セキュリティ情報共有のかんどころ

ももいやすなり <momo@iij.ad.jp>
ISOG-J / 株式会社インターネットイニシアティブ

2018-01-26 @ JANOG41 Hiroshima

軽く自己紹介

・ ももいやすなり

・ Facebook ymomoi　Twitter @sbg

・ 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

・ 開発、セキュリティ

・ 食べ物、ヘヴィメタル、ねこ

ISOG-J のご紹介

- 日本セキュリティオペレーション事業者協議会
- http://isog-j.org/
- blog 書いた →

セキュリティ関連の情報

- 流通している情報が増えた
  - OSINT
- 情報交換のフレームワークや場ができた
  - CYBEX, STIX/TAXII
  - サイバー情報共有イニシアティブ J-CSIP
  - 日本シーサート協議会、各種 ISAC

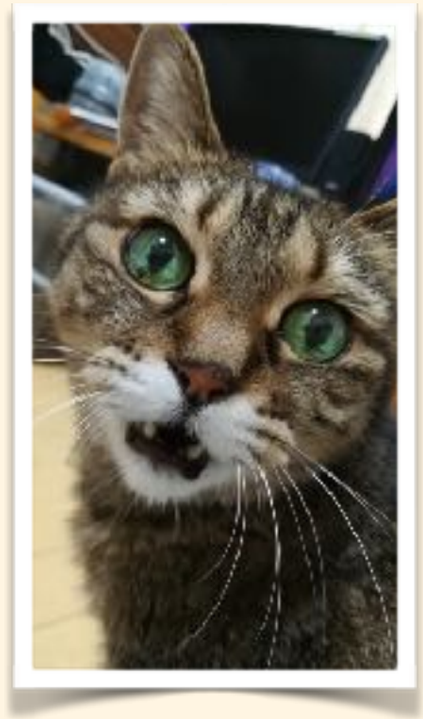
ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

CSIRT
日本シーサート協議会

なぜ今、情報共有が課題？

- セキュリティ対応組織 (SOC/CSIRT) 作った！
- 情報収集してみたけどけっこうたいへん
  - みんなで共有して楽しよう！
- 団体やコミュニティに所属して情報集め
  - うまくいきましたか？
  - 情報をうまく使えてますか？

情報共有のミスマッチ



- 欲しい情報はそれぞれに異なる
  - 組織の業種、規模、組織の成熟度、担当者の職種…
- どれが食い違ってもミスマッチは起こりえる
  - 「フレームワーク」や「場」の問題ではない
- 「セキュリティ情報」は多岐にわたる
  - 情報提供元は受け取り側での必要性を判断できない

セキュリティ対応組織を作る

Internet Week 2015

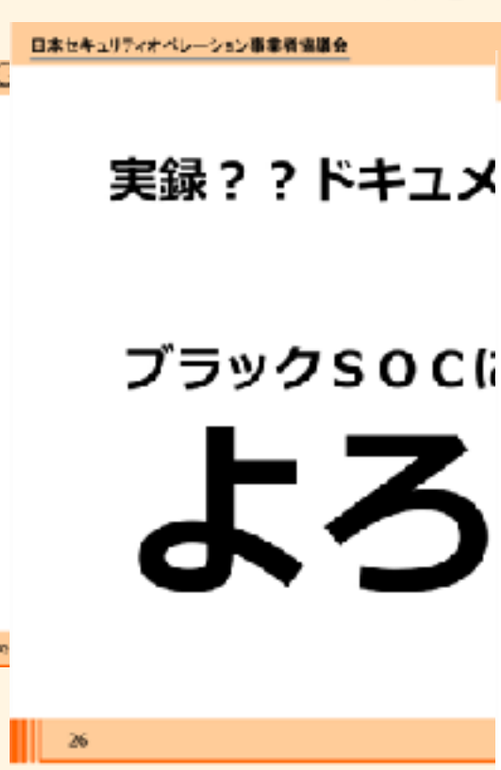
- S13 150分でわかるセキュリティ対応できる組織にする10のコツ
- S14 CSIRT時代のSOCとのつき合い方 2015
- SOCが悩むセキュリティ対応の現実 2015

Internet Week 2015 プレゼンテーション
https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/

Ten Strategies of a World Class Cybersecurity Operations Center
https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center

Internet Week 2016

- D1 法規制とサイバー攻撃対策の動向を見抜く
- 第3部　失敗から学ぶ、SOC／CSIRTのあり方
  - 失敗から学ぶ、セキュリティ対応組織が担うべき役割



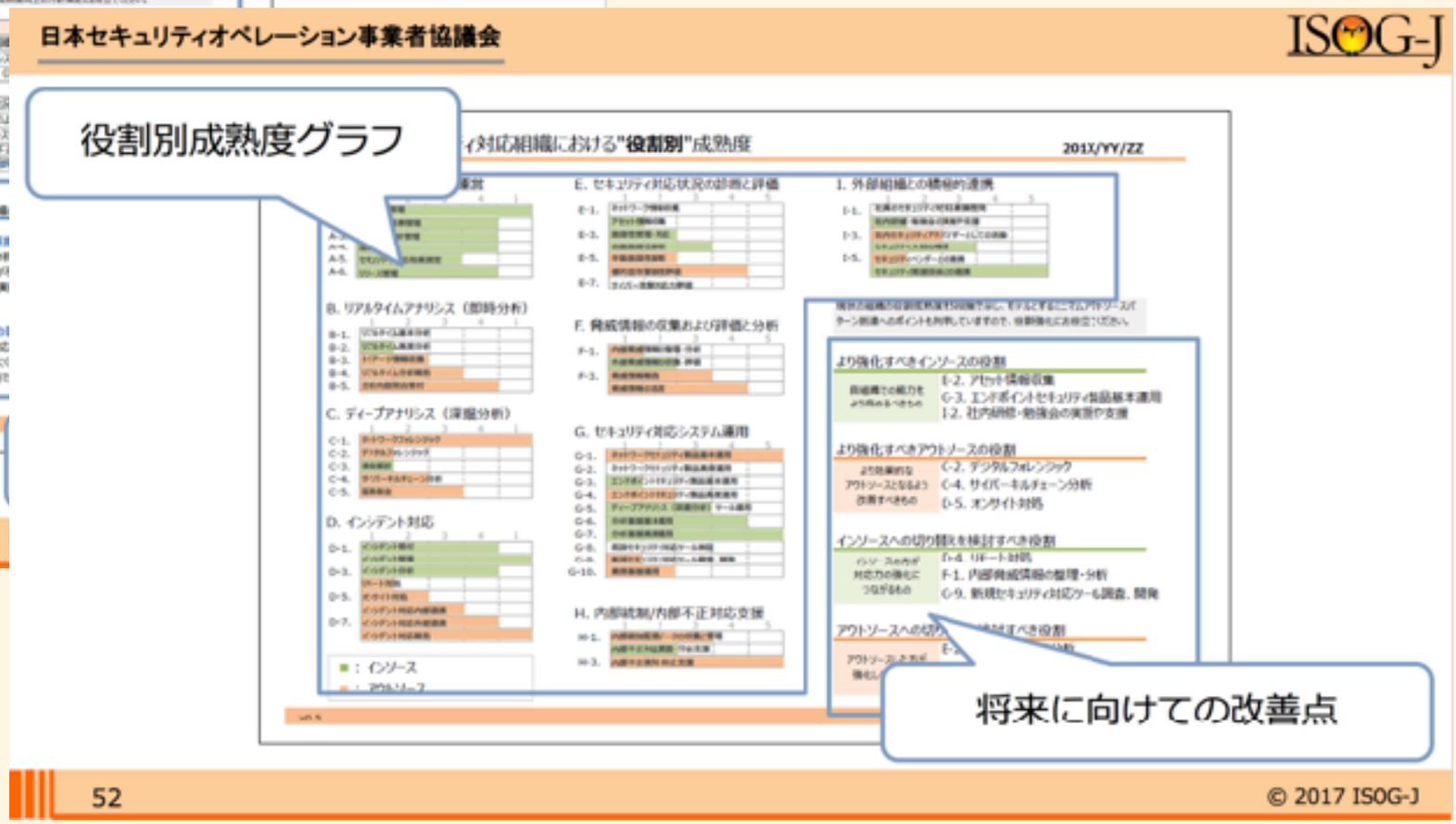
Internet Week 2016 プレゼンテーション
https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/

セキュリティ対応組織の教科書

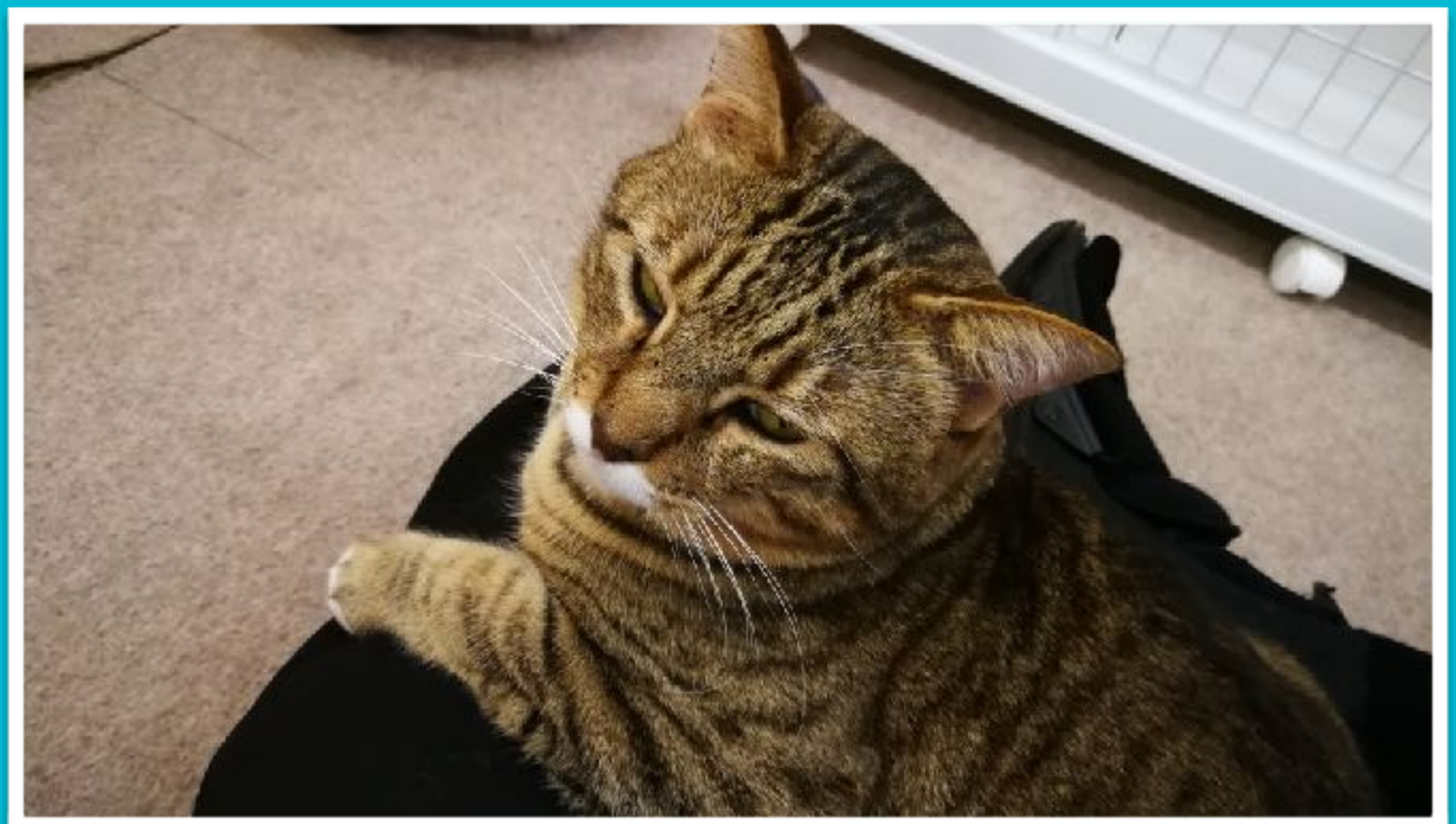
- セキュリティ対応組織の教科書v2.0
  - https://goo.gl/soVWUZ
- ISOG-J によるセキュリティ組織の考え方
  - セキュリティ対応に必要な機能による整理
  - 組織の到達目標と成熟度という評価軸

成熟度チェックシート

・Excel シートでセルフチェックできます



己を知る

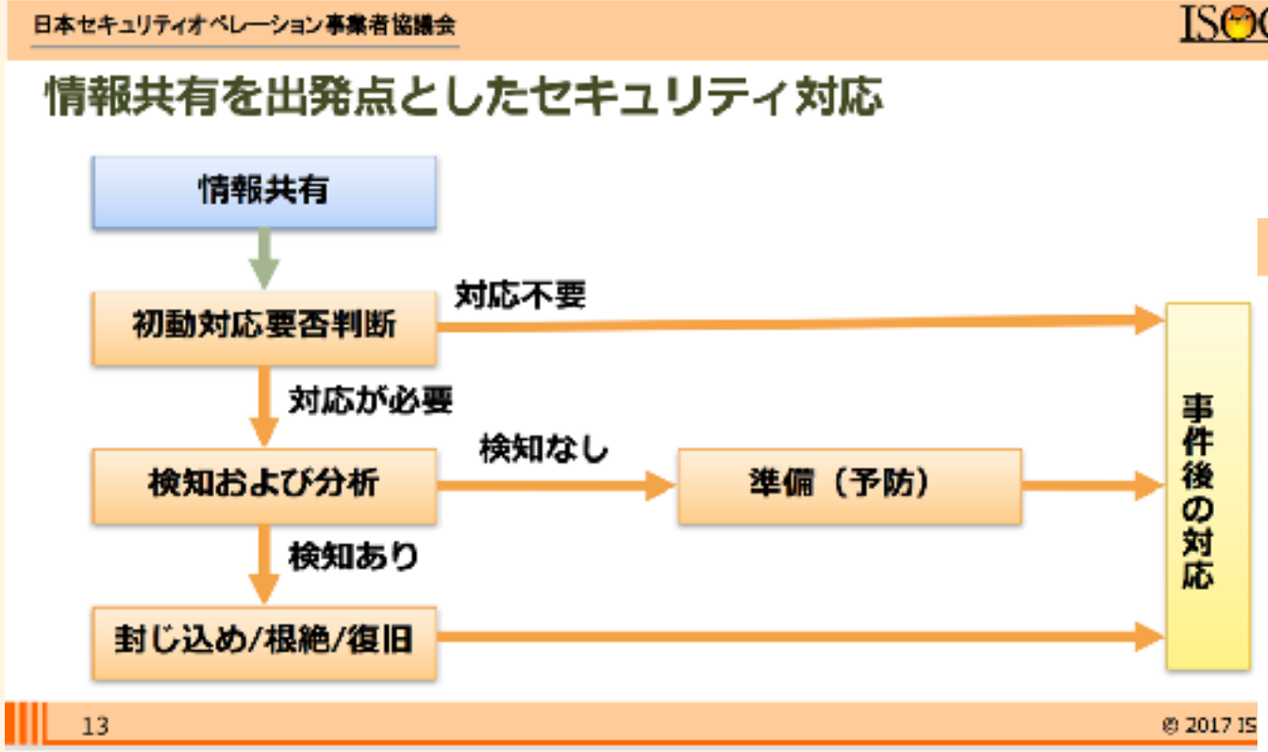


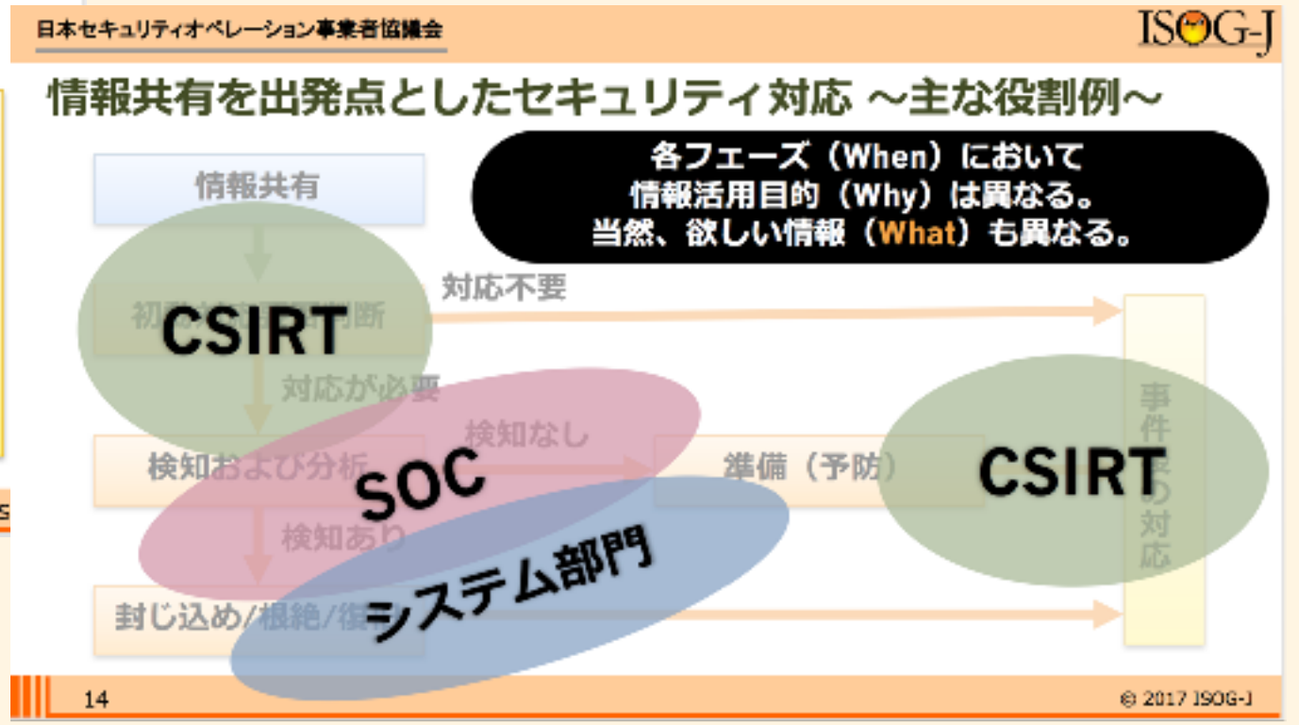
セキュリティ情報共有の 5W1H

- 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」 v1.0
  - https://goo.gl/s8TRxZ
- 情報を提供する側、受け取る側の考え方
  - フレームワークや場をうまく使うために

情報を基にした対応フロー

・いつ、何に使うのかで必要な情報は異なる



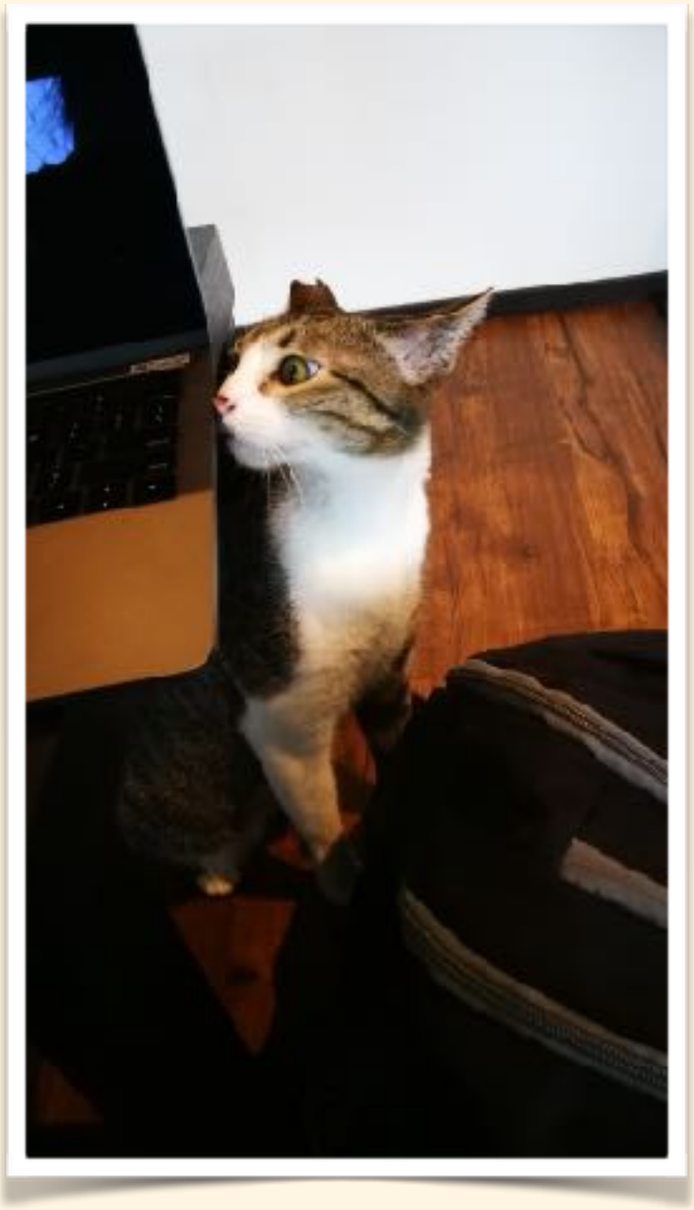


情報収集あるある

・集めすぎ、掘りすぎ、気になりすぎ

・何事もやりすぎは禁物

・目的を見失わない

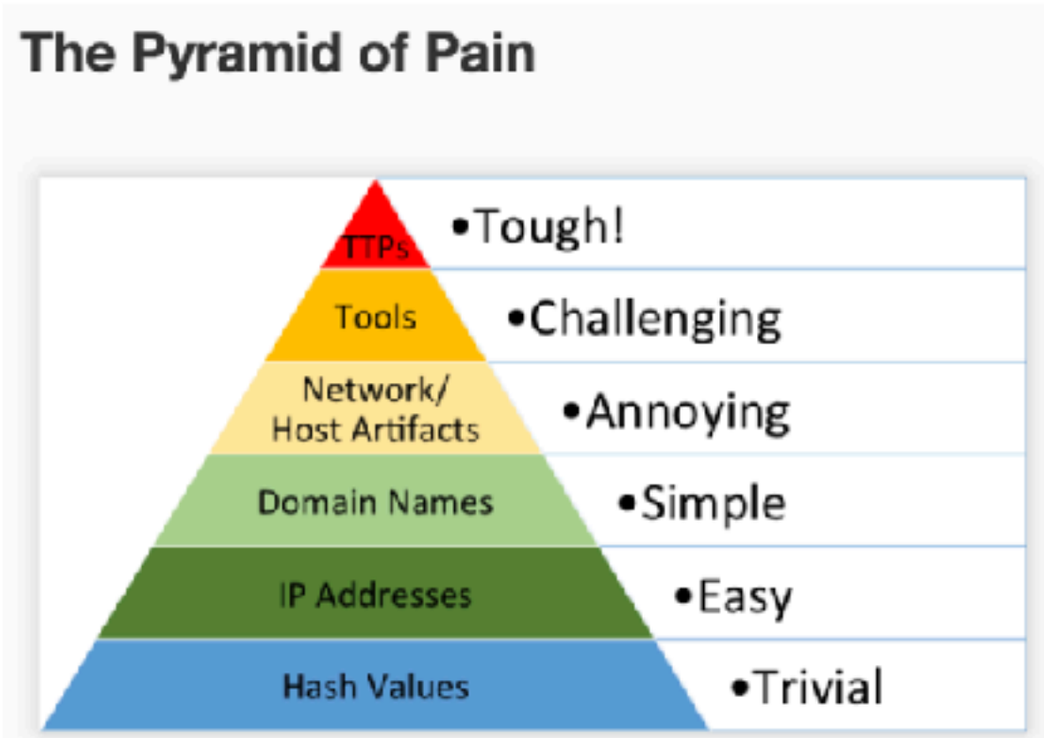


Pyramid of Pain

・行為者、背景、組織 -> あなたに必要ですか？

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

己を知る

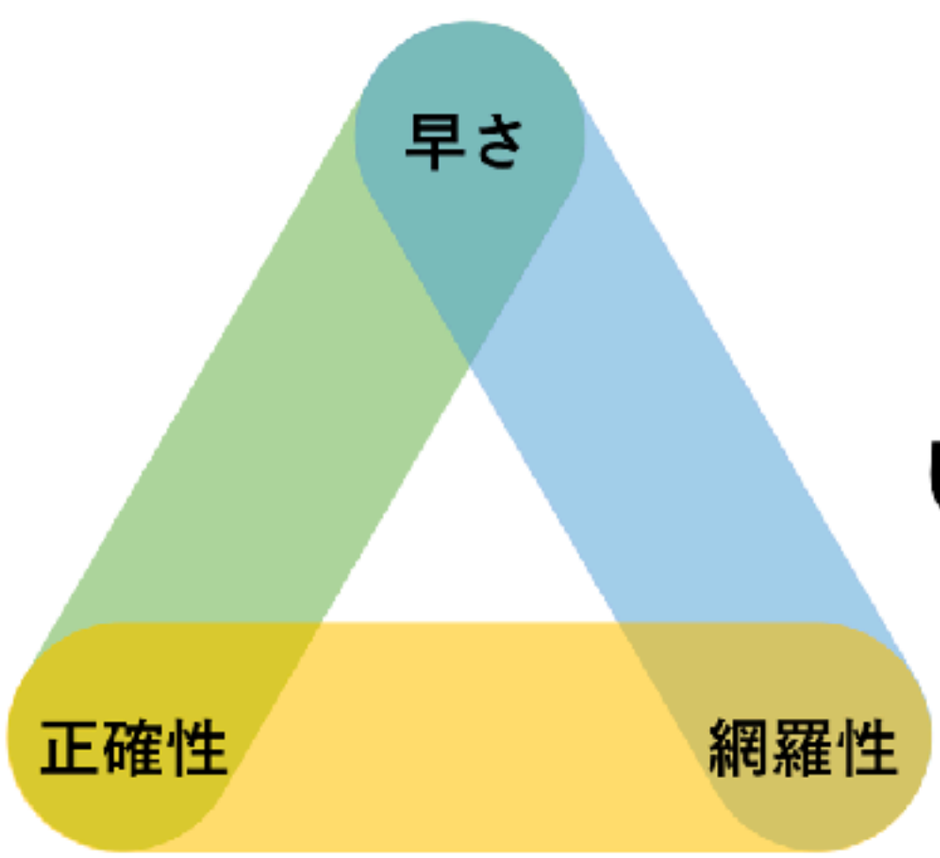
情報共有のしかた

- 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立つ(だろう)情報を発信する

情報共有のジレンマ

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

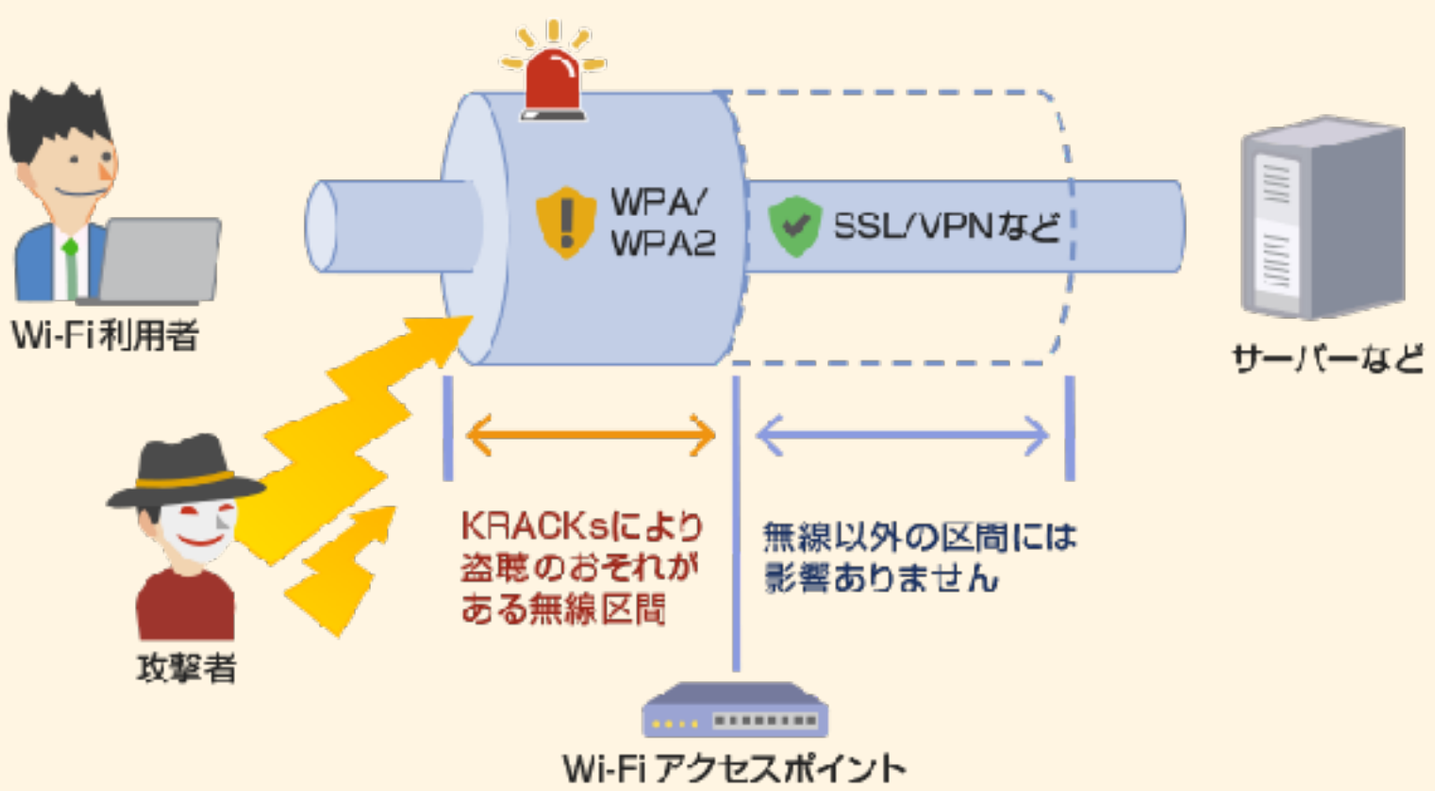
出典：27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)

事例から考えてみる (1)

- Struts2, bind祭り
- もう皆さん慣れてます(よね？)
  - 練習は重要です
- こなれるまでどのくらいかかりましたか？

事例から考えてみる (2)

- KRACKs (Wi-Fi WPA/WPA2 脆弱性)
- なぜか詳細が出る前に大ニュースになった
- 正しく怖がる



【緊急レポート】KRACKs（key reinstallation attacks：鍵再インストール攻撃）について | NTTデータ先端技術株式会社
http://www.intellilink.co.jp/article/vulner/171019.html

職種が似れば
欲しい情報も似る？

オペレーター向け ISAC あり☑

- JANOG39 金沢の BoF で…
  - 「脆弱性ハンドリングを楽にするBoF」
- OPS-ISAC

16:30	本会議場	セキュリティ人材育成の取り組み	酒井 正幸（北陸通信ネットワーク）
	第5会議室	コーポレートIT担当者全員集合BoF 第1弾	近藤 羽浩（GMOクラウド株式会社） 堀内 克昌（楽天株式会社）
	第6会議室	多品種少量サービス運用について その3	冨永 良明（株式会社エヌ・ティ・ティ エムイー）
	大集会室	サイバーセキュリティbof#2	富樫 健太（株式会社KDDI ウェブコミュニケーションズ） 杉山 幸太（株式会社KDDI ウェブコミュニケーションズ） 小林 裕士（東京大学） 青木 翔（一般社団法人JPCERTコーディネーションセンター） 山下 健一（さくらインターネット株式会社） 寺岡 良真（株式会社神戸デジタル・ラボ）
	第2会議室	コミュニティの行動規範 - jancgはどうする？	松崎 吉伸（JANOG運営委員会）
	本会議場	Peering In Japan BoF	平井 則晴（ソフトバンク株式会社）
	大集会室	見つけた！モダンなトラフィック可視化 BoF	西塚 要（エヌ・ティ・ティ・コミュニケーションズ株式会社）
	本会議場	脆弱性ハンドリングを楽にするBoF	中島 智広（NRIセキュアテクノロジーズ株式会社）