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～
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」

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：司会進行

- 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

講演者

@NTTSec_JP

- **阿部 慎司**
  - 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
  - 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

- 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

講演者

- 市川　隆義　です。
  - ソフトバンク・テクノロジー セキュリティソリューション本部
  - ソフトバンクグループ内に存在する「3つ」のSOCに勤務

2002年

サーバー、ストレージの構築、保守、販売

セキュリティ機器提案・構築
セキュリティ製品のトレーナー（教育）
SOCにおけるセキュリティ監視・イベント分析

現在

SOCアナリストのマネジメント

講演者

- **亀田　勇歩**

  SCSK株式会社　セキュリティアナリスト
  - Web/PF脆弱性診断
  - SOC監視業務
  - インシデントレスポンス

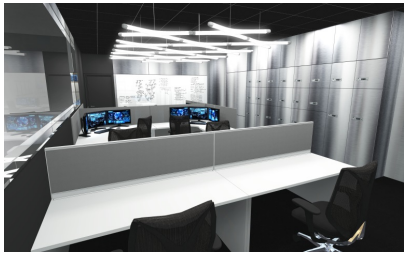
  ISOG-J / OWASP
  - **ZAP**エヴァンジェリスト
  - **脆弱性診断士**の活動

  趣味
  - 今年のラスベガスで開催された**DEFCON OSINT CTF**で**8位**入賞してきました
  - 今年の11/11に国内で2回目の**Open xINT CTF**を**開催**してきました

講演者

- ももいやすなり
  株式会社インターネットイニシアティブ
  セキュリティ本部 セキュリティ情報統括室 リードエンジニア
  - サービス開発、システム開発、研究開発、ネタ披露
  - IIJ-SECT (CSIRT)、関連団体 (ISOG-J など)、コミュニティ (Vuls など)
  - 食べ物、ヘヴィメタル、ねこ

- SOC できました
  - 見学できます！ ご連絡ください！



- セキュリティ情報発信
  - wizSafe Security Signal 始まりました！
  - IIR, IIJ Security Diary もやってます

IIJ-SECT
IIJ Group Security Coordination Team

wizSafe
安全をあたりまえに

このセッションは？

- ISOG-Jが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？？

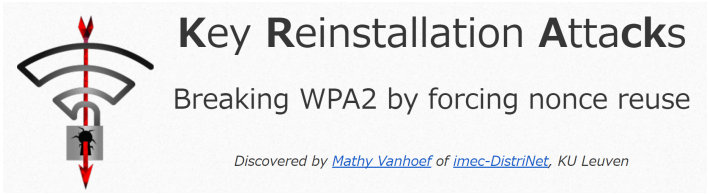
例えば、Struts2やTomcat

- 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？

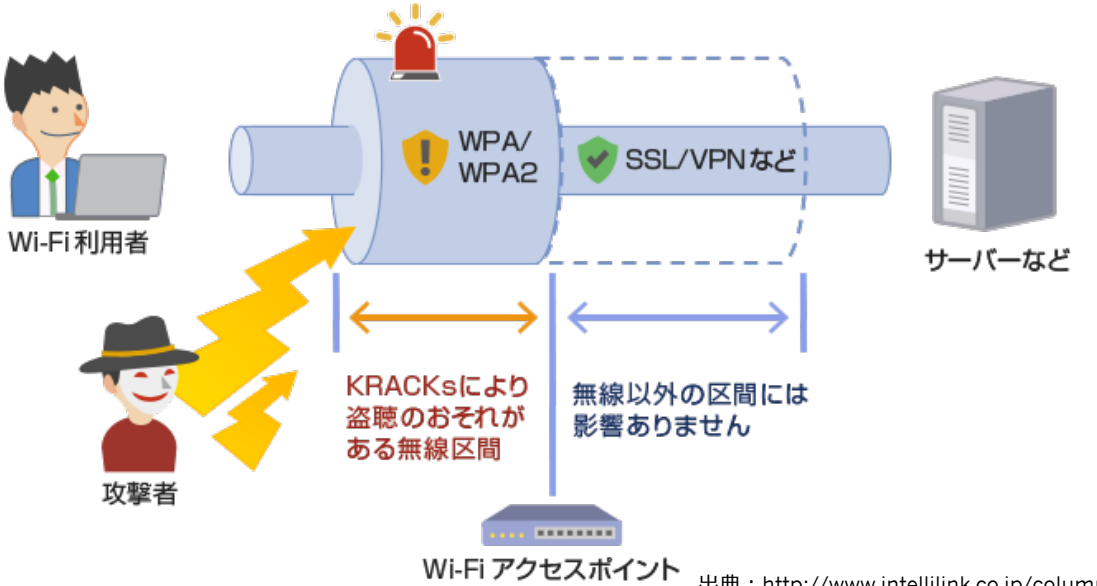
- 「慣れ」だけではやっぱり慌てません？

そんなところでKRACKsが！

- **K**ey **R**einstallation **A**tta**CKs** (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

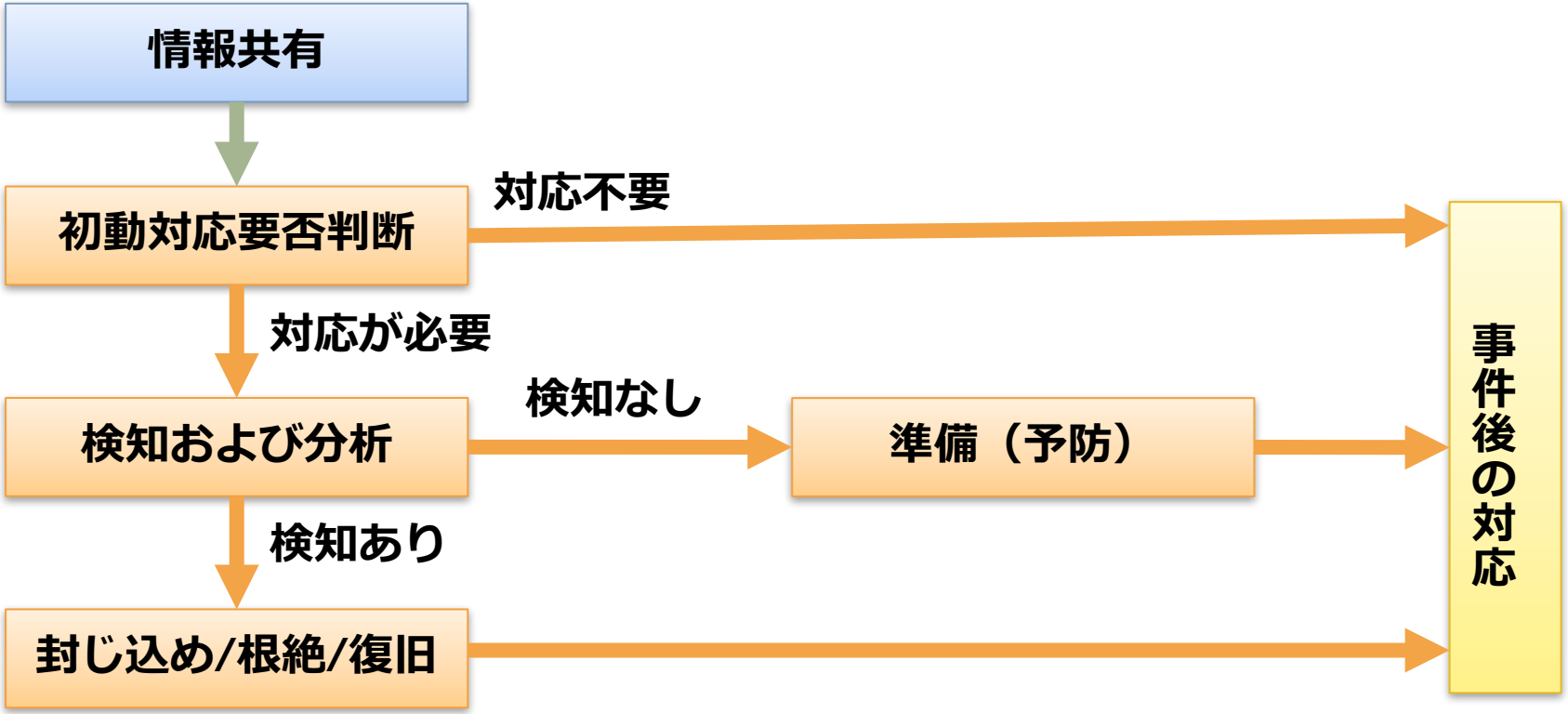


出典：http://www.intellilink.co.jp/column-tps

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

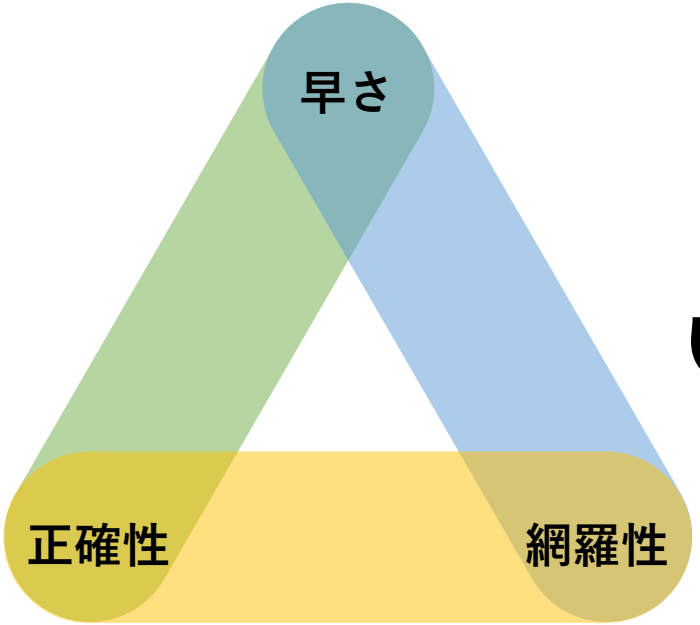
- 初動対応要否判断
  - いつどこから情報を得たか
  - どのように対応要否を判断したか（プロセス、ルール等含めた当時の状況）
- 検知と分析
  - 攻撃や被害の有無を確認した具体的な方法（どのログをどんな条件で探した、具体的にこんな痕跡があった、など）
- 封じ込め/根絶/復旧と準備（予防）
  - 実際に行った対応内容（システムにどんな設定を行ったか、どのセキュリティ製品にどんな設定を行ったか）
- 対応全体通して
  - うまくいった点
  - うまくいかなかった点
- 今後の具体的な改善ポイント

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

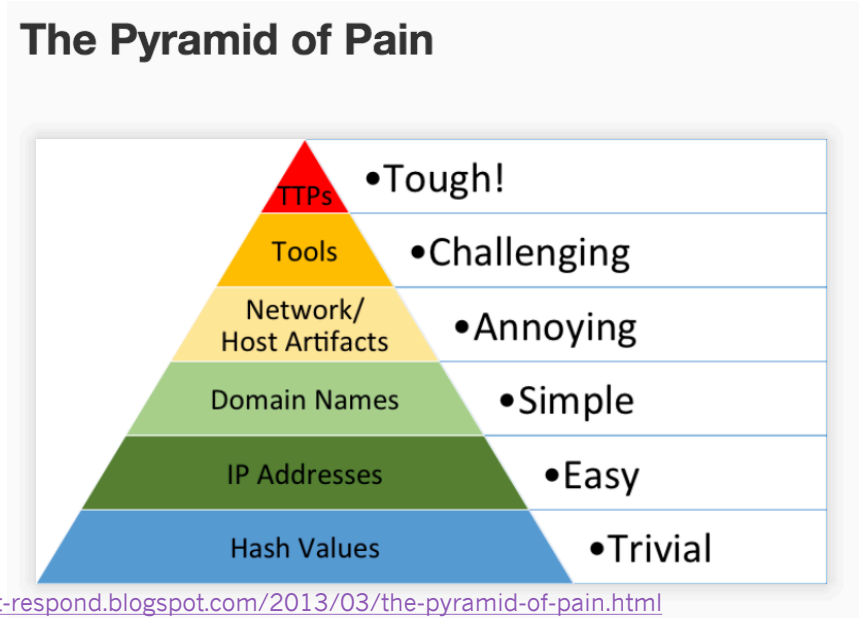
- 世の中には情報があふれている
  - 情報はたいてい「誰かの」役に立っている
- 情報の選び方
  - 場を選ぶ、相手を選ぶ
    - 同じ業種、似た業態、似た規模…
  - 情報を使う状況に応じて選ぶ
- 情報発信する
  - 自分と似た境遇の人に役に立つ(であろう)情報を発信する
- 情報共有のトライアングルを忘れない

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

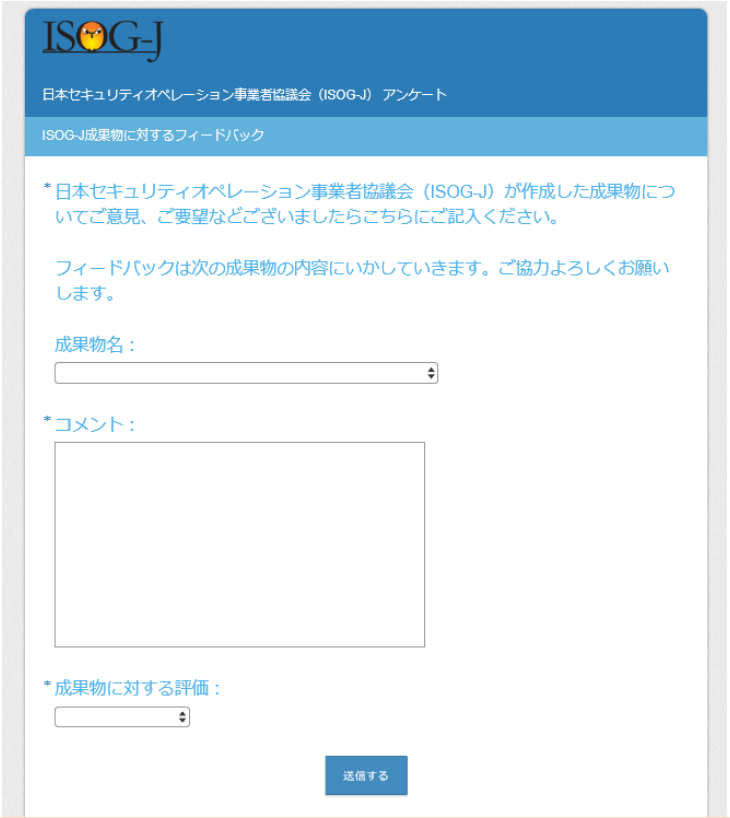
- 現在の情報共有に関する課題に対して、どう考えるべきかを整理しました。
- まだ、以下の課題があると認識しています
  - 発信者側と受信者側の「How」の標準化、自動化
  - 情報の信頼度、有効性の可視化
  - 発信者と受信者をつなぐ、フィードバックの連携

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