D1-2 今求められるSOC,CSIRTの姿とは
～世界の攻撃者をOMOTENASHIしないために～
イントロダクション ～ザ・ワールド～

2017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)

講演者

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
- NTTテクノクロス株式会社
  - クラウド＆セキュリティ事業部　第一事業ユニット　勤務
  - 去年までは社名が「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

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11月9日現在、40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：　http://isog-j.org
- facebook：/isogj
- twitter：@isog_j

今年は2つ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 v2.0
  - http://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

- 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」
  - http://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.html

- いますぐダウンロードを！

3年連続3回目ですよね？

- はい！
- 2015年：「150分でわかる！セキュリティ対応ができる組織になる10のコツ」
  - SOCやCSIRTのための10のコツを発表しました。
- 2016年：「失敗から学ぶ、SOC/CSIRTのあり方」
  - もう一歩具体的に、「セキュリティ対応組織の教科書」を提唱し、組織の具体例を示しました。
- 過去の資料はInternetWeekの「過去のIW」から辿れます

前回までの発表のおさらい
←ココから

（参考）2015年の10のコツ

1. 防御から対応までのすべてをSOCに統合せよ
2. 規模と透明性/俊敏性のバランスを取れ
3. SOCに適切な権限を与えよ
4. できる事をやろう
5. メンバーは量より質を重視せよ
6. 買った技術は最大限利用せよ
7. データを集めて整理せよ
8. SOCの任務遂行を保護する
9. 脅威情報の賢い消費者であり供給者であれ
10. 冷静に・計算高く、プロらしく対応せよ

資料URL（約100ページ、4.74MB）
https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/s13/

(参考) 2016年の「失敗から学ぶ」から

- セキュリティの対応組織の構築時、運用時、インシデントレスポンス時に分けて、ありがちな「失敗あるある」を定義。

- 「失敗あるある」に陥らないために「セキュリティ対応組織の教科書 v1.0」をリリース。

資料URL（58ページ、5.1MB）

https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/d1/d1-3-hayakawa.pdf

(参考) 2016年のセキュリティ対応組織の教科書から

- 組織全体を俯瞰すべく、**9つの機能と54の役割**で定義
- 54の役割を**4つの領域**に分類
- 4つの領域について、自組織で実施すべきもの（インソース）と専門組織へ依頼するもの（アウトソース）のパターンを**4つのパターン**で定義

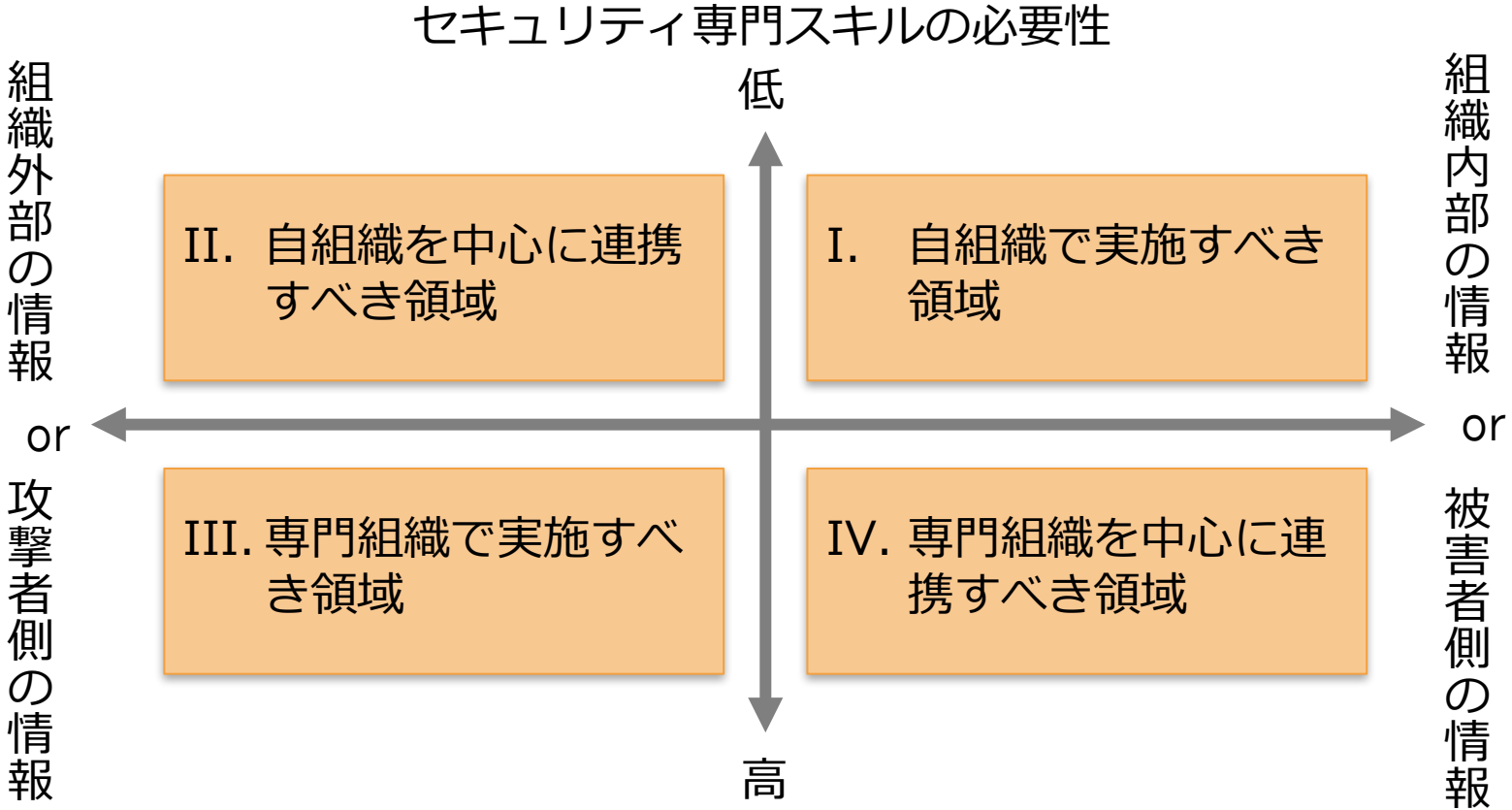
組織の持つ9つの機能、54の役割

9つの機能

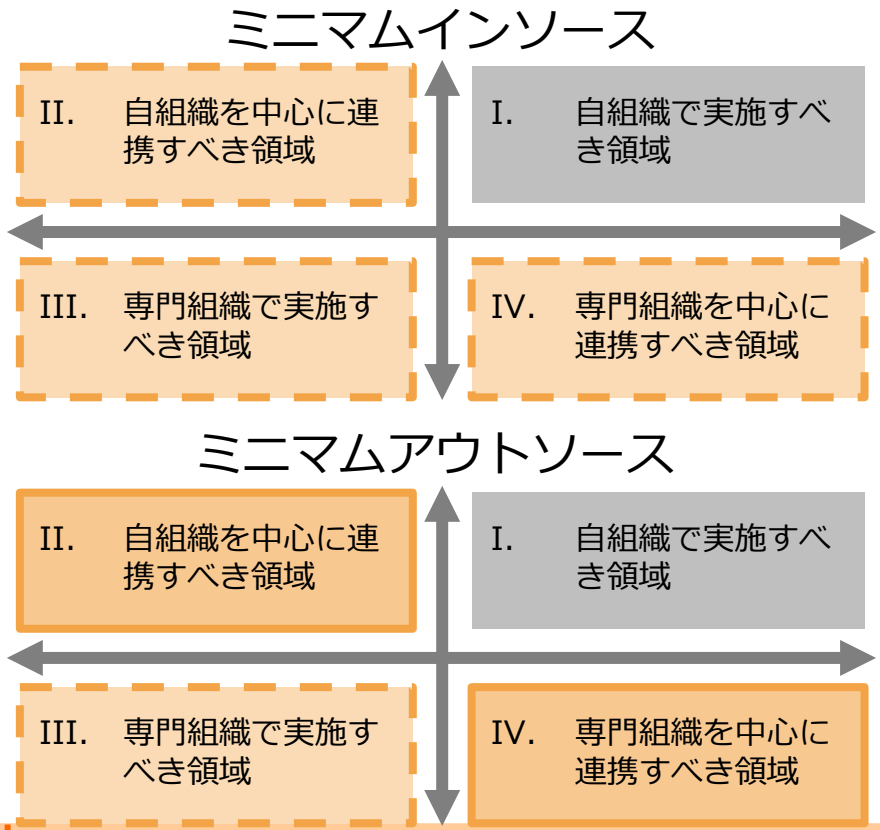
A. セキュリティ対応組織運営
B. リアルタイムアナリシス（即時分析）
C. ディープアナリシス（深堀分析）
D. インシデント対応
E. セキュリティ対応状況の診断と評価
F. 脅威情報の収集および分析と評価
G. セキュリティ対応システム運用・開発
H. 内部統制・内部不正対応支援
I. 外部組織との積極的連携

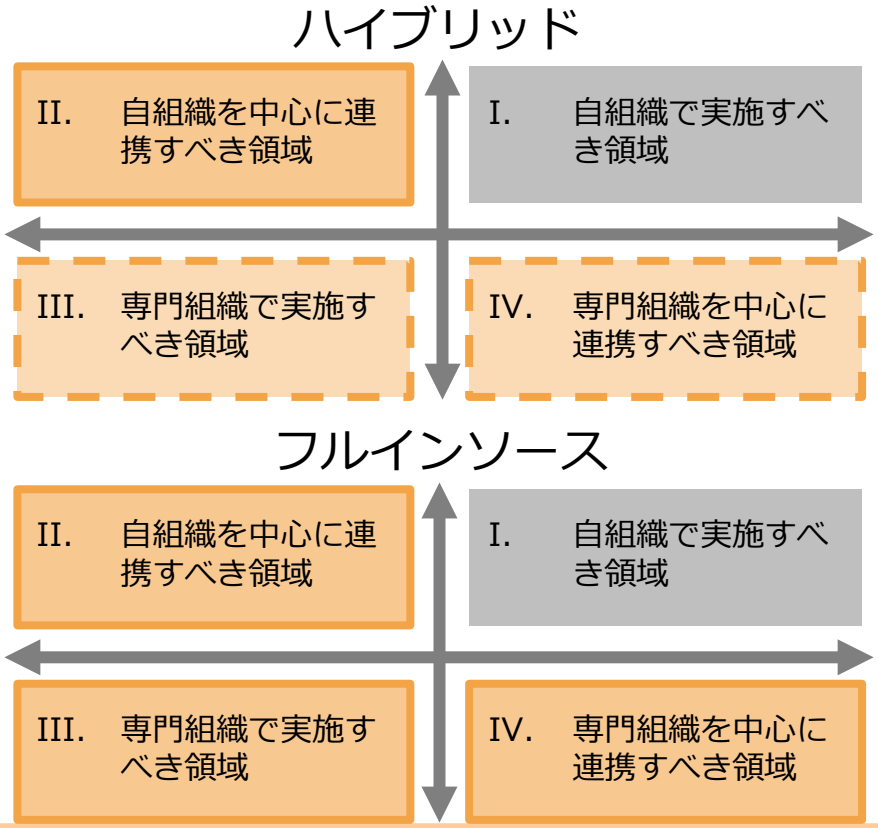
各項目にさらに複数の役割が存在
合計54の役割が存在する

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





前回までの発表のおさらい
←ココまで

あれから1年……

- サイバーセキュリティ経営ガイドライン改訂(経産省)
- サイバーセキュリティ2017(NISC)

- 脆弱性情報と適用の対応に注目が集まる
  - WannaCry, Struts2, Tomcat
- 多数のDDoS、IoTに広がる不安

情報の共有について注目が集まる

その他にも求められることが増える

「CSIRT高度化」「プライベートSOC」……

新しい言葉に踊らされずに、全体から見ましょう
「できる事をやろう」。
時間がかかります。アウトソースも活用を。

今日はSOCやCSIRTの具体的な業務フローや
組織の成熟度で全体の考え方を深めつつ、
情報共有の課題を整理してこれからの
セキュリティ対応について考えます。

(参考：アイコン類) http://www.security-design.jp/