【情報セキュリティ技術】

情報漏洩を抑止・防止する
（課題とその解決事例）

ALways Security OK

ALSOK

Agenda

1. 情報漏洩事故を検証する
2. 情報には「価値」がある
3. 情報を漏洩させないために
   （情報漏洩対策ソリューション）
4. 情報を漏洩させないために
   （新たな脅威に対する研究開発事例）
5. まとめ

1.　情報漏洩事故を検証する

個人情報漏洩事故データ

項目	2013年データ	2012年データ	2011年データ
個人情報の漏洩事件	1388件	2357件	1551件
漏洩した個人情報	925万4513人分	972万65人分	628万4363人分
想定する損害賠償の総額	1438億7184万円	2132億6405万円	1899億7379万円
漏洩した個人情報／1件	7027人分	4245人分	4238人分
平均想定損害賠償額／1件	1億924万円	9313万円	1億2810万円
平均想定損害賠償額／1人	2万7707円	4万4628円	4万8533円

JNSA 2011～2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

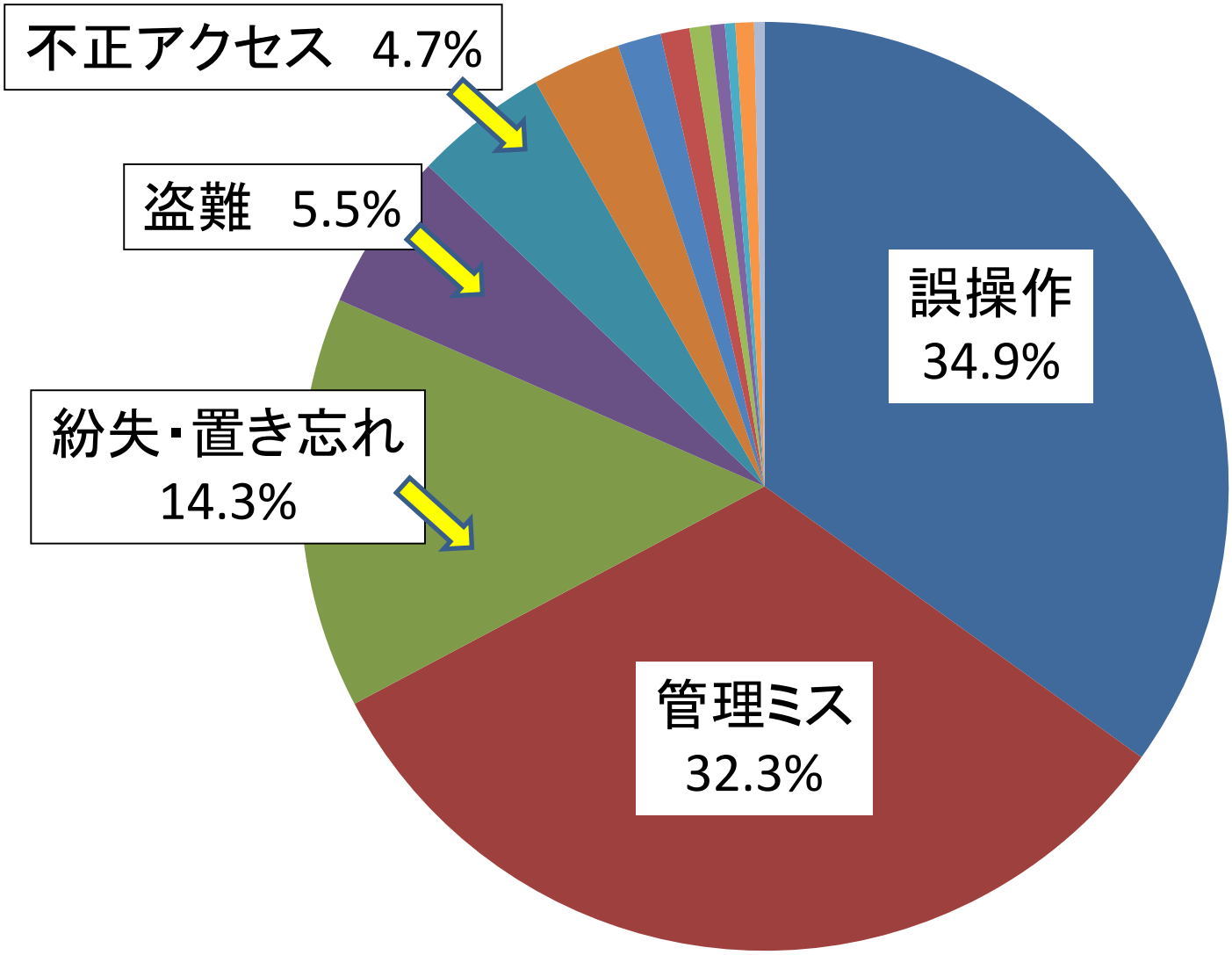
2013年　個人情報漏洩事故・トップ10

業種	漏洩した個人情報	原因
情報通信業	400万人分	不正アクセス
情報通信業	169万2496人分	不正アクセス
卸売業，小売業	47万人分	不正アクセス
公務	42万6000人分	紛失・置忘れ
情報通信業	24万3266人分	不正アクセス
情報通信業	17万5297人分	設定ミス
卸売業・小売業	15万0165人分	不正アクセス
金融業・保険業	12万0616人分	管理ミス
情報通信業	10万9112人分	不正アクセス
情報通信業	9万7438人分	不正アクセス

JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

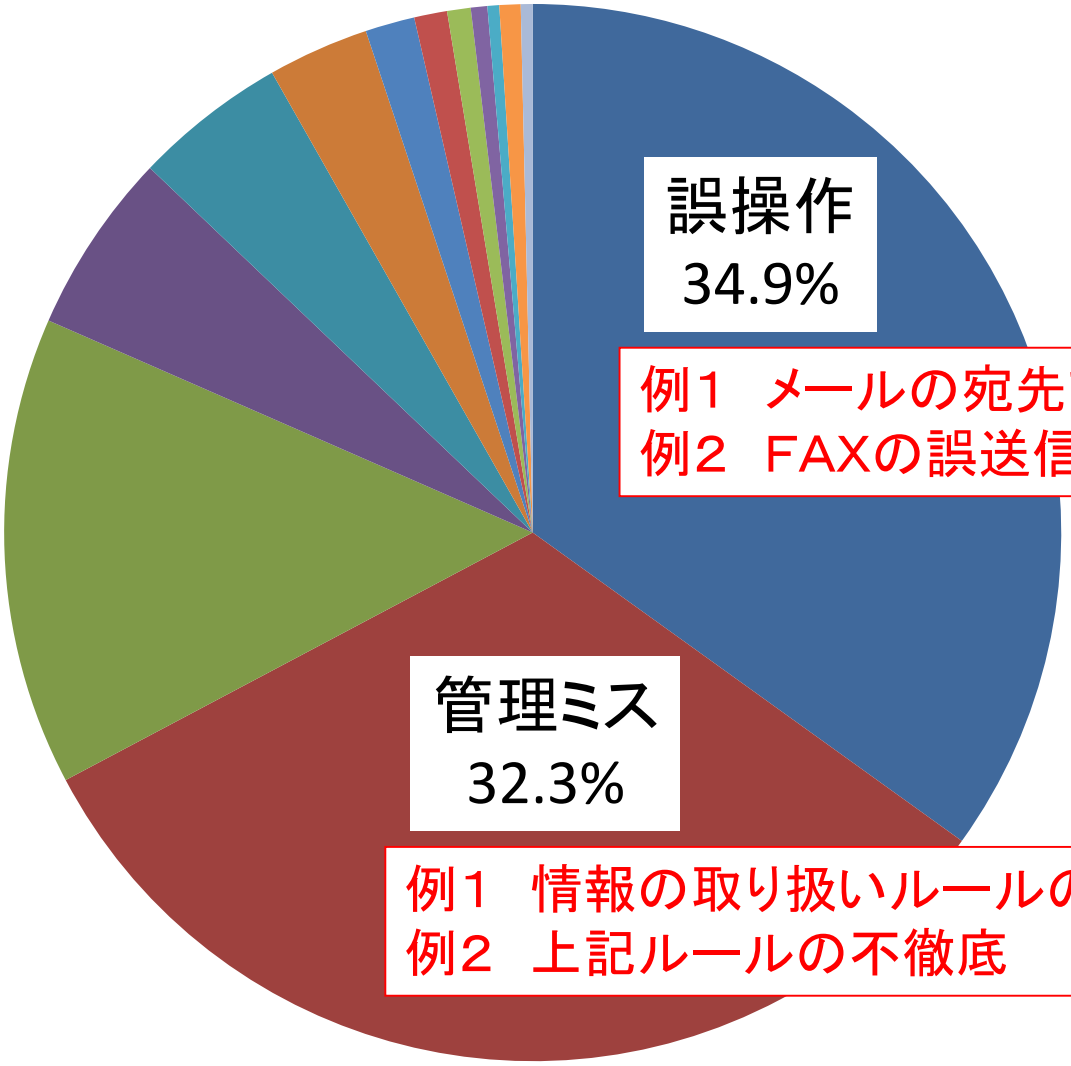
漏洩事故の原因



JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

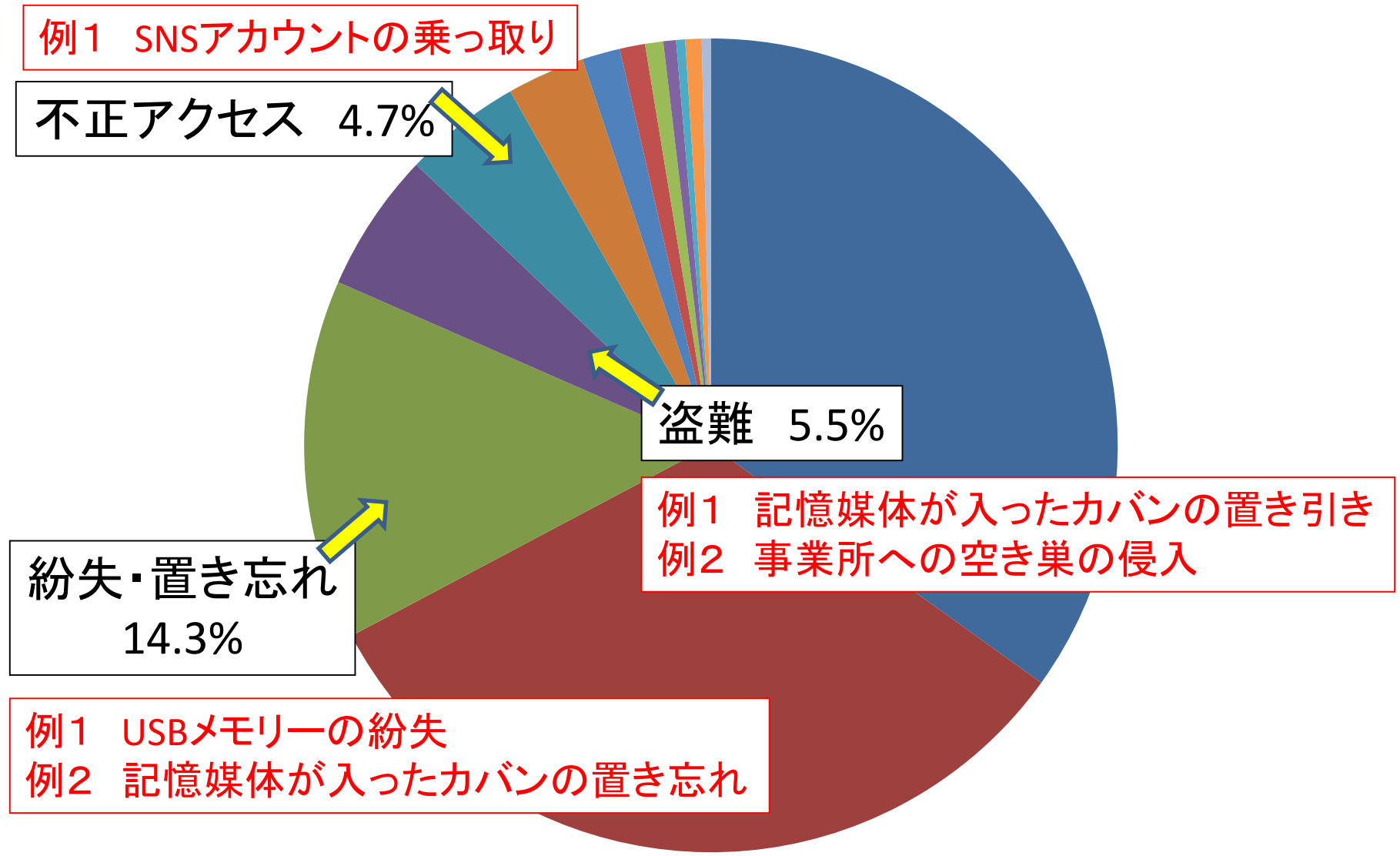
漏洩事故の原因（例）



JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

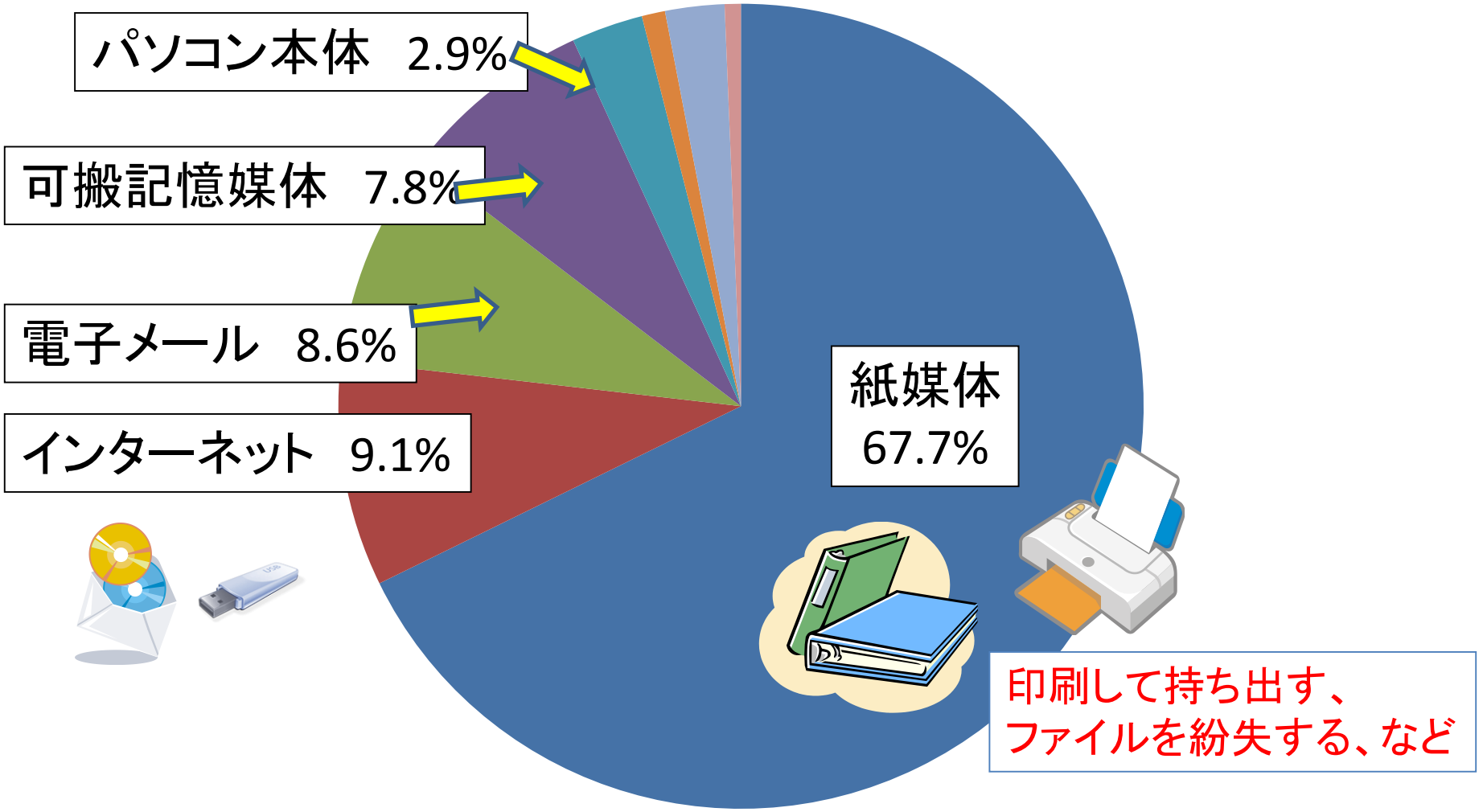
漏洩事故の原因（例）



JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

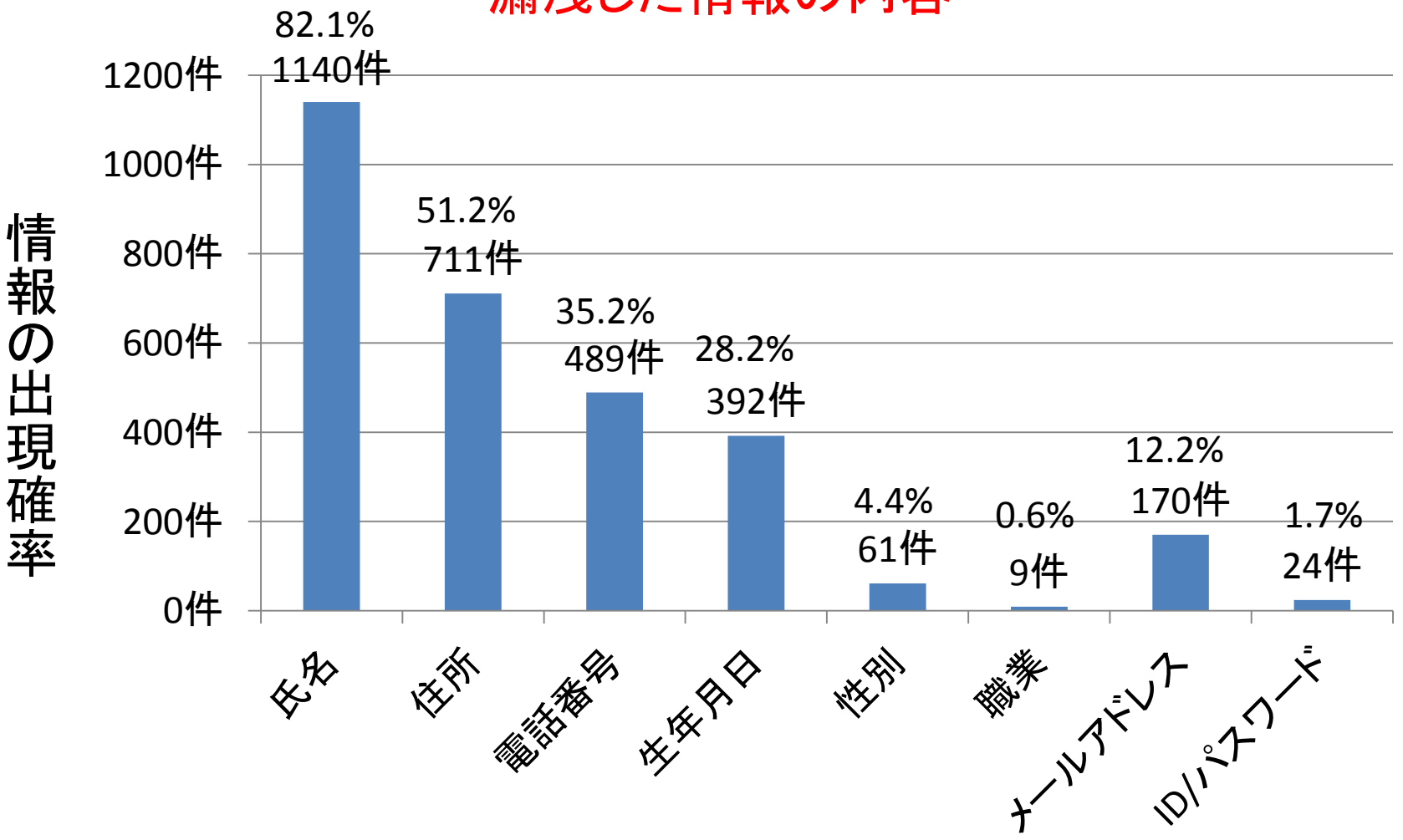
漏洩の経路



JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

漏洩した情報の内容



JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

シンプルEP（Economic-Privacy）図による情報のレベル分け

精神的苦痛レベル

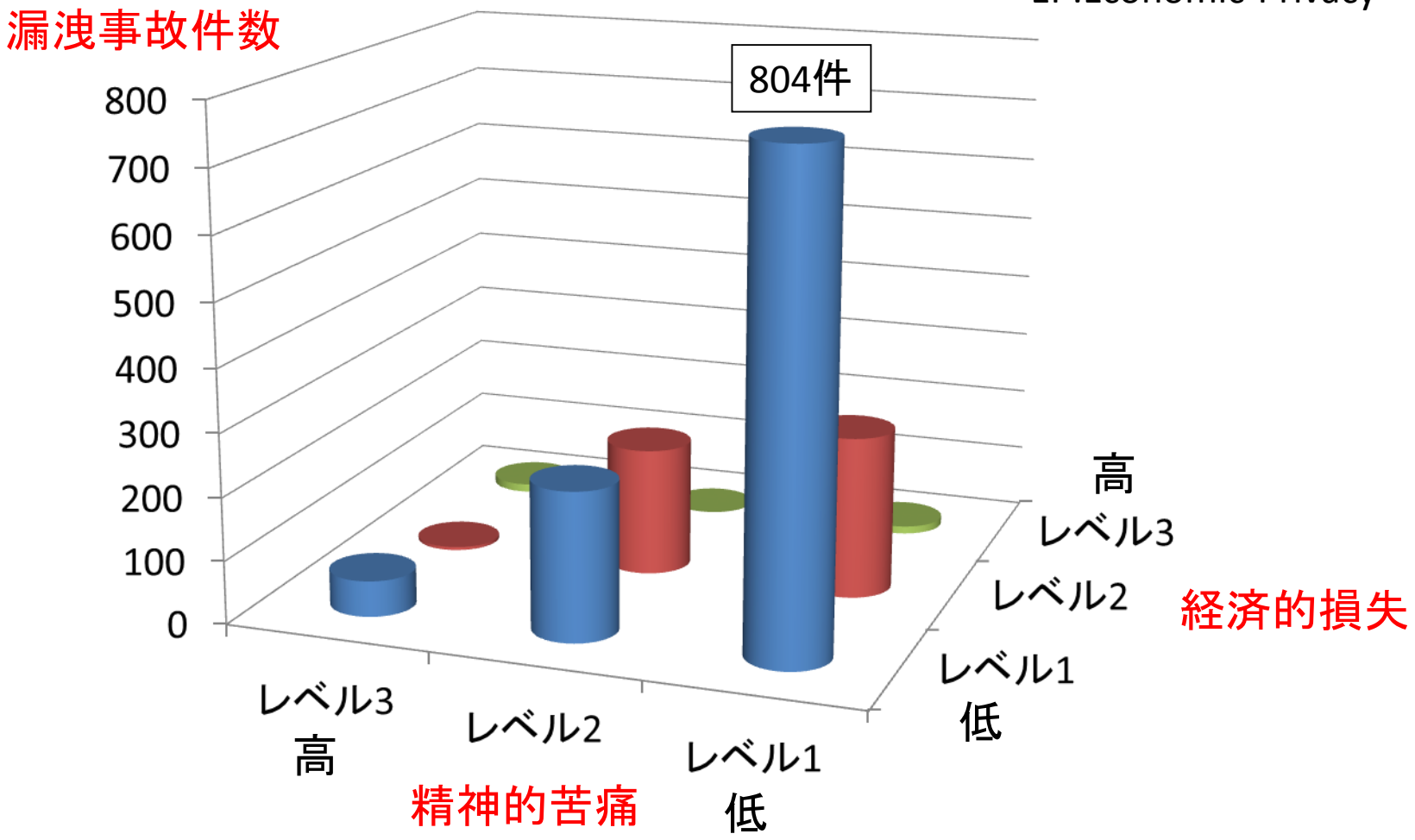
経済的損失レベル	レベル1	レベル2	レベル3
低 レベル1	氏名、住所、生年月日、性別、金融機関名、住民票コード、メールアドレス、健康保険証番号など	健康診断結果、心理テスト結果、性格判断結果、病歴、手術歴、妊娠歴、看護記録、生体認証情報など	加盟政党、政治的見解、加盟労働組合、信条、思想、宗教、信仰、本籍、保有感染症情報など
レベル2	パスポート情報、購入記録、ISPのアカウント・パスワード、口座番号、クレジットカード番号など	年収、所得、資産、建物、土地、残高、借入情報、購入履歴、給与額、賞与額、納税金額、寄付金額など	
レベル3 高	口座番号＋暗証番号、クレジットカード番号＋カード有効期限、決済系Webサイトの顧客登録情報など	遺言書	前科前歴、犯罪歴、与信ブラックリストなど

JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

1.　情報漏洩事故を検証する

シンプルEP図分析による経済的損失・精神的苦痛の可視化

EP:Economic-Privacy



JNSA 2013年情報セキュリティインシデントに関する調査報告書より作成

Agenda

1. 情報漏洩事故を検証する
2. 情報には「価値」がある
3. 情報を漏洩させないために
   （情報漏洩対策ソリューション）
4. 情報を漏洩させないために
   （新たな脅威に対する研究開発事例）
5. まとめ

2.　情報には「価値」がある

情報セキュリティ技術を実用化している企業（業種別）

業種	企業例（一部）
System Integrator いわゆるSier。個別企業のために情報システムを構築する	メーカー系 日立システムズ、NECソフト、富士通エフ・アイ・ピー、東芝ソリューション、三菱電機インフォメーションシステムズ、など。 ユーザー系 NTTデータ、インフォセック、伊藤忠テクノソリューションズ、など。 独立系 大塚商会、SCSK、オービック、内田洋行、など。
SE系 情報セキュリティに関する技術者集団。情報システムの設計、開発、運用を実施する。	外資系 シマンテック、マカフィ、トレンドマイクロ、カスペルスキー、FireEye、など。 メーカー（日本企業） 日立製作所、三菱電機、NEC、富士通、など。 独立系（日本企業） ラック、ソリトンシステムズ、ディアイティ、セキュアブレイン、フォティーンフォティ技術研究所、サイエンスパーク、など。
サービス業 （警備業）	ALSOK（綜合警備保障）、セコム、セントラル警備保障、など。

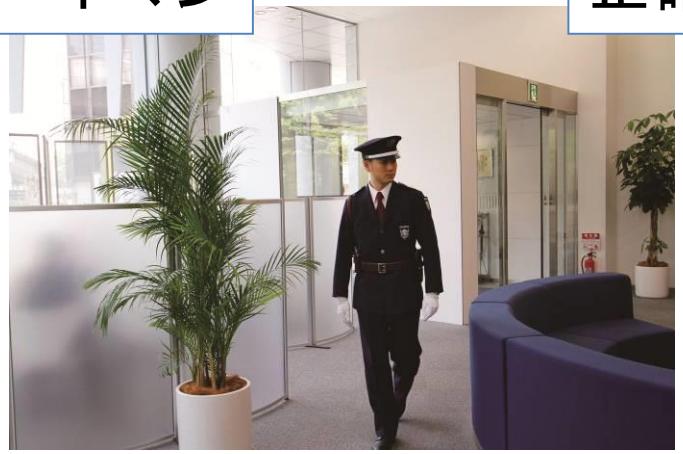
2.　情報には「価値」がある

よく見かける警備会社の業務（物理セキュリティ）

迅速

強力

ガードマン



正確

誠実

なぜ、物理セキュリティを生業とする警備会社が
情報セキュリティ技術を実用化しているのか？

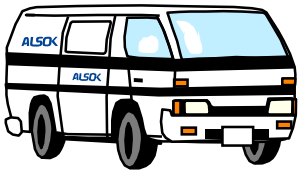
2.　情報には「価値」がある

基本的な警備対象＝「ヒト」、「モノ」、「カネ」

警備会社の業務

1号業務（施設警備）
　＝施設内の「モノ」、「カネ」を守る

2号業務（雑踏警備）
　＝イベント会場、工事現場周辺の「ヒト」、「モノ」を守る



3号業務（警備輸送）
　＝輸送する「モノ」、「カネ」を守る

4号業務（身辺警備）
　＝特定の「ヒト」を守る

ニーズの変化（1）

2.　情報には「価値」がある

ニーズの変化（1）＝「ヒト」、「モノ」、「カネ」＋「（物理的な）情報」

警備会社の業務

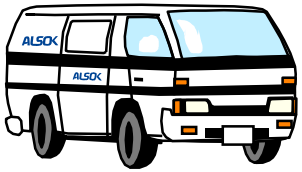
1号業務（施設警備）
　＝施設内の「モノ」、「カネ」、「情報」を守る

物理的な情報

2号業務（雑踏警備）
　＝イベント会場、工事現場周辺の「ヒト」、「モノ」を守る

3号業務（警備輸送）
　＝輸送する「モノ」、「カネ」、「情報」を守る

物理的な情報



4号業務（身辺警備）
　＝特定の「ヒト」を守る

ニーズの変化（2）

2.　情報には「価値」がある

ニーズの変化（2）＝「（物理的でない）情報」を保護する

価値ある情報の保護
（例1）企業⇔特許事務所間で送受信される電子メール

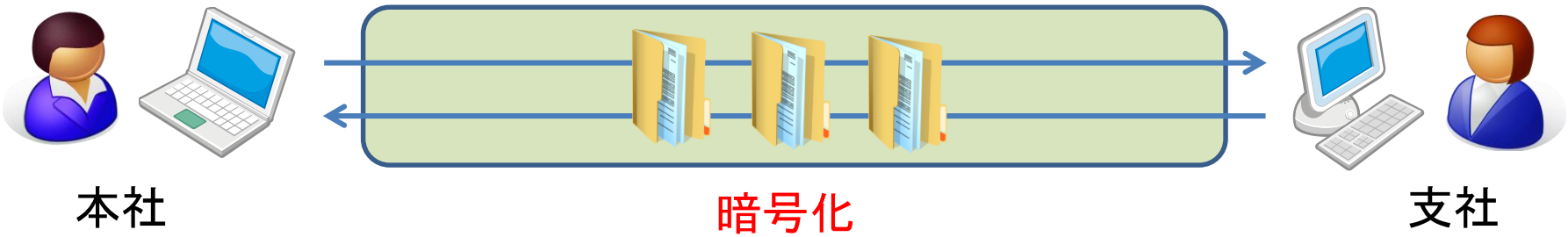
特定のメール本文／添付ファイルの暗号化
→　他人が情報を見られないようにする（情報の保護）。

提供するソリューションの例：
- ファイル暗号化／復号ソフトウェア
- 電子証明書（電子メール用）

2.　情報には「価値」がある

ニーズの変化（2）＝「（物理的でない）情報」を保護する

価値ある情報の保護
（例2）本社⇔支社間で送受信されるデータ



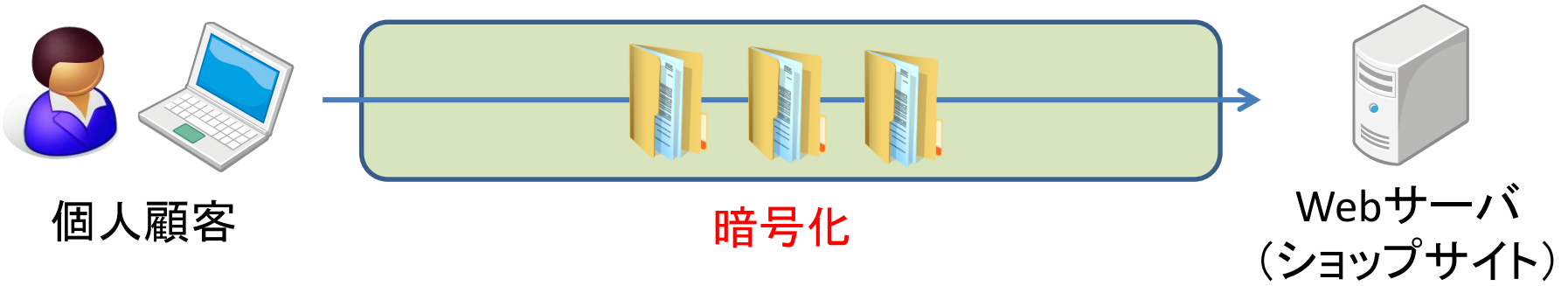
すべての情報を暗号化
→　他人が情報を見られないようにする（情報の保護）。

提供するソリューションの例：
- VPNルータ

2.　情報には「価値」がある

ニーズの変化（2）＝「（物理的でない）情報」を保護する

価値ある情報の保護
（例3）Webサーバに送信される個人情報／取引情報



アップロードされる情報を暗号化
→　他人が情報を見られないようにする（情報の保護）。

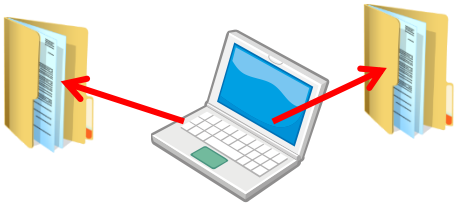
提供するソリューションの例：
- 電子証明書（Webサーバ用）

ニーズの変化（3）

2.　情報には「価値」がある

ニーズの変化（3）＝「情報の漏洩／持ち出し」を防止する

「情報漏洩」＝「信用の失墜」
情報の漏洩／持ち出しを防止する商品・サービスの普及拡大



パソコンのデバイス制御
　→　勝手な持ち出しの防止／持ち出しルールの制定
パソコンの操作をチェック
　→　情報漏洩に結びつく操作を可視化
内から外への通信をチェック
　→　情報の漏洩を防止

提供するソリューションの例：
・　次の章（第3章）にて解説します。

Agenda

1. 情報漏洩事故を検証する
2. 情報には「価値」がある
3. 情報を漏洩させないために
   （情報漏洩対策ソリューション）
4. 情報を漏洩させないために
   （新たな脅威に対する研究開発事例）
5. まとめ

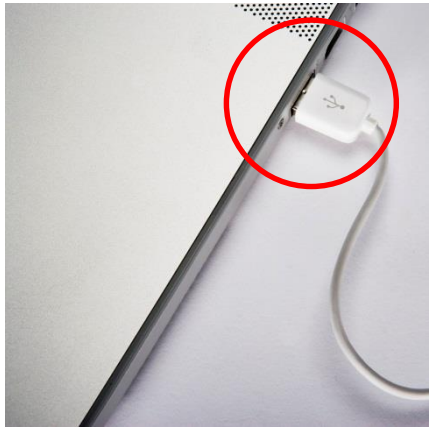
（1）パソコンのデバイス制御

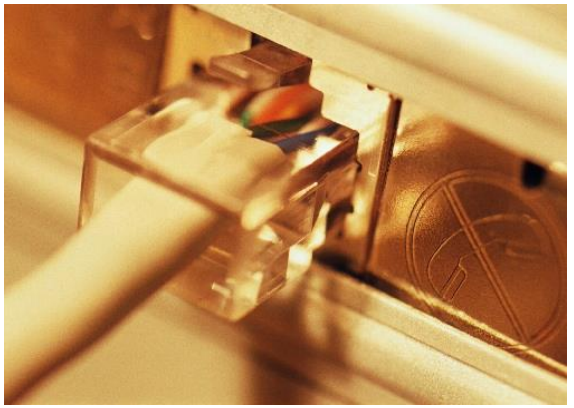
３．　情報漏洩対策ソリューション

（1）パソコンのデバイスを制御する

デバイスの例

USBデバイス、CD/DVD記録デバイス、通信デバイス（有線LAN／無線LANなど）





なぜ、デバイスの制御が必要なのか？

- パソコンの中に保存されている情報は、デバイスを経由してパソコンの外に持ち出せる（コピー、印刷、メール送信、など）。

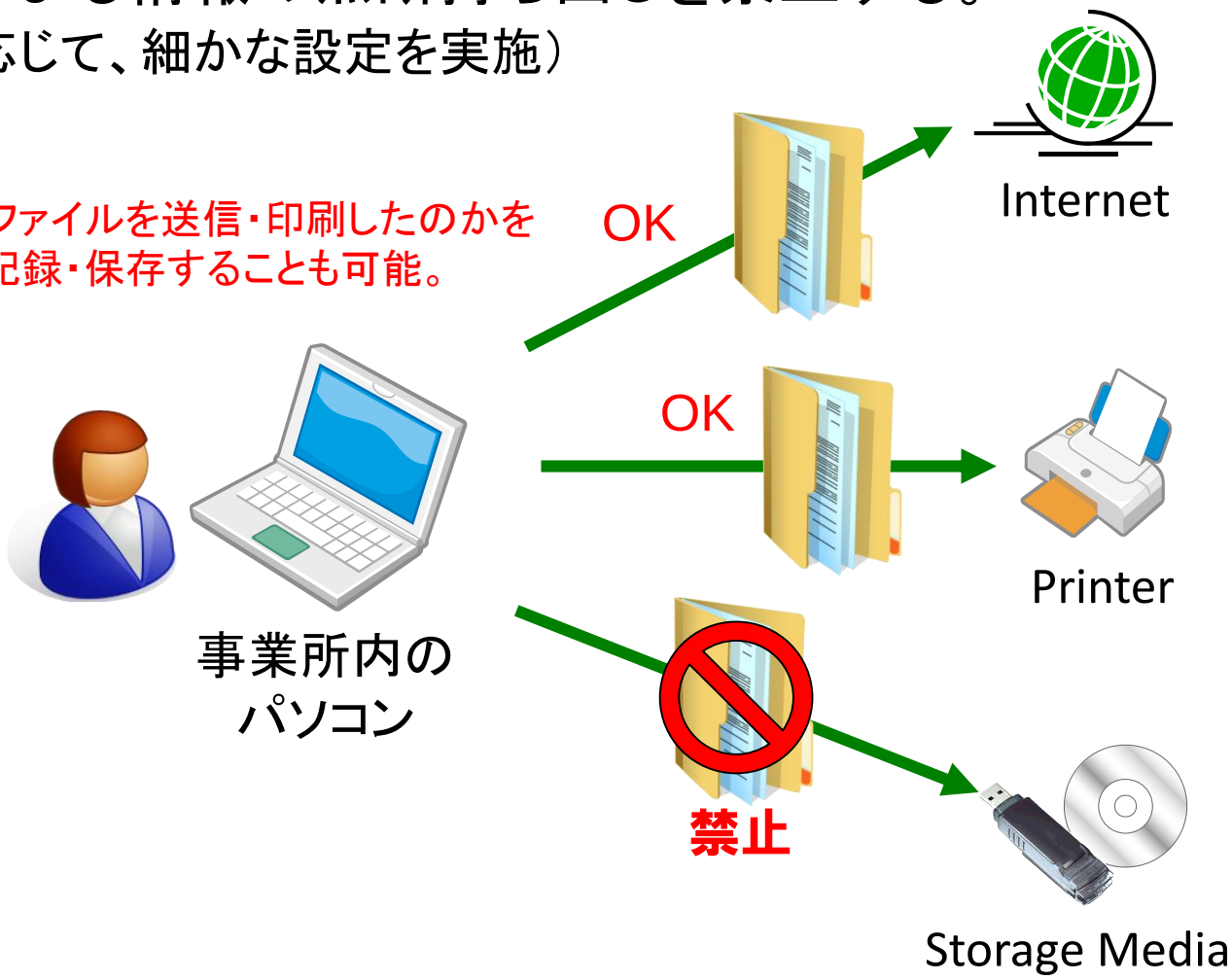
- 情報の持ち出しを制御するためには、情報の出口となるデバイスを適切に制御する必要がある。

3.　情報漏洩対策ソリューション

（1）パソコンのデバイスを制御する

従業員による情報の無断持ち出しを禁止する。
（用途に応じて、細かな設定を実施）

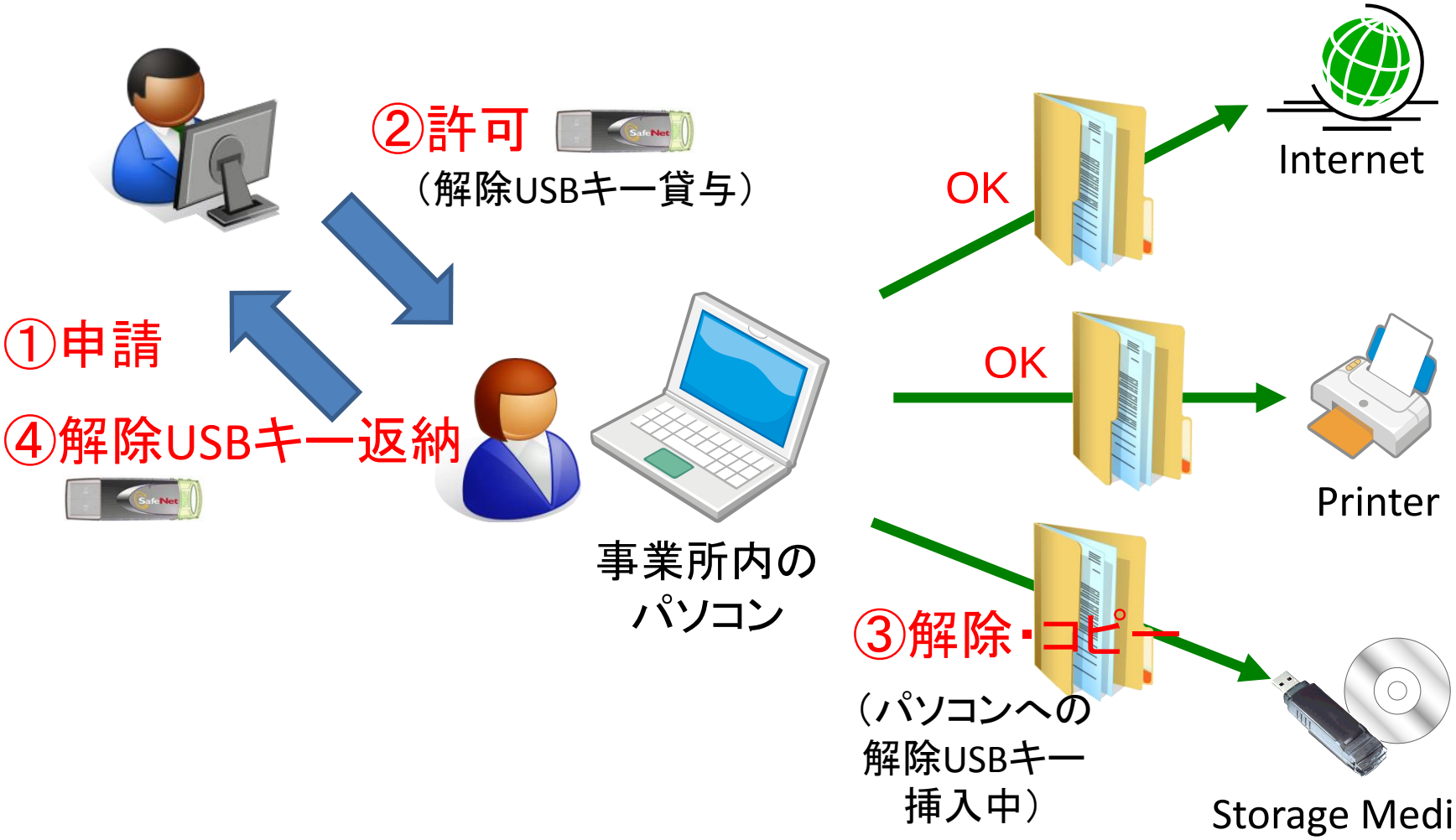
どのようなファイルを送信・印刷したのかを
ログとして記録・保存することも可能。



3.　情報漏洩対策ソリューション

（1）パソコンのデバイスを制御する

ルールを遵守して情報を取り扱う。
（情報を持ち出す前に申請する／上司の許可を得る）

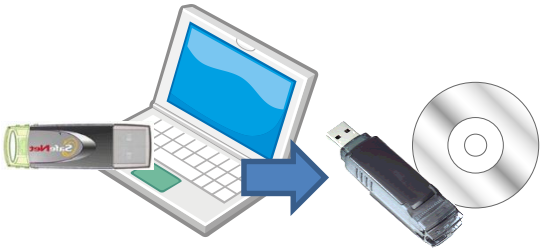


３．　情報漏洩対策ソリューション

（1）パソコンのデバイスを制御する

デバイス制御のながれ（外部記憶媒体の場合）

① 解除USBキー挿入前
パソコンにあらかじめインストールしているセキュリティソフトウェアが、デバイスによる出力を無効化している。
（＝記憶媒体を読むことはできるが、書き込むことはできない）



② 解除USBキー挿入中
セキュリティソフトウェアは、解除USBキーを認証し、その結果がOKの場合、出力の無効化を解除する。
（＝記憶媒体への書き込みができる）

③ 解除USBキー取り外し後
セキュリティソフトウェアは、出力を無効化する。
（＝①の状態に戻る）

管理者／ユーザともに、システムの理解が容易

（2）パソコンの操作をチェックする

３．　情報漏洩対策ソリューション

（２）パソコンの操作をチェックする

パソコンの操作（例）

ファイルのコピー／名前変更、電子メールへのファイル添付・ファイル送信など。




なぜ、チェックが必要なのか？

システム管理者は、個々のパソコンにおいて情報漏洩に結びつくパソコンの操作があったとしても、これを把握できない。これにより、従業員による情報の無断持ち出しが発生する。

（例）従業員が、機密情報や個人情報を、ファイルサーバから自分のパソコンにコピーしたり、名前を変えて保存したりする。
（例）従業員が、上記のファイルを電子メールに添付したり、ファイル送信サービスを用いて社外に送信したりする。
（例）従業員が、ファイル共有ソフトウェアを使用する。
（例）従業員が、顧客情報を印刷する。

３．　情報漏洩対策ソリューション

（２）パソコンの操作をチェックする

情報漏洩に結びつくパソコンの操作を「可視化」する。

ファイル送信ツールの利用	印刷情報	Webブラウザ利用・閲覧情報
FTP通信ソフトなど	印刷ファイル名、印刷枚数など	閲覧先のURL・タイトルなど
ファイル名変更操作	ファイル共有ソフトの使用	メッセンジャーの使用
変更前後のファイル名など	Winny/Share/Bittrentなど	MS Messengerなど
記憶媒体等へのコピー	メールへのファイル添付	Media Playerの使用
記憶媒体名、コピーファイル名など	メールソフト名、添付ファイル名など	MS Media Playerなど

Youtube：ALSOK「情報警備」紹介動画（ドラマ風）にてPV配信中

3.　情報漏洩対策ソリューション

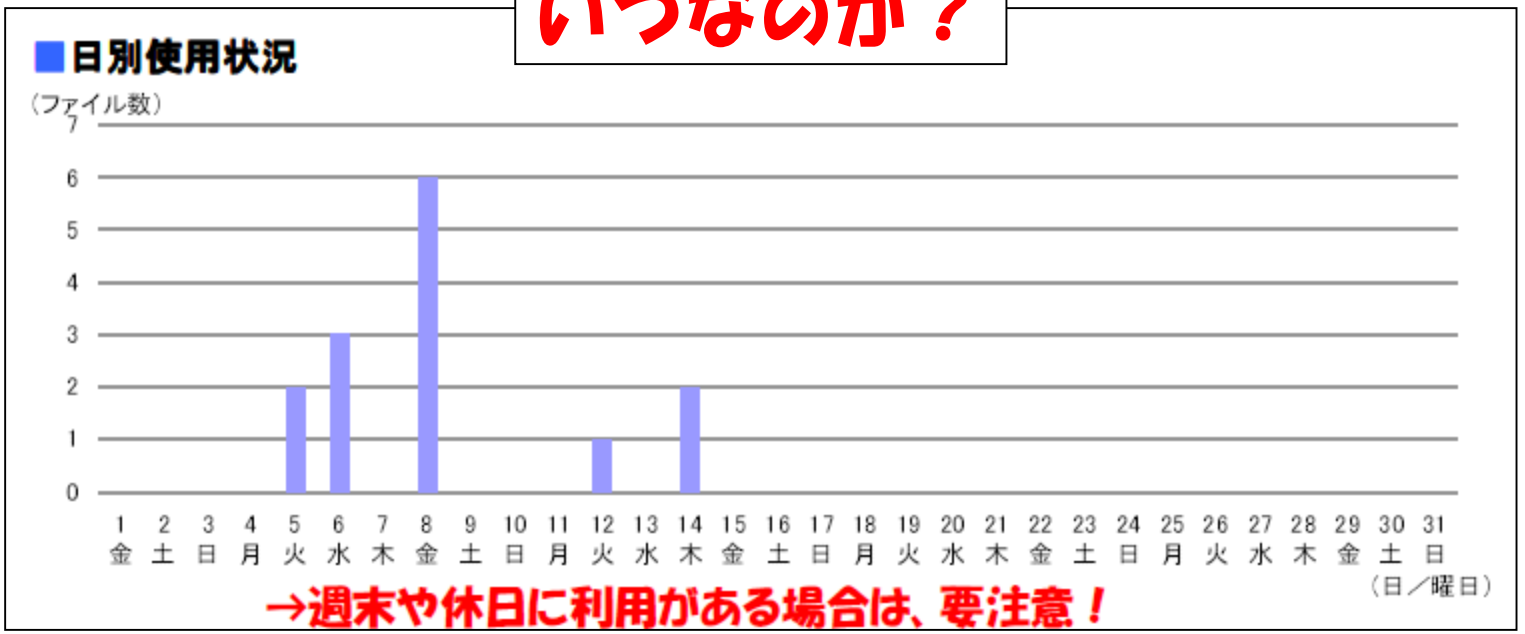
（2）パソコンの操作をチェックする

情報漏洩に結びつくパソコンの操作を「可視化」する。

システム管理者は、レポートを見ることで対策の効果を把握できるほか、経営陣に対してレポートを示しながら報告できる。

（例）外部記憶媒体へのファイルのコピー

いつなのか？



3.　情報漏洩対策ソリューション

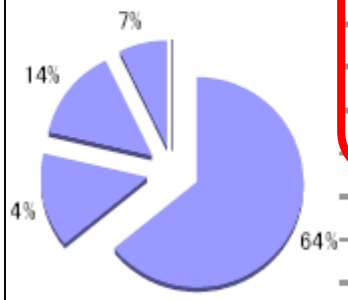
（2）パソコンの操作をチェックする

情報漏洩に結びつくパソコンの操作を「可視化」する。

3.1. 外部記録媒体へのファイルのコピー

3.1.2.　部署・パソコン別使用状況　**どの部署が？？**

■部署別使用状況



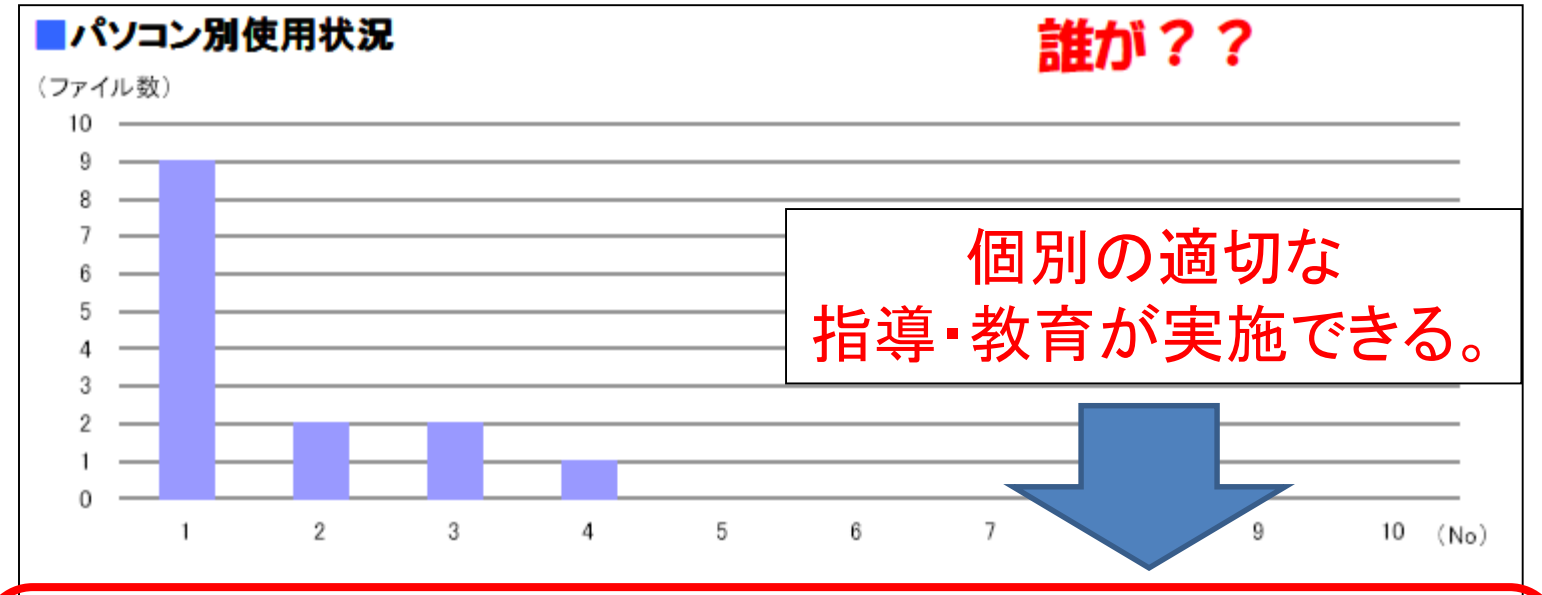
No.	部署名	ファイル数
1	営業3課	9
2	営業9課	2
3	営業6課	2
4	人事部	1
5		
6		
7		
8		
9		
10		

●「ファイル数」とは、外部記憶媒体にコピーされたファイルの数を指します。

3.　情報漏洩対策ソリューション

（2）パソコンの操作をチェックする

情報漏洩に結びつくパソコンの操作を「可視化」する。



No.	部署名	使用者名	コンピュータ名	ユーザ名	ファイル数
1	営業3課	三浦	PC-3	miura	9
2	営業9課	九鬼	PC-9	kuki	2
3	営業6課	六藤	PC-6	mutou	2
4	人事部	十河	PC-J	sogou	1

3.　情報漏洩対策ソリューション

（2）パソコンの操作をチェックする

緊急レポート／月次レポートによる報告の実施

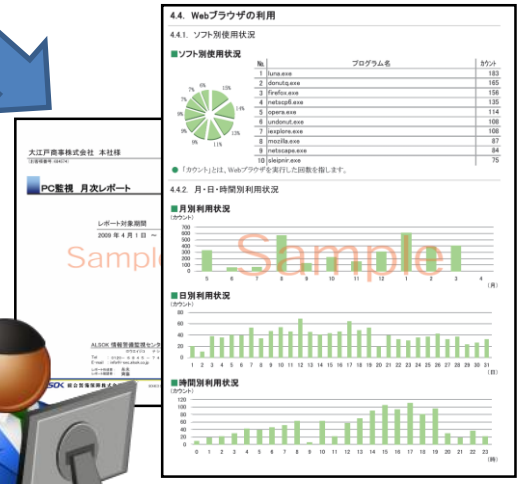
緊急レポートの発行タイミング：ファイル共有ソフトの起動、記憶媒体へのコピー検知時

②ログの分析・レポート作成

ALSOK

①パソコンの
操作ログ送信

③レポート送信



従業員のパソコン

④指導・教育／対策

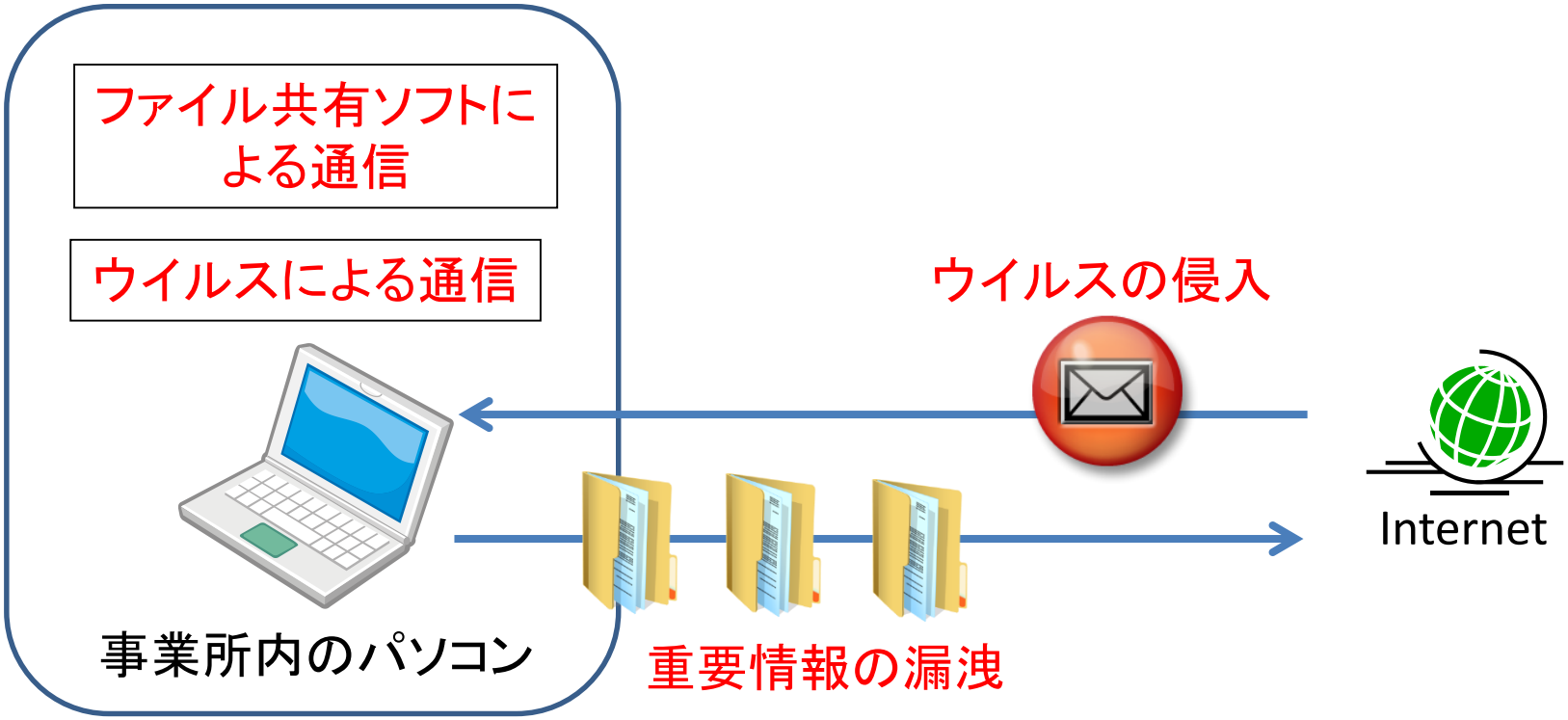
情報資産管理者

（３）内から外への通信をチェック

3.　情報漏洩対策ソリューション

（3）内から外への通信をチェック

情報の漏洩方法には、「人為的操作」や「外部からの不正アクセス」があるが、
最近は、「ウイルス」がパソコンやソフトウェアを乗っ取って、勝手に持ち出す。



情報漏洩事故に結びつく脅威も存在する
（従業員が、業務とは関係のないWebサイトを閲覧する、など）

3.　情報漏洩対策ソリューション

（3）内から外への通信をチェック

ファイル共有ソフトによる通信

Winny/Share/Bittrent/etc

③接続要求の拒否／通信のブロック

②リストを参照

監視装置

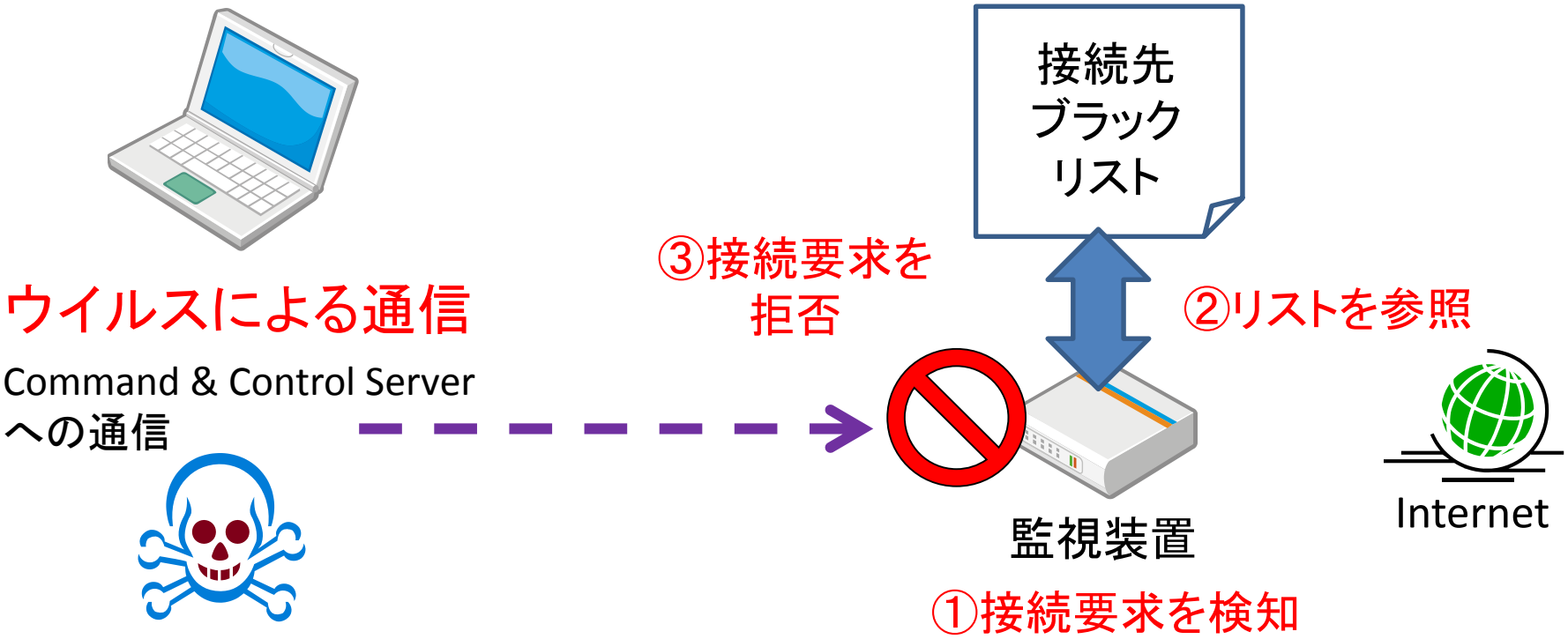
①接続要求や通信プロトコルを検知

Internet

Youtube：ALSOK「情報警備」紹介動画（ドラマ風）にてPV配信中

3.　情報漏洩対策ソリューション

（3）内から外への通信をチェック



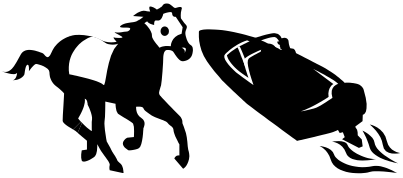
Youtube：ALSOK「情報警備」紹介動画（ドラマ風）にてPV配信中

3.　情報漏洩対策ソリューション

（3）内から外への通信をチェック

業務とは関係のない
Webサイトへの接続

ギャンブル、SNS、2ch、etc



③接続要求を
拒否

接続先
ブラック
リスト

②リストを参照

監視装置

①接続要求を検知

Internet

Youtube：ALSOK「情報警備」紹介動画（ドラマ風）にてPV配信中

Agenda

1. 情報漏洩事故を検証する
2. 情報には「価値」がある
3. 情報を漏洩させないために
   （情報漏洩対策ソリューション）
4. 情報を漏洩させないために
   （新たな脅威に対する研究開発事例）
5. まとめ

4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

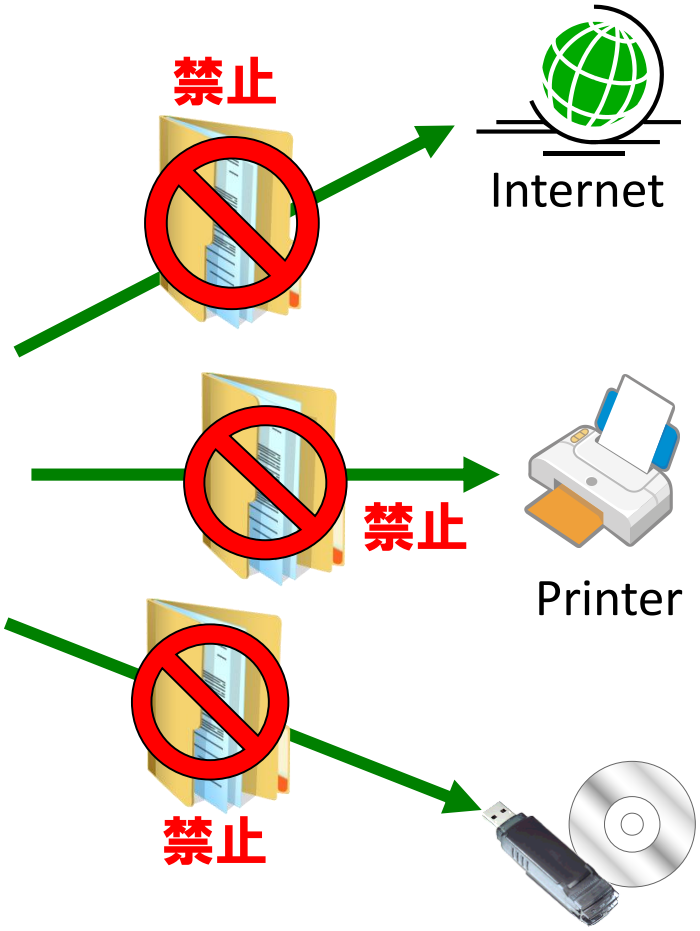
撮影による情報の持ち出しに対抗するシステムの研究

背景

【新しい脅威】
ディスプレイの撮影による
コンテンツの持ち出し

カメラ･ビデオ
スマートフォン

事業所内のPC



デジタルカメラ･ビデオは、多くの
コンテンツを撮影･記録できる。
Insider threat (Industrial piracy) :
　従業員が、重要な情報を撮影
　して持ち出すかもしれない。

4.　新たな脅威に対する研究開発事例

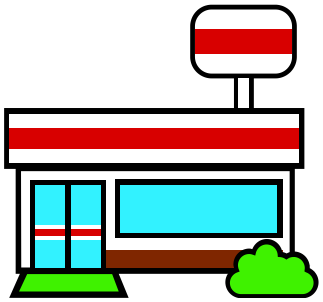
平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

持ち出しの事例

羽田空港管制官による情報漏洩
（エアフォースワン等の飛行計画）
東京メトロ職員によるパスモ利用履歴

ﾃﾞｨｽﾌﾟﾚｲ上の情報の撮影
（機密情報／個人情報の漏洩）



コンビニエンスストアに来店した
アイドルグループの様子を
ツイッターにアップロード

防犯カメラ映像の目的外使用
（肖像権／プライバシー侵害）

展示されているアニメ原画の撮影

作品の無断撮影
（著作権／所有権の侵害）

潜在的ニーズ		
防衛関係産業	コンビニ店舗	レンタルビデオ店舗
映画・映像制作	在宅勤務派遣	美術館・博物館

4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

アプローチ

①　撮影した画像・映像にノイズを混在させる

カメラの撮像素子（CCD/CMOS）は、赤外線を光として認識しやすいが、人間の目は光として認識しにくい。

（例）カメラを撮影モードにした状態で、リモコンの発光部分を見ると、発光している赤外線の様子を容易に観測できる。しかし、人間は発光部分を直接見ても、発光の様子を見ることはできない。

リモコン前部における
赤外線の発光部分

この性質を利用して、ディスプレイの表面に赤外線を発光するシートを貼り付けることで、ディスプレイに表示されている情報を撮影したとしても、クリアーな情報を得ることができなくなる（＝撮影した情報に光学的なノイズを混在させる）。

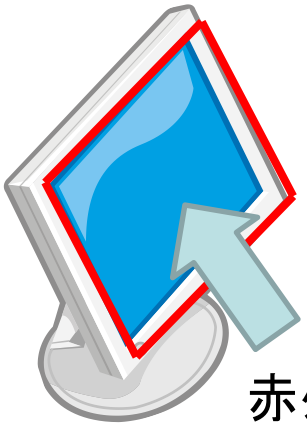
4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

アプローチ

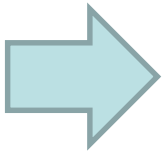
① 撮影した画像・映像にノイズを混在させる



Video/Camera

赤外線発光シート（波長870nm）を
ディスプレイ表面に貼り付ける。

表示されているコンテンツ



撮影されたコンテンツ
(Low quality)

870nm : CCD/CMOS image sensors can easily detect this as information.
The human eye cannot detect this as information.

4.　新たな脅威に対する研究開発事例

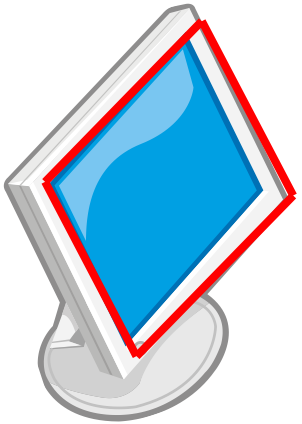
平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

アプローチ

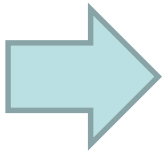
① 撮影した画像・映像にノイズを混在させる

→「赤外線カットフィルタ」を用いて撮影すると、ノイズを含まない情報を得ることができる（新たな課題の発生）。



Video/Camera

表示されているコンテンツ



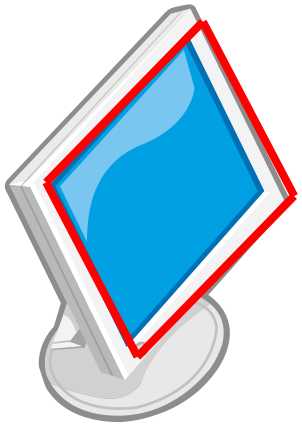
撮影されたコンテンツ

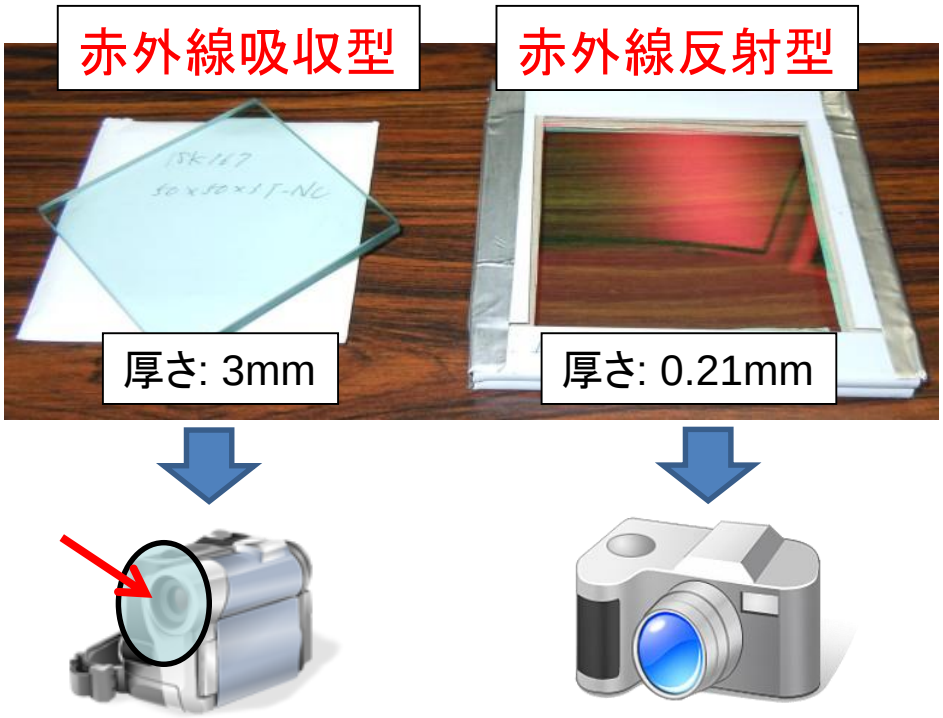
4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

赤外線カットフィルタの例





赤外線カットフィルタ
（外付け）を用いた撮影

赤外線カットフィルタ
（内蔵）を用いた撮影

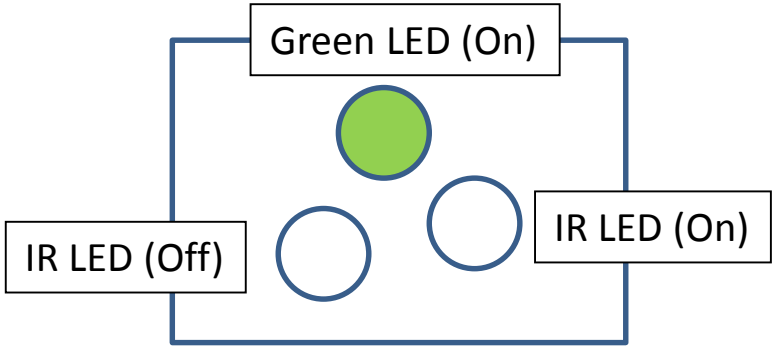
赤外線をカットできる＝ノイズレスな情報を撮影できる

4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

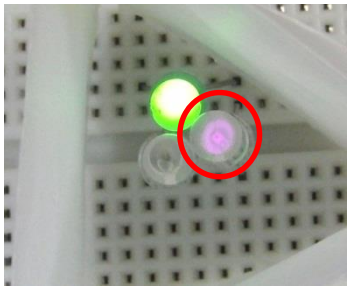
赤外線がカットできることを検証した実験



Layout sketch of each LED

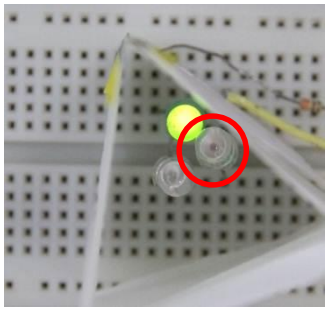
- LEDを上記のように配置。
- 緑のLEDと赤外線LEDを点灯させる。
- 比較のため、もうひとつの赤外線LEDは消灯しておく。

上記の様子を、2種類のカメラで撮影。
- コンパクトカメラ（赤外線カットフィルタなし）
- 一眼レフカメラ（赤外線カットフィルタあり）



コンパクトカメラで
撮影した画像

赤外線が観測できる
→ノイズ効果が期待できる。



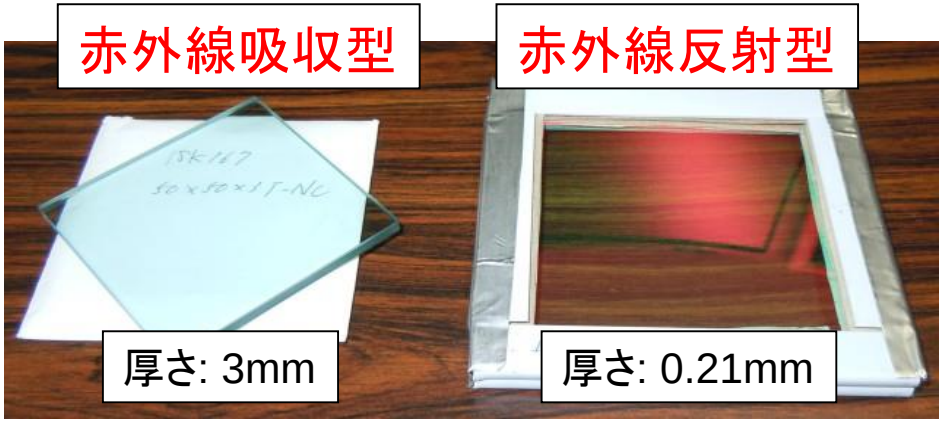
一眼レフカメラで
撮影した画像

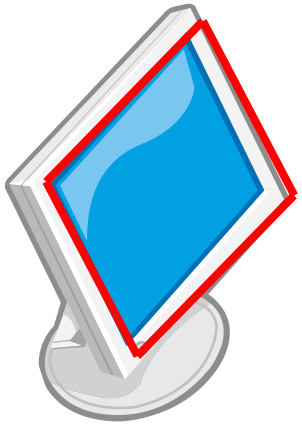
赤外線が観測できない
→ノイズ効果が期待できない。

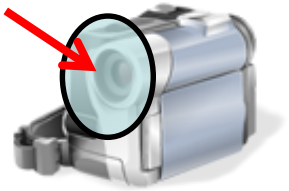
4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究







赤外線カットフィルタ
（外付け）を用いた撮影

赤外線カットフィルタ
（内蔵）を用いた撮影

新たな脅威に対抗する。
→　ディスプレイ側に、撮影行為を検知できるシステムを設置。
　　撮影行為を検知すると、画面を切り替えてコンテンツを保護。

4.　新たな脅威に対する研究開発事例

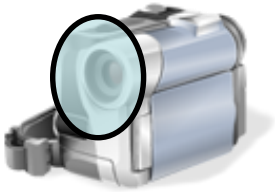
平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

アプローチ

② 撮影行為を検知する

デスクワーク
環境下を想定



赤外線カットフィルタ
（外付け）を用いた撮影

赤外線カットフィルタ
（内蔵）を用いた撮影
【高スペックカメラ】

人間の撮影行為に着目

- 片手／両手でカメラを構える。
- 三脚／ペットボトルホルダーでカメラを保持する。

→ kinectをディスプレイに設置し、ディスプレイ直近の直線成分をリアルタイムに検知する（＝疑わしい動きを検知した場合は、積極的にコンテンツを保護する）。

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

アプローチ①の研究
撮影した画像・映像にノイズを混在させる

4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

アプローチ①の研究

赤外線発光シートの実現可能性
（透明、柔軟、赤外線の発光）　→　実現可能性は高い

要素技術	開発している企業・研究機関（一例）
透明有機EL照明	有機エレクトロニクス研究所、フィリップス、AGFAなど。
透明有機ELディスプレイ	イリノイ大学、TDK、セイコーエプソン、サムスン、LGなど。

４．　新たな脅威に対する研究開発事例

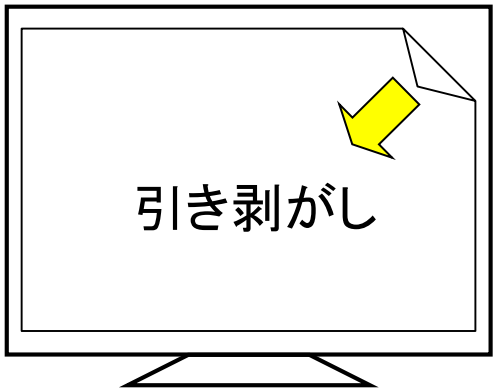
平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

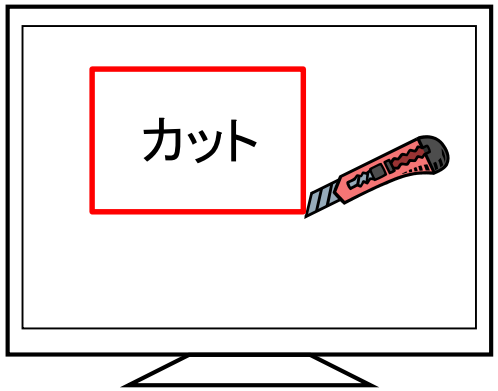
撮影による情報の持ち出しに対抗するシステムの研究

アプローチ①の研究

新たな脅威　→　赤外線発光シートの引き剥がし、カット

ディスプレイに貼り付けている赤外線発光シートの一部、または全部を引き剥がしたり、鋭利な刃物でカットしたりしてディスプレイを露出させたあと、コンテンツを撮影することが考えられる。





赤外線発光シートの引き剥がしやカットを検知したときに、
画面を切り替えてコンテンツを保護するシステムを開発する。

4.　新たな脅威に対する研究開発事例

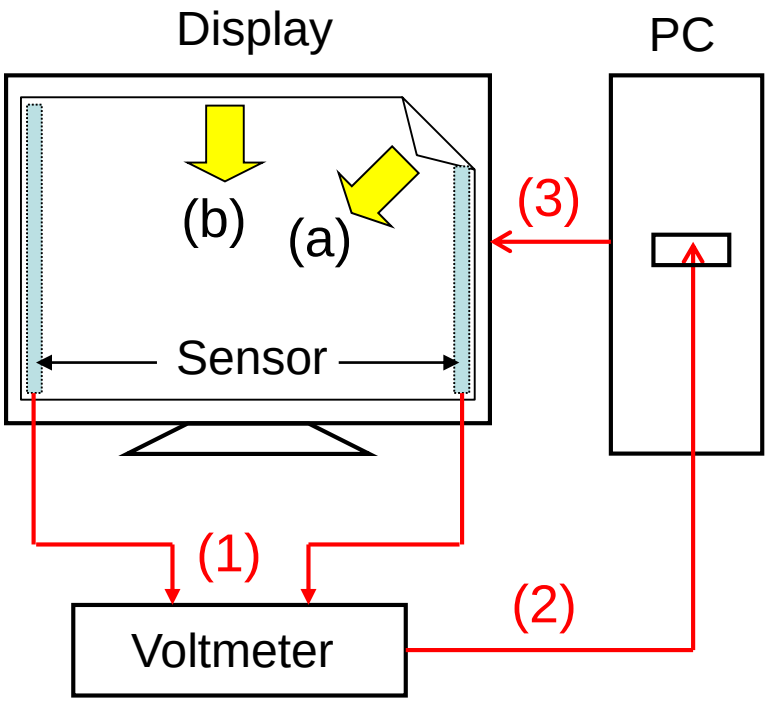
平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

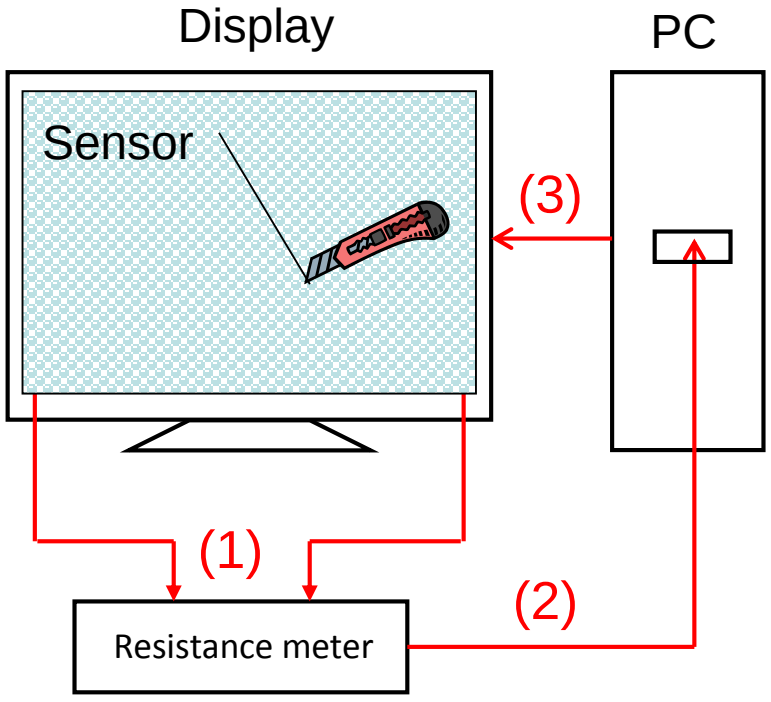
アプローチ①の研究

赤外線発光シートの引き剥がし、カットの検知

引き剥がしの検知方法（曲がり具合）



カットの検知方法（電気抵抗の変化）



平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

アプローチ②の研究
撮影行為を検知する

4.　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

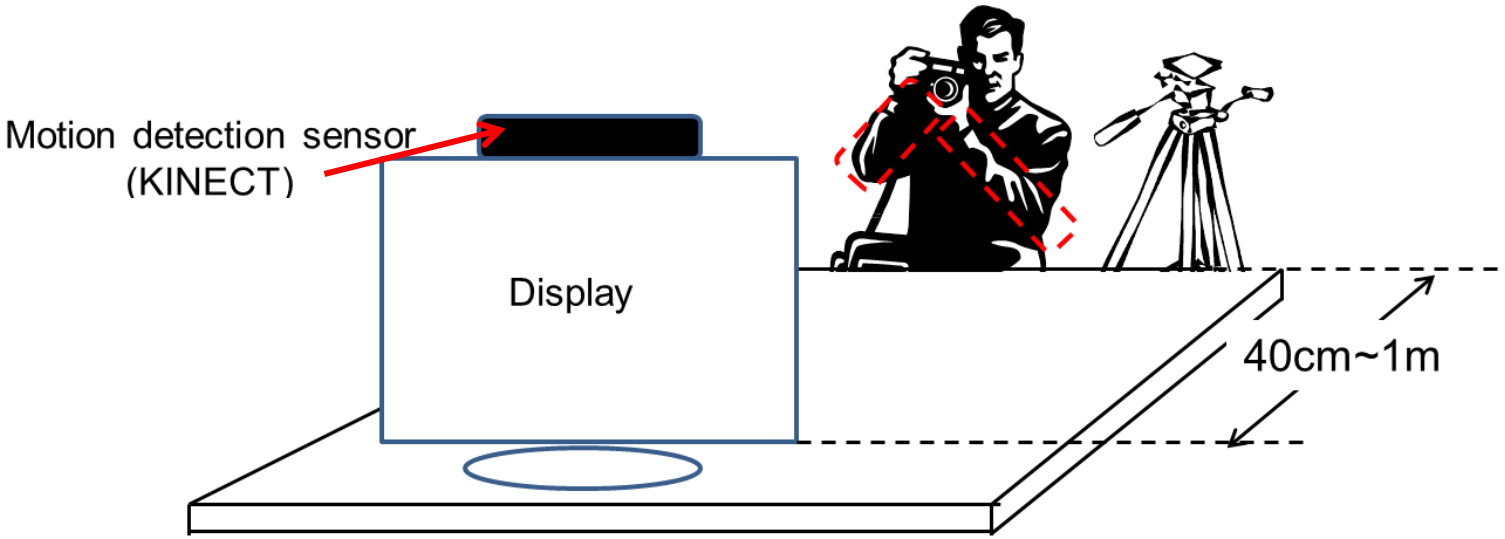
撮影による情報の持ち出しに対抗するシステムの研究

アプローチ②の研究

前腕のリアルタイム追跡

○　三脚／ペットボトルホルダーを用いた撮影にも対応。

○　照明が十分に当らない（薄暗い）環境でも、撮影を検知。



４．　新たな脅威に対する研究開発事例

平成22～23年度　経済産業省
新世代情報セキュリティ研究開発事業

撮影による情報の持ち出しに対抗するシステムの研究

今後取り組むべき課題

（1）誤検知の抑制

- 撮影とは関係のない腕の動きを、誤って検知する。
  （メガネをかけ直す、髪をかき上げる、頬杖をつく、など）

（2）失報の抑制

- システムが検知できない位置から撮影をする。
  （望遠レンズを装着したカメラを使用する、斜め横から撮影する、など）

- 隠し撮りをする（ピンホールカメラを衣服に装着する。カメラを撮影状態にしておき、パソコン操作をしながら撮影する）。

Agenda

1. 情報漏洩事故を検証する
2. 情報には「価値」がある
3. 情報を漏洩させないために
   （情報漏洩対策ソリューション）
4. 情報を漏洩させないために
   （新たな脅威に対する研究開発事例）
5. まとめ

５．まとめ

１．　情報漏洩事故を検証する
- 事故の概要、原因、漏洩経路、内容、EP図

２．　情報には「価値」がある
- ヒト、モノ、カネ＋情報
- ニーズの変化

３．　情報漏洩対策ソリューション
- パソコンのデバイス制御
- パソコンの操作をチェック
- 情報漏洩を止める

４．　新たな脅威に対する研究開発事例
- 撮影による情報漏洩を防止するための研究開発