情報セキュリティマネジメントを機能させる組織づくりと対策の考え方

独立行政法人 情報処理推進機構

セキュリティセンター　河野省二, CISSP

なぜ情報セキュリティはどこまでやっても満足できないのか

最近の事故で確認する情報セキュリティ対策の方針

2014年の事故を振り返る

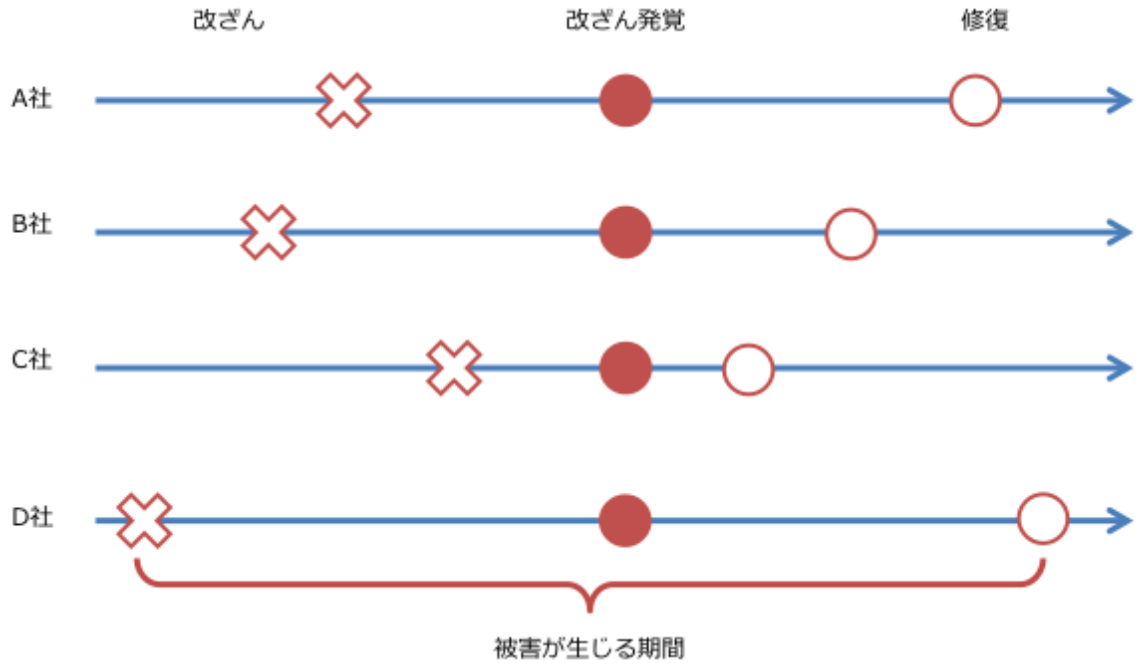
大手通信教育事業者	航空会社	運送業者など
社内不正による情報の持ち出しと売却	ウイルス感染による情報の不正送信	アカウントリスト型攻撃
関係子会社の契約社員による情報窃盗 持ち出しを制限していたつもりで実際にはできていなかったことが事件が起きた原因 １年近くもの間、事故が起きていたことに気付かなかった	ウイルス感染による、サーバへの不正アクセスと、サーバから取得した情報の外部サーバへの不正送信 システムのパフォーマンスダウンによる調査によって発覚	他社から漏れた可能性の高いアカウント（IDとパスワードの組み合わせ）を再利用した、不正アクセスの試み IDがメールアドレスになっていること、パスワードを使いまわしていることが原因で各所で起きている
約3504万件	約10000件	数万件から数十万件

これらの事故の本質はなにか

- 通信教育事業者の事故では約１年気が付かなかった
  - 顧客からの問い合わせにより、漏えいが発覚
  - 調査によって社内不正が発覚し、それが約１年前から繰り返し行われていたことに気づく
- 航空会社ではゼロデイ攻撃の疑い？
  - アンチウイルスソフトウェアがウイルスを検知できなかった？
  - ウイルスの種類も感染経路もわからない
- インシデント管理の原則は「被害の極小化」
  - 事故が発生しても影響がないような仕組みづくり
  - 影響を少なくするには「事故に気づく」体制づくりが必要

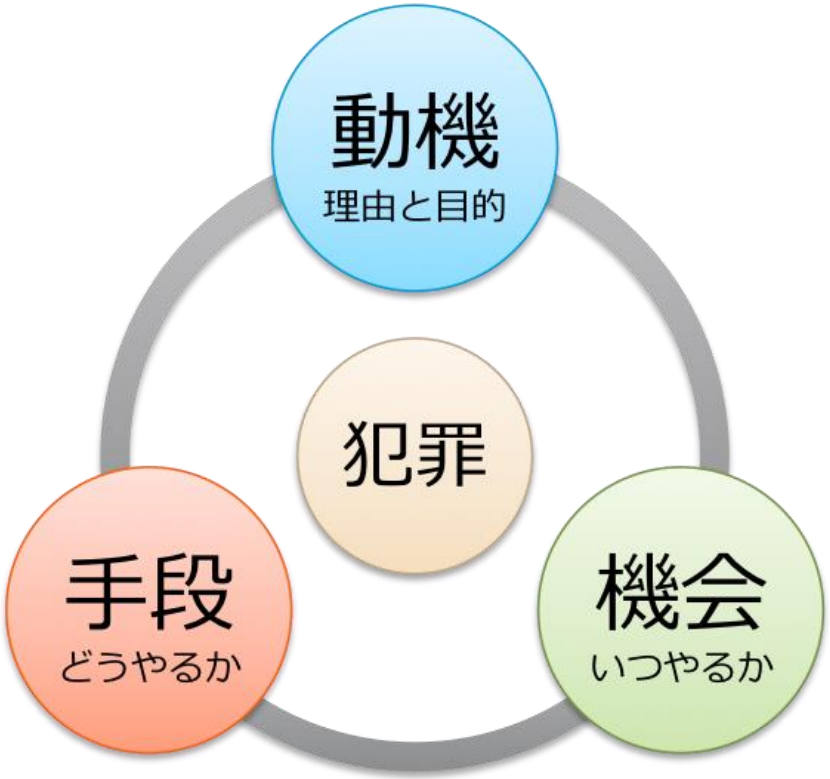
事故の発覚と被害の大きさ

Webサイト改ざんの被害について



サイト改ざんは同時に発生しているわけではない。気づいた時が一緒なだけで、被害は改ざんが発生してから修復が終わるまで続いている

内部犯罪は気づくまで永遠につづく



- 犯罪は動機を満足させるまで続く
  - ギャンブルや交遊費に使っている場合は気づかれるまで永遠に犯行は続く
- 事故の防止と抑止
  - 手段と機会をなくすことで犯罪はなくなる
  - 手段はイタチごっこ、まずはきっかけ（機会）を与えない職場環境づくり

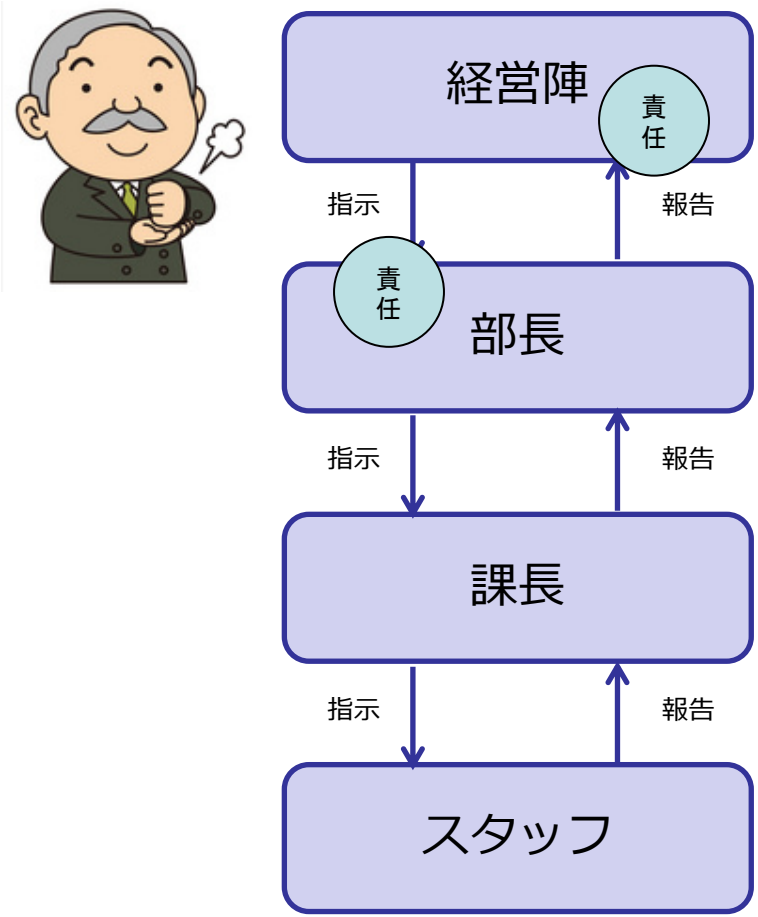
組織はどのようにあるべきか

誰よりも早く異常に気づくための情報セキュリティの体制づくり

不祥事が発生した時に備えて

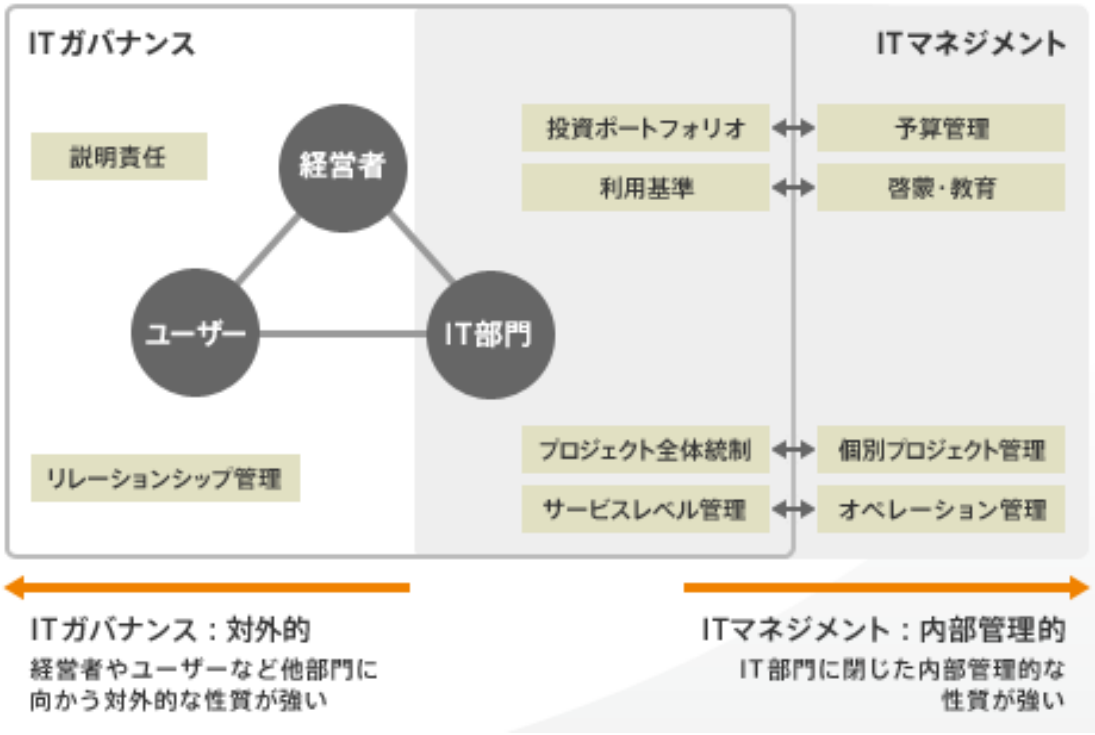
- 情報セキュリティに限らず、不祥事が発生した場合に十分な情報を持っておく
  - 不祥事が発生した場合の対応において、十分な情報がないことで被害が大きくなることがある
  - 情報が十分になかったために、対応が遅れてしまったり、間違った対応をしてしまい、対応のコストが莫大になってしまうことがある
- 事故に備えて、いつでも情報が上がってくる体制を作っておくことが重要です

トップがすべての責任を負う？



- 指示と報告による組織づくりと責任の明確化
  - 上司は部下に指示をし、部下はそれが完了したことを報告する。もしも問題がある場合は相談や連絡を行う
- 最終責任は経営陣
  - ITに関する指示は経営陣が行う
  - それに応えて組織はすべての報告（情報）が経営陣に集まるようにする

ITマネジメントからガバナンス



経済産業省「IT経営ポータル」

http://www.meti.go.jp/policy/it_policy/it_keiei/

マネジメントは部門のものだが、ガバナンスは経営を含む組織全体のもの。
「現場のマネジメント」を経営陣が統制できるように、ガバナンスの仕組みを利用して、効率的に全体を統制していく。
トップダウンではなく、現場からの意見を取り入れることができるように、報告の体制づくりなどをしていくことも重要な要素となる。
ITを活用した経営をIT経営といい、ガバナンスをベースに企業内の情報管理を行うことで、効果的な経営を行うことを目指す。

トップが全てを把握するために

経営者は全体を
把握したい

事業計画 → KPI ↔ 現場からの
情報収集

KPI → SLA

手打ち
報告書

自動
入力

NG!!
誰も読んでないし、
集計できない

OK!
リアルタイムに集計

ITの効果も
計測したい

サービス指向アーキテクチャによるITサービス開発と効果測定

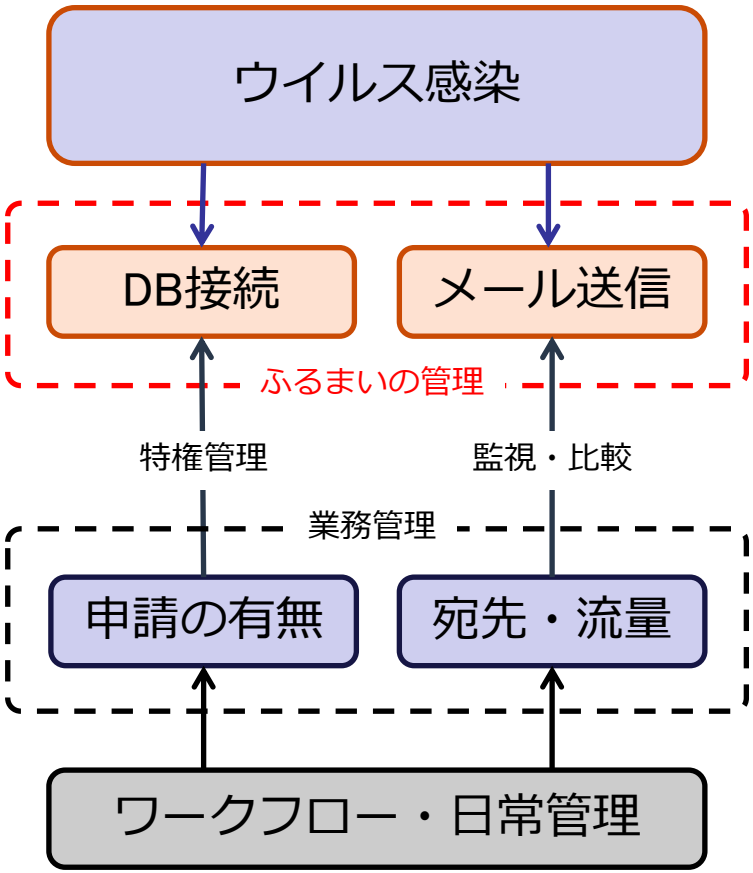
あんまり使っていないサービスのためにハードウェアを確保するのはもったいない　→仮装化　→分散処理

いわゆるIT経営 → **クラウドのはじまり**

なにを把握すればよいのか

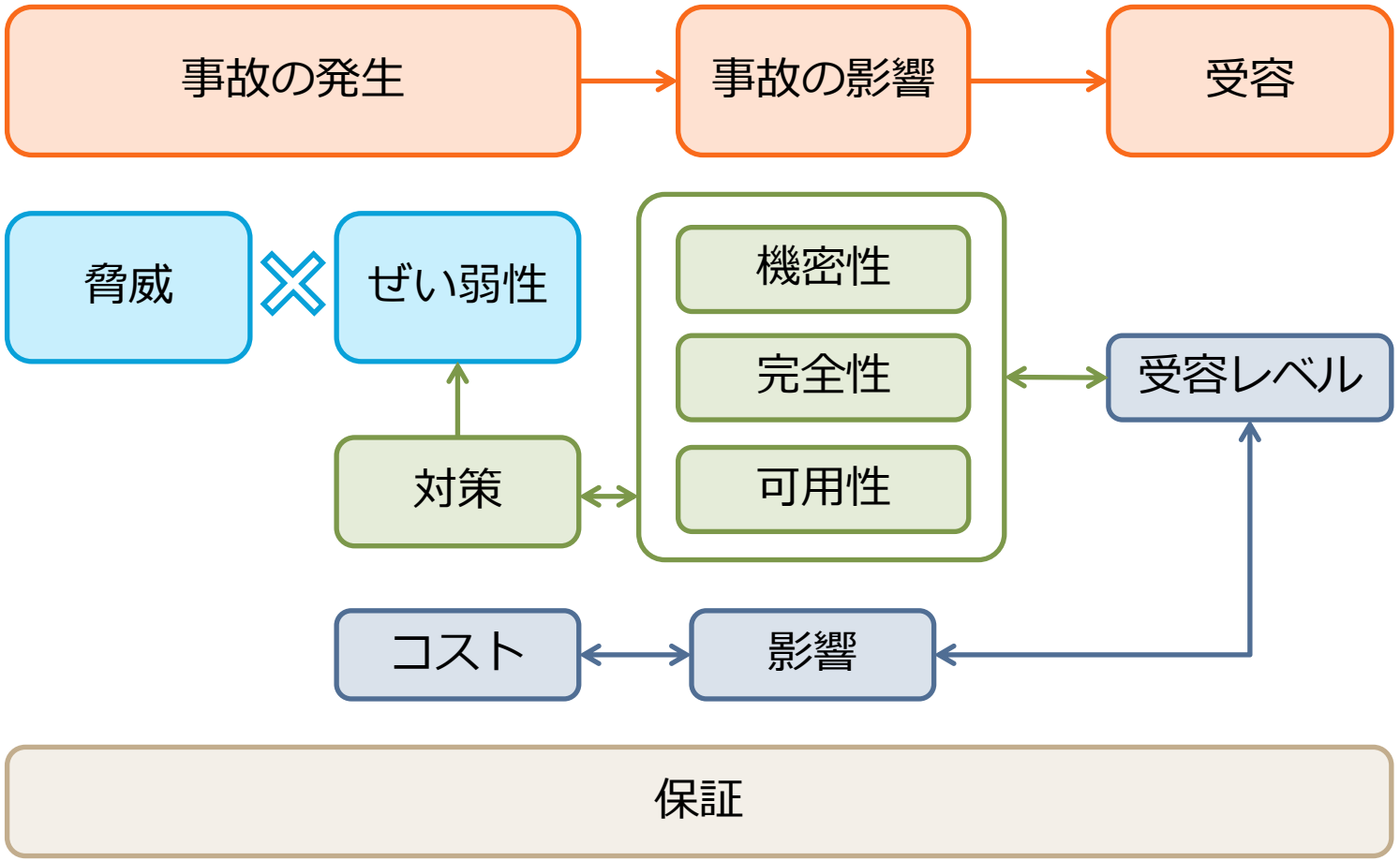
- 情報セキュリティにおいては、事故の兆候が把握できるようになることが重要です
  - 事故が起きる前には、いつもと違った現象が発生していることがほとんどです。事故であっても、犯罪であっても、準備段階で気づくことができれば被害は最小限に収まります
- 日常の監視による把握が重要です
  - 監視対象が増えると管理が大変になり、管理できない情報が増えてきます

日常を知ることが「異常」を知ること



- ゼロデイ攻撃には気づけないのか
  - 監視のポイントが「ウイルス感染」では気づけない
  - ウイルスはなにをするのか、そこを監視する
    - サーバに接続
    - メール送信 など
  - いつもと違う行動はないか
- システムだけでは気づけないことも
  - 特権業務のワークフロー
  - 申請していない業務が実施されていないか

リスクマネジメントフレームワーク



「情報資産の保護」からの脱却

- 情報セキュリティの３つ項目と影響の関係
  - 可用性・・・情報が使えない時の影響の度合い
  - 完全性・・・情報が壊れてしまった時の影響の度合い
  - 機密性・・・情報が漏れてしまった場合の影響の度合い
- 情報資産の重要度についてはあまり考えなくても良い
  - 重要度は主観的であることが多く、定量化できない
  - 情報資産そのものの価値よりも、それをとりまく環境のほうが重要な判断要素となることが多い
- 影響に合わせたコスト計算が必要
  - 情報セキュリティはどこまでやればよいのか

「個人情報」というラベルはうまく活用できない

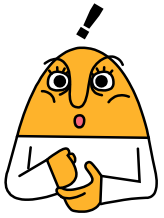
ガバナンスを効かせるための情報管理の考え方

誰がやっても同じ結果が出るために

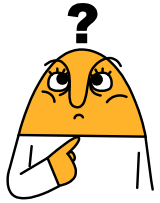
- 情報セキュリティは「科学」です
  - 人間は失敗する。これが最大のリスク。
  - 個人の努力に依存していると情報セキュリティは失敗します
  - 誰でもが同じ方法でやればちゃんと安全を確保できる情報セキュリティ対策を考えていく必要があります
- 複雑なパスワード、推測しにくいパスワード？
  - どんなに複雑なパスワードを付けても、インターネット上で攻撃される確率は変わりません
    - 人間が手で打たなくちゃいけない時だけに対応できる対策
  - 目的に応じたセキュリティ対策を検討しましょう

書類ラベルは「行動」がわかるように

社内だけの閲覧
社外持ち出し禁止



大事にしなくちゃいけない？



- 書類だけを見てわかる？
  - 個人情報というラベルは実は意味が無い
    - オーナーはご本人
    - 利用者は○○部の人
    - 管理者は○○部

    →これは「取扱注意」で十分に設定できる
- 行動がわからないとシステムに落とせない
  - システムで扱うためにはケイパビリティを明確にしなければいけない
  - システムに落とせなければ監視することもできない

ガバナンス視点での情報管理

- 情報資産が増えると、管理コストが増える
  - 出来る限りコピーを増やさない
    - 情報は一元管理することが最も管理コストが減り、ライフサイクルにおける管理が容易になる
    - 個人情報保護法ができた時にも内閣官房からは個人情報を一元管理することという提案があった（はずなのに・・・）
  - 紙は管理がしにくい
    - 紙は暗号化できない、管理のために物理的な対策が必要など、安全性もコストも増大するばかり
    - たとえば、建築現場では紙のデータを車に置いたまま車上ねらいの被害に
      → 対策として、必要な情報は電子化してタブレットなどに入れた。これで車の中に情報を置きっぱなしにしなくなった

セキュリティは機能ではなく業務で

- メールの送信をするから「暗号化」？
  - メールの送信をする際に「盗聴防止」のために添付書類に「暗号化」や「パスワード付与」をしています
  - でも、同じ経路（メール）でパスワードを送っているなんてことはありませんか？
- 情報セキュリティの目的を明確に
  - 情報セキュリティはITセキュリティです
  - ITを最大限に活用するために必要最低限のセキュリティ対策を行いましょう
  - 過剰なセキュリティ対策を行わないためにも、情報資産ベースではなく、業務ベースのセキュリティ対策を実施しましょう

IPAの動画サイトもご覧ください

3つのかばん
－新入社員が知るべき情報漏えいの脅威－

〈乗っ取り〉の危険が
あなたのスマートフォンにも！

あなたの書き込みは世界中から
見られてる －適切なSNS利用の心得－

その他のタイトル

- ウイルスはあなたのビジネスもプライベートも狙っている！
- あなたの組織が狙われている！-標的型攻撃 その脅威と対策-
- 大丈夫？あなたのスマートフォン -安心・安全のためのセキュリティ対策-
- あなたのスマートフォン、ウイルスが狙っている！
- ワンクリック請求のワナを知ろう! -巧妙化する手口とその対策-
- 今　制御システムも狙われている！ -情報セキュリティの必要性-
- 東南アジアの情報セキュリティ -現状と対策について-
- 7分で気づく身近にある情報漏えいの脅威
- キミはどっち？ -パソコン・ケータイ・スマートフォン 正しい使い方-
- ほんとにあったセキュリティの話

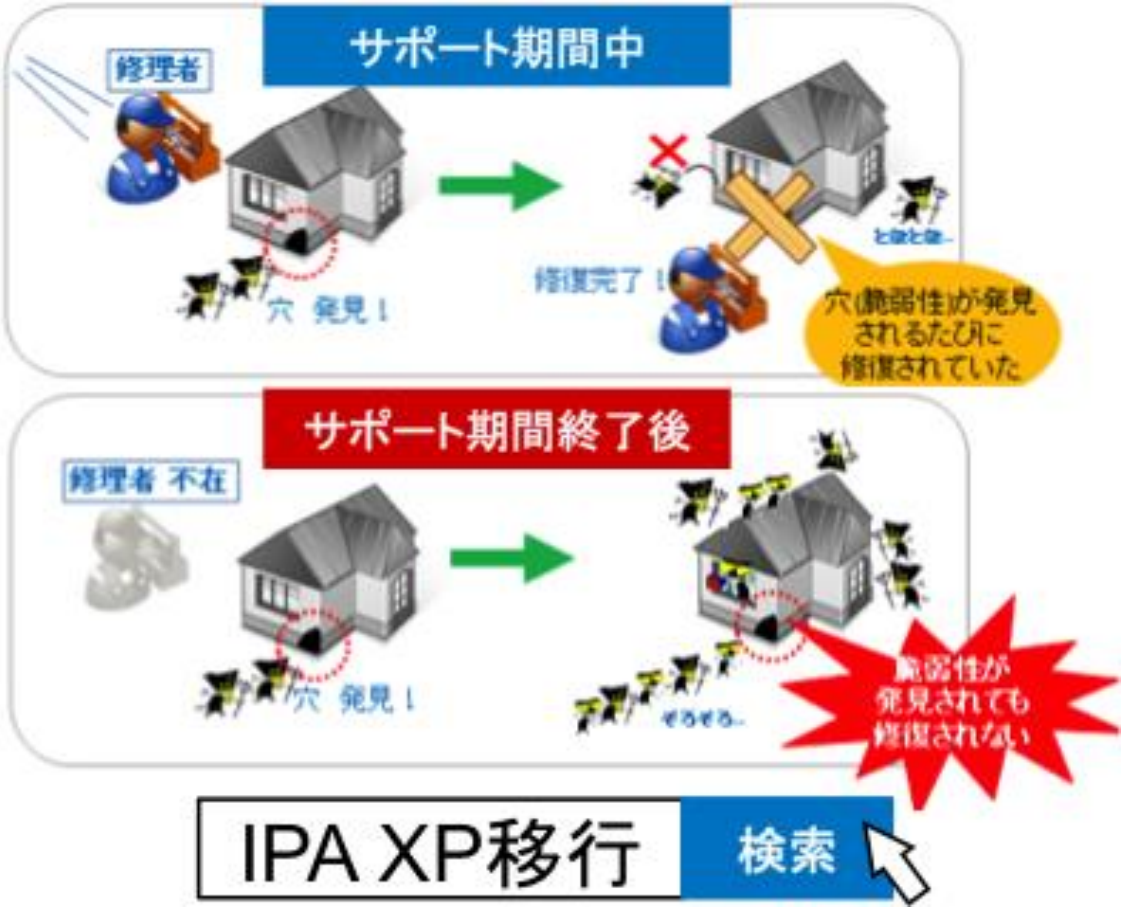
http://www.ipa.go.jp/security/keihatsu/videos/

セキュリティ研修にご利用ください

そのままセキュリティ研修に使える情報が満載です。

http://www.ipa.go.jp/security/antivirus/shiori.html

IPAからのおねがい



Windows XPのサポートが、2014年4月9日に終了しました。

まだ移行していない方は、不正アクセス等を回避するためサポートの継続する後継OS、または代替OSへの移行が望まれます。

iパス ITパスポート試験

IPA

ITを利活用する**すべての社会人・学生**
のための**国家試験**

iパス公式キャラクター
上峰　亜衣

情報セキュリティ対策の重要性の高まりを踏まえ、
情報セキュリティの出題を強化！

i パス　検索

お問い合せは

独立行政法人 情報処理推進機構
セキュリティセンター

〒113-6591
東京都文京区本駒込２－２８－８
文京グリーンコート センターオフィス１６階
ＴＥＬ ０３（５９７８）７５０８／ＦＡＸ ０３
（５９７８）７５１８
電子メール　isec-info@ipa.go.jp
ＵＲＬ　http://www.ipa.go.jp/security/