RITSUMEIKAN UNIVERSITY

# 『事件駆動型セキュリティ』から脱却するための戦略とは？

立命館大学情報理工学部　上原哲太郎

Futurize.
きみの意志が、未来。

# 企業経営に課題は多い…

物価高騰
原材料費上昇

人材不足
生産性問題

伸びない
個人消費

賃上げ圧力

# そのせいかITは後回し・丸投げに

セキュリティは
金食い虫なので
最低限でやっといて！

それよりDXお願いね！

予算は限られるから
削りしろも考えて！


IT関連になると
自分の仕事だと
思わなくなる人は多い
経営も現場も
そこで思考停止

セキュリティだと
その傾向は
さらに強まる

# 経営陣にわかってもらうには…？

どうすれば経営陣に
セキュリティの重要性が
わかって貰えるかねぇ？

いっそインシデントでも
起きりゃ気がつくだろ
（邪悪）

# 「インシデント待望論」は割とある話

- 多くの人は「数字」や「論理」より「物語」に心を動かされる

- セキュリティも事件があればその対策が急務とされて組織や制度の改革が進む

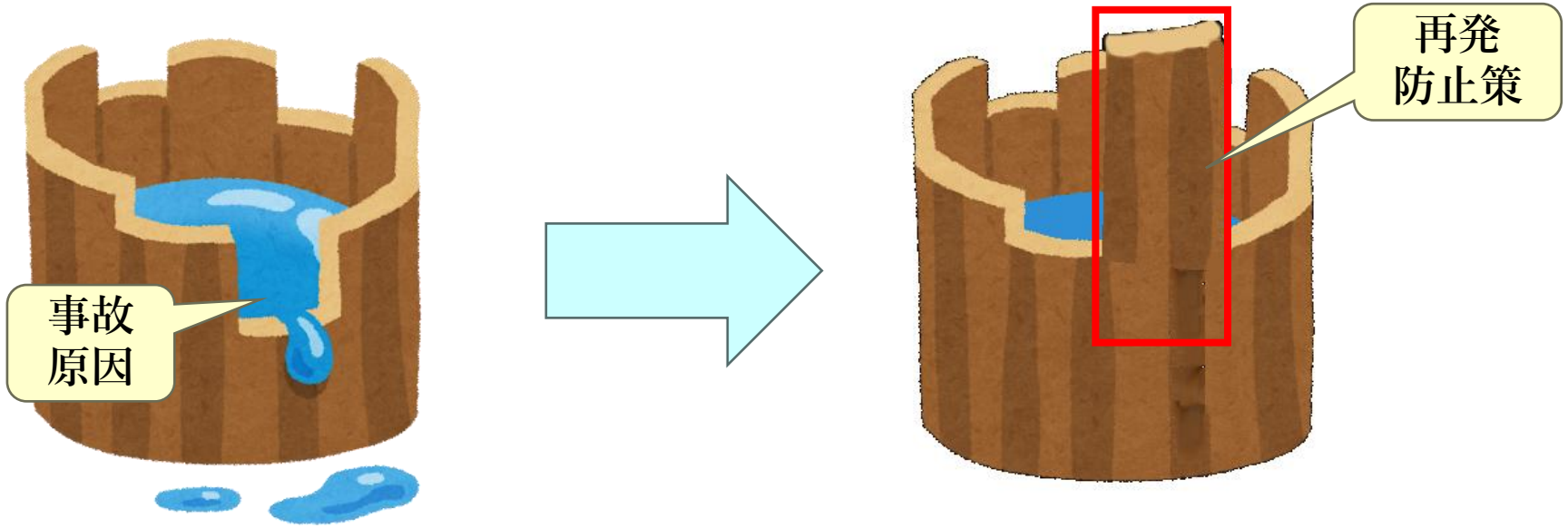
# 大きな事件の後には変化がある

- 第三者委員会が事件後ずっと伴走する例
- 法改正や制度が変わった例
  - ベネッセ事件（2014）→個人情報保護法の改正
  - 年金機構事件（2015）→自治体強靭化

- 事件事故の教訓を生かすのは良い、が…

# 「事件駆動型セキュリティ」の欠点

- 「再発防止」「同事故防止」に重点
  しばしばバランスを欠く対策になる
- 持続的ではない・喉元過ぎれば…



# よくある話…

事件発生

再発防止・対策強化

対策技術の導入

運用でカバー


抜け穴探索…
別のところにリスク…

# 何が欠けているのか

- 事件事故から学ぶことは悪くない
- ただし、教訓を取り入れるときは「セキュリティ対策優先順位」の変更だけを行うべき
- セキュリティ強化のために業務の効率を落とすのを出来るだけ避けるべき
  - つまり、業務プロセス見直しの機会とすべき

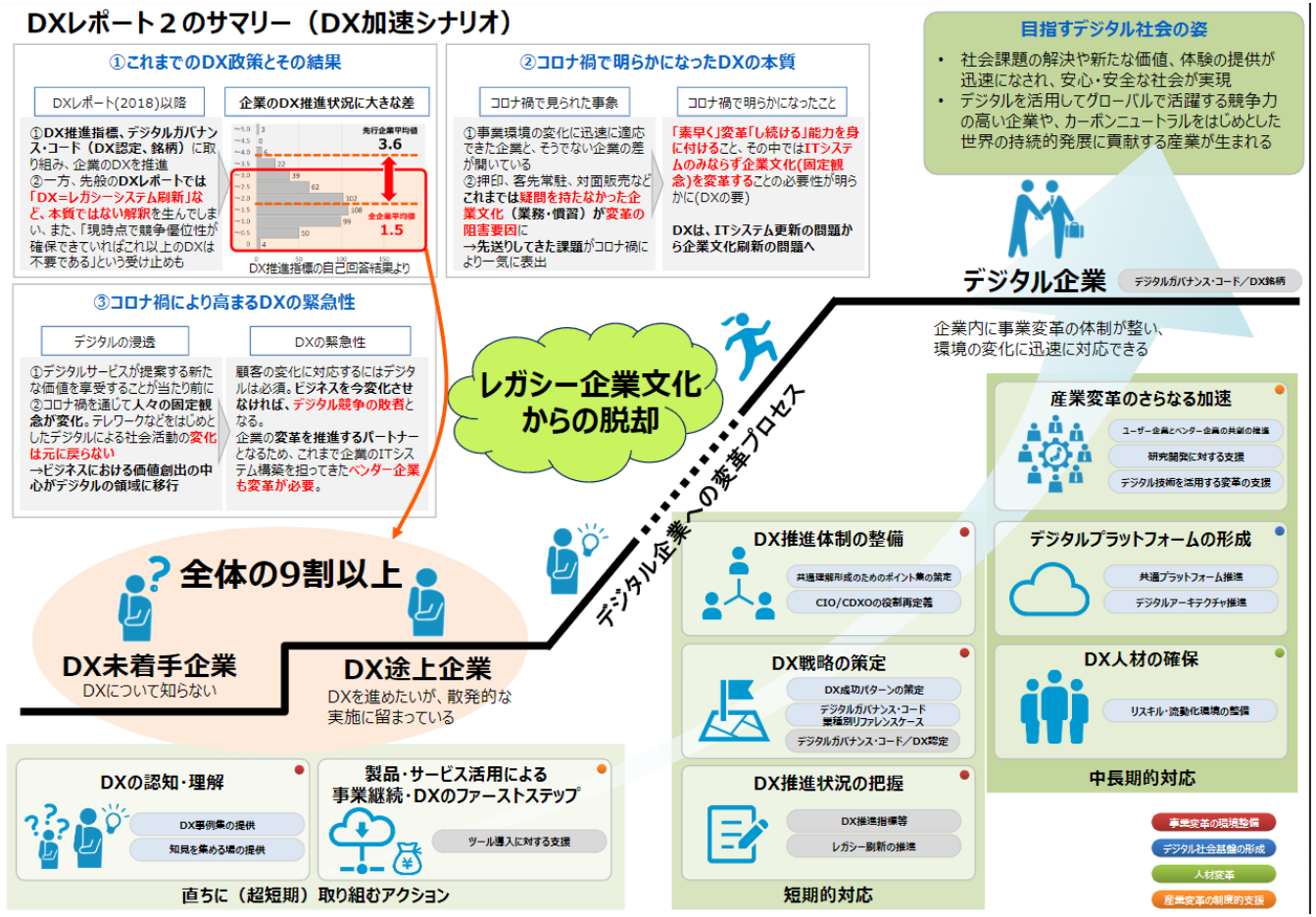
# どういうことかというと…

- 「ランサムウェアにやられました！」
  - 原因：VPNの脆弱性を突かれた
    - 脆弱性管理の徹底→生産性を落とすものではないのでOK
    - 認証手法の変更→内容によっては手間を増やすので
      できるだけ手間の少ないものを
      - そもそもVPNないとだめなのか？から始めるのも手かも
  - 原因：怪しいリンクを踏んでファイル開いた
    - Webフィルタリングの強化はOKだが…

# 業務効率＝生産性とセキュリティは両立する

- 脆弱性対策はシステム管理でやればよい
- 現状狙われているのは「人」に不定型なデータを拾わせる機会
  本当にそのデータを人手で扱わせるのは必要なのか問い直す
- そのためにワークフローの分析と業務のシステム化を進める


# デジタル・トランスフォーメーション(DX)

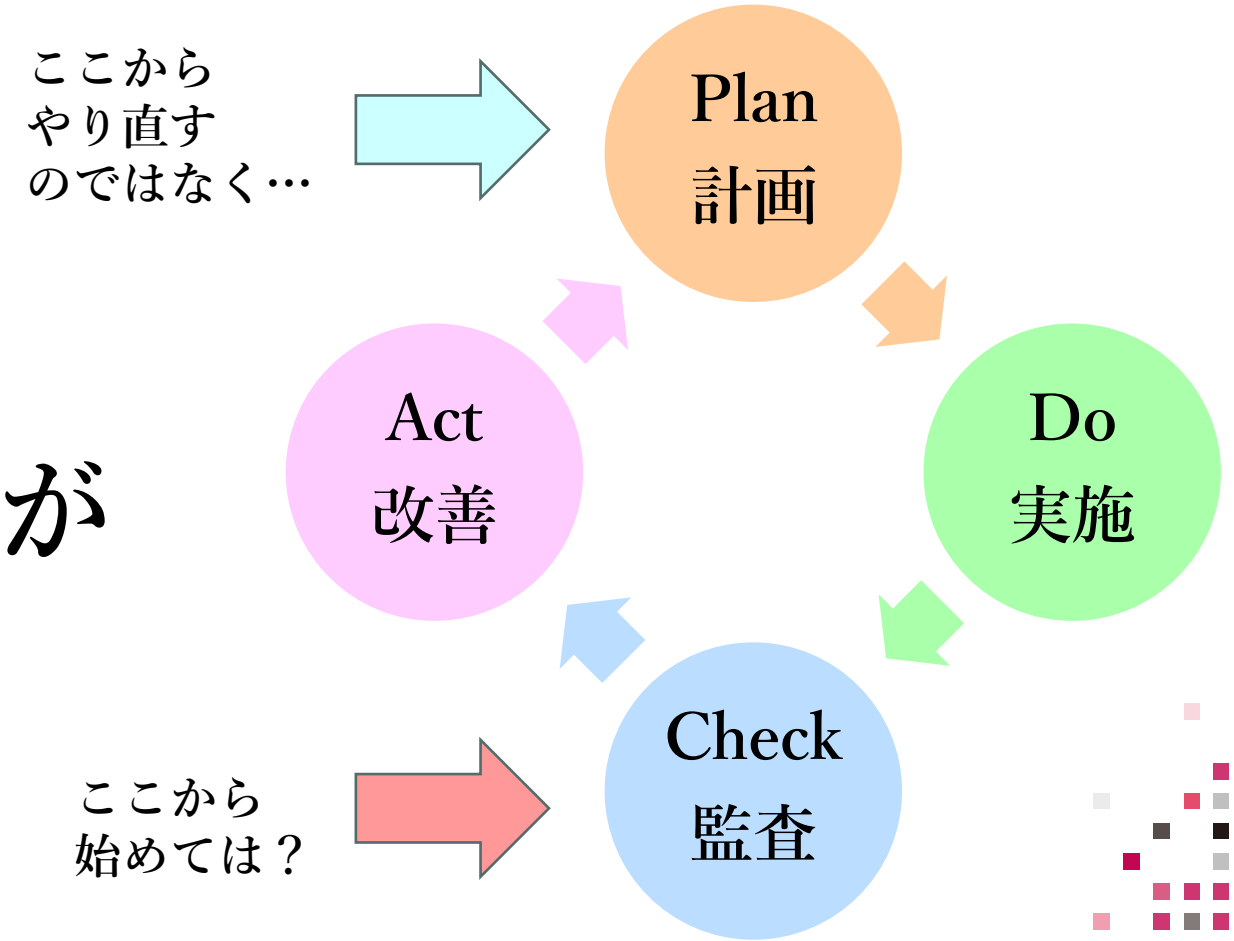



経済産業省「DXレポート２」

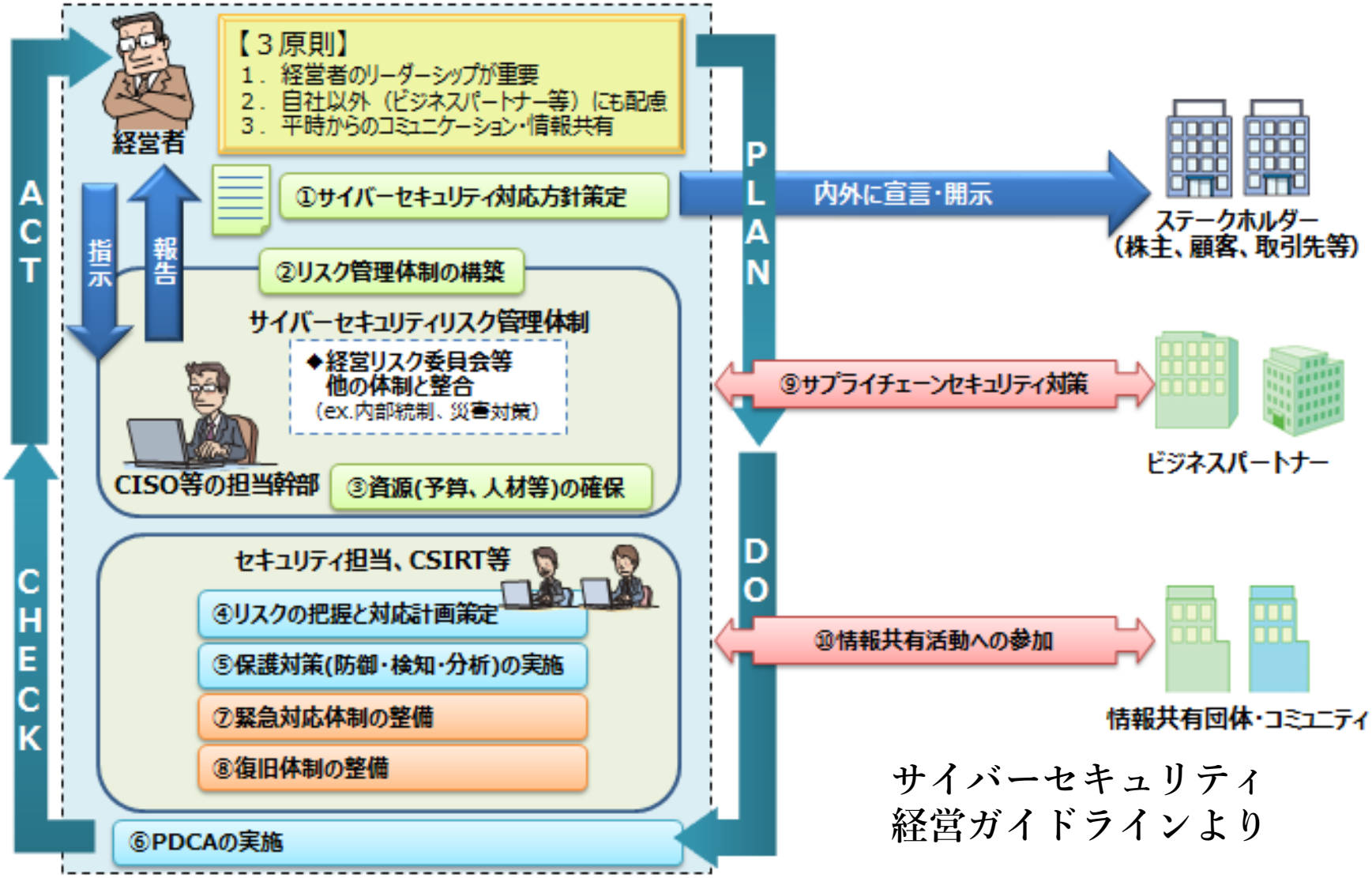
- 単なる
デジタル化ではない
- 本質はICTによる
付加価値創造
- 大切なのは
生産性向上を
- セキュリティは
できるだけ
システム側で担保

# PDCAのCから始めては？

- 事件の教訓を
  生かすときに
  まず現状の
  セキュリティ対策が
  どうだったか
  見直しては？



# まずはガバナンスから




サイバーセキュリティ
経営ガイドラインより

# サイバーセキュリティ経営ガイドライン Ver.3

- サイバーセキュリティ経営の３原則
  1. 経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
  2. サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
  3. 平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

これに沿った重要10項目を提示

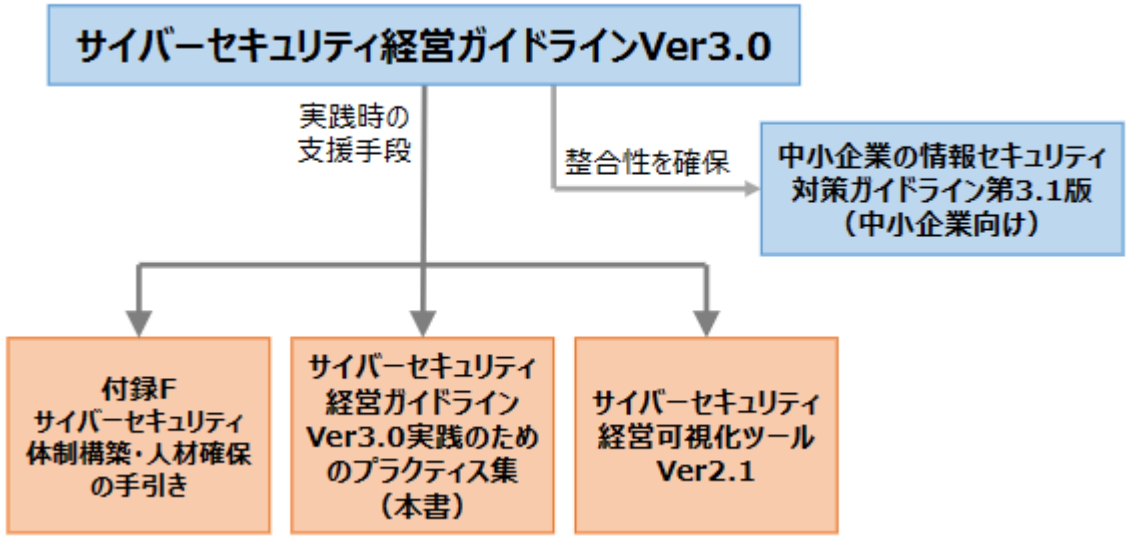
セキュリティそのものを投資と捉えるべきとする記述を強調　リスクマネジメントの考え方を明記

# まずはマネジメントを確立しよう

サイバーセキュリティ経営ガイドラインVer3.0
実践のためのプラクティス集　第4版

IPA
独立行政法人　情報処理推進機構

- IPAから出ている
  プラクティス集は
  実践的内容でオススメ

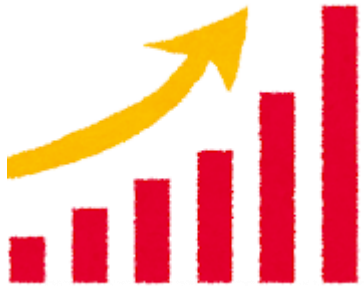


# リスクアセスメントの一歩は情報＆機器の把握精度

- 重要情報がどこにあるか
  ＆誰が管理してる・アクセス可能か
  把握漏れがあると対策は無理
- 機器把握も同様に重要
  脆弱性管理漏れが怖いのは「野良IoT」

# 経営陣に理解してもらうためリスク可視化を

- いわゆるインシデント未満の「ヒヤリハット」件数を集めてグラフ化するだけでもOK
- もちろんSIEM/UTMなどがあれば尚よし



# 情報セキュリティマネジメント試験
# 情報処理安全確保支援士


国家試験

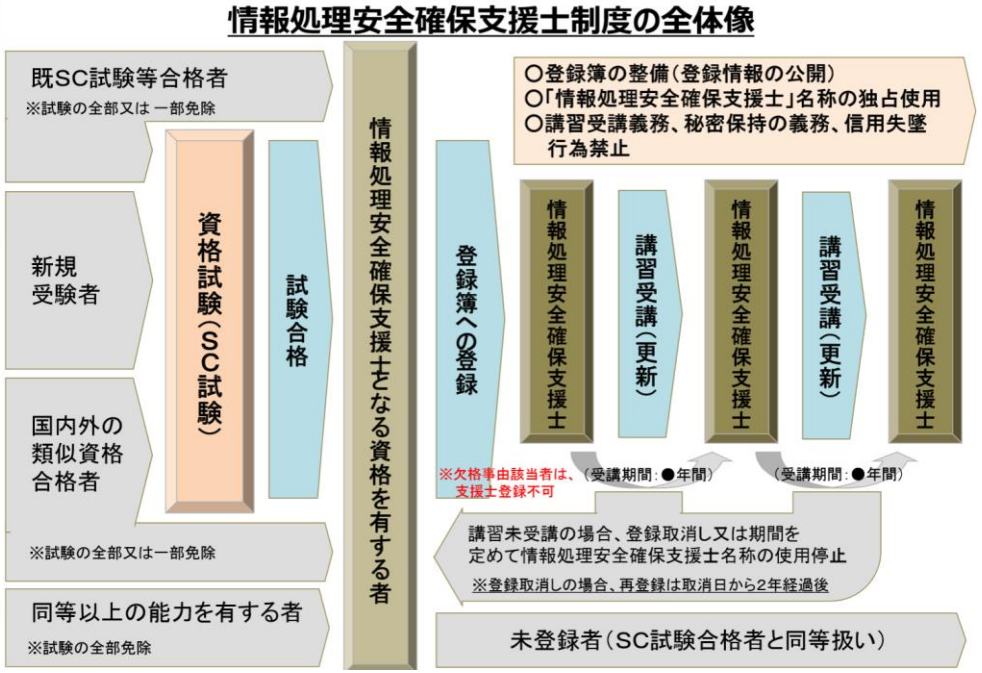
## 「情報セキュリティマネジメント試験」とは？

NEW!

ITの高度化やインターネットの普及が社会に様々な恩恵をもたらす一方、サイバー攻撃の手口はますます巧妙化・複雑化し、社会全体に対する非常に大きな脅威となっています。

「情報セキュリティをいかに確保するか」は今や組織にとって大きな経営課題ですが、標的型攻撃、内部不正などの多種多様な脅威は、「ITによる対策（技術面の対策）」だけではなく、適切な情報管理、業務フローの見直し、組織内規程順守のための従業員の意識向上といった、「人による対策（管理面の対策）」についてもしっかりとした取組みが重要です。
そのための情報セキュリティマネジメントを担う人材の育成をいかに推進していくかが、社会全体での課題であると言えます。

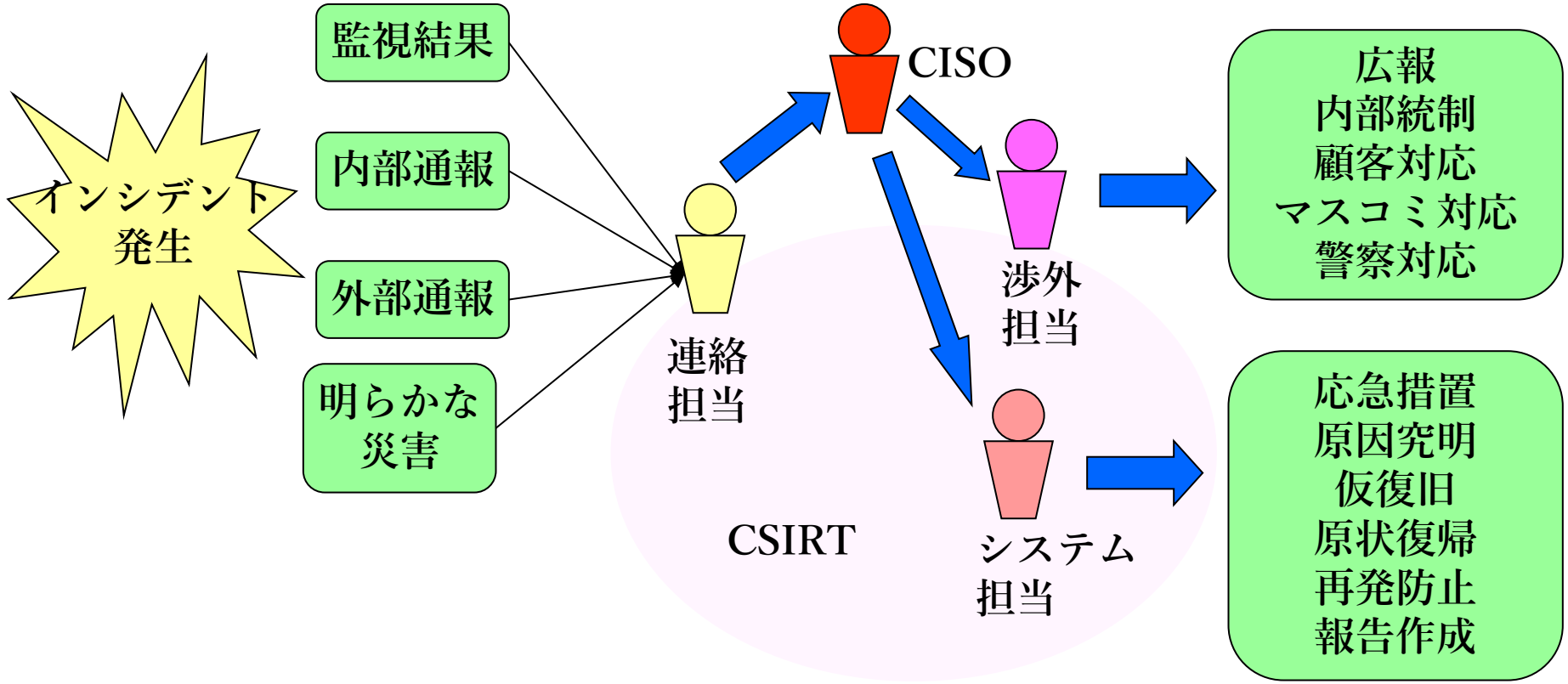
「情報セキュリティマネジメント試験」は、このような社会ニーズの高まりを背景に、政府の『「日本再興戦略」改訂2015』（平成27年6月閣議決定）や経済産業省 産業構造審議会で示された方向性を踏まえて、国家試験「情報処理技術者試験」の新たな試験区分として創設されました（平成28年度春期から試験開始。春期（4月）、秋期（10月）の年2回実施）。




あたらしい資格試験
より経営サポートをする層を創出

従来の情報セキュリティ
スペシャリスト
試験合格者を中心に「士業」に
登録・更新制を採る

# 緊急時対応計画は傷を浅くするためのもの



# DBのセキュリティは内部不正が大きな脅威

- 内部不正防止の基本原則
  - 犯行を難しくする
  - 捕まるリスクを高める
  - 犯行の見返りを減らす
  - 犯行の誘因を減らす
  - 犯罪の弁明をさせない
- 情報セキュリティ対策に
  内部通報の体制や
  モニタリング告知など
  主に人事・労務管理の面から
  必要な項目を加えたもの

# 具体策は付録が分かりやすい

## 付録Ⅵ：内部不正防止の基本 5 原則と 25 分類

状況的犯罪予防に基づく、内部不正防止の基本 5 原則と 25 分類、及び各々の対策例、関連する本ガイドラインの対策項目を以下に示します。「主な対策項目」は、本ガイドラインの対策項目の番号を表しています。

（出典）5 カテゴリ 25 分類は、社会安全研究財団：「環境犯罪学と犯罪分析」 P191 を参考とし、IPA が作成

| 基本 5 原則と 25 分類 | 対策例※ | 主な対策項目 |
|---|---|---|
| 犯行を難しくする(やりにくくする)：対策を強化することで犯罪行為を難しくする | | |
| 対象の防御策を強化する | アクセス制御、パスワードポリシーの設定、退職者の ID 削除、セキュリティワイヤーによる PC 固定 | (5)(6)(7)(9)(15)(24) |
| 施設への出入りを制限する | 外部者の立ち入り制限、入退出管理 | (8) |
| 出口で検査する | ノート PC 等の持ち出し検査、メールやネットの監視 | (8)(10)(12)(18)(19) |
| 犯罪者をそらす | 物理レベルに応じた入退制限 | (8) |
| 情報機器やネットワークを制限する | 未許可の PC/USB メモリの持ち込み禁止、SNS の利用制限、ホテル及び公衆の無線 LAN の利用制限 | (11)(13)(16) |
| 捕まるリスクを高める（やると見つかる）：管理や監視を強化することで捕まるリスクを高める | | |
| 監視を強化する | アクセスログの監視、複数人での作業環境、情報機器の棚卸し、モバイル機器の持出管理、入退室記録の監査 | (6)(8)(9)(10)(12)(18)(19)(33) |
| 自然監視を支援する | 通報制度の整備 | (32) |
| 匿名性を減らす | ID 管理、共有アカウント廃止、台帳による持出し管理 | (7)(9)(10) |
| 現場管理者を利用する | 単独作業の制限 | (29) |
| 監視体制を強化する | 監視カメラの設置、機械警備システムの導入 | (8)(12) |
| 犯行の見返りを減らす（割に合わない）：標的を隠す/排除する、利益を得にくくすることで犯行を防ぐ | | |
| 標的を隠す | アクセス権限の設定、モバイル機器等の施錠保管、覗き見防 | (5)(6)(9)(16) |

「内部不正防止ガイドライン」付録VI抜粋

# JNSA DBS-WGの前身でもガイドラインを…

DB 内部不正対策ガイドライン

第 1.0 版

2015 年 9 月 29 日

データベース・セキュリティ・コンソーシアム

DB 内部不正対策 WG

1



## 7 DB 内部不正対策マップ

本ガイドラインの対処項目の鳥瞰図を以下の通りに示す。責任者・管理者・分析者の相関関係については「1.2 本ガイドラインの前提」を参照のこと。

この対策マップと先のチェックシートを活用し、未対処項目の可視化と漏れのない対策の実施に役立てて頂きたい。

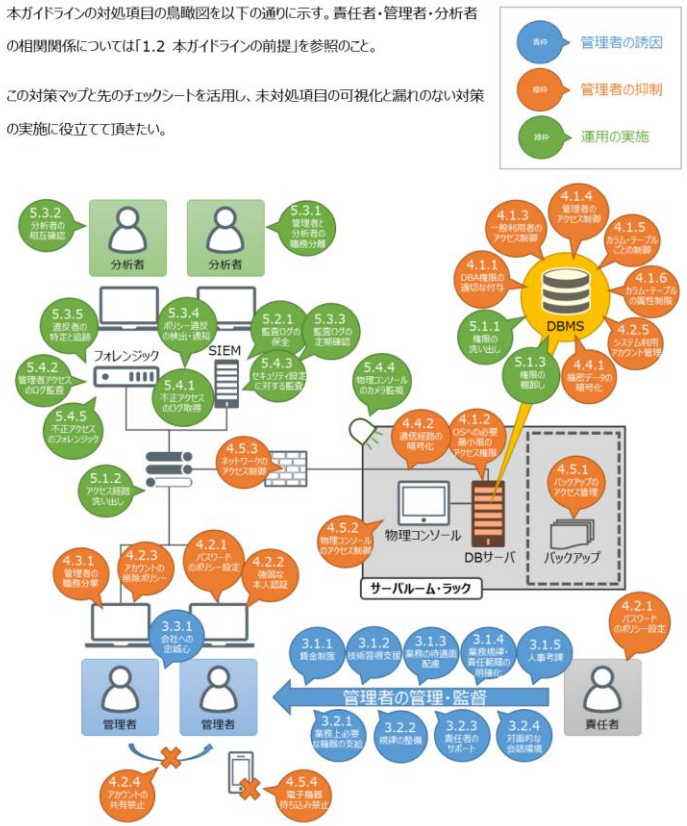



図 7.1 DB 内部不正対策マップ

# 終わりに…

- セキュリティに「これをやればOK」は存在しない
- 下手にセキュリティ機器を入れると業務効率低下
- リスクを減らすには業務から
  「人の手作業」を減らすことが大切
  - そうすれば多くのことが脆弱性管理の範囲に収まる
- セキュリティを自己目的化させず
  ちゃんと業務とリンクさせ続けることが大切