JNSA全国横断サイバーセキュリティセミナー2018

セキュリティ対応組織と成熟度診断

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普及・啓発WG(WG4)
セキュリティオペレーション連携WG(WG6)
セキュリティ対応組織成熟度調査タスクフォース

（日本ネットワークセキュリティ協会(JNSA)）

公開情報

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7月1日現在、45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。

- ISOG-Jは日本ネットワークセキュリティ協議会（JNSA）の部会です

- ホームページ：　http://isog-j.org
- facebook：/isogj
- twitter：@isog_j

公開情報

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)

のご紹介

公開情報

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

公開情報

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

公開情報

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。

公開情報

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

公開情報

強いセキュリティ対応組織

＝

それぞれの機能と役割が実行できているか

公開情報

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)

公開情報

最近、いろいろなガイドや
チェックリストが増えましたね？
ありがたいことですが。

公開情報

私見で3つの立ち位置を整理する

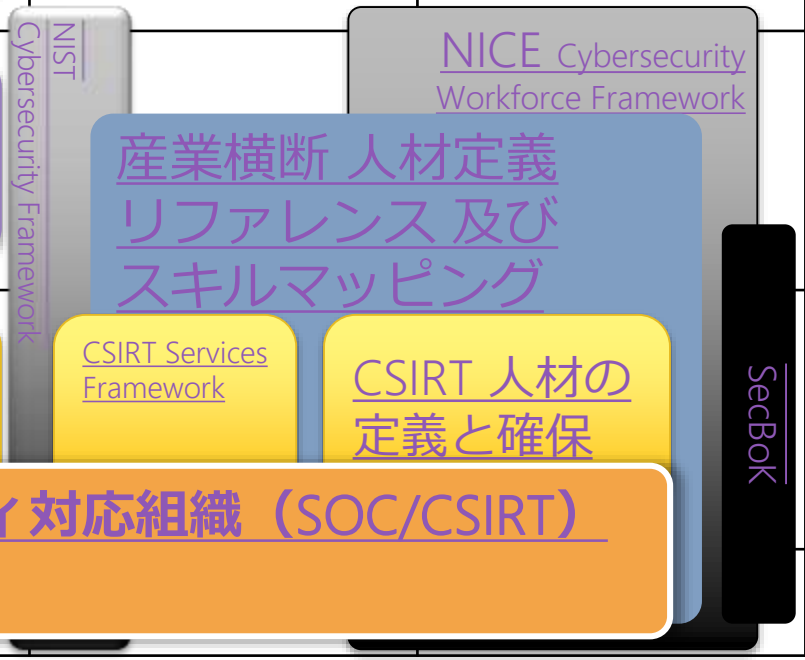
- サイバーセキュリティ経営ガイドライン（経済産業省）
  - 産業横断サイバーセキュリティ人材育成検討会
    人材定義リファレンス
    セキュリティ対策カレンダー
    - 日本シーサート協議会(NCA)
      CSIRT 人材の定義と確保
      （CERT/CC,ENISAも参照）

- ISOG-J
  セキュリティ対応組織の教科書（IT型人材を定義）
  成熟度チェックリスト
  （JNSA セキュリティ知識分野(SecBoK)も参照）

公開情報

セキュリティ対応組織に関する各種ドキュメント等の関係性

	指針	機能・業務	人材・スキル	指標
経営者	サイバーセキュリティ経営ガイドライン	—	—	
CISO	CISOハンドブック			
CSIRT	CSIRT 構築マテリアル	CSIRT Services Framework	CSIRT 人材の定義と確保	SIM3 Security Incident Management Maturity Model
SOC				ISOMM セキュリティ対応組織成熟度モデル



公開情報

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

公開情報

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

公開情報

ISOMMの使い方

公開情報

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

公開情報

ISOG-Jのホームページからダウンロードできます

ダウンロードするファイルは2つ

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

ISOMM 本体
http://isog-j.org/output/2017/Textbook_soc-csirt_v2.1_maturity-checklist.xlsx

WindowsのExcelでの利用を推奨します。
ダウンロードしたらExcelファイルを開きましょう

公開情報

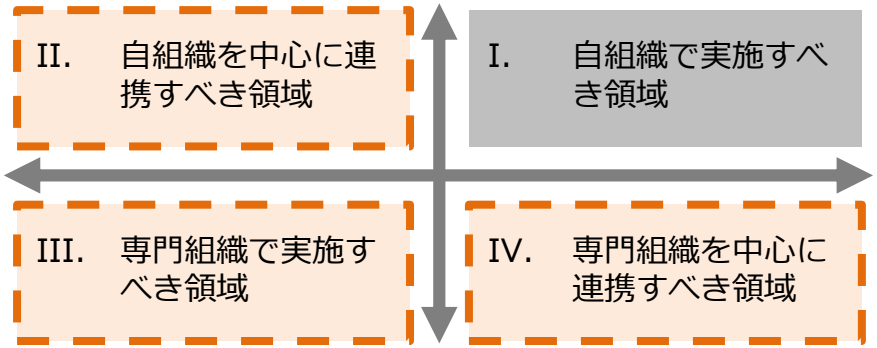
① 組織パターンの設定

公開情報

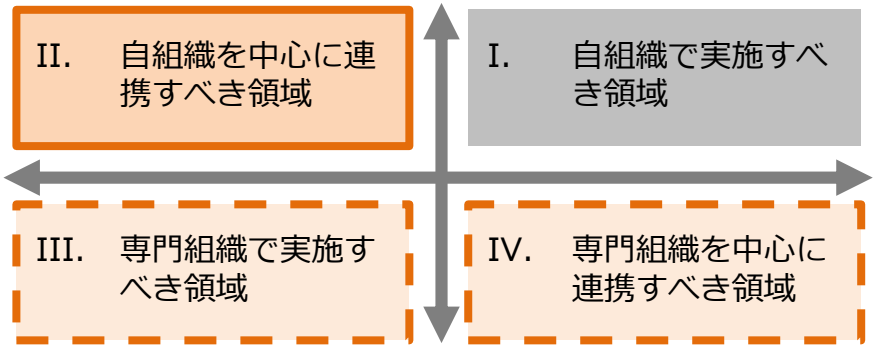
セキュリティ対応組織パターンを自覚する（教科書を参考）

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）

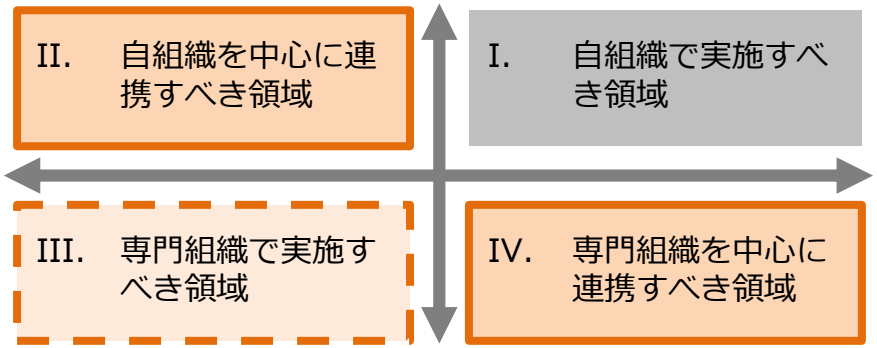
ミニマムインソース



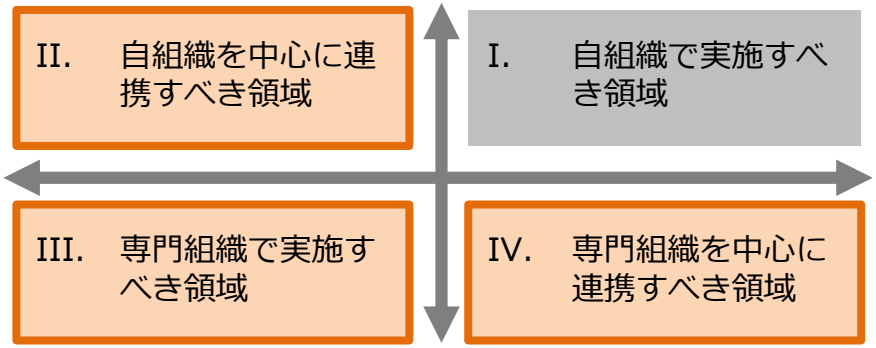
ハイブリッド



ミニマムアウトソース

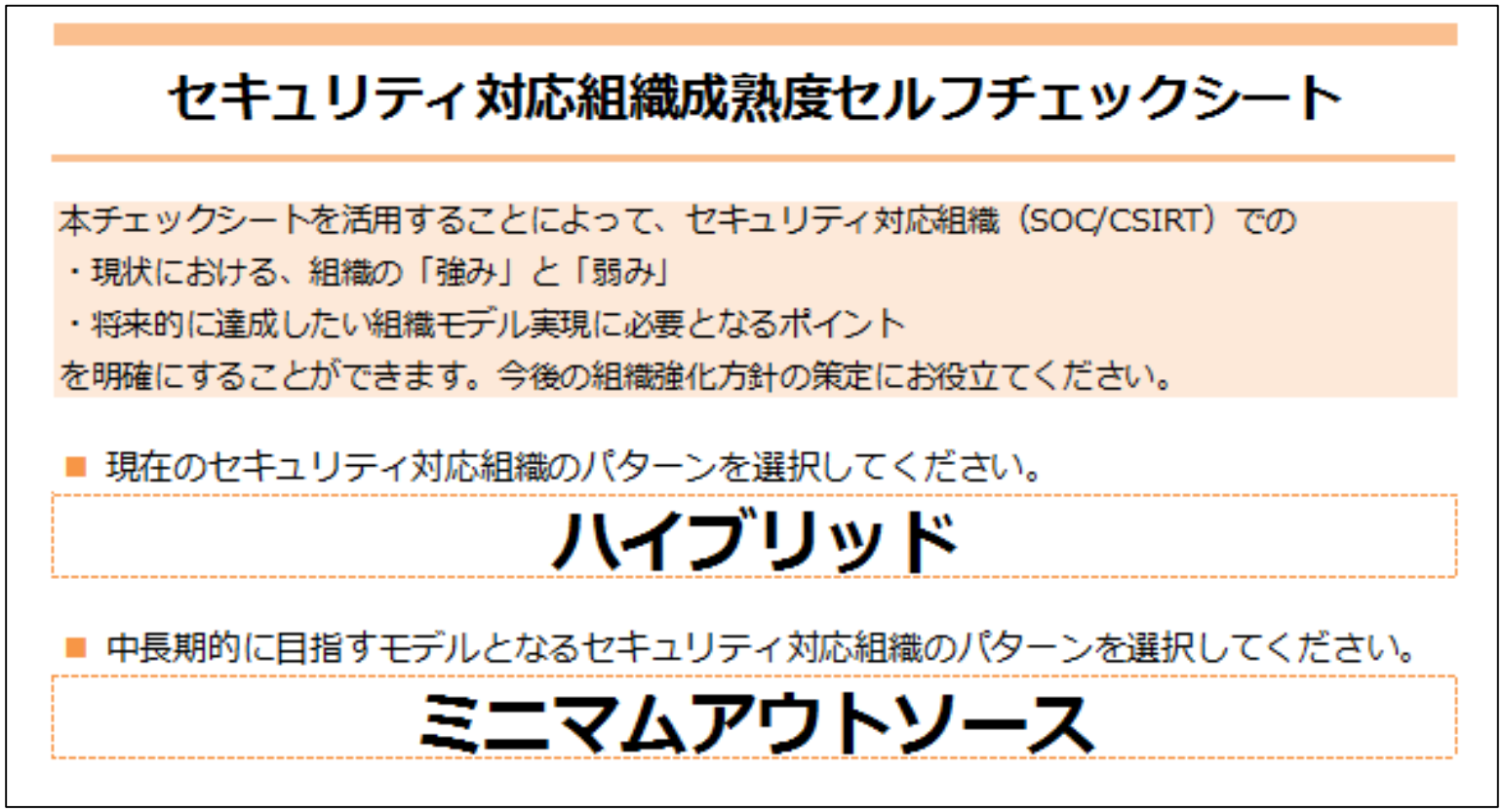


フルインソース



アウトソース　インソース

公開情報



現在と、将来的なモデルとするパターンを選択。

公開情報

② 機能ごとに点数化

公開情報

記入日 201X/YY/ZZ

機能	役割	領域	インソース 0	インソース 1	インソース 2	インソース 3	インソース 4	インソース 5	アウトソース 0	アウトソース 1	アウトソース 2	アウトソース 3	アウトソース 4	アウトソース 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	
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。

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。

公開情報

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

公開情報

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

公開情報

54の役割を見ながら
チェックをして見ましょう

公開情報

A. セキュリティ対応組織運営

- A-1. 全体方針管理
  - セキュリティ対応における全体方針を管理する。守るべき資産とそれらを守る仕組みの全体像を把握して、今後行うべき取り組みなど管理する
- A-2. トリアージ基準管理
  - 取り決められた対応範囲において発覚する事象への具体的なトリアージ（対応優先度基準）と取り決める
- A-3. アクション方針管理
  - トリアージ基準に対し、具体的な対応（アクション）の方針を取り決める

公開情報

A. セキュリティ対応組織運営

- A-4. 品質管理
  - ある程度の期間において行われた各種分析や対応の棚卸しをし、対応の品質に問題がなかったか確認する
- A-5. セキュリティ対応効果測定
  - 対応がもたらす効果を測定する。インシデント対応数や攻撃の遮断数など
- A-6. リソース管理
  - 対応するにあたり必要となるリソース（人員、予算、システム）などの計画、各機能への分配

公開情報

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
  - ログを監視し、リアルタイムに分析を行う
- B-2. リアルタイム高度分析
  - 基本分析だけでは影響度や内容が把握できない場合のより詳細な分析
- B-3. トリアージ情報収集
  - トリアージの判断がリアルタイム分析の情報だけではできない場合、「E セキュリティ対応状況の診断と評価」の情報や普段扱っていないログソースからさらに情報を収集する
- B-4. リアルタイム分析報告
  - リアルタイム分析によって判明した情報を、対応に必要な情報を最低限含めてドキュメント化する。
- B-5. 分析結果問合受付
  - 分析に関するデータや提供したレポートについての問い合わせ対応

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
  - リアルタイム分析に対して、ネットワークログやPCAPを改めて分析する
- C-2. デジタルフォレンジック
  - 被害にあった端末やサーバのHDD/SSD、メモリ、外部記憶媒体などに保存されたデジタルデータ全般の分析を行う
- C-3. 検体解析
  - マルウェアや攻撃やが配置したプログラムやスクリプトの機能を解析する。
- C-4. 攻撃全容解析
  - フォレンジックや検体解析の結果をもとに、攻撃活動の全容を明らかにする
- C-5. 証拠保全
  - 犯罪捜査や法的措置を行う可能性がある場合には、各過程において電磁的証拠の保全を行う

公開情報

D. インシデント対応

- D-1. インシデント受付
  - 運用からの分析報告や、社内外からの通報を受ける。
- D-2. インシデント管理
  - トリアージにより対応が決まったインシデントについて進捗状況や対応状況を完了するまで管理する
- D-3. インシデント分析
  - 受け付けたインシデント情報の対応可否および優先度を判断する
- D-4. リモート対処
  - 電話やメール、リモートアクセス(リモートデスクトップやSSH)でのインシデント対応を行う。
- D-5. オンサイト対処
  - 物理的拠点まで出向いて対応を行う。

D. インシデント対応

- D-6. インシデント対応内部連携
  - 内部関係者（経営層、関連する社内他部門）、社外の協力者（開発ベンダー、サービス提供者）と連携、調整を行う。
- D-7. インシデント対応外部連携
  - 外部関係者（監督官庁、取引関係組織、エンドユーザー）との連携、調整を行う
- D-8. インシデント対応報告
  - 対応により解明した影響内容、発生要因、実施した対処および根本対策方針などまとめてドキュメント化する

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
  - 守るべき対象のネットワーク構成の概要を把握する
- E-2. アセット情報収集
  - 情報資産管理情報に加えて、ファームウェアやインストールされているアプリケーションなどの情報までも収集が望ましい。
- E-3. 脆弱性管理・対応
  - 脆弱性の対処が必要となるシステムを特定する。対処の進捗状況も管理する
- E-4. 自動脆弱性診断
  - 守るべきシステムやネットワーク、アプリケーションに脆弱性がないかをツール使って確認する。
- E-5. 手動脆弱性診断
  - 専門の人員による「手動」で脆弱性がないかを診断する

公開情報

E. セキュリティ対応状況の診断と評価

- E-6. 標的型攻撃耐性評価
  - 標的型メール訓練やソーシャルエンジニアリングテストを実施する。
- E-7. サイバー攻撃対応力評価
  - シナリオに基づき、インシデント終息までたどり着けるか、サイバー攻撃対応演習を実施する

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
  - リアルタイム分析やインシデント対応に関する情報を収集し、自社内のインシデント根本原因を分析して対策をできるよう整理する
- F-2. 外部脅威情報の収集・評価
  - 新たな脆弱性情報、攻撃傾向、マルウェア挙動情報や悪性IPアドレスやドメイン情報などを収集し、信頼性を評価、取捨選択をしてE-3 脆弱性管理へインプットする
- F-3. 脅威情報報告
  - 内部脅威情報や外部脅威情報を取りまとめて、詳細も含みドキュメント化する
- F-4. 脅威情報の活用
  - 取りまとめた情報を周知をしたりフィードバックを受ける

公開情報

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
  - ファイヤウォール、IDS/IPS、WAF、プロキシなどを運用する
- G-2. ネットワークセキュリティ製品高度運用
  - 独自シグネチャの作成や適用を行う
- G-3. エンドポイントセキュリティ製品基本運用
  - アンチウイルスソフトなどのエンドポイント対策製品の運用を行う
- G-4. エンドポイントセキュリティ製品高度運用
  - レジストリの状態やプロセスの実行状況を収集して分析し、カスタムIOC(Indicator of Compromise)を定義する
- G-5. ディープアナリシス(深掘分析)ツール運用
  - デジタルフォレンジックやマルウェア解析ツールを運用する

G. セキュリティ対応システム運用・開発

- G-6. 分析基盤基本運用
  - リアルタイムアナリシスでログデータを保存し、定常的に分析するSIEMなどを運用する
- G-7. 分析基盤高度運用
  - SEIMが取り込めないシステムログやパケットキャプチャデータを独自に分析する
- G-8. 既設セキュリティ対応ツール検証
  - 製品のバージョンアップや設定変更などの可用性への影響を検証する
- G-9. 新規セキュリティ対応ツール調査、開発
  - 新たな対策が必要になった場合、新たなツールを検証する
- G-10. 業務基盤運用
  - セキュリティ対応に必要なシステムの運用を行う

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
  - 内部統制に必要なログを定義して収集する
- H-2. 内部不正対応の調査・分析支援
  - 内部不正が発覚した場合に、ログから活動内容を整理するなどし、内部不正に対応している組織を支援する
- H-3. 内部不正検知・防止支援
  - 内部不正がログから検知できる場合、検知ロジックとして実装する。

公開情報

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
  - 社内での啓発を行う
- I-2. 社内研修・勉強会の実施や支援
  - 社内での研修や勉強会を行う
- I-3. 社内セキュリティアドバイザーとしての活動
  - 社内のお客様向けのサービスの部門から相談を受ける
- I-4. セキュリティ人材の確保
  - 人事組織と連携して人材を確保する
- I-5. セキュリティベンダーとの連携
  - 購入した製品やサービスについて提供元と直接対話できる関係を築く。
- I-6. セキュリティ関連団体との連携
  - NCAや各種ISACなどへ参加して、情報交換や共有、情報活用をする

③ 結果を見てみる

公開情報

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　応組織における"**機能別**"成熟度

201X/YY/ZZ

現状の組織（ハイブリッドパター　能別成熟度を5段階で評価しています。
組織の「強み」と「弱み」を抽出　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　ます。
マクロな観点での指標とし　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業務を見直してください。

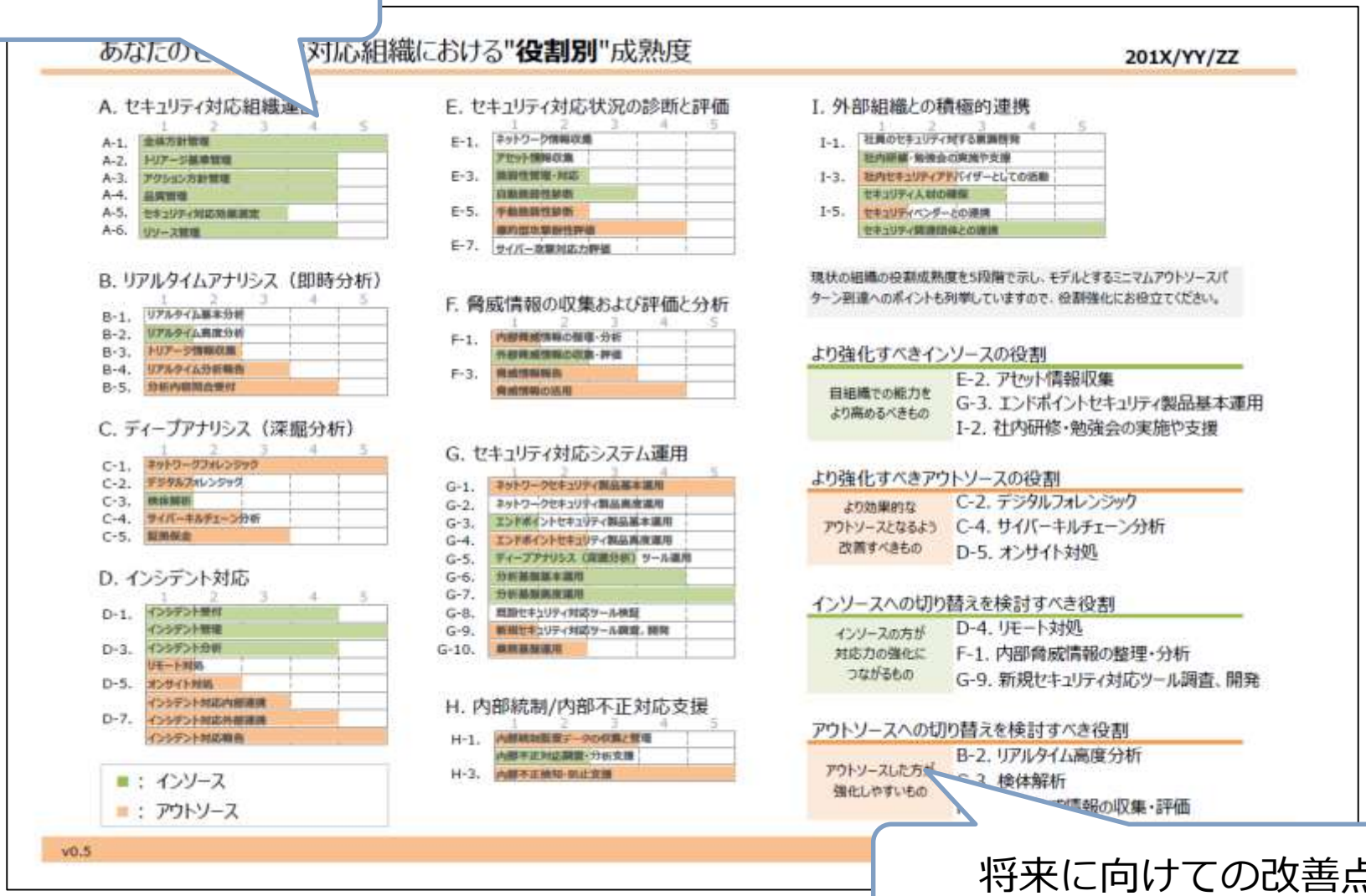
v0.5　© 2017 ISOG-J

現在の「強み」：成熟度高

現在の「弱み」：成熟度低

公開情報

役割別成熟度グラフ



将来に向けての改善点

公開情報

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

公開情報

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。

公開情報

まとめ

★セキュリティ対応組織が担うべき機能、役割を理解したい

- セキュリティ対応組織（SOC/CSIRT）の教科書 v2.1

★セキュリティ対応組織の実態を客観的に把握したい

- セキュリティ対応組織成熟度セルフチェックシート

★突然の情報でも焦らず対応できるよう心構えをしたい

- 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」

ISOG-J公式サイトにて公開中
http://isog-j.org/activities/result.html

公開情報

成熟度セルフチェックシート（ISOMM）の結果について アンケートを実施しています。

- https://bit.ly/2N0niDk
  - アンケートの結果から、各組織のセキュリティ対応における成熟度の状況確認や分析を実施。

ご協力よろしくお願いします。

公開情報

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://bit.ly/2MlDpim
  - 常時受け付けております
  - 匿名での投稿が可能です

公開情報