니다. 또한 Sharon은 이들만을 로딩 도크의 워크스테이션에 사인 온할 수 있도록 허용했습니다.

보안 담당자 또는 서비스 권한을 가진 사용자가 모든 워크스테이션에서 사인 온하지 못하도록 선택할 수 있습니다. 이를 수행하기 위해 QLMTSECOFR 시스템 값을 사용하는 경우, 보안 담당자 권한을 가진 사용자는 특별히 권한이 있는 워크스테이션에서만 사인 온할 수 있습니다.

출력 대기행렬 및 워크스테이션 보안 양식의 워크스테이션 부분을 준비하십시오.

출력 대기행렬 및 워크스테이션 보안 양식의 워크스테이션 부분을 준비할 때 Sharon이 워크스테이션에 대한 보안을 계획한 방법의 예를 볼 수 있습니다. 자원 보안 권장사항 리스트도 검토하여 자원 보안 계획을 단순하면서도 완벽하게 만드십시오. 예와 권장사항을 검토했으면 어플리케이션 설치 계획을 시작할 수 있습니다.

예: JKL Toy사의 출력 대기행렬 및 워크스테이션 보안 양식 -- 워크스테이션 부분

Sharon Jones는 보안 노출의 가능성이 있는 워크스테이션을 판별하기 위해 물리적 보안 계획을 검토했습니다. 예를 들어, JKL Toy사에서는 직원이 아니더라도 출고지나 영업 지사에 있는 워크스테이션에 쉽게 접근할 수 있습니다. Sharon은 물리적 보안 계획에 이와 같은 워크스테이션들이 잠재적인 보안 노출 가능성을 가지고 있음을 표시했습니다.

워크스테이션의 기능을 제한하는 가장 쉬운 방법은 제한된 기능으로 사용자 프로파일을 제한하는 것입니다. Sharon Jones는 JKL Toy사의 자재 관리 부서에 이 방법을 사용했습니다. Sharon은 출고지에서 근무하는 Ray Wagner 및 Janice Ames에게 재고 입고 프로그램만 실행할 수 있게 허용했습니다. 또한 Sharon은 이 사람들만 출고지의 워크스테이션에 사인 온할 수 있도록 허용했습니다.

Sharon은 QLMTSECOFR 시스템 값에 대한 자신의 선택을 재평가했습니다. Sharon은 출고지와 영업 지사에 설치한 워크스테이션의 추가적인 보호를 위해 값을 1(예)로 설정하기로 결정했습니다.

아래 표는 Sharon이 준비한 출력 대기행렬 및 워크스테이션 보안 양식의 워크스테이션 부분을 보여줍니다.

표 55. JKL Toy사의 출력 대기행렬 및 워크스테이션 보안 양식: 워크스테이션의 예

보안 담당자 워크스테이션: 특정 워크스테이션(시스템 값 QLMTSECOFR이 '예'일 경우)으로 보안 담당자를 제한할 경우 보안 담당자 및 *ALLOBJ 권한이 있는 사용자에게 허용된 워크스테이션 모두를 아래에 나열하십시오. 기타 모든 워크스테이션은 그 아래에 나열하십시오.	
제한된 워크스테이션을 위한 권한을 아래 리스트에 나열하십시오.	
워크스테이션 이름	권한이 있는 그룹 및 사용자(*CHANGE 권한)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB

표 55. JKL Toy사의 출력 대기행렬 및 워크스테이션 보안 양식: 워크스테이션의 예 (계속)

RMT02	UNGERJ, BELLB

어플리케이션 설치 계획을 세우기 전에 자원 보안 권장사항의 요약을 검토할 수 있습니다.

자원 보안 권장사항 요약

워크스테이션 보안 계획을 완료했으면 다음에 나오는 자원 보안 권장사항을 검토할 수 있습니다. iSeries 시스템은 시스템에 있는 정보를 보호하기 위한 많은 옵션들을 제공합니다. 이 옵션들은 회사를 위한 최적의 자원 보안 계획을 설계할 수 있는 유연성을 제공합니다. 그러나 이 많은 옵션들이 혼란스러울 수도 있을 것입니다.

이 주제에서는 JKL Toy사의 예를 통해 다음 지침을 사용하는 자원 보안 계획의 기본적인 접근방식을 설명합니다.

- 일반적인 것에서 세부적인 것으로 이동하십시오.
  - 라이브러리에 대한 보안을 계획하십시오. 필요한 경우에만 개별 오브젝트를 처리하십시오.
  - 먼저 공용 권한을 계획하고 그 다음에 그룹 권한과 개별 권한을 계획하십시오.
- 성능을 향상시키고 백업 및 회복을 단순화하기 위해 공용 권한을 사용하여 보안 요구사항을 충족할 수 없는 오브젝트에 대해서만 특정 보안을 정의하십시오.
- 라이브러리의 신규 오브젝트에 대한 공용 권한(CRTAUT)을 라이브러리에 있는 다수의 기존 오브젝트에 대해 정의한 공용 권한과 같게 만드십시오.
- 그룹이나 개인에게 공용 권한 미만의 권한을 부여하지 않도록 하십시오. 이 경우 성능이 저하되고 오류의 원인이 될 수 있으며 감사가 힘들어집니다. 모든 사용자가 적어도 오브젝트에 대해 공용 권한과 동일한 권한을 갖는다는 것을 알면 보안 계획과 감사가 쉽습니다.
- 권한 부여 리스트를 사용하여 같은 보안 요구사항을 가진 오브젝트를 그룹화하십시오. 권한 부여 리스트는 개별 권한보다 관리가 간단하며 보안 정보 회복을 도와줍니다.
- 특수 사용자 프로파일을 어플리케이션 소유자로 작성하십시오. 소유자 암호를 *NONE으로 설정하십시오.
- IBM 제공 프로파일(예: QSECOFR 또는 QPGMR)이 어플리케이션을 소유하지 않도록 하십시오.
- 기밀 보고서에 특별한 출력 대기행렬을 사용하십시오. 출력 대기행렬을 기밀 정보와 같은 라이브러리에 위치시키십시오.
- 보안 담당자 권한을 가진 사용자 수를 제한하십시오.

- 오브젝트나 라이브러리에 *ALL 권한을 부여할 때에는 주의하십시오. *ALL 권한을 가진 사람들이 실수로 내용을 삭제할 수 있습니다.

다음 정보를 수집하여 자원 보안 설정을 위해 성공적으로 계획했는지 확인하십시오.

- 모든 어플리케이션 라이브러리에 대해 라이브러리 설명 양식의 파트 1과 파트 2를 채우십시오.
- 개별 사용자 프로파일 양식의 **작성된 오브젝트 소유자**와 **작성된 오브젝트에 대한 그룹 권한** 필드를 채우십시오.
- 명명 규칙 양식에 권한 부여 리스트를 명명하기 위해 계획한 방법을 설명하십시오.
- 권한 부여 리스트 양식을 준비하십시오.
- 라이브러리 설명 양식에 권한 부여 리스트 정보를 추가하십시오.
- 출력 대기행렬 및 워크스테이션 보안 양식을 준비하십시오.

이제 어플리케이션 설치 계획을 수립할 준비가 되었습니다.

어플리케이션 설치 계획

자원 보안 계획을 완료하기 위해서는 어플리케이션 설치를 준비해야 합니다. 다음 주제는 어플리케이션을 설치한 후 어플리케이션에 대한 소유권 및 권한을 계획할 때 도움을 줍니다. 여기에서 설명하는 방법이 모든 어플리케이션에 적용되는 것은 아닙니다. 훌륭한 설치 계획을 개발하기 위한 도움을 받으려면 프로그래머나 어플리케이션 제공자에게 문의하십시오.

어플리케이션 제공자로부터 어플리케이션을 구입하려는 경우 이 정보를 사용하여 어플리케이션 라이브러리를 로드하기 전과 그 후에 수행해야 하는 보안 활동을 계획하십시오.

사용자 소유의 시스템에 프로그래머가 개발한 어플리케이션을 설치하려는 경우 이 정보를 사용하여 테스트에서 제품 상태로 어플리케이션을 이동시키는 데 필요한 보안 활동을 계획하십시오.

하나의 어플리케이션에 대해 이 단계를 모두 완료하십시오. 그런 다음 다시 돌아가서 추가 어플리케이션에 대해 어플리케이션 설치 양식을 준비하십시오.

필요한 양식

다음 양식을 복사하여 이 주제를 완료할 때 양식을 채우십시오.

표 56. 어플리케이션 설치 계획에 필요한 계획 양식

양식명	필요한 사본 수
어플리케이션 설치 양식	어플리케이션당 한개

어플리케이션 설치를 계획하기 위해 정보를 수집하려면 앞에서 작업한 다음 양식을 사용하십시오.

양식명	준비 위치:
라이브러리 설명 양식	라이브러리 정보 설명
권한 부여 리스트 양식	오브젝트 그룹화

어플리케이션 로드 주제에서 어플리케이션 설치에 필요한 각 단계를 수행하는 방법에 관해 설명합니다.

어플리케이션 설치를 계획하려면 다음 주제를 참조하십시오.

- 어플리케이션에 대한 사용자 프로파일 및 설치 값 판별
- 설치 값 변경

어플리케이션에 대한 사용자 프로파일 및 설치 값 판별

어플리케이션 설치 계획을 수립할 때에는 먼저 각 어플리케이션에 대해 사용자 프로파일과 설치 값을 결정해야 합니다. 그리고 다른 시스템에서 작성한 어플리케이션을 설치하기 위해서는 먼저 사용자 프로파일을 하나 이상 작성해야 할 수 있습니다. 라이브러리를 로드하기 전에 어플리케이션 라이브러리와 오브젝트를 소유하는 사용자 프로파일이 시스템에 있어야 합니다. 각 라이브러리에 대해 작성해야 하는 프로파일을 기록하고 어플리케이션 설치 양식에 프로파일이 필요로 하는 매개변수를 기록하십시오.

필요한 설치 값을 판별하려면 프로그래머나 어플리케이션 제공자에게 다음 사항을 문의하여 어플리케이션 설치 양식에 응답을 기록하십시오.

- 어플리케이션 라이브러리를 소유하는 프로파일이 어느 것입니까?
- 라이브러리의 오브젝트를 소유하는 프로파일이 어느 것입니까?
- 라이브러리에 대한 공용 권한(AUT)이 무엇입니까?
- 신규 오브젝트에 대한 공용 권한(CRTAUT)이 무엇입니까?
- 라이브러리의 오브젝트에 대한 공용 권한이 무엇입니까?
- 소유자의 권한을 허용하는 프로그램이 있다면 어느 것입니까?

프로그래머나 어플리케이션 제공자가 어플리케이션에 대해 권한 부여 리스트를 작성했는지 확인하십시오. 작성된 각각의 권한 부여 리스트에 대해 권한 부여 리스트 양식을 준비하거나 프로그래머에게 리스트에 관한 정보를 요청하십시오.

설치 값을 변경해야 하는지를 판별할 수 있습니다.

어플리케이션에 대한 설치 값 변경

어플리케이션 설치 양식의 정보를 라이브러리 설명 양식의 라이브러리에 대한 자원 보안 계획과 비교하십시오. 서로 다르면 어플리케이션을 설치한 후 변경할 사항을 결정해야 합니다.

어플리케이션 소유권 변경

프로그래머나 어플리케이션 제공자가 어플리케이션 라이브러리와 오브젝트를 소유하기 위해 특별한 프로파일을 작성한 경우 명명 규칙과 일치하지 않더라도 그 파일을 사용할 것을 고려하십시오. 오브젝트 소유권을 전송하는 것은 긴 시간이 걸릴 수 있으므로 피해야 합니다.

IBM 제공 그룹 프로파일 중 하나(예: QSECOFR 또는 QPGMR)가 어플리케이션을 소유하면 어플리케이션을 설치한 후 소유권을 다른 프로파일로 전송해야 합니다.

오브젝트 소유권을 변경하지 못하도록 프로그래머가 어플리케이션을 설계하는 경우도 있습니다. 제한 범위내에서 작업을 하고 보안 관리를 위한 사용자 고유의 요구사항을 계속해서 충족시키도록 하십시오. 그러나 IBM 제공 프로파일(예: QSECOFR)이 어플리케이션을 소유하는 경우 사용자 및 프로그래머 또는 어플리케이션 제공자가 소유권을 변경하기 위한 계획을 수립해야 합니다. 어플리케이션을 설치하기 전에 소유권을 변경하는 것이 이상적입니다.

공용 권한 변경

오브젝트를 저장할 때 오브젝트와 함께 공용 권한도 저장하십시오. 시스템에 어플리케이션 라이브러리를 복원할 때 라이브러리와 모든 오브젝트가 저장 당시와 동일한 공용 권한을 갖게 됩니다. 이것은 다른 시스템에 라이브러리를 저장한 경우에도 해당합니다.

라이브러리에 대한 CRTAUT 값(신규 오브젝트에 대한 공용 권한)은 복원된 오브젝트에는 영향을 주지 않습니다. 라이브러리에 대한 CRTAUT에 관계 없이 저장된 공용 권한으로 복원됩니다.

라이브러리 및 오브젝트의 공용 권한을 변경하여 라이브러리 설명 양식의 계획과 일치시켜야 합니다.

어플리케이션 설치를 계획할 때 JKL Toy사의 Sharon Jones가 어플리케이션 설치를 계획한 방법을 보여주는 예를 검토할 수 있습니다.

다음과 같이 하여 어플리케이션 설치를 완벽하게 계획했는지 확인하십시오.

- 초기 어플리케이션 설치 양식을 모두 채우십시오. 그런 다음 다시 돌아가서 추가 어플리케이션마다 양식을 준비하십시오.
- 모든 양식을 작성했는지 확인하십시오. 양식을 복사하여 시스템과 사용권 프로그램을 설치할 때까지 안전한 장소에 보관하십시오.

계획 타스크를 완료했으면 사용자 보안 설정 준비가 된 것입니다.

예: JKL Toy사의 어플리케이션 설치 양식

JKL Toy사는 어플리케이션 제공자로부터 고객 주문 관리 및 미수금 관리 어플리케이션을 구매했습니다. 이 회사에서는 외부 프로그래머를 고용하여 계약 및 가격 관리 어플리케이션을 개발하고 고객 주문 관리 어플리케이션에 링크시켰습니다.

Sharon Jones는 어플리케이션 설치 양식을 준비하기 위해 라이브러리 설명 양식의 정보를 사용했습니다. 아래 표는 CUSTLIB을 위한 Sharon의 라이브러리 설명 양식에 대한 사본을 보여줍니다(″라이브러리 정보 설명″ 주제 참조).

표 57. JKL Toy사의 라이브러리 설명 양식: 예

라이브러리 설명 양식	**파트 2의 1**
작성자: Sharon Jones	날짜: 1999년 9월 9일
라이브러리 이름: CUSTLIB	설명(텍스트): 고객 레코드 라이브러리
간단한 라이브러리 기능 설명: 주문 및 계정을 포함하여 모든 고객 파일을 보유합니다.	
라이브러리에 대한 보안 목적 정의(예: 기밀 정보 여부 판별): 현재로는 회사의 모든 사람들이 고객 주문 정보를 볼 수 있습니다. 정보의 정확성을 보호하기 위해 정보를 변경할 사람들을 제어해야 합니다.	
라이브러리의 공용 권한: *USE 라이브러리내 오브젝트의 공용 권한: *CHANGE 신규 오브젝트의 공용 권한(CRTAUT): *CHANGE 라이브러리 소유자: OWNAR	

아래 표는 Sharon이 고객 주문 관리 어플리케이션을 위해 준비한 어플리케이션 설치 양식을 보여줍니다. Sharon이 어플리케이션 제공자가 작성한 소유자 프로파일을 사용하기로 한 점에 주목하십시오. COWNER 프로파일이 파일 및 프로그램 라이브러리 모두 소유합니다.

어플리케이션을 설치했으면 Sharon이 다음과 같이 해야 합니다.

- 라이브러리 설명 양식에 있는 자원 보안 계획에 일치하도록 라이브러리에 대한 공용 권한을 변경합니다.
- COWNER 프로파일의 사용자 클래스를 *USER로 변경하고 모든 특수 권한을 제거합니다.
- COWNER 프로파일의 암호를 *NONE으로 변경합니다.

표 58. JKL Toy사의 어플리케이션 설치 양식: 예

어플리케이션 이름: 고객 주문 관리(CO)	설명: 주문 입력, 추적, 선적
어플리케이션 설치에 필요한 모든 프로파일 나열 및 설명: 파일이 들어 있는 라이브러리는 COWNER라는 프로파일이 소유합니다. 프로그램 라이브러리는 QPGMR이 소유합니다.	
라이브러리 이름: CUSTLIB	

표 58. JKL Toy사의 어플리케이션 설치 양식: 예 (계속)

	설치 전	설치 후
라이브러리 소유자	COWNER	COWNER
오브젝트 소유자	COWNER	COWNER
라이브러리 공용 권한	*EXCLUDE	*USE
오브젝트 공용 권한	*ALL	*CHANGE
신규 오브젝트를 위한 공용 권한	*CHANGE	*CHANGE
라이브러리 이름: COPGMLIB		
	설치 전	설치 후
라이브러리 소유자	QPGMR	COWNER
오브젝트 소유자	QPGMR	COWNER
라이브러리 공용 권한	*EXCLUDE	*USE
오브젝트 공용 권한	*ALL	*CHANGE
신규 오브젝트를 위한 공용 권한	*CHANGE	*CHANGE

이제 계획 타스크를 완료했으므로 사용자 보안 설정을 시작할 수 있습니다.

제 6 장 사용자 보안 설정

이 주제에서는 명령행 인터페이스를 사용하여 시스템에 사용자 보안을 설정하는 데 필요한 타스크를 설명합니다. 신규 시스템을 설정할 경우 순서대로 이 단계를 완료해야 합니다. 다음 단계로 계속 진행할 때 시스템이 각 단계에서 나온 정보를 사용합니다. 기본 시스템 보안을 설정하기 위해서는 두 가지의 타스크 세트를 완료해야 합니다. 먼저 사용자 보안을 정의하고 두 번째로 시스템의 자원을 보호해야 합니다. 아래에 나오는 두 개의 표는 사용자 보안 및 자원 보안을 설정하기 위해 구성해야 하는 각 단계를 정리한 것입니다.

주: 반드시 사용자 보안을 설정하기 위한 모든 단계를 완료한 후에 자원 보안 설정을 시작해야 합니다.

표 59. 사용자 보안 설정 단계

단계	이 단계에서 수행해야 할 일	사용하는 양식
종합적인 환경 설정	초기 시스템 값과 네트워크 속성을 설정하십시오. 보안 담당자 프로파일을 작성하십시오.	시스템 값 선택 양식
보안을 위한 시스템 값 설정	추가 시스템 값을 설정하십시오.	시스템 값 선택 양식
어플리케이션 로드를 위한 기본 보안 단계 준비	소유자 프로파일을 작성하십시오. 어플리케이션을 로드하십시오. 나머지 단계를 완료하기 전에 어플리케이션 라이브러리와 오브젝트가 시스템에 있어야 합니다.	어플리케이션 설치 양식
사용자 그룹 설정	작업 설명, 그룹 라이브러리, 그룹 프로파일을 작성하십시오.	사용자 그룹 설명 양식
개별 사용자 설정	개별 라이브러리와 사용자 프로파일을 작성하십시오.	개별 사용자 프로파일 양식

표 60. 자원 보안 설정 단계

단계	이 단계에서 수행해야 할 일	사용하는 양식
소유권 및 공용 권한 설정	라이브러리와 오브젝트에 대해 소유권 및 공용 권한을 설정하십시오.	어플리케이션 설치 양식
권한 부여 리스트 작성	권한 부여 리스트를 작성하십시오.	권한 부여 리스트 양식
특정 권한 설정	라이브러리와 개별 오브젝트에 대한 액세스를 설정하십시오.	라이브러리 설명 양식
프린터 출력 보안	출력 대기행렬을 작성하여 프린터 출력을 보호한 후 출력을 할당하십시오.	출력 대기행렬 및 워크스테이션 보안 양식
워크스테이션 보안	워크스테이션을 보호하십시오.	출력 대기행렬 및 워크스테이션 보안 양식

앞의 표에 나오는 주제와 함께 다음 주제를 참조하여 시스템 보안을 관리하십시오.

- 보안 테스트
- 보안 정보 변경

- 보안 정보 저장
- 보안 모니터

시작하기 전에

신규 시스템을 설치할 경우 보안 설정을 시작하기 전에 다음과 같이 하십시오.

- 시스템 장치 및 장치가 설치되어 작동하는지 확인하십시오. 장치에 iSeries 명명 처리를 사용하지 않을 계획이면 장치 이름의 지정 방식(QDEVNAMING)을 결정하는 시스템 값을 변경할 때까지 기다리십시오. 신규 시스템 값 적용을 통해 장치를 접속할 시기를 알 수 있습니다.
- 사용하려는 사용권 프로그램을 로드하십시오.

종합적인 환경 설정

사용자 보안 설정을 시작하려면 사용자에 대한 종합적인 환경을 설정해야 합니다. 설정 메뉴를 사용하여 시스템 값을 설정했으면 고유의 사용자 프로파일을 작성하십시오. DST(전용 서비스 툴) 프로파일에 대해 사용자 ID와 암호도 변경하게 됩니다.

다음 프로시듀어에는 이 단계를 설명하는 명령행 화면에 대한 예가 나옵니다. 그러나 전체 화면을 표시하지는 않습니다. 타스크를 수행하는 데 필요한 정보만 표시합니다.

필요한 양식

"종합적인 보안 전략 계획"에서 준비한 시스템 값 선택 양식의 정보를 입력하십시오.

종합적인 환경을 설정하려면 다음 타스크를 수행해야 합니다.

1. 시스템에 사인 온
2. 올바른 지원 레벨 선택
3. 다른 사용자의 사인 온 방지
4. 보안을 위한 시스템 값 입력
5. 신규 시스템 값 적용
6. 보안 담당자 프로파일 작성

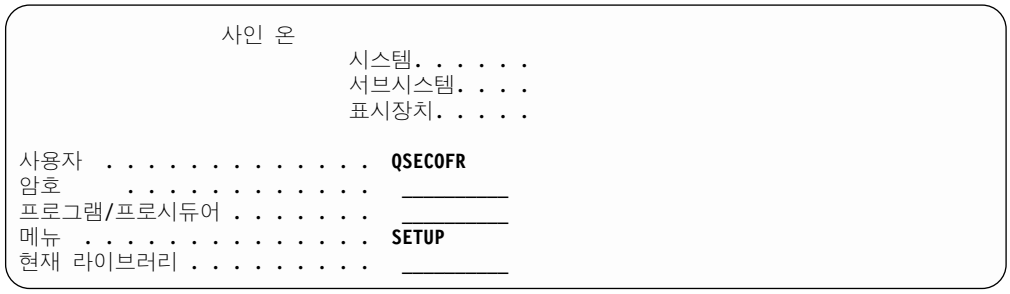
위의 단계를 완료한 후에, 서비스 툴 암호를 변경하여 누군가가 부적절하게 사용하지 못하게 해야 합니다. 세부사항은 서비스 툴을 참조하십시오.

시스템에 사인 온

시스템 환경 설정을 시작하려면 시스템에 사인 온해야 합니다.

1. 콘솔에서 보안 담당자(QSECOFR)로 사인 온하십시오. 처음 사인 온하는 경우, 암호 QSECOFR을 사용하십시오. 암호 만기를 설정한 상태에서 시스템이 제공되므로 암호를 변경하도록 프롬트가 제공됩니다. 사인 온하려면 이 암호를 변경해야 합니다.
2. 사인 온 화면의 *메뉴* 필드에 SETUP을 입력하십시오.

주: 설정 메뉴를 시스템, 사용자 및 장치 사용자 정의 메뉴라고 합니다. 이 텍스트에서는 설정 메뉴라고 합니다.



시스템에 사인 온한 다음 적절한 지원 레벨을 선택해야 합니다.

올바른 지원 레벨 선택

시스템에 사인 온했으면 사용자에게 적절한 지원 레벨을 선택할 수 있습니다. **지원 레벨**이 사용자가 보게 될 표시장치의 버전을 판별합니다. 많은 시스템 표시장치들이 서로 다른 두 개의 다른 버전을 가집니다.

- 기본 지원 레벨 버전은 표시하는 정보가 적고 기술적 용어를 사용하지 않습니다.
- 중간 지원 레벨 버전은 많은 정보를 표시하고 기술적 용어를 사용합니다.

일부 필드나 기능들은 특정 버전의 표시장치에서만 사용할 수 있습니다. 지침을 통해 사용할 버전을 알 수 있습니다. 한 지원 레벨을 다른 지원 레벨로 변경하려면 **F21**(지원 레벨 선택)을 사용하십시오. **F21**을 모든 표시장치에서 사용할 수 있는 것은 아닙니다.

지원 레벨을 선택했으면 보안을 설정하는 동안 시스템에 다른 사용자의 사인 온을 방지해야 합니다.

다른 사용자의 사인 온 방지

적절한 지원 레벨을 선택했으면 다른 사용자가 시스템에 사인 온하지 못하도록 해야 합니다. 시스템을 보안시키기 전에 사람들이 시스템을 손상시키는 문제가 걱정이 되면 사람들이 다른 워크스테이션에서 사인 온하지 못하게 할 수 있습니다. 이것은 선택입니다. 임시 보안이 필요할 경우에만 그렇게 하십시오.

1. 설정 메뉴에서 **F9**를 눌러 명령행을 표시하십시오.
2. 명령행에 GO DEVICESTS를 입력하십시오.

3. 화면에 장치 상태 타스크 메뉴가 표시됩니다. 구성 상태에 대한 작업 메뉴가 나오면 **F21**(지원 레벨 선택)을 사용하여 기본 지원 레벨로 변경하십시오.
4. 옵션 **1**(표시장치에 대한 작업)을 선택하십시오.
5. 표시장치에 대한 작업 화면에서 사용 중인 워크스테이션을 제외한 모든 워크스테이션을 사용 불가능하게 만드십시오. 각 워크스테이션 이름 앞에 **2**를 입력하고 **Enter** 키를 눌러 사용 불가능하게 만드십시오.
6. **F3**(나감)을 두 번 눌러 설정 메뉴로 리턴하십시오.
7. **F12**(취소)를 눌러 명령행을 제거하십시오.

```
                          표시장치에 대한 작업

아래 옵션을 입력하고 Enter 키를 누르십시오.
  1=사용 가능          2=사용 불가능          5=표시
  7=메세지 표시  8=제어기와 행에 대한 작업
  13=설명 변경
Opt  장치         유형     상태
__   DSP01        3196     QSECOFR
2_   DSP02        3196     사용 가능
2_   DSP03        3196     사용 가능
2_   DSP04        3196     사용 가능
```

장치를 사용 불가능하게 만들면 전원이 공급되더라도 장치에 사인 온 화면이 나오지 않습니다. 시스템을 중단시켰다가 재시작할 때까지만 워크스테이션을 사용할 수 없습니다. 이 단계를 반복해야 할 수 있습니다.

다른 사람이 시스템에 사인 온하지 못하게 했으면 보안을 위한 시스템 값을 입력할 수 있습니다.

보안을 위한 시스템 값 입력

다른 사용자의 사인 온 방지를 한 다음 시스템에 시스템 값을 입력해야 합니다.

다음 프로시듀어를 사용하여 시스템 값 선택 양식의 파트 1의 정보를 입력하십시오.

1. 설정 메뉴에서 옵션 **1**(시스템 옵션 변경)을 선택하십시오.
2. 시스템 옵션 변경 화면의 시스템 값 선택 양식의 정보를 입력하십시오. 화면에 선택사항 중 하나를 변경하지 않으려면 Tab 키를 사용하여 건너뛸 수 있습니다.
3. 날짜와 시간이 시스템 시작 시 설정되어 있지 않은 경우, 이 화면에 올바른 날짜와 시간을 입력하십시오.
4. 이 페이지에 정보를 입력했으면 다음 페이지로 이동하십시오. 화면의 우측 하단 모서리에 있는 *계속...*은 화면에 적어도 하나 이상의 페이지가 있음을 의미합니다.

```
                          시스템 옵션 변경
시스템:
아래 선택사항을 입력하고 Enter 키를 누르십시오.

시스템명  . . . . . .  JKLTOY     이름

날짜 및 시간 옵션:
  시스템 날짜 . . . . . .  09/21/99     월/일/연도
  시스템 시간 . . . . . .  10:52:57     시/분/초
  날짜 분리자 . . . . . .  1           1=/
                                       2=-
                                       3=.
                                       4=,
                                       5=공백
  날짜 형식 . . . . . .  MDY           YMD, MDY, DMY, JUL
  시간 분리자 . . . . . .     1        1=:
                                       2=.
                                       3=,
                                       4=공백


                                                    계속...
F1=도움말   F3=나감   F5=화면정리   F12=취소
```

5. 화면의 두 번째 페이지에 선택사항을 입력하고 다음 페이지로 이동하십시오.

```
                          시스템 옵션 변경

아래 선택사항을 입력하고 Enter 키를 누르십시오.

보안 옵션:
  보안 레벨  . . . . . .  40
    :
    :
  보안 담당자에게 모든 표시장치에
    대한 사인 온 허용. . .  N
```

6. 화면의 세 번째 페이지에 선택사항을 입력하고 **Enter** 키를 누르십시오.

```
                          시스템 옵션 변경

아래 선택사항을 입력하고 Enter 키를 누르십시오.

장치 옵션:
  신규 장치에 대한
  명명 형식 . . . . . .  1


  디폴트 시스템 프린터  . . . .  PRT01

추가 옵션:
  사인 온을 할 때, 사용자가 S/36 환경에
    있습니다. . . . . .  N
  프린터 출력에 대해 작업 사용 통계를
    저장합니다. . . . . .  Y
```

7. 다시 설정 메뉴가 나타납니다. 화면 맨 아래에서 **시스템 옵션이 변경되었습니다. IPL required**라는 메세지에 주목하십시오.

주: 단, 보안 레벨을 변경한 경우, 시스템에 IPL이 필요합니다.

대부분의 시스템 타스크 주제 끝에 가능한 오류 및 회복 단계를 설명하는 표가 있습니다. 앞서 설명한 결과와 다를 경우, 도움을 받으려면 이 표를 사용하십시오. 이 표에서 모든 문제를 예측할 수는 없습니다. 표를 제공하는 목적은 문제해결시 지침을 제공하여 보다 편리하게 시스템을 사용하기 위한 것입니다.

가능한 오류	회복
MAIN 메뉴가 표시됩니다.	**F3**(나감) 또는 **F12**(취소)를 눌렀습니다. GO SETUP을 입력하고 재시도하십시오.
클린업 옵션 변경 화면과 같은 다른 화면이 나옵니다.	설정 메뉴에서 잘못된 옵션을 선택했습니다. **F3**(나감)을 눌러 메뉴로 리턴한 후 재시도하십시오.
Enter 키를 누르면 시스템 옵션 변경 화면이 다시 나옵니다.	화면 맨 아래에서 오류 메세지를 찾아보십시오. 허용되지 않는 값을 입력했습니다. 자세한 정보가 필요하면 **F1**(도움말)을 사용하십시오. 시스템이 입력을 시작하기 전의 값으로 모두 복원하려면 **F5**(화면정리)를 사용하십시오. 재시도하십시오.
화면에 모든 선택사항을 입력하기 전에 **Enter** 키를 눌렀습니다.	시스템 값 변경이 필요할 때마다 이 화면을 사용할 수 있습니다. 설정 메뉴에서 옵션 **1**을 선택하고 처음에 누락시켰던 값을 입력하십시오. **주의: 일단 시스템이 작동하면 프로그래머와 상의없이 보안 레벨을 변경하지 마십시오. 또한 iSeries Access를 사용하고 있거나 다른 컴퓨터와 통신하고 있는 경우 시스템명을 변경하지 마십시오.**
뒷장 키를 누르지 않고 **Enter** 키를 눌렀습니다.	다시 설정 메뉴에서 옵션 **1**을 선택하고 뒷장 키를 눌러 두 번째 페이지를 표시하십시오. 선택사항을 입력하고 **Enter** 키를 누르십시오.

시스템 값을 입력했으면 신규 시스템 값을 적용해야 합니다.

신규 시스템 값 적용

시스템 값을 입력했으면 이 값 중 일부를 적용해야 합니다. 시스템 값에 대한 대부분의 변경사항은 즉시 적용됩니다. 그러나 시스템에서 보안 레벨을 변경할 경우에는 시스템을 중단시켰다가 다시 시작할 때까지 적용되지 않습니다. 시스템 옵션 변경 화면에 모든 값을 올바로 입력했는지 확인했으면 새로운 값을 적용할 수 있습니다.

주: 워크스테이션을 시스템에 아직 접속하지 않았으면 지금 접속하십시오. 시스템을 시작할 때 시스템 옵션 변경 화면에서 선택한 명명 형식을 사용하여 시스템이 그 장치들을 자동으로 구성합니다.

시스템을 중단시켰다가 재시작하려면 다음 프로시듀어를 사용하십시오. 시스템이 시작할 때 시스템 옵션 변경 화면에 입력한 값이 적용됩니다.

1. 콘솔에서 사인 온했는지 확인하고 다른 워크스테이션이 사인 온되어 있지는 않은지 확인하십시오.
2. 프로세서 장치의 키잠금 스위치가 정상 위치에 있는지 확인하십시오.
3. 설정 메뉴에서 전원 공급 및 차단 타스크 옵션을 선택하십시오.

4. 즉시 시스템 전원을 차단했다가 다시 공급하는 옵션을 선택하십시오. **Enter** 키를 누르십시오.
5. 시스템이 전원 차단 요구를 확인하도록 요구하는 화면을 표시합니다. **F16**(확인)을 누르십시오.

이렇게 하면 시스템이 중단되었다가 자동으로 재시작합니다. 화면이 몇 분간 공백 상태가 됩니다. 그리고 나서 사인 온 화면을 다시 표시합니다.

신규 시스템 값을 적용했으면 시스템에 자신을 위한 보안 담당자 프로파일을 작성해야 합니다.

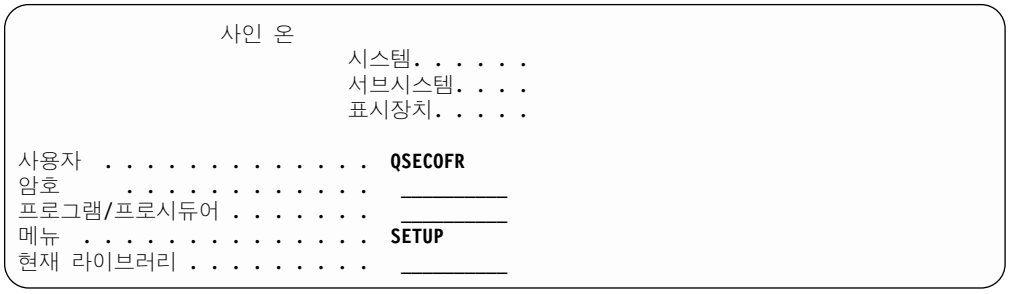
보안 담당자 프로파일 작성

시스템의 **보안 담당자**는 *SECOFR 사용자 클래스 또는 *ALLOBJ 및 *SECADM 특수 권한을 가진 사용자입니다.

시스템 옵션 변경 화면에서 시스템 값 적용을 수행했으면 자신과 대체 보안 담당자용 사용자 프로파일을 작성하십시오. 앞으로는 보안 담당자 기능을 수행할 때 QSECOFR 프로파일이 아닌 사용자 프로파일을 사용하십시오.

1. 시스템에 QSECOFR로 사인 온하여 설정 메뉴를 요구하십시오.

   선택한 시스템명이 사인 온 화면의 우측 상단에 나오는 것에 주의하십시오.



2. 설정 메뉴에서 *사용자 등록에 대한 작업* 옵션을 선택하십시오. 사용자 등록에 대한 작업 화면에 시스템의 현재 프로파일이 나옵니다.

   주: 사용자 프로파일에 대한 작업 화면이 나오면 **F21**(지원 레벨 선택)을 누르고 기본 지원 레벨로 변경하십시오.
3. 신규 프로파일을 작성하려면 *Opt*(옵션) 열에 **1**(추가)을 입력하고 *사용자* 열에 프로파일명을 입력하십시오. **Enter** 키를 누르십시오.

```
                        사용자 등록에 대한 작업

아래 옵션을 입력하고 Enter 키를 누르십시오.
  1=추가   2=변경   3=복사   4=제거   5=표시

Opt     사용자          설명
1       JONESS
QDOC                            문서 사용자 프로파일
QSECOFR                         보안 담당자 사용자 프로파일
```

4. 사용자 추가 화면에서 암호를 할당하십시오.
5. 사용자 자신의 해당 정보로 샘플 화면에 나오는 필드를 채우십시오.
6. 뒷장 키를 눌러 화면의 다음 페이지로 이동하십시오.

```
                           사용자 추가

아래 선택사항을 입력하고 Enter 키를 누르십시오.

사용자. . . . . .  JONESS
사용자 설명 . . . . . .  Jones, Sharon
암호. . . . . .  secret
사용자 유형 . . . . . .  *SECOFR
사용자 그룹 . . . . . .  *NONE

명령행 사용 제한  . . . .  _____
디폴트 라이브러리 . . . .
디폴트 프린터 . . . . . *WRKSTN
프로그램에 사인 온. . . . *NONE
  라이브러리. . . . . .

첫 번째 메뉴 . . . . . .
  라이브러리. . . . . .
```

7. 화면의 두 번째 페이지를 작성하고 **Enter** 키를 누르십시오.
8. 사용자 등록에 대한 작업 화면 맨 아래에 있는 확인 메세지를 검토하십시오.
9. **F3**(나감)을 눌러 설정 메뉴로 리턴하십시오.

```
                           사용자 추가

아래 선택사항을 입력하고 Enter 키를 누르십시오.

어텐션 키 프로그램  . . .  *SYSVAL
  라이브러리. . . . . .
```

가능한 오류	회복
모든 필드에 정보를 입력하기 전에 **Enter** 키를 눌렀습니다.	사용자 등록에 대한 작업 화면에서 *변경* 옵션을 사용하여 방금 작성한 프로파일을 변경하십시오. 프로파일이 리스트에 없으면 **F5**(화면정리)를 누르고 뒷장 키를 눌러 프로파일을 찾으십시오.

사용자 자신을 위한 보안 담당자 프로파일을 작성했으면 서비스 툴 사용자에 대한 사용자 ID와 암호를 변경해야 합니다. Information Center에서 서비스 툴 주제를 참조하십시오.

보안을 위한 시스템 값 설정

이 주제에서 시스템 값을 변경하고 표시하려면 WRKSYSVAL(시스템 값에 대한 작업) 명령을 사용하십시오.

필요한 양식

"종합적인 보안 전략 계획"에서 준비한 시스템 값 선택 양식의 정보를 입력하십시오.

시스템 값을 설정하려면 다음 타스크를 완료하십시오.

1. 보안 시스템 값 변경
2. 개별 시스템 값 변경

명령행 인터페이스에 사인 온

다음 정보를 사용하여 시스템에 사인 온하십시오.

프로파일
사용자 소유(*SECADM 및 *ALLOBJ 권한이 필요합니다.)

메뉴 기본

사인 온했으면 보안 시스템 값 변경을 시작할 수 있습니다.

보안 시스템 값 변경

시스템에 사인 온했으면 다음 프로시듀어를 사용하여 시스템 값 선택 양식의 파트 2에 나오는 보안 시스템 값을 입력하십시오.

1. 명령행에 WRKSYSVAL *SEC를 입력하고 **Enter** 키를 누르십시오. 명령어 다음의 *SEC는 보안과 관련된 시스템 값만 보는 것을 의미합니다.
2. 시스템 값에 대한 작업 화면에서 변경하려는 시스템 값 앞에 있는 옵션 열에 **2**(변경)를 입력하십시오. 변경하려는 시스템 값이 화면에 없으면 찾을 때까지 뒷장 키를 누르십시오.

```
                        시스템 값에 대한 작업

위치          . . . . . .                 시작 문자
유형별 서브세트  . . . .   *SEC           F4=리스트

옵션을 입력하고 Enter 키를 누르십시오.
  2=변경    5=표시

       시스템
옵션   값          유형        설명
       QINACTMSGQ  *SEC        비활동 작업 메세지 대기행렬
2      QLMTDEVSSN  *SEC        장치 세션 제한
       QLMTSECOFR  *SEC        보안 담당자 장치 제한
       QMAXSGNACN  *SEC        실패했을 경우의 조치
  ⋮
```

3. 시스템 값에 대해 선택사항을 입력하고 **Enter** 키를 누르십시오. 시스템 값에 대한 작업 화면이 다시 나옵니다.

```
                          시스템 값 변경

시스템 값    . . . . . :   QLMTDEVSSN
설명 . . . . . . . . . :   장치 세션 제한


선택사항을 입력하고 Enter 키를 누르십시오.

  장치 세션 제한 . . . . . .  0          0=제한 안함
                                         1=제한함
```

4. 화면 맨 아래의 확인 메세지를 검토하십시오.

가능한 오류	회복
시스템 값에 대한 작업 화면의 예에 나온 것과 다른 시스템 값이 표시됩니다.	*SEC를 입력하지 않았습니다. 화면 맨 위의 *유형별 서브세트* 필드를 샘플 화면과 커서를 *유형별 서브세트* 필드로 이동하십시오. *SEC를 입력하고 **Enter** 키를 누르십시오.
시스템이 명령을 처리하지 않았습니다. 계속해서 메뉴가 나옵니다.	화면 맨 아래의 오류 메세지를 확인하십시오. 명령어 이름을 잘못 입력했습니다. 재시도하십시오. 메세지에서 권한이 없음을 나타내면 사인 오프한 다음 보안 담당자 권한을 가진 프로파일을 사용하여 다시 사인 온하십시오.
Enter 키를 누르면 시스템 값 변경 화면이 다시 나옵니다.	화면 맨 아래의 오류 메세지를 확인하십시오. 선택사항을 잘못 입력했거나 허용 범위를 벗어난 값을 입력했습니다. 추가 정보를 보려면 **F1**(도움말)을 사용하십시오.
시스템 값에 대한 작업 화면이 아니라 메뉴가 나옵니다.	**Enter** 키를 두 번 눌렀습니다. WRKSYSVAL *SEC를 입력하십시오.
변경하지 않을 시스템 값을 선택했습니다.	**F12**(취소)를 눌러 시스템 값에 대한 작업 화면으로 리턴하십시오.

*(별표)의 의미

어떤 값에는 앞에 별표(*)가 나오는 것을 볼 수 있습니다. 시스템은 특별한 값들과 기본 단어들을 구별하기 위해 별표(*)를 사용합니다. 예를 들어, 사용자 프로파일에서 암

호를 *NONE으로 지정하면 해당 프로파일을 사용하여 시스템에 사인 온할 수 없다는 것을 의미합니다. 암호를 NONE으로 지정하면 암호로 문자 NONE을 입력해야 합니다.

시스템에 보안을 설정하는 중에는 명령어와 양식에 별표(*)를 사용할 때 주의하십시오.

보안 시스템 값을 변경했으면 개별 시스템 값을 변경할 수 있습니다.

개별 시스템 값 변경

보안 시스템 값을 변경했으면 개별 시스템 값을 변경할 수 있습니다.

예를 들면, QDSCJOBITV(단절 작업 시간종료 간격) 시스템 값은 보안 시스템 값에 포함되지 않습니다. 이 값은 시스템 값에 대한 작업 화면의 *SEC 서브세트에 나오지 않습니다. QDSCJOBITV 시스템 값이나 개별 시스템 값을 변경하려면 다음 프로시듀어를 사용하십시오.

1. WRKSYSVAL QDSCJOBITV를 입력하고 **Enter** 키를 누르십시오.
2. 시스템 값에 대한 작업 화면에서 QDSCJOBITV 앞의 *옵션* 열에 **2**(변경)를 입력하십시오.
3. QDSCJOBITV에 대해 선택사항을 입력하십시오.
4. 확인 메세지를 검토하십시오.

```
                          시스템 값 변경

시스템 값    . . . . . :   QDSCJOBITV
설명         . . . . . :   Disconnected job time-out interval


선택사항을 입력하고 Enter 키를 누르십시오.

  단절된 작업 시간종료 간격  ..... 300
```

보안 값 나열

시스템 값 선택 양식의 정보 모두를 입력했으면 모든 보안 시스템 값 리스트를 인쇄할 수 있습니다. WRKSYSVAL *SEC OUTPUT(*PRINT)을 입력하십시오. 리스트 사본을 시스템 값 선택 양식과 함께 보관하십시오. 보안 시스템 값을 변경할 때마다 리스트를 다시 인쇄하십시오.

시스템 값 선택 양식에서 시스템 값에 대해 모든 선택사항을 입력했으면 어플리케이션 로드를 준비할 수 있습니다.

어플리케이션 로드를 위한 보안 단계 실행

시스템 값 설정을 완료했으면 어플리케이션을 로드할 준비가 된 것입니다. 이 주제에서는 시스템에 어플리케이션 라이브러리를 로드하기 위해 필요한 보안 단계를 다룹니다. 프로파일과 다른 보안 오브젝트를 작성했으면 ″소유권 및 공용 권한 설정″ 그리고 ″자원 보안 설정″에서 어플리케이션에 대한 소유권 및 권한을 설정하는 방법에 관해 알려줍니다.

가능하면 사용자 그룹과 개별 프로파일을 설정하기 전에 시스템에 어플리케이션 라이브러리를 로드하십시오. 작업 설명과 프로파일을 작성할 때 어플리케이션 오브젝트를 참조해야 합니다.

그룹 및 개별 프로파일을 작성하기 전에 어플리케이션을 로드할 수 없으면 다음과 같은 경고 메세지를 수신할 수 있습니다.

- 작업 설명을 작성할 때 시스템이 초기 라이브러리를 찾지 못합니다.
- 프로파일을 작성할 때 시스템이 초기 프로그램이나 메뉴를 찾지 못합니다.

어플리케이션 라이브러리를 로드할 때까지 작업 설명과 프로파일을 성공적으로 테스트할 수 없습니다.

″어플리케이션 설치 계획″에 준비한 어플리케이션 설치 양식을 사용하십시오.

각 어플리케이션을 로드하려면 다음 타스크를 완료하십시오.

1. 소유자 프로파일 작성
2. 어플리케이션 로드

시스템에 사인 온

- 소유자 프로파일 작성

  프로파일

  사용자 소유(*SECADM 권한이 필요합니다.)

  메뉴 기본

- 어플리케이션 라이브러리 로드

  어플리케이션 라이브러리를 로드할 때 소유자가 보안 담당자나 어플리케이션 소유자로 사인 온해야 하는지 어플리케이션 제공자에게 알아보십시오.

사인 온했으면 어플리케이션을 위한 소유자 프로파일 작성이 가능합니다.

소유자 프로파일 작성

시스템에 사인 온한 후 어플리케이션을 로드하기 전에 프로파일을 작성해야 하는지 알아보려면 어플리케이션 설치 계획을 확인하십시오. 프로파일을 작성하려면 다음과 같이 하십시오.

1. CRTUSRPRF(사용자 프로파일 작성)를 입력한 후 **F4**(프롬트)를 누르십시오.
2. 사용자 프로파일 작성 화면에서 프로그래머나 어플리케이션 제공자의 지시에 따라 필드를 채우십시오.
3. 추가 필드를 표시하려면 **F10**(추가 필드)과 뒷장 키를 사용하십시오.

```
CRTUSRPRF(사용자
프로파일 작성)
선택사항을 입력하고 Enter키를 누르십시오.

사용자 프로파일. . . . . >
사용자 암호. . . . . .  *USRPRF
암호 만기 설정. . . . . .  *NO
상태 . . . . . .  *ENABLED
사용자 클래스. . . . . .  *USER
보조 레벨. . . . . .  *SYSVAL
현재 라이브러리 . . . . . .  *CRTDFT
호출할 초기 프로그램 . . . . . .  *NONE
  라이브러리 . . . . . .
초기 메뉴. . . . . .  MAIN
  라이브러리 . . . . . .  *LIBL
기능 제한. . . . . .  *NO
텍스트 '설명'. . . . . .  xxxxxx 소유자
```

4. 메세지를 보려면 화면 맨 아래를 확인하십시오.

주: 그룹 프로파일 작성에 프로파일 작성에 대한 자세한 설명이 나옵니다.

어플리케이션 소유자를 작성했으면 어플리케이션 로드를 시작할 수 있습니다.

어플리케이션 로드

어플리케이션 라이브러리를 로드하기 위한 어플리케이션 제공자의 지침을 따르십시오. "소유권 및 공용 권한 설정"에서 어플리케이션에 소유권과 공용 권한을 설정하는 방법을 알 수 있습니다.

모든 어플리케이션을 로드했으면 사용자 그룹을 설정할 수 있습니다.

사용자 그룹 설정

어플리케이션 로드를 위한 보안 단계 실행을 완료했으며 사용자 그룹을 설정할 수 있습니다. 그룹 라이브러리, 작업 설명, 그룹 프로파일을 작성합니다. 사용자 그룹 중 하나를 이용하여 전체 주제에 걸쳐 작업한 다음 되돌아 가서 나머지 그룹에 대해 각 단계를 반복하십시오. 샘플 화면에 JKL Toy사 판매 및 마케팅 부서와 자재 관리 부서의 사용자 그룹 설명 양식에서 나온 정보가 표시됩니다.

"사용자 그룹 계획"에서 준비한 사용자 그룹 설명 양식을 사용하십시오.

사용자 그룹을 설정하려면 다음 타스크를 완료하십시오.

1. 사용자 그룹용 라이브러리 작성.

2. 작업 설명 작성.
3. 그룹 프로파일 작성.

시스템에 사인 온

프로파일

사용자 소유(*SECADM 권한이 필요합니다.)

메뉴 기본

사인 온했으면 사용자 그룹용 라이브러리 작성이 가능합니다.

사용자 그룹용 라이브러리 작성

시스템에 사인 온했으면 사용자 그룹용 라이브러리를 작성해야 합니다. 조회 프로그램과 같이 그룹에서 작성한 오브젝트에 대해 라이브러리를 공유하려는 경우 그룹 프로파일을 작성하기 전에 라이브러리를 작성하십시오.

1. CRTLIB(라이브러리 작성)를 입력한 후 **F4**(프롬트)를 누르십시오.
2. 화면의 필드를 채우십시오. 라이브러리명이 그룹 프로파일 이름이어야 합니다.
3. **F10**(추가 매개변수)을 누르십시오.
4. 라이브러리와 그 라이브러리에 작성되어 있는 신규 오브젝트에 대한 공용 권한을 채우십시오.
5. **Enter** 키를 누르십시오. 확인 메세지를 검토하십시오.

```
                          라이브러리 작성

선택사항을 입력하고 Enter키를 누르십시오.

라이브러리 . . . . . .  DPTWH
라이브러리 유형. . . . . .  *PROD
텍스트 '설명'. . . . . .  자재 관리 라이브러리

                              추가 매개변수

권한 . . . . . .  *USE
보조 기억장치 풀 ID. . . . . .  1
작성 권한. . . . . .  *CHANGE
오브젝트 감사 작성 . . . . . .  *SYSVAL
```

가능한 오류	회복
라이브러리의 설명을 입력하기 전에 **Enter** 키를 눌렀습니다.	**CHGLIB**를 입력한 후 **F4**(프롬트)를 누르십시오. 프롬트에 라이브러리명을 입력하고 **Enter** 키를 누르십시오. 라이브러리 변경 화면에 설명을 입력하십시오.
라이브러리에 틀린 이름을 지정했습니다.	RNMOBJ(오브젝트 이름 변경) 명령을 사용하십시오.

그룹용 라이브러리를 작성했으면 작업 설명 작성이 가능합니다.

작업 설명 작성

그룹용 라이브러리 작성했으면 각 그룹에 대한 작업 설명을 작성할 수 있습니다.

초기 라이브러리 리스트에 필요한 라이브러리를 시스템에 아직 설치하지 않았으면 작업 설명을 작성할 때 경고 메세지가 나옵니다.

1. **CRTJOBD**(작업 설명 작성)를 입력하고 **F4**(프롬트)를 누르십시오.
2. 다음 필드를 채우십시오.

   작업 설명:

   그룹 프로파일 이름과 같습니다.

   라이브러리명:

   QGPL

   텍스트:

   그룹 설명
3. **F10**(추가 매개변수)를 누르십시오.
4. *초기 라이브러리 리스트* 필드로 화면을 이동하십시오.

```
                        작업 설명 작성

선택사항을 입력하고 Enter키를 누르십시오.

작업 설명. . . . . . . . . . . . .   DPTSM
라이브러리 . . . . . . . . . . . .   QGPL
작업 대기행렬. . . . . . . . . . .   QBATCH
  라이브러리 . . . . . . . . . . .     *LIBL
작업 우선순위(JOBQ에서). . . . . .   5
출력 우선순위(OUTQ에서). . . . . .   5
인쇄 장치. . . . . . . . . . . . .   *USRPRF
출력 대기행렬. . . . . . . . . . .   *USRPRF
  라이브러리 . . . . . . . . . . .
텍스트 '설명'. . . . . . . . . . .   판매 및 마케팅
```

5. *초기 라이브러리 리스트* 필드의 *SYSVAL에 **+**(더하기)를 입력하여 값 리스트를 입력할 것임을 지정하십시오. **Enter** 키를 누르십시오.

```
계정 코드 . . . . . . . . . . . . .   *USRPRF
   :
   :
CL 구문 검사. . . . . . . . . . . .   *NOCHK
초기 라이브러리 리스트  . . . . . .   +
             추가하려면 + 입력
```

6. *초기 라이브러리 리스트* 필드에 사용자 그룹 설명 양식에서 표시(✓)되어 있는 라이브러리명을 입력하십시오.
   - 행마다 하나의 라이브러리명을 입력하십시오.

- QGPL 및 QTEMP를 포함시키십시오. 모든 작업은 임시 오브젝트를 사용할 때 QTEMP 라이브러리를 사용합니다. **모든 초기 라이브러리 리스트에 QTEMP 라이브러리가 반드시 있어야 합니다.** 대부분의 어플리케이션에서는 QGPL 라이브러리도 초기 라이브러리 리스트에 있어야 합니다.
- 라이브러리 리스트에는 현재(디폴트) 라이브러리를 포함시킬 필요가 없습니다. 사인 온할 때 시스템이 그 라이브러리를 자동으로 추가합니다.

7. **Enter** 키를 누르십시오. 메세지를 확인하십시오. (모든 메세지를 보려면 다음 화면으로 이동하십시오).

```
선택사항을 입력하고 Enter키를 누르십시오.

초기 라이브러리 리스트 . . . . .   CUSTLIB
                                    ITEMLIB
                                    COPGMLIB
                                    ICPGMLIB
                                    QGPL
                                    QTEMP
```

가능한 오류	회복
F10 대신 **Enter** 키를 눌렀습니다.	초기 라이브러리 리스트에 올바른 라이브러리를 넣으려면 **CHGJOBD**(작업 설명 변경)를 입력하고 **F4**를 누르십시오.
작업 설명을 작성하려고 시도할 때 오류 메세지를 받습니다.	시스템에 없는 라이브러리를 포함시키려고 하면 가장 일반적인 오류 메세지가 나옵니다. 이 오류 메세지가 경고 메세지입니다. 작업 설명이 초기 라이브러리 리스트 안에 있는 라이브러리를 이용하여 계속해서 작성됩니다. 시스템에 라이브러리가 있을 때까지 작업 설명을 지정하는 프로파일로 사인 온할 수 없습니다. 시스템에 라이브러리가 있으면 이름을 잘못 입력한 것입니다. 라이브러리명을 확인하고 재시도하십시오.

작업 설명을 작성했으면 그룹 프로파일 작성이 가능합니다.

그룹 프로파일 작성

작업 설명 작성을 완료했으면 그룹 프로파일을 작성할 수 있습니다. 그룹 프로파일을 작성하려면 사용자 그룹 설명 양식의 파트 2에서 나온 정보를 사용하십시오.

1. 사용자 프로파일에 대한 작업 명령을 사용하십시오. WRKUSRPRF *ALL을 입력하십시오. 처음에는 화면에 IBM이 제공하는 프로파일이 나옵니다.

   주: 사용자 등록에 대한 작업 화면이 나오면 **F21**을 눌러 중간 지원 레벨로 변경하십시오.

2. 신규 프로파일을 작성하려면 **1**을 *Opt*(옵션)열에 입력하고 프로파일 이름을 *사용자 프로파일* 열에 입력하십시오. **Enter** 키를 누르십시오.

```
                        사용자 프로파일에 대한 작업

옵션을 입력하고 Enter 키를 누르십시오.
  1=작성   2=변경   3=복사   4=삭제   5=표시
  12=소유자의 오브젝트에 대한 작업

     사용자
Opt  프로파일      텍스트
1    DPTSM
     QDOC         사용자 프로파일 문서
     QSECOFR      보안 담당자 프로파일
```

3. 사용자 그룹 설명 양식의 적절한 필드에 정보를 입력하십시오.
4. **탭** 키를 사용하여 디폴트 값을 사용하는 모든 필드를 건너 뛰십시오.
5. **F10**(추가 매개변수를 누르십시오.
6. 다음 화면으로 이동하십시오.

```
                    사용자 프로파일 작성(CRTUSRPRF)

선택사항을 입력하고 Enter키를 누르십시오.

사용자 프로파일. . . . . > DPTSM
사용자 암호. . . . . .   *none
암호 만기 설정 . . . . . .   *NO
상태 . . . . . .   *ENABLED
사용자 클래스. . . . . .   *USER
지원 레벨. . . . . .   *SYSVAL
현재 라이브러리  . . . . . .   *CRTDFT
호출할 초기 프로그램 . . . . . .   cpsetup
  라이브러리 . . . . . .   cppgmlib
초기 메뉴. . . . . .   cpmain
  라이브러리 . . . . . .   cppgmlib
기능 제한. . . . . .   *yes
텍스트 '설명'. . . . . .   판매 및 마케팅
```

7. 화면의 추가 페이지에 있는 사용자 그룹 설명 양식에서 나머지 필드를 채우고 **Enter** 키를 누르십시오.

```
                        사용자 프로파일 작성

                          추가 매개변수

특수 권한. . . . . .   *USRCLS

  :
작업 설명. . . . . .   DPTSM
  라이브러리 . . . . . .   QGPL
```

```
                    사용자 프로파일 작성

그룹 권한. . . . . . . . . . . .   *NONE
  :
인쇄 장치. . . . . . . . . . . .   PRT03
```

8. 메세지를 검토하십시오.

주의

그룹 프로파일은 특별한 유형의 사용자 프로파일입니다. 많은 메세지와 화면들이 그룹 프로파일을 사용자나 사용자 프로파일로 참조합니다. 시스템에 멤버를 추가하거나 그룹 식별 번호(gid)를 할당하면 사용자가 그룹 프로파일을 작성한 것으로 시스템이 인식합니다.

가능한 오류	회복
그룹 프로파일에 모든 값을 입력하기 전에 **Enter** 키를 눌렀습니다.	**F5**(화면정리)를 눌러서 사용자가 작성한 프로파일을 사용자 프로파일에 대한 작업 화면에 추가하십시오. 옵션 **2**(변경)를 사용하여 프로파일을 정정하십시오.
잘못된 이름으로 프로파일을 작성했습니다.	프로파일 이름은 변경할 수 없습니다. 복사 옵션(**3**)을 사용하여 올바른 이름의 신규 프로파일을 작성하십시오. 그런 다음 잘못된 이름의 프로파일을 삭제(옵션 **4**)하십시오.
사용자 그룹 설명 양식의 일부 필드들은 화면에 나오지 않습니다.	중간 지원 레벨을 사용하고 있는지 확인하십시오. 기본 지원 레벨 버전의 사용자 프로파일 작성을 사용자 추가 화면이라고 합니다. 지원 레벨을 변경하려면 **F12**(변경)를 눌러 사용자 등록에 대한 작업 화면으로 리턴하십시오. **F21**을 사용하여 지원 레벨을 변경하십시오. "올바른 지원 레벨 선택"을 참조하십시오.
사용자 프로파일 작성 화면에서 디폴트 정보 중 일부를 실수로 지워졌습니다.	필드를 공백이면 사용자 프로파일을 작성할 때 시스템이 디폴트 값을 사용합니다. 디폴트 값을 보려면 **F5**(화면정리)를 눌러 전체 화면을 복원하십시오. 사용자 정보를 다시 입력하십시오.

결과 나열

DSPAUTUSR(권한이 있는 사용자 표시) 명령을 사용하여 시스템에 모든 프로파일의 이름과 설명을 나열하십시오. DSPAUTUSR OUTPUT(*PRINT)을 입력하십시오. 모든 그룹 프로파일에 암호가 *NONE으로 되어 있는지 확인하십시오.

개별 사용자를 설정하기 전에 다음을 완료하십시오.

- 각 사용자 그룹에 대한 작업 설명을 작성하십시오.
- 선택적으로 각 그룹에 대한 라이브러리를 작성하십시오.
- 각 사용자 그룹에 대한 그룹 프로파일을 작성하십시오.

개별 사용자 설정

사용자 그룹을 설정할 때 그룹 프로파일을 작성하기 위한 단계를 완료했습니다. 이제 그룹의 멤버에 대한 개별 프로파일을 작성하십시오.

한 사용자 그룹의 모든 멤버에 대해 전체 주제에 걸쳐 작업했으면 되돌아가서 기타 그룹에 대해 각 단계를 반복하십시오. 샘플 화면은 JKL Toy사의 판매 및 마케팅 부서와 자재 관리 부서에 대해 Sharon Jones가 준비한 개별 사용자 프로파일 양식의 사용자를 보여줍니다. ″개별 사용자 프로파일 계획″에서 다음 양식의 사본을 찾을 수 있습니다.

″개별 사용자 프로파일 계획″에서 준비한 개별 사용자 프로파일 양식을 사용하십시오.

그룹 멤버에 대해 개별 프로파일을 작성하려면 다음 타스크를 완료하십시오.

1. 개인용 라이브러리 작성(선택적)
2. 그룹 프로파일 복사
3. 암호 만기 설정
4. 추가 사용자 작성(선택적)

   주: 모든 그룹 멤버가 사용자 프로파일을 가질 때까지 개인용 라이브러리 작성 및 추가 사용자 작성을 반복하십시오.
5. 필요하면 사용자 정보를 변경하십시오.
6. 결과 표시

시스템에 사인 온

프로파일

사용자 소유(*SECADM 권한이 필요합니다.)

메뉴 SETUP

개인용 라이브러리 작성

개별 사용자 설정을 시작하려면 조회 프로그램과 같은 오브젝트의 각 매개변수에 대해 개인용 라이브러리를 작성해야 합니다. 개별 사용자 프로파일을 작성하기 전에 개인용 라이브러리를 작성하십시오.

1. **CRTLIB**를 입력하고 **F4**(프롬트)를 누르십시오.
2. 사용자 프로파일과 동일한 이름을 라이브러리에 지정하십시오.
3. **F10**(추가 매개변수)을 누르십시오.
4. 라이브러리와 그 라이브러리에 작성한 신규 오브젝트에 대해 공용 권한을 작성하십시오.
5. **Enter** 키를 누르십시오. 확인 메세지를 검토하십시오.

```
                          라이브러리 작성

선택사항을 입력하고 Enter키를 누르십시오.

라이브러리 . . . . . .  DPTSM
라이브러리 유형. . . . . .  *PROD
텍스트 '설명'. . . . . .  자재 관리 라이브러리

                       추가 매개변수

권한 . . . . . .  *EXCLUDE
보조 기억장치 풀(pool) ID. . . .  1
작성 권한. . . . . .  *CHANGE
작성 오브젝트 감사 . . . . . .  *SYSVAL
```

개인용 라이브러리를 작성했으면 그룹 프로파일을 복사하여 개별 프로파일을 작성할 수 있습니다.

그룹 프로파일 복사

그룹 프로파일에는 두가지 역할이 있습니다.

1. 시스템이 그룹 프로파일을 사용하여 그룹 멤버에 오브젝트 사용 권한이 있는지를 판별합니다.
2. 그룹 프로파일을 패턴으로 사용하여 개별 그룹 멤버를 위한 사용자 프로파일을 작성할 수 있습니다.

사용자 그룹을 설정할 때 그룹 프로파일을 작성했습니다. 이제 그룹 프로파일을 복사하여 개별 프로파일을 작성할 수 있으며 개별 프로파일을 복사하여 그룹에 다른 프로파일을 작성할 수 있습니다.

1. 설정 메뉴에서 사용자 등록에 대한 작업 옵션을 선택하십시오.

   주: 사용자 프로파일에 대한 작업 화면이 나오면 **F21**(지원 레벨 선택)을 사용하여 기본 지원 레벨로 변경하십시오.

2. **3**(복사)을 사용자 그룹 앞에 있는 *Opt* 열에 입력하십시오. 사용자 복사 화면이 나옵니다(복사하려는 사용자 그룹이 화면에 없으면 찾을 때까지 뒷장 키를 누르십시오). 시스템이 사용자 이름 필드를 공백으로 남긴 채 복사한 그룹 프로파일에서 나머지 필드를 채웁니다.

```
                        사용자 등록에 대한 작업

아래 옵션을 입력하고 Enter 키를 누르십시오.
  1=추가   2=변경   3=복사   4=제거   5=표시

Opt     사용자         설명

        DPTSM          판매 및 마케팅 부서
3       DPTWH          자재 관리 부서
```

3. 작성할 사용자 프로파일의 이름과 설명을 입력하십시오.
4. 암호는 공백으로 남겨 놓으십시오. 시스템이 신규 사용자 프로파일 이름과 동일한 암호를 자동으로 작성합니다.
5. *사용자 그룹* 필드에 그룹 프로파일 이름을 입력하십시오.
6. 개별 사용자 프로파일 양식을 확인하여 사용자가 그룹과 다른 값을 갖고 있는지 확인하십시오. 그 값을 입력하십시오.
7. 다음 화면으로 이동하십시오.

```
                        사용자 복사

복사 대상 사용자. . . . :   DPTWH

아래 선택사항을 입력하고 Enter 키를 누르십시오.

사용자. . . . . . . . . .   WILLISR
사용자 설명 . . . . . . .   Willis, Rose
암호. . . . . . . . . . .
사용자 유형 . . . . . . .   *SYSOPR
사용자 그룹  . . . . . . .   DPTWH

제한 명령행 제한   N

디폴트 라이브러리 . . . . .   DPTWH
디폴트 프린터 . . . . .   PRT04
프로그램에 사인 온 . . . . .   *NONE
  라이브러리 . . . . . . . .

첫 메뉴  . . . . . .   ICMAIN
  라이브러리 . . . . . . . .     ICPGMLIB
```

8. 화면의 다음 페이지에서 필요한 변경사항을 작성하고 **Enter** 키를 누르십시오.
9. 사용자 등록에 대한 작업 화면 맨 아래에 있는 확인 메세지를 검토하십시오.

```
                        사용자 복사

복사 대상 사용자. . . . :   DPTWH

아래 선택사항을 입력하고 Enter 키를 누르십시오.

어텐션 키 프로그램. . . .   *SYSVAL
  라이브러리. . . . . . .
```

가능한 오류	회복
사용자 복사 화면 대신에 사용자 프로파일 작성 화면이 나옵니다.	**F12**(취소)를 눌러 사용자 프로파일에 대한 작업 화면으로 리턴하십시오. **F21**을 사용하여 기본 지원 레벨로 변경하십시오. 복사 조작을 다시 시작하십시오.
선택한 사용자 프로파일명이 사용자 프롬트에 맞지 않습니다.	사용자 프로파일명에 10자까지 사용할 수 있으나 사용자 복사와 사용자 추가 화면이 8자 이상을 지원하지 않습니다. 더 짧은 사용자 이름을 선택하거나 중간 지원 레벨를 사용하여 개별 사용자 프로파일을 작성하십시오.

사용자 프로파일 테스트

그룹에 첫 번째 개별 프로파일을 작성할 때 그 프로파일로 사인 온하여 테스트해야 합니다. 처음에 첫 메뉴로 올바른 메뉴가 나오는지 그리고 사인 온 프로그램이 실행되는지 확인하십시오.

그 프로파일로 사인 온할 수 없으면 시스템이 프로파일에 지정된 항목을 찾지 못할 수 있습니다. 그 항목이 사인 온 프로그램, 작업 설명 또는 초기 라이브러리 리스트에 있는 라이브러리 중 하나일 수 있습니다. 프린터 출력에 대한 작업 화면을 사용하여 사인 온시 작성된 작업 기록부를 찾으십시오. 작업 기록부를 통해 발생한 오류를 알 수 있습니다.

보안 사항을 변경할 때의 테스트와 문제점 진단에 관한 정보는 "보안 테스트"를 참조하십시오.

사용자 프로파일을 테스트했으면 암호 만기 설정을 수행할 수 있습니다.

암호 만기 설정

사용자가 처음에 사인 온할 때 암호를 변경하도록 개별 프로파일을 설정하십시오. 기본 지원 레벨 버전의 사용자 복사 화면에는 *암호 만기 설정* 필드가 나오지 않습니다. 복사 기능으로 사용자 프로파일을 작성했으면 사용자 프로파일을 각각 변경하십시오. *암호 만기 설정* 필드를 변경하려면 CHGUSRPRF *profile-name* PWDEXP(*YES)를 입력하십시오.

주: 사용자 프로파일을 사인 온하여 테스트하려면 암호 만기를 설정하기 *전에* 테스트하십시오.

가능한 오류	회복
프로파일을 테스트했으므로 암호를 변경하여야 합니다.	**CHGUSRPRF** *profile-name*을 입력하고 **F4**(프롬트)를 누르십시오. 사용자 프로파일명에 다시 암호를 설정하십시오(사용자 프로파일명을 암호 필드에 입력하십시오). ***YES**를 *암호 만기 설정* 필드에 입력하십시오. 이 작업에는 중간 지원 레벨이 필요합니다.

첫 번째 개별 사용자 프로파일을 작성했으면 추가 사용자 작성이 가능합니다.

추가 사용자 작성

첫 번째 개별 프로파일을 작성하기 위한 그룹 프로파일 복사를 완료했으면 추가 사용자를 작성할 수 있습니다. 첫 번째 개별 사용자 프로파일을 복사하여 그룹에 추가 멤버를 작성하십시오. 복사 방법으로 개별 프로파일을 작성할 경우 각 개별 프로파일을 주의깊게 살펴보십시오. 개별 사용자 프로파일 양식을 확인하여 신규 사용자 프로파일별로 고유한 필드를 확실히 변경했는지 확인하십시오.

1. 사용자 등록에 대한 작업 화면에서 복사하려는 프로파일 앞에 **3**(복사)을 입력하십시오.

2. 사용자 복사 화면에서 프로파일 이름과 설명을 입력하십시오.
3. 신규 사용자별로 해당 필드에 정보를 입력하십시오.

```
                    사용자 등록에 대한 작업

아래 옵션을 입력하고 Enter 키를 누르십시오.
  1=추가   2=변경   3=복사   4=제거   5=표시

Opt     사용자         설명

     DPTSM       판매 및 마케팅 부서
        DPTWH          자재 관리 부서
3       WILLISR        Willis, Rose
```

가능한 오류	회복
복사하려는 프로파일이 사용자 등록 작업에 대한 작업 화면에 나오지 않습니다.	**F5**(화면정리)를 누르십시오. 앞장 및 뒷장으로 이동하십시오. 리스트는 프로파일 이름별 알파벳순입니다.

사용자에 대한 정보를 변경하려면 사용자에 대한 정보 변경을 참조하십시오.

사용자에 대한 정보 변경

일부 사용자에 대해서는 사용자 복사 화면에 나오지 않은 값을 설정해야 할 경우가 있습니다. 예를 들어, 사용자가 두 개 이상의 그룹 프로파일에 속할 수 있습니다. 이 경우 복사 방법을 사용하여 사용자 프로파일을 작성한 후 변경할 수 있습니다.

1. 사용자 등록에 대한 작업 화면에서 **F21**을 눌러 중간 지원 레벨로 변경하십시오.
2. 사용자 프로파일에 대한 작업 화면에서 변경하려는 프로파일 다음의 *Opt*(옵션) 열에 **2**(변경)를 입력하십시오. **Enter** 키를 누르십시오.

```
                  사용자 프로파일에 대한 작업

옵션을 입력하고 Enter 키를 누르십시오.
  1=작성   2=변경   3=복사   4=삭제   5=표시
  12=소유자별 오브젝트에 대한 작업

     사용자
Opt  프로파일    텍스트
2    AMESJ       Ames, Janice
     DPTSM       판매 및 마케팅 부서
     QDOC        사용자 프로파일 문서
     QSECOFR     보안 담당자 프로파일
     WAGNERR     Wagner, Ray
     WILLISR     Willis, Rose
```

3. 사용자 프로파일 변경 화면에서 **F10**(추가 매개변수)을 누르십시오.
4. 변경하려는 필드를 찾을 때까지 다음 페이지로 이동하십시오. 예를 들어, 사용자를 추가 그룹 프로파일의 멤버로 만들 경우 *추가 그룹* 필드를 찾을 때까지 다음 페이지로 이동하십시오.

5. 원하는 값을 입력하고 **Enter** 키를 누르십시오. 확인 메세지가 나오고 사용자 프로파일에 대한 작업 화면이 다시 표시됩니다.

```
                사용자 프로파일 변경(CHGUSRPRF)

선택사항을 입력하고 Enter키를 누르십시오.

최대 허용 기억장치 . . . . . .   *NOMAX
스케줄링의 최우선 순위 . . . . .  3
작업 설명. . . . . . . . . . . .  DPTWH
  라이브러리 . . . . . . . . . .    QGPL
그룹 프로파일  . . . . . . . . .  DPTWH
소유자 . . . . . . . . . . . . .  *GRPPRF
그룹 권한. . . . . . . . . . . .  *USEE
그룹 권한 유형 . . . . . . . . .  *PGP
보충 그룹. . . . . . . . . . . .  DPTIC
             추가하려면 + 입력
```

일단 사용자 정보를 변경했으면 결과를 표시하여 프로파일을 확인할 수 있습니다.

사용자 프로파일 표시

작성한 프로파일을 표시할 수 있는 방법에는 여러 가지가 있습니다.

하나의 프로파일 표시

사용자 등록에 대한 작업 화면이나 사용자 프로파일에 대한 작업 화면에서 **5**(표시)를 사용하십시오.

하나의 프로파일 나열

사용자 프로파일 표시 명령 DSPUSRPRF *profile-name* DETAIL(*BASIC) OUTPUT(*PRINT)을 사용하십시오.

그룹 멤버 표시

DSPUSRPRF *group-profile-name* *GRPMBR을 입력하십시오. OUTPUT(*PRINT)를 사용하여 리스트를 인쇄할 수 있습니다.

모든 프로파일 나열

그룹별로 정렬시킨 모든 프로파일의 이름과 설명을 나열하려면 권한이 있는 사용자 표시 명령 DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT)을 사용하십시오.

소유권과 공용 권한 설정에 앞서 다음 타스크를 수행하십시오.

- 모든 개별 사용자 프로파일을 작성하십시오.
- 각 프로파일에 대해 암호 만기를 설정하십시오.
- 그룹별로 정렬시킨 모든 프로파일 리스트를 인쇄하여 사용자 그룹 설명 양식과 함께 보관하십시오. 신규 사용자들을 추가할 때 리스트를 다시 인쇄하십시오.

제 7 장 자원 보안 설정

이 주제에서는 오브젝트에 대한 소유권과 공용 권한 그리고 어플리케이션에 대한 특정 권한을 설정합니다. 워크스테이션과 프린터에 대한 자원 보안도 설정합니다. 하나의 라이브러리에 대해 전체 주제에 걸쳐 작업했으면 되돌아 가서 어플리케이션에 사용되는 모든 추가 라이브러리에 대해 각 단계를 반복하십시오. 하나의 어플리케이션에 대해 자원 보안을 설정했으면 다른 어플리케이션에 대해 각 단계를 반복하십시오.

시스템에 신규 어플리케이션을 설치하거나 기존 어플리케이션에 대해 자원 보안을 설정할 때 여기에 나오는 프로시듀어를 사용하십시오.

이 주제에 나오는 샘플 화면은 권한 부여 리스트 양식, 라이브러리 설명 양식, JKL Toy 사의 출력 대기행렬과 워크스테이션 보안 양식을 보여줍니다. "소유권 및 공용 권한 설정"에서 이 샘플 양식의 예를 볼 수 있습니다.

필요한 양식

- "어플리케이션 설치 계획"에서 준비한 어플리케이션 설치 양식
- "그룹 오브젝트"에서 준비한 권한 부여 리스트 양식
- "라이브러리와 오브젝트의 소유권 판별"에서 준비한 라이브러리 설명 양식
- "프린터 출력 보호" 및 "워크스테이션 보호"에서 준비한 출력 대기행렬과 워크스테이션 보안 양식
- "종합적인 보안 전략 계획"에서 준비한 시스템 책임 양식

여러 가지 방법으로 자원 보안을 설정할 수 있습니다. 이 주제에 나오는 각 단계별 순서는 어플리케이션 설치 양식, 권한 부여 리스트 양식, 라이브러리 설명 양식에 나오는 정보의 순서와 일치합니다.

1. 소유권 및 공용 권한 설정
2. 권한 부여 리스트 작성
3. 권한 부여 리스트로 오브젝트 보안
4. 권한 부여 리스트에 사용자 추가
5. 특정 권한 설정
6. 프린터 출력 보안
7. 워크스테이션 보안
8. 시스템 오퍼레이터 메세지 대기행렬에 액세스 제한

소유권 및 공용 권한 설정

이 주제에서는 어플리케이션 라이브러리, 그룹 라이브러리, 개인용 라이브러리에 대한 소유권 및 공용 권한을 설정합니다. 하나의 어플리케이션에 대해 전체 주제에 걸쳐 작업했으면 되돌아 가서 나머지 어플리게이션에 대해 각 단계를 반복하십시오. 샘플 화면에는 Sharon Jones가 ″어플리케이션 설치 계획″에서 고객 주문 관리 어플리케이션에 대해 준비한 어플리케이션 설치 양식이 나옵니다.

시스템에 신규 어플리케이션을 설치하거나 기존 어플리케이션에 보안을 설정할 때 이 주제에 나오는 프로시듀어를 사용하십시오.

″어플리케이션 설치 계획″에서 준비한 어플리케이션 설치 양식을 사용하십시오.

소유권과 공용 권한을 설정하려면 다음 타스크를 수행하십시오.

1. 소유자 프로파일 작성
2. 라이브러리 소유권 변경
3. 어플리케이션 오브젝트에 대한 소유권 설정
4. 라이브러리에 공용 액세스 설정
5. 라이브러리의 모든 오브젝트에 공용 권한 설정
6. 신규 오브젝트에 대한 공용 권한 설정
7. 그룹 및 개인용 라이브러리에 대해 작업

시스템에 사인 온

프로파일

사용자 소유(*ALLOBJ 권한이 필요합니다.)

메뉴 기본

소유자 프로파일 작성

소유자 프로파일이 아직 없으면 다음과 같이 하십시오.

- CRTUSRPRF(사용자 프로파일 작성) 명령을 사용하여 소유자 프로파일을 작성하십시오. 암호를 *NONE으로 설정하십시오.

소유자 프로파일이 이미 있으면 다음과 같이 하십시오.

- CHGUSRPRF(사용자 프로파일 변경) 명령을 사용하여 암호를 *NONE으로 설정하십시오.

소유자 프로파일을 작성했으면 라이브러리 소유권 변경이 가능합니다.

라이브러리 소유권 변경

다음 단계는 라이브러리에 있는 오브젝트는 변경하지 않고 라이브러리의 소유권을 변경합니다.

주의: 어플리케이션 오브젝트에 대한 소유권을 변경하기 전에 어플리케이션 제공자에게 확인을 받으십시오. 일부 어플리케이션들은 특정 오브젝트 소유권에 의존하는 기능을 사용합니다.

1. CHGOBJOWN(오브젝트 소유자 변경)을 입력하고 **F4**(프롬트)를 누르십시오.
2. 라이브러리명, 오브젝트 유형(*LIB), 신규 소유자를 작성하십시오.
3. 확인 메세지를 검토하십시오.

```
                    오브젝트 소유자 변경(CHGOBJOWN)

선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . > COPGMLIB
  라이브러리 . . . . . >   *LIBL       이름,
오브젝트 유형  . . . . . > *LIB
신규 소유자  . . . . . .   COWNER
현재 소유자 권한 . . . . . .   *REVOKE
```

가능한 오류	회복
오류 메세지가 나옵니다.	가장 일반적인 메세지는 라이브러리나 신규 소유자 프로파일을 찾을 수 없다는 것입니다. 입력 오류를 확인하고 재시도 하십시오.

라이브러리 소유권을 변경했으면 어플리케이션 오브젝트에 대한 소유권 설정이 가능합니다.

어플리케이션 오브젝트에 대한 소유권 설정

어플리케이션 오브젝트에 대한 소유권 변경은 각 오브젝트를 개별적으로 변경해야 하는 번거로운 타스크입니다. 가능하면 프로그래머나 어플리케이션 제공자에게 소유권 설정을 요청하십시오.

라이브러리의 오브젝트 나열

소유권을 변경하기 전에 라이브러리 표시 명령을 사용하여 라이브러리 안의 모든 오브젝트 리스트를 인쇄하십시오. 오브젝트 리스트를 체크 리스트로 사용할 수 있습니다. DSPLIB *library-name* *PRINT를 입력하십시오.

최적의 방법 선택

어플리케이션 라이브러리에서 오브젝트에 대한 소유권을 변경하려면 다음 두 방법 중 하나를 선택하십시오.

표 61. 오브젝트 소유권 변경 방법

방법	용도	사용 시기
소유자별 오브젝트에 대한 작업 명령	프로파일이 소유하고 있는 모든 오브젝트가 나오는 화면을 보여줍니다. 오브젝트의 소유권을 변경할 화면에서 옵션을 사용하십시오.	이 방법이 사용하기에 더 쉽습니다. 그러나 QPGMR이나 QSECOFR이 오브젝트를 소유하는 경우 IBM에서는 이 방법을 권장하지 않습니다. QPGMR이나 QSECOFR과 같은 프로파일은 많은 오브젝트를 소유하고 있으므로 나열시킨 화면이 매우 커집니다.
오브젝트 소유권 변경 명령	각 오브젝트에 대해 별도의 명령을 사용해야 합니다. 그러나 *검색*(**F9**)을 눌러 이전 명령을 반복할 수 있고 필요한 입력양을 줄일 수 있습니다.	QPGMR나 QSECOFR이 오브젝트를 소유하면 이 방법이 더 빠릅니다.

소유자별 오브젝트에 대한 작업(WRKOBJOWN) 명령 사용

QPGMR이나 QSECOFR과 같은 IBM 제공 프로파일이 오브젝트를 소유하지 않으면 이 방법을 사용하여 라이브러리에 있는 오브젝트의 소유권을 변경하십시오.

1. WRKOBJOWN *owner-profile-name*을 입력하십시오. 화면에 사용자 프로파일이 소유하는 모든 오브젝트 리스트가 표시됩니다.
2. 작업 중인 라이브러리의 각 오브젝트 앞에 **9**(소유자 변경)를 입력하십시오.
3. 화면 맨 아래의 *매개변수 또는 명령행*에서 NEWOWN(*owner-profile-name*)을 입력하고 **Enter** 키를 누르십시오.
4. 맨 아래에 입력하여 지정한 각 오브젝트 소유자를 시스템이 신규 소유자로 변경합니다. 화면 맨 아래에 확인 메세지가 나옵니다. 프로파일이 오브젝트를 더 이상 소유하지 않기 때문에 화면에는 오브젝트가 더 이상 나오지 않습니다.
5. 라이브러리에서 모든 오브젝트에 대한 소유권을 변경할 때까지 2단계와 4단계를 반복하십시오.

```
                    소유자별 오브젝트에 대한 작업

사용자 프로파일  . . . . . :   OLDOWNER

옵션을 입력하고 Enter 키를 누르십시오.
  2=권한 편집       4=삭제   5=작성자 표시
  8=설명 표시   9=소유자 변경

Opt  오브젝트      라이브러리    유형      속성
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


   ⋮

매개변수 또는 명령
===> NEWOWN(COWNER)
F3=나감    F4=프롬트    F5=화면정리    F9=검색
F18=맨 아래
```

가능한 오류	회복
오브젝트 소유자 변경 화면이 나옵니다.	**9**(소유자 변경) 옵션을 지정하고 소유자별 오브젝트에 대한 작업 화면의 맨 아래에 매개변수를 입력하지 않을 경우에 이 화면이 나옵니다. 매개변수를 잘못 입력할 경우에도 이 화면이 나옵니다. **F12**(취소)를 눌러 소유자별 오브젝트에 대한 작업 화면으로 리턴하십시오. 재시도하십시오. 예에 나오는 것처럼 매개변수를 입력하십시오.

오브젝트 소유자 변경 명령을 사용하여 QPGMR이나 QSECOFR이 소유하는 오브젝트의 소유권을 변경할 수 있습니다.

오브젝트 소유자 변경 명령 사용

QPGMR이나 QSECOFR이 오브젝트를 소유하면 라이브러리안의 오브젝트 소유자를 다음과 같이 하여 변경하십시오.

1. CHGOBJOWN을 입력하고 **F4**(프롬트)를 누르십시오.
2. 리스트에 있는 첫 번째 오브젝트에 대한 화면에 정보를 입력하고 **Enter** 키를 누르십시오.

```
                  오브젝트 소유자 변경(CHGOBJOWN)

선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . > CUSTMAS
  라이브러리 . . . . . >   CUSTLIB
오브젝트 유형  . . . . . > *FILE
신규 소유자  . . . . . .   COWNER
현재 소유자 권한 . . . . . .   *REVOKE
```

3. 오브젝트 소유권 변경을 확인하는 메세지가 나옵니다. 리스트에서 그 항목을 확인하십시오.

4. **F9**(검색)를 누르고 입력한 명령을 검색하십시오.
5. **F4**(프롬트)를 누르십시오. 오브젝트 소유자 변경 화면에서 라이브러리의 다음 오브젝트에 대해 정보를 입력하고 **Enter** 키를 누르십시오.
6. 라이브러리에 있는 각 오브젝트에 대해 4단계와 5단계를 반복하십시오.

작업 확인

라이브러리에 있는 모든 오브젝트의 소유권을 변경했는지 확인하려면 소유자별 오브젝트에 대한 작업 명령을 사용하십시오. WRKOBJOWN *new-owner-profile*을 입력하십시오. 라이브러리에 있는 오브젝트의 리스트와 그 화면을 비교하십시오.

라이브러리에 있는 오브젝트의 소유권을 변경했으면 라이브러리에 공용 액세스 설정이 가능합니다.

라이브러리에 공용 액세스 설정

어플리케이션 오브젝트에 대한 소유권 설정을 완료했으면 오브젝트 권한 편집 (EDTOBJAUT) 명령을 사용하여 라이브러리에 대한 공용 권한을 변경할 수 있습니다.

1. EDTOBJAUT *library-name* *LIB를 입력하십시오.
2. 커서를 **PUBLIC*을 표시하는 행으로 이동시키십시오.
3. 라이브러리에 대해 공용 권한을 입력하고 **Enter** 키를 누르십시오.

```
                          오브젝트 권한 편집

오브젝트 . . . . . :   CUSTLIB        소유자 . . . . . :   COWNER
  라이브러리 . . . . :     QSYS        1차 그룹 . . . . . :   *NONE
오브젝트 유형. . . . :   *LIB

현재 권한에 대한 변경사항을 입력하고 Enter 키를 누르십시오.

  권한 부여 리스트로 보안된 오브젝트 . . . . . .   *NONE

                      오브젝트
사용자      그룹        권한
COWNER                *ALL
*PUBLIC               *CHANGE
```

4. 화면에 신규 권한이 나옵니다.

이제 라이브러리내의 모든 오브젝트에 대한 공용 권한 설정이 가능합니다.

라이브러리내의 모든 오브젝트에 대해 공용 권한 설정

오브젝트 권한 취소(RVKOBJAUT) 명령을 사용하여 라이브러리내의 오브젝트에 대한 현재 공용 권한을 제거하십시오. 오브젝트 권한 부여(GRTOBJAUT) 명령을 사용하여 라이브러리내의 모든 오브젝트에 대해 공용 권한을 설정하십시오.

1. RVKOBJAUT를 입력하고 **F4**(프롬트)를 누르십시오.

2. 대체시킨 어플리케이션 라이브러리명이 나오는 화면을 채우고 **Enter** 키를 누르십시오.

```
                    오브젝트 권한 취소(RVKOBJAUT)

선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . .  *all
  라이브러리 . . . . . .    custlib
오브젝트 유형. . . . . .  *all
사용자 . . . . . .  *public
             추가하려면 + 입력
권한 . . . . . .  *all
```

주: 라이브러리에 많은 수의 오브젝트가 있으면 시스템이 사용자의 요구를 처리하는 데 2-3분 정도 걸릴 수 있습니다.

3. GRTOBJAUT를 입력하고 **F4**(프롬트)를 누르십시오.
4. 사용자가 원하는 어플이케이션 라이브러리명과 권한 이름으로 대체시킨 화면을 채우고 **Enter** 키를 누르십시오.

```
                  오브젝트 권한 부여(GRTOBJAUT)
선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . .  *all
  라이브러리 . . . . . .    custlib
오브젝트 유형. . . . . .  *all
사용자 . . . . . .  *public
             추가하려면 + 입력
권한 . . . . . .  *use
```

주: 라이브러리에 많은 수의 오브젝트가 있으면 시스템이 요구를 프로세스하는 데 2-3분 정도 걸릴 수 있습니다.

라이브러리내의 모든 오브젝트에 대해 공용 권한을 설정했으면 이제 작업 기록부를 사용하여 작업을 확인할 수 있습니다.

작업 기록부를 사용하여 작업 확인

GRTOBJAUT 명령을 사용하여 권한에 대해 여러 가지를 변경할 경우 작업 기록부를 보고 변경사항을 확인하십시오.

1. DSPJOBLOG(작업 기록부 표시)를 입력하십시오.
2. **F10**(상세 메세지 표시)을 누르십시오.
3. 라이브러리에 있는 각 오브젝트의 변경에 관한 메세지가 나옵니다. 메세지를 검토하면서 리스트에서 오브젝트를 확인하십시오.

```
                              모든 메세지 표시
   시스템:   RCHASxxx
작업. . :   QPADEV0010    사용자. . :   JCHEIDEL      번호 . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  CUSTLIB 오브젝트 유형 *FILE의 CUSTMAS 오브젝트에 대해 *PUBLIC 사용자에게
    부여한 권한.
  CUSTLIB 오브젝트 유형 *MSGQ의 CUSTMSGQ 오브젝트에 대해 *PUBLIC 사용자에게
    부여한 권한.
  두 개 오브젝트에 부여한 권한. 0 개 오브젝트에 권한 부여. 0 개 오브젝트에
    부분적으로 권한 부여.
  오브젝트 권한 부여.
7>> dspjoblog
```

가능한 오류	회복
라이브러리의 일부 오브젝트에 대해서는 권한이 변경되지 않았음을 작업 기록부가 나타냅니다.	도움말(**F1**)을 사용하여 메세지에 대한 자세한 정보를 구하십시오. 그와 같은 오브젝트에 대해서는 EDTOBJAUT를 사용하여 권한을 설정하십시오.

이제 신규 오브젝트에 대한 공용 권한 설정이 가능합니다.

신규 오브젝트에 대한 공용 권한 설정

라이브러리 설명에는 작성 권한(CRTAUT)이라는 매개변수가 있으며 이 매개변수가 라이브러리에 작성된 신규 오브젝트의 공용 권한을 판별합니다. 오브젝트를 작성하는 명령은 디폴트 값으로 오브젝트 라이브러리의 CRTAUT 권한을 사용합니다. 라이브러리에 있는 기존의 대다수 오브젝트에 대한 공용 권한과 동일하게 라이브러리에 대한 CRTAUT 권한을 부여해야 합니다.

1. CHGLIB *library-name*을 입력하고 **F4**(프롬트)를 누르십시오.
2. **F10**(추가 매개변수)을 누르십시오.
3. *작성 권한* 필드에 선택 사항을 입력하십시오.

```
                    라이브러리 변경(CHGLIB)

선택사항을 입력하고 Enter키를 누르십시오.

라이브러리 . . . . . > CUSTLIB
라이브러리 유형. . . . . .   *PROD
텍스트 '설명'. . . . . .   '고객 레코드'


                          추가 매개변수

작성 권한. . . . . .   *CHANGE
작성 오브젝트 감사 . . . . . .   *SYSVAL
```

CRTAUT를 *SYSVAL에 설정하면 라이브러리에 신규 오브젝트를 작성할 때 시스템이 QCRTAUT 시스템 값에 대해 현재 설정값을 사용합니다. 각 라이브러리별로 CRTAUT 권한을 설정하면 향후 QCRTAUT 시스템 값의 변경에 대해 보호를 받습니다.

이제 그룹 및 개인용 라이브러리에 대한 작업이 가능합니다.

그룹 및 개인용 라이브러리에 대한 작업

프로파일이 사용자 그룹 및 개별 사용자를 설정할 때 작성한 그룹 및 개인용 라이브러리를 소유합니다.

위에서 설명한 프로시듀어를 사용하여 그룹 라이브러리에 대한 소유권을 그룹 프로 파일로 변경하고 개인용 라이브러리에 대한 소유권을 개별 사용자 프로파일로 변경하십시오. EDTOBJAUT 명령을 사용하십시오.

각 그룹 및 개인용 라이브러리에 대해 작성 권한 매개변수를 설정하여 라이브러리내의 신규 오브젝트에 대한 공용 권한을 판별하십시오. CHGLIB 명령을 사용하십시오.

권한 부여 리스트 작성을 시작하기 전에 다음 타스크를 완료하십시오.

- 어플리케이션 설치 양식 및 라이브러리 설명 양식을 사용하여 모든 어플리케이션 라이브러리에 대한 소유권 및 공용 권한을 설정했는지 확인하십시오.
- 작성한 모든 그룹 및 개인용 라이브러리에 대한 소유권 및 작성 권한을 설정하십시오.

  주: DSPOBJD *ALL *LIB *PRINT를 입력하여 시스템의 모든 라이브러리 목록을 볼 수 있습니다.

권한 부여 리스트 작성

소유권 및 공용 권한 설정을 완료했으면 권한 부여 리스트를 설정할 준비가 된 것입니다. 권한 부여 리스트 양식의 정보를 사용하여 라이브러리 보안에 필요한 모든 권한 부여 리스트를 작성하십시오. 권한 부여 리스트 작성(CRTAUTL) 명령을 사용하십시오.

1. CRTAUTL을 입력하고 **F4**(프롬트)를 누르십시오.
2. 권한 부여 리스트 양식에서 나온 정보로 채우십시오.
3. **F10**(추가 매개변수를 누르십시오.
4. 권한 매개변수를 사용하여 리스트로 보안시킨 오브젝트에 대해 공용권한을 지정하십시오.
5. 확인 메세지를 검토하십시오.

```
                    권한 부여 리스트 작성(CRTAUTL)

선택사항을 입력하고 Enter키를 누르십시오.

권한 부여 리스트. . . . . .   custlst1
텍스트 '설명'. . . . . .   지워진 파일

                         추가 매개변수

권한 . . . . . .   *ALL
```

가능한 오류	회복
리스트 이름을 잘못 입력했습니다.	일단 시스템이 리스트의 이름을 작성하면 그 이름을 변경할 수 없습니다. 리스트를 삭제(DLTAUTL)하고 재시도하십시오.
리스트에 공용 권한을 지정하지 않았습니다	EDTAUTL(권한 부여 리스트 편집) 명령을 사용하십시오.

이제 권한 부여 리스트로 오브젝트 보안이 가능합니다.

권한 부여 리스트로 오브젝트 보안

권한 부여 리스트를 작성했으면 EDTOBJAUT(오브젝트 권한 편집) 명령을 사용하여 권한 부여 리스트 양식에 나오는 항목을 보안하십시오.

1. EDTOBJAUT를 입력하고 **F4**(프롬트)를 누르십시오.
2. 프롬트 화면을 채우고 **Enter** 키를 누르십시오.
3. 오브젝트 권한 편집 화면에서 권한 부여 리스트 이름을 입력하십시오.
4. 오브젝트에 대한 공용 권한이 권한 부여 리스트에서 나오면 공용 권한을 *AUTL로 변경하십시오.
5. 권한 부여 리스트 양식의 각 오브젝트에 대해 위에 나오는 단계를 반복하십시오.

```
                        오브젝트 권한 편집

오브젝트 . . . . . :   ARFILE01       소유자 . . . . . :   OWNAR
  라이브러리 . . . . :     CUSTLIB     1차 그룹 . . . . . :   *NONE
오브젝트 유형. . . . :   *FILE

현재 권한에 대한 변경사항을 입력하고 Enter 키를 누르십시오.

  권한 부여 리스트로 보안된 오브젝트 . . . . . .   CUSTLST1

                         오브젝트
사용자       그룹        권한
OWNER                    *ALL
*PUBLIC                  *AUTL
```

이제 권한 부여 리스트에 사용자 추가를 수행할 수 있습니다.

권한 부여 리스트에 사용자 추가

권한 부여 리스트로 오브젝트 보안을 완료했으면 EDTAUTL(권한 부여 리스트 편집) 명령을 사용하여 권한 부여 리스트 양식에 사용자를 추가하십시오.

1. EDTAUTL *authorization-list-name*을 입력하십시오.
2. 권한 부여 리스트 편집 화면에서 **F6**(신규 사용자 추가)을 누르십시오.
3. 리스트의 항목에 대해 있어야 할 사용자나 그룹 이름 그리고 권한을 입력하고 **Enter** 키를 누르십시오.
4. 신규 사용자가 리스트에 나옵니다.

```
                          신규 사용자 추가

오브젝트 . . . . . :   WSLST1         소유자  . .
  라이브러리 . . . . :     QSYS

신규 사용자를 입력하고 Enter 키를 누르십시오.

             오브젝트  리스트
User         권한      관리
QSECOFR     *CHANGE
```

가능한 오류	회복
사용자나 그룹에 리스트에 대한 잘못된 권한을 부여했습니다.	권한 부여 리스트 편집 화면에서 권한을 변경할 수 있습니다.
리스트에 잘못된 사용자 또는 그룹을 추가했습니다.	권한 부여 리스트 항목 제거(RMVAUTLE) 명령을 사용하여 사용자 또는 그룹을 제거하거나 권한 부여 리스트 편집 화면에서 사용자의 권한을 공백으로 남길 수 있습니다.

작업 확인

권한 부여 리스트에 대한 모든 사용자 권한을 나열하려면 DSPAUTL(권한 부여 리스트 표시) 명령을 사용하십시오. 권한 부여 리스트로 보안된 모든 오브젝트를 나열하려면 화면에서 **F15**를 사용하십시오.

특정 권한을 설정 하기 전에 다음 타스크를 완료하십시오.

- CRTAUTL 명령을 사용하여 어플리케이션에 필요한 권한 부여 리스트를 작성하십시오.
- EDTOBJAUT 명령을 사용하여 권한 부여 리스트로 오브젝트를 보안하십시오.
- EDTAUTL 명령을 사용하여 권한 부여 리스트에 사용자를 추가하십시오.

특정 권한 설정

지금까지 ″소유권 및 공용 권한 설정″에서 라이브러리 설명 양식 파트 1의 정보를 근거로 GRTOBJAUT 명령을 사용하여 라이브러리의 모든 오브젝트에 대해 공용 권한을 설정하는 방법을 배웠습니다. 이제 EDTOBJAUT(오브젝트 권한 편집) 명령을 사용하여 라이브러리 설명 양식 파트 2의 정보를 근거로 라이브러리에서 라이브러리와 오브젝트에 대해 특정 권한을 설정할 수 있습니다.

특정 권한을 설정하려면 다음 주제를 참조하십시오.

- 라이브러리에 대한 특정 권한 설정
- 오브젝트에 대한 특정 권한 설정
- 한 번에 두 개 이상의 오브젝트에 대한 권한 설정

라이브러리에 대한 특정 권한 설정

라이브러리는 실제로 특별한 유형의 오브젝트입니다. 다른 오브젝트에 대해 권한을 설정할 때와 마찬가지로 라이브러리에 대해서도 EDTOBJAUT 명령을 사용하여 권한을 설정하십시오. 모든 라이브러리는 QSYS라고 하는 IBM 제공 라이브러리에 있습니다. 다음 예에 나오는 화면은 JKL Toy사 CONTRACTS 라이브러리에 대한 라이브러리 설명 양식 파트 2를 사용합니다.

라이브러리 오브젝트에 대해 특정 권한 나열				
그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. EDTOBJAUT를 입력하고 **F4**(프롬트)를 누르십시오.
2. 프롬트 화면을 채우고 **Enter** 키를 누르십시오.

```
                  오브젝트 권한 편집(EDTOBJAUT)

선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . .  CONTRACTS
  라이브러리 . . . . . .  QSYS
오브젝트 유형  . . . . . .  *LIB
```

3. 오브젝트 권한 편집 화면에서 **F6**(신규 사용자 추가)을 누르고 화면에 나오지 않은 사용자에게 권한을 부여하십시오.
4. **Enter** 키를 누르십시오.

```
                              신규 사용자 추가

오브젝트 . . . . . :   CONTRACTS      소유자 . . . . . :   OWNCP
  라이브러리 . . . . :     QSYS        1차 그룹 . . . . . :   *NONE
오브젝트 유형. . . . :   *LIB


신규 사용자를 입력하고 Enter 키를 누르십시오.

              오브젝트
사용자        권한
DPTSM         *USE
DPTMG         *USE
```

5. 오브젝트 권한 편집 화면이 라이브러리 설명 양식 파트 1과 파트 2에 나오는 정보와 일치해야 합니다.

```
                          오브젝트 권한 편집

오브젝트 . . . . . :   CONTRACTS      소유자 . . . . . :   OWNCP
  라이브러리 . . . . :     QSYS        1차 그룹 . . . . . :   *NONE
오브젝트 유형. . . . :   *LIB

현재 권한에 대한 변경사항을 입력하고 Enter 키를 누르십시오.

  권한 부여 리스트로 보안된 오브젝트 . . . . . .   *NONE

                        오브젝트
사용자       그룹       권한
OWNCP                   *ALL
DPTSM                   *USE
DPTMG                   *USE
*PUBLIC                 *EXCLUDE
```

라이브러리를 위한 오브젝트 권한 편집 화면에는 신규 오브젝트에 대한 공용 권한(CRTAUT)이 나오지 않습니다. 라이브러리에 대한 CRTAUT를 보려면 라이브러리 표시(DSPLIB) 명령을 사용하십시오.

시스템의 오브젝트에 대해 특정 권한을 설정하려는 경우에도 이 프로시듀어를 사용할 수 있습니다.

이제 오브젝트에 대한 특정 권한 설정이 가능합니다.

오브젝트에 대한 특정 권한 설정

어플리케이션 라이브러리 안의 오브젝트에 대해 특정 권한을 설정하는 프로시듀어는 라이브러리에 대해 특정 권한 설정하는 것과 동일합니다. 예에서는 JKL Toy사의 COPGMLIB 라이브러리에 대한 라이브러리 설명 양식 파트 2를 사용합니다.

표 62. JKL Toy사의 라이브러리 설명 양식

그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. EDTOBJAUT를 입력하고 **F4**(프롬트)를 누르십시오.
2. 프롬트 화면에 정보를 채우고 **Enter** 키를 누르십시오.
3. 오브젝트 권한 편집 화면에 권한 정보를 입력하고 **Enter** 키를 누르십시오.

```
                          오브젝트 권한 편집

오브젝트 . . . . . :   COMSGQ01       소유자 . . . . . :   OWNCO
  라이브러리 . . . . :     COPGMLIB    1차 그룹 . . . . . :   *NONE
오브젝트 유형  . . . :   *MSGQ

현재 권한에 대한 변경사항을 입력하고 Enter 키를 누르십시오.

  권한 부여 리스트로 보안된 오브젝트 . . . . . .  *NONE

                       오브젝트
사용자      그룹         권한
OWNCO                  *ALL
*PUBLIC                 *CHANGE
```

이제 한 번에 두 개 이상의 오브젝트에 대한 권한설정이 가능합니다.

한 번에 두 개 이상의 오브젝트에 대한 권한 설정

지금까지는 예에서 EDTOBJAUT 명령을 사용하여 단일 오브젝트에 대해 특정 권한을 설정했습니다. 복수 오브젝트에 대해 보안을 설정하려면 GRTOBJAUT(권한 부여) 명령을 사용하십시오. GRTOBJAUT를 입력하고 **F4**(프롬트)를 누르십시오. 다음은 권한에 대해 여러 가지를 변경하는 예입니다.

- 다음 화면에 입력된 필드들은 CUSTLIB 라이브러리의 모든 메세지 대기행렬에 대한 공용 권한을 *CHANGE로 설정합니다.

```
                    오브젝트 권한 부여(GRTOBJAUT)
선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . .  *all
  라이브러리 . . . . . .    custlib
오브젝트 유형. . . . . .  *msgq
사용자 . . . . . .  *public
            추가하려면 + 입력
권한 . . . . . .  *change
```

- 다음 화면에 입력된 필드가 CUSTLIB 라이브러리에서 WRK 문자로 시작하는 이름의 모든 파일에 대해 *ALL 권한을 사용자 AMES에 부여합니다.

```
                    오브젝트 권한 부여

선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . .  WRK*
  라이브러리 . . . . . .    custlib
오브젝트 유형. . . . . .  *file
사용자 . . . . . . . . .  AMES
             추가하려면 + 입력
권한 . . . . . . . . . .  *all
```

이 예에서는 **총칭** 명명이라는 매개변수 지정 방법을 사용합니다. 많은 명령에 있어서 매개변수의 첫 문자 다음에 별표(*)를 지정할 수 있습니다. 시스템이 그와 같은 문자로 시작하는 이름의 모든 오브젝트에 대해 연산을 수행합니다. 명령을 위한 온라인 정보를 통해 총칭명을 허용하는 매개변수를 알 수 있습니다.

- ARLST1이라는 권한 부여 리스트를 사용하여 AR 문자로 시작하는 모든 파일을 보안하고 파일이 그 리스트에서 공용 권한을 가져오게 만드는 두 가지 단계가 필요합니다. 필요한 단계들이 다음 화면에 나옵니다.

```
                    오브젝트 권한 부여

선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . .  AR*
  라이브러리 . . . . . .    CUSTLIB
오브젝트 유형 . . . . . .  *FILE

   :
권한 부여 리스트 . . . . . .  ARLST1
```

```
                    오브젝트 권한 부여

선택사항을 입력하고 Enter키를 누르십시오.

오브젝트 . . . . . .  AR*
  라이브러리 . . . . . .    CUSTLIB
오브젝트 유형 . . . . . .  *FILE
사용자 . . . . . . . . .  *PUBLIC
             추가하려면 + 입력
권한 . . . . . . . . . .  *AUTL
             추가하려면 + 입력
```

"작업 기록부를 사용하여 작업 확인"에 나오는 설명처럼 DSPJOBLOG 명령을 사용하여 시스템이 요구한 권한을 변경했는지 확인하십시오.

"프린터 출력 보안"을 시작하기 전에 EDTOBJAUT나 GRTOBJAUT 명령을 사용하여 라이브러리 설명 양식 파트 2에 대해 특정 권한을 설정하십시오.

프린터 출력 보안

특정 권한을 설정했으면 다음 주제에 나오는 정보를 사용하여 기밀 프린터 출력을 보호할 수 있습니다.

- 출력 대기행렬 작성 및 관리할 수 있는 사람 제어
- 대기행렬에 특수 프린터 출력 할당

출력 대기행렬 작성

1. CRTOUTQ(출력 대기행렬 작성)를 입력하고 **F4**(프롬트)를 누르십시오.
2. 출력 대기행렬 및 라이브러리명을 입력하십시오.
3. **F10**(추가 매개변수)를 누르십시오.
4. 출력 대기행렬에 대한 보안 정보 찾기로 화면을 이동하십시오.

```
                    CRTOUTQ(출력 대기행렬 작성)

선택사항을 입력하고 Enter키를 누르십시오.

출력 대기행렬  . . . . . . . . . >   NEWCP
  라이브러리 . . . . . . . . . .       CONTRACTS
최대 스풀 파일 크기:
  페이지 수  . . . . . . . . . .   *NONE         번호, *NONE
  시작 시간  . . . . . . . . . .                 시간
  마침 시간  . . . . . . . . . .                 시간
             추가하려면 + 입력
대기행렬의 파일 순서 . . . . . .   *FIFO
리모트 시스템  . . . . . . . . .   *NONE

   :
텍스트 '설명'. . . . . . . . . .   신규 계약 대기행렬
```

5. 출력 대기행렬을 사용하고 관리할 수 있는 사람을 제어할 출력 대기행렬과 워크스테이션 보안 양식에서 나온 정보로 채우십시오.
6. **Enter** 키를 누르고 확인 메세지를 검토하십시오.

```
                    CRTOUTQ(출력 대기행렬 작성)

선택사항을 입력하고 Enter키를 누르십시오.


추가 매개변수

파일 표시. . . . . . . . . . . .   *NO
작업 분리자. . . . . . . . . . .   0
제어 오퍼레이터. . . . . . . . .   *NO
자료 대기행렬  . . . . . . . . .   *NONE
  라이브러리 . . . . . . . . . .
검사할 권한. . . . . . . . . . .   *OWNER
권한 . . . . . . . . . . . . . .   *LIBCRTAUT
```

가능한 오류	회복
F10 대신 **Enter** 키를 눌렀습니다.	CHGOUTQ(출력 대기행렬 변경) 명령을 사용하여 추가 정보를 입력하십시오.
틀린 라이브러리에 출력 대기행렬을 작성했습니다.	MOVOBJ(오브젝트 이동) 명령을 사용하여 올바른 라이브러리로 이동시키십시오.

이제 출력 대기행렬에 프린터 출력 할당이 가능합니다.

출력 대기행렬에 프린터 출력 할당

출력 대기행렬 작성을 완료했으면 출력 대기행렬에 프린터 출력을 할당할 수 있습니다. 일반적으로 프린터 파일이 프린터 출력의 목적지를 제어합니다. 기밀 보고서용 프린터 파일의 이름과 라이브러리를 찾으려면 어플리케이션 제공자에게 알아보십시오.

이 정보에 액세스 권한이 없으면 보고서를 인쇄하여 출력 대기행렬에 보유하십시오. 프린터 파일의 이름을 찾으려면 스풀 파일에 대한 작업 화면에 나오는 속성 옵션을 사용하십시오. 스풀 파일 속성에 대한 작업 화면의 *장치 파일* 필드에 프린터 파일이 나옵니다.

프린터 파일의 목적지(출력 대기행렬)를 변경하려면 다음에 나오는 CHGPRTF(프린터 파일 변경) 명령을 사용하십시오.

```
CHGPRTF FILE(library-name/printer-file-name)
        OUTQ(library-name/output-queue-name)
```

누군가 보고서를 다시 요구할 때마다 보고서가 신규 목적지로 갑니다. 출력 대기행렬에 이미 스풀되어 있는 파일의 목적지를 변경하려면 스풀 파일에 대한 작업 화면에서 변경 옵션을 사용하십시오.

예를 들어, Sharon Jones가 JKL Toy사의 가격 리스트 프린터 파일(PRCLST1)을 출력 대기행렬(PRICEQ)에 할당하려고 합니다. 그리고 다음과 같이 입력합니다.

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

모든 가격 리스트 보고서를 출력 대기행렬(PRICEQ)에 할당하기 위해 Sharon은 총칭 프린터 파일 이름을 사용할 수 있습니다.

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

모든 신규 계약을 출력 대기행렬(NEWCP)에 지정하기 위해 Sharon은 계약을 작성할 때 사용되는 샘플 문서와에 연관된 출력 대기행렬을 변경할 수 있습니다.

작업 확인

기밀 프린터 출력의 보호 전략을 확인하는 최선의 방법은 기밀을 인쇄해보는 것입니다. 올바른 출력 대기행렬로 가는지 확인하십시오. 시스템 오퍼레이터로 사인 온하여 대기행렬의 파일을 보거나 파일을 조작할 수 있는지 확인하십시오.

워크스테이션 보안을 실행하기 전에 다음을 수행해야 합니다.

- CRTOUTQ 명령을 사용하여 출력 대기행렬과 워크스테이션 보안 양식에 나오는 출력 대기행렬을 작성하십시오.
- CHGPRTF 명령을 사용하여 신규 출력 대기행렬에 프린터 출력을 할당하십시오.

워크스테이션 보안

프린터 출력을 보안했으면 워크스테이션을 보안해야 합니다. 시스템의 다른 오브젝트에 권한을 부여한 것처럼 워크스테이션에 권한을 부여하십시오. 워크스테이션에 사용자 권한을 부여하려면 EDTOBJAUT 명령을 사용하십시오.

워크스테이션에서 사인 온하기 위해서는 사용자에게 *CHANGE 권한이 반드시 있어야 합니다. QLMTSECOFR 시스템 값이 아니오(0)이면 보안 담당자나 *ALLOBJ 권한을 가진 사람이면 누구나 워크스테이션에서 사인 온할 수 있습니다.

QLMTSECOFR 시스템 값이 예(1)이면 다음 지침을 사용하여 워크스테이션에 대한 권한을 설정하십시오.

워크스테이션에서 사인 온할 수 있는 사용자	공용 권한	**QSECOFR** 권한	개별 사용자 권한
모든 사용자	*CHANGE	*CHANGE	요구하지 않음
선택 사용자 전용	*EXCLUDE	권한 없음	*CHANGE
선택 사용자 및 모든 오브젝트에 대해 권한을 가진 사용자	*EXCLUDE	*CHANGE	*CHANGE
모든 오브젝트에 대해 권한이 있는 사용자를 제외한 모든 사용자	*CHANGE	권한 없음	요구하지 않음

시스템 오퍼레이터 메세지 대기행렬에 대한 액세스를 제한하기 전에 EDTOBJAUT 명령을 사용하여 출력 대기행렬 및 워크스테이션 보안 양식의 정보를 근거로 워크스테이션을 보안하십시오.

시스템 오퍼레이터 메세지 대기행렬에 액세스 제한

프린터 출력 보안, 워크스테이션 보안, 시스템 오퍼레이터 메세지 대기행렬에 엑세스 제한을 실행하여 보안을 향상시킬 수 있습니다.

ASSIST 메뉴의 메세지 처리 옵션은 사용자가 기능 키를 사용하여 시스템 오퍼레이터 (QSYSOPR) 메세지 대기행렬을 표시할 수 있게 해줍니다. 시스템 오퍼레이터 메세지에 응답을 틀리게 할 경우 시스템에 문제를 일으킬 수 있습니다. 메세지 대기행렬에 있는 메세지에 응답하고 메세지를 삭제하기 위해서는 사용자에게 *CHANGE 권한이 필요합니다. 시스템 오퍼레이터에게만 이 권한이 있어야 합니다. 시스템 책임 양식을 참조하여 시스템 오퍼레이터 메세지 대기행렬에 대해 *CHANGE 권한을 가져야 하는 사람들을 알아보십시오.

다음과 같이 EDTOBJAUT 명령을 사용하십시오.

1. EDTOBJAUT QSYSOPR *MSGQ를 입력하고 **Enter** 키를 누르십시오.
2. **F11**을 누르고 자세한 오브젝트 권한 정보를 표시하십시오.
3. 샘플 화면에 나오는 것처럼 공용 *OBJOPR 권한을 부여하고 **Enter** 키를 누르십시오.

```
                          오브젝트 권한 편집

오브젝트 . . . . . :   QSYSOPR        소유자 . . . . . :   QSYS
  라이브러리 . . . :     QSYS         1차 그룹 . . . . . :   *NONE
오브젝트 유형  . . :   *MSGQ

현재 권한에 대한 변경사항을 입력하고 Enter 키를 누르십시오.

  권한 부여 리스트로 보안된 오브젝트 . . . . . .   *NONE

                       오브젝트  ---------오브젝트----------
사용자      그룹         권한      Opr  Mgt  Exist  Alter  Ref
*PUBLIC                USER DEF             X
```

4. 시스템이 *오브젝트 권한* 열을 USER DEF(정의된 사용자)로 변경합니다.
5. **F11**을 다시 누르고 자세한 자료 권한 정보를 표시하십시오.
6. 샘플 화면에 나오는 것처럼 공용 *ADD 권한를 부여하고 **Enter** 키를 누르십시오.

```
                          오브젝트 권한 편집

오브젝트 . . . . . :   QSYSOPR        소유자 . . . . . :   QSYS
  라이브러리 . . . :     QSYS         1차 그룹 . . . . . :   *NONE
오브젝트 유형  . . :   *MSGQ

현재 권한에 대한 변경사항을 입력하고 Enter 키를 누르십시오.

  권한 부여 리스트로 보안된 오브젝트 . . . . . .   *NONE

                       오브젝트  ---------------자료---------------
User        Group      Authority   읽기   추가   갱신   삭제   실행
*PUBLIC                USER DEF             X
```

7. **F6**(추가 사용자)을 사용하여 QSYSOPR 메세지에 응답해야 할 사용자를 추가하십시오. *CHANGE 권한을 메세지 응답 사용자에게 부여하십시오.

주의: *EXCLUDE 공용 권한은 작성하지 마십시오. 모든 작업(및 사용자)이 QSYSOPR 메세지 대기행렬에 메세지를 추가할 수 있어야 합니다.

자원 보안 설정을 완료하려면 다음과 같이 하십시오.

- 권한 부여 리스트 양식 및 라이브러리 설명 양식을 사용하여 모든 어플리케이션 라이브러리에 대한 보안을 설정했는지 확인하십시오.
- 출력 대기행렬 및 워크스테이션 보안 양식을 확인하여 워크스테이션을 보호하고 특수 출력 대기행렬을 작성했는지 확인하십시오.
- 시스템 오퍼레이터(QSYSOPR) 메세지 대기행렬에 엑세스를 제한하십시오.

- 어플리케이션과 함께 제공된 지침에 따라 어플리케이션 라이브러리를 저장하십시오. 시스템이 소유권과 공용 권한 정보를 어플리케이션과 함께 저장합니다.
- 작성한 보안 정보를 SAVSECDTA(보안 자료 저장) 명령을 사용하여 저장하십시오. 보안 정보 저장 방법에 관한 자세한 정보는 ″보안 정보 저장″을 참조하십시오.

이제 보안 설정 테스트를 시작할 수 있습니다.

제 8 장 보안 테스트

이 주제에서는 시스템에 설정한 보안을 테스트하는 방법을 설명합니다. 여기서 테스트란 의도한 대로 작업을 설정하였는지 확인하는 것을 말합니다. "보안 모니터" 주제에서는 시스템에 설정된 보안의 효율성을 평가하는 방법에 관해 설명합니다.

시스템에 주요한 변경이 있을 때마다 보안을 테스트하십시오. 그와 같은 예로는 신규 어플리케이션 추가, 기존 어플리케이션에 대해 자원 보안 설정, 신규 사용자 그룹 추가, 보안 레벨을 변경 등이 있습니다.

보안 변경이 있을 때의 테스트와 문제점 진단 방법에 관해 알아보려면 다음 주제를 검토하십시오.

- 사용자 프로파일 테스트
- 자원 보안 테스트

사용자 프로파일 테스트

보안 테스트를 시작하기 위해서 시스템에 신규 그룹을 설정할 때마다 사용자 프로파일을 테스트할 수 있습니다. 이 경우 그룹 프로파일에서 복사한 개별 프로파일 중 하나를 테스트하십시오.

- 사용자 프로파일로 성공적으로 사인 온할 수 있습니까? 사인 온할 수 없으면 사인 온 시도 실패에 대해 기록한 작업 기록부를 확인하십시오. 자세한 정보를 위해 작업 기록부를 찾으려면 ASSIST 메뉴에서 프린터 출력에 대한 작업 옵션을 사용하십시오.

  다음은 발생할 가능성이 많은 문제점입니다.

  – 초기 메뉴, 현재 라이브러리 또는 초기 프로그램과 같은 필요한 오브젝트 중 하나가 없습니다.

  – 작업 설명에 지정된 라이브러리 리스트가 오류를 일으킵니다. 라이브러리가 없거나 QGPL 및 QTEMP를 라이브러리 리스트에 포함시키지 않았습니다.

  – 사용자에게 워크스테이션에 대한 권한이 없습니다.
- 사인 온할 때 화면이 올바른 초기 메뉴나 프로그램을 표시합니까?
- 사인 온 화면에 초기 메뉴나 현재 라이브러리를 입력하면 어떻게 됩니까? 사용자 프로파일이 제한 기능(YES)이면 오류 메세지가 나옵니다.
- 어텐션 키를 누를 때 올바른 화면이 나옵니까?
- 출력이 올바른 프린터로 나갑니까? 그렇지 않으면 ASSIST 메뉴에서 프린터 출력에 대한 작업 옵션을 사용하여 출력이 나가는 위치를 알아보십시오. 사용자 프로파일과 작업 설명을 확인하여 출력이 다른 프린터로 나가는 원인을 판별하십시오.

- 명령행을 사용할 수 있습니까?
- 보안 오류 없이 필요한 어플리케이션 기능을 수행할 수 있습니까? 자세한 정보는 "자원 보안 테스트"를 참조하십시오.
- 프린터 관리나 라이브러리 저장과 같은 필요한 시스템 타스크를 수행할 수 있습니까?

프로파일로 사인 온할 때 시스템이 신규 암호를 지정하도록 요구하면 테스트를 완료한 후 사용자 프로파일 이름에 암호를 다시 설정하십시오.

1. 고유 프로파일(보안 담당자 권한을 가진)로 사인 온하십시오.
2. CHGUSRPRF *profile-name* PASSWORD(*profile-name*) PWDEXP(*YES)를 입력하십시오.

사용자 프로파일을 테스트했으므로 이제 자원 보안 테스트를 할 수 있습니다.

자원 보안 테스트

사용자 프로파일 테스트를 완료하면 자원 보안도 테스트해야 합니다. 자원 보안을 테스트할 때 다음과 같은 사용자가 있는지 찾아보십시오.

- 작업을 수행할 충분한 권한이 없는 사용자
- 의도한 것 보다 많은 권한을 가진 사용자

불충분한 권한에 대한 테스트

대화식 처리 기능과 일괄처리 기능을 모두 테스트하여 사용자 프로파일에 충분한 권한이 있는지 확인하십시오.

대화식 테스트

어플리케이션에 대한 자원 보안을 테스트하려면 서로 다른 여러 사용자 프로파일로 사인 온해야 합니다. 할당한 권한이 충분한지 확인하기 위해 샘플 사용자를 테스트하는 것이 목적입니다.

- 다른 레벨의 권한(보기, 변경, 삭제)을 필요로 하는 기능들을 테스트하십시오.
- 메뉴 뿐만 아니라 프로그램도 테스트하십시오. 메뉴 옵션을 선택하는 것으로는 권한을 테스트하기에 충분하지 않을 수 있습니다. 레코드 삭제와 같은 조작을 실제로 수행할 때까지 시스템이 파일에 액세스하지 않는 경우가 있습니다. 시스템이 파일 열 때 권한 확인이 이루어집니다. 어플리케이션 설계에서 시스템이 파일을 여는 시기가 결정됩니다.
- 보안 오류 기록을 보유하여 그 오류들을 해결하십시오. 권한 오류가 발생하면 연산처리 및 사용하려는 오브젝트에 대해 권한이 충분하지 않은 것을 나타내는 오류 메세지가 나옵니다.

일괄처리 테스트

- 작업을 제출할 사용자의 프로파일로 어플리케이션에서 나온 샘플 일괄처리 작업을 실행하십시오.
- 정보 인쇄, 정보 변경 또는 월 말에 파일 지우기 등과 같은 다른 레벨의 권한을 필요로 하는 일괄처리 작업을 테스트하십시오.
- QSYSOPR 메세지 대기행렬과 보안 오류에 대해 QHST 기록부를 확인하십시오. DSPLOG 명령을 사용하여 QHST 기록부를 보십시오. 보안 메세지는 CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00, CPD4A00 범위에 있습니다.

  권한 실패와 기타 보안 관련 이벤트를 기록하기 위해 보안 감사 기능을 사용할 수도 있습니다.

과도한 권한에 대한 테스트

기밀 정보를 보호할 자원 보안을 설정하려면 샘플 사용자 프로파일을 테스트하여 보안이 작동하는지 확인하십시오. 기밀 파일에 액세스해서는 안 될 사용자의 프로파일로 사인 온하십시오.

- 파일에 액세스를 허용하는 메뉴를 사용할 수 있습니까?
- 파일을 사용하는 메뉴 옵션을 선택하면 어떻게 됩니까?
- 명령행을 사용할 수 있습니까?
- CPYF FROMFILE(*file-name*) TOFILE(QSYSPRT)과 같은 파일을 나열하는 명령을 실행할 수 있습니까?
- 파일을 보기 위한 조회 툴을 사용할 수 있습니까?

테스트 결과, 보안 정보 변경이 필요할 수 있습니다.

제 9 장 보안 정보 변경

시스템에 대한 보안을 계획했으므로 회사에서 변경이 필요할 때마다 그 계획이 여전히 유효한 것인지를 확인해야 합니다.

이 주제는 보안을 설계에 있어서 필수적인 목표로 단순성을 강조합니다. 사용자가 개별 사용자를 위한 패턴으로 사용자 그룹을 설계했습니다. 또한 특정한 개별 권한을 사용하기보다는 공용 권한, 권한 리스트, 라이브러리 권한을 사용하고 있습니다. 보안을 관리할 때 그러한 방식을 활용하십시오.

- 신규 사용자 그룹이나 신규 어플리케이션을 추가할 때 보안 계획에 사용한 방법을 사용하십시오.
- 보안을 변경해야 할 경우 특정한 문제를 해결하기 위해 예외를 작성하기 보다는 일반적인 접근방식을 사용하십시오.

보안 명령 주제에서는 보안 정보 표시, 변경, 삭제에 사용할 명령을 설명합니다.

다른 유형의 변경을 처리하는 것에 관한 제안사항은 다음 주제를 참조하십시오.

- 시스템에 신규 사용자 추가
- 신규 사용자 그룹 작성
- 사용자 그룹 변경
- 신규 어플리케이션 추가
- 신규 워크스테이션 추가
- 사용자 책임 변경
- 시스템에서 사용자 제거

보안 명령

아래 표는 시스템의 보안 오브젝트에 대한 작업에 사용하는 명령을 보여줍니다. 타스크를 수행하기 위해 다음 명령을 사용할 수 있습니다.

- 보안 정보 보기 및 나열
- 보안 정보 변경
- 보안 정보 삭제

표 63. 보안 명령

보안 오브젝트	보는 방법	변경 방법	삭제 방법
시스템 값	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	삭제시킬 수 없음

표 63. 보안 명령 (계속)

보안 오브젝트	보는 방법	변경 방법	삭제 방법
작업 설명	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
그룹 프로파일	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
사용자 프로파일	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
오브젝트 권한	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
오브젝트 소유권	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN은 이전 소유자의 권한을 취소할 수 있게 해줍니다.
1차 그룹	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP는 1차 그룹을 *NONE으로 설정합니다.
오브젝트 감사	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD(*NONE으로 설정) CHGAUD
권한 부여 리스트	DSPAUTL DSPAUTLOBJ	EDTAUTL(리스트에 대한 사용자 권한) EDTOBJAUT(리스트로 보안한 오브젝트) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL(전체 리스트)[3] RMVAUTLE(리스트에 대한 사용자 권한 삭제) EDTOBJAUT(리스트로 보안한 오브젝트) RVKOBJAUT

1. IBM은 프로파일을 삭제하기 위해 사용자 등록에 대한 작업 화면의 제거 옵션을 사용할 것을 권장합니다. 이 옵션을 사용하여 프로파일이 소유하는 오브젝트를 삭제하거나 신규 소유자에게 오브젝트를 다시 할당할 수 있습니다. 특정 DLTUSRPRF 명령 매개변수는 사용자가 소유하는 모든 오브젝트를 삭제하거나 신규 소유자가 오브젝트를 할당할 수 있게 해줍니다. 소유한 오브젝트를 삭제하거나 할당하지 않으면 프로파일을 삭제할 수 없습니다. 모든 오브젝트에 대한 1차 그룹인 프로파일은 삭제할 수 없습니다.
2. 모든 멤버를 가진 그룹 프로파일은 삭제할 수 없습니다. 그룹의 멤버를 나열하려면 DSPUSRPRF 명령의 *GRPMBR 옵션을 사용하십시오. 그룹 프로파일을 삭제하기 전에 각 개별 그룹 프로파일에서 *그룹 프로파일* 필드를 변경하십시오.
3. 보안 오브젝트에 사용되는 권한 부여 리스트는 삭제할 수 없습니다. 리스트로 보안한 오브젝트를 나열하려면 DSPAUTLOBJ 명령을 사용하십시오. EDTOBJAUT 명령을 사용하여 리스트로 보안한 모든 오브젝트의 권한을 변경하십시오.

보안 정보 보기 및 나열

인쇄(*PRINT) 옵션과 함께 DSP(화면 표시) 명령을 사용하여 보안 정보를 나열할 수 있습니다. 예를 들어, MYLIST라는 권한 부여 리스트를 표시하려면 DSPAUTL MYLIST *PRINT라고 입력하십시오.

일부 표시 명령은 다른 리스트 유형에 대한 옵션을 제공합니다. 예를 들어, 개별 사용자 프로파일을 작성할 때 그룹 프로파일의 모든 멤버를 나열하기 위해 DSPUSRPRF 명령의 *GRPMBR 옵션을 사용합니다. 이 경우 보안 오브젝트에 사용할 수 있는 리스트를 찾으려면 **F4**(프롬트) 및 온라인 정보를 사용하십시오.

현재 사용하는 화면에서 표시 명령을 사용하여 보안 정보를 볼 수 있습니다. 또한 그보다 더 많은 기능을 제공하는 WRK(...에 대한 작업) 명령을 사용할 수도 있습니다. ...에 대한 작업 명령은 리스트 화면을 제공합니다. 이 화면을 통해 정보를 변경하거나 삭제하거나 볼 수 있습니다.

또한 총칭명을 사용하여 정보를 나열하거나 보기 위해 보안 명령을 사용할 수도 있습니다. WRKUSRPRF DPT*를 입력하면 사용자 등록에 대한 작업 화면이나 사용자 프로파일에 대한 작업 화면에 *DPT*라는 문자로 시작하는 프로파일만 표시됩니다. 총칭명을 허용하는 매개변수를 찾으려면 명령을 위한 온라인 정보를 사용하십시오.

보안 정보 변경

WRK(...에 대한 작업) 또는 EDT(...편집) 명령을 사용하여 보안 정보를 대화식으로 변경할 수 있습니다. 정보를 보거나 변경할 수 있으며 변경 후 다시 정보를 볼 수 있습니다.

CHG(...변경) 또는 GRT(...부여) 명령을 사용하여 변경 이전 및 이후에 정보를 보지 않고도 보안 정보를 변경할 수 있습니다. 이 방법은 한 번에 하나 이상의 오브젝트를 변경할 때 특히 유용합니다. 예를 들어, 라이브러리내의 모든 오브젝트에 대해 공용 권한을 설정하기 위해 GRTOBJAUT 명령을 사용합니다(128 페이지의 『라이브러리내의 모든 오브젝트에 대해 공용 권한 설정』 참조).

보안 정보 삭제

WRK(...에 대한 작업) 또는 EDT(...편집) 명령을 사용하여 특정 유형의 보안 정보를 대화식으로 삭제하거나 제거할 수 있습니다. 또한 DLT(...삭제), RMV(...제거), RVK(...취소) 명령을 사용하여 보안 정보를 삭제할 수도 있습니다. 보안 정보를 삭제할 수 있으려면 먼저 특정 조건을 충족시켜야 할 경우가 있습니다. 보안 명령에 나오는 주에서 그와 같은 일부 조건에 관해 설명합니다.

시스템에 신규 사용자 추가

시스템에 신규 사용자를 추가할 경우 다음 프로시듀어를 사용하십시오.

1. 사용자 그룹에 사용자를 할당하십시오. 참조를 위해 사용자 그룹 설명 양식을 사용하십시오.
2. 신규 사용자가 시스템 기능을 수행해야 하는지 결정하십시오. 수행해야 한다면 시스템 책임 양식에 그 정보를 추가하십시오.
3. 개별 사용자 프로파일 양식에 사용자를 추가하십시오.
4. 신규 사용자가 그룹내의 다른 사용자들과 다른 값을 필요로 하는지 판별하려면 시스템 책임 양식 및 사용자 그룹 설명 양식을 검토하십시오.
5. 그룹 프로파일이나 그룹 멤버의 프로파일을 복사하여 사용자 프로파일을 작성하십시오. 반드시 암호 만기를 설정하십시오(″그룹 프로파일 복사″ 참조).
6. 보안 메모의 사본을 신규 사용자에게 제공하십시오.

신규 사용자 그룹을 작성하는 방법은 ″신규 사용자 그룹 작성″을 참조하십시오.

신규 사용자 그룹 작성

다음과 같은 몇 가지 이유로 인해 신규 사용자 그룹을 작성해야 할 경우가 있습니다.

- 새로 조직된 부서가 시스템을 사용해야 합니다.
- 자원 보안 요구를 충족시키기 위해 사용자 그룹을 보다 세분화할 필요가 있습니다.
- 회사에서 일부 부서들을 재편합니다.

신규 사용자 그룹을 작성하려면 다음과 같이 하십시오.

1. ″사용자 그룹 계획″의 지침을 따라 사용자 그룹 설명 양식을 작성하십시오.
2. 어플리케이션, 라이브러리 및 사용자 그룹의 다이어그램에 사용자 그룹을 추가하십시오.
3. 모든 그룹 멤버가 시스템 기능을 수행해야 하는지 결정하십시오. 시스템 책임 양식을 갱신하십시오(″시스템 기능에 책임이 있는 사용자″ 참조).
4. 사용자 그룹 설명 양식 및 시스템 책임 양식의 정보를 사용하여 개별 사용자 프로파일 양식을 작성하십시오.
5. 그룹 라이브러리를 작성하십시오.
6. 그룹에 대한 작업 설명을 작성하십시오.
7. 그룹 프로파일을 작성하십시오.

   주: 5, 6, 7단계를 수행에 대한 지침은 ″사용자 그룹 설정″을 참조하십시오.
8. 그룹 멤버에 대한 개별 사용자 프로파일을 작성하십시오(″개별 사용자 설정″ 참조).
9. 그룹에 필요한 모든 어플리케이션의 라이브러리 설명 양식을 검토하십시오. ″자원 보안 설정″에서 설명한 방법을 사용하여 어플리케이션 오브젝트에 그룹 액세스를 부여하는 데 필요한 모든 단계를 실행하십시오.
10. 그룹의 모든 멤버에게 보안 메모의 사본을 제공하십시오.

사용자 그룹을 변경하는 방법은 ″사용자 그룹 변경″을 참조하십시오.

사용자 그룹 변경

그룹의 특성에 대한 다른 유형의 변경들은 다른 방법으로 처리해야 합니다. 다음에 일부 변경의 예와 그 처리 방법이 나옵니다.

그룹 권한 변경

처음에 계획할 때 예상하지 못했던 오브젝트 권한이 그룹에 필요하다는 것을 발견할 수 있습니다. 이 경우 다음과 같이 하십시오.

1. 그룹으로 오브젝트나 적절한 권한 부여 리스트에 대한 올바른 액세스를 부여하려면 EDTOBJAUT(오브젝트 권한 편집) 명령을 사용하십시오. 134 페이지의 『특정 권한 설정』에 이 명령을 사용하는 방법의 예가 나옵니다. 그룹 권한을 부여하면 그룹의 모든 멤버가 오브젝트에 대한 권한을 가집니다.
2. 기밀 자원에 대해 그룹 권한을 부여한 경우 그룹의 현재 멤버를 확인할 수 있습니다. 그룹 멤버를 나열하려면 사용자 프로파일 표시 명령(DSPUSRPRF *group-profile-name* *GRPMBR)을 사용하십시오.

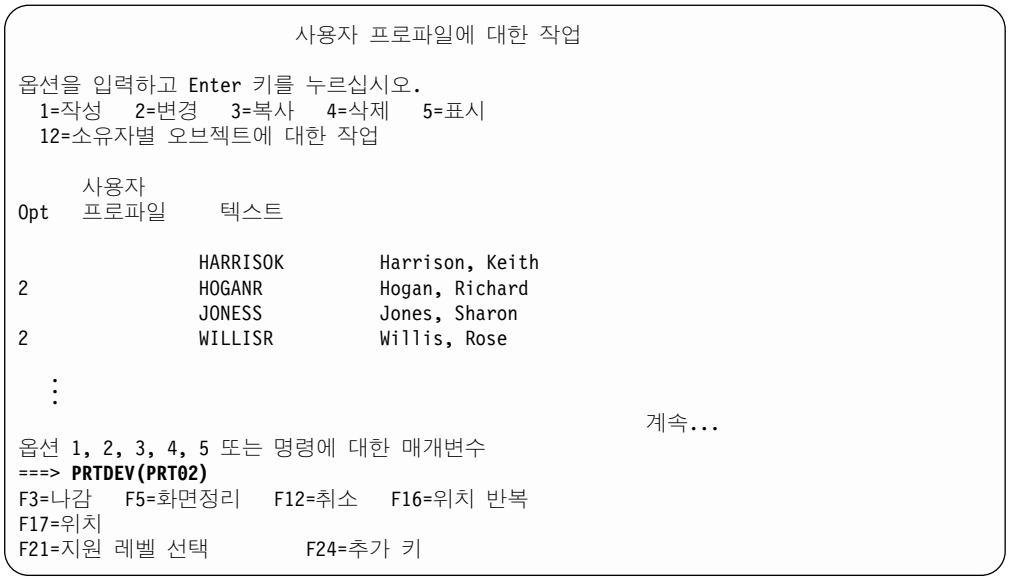
그룹에 대한 사용자 정의 변경

그룹 멤버를 위해 사용자 환경 설정을 변경해야 할 경우가 있습니다. 예를 들어, 한 부서에 부서 고유의 프린터가 있으면 신규 프린터를 그 부서의 사용자 그룹 멤버를 위한 디폴트로 만들 수 있습니다. 또는 시스템에 신규 어플리케이션을 설치했을 때 한 사용자 그룹의 멤버들이 다른 초기 메뉴(사인 온시)를 원할 수도 있습니다.

그룹 프로파일은 그룹 멤버를 위한 개별 프로파일을 작성하기 위해 복사할 수 있는 패턴을 제공합니다. 그러나 그룹 프로파일 안의 값을 조정하는 것은 개별 사용자 프로파일을 작성한 후 그 프로파일에 영향을 미치지 않습니다. 예를 들어, 그룹 프로파일에서 *프린터 장치*와 같은 필드를 변경하는 것은 그룹 멤버에 아무런 영향이 없습니다. 개별 사용자 프로파일에서 *프린터 장치*를 변경해야 합니다.

한 번에 둘 이상의 사용자에 대한 매개변수를 변경하려면 사용자 프로파일에 대한 작업 화면을 사용할 수 있습니다. 다음은 그룹의 모든 멤버에 대한 출력 대기행렬을 변경하는 예입니다.

1. WRKUSRPRF *ALL을 입력하고 **Enter** 키를 누르십시오.
2. 사용자 등록에 대한 작업 화면을 보려면 **F21**(지원 레벨 선택)을 눌러 사용자 프로파일에 대한 작업 화면으로 변경하십시오.



3. 변경하려는 각 프로파일 옆에 **2**(변경)를 입력하십시오.
4. 화면 맨 아래의 매개변수 행에 매개변수 이름 및 새로운 값을 입력하십시오. 매개변수 이름을 모르면 **F4**(프롬트)를 누르십시오.
5. **Enter** 키를 누르십시오. 변경된 각 프로파일에 대한 확인 메세지가 나옵니다.

   그룹 프로파일에서 사용자 정의 필드를 변경하는 것이 그룹 멤버에 아무런 영향이 없더라도 나중에 도움이 될 수 있습니다. 나중에 그룹에 멤버를 추가할 때 그룹 프로파일이 하나의 패턴을 제공합니다. 또한 그룹을 위한 표준 필드 값의 레코드가 됩니다.

신규 어플리케이션에 그룹 액세스 부여

사용자 그룹이 신규 어플리케이션에 대한 액세스를 필요로 할 경우 그룹 및 어플리케이션에 관한 정보를 분석해야 합니다. 다음 제안 사항을 참조하십시오.

1. 신규 어플리케이션과 어플리케이션, 라이브러리 및 사용자 그룹의 다이어그램에 대한 어플리케이션 설명 양식을 보고 어플리케이션이 어떤 라이브러리를 사용하는지 확인하십시오. 그 라이브러리를 사용자 그룹 설명 양식에 추가하십시오.
2. 사용자 그룹 및 어플리케이션간에 새로운 관계를 표시하도록 어플리케이션, 라이브러리 및 사용자 그룹의 다이어그램을 갱신하십시오.
3. 그룹의 초기 라이브러리 리스트에 라이브러리를 포함시켜야 할 경우 CHGJOBD(작업 설명 변경) 명령을 사용하여 그룹의 작업 설명을 변경하십시오. 작업 설명에 대한 도움말은 113 페이지의 『작업 설명 작성』을 참조하십시오.

   주: 작업 설명에 나오는 초기 라이브러리 리스트에 라이브러리를 추가할 때 그 작업 설명을 사용하는 사용자 프로파일은 변경할 필요가 없습니다. 사용자가 다음에 사인 온할 때 초기 라이브러리 리스트가 자동으로 그 라이브러리를 추가합니다.

4. 신규 어플리케이션에 액세스를 제공하기 위해 그룹에 대한 초기 메뉴나 초기 프로그램을 변경해야 하는지 결정하십시오. CHGUSRPRF 명령을 사용하여 각 사용자 프로파일의 초기 메뉴나 프로그램을 개별적으로 변경해야 합니다.
5. 어플리케이션이 사용하는 모든 라이브러리의 라이브러리 설명 양식을 검토하십시오. 라이브러리에 사용할 수 있는 공용 권한이 그룹의 필요에 충분한지 판별하십시오. 충분하지 않으면 라이브러리, 특정 오브젝트, 권한 부여 리스트에 그룹 권한을 부여해야 할 수 있습니다. 이와 같이 하려면 EDTOBJAUT(오브젝트 권한 편집) 및 EDTAUTL(권한 부여 리스트 편집) 명령을 사용하십시오(추가 정보가 필요하면 ″자원 보안 설정″을 참조하십시오).

시스템에 어플리케이션을 추가하려면 ″신규 어플리케이션 추가″를 참조하십시오.

신규 어플리케이션 추가

현재 어플리케이션에 대해 계획한 것처럼 신규 어플리케이션에 대해서도 신중하게 보안 계획을 세워야 합니다. 같은 프로시듀어를 따르십시오.

1. 어플리케이션을 위한 어플리케이션 설명 양식 및 라이브러리 설명 양식을 준비하십시오.
2. 어플리케이션, 라이브러리 및 사용자 그룹의 다이어그램을 갱신하십시오.
3. 신규 어플리케이션의 보안 방법을 결정하려면 ″자원 보안 결정″에 나오는 프로시듀어를 따르십시오.
4. ″어플리케이션 설치 계획″에서 설명하는 방법으로 어플리케이션 설치 양식을 준비하십시오.
5. 어플리케이션의 프린터 출력이 기밀사항으로서 보호를 필요로 하는 것인지 평가하십시오. 필요하다면 출력 대기행렬 및 워크스테이션 보안 양식을 갱신하십시오.
6. 어플리케이션을 설치하고 보안하려면 ″소유권 및 공용 권한 설정″ 및 ″자원 보안 설정″에 나오는 단계를 따르십시오.

시스템에 워크스테이션을 추가하려면 ″신규 워크스테이션 추가″를 참조하십시오.

신규 워크스테이션 추가

시스템에 신규 워크스테이션을 추가할 경우 다음에 나오는 보안 요구사항을 고려하십시오.

1. 신규 워크스테이션의 물리적 위치가 보안 노출 가능성이 있습니까?(앞에서 설명한 ″물리적 보안 계획″을 다시 참조하십시오.)
2. 워크스테이션에 위험 노출 가능성이 있으면 출력 대기행렬 및 워크스테이션 보안 양식을 갱신하십시오.

3. 일반적으로 *CHANGE 공용 권한으로 신규 워크스테이션을 작성할 수 있습니다. 위의 방법으로 워크스테이션의 보안 요구사항을 충족시킬 수 없으면 EDTOBJAUT 명령을 사용하여 다른 권한을 지정하십시오.

시스템에서 사용자의 책임을 변경하려면 "사용자 책임 변경"을 참조하십시오.

사용자 책임 변경

시스템 사용자가 회사에서 새로운 업무나 책임을 담당할 경우에 사용자 프로파일에는 어떤 영향이 있는지를 평가해야 합니다.

1. 사용자가 다른 사용자 그룹에 속해야 합니까? 사용자 그룹을 변경하려는 경우 CHGUSRPRF 명령을 사용할 수 있습니다.
2. 프로파일에서 프린터나 초기 메뉴와 같은 사용자 정의 값을 변경해야 합니까? 변경하려는 경우 CHGUSRPRF 명령을 사용할 수 있습니다.
3. 신규 사용자 그룹의 어플리케이션 권한이 이 사람에게 충분합니까?
   - 이전 및 신규 사용자 그룹 프로파일의 권한을 보려면 DSPUSRPRF(사용자 프로파일 표시) 명령을 사용하십시오.
   - 개별 사용자 프로파일의 권한도 보십시오.
   - EDTOBJAUT 명령을 사용하여 필요한 모든 변경을 수행하십시오.
4. 사용자가 오브젝트를 소유합니까? 그 오브젝트의 소유권을 변경해야 합니까? WRKOBJOWN(소유자별 오브젝트에 대한 작업) 명령을 사용하십시오.
5. 사용자가 시스템 기능을 수행합니까? 사용자가 새로운 작업을 위해 시스템 기능을 수행해야 합니까? 필요하면 시스템 책임 양식을 갱신하고 사용자 프로파일을 변경하십시오.

시스템에서 사용자를 제거하는 방법은 "시스템에서 사용자 제거"를 참조하십시오.

시스템에서 사용자 제거

퇴사하는 사람이 있으면 시스템에서 즉시 사용자 프로파일을 제거해야 합니다. 사용자 프로파일을 제거하기 전에 프로파일이 소유하는 모든 오브젝트의 소유권을 삭제하거나 전송하십시오. 이 작업을 위해 WRKOBJOWN 명령을 사용하거나 사용자 등록에 대한 작업 화면에서 옵션 **4**(제거)를 사용할 수 있습니다.

사용자 등록에 대한 작업 화면에서 프로파일을 위한 옵션 **4**(제거)를 선택하면 사용자가 소유하고 있는 모든 오브젝트를 처리할 수 있게 해 주는 추가 화면을 볼 수 있습니다. 모든 오브젝트를 신규 소유자에게 제공하거나 개별적으로 오브젝트를 처리하게 만들 수 있습니다.

```
                              사용자 제거

사용자 . . . . . :   HOGANR
사용자 설명  . . . . . . . :   판매 및 마케팅 부서

이 사용자를 제거하려면 아래의 선택사항을 입력하고 Enter 키를 누르십시오.

    1. 이 사용자가 소유하는 모든 오브젝트를 신규 소유자에게 제공합니다.
    2. 이 사용자가 소유하는 특정 오브젝트의 소유자를 삭제 또는 변경합니다.
```

개별적으로 오브젝트 처리하도록 선택하면(옵션 **2**) 화면에 사용자가 소유한 모든 오브젝트의 리스트가 나옵니다.

```
                              사용자 제거

사용자 . . . . . :   HOGANR
사용자 설명  . . . . . . . :   판매 및 마케팅 부서

신규자 . . . . . .                    이름, 리스트는 F4

이 사용자를 제거하려면 모든 오브젝트의 소유자를 삭제 또는 변경하십시오.
아래의 옵션을 입력하고 Enter 키를 누르십시오.
  2=신규 소유자로 변경   4=삭제   5=세부사항 표시

Opt  오브젝트      라이브러리    설명
 4   HOGANR       QUSRSYS      Hogan, Richard 메세지 대기행렬
 4   QUERY1       DPTWH        재고 조회
```

오브젝트 삭제를 선택하면 삭제 확인 화면이 나옵니다. 일단 시스템에서 오브젝트가 삭제되면 사용자 프로파일을 제거할 수 있습니다. 그리고 나면 시스템이 사용자를 제거했다는 메세지와 함께 사용자 등록에 대한 작업 화면이 다시 나옵니다.

제 10 장 보안 정보 저장

이 주제에서는 보안 정보를 저장하고 복원하는 방법에 대한 개요를 제공합니다. 시스템에 대한 백업 및 회복을 계획할 때 정보 자체는 물론 정보의 보안을 함께 고려해야 합니다. Information Center에서 백업, 회복 및 가용성 주제를 참조하여 완벽한 백업 및 회복 계획을 설계하십시오.

다음 주제에서는 보안을 설정할 때 작성하는 보안 정보를 백업 및 복원하는 방법에 관해 설명합니다.

- 시스템 값 저장
- 그룹 및 사용자 프로파일 저장
- 작업 설명 저장
- 자원 보안 정보 저장
- 디폴트 소유자 프로파일(QDFTOWN) 사용
- 손상된 권한 부여 리스트 회복

시스템 값 저장

시스템 값은 시스템 라이브러리인 QSYS에 저장됩니다. 다음과 같이 QSYS 라이브러리에 저장하십시오.

- 시스템 저장(SAVSYS) 명령을 사용하십시오.
- 저장 메뉴에서 전체 시스템을 저장하기 위한 옵션을 사용하십시오.
- 저장 메뉴에서 시스템 정보를 저장하기 위한 옵션을 사용하십시오.
- 백업 실행(RUNBCKUP) 메뉴에서 전체 시스템을 백업하기 위한 옵션을 사용하십시오.

전체 시스템을 회복시켜야 할 경우 오퍼레이팅 시스템을 복원시킬 때 시스템 값도 자동으로 복원됩니다.

이제 "그룹 및 사용자 프로파일 저장"을 참조하십시오.

그룹 및 사용자 프로파일 저장

그룹 및 사용자 프로파일은 QSYS 라이브러리에 저장됩니다. 전체 시스템을 저장하려는 경우 메뉴 옵션을 선택하거나 SAVSYS(시스템 저장) 명령을 사용하여 저장할 수 있습니다.

또한 SAVSECDTA(보안 자료 저장) 명령을 사용하여 그룹 및 사용자 프로파일을 저장할 수 있습니다.

RSTUSRPRF(사용자 프로파일 복원) 명령을 이용하여 사용자 프로파일을 복원하십시오. 정상적인 순서는 다음과 같습니다.

1. 오퍼레이팅 시스템을 복원하십시오. 이 결과 QSYS 라이브러리가 복원됩니다.
2. 사용자 프로파일을 복원하십시오.
3. 나머지 라이브러리를 복원하십시오.
4. RSTAUT(권한 복원) 명령을 사용하여 오브젝트에 대한 권한을 복원하십시오.

이제 "작업 설명 저장"을 참조하십시오.

작업 설명 저장

작업 설명을 작성할 때 작업 설명이 위치할 라이브러리를 지정하십시오. IBM에서는 QGPL 라이브러리에 작업 설명을 작성할 것을 권장합니다.

작업 설명이 상주하는 라이브러리를 저장하여 작업 설명을 저장할 수 있습니다. SAVLIB(라이브러리 저장) 명령으로 이 작업을 수행하십시오. 또한 SAVOBJ(오브젝트 저장) 명령을 사용할 수도 있습니다.

RSTLIB(라이브러리 복원) 명령을 사용하여 라이브러리의 내용을 복원할 수 있습니다. 그리고 RSTOBJ(오브젝트 복원) 명령을 사용하여 개별 작업 설명을 복원할 수 있습니다.

이제 "자원 보안 정보 저장"을 참조하십시오.

자원 보안 정보 저장

오브젝트에 대해 작업할 수 있는 방법을 정의하는 자원 보안은 여러 다른 장소에 저장되어 있는 서로 다른 정보 유형으로 구성됩니다.

표 64. 자원 보안 정보 저장 및 복원

정보 유형	저장 장소	저장 방법	복원 방법
공용 권한	오브젝트 포함	SAVxxx 명령 [1]	RSTxxx 명령 [2]
오브젝트 감사 값	오브젝트 포함	SAVxxx 명령 [1]	RSTxxx 명령 [2]
오브젝트 소유권	오브젝트 포함	SAVxxx 명령 [1]	RSTxxx 명령 [2]
1차 그룹	오브젝트 포함	SAVxxx 명령 [1]	RSTxxx 명령 [2]
권한 부여 리스트	QSYS 라이브러리	SAVSYS 또는 SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
오브젝트 및 권한 부여 리스트간의 링크	오브젝트 포함	SAVxxx 명령 [1]	RSTxxx 명령 [2]
개별 권한	사용자 프로파일 포함	SAVSYS 또는 SAVSECDTA	RSTAUT

표 64. 자원 보안 정보 저장 및 복원 (계속)

정보 유형	저장 장소	저장 방법	복원 방법

1. SAVOBJ 또는 SAVLIB 명령을 사용하여 대부분의 오브젝트 유형을 저장할 수 있습니다. 구성과 같은 일부 오브젝트 유형에는 특별한 저장 명령이 있습니다.
2. 대부분의 오브젝트 유형은 RSTOBJ나 RSTLIB 명령으로 복원할 수 있습니다. 구성과 같은 일부 오브젝트 유형에는 특별한 복원 명령이 있습니다.

어플리케이션이나 전체 시스템을 회복시켜야 할 경우 오브젝트 권한을 회복시키는 것을 포함하여 각 단계를 신중하게 계획해야 합니다. 다음은 어플리케이션의 자원 보안 정보를 회복할 때 필요한 기본 단계입니다.

1. 필요한 경우 어플리케이션을 소유하는 프로파일을 포함하여 사용자 프로파일을 복원하십시오. RSTUSRPRF 명령을 사용하여 특정 프로파일이나 모든 프로파일을 복원할 수 있습니다.
2. 어플리케이션이 사용하는 모든 권한 부여 리스트를 복원하십시오. RSTUSRPRF USRPRF(*ALL)를 사용하여 권한 부여 리스트를 복원할 수 있습니다.

   주: 이것은 백업 매체에서 암호를 포함하여 모든 사용자 프로파일 값을 복원합니다.
3. RSTLIB 또는 RSTOBJ 명령을 사용하여 어플리케이션 라이브러리를 복원하십시오. 이 작업은 오브젝트 소유권, 공용 권한, 오브젝트와 권한 부여 리스트간의 링크를 회복시킵니다.
4. RSTAUT 명령을 사용하여 오브젝트에 대한 개인 권한을 복원하십시오. 또한 RSTAUT 명령으로 권한 부여 리스트에 대한 사용자 권한을 복원시킬 수 있습니다. 특정 사용자나 모든 사용자에 대한 권한을 복원시킬 수 있습니다.

시스템에 없는 소유자 프로파일과 오브젝트를 복원하는 것에 관한 정보는 ″디폴트 소유자 프로파일(QDFTOWN)사용″을 참조하십시오.

디폴트 소유자 프로파일(QDFTOWN) 사용

시스템에 없는 소유자 프로파일과 오브젝트를 복원할 경우 시스템이 QDFTOWN이라는 디폴트 프로파일에 오브젝트에 대한 소유권을 전송합니다. 일단 소유자 프로파일을 회복하거나 다시 작성했으면 소유자별 오브젝트에 대한 작업(WRKOBJOWN) 명령을 사용하여 소유권을 다시 전송할 수 있습니다.

권한 부여 리스트를 회복시키는 것에 관한 정보는 ″손상된 권한 부여 리스트 회복″을 참조하십시오.

손상된 권한 부여 리스트에서 회복

오브젝트를 보안하는 권한 부여 리스트가 손상되면 모든 오브젝트(*ALLOBJ) 특수 권한이 있는 사용자만 오브젝트에 액세스할 수 있습니다.

손상된 권한 부여 리스트로부터의 회복에는 두 가지 단계가 필요합니다.

1. 권한 부여 리스트에 대한 사용자 및 사용자의 권한을 회복하십시오.
2. 권한 부여 리스트와 오브젝트의 연관성을 회복시키십시오.

*ALLOBJ 특수 권한이 있는 사용자가 다음 단계를 수행할 수 있습니다.

1단계: 권한 부여 리스트 회복

권한 부여 리스트에 대한 사용자 권한을 알면 권한 부여 리스트를 삭제한 후 다시 작성하여 사용자를 추가하십시오.

권한 부여 리스트에 대한 사용자 권한을 알지 못하면 다음 단계를 사용하여 최근 SAVSYS 또는 SAVSECDTA 테이프에서 권한 부여 리스트를 복원하십시오.

1. 손상된 권한 부여 리스트를 삭제하십시오.

   ```
   DLTAUTL AUTL(authorization-list-name)
   ```

2. 권한 부여 리스트를 복원하십시오.

   ```
   RSTUSRPRF USRPRF(*ALL)
   ```

3. RSTAUT(권한 복원) 명령을 사용하여 리스트에 사용자를 추가하십시오.

2단계: 권한 부여 리스트와 오브젝트의 연관성 회복

권한 부여 리스트를 복원하거나 다시 작성했을 경우 리스트로 보안 처리한 오브젝트와 리스트간에 링크를 설정해야 합니다.

1. RCLSTG(기억장치 재생) 명령을 사용하십시오. RCLSTG는 QRCLAUTL이라는 디폴트 리스트에 손상되거나 누락된 권한 부여 리스트로 보안시킨 오브젝트를 할당합니다.
2. QRCLAUTL 권한 부여 리스트로 보안시킨 오브젝트를 나열하십시오.

   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```

3. GRTOBJAUT 명령을 사용하여 올바른 권한 부여 리스트로 오브젝트를 보안시키십시오. 예를 들어, ARLST01 권한 부여 리스트로 CUSTLIB 라이브러리에 있는 ARWRK01 파일을 보안시키려면 다음을 입력하십시오.

   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

제 11 장 보안 모니터링

이 주제는 시스템에 있어서 보안 처리의 효율성을 모니터링하기 위한 기본 제안 사항을 제공합니다.

정기적인 보안 모니터링에는 두 가지의 기본 목적이 있습니다.

- 회사의 자원을 적절히 보호하고 있는지를 확인합니다.
- 권한이 없는 사람들이 시스템 및 회사 정보에 액세스하는지를 감지합니다.

정기적으로 수행해야 하는 모니터링 타스크를 결정할 때 사용자 보안 메모 및 보안 정책 발표문을 검토하십시오.

보안 모니터링에 대한 자세한 정보는 다음 주제를 참조하십시오.

- 보안 모니터링 체크 리스트
- 보안 감사

보안 모니터링 체크 리스트

다음은 시스템에 있어서 보안의 다른 측면을 검토하기 위한 체크 리스트입니다. 계획을 수립할 때 사용하십시오.

물리적 보안 모니터링

- 손상이나 도난으로부터 백업 매체를 보호합니다.
- 공용 장소의 워크스테이션에 대한 액세스를 제한합니다. DSPOBJAUT 명령을 사용하여 워크스테이션에 대해 *CHANGE 권한이 있는 사용자를 확인하십시오.

시스템 값 모니터링

- 설정 값이 시스템 값 선택 양식에 일치하는지 확인하십시오. PRTSYSSECA(시스템 보안 속성 인쇄) 명령을 사용하십시오.
- 특히 신규 어플리케이션을 설치할 때 시스템 값에 대한 결정사항을 검토하십시오.

그룹 프로파일 모니터링

- 그룹 프로파일에 암호가 없는 것을 확인하십시오. DSPAUTUSR 명령을 사용하여 모든 그룹 프로파일이 *NONE 암호를 가지고 있는지 확인하십시오.
- 올바른 사람들이 그룹의 멤버인지 확인하십시오. 그룹의 멤버를 나열하려면 DSPUSRPRF 명령을 *GRPMBR 옵션과 함께 사용하십시오.

- 각 그룹 프로파일에 대해 특수 권한이 있는지 확인하십시오. DSPUSRPRF 명령을 사용하십시오. 30, 40 또는 50의 보안 레벨에서 실행할 경우 그룹 프로파일에 *ALLOBJ 권한이 있어서는 안됩니다.

사용자 프로파일 모니터링

- 시스템의 사용자 프로파일이 다음 범주 중 하나에 속하는지 확인하십시오.
  - 현재 직원들을 위한 사용자 프로파일
  - 그룹 프로파일
  - 어플리케이션 소유자 프로파일
  - IBM 제공 프로파일(Q로 시작)
- 이직이나 퇴사가 발생할 경우 사용자 프로파일을 제거하십시오. CHGEXPSCDE(만기 스케줄 항목 변경) 명령을 사용하여 퇴사와 동시에 자동으로 프로파일을 삭제시키거나 작동 불가능하게 만드십시오.
- 비활동 프로파일을 찾아서 제거하십시오. 일정 시간 동안 비활동 상태로 있었으면 ANZPRFACT(프로파일 활동 분석) 명령을 사용하여 자동으로 프로파일이 작동하지 않게 만드십시오.
- 사용자 프로파일 이름과 같은 암호를 가진 사용자를 판별하십시오. ANZDFTPWD(디폴트 암호 분석) 명령을 사용하십시오. 이 명령의 옵션을 이용하여 사용자들이 다음 번에 시스템에 사인 온할 때 암호를 변경하게 만드십시오.

  주의: 시스템에서 어떤 IBM 제공 프로파일도 제거하지 마십시오. IBM 제공 프로파일은 Q 문자로 시작합니다.
- *USER 이외의 사용자 클래스를 가지고 있는 사람과 그 이유에 유의하십시오. 모든 사용자, 사용자 클래스, 특수 권한에 대한 리스트를 작성하려면 PRTUSRPRF(사용자 프로파일 인쇄) 명령을 사용하십시오. 시스템 책임 양식과 이 정보를 일치시키십시오.
- *기능 제한* 필드가 *NO로 설정되어 있는 사용자 프로파일이 어느 것인지 제어하십시오.

중요한 오브젝트 모니터링

- 누가 중요한 오브젝트에 액세스하는 사람이 누구인지 검토하십시오. 오브젝트를 모니터하려면 PRTPVTAUT(개인 권한 인쇄) 명령 및 PRTPUBAUT(공용 권한 오브젝트 인쇄) 명령을 사용하십시오. 그룹이 액세스를 가지고 있으면 DSPUSRPRF 명령의 *GRPMBR 옵션을 사용하여 그룹 멤버를 확인하십시오.
- 허용된 권한과 같은 기타 보안 방법을 통해 오브젝트에 액세스가 제공되는 어플리케이션 프로그램을 사용할 수 있는 사람들을 확인하십시오. PRTADPOBJ(허용된 오브젝트 인쇄) 명령을 사용하십시오.

권한이 없는 액세스 모니터링

- 시스템 오퍼레이터에게 QSYSOPR 메세지 대기행렬에서 보안 메세지에 주목하도록 지시하십시오. 특히, 반복적인 사인 온 시도 실패의 경우 시스템 오퍼레이터가 보안 담당자에게 통지하게 만드십시오. 보안 메세지는 2200에서 22FF 그리고 4A00에서 4AFF의 범위에 있습니다. 보안 메세지에는 CPF, CPI, CPC, CPD 접두부가 있습니다.
- 오브젝트 액세스에 대한 권한이 없는 시도를 기록하도록 보안 감사를 설정하십시오.

이제 보안 감사를 검토하십시오.

보안 감사

보안을 모니터할 때 오퍼레이팅 시스템이 시스템에서 발생하는 보안 이벤트를 기록합니다. 이 이벤트는 **저널 리시버**라고 하는 특별한 시스템 오브젝트에 기록됩니다. 시스템 값이나 사용자 프로파일의 변경 또는 오브젝트 액세스 실패와 같이 서로 다른 유형의 보안 이벤트를 기록하도록 저널 리시버를 설정할 수 있습니다. 다음 값들이 기록되는 이벤트를 제어합니다.

- 감사 제어(QAUDCTL) 시스템 값
- 감사 레벨(QAUDLVL) 시스템 값
- 사용자 프로파일의 감사 레벨(AUDLVL) 값
- 사용자 프로파일의 오브젝트 감사(OBJAUD) 값
- 오브젝트의 오브젝트 감사(OBJAUD) 값

감사 저널의 정보는 다음 목적에 사용됩니다.

- 보안 위반 시도를 감지하기 위해
- 상위 보안 레벨로 마이그레이션을 계획하기 위해
- 기밀 파일과 같은 민감한 오브젝트를 사용하는 것을 모니터하기 위해

감사 저널의 정보를 여러 가지 방법으로 볼 수 있는 명령들이 있습니다.

제 12 장 기본 시스템 보안 계획 양식

브라우저에서 다음 양식을 복사하거나 인쇄할 수 있습니다.

전체 보안 기본 정보를 인쇄하려면 오른쪽 분할 창을 선택한 후 Information Center 표제에서 PDF 아이콘을 클릭하십시오.

하나의 계획 양식을 인쇄하려면 인쇄하려는 계획 양식에 해당하는 링크를 클릭하십시오. 오른쪽 분할창을 클릭한 후 브라우저에서 인쇄 아이콘을 클릭하십시오. 이렇게 하면 선택한 양식이 인쇄됩니다.

다음은 기본 시스템 보안을 계획하고 사용하는 데 필요한 모든 계획 양식의 전체 리스트입니다.

- 물리적 보안 계획 양식
- 어플리케이션 설명 양식
- 명명 규칙 양식
- 라이브러리 설명 양식
- 시스템 값 선택 양식
- 시스템 책임 양식
- 사용자 그룹 식별 양식
- 사용자 그룹 설명 양식
- 개별 사용자 프로파일 양식
- 권한 부여 리스트 양식
- 출력 대기행렬 및 워크스테이션 보안 양식
- 어플리케이션 설치 양식

물리적 보안 계획 양식

표 65. 물리적 보안 계획 양식

물리적 보안 계획 양식	
작성자:	날짜:
지침 • "자원 보안 계획"에서 이 양식에 관해 알아보십시오. • 시스템 장치 및 접속된 장치의 물리적 위치와 관련된 모든 보안 문제를 설명할 때 이 양식을 사용하십시오. • 이 양식에 있는 정보는 시스템에 입력하지 않아도 됩니다.	
시스템 장치:	

표 65. 물리적 보안 계획 양식 (계속)

시스템 장치를 보호하기 위한 보안 조치(예: 잠금 장치가 설치된 방)를 서술하십시오.	
일반적으로 사용하는 키 잠금 위치는 무엇입니까?	
키를 보관하는 곳은 어디입니까?	
시스템 장치와 관련된 기타 주석:	
백업 매체 및 문서:	
사무실의 어느 곳에 백업 테이프를 저장합니까?	
사무실과 떨어진 어느 곳에 백업 테이프를 저장합니까?	
보안 담당자, 서비스, DST 암호를 어디에 보관합니까?	
일련 번호나 구성과 같은 중요한 시스템 문서를 어디에 보관합니까?	

물리적 보안 계획 양식			파트 2의 2
파트 2에 대한 추가 지침 • 보안을 노출시킬 가능성이 있는 장소의 모든 워크스테이션이나 프린터를 아래에 나열하십시오. 적용시킬 보호 조치를 표시하십시오. 프린터의 경우 *보안 노출* 열 아래에 기밀이 담긴 인쇄 보고서의 예를 나열하십시오. • 시스템이 자동으로 로컬 장치를 구성하도록 허용할 경우 시스템을 설치하기까지 워크스테이션이나 프린터의 이름을 모를 수 있습니다. 이 양식을 준비할 때 이름을 모르면 설명(위치와 같은)을 기록했다가 나중에 이름을 추가하십시오.			
워크스테이션 및 프린터의 물리적 보안			
워크스테이션 또는 프린터 이름	위치 또는 설명	보안 노출	적용시킬 보호 조치

어플리케이션 설명 양식

표 66. 어플리케이션 설명 양식

어플리케이션 설명 양식	
작성자:	날짜:
지침 • "어플리케이션 설명" 및 "자원 보안 계획"에서 이 양식에 관해 알아보십시오. • 각 어플리케이션을 위한 분리 양식을 준비하십시오. • 이 양식에 나오는 정보는 시스템에 입력하지 않아도 됩니다.	
어플리케이션 이름:	약어:
어플리케이션에 대한 간단한 설명:	
1차 메뉴 이름:	라이브러리:

표 66. 어플리케이션 설명 양식 (계속)

초기 프로그램 이름:	라이브러리:
파일 및 프로그램을 위해 어플리케이션이 사용하는 라이브러리 나열:	
어플리케이션에 대한 보안 목적 정의(예: 기밀 정보 여부 판별):	

명명 규칙 양식

표 67. 명명 규칙 양식

명명 규칙 양식	
작성자:	날짜:
지침 • "어플리케이션 설명"에서 이 양식에 관해 알아보십시오. • 이 양식에서 나온 정보는 시스템에 입력하지 않아도 됩니다. • 시스템의 오브젝트에 이름을 할당할 방법을 설명할 때 이 양식을 사용하십시오. 각각에 대해 예를 제공하십시오.	
오브젝트 유형	**명명 규칙**
그룹 프로파일	
사용자 프로파일	
권한 부여 리스트	
라이브러리	
파일	
캘린더	
장치	
테이프	

라이브러리 설명 양식

표 68. 라이브러리 설명 양식

라이브러리 설명 양식	파트 2의 1
작성자:	날짜:
지침: • "사용자 보안 계획" 및 "자원 보안 계획"에서 이 양식에 관해 알아보십시오. • 기본 라이브러리를 설명하고 그에 대한 자원 보안 요구사항을 정의할 때 이 양식을 사용하십시오. • 시스템에 있는 주요 어플리케이션 라이브러리별로 하나의 양식을 채우십시오. • "자원 보안 설정"에서 이 양식에 정보를 입력하는 방법을 알아보십시오.	
라이브러리 이름:	설명(텍스트):
이 라이브러리의 기능을 간단히 서술하십시오.	
라이브러리에 대한 보안 목적 정의(예: 기밀 정보 여부 판별):	
라이브러리의 공용 권한:	
라이브러리내 오브젝트의 공용 권한:	
신규 오브젝트의 공용 권한(CRTAUT):	

표 68. 라이브러리 설명 양식 (계속)

라이브러리 소유자:	

라이브러리 설명 양식				파트 2의 2
작성자:			날짜:	
라이브러리 이름:				
파트 2에 대한 추가 지침: • 아래 도표에 특정 권한을 필요로 하는 모든 개인이나 오브젝트를 나열하십시오. • 필요한 권한 유형(*ALL, *CHANGE, *USE 또는 *EXCLUDE)을 지정하십시오.				
라이브러리 오브젝트를 위한 특정 권한을 나열하십시오.				
그룹 프로파일 또는 사용자 프로파일	오브젝트 이름	오브젝트 유형	필요한 권한	권한 부여 리스트

시스템 값 선택 양식

표 69. 시스템 값 선택 양식

시스템 값 선택 양식		파트 2의 1
작성자:		날짜:
지침 • "종합적인 접근방식 계획"에서 이 양식에 관해 자세히 알아보십시오. • 보안 및 사용자 정의에 영향을 미치는 시스템 값의 선택사항을 기록할 때 이 양식을 사용하십시오. • 이 양식의 파트 1을 입력하려면 설정 메뉴에서 옵션 **1**을 사용하십시오.		
시스템 옵션 변경 화면의 값		
시스템 값/네트워크 속성	**권장 선택사항**	**사용자 선택사항**
시스템 이름		
날짜 분리자(QDATSEP)		
날짜 형식(QDATFMT)		
시간 분리자(QTIMSEP)		
신규 장치를 위한 장치 명명 형식 (QDEVNAMING)	1(iSeries 시스템)	
시스템 프린터(QPRTDEV)		
보안 레벨(QSECURITY)	40	
보안 담당자에게 모든 표시장치에 대한 사인 온 허용(QLMTSECOFR)	N	

표 69. 시스템 값 선택 양식 (계속)

완료된 프린터 출력에 관한 작업 계정 정보 저장(QACGLVL)	N(*NONE)	

시스템 값 선택 양식		파트 2의 2
파트 2에 대한 추가 지침 • "시스템 값 설정"에서 이 양식의 파트 2에 관해 자세히 알아보십시오. • 파트 2를 입력하려면 WRKSYSVAL(시스템 값에 대한 작업) 명령을 사용하십시오.		
보안 시스템 값		
시스템 값	**권장 선택사항**	**사용자 선택사항**
비활동 작업 시간 종료 간격 (QINACTITV)	30에서 60	
비활동 작업 메세지 대기행렬 (QINACTMSGQ)	*DSCJOB	
장치 세션 제한(QLMTDEVSSN)	1(YES)	
실패한 사인 온 시도에 대해 취할 조치 (QMAXSGNACN)	3(양쪽 모두 작동 불가능)	
최대한 허용되는 사인 온 시도 횟수 (QMAXSIGN)	3에서 5	
암호 만기 간격(QPWDEXPITV)	30에서 60	
암호의 최대 길이(QPWDMAXLEN)	8	
암호의 최소 길이(QPWDMINLEN)	6	
다른 암호 요구(QPWDRQDDIF)	7(6개의 고유 암호)	
다른 시스템 값		
시스템 값	**권장 선택사항**	**사용자 선택사항**
단절된 작업 시간 종료 간격 (QDSCJOBITV)	300	
주: 보안과 관련된 기타 시스템 값을 설정하려는 경우가 있습니다. 이 때에는 *보안 참조서*(SA30-0237-04)의 제 3 장에서 보안에 관계된 시스템 값 및 그에 대한 권장사항의 전체 리스트를 참조하십시오.		

시스템 책임 양식

표 70. 시스템 책임 양식

시스템 책임 양식	
작성자:	날짜:
지침: • "개별 사용자 프로파일 계획"에서 이 양식에 관해 알아보십시오. • *USER 이외의 사용자 클래스를 가진 사람들을 나열할 때 이 양식을 사용하십시오. • 이 양식에서 나온 정보를 개별 사용자 프로파일 양식의 *사용자 클래스* 열로 전송하십시오.	
1차 보안 담당자는 누구입니까? 백업 보안 담당자는 누구입니까?	

표 70. 시스템 책임 양식 (계속)

프로파일 이름	사용자 이름	클래스	주석

사용자 그룹 식별 양식

표 71. 사용자 그룹 식별 양식

사용자 그룹 식별 양식								
작성자:		날짜:						
지침: • "사용자 그룹 계획"에서 이 양식에 관해 알아보십시오. • 이 양식은 유사한 어플리케이션을 필요로 하는 사용자 그룹을 식별할 때 도움이 됩니다. 1. 주요 어플리케이션을 양식의 맨 위에 가로로 나열하십시오. 2. 사용자를 왼쪽 열에 나열하십시오. 3. 모든 사용자별로 필요한 어플리케이션을 표시하십시오. • 이 양식에 나오는 정보는 시스템에 입력하지 않아도 됩니다.								
		어플리케이션에 필요한 액세스						
사용자 이름	부서	APP:	APP:	APP:	APP:	APP:	APP:	APP:
주: • *저(relaxed)* 상태의 보안 환경에서는 사용자가 필요로 하는 어플리케이션에 **X** 표시를 하십시오. • *고(strict)* 상태의 보안 환경에서는 **C**(변경)와 **V**(보기)를 표시하여 어플리케이션이 사용되는 *방법*을 지정할 수 있습니다.								

사용자 그룹 설명 양식

표 72. 사용자 그룹 설명 양식

사용자 그룹 설명 양식	파트 2의 1
작성자:	날짜:

표 72. 사용자 그룹 설명 양식 (계속)

파트 1에 대한 지침 • "사용자 그룹 계획"에서 이 양식을 준비하는 방법에 관해 알아보십시오. • "사용자 보안 설정"에서 이 양식을 입력하는 방법에 관해 알아보십시오. • 시스템을 사용할 각 그룹에 대해 별도의 양식을 준비하십시오. • 그룹을 위한 작업 설명을 작성하려면 CRTJOBD(작업 설명 작성) 명령을 사용하십시오. 작업 설명에는 그룹의 초기 라이브러리 리스트가 있습니다.
그룹 프로파일 이름: 그룹 설명:
그룹에 대한 1차 어플리케이션: 그룹이 필요로 하는 다른 어플리케이션 나열:
그룹에 필요한 각 라이브러리를 나열하십시오. 그룹을 위한 초기 라이브러리 리스트에 있어야 할 각 라이브러리를 표시(✓)하십시오.
주: 어플리케이션이 어떤 라이브러리를 사용하는지 알아보려면 이전 섹션에 나오는 각 어플리케이션을 위한 어플리케이션 설명 양식을 보십시오.

사용자 그룹 설명 양식		파트 2의 2
파트 2에 대한 추가 지침 • 아래 표는 사용자 프로파일 작성 화면에 나오는 모든 필드를 나열한 것입니다. 각 필드는 사용자가 선택해야 할 부분과 IBM이 디폴트 값으로 권장하는 부분의 두 그룹으로 나누어집니다. • 양식에 있는 정보를 시스템에 입력하려면 사용자 프로파일에 대한 작업 화면이나 사용자 프로파일 작성(CRTUSRPRF) 명령을 사용하십시오.		
그룹 프로파일에서 다음 필드를 위한 값을 선택하십시오.		
필드 이름	**권장 선택사항**	**사용자 선택사항**
그룹 프로파일 이름(사용자)		
암호	*NONE	
사용자 클래스(사용자 유형)	*USER	
현재 라이브러리(디폴트 라이브러리)	*그룹 프로파일 이름과 같음*	
호출할 초기 프로그램(사인 온 프로그램)		
초기 프로그램 라이브러리		
초기 메뉴(첫 번째 메뉴)		
초기 메뉴 라이브러리		
기능 제한(제한적인 명령행 사용)	*YES	
텍스트(사용자 설명)		
작업 설명	*그룹 프로파일 이름과 같음*	
작업 설명 라이브러리		
그룹 프로파일 이름(사용자 그룹)	*NONE	
인쇄 장치(디폴트 프린터)		
출력 대기행렬	*DEV	
주: 다음 필드는 사용자 프로파일 작성 화면(F4 사용)에 나오는 순서로 배열한 것입니다.		

아래 필드의 경우 시스템 제공 값(디폴트)을 사용하십시오.		
계정 코드	키보드 버퍼링	공용 권한
지원 레벨	언어 ID	암호 만기 설정
어텐션 프로그램	장치 세션 제한	정렬 순서
코드화 문자 세트 ID	최대 기억장치	특수 권한
국가 및 영역 ID	메세지 대기행렬	특수 환경
표시장치 사인 온 정보	암호 만기 간격	상태
문서 암호	우선순위 한계	사용자 옵션
주: 다음 리스트의 필드는 알파벳 순서로 정렬한 것입니다.		

개별 사용자 프로파일 양식

표 73. 개별 사용자 프로파일 양식

개별 사용자 프로파일 양식						
작성자:			날짜:			
지침: • "개별 사용자 프로파일 계획"에서 이 양식을 준비하는 방법에 관해 알아보십시오. • 개별 시스템 사용자에 대한 정보를 기록할 때 이 양식을 사용하십시오. 시스템에 있는 각 사용자 그룹(그룹 프로파일)별로 하나의 양식을 채우십시오. • 개별 사용자를 위해 지정하려는 추가 필드에 대해서는 오른쪽에 나오는 공백 열을 사용하십시오. • "개별 사용자 설정"에서 이 양식에 입력하는 방법에 관해 알아보십시오.						
그룹 프로파일 이름:						
작성된 오브젝트의 소유자:			작성된 오브젝트의 그룹 권한:			
그룹 권한 유형:						
그룹의 각 멤버별로 항목 작성:						
사용자 프로파일	텍스트(설명)	사용자 클래스	기능 제한			

권한 부여 리스트 양식

표 74. 권한 부여 리스트 양식

권한 부여 리스트 양식

표 74. 권한 부여 리스트 양식 (계속)

작성자:	날짜:
지침 • "자원 보안 계획"에서 이 양식에 관해 알아보십시오. • 권한 부여 리스트별로 하나의 양식을 준비하십시오. • 보안시킨 리스트에 대해 액세스를 가진 리스트와 그룹 및 개별 오브젝트를 나열할 때 이 양식을 사용하십시오. • "자원 보안 설정"에서 이 양식에 입력하는 방법을 알아보십시오.	
권한 부여 리스트 이름:	
설명:	
리스트로 보안시킨 오브젝트를 나열하십시오.	

오브젝트 이름	오브젝트 유형	오브젝트 라이브러리	오브젝트 이름	오브젝트 유형	오브젝트 라이브러리

리스트에 대해 액세스를 가진 그룹 및 사용자 나열

그룹 또는 사용자	허가된 액세스 유형	리스트 관리?	그룹 또는 사용자	허가된 액세스 유형	리스트 관리?

프린터 출력 대기행렬 및 워크스테이션 보안 양식

표 75. 프린터 출력 대기행렬 및 워크스테이션 보안 양식

프린터 출력 대기행렬 및 워크스테이션 보안 양식	
작성자:	날짜:
지침 • "프린터 출력 보호"에서 이 양식에 관해 알아보십시오. • 특별한 보호를 필요로 하는 모든 워크스테이션이나 출력 대기행렬의 경우 이 양식에 항목을 작성하십시오. • "워크스테이션 보호"에서 이 양식에 입력하는 방법을 알아보십시오.	
제한적인 출력 대기행렬의 매개변수 나열:	

표 75. 프린터 출력 대기행렬 및 워크스테이션 보안 양식 (계속)

출력 대기행렬 이름	출력 대기행렬 라이브러리	모든 파일 표시 (DSPDTA)	검사 권한(AUTCHK)	오퍼레이터 제어 (OPRCTL)

보안 담당자 워크스테이션:

보안 담당자를 특정 워크스테이션(QLMTSECOFR 시스템 값이 '예'일 경우)으로 제한할 경우 보안 담당자에게 권한이 있는 워크스테이션 및 *ALLOBJ 권한이 있는 모든 사용자를 아래에 나열하십시오.

제한된 워크스테이션을 위한 권한을 아래 리스트에 나열하십시오.

워크스테이션 이름	권한이 있는 그룹 또는 사용자(*CHANGE 권한)

주: 제한적인 워크스테이션에는 공용 권한을 *EXCLUDE로 설정해야 합니다.

어플리케이션 설치 양식

표 76. 어플리케이션 설치 양식

어플리케이션 설치 양식		파트 2의 1
작성자:		날짜:

지침

- "어플리케이션 설치 계획"에서 이 양식에 관해 알아보십시오.
- 설치할 각 어플리케이션별로 하나의 양식을 준비하십시오.
- 어플리케이션을 로드한 후 어플리케이션에 소유권 및 공용 권한을 설정할 방법을 계획할 때 이 양식을 사용하십시오.
- "자원 보안 설정"에서 이 양식에 입력하는 방법을 알아보십시오.

어플리케이션 이름:		
설명:		
어플리케이션에 필요한 프로파일 나열 및 설명:		
라이브러리 이름:		
	설치 전	설치 후
라이브러리 소유자		
오브젝트 소유자		
라이브러리 공용 권한		
오브젝트 공용 권한		
신규 오브젝트를 위한 공용 권한		
라이브러리 이름:		
	설치 전	설치 후
라이브러리 소유자		
오브젝트 소유자		

표 76. 어플리케이션 설치 양식 (계속)

라이브러리 공용 권한		
오브젝트 공용 권한		
신규 오브젝트를 위한 공용 권한		

어플리케이션 설치 양식		파트 2의 2
라이브러리 이름:		
	설치 전	설치 후
라이브러리 소유자		
오브젝트 소유자		
라이브러리 공용 권한		
오브젝트 공용 권한		
신규 오브젝트를 위한 공용 권한		
라이브러리 이름:		
	설치 전	설치 후
라이브러리 소유자		
오브젝트 소유자		
라이브러리 공용 권한		
오브젝트 공용 권한		
신규 오브젝트를 위한 공용 권한		
라이브러리 이름:		
	설치 전	설치 후
라이브러리 소유자		
오브젝트 소유자		
라이브러리 공용 권한		
오브젝트 공용 권한		
신규 오브젝트를 위한 공용 권한		

Printed in U.S.A