CATIAデータセキュリティ

－ データセキュリティシステムのご紹介 -

2006年9月1日

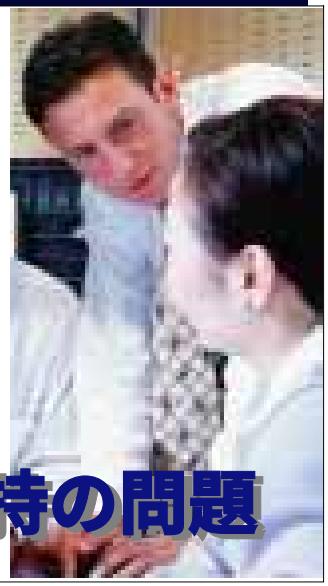
株式会社ダイゾー
情報システム事業部

DAIZO

エンジニアリングの課題

分散エンジニアリング

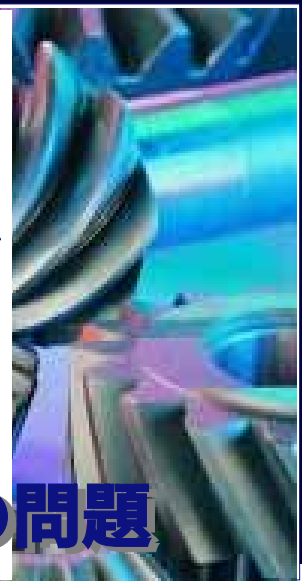
- パートナー間、サプライヤー・OEM間などの協業による様々な技術情報交換の必要性
- サプライヤ側におけるデータの再利用



データ機密保持の問題

製品がさらに複雑に

- 複数の派生ごとの設計の考慮の必要性
- 少量多品種生産と製品サイクルの短命化
- 製品成果物の評価の困難さ



ノウハウ混入の問題

コストへの圧力

- 外注の依存度の高さ
- 更なる設計データ再利用への要求
- フルデジタルモックアップへの要求

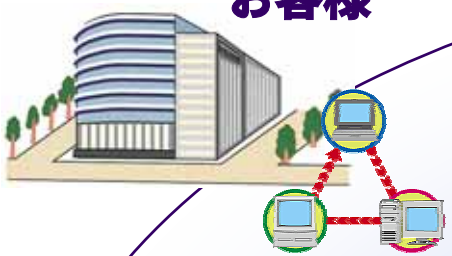
データ再利用の問題

設計環境の複雑化

- コンカレント作業プロセス
- グローバリゼーション（世界的対応）の必要性
- 単純な設計データだけではない情報の取り扱いの難しさ

情報管理の問題

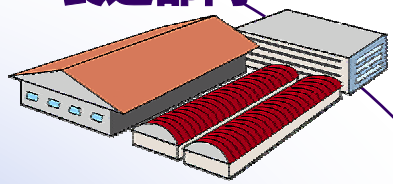
エンジニアリング全体のプラットフォーム



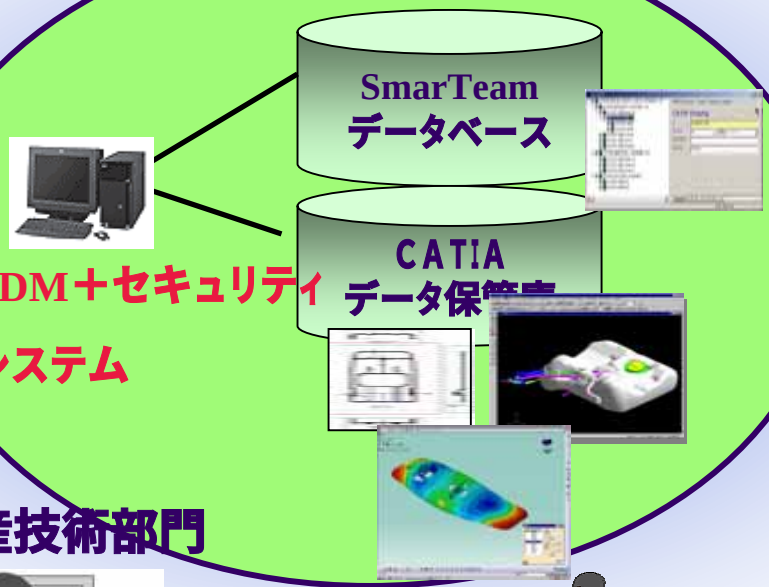
お客様

企画部門

保全部門



製造部門



営業部門

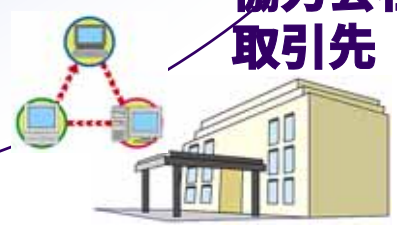
生産管理部門

設計部門

生産技術部門

購買部門

協力会社
取引先



DAIZO

ＣＡＴＩＡデータセキュリティ

DAIZO

現代のビジネス環境

- **現代のビジネスに求められる条件**
  - **ビジネスのスピード**
    - 現在のビジネスではスピードが要求されています。そのためには、ビジネスの参加メンバー同士のコミュニケーションを速く、緊密に行う必要があります。それはプロジェクト内メンバー間、バイヤー⇔サプライヤー間、または社内外を問わないコミュニケーションです。
  - **電子化による情報共有**
    - 今までの紙データを電子データにして取り扱いやすくし、情報の共有や有効利用を図ることが当たり前になってきています。その対象には例外はなく、最近では基幹データも電子データとして簡単に取り出す仕組みが構築されつつあります。
    - 3次元モデルや音声などいろいろなデータを共有することでより精度の高い情報交換が可能になってきました。

DAIZO

データセキュリティの必要性 (1)

- **情報は守るべき重要な資産**
  - **情報は企業の資産**
    - 情報 (データ) にはいろんなものがあります。
    - ものを作るためのアイデアやノウハウ、製品やサービスにまつわるお金の情報または社員やお客様の個人情報まで企業のデータはどれをとっても重要なもので、これは「**情報資産**」といえます。
    - 資産である「ひと・もの・かね」に保険や防犯対策をとるように「情報」にも対策が必要です。
  - **CATIAデータは重要な資産のひとつ**
    - 特許に何億もの価値が取り沙汰されるようにアイデアは重要なデータといえます。
    - アイデアの詰まったCATIA**データは企業のライフライン**です。

DAIZO

データセキュリティの必要性 (2)

- なぜデータセキュリティは必要なのか？
  - 外部からの侵入者 (クラッカー)
    - 先ほどもあげたように、電子メールやインターネットの普及はいまや一般的なものとなっています。最近はこの電子メールなどを仲介としたウィルス、ワームが問題としてあげられています。
    - インターネットは便利さと引き換えに社内のネットワークに外から侵入するための扉をつけてしまいました。外部の侵入者はこの扉からいろんな方法で侵入・破壊を企んでおり、企業の重要なデータが危険に晒されています。
  - 内部からの情報漏洩
    - いろんな情報が電子データとしてアクセスできてしまうがため、意図する・しないに係わらず内部の人間が機密データの漏洩者となってしまうことが今問題となっています。ニュースで問題となっている個人情報の漏洩など枚挙に暇がありません。

社内外で情報共有化で、守らないといけないデータが危険に晒される今、データセキュリティを考えることは重要です。

DAIZO

CATIAデータのセキュリティに対する実際

- **セキュリティの重要性に対しての実際は？**
  - **設計データにおける設計者の認識（モラル）**
    - 「気になっているが今は問題が起こっていないし。。。」
    - 「セキュリティは大事だが操作性が下がるのはいや。」
  - **ツールの機能不足**
    - ライセンスの管理はしっかりしているが、それは認証などといったセキュリティの観点ではありません。
    - PDMなどの普及でデータの管理は行われるようになってはきたが、あくまでもファイルや属性データの管理だけ。ツールさえあれば誰でも参照はできてしまいます。

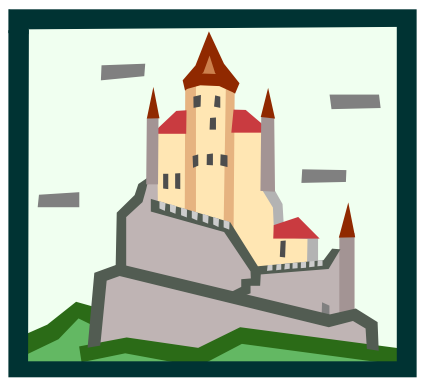
このままでは大事な情報資産が漏洩するかも？

DAIZO

データセキュリティを守るために

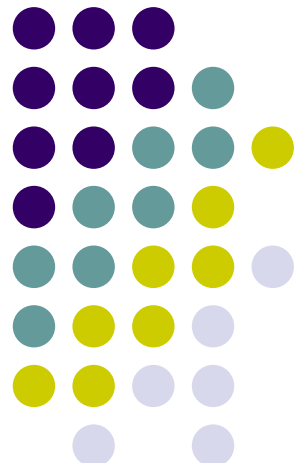
- いまこそCATIAデータにもセキュリティを
  - 安全でオープンなリアルタイムコミュニケーションのために
    - スピードが要求される今、オープンな環境のインターネットや電子メールを利用したビジネスプロセスは必須です。
    - 一方、情報（データ）は資産です。安全に守られなければなりません。

安全なシステムを構築し、データのセキュリティを守りましょう！



DAIZO

セキュリティ実現の方法



DAIZO

認証によるデータセキュリティ

- **情報を保護するための電子認証**

  データの不正な利用としてなりすましや盗聴、改竄などがあげられます。これを防ぐには「認証」や「暗号化」などを技術駆使して対抗する必要があります。この暗号化や認証を実現する「電子認証」の仕組みを使ってデータのセキュリティ実現を検討します。

  - **認証方法　3つの種類**
    - 本人が知っている「情報」を基に認証（パスワードなど）
    - 本人が持っている「もの」を基に認証（ICカード、トークンデバイスなど）
    - 本人の「生体情報」を基に認証（バイオメトリックス）
  - **各認証方法の特徴を次から示します**

DAIZO

パスワード認証を使ったセキュリティ

- **パスワード認証**

  パスワードによる個人の認証を行います。席を離れるときのＰＣのロック／解除や暗号・復号時にはパスワードを用います。

  - **長所**
    - **操作がわかりやすく広く普及しています。**
    - **仕組みは比較的安価に実現できます。**

  - **短所**
    - **パスワードは推測されやすいパスワードなどでセキュリティが甘くなってしまいがちです。**
    - **セキュリティを保つためには長いパスワードが必要ですが、ユーザーへの負担が大きくなります。**
    - **パスワードがきちんと管理されているかどうかの確認が大変です。（システム管理者への負担増）**

DAIZO

トークン認証を使ったセキュリティ

- **トークン認証**

  ハードウエアキー*による個人の認証を行います。席を離れるときのＰＣのロック／解除や暗号･復号時にはセキュリティデバイスを用います。

  - **長所**
    - 操作がわかりやすい。
    - ユーザーは長いパスワードを覚える必要はありません。
  - **短所**
    - ユーザー毎にセキュリティデバイスが必要で、数が多いと高価なシステムになります。
    - 紛失、置忘れや盗難などで再発行が頻繁に必要となります。

USBトークンの例。

*ソフトウエアトークンもありますが暗号キーが端末の中に保存されるため、ハードウエアトークンに比べ、セキュリティがやや甘くなります。（例えばPC自身を取られてしまうなど。）

DAIZO

生体認証（指紋認証）を使ったセキュリティ

- **生体認証**

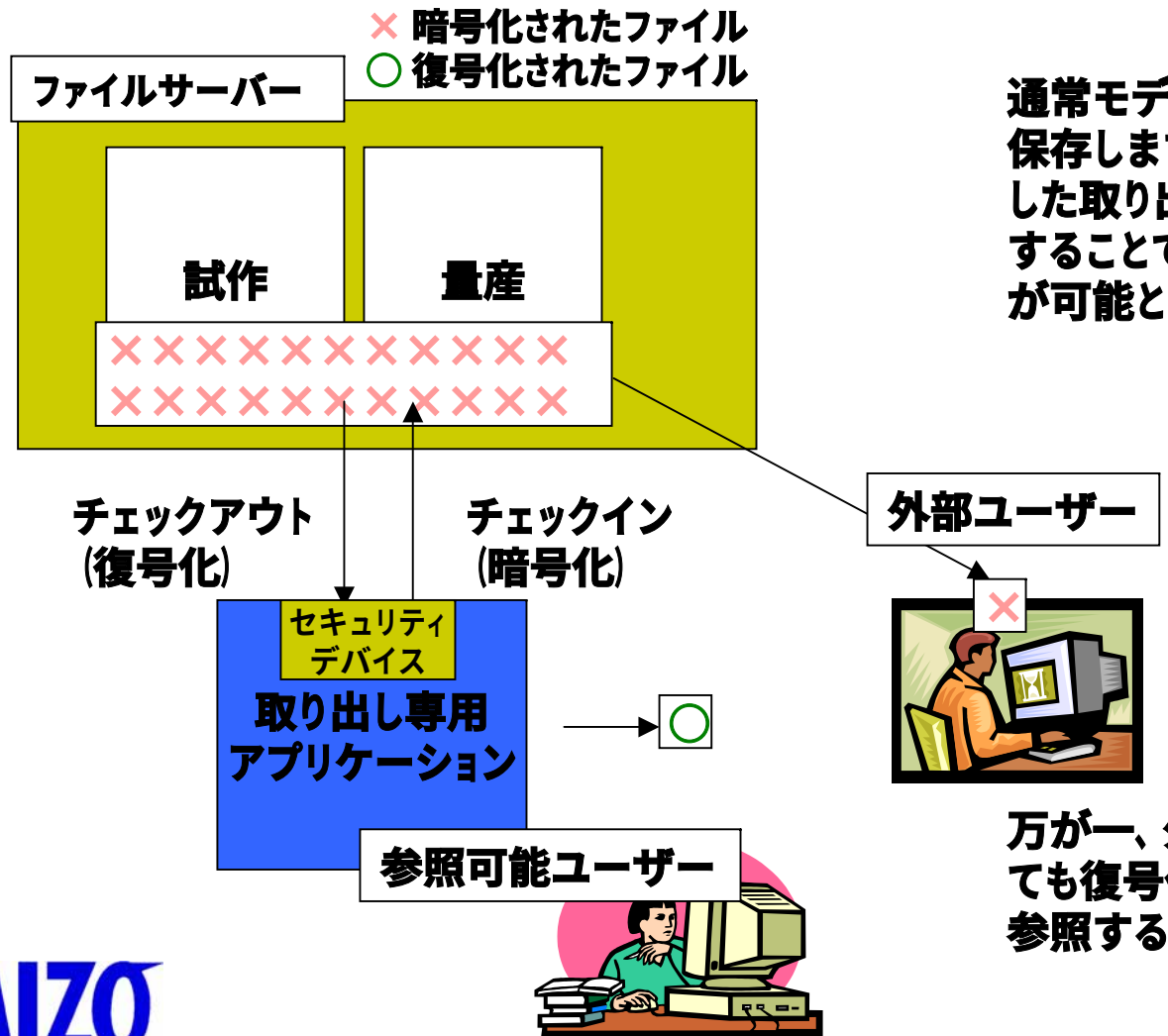
  指紋などによる個人の認証を行います。席を離れるときのＰＣのロック／解除や暗号・復号時にはにはセキュリティデバイスを用います。

  - **長所**
    - 認証の操作がわかりやすい。
    - ユーザーはなにも覚える必要はありません。
  - **短所**
    - 他の認証システムに比べ高価です。
    - ユーザーは事前登録が必要、登録方法はやや難しいです。
    - 認識できないユーザーのために別途方法を用意する必要があります。

指紋データは可逆性がありませんので指紋データも解析されません。

DAIZO

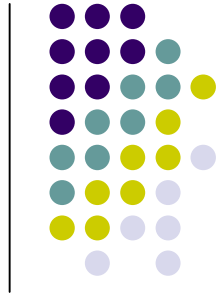
CATIAデータセキュリティのシステムイメージ



通常モデルデータは暗号化された状態で保存します。セキュリティデバイスを利用した取り出し専用アプリケーションを利用することで特定のクライアントでのみ参照が可能となります。

万が一、外部ユーザーにファイルが渡っても復号化するための暗号キーがないと参照することはできません。

DAIZO



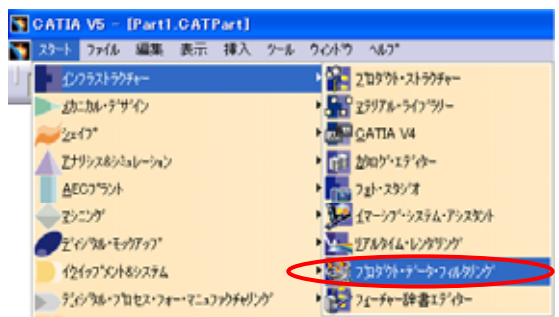
モデル内の情報への対応
Product Data Filtering

DAIZO

プロダクト・データ・フィルタリング (DF1)

- サププライヤなどとデータを交換する時に、モデルに組み込まれたパラメータ・式・注釈などのノウハウを保護するためのフィルター機能を提供するCATIAモジュールです。

- パートモデル・プロダクトモデルから、ノウハウにフィルターをかけたCATPartファイルを出力データとして作成できます。



システム･イメージ

DAIZO

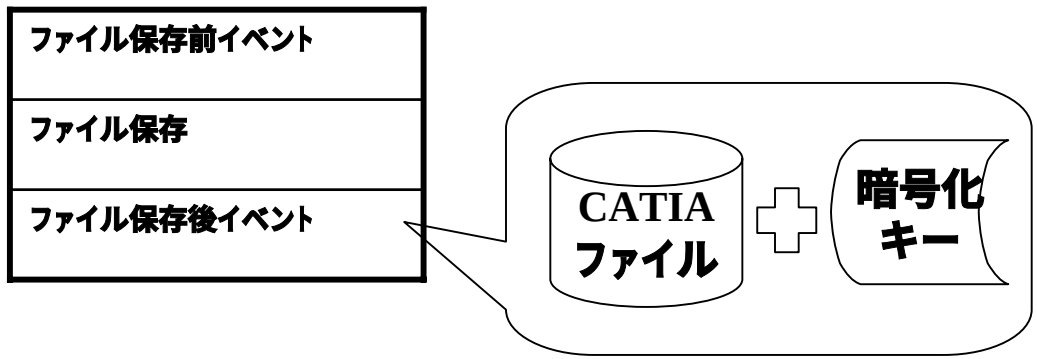
CATIAモデル･セキュリティソリューションの概略

- CATIAモデルに対して。。。。
- 特定のクライアントのみで参照/編集したい。
  - ここまでは、割と簡単！
- ただし、特別なキーを与えると、他のクライアントでも参照/編集可能
  - 送った先では、フリーでいいの？
    - 電子透かしなどの技術

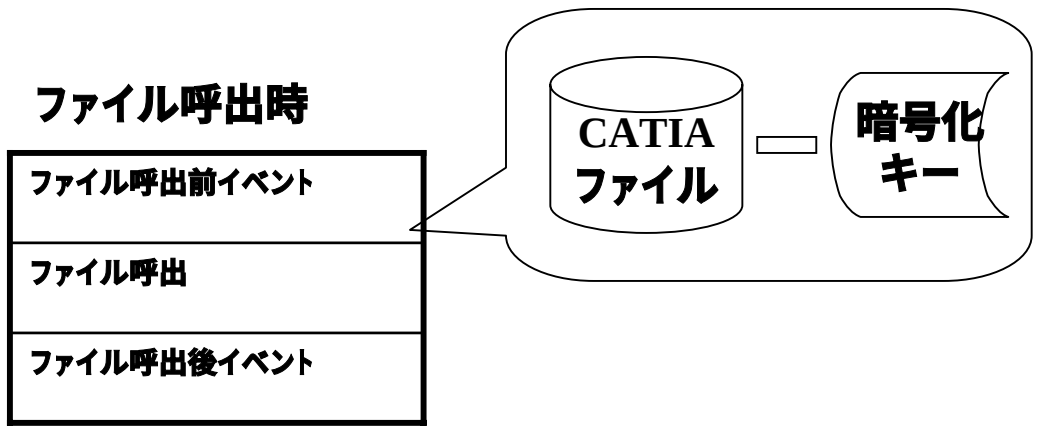
※ポイント
･暗号化キーの生成方法
･暗号化キーの管理方法
･CATIA独特のデータ保持要領

CATIAおよび、SmaTermで以下の処理を組み込み

ファイル保存時

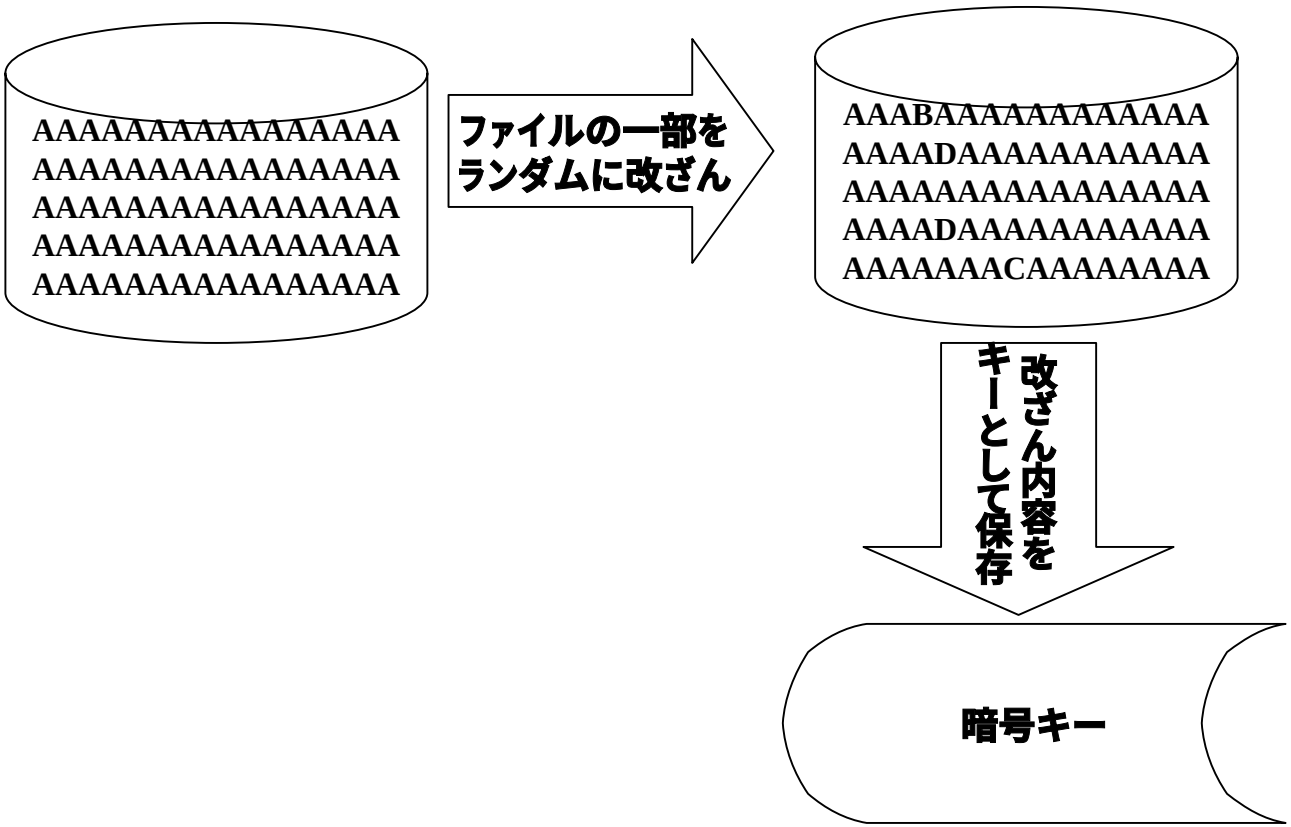


ファイル呼出時



DAIZO

暗号化のイメージ



一般的な暗号化のイメージは上記のとおりです。

図中の「暗号キー」をのひとつ、「指紋認証」技術を用いて構築する例を次のページに示します。

DAIZO

システム構築インプリ例

× 暗号化されたファイル
○ 復号化されたファイル

VOLTServer

試作

量産

.model

.xvl

.JPEG

チェックアウト
(復号化)

チェックイン
(暗号化)

オリジナル
SmarTeam
クライアント

構成ツリー

パーツA

パーツB

参照可能ユーザー

外部ユーザー

モデルデータは暗号化された状態で保存します。指紋認証デバイス*を用いて作成された専用SmarTeamクライアントでのみ復号化が可能となります。

指紋認証
デバイス

万が一、外部ユーザーにファイルが渡っても復号化するための暗号キーがないと参照することはできません。

*セキュリティデバイスは指紋認証キーのほかUSBトークンや、SecurIDなどが考えられます。

DAIZO

まとめ

- CATIAデータは、重要な資産である。
- PDMを中核にセキュアなグローバル・エンジニアリングが有効。
- 豊富な経験と実績を活かします。
- DAIZOは、皆様のセキュリティシステム構築のお手伝いをさせていただきます。

ご清聴ありがとうございました。

DAIZO