実はあなたも関わっている？ 組織のセキュリティ対応度合いを測る BoF

2018/7/11

ももい
たけい

「運用」してますか？

運用いろいろ

- ネットワーク、サーバ
- ステータス監視
- セキュリティ監視
- インシデント対応

なし崩しに全部まとめてやってません？

ネットワーク、サーバ
ステータス監視

当初の範囲

セキュリティ監視
インシデント対応

増えた範囲

最近色々なガイドラインと成熟度が！

各社や組織にセキュリティの
対応する組織ができつつあり、
次はどこまでできているかなと
測りたくなる時期ですね。

私見で4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(METI)

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）

セキュリティの側から業務役割を整理してみる

セキュリティ監視　インシデント対応

9つの機能　**54**の役割

整理してみた。

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

役割を分類した

セキュリティ専門スキルの必要性

低

高

組織外部の情報 or 攻撃者側の情報

組織内部の情報 or 被害者側の情報

Ⅱ．自組織を中心に連携すべき領域

- A-2．トリアージ基準管理
- A-5．セキュリティ対応効果測定
- D-1．インシデント受付
- D-3．インシデント分析
- D-4．リモート対処
- D-7．インシデント対応外部連携
- E-3．脆弱性管理･対応
- 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-1．内部脅威情報の整理･分析
- F-3．脅威情報報告
- H-2．内部不正対応調査･分析支援
- I-3．社内セキュリティアドバイザーとしての活動
- I-6．セキュリティ関連団体との連携

Ⅰ．自組織で実施すべき領域

- A-1．全体方針管理
- A-3．アクション方針管理
- A-4．品質管理
- A-6．リソース管理
- D-2．インシデント管理
- D-6．インシデント対応内部連携
- D-8．インシデント対応報告
- E-1．ネットワーク情報収集
- E-2．アセット情報収集
- F-4．脅威情報の活用
- G-10．業務基盤運用
- H-1．内部統制監査データの収集と管理
- 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-4．セキュリティ人材の確保
- I-6．セキュリティ関連団体との連携

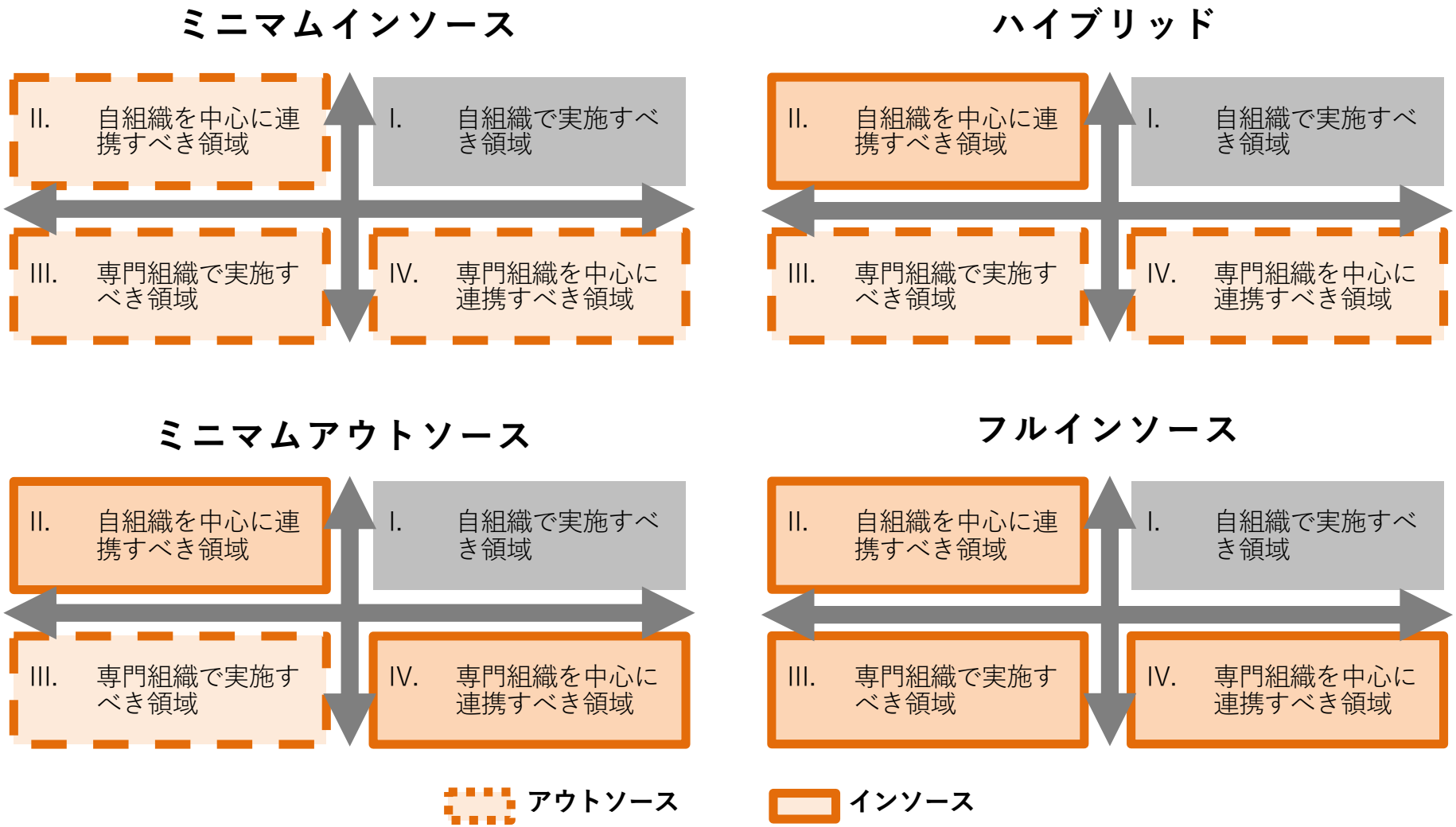
Ⅲ．専門組織で実施すべき領域

- B-2．リアルタイム高度分析
- 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．サイバーキルチェーン分析
- C-5．証拠保全
- D-5．オンサイト対処
- E-5．手動脆弱性診断
- F-2．外部脅威情報の収集･評価
- G-2．ネットワークセキュリティ製品高度運用
- 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-7．分析基盤高度運用
- G-9．新規セキュリティ対応ツール調査、開発
- I-6．セキュリティ関連団体との連携

Ⅳ．専門組織を中心に連携すべき領域

- B-1．リアルタイム基本分析
- 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．問合せ受付
- E-4．自動脆弱性診断
- G-1．ネットワークセキュリティ製品基本運用
- G-3．エンドポイントセキュリティ製品基本運用
- G-6．分析基盤基本運用
- G-8．既設セキュリティ対応ツール検証
- H-3．内部不正検知･防止支援
- 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

組織のパターンが見えた



組織の成熟度を測るチェックリストができた

機能と役割に注目し、
どこまでできているかで
点数をつける

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)

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。

セルフチェックシート

Excel (Windows版) を持っている方、
手元で試せます

続きは BoF で！！