サイバーセキュリティ事始め

～サイバーセキュリティとどう向き合うか？非技術者セキュリティ担当の四方山話～

カーディフ生命保険株式会社
シニアセキュリティオフィサー　森岡　聡一郎

話者について

- 1991年朝日生命保険相互会社入社
  - 営業管理、現地での営業担当を5年経験後、情報システム部門に異動し、導入直後の「オープン系システム」に関する基盤開発やアプリケーション開発担当として5年間過ごす。
- 2002年アクサ生命株式会社に移る
  - 事務企画、ITBRM、マーケティング部門を経て、2008年よりアクサフィナンシャル生命保険においてシステム開発部門のリーダーを経験。
- 2010年カーディフ生命保険会社（当時、現カーディフ生命保険株式会社）に移る
  - ITコーディネータ、システム運用管理リーダーを経て、2012年よりセキュリティオフィサーとして、サイバー、情報セキュリティ対策やBCP策定等に勤しみ中。
- 金融ISAC：AKC WG　座長、スキルアップWG　副座長
- ISACA東京支部基準委員会メンバー
- CISM、CISA、CISSP

はじめに

当講演の内容は、あくまでも話者の経験等に基づいた個人的な見解であり、小職が所属する企業、団体等の公式見解を表すものではありません。

１．サイバーセキュリティは重要な経営リスク

◆ サイバーセキュリティ経営ガイドライン　Ver.2.0（経済産業省）

１．経営者が認識すべき３原則
（１）経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
（２）自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
（３）平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

◆ 金融分野におけるサイバーセキュリティ強化に向けた取組方針　（金融庁）

（P11）
サイバーセキュリティ対策を進めていく上では、経営層の積極的な関与が非常に重要であり、「サイバーセキュリティ戦略」においても、「経営層の意識改革」が掲げられている。金融機関が、実効性のあるサイバーセキュリティ管理態勢を構築するためには、サイバーセキュリティに係るリスクを、

- 技術・システム部門の対応→管理・組織としての対応
- 現場の問題→経営の問題
- IT リスクの領域→危機管理・リスク管理の領域

として認識した上で、組織全体での対応が必要なビジネスリスク・コーポレートリスクとして対策を進めることが極めて重要であり、そのためには経営層の意識改革が不可欠となる。

１．サイバーセキュリティは重要な経営リスク

◆2017年ビジネスリスクマネジメント委員会報告書（公益社団法人　経済同友会）

- 企業のグローバル化に伴うビジネスリスクについて、企業 経営者が特に強い関心を示したのが、①海外 M&A の失敗、②海外子会社の会計不正、③サイバー攻撃であった。（P2）
- 企業経営者は、真のグローバル・マネジメントのために、経営管理機能（人事、財務・経理、IT 等）のグローバル・プラットフォーム化を 実現するとともに、十分なコストをかけてサイバーセキュリティ体制 （態勢）を構築すべきである。 （P7）
- 企業経営者も法務、財務と同様、技術・IT リテラシーを身に付ける必要がある。（P8）

これだけ謳われているにもかかわらず、サイバーセキュリティに関心がない企業・経営層は・・・

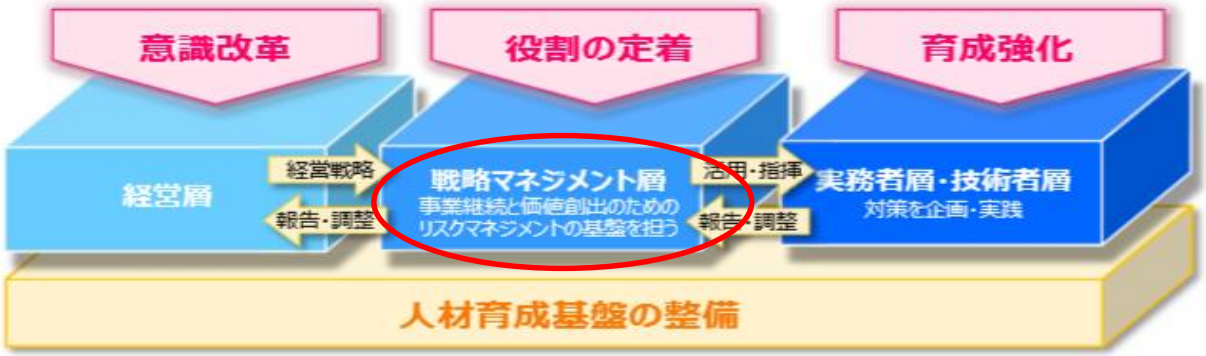
2．CISOは橋渡し人材から戦略マネジメント層へ

◆ サイバーセキュリティ人材育成プログラム（サイバーセキュリティ戦略本部、平成２９年４月１８日発表）

（図７）新しいITの利活用における体制例（２）

- 多様な役割においてサイバーセキュリティの素養を持った人材が必要。
- 経営層のリーダーシップによる体制の下で、橋渡し人材層が様々な部署の実務者層を指揮しつつサイバーセキュリティを推進することが必要。

◆ サイバーセキュリティ戦略（閣議決定）の全体概要　（内閣サイバーセキュリティセンター　平成30年7月27日発表）



2．CISOは橋渡し人材から戦略マネジメント層へ

◆ サイバーセキュリティ人材育成取組方針（サイバーセキュリティ戦略本部　平成30年５月31日発表）

３．サイバーセキュリティにどう取り組むか

投影のみ

３．サイバーセキュリティにどう取り組むか

投影のみ

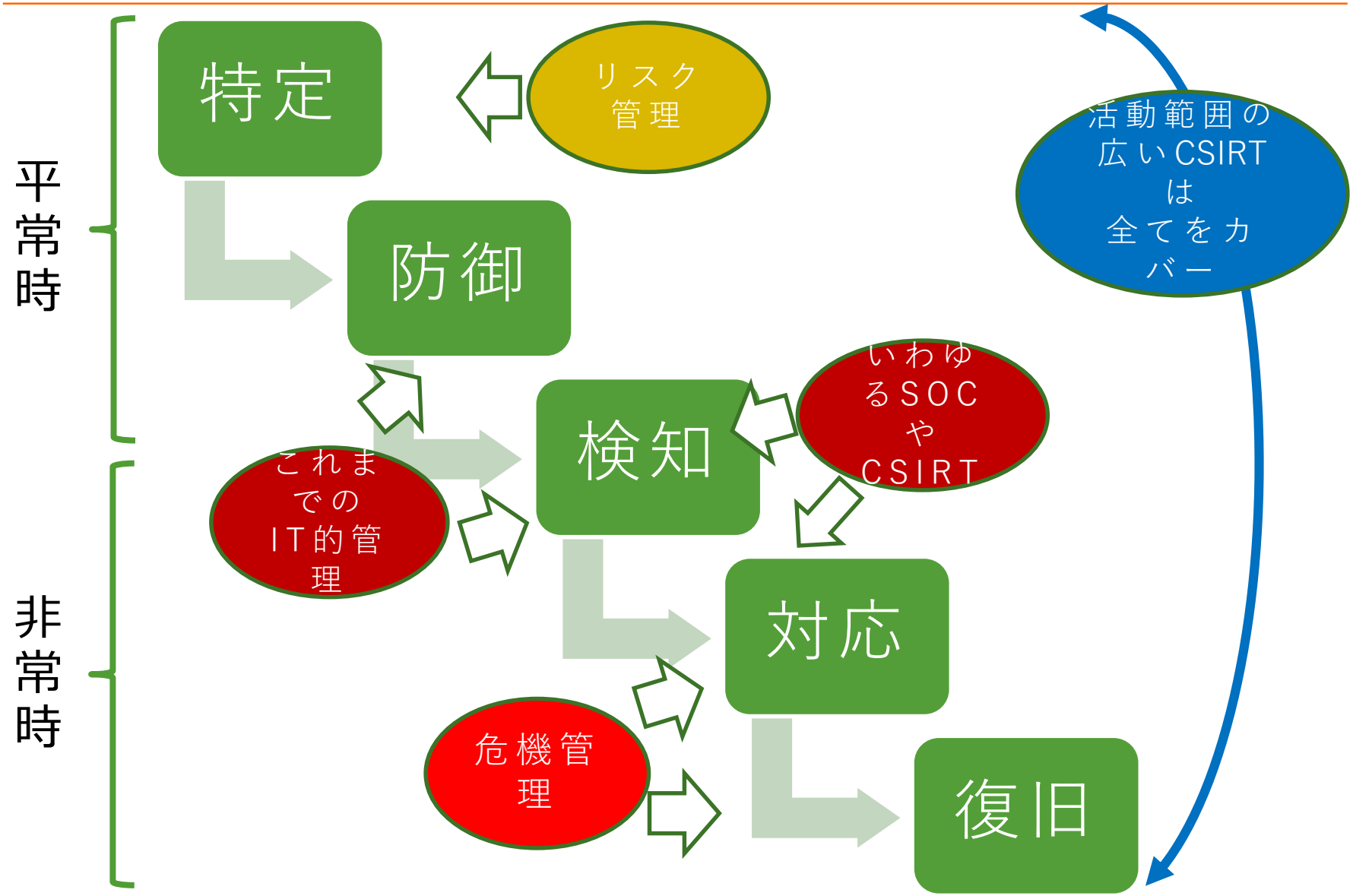
３．サイバーセキュリティにどう取り組むか

投影のみ

３．サイバーセキュリティにどう取り組むか

投影のみ

４．C-SIRT活動をどう進めるか



鎌田敬介著「サイバーセキュリティマネジメント入門」より

5．特定：リスク管理について

敵を知り己を知らば百戦危うからず

◆ 敵を知る

➢ 最新の攻撃手法（目的）や動向を把握する

「世に盗人の種は尽きまじ」

多様化する目的

- ✓ 愉快犯
- ✓ 主義主張（ハクティビスト）
- ✓ 金銭・情報詐取
- ✓ 国内混乱

5．特定：リスク管理について

幅広な情報収集

- ✓ 政府系機関からの提供情報
- ✓ 業界団体からの提供情報
- ✓ 業界ISAC等からの共有情報
- ✓ OSINT（open-source intelligence）

➢ 攻撃手法（内容）と結果事象を想定した影響範囲の特定

影響評価の例

攻撃手法（内容）	可能性	結果事象	影響範囲
DDoS	低	WEB サイトの停止	HP利用不可
ランサムウエア	高	業務上必要なファイルの暗号化	社内業務停止
標的型攻撃	高	社内システムのBot化	重要情報の漏えい
：		：	：

5．特定：リスク管理について

◆ 己を知る

➢ 適切な情報資産評価

「千里の堤も蟻の一穴から」

網羅性の担保と重要性の評価

- ✓ アプリケーション
- ✓ ミドルウエア
- ✓ OS
- ✓ ハードウエア
- ✓ サプライチェーン　等々

5．特定：リスク管理について

➢ 各シナリオに対する影響評価

「段取り八分仕上げ二分」

影響範囲	影響度合い				
	財務	営業	評判	法律・行政	総合
HP利用不可	低	低	低	低	低
社内業務停止	低	低	中	中	中
金銭詐取	高	低	中	中	高
重要情報の漏えい	高	高	高	高	高
：	：	：	：	：	：

5．特定：リスク管理について

己を知る

「NOTICE」ポスター

６．防御、検知：システム管理について

備えあれば憂いなし

- 身の丈にあった対策とは？

「過ぎたるは及ばざるがごとし」
「出船によい風は入船に悪い」

ゼロリスクベースと付和雷同による思考停止

- ✓ 物理分離によりサイバー対策が完了？？
- ✓ 物理分離による業務効率阻害
- ✓ HPがないのに・・・
- ✓ ZIP＋PWDはガラパゴス・・・
- ✓ 100万円の損害予想に1000万円投資？

６．防御、検知：システム管理について

➢ サイバーセキュリティの重要性を理解してもらう

「百聞は一見に如かず」

相手の目線に合わせたコミュニケーション

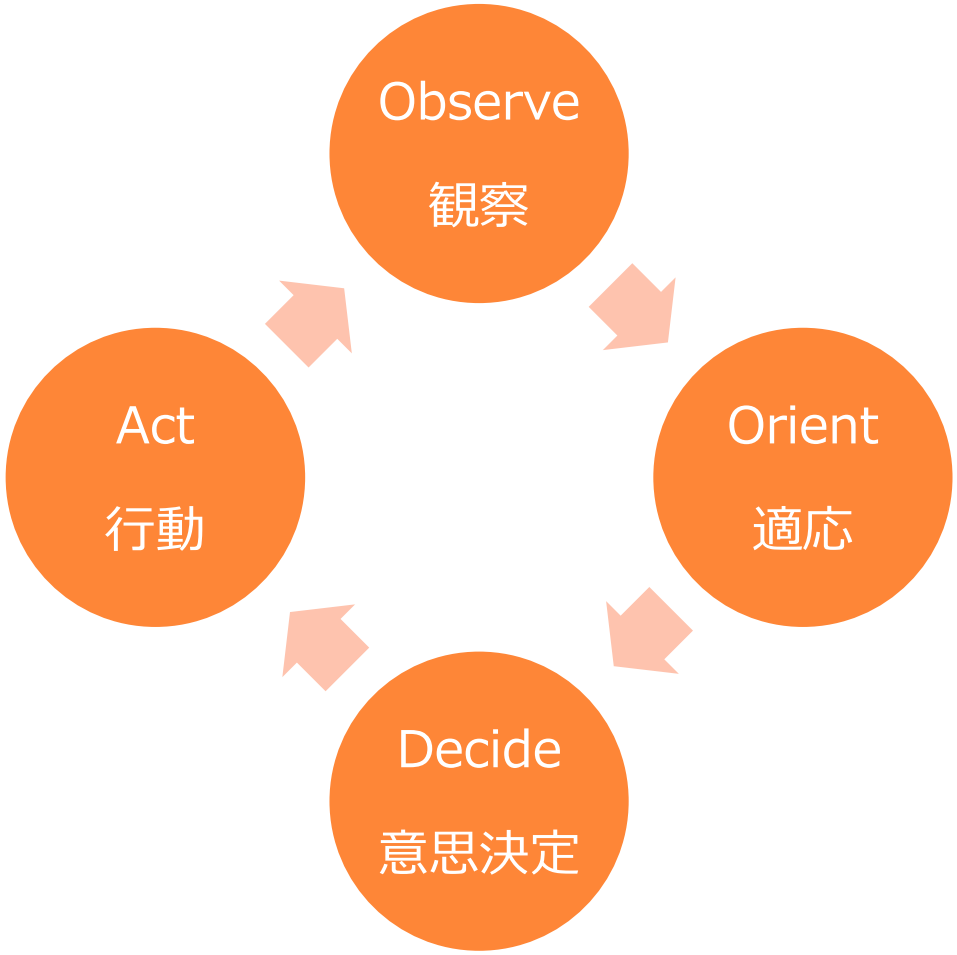
- ✓ 専門用語を排する
- ✓ 具体的事例を挙げる
- ✓ 繰り返す
- ✓ 隠さない風土の醸成

https://cybermap.kaspersky.com/ja/

7．対応、復旧：危機管理

インシデントは会議室で起きるんじゃない！

- 対策はPDCA、インシデントはOODAで対応する



7．対応、復旧：危機管理

“Simple is the best”
「幽霊の正体見たり枯れ尾花」

適切な危機管理とは

- ✓ 軽挙妄動を慎む（サイバーセキュリティシンドローム）
  - 標的型攻撃にやられた？
  - メールサーバが乗っ取られた？
- ✓ 適切な情報収集
- ✓ 役に立たない膨大な手順書
- ✓ ワーストケースの想定
- ✓ シンプルなトールゲートの設定
- ✓ 素早い判断と報告

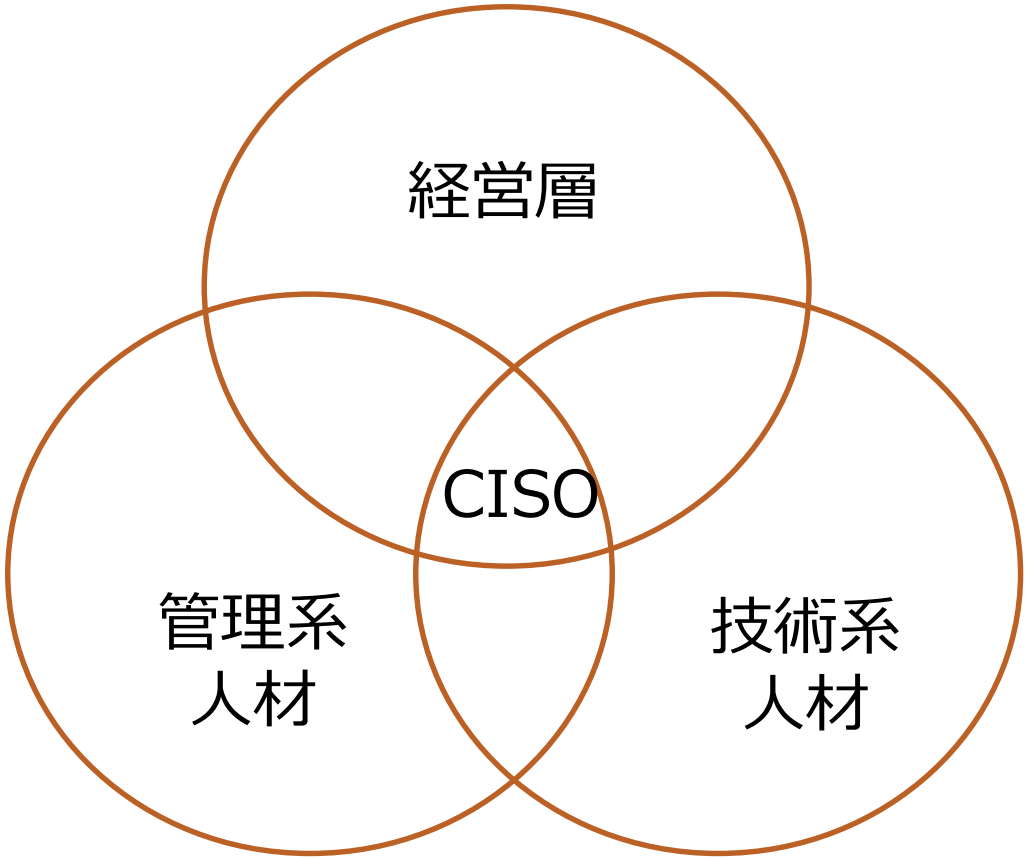
金融ISAC主催：サイバークエスト２（日本経済新聞社提供）

７．対応、復旧：危機管理

投影のみ

7．対応、復旧：危機管理

四人寄れば文殊の知恵



鎌田敬介著「サイバーセキュリティマネジメント入門」より

最後に

本日の講演で大いに参考にさせていただいた著書を紹介します。

- 「サイバーセキュリティマネジメント入門」
  鎌田敬介著　KINZAIバリュー叢書

  アマゾンのサイト

また、直近ですが２月１９日に鎌田さんの講演もありますので、よろしければどうぞ！

- **デジタルイノベーション2019　KEYNOTE**
  「これからの時代を担う人材に必要なIT・セキュリティスキルとセンス」
  2019年2月19日（火）12:30－13:10

  デジタルイノベーション2019申込みサイト

ご清聴ありがとうございました