NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

公開資料

ISOG-Jの2018年度の成果あれこれ

2019年6月12日

日本セキュリティオペレーション事業者協議会

日本セキュリティオペレーション事業者協議会

公開資料

- 49社、約300人
  - 2018年度で42社から47社に増加
- 2018年で10年。

WG		リーダー
1	セキュリティオペレーションガイドラインWG	トライコーダ 上野さん
2	セキュリティオペレーション技術WG	川口設計 川口さん
4	セキュリティオペレーション認知向上・普及啓発WG	NTTセキュリティジャパン 阿部さん
6	セキュリティオペレーション連携WG	NTTテクノクロス 武井
	新技術とオペレーションのプロジェクト	IIJ ももいさん SCSK 亀田さん

- 2018年度 JNSA賞 ワーキンググループ(WG)の部 受賞

2018年度成果物

公開資料

日時	タイトル	発表
4/9	セキュリティ対応組織の教科書 v2.1	WG6
5/28	Webアプリケーション脆弱性診断ガイドライン、スキルマップ＆シラバス	WG1 ※
9/19	セキュリティ対応組織の教科書 ハンドブック	WG6
1/15	Webシステム/Webアプリケーションセキュリティ要件書 Ver.3.0	WG1 ※
4/5	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	WG6

※OWASP JAPANと共同発表

2018年度各種発表など

月日	発表場所
5/31	Internet Week ショーケース in 広島
7/11	JANOG 42 ミーティング BoF
7/21	ISACA名古屋支部 月例会
8/23	IT協会様2018年度第2回会員交流会
8/29-10/4	JNSA全国横断サイバーセキュリティセミナー2018
11/10	セキュリティうどん（かまたま） 16杯目 (香川県)
11/13	IT協会様第4期サイバーセキュリティ戦略マネジメント研究会
11/28	Internet Week 2018
12/3	ISOG-J内セミナー、事業者連絡会
1/22	JNSA Network Security Forum 2019
1/24	JANOG43 ミーティング
3/8	Security Days Spring 2019
3/13	IT協会様情報セキュリティシンポジウム
	警視庁様サイバーセキュリティサポーター活動支援

セキュリティ対応組織(SOC,CSIRT)の教科書

公開資料

- 参照されることが増えました
- 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)

公開資料

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

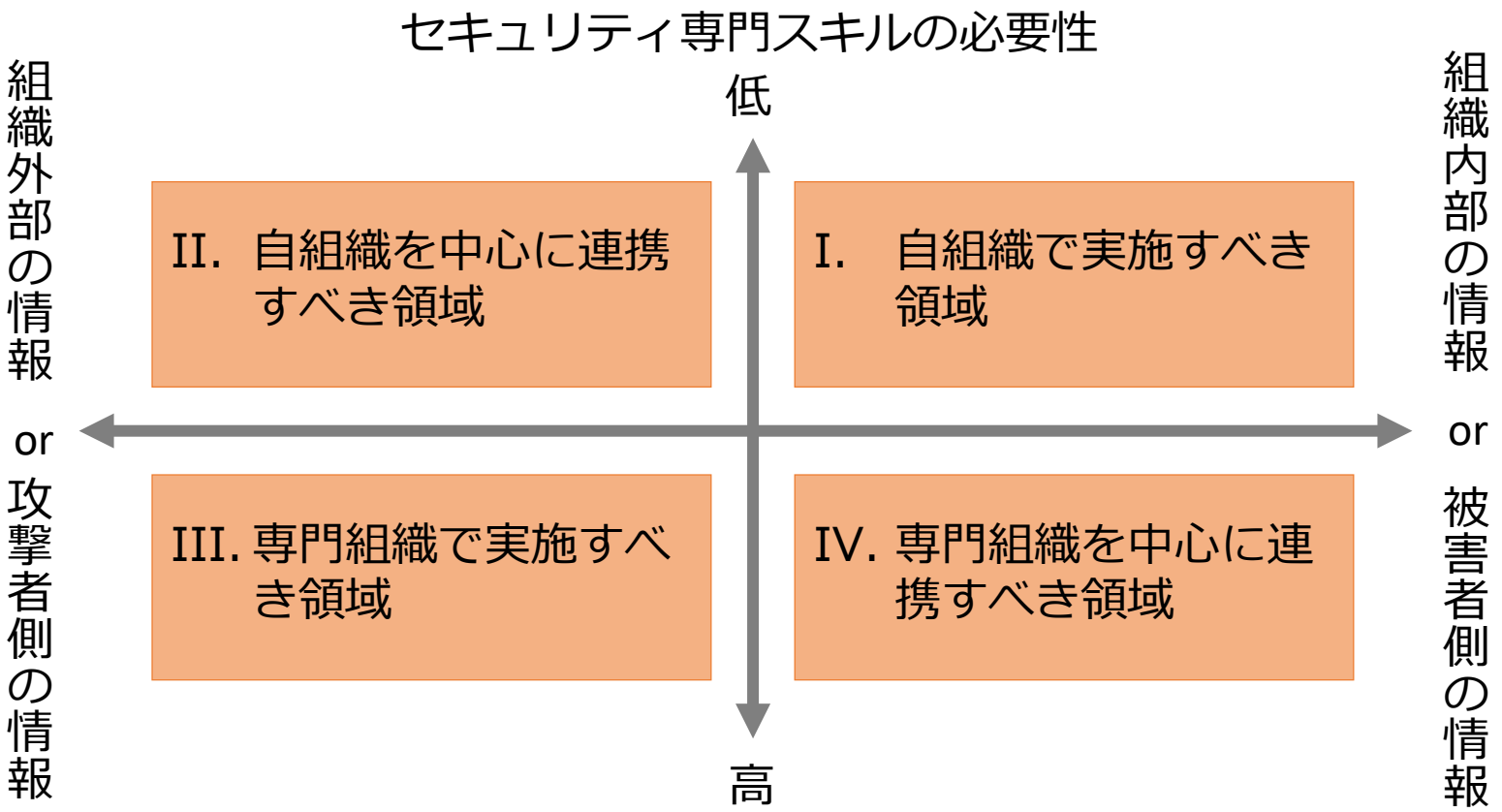
企業・組織ごとに異なる

公開資料

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。

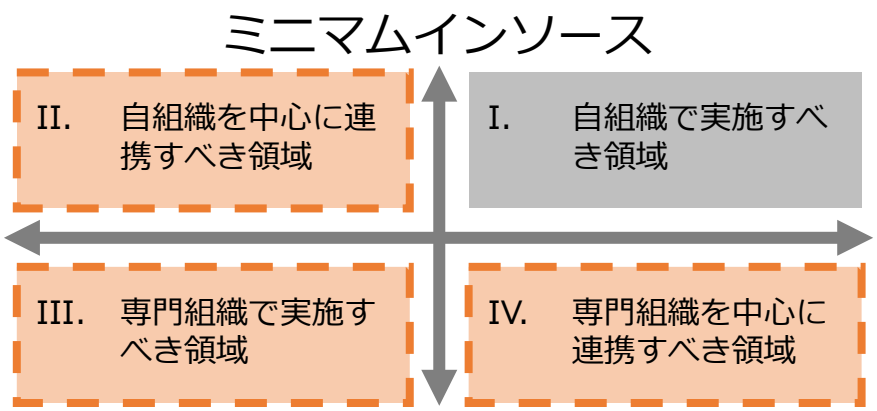
4つの領域への役割の分類

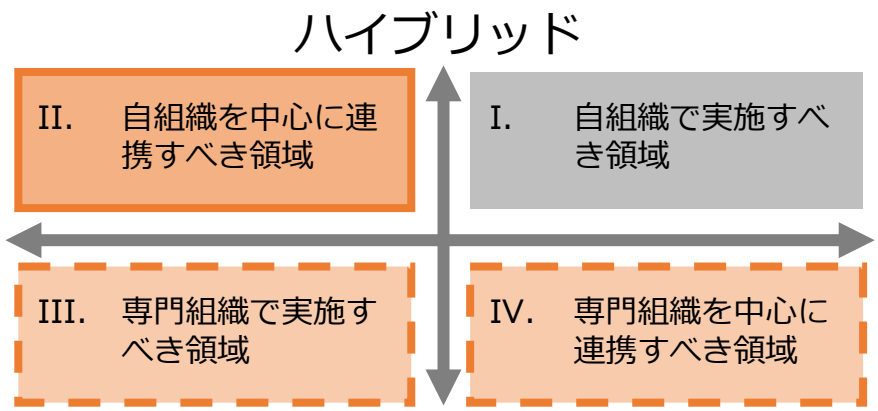
公開資料

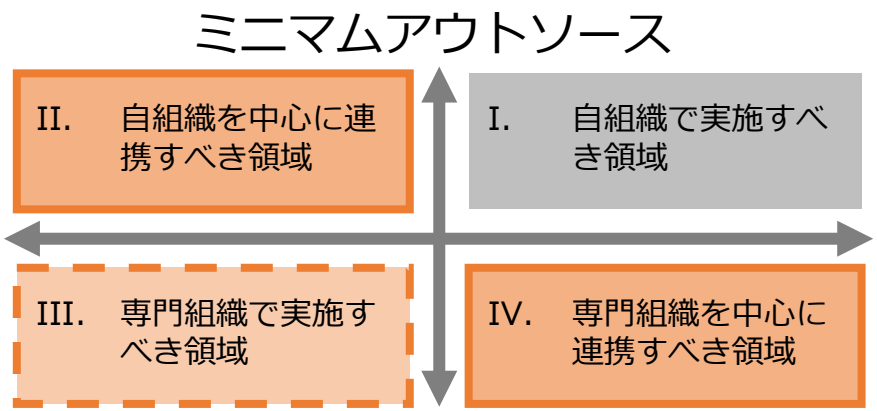


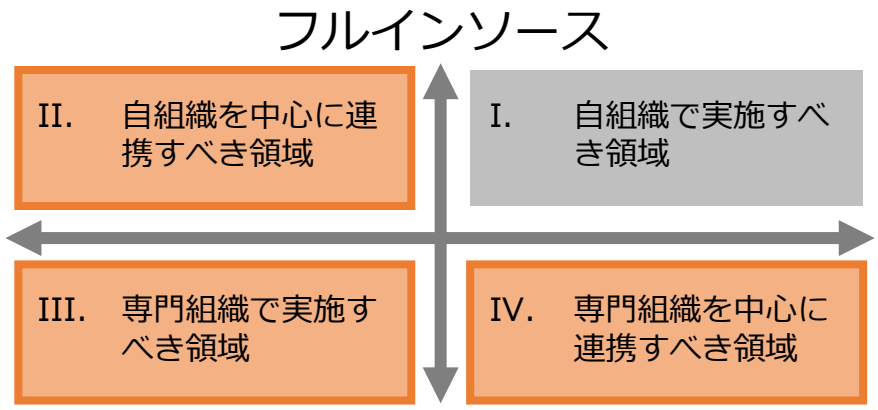
インソースとアウトソースで4つの実現パターン例を定義

公開資料









公開資料

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)

公開資料

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

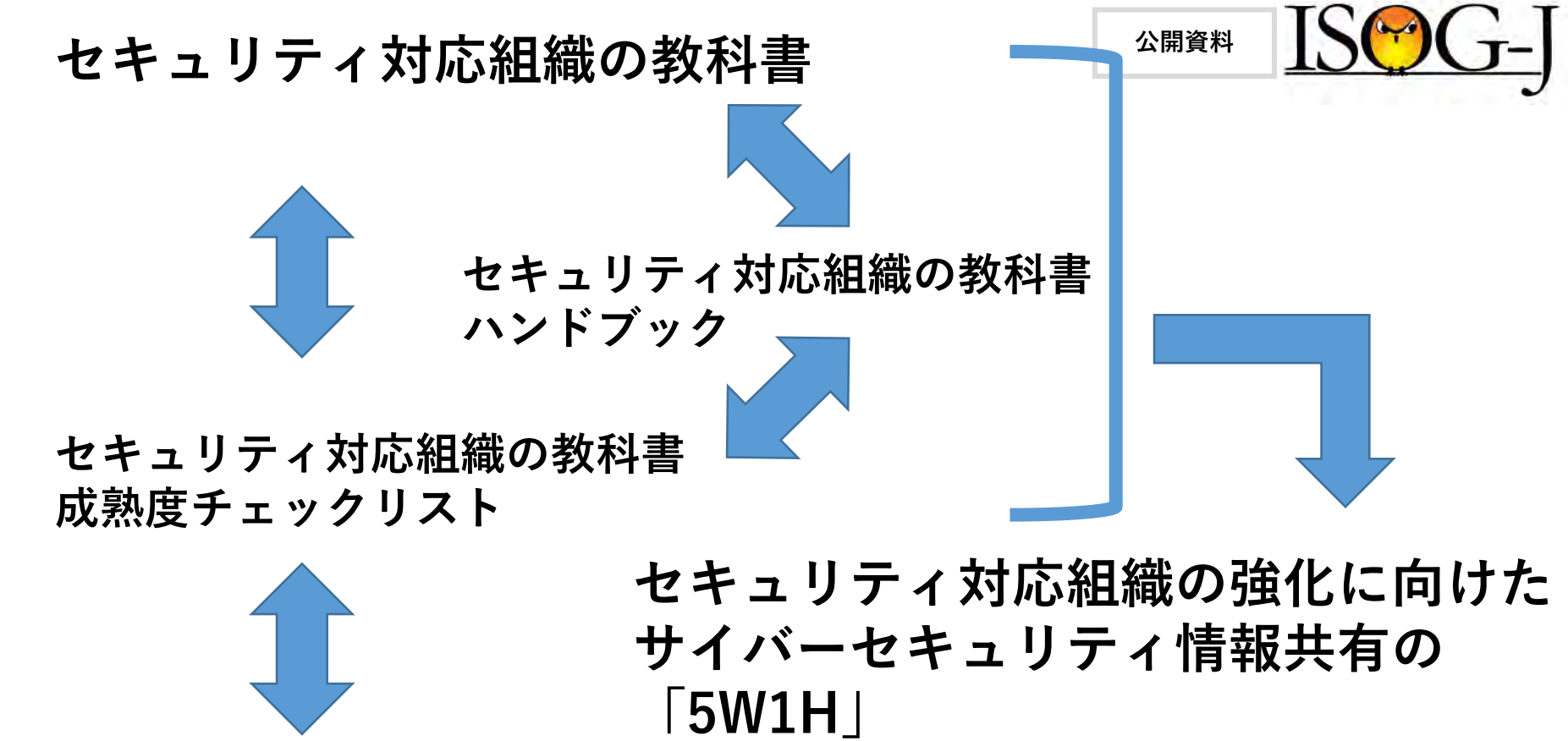
セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」

公開資料

- 初版は情報共有の課題提起で終わっていました。
- 第2版では情報共有の各段階の具体例を追記しました。

- 第1版は人気なので英語版あります！「6Ws」
  - 第2版も反応次第で英語版を改版！？

成果物シリーズ



InternetWeek 2018

公開資料

- 2015年から4年連続4回目です！
- 「もう一人で困らない！セキュリティ対応のアウトソース」と題して発表しました

- 5/31にInternet Week ショーケース in 仙台で仙台の皆さんに披露しました

原点に立ち返る

公開資料

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

公開資料

ISOG-J

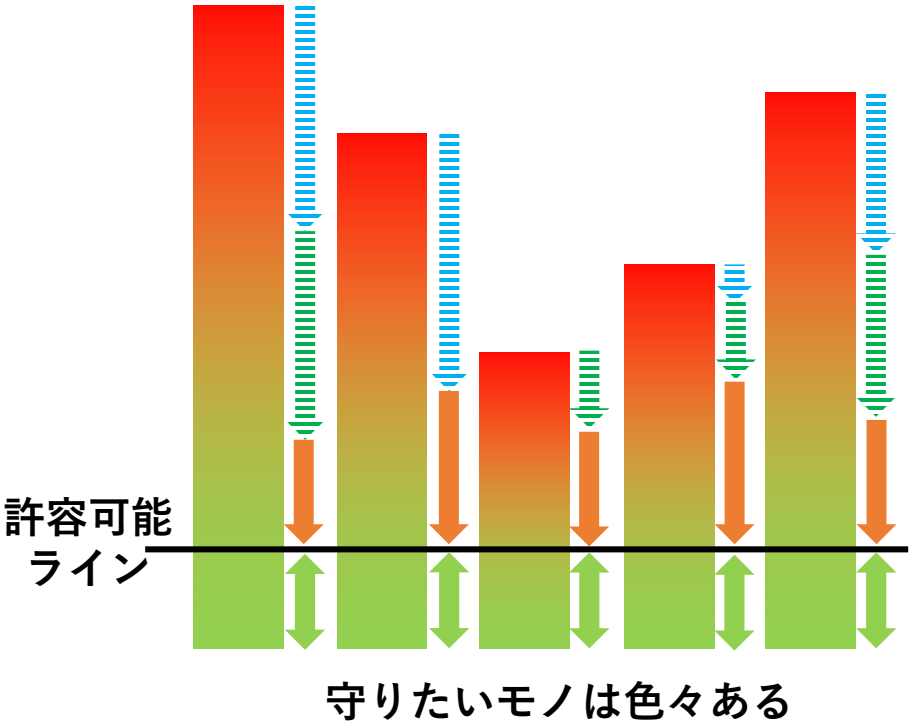
（ゼロにはならないが許容範囲はある）

想定される被害 ＝ 価値（守りたいモノの） 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

公開資料



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・・・

公開資料

- **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

当日の模様

JNSA

公開資料 ISOG-J

公開資料

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！

WG6 2019年度の議題や発表予定

公開資料

- SOC,CSIRTの成熟度チェックリスト（通称：ISOMM)の各地での説明と展開、データ収集、分析
- 「マネージドセキュリティサービス選定ガイド v1.0」(2010年発表） v2.0 リリース
  - 各地での説明や展開も並行して行います
- 「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」 v3.0」の更改に向けた議論
- InternetWeek 2019 における発表

終わりに

公開資料

今年度もセキュリティオペレーションサービスの普及とサービスレベルの向上に貢献できるよう活動を続けます