D2-2 もう一人で困らない！
セキュリティ対応のアウトソース
マネージドセキュリティサービスを考える

2018年11月28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)

司会進行

- 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

阿部 慎司

Abe Shinji

- NTTセキュリティ・ジャパン
  セキュリティアナリストマネージャー
- NTTグループ　セキュリティプリンシパル
- 日本セキュリティオペレーション事業者協議会（ISOG-J）副代表
- 日本SOCアナリスト情報共有会（SOCYETI）主宰
- CISSP
- 第12回年間アジア・パシフィック情報セキュリティ・リーダーシップ・アチーブメント(ISLA®)受賞
- Security along DesigN http://www.security-design.jp/
- 主な著書：セキュリティのためのログ分析入門 サイバー攻撃の痕跡を見つける技術

講演者

- 伊藤彰嗣（@springmoon6）
- 株式会社メルカリ CSO

Product Security

- Consulting / Testing
- Coding (Automation)
- Monitoring

Security Management

- 体制の整備 / ポリシーの策定
- セキュリティマネジメント
- セキュリティソリューション導入支援

講演者

- **砂田　浩行**
  - 日本総合研究所 開発推進部門 セキュリティ統括室長
  - 三井住友フィナンシャルグループ 上席推進役
  - 日本セキュリティオペレーション事業者協議会
    （ISOG-J： WG4、WG6メンバー）
  - 岡山大学 工学部 非常勤講師（enPIT Securityにて講義・CTF提供）
  - 早稲田大学 基幹理工学部 招聘講師（NTT寄付講座にて講義提供）

講演者

- **亀田　勇歩**

SCSK株式会社　セキュリティアナリスト
- Web/PF脆弱性診断
- SOC監視業務
- インシデントレスポンス

ISOG-J / OWASP / 他
- **ZAP**エヴァンジェリスト
- **脆弱性診断士**の活動
- 東京電機大学 国際化サイバーセキュリティ学特別コース(CySec) 外部講師

趣味
- 2018年のラスベガスで開催された**DEFCON OSINT CTF**で**6位**入賞してきました
- 2018年の11/3に国内で3回目の**Open xINT CTF**を**開催**してきました

本日の発表

1. MSSとは、SOCとは

2. 選ぶ前のポイント

3. 選ぶ時のポイント

4. 導入後のポイント

MSSとは？
SOCとは？

阿部 慎司

Abe Shinji

- NTTセキュリティ・ジャパン
  セキュリティアナリストマネージャー
- NTTグループ　セキュリティプリンシパル
- 日本セキュリティオペレーション事業者協議会（ISOG-J）副代表
- 日本SOCアナリスト情報共有会（SOCYETI）主宰
- CISSP
- 第12回年間アジア・パシフィック情報セキュリティ・リーダーシップ・アチーブメント(ISLA®)受賞
- Security along DesigN http://www.security-design.jp/
- 主な著書：セキュリティのためのログ分析入門 サイバー攻撃の痕跡を見つける技術

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。

MSS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

MSSで具体的に提供されるものは、

8年前とあまり変わっていない…？

境界防御”だけ”では
不十分に

働き方改革などにより
「社内」という概念が
変化

守る
エ
ラ

普及

提供形態はそれほど変わっていないが
そのあり方は大きく変わってきている

監視・分析対象の
多様化

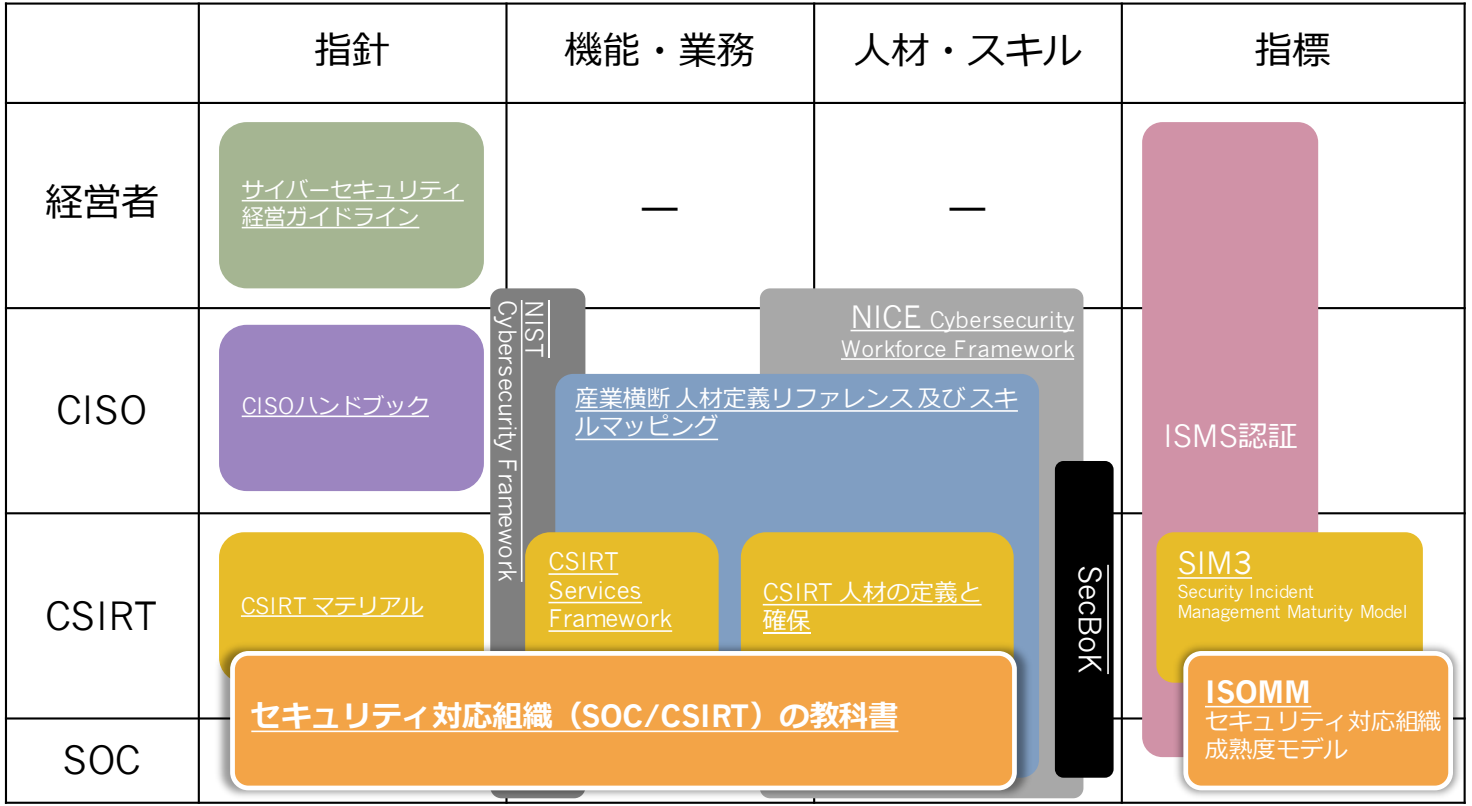
MSSPとユーザー企業
の役割分担の複雑化

図 1　利用者と MSSP の関係

悩みは尽きない・・・

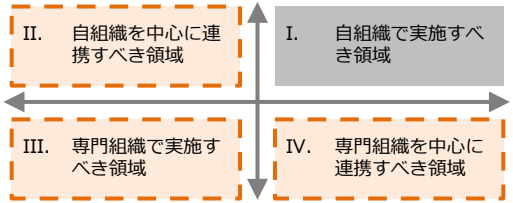
何をどこまでやる？

機能的な整理はなされてきている

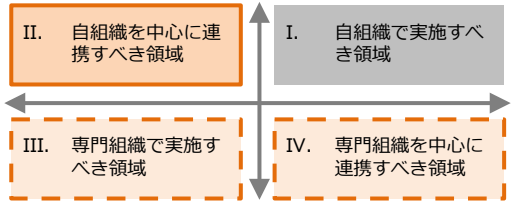


セキュリティ対応組織（SOC/CSIRT）の教科書

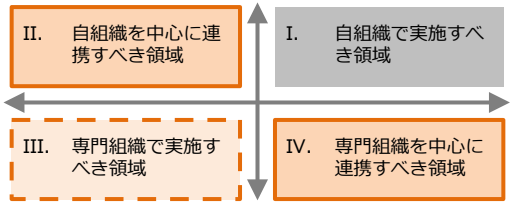
ミニマムインソース



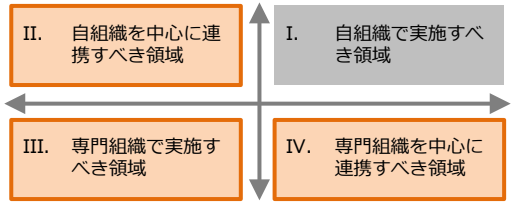
ハイブリッド



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

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

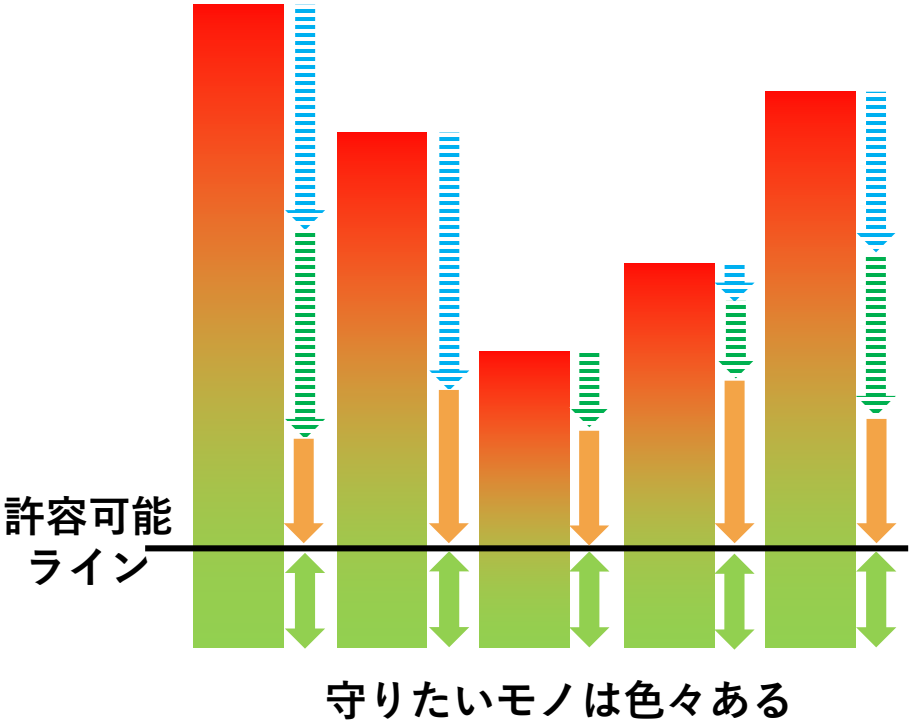
例えばこういう考え方

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MSSPを選定する
  - MSSPの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。

（10分休憩）

選ぶ前のポイント

講演者

- 伊藤彰嗣（@springmoon6）
  - 株式会社メルカリ CSO
  - CISSP

- 現在の活動
  - Product Security Team Manager
  - セキュリティポリシーの策定やシステムリスクの軽減

- 趣味
  - OWASP：OWASP SAMM の活用 / PSIRT Framework の紹介
  - トレーディングカードゲーム（元セミプロ / ゲームのテストプレイ）

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

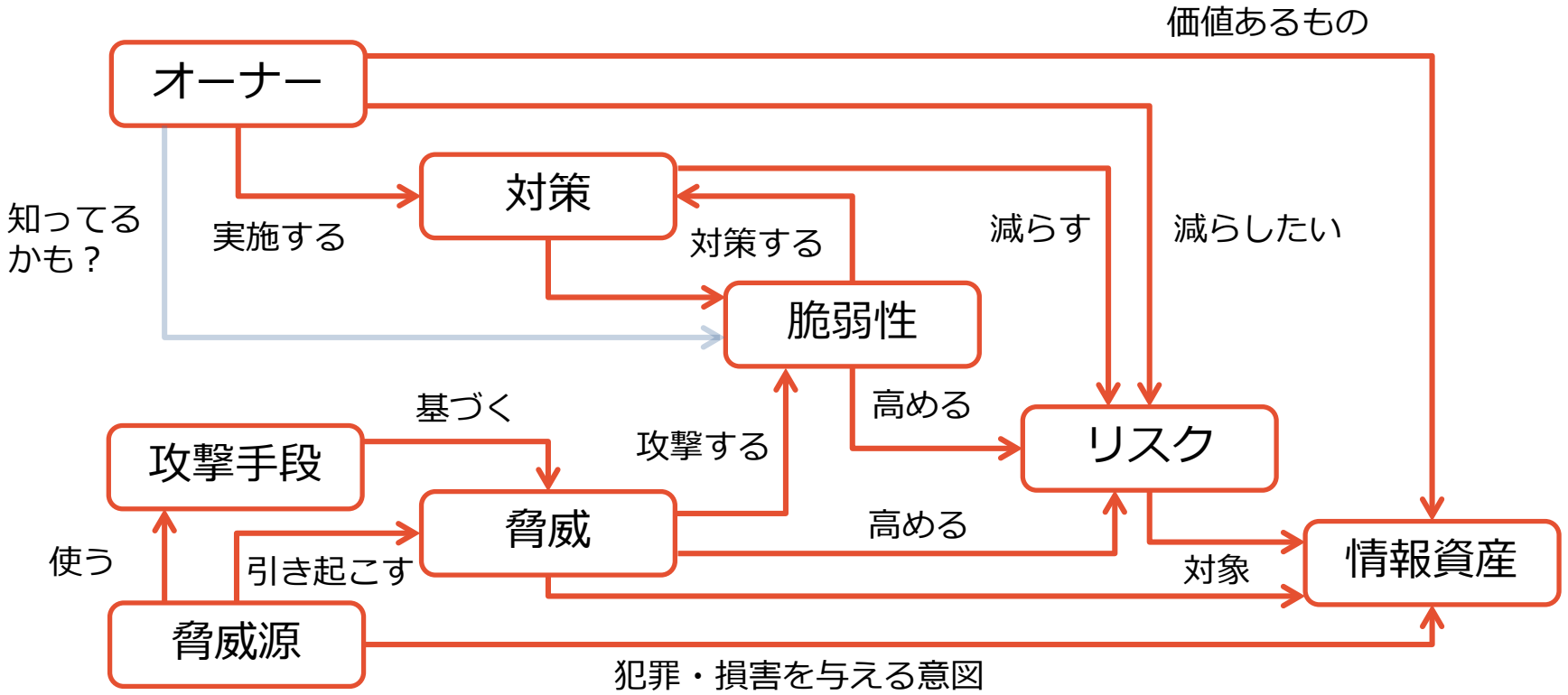
ゼロにはならないが
許容範囲はある

守りたいモノの

想定される被害 ＝ 価値 x 影響度 x 頻度

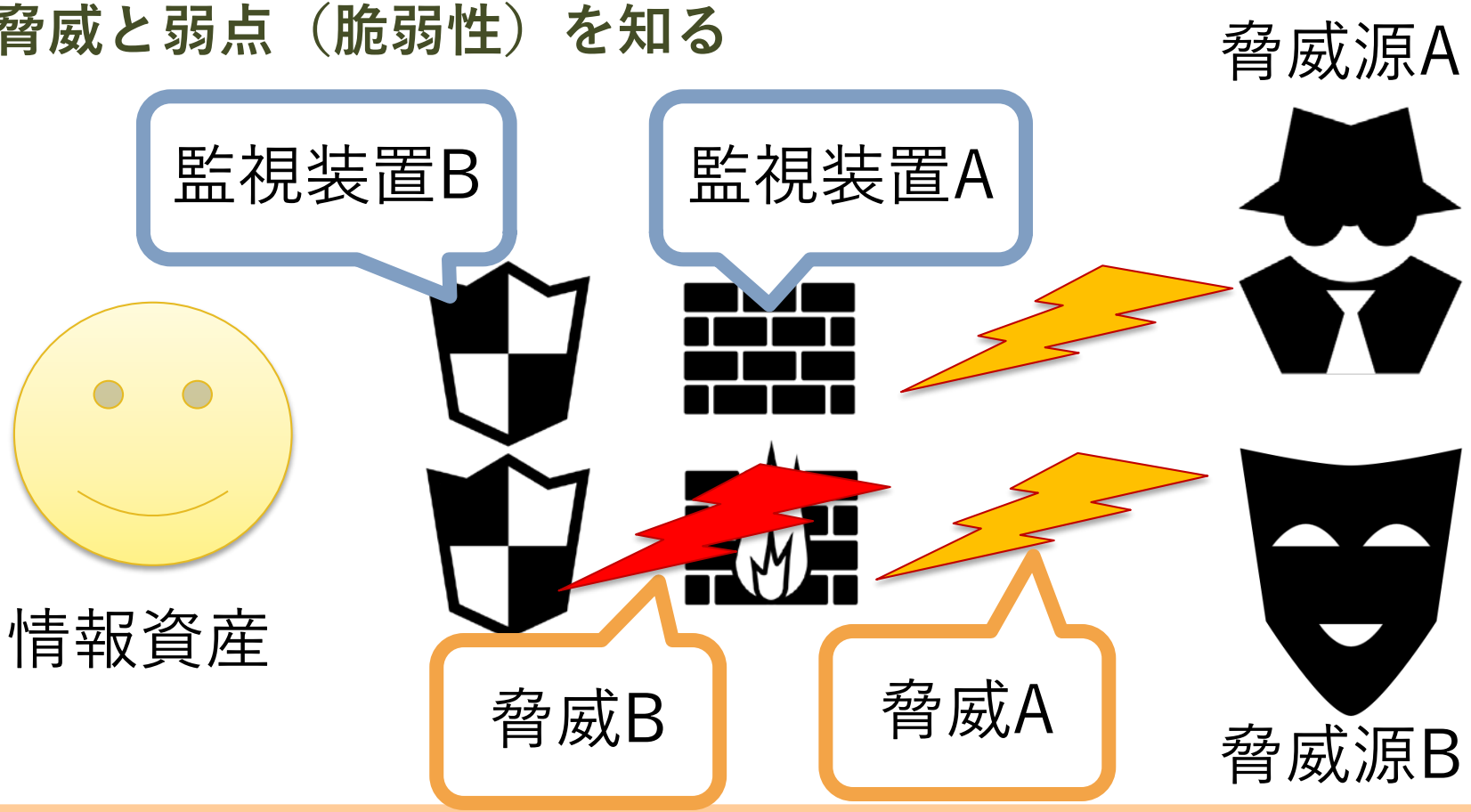
想定される被害が許容範囲を超えないように
影響度と頻度を下げることが求められる

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

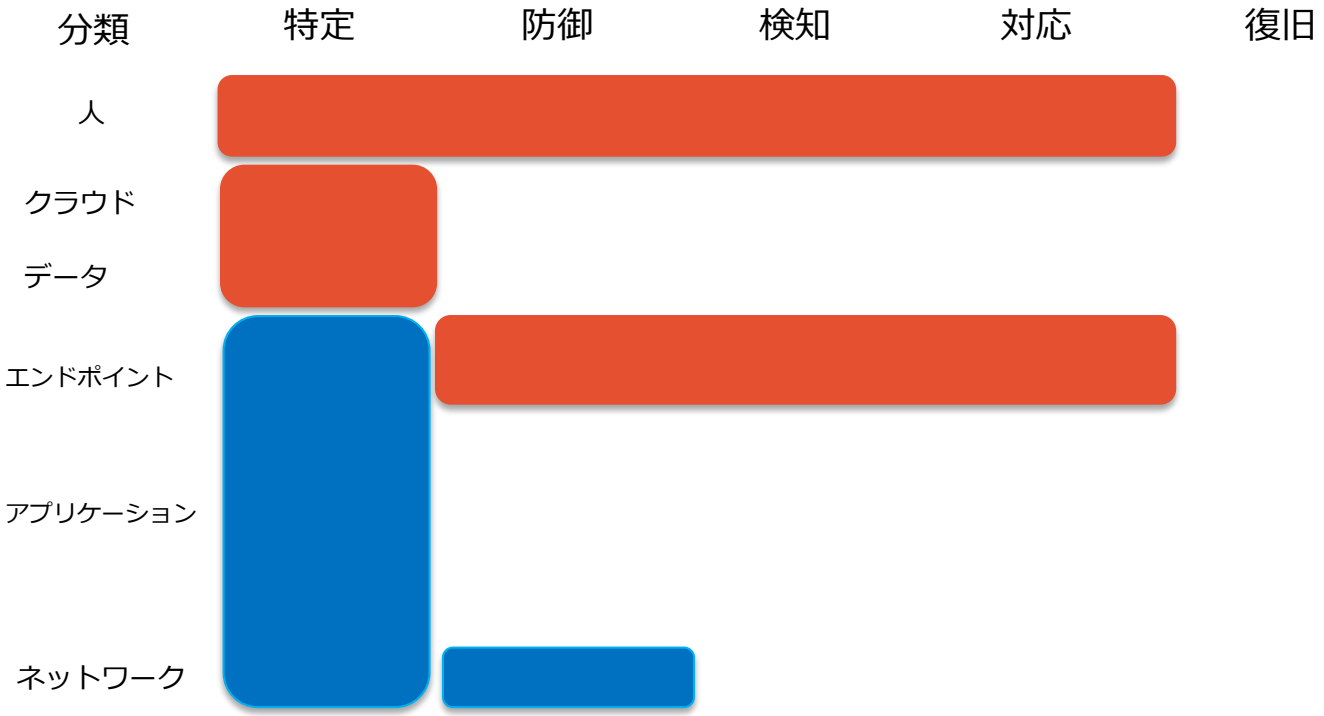
脅威と弱点（脆弱性）を知る



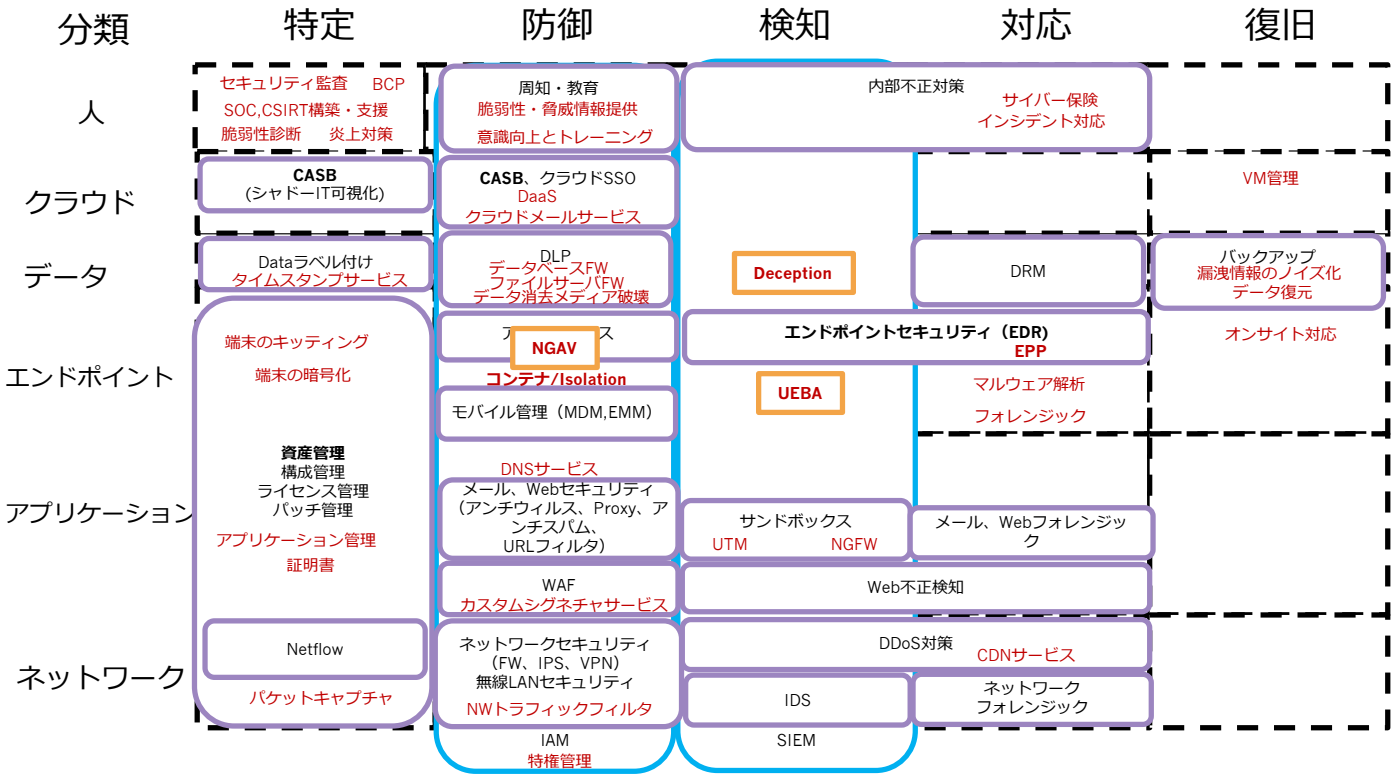
影響度と頻度を測る

- 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
  - MSSP 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

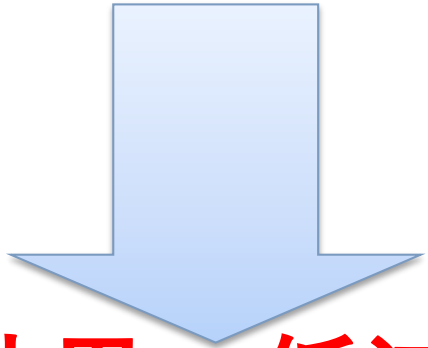
講演者

- **砂田　浩行**
  - 日本総合研究所 開発推進部門 セキュリティ統括室長
  - 三井住友フィナンシャルグループ 上席推進役
  - 日本セキュリティオペレーション事業者協議会
    （ISOG-J： WG4、WG6メンバー）
  - 岡山大学 工学部 非常勤講師（enPIT Securityにて講義・CTF提供）
  - 早稲田大学 基幹理工学部 招聘講師（NTT寄付講座にて講義提供）

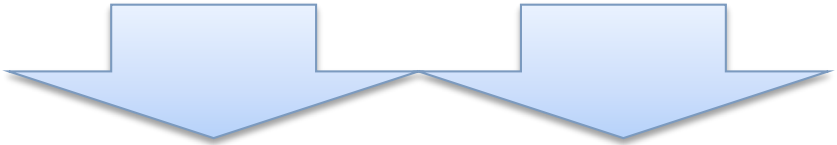
MSSは、なんのため？

（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



結果、低減される



影響を抑える

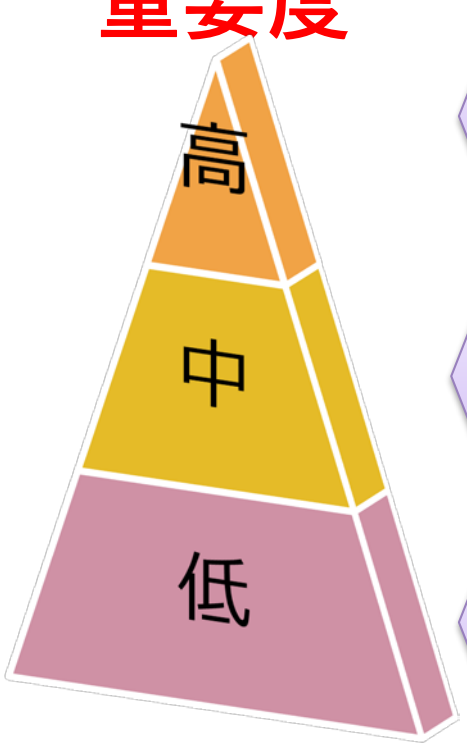
頻度を下げる

自分たちに合うMSS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「MSS」の適合



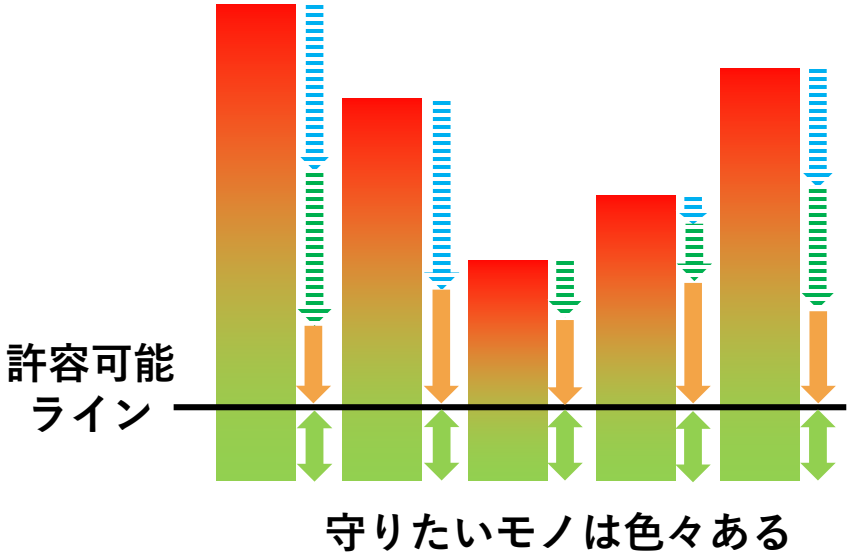
多層的にしっかり監視したい
複数の機器で多面的に監視するレベル

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」MSS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MSS
- 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

- MSS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

MSS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

- MSS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MSS活用も検討する

能動的にMSS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、MSS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）＋MSS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MSSによる監視サービスも導入

2. 既存設置監視機器にMSS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、
MSS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+MSS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

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) + MSS導入

- 監視機器導入ベンダーとMSS事業者は異なるケースがある
- 利用する側が導入ベンダーと監視事業者をコントロールする
- 監視機器のログレベル等、監視運用を考えた導入機器の設定が必要
- 監視運用の要件を導入ベンダー側にきちんと伝える
- 利用者側の導入部署と運用部署が異なるケースもあるので要注意
- 既に他のMSSを利用していたり、自社内で監視をしている場合は運用フローの整理とサービスレベルの基準を統一する

導入パターンごとに考える

2. 既存設置監視機器にMSS追加導入

- 既存設置監視機器保守ベンダーに監視要件を伝えて、監視に必要なログ出力等の設定がなされているか確認する
- MSS事業者側で監視可能なようにネットワークの設定変更や外部からリモートアクセスを許容する
- その際に自社のセキュリティポリシーを確認し、セキュリティホールが出来ないように留意する
- 監視要件に合わせて、既存設置監視機器の保守契約を見直す必要がある場合がある

導入パターンごとに考える

3．（非オンプレ）セキュリティサービス+MSSの導入

- オンプレミスで導入している機器の監視に比べて、監視可能な範囲に制限がある場合がある(ログの保存期間、アラートレベル等)
- 特に海外MSSの場合、24h365d監視の場合に日中・夜間の連絡体制が異なる可能性がある
- クラウド上に監視の為にログやファイルを送付する場合は、ログやファイルの暗号化・匿名化について確認する
- 海外のサーバ等を利用しているクラウドサービス事業者の場合は当該国の規制に対応しているかも留意（GDPR等）

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MSS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MSS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

講演者

- **亀田　勇歩**

SCSK株式会社　セキュリティアナリスト
- Web/PF脆弱性診断
- SOC監視業務
- インシデントレスポンス

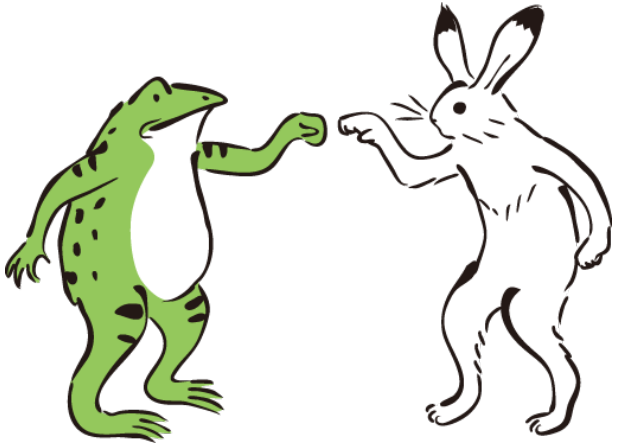
ISOG-J / OWASP / 他
- **ZAP**エヴァンジェリスト
- **脆弱性診断士**の活動
- 東京電機大学 国際化サイバーセキュリティ学特別コース(CySec) 外部講師

趣味
- 2018年のラスベガスで開催された**DEFCON OSINT CTF**で**6位**入賞してきました
- 2018年の11/3に国内で3回目の**Open xINT CTF**を**開催**してきました

ここまでのストーリー

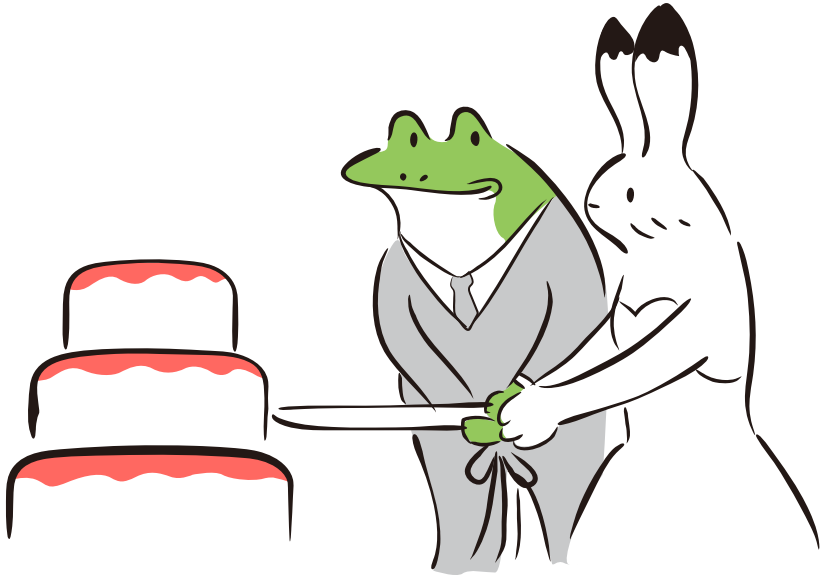
出会い
お互いを知る
末長くやっていけるか
……
これって……





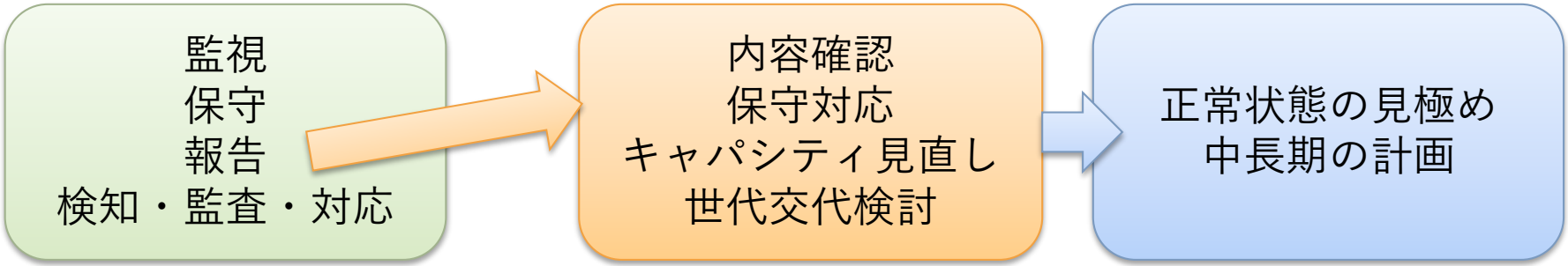
ここまでのストーリー

ゴールじゃなくてこれからのスタート、ってやつだ……



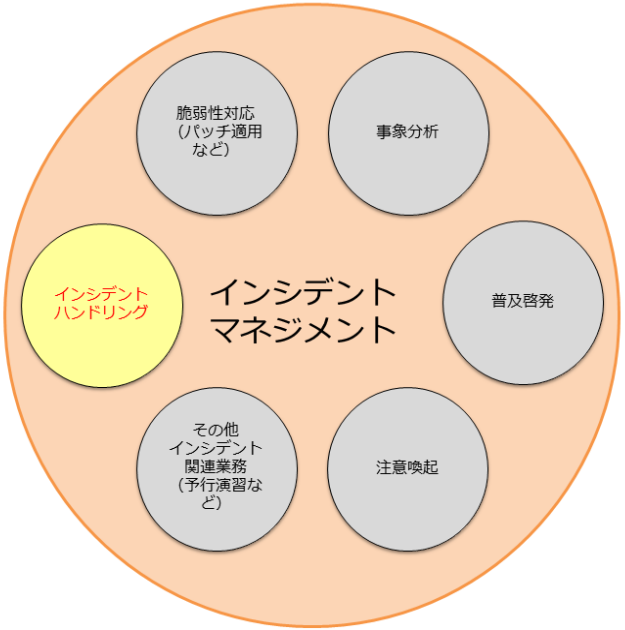
平時のポイント

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

(IW2017から再掲)平時の活動例



- 脆弱性対応（パッチ適用など）
- 事象分析
- 普及啓発
- 注意喚起
- その他インシデント関連業務（予行演習など）

http://www.jpcert.or.jp/m/csirt_material/files/manual_ver1.0_20151126.pdf より

(IW2017から再掲)平時の対応例

- まとめ
  - 平時の活動が有事のスムーズな対応に影響している
  - 平時の活動を通じて社内から必要とされる仲間になること
  - 平時の活動をまとめセキュリティ対応組織活動をアピール

インシデント時のポイント

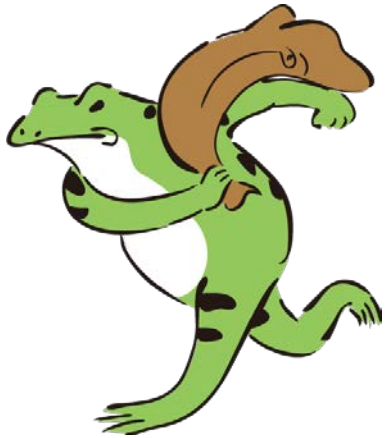
- インシデント時は、MSSから提供される情報を元に自分たちが判断、指示をする意識をもつ。
  - 起きてから焦るのではなく、普段から演習や訓練を！

提供されるサービス　　受けて行うこと

検知・報告

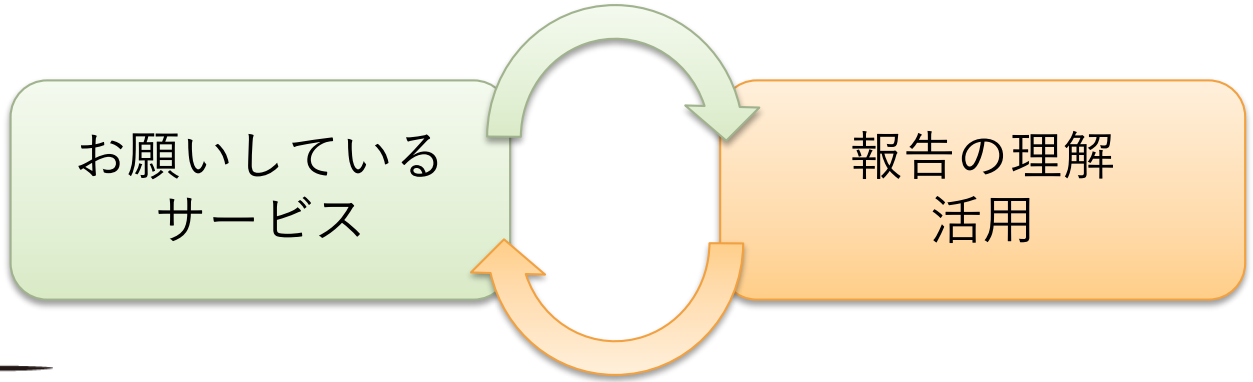
各種対応サービス
監査
など

対応基準で判断
必要なサービスの選択



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？



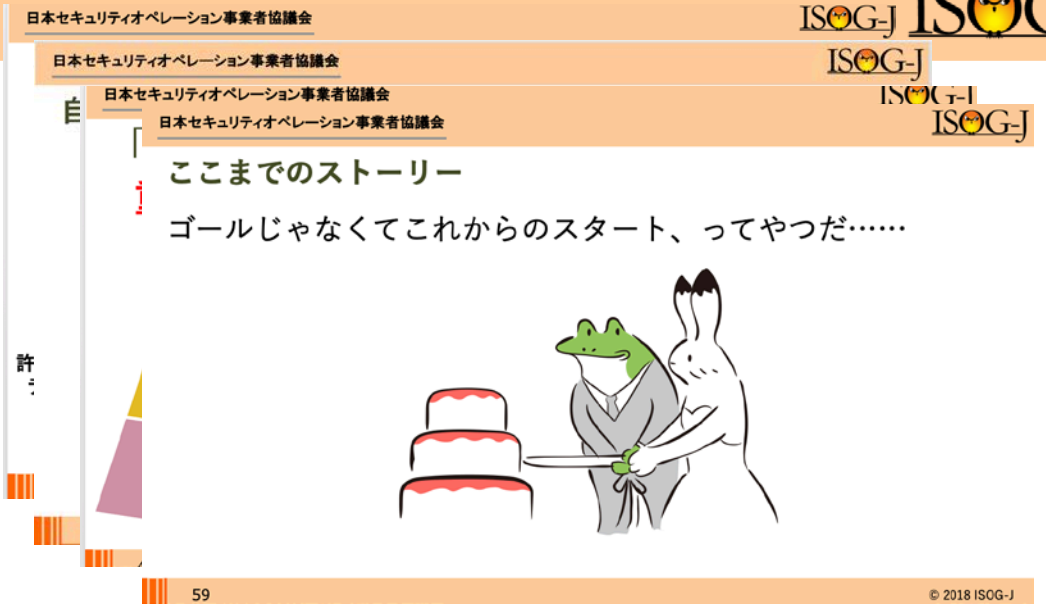
導入後のポイントまとめ

- 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. MSSとは、SOCとは
   - 被害を低減をするもの
2. 選ぶ前のポイント
   - 自分の今を見つめ直す
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/