S O C / C S I R T

セキュリティ対応組織の教科書

～ 機能・役割・人材スキル ～

第 1.0 版

2016 年 11 月 25 日

日本セキュリティオペレーション事業者協議会 （ISOG-J）

改版履歴

2016/11/25	初版作成

目次

1. はじめに

本書「セキュリティ対応組織の教科書」は、SOC (Security Operation Center)や CSIRT (Computer Security Incident Response Team)と言ったセキュリティ対応組織において、どのような機能や役割、人材が必要となるかについてまとめたものである。

昨今、企業内の CSIRT 構築や企業内に閉じたプライベート SOC の構築が広く検討、あるいは実際に実行されるようになってきている。しかしながらその構築や運営にあたっては、セキュリティ対応に必要となる機能や役割をしっかりと理解している必要があり、そのうえで、例えば、自社でどこまで実現できるのか、専門業者へアウトソースすべきことは何か、というような組織の全体像も見据えた判断を行い、「名ばかり」にならない実行的な組織づくりを目指すことが重要となる。

本書では、セキュリティ対応を専門として実施しているセキュリティオペレーション事業者の視点から、改めてセキュリティ対応組織における実用的な機能や役割について整理する。

なお、本書は「SOC の役割と人材のスキル」の第 2 版として作成される予定だったが、内容の全面的な見直しに伴い、タイトルを一新し、新たなドキュメントとして発行する。

2. セキュリティ対応組織の存在意義

SOC や CSIRT といったセキュリティ対応組織を立ち上げることとなった契機や動機は、情報漏えい事故を発端にしたケース、同業他社に倣ったケース、役員の一言で決まったケース、親会社や監督省庁によるプレッシャーなど、企業によって異なる。組織の位置づけも、社長直下の場合もあれば、独立した部門の場合、ある部門に所属する一担当の場合など、こちらも異なる。

その理由は、各企業の事業戦略やその中のセキュリティ戦略に違いがあるからで、一言に「セキュリティ対応組織」と言っても様々な形態があり、それゆえ、ノウハウが集約されにくく、体系的に知識を得て実践することが難しくなってしまっている。

一方で、セキュリティ対応組織に共通していることもある。それは、目的が「事業におけるセキュリティリスクの低減」だということである。そのリスクが表出した事象を「インシデント」と呼ぶが、リスクの低減を実現するために、セキュリティ対応組織が叶えるべきことも、共通して概ね下記の二点になる。

- ✧ **インシデント発生の抑制**
- ✧ **インシデント発生時の被害最小化**

これらの実現があらゆるセキュリティ対応組織に共通する存在意義であり、以降の章では、その二点の達成に向け、可能な限り体系立てて、セキュリティ対応組織に求められる機能や役割等についてまとめていく。

3. セキュリティ対応組織の実行サイクル

セキュリティ対応組織についての詳細な機能を列挙する前に、SOC や CSIRT といったセキュリティ対応組織を実働させる大枠の実行サイクルについてイメージを持っていただきたい。具体的には、大きく 3 つの工程を 2 種類のサイクルで回していく必要がある。

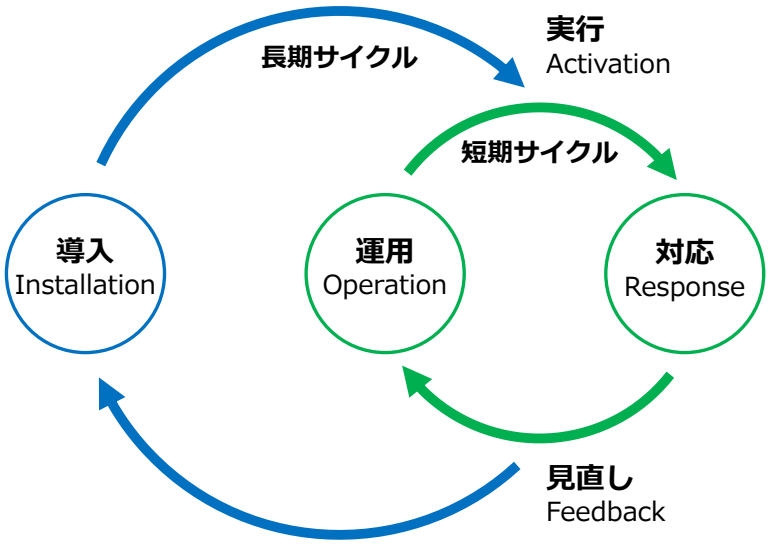

図 1　セキュリティ対応実行サイクル

- **導入**

「導入」では、セキュリティ対応の方針に基づき、その実行に必要となる仕組み（体制、業務プロセス、システムなど）の検討、構築、追加を行う。

- **運用**

「運用」では、導入された仕組みの定常的な実行と維持を行う。概ね平時の営みがこれにあたる。インシデント検知のための分析を行ったり（このような分析を行う組織は SOC と呼ばれることが多い）、セキュリティ対応システムの監視やメンテナンスなども行ったりする。

- **対応**

「運用」での分析で検知された事象に対し、インシデント対応を実行する。インシデント対応を行う組織は CSIRT と呼ばれることが多い。インプットは「運用」からだけとは限らず、自組織外からの申告や、外部団体からの通達などを発端にした対応も行う。概ね有

事の営みがこれにあたる。

- **短期サイクル**

「運用」と「対応」の業務が日々行われていく。その中で、業務プロセス上の問題点や、セキュリティ対応システムにおける課題が必ず発現するため、必ず見直しを行い、それらの課題に対し、導入された仕組みの中で、短いサイクルで改善を行っていく必要がある。例えば、単純業務の簡単な自動化や、分析精度向上のためのツール改善、レポート項目の見直しなどがそれにあたる。あくまで、割り当てられたリソース（人員、予算、システム）内での見直しが該当する。あえて図示はしていないが、当然ながら「導入」「運用」「対応」それぞれの中に閉じた見直しもある。

- **長期サイクル**

「短期サイクル」の見直しにおいて、導入された仕組みの中では解決できないような課題が挙げられた場合は、長期的な視点、計画をもって対応を行う。例えば、新たなセキュリティ製品の導入や、大幅なセキュリティ対応方針の見直し、運用基盤の大規模な構成変更などがそれにあたる。新たなリソースの割り当てが必要となるような見直しが該当する。

昨今の CSIRT 構築においては、「対応」の段階を中心に組織を組み上げセキュリティ対応を行っていこうとするケースが多く見られる。しかし、そこだけを切り取り組織化するだけでは、「運用」が上手く回らずインシデントを見逃してしまったり、そもそも自社の守りたいものがはっきりしない中でセキュリティ製品を選定してしまうなど、「導入」の時点で失敗したりと、様々な問題に直面してしまう可能性がある。

そうならないためにも、「導入」「運用」「対応」という軸をおさえ、「実行」と「見直し」によるサイクルを回していくというイメージを持つことが重要である。

4. セキュリティ対応組織の機能

セキュリティ対応組織の実行サイクルは、主に以下の９つの機能によって実現される。

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と共に、分析やインシデント対応の負荷削減へ繋がるよう、インシデントの予防、インシデント対応に関する練度の向上を目的とする。

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、ログ収集データベース、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、内部不正捜査そのものは内部統制部門や法務部門が主体となって対応することが一般的であるが、ログ提供や分析によりその対応の補助し、解決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。

実行サイクルの図に当てはめると、下記のようにまとめられる[1]。

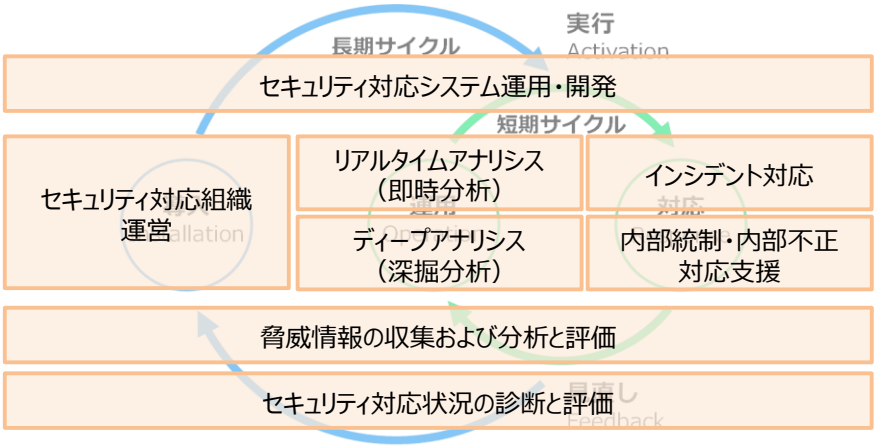

図 2　機能と実行サイクル

「セキュリティ対応組織運営」での決定方針に基づき、「セキュリティ対応システム運用・開発」において、その目的を満たすシステム実装によりセキュリティ対応を実行できるようにする。そして、そのシステムを活用しながら、「リアルタイムアナリシス（即時分析）」や必要に応じて「ディープアナリシス（深掘分析）」の運用を行い、何かインシデントたるものが発見されれば「インシデント対応」を行ったり、「内部統制・内部不正対応支援」を行ったりする。

これらの運用や対応の結果も含め「脅威情報の収集および分析と評価」により自社を取り巻く脅威を把握しつつ、「セキュリティ対応状況の診断と評価」により自社の守備力を評価する。その評価をもとに、すぐに実施できる改善は短期サイクルで実施し、より抜本的な見直しが必要な場合は、改めて「セキュリティ対応組織運営」で決定し、次なる「セキュリティ対応システム運用・開発」を実行するという長期的なサイクルを回すこととなる。

なお、必ずしも一つの組織内に全ての機能を保持し実行サイクルを回す必要はない。実情を鑑みても各機能が社内の別組織と連携しながら実行されるケースが一般的だろう。しかしながら、組織間で連携する場合には、非常に緊密な関係が維持される必要があり、物理的にも心理的にも近い状態であることが極めて重要である。

---

1 「外部組織との積極的連携」についてはどの役割にも付随するものであるため、図に含めていない。

5. セキュリティ対応組織の機能と役割

ここでは先の９つの機能についてそれぞれどのような役割を持つか説明をする。

A. セキュリティ対応組織運営

A-1. 全体方針管理

組織におい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、運営体制（24/365 なのか日勤だけなのか）などの、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（体制、業務プロセス、システム、人材育成、キャリアパスなど）の全体像把握しながら、今後行っていくべき取り組みなども管理していく。

A-2. トリアージ基準管理

全体方針として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）基準を取り決める。大きくは２つの基準を事前に定める必要がある。

- インシデント発生時のトリアージ基準
  想定される攻撃の種別、攻撃進行度や危険度[2]、アセットの重要度などによる分類を行う。
- 脆弱性発見時のトリアージ基準
  脆弱性を突かれた場合に想定される被害、攻撃の容易性、アセットの重要度などによる分類を行う。

いずれの場合も「インシデントとしない基準」も意識して定義すると、判断のぶれを軽減できる。

A-3. アクション方針管理

「A-2 トリアージ基準管理」に対し、それぞれの分類での具体的な対応（アクション）の方針を取り決める。トリアージ基準に相対させる形で、大きくは２つの方針を事前に定める必要がある。

- インシデント発生時のアクション
- 脆弱性発見時のアクション

ここで取り決めたアクションは、システム管理者など、実際に対処を行う関係者との共通認識とし、トリアージ基準に該当する際にただちにアクションに移れるようにしなけれ

[2] 攻撃の種別のネーミングや危険度は一意に定まった定義がなく、セキュリティ製品やサービスごとに異なるため、複数の製品・サービスを導入する際は整理が必要となる。

ばならない。

A-4. 品質管理

１週間あるいは１か月など、ある程度の期間において行われた各種の分析や対応について棚卸をし、対応品質に問題が無かったか確認する。対応先となった組織からのフィードバック（問い合わせ内容、意見など）も積極的に取り入れ、問題があった場合には是正しつつ、より高い品質での対応が行われるよう改善する。

A-5. セキュリティ対応効果測定

セキュリティ対応がもたらす効果を測定する。インシデント対応数や、セキュリティ装置による攻撃の遮断数、脆弱性管理の結果など、各機能からアウトプットを収集し、成果として取りまとめる。

A-6. リソース管理

セキュリティ対応するに当たり必要となるリソース（人員、予算、システムなど）の計画を行い、各機能に適切に配分する。

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

主に下記のようなログを監視し、リアルタイムに分析を行う。

- ファイアウォールなどのネットワーク装置からのログやネットフロー
- IPS/IDS などのセキュリティ装置からのログ
- AD や DNS などの各種システムからのログ
- ユーザ利用端末に関するログ

多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEM を利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットフローの情報も扱う。

B-2. リアルタイム高度分析

ログやネットフローの情報などの基本分析だけでは影響度やその内容が把握しきれない場合に、より詳細な分析を行う。例えば、専用のネットワークキャプチャ装置やセキュリティ装置に付随の機能で検知に関わるパケットキャプチャを取得したり、エンドポイントやサーバから必要なデータを即時取得したりして、より多くの証拠を元に、正確な状況把握、影響判断を行う。

B-3. トリアージ情報収集

トリアージとはインシデントの優先順位付けのことであるが、リアルタイム分析やPCAP 分析で収集しているデータだけその判断を行えないケースが出てくる。その場合、「E セキュリティ対応状況の診断と評価」の情報を参考にしたり、普段扱っていないログソースからさらに情報を収集したりする。自組織にそのログソースへのアクセス権限が無く、他組織との調整が必要な場合は、次節のインシデント対応の役割として扱われることもある。

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、被害端末の情報、攻撃手法、攻撃経路、情報漏えいの有無、影響度、すぐに行うべき短期的な対処策などを取りまとめ、ドキュメント化する。インシデント対応の引き金となるレポートであるため、対応に必要となる情報は最低限含まれるよう、項目は事前に取り決めておくことが望ましい。ただし、この時点での分析で全てが明確になるわけではなく、不明なものは不明と明記し、その他の機能で補完する必要がある。

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合せ対応を行う[3]。電話やメール、ウェブサイトでやり取りが行われる。応対の履歴をしっかり残すため、電話の利用は最低限にし、電話の内容についても改めてメールやウェブサイトに書き残すことが推奨される。

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

リアルタイム分析は即時性が求められるため、全てのネットワークログや PCAP を分析できていない場合があり、改めてそれらの分析を行う。また、リアルタイム分析の対象ではないログや PCAP がある場合には、合わせて分析対象とし、ネットワーク上で見られた挙動を明らかにする。

C-2. デジタルフォレンジック

必要に応じて、ネットワークだけでなく、被害に遭った端末やサーバの HDD/SSD、メモリ、外部記憶媒体などに保持されたデジタルデータ全般の分析を行う。ネットワーク上の挙動だけでは判断しにくい攻撃者が標的とした情報の特定、その漏えいの成功可否などを明らかにする。

---

[3]問合せ対応は集約効果が高いため、基盤運用の一時切り分けなど、他の機能におけるフロント業務の窓口としても活用される場合も多い。

C-3. 検体解析

各フォレンジックの過程において、マルウェアや攻撃者が配置したプログラムやスクリプト）が発見された場合、それらの機能を解析する。実際に動作させながら解析を行う動的解析や、リバースエンジニアリングによる静的解析などを組み合わせて実施する。

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。分析材料が不足している場合には、公開されている脅威情報なども参考に、仮説を組み込みながら、情報を補強していく。十分な証拠がそろっている場合には、攻撃者のプロファイル（所属組織、組織の活動目的など）の想定も試みる。

C-5. 証拠保全

サイバー犯罪捜査や法的措置を行う可能性がある場合には、分析の各過程において電磁的証拠の保全を行う。

D. インシデント対応

D-1. インシデント受付

主には運用からの分析報告を受け付ける。ただし、社内の別組織からの申告や社外の組織からの通報を受ける可能性もあり、この組織外からの受付窓口の存在は、専用のメールアドレスを準備するなどして、社内外に広く浸透させる必要がある。十分なリソースが無い場合には、「B-5 分析結果問合受付」を活用してもよい。なお、外部からのインシデント受付については、WHOIS データベースに登録してあるメールアドレス等が通報先として利用されることもあるため、登録情報は常に更新し、セキュリティ対応組織へ連絡内容が届くように（別の組織が受け付けている場合は内容が共有されるように）する。

D-2. インシデント管理

トリアージにより対応することが決まったインシデントについて、「A-3 アクション方針管理」での方針に従い対応されているか、インシデント分析の進捗状況など、対応状況の管理を、インシデント対応が完了するまで行う。

D-3. インシデント分析

受け付けたインシデント情報を、「A-2 トリアージ基準管理」に則り、対応可否および優先度を判断する。判断の材料が少ない場合には、「B-3 トリアージ情報収集」と連携する。トリアージ基準に該当しないような判断を行った場合には、「A-2 トリアージ基準管

理」へフィードバックを行う。判断後は、インシデントの全体像、直接的なビジネスへの影響（サービス停止に伴う損失、復旧/対策に必要となったコスト）や間接的な影響（社会的信用低下、業務効率低下）を究明する。その暫定対処策、最終的な再発防止策の検討も行う。情報の不足があり、分析が不十分な場合は「C ディープアナリシス（深掘分析）」と密に連携する。

D-4. リモート対処

実際のインシデント対応に当たり、優先度の低いインシデントにおいて、電話やメールで対応を行う。厳格な証拠保全が求められない場合には、リモートアクセス（リモートデスクトップや SSH など）で対処を完了させる。対処結果については「B リアルタイムアナリシス（即時分析）」へ必ず共有し、不要な分析、インシデント化が行われないようにする。

D-5. オンサイト対処

実際のインシデント対応に当たり、リモート対処では解決できない場合、あるいは厳格な証拠保全が求められる場合は、専門員が対処の必要となるシステムが存在する物理的拠点まで出向いて対応を行う。対処結果については「B リアルタイムアナリシス（即時分析）」へ必ず共有し、不要な分析、インシデント化が行われないようにする。

D-6. インシデント対応内部連携

内部関係者との連携、調整を行う。内部関係者とは、経営層、関連する社内他部門（システム部門や法務部門など）、および社外の協力組織（開発ベンダー、サービス提供事業者など）が挙げられ、主に「インシデントの全容解明を共に行うべき関係者」を指す。インシデントに関する報告や、情報共有、分析に必要なデータの共有などの調整を行う。

D-7. インシデント対応外部連携

外部関係者との連携、調整を行う。外部関係者とは、監督官庁、社外の取引関係組織、エンドユーザーが挙げられ、主に「インシデントによって影響を与えてしまう関係者」を指す。インシデントに関する説明や、被害状況の確認、具体的な被害内容の収集などの調整を行う。

D-8. インシデント対応報告

インシデント対応によって解明した、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を取りまとめ、ドキュメント化する。内部向け4の報告書と、外部向けの報告

[4] 忘れがちなのがリアルタイムアナリシス側へのフィードバックである。リアルタイム分析が正しかったのか、何らの対処が行われたのか、それによって解決できているのかなどが

書は粒度が異なるため、それぞれ作成する。この報告書の完成・配布によって、インシデント対応としては完了（クローズ）となる（対策の取り組みが長期化する場合には「A-1 全体方針管理」に引き継いで管理を行う）。

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。詳細な構成を全て完璧に理解するということではなく、各種ネットワーク装置とセキュリティ装置との位置関係やその種類、セキュリティ装置がインラインなのかそうではないのか、といったことがすぐに調べられるようにしておく。把握するにはシステム部門などの別組織との連携が必須となる。脆弱性管理だけでなく、分析やインシデント対応時の参照情報ともなる。

E-2. アセット情報収集

守るべき対象のサーバや端末、ネットワーク装置などのアセット情報を収集する。ISMS などでの情報資産管理情報をベースにしつつ、さらに詳細なファームウェアのバージョンや、インストールされているアプリケーションのバージョンなどまで収集できていることが望ましい。ただし、情報収集は非常に難しいため、ISMS 関連部門と連携し社内プロセスに情報の登録を義務付けるルールを策定したり、後述する脆弱性診断時の情報を集めたりする工夫が求められる。こちらも、脆弱性管理だけでなく、分析やインシデント対応時の参照情報ともなる。

E-3. 脆弱性管理・対応

脆弱性情報と前述のネットワークマッピングやアセット情報とを突合することで、対処が必要となるシステムを特定する。システムの管理主体へ通達を実施し、対処の進捗状況も合わせて管理していく。新たな脅威情報は「F-2 外部脅威情報の収集・評価」から受けるが、主要なソフトウェアや製品の脆弱性情報については、その提供元の Web サイトなどから随時収集する。

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無いかをツールを使って確認する。プラットフォーム診断、Web アプリケーション診断など、目的に合わせた診断の種類を選択する。ツールでの確認であるため、精度の問題はあるものの、低コストかつ短期間で実施できるため、より多くのシステムに対する定期的な診断も行う。

把握できないと、以降のリアルタイム分析結果の精度が上がらなくなってしまう。

E-5. 手動脆弱性診断

こちらは「自動」ではなく、専門の人員による「手動」で実施される。ツールと比較し、コストと時間はかかるものの、より精度の高い結果を得ることができる。重要度の高いシステムに対しては必ず行う必要がある。新システムの立上げ、大規模なシステム改修など、重要なマイルストーンに合わせた診断も行う。

E-6. 標的型攻撃耐性評価

標的型攻撃に対する自社の耐性を測るために、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。その結果は、社員教育に生かしたり、会社に対しセキュリティ対策の必要性を訴える根拠として活用したりする。

E-7. サイバー攻撃対応力評価

攻撃が起きたことを想定したシナリオに基づき、実際のセキュリティ対応の営みを発動し、滞りなくインシデント終息までたどり着けるか確認する（サイバー攻撃対応演習と呼ばれる）。問題があった場合は、原因の分析を行い、対応力の強化につなげる。

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（内部インテリジェンス）を収集する。自社内で発生しているインシデントの根本的な要因を分析し（システムの観点だけでなく、社内のルールやプロセスも含む）、中長期的な対策に繋げられるような整理を行う。合わせて、リアルタイム分析やインシデント対応そのものにおける課題点も整理することで、セキュリティ対応全体の改善へ繋げられるようにする。

F-2. 外部脅威情報の収集・評価

公開された新たな脆弱性情報、攻撃動向、マルウェア挙動情報や悪性 IP アドレス/ドメイン情報などの情報（外部インテリジェンス）を収集する。得られた情報の信頼度、自社に与える影響などを評価し、対応すべき脆弱性を取捨選択し、「E-3 脆弱性管理」へインプットする。情報ソースについては逐次見直しを行い、常に鮮度の高い情報を収集する必要がある。また、本来分析において発見されるべきであった事象や、その時点で対策が困難な情報を得た場合には、必要に応じて運用の見直しを行う。

F-3. 脅威情報報告

収集した内部脅威情報と外部脅威情報について取りまとめ、詳細も含めドキュメント化

する。月毎や四半期毎など、決まったタイミングで定点観測的に生成することが望ましいが、セキュリティを取り巻く状況の変化は目まぐるしく、あまり形にこだわり過ぎるとすぐに形骸化してしまうため、内容の見直しは必須であり、変更を恐れてはならない。また、想定される影響が甚大な脅威情報については、速報を準備する必要もある。

F-4. 脅威情報の活用

取りまとめた脅威情報は、セキュリティ対応に関わるすべての機能に対して周知が必要である。各機能において興味を持つ部分は異なってくるが、情報把握状況の偏りが無い状態にすることで、各機能のスムーズな連携が期待される。各機能へのより具体的な活用指示、あるいは逆に各機能からのフィードバックがなされるよう、セキュリティ対応方針管理の中でそのプロセスやルールを決める必要がある。

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

ファイアウォール、IDS/IPS、WAF、プロキシなどのネットワーク装置の運用を行う。ネットワーク構成を把握したうえで、ネットワークセキュリティ製品の種類、配置場所、設置構成（インラインかタップかなど）、機器/ファームウェアバージョン、設定内容などを管理する。各製品が適切に動作しているか、死活監視や検知シグネチャの更新の監視を行う。構成変更や設定変更がネットワークへ大きな影響を与える可能性があるため、作業についての手順やプロセスの策定が必須である。

G-2. ネットワークセキュリティ製品高度運用

IDS/IPS や WAF に代表される攻撃検知機能を持った製品において、製品ベンダーの検知シグネチャが不十分な場合に、独自にシグネチャを作成し（カスタムシグネチャ）、適用を行う。また、過剰な検知や誤った検知による検知ログの暴発や誤遮断の発生リスクを抑えるため、各シグネチャの特性を理解したシグネチャ設定ポリシー（マスターポリシー）の策定、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に代表される、エンドポイントでの対策製品の運用を行う。近年ではエンドポイントでのマルウェア挙動や脆弱性を突く攻撃を検知あるいは記録する機能を有するものもある。インストール漏れが無いか、パターンアップデートが適切になされているか、スキャン機能が有効かなどを監視し、可能な限り漏れのない管理を行う。

G-4. エンドポイントセキュリティ製品高度運用

エンドポイント対策製品において、そのエンドポイント内での不審なプログラムの活動を検知するため、レジストリの状態やプロセスの実行状況などを収集し分析する。必要に応じて、独自に IOC（Indicators of Compromise）を定義し（カスタム IOC)、それを元にエンドポイントで検知を行えるようにする。

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、マルウェア解析などで用いられるツールを運用する。深掘分析においては、扱うデータの中に機密情報や個人情報が含まれていたり、マルウェアなど非常に危険なプログラムが含まれていたりするため、ツールの利用方法や手順、作業の認可プロセスなど、厳重な管理が求められる。

G-6. 分析基盤基本運用

分析基盤とは、主にリアルタイムアナリシスにおいて、必要となるログデータを保存し、定常的に行われる分析を実現するシステムを指す。SIEM がこれに含まれる。どのようなデータをどれだけの期間保持するか決め、分析ルールのアップデートや追加を行う。データが保存できているか、分析処理が常時行えているかなどの監視を行う。

G-7. 分析基盤高度運用

市販の SIEM が取り込むことのできないシステムのログやパケットキャプチャデータなどを独自のシステムで保持し、それらを対象にした分析アルゴリズムやロジックおよびそれらが動作するシステムも独自に開発を行い、より詳細で精度の高い分析を実現する。

G-8. 既設セキュリティ対応ツール検証

既設のセキュリティ対応ツールにおいて、製品のバージョンアップや設定の変更を行う場合に、他システムや運用への、主に可用性についての影響を検証する。

G-9. 新規セキュリティ対応ツール調査、開発

一連のセキュリティ対応の中で新たな対策が必要となった場合、それを実現するための新たなツールの導入を検討する。市販製品の調査を行い、トライアル利用により、期待される効果を実現できるかや、現行の運用への影響度合いなどの確認を行う。要求を満たせる市販製品がなければ、独自開発を行う。

G-10. 業務基盤運用

業務基盤とは、上記の各種セキュリティ対応ツール運用や各種レポートの生成、問合せ対応、脆弱性管理システムなど、セキュリティ対応業務に必要な業務を実現するシステム

を指す。必要となる業務についてのフロー、プロセス、手順に基づき実装し、その他のシステムにおける不足機能の穴埋め、オペレーションミスの防止、作業の効率化や自動化を行う。

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

内部統制で必要となる監査データについて、収集すべきログを定義し収集する。必要に応じて、定型的なフォーマットに落とし込み、定期的なレポートとして関連組織が利用できるようにする。

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、セキュリティ対応組織で収集しているログからその活動内容について整理するなど、内部不正に対応している組織の支援を行う。

H-3. 内部不正検知・防止支援

発覚した内部不正の活動内容について分析し、ログから検知できないか検討し、可能な場合、検知ロジックとして実装する。検知した場合には、内部不正に対応している組織への連絡を行い、内部不正の抑止に貢献する。

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

実際のセキュリティ対応事例や統計的なデータを取りまとめ、身近な問題として社員に認識してもらえるよう、関連部門と連携し、ポータルサイトの作成や、ビデオ作成、ポスター配布、教材化などを通し、啓発を行う。

I-2. 社内研修・勉強会の実施や支援

セキュリティ対応において得られた専門的知見について、セキュリティに関する社内研修や勉強会を行い、セキュリティ対応組織以外の部門における理解度を高めていく。

I-3. 社内セキュリティアドバイザーとしての活動

社内のシステム開発や、お客さま向けのサービス運営などにおいてその主体となっている部門からのセキュリティに関わる相談を受け、アドバイスを行う。この活動を通して、Security By Design の浸透に貢献する。

I-4. セキュリティ人材の確保

人事組織と連携し、セキュリティ人材の確保を行う。優秀な人材を確保するための登用制度、人材を手放さないためのキャリアパス構築、スキルアップのためのカリキュラムの見直しや新設を検討する。他部門との人材交流による全社的なセキュリティレベルの向上なども視野に入れる。

I-5. セキュリティベンダーとの連携

購入したセキュリティ製品、あるいはセキュリティサービスについて、その提供元と直接対話できる関係を築く。セキュリティ対応の中で発見した不具合への対応要請や、改良すべき点についての前向きな意見交換を行う。

I-6. セキュリティ関連団体との連携

セキュリティ対応を行っている組織の集まり（NCA、各種 ISAC など）へ参加し、開示可能な範囲で積極的な情報交換を行い、情報共有、情報活用の輪を広げる。

6. セキュリティ対応組織の役割分担と体制

6.1. 日本における SOC・CSIRT の呼称について

具体的な組織論に入る前に、最もポピュラーなセキュリティ対応組織である SOC と CSIRT について、一般的に想定されている区分をおさらいする。イメージをクリアにするため、ここでは狭義の SOC（本書で言うところの、B、C の機能に限定）とする。

日本においては、インシデント対応の主体を CSIRT とした場合に、そのインシデントの発生を検知するためのセキュリティログ監視や、インシデント発生後の深掘分析（レスキューサービスあるいは緊急対応サービスと呼ばれる）を行う組織を SOC と呼称することが多い。

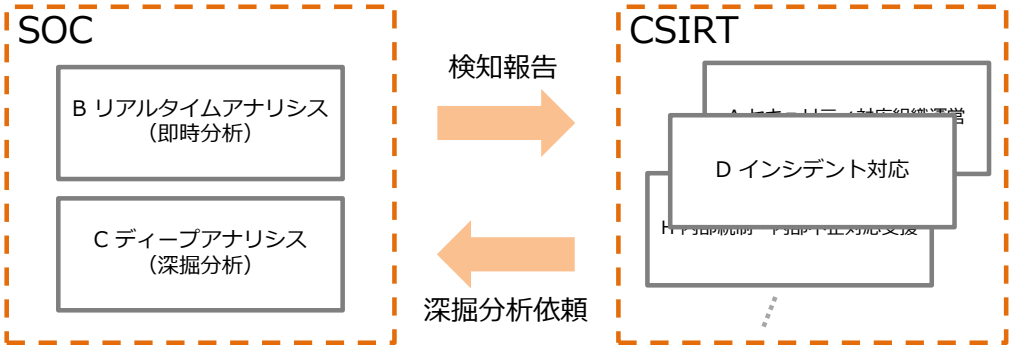

図 3　SOC と CSIRT の一般的な区分

しかし、昨今のセキュリティニーズ・意識の高まりにより、SOC はそのサービス範囲をインシデント対応の支援へ広げたり、CSIRT は基本的な分析は自身で行えるように技術レベルを上げたり、自組織内にプライベート SOC を持ったりと、その境界線は SOC 事業者や CSIRT の規模やレベルによって多様化してきている。よって、画一的な区分により、例えば「ここまでは CSIRT の役割だから自組織で、ここからは SOC の役割だから専門組織へお願いする」というような線を引くのは難しくなってきている。ではどのようにその区分を決めればよいか、次節ではその「線引き」について、考え方をまとめていく。

6.2. 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。

これらの指標を軸にすると４つの領域に分類することができる。

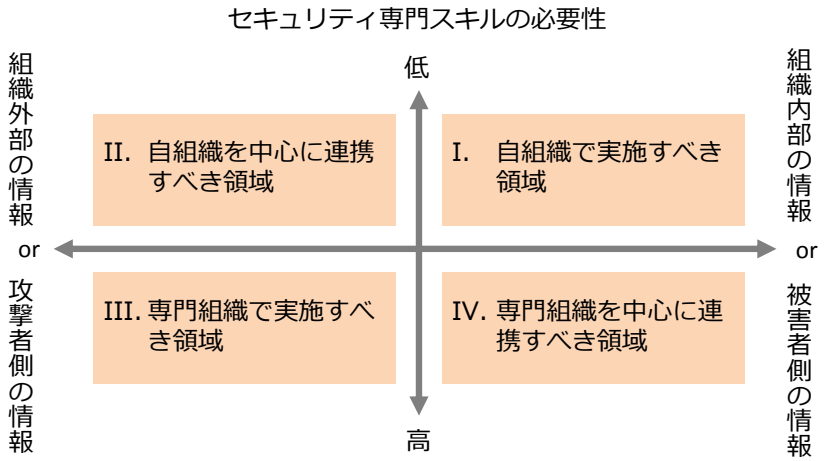

図 4　セキュリティ対応の4領域

領域I.　自組織で実施すべき領域

組織内部の情報の取り扱いにおいて、専門性がそれほど高く求められない、あるいは通用しない（裏を返せば、社内スキルが重要となる）ものは、自組織内にて実施する必要がある。外部の組織に頼ることが困難な領域。

領域II.　自組織を中心に連携すべき領域

組織外部に関する情報ではあるものの、求められる専門性がそれほど高くなく、主に社内スキルが求められる場合、実行・管理は自組織を中心に、専門組織はその支援を行う。

領域III. 専門組織を中心に連携すべき領域

組織内部に関する情報ではあるものの、専門スキルが必要となるため、実行面では専門組織を中心に、自組織はその管理・支援を行う。

領域IV. 専門組織で実施すべき領域

組織外部の情報、つまり攻撃に関する情報について、専門的スキルをもって対応するため、専門組織にて実施することとなる。専門的スキルを持ったメンバーが自組織内にいない限り、自組織での対応は困難な領域。

6.3. セキュリティ対応の組織パターン

セキュリティ対応組織のパターンは、前節で整理した自組織での実行が必須な領域 I 以外の 3 領域について、どこまで自組織のリソースでカバーするかで大別される。

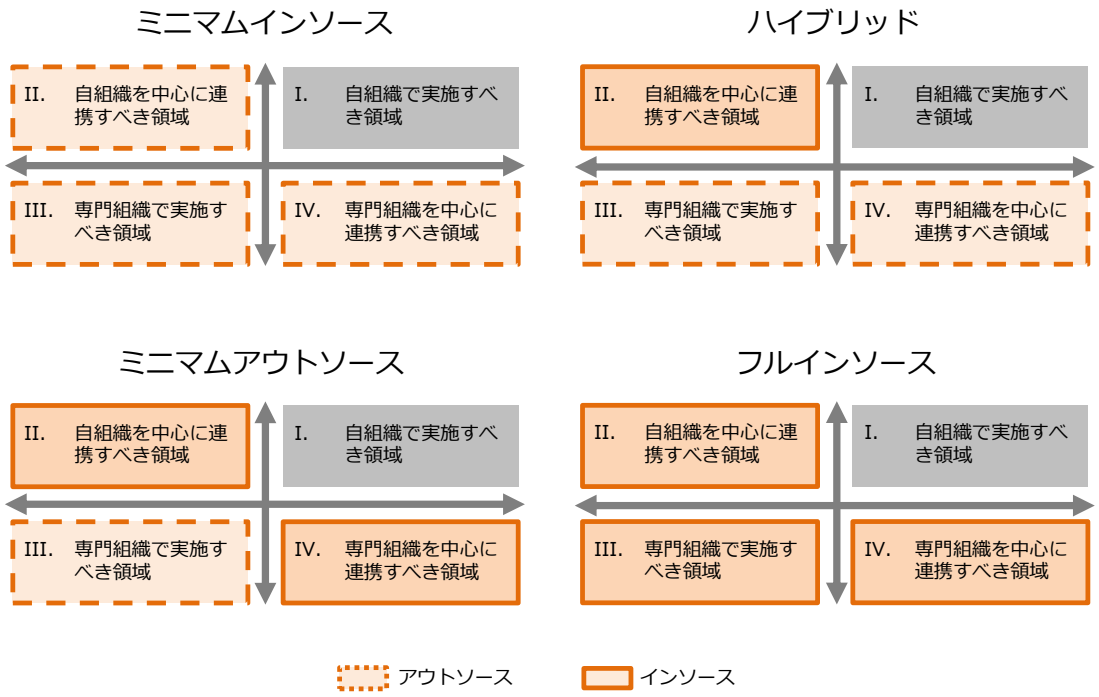

図 5　セキュリティ対応の組織パターン

パターン1.　　ミニマムインソース

自組織内にセキュリティ対応に関わる専門的知見がほとんどなく、領域Ⅱにおいても、外部の専門組織に大きく頼らなければならないパターン。例えば、非 IT 系のユーザ企業において総務部門等を主体としてセキュリティ組織を初めて作るようなケースでは実態としてこのパターンになる。

パターン2.　　ハイブリッド

自組織内でセキュリティ対応に関わる知見を最低限持ち、領域Ⅱにおいても自組織が中心となって実行できるパターン。例えば、ユーザ企業やそのシステム子会社が情報システムに関する専門部門を主体として組織を作るケースではこのパターンが多く、最も一般的な形態であると言える。

パターン3.　　ミニマムアウトソース

自組織内でセキュリティ対応に関わる知見を持ち、領域Ⅲ以外を自組織が中心となって

実行できるパターン。例えば、IT 系の企業において情報セキュリティに関する専門部門を主体として組織を作るケースではこのパターンが多い。

パターン4.　　フルインソース

自組織内で全てのセキュリティ対応機能・役割を担うことができるパターン。一部の IT 企業やセキュリティ専門企業あるいは、極めて高いセキュリティレベルが問われる特殊な組織においてはこのパターンが目標となる[5]。

[5]念のため断っておくが、「フルインソース」を絶対的な目標とする必要はない。自組織のスキルやリソースを鑑み、全体方針に従って必要な各機能・役割が満たされ実行サイクルが回るのであれば、アウトソース比率が大きくても何ら問題は無い。むしろ無理にインソース比率を高めてしまって実態が伴わないことの方が問題となる。

6.4. セキュリティ対応における役割分担

４領域に役割を割り振っていくと概ね下記のようにまとめられる。自組織の組織パターンを意識し、どんな役割をアウトソースすればよいか、インソースする場合にはどのような役割を実現する必要があるかといった検討の参考としてほしい。

図 6　セキュリティ対応の役割分担

6.5. セキュリティ対応組織の体制について

「機能」=「体制」となっていれば非常に議論はしやすいが、実態はそうではないため、この章で「体制」について整理する。
とは言え、実際の組織体制は各企業で千差万別であり、それらを加味しながら議論するのは非常に難しい。そのため、ここではあえて、CISO の配下に各機能・役割がフラットな体制で配置されているという理想的な前提でまとめていく。こういった体制は「フルインソース」パターンのセキュリティ専門組織・企業などにみられる。

具体的な体制について、次ページに表でまとめている[6]。「担当名」と「領域」のマトリックスの中に、「役割」を列挙している。

自組織の実態とは異なるとは思うが、これまで整理してきたとおり「役割」については明確であるため、「自組織の体制だとここは○○部門でやっているな、こっちは○○社に委託しているな」というように、頭の中でうまく当てはめていただければ幸いである。また、これからセキュリティ対応組織を作る場合には、こういった体制を念頭に、実際の体制づくりに生かしてほしい。

6

- 「領域」をⅠ・Ⅱ・Ⅳ・Ⅲの順としている。これは、専門組織への依存度が段々と高まるように並べたためである。
- 複数の担当に同じ役割が記載されているものは、共に取り組む可能性が高い業務である。実際のセキュリティ対応においてはより多くの担当が共同で対処に当たる場合ももちろんあるため、代表的な例として捉えていただきたい。なお、同一担当内の連携は当たり前のものとして考え、表が複雑化しないよう、同じ役割を複数の領域に記載することは避けている。

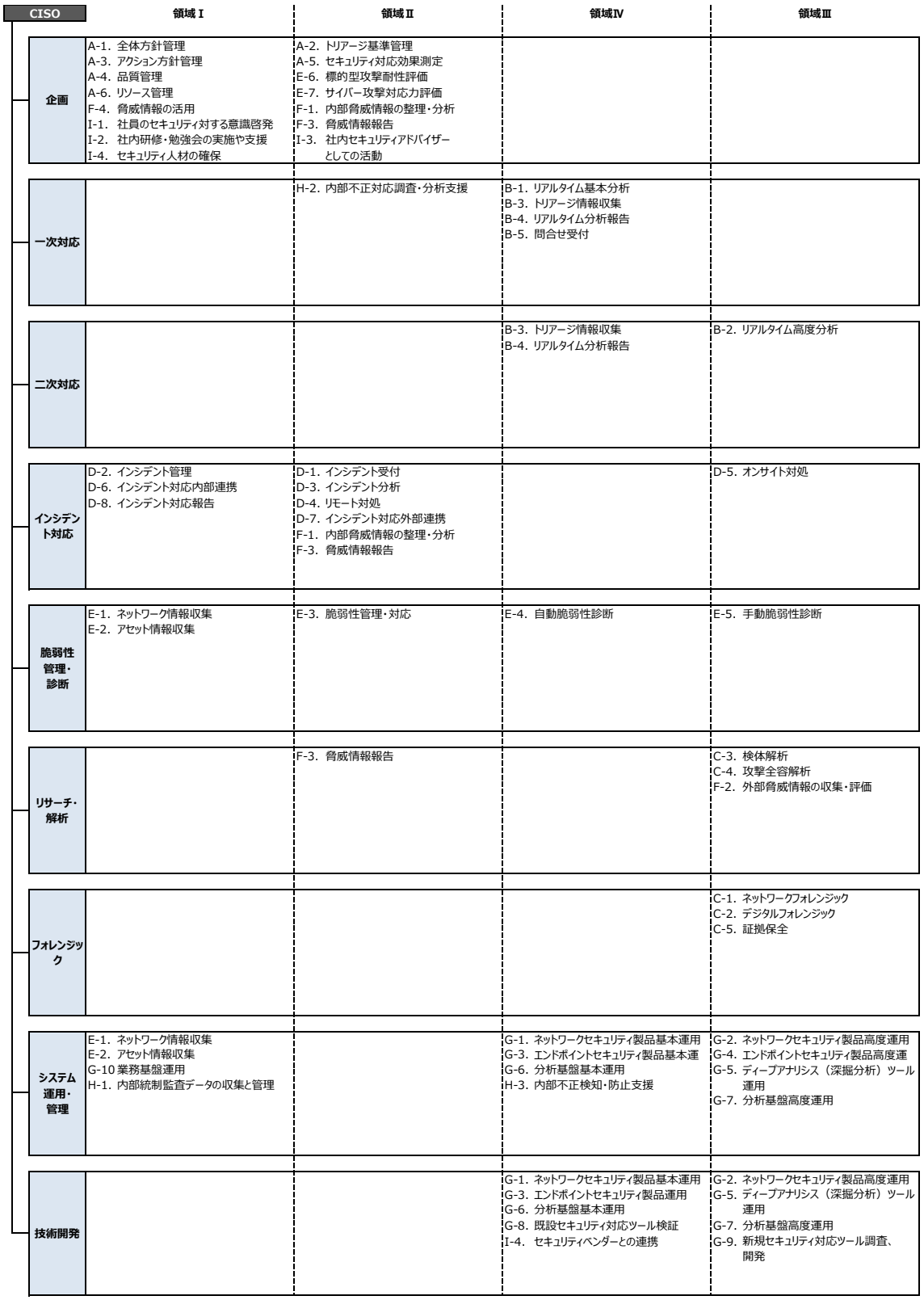

図 7　セキュリティ対応の組織体制

6.6. セキュリティ対応組織の要員数について

セキュリティ対応組織の体制の検討において、必要となる人材の数は非常に重要な観点の一つとなる。自組織が行うべき領域Ⅰ・Ⅱについては、自組織の人員や社内で既に存在する別部門の人員など、ある程度これまでの業務の延長線上で、実行する機能・役割さえ見えてくれば想定は可能だろう。一方で、その延長線上にはなく、組織によっては全く新しい機能・役割となることもある領域Ⅲ・Ⅳについては人員の想定が難しい。

しかし、この領域Ⅲ・Ⅳこそが、自組織でカバーすべきかアウトソースするかと言う大きな判断が必要な部分であり、その判断ためにも、必要人員の算出シミュレーションを避けては通れない。

本節では、前節の体制表の領域Ⅲ・Ⅳの要員について、自組織で確保し稼働させるシミュレーションとして 4 つのモデルケースにまとめた。

	Level 0	Level 1	Level 2	Level 3
一次対応	日勤 1 名	日勤 2 名	常時 1 名 (全 6 名)	常時 2 名 (全 12 名)
二次対応	日勤 1 名	日勤 1 名	日勤 2 名	常時 1 名 (全 6 名)
インシデント 対応	二次対応が 兼務	日勤 1 名	日勤 1 名	日勤 2 名
脆弱性 管理・診断	二次対応が 兼務	インシデント 対応が兼務	インシデント 対応が兼務	インシデント 対応が兼務
リサーチ・ 解析	しない	二次対応が 兼務	二次対応が 兼務	日勤 1 名
フォレンジック	しない	しない	二次対応が 兼務	リサーチ・ 解析が兼務
システム 運用・管理	日勤 1 名	日勤 2 名	日勤 2 名	日勤 3 名
技術開発	日勤 1 名	日勤 1 名	日勤 1 名	日勤 2 名
合計	4 名	7 名	12 名	26 名

表 1　セキュリティ専門性の高い役割の要員モデル

Level 0

必要なチームを最小人数で構成し、フォレンジックやリサーチ・解析などは諦め、非常に単純な対応ルールでセキュリティ対応を行う最小モデル。立上げ最初期の試験的チーム体制の目安となる。実際にはインシデントが一つ起こっただけで対応は手いっぱいになり、セキュリティ関連システムに少しでも障害が発生すればシステム管理側も手いっぱいになるため、領域Ⅰ・Ⅱの体制でこちらの領域を支援できない限り、実行的な体制にはなりえない。

Level 1

実行的な体制として最低限の構成。24 時間 365 日の対応やフォレンジックは実施しないものの、必要最低限の対応は可能なモデル。もし別組織に NOC（ネットワークオペレーションセンター）などの 24 時間 365 日体制が存在しているのであれば、「一次対応」や「システム運用・管理」のうち手順化が容易な業務を一部委託し、補完し合うと良い。

Level 2

セキュリティ専門の 24 時間 365 日体制を持つモデル。この規模の体制を持つことができれば、一通りのセキュリティ対応を実現できる。いわゆるプライベート SOC を自組織に構えたいのであればこの体制がスタートラインとなる。なお、Level 2 および後述の Level 3 では体制の効率化のため、「システム運用・管理」における一次切り分けの機能を「一次対応」に含めるものとし、システム運用・管理における 24 時間 365 日体制を不要としている。

Level 3

1 社のセキュリティを見るというよりは、全国の支店、支社やグループ会社など、関連する複数の大組織をまとめて対象とするような SOC モデル。グローバル企業の場合は、Level 3 の規模を拡大して 1 拠点に集約するか、各リージョンの事業規模に応じて Level 1 か Level 2 の体制をブランチとして配備し、最も事業規模の大きなリージョン設置した Level 3 にその統括もさせるような階層型になる。

7. セキュリティ対応組織の人材スキルと育成

ここではそれぞれの役割での必要なスキルについてまとめる。

7.1. 「SecBoK」による整理

まずは、JNSA が取りまとめた「セキュリティ知識分野（SecBoK: Security Body of Knowledge）スキルマップ 2016 年版」をベースに整理する。SecBoK は、米国国立標準技術研究所（NIST）が作成した“NICE Cybersecurity Workforce Framework (NCWF)”に原則準拠する形で整理されている。

SecBoK においても「役割」が定義され、それごとにスキルがまとめられている。本節では、その「役割」と本紙での「役割」をマッピングすることで、SecBoK のスキルと紐付けられるよう次ページに整理した[7]。詳細なスキルについては、このマッピングを参考に、SecBoK を参照いただきたい。

なお、脆弱性診断に関わるスキルについては、ISOG-J と OWASP Japan の共同ワーキンググループにおいて非常に詳細なスキルマップを公開している。こちらも合わせてぜひ参考としていただきたい。

- 脆弱性診断士(Web アプリケーション)スキルマップ
  - http://isog-j.org/output/2014/pentester-web-skillmap-201412.pdf
- 脆弱性診断士（プラットフォーム）スキルマップ＆シラバス
  - https://www.owasp.org/index.php/File:Pentester-Platform-Skillmap_and_Syllabus-201604.pdf

[7]
- SecBoK の「役割」と本紙での「役割」が必ずしも 1 対 1 で対応しているわけではないため、複数の「○」が付く部分がある。
- 「CISO（最高情報セキュリティ責任者)」については本紙では扱っていないため、対象外（”-“表記）としている。

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 コマンダー、トリアージ ノーティフィケーション	4 インシデントマネージャー、インシデントハンドラー	5 キュレーター	6 リサーチャー	7 セルフアセスメント・ソリューションアナリスト	8 脆弱性診断士	9 教育・啓発	10 フォレンジックエンジニア	11 インベスティゲーター	12 リーガルアドバイザー	13 IT企画部門／コンサルタント	14 ITシステム部門／ネットワークアナリスト	15 情報セキュリティ監査人	16
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	–										○					
インシデント対応	D-1.	インシデント受付	領域Ⅱ	–	○														
	D-2.	インシデント管理	領域Ⅰ	–				○											
	D-3.	インシデント分析	領域Ⅱ	–			○								○				
	D-4.	リモート対処	領域Ⅱ	–															
	D-5.	オンサイト対処	領域Ⅲ	–															
	D-6.	インシデント対応内部連携	領域Ⅰ	–	○														
	D-7.	インシデント対応外部連携	領域Ⅱ	–	○											○			
	D-8.	インシデント対応報告	領域Ⅰ	–			○	○											
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	領域Ⅰ	–					○									○	
	E-2.	アセット情報収集	領域Ⅰ	–					○									○	
	E-3.	脆弱性管理・対応	領域Ⅱ	–					○			○							
	E-4.	自動脆弱性診断	領域Ⅳ	–								○							
	E-5.	手動脆弱性診断	領域Ⅲ	–								○							
	E-6.	標的型攻撃耐性評価	領域Ⅱ	–									○						
	E-7.	サイバー攻撃対応力評価	領域Ⅱ	–									○						
脅威情報の収集および評価と分析	F-1.	内部脅威情報の整理・分析	領域Ⅱ	–					○										
	F-2.	外部脅威情報の収集・評価	領域Ⅲ	–					○	○									
	F-3.	脅威情報報告	領域Ⅱ	–		○													
	F-4.	脅威情報の活用	領域Ⅰ	–		○													
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	–														○	
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	領域Ⅰ	–															○
	H-2.	内部不正対応調査・分析支援	領域Ⅱ	–											○	○			
	H-3.	内部不正検知・防止支援	領域Ⅳ	–															
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	領域Ⅰ	–									○						
	I-2.	社内研修・勉強会の実施や支援	領域Ⅰ	–									○						
	I-3.	社内セキュリティアドバイザーとしての活動	領域Ⅱ	–									○						
	I-4.	セキュリティ人材の確保	領域Ⅰ	–									○						
	I-5.	セキュリティベンダーとの連携	領域Ⅳ	–															
	I-6.	セキュリティ関連団体との連携	全領域	–															

見ていただくとわかるとおり、自組織が行うべき領域Ⅰ・Ⅱについては、SecBoK でカバーされているものの、専門性の高い領域Ⅲ・Ⅳにおいては多くが未整理となっている。これらについては次節で整理を行う。

7.2. 「NICE」による整理

SecBoK では未整理となっている役割について、SecBoK と同様に“NICE Cybersecurity Workforce Framework (NCWF)”をベースとしてスキルを別表にまとめた。それぞれの役割でどのようなスキルが必要になるかの参考として欲しい。

並べてみると、かなり広範囲のスキルが求められることがわかる。それゆえ人材の確保、人選が難しいのだが、どの人材も初めから多くのスキルを持てるわけではない。次節では、その人材スキルがどのように広がり、また、専門家として尖っていくのか考察する。

7.3. IT 型人材育成

「セキュリティ人材」というと「トップガン」や「ホワイトハッカー」という言葉に代表されるように、非常に尖った専門性を有するイメージが持たれている。一般的には、ある分野に突出した人材は「I 型人材」と呼ばれるが、その確保は非常に難しい。近年でこそ、産学共にサイバーセキュリティに注目し、セキュリティ領域の研究をする学生が増えたり、「SECCON」や「Hardening Project」で活躍する若者が増えたりしているものの、そういった人材はセキュリティ業界が争奪戦を繰り広げ、ユーザ企業は特にリーチしにくい状況にある。

ユーザ企業では、初めはセキュリティサービスを受けることで最低限のスキルを得て、場合によってはセキュリティアナリストを外部から召喚し常駐してもらう、転職エージェントに人材を探してもらうなど色々な工夫をしながら、それでも間に合わず、結局のところは社内の技術要員を育成せざるをえない状況になってしまうことが多いのではないだろうか。

仮に運よく「I 型人材」を招くことができたとしても、実際のセキュリティ対応組織においては前節でまとめたように幅広いスキルが求められるため「トップガンがいれば何とかなる」というものではなく、現実的には、ある得意領域にプラスして社内スキルも含め「広い知見」を持った、いわゆる「T 型人材」になってもらう必要がある。しかし、そのI 型人材がそういった方針を理解し、組織に馴染んでくれるかもまた別の問題として存在する。

そこで必要となるのは「**IT 型人材育成**」である。

初めはセキュリティ領域ではない IT スキルで実力を磨き、その後、実行的なセキュリティ対応組織を通して、セキュリティに関する様々なスキル領域を体験する（T 型化)。その中で、これまでの彼の能力にマッチした、あるいは新たに目覚めたセキュリティスキル領域を選択し、さらにそこを伸ばしていってもらう（I 型化)。このように、I 型と T 型が融合した育成が「IT 型人材育成」である。

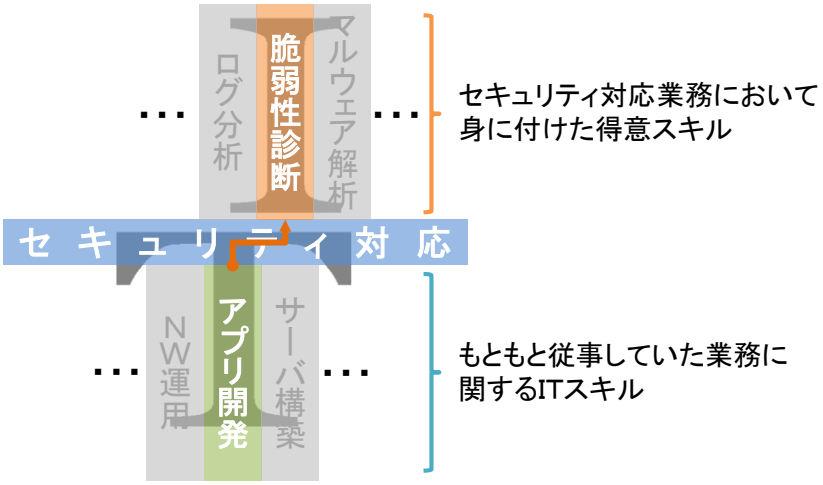

図 8　IT 型人材育成のイメージ

今現在、セキュリティ業界において実行的に活躍している人材においても、セキュリティ領域を出自とせず、ソフトウェア開発やネットワーク運用、システム管理など、他の IT スキル領域を生業としていた人材は多く、企業側が意識していたかどうかはともかく、結果として IT 型人材育成のようになってきたと考えられる。

「IT 型人材育成」においては、もともと保持していた IT スキルと親和性の高い役割をはじめに与えることが重要である。例えば、ネットワーク運用を行っていた人材であれば「ネットワークセキュリティ製品基本運用」を、監査に関わっていたのであれば「内部統制監査データの収集と管理」を、Web アプリケーション開発者であれば「自動脆弱性診断」を、という具合である。基礎スキルが身についているため、成長が促進される。

役割のマッチングは、過去の経歴から候補となる役割を絞り込んだ状態で面談するとよい。この面談においては、業務経歴の他に個人的に身に着けている IT スキルがないかも差支えのない範囲で答えてもらうと、選択肢が広がる可能性がある。優秀なエンジニアは「趣味の範囲で」と言いながらも、本業とは若干異なる IT スキルを有していることがある。幅広いスキルが求められるセキュリティ対応においては、そのスキルが生かされる場面が必ずと言っていいほど訪れるため、そういった個人的なスキルの把握も重要である。

過去の経歴と親和性の高い役割でセキュリティに関する最初のスキルを身に着けた後は、「セキュリティ対応状況の診断と評価」のいずれかの役割か「リアルタイムアナリシス（即時分析）」のいずれかの役割を経験すると、前者は、新旧の攻撃や脆弱性とその対策について幅広く学びつつ、社内にどのようなシステムがあるかなども理解することができ、後者は、実際に日々発生している「生」の攻撃と、その対処を学ぶことができる。様々なパタ

ーンの攻守両面を経験することが重要となる。

これらの経験を経たのち、「インシデント対応」の業務にて、攻撃の実害を目の当たりにし、関連部門と共に実際にインシデントを収束に導く体験をすることで、社内のセキュリティ対応の「いろは」を経験した「T 型人材」になるだろう。

これらの経験を行う中でも、自身が好むスキルについては、手を動かす機会が自ずと増えるため、他の人材よりも伸びてきていることがわかるはずである。そのスキルを発揮できる役割へステップアップさせ、そのまま興味、志向を貫き「I 型」として特化できるように支援していく。

また、このような IT 型のスキルアップが期待されるということは、キャリアパスやキャリアプランの方針として、早いうちから育成対象の人材に提示しておくことが大切である。道筋が見えることで迷いなく役割を担うことができるはずである。

IT 型育成に成功した人材の意見は積極的に取り入れ、もし本人にモチベーションがあれば、後進育成に直接関わってもらうことで、さらに組織の育成力を高めることができる。

育成対象人材が複数いる場合は、CTF（Capture The Flag）のイベントや、セキュリティ団体の活動などにグループとして参加させると、お互いの存在が刺激となり、良い影響を与え合う関係になる場合がある。また、このような異なる役割を持った人材同士の交流は業務における部署間の連携においても大きな効力を発揮するため、非常に重要な施策となりうる。

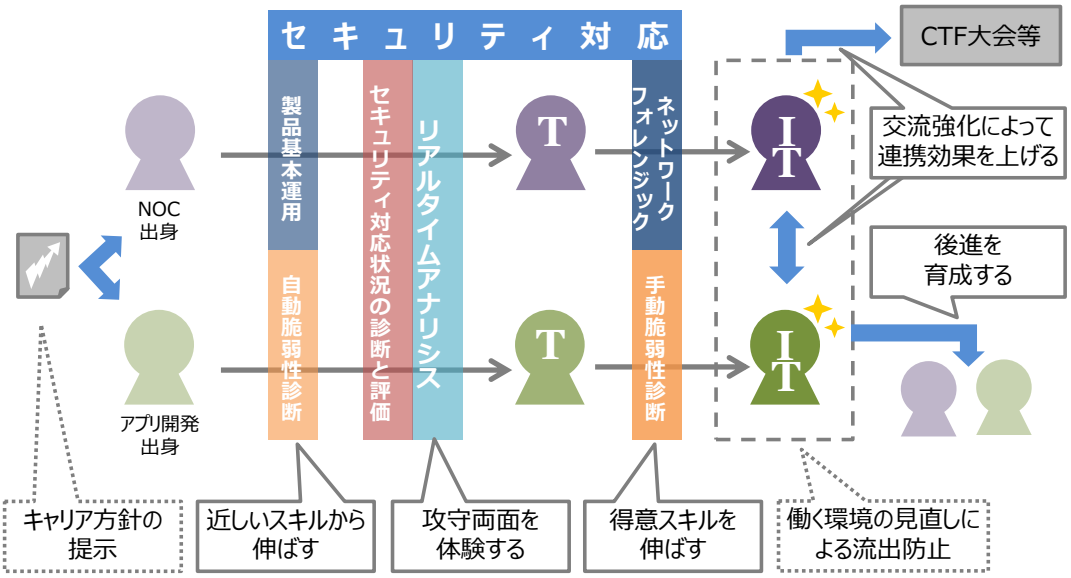

図 9　IT 型人材育成

一方で、気を付けなければならないのは、人材の流出である。現在、セキュリティ人材については売り手市場であり、転職が容易であるだけでなく、ヘッドハンティングも大々

的に行われているため、IT 型人材の流出は大きな懸念事項となる。IT 型人材についての業務内容、労働環境、待遇、裁量などは適宜見直す必要があることは決して忘れてはならない。セキュリティ人材に限ったことではないが、「やりたいことをやれるのか」という部分が重視されることも多いため、働く環境や裁量については特にケアが必要となる。

8. おわりに

本書では、セキュリティ対応組織に求められる機能・役割・スキルについてまとめた。これらの機能や役割全てを満たす組織を作り上げることは非常に難しく、現実的には段階を踏んで少しずつ形作られるものである。本書を通じて、今何ができていて何が足りないのか、これから何をすべきなのか、その把握に少しでも役立てていただければ幸いである。

自組織の「できていること、できていないこと」、あるいは「できているレベル」を認識することはセキュリティ対応能力を向上させるうえで大切なことであり、その点では、「成熟度モデル」と言うような形で、誰もが客観的に自組織の状態を把握できるような指標が必要なのかもしれない。また、今後もセキュリティを取り巻く環境は変化しつづけることは容易に想像できるため、本書のアップデートも継続的に行っていきたい。

日本セキュリティオペレーション事業者協議会 （ISOG-J）は引き続き、セキュリティオペレーション事業者の連携によって生まれるノウハウやナレッジを広く提供していく。

9. 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
- 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/

執筆　　阿部 慎司（ISOG-J / NTT セキュリティ・ジャパン株式会社）

協力　　ISOG-J　セキュリティオペレーション連携 WG（WG6）