45分で分かる！
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～

2018年6月1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)

45分で分かる！
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～

講演者１

- 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
  - セキュアシステム事業部　第三ビジネスユニット　勤務
  - ２０１７年３月までは社名が「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2018年5月11日現在、44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 v2.1
  - 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

  ※英語版もあります！！
  Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT

- 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。
- 2017年：「今求められるSOC,CSIRTの姿とは」
  - 今回はInternet Week2017の内容をもとに要点を整理しました。
- 過去の資料はInternetWeekの「過去のIW」から辿れます

その前に。

（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

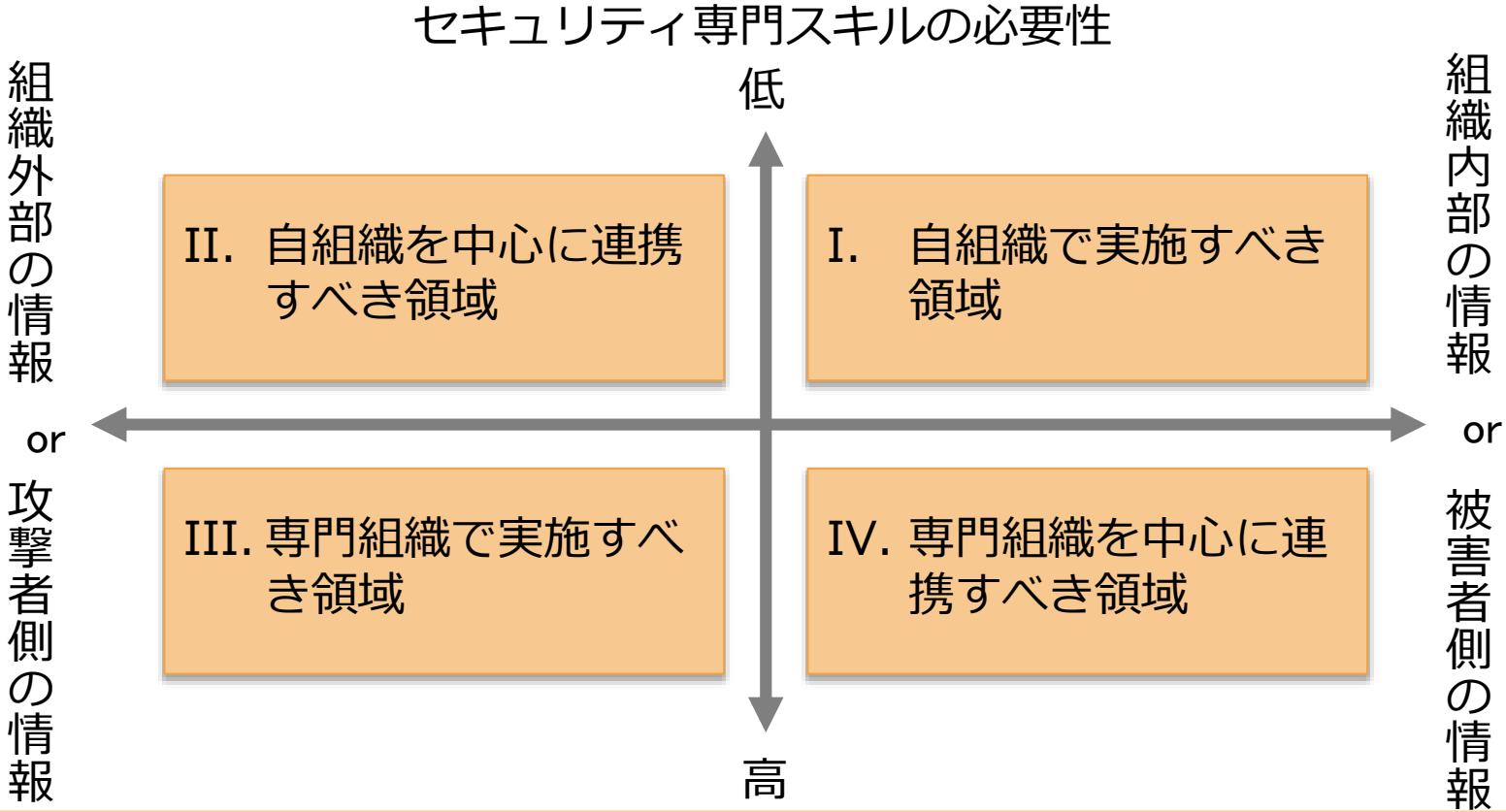
組織の持つ9つの機能、54の役割

9つの機能

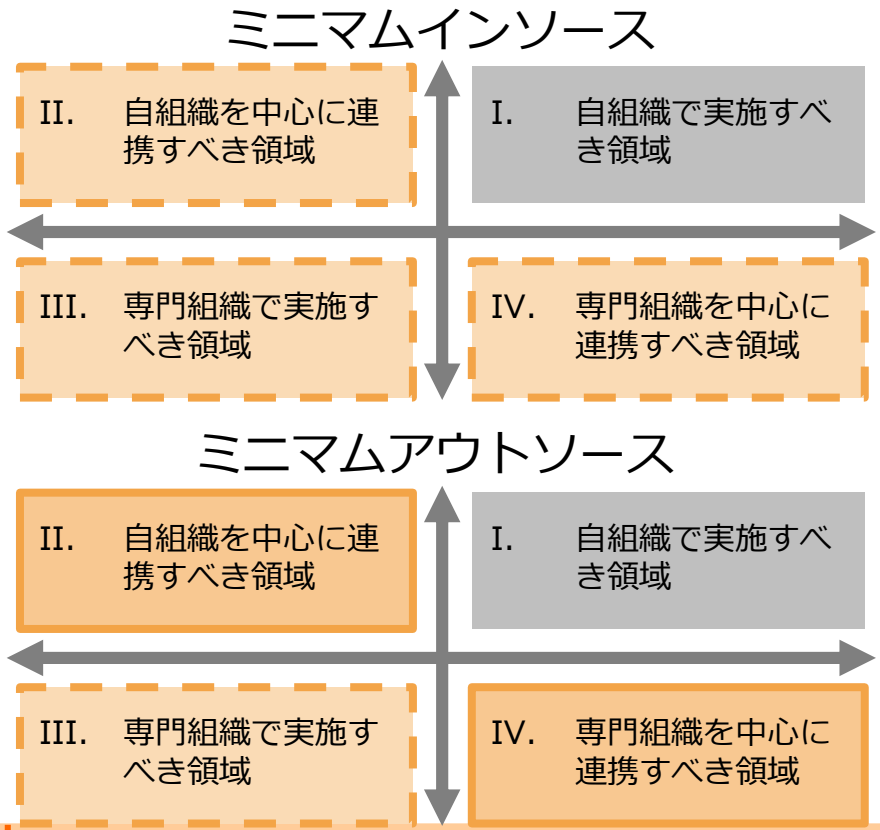
A. セキュリティ対応組織運営
B. リアルタイムアナリシス（即時分析）
C. ディープアナリシス（深堀分析）
D. インシデント対応
E. セキュリティ対応状況の診断と評価
F. 脅威情報の収集および分析と評価
G. セキュリティ対応システム運用・開発
H. 内部統制・内部不正対応支援
I. 外部組織との積極的連携

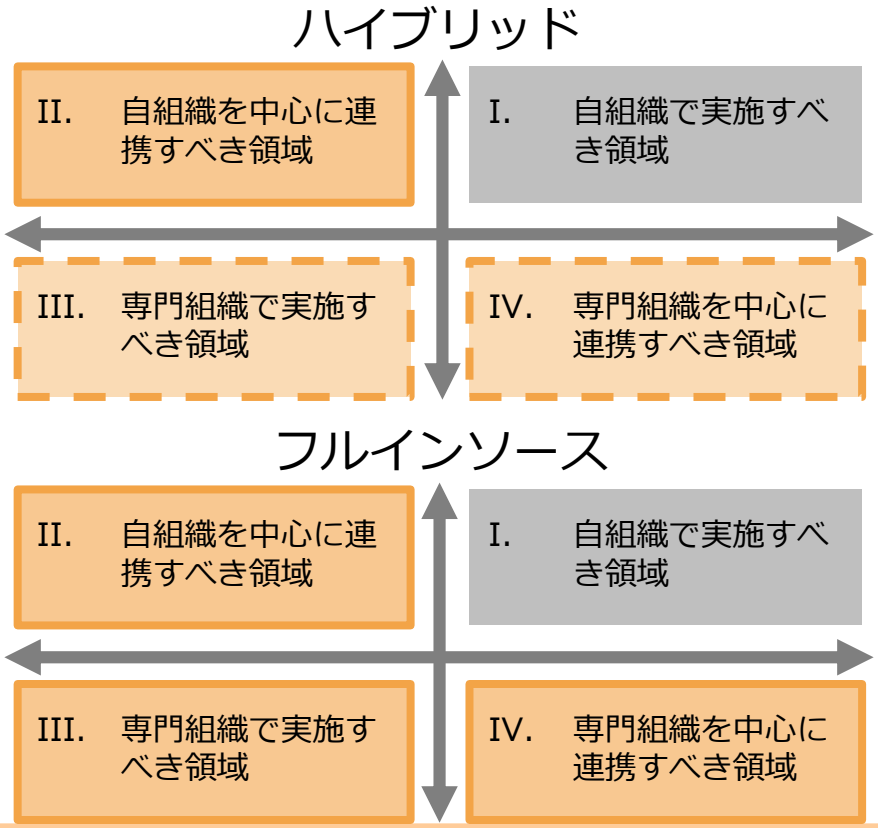
各項目にさらに複数の役割が存在
合計54の役割が存在する

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





それでは本題に

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案(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。

45分で分かる！
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～

セキュリティ対応組織(SOC,CSIRT)の成熟度について

講演者２

- 早川　敦史　です。
  - NECソリューションイノベータ株式会社
  - ISOG-J運営委員、ISOG-J運営サポートグループリーダー

２００２年～　統合ID管理、認証等基盤システム構築運用

２０１４年～　インシデント対応体制構築等コンサルティング

　　セキュリティインシデント対応教育／演習

２０１６年～　現在ＳＯＣ運用と自組織のサービスのインシデント対応等に従事。

セキュリティ対応組織での失敗あるある

セキュリティ対応組織、その後

©ブラックジャックによろしく 佐藤 秀峰（漫画 on web http://mangaonweb.com/）

セキュリティ対応組織、その後

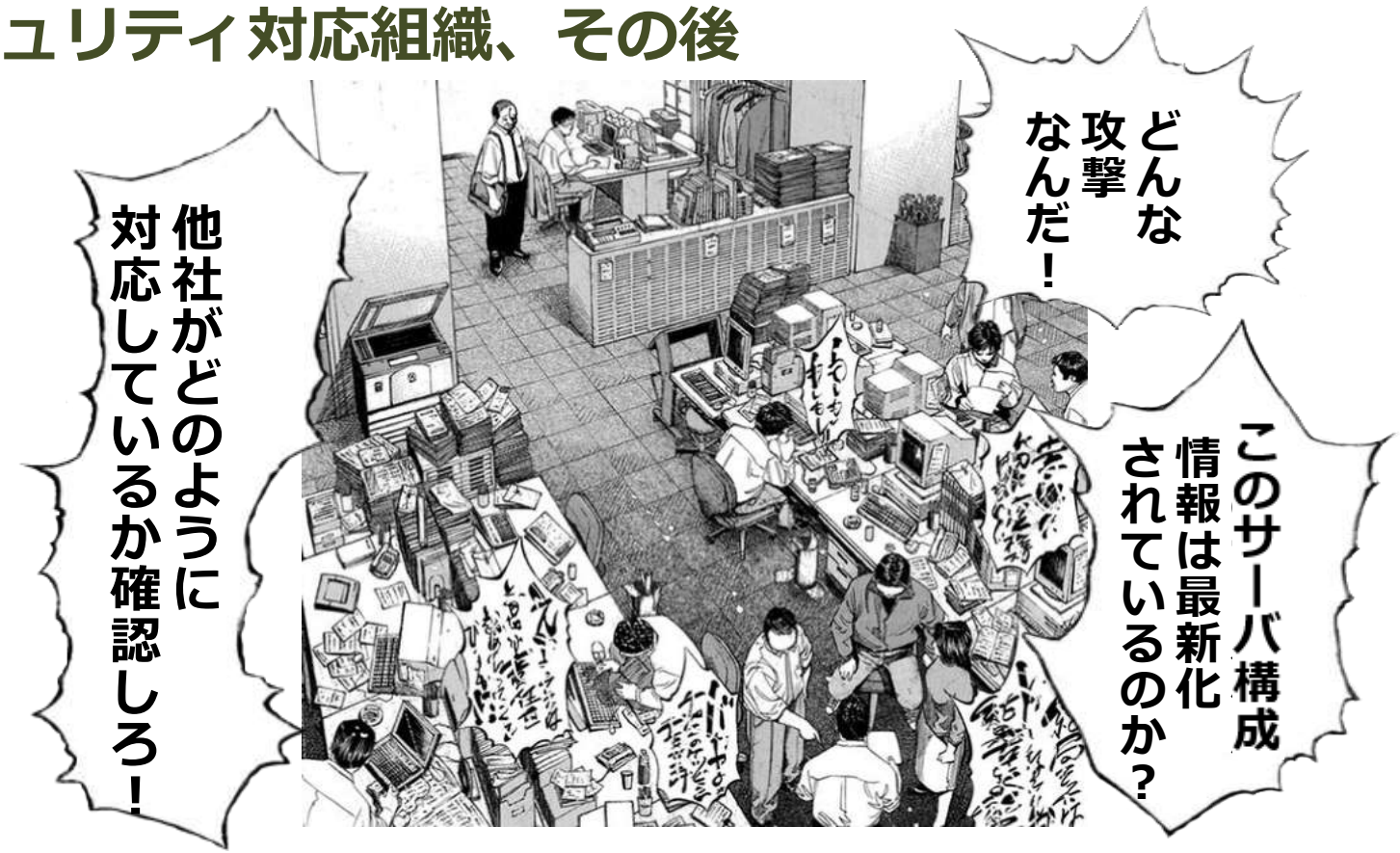
あれから1年
セキュリティ対応組織メンバーは
バーチャル組織として
奮闘していた。

日々イベントが発生し
いくつものインシデント対策が
課題にあがっていた・・・

©ブラックジャックによろしく 佐藤 秀峰（漫画 on web http://mangaonweb.com/）

セキュリティ対応組織、その後

セキュリティ対応組織、その後



©ブラックジャックによろしく 佐藤 秀峰（漫画 on web http://mangaonweb.com/）

セキュリティ対応組織、その後

©ブラックジャックによろしく 佐藤 秀峰（漫画 on web http://mangaonweb.com/）

セキュリティ対応組織（SOC/CSIRT）

- よく聞く組織となりましたが、運営は楽ではありません。
  - Struts、WordPress などWebアプリ基盤の脆弱性
  - WannaCry、Petya などの暗号型ランサムウェア
  - KRACKs WPA/WPA2の仕様に関する脆弱性
  - WordPress、Drupal などCMSの脆弱性
- 皆さんどのように対応をされたでしょうか？
- 普段はどのような活動をされているでしょうか？

組織の持つ9つの機能（54の役割）

平時の役割

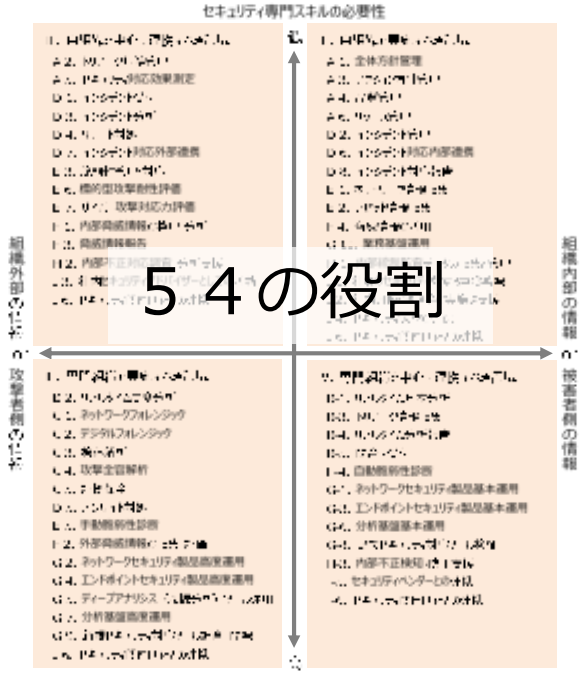
A. セキュリティ対応組織運営
B. リアルタイムアナリシス（即時分析）
C. ディープアナリシス（深堀分析）
D. インシデント対応
E. セキュリティ対応状況の診断と評価
F. 脅威情報の収集および分析と評価
G. セキュリティ対応システム運用・開発
H. 内部統制・内部不正対応支援
I. 外部組織との積極的連携

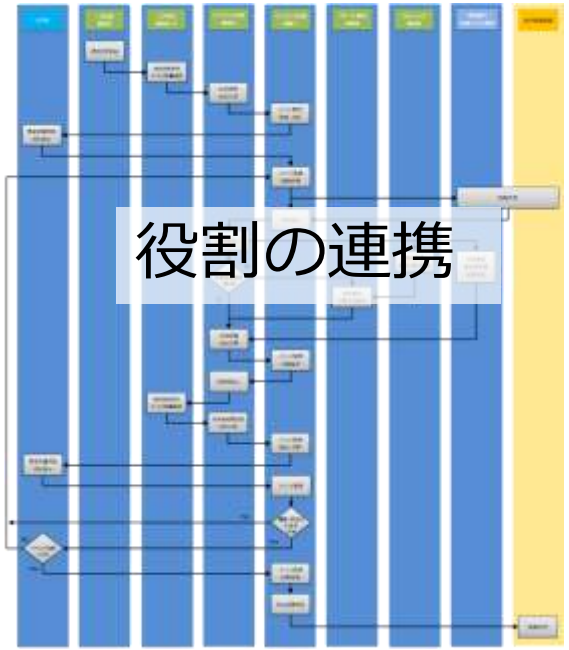
インシデント時の役割

有事(インシデント)時 / 平時はどのような役割があるのか？

インシデント(有事)の対応例

役割ごとのインシデント対応例をフローで紹介

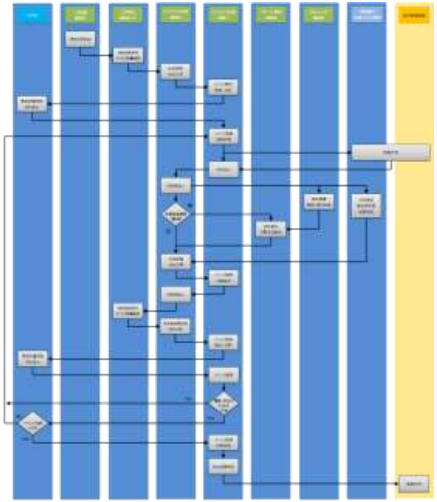




有事の流れの紹介

- インシデント事例の振り返り　WannaCry

- インシデント対応の流れ
  - 通常時の監視情報を基に異常の有無を確認
  - 状況の整理、対策立案、対策指示
  - 対策実施、結果報告
  - 異常発見時の専門的な対応
  - 収集した情報を基に異常の有無を再確認
  - インシデント対応の収束/継続判断



インシデント事例：WannaCry

ITPro IPA緊急記者会見 5/14

出所：Itpro 5/14 http://itpro.nikkeibp.co.jp/atcl/news/17/051401395/

不審なメール
開かないで

日本経済新聞 5/15

サイバー攻撃、150カ国で20万件以上被害　欧州警察機関

共同通信 5/15

日本政府が首相官邸危機管理センターに情報連絡室を設置

NHK NEWS Web 5/16

米高官 サイバー攻撃の被害は約150か国で30万件以上

など報道多数

©ブラックジャックによろしく 佐藤 秀峰（漫画 on web http://mangaonweb.com/）

インシデント事例：WannaCry

- 445/tcpがOpen、SMB v1が有効、MS17-010未適応なWindowsOS
- ネットワーク経由で感染拡大、ファイルを暗号化

- 300ドル相当のビットコインの支払いを要求する。
- KillSwitchが存在した。

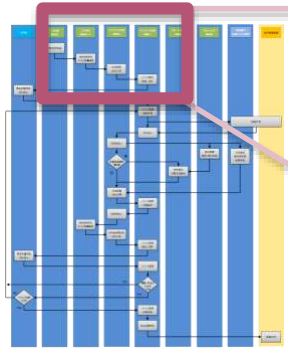
出所：大規模ランサムウェア感染について
http://www.nttdata.com/jp/ja/news/information/2017/pdf/NTTDATA_wannacry_report.pdf

こんなしくじりありませんでしたか？

©ブラックジャックによろしく 佐藤 秀峰（漫画 on web http://mangaonweb.com/）

有事の対応例　WannaCryだったら

- 通常時の監視情報を基に異常の有無を確認



【一・二次対応(監視)チーム】

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.問い合わせ窓口

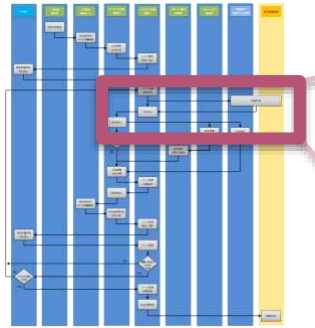
ファイル改ざん(暗号化)ログ確認

不正アクセス(AV・EDR)ログ確認

アノーマリ確認

有事の対応例　WannaCryだったら

- 状況の整理、対策立案、対策指示



【インシデント対応チーム】

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-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

自組織監視状況把握

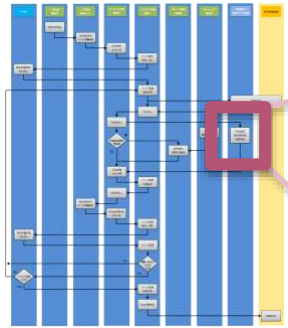
情報交換
　攻撃通信(SMBv1,CVE)、暗号化

自組織システムの評価
(パッチ、オープンポート、バックアップ)

対策指示・管理
(MS17-010適用・ポートクローズ、隔離)

有事の対応例　WannaCryだったら

- 対策実施、結果報告



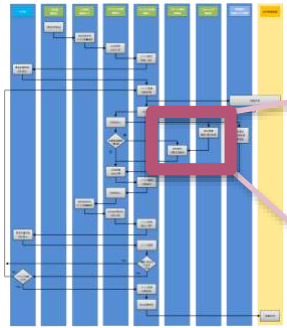
【情シス・ビジネス部門】

対策実施
　SMBv1無効化
　Port遮断
　パッチ確認・適用
　感染状況確認
　バックアップの確認

対策/影響有無報告

有事の対応例　WannaCryだったら

- 異常発見時の専門的な対応



【リサーチ・フォレンジック】

C1.ネットワークフォレンジック
C2.デジタルフォレンジック
C3.検体解析
C4.攻撃全容解析
F2.脅威情報の収集評価

検体/亜種 捕獲

検体/亜種 挙動解析
(KillSwitch、DoublePulsar、Hash値)

対策分析

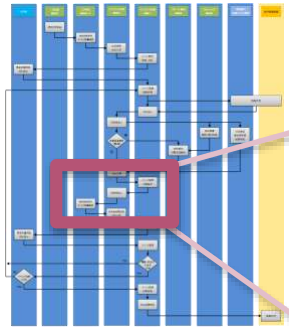
感染端末対応

The Equation Group
vs
The Shadow Brokers

EternalBlue（Windows SMBのエクスプロイト）
DoublePulsar（エグゼキューションツール）

有事の対応例　WannaCryだったら

- 収集した情報を基に異常の有無を再確認



【インシデント対応チーム】

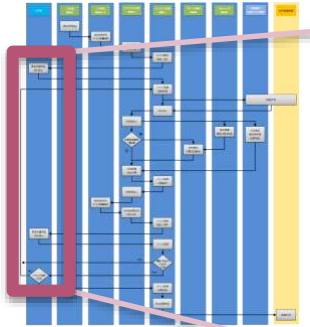
B-4.リアルタイム分析報告(依頼)
D-2.インシデント管理
D-3.インシデント分析
D-8.インシデント対応報告

脅威情報によるチェック
　攻撃通信
　（SMBv1、KillSwitch）
　Malware確認
　（DoublePulsar、Hash値）
　暗号化ファイルの有無
　BackDoor通信

事業への影響とりまとめ

有事の対応例　WannaCryだったら

- インシデント対応の収束/継続判断



【CISO】

事業継続判断
(WannaCry,DublePulsarによる影響)

外部情報公開判断

収束判断・宣言

なんちゃって組織のしくじり

- ウチは95%できているんだよね。

©ブラックジャックによろしく 佐藤 秀峰（漫画 on web http://mangaonweb.com/）

有事の対応例

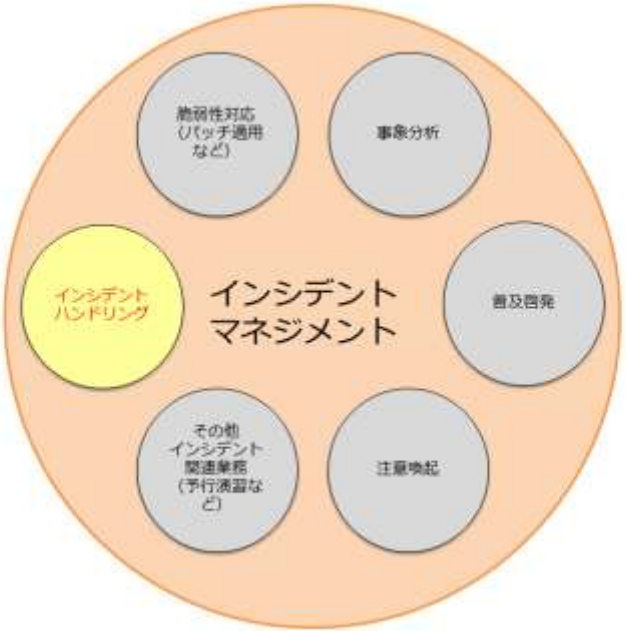
- まとめ
  - 大まかな流れと役割(組織)間の連携を確認しました
  - WannaCryを例に、簡略化してスムーズに話をまとめました
  - Strutsなど他のインシデント対応でも同様の流れとなります

- 気付き
  - 平時の取り組みがスムーズな対応に影響しています

平時の活動を見ていく

平時がアピールできていなかった組織のしくじり

平時の活動例



- 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

平時の活動例

- 脆弱性対応（パッチ適用など）
  - 自社の管理するシステムの状況を把握する

- 効果

例として、以下の効果などが挙げられる
- 最新のシステム構成状況（SMBを使った運用をおこなっているか）
- 最新のシステムパッチ適用状況（MS17-010は何時適用されるか）
- 上記活動の取りまとめによるセキュリティ対応組織の活動報告 Microsoft

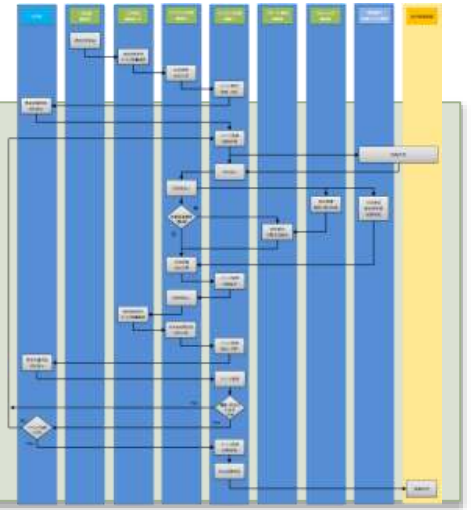
とは言いますが……

平時の活動例

- インシデント関連業務（予行演習など）
  - インシデントが起きたと仮定し、対処手順の確認や、経営層も含めた判断ポイントの確認を実施する

- 効果

例として、以下の効果などが挙げられる
- 自組織に足りない運用が見つかる
- 有事の際の行動が明確になる
- 行動がスムーズになる
- 他の平時の活動の意味を理解できる



とは言いますが……

平時の活動例

- 事象分析
  - インシデント情報の収集により、分析力を向上させ、自社への脅威を把握する

- 効果

例として、以下の効果などが挙げられる

- 情報収集過程でコミュニティ仲間を増やせる（信頼性の高い情報）
- 過去の類似の事象から対策や対応のヒントを得る（Nimda,Slammer）
- 社会的に起きている攻撃の手法や傾向を知る（NSAからの情報漏えい?）
- 自社への攻撃傾向を把握する（自組織の通常状態の把握）

とは言いますが……

平時の活動例

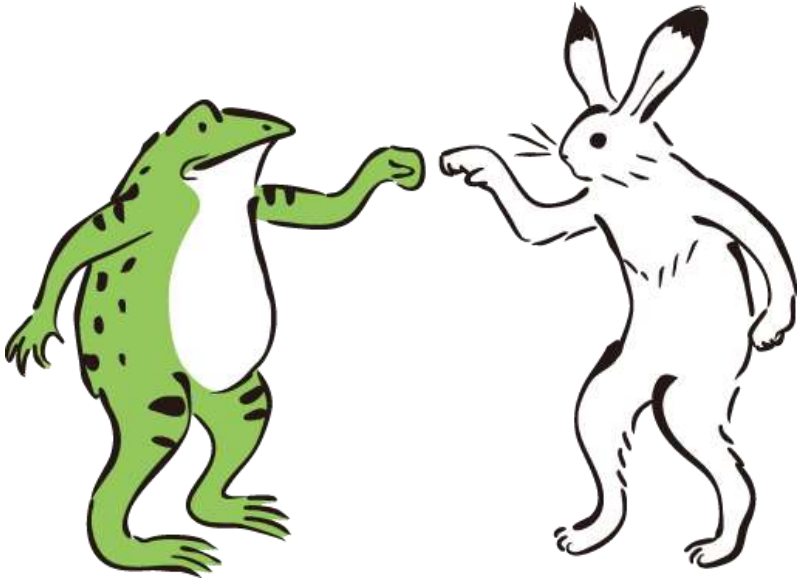
- 普及啓発、注意喚起
  - 平時から事業部門とコミュニケーションを取り、リテラシーの向上を行う

- 効果

例として、以下の効果などが挙げられる

- 脆弱性情報の共有（CVE2017-0145の共有　CVSS v3 Base Score:8.1 High ）
- セキュリティ対応組織が社内の皆から仲間だと思ってもらうこと
  - 脆弱なシステムの把握の促進、改善
  - インシデントを隠ぺいする体質の改善や早期イベント報告
- 脆弱性対応・事象分析活動と併せセキュリティ対応組織のPR

とは言いますが……



平時の対応例

- まとめ
  - 平時の活動が有事のスムーズな対応に影響している
  - 平時の活動を通じて社内から必要とされる仲間になること
  - 平時の活動をまとめセキュリティ対応組織活動をアピール

One More Thing…

今どこまでできているの？
これからどうすればいいの？

成熟度、始めました！！
“ISOMM”（ ISOG-J SOC/CSIRT Maturity Model）

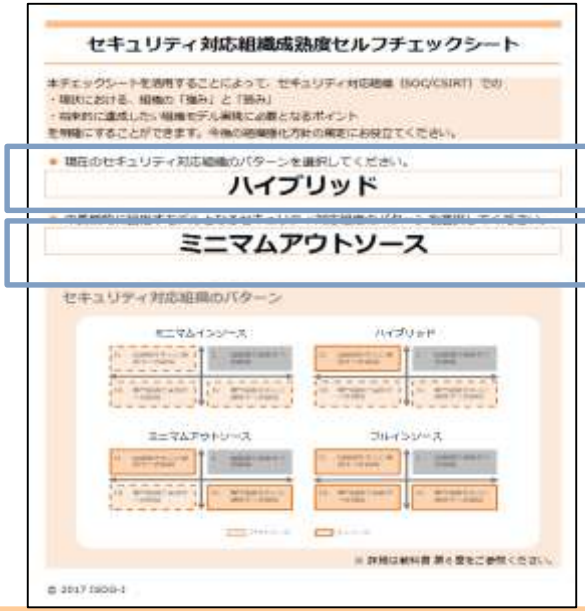
- 今どこまでできているのか、これから目指す姿とのギャップは何か、見える化するための成熟度チェックリストを作りました。

- 議論するなかで、日本にあったものにしようと新しく作りました！

- ISOG-Jのホームページからダウンロードできます
  - http://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

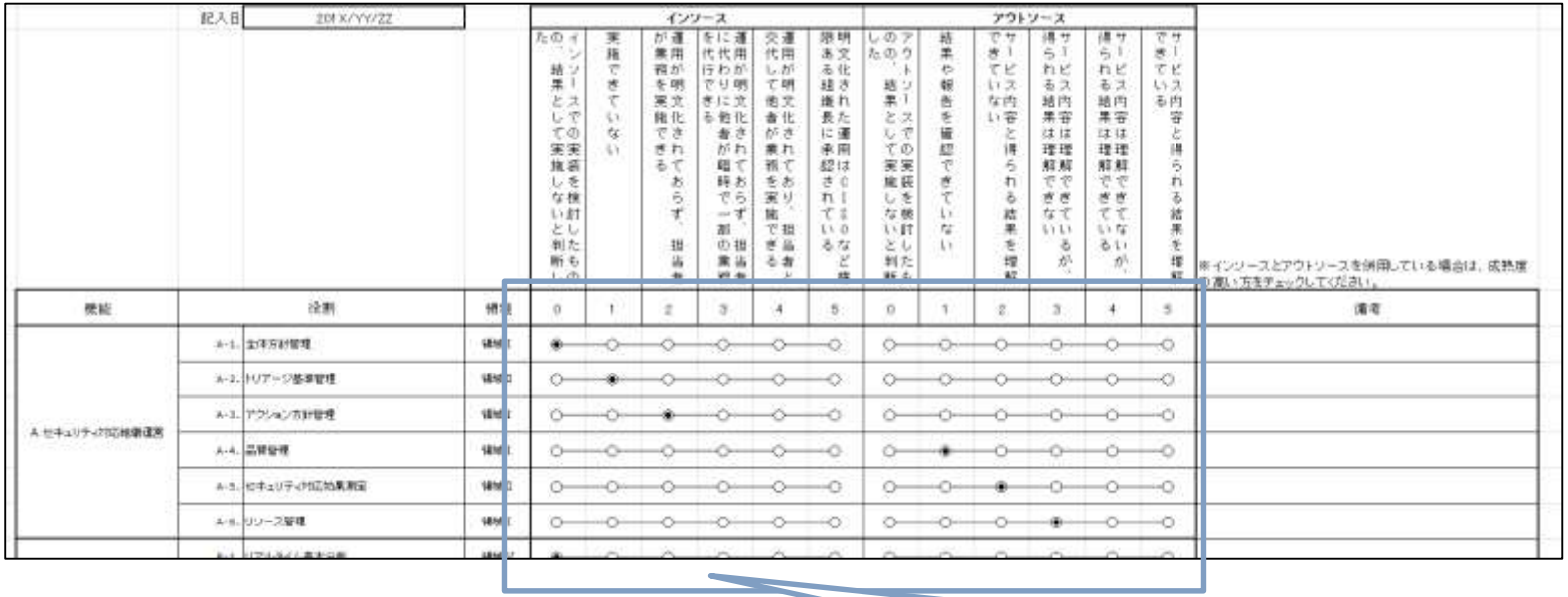
成熟度セルフチェックシートの使い方

- Excelファイルでできています。



1. 現在の組織のパターンを選択

2. 将来のモデルとなるパターンを選択



記入日 20XX/YY/ZZ

			インソース						アウトソース						
			インソースでの実施を検討したものの、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、担当者に代わりに他者が暗黙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	運用はCISOなど責任ある経営層に承認されている	明文化された	アウトソースでの実施を検討したものの、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いるが、得られる結果は理解できていない	サービス内容と得られる結果を理解できている	
機能	注釈	補足	0	1	2	3	4	5	0	1	2	3	4	5	備考
A.セキュリティ対応機能運用	A-1. 全体方針管理	補足1	●	○	○	○	○	○	○	○	○	○	○	○	
	A-2. トリアージ基準管理	補足2	○	●	○	○	○	○	○	○	○	○	○	○	
	A-3. アクション方針管理	補足3	○	○	●	○	○	○	○	○	○	○	○	○	
	A-4. 品質管理	補足4	○	○	○	○	○	○	○	●	○	○	○	○	
	A-5. セキュリティ対応効果測定	補足5	○	○	○	○	○	○	○	○	●	○	○	○	
	A-6. リソース管理	補足6	○	○	○	○	○	○	○	○	○	●	○	○	
			●	○	○	○	○	○							

※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。

3. 入力シートで現在の状況を選択

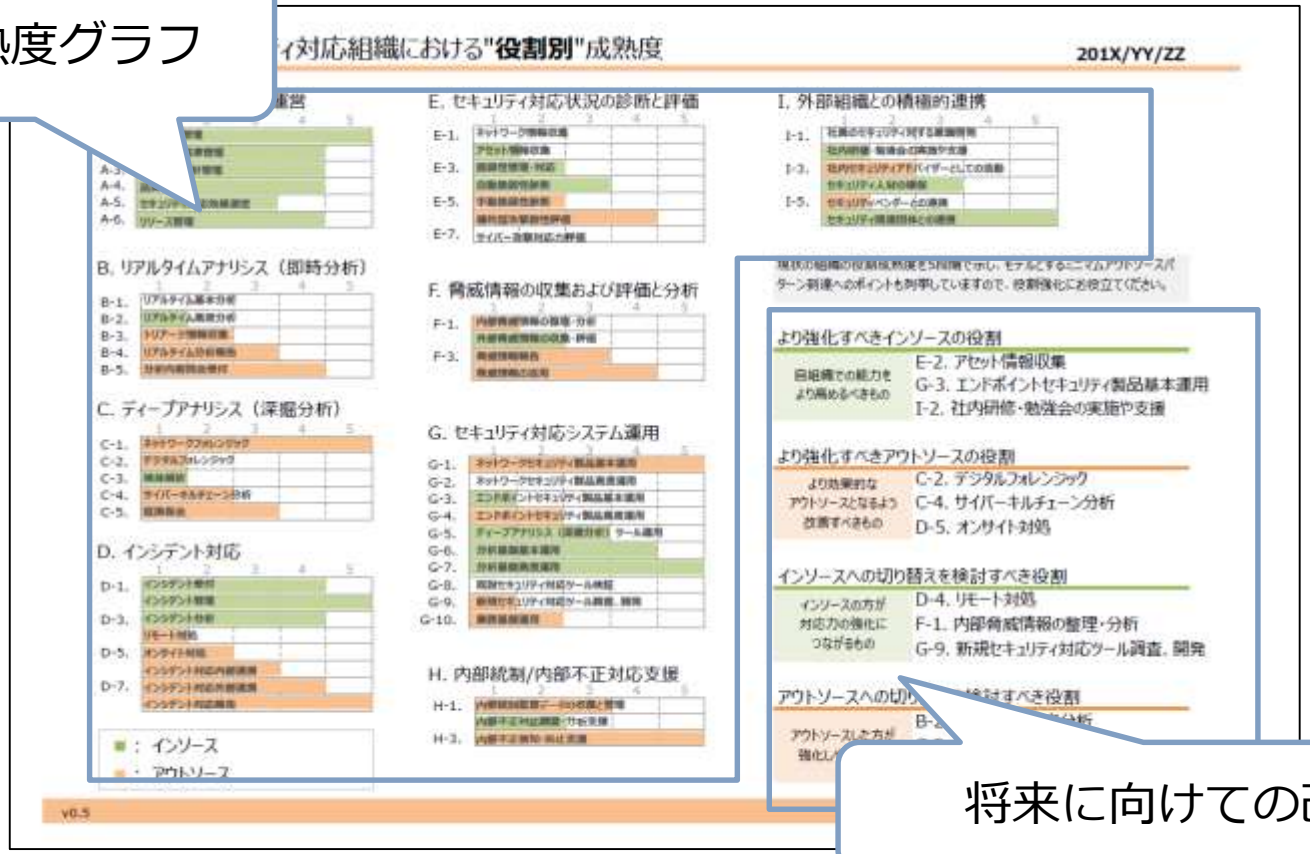
機能別レーダーチャート

レーダーチャートの数値一覧

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

まとめ

今回はインシデント対応における実際に起こったしくじりや課題を見ていただきました。

- インシデントも含めたセキュリティ対応は平時“も”大事。
- セキュリティ対応は一人ではできないので組織内に協力者を作り、良い関係性を平時より築くことが大切。
- その関係性の中で役割分担を行いつつ、お互いの足りない部分を補う形で協力し合えるとよい。

45分で分かる！
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～

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」

このセッションは？

- ISOG-Jが2017年10月に公開したドキュメント、**「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」」**をベースにディスカッションします。
- **最近流行りの「情報共有基盤」を作ろうとか、共有のフォーマットを提案するものではありません。**

資料URL（21ページ、98KB）

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

なぜ今、情報共有が課題なのか

（ちょっと前）CSIRT設立がブーム

どうやったら情報収集できるかが課題

1人では専門家のようにできないことがわかる

……そうだ！みんなで共有すれば！！←イマココ

脅威情報を共有してもらおう！

複数の団体やコミュニティに所属して、
情報を集めようとしました

…… 解決しました？？

例えば、Struts2やTomcat

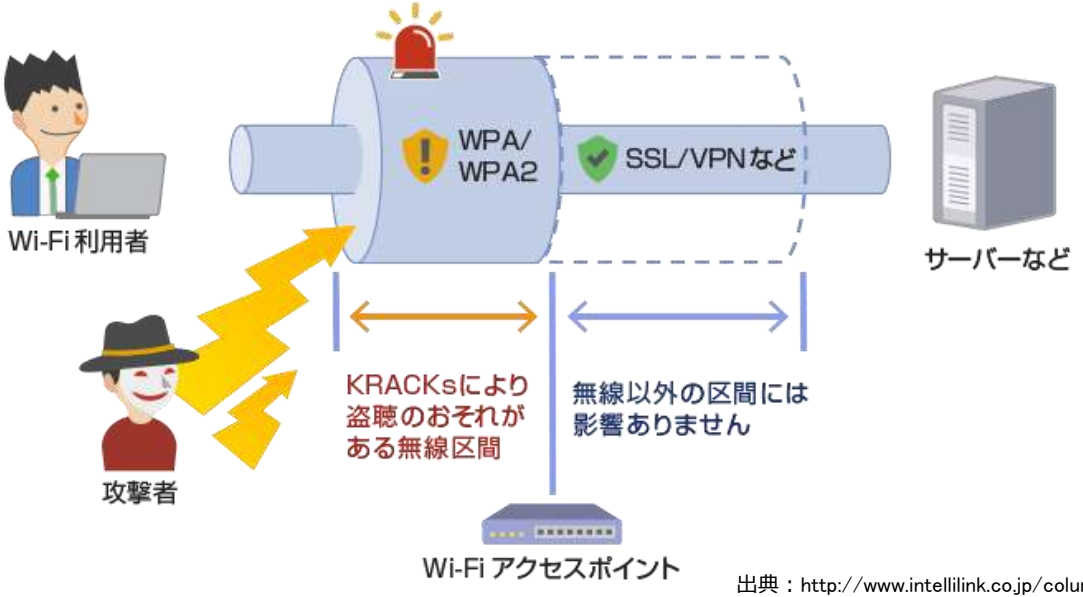
- 最初は慌てましたが、もう慣れましたか？
- 脆弱性は開発者のやりとりの時点で公開され、パッチが出た瞬間には攻撃が始まることもあります
- みなさん、この流れに慣れて開発者のやりとりは見ていたりしますか？

- 「慣れ」だけではやっぱり慌てません？

そんなところでKRACKsが！

- **K**ey **R**einstallation **A**tta**CK**s (KRACKs)
- 無線LANのWi-Fiでの暗号化をする規格、WPA2の脆弱性

出典：https://www.krackattacks.com/#wpa3

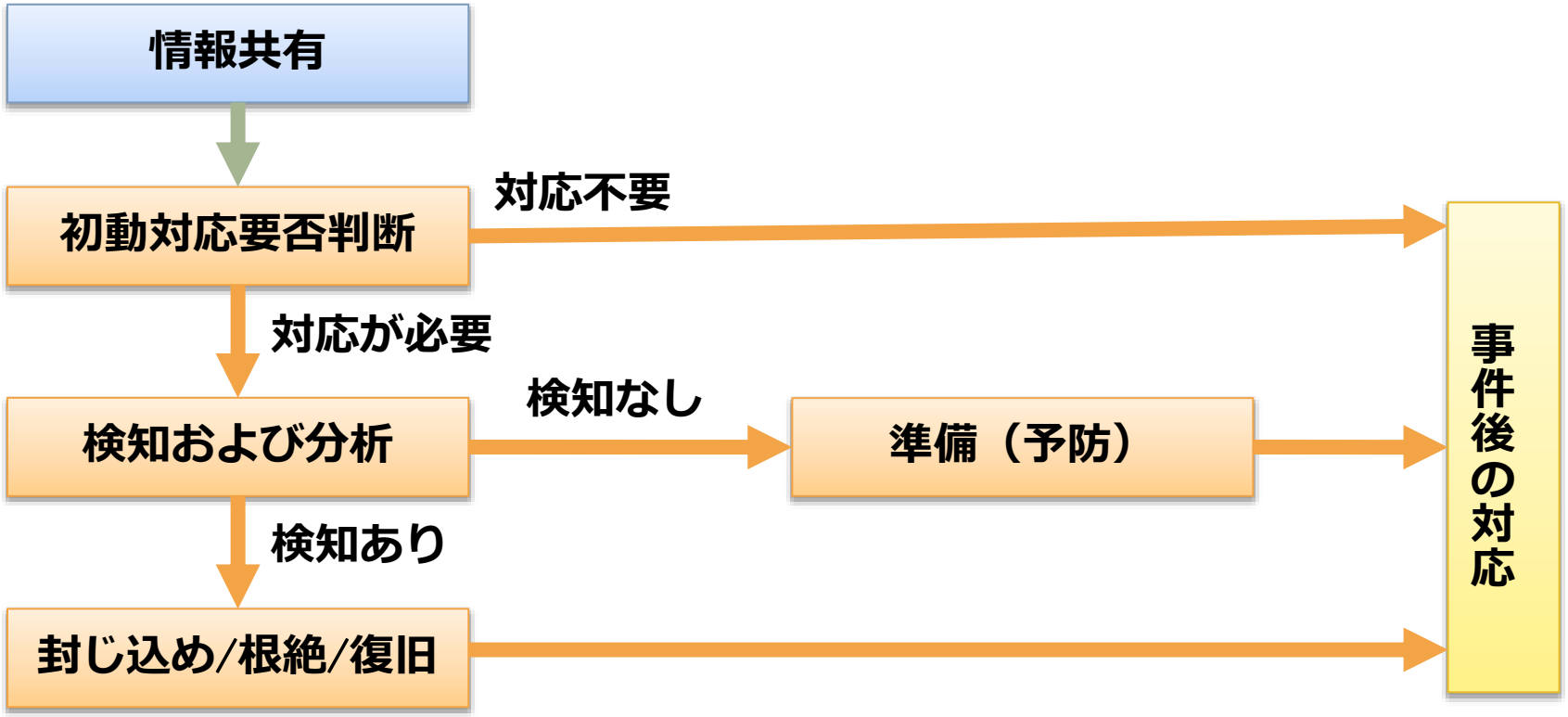


出典：http://www.intellilink.co.jp/column-tps

よくある共有される情報の例

- こんな情報が共有されていませんか？
  - 標的型攻撃のIPアドレス
  - 危ないと言われるURL、FQDN
  - 脆弱性が出ました！CVE-2017-******
- 共有された後、どうしてますか？

情報共有を出発点としたセキュリティ対応



情報共有を出発点としたセキュリティ対応 ～主な役割例～

When 初動対応要否判断

Why 対応が必要かどうか判断するため

脆弱性情報のWhat（例）

- 脆弱性識別子
  - CVE やパッチ番号など
- 脆弱性の対象となる
  - システム種別
  - バージョン
  - 条件（システム構成、設定など）
- 各セキュリティ製品における対応状況

攻撃関連情報のWhat（例）

- 該当の攻撃情報を示す名称
  - 攻撃名称、マルウェア名など
- 攻撃のターゲット
- 攻撃ベクター
  - どこから侵攻してくるか

When 検知および分析

Why 攻撃の発生有無、被害の有無を確かめるため

脆弱性情報のWhat（例）

- 攻撃の特徴
  - 攻撃形態、関連する通信の内容
  - 核心となる攻撃コード
- 各セキュリティ製品における検知名
- 攻撃によって残る痕跡
  - サーバやクライアントに残るログ

攻撃関連情報のWhat（例）

- 攻撃の特徴
  - 攻撃の通信内容、攻撃コード
  - 攻撃に関わるインジケーター
    - IP アドレス、メール件名など
- 各セキュリティ製品における検知名
- 攻撃を受けた場合の痕跡
  - サーバやクライアントに残るログ

When **封じ込め/根絶/復旧**

Why 被害の拡大抑止、沈静化のため

When **準備（予防）**

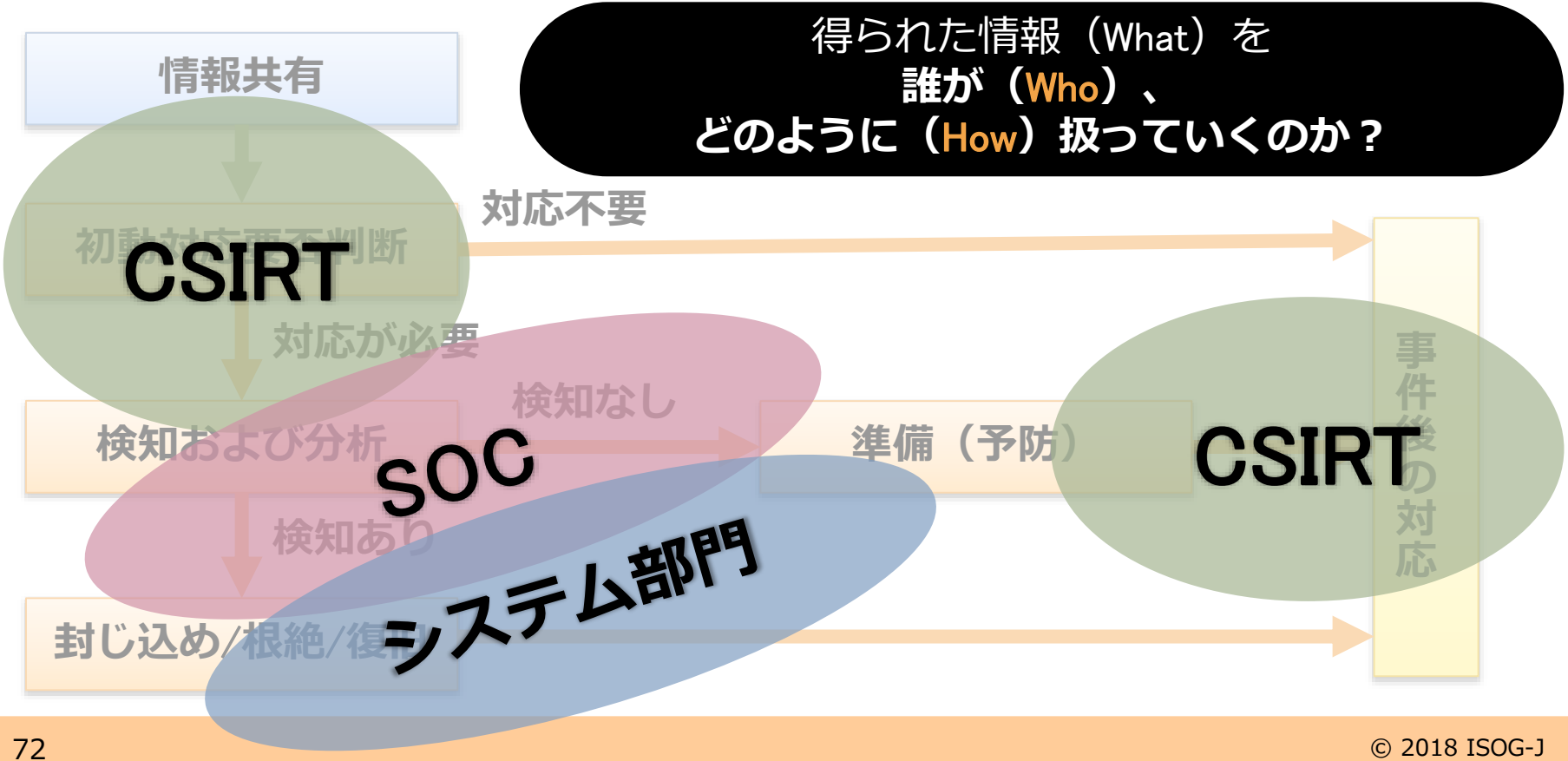
Why 被害防止のため

目的は異なるが
必要な情報はほぼ同等

脆弱性情報、攻撃関連情報のWhat（例）

- 攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件
- 攻撃を無効化する方法（パッチの適用、設定変更など）
- 被害を受けたシステムの復旧方法

情報共有を出発点としたセキュリティ対応 ～主な役割例～



「セキュリティ対応組織の教科書」をぜひ振り返ってみてください。
詳細な対応フロー例は教科書の7章にも記載があります。

When 初動対応要否判断

Who & How

「A-2. トリアージ基準管理」「A-3. アクション方針管理」に従い判断する。着手後は「E-3. 脆弱性管理・対応」によって組織的に対応していく。

When 検知および分析

Who & How

「B. リアルタイムアナリシス（即時分析）」を行い、より詳細な調査が必要な場 合は「C. ディープアナリシス（深掘分析）」へ進む。

When 封じ込め/根絶/復旧

Who & How

実害があった場合はインシデントとなる。「D. インシデント対応」を実施する。

When

準備（予防）

Who & How

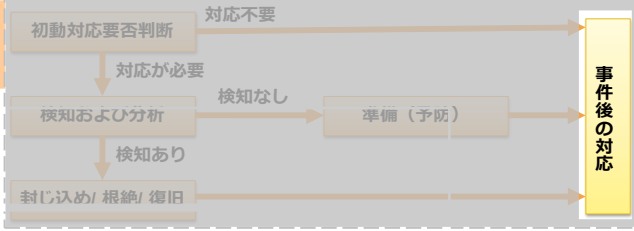
今後被害が発生しないようにするため、「G. セキュリティ対応システム運用・開発」の機能が中心となり、具体的な対策を実装する。改めて「E. セキュリティ対 応状況の診断と評価」を行うと、より万全な準備ができるだろう。

When

事件後の対応

Who & How

「F. 脅威情報の収集および分析と評価」において、実施した対応内容を客観的に評価し、改善を実施する。対応に問題が多かった場合には、 「A. セキュリティ対応組織運営」の中で抜本的な運営体制の見直しが必要なのかもしれない。さらにもう一つ大切なのは、「I. 外部組織との積極的連携」を促進するために**自身が発信者となっていく**ことである。成功談と失敗談、どちらも非常に価値のある情報である。



When **事件後の対応**

Why 自組織のみならず、世の中を少しでも安全にするため

以下のようなWhatであれば、きっとあなたも発信者になれるはず

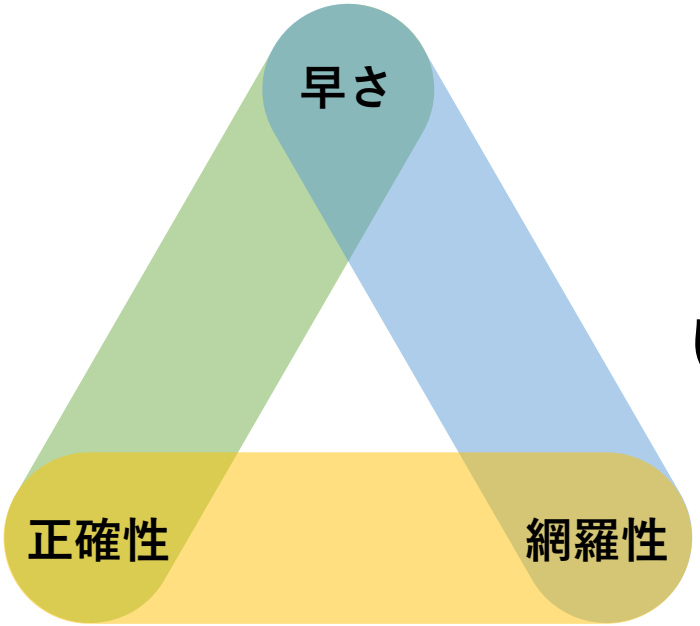
- 初動対応要否判断
  - いつどこから情報を得たか
  - どのように対応要否を判断したか（プロセス、ルール等含めた当時の状況）
- 検知と分析
  - 攻撃や被害の有無を確認した具体的な方法（どのログをどんな条件で探した、具体的にこんな痕跡があった、など）
- 封じ込め/根絶/復旧と準備（予防）
  - 実際に行った対応内容（システムにどんな設定を行ったか、どのセキュリティ製品にどんな設定を行ったか）
- 対応全体通して
  - うまくいった点
  - うまくいかなかった点
- 今後の具体的な改善ポイント

5W1Hで考える情報共有

	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？

速さと正確性と網羅性の課題

- 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

出典：27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)

情報の内容

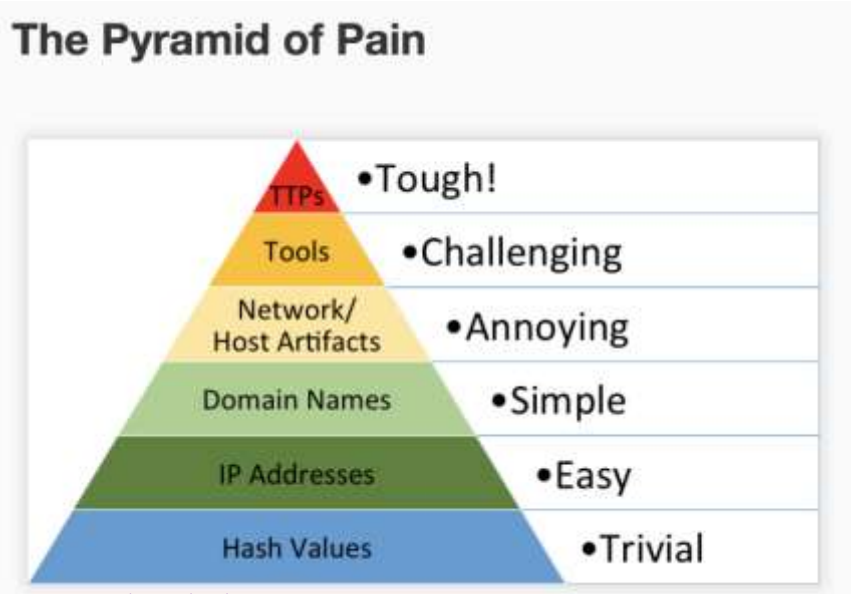
- 世の中には情報があふれている
  - 情報はたいてい「誰かの」役に立っている
- 情報の選び方
  - 場を選ぶ、相手を選ぶ
    - 同じ業種、似た業態、似た規模…
  - 情報を使う状況に応じて選ぶ
- 情報発信する
  - 自分と似た境遇の人に役に立つ(であろう)情報を発信する
- 情報共有のトライアングルを忘れない

セキュリティ情報の例: The Pyramid of Pain

- 標的型攻撃インディケーター情報分類のコンセプト図

- 上位のものほど難しい
  - 作る/使うコストが高い

- 自分に必要な情報は？



出典: Enterprise Detection & Response : The Pyramid of Pain (by David Bianco) http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

終わりに

- 現在の情報共有に関する課題に対して、どう考えるべきかを整理しました。
- まだ、以下の課題があると認識しています
  - 発信者側と受信者側の「How」の標準化、自動化
  - 情報の信頼度、有効性の可視化
  - 発信者と受信者をつなぐ、フィードバックの連携

- これからも議論を続け、成果物をリリースする予定です！

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

（参考：アイコン、漫画素材）

http://www.security-design.jp/
http://www.chojugiga.com/
http://mangaonweb.com/

（フォント類）

http://www.hakusyu.com/