

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)の成熟度について

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)

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

- 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

パネラー

● 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



パネラー

- 田中 朗（たなか あきら）
 - 三菱電機インフォメーションネットワーク株式会社
 - セキュリティサービス事業センター 兼
セキュリティ対策グループ（CSIRT）
 - JUNETの時代からインターネットにかかわる
 - お客様向けのManaged Security Services提供 &
社内のCSIRTの立上から日常運用まで

趣味はゲーム、パズル全般

パネラー

- 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

とある組織の

一年史

スタートアップ

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

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・



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。

©ブラックジャックによるしく 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、その後



セキュリティ対応組織、その後



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 話題になりそうな新たな脆弱性
- 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

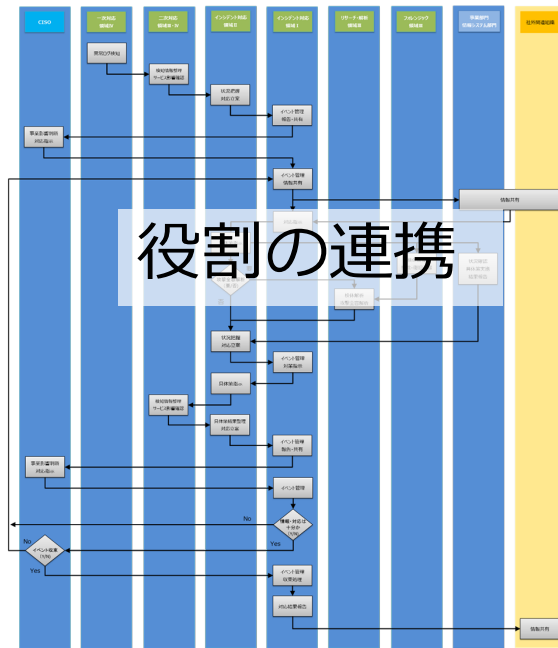
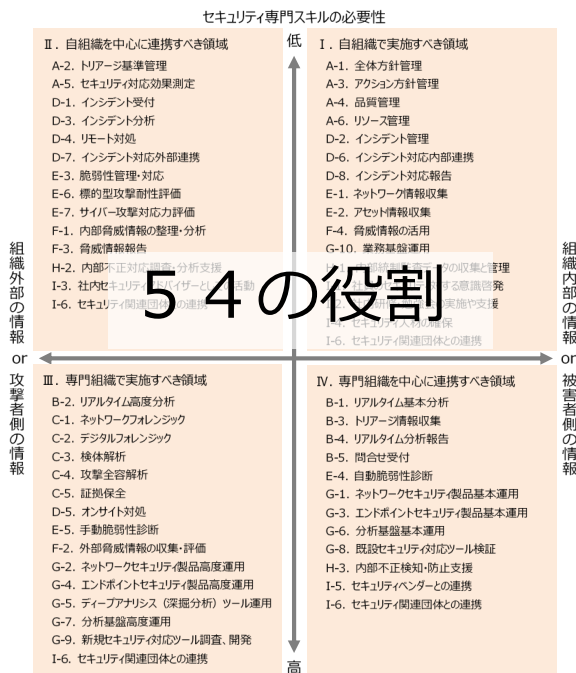
- A. セキュリティ対応組織運営
- B. リアルタイムアナリシス（即時分析）
- C. ディープアナリシス（深堀分析）
- D. インシデント対応
- E. セキュリティ対応状況の診断と評価
- F. 脅威情報の収集および分析と評価
- G. セキュリティ対応システム運用・開発
- H. 内部統制・内部不正対応支援
- I. 外部組織との積極的連携

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

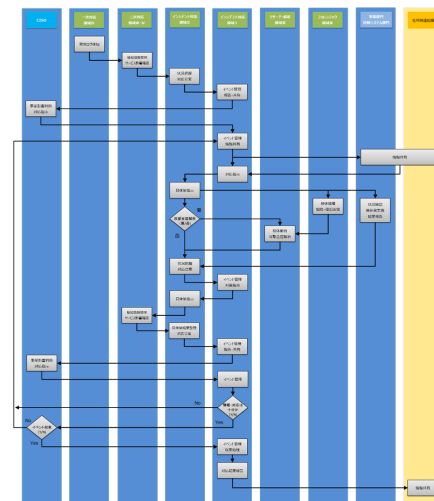


アジェンダ

- イントロ
- メンバ紹介
- アジェンダ紹介 ←いまここ
- インシデント題材 WannaCry概要説明
- 有事（インシデント）の対応例
- 平時の対応例
- パネルディスカッション（随時）

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



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 **47** NEWS 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

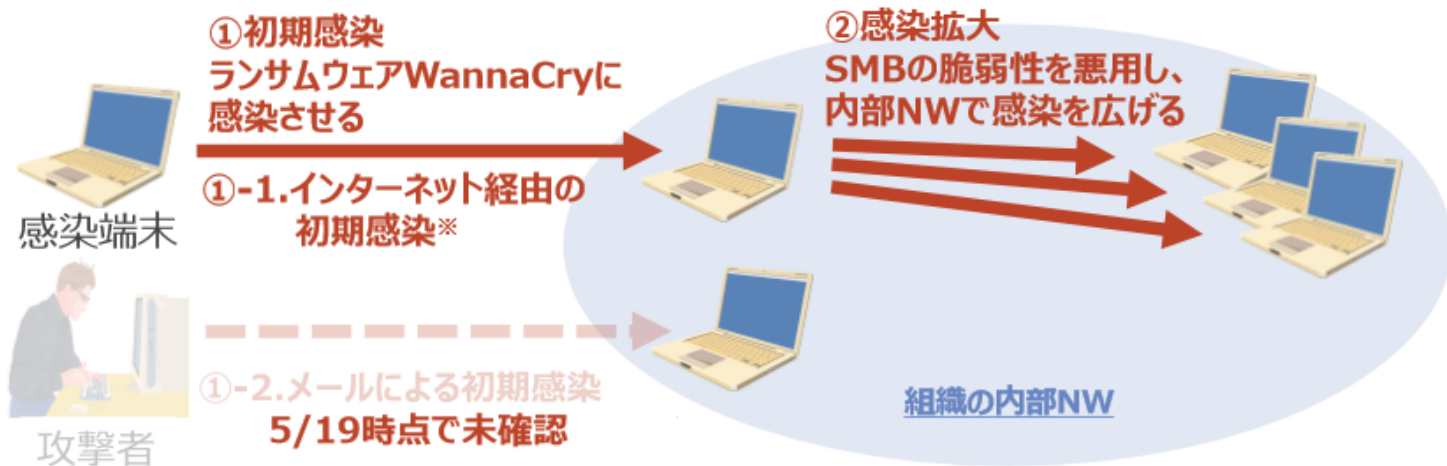
NHK NEWS WEB 5/16

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

インシデント事例：WannaCry

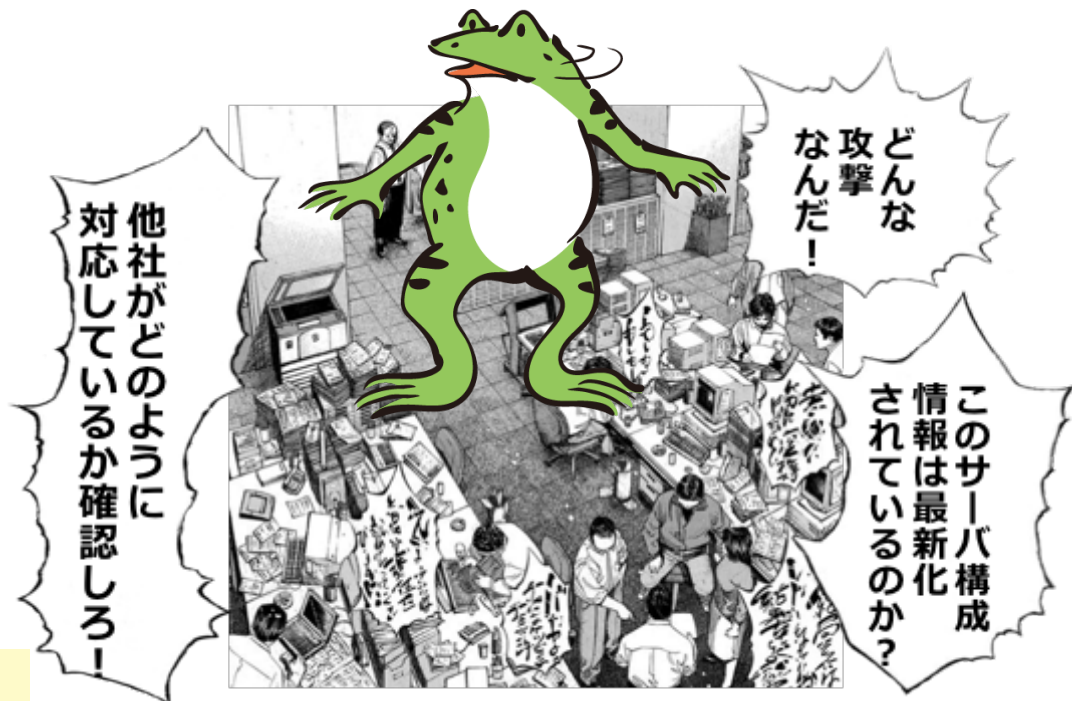
- 445/tcpがOpen、SMB v1が有効、MS17-010未適応なWindowsOS
- ネットワーク経由で感染拡大、ファイルを暗号化



- 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

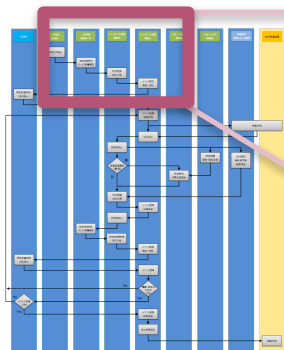
こんなしくじりありませんでしたか？



パネルパート

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



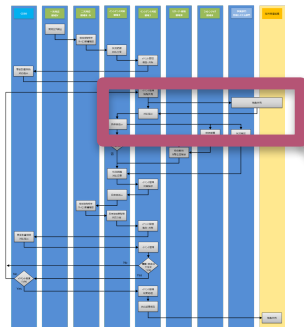
ファイル改ざん(暗号化)ログ確認
不正アクセス(AV・EDR)ログ確認
アノーマリ確認

【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.トリアーシ情報収集
- B-4.リアルタイム分析報告
- B-5.問い合わせ窓口

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

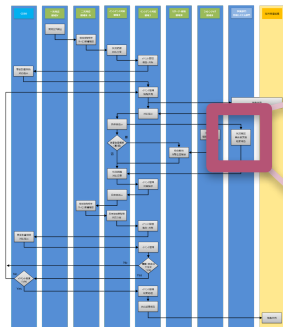
(パッチ、オープンポート、バックアップ)

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

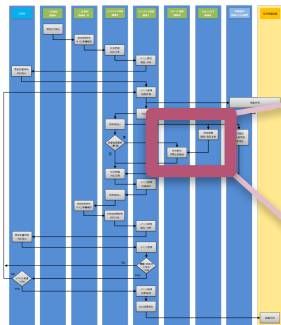
感染状況確認

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

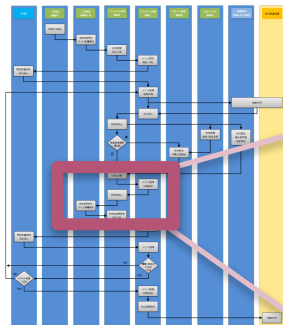


The Equation Group
vs
The Shadow Brokers

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)

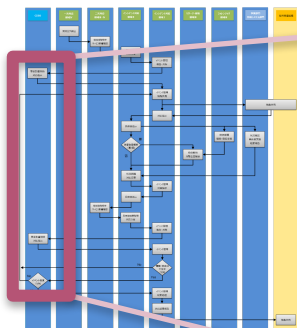
暗号化ファイルの有無

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, DubblePulsar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。



パネルパート

©ブラックジャックによるしく 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

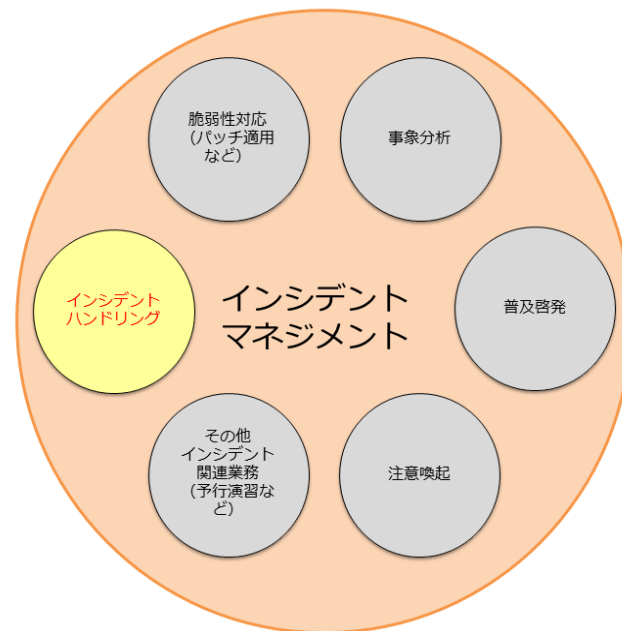
平時がアピールできていなかった組織のしくじり



パネルパート

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.jpccert.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



とは言いますが……



パネルパート

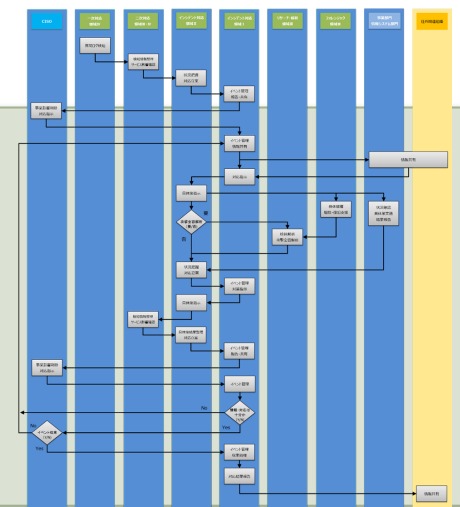
平時の活動例

- 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……



パネルパート

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……



パネルパート

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

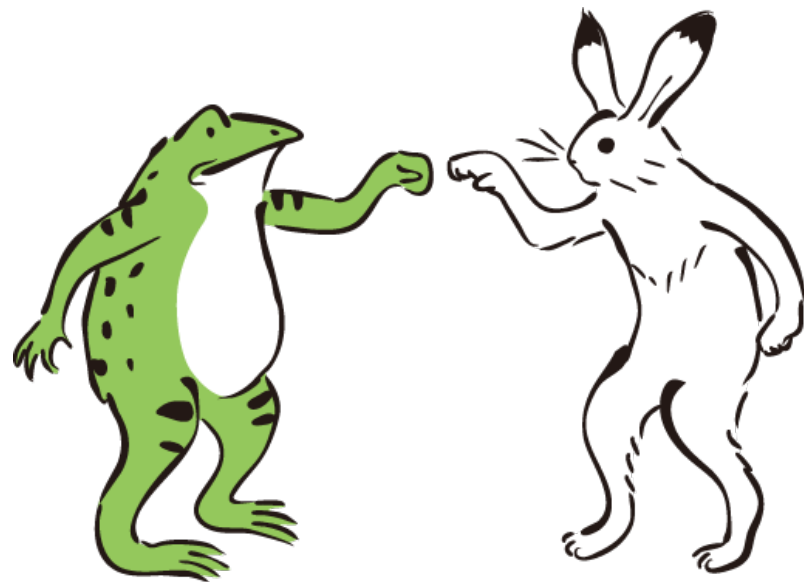
- 効果

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……



パネルパート

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

- 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して新しく作り直しました！
- 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。

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なポイント
 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 pattern を選択してください。

ミニマムアウトソース

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。

© 2017 ISOG-J

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		201X/YY/ZZ		インソース					アウトソース					備考		
				たの イン 結果 として 実施し ないと 判断し	実 施 で き て い な い	が 業 務 を 実 施 で き る	運 用 が 明 文 化 さ れ て お ら ず、 担 当 者 を 代 行 で き る	運 用 が 明 文 化 さ れ て お ら ず、 担 当 者 と 交 代 し て 他 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 と 交 代 し て 他 者 が 業 務 を 実 施 で き る	限 有 る 組 織 長 に 承 認 さ れ て い る	明 文 化 さ れ た 運 用 は C I S S O な ど 接 し た	ア ウ ト ソ ー ス で の 実 施 を 検 討 し た こ の 結 果 と し て 実 施 し な い と 判 断 さ れ 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 て い る
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II	○	○	○	○	○	○	○	○	○	○	○	○			

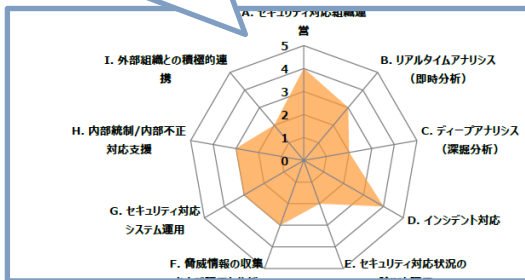
※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。

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

セキュリティ対応組織における"機能別"成熟度



現状の組織（インシデント対応）における強みと弱みを抽出し、現在の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. データアナリシス (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、具体的な対応を行っており、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. データアナリシス (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なっていません。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。

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

セキュリティ対応組織における"役割別"成熟度

201X/YY/ZZ

運営

	1	2	3	4	5
A-1. 計画管理	■	■	■	■	■
A-2. 資源管理	■	■	■	■	■
A-3. 予算管理	■	■	■	■	■
A-4. 品質管理	■	■	■	■	■
A-5. セキュリティ効果測定	■	■	■	■	■
A-6. リソース管理	■	■	■	■	■

B. リアルタイムアナリシス（即時分析）

	1	2	3	4	5
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. 分析内容問合せ受付	■	■	■	■	■

C. ディープアナリシス（深掘分析）

	1	2	3	4	5
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. サイバーキルチェーン分析	■	■	■	■	■
C-5. 証拠保全	■	■	■	■	■

D. インシデント対応

	1	2	3	4	5
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. リモート対応	■	■	■	■	■
D-5. オンサイト対応	■	■	■	■	■
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	■	■	■	■	■

■ : インソース
 ■ : アウトソース

v0.5

E. セキュリティ対応状況の診断と評価

	1	2	3	4	5
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. 標的型攻撃脆弱性評価	■	■	■	■	■
E-7. サイバー攻撃対応力評価	■	■	■	■	■

F. 脅威情報の収集および評価と分析

	1	2	3	4	5
F-1. 内部脅威情報の検出・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

	1	2	3	4	5
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

	1	2	3	4	5
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

	1	2	3	4	5
I-1. 社員のセキュリティに対する意識啓発	■	■	■	■	■
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	■	■	■	■	■

現状の組織の役割成熟度を5段階で示し、モデルとするミニマムアウトソースパターン到達へのポイントも列挙していますので、役割強化にお役立てください。

より強化すべきインソースの役割

自組織での能力をより高めるべきもの

- E-2. アセット情報収集
- G-3. エンドポイントセキュリティ製品基本運用
- I-2. 社内研修・勉強会の実施や支援

より強化すべきアウトソースの役割

より効果的なアウトソースとなるよう改善すべきもの

- C-2. デジタルフォレンジック
- C-4. サイバーキルチェーン分析
- D-5. オンサイト対応

インソースへの切り替えを検討すべき役割

インソースの方が対応力の強化につながるもの

- D-4. リモート対応
- F-1. 内部脅威情報の管理・分析
- G-9. 新規セキュリティ対応ツール調査・開発

アウトソースへの切り替えを検討すべき役割

アウトソースした方が強化しやすくなるもの

- B-2. リアルタイム高度分析

将来に向けての改善点

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おります！

- <https://goo.gl/NK9A6L>

- 業界標準を作りたいです！
- 常時受け付けております
- 匿名での投稿が可能です

A screenshot of a web form titled "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) アンケート" and "ISOG-J成果物に対するフィードバック". The form contains the following text: "*日本セキュリティオペレーション事業者協議会 (ISOG-J) が作成した成果物についてご意見、ご要望などございましたらこちらにご記入ください。" and "フィードバックは次の成果物の内容にかかっています。ご協力よろしくお願いします。". There are three input fields: "成果物名:" (a dropdown menu), "*コメント:" (a large text area), and "*成果物に対する評価:" (a dropdown menu). A blue "送信する" button is at the bottom right.

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) アンケート
ISOG-J成果物に対するフィードバック

*日本セキュリティオペレーション事業者協議会 (ISOG-J) が作成した成果物についてご意見、ご要望などございましたらこちらにご記入ください。

フィードバックは次の成果物の内容にかかっています。ご協力よろしくお願いします。

成果物名：

*コメント：

*成果物に対する評価：

送信する

(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/>

- ・本資料の著作権は日本セキュリティオペレーション事業者協議会(以下、ISOG-J)に帰属します。
- ・引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
- ・なお、引用の範囲を超えられる場合もISOG-Jへご相談ください(info (at) isog-j.org まで)。
- ・本文書に登場する会社名、製品、サービス名は、一般に各社の登録商標または商標です。®やTM、©マークは明記しておりません。
- ・ISOG-Jならびに執筆関係者は、このガイド文書にいかなる責任を負うものではありません。全ては自己責任にてご活用ください。