# 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

@NTTSec_JP

- 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

# 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


©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、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　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

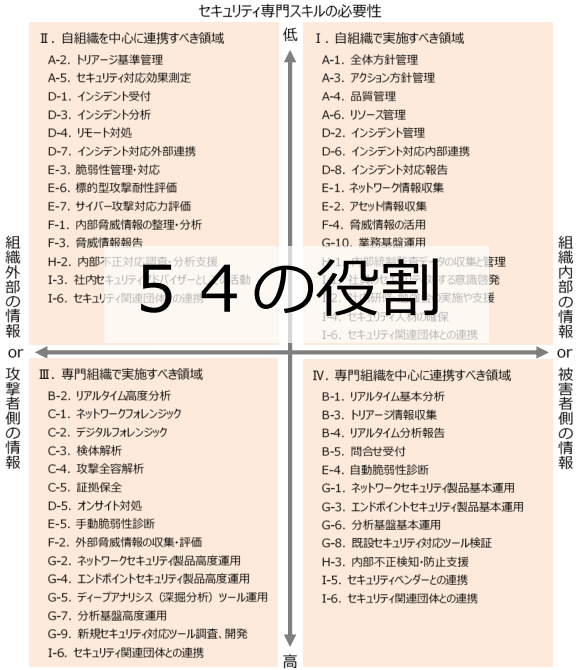
A. セキュリティ対応組織運営
B. リアルタイムアナリシス（即時分析）
C. ディープアナリシス（深堀分析）
D. インシデント対応
E. セキュリティ対応状況の診断と評価
F. 脅威情報の収集および分析と評価
G. セキュリティ対応システム運用・開発
H. 内部統制・内部不正対応支援
I. 外部組織との積極的連携

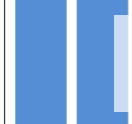
インシデント時の役割

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



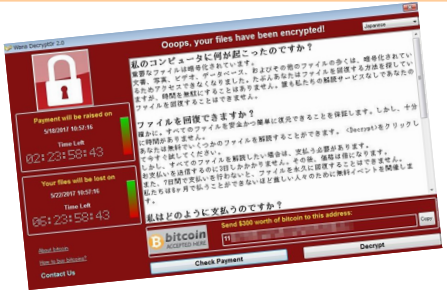
# アジェンダ

- 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

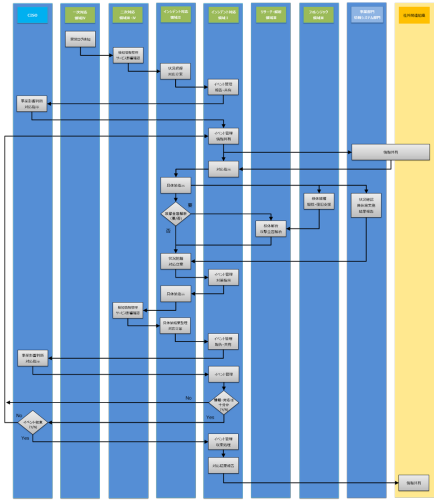
- パネルディスカッション（随時）

# 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


ITpro IPA緊急記者会見 5/14


不審なメール
開かないで

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

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 47NEWS 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

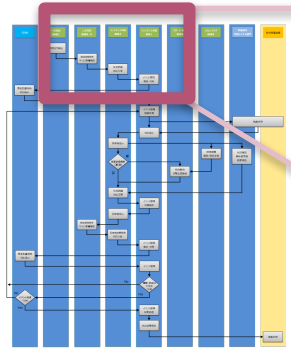
# こんなしくじりありませんでしたか？


パネルパート

©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

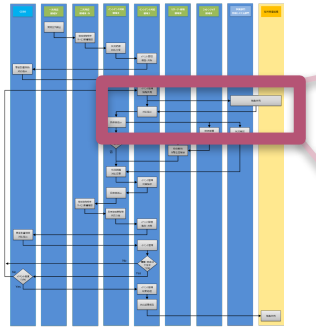
ファイル改ざん(暗号化)ログ確認

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

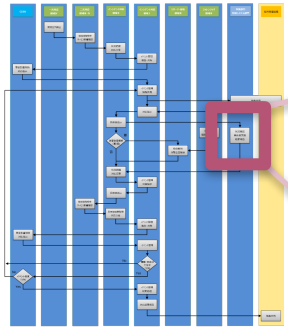
情報交換
　攻撃通信(SMBv1,CVE)、暗号化

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



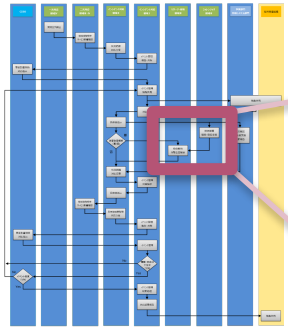
【情シス・ビジネス部門】

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

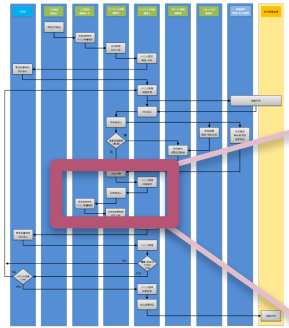
感染端末対応

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】

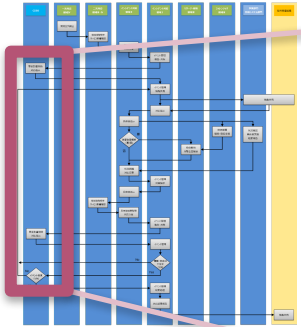
B-4.リアルタイム分析報告(依頼)
D-2.インシデント管理
D-3.インシデント分析
D-8.インシデント対応報告

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。


パネルパート

# 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

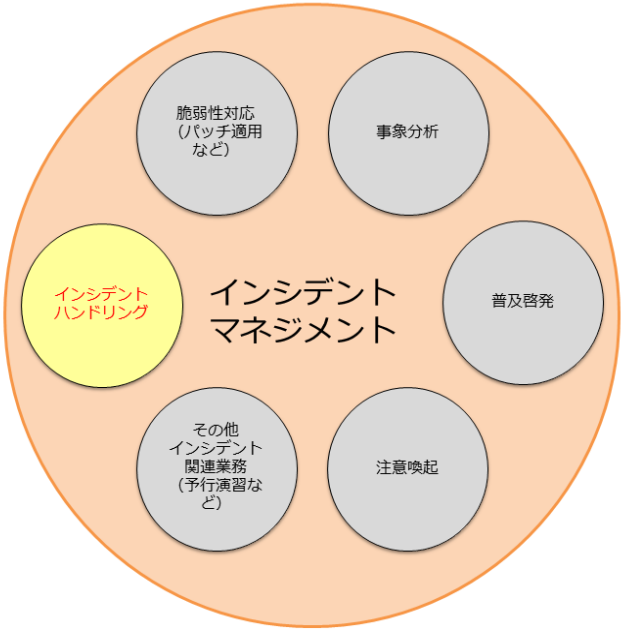
- 気付き
  - 平時の取り組みがスムーズな対応に影響しています

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.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

# とは言いますが……

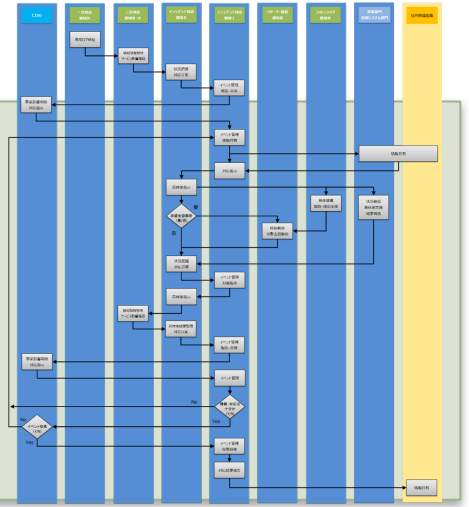
パネルパート

# 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

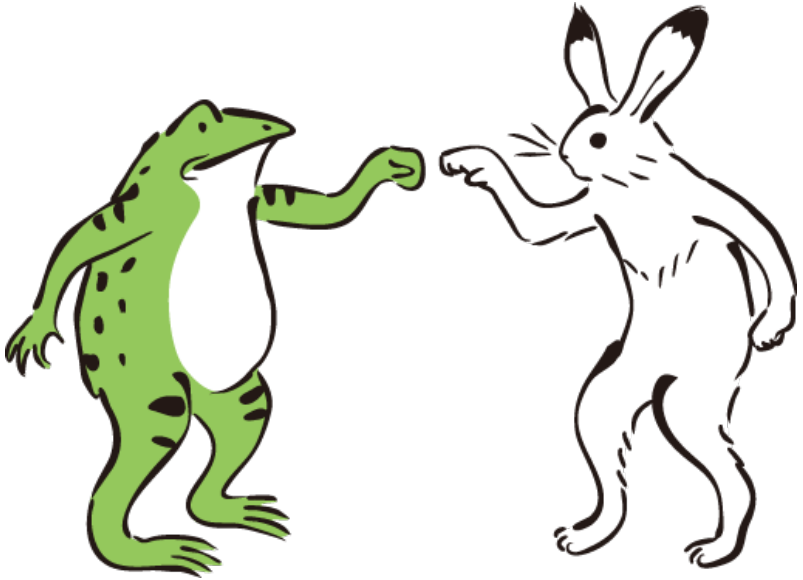
- 普及啓発、注意喚起
  - 平時から事業部門とコミュニケーションを取り、リテラシーの向上を行う

- 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

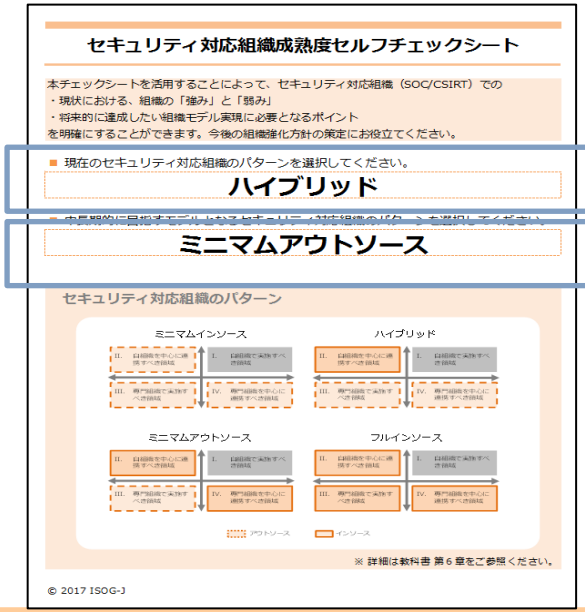
- 今どこまでできているのか、これから目指す姿とのギャップは何か、見える化するための成熟度チェックリストを作りました。

- 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

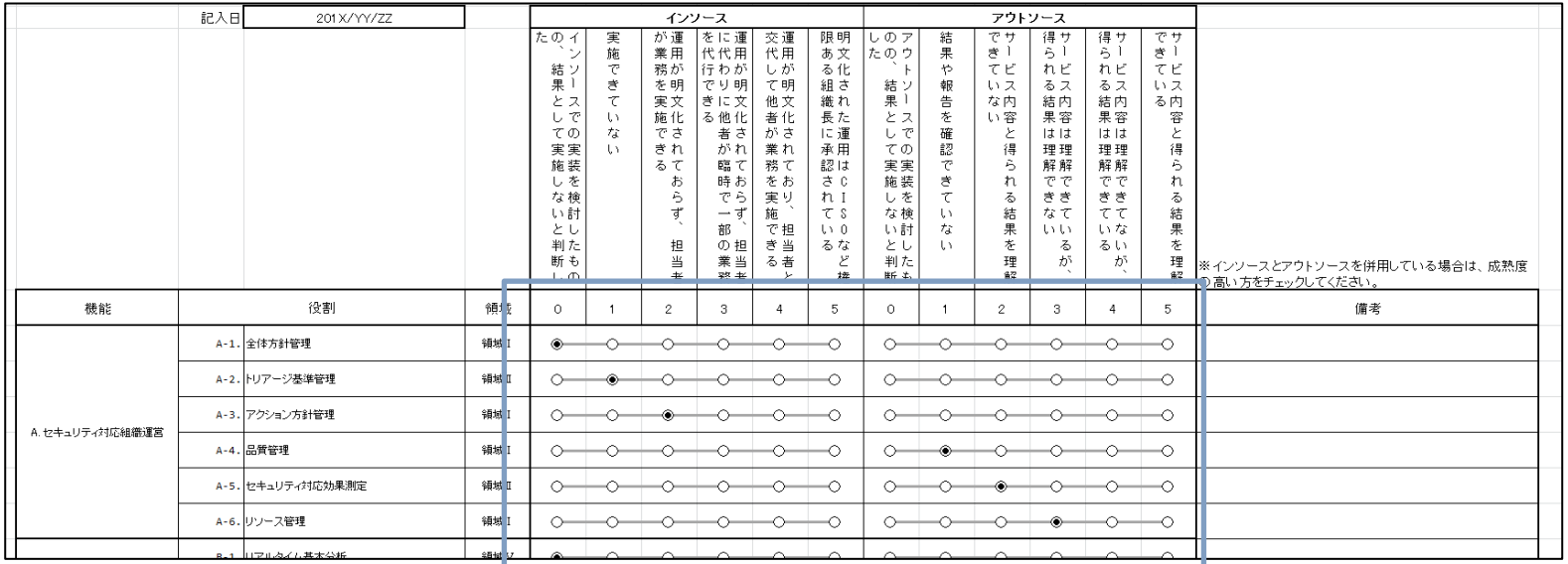
# 成熟度セルフチェックシートの使い方

- 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 | 201X/YY/ZZ | | インソース | | | | | | アウトソース | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 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 | サービス内容は理解できてないが、得られる結果は理解できている | 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◎高い方をチェックしてください。 |
| 機能 | 役割 | 傾域 | 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Ⅴ | ◉ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |

3. 入力シートで現在の状況を選択

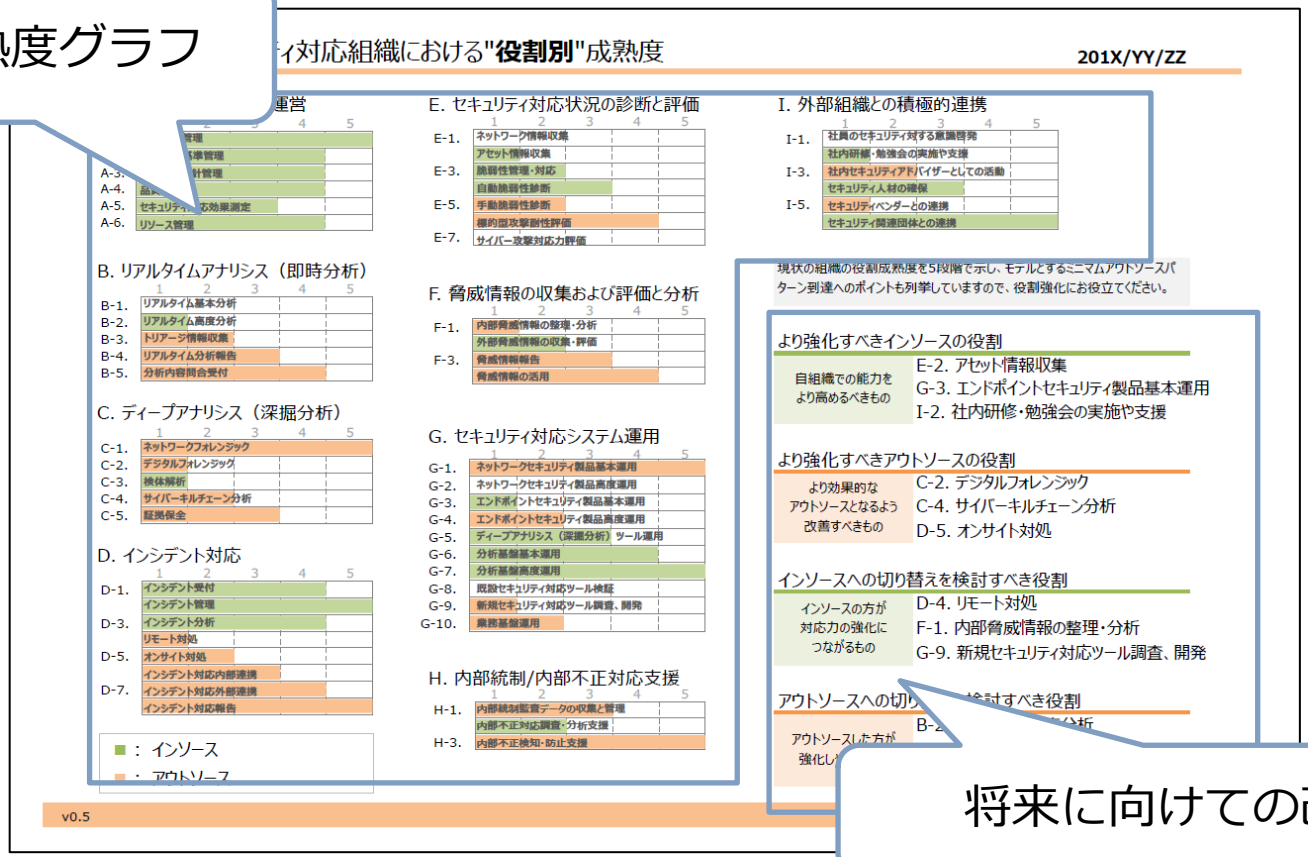
機能別レーダーチャート

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

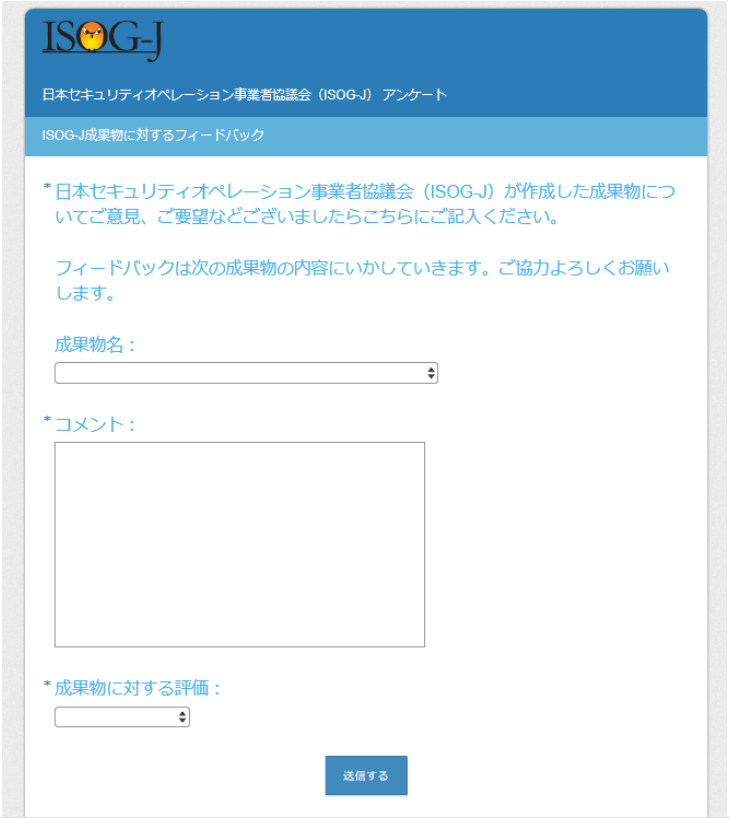



将来に向けての改善点

# 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
  - 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



(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/