D2-2 もう一人で困らない！ セキュリティ対応のアウトソース

各種ドキュメントで考える、セキュリティ対応組織のあり方

2018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)

司会進行

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- 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
  - 2016年度までは社名が「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

- 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

2000年代初頭のJNSAのChallengePKI PJにてセキュリティに目覚め、
SSOや統合ID管理基盤システム構築運用を経てサイバーセキュリティの世界へ。
セキュリティシステムやインシデント対応体制の構築、
セキュリティインシデント対応教育／訓練・演習などの業務に従事。
現在はＳＯＣでの運用と自組織サービスのインシデント対応チームに所属。

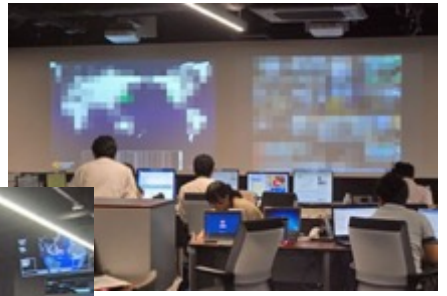
講演者

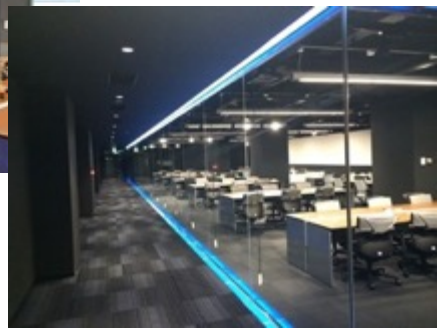
- 河島　君知　です。
  - NTTデータ先端技術株式会社　セキュリティ事業部
  - JNSAのISOG-J運営委員

2003年　セキュリティ監視業務

セキュリティインシデント対応
セキュリティ製品開発
セキュリティサービス企画・開発・立上

現在　セキュリティ対応組織構築支援





Itmediaエグゼクティブ様取材記事より

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、宴会調整
  - IIJ-SECT (CSIRT)、関連団体 (ISOG-J, ICT-ISAC など)、コミュニティ (Vuls など)
  - 食べ物、ヘヴィメタル、ねこ



- SOC 見学やってます
- セキュリティ情報発信
  - wizSafe Security Signal
  - IIR, IIJ Security Diary, IIJ Engineers blog
    - IIR Vol.40 の記事を書きました

IIJ-SECT
IIJ Group Security Coordination Team
wizSafe
安全をあたりまえに

講演者

- 田中　朗（たなか　あきら）　（ISOG-J フェロー）
  - 某社でCISOというセキュリティ責任者やってます

1980年代、1990年代　メーカの研究所でソフトウェアの研究・開発
　　プログラミング色々、JUNETからWIDEの変化をすぐそばで
1998年　セキュリティ事業立上げ、顧客向けのMSS(Managed Security Service)提供
2011年　ISOG-J活動に参加
2015年　社内CSIRT設立、その後CSIRTリーダー
2016年　JNSA　CISO支援WG
2018年　ユーザ企業に転職

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11月8日現在、46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：　https://isog-j.org
- facebook：/isogj
- twitter：@isog_j

第一部のメニュー

1. 前回までのおさらい
2. 「セキュリティ対応組織の教科書 ハンドブック」と「成熟度チェックリスト(ISOMM)」の紹介
3. 「セキュリティ対応組織強化のための情報共有の5W1H」の実体的なフローの紹介と英語版の紹介
4. JNSA発行「CISOハンドブック」の紹介と現場レベルでの活用について

前回までのおさらい

←ココから

（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

（参考）2017年の「今求められるSOC,CSIRTの姿とは」から

- 教科書を元にしたインシデント時の実際のフロー、何もない平時に何をすべきか。そこから成熟度モデルの紹介へ。

- 現在の情報共有のニーズと、一方現場で起きている課題の整理。

資料URL（2つ、5.24MB+3.78MB）

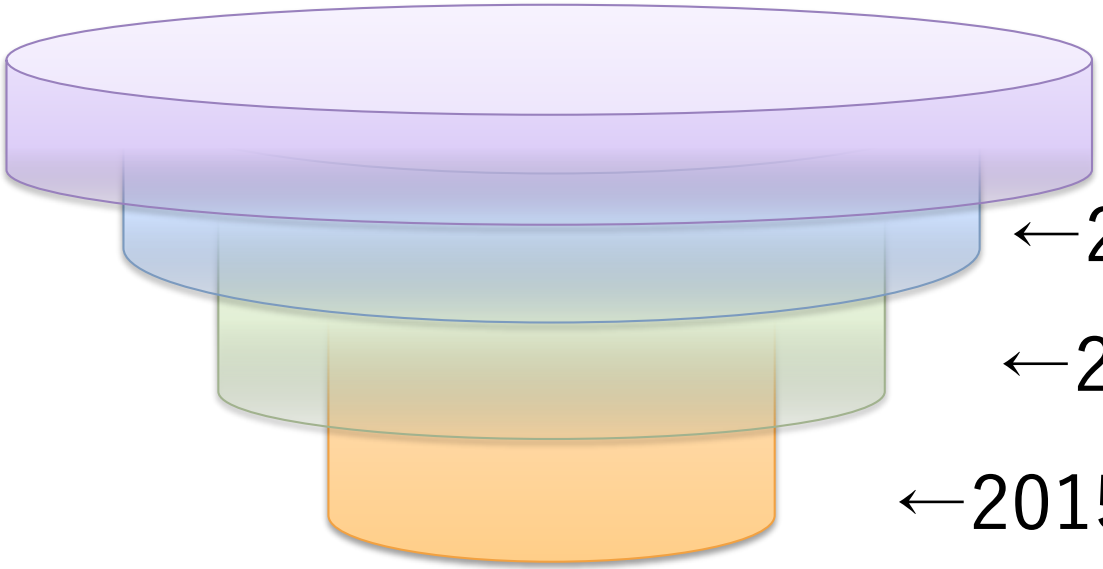
https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/d1/

前回までのおさらい

←ココまで

心構えから、実際の業務、そしてアウトソースの分担へ

どこまでを自分たちでやるか、ユーザー目線で
アウトソースをどうするか。



←2018:今年！

←2017:周辺にある諸課題

←2016:対応の全体像

←2015:心構え

第一部、このあとは

- 「セキュリティ対応組織の教科書 ハンドブック」と「成熟度チェックリスト(ISOMM)」の紹介

- 「セキュリティ対応組織強化のための情報共有の5W1H」の実体的なフローの紹介と英語版の紹介

- JNSA発行「CISOハンドブック」の紹介と現場レベルでの活用について

「セキュリティ対応組織の教科書 ハンドブック」と「成熟度チェックリスト(ISOMM)」の紹介

自己紹介

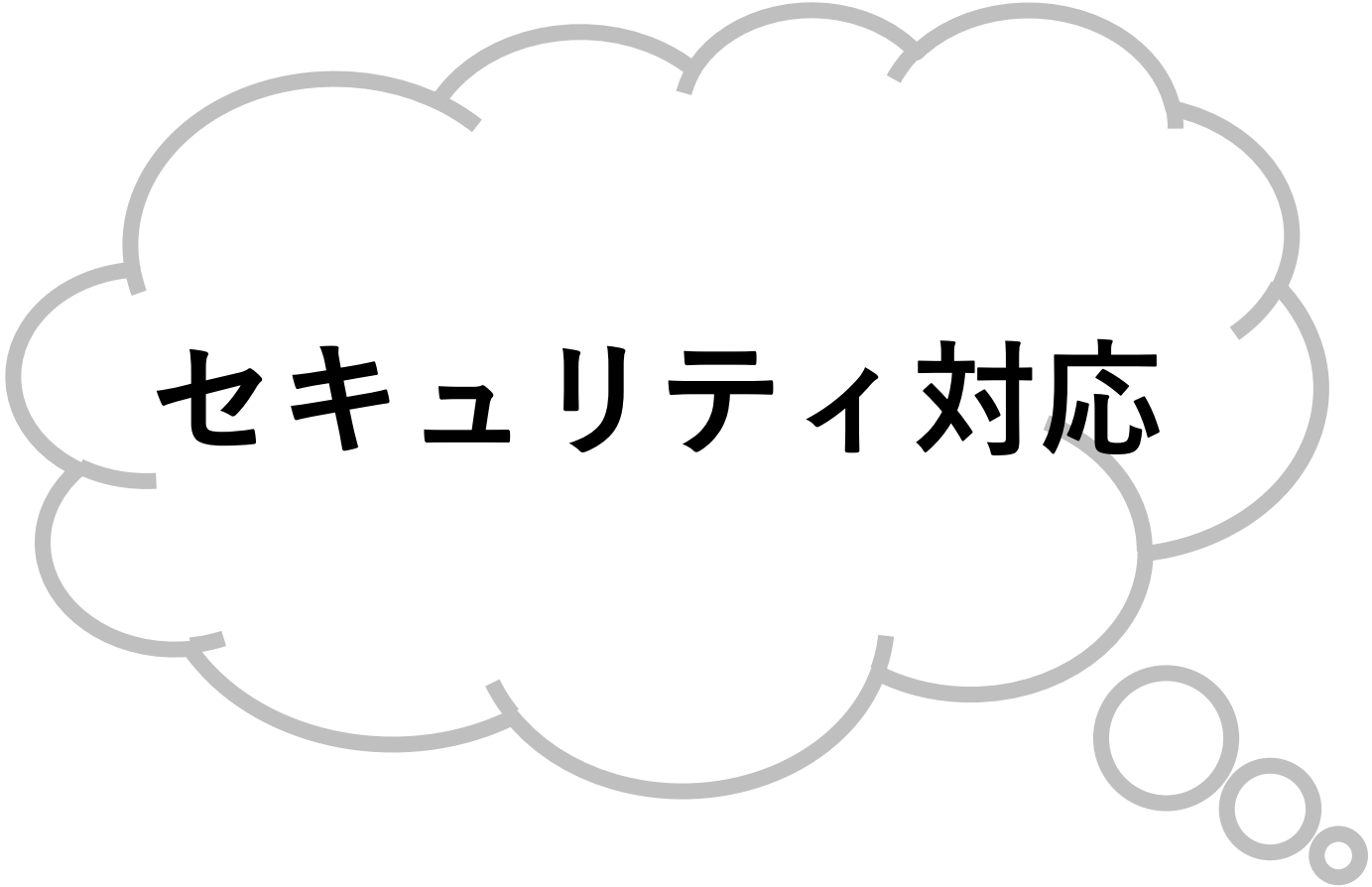
- 早川　敦史　です。
  - NECソリューションイノベータ株式会社
  - ISOG-J運営委員、ISOG-J運営サポートグループリーダー

2000年代初頭のJNSAのChallengePKI PJにてセキュリティに目覚め、
SSOや統合ID管理基盤システム構築運用を経てサイバーセキュリティの世界へ。
セキュリティシステムやインシデント対応体制の構築、
セキュリティインシデント対応教育／訓練・演習などの業務に従事。
現在はＳＯＣでの運用と自組織サービスのインシデント対応チームに所属。

セキュリティ対応組織の教科書
ハンドブック
と
成熟度セルフチェックシート
ISOMM
(ISOG-J SOC/CSIRT Maturity Model)
のご紹介

ISOG-J ホームページ
https://isog-j.org
よりダウンロード可能

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



- 経営者の思うセキュリティ対応
- セキュリティ責任者が思うセキュリティ対応
- 現場が思うセキュリティ対応

立場によって考えることが異なることを理解しつつ
それぞれに合った考え方（ガイドライン）を把握する

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

CSIRTとSOCの役割は
その境界線が
企業・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 v2.1

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

上司は読んでくれるだろうか…

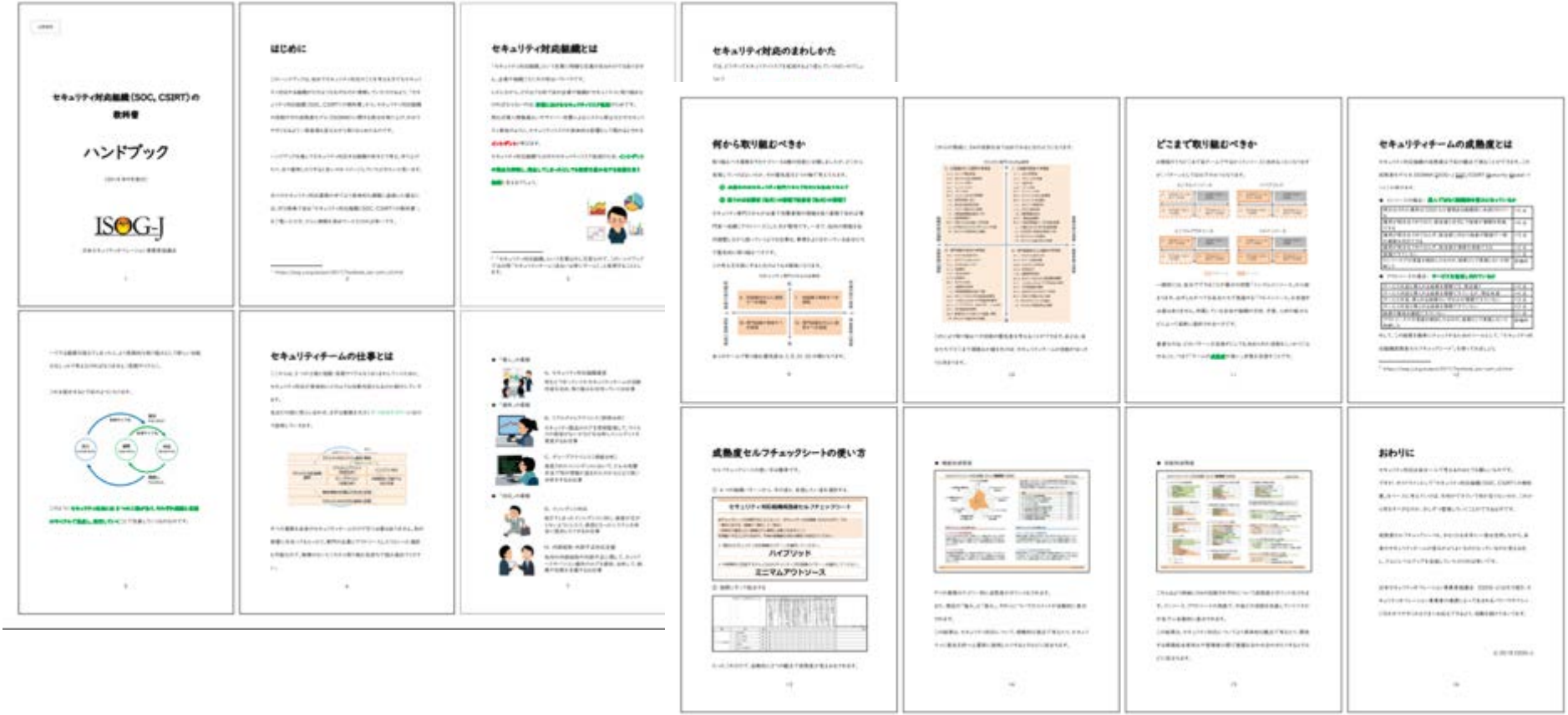
もっと簡単に「セキュリティ対応組織の教科書」を理解したい（してもらいたい）

セキュリティ対応組織の教科書 ハンドブック v1.0

読みやすい概要版。

A3 8up両面で印刷にちょうどいい

16ページ＋1枚



https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0.pdf

日本セキュリティオペレーション事業者協議会 ISOG-J

セキュリティ対応組織（SOC/CSIRT）の教科書 ハンドブック 別紙

セキュリティ対応の役割一覧

	A セキュリティ対応組織運営	
	何をどう守っているのかセキュリティチームの活動内容を決め、具体的な取り組みを仕切っていくお仕事	
A-1	全体方針管理	セキュリティ対応全体の活動についての方針を管理し、推進する
A-2	トリアージ基準管理	セキュリティ事故が起こってしまったときの対応優先度を決める
A-3	アクション方針管理	セキュリティ事故が起こってしまったときの対処方針を決める
A-4	品質管理	運用や対応において問題がなかったか把握し、改善する
A-5	セキュリティ対応効果測定	全体としてのセキュリティ対策がよくいっているか指標をまとめ、効果を確認する
A-6	リソース管理	セキュリティ対応に必要な予算、人員、システムを計画し、配分する

	B リアルタイムアナリシス（即時分析）	
	セキュリティ製品のログを常時監視して、ウイルスの感染がないかなどを分析し、インシデントを発見するお仕事	
B-1	リアルタイム基本分析	ネットワークやサーバーのログを分析する
B-2	リアルタイム高度分析	基本分析で足りない場合、より多くのログやデータ等含めた分析する
B-3	トリアージ情報収集	対応優先度を決めるため、分析結果以外の関連情報を集める
B-4	リアルタイム分析報告	リアルタイム分析で分かったことを取りまとめて報告する
B-5	分析結果照会受付	報告した内容について問い合わせ対応する

	C ディープアナリシス（深掘分析）	
	発見されたインシデントにおいて、どんな攻撃手法で何の情報が盗まれたのかなど、より深い分析をするお仕事	
C-1	ネットワークフォレンジック	リアルタイムで行いきれなかった詳細な分析を行う
C-2	デジタルフォレンジック	被害に遭った端末で何が起こったのか明らかにする
C-3	検体解析	ウイルスがどのような動きをするものだったか解析する
C-4	改善全般解析	これまでの分析結果全てをふまえ、攻撃の目的や手法を明らかにする
C-5	証拠保全	裁判などの法的な対応に必要な証拠を保存しておく

	D インシデント対応	
	起きてしまったインシデントに対し、被害拡大がないようにしたり、原因となったシステムを安全に復旧したりするお仕事	
D-1	インシデント受付	即時分析で見つかったり、外部からの報告されたインシデントを受け付ける
D-2	インシデント管理	受け付けたインシデントの対応進捗管理を行う
D-3	インシデント分析	受け付けたインシデントをどのように対応していくべき判断する
D-4	リモート対処	監視センターなどからリモートで対処、復旧する
D-5	オンサイト対処	現場に駆けつけて対処、復旧する
D-6	インシデント対応内部連携	社内の関係者（経営者、関係部門）などへ報告、協力依頼する
D-7	インシデント対応外部連携	社外の関係者（顧客、取引企業）などへの説明、調整をする
D-8	インシデント対応報告	インシデントの影響や原因、対処内容についてとりまとめる

	E セキュリティ対応状況の診断と評価	
	脆弱性診断や標的型メール訓練などによりセキュリティが古ちんと守られているか評価するお仕事	
E-1	ネットワーク情報収集	守るべきネットワークの構成を把握する
E-2	アセット情報収集	守るべき端末やサーバーの情報に加えてアプリケーションの情報も収集する
E-3	脆弱性管理・対応	ネットワークやアセット情報と脆弱性情報を突き合わせシステムを把握、対応する
E-4	自動脆弱性診断	簡易な診断として、機械的な脆弱性診断を行う
E-5	手動脆弱性診断	より正確な診断として、手動による脆弱性診断を行う
E-6	標的型攻撃耐性評価	標的型メール訓練などにより高度な攻撃へに耐えられるか確かめる
E-7	サイバー攻撃対応力評価	サイバー攻撃対応訓練を行い、きちんと対処できるか確かめる

	F 脅威情報の収集および分析と評価	
	ネット上のセキュリティニュースやこれまでチームで見つけたインシデントを取りまとめ、次に生かすお仕事	
F-1	内部脅威情報の整理・分析	社内で発生したインシデントに関する情報を集めや長期的な改善案を整理する
F-2	外部脅威情報の収集・評価	公開されたセキュリティ情報を収集し、本対策の脅威がないか確認する
F-3	脅威情報報告	内部外部の脅威情報を定期的に取りまとめ報告する
F-4	脅威情報の活用	脅威情報を関係者へ展開し、みんなに活用してもらう

	G セキュリティ対応システム運用・開発	
	セキュリティ対応に必要なシステムを設置したり、管理したりするお仕事	
G-1	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品の設置や設定、その運用を行う
G-2	ネットワークセキュリティ製品高度運用	ネットワークセキュリティ製品のオプション機能などをより深的に活用する
G-3	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品の導入や設定、その運用を行う
G-4	エンドポイントセキュリティ製品高度運用	エンドポイントセキュリティ製品のオプション機能などをより深的に活用する
G-5	ディープアナリシス（深掘分析）ツール運用	フォレンジックやウイルス解析のためのツールを管理、運用する
G-6	分析基盤基本運用	SIEMなどに代表される分析用システムを導入、運用する
G-7	分析基盤高度運用	SIEMのカスタマイズや検知開発により、より高い性能を引き出す
G-8	既設セキュリティ対応ツール検証	すでにあるセキュリティ製品のバージョンアップ検証などを行う
G-9	新規セキュリティ対応ツール調査、開発	今後導入予定の新たなセキュリティ製品の資料作やトライアルなどを実施する
G-10	業務基盤運用	レポート生成や問合せ受付などの業務上必要なシステム運用する

	H 内部統制・内部不正対応支援	
	社内の内部統制や内部不正に関して、ネットワークやパソコン操作のログを提供、分析して、前携や法務を支援するお仕事	
H-1	内部統制監査データの収集と管理	内部監査などに必要なデータを集められるように、定期的にレポートする
H-2	内部不正対応の調査・分析支援	内部不正が発覚した際のログ情報の提供などを通し支援する
H-3	内部不正検知・防止支援	内部不正が起こる前にないよう、検知や防止ができないか検討する

	I 外部組織との積極的連携	
	社内社外問わず勉強会などへ参加したり、自ら催したり、セキュリティ仲間を増やすお仕事	
I-1	社員のセキュリティ対する意識啓発	実際のインシデント事例などをもとに社員へ意識啓発する
I-2	社内研修・勉強会の実施や支援	自分たちが得た知見を他の社員に対して広めていく
I-3	社内セキュリティアドバイザーとしての活動	開発部門などに対して、セキュリティの観点での助言や支援などを行う
I-4	セキュリティ人材の確保	人事と連携して人材の登用戦略化、流出防止施策などを行う
I-5	セキュリティベンダーとの連携	製品やサービスを提供するベンダーと良好な関係を築く
I-6	セキュリティ関連団体との連携	セキュリティ関連団体へ加盟し、情報共有、活用の輪を広げる

https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0_appendix.pdf

ハンドブック読んだよ！
ではまずは自組織の状況を把握
してから組織づくりしなきゃね！！

やったぜ！

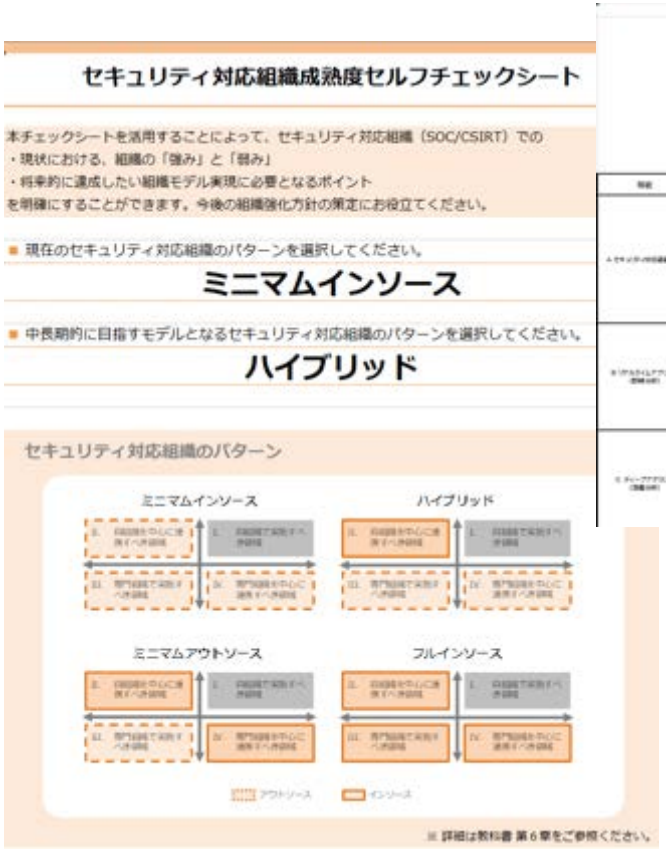
セキュリティ対応組織力

＝

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
ISOMM(ISOG-J SOC/CSIRT Maturity Model)



セキュリティ対応組織成熟度セルフチェックシート

本チェックシートを活用することによって、セキュリティ対応組織（SOC/CSIRT）での
・現状における、組織の「強み」と「弱み」
・将来的に達成したい組織モデル実現に必要となるポイント
を明確にすることができます。今後の組織強化方針の策定にお役立てください。

■ 現在のセキュリティ対応組織のパターンを選択してください。

ミニマムインソース

■ 中長期的に目指すモデルとなるセキュリティ対応組織のパターンを選択してください。

ハイブリッド

セキュリティ対応組織のパターン

※ 詳細は教科書 第6章をご参照ください。

あなたのセキュリティ対応組織における"機能別"成熟度

201X/YY/ZZ

機能	成熟度
A. セキュリティ対応組織運営	3.0 /5
B. リアルタイムアナリシス（即時分析）	4.0 /5
C. ディープアナリシス（深掘分析）	4.0 /5
D. インシデント対応	4.0 /5
E. セキュリティ対応状況の診断と評価	3.0 /5
F. 脅威情報の収集および評価と分析	3.0 /5
G. セキュリティ対応システム運用	3.9 /5
H. 内部統制/内部不正対応支援	3.0 /5
I. 外部組織との積極的連携	4.0 /5

現状のセキュリティ対応組織の強み

B. リアルタイムアナリシス（即時分析）
各種システムで収集される情報をもとに、即時性の高い分析が行われ、迅速で適切なインシデント対応に繋げられています。実務レベルにおいては問題のない状況と言えますが、より組織的な高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。

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、深い分析が行われ、インシデントの全容解明と影響の特定に繋げられています。実務レベルにおいては問題のない状況と言えますが、より組織的な高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

H. 内部統制/内部不正対応支援
内部統制、内部不正に関する対応の支援を十分行えておらず、ガバナンスやコンプライアンス面で貢献しにくくなっています。組織的に機能していない部分が多いので、業務の棚卸、改善が必要となります。

F. 脅威情報の収集および評価と分析
組織内外の脅威情報収集、活用が満足に行えており、各種分析、インシデント対応など、他の機能の改善につなげられていません。組織的に機能していない部分が多いので、業務の棚卸、改善が必要となります。

https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1_maturity-checklist.xlsx

ISOMMの使い方

ISOMMの使い方概要

1. セキュリティの対応の全体を知る
2. 自組織でどこを対応するか決める
3. 自組織の現在のパターンを知る
4. 今後どんなパターンになりたいかを決める
5. 現在の範囲でどこまでできているかをする
6. チェック結果を見て、どこを強化するかを決める

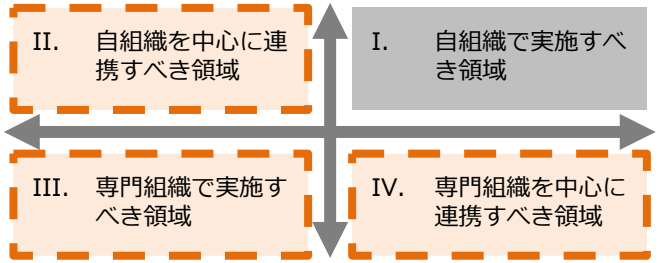
① 組織パターンの設定

セキュリティ対応組織パターンを自覚する（教科書を参考）

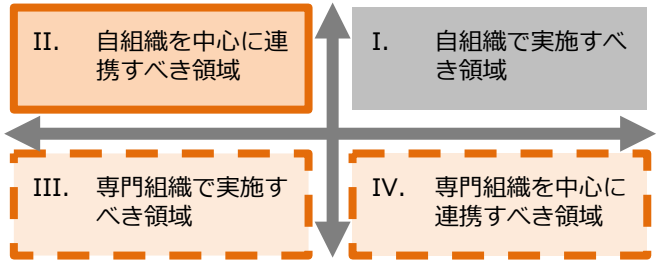
役割を専門性や組織の内外で四象限に整理

セキュリティ対応組織パターンを自覚する（教科書を参考）

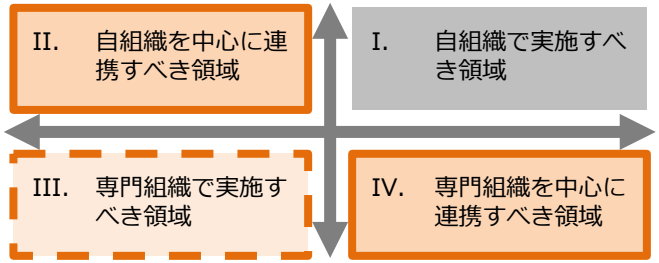
ミニマムインソース



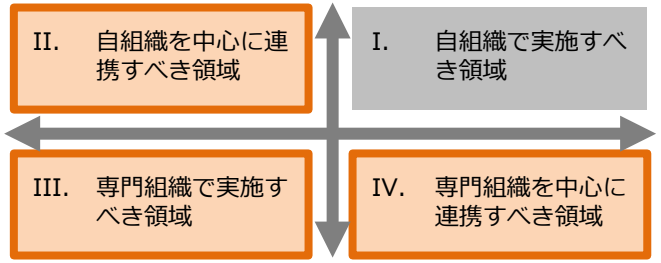
ハイブリッド



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

セキュリティ対応組織成熟度セルフチェックシート

本チェックシートを活用することによって、セキュリティ対応組織（SOC/CSIRT）での
・現状における、組織の「強み」と「弱み」
・将来的に達成したい組織モデル実現に必要となるポイント
を明確にすることができます。今後の組織強化方針の策定にお役立てください。

■ 現在のセキュリティ対応組織のパターンを選択してください。

ハイブリッド

■ 中長期的に目指すモデルとなるセキュリティ対応組織のパターンを選択してください。

ミニマムアウトソース

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

機能	役割		領域	インソース 0	1	2	3	4	5	アウトソース 0	1	2	3	4	5	備考
				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	サービス内容と得られる結果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	※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。
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	○	○	○	○	○	○	○	○	○	◉	○	○	
				◉	○	○	○	○	○	○	○	○	○	○	○	

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。

スコアの付け方

	インソース	アウトソース
0	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	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
1	実施できていない	結果や報告を確認できていない
2	運用が明文化されておらず、担当者が業務を実施できる	サービス内容と得られる結果を理解できていない
3	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	サービス内容、得られる結果のいずれかが理解できていない
4	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	サービス内容と得られる結果を理解できているが、想定未満
5	明文化された運用はCSIOなど権限ある組織長に承認されている	サービス内容と得られる結果を理解でき、想定通り

チェック時のFAQ

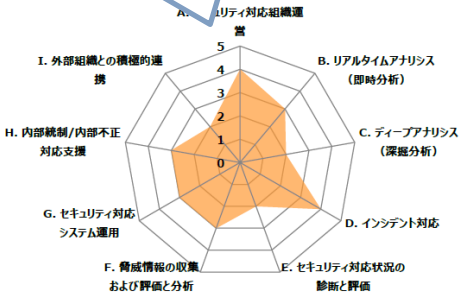
- 判断も何もせずに、「何もしていない」場合は1点
- 現状が把握できておらず、わからない場合も1点
- チェックする立場により評価が変わります。
  立場の違いによる認識の差を可視化できますので、
  気にせずチェックしましょう
- 最近できた組織では「わからない」や「できていない」
  のは当然です。ありのままをチェックして見ましょう

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　組織における"機能別"成熟度　J1X/YY/ZZ



現状の組織（ハイブリッドパターン）における機能　と評価しています。
組織の「強み」と「弱み」を抽出し、現在のセキュリ　有効に働いている機能と、
改善が必要な機能を見える化しています。
マクロな観点での指標として、成熟度向上の方針策定　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　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

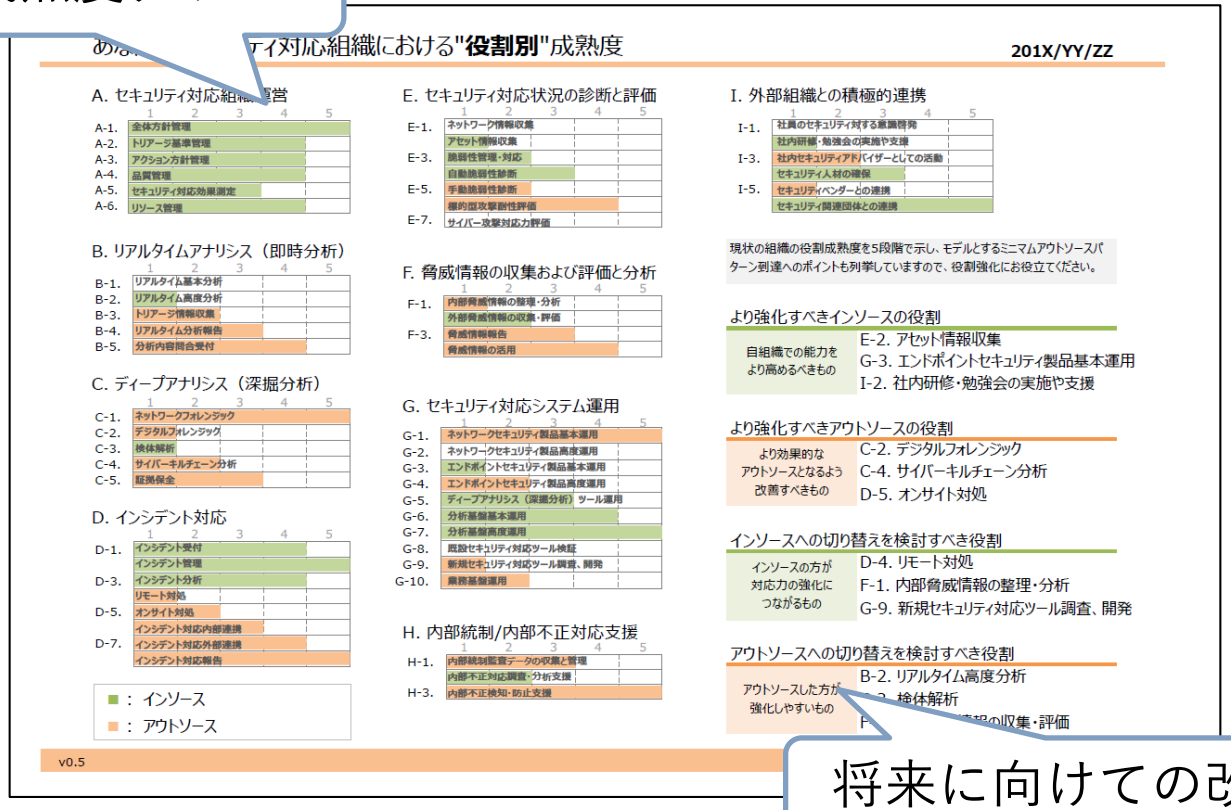
C. ディープアナリシス（深掘分析）
被害状況調査、攻撃手法分析など、深い分析が行い切れておらず、インシデントの全容解明と影響の特定が不十分になっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

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　を見直してください。

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

組織による結果の傾向

- ２，３年で担当が入れ替わる組織では、
  担当が変わった直後では出る点数が低めの傾向です
- 管理職やリーダーの採点では高めに、担当の方の
  採点では低めになる傾向です
- アウトソースしている項目は高めに点がつく傾向です

こんな方に気軽に使って頂きたい

組織の管理者やリーダー

業務設計や役割分担の観点から、どこをやるか知りたい

現場の担当者

自分たちがどの範囲を担当しているかの業務役割の認識に

1人CSIRTや1人情シスの方

セキュリティの対応として現在どこまでやっているかの把握に

ISOMMの活用方法

- 気軽に誰でもチェックできる
- 組織の業務で抜けや漏れがないか見つける
- 組織内の業務認識のギャップを見つける
- 弱い部分の強化方針を決める

さらなる活用へ！

- アウトソースに対しての費用対効果を測る
- 他の観点の成熟度も利用して多面的に測る
- この結果を第三者のアセスメントと合わせて評価に利用する

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。

「セキュリティ対応組織強化のための情報共有の5W1H」の実体的なフローの紹介

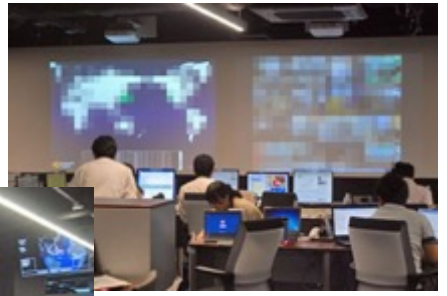
講演者

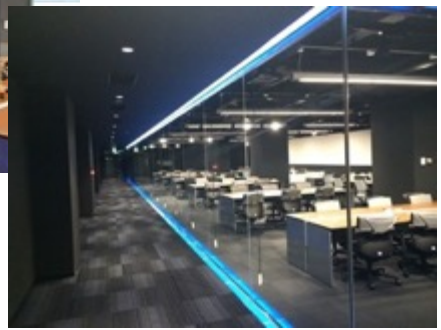
- 河島　君知　です。
  - NTTデータ先端技術株式会社　セキュリティ事業部
  - JNSAのISOG-J運営委員

2003年　セキュリティ監視業務

セキュリティインシデント対応
セキュリティ製品開発
セキュリティサービス企画・開発・立上

現在　セキュリティ対応組織構築支援





Itmediaエグゼクティブ様取材記事より

このセッションは？

- 昨年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」**」を振り返る。
- 「**セキュリティ対応組織の教科書**」で解説したインシデント対応フローに基づきサイバーセキュリティ情報共有の流れを考察する。
- **「情報共有基盤」の構築検討や、情報共有フォーマットを提案するものではありません。**

資料URL
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v1.0
http://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.html
セキュリティ対応組織の教科書v2.1
https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

なぜ今、情報共有が課題なのか

（数年前より）CSIRT設立がブーム

1人では専門家のように情報収集活動ができない

どうやったら情報収集できるかが課題

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を活用して、
情報を集めようとしましたよね

情報は溢れかえるように増えてきましたが
CPUの脆弱性Meltdown/Spectreの件、
Strutsに続くDrupalの件、
現場、経営層で情報錯綜しませんでしたか？
必要となる情報を確認してみましょう。

情報の受け渡し内容を明確にする

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？

自分からも発信者になれるように心がけよう！

参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P2

共有情報を用いたセキュリティ対応の流れ（Why&When）

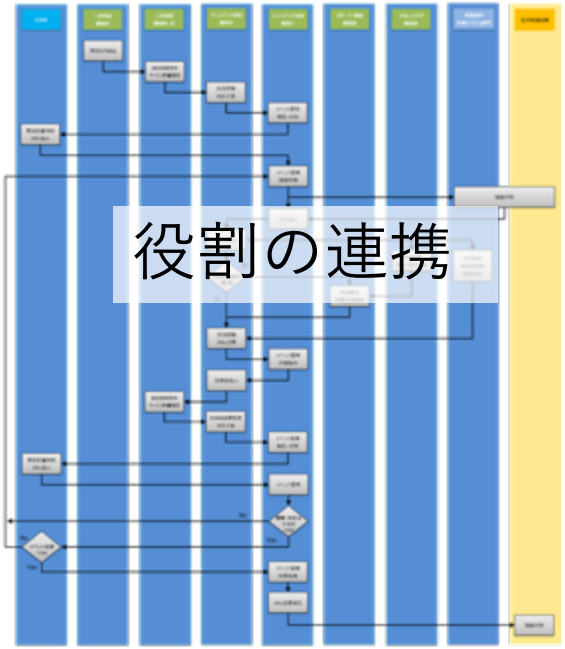
参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

では、実際の共有情報はどのように活用されるのか？
セキュリティ対応組織の教科書v2.1での
インシデント対応フローを用いて
情報共有のながれを考えてみましょう。

セキュリティ対応組織の教科書v2.1
https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

インシデント(有事)の対応例

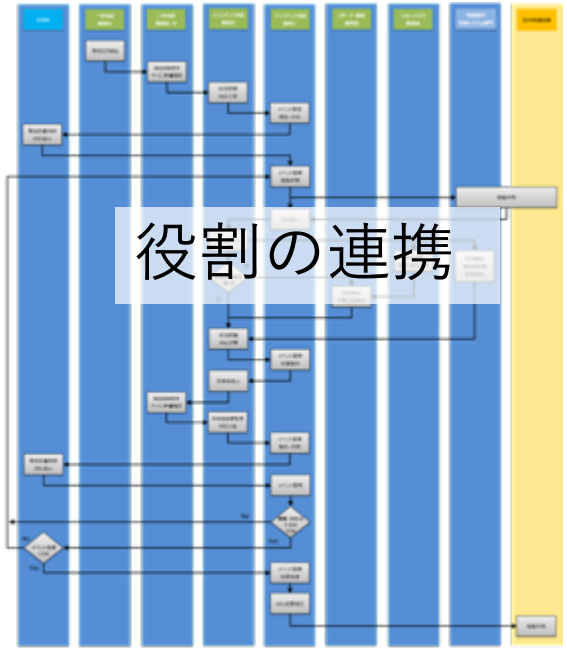
役割ごとのインシデント対応例をフローで紹介

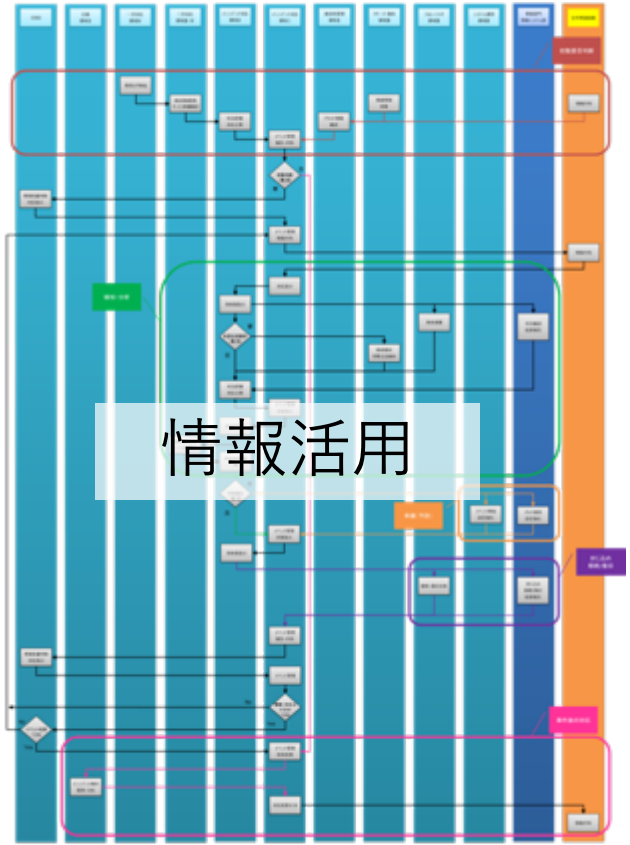


セキュリティ対応組織の教科書v2.1 https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

インシデント(有事)の対応例

情報共有フェーズを意識したフロー





インシデント対応に活躍する９つの機能（Who）

A. セキュリティ対応組織運営

D. インシデント対応

G. セキュリティ対応システム運用・開発

B. リアルタイムアナリシス（即時分析）

E. セキュリティ対応状況の診断と評価

H. 内部統制・内部不正対応支援

C. ディープアナリシス（深堀分析）

F. 脅威情報の収集および分析と評価

I. 外部組織との積極的連携

脆弱性のおさらい：Drupalの場合

Drupal™

Drupal 7 and 8 core highly critical release on March 28th, 2018 PSA-2018-001

Posted by Drupal Security Team on *21 Mar 2018 at 19:13 UTC*

- Advisory ID: DRUPAL-PSA-2018-001
- Project: Drupal Core
- Version: 7.x, 8.x
- Date: 2018-March-21

Description

There will be a security release of **Drupal 7.x, 8.3.x, 8.4.x, and 8.5.x on March 28th 2018 between 18:00 - 19:30 UTC**, one week from the publication of this document, that will fix a highly critical security vulnerability. The Drupal Security Team urges you to reserve time for core updates at that time because exploits *might* be developed within hours or days. Security release announcements will appear on the Drupal.org security advisory page.

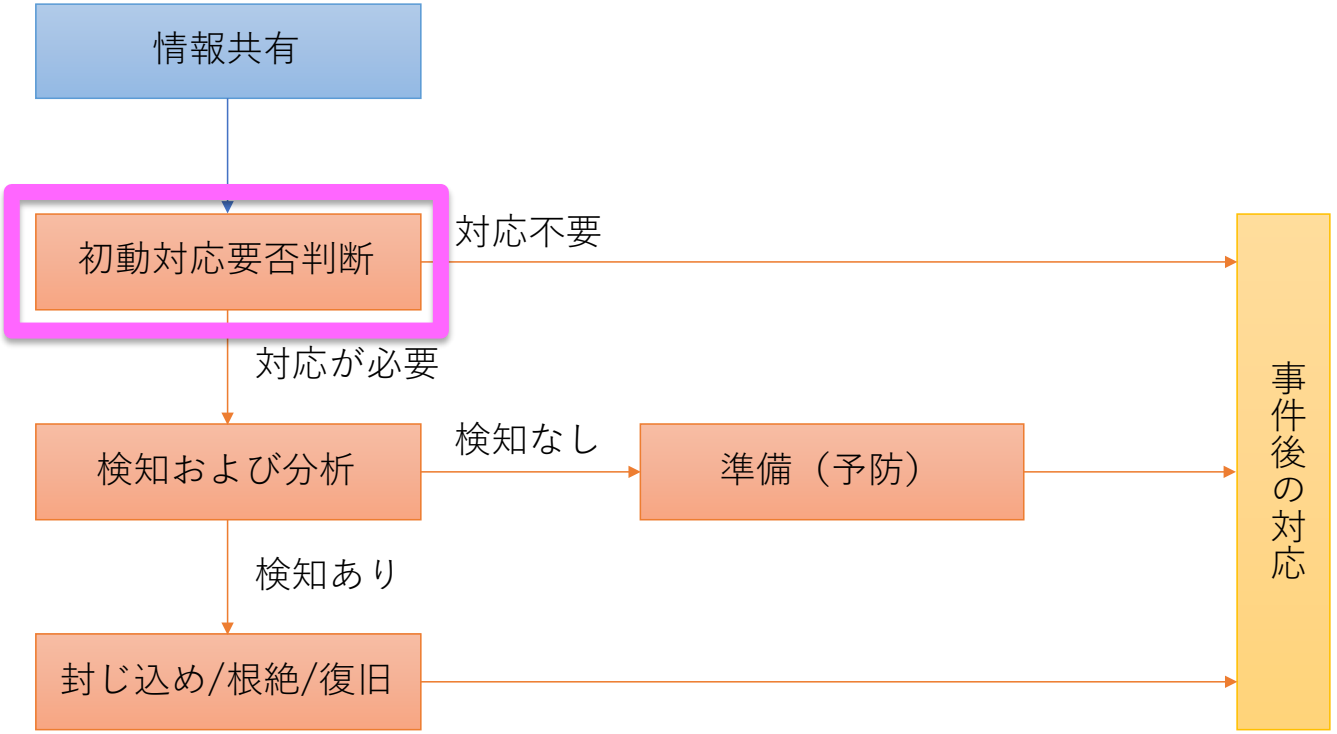
２０１８/３/２１
Drupal に非常に危険な脆弱性があることを公表

パッチは２０１８/３/２８に公開予定

脆弱性のおさらい：Drupalの場合

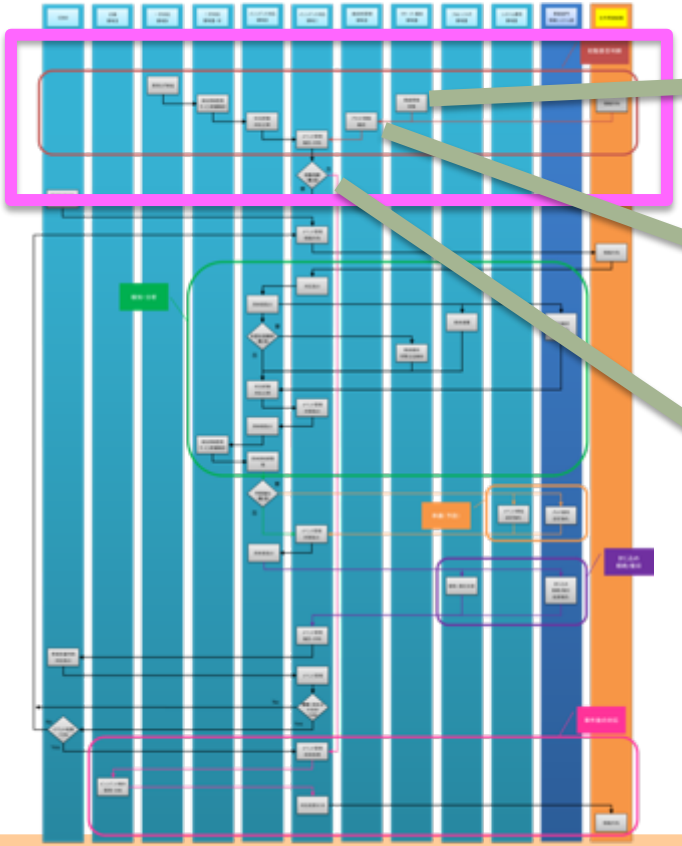
©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

共有情報を用いたセキュリティ対応の流れ（Why&When）



参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

初動対応



Who

F. 脅威情報の収集および分析と評価

E. セキュリティ対応状況の診断と評価

D. インシデント対応

初動対応

What

- 脆弱性識別子(CVEやパッチ番号など)
  → Drupalの遠隔コード実行の脆弱性
  CVE-2018-7600

- 脆弱性の対象：システム種別 / バージョン / 条件(システム構成、設定など)
  → サポート内　Drupal 7.58未満、Drupal 8.5.1未満
  サポート外　Drupal 6.x 、Drupal 8.4.x以前

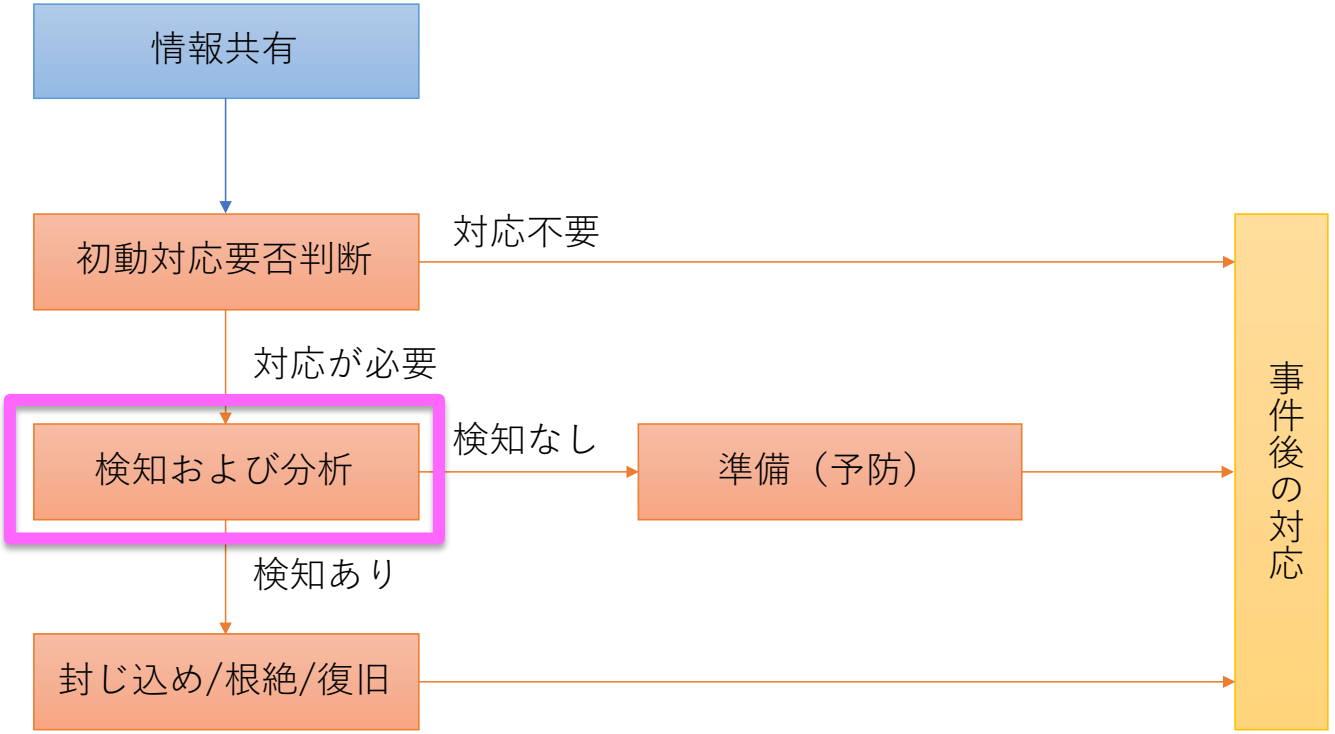
EOLのVerが含まれる

How

- 各セキュリティ製品における対応状況
  → ＩＤＳ、ＦＷ，ＷＡＦなどで対応シグネチャの有無

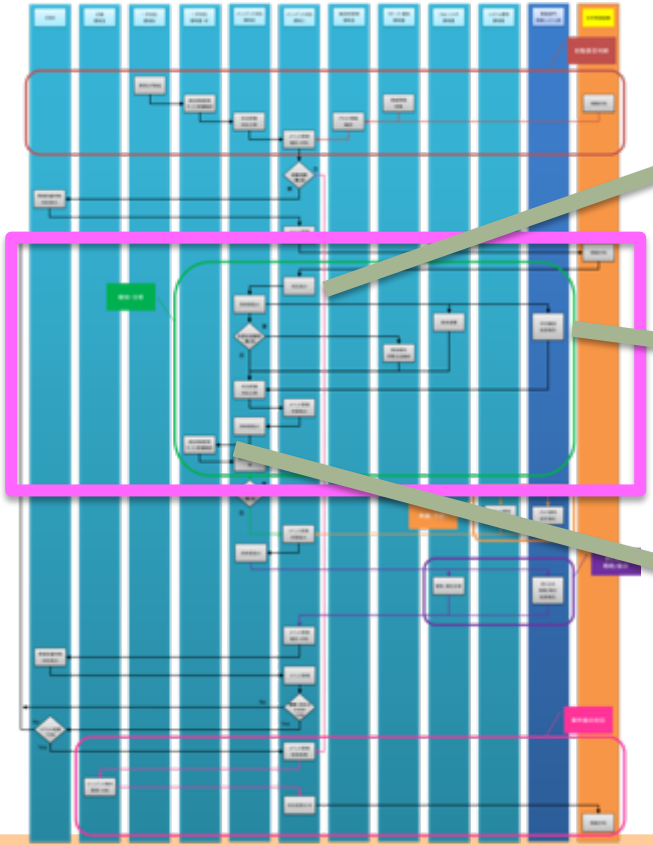
情報が少なく防ぎ方が不明

共有情報を用いたセキュリティ対応の流れ（Why&When）



参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

検知および分析



Who

D. インシデント対応

X. 事業部門・システム運用部門

B. リアルタイムアナリシス
（即時分析）

検知および分析

パッチの提供が1週間後

What

- 攻撃の特徴(攻撃コードなど)
  → パッチから攻撃コードを類推
  攻撃実証コードを参照
- 検知するための手段
  → ＨＴＴＰリクエスト内の特定文字列

パッチの提供から2週間後に攻撃実証コードが公開

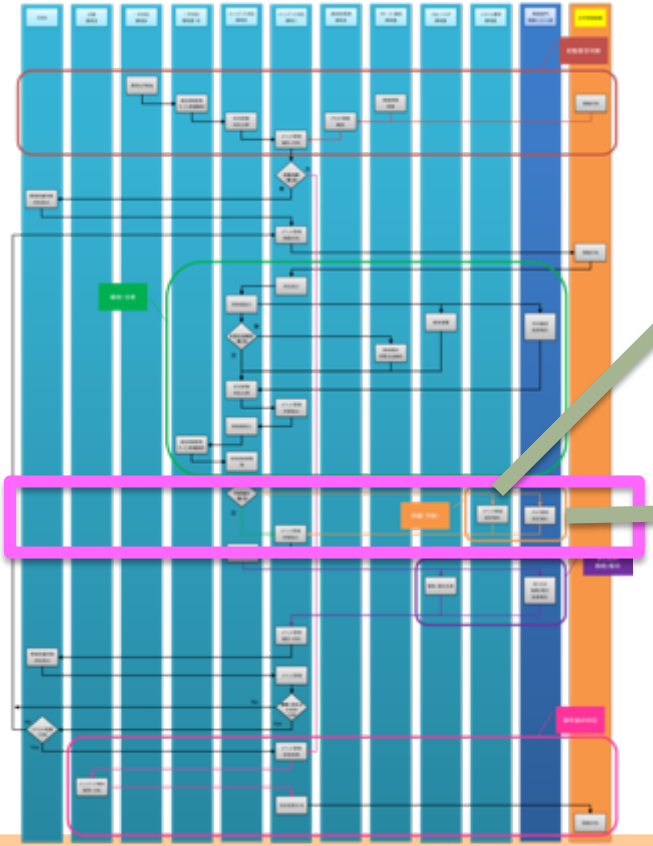
How

- 各セキュリティ製品における対応状況
  → ＩＤＳ、ＦＷ，ＷＡＦで提供されているシグネチャを利用
  提供されていない場合は、カスタムシグネチャを作成

共有情報を用いたセキュリティ対応の流れ（Why&When）

参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

準備（予防）



Who

G. セキュリティ対応システム
運用・開発

X. 事業部門・システム運用部門

準備（予防）

What

- 攻撃を検知・遮断するための手段
  → ＨＴＴＰリクエスト内の特定文字列（検知および分析と同様）
- パッチ
  → Drupal core - Highly critical - Remote Code
  https://www.drupal.org/sa-core-2018-002

Dlupalの使ったサービス保有の有無が不明

How

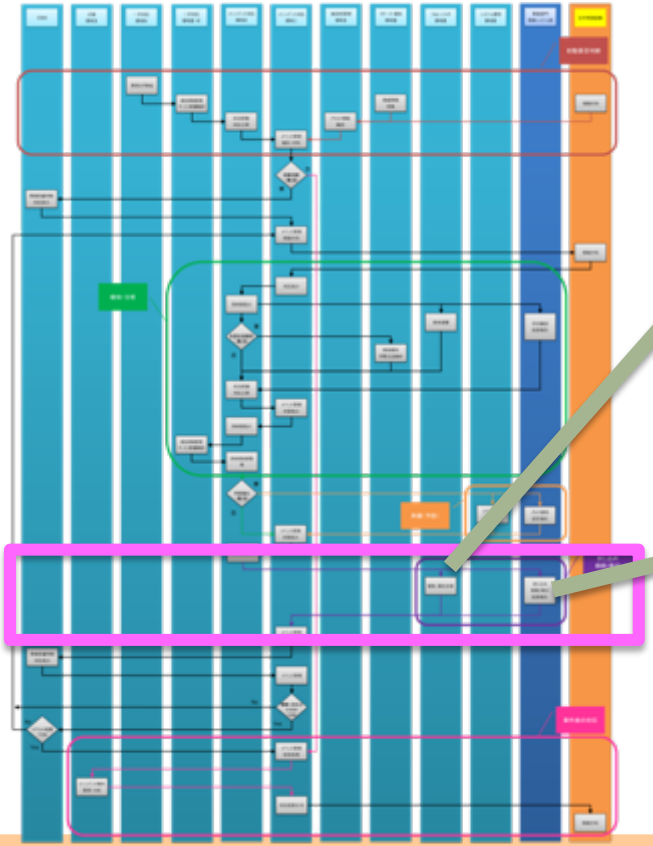
- 各セキュリティ製品での検知・遮断
  → ＩＤＳ、ＦＷ，ＷＡＦでシグネチャを適用
- 攻撃を無効化
  → 脆弱なＤＲＵＰＡＬへのパッチ適用

経験が少なくセキュリティパッチ適用の影響が不透明

共有情報を用いたセキュリティ対応の流れ（Why&When）

参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

封じ込め/根絶/復旧



Who

C. ディープアナリシス
（深堀分析）

X. 事業部門・システム運用部門

封じ込め/根絶/復旧

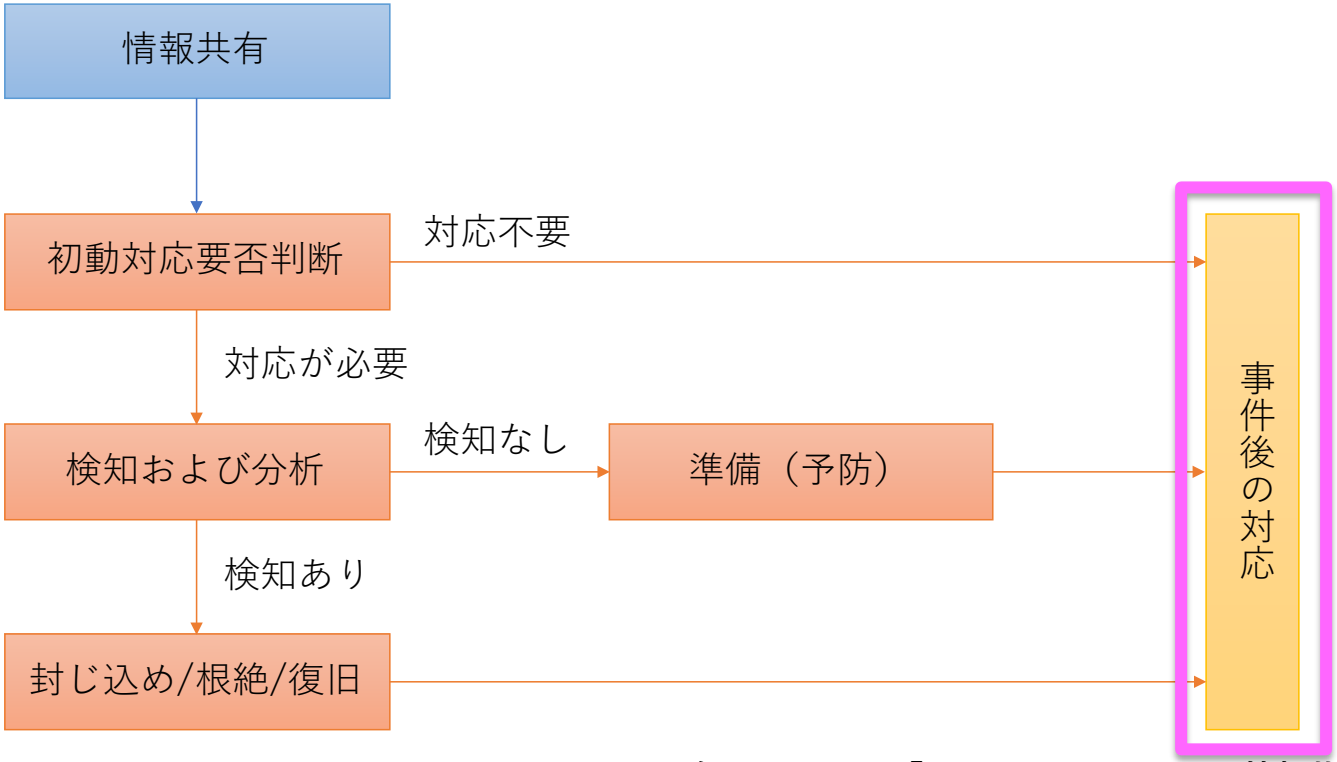
What

- 攻撃によって残る痕跡の調査
  → 被害を受けた後の通信内容
  サーバやクライアントに残るログや特徴的な変化

How

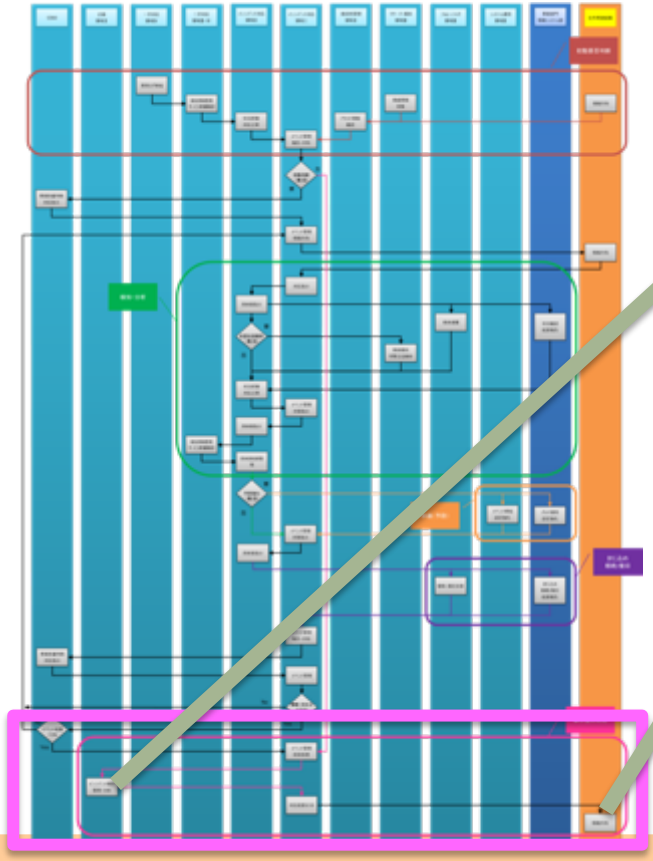
- 各セキュリティ製品での検知・遮断
  → ＩＤＳ、ＦＷ，ＷＡＦでシグネチャを適用（準備と同様）
- 攻撃を無効化
  → 脆弱なＤＲＵＰＡＬへのパッチ適用（準備と同様）
- 被害を受けたシステムの復旧
  → バックアップからのリストアなど

共有情報を用いたセキュリティ対応の流れ（Why&When）



参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

事件後の対応



Who

F. 脅威情報の収集および分析と評価

I. 外部組織との積極的連携

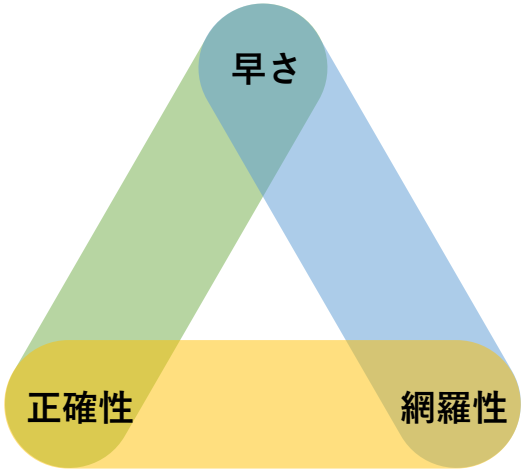
まとめ

- 「**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」**」を振り返りました。

- 「**セキュリティ対応組織の教科書**」で解説したインシデント対応フローに基づきサイバーセキュリティ情報共有の流れを考察しました。

- 最後に・・
  情報共有のトライアングル（ジレンマ）のご紹介

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

「セキュリティ対応組織強化のための情報共有の5W1H」の英語版の紹介

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、宴会調整
  - IIJ-SECT (CSIRT)、関連団体 (ISOG-J, ICT-ISAC など)、コミュニティ (Vuls など)
  - 食べ物、ヘヴィメタル、ねこ



- SOC 見学やってます
- セキュリティ情報発信
  - wizSafe Security Signal
  - IIR, IIJ Security Diary, IIJ Engineers blog
    - IIR Vol.40 の記事を書きました

IIJ-SECT
IIJ Group Security Coordination Team
wizSafe
安全をあたりまえに

5W1H 文書、2月に英語版をリリースしました！

- リリース後、各所からの要望を受け…英語版を作成！
  - ISOG-J 初の英語文書リリース
- Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT
  - 英語では “6W” になるんですね…
  - 「セキュリティ対応組織」の部分はいい感じにならず… SOC/CSIRT としました
- 翻訳: Ryu Hiyoshi (NTT Security)

5W1H 文書をまるごと英語化

Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT

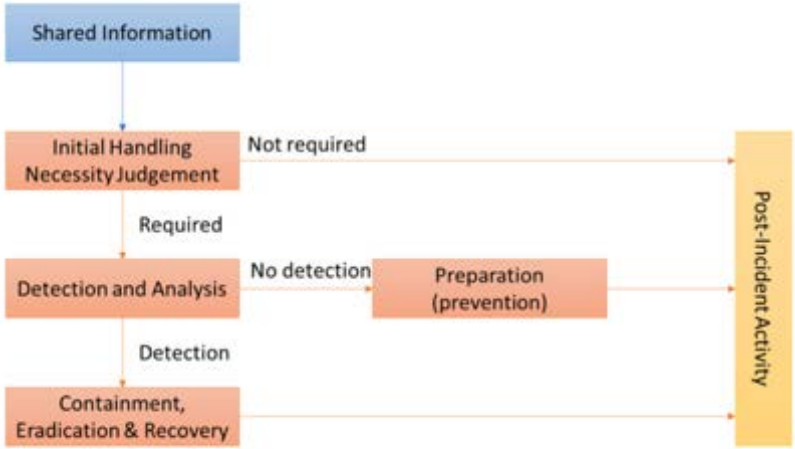


Figure 3 : Incident handling triggered by shared information

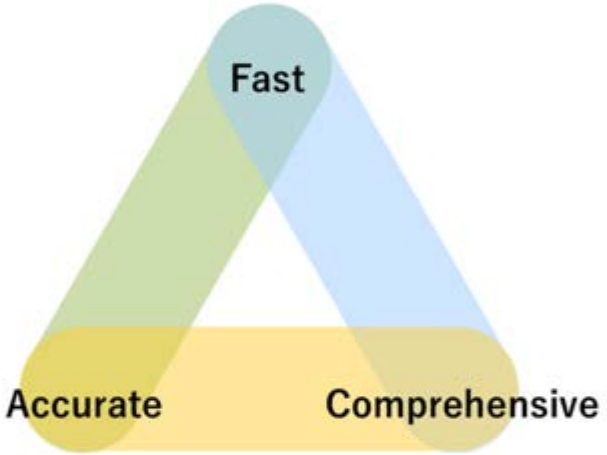


Figure 4 : Triangle in information sharing

In short, this figure says that only two of accurate, comprehensive, and fast could be realized at once. In other words, it could be summarized as follows:

[11] 27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)
[12] https://www.first.org/resources/papers/conf2015/first_2015-rasmussen-rod_cutting-through-cyberthreat-intelligence-noise_20150615.pdf

海外カンファレンスで広報(1)

Information Security Operation providers Group Japan ISOG-J

What is ISOG-J

- the Information Security Operation providers Group Japan
  - established 2008
  - ISOG-J is a professional community for security operation providers
  - a forum to share information about security operation and resolve common issues.
- ISOG-J's pronunciation is "ee-sog-jay"
  - the meaning is "Got to hurry, Japan!"
- http://isog-j.org/e/

APRICOT 2018
APNIC 45
KATHMANDU NEPAL
19 – 28 February 2018

Information Security Operation providers Group Japan ISOG-J

ISOG-J member growth

ISOG-J Working Groups (1)

peration Guideline WG
te with OWASP Japan
entesters' skill map and syllabus
peration Technology WG
te friendship among the members
nternal seminar of technical topics, then drink together
these timetable "sub part" and "main part"
to join only "main part" :D

©ISOG-J

tection, Eradication & Forensic: Cyber Threats Intelligence Model for CNII Organizations

Information Security Operation providers Group Japan ISOG-J

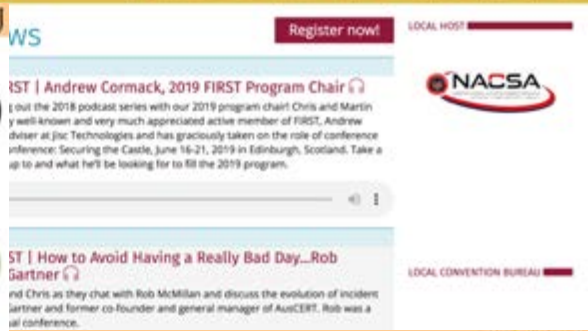
海外カンファレンスで広報(2)

LT: ISOG-J publishes "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT."

Yasunari Momoi momo@iij.ad.jp
Internet Initiative Japan Inc. / ISOG-J

FIRST Annual Conference 2018

Difference between each phases



the point of this Six Ws document

- the basics of security information sharing for members of SOC/CSIRT
- Why mismatches when sharing information?
  - rethinking back to basics

	Submitter	Receiver
Who	who will	who will
What	what information	what information
Where	in which medium for sharing	from which medium for sharing
When	in which phase	in which phase
Why	for what objective	for what objective
How	in what manner	in what manner
	submit information	utilize information

Table 1 : Six Ws in cybersecurity information sharing

そして…

- 5W1H 文書改め 6Ws 文書の紹介で
  ちょっと困ったこと…

- 参照元が日本語しかないものが
  いっぱい！
  - 外部ドキュメントはまあしょうがない
  - 「セキュリティ対応組織の教科書」を
    たくさん参照している…
    - というか、内容もだいぶ依存している…

もうちょっと英語版をなんとかしよう！

- 教科書…は正直厳しい
  - チェック項目リストだけでも英訳してみた
    - セキュリティやってたら雰囲気はわかる(はず)
  - 概略を作って、模式図を多くして英語版を…
- あ…ハンドブック？
  - これを英語にする？
- 乞うご期待！

F. Threat Information Collection, Analysis and Evaluation / 脅威情報の収集および分析と評価
F-1. Internal Threat Intelligence / 内部脅威情報の整理・分析
F-2. External Threat Intelligence / 外部脅威情報の収集・評価
F-3. Reporting / 脅威情報報告
F-4. Using Threat Intelligence / 脅威情報の活用

G. Systems Development and Operation / セキュリティ対応システム運用・開発
G-1. Basic Operation of Network Security Devices / ネットワークセキュリティ製品基本運用
G-2. Advanced Operation of Network Security Devices / ネットワークセキュリティ製品高度運用
G-3. Basic Operation of Endpoint Security Products / エンドポイントセキュリティ製品基本運用
G-4. Advanced Operation of Endpoint Security Products / エンドポイントセキュリティ製品高度運用
G-5. Operation of Tools for Deep Analysis / ディープアナリシス(深掘分析)ツール運用
G-6. Basic Operation of Analysis Systems / 分析基盤基本運用
G-7. Advanced Operation of Analysis Systems / 分析基盤高度運用
G-8. Verifying Existing Security Products and Tools / 既設セキュリティ対応ツール検証

JNSA発行「CISOハンドブック」の紹介と現場レベルでの活用について

講演者

- 田中　朗（たなか　あきら）　（ISOG-J フェロー）
  - 某社でCISOというセキュリティ責任者やってます

1980年代、1990年代　メーカの研究所でソフトウェアの研究・開発
　　プログラミング色々、JUNETからWIDEの変化をすぐそばで
1998年　セキュリティ事業立上げ、顧客向けのMSS(Managed Security Service)提供
2011年　ISOG-J活動に参加
2015年　社内CSIRT設立、その後CSIRTリーダー
2016年　JNSA　CISO支援WG
2018年　ユーザ企業に転職

CISOハンドブック（２０１８年5月公開）


CISO ハンドブック

業務執行として考える情報セキュリティ

Ver. 1.1β

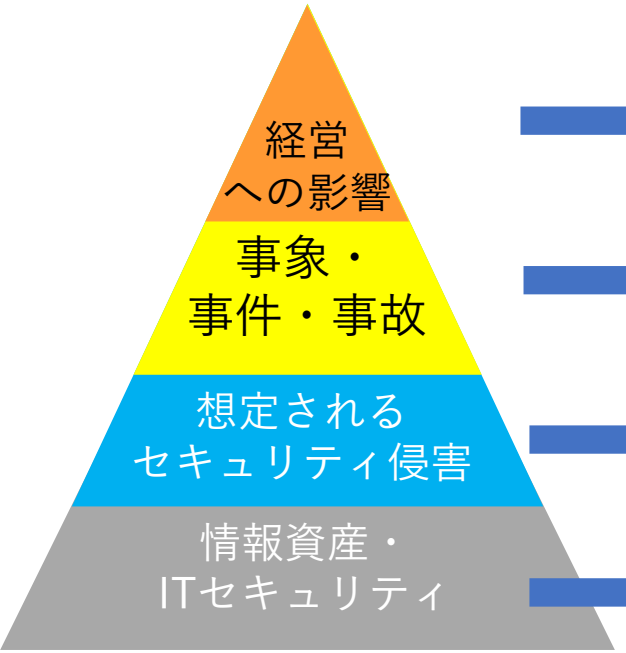
特定非営利活動法人　日本ネットワークセキュリティ協会
社会活動部会　CISO 支援ワーキンググループ

2018 年 6 月 22 日（1.1β）
2018 年 4 月 27 日(1.0β)

- 経営会議で資料を作る際のひな型として
- 技術担当からCISOになった人がビジネスを理解するための参考として
- セキュリティ経験の少ないCISOがセキュリティ業務を理解するための参考として
- 経営会議で話される業務執行（CISOの役割と責任、業務）の概要を理解する参考として
- ビジネスに関連付けた計測項目と判断基準の例として
- ビジネスに沿ったセキュリティ計画や、事業継続計画の策定の資料として

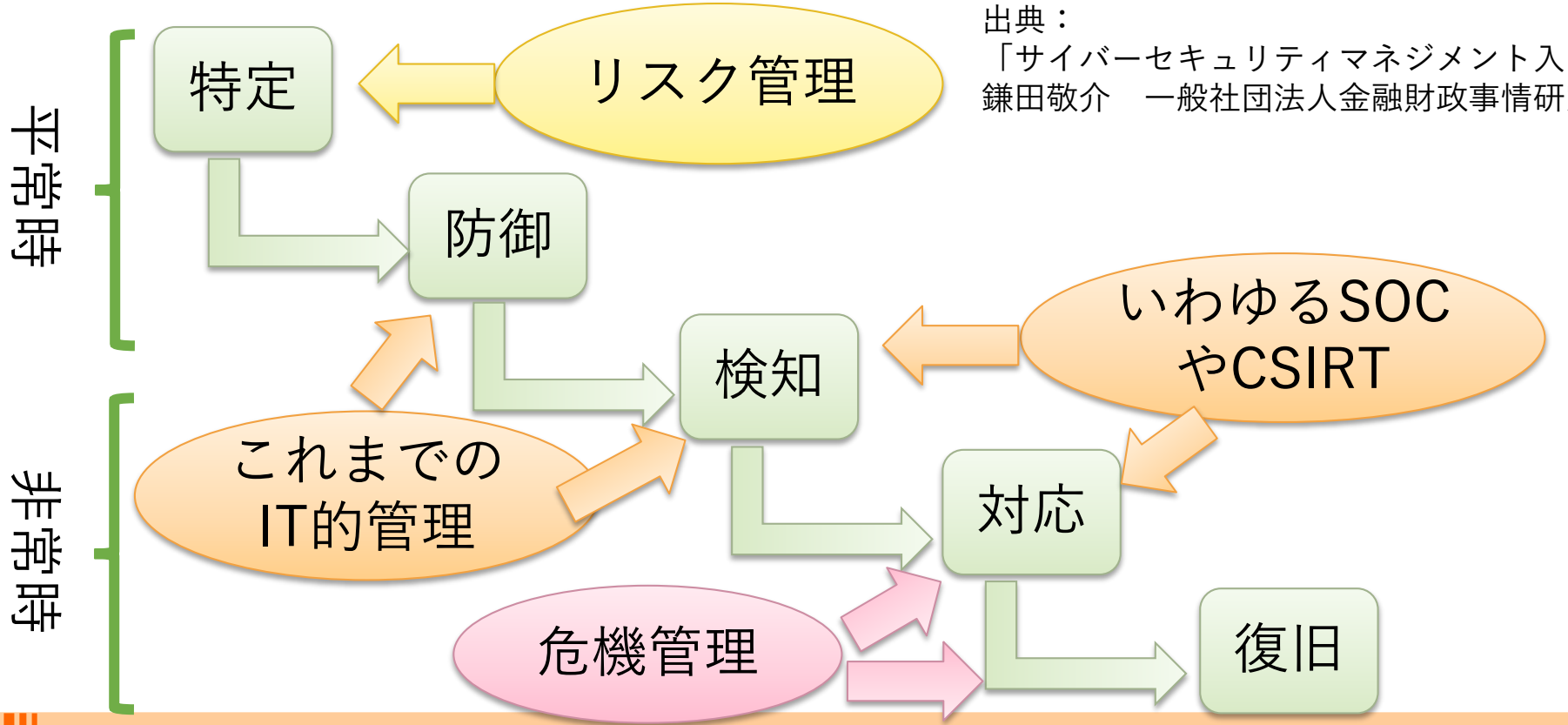
https://www.jnsa.org/result/2018/act_ciso/index.html

ビジネスリスクとセキュリティリスクの関係



Confidentiality（機密性）	Integrity（完全性）	Availability（可用性）
競合優位性の低下：競合の躍進、評判の低下 費用的な損失：損害賠償、営業機会損失 事業への影響：営業停止		
ストーキング 秘密の暴露 スパイ行為	システム誤作動 偽の発注・契約 紛争の誘発	システムの停止 社員間の連絡できない 社外との連絡できない 売上が立たない
利用状況の漏洩 画像・音声の漏洩 踏み台による漏洩	プログラム等の改ざん データの改ざん	プログラム等の改ざん 制御データの改ざん 通信経路の遮断
ソフトウェアの脆弱性 設定の不備 プロトコルや暗号の不備 ネットワークや通信の不備		運用上の不備 利用者による改造 認証の不備 ワーム・ウィルス

サイバーセキュリティフレームワーク



出典：
「サイバーセキュリティマネジメント入門」
鎌田敬介　一般社団法人金融財政事情研究所

サイバーセキュリティフレームワーク（つづき）

機能の一意の識別子	機能	カテゴリーの一意の識別子	カテゴリー
ID	特定	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスク管理戦略
PR	防御	PR.AC	アクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	伝達
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	伝達

機能	カテゴリー	サブカテゴリー	参考情報
特定（ID）	資産管理（ID.AM）：組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。	ID.AM-1: 企業内の物理デバイスとシステムの一覧を作成している。	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: 企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: 企業内の通信とデータの流れの図を用意している。	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: 外部情報システムの一覧を作成している。	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: リソース（例：ハードウェア、デバイス、データ、ソフトウェア）を、分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: すべての従業員と第三者である利害関係者（例：供給業者、顧客、パートナー）に対して、サイバーセキュリティ上の役割と責任を定めている。	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

出典：IPA 重要インフラのサイバーセキュリティを 向上させるためのフレームワーク
https://www.ipa.go.jp/files/000038957.pdf

CISO ダッシュボード：業務執行としてのセキュリティ

CSIRTではなく、業務執行としてのセキュリティ

Governance	CISOが果経営会議で報告すべきたすべきガバナンス ＝業務執行に関わる事項
Risk	Risk = ≒ *f(Attack condition, Protect condition, suspicious activity, Indirect activity)* Security and Risk condition

Attack

1. Attack condition
攻撃検出状況に関するKPI

AV/IDS等による検出
セキュリティ製品のアラート等
攻撃などに関する情報

2. Protect condition
対策状況に関するKPI

ウィルス対策, システムバージョン、パッチ、コンフィグレーション等、セキュリティ対策として実施すべき項目の適用率等
脆弱性情報

3. Suspicious activity
侵入が疑われる状況のKPI

SIEM/ATA/WDATP等による検出や、その他の侵入が疑われるもの
内部犯行を含んだ、疑わしいイベント

4. Indirect activity
人事的、物理的等、直接ITとは関係しない状況のKPI

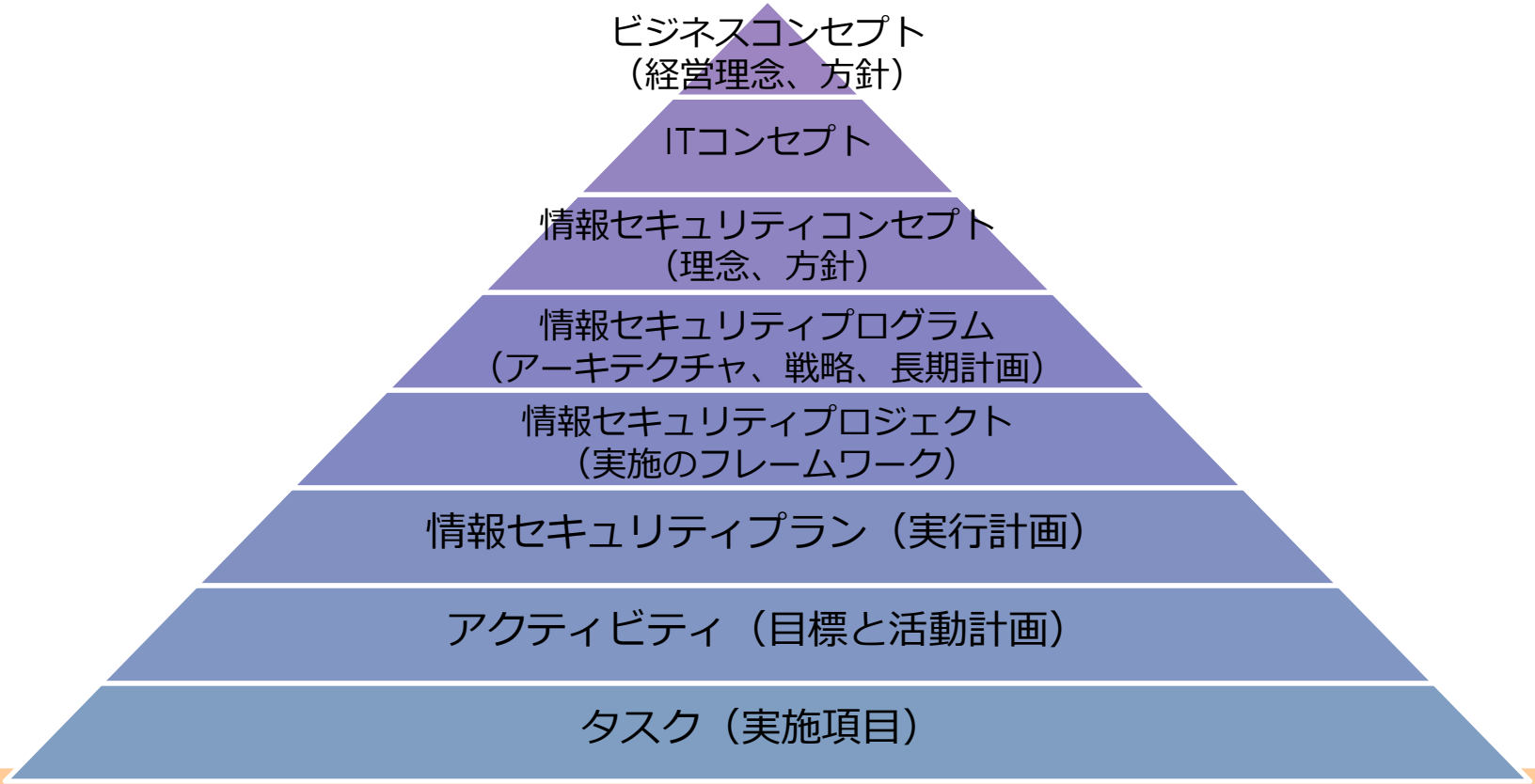
退職者、PCやデバイスの紛失・盗難
外部からのインテリジェンス

経営会議で何を報告すべきなのか
どのように決裁を仰ぐべきなのか

セキュリティ報告書（XX年度XX月　経営会議向け）

			備考
Attack condition	技術的	2	弊社を狙ったと思われる攻撃メールが、XX月XX日-XX月XX日にかけて、SPAMフィルターとAVで検知された。総数は、23件で、開発の特定部門に集中している。現段階では、全てブロックできたと判断しているが、警戒を続ける必要がある
	概況的	1	海外で大規模なインシデントが報道されているが、報道を見る限り対策済みの手法と判断される（別紙１）
Protect condition	技術的	2	先月から配布されたPCのキッティングに問題のある事が判明。既に回収をしているが、まだ最終確認がとれていない。XX月XX日までに狩猟予定。一部業務に影響が出るが、協力をお願いしたい。
	概況的	1	ネットワークデバイスへの深刻な脆弱性*xxxが報告されているが、弊社では使用していないことが確認されている（参考資料2）
Suspicious activity	技術的	3	外向けの通信に、不審な接続先との通信が記録されている。現在詳細を分析中だが、大規模な調査が必要となる可能性がある。上記攻撃メールとの関連も疑われるため、早急な調査が必要。 分析を早め、より効果的な防御を行うためには、より精度の高いブラックリストの入手が効果的と考えている(**別紙2：決済申請**)
	概況的	2	データベース保守を担当するベンダーが懲戒解雇となっている。プロシージャに沿ってアカウントなどの停止を実施した。
Indirect activity	技術的	2	1台のPCと、2台の会社貸与スマホが紛失。リモートワイプで対策済み
	概況的	1	経済産業省から、「サイバーセキュリティ経営ガイドライン」が公表され、注目されている。IT/セキュリティ部門では展開済み。 当ミーティングでコピーを配布します

情報セキュリティ計画フェーズの実施モデル



CISOとセキュリティ対応組織の連携

CISOの役割

- セキュリティポリシーを策定する。
- サイバーセキュリティリスク管理体制を構築する。
- 自社のサイバーセキュリティリスクを把握し、リスク対応計画を策定する。
- 対策実施に掛かる費用について経営層の承認を得る。
- 構築した体制を維持、改善するためのPDCAサイクルを統括、監督する。
- インシデント対応の陣頭指揮を執る。
- 新規IT導入時等、事業部門に対するセキュリティの技術的観点からのアドバイスをする

等

出典：IPA「サイバーセキュリティフレームワーク経営ガイドライン解説書」

CISOとセキュリティ対応組織の連携

- セキュリティ対応組織（SOC,CSIRT)の役割
  - インシデント発生の抑制
  - インシデント発生時の被害最小化

- CISOは戦略的活動
  - SOC,CSIRTはその一部
- SOC,CSIRTは戦術的活動
  - ビジネスリスクの低減の目的は同じ

第一部、まとめ

まとめ

1. 「セキュリティ対応組織の教科書 ハンドブック」と「成熟度チェックリスト(ISOMM)」の紹介
   - みなさんもやってみましょう！

2. 「セキュリティ対応組織強化のための情報共有の5W1H」の実体的なフローの紹介と英語版の紹介
   - 情報をもらったら誰がどうするか、までが大事です！

3. JNSA発行「CISOハンドブック」の紹介と現場レベルでの活用について
   - 現場レベルでも意識してみましょう！

このまま第二部に続きます。休憩はその途中にて。

(参考：アイコン、漫画素材)
いらすとや　https://www.irasutoya.com/
©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

- 本資料に関し、利用実態を把握するため、ご利用の際にはISOG-Jの窓口（info (at) isog-j.org）までご一報いただけますと幸いです。
- 本資料に関するご意見、ご要望などは下記よりご連絡ください。
  - https://jp.surveymonkey.com/r/W9HCMFP