セキュリティオペレーションと インシデントレスポンスの蜜月

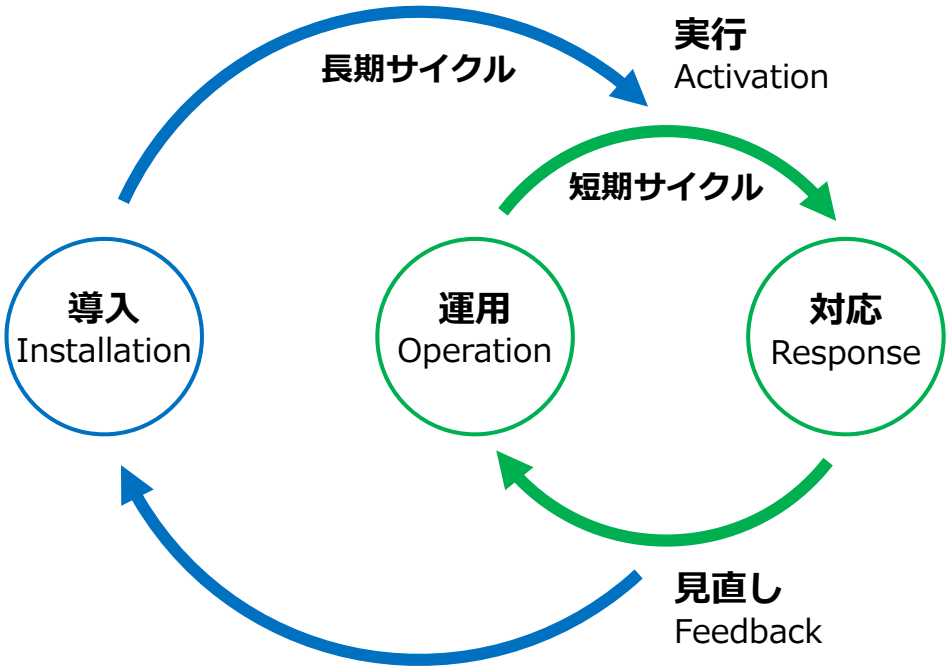
日本セキュリティオペレーション事業者協議会（ＩＳＯＧ－Ｊ）
セキュリティオペレーション認知向上・普及啓発WGリーダー

ＮＴＴセキュリティ・ジャパン株式会社
アナリストチームリーダー ／ セキュリティプリンシパル

阿部　慎司

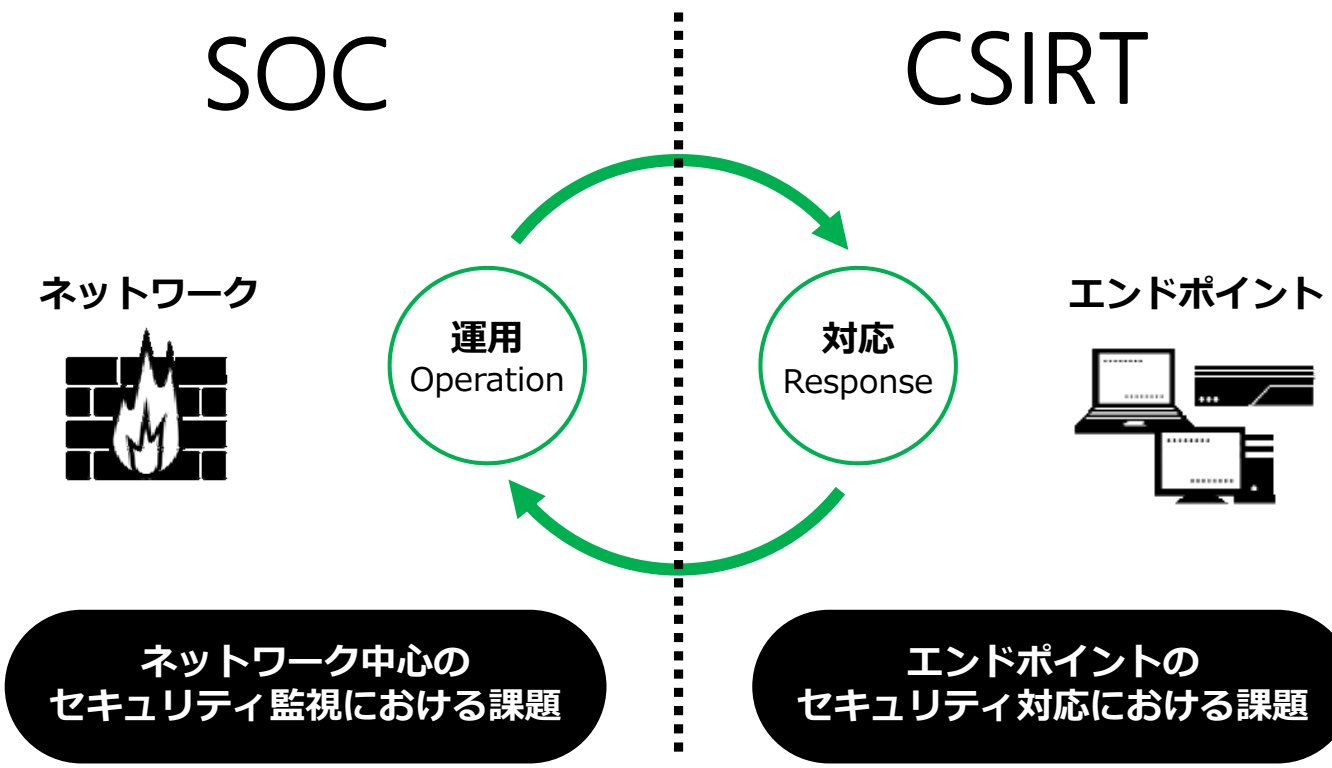
- **阿部　慎司**
  - 日本セキュリティオペレーション事業者協議会（ISOG-J）
    セキュリティオペレーション認知向上・普及啓発WG（WG4）リーダー
  - NTTセキュリティ・ジャパン SOCアナリストリーダー
  - NTTグループ セキュリティプリンシパル
- 個人の活動
  - Security along DesigN http://www.security-design.jp/
  - セキュリティアイコンをパブリックドメイン提供

セキュリティ対応実行サイクル



参照：ISOG-J『セキュリティ対応組織（SOC/CSIRT）の教科書』P4

セキュリティオペレーションとインシデントレスポンス



運用 Operation

ネットワーク中心の セキュリティ監視における課題

1. **見えない**（通信の中身が）
   - HTTPSの普及
   - マルウェア独自の暗号通信
2. **見てない**（監視対象NW以外で接続）
   - リモートワーク
   - 公衆Wi-Fi、テザリング
3. **見ようがない**（通信が出ない、正常通信と区別がつかない）
   - 内部感染
   - 正規Webサービスを活用した悪性通信

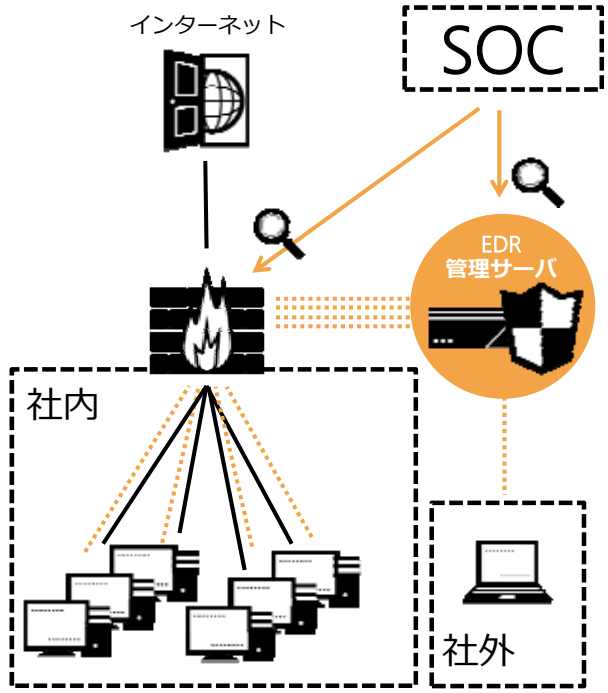
対応 Response

エンドポイントの セキュリティ対応における課題

1. **ない**（そこにあるはずの被害端末が）
   - DHCP
   - フリーアドレス
2. **いない**（判断、対処できる人が）
   - 夜間、休日
   - 属人化
3. **わからない**（今起こっている正しい状況が）
   - 判断材料不足
   - 判断スキル不足

エンドポイントレスポンス（ＥＤＲ）
有効活用のひとつの理想形

EDR概念図



運用
Operation

- **見えない**（通信の中身が）
  - エンドポイント側で検知
- **見てない**（監視対象NW以外で接続）
  - 社外からでもEDRサーバにつながるように設定
- **見ようがない**（通信が出ない、正常通信と区別がつかない）
  - エンドポイント側で挙動を確認

対応
Response

- **ない**（そこにあるはずの被害端末が）
  - EDR管理サーバで一元的に管理
- **いない**（判断、対処できる人が）
  - 24/365のSOCから一次対処
    （論理隔離、プロセスキル等）
- **わからない**（今起こっている正しい状況が）
  - NWとエンドポイント両方でデータ収集
    （現行MSS＋EDRというイメージ）

現実にこのレベルまで昇華するには
製品が成熟していない、
SOCの実績が不足している、といった課題がある

知っトク情報

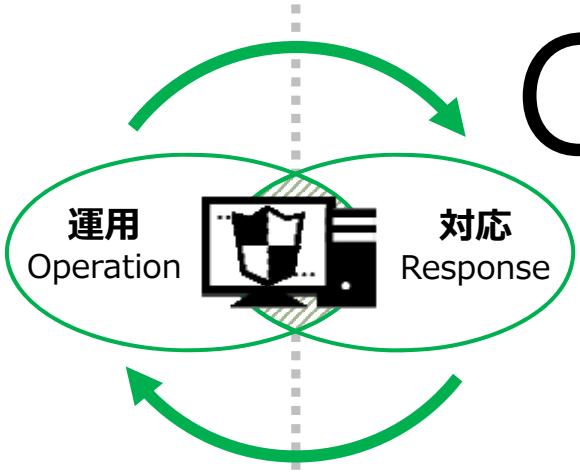
そもそも自組織はどのくらいちゃんとやれているのだっけ…

セキュリティ対応組織
成熟度セルフチェックシート

http://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

自組織の強み、弱みや
将来に向けた改善点が
可視化されます。

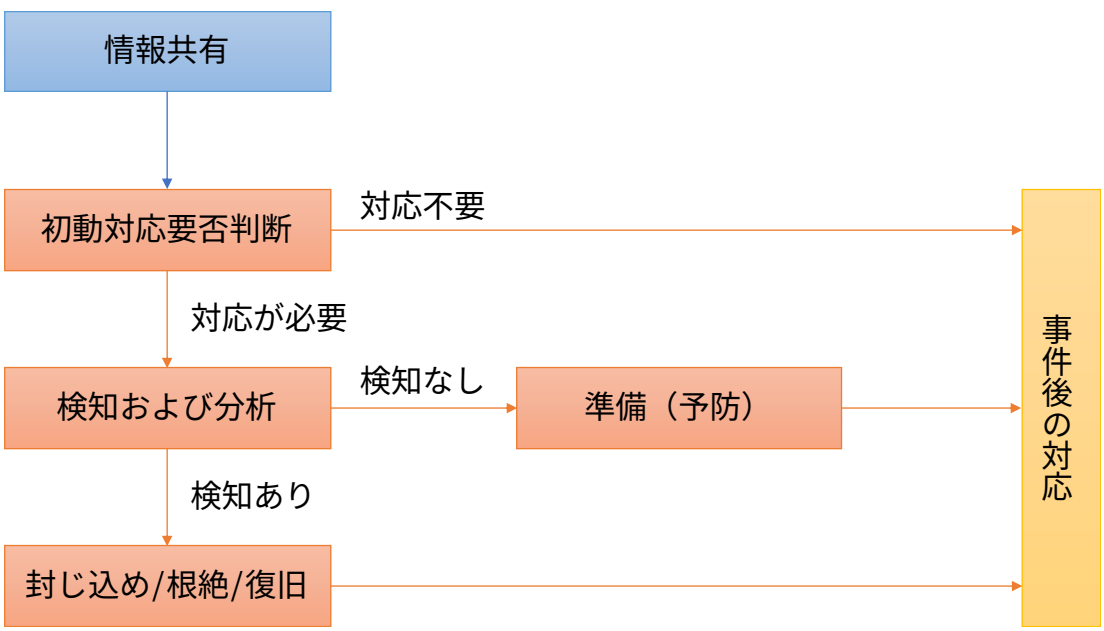
SOC CSIRT



緊急対応サービス
（フォレンジック等）

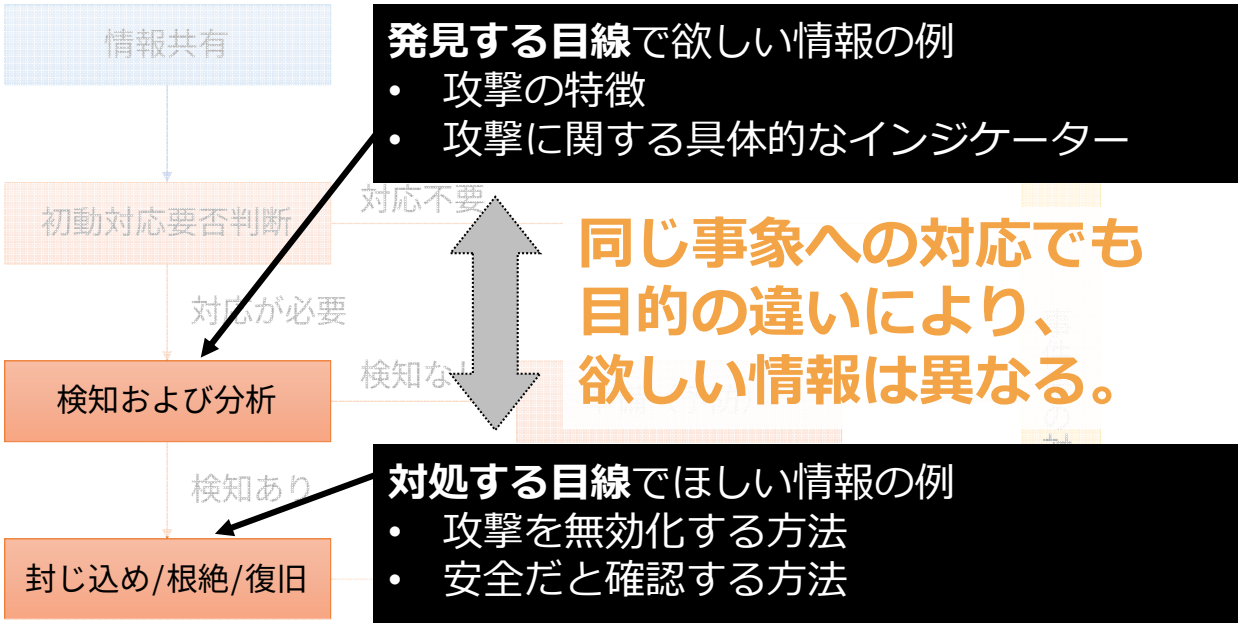
対応領域が重なり、より密接に関連。
情報連携が今まで以上に重要に。

情報共有を出発点としたセキュリティ対応



参照：ISOG-J『**サイバーセキュリティ情報共有の「5W1H」**』P4

情報共有を出発点としたセキュリティ対応



情報の受け渡しにおいてお互いに明確にすべき点

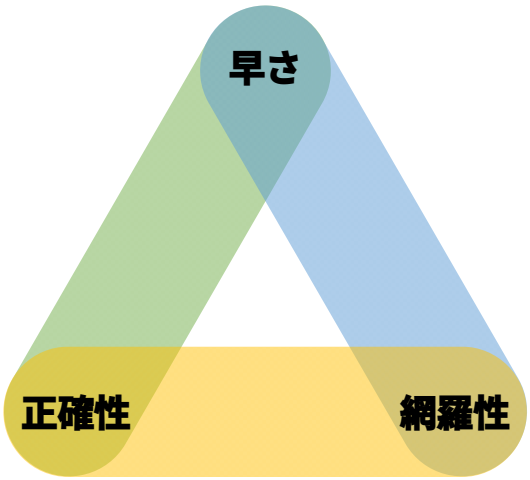
サイバーセキュリティ情報共有における 5W1H

	発信側	受信側
Why	何を目的に	何を目的に
When	どのようなタイミングで	どのようなタイミングで
What	何の情報を	何の情報を
Where	どの情報共有の場において	どの情報共有の場から得て
Who	誰が	誰が
How	どのように発信するのか	どのように活用するのか

参照：ISOG-J『**サイバーセキュリティ情報共有の「5W1H」**』P2

知っトク情報

情報共有のトライアングル（ジレンマ）



早さ、正確性、網羅性は
いずれか 2 つしか満たせない

- **早くて正確なものは網羅性に問題が出る**
  - 例 攻撃に関する情報として特定の IP アドレスが提示されたものの、他にも 関連していた IP アドレスが多数あったことがあとから判明する
- **早くて網羅的なものは正確性に問題が出る**
  - 例 攻撃に関連する情報として多数のドメインが提示されていたものの、無害 なドメインも含まれてしまっている
- **正確で網羅的なものは早さに問題が出る**
  - 例 攻撃に関連する情報として、IP アドレスもドメインも抜け漏れなく、正確 に整理されたものが提示されるのは、しばらく時間がたってからである

お互いによく理解して、
建設的なフィードバックをする関係を
構築していきましょう

参照：
・27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)
・ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P15

まとめ

ネットワーク中心の
セキュリティ監視における課題

1. **見えない**（通信の中身が）
2. **見てない**（監視対象NW以外で接続）
3. **見ようがない**（通信が出ない等）

エンドポイントの
セキュリティ対応における課題

1. **ない**（そこにあるはずの被害端末が）
2. **いない**（判断、対処できる人が）
3. **わからない**（今起こっている正しい状況が）

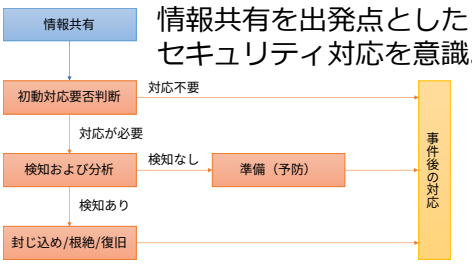
ネットワークとエンドポイントの両方を監視

SOC　運用 Operation　対応 Response　CSIRT

MSS+EDR

緊急対応サービス
（フォレンジック等）

三者の対応領域が重なり、より密接に関連。情報連携が今まで以上に重要に。



情報共有を出発点とした
セキュリティ対応を意識。

情報連携の際は、お互いに
目的や求めている情報を明確に。

	発信側	受信側
Why	何を目的に	何を目的に
When	どのようなタイミングで	どのようなタイミングで
What	何の情報を	何の情報を
Where	どの情報共有の場において	どの情報共有の場から得て
Who	誰が	誰が
How	どのように	どのように
	発信するのか	活用するのか

ISOG-J成果物に対するフィードバックのお願い

- ご意見ご要望お待ちしています！

- https://goo.gl/NK9A6L
  - 常時受け付けております
  - 匿名での投稿が可能です

(アイコン画像提供) http://www.security-design.jp/