

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

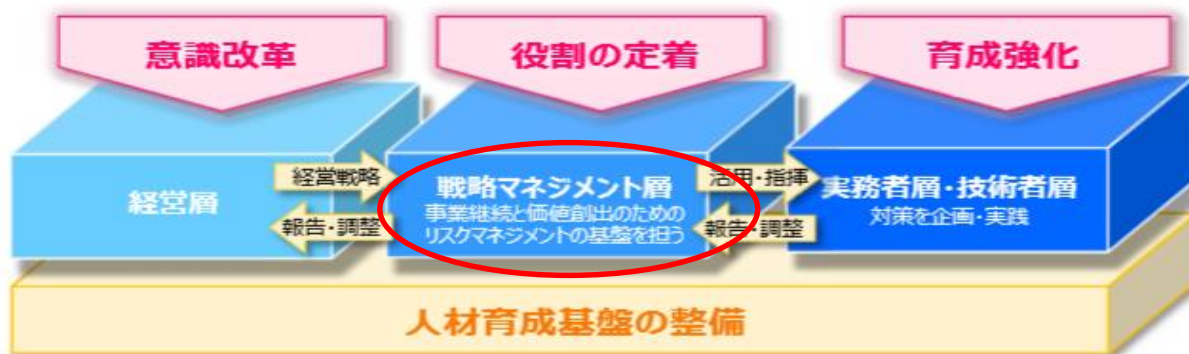
- ◆ サイバーセキュリティ人材育成プログラム（サイバーセキュリティ戦略本部、平成29年4月18日発表）



(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 ～事業継続と価値創出に向けた産学官連携の推進～

※基本的には、経営層及び中小企業関連の取組については企業経営WG、それ以外の部分は施策間連携WGの報告書に基づく。

	経営層	戦略マネジメント層	実務者層・技術者層
役割	<ul style="list-style-type: none"> 企業においては、ビジネスやサービスの着実な遂行（任務保証）が最重要の課題 このような観点から、事業継続と新たな価値創出のためのリスクマネジメントの一環として、サイバーセキュリティ対策を推進することが重要 	<ul style="list-style-type: none"> 経営・事業戦略におけるサイバーセキュリティのリスクを認識しつつ、事業継続と価値創出に係るリスクマネジメントを中心となって支える役割を担う 経営層の方針を踏まえた対策立案・報告、実務者・技術者の指揮 インシデント発生時には、経営・事業に対する影響を考慮しつつ、経営層の判断の支援や実務者・技術者を指揮し、対処の中核を担う 	<ul style="list-style-type: none"> 戦略マネジメント層の示す方針を踏まえ、リスクを把握し、セキュリティ対策を企画・構築・実施 インシデント発生時には、その影響範囲を特定し、戦略マネジメント層の指示の下で関係者との連絡・調整や技術的な対処を実施
課題	<ul style="list-style-type: none"> サイバーセキュリティのリスクマネジメントに向けた、経営層の理解と意識改革の推進 業種・業態の違いを踏まえた、企業経営におけるサイバーセキュリティの位置付けの明確化と組織におけるリスクマネジメントの浸透 サイバーセキュリティの取組に対する経営上のインセンティブ付与（市場や出資者等による評価の仕組み等） 	<ul style="list-style-type: none"> 企業の事業部門において、サイバーセキュリティのリスクを考慮する機能が不明確。マネジメント機能とサイバーセキュリティ対策が乖離 事業部門の人材向けのサイバーセキュリティに関する適切な教材やプログラムが存在しない 	<ul style="list-style-type: none"> 経営層・戦略マネジメント層を支え、他の専門人材と円滑にコミュニケーションをとりながらチームの一員として対処できる人材の育成 新たな技術やシステム開発手法を積極的に活用するための知識・スキルの育成
今後の施策の方向性（産学官の連携）	<ul style="list-style-type: none"> 経営層の理解と意識改革の推進 <ul style="list-style-type: none"> サイバーセキュリティ対策について経営層が果たすべき役割、持つべき認識についての考え方の共有 サイバーセキュリティ対策の基本方針・内容について、マークやスローガンなど、分かりやすく表現し普及するためのツールの検討 経営層向け伝道師の発掘・派遣 「経団連サイバーセキュリティ経営宣言」の普及、経営層向けセミナーの開催 業種・業態別の差異を踏まえた基盤の整備 <ul style="list-style-type: none"> 業種・業態別に平均的対策のレベル感と望ましい対策のレベルを示すツールの整備 企業が参照可能な関係法制度の整理に向けた検討 サイバーセキュリティ投資のためのインセンティブ <ul style="list-style-type: none"> 情報開示による見える化を推進するためのツールの整備（ガイドラインの策定等） 税制優遇の執行やサイバー保険の活用方策の検討 	<ul style="list-style-type: none"> 組織における戦略マネジメント層の定着 <ul style="list-style-type: none"> 戦略マネジメント層の意義に対する経営層の理解の推進 戦略マネジメント層の組織における位置付け及び機能の明確化、ベストプラクティスの共有 事業部門のマネジメントとサイバーセキュリティ対策が調和したフレームワークの整備 カリキュラム・教材開発と学び直しプログラムの推進 <ul style="list-style-type: none"> 経営・事業戦略の視点でサイバーセキュリティを実践するための教材開発・学び直しプログラムの推進（試行的取組から開始） サイバーセキュリティ人材育成施策の充実・強化と施策間連携の推進 <ul style="list-style-type: none"> 各省庁における施策の充実・強化を図るとともに、効果的・効果的な実施に向けて、施策間の連携を推進 人材育成の「見える化」の推進 <ul style="list-style-type: none"> 米国NISTによる人材育成のポータルサイトの取組等を参考にしつつ、需要と供給の「見える化」、産学官連携の「見える化」等の取組を推進 （例）人材規模・キャリアパスの明確化、カリキュラム・教材等が一覧になったポータルサイトの整備 育成プログラムの適切な評価基準の策定等 	<ul style="list-style-type: none"> 経営層・戦略マネジメント層を支える人材育成 <ul style="list-style-type: none"> 産業界、教育機関、研究機関等の連携によるカリキュラムの検討・実施、継続的な見直し クラウドや先端技術等の利用に係る人材育成 <ul style="list-style-type: none"> クラウド活用やDevOpsによるシステム開発、先端技術等の利用に関わるセキュリティの知識・スキル育成のための人材育成策、コミュニティ形成の検討

人材規模・キャリアパス（需要）と、

人材育成施策（供給）の好循環

若年層における教育の充実

<課題> 発達段階に応じてコンピュータなどの情報技術の原理や仕組みなどを理解し、論理的思考力を育てるとともに、情報モラル教育も重要
<施策> 初等中等教育段階での教育課程内の取組に加え、教育課程外で地域、企業、団体等において、自由に機器・ツールを用いて興味を持って学べる機会を創出

中小企業関連の取組

<課題> 中小企業にサイバーセキュリティの知識・スキルが十分ではなく、セキュリティ対策に投資することは難しい。踏み台となった場合、自社だけでなく社会への影響が大きい。
<施策> サプライチェーンや類似業務を持つ業種などカテゴライズしたアプローチ
・セキュアモデル（クラウド活用等）と一体となった対策集の策定・普及啓発
・対策促進に向けたインセンティブの仕組み（例：税制優遇）の検討

次期サイバーセキュリティ戦略に反映し、具体的な取組を推進するとともに、継続的にフォローアップを行う

◆ 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

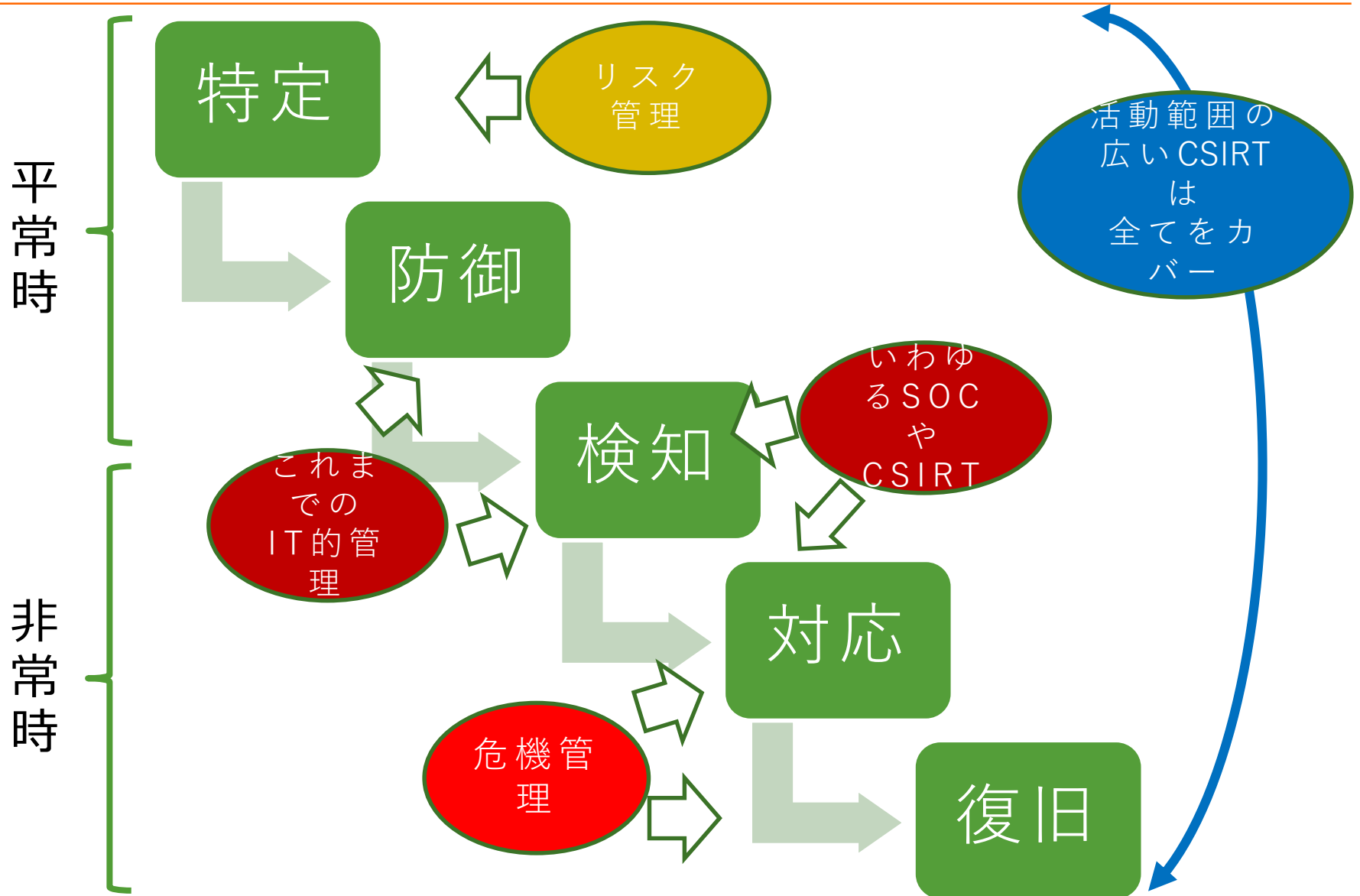
3. サイバーセキュリティにどう取り組むか

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



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
ランサムウェア	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
- ✓ ミドルウェア
- ✓ OS
- ✓ ハードウェア
- ✓ 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

おかしいだろ?

IoTセキュリティだけテキストで

家のカギ

サイフ置きっぱなしじゃないかな?

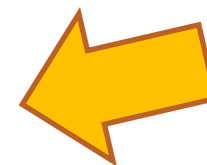
2019年2月より、サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト「NOTICE」^{※1}を実施します。

セキュリティ対策が必要なIoT機器のユーザには、ご契約のインターネットプロバイダからパスワード設定変更などの注意喚起を行います。お問い合わせは、NOTICEサポートセンターまで。^{※2}

※1:総務省、国立研究開発法人情報通信研究機構(NICT)、インターネットプロバイダが連携して実施するプロジェクトです。

※2:インターネットプロバイダからの注意喚起や、NOTICEサポートセンターでの案内あたり、費用の請求や、設定しているパスワードを開き出すことは絶対にありません。

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

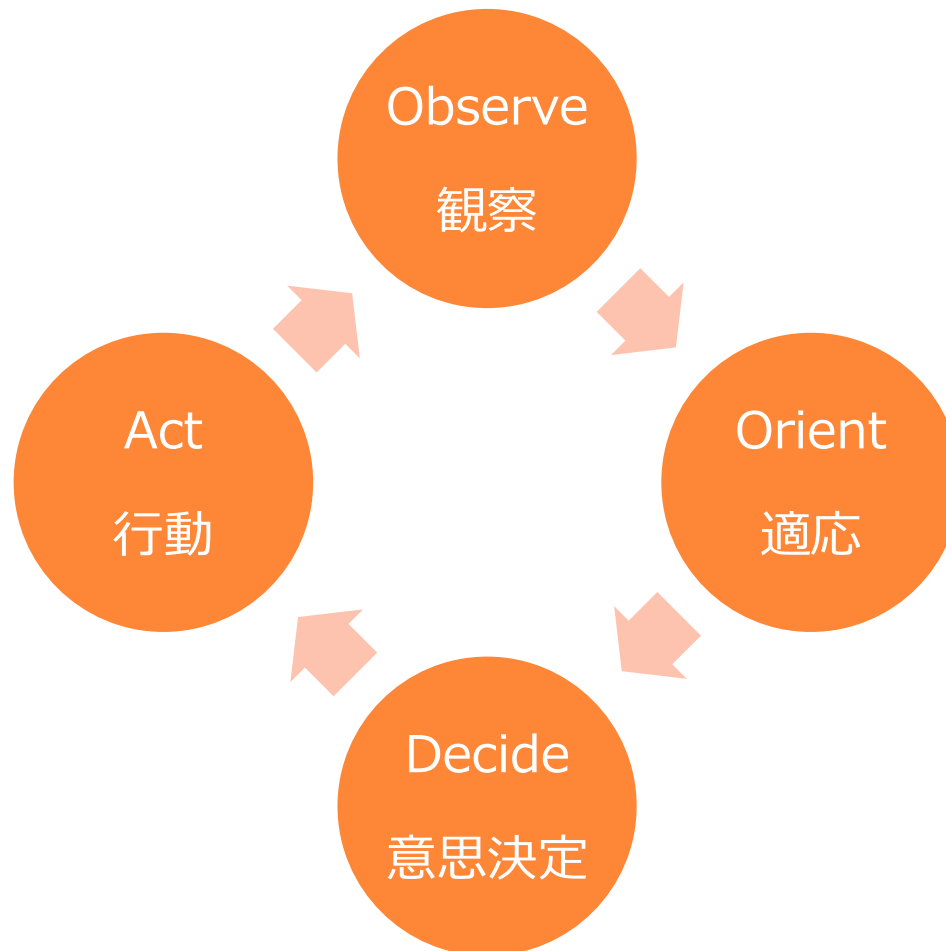
- ✓ 専門用語を排する
- ✓ 具体的事例を挙げる
- ✓ 繰り返す
- ✓ 隠さない風土の醸成

<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

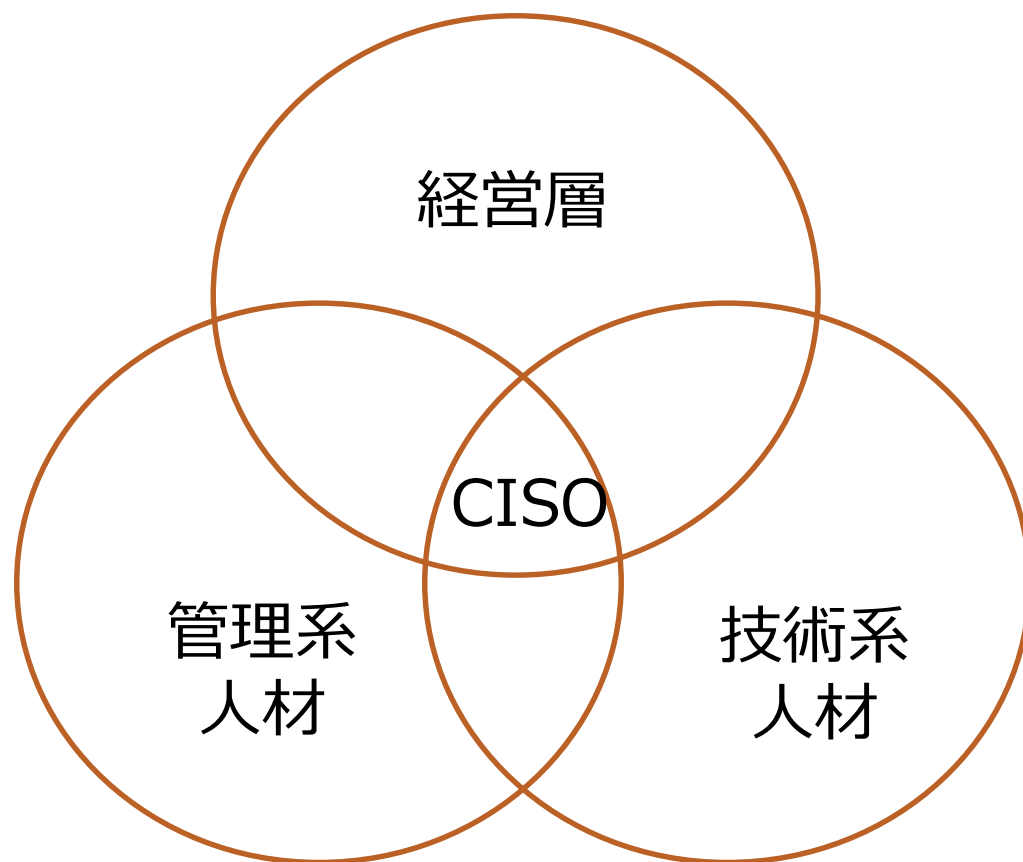
金融ISAC主催：サイバークエスト2（日本経済新聞社提供）

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



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