セキュリティ対応組織力を上げるコツ
～成熟度の可視化と、情報共有の心得～

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
セキュリティ対応組織成熟度調査タスクフォース 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兼マネージャー / 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
    - セキュリティ対応組織成熟度調査タスクフォース 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兼マネージャー
  - 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

セキュリティ対応組織とは

SOC
(セキュリティオペレーションセンター)

＋

CSIRT

しかしながら、
CSIRTとSOCの役割は
その境界線が組織ごとに異なる

そもそも「役割」とは？
その理解が重要。

セキュリティ対応組織の教科書 v2.0

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。

A. セキュリティ対応組織運営
A-1. 全体方針管理
A-2. トリアージ基準管理
A-3. アクション方針管理
A-4. 品質管理
A-5. セキュリティ対応効果測定
A-6. リソース管理

B. リアルタイムアナリシス（即時分析）
B-1. リアルタイム基本分析
B-2. リアルタイム高度分析
B-3. トリアージ情報収集
B-4. リアルタイム分析報告
B-5. 分析結果問合受付

C. ディープアナリシス（深掘分析）
C-1. ネットワークフォレンジック
C-2. デジタルフォレンジック
C-3. 検体解析
C-4. 攻撃全容解析
C-5. 証拠保全

D. インシデント対応
D-1. インシデント受付
D-2. インシデント管理
D-3. インシデント分析
D-4. リモート対処
D-5. オンサイト対処
D-6. インシデント対応内部連携
D-7. インシデント対応外部連携
D-8. インシデント対応報告

E. セキュリティ対応状況の診断と評価
E-1. ネットワーク情報収集
E-2. アセット情報収集
E-3. 脆弱性管理・対応
E-4. 自動脆弱性診断
E-5. 手動脆弱性診断
E-6. 標的型攻撃耐性評価
E-7. サイバー攻撃対応力評価

F. 脅威情報の収集および分析と評価
F-1. 内部脅威情報の整理・分析
F-2. 外部脅威情報の収集・評価
F-3. 脅威情報報告
F-4. 脅威情報の活用

G. セキュリティ対応システム運用・開発
G-1. ネットワークセキュリティ製品基本運用
G-2. ネットワークセキュリティ製品高度運用
G-3. エンドポイントセキュリティ製品基本運用
G-4. エンドポイントセキュリティ製品高度運用
G-5. ディープアナリシス(深掘分析)ツール運用
G-6. 分析基盤基本運用
G-7. 分析基盤高度運用
G-8. 既設セキュリティ対応ツール検証
G-9. 新規セキュリティ対応ツール調査、開発
G-10. 業務基盤運用

H. 内部統制・内部不正対応支援
H-1. 内部統制監査データの収集と管理
H-2. 内部不正対応の調査・分析支援
H-3. 内部不正検知・防止支援

I. 外部組織との積極的連携
I-1. 社員のセキュリティ対する意識啓発
I-2. 社内研修・勉強会の実施や支援
I-3. 社内セキュリティアドバイザーとしての活動
I-4. セキュリティ人材の確保
I-5. セキュリティベンダーとの連携
I-6. セキュリティ関連団体との連携

セキュリティ対応組織力

＝

それぞれの機能と役割が実行できているか

自組織の力を
どう把握するか？

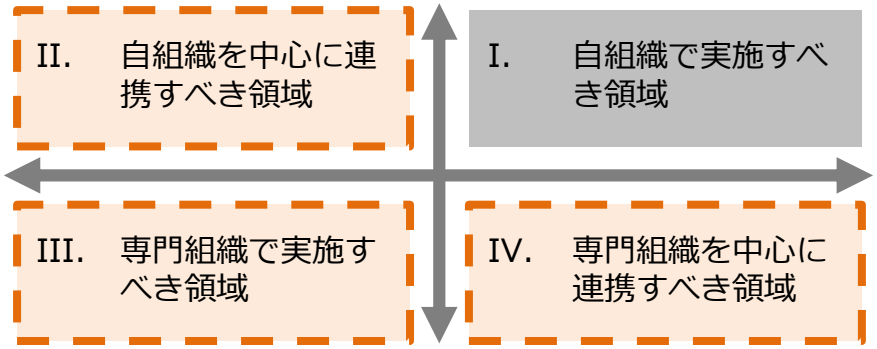
セキュリティ対応組織
成熟度セルフチェックシート

① 組織パターンの設定

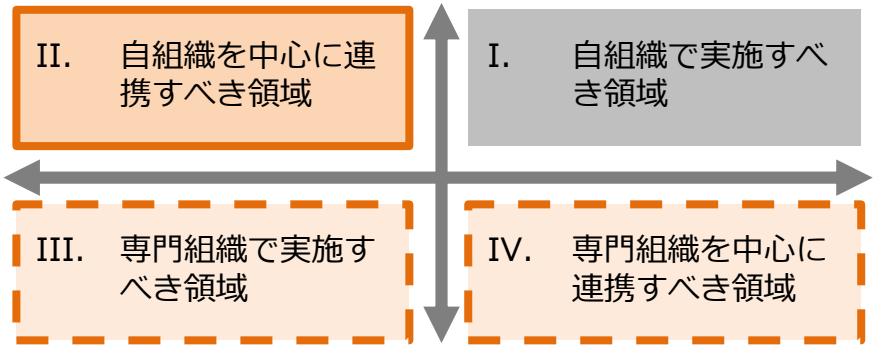
セキュリティ対応組織パターンを自覚する

セキュリティ対応組織パターンを自覚する

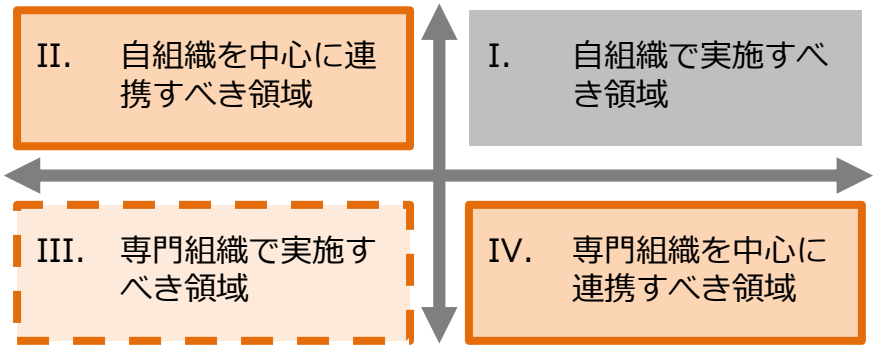
ミニマムインソース



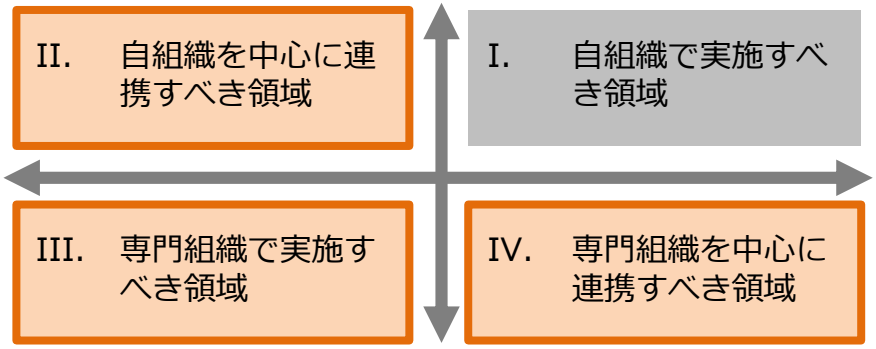
ハイブリッド



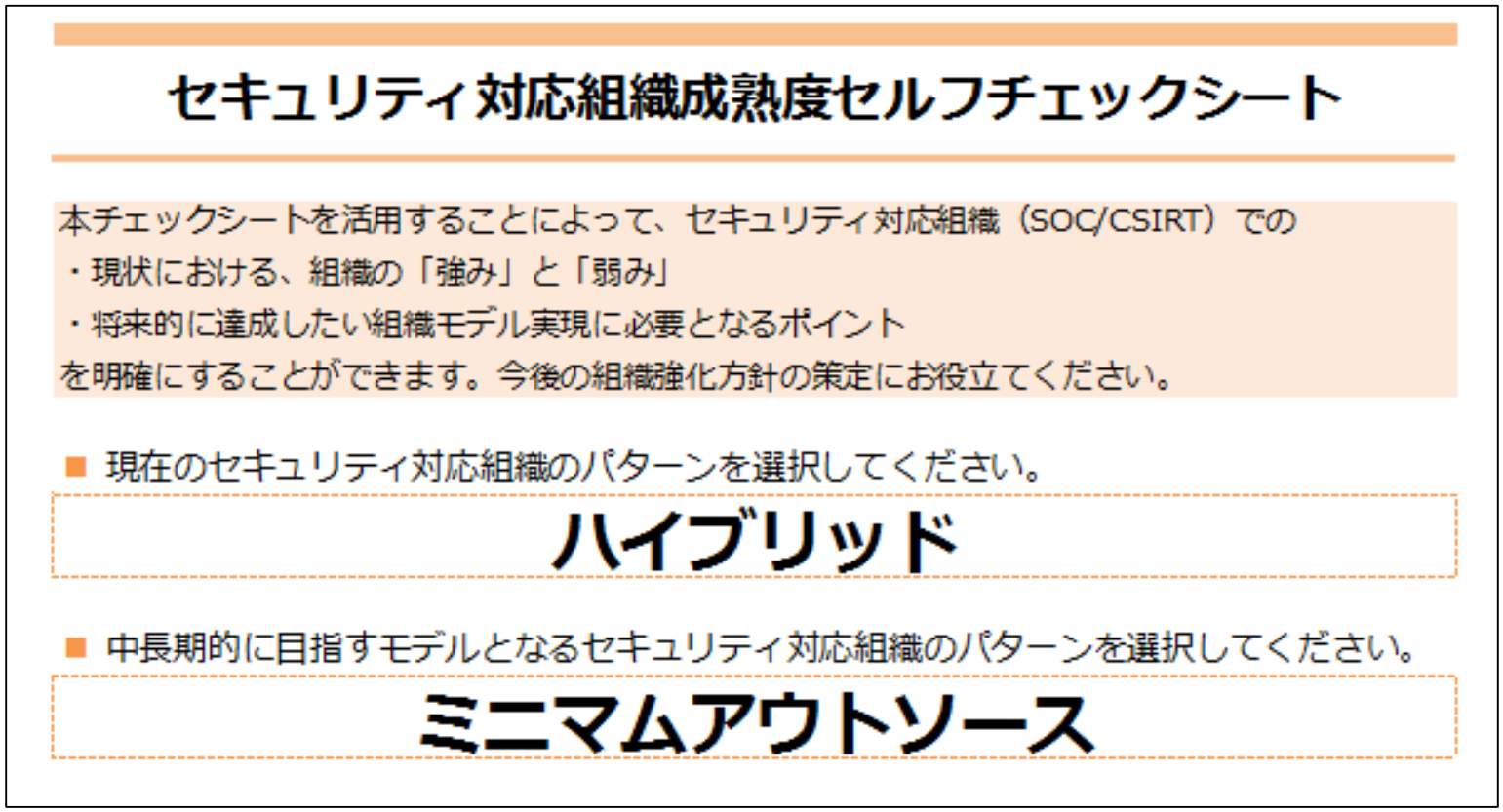
ミニマムアウトソース



フルインソース



アウトソース　インソース



現在と、将来的なモデルとするパターンを選択。

② 機能ごとに点数化

記入日：201X/YY/ZZ

			インソース						アウトソース						
			インソースでの実装を検討したものの、結果として実施しないと判断した	実施できていない	運用が明文化されておらず、担当者が業務を実施できる	運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	運用が明文化されており、担当者と交代して他者が業務を実施できる	明文化された運用はCISOなど権限ある組織長に承認されている	アウトソースでの実装を検討したものの、結果として実施しないと判断した	結果や報告を確認できていない	サービス内容と得られる結果を理解できていない	サービス内容は理解できているが、得られる結果は理解できない	サービス内容は理解できてないが、得られる結果は理解できている	サービス内容と得られる結果を理解できている	※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。
機能	役割	領域	0	1	2	3	4	5	0	1	2	3	4	5	備考
A. セキュリティ対応組織運営	A-1. 全体方針管理	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
	A-2. トリアージ基準管理	領域Ⅱ	○	◉	○	○	○	○	○	○	○	○	○	○	
	A-3. アクション方針管理	領域Ⅰ	○	○	◉	○	○	○	○	○	○	○	○	○	
	A-4. 品質管理	領域Ⅰ	○	○	○	○	○	○	○	◉	○	○	○	○	
	A-5. セキュリティ対応効果測定	領域Ⅱ	○	○	○	○	○	○	○	○	◉	○	○	○	
	A-6. リソース管理	領域Ⅰ	○	○	○	○	○	○	○	○	○	◉	○	○	
	B-1. リアルタイム基本分析	領域Ⅳ	◉	○	○	○	○	○	○	○	○	○	○	○	

インソースとアウトソース、それぞれの観点において、6段階で評価。

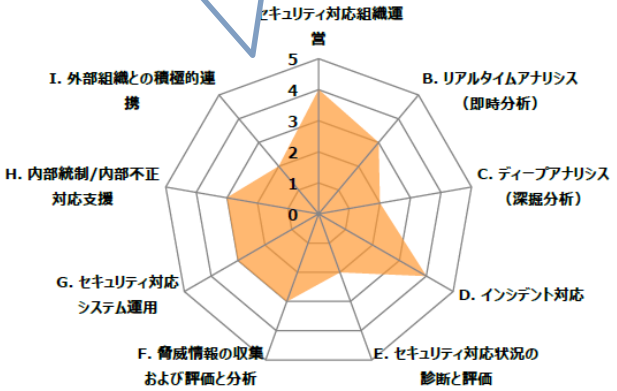
③ 結果を見てみる

機能別レーダーチャート

レーダーチャートの数値一覧

あなたのセキュ　応組織における"**機能別**"成熟度

201X/YY/ZZ



現状の組織（ハイブリッドパター　能別成熟度を5段階で評価しています。
組織の「強み」と「弱み」を抽出　セキュリティ対応において有効に働いている機能と、
改善が必要な機能を見える　ます。
マクロな観点での指標とし　熟度向上の方針策定にお役立てください。

機能	成熟度
A. セキュリティ対応組織運営	**4** /5
B. リアルタイムアナリシス（即時分析）	**3** /5
C. ディープアナリシス（深掘分析）	**2** /5
D. インシデント対応	**4** /5
E. セキュリティ対応状況の診断と評価	**2** /5
F. 脅威情報の収集および評価と分析	**3** /5
G. セキュリティ対応システム運用	**3** /5
H. 内部統制/内部不正対応支援	**3** /5
I. 外部組織との積極的連携	**2** /5

現状のセキュリティ対応組織の**強み**

A. セキュリティ対応組織運営
セキュリティ対応全体の方針や、各種のルール、基準が定まっており、安定的な運用が実現できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

D. インシデント対応
分析結果や脅威情報を元に、具体的な対応を行えており、システムやビジネスへの影響を低減できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

現状のセキュリティ対応組織の**弱み**

C. ディープアナリシス（深掘分析）
被害状況調査、攻撃手法分析など、深い分析が行い切れておらず、インシデントの全容解明と影響の特定が不十分になっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

E. セキュリティ対応状況の診断と評価
脆弱性診断やインシデント対応訓練などの実施と評価が不十分であり、セキュリティ対応のレベルアップが図りにくくなっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

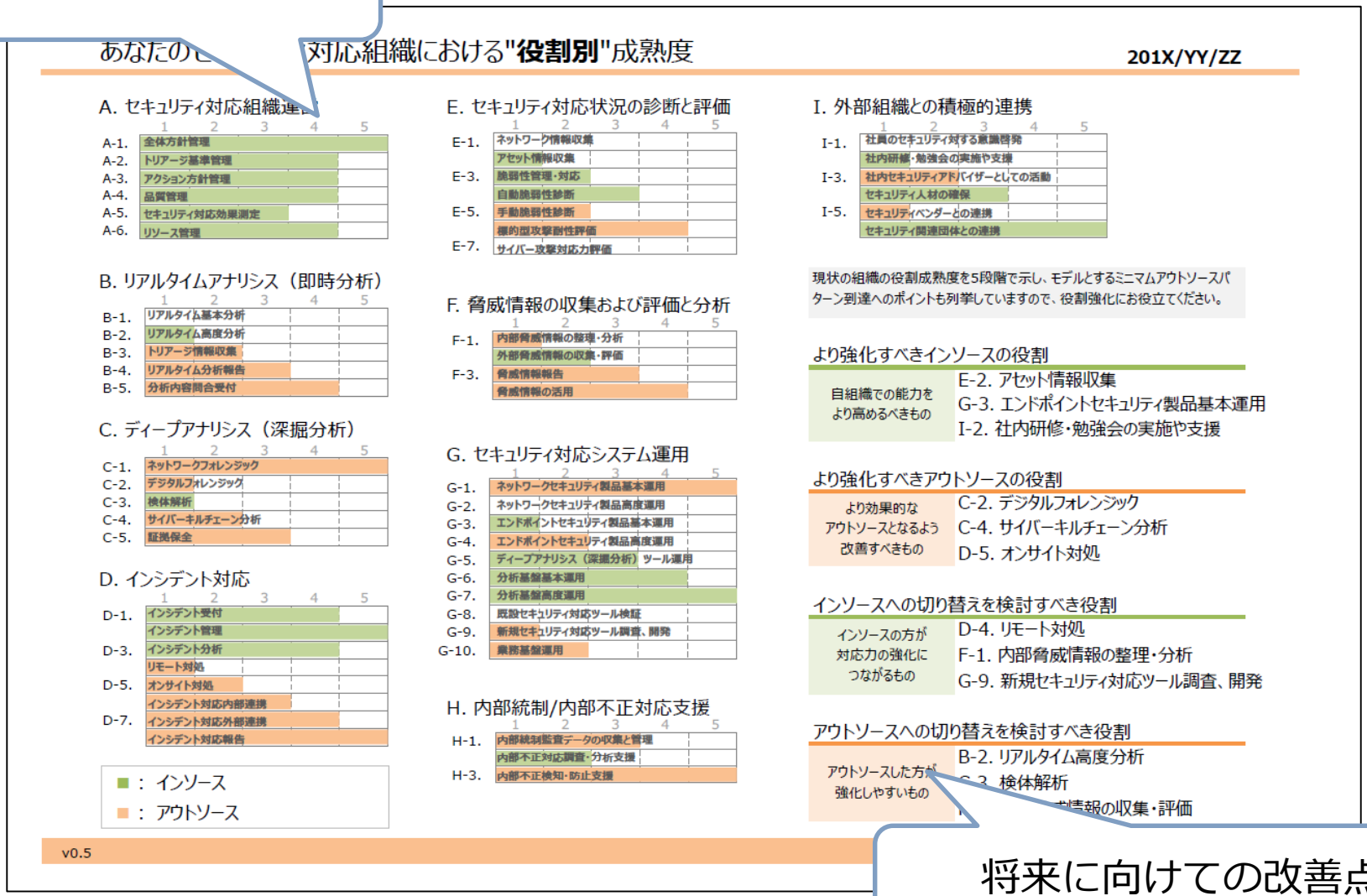
v0.5

© 2017 ISOG-J

現在の「強み」：成熟度高

現在の「弱み」：成熟度低

役割別成熟度グラフ



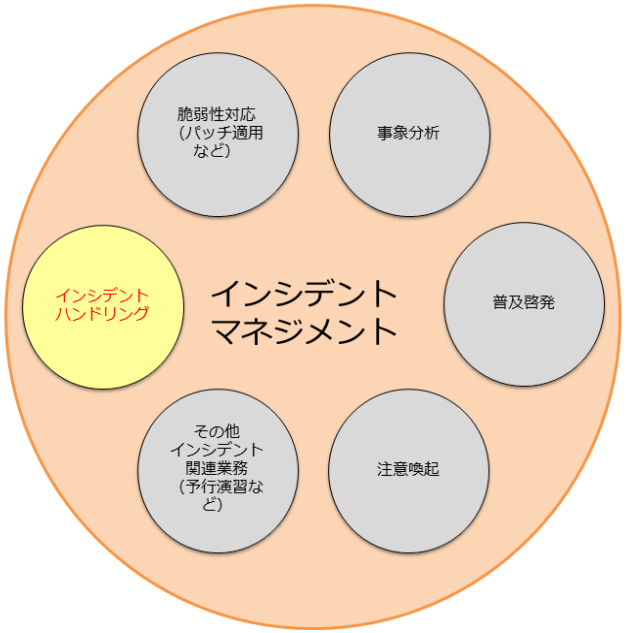
将来に向けての改善点

セキュリティ対応組織における、現状の把握と今後の方針策定にご活用ください。

さらに、
セキュリティ対応組織の教科書v2.0は
実践面での対応力の向上にも活用可能

平時の活動とその成果物を例示

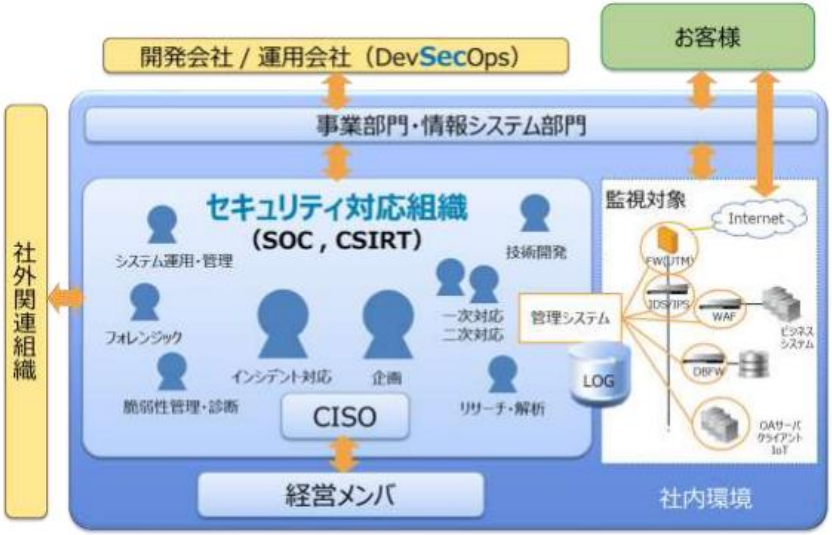
- 脆弱性対応（パッチ適用など）
- 事象分析
- 普及啓発
- 注意喚起
- その他インシデント関連業務（予行演習など）

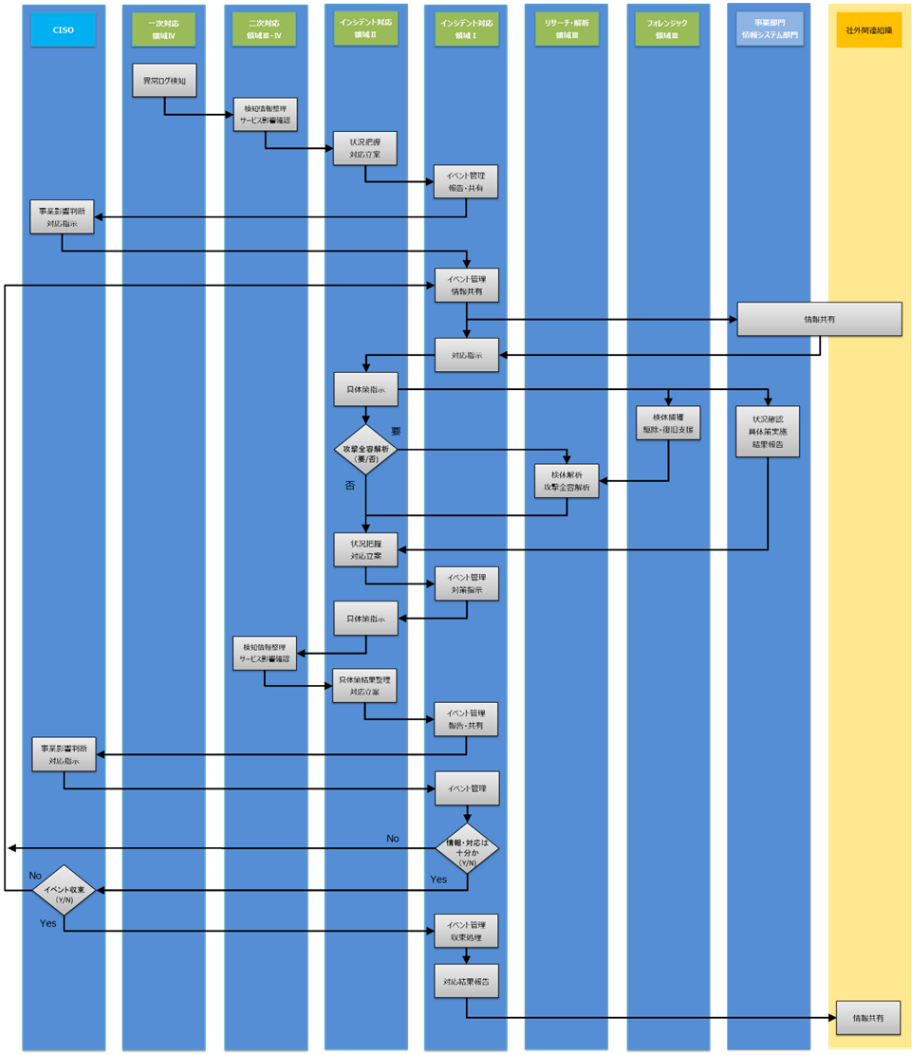


http://www.jpcert.or.jp/m/csirt_material/files/manual_ver1.0_20151126.pdf より

有事の際の対応フロー例

- ランサムウェアによる被害のケース
- ウェブサービスからの個人情報の窃取のケース



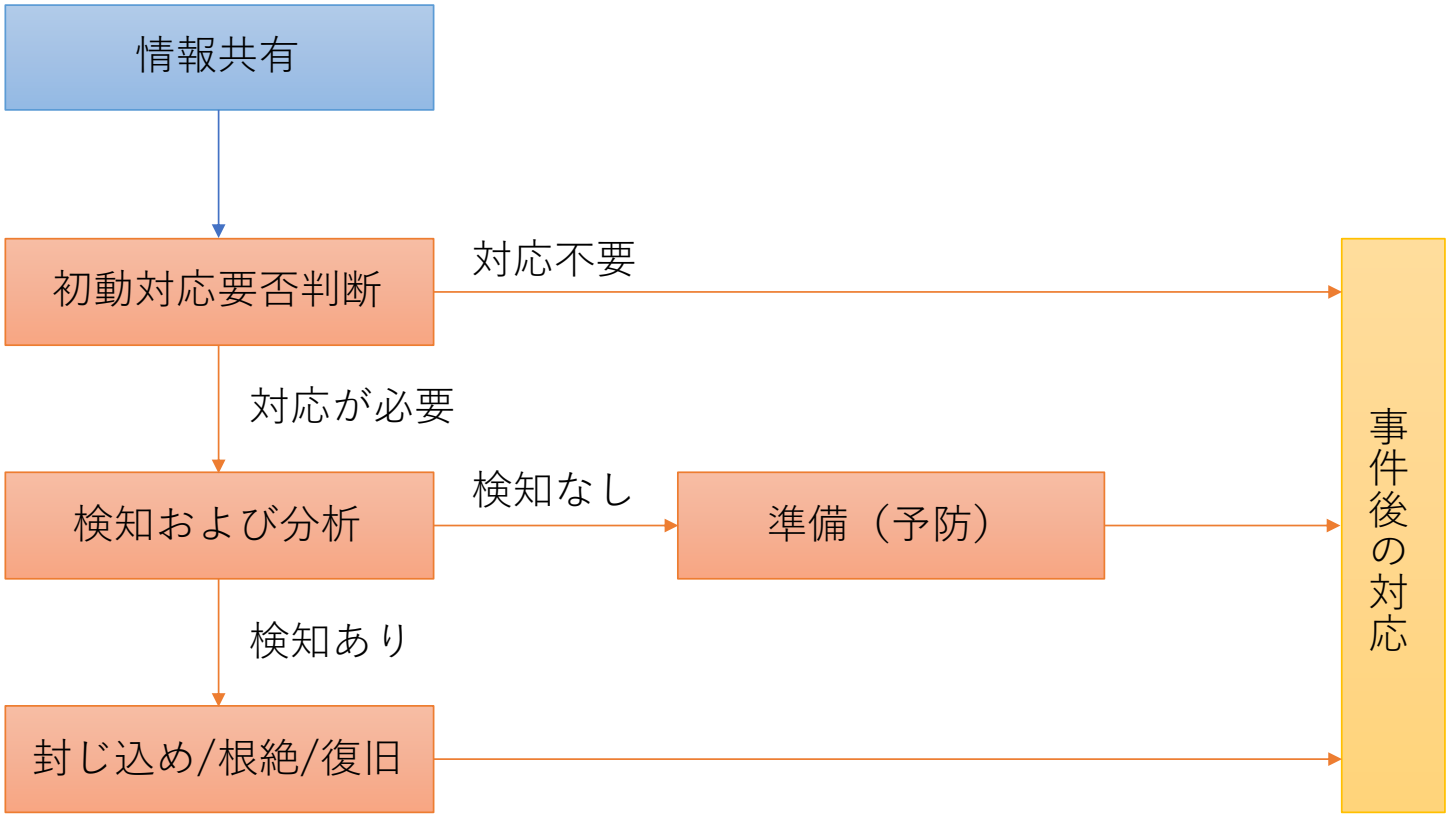


ところで、
Meltdown/Spectreの件、
現場、経営層は混乱しませんでしたか？

有事の対応として、こういった
発信された情報がトリガーとなって発動
されることも少なくない。

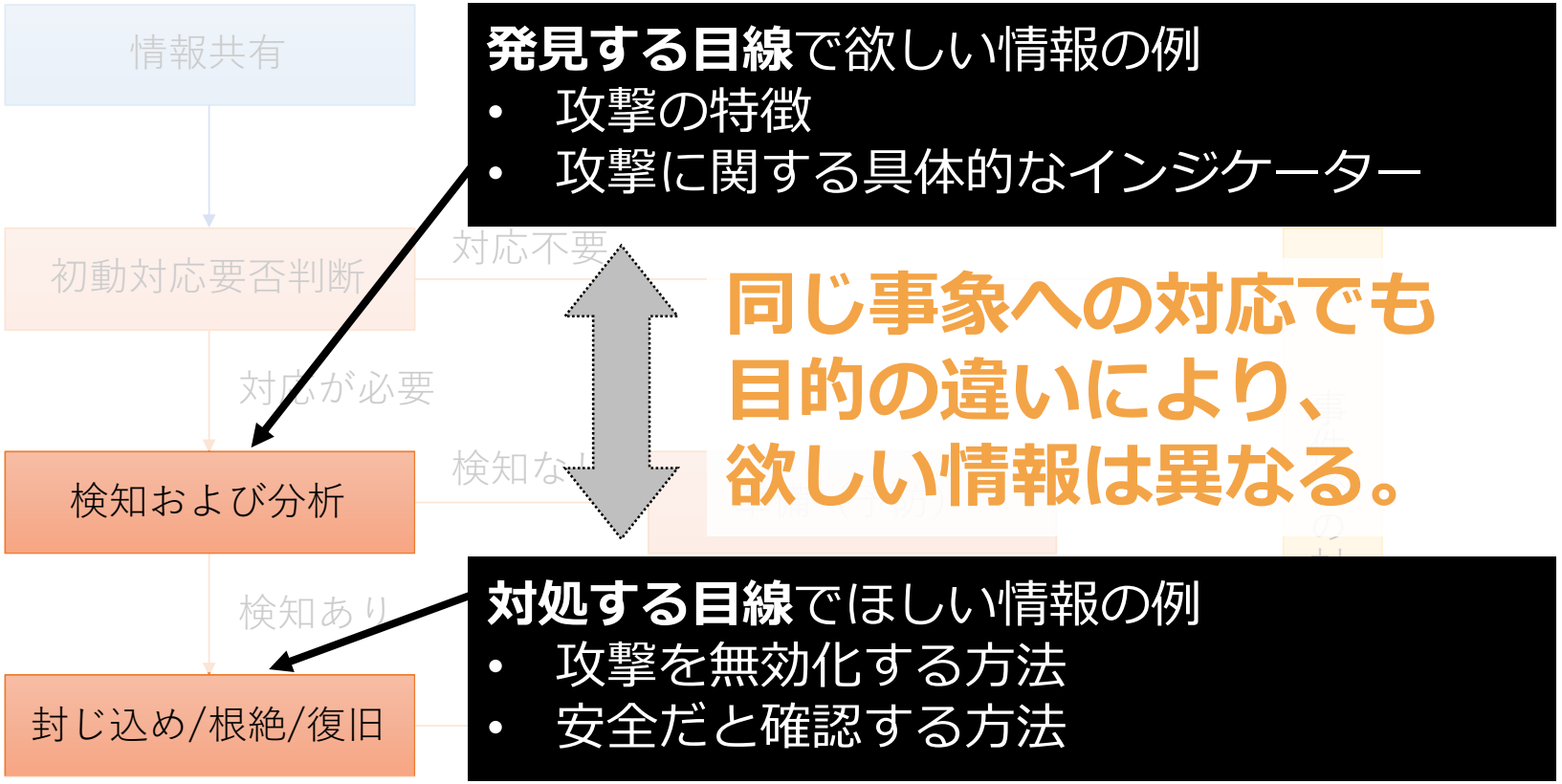
セキュリティ対応組織
(SOC,CSIRT)強化に向けた
サイバーセキュリティ情報共有の
「5W1H」

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



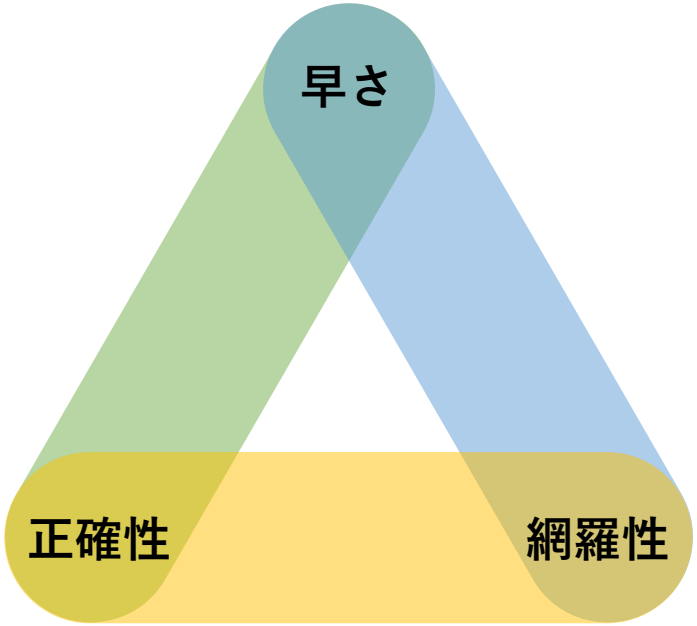
情報の受け渡しにおいてお互いに明確にすべき点

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	どのように
	発信するのか？	**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

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

建設的にフィードバックしながら、
情報の質を上げ、適切に対応していきましょう。

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

★セキュリティ対応組織が担うべき機能、役割を理解したい

- セキュリティ対応組織（SOC/CSIRT）の教科書 v2.0

★セキュリティ対応組織の実態を客観的に把握したい

- セキュリティ対応組織成熟度セルフチェックシート

★突然の情報でも焦らず対応できるよう心構えをしたい

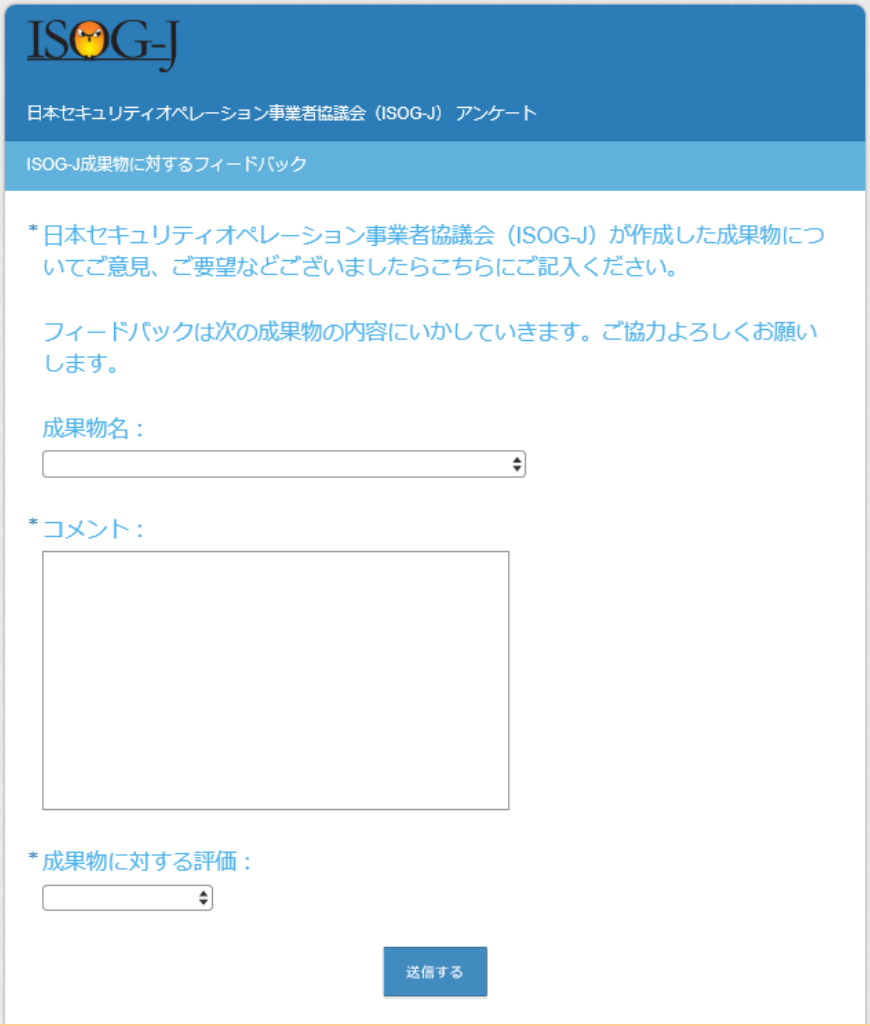
- セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」

ISOG-J公式サイトにて公開中
http://isog-j.org/activities/result.html

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/