これからのセキュリティサービスの選び方

2020年11月13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)

自己紹介

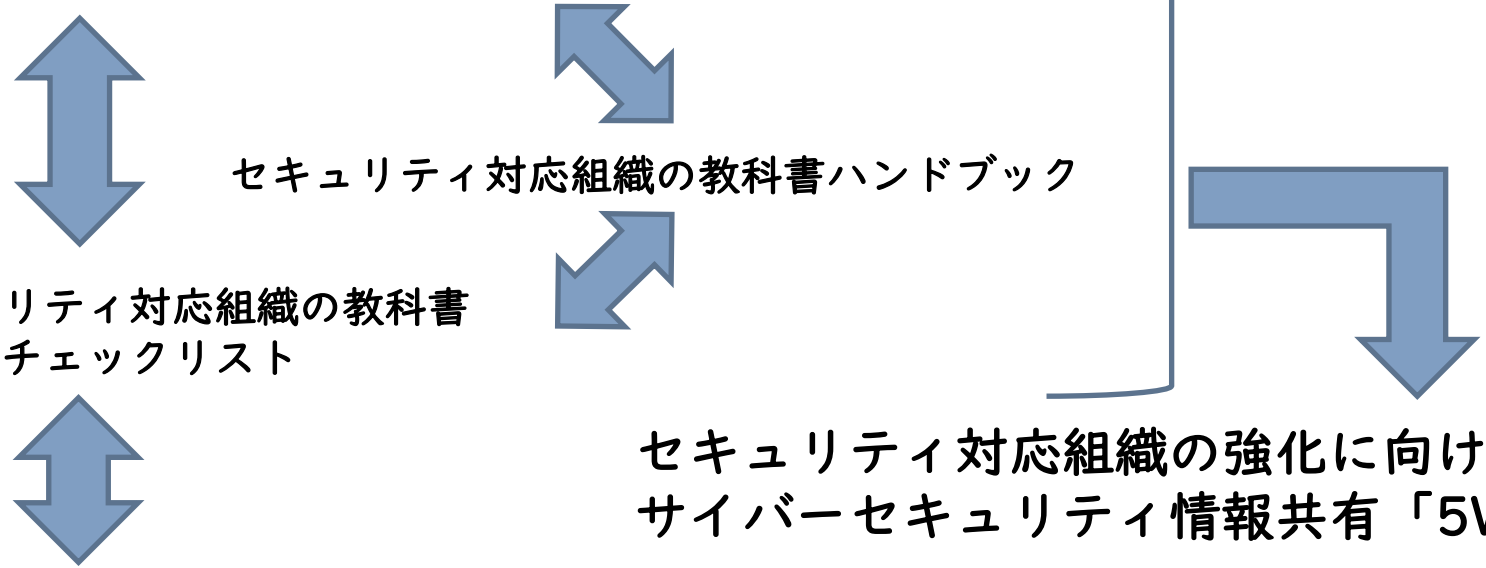
- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- NTTテクノクロス株式会社
  - セキュアシステム事業部　第三ビジネスユニット　勤務
  - 2016年度までは社名が「NTTソフトウェア株式会社」でした
  - NTTグループ セキュリティプリンシパル
  - ITU-T SG17 WP1 Q3 X.framcdc Editor
  - CISSP、情報処理安全確保支援士

ISOG-J とは

- 日本セキュリティオペレーション事業者協議会
  - the Information Security Operation providers Group Japan
  - 2008年創立、2020年11月現在 56組織が加盟
  - プロのセキュリティオペレーター、事業者の集まり
  - 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
  - 親団体は日本ネットワークセキュリティ協会(JNSA)
- http://isog-j.org/
  - Facebook ページ: /isogj
  - ISOG-J の読み方: いそぐじぇい

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の教科書



マネージドセキュリティサービス選定ガイドライン（10年ぶりに更新）
https://isog-j.org/output/2020/MSS-Guideline_v200.html

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
  - 添付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

今回お伝えしたいこと

- セキュリティはビジネスのリスクの一つと考え、そこから必要な対策を導き出す

- 導入するまでだけではなく、導入した後も継続的に見直す

- セキュリティはビジネスのリスクの一つと考え、そこから必要な対策を導き出す

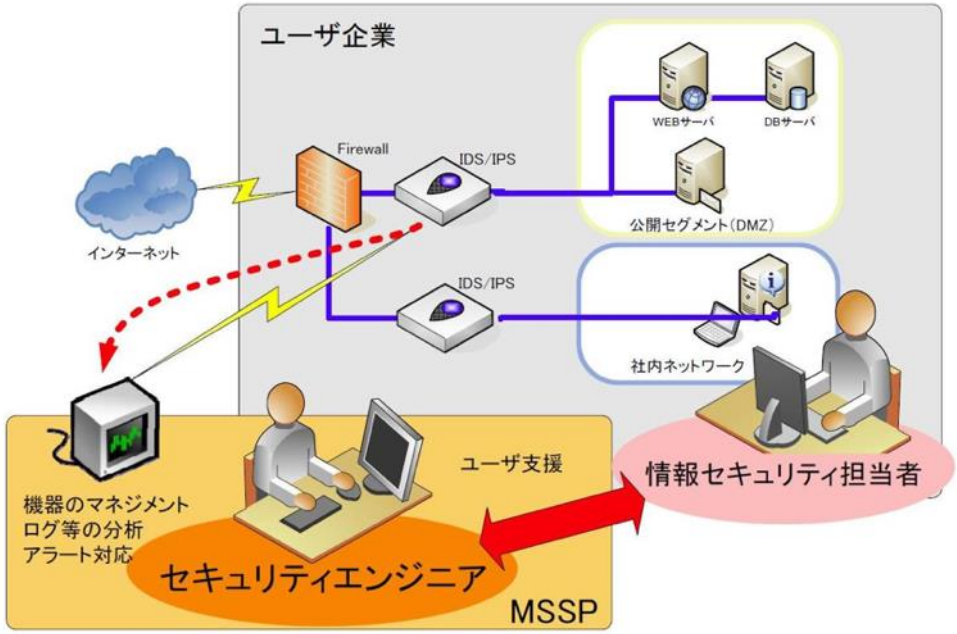
- 導入するまでだけではなく、導入した後も継続的に見直す

マネージドセキュリティサービス選定ガイドライン v1.0

- 2010年、初版公開
- 当時から行われていたセキュリティオペレーションセンター(SOC)による監視
- マネージドセキュリティサービスとして提供しているメンバーが作り上げた選定のためのガイドライン

変わるセキュリティ対策

・ 10年で変わったこと、変わらなかったこと



マネージドセキュリティサービス選定ガイドライン(2010, ISOG-J)
https://isog-j.org/output/2010/MSS-Guideline_v100.pdf

10年で変わったこと

サービスの範囲や製品が広がった

いわゆるSOCサービスの形態も様々になった

ユーザー企業などにCSIRTやセキュリティに対応する組織ができた

インシデントの影響がビジネスにおいて大きくなった

10年で変わらなかったこと

サービスを選定するまでの全体的な流れ

何を守りたいかはっきりさせること

最後の判断はユーザー側にあること

大きな変化の要因：各部署や部門との連携の必要性

インシデントの影響がビジネスにおいて大きくなった

- セキュリティが情報システム部門の一部分の技術の話ではなくなった
- サプライチェーン、IoT、制御システム、産業システムに広がるセキュリティ

ビジネスの全体の影響を各部署や部門と連携して考える必要性

セキュリティ対策までの検討の流れ：ガイドライン

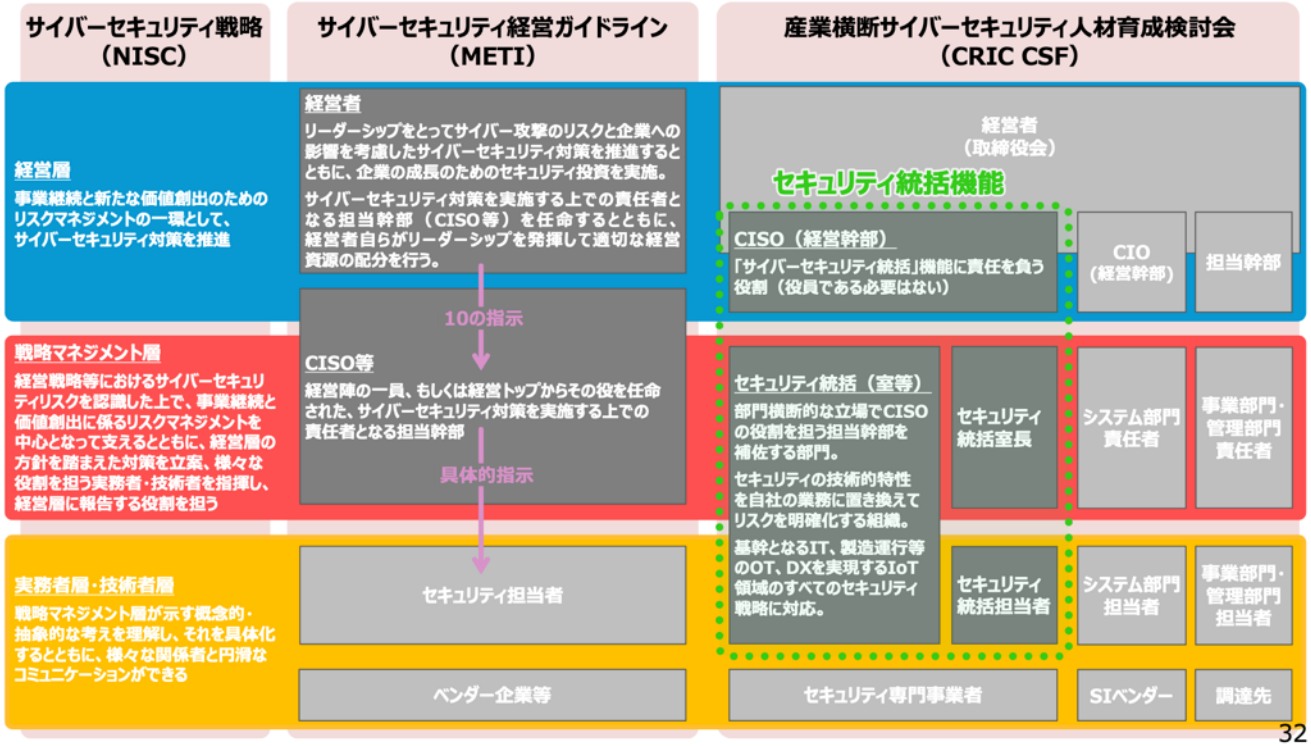
- サイバーセキュリティ経営ガイドラインv2.0(経済産業省)
  - https://www.meti.go.jp/policy/netsecurity/mng_guide.html

- サイバーセキュリティ経営ガイドラインv2.0 付録F サイバーセキュリティ体制構築・人材確保の手引き(経済産業省)
  - https://www.meti.go.jp/press/2020/09/20200930004/20200930004-1.pdf

- 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 第2版(IPA)
  - https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

- ユーザー企業のためのセキュリティ統括室構築・運用キット(統括室キット)(産業横断サイバーセキュリティ検討会)
  - https://cyber-risk.or.jp/contents/

セキュリティ統括、という考え方



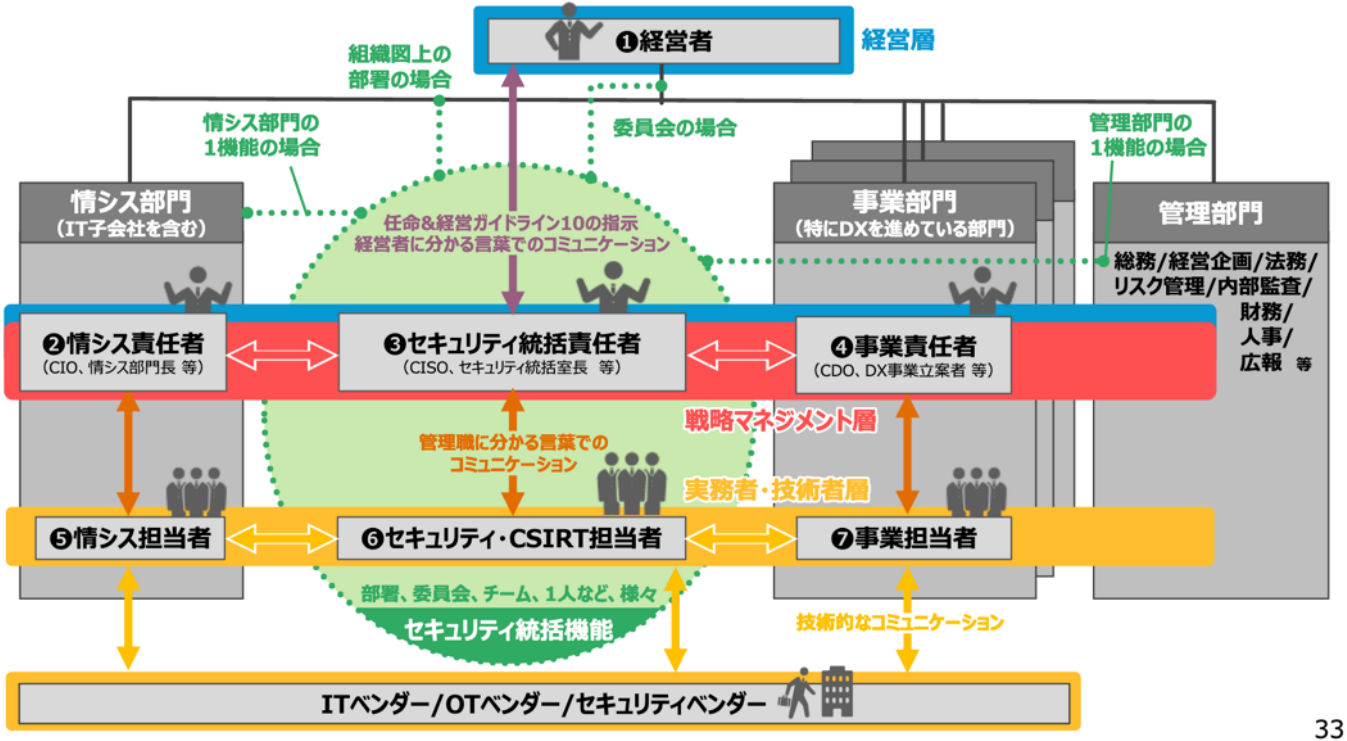
CISOや経営層を筆頭

CISOや経営層を補佐
各部署や部門と連携
組織横断的に統括

実務者や技術者も含む

第4回産業サイバーセキュリティ研究会ワーキンググループ2(経営・人材・国際) 資料３事務局説明資料
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf

セキュリティ統括、という考え方



第4回産業サイバーセキュリティ研究会ワーキンググループ2(経営・人材・国際) 資料３事務局説明資料
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf

例：テレワークの対応で、何が必要だったか？

ポリシー → 管理策 → 対策や手順

ビジネスの
リスク

会社のルール
法律や規制

VPN?
持ち出すPC?
ゼロトラスト？何それ？

守るべきものは何？
それはどこにある？
ビジネスのリスクは何？

今までのルール
新たに必要なルール
ここではどうするか

いきなりここの話だけを
していなかったか？

導入企画

- 導入企画時に検討すべき内容
- 保護対象

何が必要かを知る

- MSSPが提供するサービスの情報収集
- MSSPの選定
- 契約・SLA

自分たちに合うサービスを探す

何が必要かを知る

ポリシーの決定の要素

- 保護すべき資産やサービスを定義する
- 保護すべき情報を定義する
- 情報利用者を定義する
- 情報の維持方法を定義する
- 情報の廃棄方法を定義する
- システムから取得できる情報（ログ）を定義する
- サービスを見直すタイミングを定義する

- インシデント時の影響を明確化する
- インシデント判断の根拠を明確化する

現状の把握

- システムやネットワークの現状把握
  - ネットワーク構成、ネットワーク帯域、リモートメンテナンス回線、アクセス数、クライアント数、利用者数、ログ量、システムやネットワークを管理している主体の把握、利用しているクラウドサービス
- 保護対象と保護方法の定義
  - 対象サービス、対象マシン、対象マシン詳細、対象通信、アプリケーション、監視目的、委託範囲、社内体制

何が必要かを知る

図2-4.2 S社で利用した被害発生可能性と重要度からリスク値を判定する方法の例[9]

①：被害発生可能性

被害発生可能性		脆弱性		
		低	中	高
脅威	高	中	高	高
	中	低	中	高
	低	低	低	中

②：重要度

重要度	情報資産の価値・事故の影響の大きさ
高	事故が起きると、法的責任を問われたり、取引先、顧客、個人に大きな影響がある等事業に深刻な影響を及ぼす
中	事故が事業に重大な影響を及ぼす
低	事故が発生しても事業にほとんど影響はない

①被害発生可能性と②重要度の掛けあわせで算出

※脅威と脆弱性の基準

脅威	高	通常の状況で脅威が発生する（いつ発生してもおかしくない）
	中	特定の状況で脅威が発生する（年に数回程度）
	低	通常の状況で脅威が発生することはない
脆弱性	高	対策を実施していない（ほぼ無防備）
	中	部分的に対策を実施している
	低	必要な対策をすべて実施している

①×②：リスク値

リスク値		重要度		
		低	中	高
被害発生可能性	高	2	3	3
	中	1	2	3
	低	1	1	2

ビジネスのリスクに対してリスク値を算定して優先度やコスト決定の参考にする

9 リスク値の算定方法の詳細については、中小企業の情報セキュリティ対策ガイドライン(IPA)を参照。
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

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 第2版(IPA)
https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

自分たちに合うサービスを探す

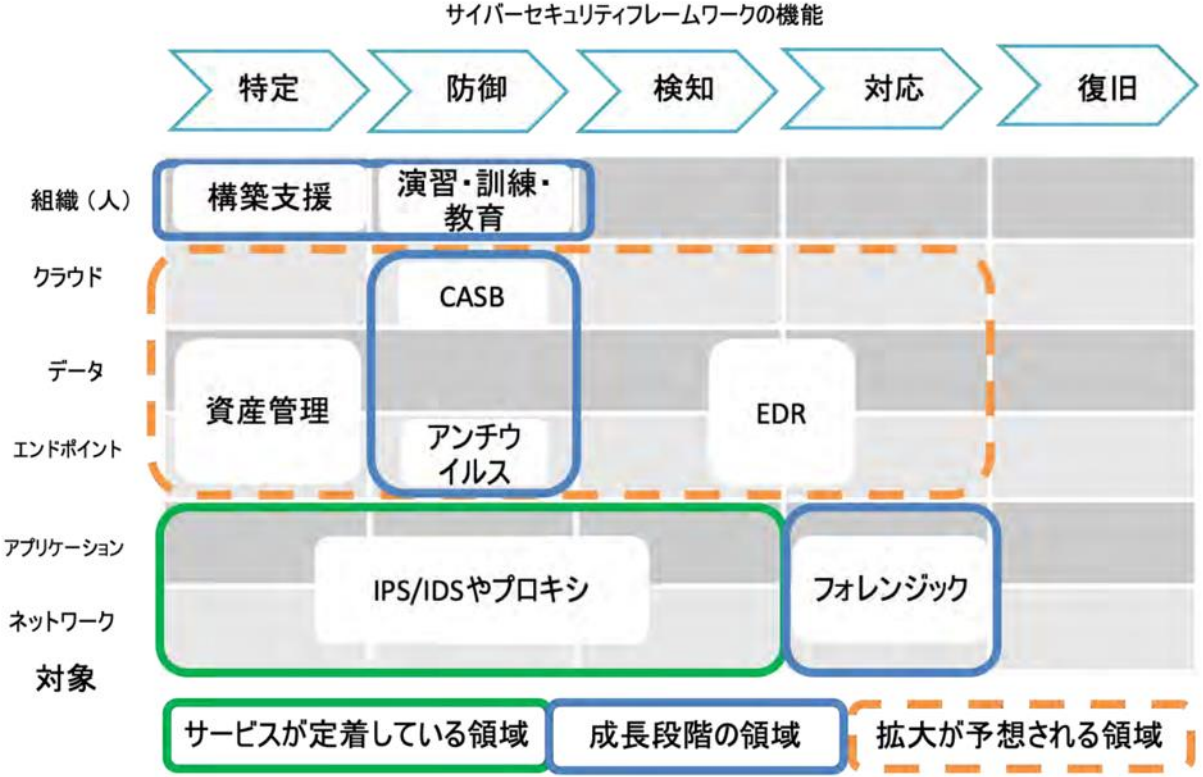


図 4 サイバーセキュリティフレームワークと MSSP が提供するサービスのマッピング

サービスの情報例

- サービス導入に必要な機材
- 緊急時対応
- 定期的なコミュニケーション
- セキュリティインシデント判断基準（レポートの危険度の考え方）
- サービスのカスタマイズ
- 独自の脅威情報などの入手
- サービス品質
- サービス価格
- サービス提供体制
- サービス提供手段

SOCの通知も様々

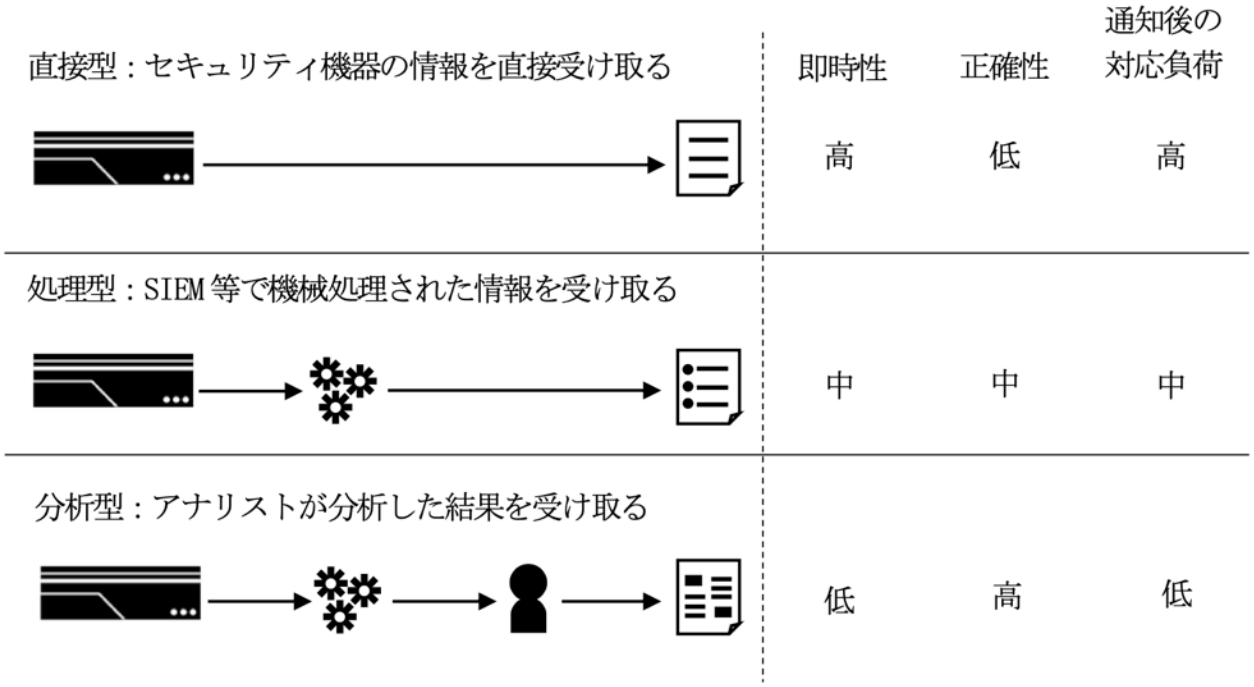


図 6　MSSP ごとのインシデント通知内容の差異

通知の内容の違い

通知内容の違いがコストにも影響する

自分たちがどう活用したいか、どこまでできるかで選ぶ

導入設計・構築

- MSSの導入パターン
- 監視環境の構築・導入・運用開始まで
- ライセンス・サポート

導入設計・構築

導入済みのセキュリティ機器
やソフトウェア
監視サービスを追加

新規導入のセキュリティ機器
やソフトウェア
と監視サービス

監視サービスのあるクラウド
によるセキュリティサービス

セキュリティの
設定
関連機器の設定
導入場所

MSSPへの接続可否
監視運用試験
エージング・チューニング・学習期間

- セキュリティはビジネスのリスクの一つと考え、そこから必要な対策を導き出す

- 導入するまでだけではなく、導入した後も継続的に見直す

平時の運用

- サービス
- 機器やサービスの世代交代
- 監視
- ログの取り扱い
- 平時の定期的な報告

- 何も起きていないうちにできる準備を
- 継続した監視からインシデントへの移行
- 平時のデータの積み上げで定期的な見直しを

インシデント時の運用

- インシデントの定義
- インシデントの検知
- 原因の追及
- 対応策の検討
- 利用者側との調整
- 対策の実施
- 有効性の確認

インシデント時の運用

・ 事前の準備と密接なやりとり

検知・通知

対応・復旧・回復

（事前準備）
インシデントの定義
判断基準

判断・指示

有効性の確認

継続的な運用のための2つのサイクル

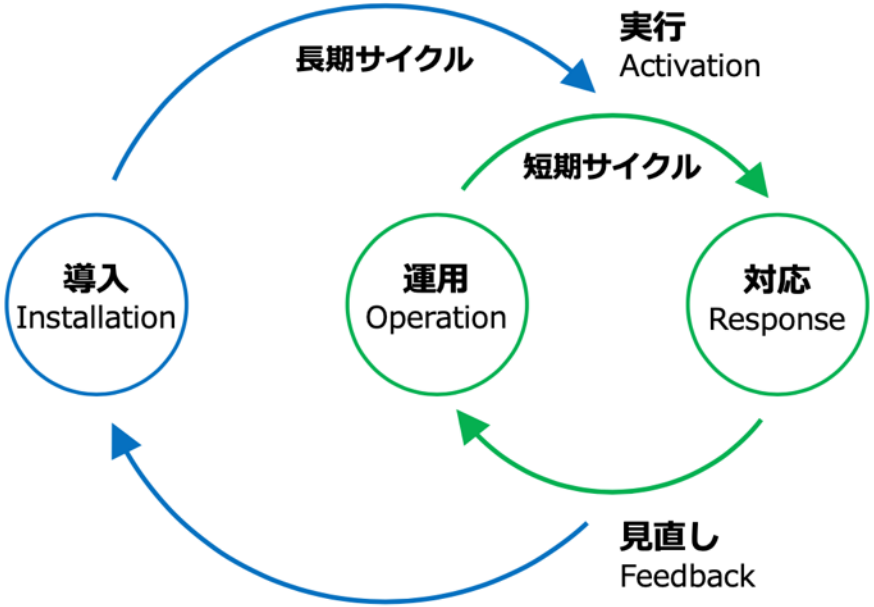


図 1　セキュリティ対応実行サイクル

長期サイクル
短期サイクル

2つのサイクルで継続的に効果的な運用を

見直す契機は様々

セキュリティ対応組織の教科書より

まとめ

- セキュリティはビジネスのリスクの一つと考え、そこから必要な対策を導き出す
  - セキュリティ統括を中心に全体として必要なものは何かを考える
  - 自分たちに合うサービスを選定する

- 導入するまでだけではなく、導入した後も継続的に見直す
  - 社会的な変化や周辺環境の変化に対応できるような見直しを

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