電子コンテンツの不正利用とその対策

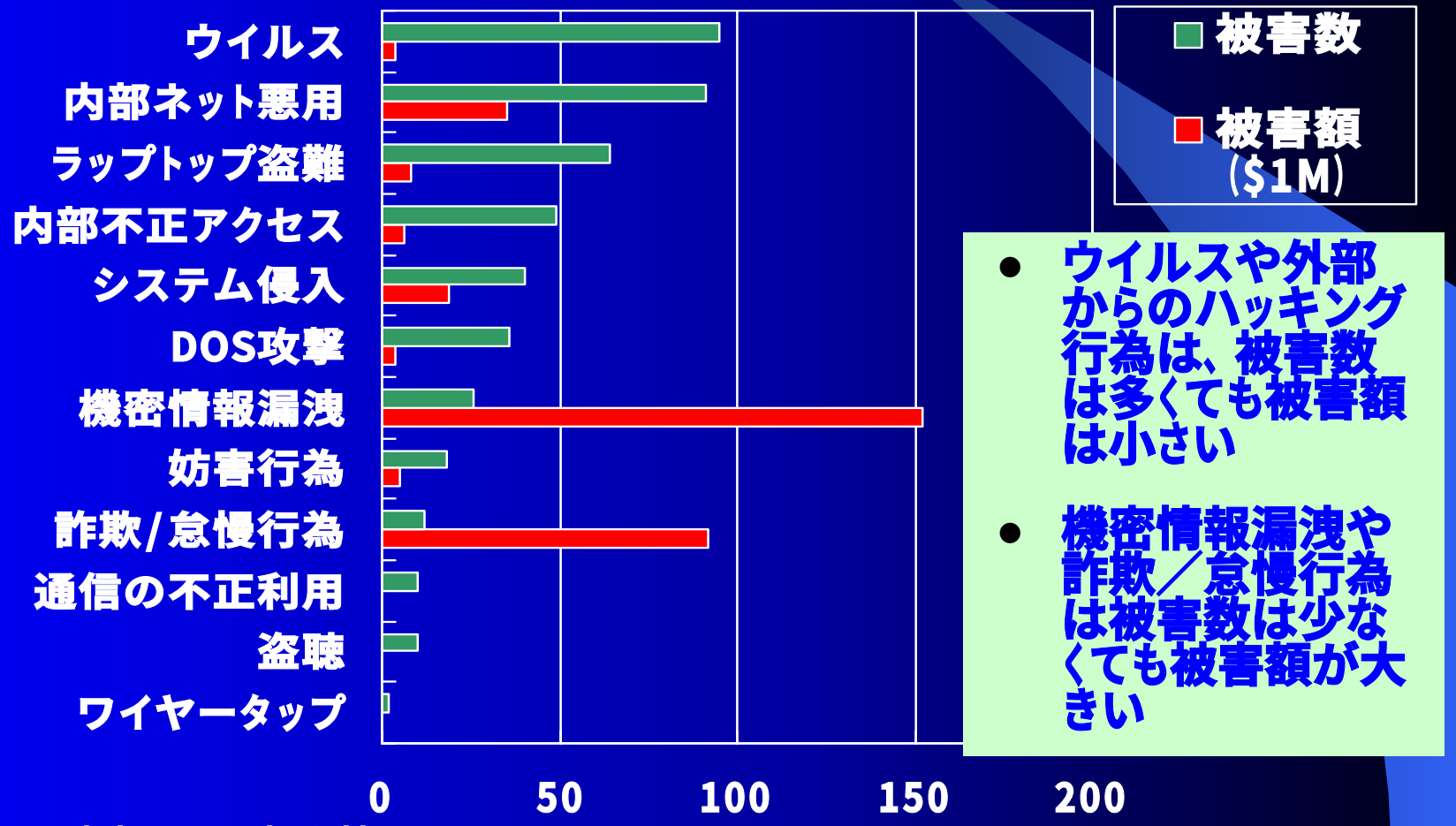
株式会社アークン
渡部　章

市場　(デジタル・コンテンツの氾濫)

- マルチメディア系コンテンツ配信ビジネス（BtoC)
  - ビデオ、音楽、写真、電子書籍
  - 配信方法
    - ストリーミング　(ADSL等によるブロードバンドで加速)
    - ファイル・ダウンロード
    - パッケージ配布
- 組織内、組織間における情報交換（BtoB)
  - 契約書、技術情報、顧客情報、マルチメディア
  - 配信方法
    - 社内ＬＡＮ　(ファイル・ダウンロード、イントラWeb)
    - インターネット　(メール、ファイル転送、Web、VPN)
- IT書面一括法／電子政府への対応

米国：被害数と被害額の実態

出典：米国 CSI/FBI 2001 Computer Crime and Security Survey　調査数：534社



- ウイルスや外部からのハッキング行為は、被害数は多くても被害額は小さい
- 機密情報漏洩や詐欺／怠慢行為は被害数は少なくても被害額が大きい

国内情報漏洩事件

出典：各新聞より

■内部犯罪による情報漏洩事件・事故

2001年　11月20日●宗教信者を逮捕 勤務先から機密情報を持ち出し
　　10月23日●税務署のパソコンが盗難「内部犯行」の可能性
2000年　 8月 1日●犯罪歴データ流出 現職警官関与の疑い
　　7月31日●大手通信会社から顧客情報400人分が漏えい
　　6月20日●京都で介護保険の個人データ1836人分が入ったPC盗難

■人的ミスによる情報漏洩事件・事故

2001年　10月30日●大手アパレル会社から570人のメールアドレスが流出
　　10月26日●航空券予約サイトから4000人分の顧客アドレス流出
2000年　11月20日●教育出版大手の関連広告会社から求人情報が流出
　　3月13日●大手製薬会社から個人情報9900人分漏えい
　　2月25日●民間シンクタンクのHPで16000人の個人情報閲覧可能に

■外部からの侵入による情報漏洩事件・事故

2001年　11月21日●米男性誌のサイトにハッカー侵入 顧客情報が盗まれる
　　7月26日●FBIが「サーカム」の被害 内部文書が漏洩
　　6月25日●英クレジットカード会社でカードの個人情報流出
　　2月 5日●ダボス会議で要人データ盗難

情報漏洩とITロス

- 社内の正規ユーザー・・・
  - 文書ファイルなどの契約情報の漏洩
  - CADデータなどのデザインや技術情報の漏洩
  - データベースなどの顧客情報の漏洩
  - 音声、ビデオなどのマルチメディア情報の漏洩
  - サボタージュ
- 外部の不正者・・・
  - 委託社員、メンテナンス要員によるスパイ行為
  - セミナー、展示会、研究所、研修所での情報漏洩
  - モバイル端末を利用した情報漏洩

データセキュリティの問題点と対策

- サーバー・シャット・ダウンによるデータ・ロス
  対策：バックアップ・システム
- コンピュータ・ウイルスによるデータ・ロス
  対策：ウイルス対策ソフトウエア
- 不正アクセス者によるデータの改竄、削除、漏洩
  対策：アクセス・コントロール・ツール
  ファイア・ウォール、ＩＤＳ、暗号（VPN）
- 正規アクセス者によるデータの漏洩、ITロス
  対策：セキュリティ・ポリシ、教育→モラルの向上
  技術的対策は なし

従来システムの問題点と影響

- Webからのファイル･ダウンロード
  - コピー、不正利用、改ざん、再配布、転売、しかも同品質
- ストリーミング配信
  - 専用プレーヤーによる安全神話、録音･録画ソフトの普及
- メール
  - S/MIMEなどによるﾒｯｾｰｼﾞの暗号化 ⇒ 通信路以外は×
- VPN環境などによるファイル転送
  - IPSec（IPｾｷｭﾘﾃｨﾌﾟﾛﾄｺﾙ） ⇒ VPN機器外の通信は×
  - SSL（ｾｷｭｱ･ｿｹｯﾄ･ﾚｲﾔ） ⇒ PCで復号化された後のｾｷｭﾘﾃｨに不安
- パッケージ配布
- その結果･･･
  - 営業機会損失、価格破壊、機密漏洩、信用の失墜 ⇒ ビジネス危機

DRM＝Digital Rights Management

- デジタル著作権管理技術
  - 利用権限の設定／管理
  - 権利者のみが権利範囲で利用可能
- 不正コピーの防止
  - コピー、抽出、キャプチャー、印刷、保存
- 不正利用の防止
  - 起動制御、有効期間
- 利用権限の管理
  - 貸し借り、譲渡

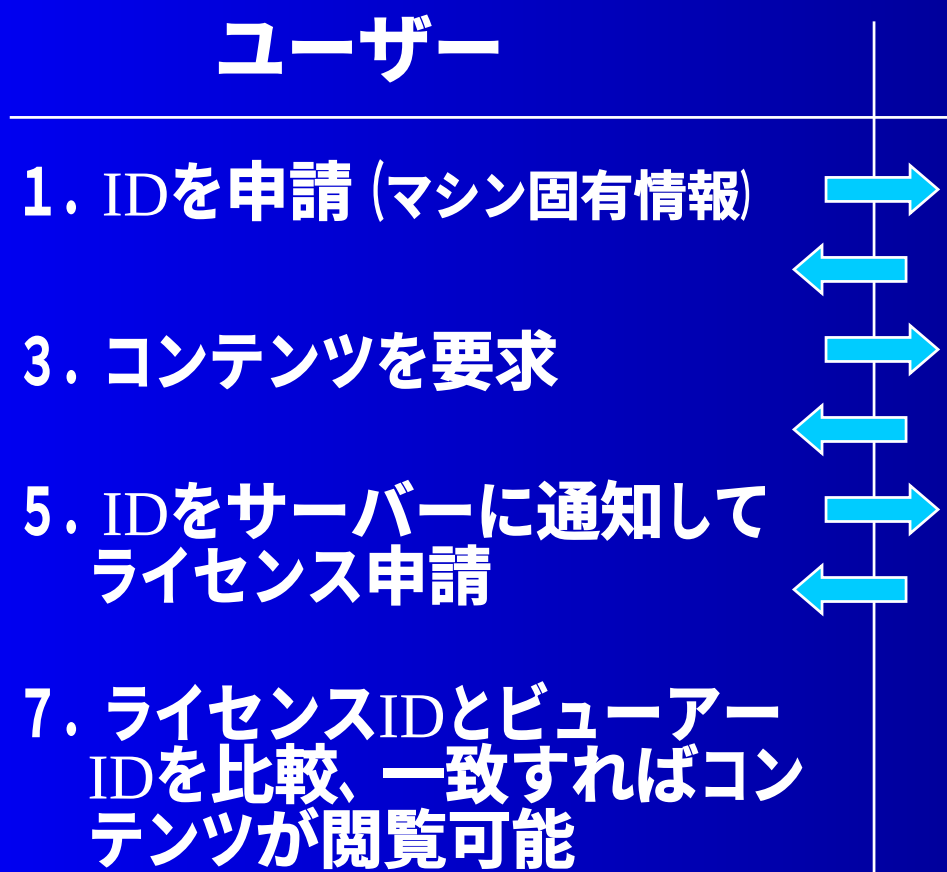
コンテンツ・ビジネスにおけるDRM

- コンテンツを利用制限する場合
  - 暗号化
    - 配信するコンテンツをあらかじめ暗号化しておく
  - ライセンス（復号カギを含んだ利用許可書）
    - 交付先：データ、人、マシン
    - 有効期間、編集・印刷権利、権限譲渡
  - 専用ビューア
    - 固定ID
    - コンテンツの復号化
    - 利用制限に従った実行
    - データの保存不可

DRM：ライセンス場所による分類

- 専用ビューアー（DRM製品ではこの方式が多い）
  - 利点
    - 1度ライセンスを取得するだけ
    - オフラインユーザー／不特定多数のユーザーに有利
  - 欠点
    - ライセンスの改ざん／不正利用の可能性、回収／失効は不可
- サーバー
  - 利点
    - ライセンスを安全に確保、発行後に内容変更可能
  - 欠点
    - コンテンツを閲覧する度に確認（ダウンロード済みデータでも）

DRM：専用ビューアの利用とその仕組み
(ライセンスを専用ビューアに持たせる場合)



企業情報漏洩におけるDRM

- 専用ビューアタイプ
  - 特徴：データ管理ソフトで暗号化、専用ビューアで閲覧
  - 利点：データ毎に制限設定が容易
  - 欠点：アプリケーション、データフォーマットに依存
- OS監視タイプ
  - 特徴：オリジナル・アプリケーションで暗号作成／閲覧
  - 利点：アプリケーション、データフォーマットに依存しない
    データの編集が容易、ユーザー管理が容易
  - 欠点：OSに依存

情報漏洩手段と対策

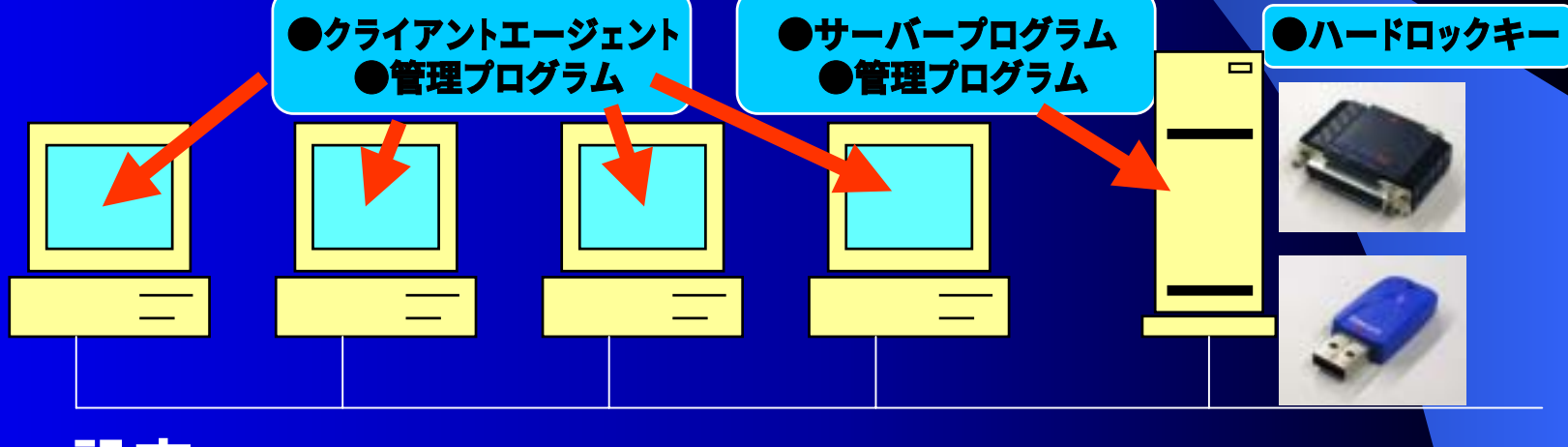
場所	情報漏洩手段	正規アクセス者	不正アクセス者	対策
内部から	印字データの持出し	○	×	物理的監視
	ＦＤ等の持出し	○	×	FDD の無いPC
	電子メールによる転送	○	×	コンテンツ・フィルタリング
外部から	インターネットを介してのアクセス	○	○	ファイア・ウォール アクセス・コントロール（ユーザ認証システム） 暗号（VPN）、I DS

情報漏洩とITロスを軽減する機能要件

- リアルタイムな暗号・復号機能
  - パスワードを必要としない機密データの取り扱い
- データ複製防止機能
  - コピー、カット&ペーストによるデータの複製防止
- プリントアウト防止機能
  - プリントアウトによる情報の漏洩防止
- イメージ複製防止機能
  - プリントスクリーンキーなどのイメージの漏洩防止
- クライアント管理機能
  - サボタージュの軽減、クライアント・セキュリティの監査

技術的対策事例：DataLock 構成と設定

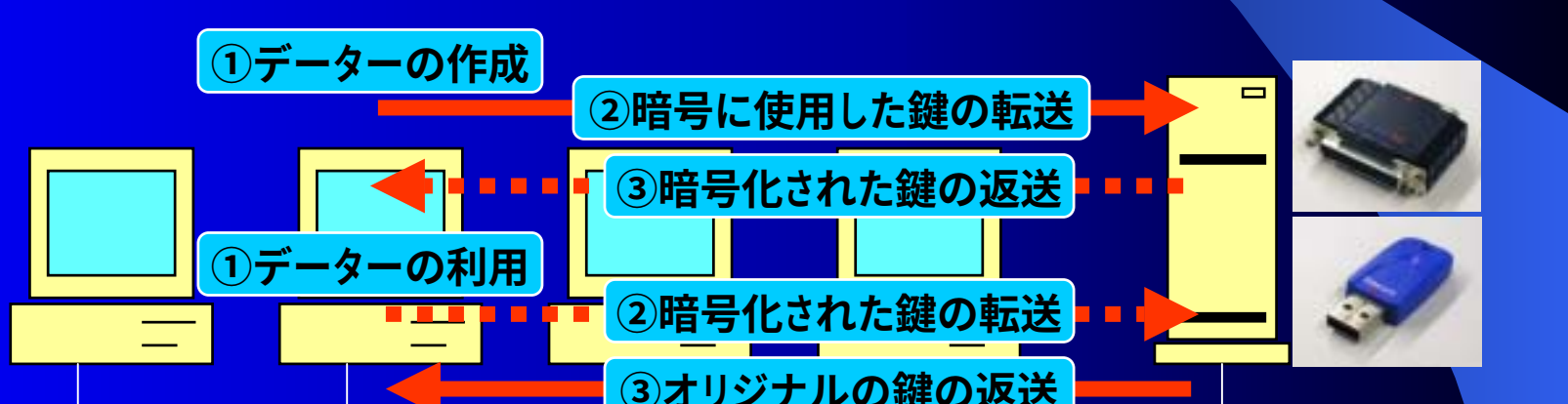
- インストール
  - サーバーにサーバープログラムをインストール
  - サーバーにハードロックキーを接続
  - クライアントにクライアントエージェントをインストール



- 設定
  - サーバープログラムを起動、クライアントエージェントを常駐
  - 管理プログラムにて、管理者とアプリケーションをサーバーに登録

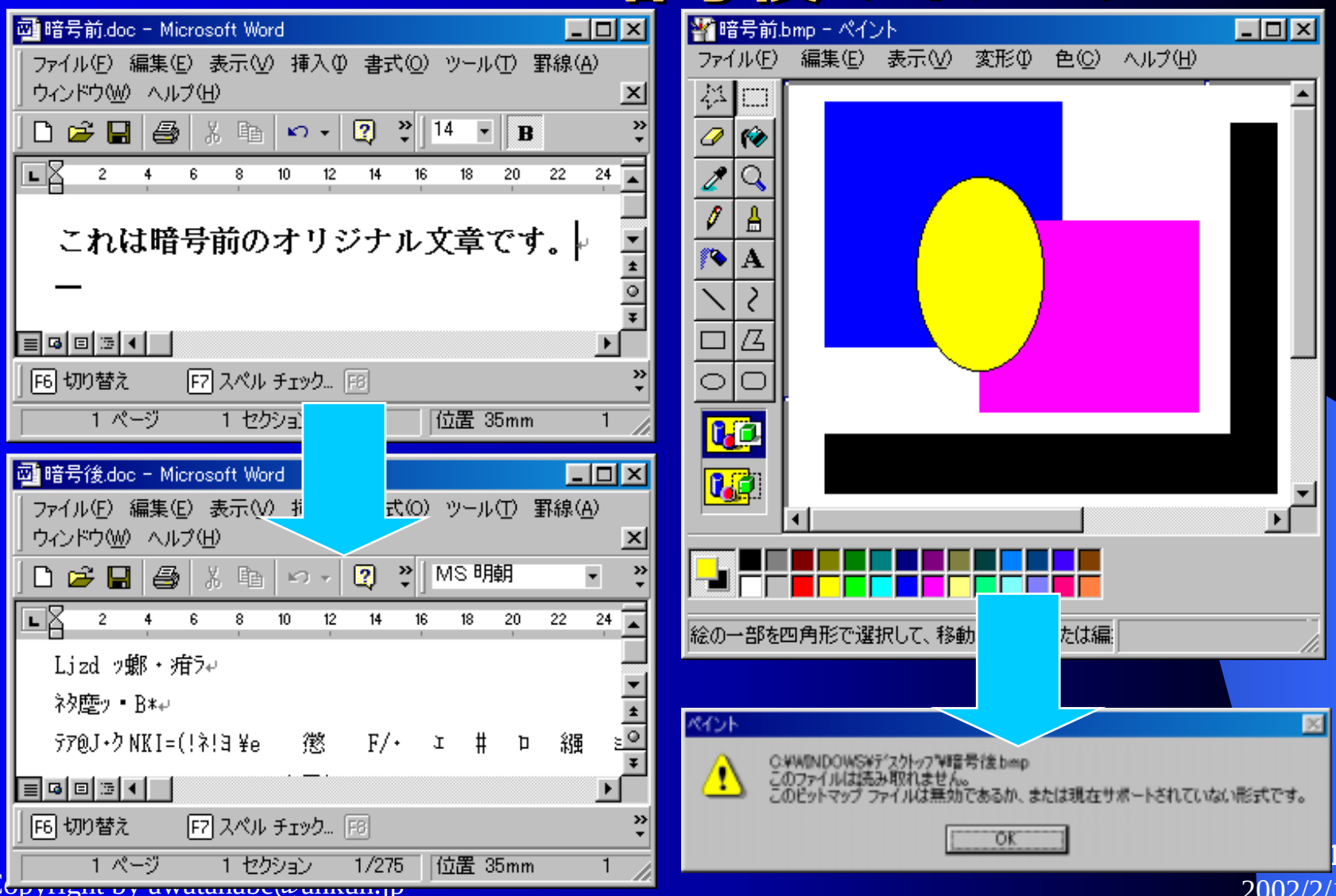
技術的対策事例：DataLock 動作イメージ

- **機密データー作成時**
  - ① 保存時にランダム生成した鍵でデーターを自動的に暗号化する
  - ② 暗号に利用した鍵をサーバーに転送（暗号通信）して暗号化する
  - ③ 暗号化された鍵が返送され暗号データーと共に保存される



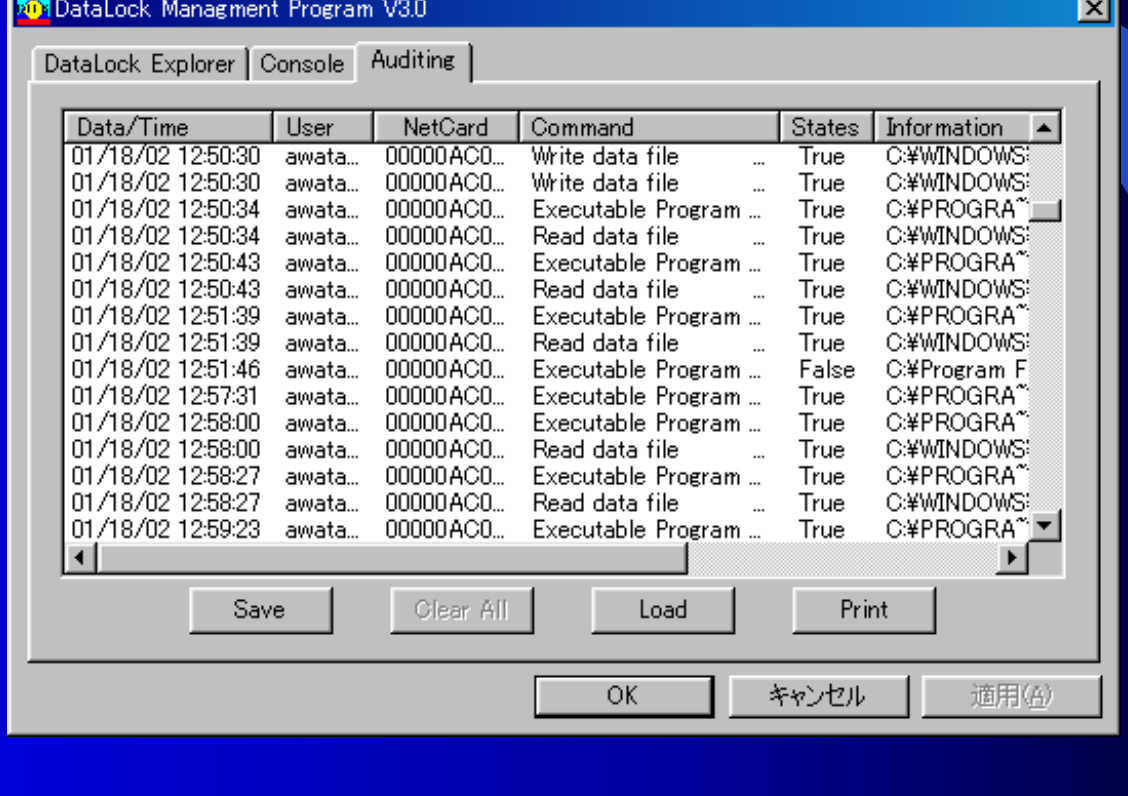
- **機密データー利用時**
  - ① 暗号ファイルをオープンしようとすると・・・
  - ② 自動的に暗号化された鍵をサーバーに転送して復号化する
  - ③ オリジナルの鍵でファイルを復号化してオープンする

技術的対策事例：DataLock
暗号後のイメージ



技術的対策事例：DataLock
クライアントのイベント（ログ）管理

いつ、誰が、どこで、なにを、どうした・・・



デモ