もう一人で困らない！
マネージドセキュリティサービスの利活用

2019年5月16日

日本セキュリティオペレーション事業者協議会
セキュリティオペレーション連携WG(WG6)

講演者

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- NTTテクノクロス株式会社
  - セキュアシステム事業部　第三ビジネスユニット　勤務
  - 2016年度までは社名が「NTTソフトウェア株式会社」でした
  - NTTグループ セキュリティプリンシパル
  - CISSP, RISS

ISOG-J 日本セキュリティオペレーション事業者協議会

ISOG-Jは2019年4月18日現在、48社が加入しています。

加入すると何か教えてもらえるような団体ではなく、業界の発展のために課題を議論したり、互いに情報を出し合うことで外部へ成果を発表する団体です。

- ホームページ：　https://isog-j.org
- facebook：/isogj
- twitter：@isog_j

こんなドキュメントをリリースしています！

- セキュリティ対応組織(SOC,CSIRT)の教科書 v2.1
  - http://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
  - ハンドブックや組織の成熟度を測るチェックリストも配布しています

- セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v2.0
  - http://isog-j.org/output/2019/5W1H-Cyber_Threat_Information_Sharing_v2.html

  ※英語版もあります！！
  Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT

- 是非ご活用ください！

「セキュリティ対応の教科書」、参照されております！

- 経済産業省「サイバーフィジカルセキュリティ対策フレームワーク」
  - 添付C 対策要件に応じたセキュリティ対策例
  - D.3 ISO/IEC 27001 の管理策群と「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表

- 経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0 実践のためのプラクティス集」
  - プラクティス 2-1 サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
  - 付録 サイバーセキュリティリスクの管理体制構築(指示1,2,3)

ISOG-J ホームページ
https://isog-j.org
よりダウンロード可能

セキュリティの対応の全体像
アウトソース
組織の成熟度
まで

セキュリティ対応組織とは

SOC（セキュリティオペレーションセンター） ＋ CSIRT

CSIRTとSOCの役割は

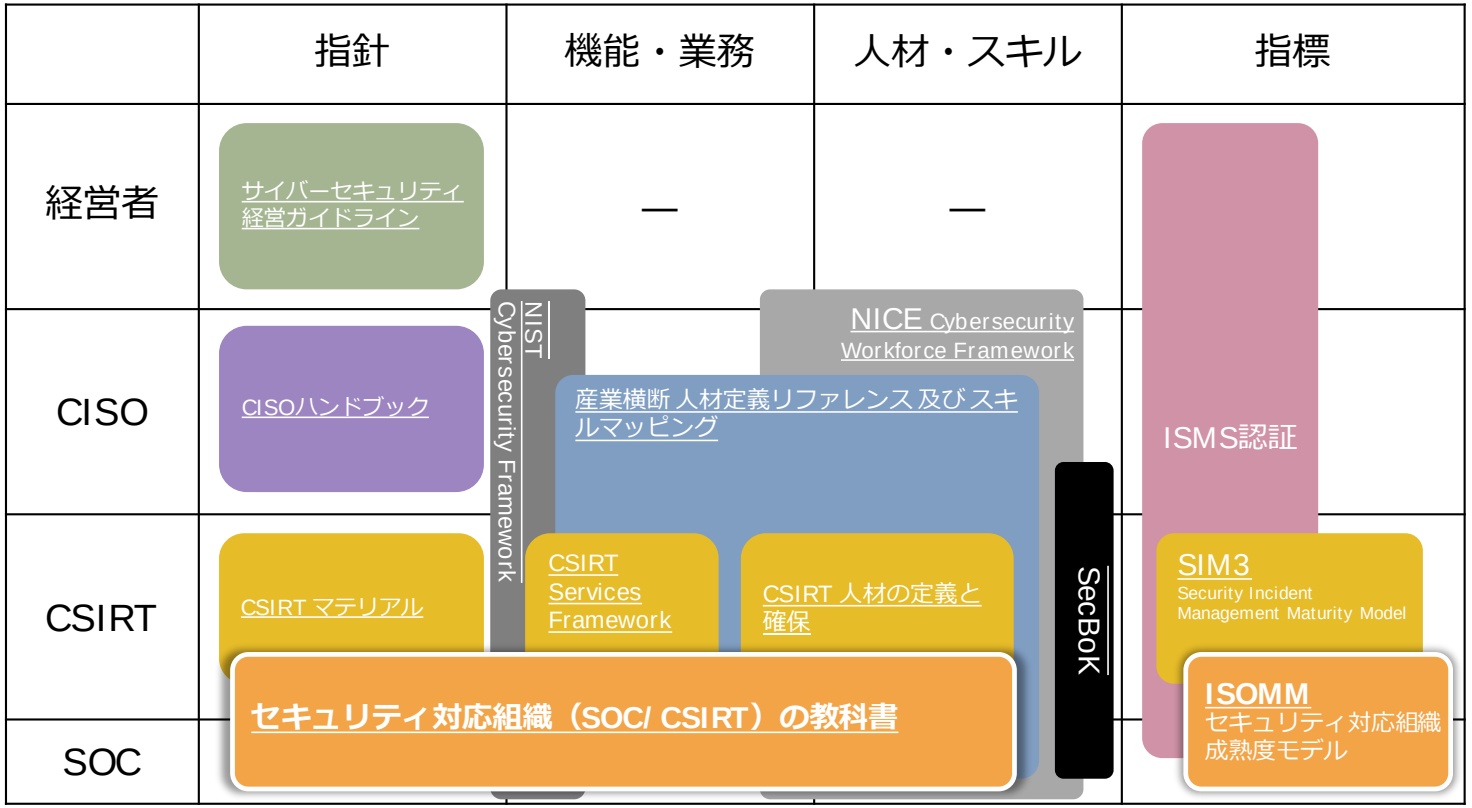
その境界線が

企業・組織ごとに異なる

- 経営者の思うセキュリティ対応
- セキュリティ責任者が思うセキュリティ対応
- 現場が思うセキュリティ対応

立場によって考えることが異なることを理解しつつ
それぞれに合った考え方（ガイドライン）を把握する

各種のガイドラインのマッピング



そもそも「役割」とは？
その理解が重要。

セキュリティ対応組織の教科書 v2.1

セキュリティ対応する
組織が持つべき、
9つの機能と
その機能が担うべき
54の役割を定義。

A. セキュリティ対応組織運営
A-1. 全体方針管理
A-2. トリアージ基準管理
A-3. アクション方針管理
A-4. 品質管理
A-5. セキュリティ対応効果測定
A-6. リソース管理

B. リアルタイムアナリシス（即時分析）
B-1. リアルタイム基本分析
B-2. リアルタイム高度分析
B-3. トリアージ情報収集
B-4. リアルタイム分析報告
B-5. 分析結果問合受付

C. ディープアナリシス（深掘分析）
C-1. ネットワークフォレンジック
C-2. デジタルフォレンジック
C-3. 検体解析
C-4. 攻撃全容解析
C-5. 証拠保全

D. インシデント対応
D-1. インシデント受付
D-2. インシデント管理
D-3. インシデント分析
D-4. リモート対処
D-5. オンサイト対処
D-6. インシデント対応内部連携
D-7. インシデント対応外部連携
D-8. インシデント対応報告

E. セキュリティ対応状況の診断と評価
E-1. ネットワーク情報収集
E-2. アセット情報収集
E-3. 脆弱性管理・対応
E-4. 自動脆弱性診断
E-5. 手動脆弱性診断
E-6. 標的型攻撃耐性評価
E-7. サイバー攻撃対応力評価

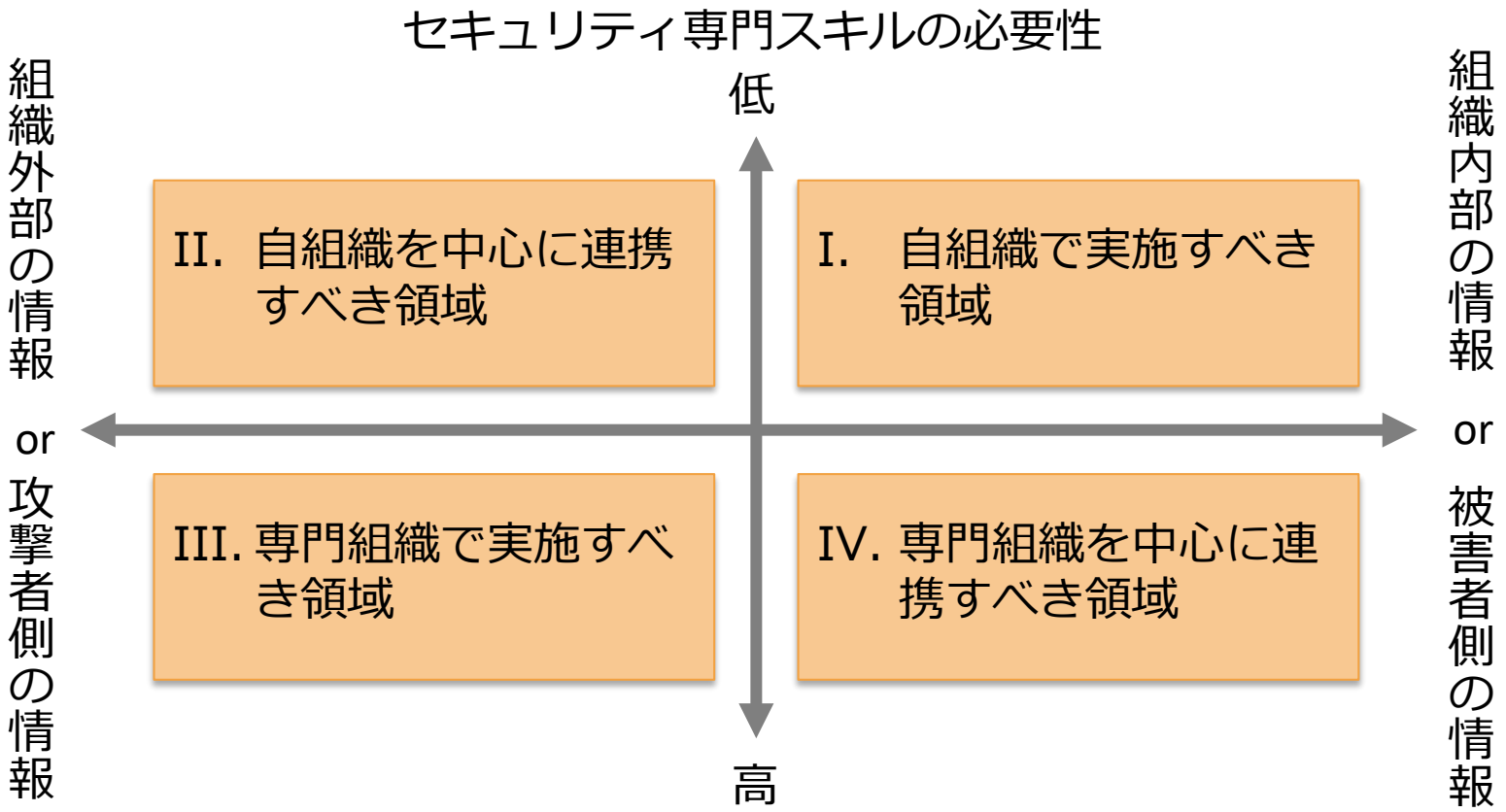
F. 脅威情報の収集および分析と評価
F-1. 内部脅威情報の整理・分析
F-2. 外部脅威情報の収集・評価
F-3. 脅威情報報告
F-4. 脅威情報の活用

G. セキュリティ対応システム運用・開発
G-1. ネットワークセキュリティ製品基本運用
G-2. ネットワークセキュリティ製品高度運用
G-3. エンドポイントセキュリティ製品基本運用
G-4. エンドポイントセキュリティ製品高度運用
G-5. ディープアナリシス(深掘分析)ツール運用
G-6. 分析基盤基本運用
G-7. 分析基盤高度運用
G-8. 既設セキュリティ対応ツール検証
G-9. 新規セキュリティ対応ツール調査、開発
G-10. 業務基盤運用

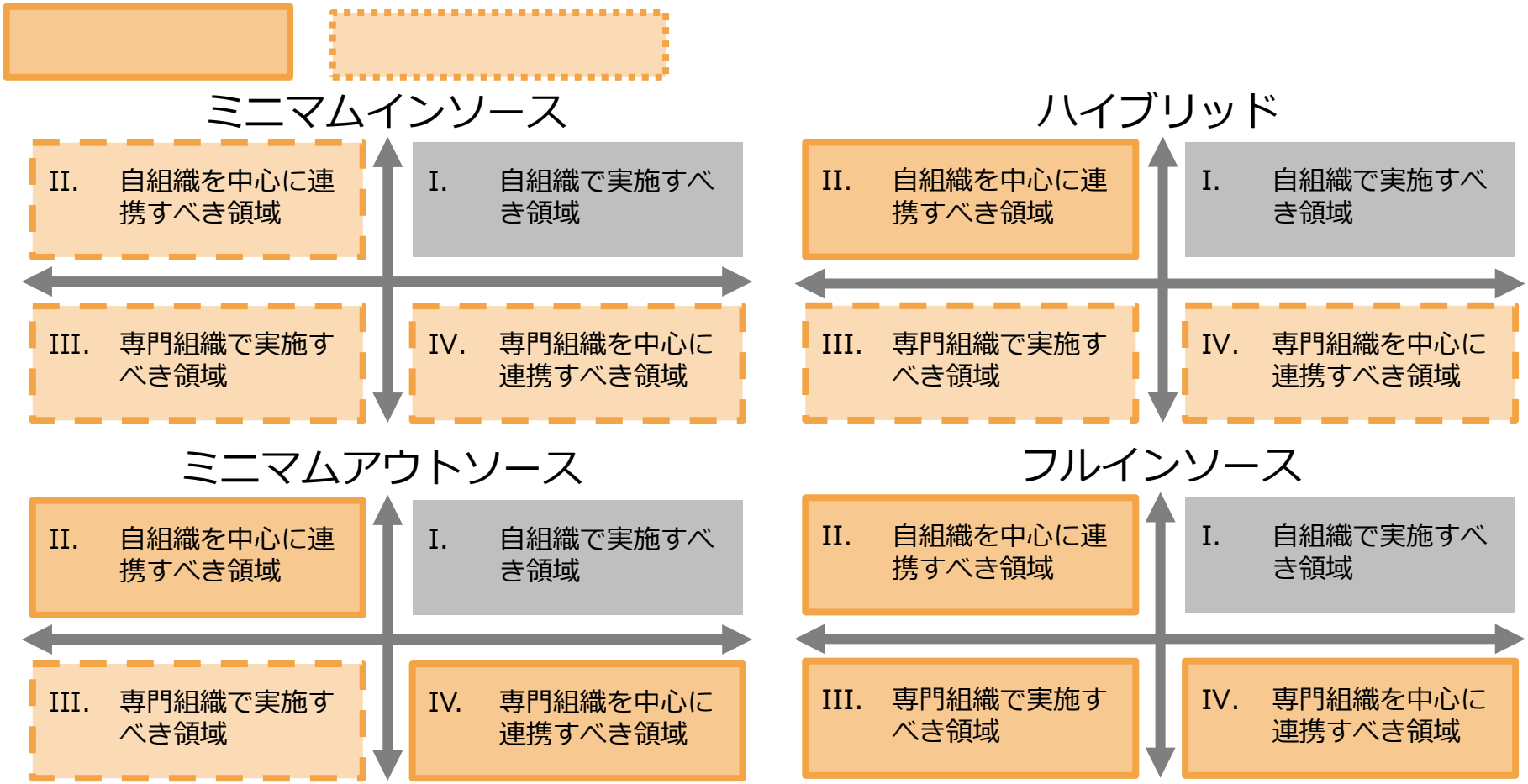
H. 内部統制・内部不正対応支援
H-1. 内部統制監査データの収集と管理
H-2. 内部不正対応の調査・分析支援
H-3. 内部不正検知・防止支援

I. 外部組織との積極的連携
I-1. 社員のセキュリティ対する意識啓発
I-2. 社内研修・勉強会の実施や支援
I-3. 社内セキュリティアドバイザーとしての活動
I-4. セキュリティ人材の確保
I-5. セキュリティベンダーとの連携
I-6. セキュリティ関連団体との連携

4つの領域への役割の分類



インソースとアウトソースで4つの実現パターン例を定義



セキュリティ対応組織力

＝

それぞれの機能と役割が実行できているか

自組織の力を
どう把握するか？

セキュリティ対応組織
成熟度セルフチェックシート
ISOMM(ISOG-J SOC/CSIRT Maturity Model)

https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1_maturity-checklist.xlsx

どうやって
アウトソースするか？

An **managed security service provider (MSSP)** provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. MSSPs use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.

出典：Gartner（https://www.gartner.com/it-glossary/mssp-managed-security-service-provider）

マネージドセキュリティサービスプロバイダ（MSSP）は、セキュリティデバイスやシステムの監視および管理を請け負います。一般的には、ファイアウォールやIDS、VPN、脆弱性診断、アンチウイルスサービスなどが含まれます。MSSPは、可用性の高いセキュリティオペレーションセンター（自社設備、または他のデータセンター設備を利用）を活用し、ユーザー企業が本来雇用・育成し、維持しなければならないセキュリティ運用にかかわる人材を削減できるよう、24/7のサービスとして提供します。

アウトソースで具体的に提供されるものは？

「**マネージドセキュリティサービス選定ガイドライン**」（2010）より

- セキュリティ対策装置のアラートやログをリアルタイムに監視
- 攻撃アラートの検知時、セキュリティ技術者が調査・分析し、利用者に重要度や影響度を通知、対応を実施
- セキュリティ対策装置のポリシー設定変更やシグネチャ更新を実施
- セキュリティ対策装置の通信・稼動状況や作業／対応作業を報告
- ポータル等によりリアルタイムに状況をレポート
- 利用者からの問い合わせへの対応（電話、メール、Web）
- セキュリティ対策装置のソフトウェア更新

悩みは尽きない・・・

何をどこまでやる？

それ以外にも悩みが・・・

- どれだけのコストをかければよいのか？
- そのコストに見合っているのか？

原点に立ち返る

セキュリティ対応組織が目指すところ

- インシデントの発生をなるべく抑える
  - 発生頻度を小さく
- インシデントが起きてしまっても被害を最小化する
  - 影響度を小さく

例えばこういう考え方

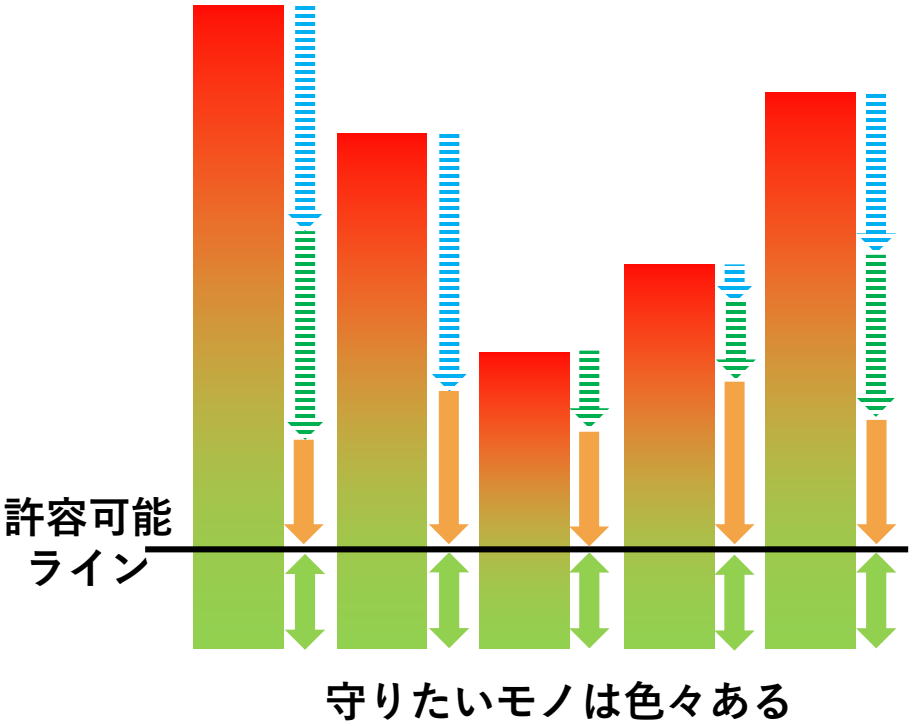
ゼロにはならないが
許容範囲はある

守りたいモノの

想定される被害 ＝ 価値 x 影響度 x 頻度

許容範囲を超えないように
影響度と頻度を下げることが求められる

想定される被害への対応



リスクの移転：保険などでカバーできる分

リスクの回避：根本を排除してしまえる分

リスクの低減：日々のセキュリティ対応で減らす分！

リスクの保有：受容できる分

理想的には・・・

- **どれだけのコストをかければよいのか？**
  - 守りたいモノをすべて明確になっている
  - 低減すべき想定被害が見積れている
- **そのコストに見合っているのか？**
  - 期待した分だけ（あるいはそれ以上に）リスク低減可能なアウトソース先を選定する
  - アウトソースした運用によってリスク低減が叶えられているかを確認する

それでは、

具体的な考え方、
取り組みを見ていきましょう。

選ぶ前のポイント

選ぶ際のポイント

導入後のポイント

選ぶ前のポイント

選ぶ前に考えたい

スムーズに選ぶためには、
選ぶ前に自分を知っておく

自分を知る

何を
持っているか

何を
守りたいか

何を持っているか

誰が

- オーナーシップを明確にする

何を

- 資産価値を把握する

どこに

- 利用されている「サービス」を把握する

何を守りたいか

- システムを取り巻く状況の変化
  - これまでは「防御したい」＝「DMZのサーバーを守る」
  - 今は、守る場所・モノが「多様化」している

クラウド

エンド
ポイント

ネット
ワーク

人

戦略を立てることが重要
何をやるのか？何をやらないのか？

「リスク（被害）」ベースで守る水準を決める

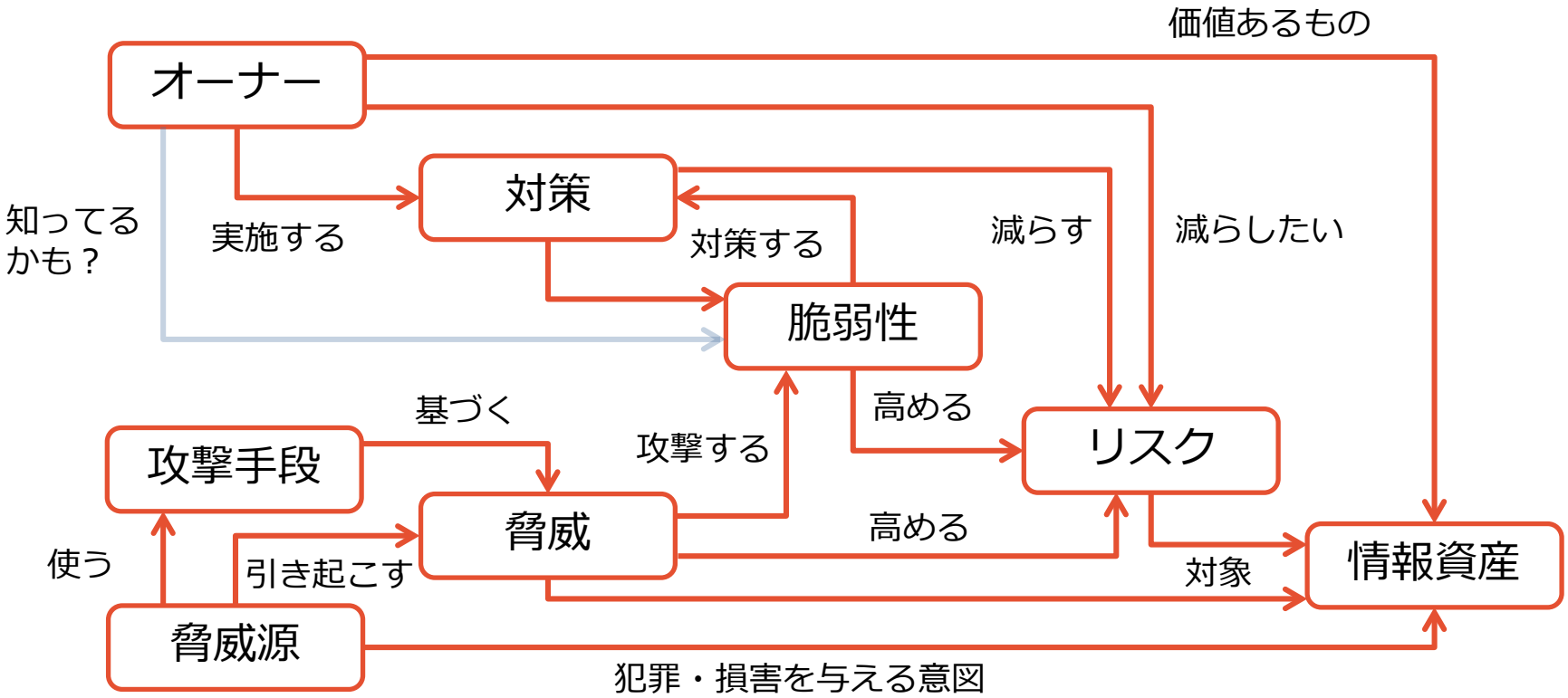
ゼロにはならないが
許容範囲はある

守りたいモノの

想定される被害 ＝ 価値 x 影響度 x 頻度

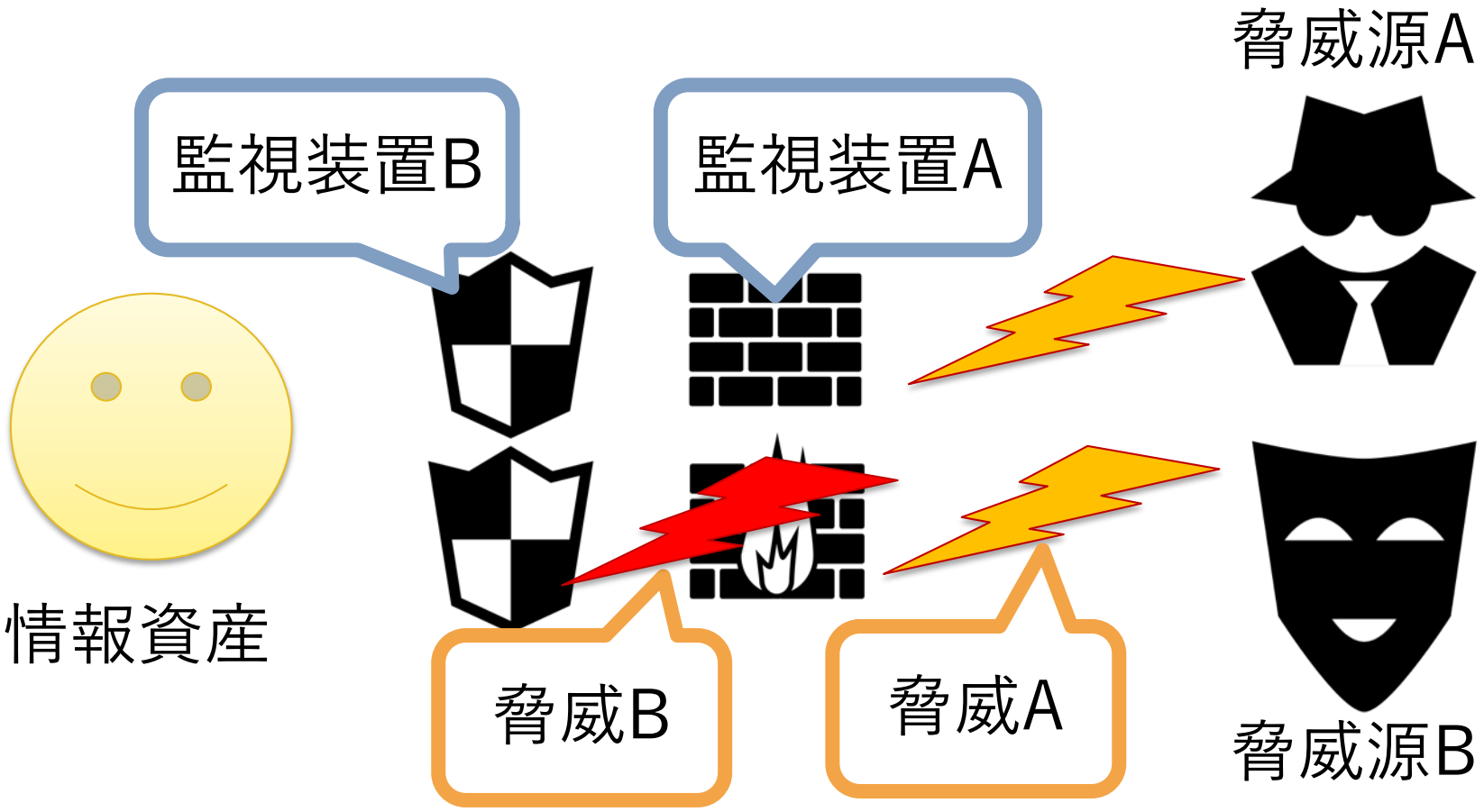
想定される被害が許容範囲を超えないように
影響度と頻度を下げることが求められる

リスクとそれを取り巻く要素の関係性



ENISA Threat Landscape Report 2017
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

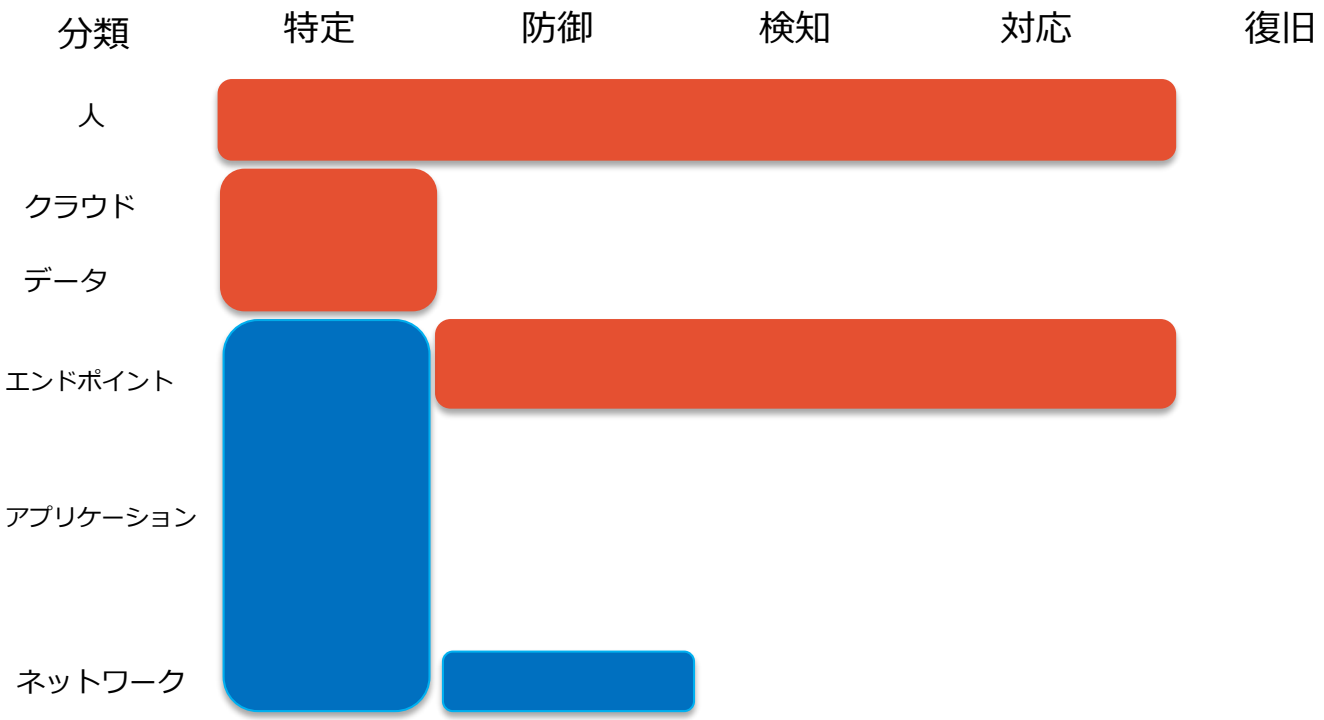
脅威と弱点（脆弱性）を知る



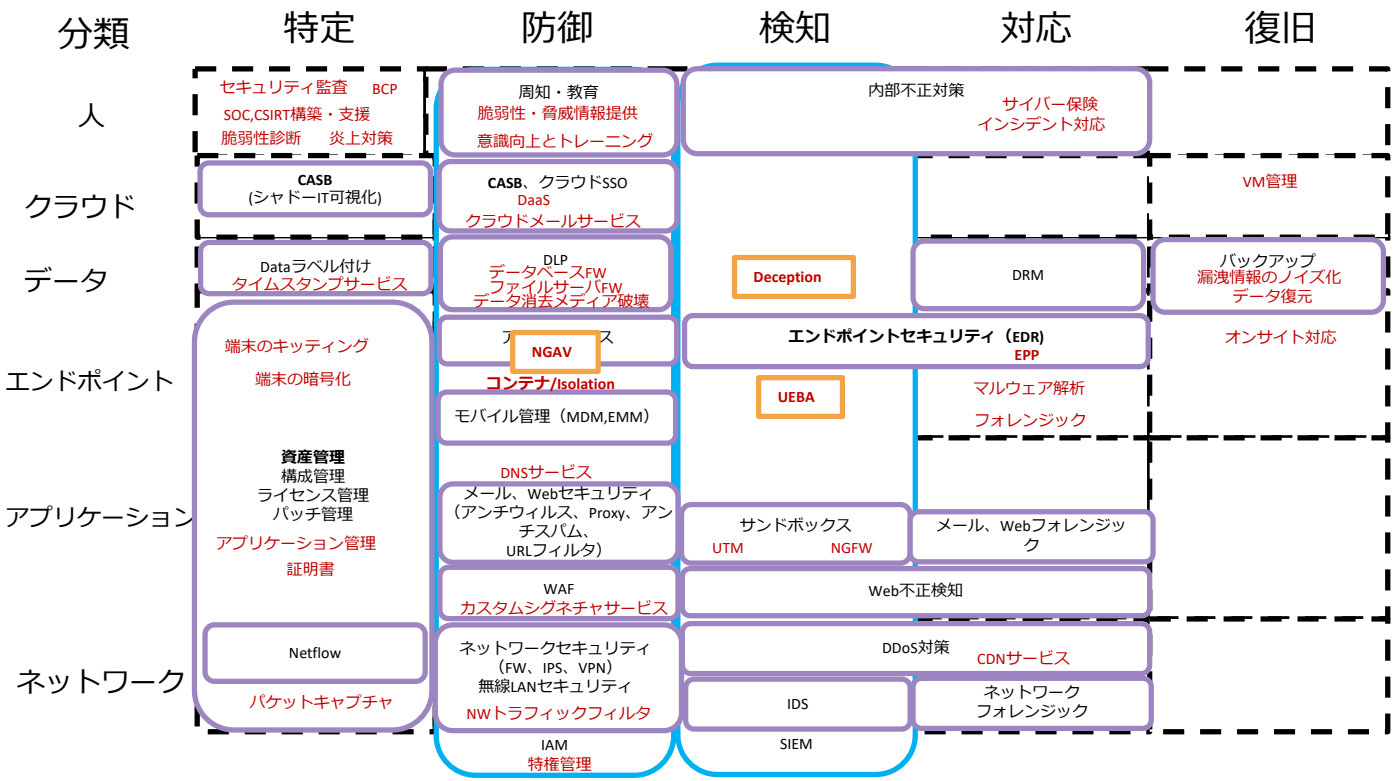
影響度と頻度を測る

- 組織として合意された指標を用いることが重要
  - 指標がない場合、闇雲に測り始めるよりも、どうやって測るか組織内でコミュニケーションを進める方がスムーズに進みやすい
- オーナーとコミュニケーションを取る
  - コミュニケーションを取るための体制を作る

何をやるのか？何をやらないか？



どう守るか



どこまでやるのか

- 低減すべき想定被害に応じて決めるのが理想
  - アウトソース は被害を低減するための対策の１つ
  - 「守る」ための施策が有効に機能しているか測定する仕組みを作る

- 「守られている」状態の要件を定める
  - 現在のネットワークやシステムはどうなってますか？
  - 守りたいシステムには普段どれくらいアクセスが来ていますか？
  - どの程度稼働しているものですか？
  - サービスであれば、どれくらいリソースを使っていますか？

選ぶ前のポイント　まとめ

- 自分を知る
  - 何を持っているか
  - 何を守りたいか
  - 脅威・弱点（脆弱性）は何か
  - 想定される被害を見積る

- どうやって守るか
  - 何をやるのか、何をやらないのかを決める
  - どう守るかを決める

選ぶ際のポイント

MSSは、なんのため？

（ゼロにはならないが
許容範囲はある）

想定される被害 ＝ 守りたいモノの価値 x 影響度 x 頻度

結果、低減される

影響を抑える　頻度を下げる

自分たちに合うアウトソースを選ぶ

- **「守りたいものの価値」に適合**して、**導入可能な形態**のサービスを選ぶ
  - それぞれの重要度に合わせたサービスでメリハリをつける
  - 導入できる形態かどうかも確認しておく

- 監視運用は、**監視を開始してからが長く重要**
  - 一緒に長くやっていけるサービス事業者を選びたい

「守りたいもの」と「アウトソース」の適合

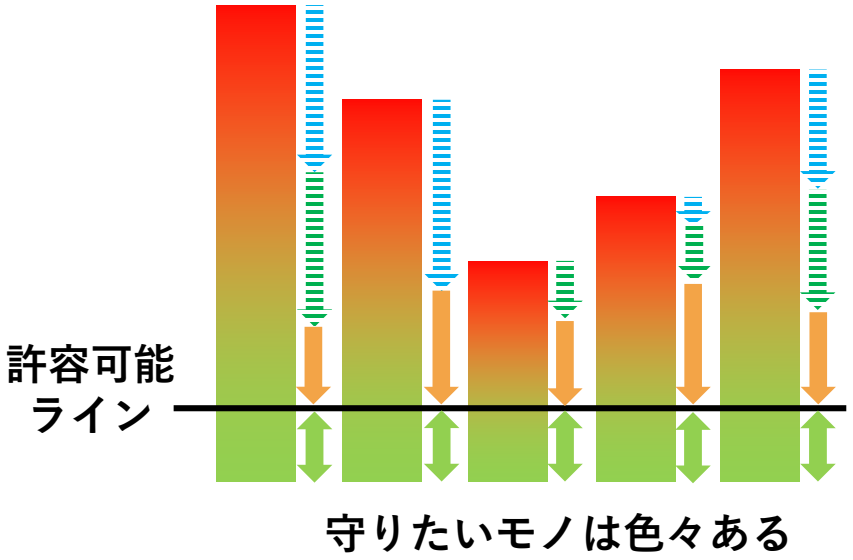
多層的にしっかり監視したい
複数の機器で多面的に監視するレベル

しっかり監視したい
分析官の分析も行うレベル

とりあえず、監視したい
最低限監視するレベル

「身の丈にあった」アウトソースを選ぶ

- どこまでやってくれるか、ずっと付き合えるか。
- 「身の丈にあった」ってどうやって見るの？



- 自組織の考えるリスクレベルにあった対応可能なアウトソース
- ハイスペックすぎず、安過ぎず

- 監視のために機器を使う場合もあればサービスの場合もある

どこまでやってくれるか、ずっと付き合えるか

監視のレベルをお互いに向上させていけるかがポイント

- 定期的な報告やコミュニケーションでの意思疎通ができるか
  - 自分たちが決めた判断の基準に活用できる内容か
- 異常時の連絡や報告のタイミングと自組織側の対応体制が合っているか

導入して終わり、ではない

- 自組織側にアラートの内容を理解し、重要性・緊急性を判断・対処可能な体制構築が必要
  - 数年かけて自組織の言葉に翻訳できる人材を育成する
- アウトソースで早期検知出来ても、連絡を受けた側が気づかなかったり判断できなければ意味がない
  - 何か起きた時の社内規定や連絡体制の整備も必要

アウトソースの限界を理解する

- 中でしか見えないことは、**内部のインシデントレスポンス体制と組み合わせて**活用する
  - 社内OA環境での感染の広がりや内部犯行等
  - 金融業界：不正送金やクレジットカードの不正利用監視
  - EC事業者や航空会社：不正取引監視

- アウトソースで監視できない範囲がある事を理解した上で、**自組織の監視の全体像を定義**する
  - 海外に拠点がある場合は、当該拠点にサービス提供が可能か確認が必要であり、不可能な場合は現地のアウトソースの活用も検討する

能動的にアウトソースを活用するために

- セキュリティ対応組織と休日夜間含む経営層向け連絡体制の整備

- インシデント対応で判断をするのは自分たちであり、アウトソースは必要な情報を提供する役割である意識を持つ
  - 役割・責任分界点を事前に明確にしておく

導入パターンごとに考える

1. 新規監視機器(購入orレンタル）＋アウトソース導入

IPSやFW等の監視機器を購入もしくはレンタルで新規導入し、
合わせてアウトソースによる監視サービスも導入

2. 既存設置監視機器にアウトソース追加導入

元々導入していたIPSやFW等の監視機器の監視を強化する為、
アウトソースによる監視サービスのみ導入

3. （非オンプレ）セキュリティサービス+アウトソースの導入

クラウドサービスのWAFやDDoS対策、EDRサービス等を新規
に利用する

監視開始までにやるべき作業を理解する

- **監視開始までに期間が必要**な場合もある
  - 各種設定、性能が出るまでの期間が必要
- **SIEM監視の場合は更に時間を必要**とする
  - いくつものログの相関を取るのは準備が必要
- **エージングやチューニング、学習期間**も考慮する
  - ノイズのない定常状態の見極めや学習が必要

「レポートの意味」を正しく理解し有効に活用する

- **影響度と頻度を下げること**ができているか、自分たちで分析できるレポートを出してもらう

- **自分たちで効果測定**できるためには何が必要か考える
  - 相談ができるアウトソース事業者を選ぶ
  - 効果測定はCISOダッシュボードで活用する

「レポート」を有効活用する

- 「レポート」：定期レポート、個別の脅威に関するレポート

- 内容を上手に分析・活用できるかは**受け取り側次第**
  - アラートを中長期で定点観測して、**異常を発見**する
  - 社内や組織の**中長期のセキュリティ対策**に活用する
  - セキュリティ投資予算獲得の為の**経営層宛説得材料**に活用する

選ぶ際のポイント　まとめ

- 自分たちに合うアウトソースを選ぶ
- 導入パターン毎に考える
- 監視開始までにやるべき作業を理解する
- レポートの意味を正しく理解し活用する

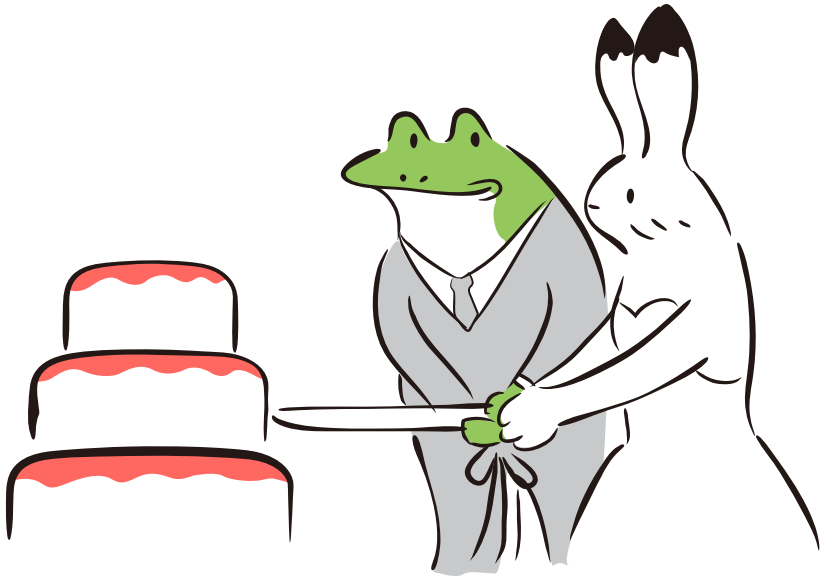
導入後のポイント

ここまでのストーリー

出会い
お互いを知る
末長くやっていけるか
……
これって……

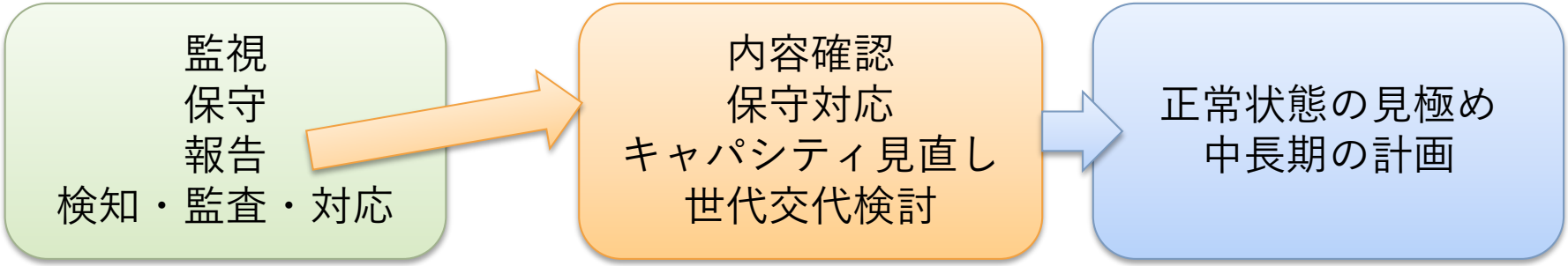
ここまでのストーリー

ゴールじゃなくてこれからのスタート、ってやつだ……



平時のポイント

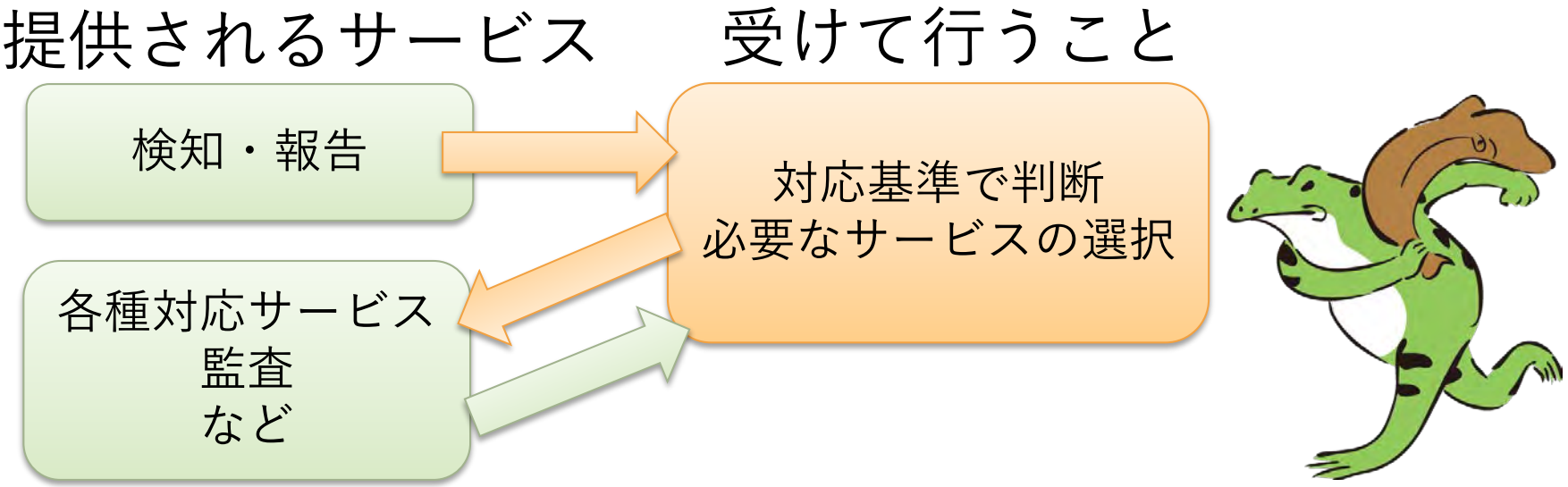
提供されるサービス　受けて行うこと　活用すること



- サービスの状況を知るのが報告です
  - 連絡の方法、頻度、どんな内容が提供されるか
- 普段やるべきこと、その成果の社内アピールも大事です
  - 参考：「セキュリティ対応組織の教科書 v2.1」、IW2017発表

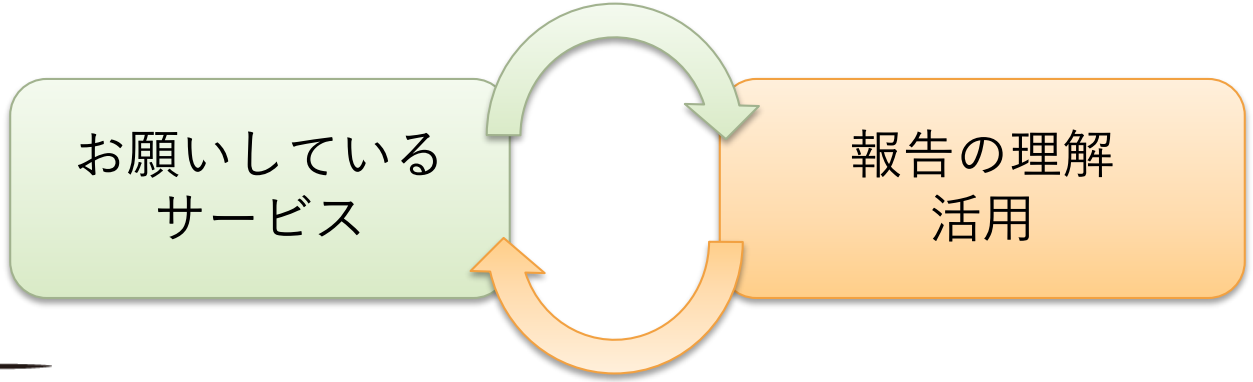
インシデント時のポイント

- インシデント時は、アウトソースから提供される情報を元に自分たちが判断、指示をする意識をもつ。
  - 起きてから焦るのではなく、普段から演習や訓練を！



常に見直す

- 目的は異常を早期に発見して、「影響度」や「頻度」を下げること。
  - CISOも巻き込んで効果測定できていますか？
- お願いしているサービスの内容を理解しつつ、報告を理解
  - そこからより良い監視のために見直しを続けていますか？



導入後のポイントまとめ

- 買ったらゴールインではなくて、そこからがスタート。
- 平時とインシデント時、それぞれに何をするか確認しましょう
  - 何もない時こそ、インシデント時の準備をしっかりやる時です
- 見直しを続けよう。CISOと一緒に考えれるように、してみよう。

まとめ

まとめ

1. アウトソースは何
   - 被害を低減をする
2. 選ぶ前のポイント
   - 自分の今を見つめ
3. 選ぶ時のポイント
   - 身の丈にあっており、ずっと付き合える相手を選ぶ
4. 導入後のポイント
   - 導入はゴールではない。スタートだ！

予告！

マネージドセキュリティサービス(MSS)選定ガイドライン Ver.2.0

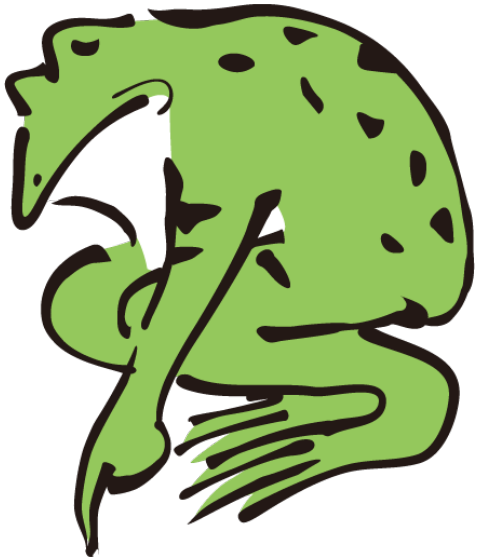
現在ISOG-J WG6にて執筆中！

（参考：アイコン、漫画素材）
http://www.security-design.jp/
http://www.chojugiga.com/

- 本資料に関し、利用実態を把握するため、ご利用の際にはISOG-Jの窓口（info (at) isog-j.org）までご一報いただけますと幸いです。
- 本資料に関するご意見、ご要望などは下記よりご連絡ください。
  - https://jp.surveymonkey.com/r/W9HCMFP

付録1. ハンドブックの紹介

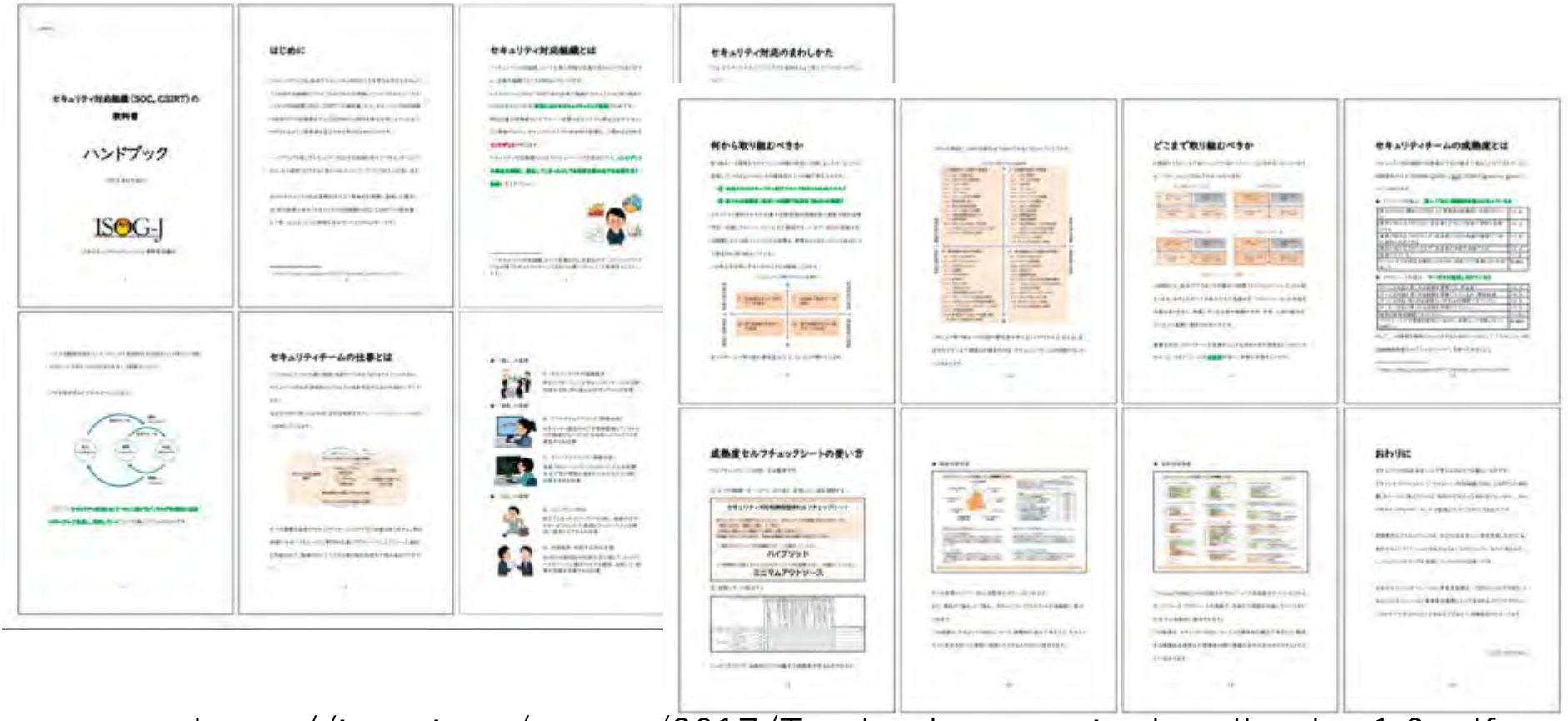
上司は読んでくれるだろうか…



もっと簡単に「セキュリティ対応組織の教科書」を理解したい（してもらいたい）

セキュリティ対応組織の教科書 ハンドブック v1.0

読みやすい概要版。
A3 8up両面で
印刷にちょうどいい
16ページ＋1枚



https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0.pdf

セキュリティ対応組織（SOC/CSIRT）の教科書 ハンドブック 別紙

ISOG-J

セキュリティ対応の役割一覧

A セキュリティ対応組織運営

B リアルタイムアナリシス（即時分析）

C ディープアナリシス（深掘分析）

D インシデント対応

E セキュリティ対応状況の診断と評価

F 脅威情報の収集および分析と評価

G セキュリティ対応システム運用・開発

H 内部統制・内部不正対応支援

I 外部組織との積極的連携

https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0_appendix.pdf

ハンドブック読んだよ！
ではまずは自組織の状況を把握
してから組織づくりしなきゃね！！

やったぜ！

付録2. ISOMMの使い方

ISOMMの使い方概要

1. セキュリティの対応の全体を知る
2. 自組織でどこを対応するか決める
3. 自組織の現在のパターンを知る
4. 今後どんなパターンになりたいかを決める
5. 現在の範囲でどこまでできているかをする
6. チェック結果を見て、どこを強化するかを決める

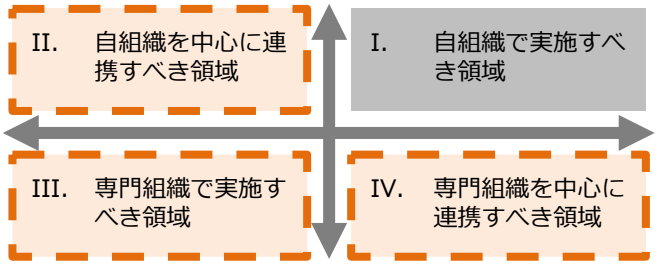
① 組織パターンの設定

セキュリティ対応組織パターンを自覚する（教科書を参考）

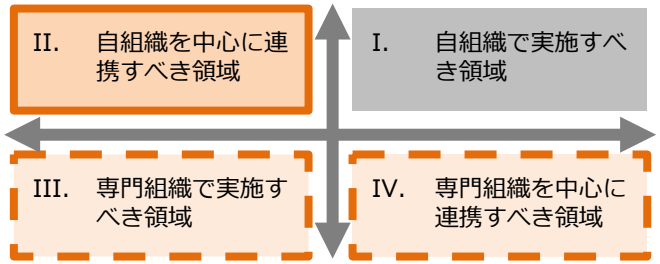
役割を専門性や組織の内外で
四象限に整理

セキュリティ対応組織パターンを自覚する（教科書を参考）

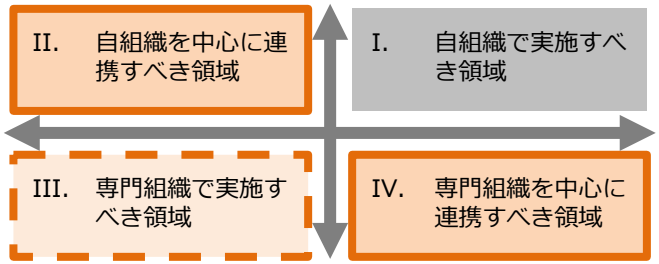
ミニマムインソース



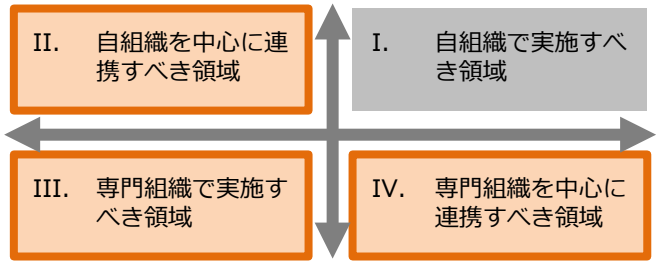
ハイブリッド



ミニマムアウトソース



フルインソース



アウトソース　インソース

セキュリティ対応組織成熟度セルフチェックシート

本チェックシートを活用することによって、セキュリティ対応組織（SOC/CSIRT）での
・現状における、組織の「強み」と「弱み」
・将来的に達成したい組織モデル実現に必要となるポイント
を明確にすることができます。今後の組織強化方針の策定にお役立てください。

■ 現在のセキュリティ対応組織のパターンを選択してください。

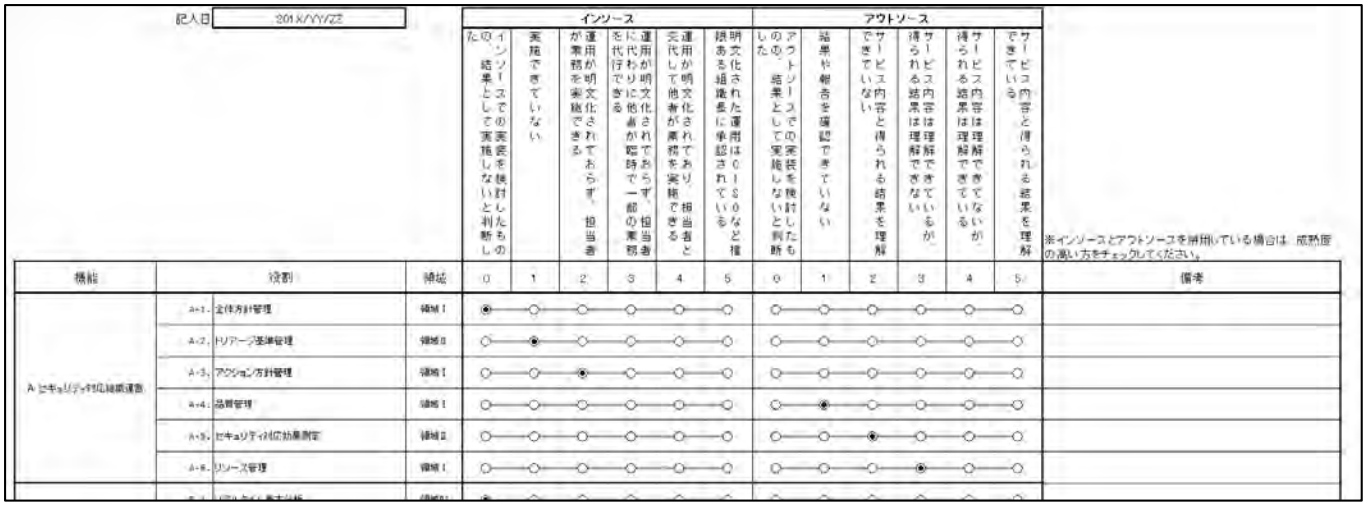
ハイブリッド

■ 中長期的に目指すモデルとなるセキュリティ対応組織のパターンを選択してください。

ミニマムアウトソース

現在と将来的なモデルとするパターンを選択。

② 機能ごとに点数化



記入日 20XX/YY/ZZ

			インソース						アウトソース						
			インソースでの実装を検討したものの、結果として実施しないと判断した	実施できていない	運用が明文化されておらず、担当者が業務を実施できる	運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	運用が明文化されており、担当者と交代して他者が業務を実施できる	明文化された運用はCISOなど権限ある組織長に承認されている	アウトソースでの実装を検討したものの、結果として実施しないと判断した	結果や報告を確認できていない	サービス内容と得られる結果を理解できていない	サービス内容は理解できているが、得られる結果は理解できない	サービス内容は理解できないが、得られる結果は理解できている	サービス内容と得られる結果を理解できている	※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。
機能		役割	領域	0	1	2	3	4	5	0	1	2	3	4	5	備考
A.セキュリティ対応組織運営	A-1.	全体方針管理	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-2.	トリアージ基準管理	領域Ⅱ	○	●	○	○	○	○	○	○	○	○	○	○	
	A-3.	アクション方針管理	領域Ⅰ	○	○	●	○	○	○	○	○	○	○	○	○	
	A-4.	品質管理	領域Ⅰ	○	○	○	○	○	○	○	●	○	○	○	○	
	A-5.	セキュリティ対応効果測定	領域Ⅱ	○	○	○	○	○	○	○	○	●	○	○	○	
	A-6.	リソース管理	領域Ⅰ	○	○	○	○	○	○	○	○	○	●	○	○	

インソースとアウトソース、それぞれの観点において、6段階で評価。

スコアの付け方

	インソース	アウトソース
0	インソースでの実装を検討したものの、結果として実施しないと判断した	アウトソースでの実装を検討したものの、結果として実施しないと判断した
1	実施できていない	結果や報告を確認できていない
2	運用が明文化されておらず、担当者が業務を実施できる	サービス内容と得られる結果を理解できていない
3	運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	サービス内容、得られる結果のいずれかが理解できていない
4	運用が明文化されており、担当者と交代して他者が業務を実施できる	サービス内容と得られる結果を理解できているが、想定未満
5	明文化された運用はCSIOなど権限ある組織長に承認されている	サービス内容と得られる結果を理解でき、想定通り

チェック時のFAQ

- 判断も何もせずに、「何もしていない」場合は1点
- 現状が把握できておらず、わからない場合も1点
- チェックする立場により評価が変わります。
  立場の違いによる認識の差を可視化できますので、
  気にせずチェックしましょう
- 最近できた組織では「わからない」や「できていない」
  のは当然です。ありのままをチェックして見ましょう

③ 結果を見てみる

機能別レーダーチャート

レーダーチャートの数値一覧

あなたのセキュ　組織における"機能別"成熟度

J1X/YY/ZZ

現状の組織（ハイブリッドパターン）における機能　と評価しています。
組織の「強み」と「弱み」を抽出し、現在のセキュリテ　有効に働いている機能と、改善が必要な機能を見える化しています。
マクロな観点での指標として、成熟度向上の方針策定　立てください。

機能	成熟度
A. セキュリティ対応組織運営	4 /5
B. リアルタイムアナリシス（即時分析）	3 /5
C. ディープアナリシス（深掘分析）	2 /5
D. インシデント対応	4 /5
E. セキュリティ対応状況の診断と評価	2 /5
F. 脅威情報の収集および評価と分析	3 /5
G. セキュリティ対応システム運用	3 /5
H. 内部統制/内部不正対応支援	3 /5
I. 外部組織との積極的連携	2 /5

現状のセキュリティ対応組織の強み

A. セキュリティ対応組織運営
セキュリティ対応全体の方針や、各種のルール、基準が定まっており、安定的な運用が実現できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

D. インシデント対応
分析結果や脅威情報を元に、具体的な対応を行えており、システムやビジネスへの影響を低減できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営み　できるよう、関係組織を巻き込んだ取り組みを行ってください。

現状のセキュリティ対応組織の弱み

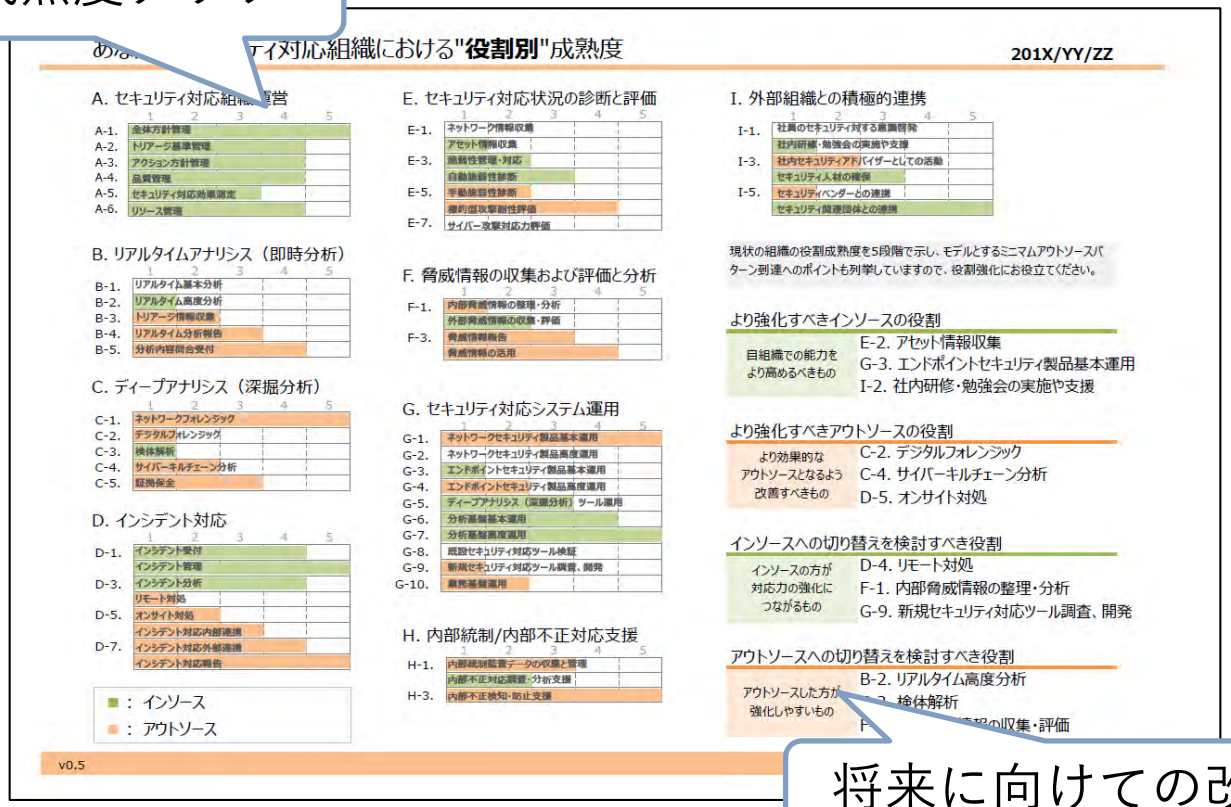
C. ディープアナリシス（深掘分析）
被害状況調査、攻撃手法分析など、深い分析が行い切れておらず、インシデントの全容解明と影響の特定が不十分になっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

E. セキュリティ対応状況の診断と評価
脆弱性診断やインシデント対応訓練などの実施と評価が不十分であり、セキュリティ対応のレベルアップが図りにくくなっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて　を見直してください。

現在の「強み」：成熟度高

現在の「弱み」：成熟度低

役割別成熟度グラフ



将来に向けての改善点

組織による結果の傾向

- ２，３年で担当が入れ替わる組織では、
  担当が変わった直後では出る点数が低めの傾向です
- 管理職やリーダーの採点では高めに、担当の方の
  採点では低めになる傾向です
- アウトソースしている項目は高めに点がつく傾向です

こんな方に気軽に使って頂きたい

組織の管理者やリーダー

業務設計や役割分担の観点から、どこをやるか知りたい

現場の担当者

自分たちがどの範囲を担当しているかの業務役割の認識に

1人CSIRTや1人情シスの方

セキュリティの対応として現在どこまでやっているかの把握に

ISOMMの活用方法

- 気軽に誰でもチェックできる
- 組織の業務で抜けや漏れがないか見つける
- 組織内の業務認識のギャップを見つける
- 弱い部分の強化方針を決める

さらなる活用へ！

- アウトソースに対しての費用対効果を測る
- 他の観点の成熟度も利用して多面的に測る
- この結果を第三者のアセスメントと
  合わせて評価に利用する

セキュリティ対応組織における、現状の把握と今後の方針策定にご活用ください。