SOC/CSIRT「セキュリティ対応組織の教科書 v1.0」の公開

阿部 慎司

（ISOG-J / NTTセキュリティ・ジャパン株式会社）

ISOG-Jについて

セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に寄与することを目的として設立。現在３３社が加盟。

WG1
- **セキュリティオペレーションガイドラインWG**
- 脆弱性診断士のスキルマップ＆シラバス

WG2
- **セキュリティオペレーション技術WG**
- 定期的な技術者交流会

WG3 休止中
- **セキュリティオペレーション関連法調査WG**
- セキュリティ関連法規について整理

WG4
- **セキュリティオペレーション認知向上・普及啓発WG**
- セミナー等の企画

WG5 準備中
- **情報利用関連WG**
- サイバーセキュリティ関連情報の利活用について検討

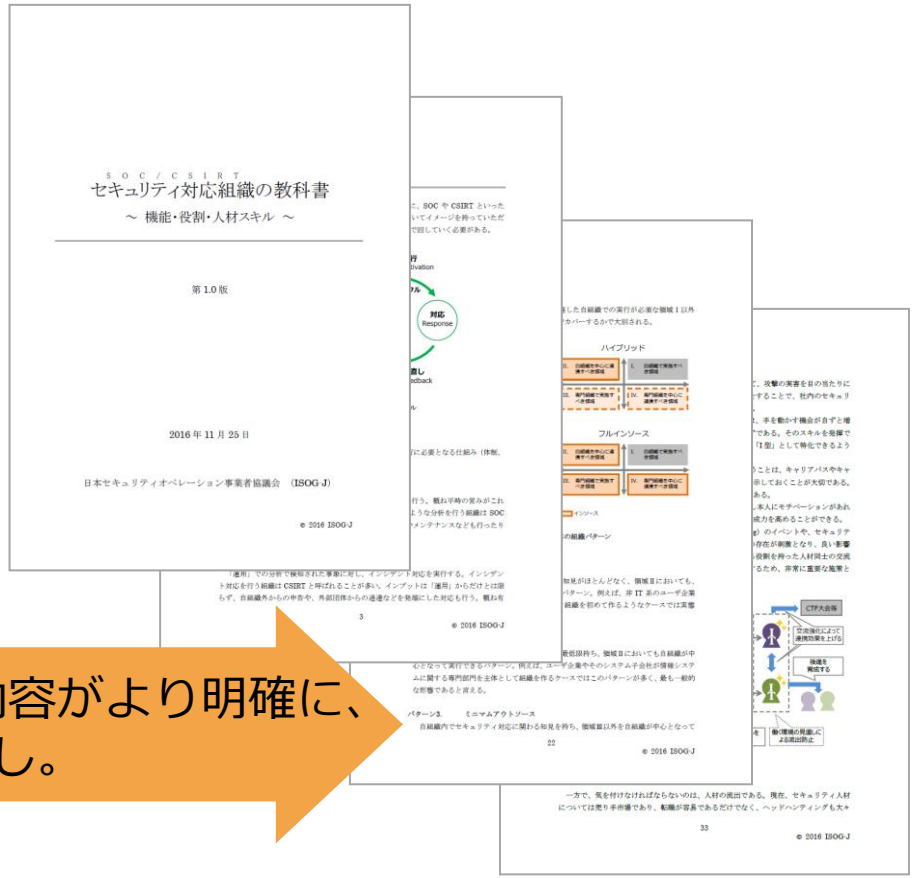
WG6
- **セキュリティオペレーション連携WG**
- セキュリティオペレーションに関する共通課題の議論、解決の検討

いまグロPJ
- **グローバル動静情報共有プロジェクト**
- セキュリティを取り巻くグローバルな変化を読み解く

S O C / C S I R T
セキュリティ対応組織の教科書について

SOCの役割と人材のスキル v1.0
(2016年07月)

セキュリティ対応組織の教科書 v1.0
(2016年11月)



ISOG-J内外で議論を深め、各項の内容がより明確に、
より汎用的になるよう全面的に見直し。

主な内容

セキュリティ対応組織に関し

- 必要となる機能（9個の機能）
- 各機能が持つべき役割（54個の役割）
- 体制/役割分担
- 人材スキル/育成

を体系的に整理

作成のモチベーション

“セキュリティ対応”とは…？

* MDR： Managed Detection & Response services

出典：
JPCERT/CC「CSIRTガイド」
p27 インシデントマネジメント、ハンドリング、レスポンスの関係

本書を通じて…

1. **セキュリティ対応としてどのような機能が求められるのかを把握する**
   - 全体を把握せず組み立てると、必ず「穴」が生まれ、そこで破綻する
2. **自組織が何ができて何ができてなくて、どこまでやるべきなのかを考える**
   - どこまでやるのか決まっていないと、「やるやらない」「やれるやれない」で揉めて、そこから進めなくなる

本書を通じて…

1. **セキュリティ対応としてどのような機能が求められるのかを把握する**
   - 全体を把握せず組み立てると、必ず「穴」が生まれ、そこで破綻する
2. **自組織が何ができて何ができてなくて、どこまでやるべきなのかを考える**
   - どこまでやるのか決まっていないと、「やるやらない」「やれるやれない」で揉めて、そこから進めなくなる

セキュリティ対応組織に求められる９つの機能

A. セキュリティ対応組織運営
セキュリティ対応するに当たって、取り扱うべき事象や対応範囲、トリアージ（対応優先度）基準などの、セキュリティ対応における全体方針を管理したり、必要となるリソース計画を行ったりする機能である。セキュリティ対応の安定的な運営を目的とする。

B. リアルタイムアナリシス (即時分析)
NW装置やサーバ、セキュリティ製品など、各種システムからのログやデータを常時監視し、分析を行う機能である。リアルタイムに脅威を発見し、迅速で適切なインシデント対応へ繋げることを目的とする。

C. ディープアナリシス (深掘分析)
被害を受けたシステムの調査や、漏えいしたデータの確認、攻撃に利用されたツールや手法の分析など、インシデントに関連するより深い分析を行う機能である。インシデントの全容解明と影響の特定を目的とする。

D. インシデント対応
リアルタイム分析結果や脅威情報を元に、脅威の拡散抑止、排除のための具体的な対応を行う機能である。関係者との調整、報告なども含め、システムおよびビジネスへの影響最小化を目的とする。

E. セキュリティ対応状況の診断と評価

守るべきシステムに対する脆弱性診断や、インシデント対応訓練およびその評価行う機能。セキュリティレベルの向上などを目的とする。

F. 脅威情報の収集および分析と評価

ネット上に公開されている、脆弱性や攻撃に関する脅威情報（外部インテリジェンス）を収集したり、リアルタイム分析やインシデント対応時の情報（内部インテリジェンス）を取り扱ったりする機能である。リアルタイム分析の精度向上やインシデント対応、セキュリティツールの改善へ繋げることを目的とする。

G. セキュリティ対応システム運用/開発

セキュリティ対応するにあたって必要となるシステム（セキュリティ製品、ログ収集DB、運用システムなど）の管理、改善や新規開発を行う機能。他の機能が円滑かつ持続的に活動可能な状態を実現することを目的とする。

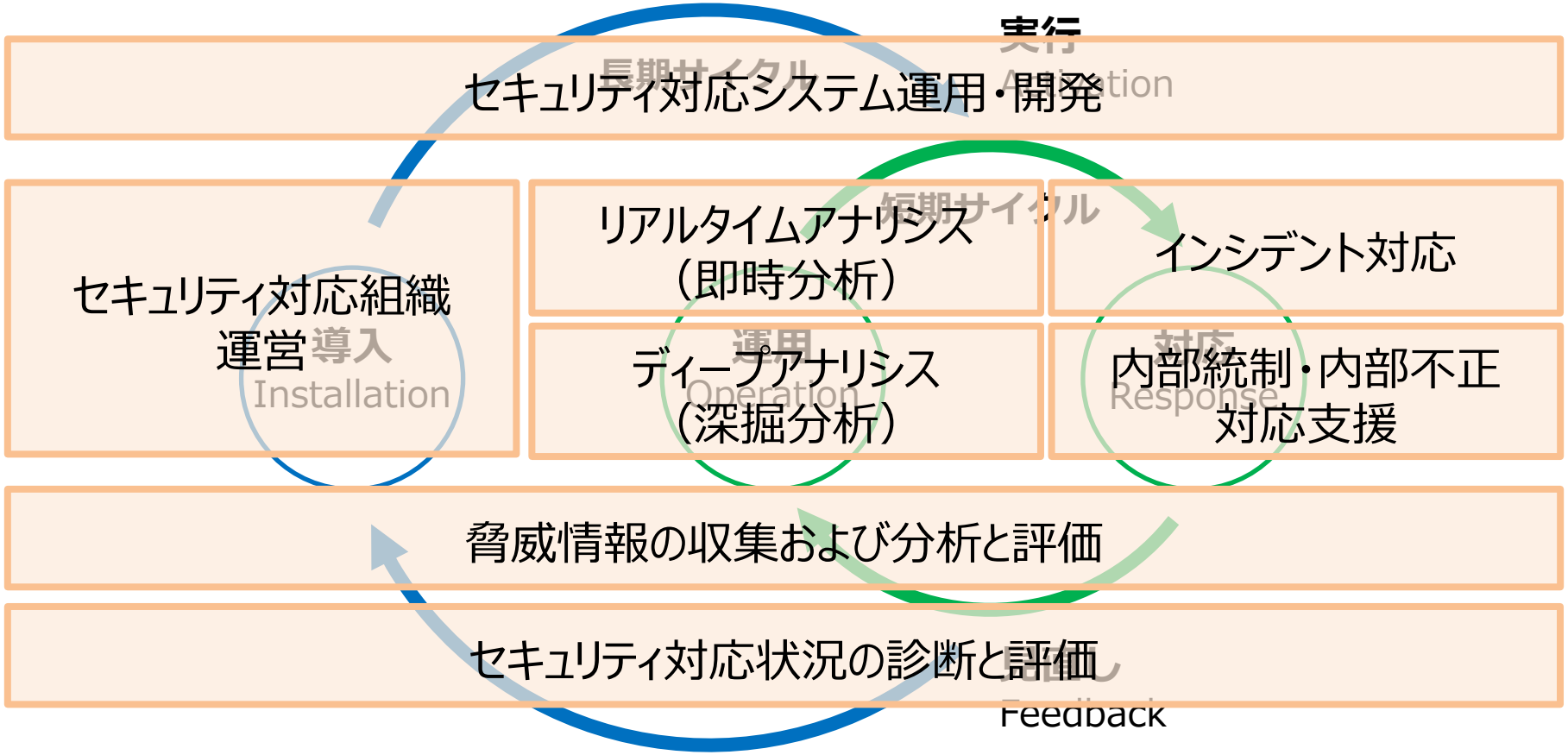
H. 内部統制・内部不正対応支援

内部統制の営みで必要となる監査データの収集や、内部不正に関する対応支援を行う機能。内部統制そのものや、内部不正捜査の支援を行うことを目的とする。

I. 外部組織との積極的連携

セキュリティ対応組織ではない組織（社外、社内問わず）との連携を行う機能。波及的なセキュリティレベル向上を目指すとともに、セキュリティ対応組織の存在価値を高め、自組織のさらなる発展、強化を目的とする。

セキュリティ対応実行サイクル



セキュリティ対応組織に求められる５４の役割

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

「失敗」を少しでも遠ざけるために…

1. セキュリティ対応としてどのような機能が求められるのかを把握する
   - 全体を把握せず組み立てると、必ず「穴」が生まれ、そこで破綻する
2. **自組織で何ができて何ができてなくて、どこまでやるべきなのかを考える**
   - どこまでやるのか決まっていないと、「やるやらない」「やれるやれない」で揉めて、そこから進めなくなる

セキュリティ対応における役割分担の考え方

どこまでを自組織で担い、どこからを専門組織に頼るべきなのかという役割分担を考えるために、以下の２つの指標を導入する。

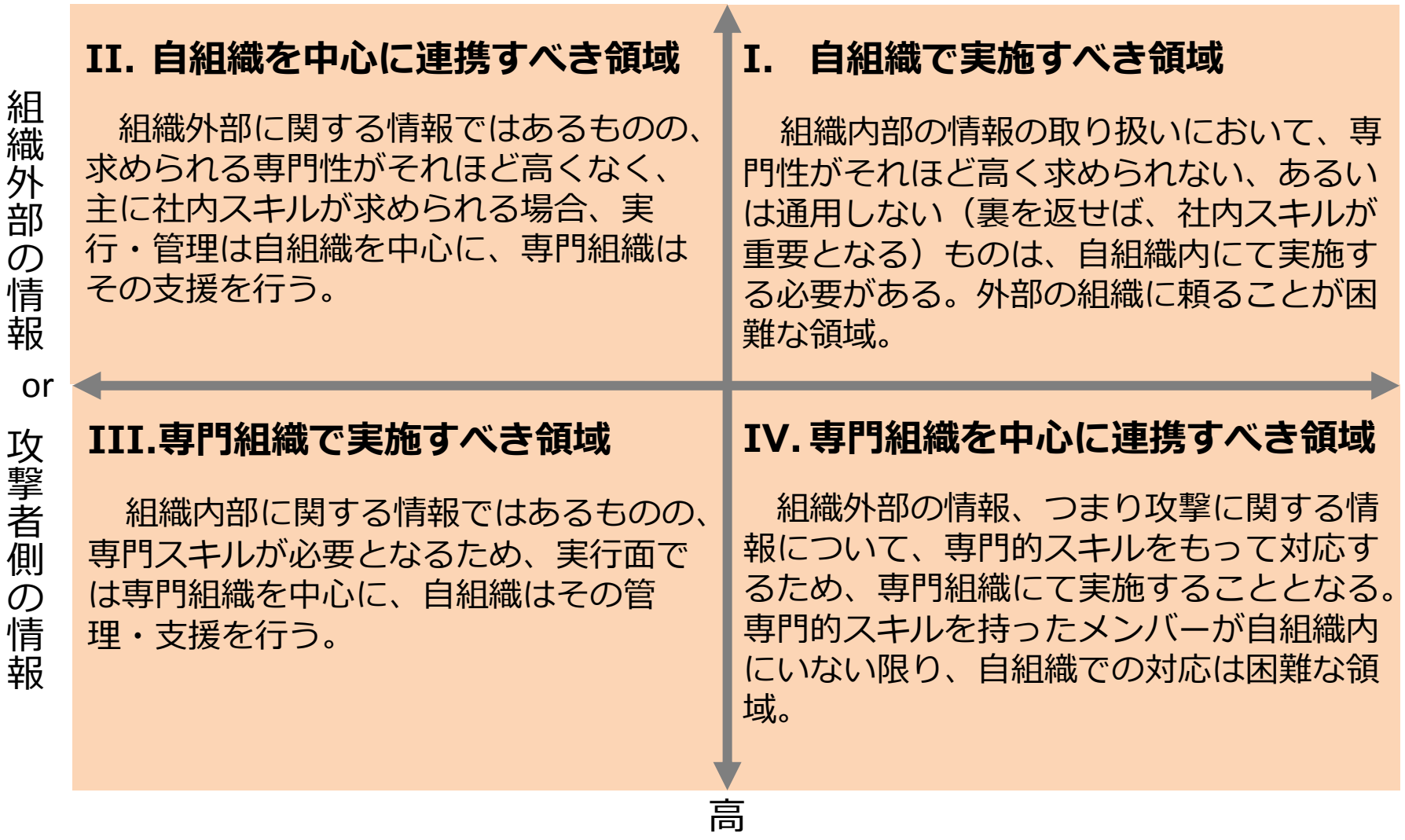
①　取り扱う情報の性質

取り扱う情報が、組織内部のものなのか、組織外部のものなのか。インシデントについては、攻撃の被害・影響に関連する情報は「内部」、攻撃そのものに関連する情報は「外部」というように考える。

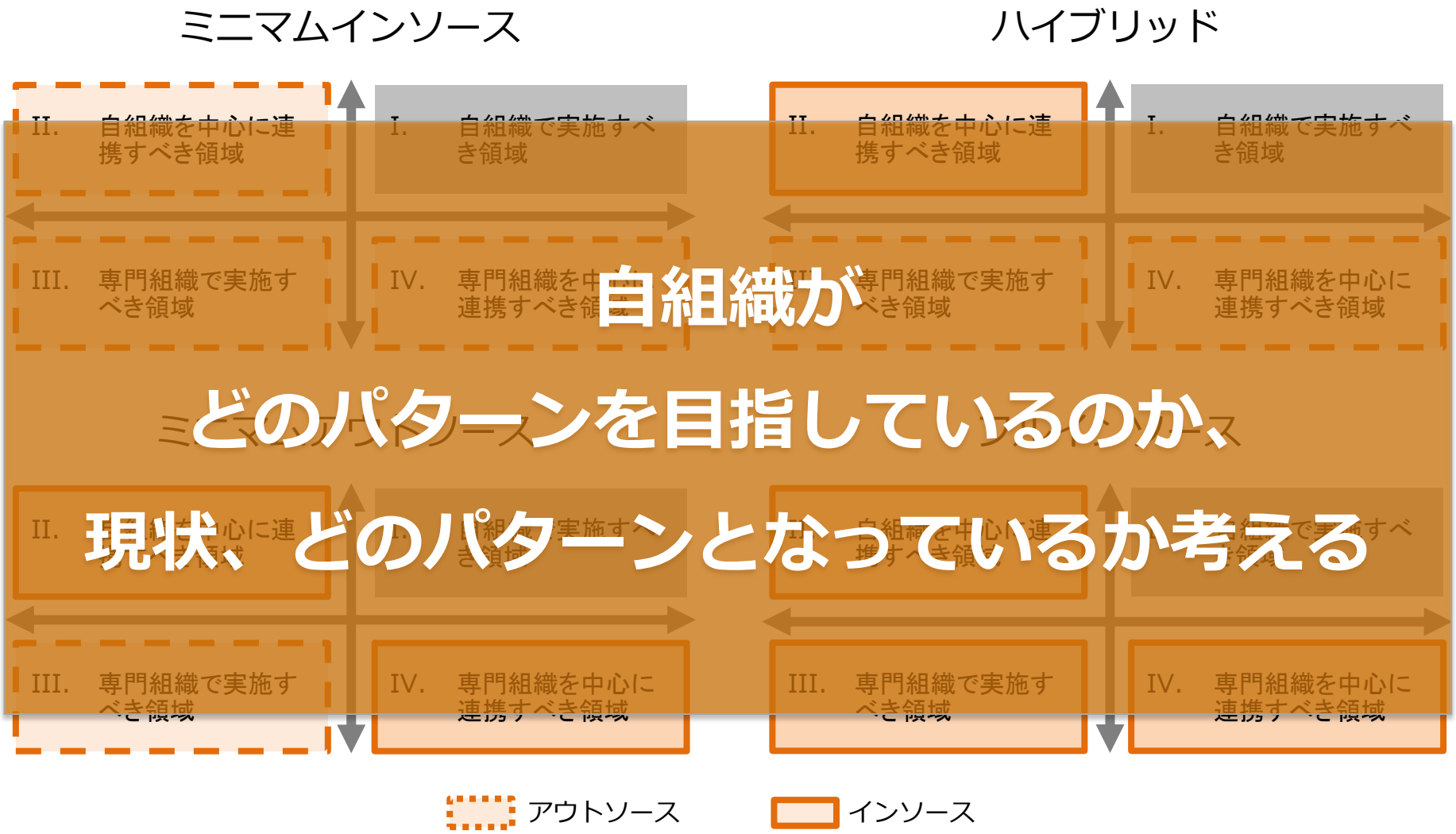
② セキュリティ専門スキルの必要性

役割を実行する際に、セキュリティ分野における専門性の高いスキルがどの程度必要とされるか。「セキュリティ専門スキル」は、どのような組織においても活用可能なセキュリティ関連スキルのことを指している。ちなみに、その対となるスキルは「社内スキル」で、これは異なる組織へそのまま転用しても通用しにくいスキルを指す。

セキュリティ専門スキルの必要性



セキュリティ対応組織のパターン



自組織が

どのパターンを目指しているのか、

現状、どのパターンとなっているか考える

参考：

５４役割の分類

人材育成/スキルについて

- JNSA「セキュリティ知識分野（SecBoK）人材スキルマップ2016年版」をベースに整理

表 2　SecBoK とのマッピング

機能	本紙での役割	領域	SecBokでの役割 1 CISO（最高情報セキュリティ責任者）	2 POC (Point of Contact)	3 ノーティフィケーション	4 コマンダー、トリアージ	5 インシデントマネージャー、インシデントハンドラー	6 キュレーター	7 リサーチャー	8 セルフアセスメント・ソリューションアナリスト	9 脆弱性診断士	10 教育・啓発	11 フォレンジックエンジニア	12 インベスティゲーター	13 リーガルアドバイザー	14 IT企画部門／コンサルタント	15 ITシステム部門／ネットワークアナリスト	16 情報セキュリティ監査人
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	–							○								
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	領域Ⅳ	–															
	B-2. リアルタイム高度分析	領域Ⅲ	–															
	B-3. トリアージ情報収集	領域Ⅳ	–															
	B-4. リアルタイム分析報告	領域Ⅳ	–															
	B-5. 分析内容問合受付	領域Ⅳ	–															
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	領域Ⅲ	–										○					
	C-2. デジタルフォレンジック	領域Ⅲ	–										○					
	C-3. 検体解析	領域Ⅲ	–															
	C-4. 攻撃全容解析	領域Ⅲ	–											○				
	C-5. 証拠保全	領域Ⅲ	–										○					
	D-1. インシデント受付			○														

SecBokで カバーされていない役割 ▼ NIST "NICE Cybersecurity Workforce Framework" とマッピング

表 2　SecBoK とのマッピング

機能	本紙での役割	領域	SecBokでの役割 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
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	領域Ⅳ	–															
	B-2. リアルタイム高度分析	領域Ⅲ	–															
	B-3. トリアージ情報収集	領域Ⅳ	–															
	B-4. リアルタイム分析報告	領域Ⅳ	–															
	B-5. 分析内容問合受付	領域Ⅳ	–															
セキュリティ対応システム運用	G-1. ネットワークセキュリティ製品基本運用	領域Ⅳ	–															
	G-2. ネットワークセキュリティ製品高度運用	領域Ⅲ	–															
	G-3. エンドポイントセキュリティ製品基本運用	領域Ⅳ	–															
	G-4. エンドポイントセキュリティ製品高度運用	領域Ⅳ	–															
	G-5. ディープアナリシス（深掘分析）ツール運用	領域Ⅲ	–															
	G-6. 分析基盤基本運用	領域Ⅳ	–															
	G-7. 分析基盤高度運用	領域Ⅲ	–															
	G-8. 既設セキュリティ対応ツール検証	領域Ⅰ	–															
	G-9. 新規セキュリティ対応ツール調査、開発	領域Ⅳ	–															
	G-10. 業務基盤運用	領域Ⅲ	–														○	

IT型人材育成という考え方

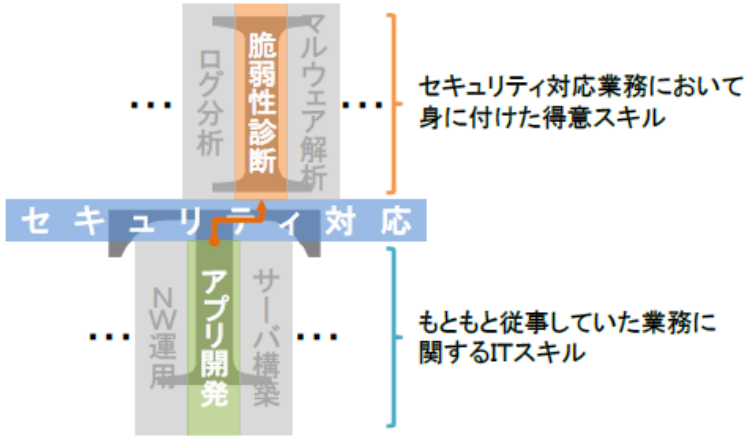


図 8　IT 型人材育成のイメージ

組織内の人材を
セキュリティ人材化する
育成方針の一つの例

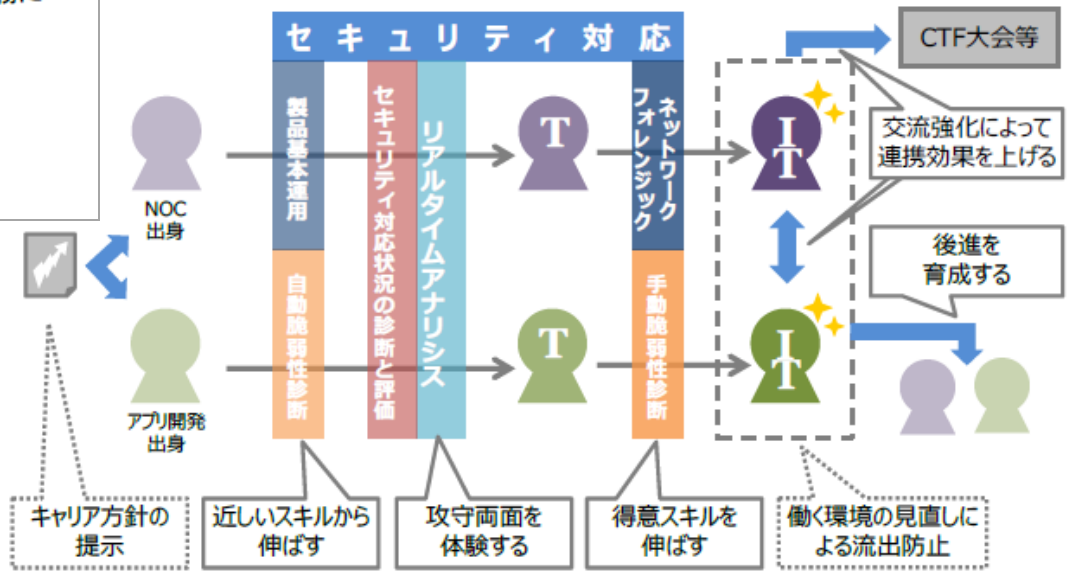


図 9　IT 型人材育成

今後について

- みなさまのご意見や、取り巻く環境の実態に合わせ、随時更新予定
- 本書をより使いやすくするため、機能や役割の充足度を見える化できるようなチェックリストや成熟度モデルについても模索中

ドキュメント作成における参考文献

- **SOCの役割と人材のスキル v1.0 (ISOG-J)**
  - http://isog-j.org/output/2016/SOC_skill_v1.0.pdf
- **Ten Strategies of a World-Class Cybersecurity Operations Center (MITRE)**
  - https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center
    - ➢ 翻訳版発行の実現に向け、ISOG-J WG6にて活動中
- **セキュリティ知識分野（SecBoK）人材スキルマップ2016年版 (JNSA)**
  - http://www.jnsa.org/result/2016/skillmap/
- **CSIRT 人材の定義と確保 Ver.1.0 (NCA)**
  - http://www.nca.gr.jp/imgs/recruit-hr20151116.pdf
- **National Cybersecurity Workforce Framework (NIST)**
  - http://csrc.nist.gov/nice/framework/