被害を最小限にするための情報管理とガバナンス

株式会社ディアイティ セキュリティサービス事業部 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

最近の情報セキュリティ事故をおさらい

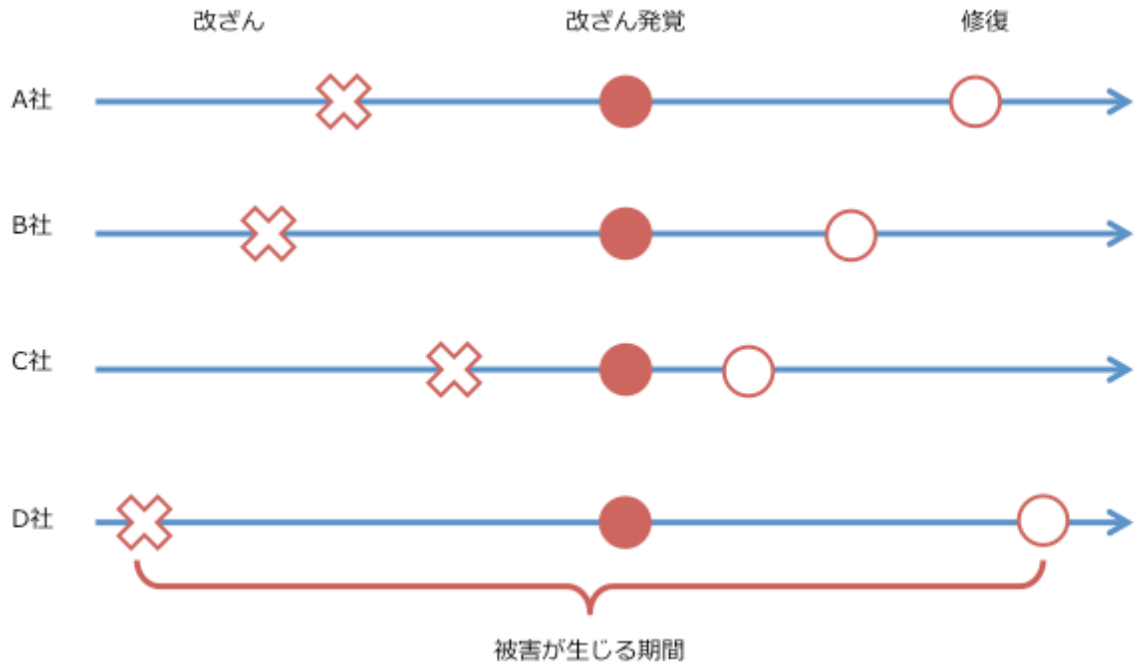
ベネッセ	JAL	ヤマトなど
社内不正による情報の持ち出しと売却	ウイルス感染による情報の不正送信	アカウントリスト型攻撃
関係子会社の契約社員による情報窃盗 持ち出しを制限していたつもりで実際にはできていなかったことが事件が起きた原因 １年近くもの間、事故が起きていたことに気付かなかった	ウイルス感染による、サーバへの不正アクセスと、サーバから取得した情報の外部サーバへの不正送信 システムのパフォーマンスダウンによる調査によって発覚	他社から漏れた可能性の高いアカウント（IDとパスワードの組み合わせ）を再利用した、不正アクセスの試み IDがメールアドレスになっていること、パスワードを使いまわ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

- ベネッセの事故では約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
- JAL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

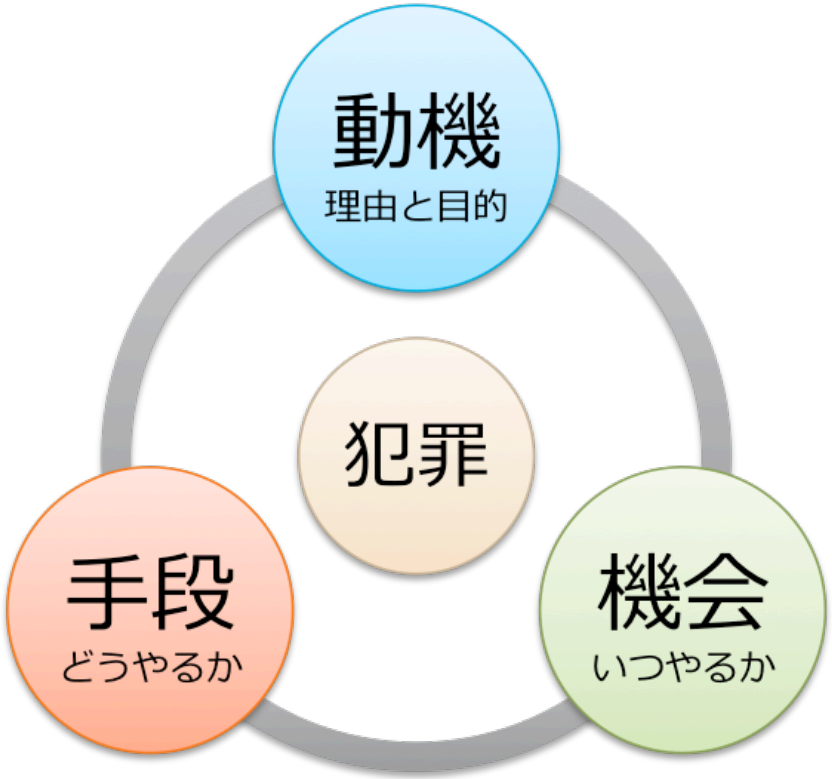
事故の発覚と被害の大きさ

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・・・

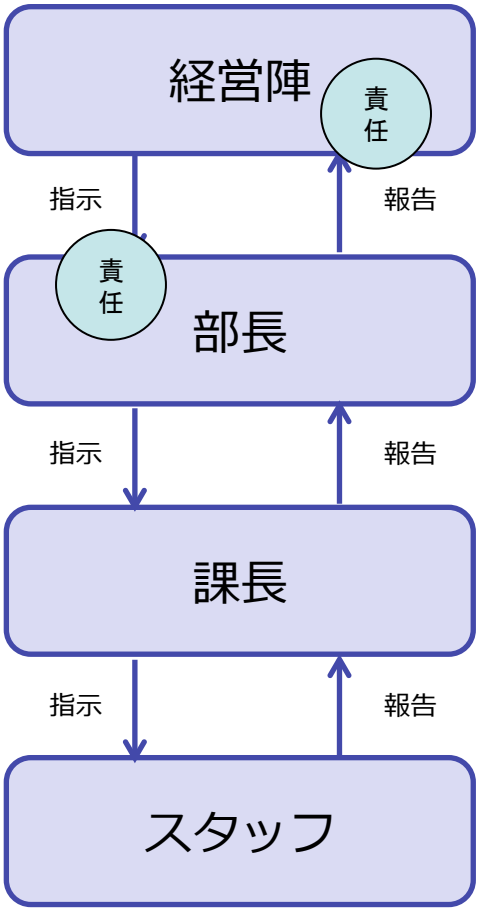


- 犯罪は動機を満足させるまで続く
  - ギャンブルや交遊費に使っている場合は気づかれるまで永遠に犯行は続く
- 事故の防止と抑止
  - 手段と機会をなくすことで犯罪はなくなる
  - 手段はイタチごっこ、まずはきっかけ（機会）を与えない職場環境づくり

組織はどのようにあるべきか

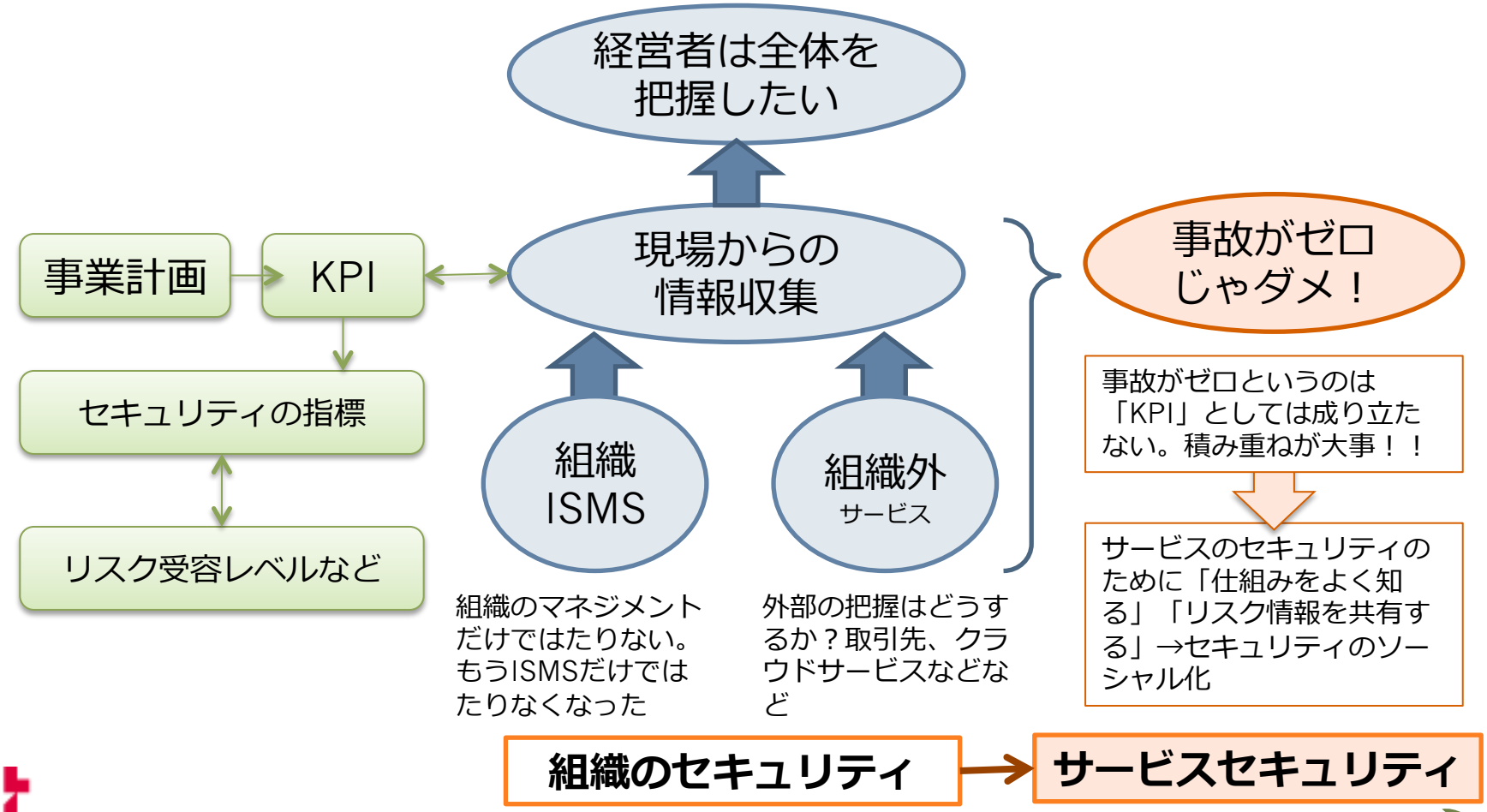
誰よりも早く異常に気づくための情報セキュリティの体制づくり

経営者が責任を負うことができる組織とは

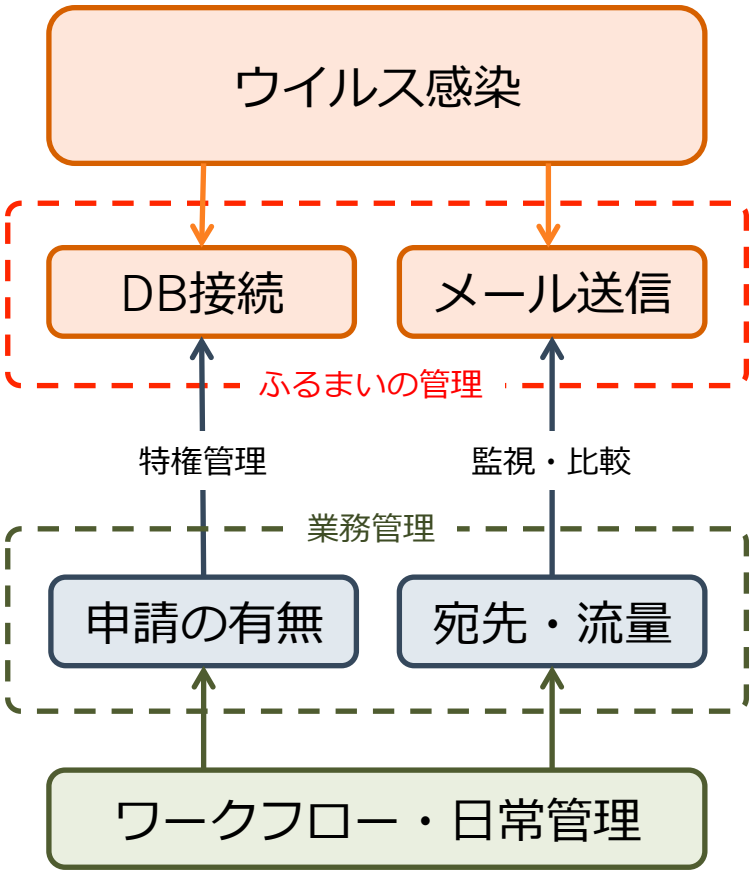


- 指示と報告による組織づくりと責任の明確化
  - 上司は部下に指示をし、部下はそれが完了したことを報告する。もしも問題がある場合は相談や連絡を行う
- 情報セキュリティの最終責任は経営陣
  - 情報セキュリティに関する指示は経営陣が行う
  - それに応えて組織はすべての報告（情報）が経営陣に集まるようにする

ガバナンスとは現場を知ること



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

「個人情報」というラベルはうまく活用できない

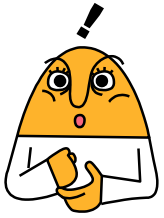
ガバナンスを効かせるための情報管理

誰がやっても同じ結果が出るセキュリティ

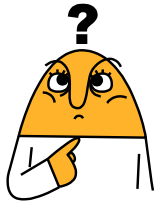
- 情報セキュリティは「科学」です
  - 人間は失敗する。これが最大のリスク。
  - 個人の努力に依存していると情報セキュリティは失敗します
  - 誰でもが同じ方法でやればちゃんと安全を確保できる情報セキュリティ対策を考えていく必要があります
- 複雑なパスワード、推測しにくいパスワード？
  - どんなに複雑なパスワードを付けても、インターネット上で攻撃される確率は変わりません
    - 人間が手で打たなくちゃいけない時だけに対応できる対策
  - 目的に応じたセキュリティ対策を検討しましょう

書類のラベルは「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？



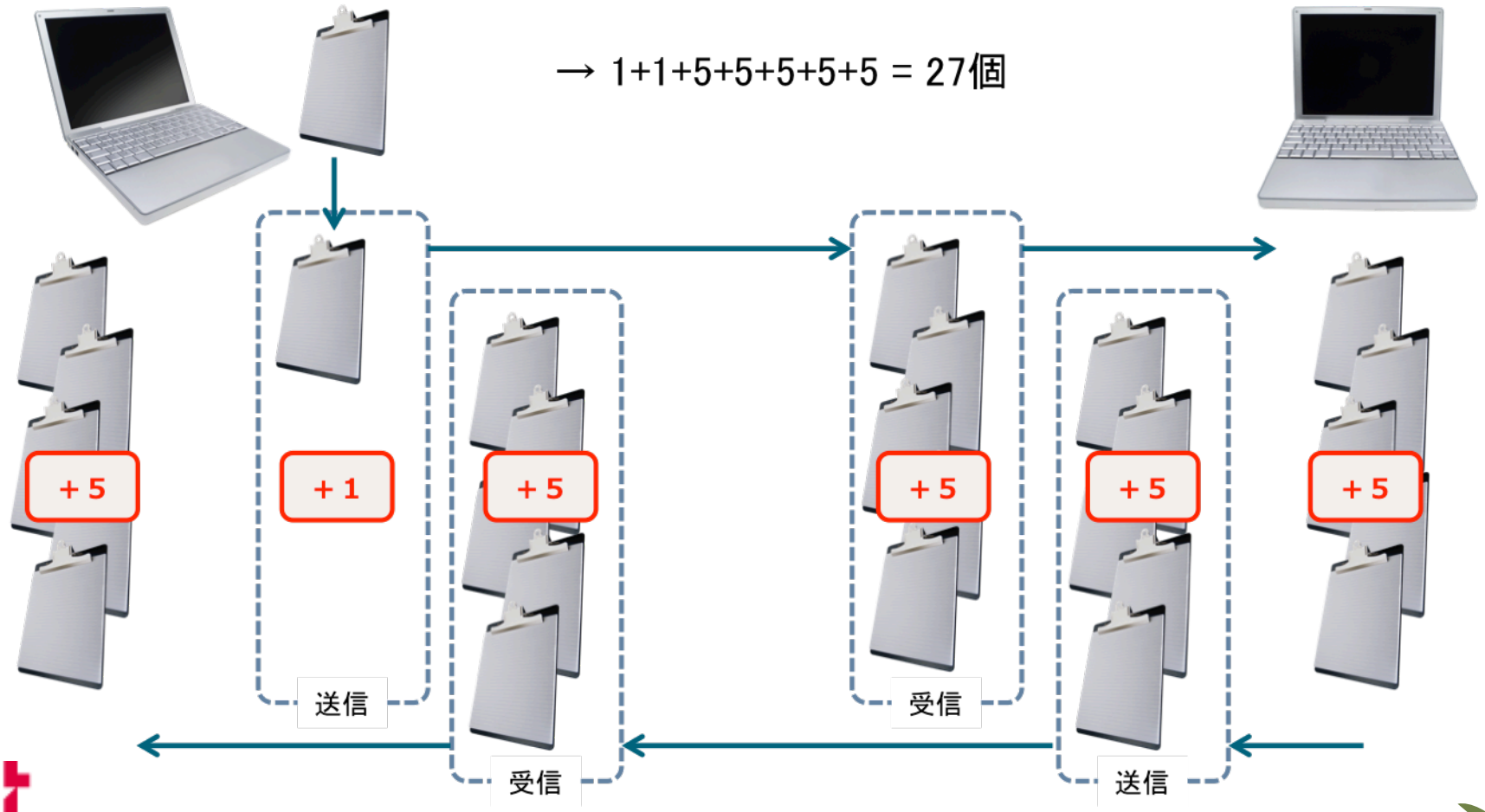
- 書類だけを見てわかる？
  - 個人情報というラベルは実は意味が無い
    - オーナーはご本人
    - 利用者は○○部の人
    - 管理者は○○部

    →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

メールの添付書類は危険？

- 課長が部門の5人にエクセルで管理表を送付しました。社員がこれらに記入してメールに添付して課長に返信した場合、添付書類は全部でいくつになったでしょうか？

実際に数えてみましょう



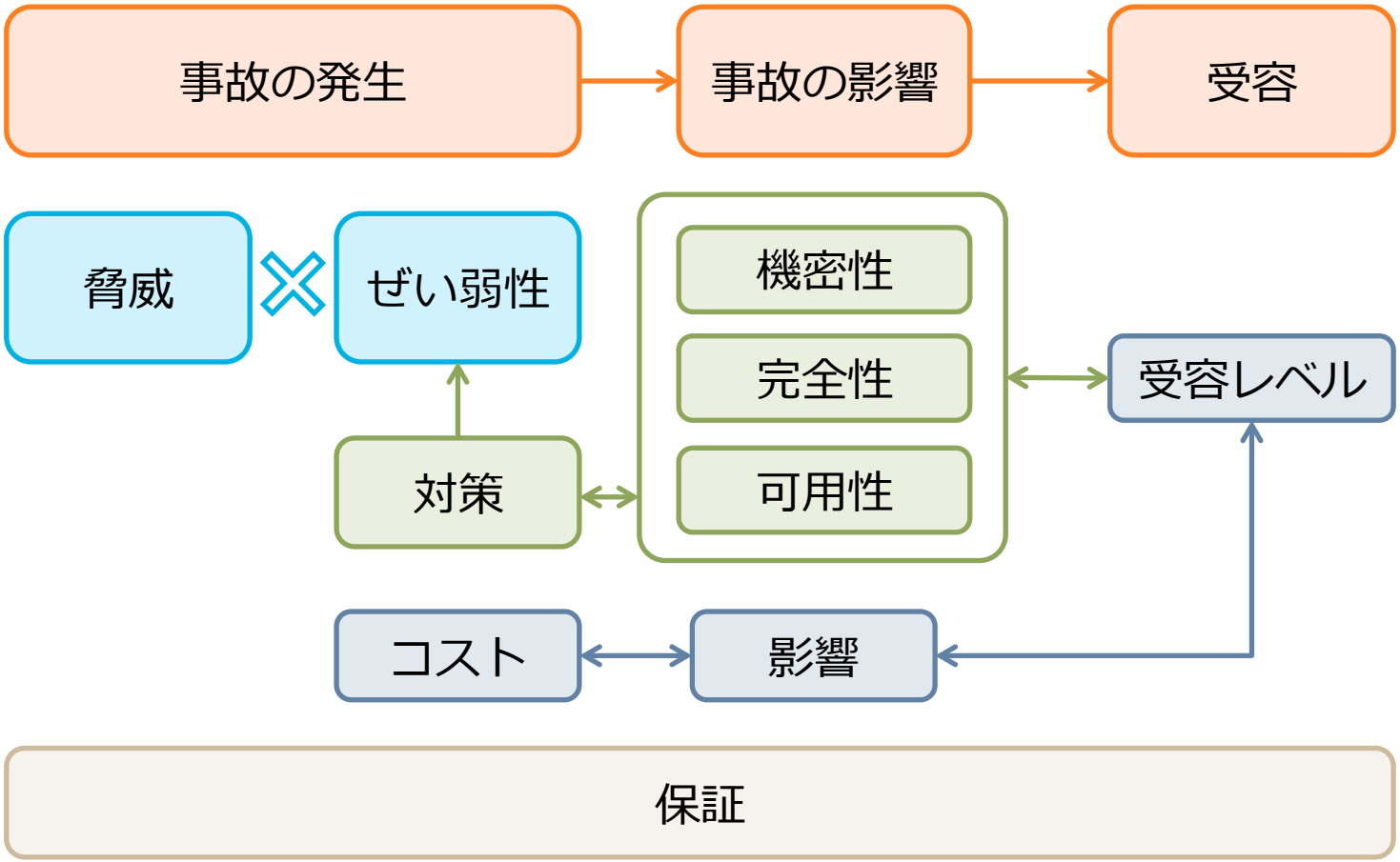
ガバナンス視点での情報管理

- 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考える

- 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
  - 過剰は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

情報セキュリティはどこまでやるか



影響度をベースにリスクマネジメント

- 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

講師の紹介

河野省二（かわのしょうじ）
株式会社ディアイティ
セキュリティサービス事業部 副事業部長
kawano.shoji@security-policy.jp

- 経済産業省
  - クラウドセキュリティ研究会
  - セキュリティガバナンス研究会
  - セキュリティ監査研究会　など
- 情報処理推進機構
  - セキュリティセンター　研究員
- 日本セキュリティ監査協会
  - スキル部会副部会長
- NPO クラウド利用促進機構
  - セキュリティアドバイザー
- 東京電機大学未来科学部 非常勤講師
- (ISC)2 認定主任講師　など