SOCの役割と人材のスキル

1.0版

2016/7/11

ISOG-J セキュリティオペレーション連携WG (WG6)

改版履歴

年月日	版	内容	備考
2016/7/11	1.0	初版	

はじめに

- 企業内で、セキュリティの対応を行う組織の構築や運用を始める際には、SOCやCSIRTと言った組織の名称はあるものの、実際には監査部門やシステム部門との連携も必要であり、どのような機能や役割、どのような人材が必要となるかが課題となっている。
- そこでセキュリティオペレーション事業者の視点でどのような役割があり、どのような人材が必要かを整理する。
- 初版としては、セキュリティの対応を行う組織全体としての機能と役割を明らかにする。

セキュリティの対応を行う組織の立ち上げから

- 大きく3段階あり、本書では運用の段階について注目をする
- セキュリティ事業者が主たる対応を行うものについては、本書ではアウトソースと表記する

導入

・セキュリティの対応について設計や構築を行う。

・サービスを受けて実現する場合は、セキュリティの要件とサービス内容のマッチングを行う。信頼の置けるサービス事業者に相談することをお勧めする。

運用

・監視して検知を行う部分を運用とする。運用監視をSOCサービスと呼ばれることが多い。

・運用実態にあった組織体制や連携ができるようにすることを本書にて整理する。

インシデント対応

・運用段階で検知した結果、インシデントとしての対応をする段階はこちらとなる。インシデントレスポンスを行う組織をCSIRTと呼ばれることが多い。

・検知だけに閉じず、組織での対応含めて行うものはこちらの段階となる。

セキュリティの対応を行う組織の持つ機能

- セキュリティの対応を行う組織として持つべき機能は以下の8つの機能とする
- 各機能は社内の別組織と連携して行うものも含む

機能	概要
リアルタイム分析	監視の結果からリアルタイムで対応を決定する
脅威情報と傾向分析	脅威情報を取り扱う
インシデント対応と分析	インシデント対応を実施する
インシデント：証拠の分析	得られた証拠の分析を行う
ツールのライフサイクルのサポート	利用するツールの開発や維持管理を行う
監査と内部犯行対応	監査と内部犯行についての対応を行う
診断と評価	脆弱性診断により評価を実施する
外部との連携	社内外との対応を行う

セキュリティの対応を行う組織の持つ機能と役割(1/10)

- 「リアルタイム分析」機能の持つそれぞれの役割と概要は以下である

機能	役割	概要
リアルタイム分析		
	コールセンター	・レポートやサービスの内容などの一次問い合わせ窓口
	NWログ分析	・IPS/IDS等のログを分析する
	PCAPログ分析	・PCAPデータによる詳細分析を行う
	トリアージ情報収集	・リアルタイムな監視からの短時間での分析
	分析妥当性確認	・オペレーターの分析の精度を確認する
	全体分析品質確認	・各チームにおける分析結果、顧客のフィードバックから、分析品質の把握を行う
	業務範囲の管理	・取り扱うインシデント/対応範囲の定義と判断

セキュリティの対応を行う組織の持つ機能と役割(2/10)

- 「脅威情報と傾向分析」機能の持つそれぞれの役割と概要は以下である

機能	役割	概要
脅威情報と傾向分析		
	脅威情報の収集・分析	・新たな脆弱性情報や、攻撃動向/攻撃トレンド、通信特徴や悪性IP/ドメイン情報などのネットワークアクティビティを調査収集する ・脅威情報を評価し、対応優先度や顧客への影響度を判断する ・脅威情報から長期的な動向を分析する
	脅威情報の配信	・集めた脅威情報を配信し、社内外と共有する
	脅威情報の作成	・インシデント対応で得られた結果から脅威情報を生成する
	定期レポートの生成	・監視における検知アラートや発生インシデントについてのレポート作成
	対策への組み込み	・脅威情報を対策へ組み込む ・検知機能や分析能力、対策提案などの機能強化に役立てる

セキュリティの対応を行う組織の持つ機能と役割(3/10)

- 「インシデント対応と分析」機能の持つそれぞれの役割と概要は以下である

機能	役割	概要
インシデント対応と分析		
	オンサイトでのインシデント対応	・インシデントの対応を現地にて実施する
	リモートでのインシデント対応	・インシデントの対応を遠隔操作で実施する。方法としては、電話やメールでの対応、場合により遠隔からのログインなどを行う
	インシデント分析	・インシデントであるかの判定、トリアージ ・詳細ログ解析の必要有無の検討 ・マルウェア解析の必要有無の検討 ・顧客への発生したインシデントの通知 ・インシデントについての問い合わせ対応
	侵入手口の分析	・どのように侵入が行われたかを分析し、現在の対策へ落とし込むための理解をする
	対策の実現	・インシデントレスポンスの結果から、どういった機器にどんな対策を行うか検討する

セキュリティの対応を行う組織の持つ機能と役割(4/10)

機能	役割	概要
インシデント対応と分析		
	インシデント対応の調整役	・顧客に影響があるような情報の収集などの調整を行う。
	監督官庁との連携	・インシデント発生時に監督官庁との窓口や連携を行う
	サプライチェーンとの連携	・インシデント発生時にビジネスに関連する企業への影響を考慮し連携を行う
	事業部門やSIerとの連携	・インシデント発生時にセキュリティ組織と当該組織の連携を行う。場合により当該組織のシステムを管理運用するSIerと連携を行う
	経営層との連携	・インシデント発生時にビジネスインパクトの分析結果を踏まえて経営層に状況の報告や対策の提案を行う
	ビジネスの影響の分析	・インシデントが事業における影響を分析する
	インシデントクローズ宣言	・インシデント対応の完了宣言をする
	インシデントクローズ報告	・インシデント対応の結果を報告する

セキュリティの対応を行う組織の持つ機能と役割(5/10)

- 「証拠の分析」機能の持つそれぞれの役割と概要は以下である
- 「インシデント対応と分析」の機能から切り出されて、フォレンジックに特化した機能としている

機能	役割	概要
証拠の分析		
	フォレンジックの証拠の取り扱い	・フォレンジックで得られたデジタルの証拠の保管や管理を行う
	マルウェアや仕掛けられたものの分析	・侵入に使われたマルウェアや仕掛けられたものを分析する
	フォレンジックの証拠の分析	・ディスクのイメージやトラフィックデータ、モバイルの端末などの証拠を分析する ・ビジネスへの影響分析に必要となる情報収集、サマリの提出など

セキュリティの対応を行う組織の持つ機能と役割(6/10)

- 「ツールのライフサイクルのサポート」機能の持つそれぞれの役割と概要は以下である
- システム管理部門と連携して行う機能である

機能	役割	概要
ツールのライフサイクルのサポート		
	境界面で防御するデバイスの管理	・ファイアウォールやメールのプロキシやコンテンツフィルタなどの運用を行う
	資産管理	・センサーやデバイスなど含めた資産管理を行う
	SOCのインフラの管理運用	・SOCで利用するツールなどの管理運用を行う
	監視設備（センサ以外も含む）のメンテナンス	・監視運用にかかるルールや手順の設計策定/承認/周知適用を行う機能 ・監視基盤の開発/デプロイ/機能追加/バグ修正/機能説明
	インシデント対応製品導入支援	・インシデント対応で利用するセキュリティ製品導入や支援

セキュリティの対応を行う組織の持つ機能と役割(7/10)

機能	役割	概要
ツールのライフサイクルのサポート		
	センサーのチューニングと維持管理	・IDS,IPS,SIEMと言ったセンサーの管理や運用を行う ・適用ポリシーチューニング（適用シグネチャ管理） ・検知精度および分析対象の検知量のコントロール
	カスタムシグネチャの作成	・センサー機器でのカスタムシグネチャを脅威情報から作成する ・検知ルール作成（カスタムシグネチャ等）
	ツールの開発と配備	・利用するツールについて、市場調査やプロトタイピングや開発を行い、ツールを更新する ・不足機能の穴埋め、オペミス防止、作業効率化、自動化
	ツールの研究開発	・ツールの研究開発を実施する
	製品情報収集/検証	・監視センサーなど現在利用している製品の調査や検証 ・監視センサーなど今後導入する製品の調査や検証 ・手順書の作成

セキュリティの対応を行う組織の持つ機能と役割(8/10)

- 「監査と内部犯行対応」機能の持つそれぞれの役割と概要は以下である
- 監査や内部調査が行えるよう支援をする機能である
- 監査自体はセキュリティの対応を行う組織の範囲からは外れる

機能	役割	概要
監査と内部犯行対応		
	監査データの収集と配布	・監査で利用するデータを収集する。要求に応じてデータを提供できるようにする。
	監査コンテンツの作成と管理	・監査で利用するためにSIEMやログ管理からデータを抽出する
	内部犯行事案のサポート	・内部犯行が起きていないか調べたり、起きている際には情報収集や分析の支援を行う
	内部犯行事案の調査	・内部犯行が起きた時に対応を行う

セキュリティの対応を行う組織の持つ機能と役割(9/10)

- 「診断と評価」機能の持つそれぞれの役割と概要は以下である
- 監視やインシデント対応の前段としての予防的な診断や評価を行う

機能	役割	概要
診断と評価		
	ネットワークのマッピング	・システム部門などから提出された情報の確認を行う ・確認のために現状のネットワークや機器のマッピングを行う
	アセット情報収集	・顧客のアセット情報の調査収集を行う ・アセット情報を活用するため、分析チームへ提供する
	脆弱性診断	・脆弱性診断を行う
	侵入テスト	・侵入テスト（ペネトレーションテスト）を実施する。RedTeam。
	脆弱性の評価	・システムを調査結果、脆弱性がどこにあり、どう対応するか報告する。Blue Team。

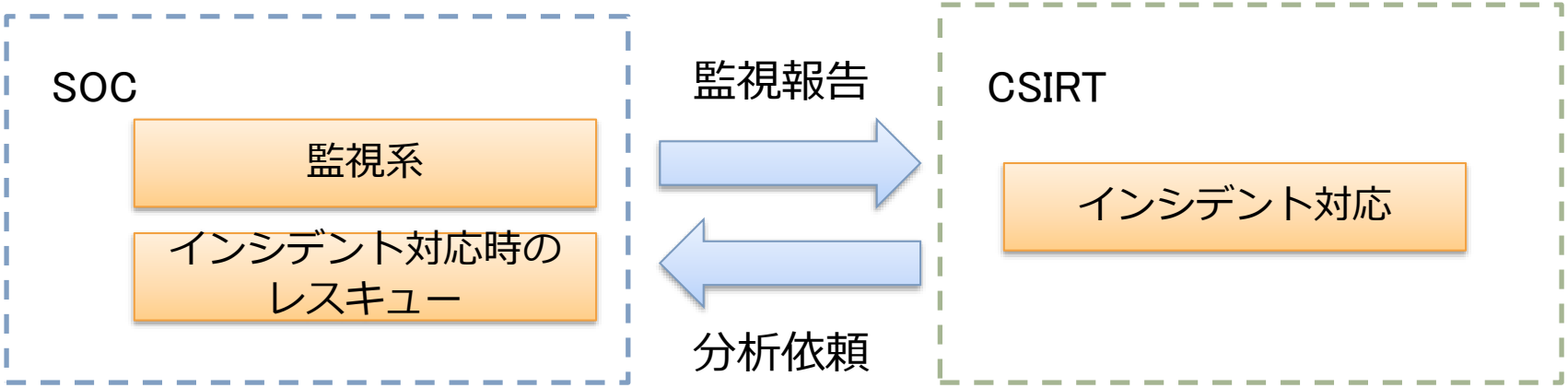
セキュリティの対応を行う組織の持つ機能と役割(10/10)

- 「外部との連携」機能の持つそれぞれの役割と概要は以下である
- 社内の他の組織の支援や連携を行う
- 支援や連携の例として広報や教育部門を想定する

機能	役割	概要
外部との連携		
	製品の評価	・社内で利用したいツールについて、セキュリティの観点から評価を行う。
	メディア対応の窓口支援	・ニュースメディアとの窓口の支援を行う
	研修や啓発	・社員に向けた研修や啓発の資材を用意して研修を支援する
	内部への把握している状況の公開	・セキュリティの対応で得られている情報を取りまとめて社内へ公開する。
	セキュリティコンサルティング	・社内における、ネットワークからの防御以外の部分についてセキュリティの観点からアドバイスを行う
	外部への脅威情報の公開	・監視やインシデント対応によって得られた情報を公開できる形式にして外部へ公開する

日本におけるSOC,CSIRTの呼称について

- セキュリティの対応をする組織については、社内の他組織とも連携しつつ一体で防御を行うべきである。
- 日本においては、監視やインシデント対応時のレスキューサービスをSOC、インシデント対応をする組織をCSIRTと呼称する場合が多い。



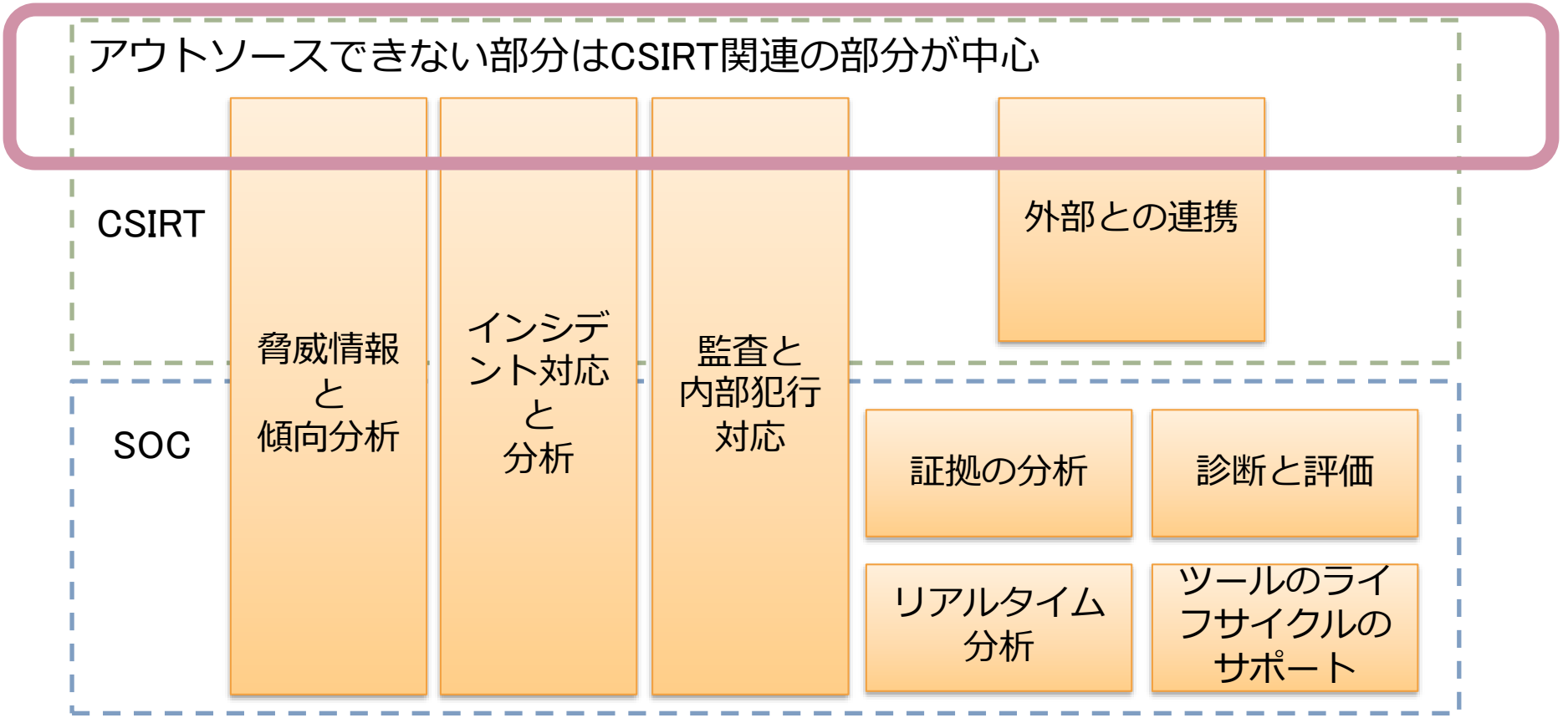
セキュリティの対応を行う組織の持つ機能と組織の関連

- それぞれの機能が主にSOC,CSIRTのどちらで実現されるかを示す

機能	組織
リアルタイム分析	SOC
脅威情報と傾向分析	SOC,CSIRT
インシデント対応と分析	SOC,CSIRT
証拠の分析	SOC
ツールのライフサイクルのサポート	SOC
監査と内部犯行対応	SOC,CSIRT
診断と評価	SOC
外部との連携	CSIRT

SOC,CSIRTの機能とアウトソースの活用

- 機能の内容によってはアウトソースが活用できない部分が存在している
- 社内での意思決定や判断、他部署との連携が必要な部分のアウトソースはできない
  - GRCのG：ガバナンスの部分はアウトソースができない



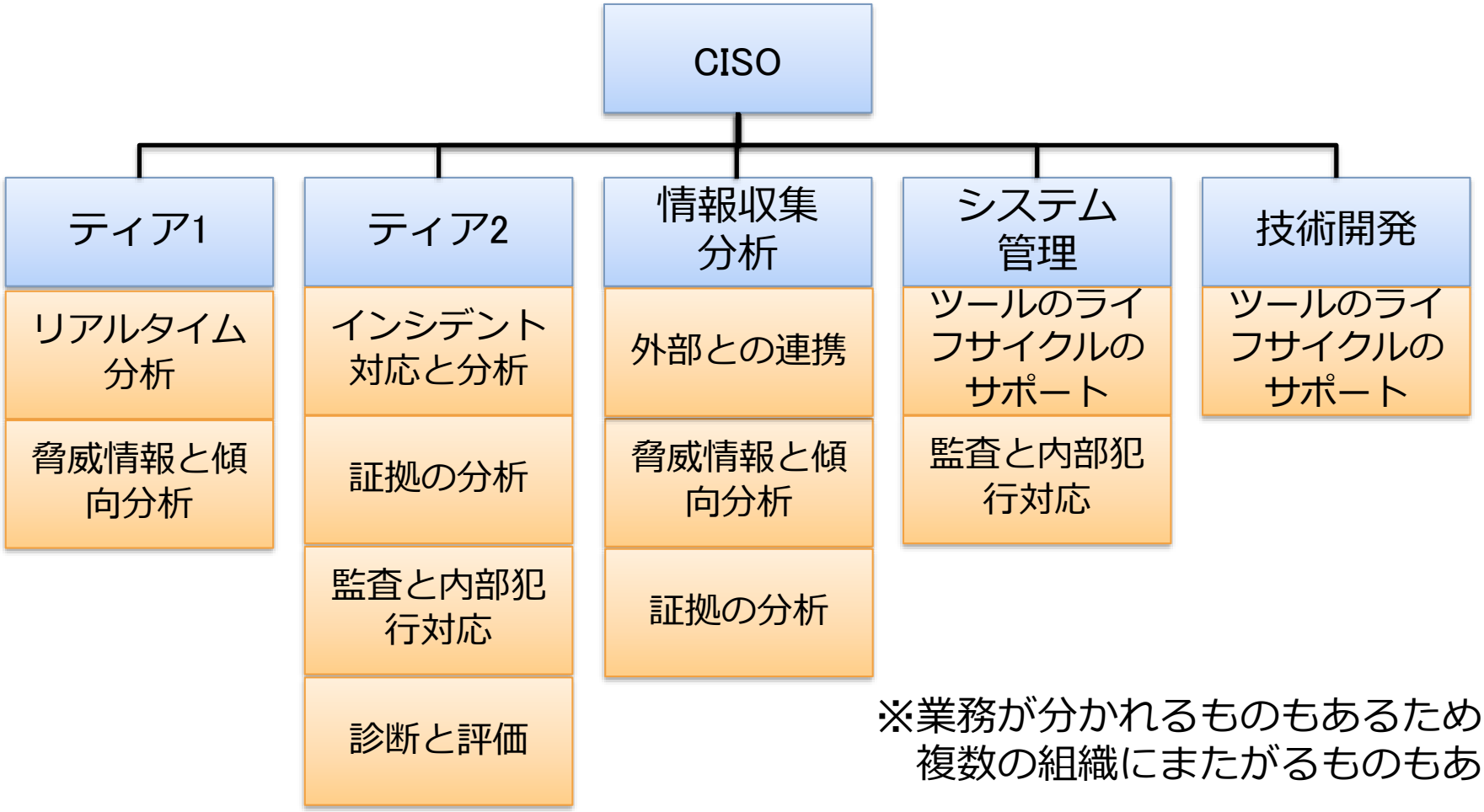
セキュリティの対応を行う組織の内部組織

- セキュリティの対応を行う組織の持つ内部の組織は以下である
  - 機能ついては、複数の組織に分散しているものもある

組織	機能
ティア1 （監視）	リアルタイム分析 脅威情報と傾向分析のための情報収集
ティア2 （高度な分析）	インシデント対応 証拠の分析 監査と内部犯行対応 診断と評価
情報収集・分析 （専門知識の活用）	脅威情報と傾向分析 証拠の分析 外部との連携
システム管理	ツールのライフサイクルのサポート 監査と内部犯行対応
技術開発	ツールのライフサイクルのサポート

セキュリティの対応を行う組織の組織図例

- セキュリティの対応をする組織図の例は以下である

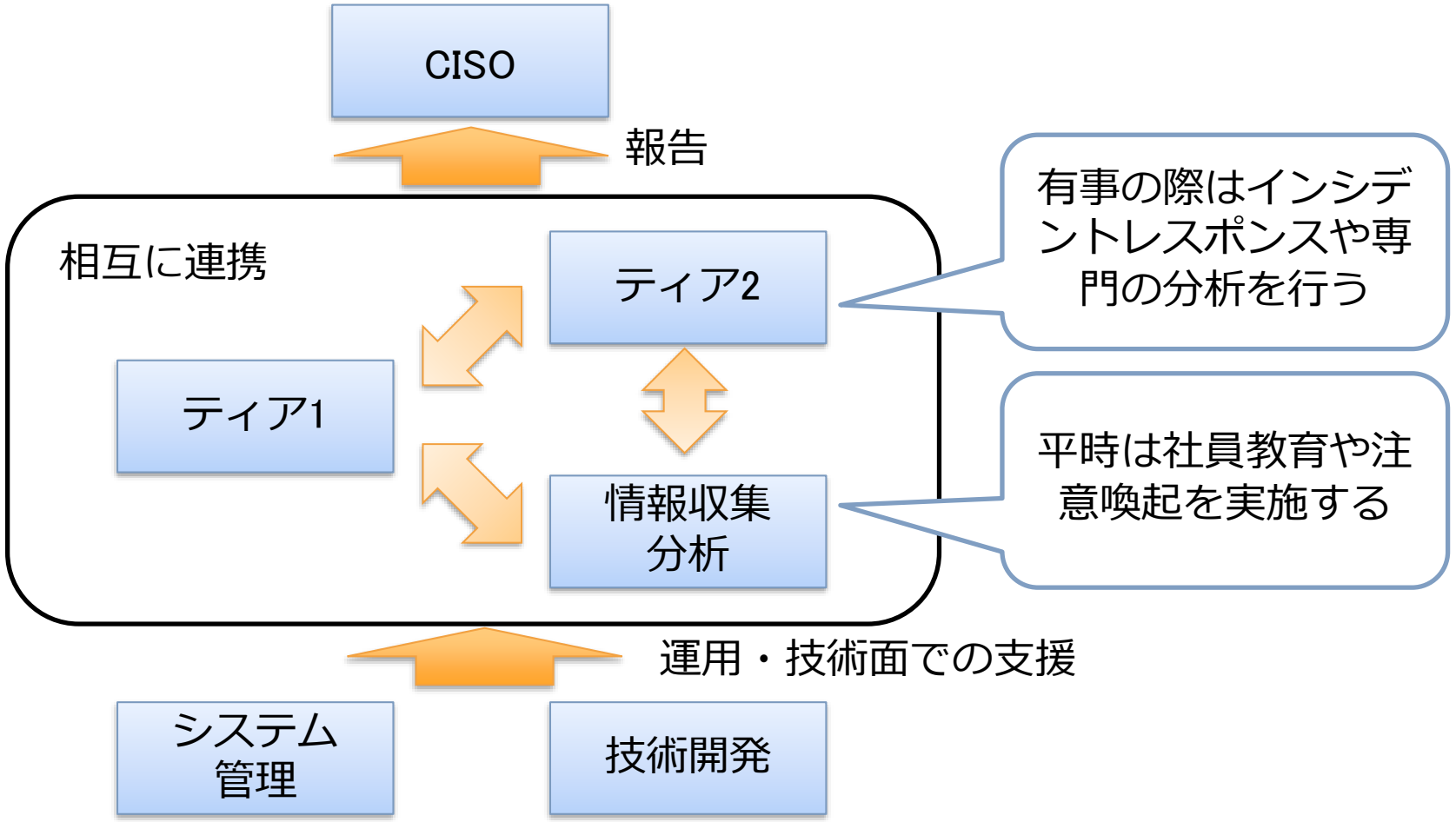


※業務が分かれるものもあるため、
複数の組織にまたがるものもある

出典：MITRE社「Ten Strategies of a World-Class Cybersecurity Operations Center」Figure10.

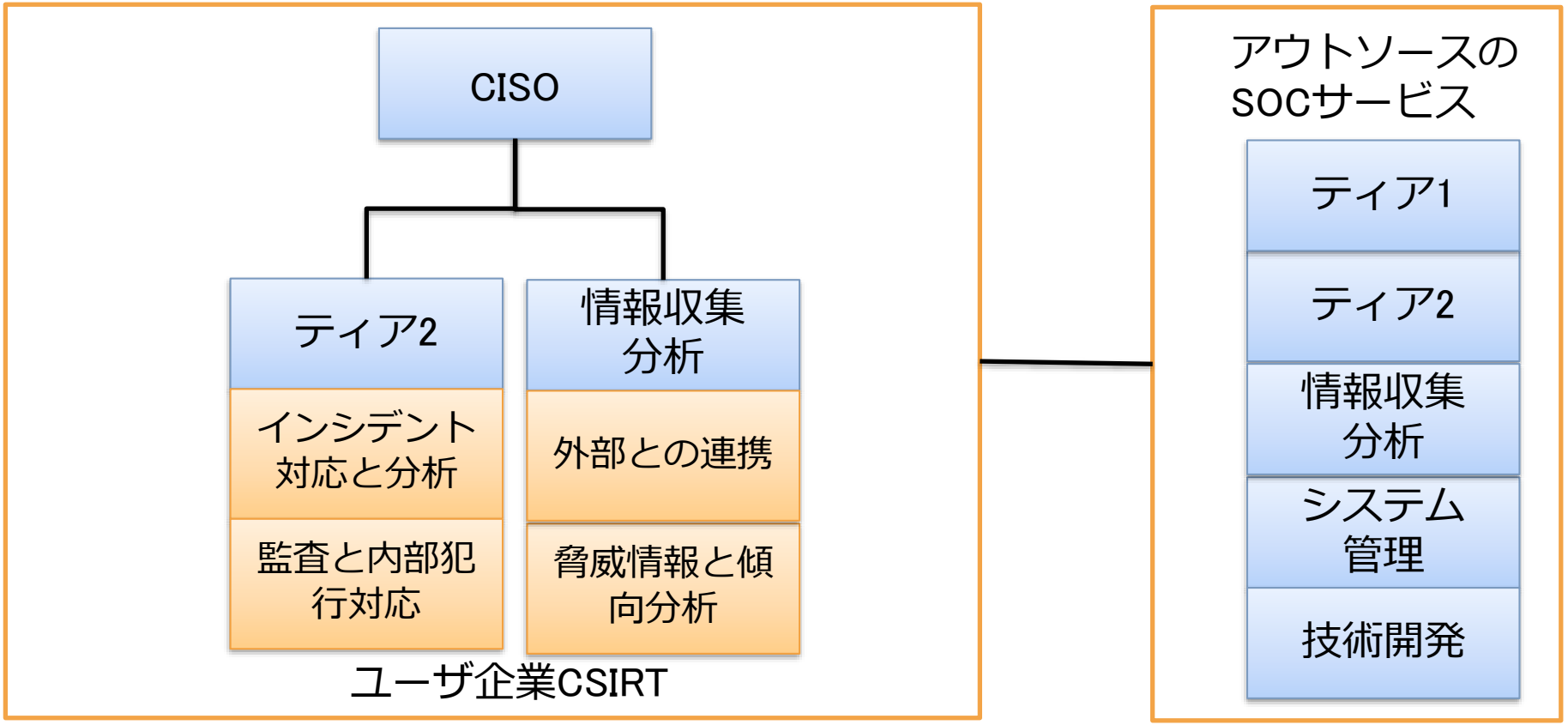
セキュリティの対応を行う組織による対応の例

- 平時は情報収集と監視を行っているため、CISOからは活動の成果が見えにくい



セキュリティの対応を行う組織の例

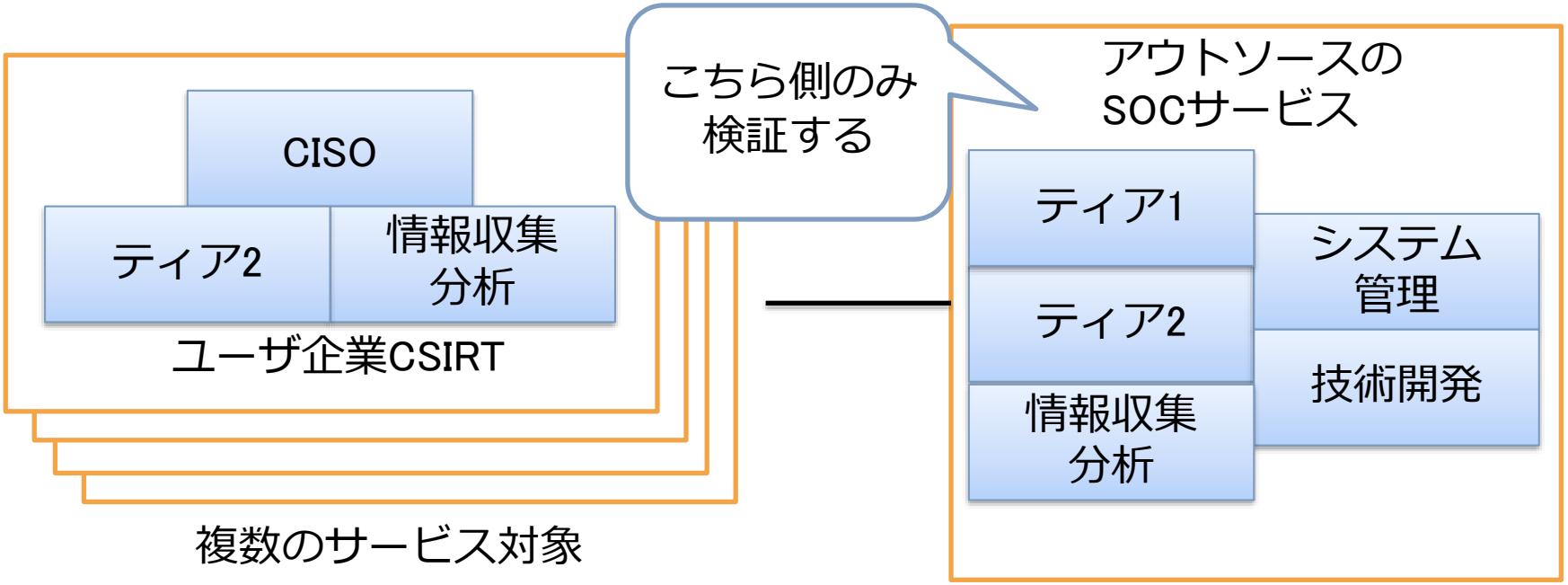
- 企業内にCSIRTを持つ場合、SOC機能をアウトソースすると次のような組織図となる



※ユーザ企業では社内外の窓口やインシデント対応の取りまとめを行い、アウトソースのSOCサービスにおいて専門分野を取り扱う

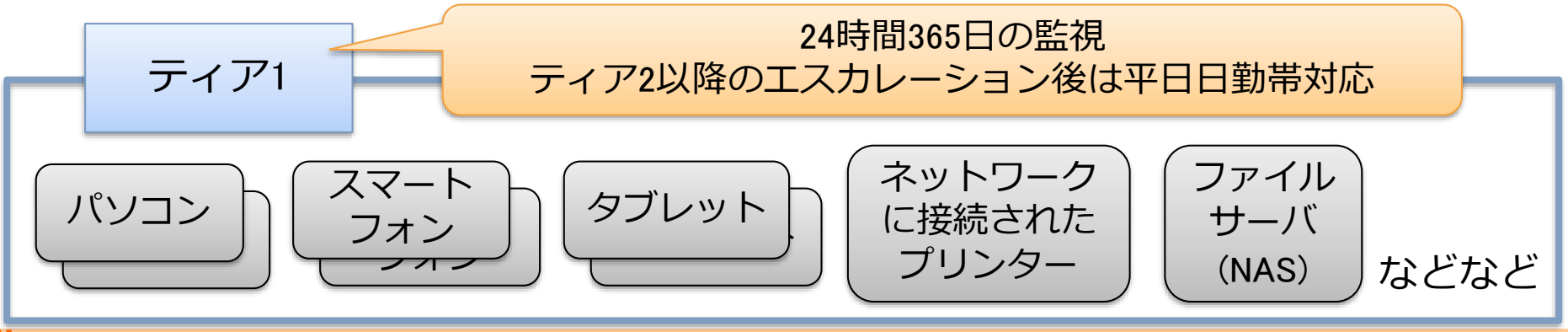
組織の構成と要員の配置例

- SOCに関連した機能について、どの程度の要員の配置が必要かを試算する
- 試算にはある程度の規模が必要なため、ここではアウトソース先のSOCサービスでの要員の配置例を整理する



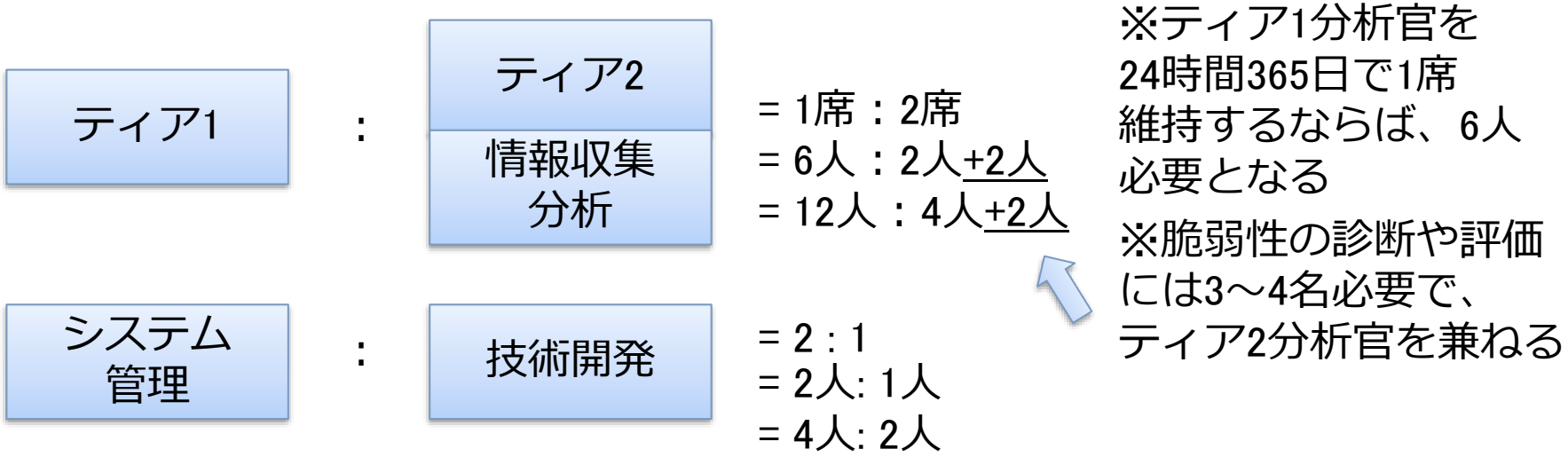
モデルケースの試算の前提

- モデルケースとして、監視対象のユーザあるいはIPアドレスが1万件程度、ティア1の監視メンバーのみ24時間365日の対応を想定する。
  - 対象となるIPアドレスとは、ユーザの扱うパソコン1台ずつだけではなく、社内に存在するスマートフォンやタブレット、プリンターなどネットワークに接続されているもの全てを想定する
- 平時の業務での想定とする。トラブルの規模によりピーク時の要員数が変化するためである。
- 地理的な条件や監視対象が分散している場合は含まず、１箇所を監視や対処を実施する想定とする



組織に必要な分析官の人数の例

- ティア1、ティア2、情報収集分析、システム管理、技術開発のそれぞれに必要な人数を整理する
- 実際の業務や監視の範囲や難易度により人数は変化する。
- ティア2分析官や情報収集分析官はよりスキルの高い要員が必要である。
- 最低限の要員数では、前述の全ての役割を実施することは難しい。



全ての役割に分析官を揃えて安定的なサービスを考慮するのであれば、24人程度は必要。

それぞれの役割での必要なスキル(1/11)

- 前提としてはコンピュータサイエンス全般の知識が必要である。
- セキュリティの状況や動向は変化するので継続的な学習も必要である。

分類	役割	スキル
リアルタイム分析		
	コールセンター	コミュニケーション
	NWログ分析	ネットワークの知識 被監視対象機器に関する知識(技術的な知識、お客様業務知識)
	PCAPログ分析	ネットワークの知識 パケットの知識

それぞれの役割での必要なスキル(2/11)

- 前提としてはコンピュータサイエンス全般の知識が必要である。
- セキュリティの状況や動向は変化するので継続的な学習も必要である。

分類	役割	スキル
リアルタイム分析		
	トリアージ情報収集	脅威情報の知識 ITIL（運用品質確保の基本条件） 被監視対象機器に関する知識(技術的な知識、お客様業務知識)
	分析妥当性確認	上記各役割のスキル
	全体分析品質確認	上記各役割のスキル
	業務範囲の管理	上記各役割のスキル

それぞれの役割での必要なスキル(3/11)

分類	役割	スキル
脅威情報と傾向分析		
	脅威情報の収集・分析	OS,NW,ソフトウェアの知識 脆弱性の知識 UGへのコネクション
	脅威情報の配信	OS,NW,ソフトウェアの知識 脆弱性の知識、文章力
	脅威情報の作成	OS,NW,ソフトウェアでの構築・検証のスキル 脆弱性の知識、文章力
	定期レポートの生成	OS,NW,ソフトウェアでの構築・検証のスキル 脆弱性の知識、文章力
	対策への組み込み	サーバやアプライアンス機器の知識 脆弱性の知識

それぞれの役割での必要なスキル(4/11)

- それぞれの役割に対して、必要なITのスキルとセキュリティのスキルは以下である。

分類	役割	スキル
インシデント対応と分析		
	オンサイトでのインシデント対応	OS,NW,脆弱性や攻撃の知識 お客様業務アプリ知識 お客様業界知識 法令知識
	リモートでのインシデント対応	(上記スキル)
	インシデント分析	(上記スキル)
	侵入手口の分析	OS,NW,脆弱性や攻撃の知識 マルウェア解析のスキル
	対策の実現	OS,NW,各種アプライアンスの設定

それぞれの役割での必要なスキル(5/11)

- それぞれの役割に対して、必要なITのスキルとセキュリティのスキルは以下である。

分類	役割	スキル
インシデント対応と分析		
	インシデント対応の調整役	コミュニケーション
	監督官庁との連携	コミュニケーション 監督官庁の法令
	サプライチェーンとの連携	コミュニケーション サプライチェーンの業務知識
	事業部門やSIerとの連携	コミュニケーション SIerの構築したシステムの知識
	経営層との連携	コミュニケーション 社内の方針や経営の知識
	ビジネスの影響の分析	社内の方針や経営の知識
	インシデントクローズ宣言	コミュニケーション
	インシデントクローズ報告	コミュニケーション 社内の方針や経営の知識、文章力

それぞれの役割での必要なスキル(6/11)

- それぞれの役割に対して、必要なITのスキルとセキュリティのスキルは以下である。

分類	役割	スキル
証拠の分析		
	フォレンジックの証拠の取り扱い	フォレンジックツールのスキル 証拠データの扱いに関する知識
	マルウェアや仕掛けられたものの分析	NWのパケットの解析 マルウェアの静的解析 マルウェアの動的解析
	フォレンジックの証拠の分析	マルウェア解析、メディアやモバイル端末のデータの解析 報告の文書化のスキル

それぞれの役割での必要なスキル(7/11)

分類	役割	スキル
ツールのライフサイクルのサポート		
	境界面で防御するデバイスの管理	各種サーバの運用の知識 アプライアンス機器運用の知識
	資産管理	ソフトウェアやハードウェア製品の知識
	SOCのインフラの管理運用	サーバー,NWの運用 ITIL（運用を意識したツール配備が必須）
	監視設備（センサ以外も含む）のメンテナンス	監視機器に関する知識(技術的な知識、お客様業務知識)
	インシデント対応製品導入支援	インシデント対応で利用されるソフトウエアやハードウェア製品の知識

それぞれの役割での必要なスキル(8/11)

分類	役割	スキル
ツールのライフサイクルのサポート		
	センサーのチューニングと維持管理	アプライアンス機器の知識
	カスタムシグネチャの作成	アプライアンス機器の知識 脆弱性と攻撃手法の知識
	ツールの開発と配備	OS,NWの知識 脆弱性と攻撃手法の知識 市場調査 プログラミング + セキュアコーディング
	ツールの研究開発	OS,NWの知識 脆弱性と攻撃手法の知識 プログラミング + セキュアコーディング
	製品情報収集/検証	ソフトウェアやハードウェア製品、アプライアンス機器の知識

それぞれの役割での必要なスキル(9/11)

分類	役割	スキル
監査と内部犯行対応		
	監査データの収集と配布	システム運用の知識
	監査コンテンツの作成と管理	SIEMやログ管理ツールの知識
	内部犯行事案のサポート	システム運用の知識 監視データの分析 法令知識
	内部犯行事案の調査	監視データの分析 外部とのコミュニケーション能力 法令知識

それぞれの役割での必要なスキル(10/11)

- 診断と評価のスキルについては、脆弱性診断士（Webアプリケーション）や脆弱性診断士（プラットフォーム）の概要やシラバスを参考頂きたい
  - http://isog-j.org/output/2014/pentester-web-skillmap-201412.pdf

分類	役割	スキル
診断と評価		
	ネットワークのマッピング	脆弱性診断士
	アセット情報の収集	脆弱性診断士
	脆弱性診断	脆弱性診断士
	脆弱性の評価	脆弱性診断士
	侵入テスト	脆弱性診断士

それぞれの役割での必要なスキル(11/11)

分類	役割	スキル
外部との連携		
	製品の評価	脆弱性診断士
	メディア対応の窓口	コミュニケーション能力、文書力 脆弱性や攻撃手法の知識
	研修や啓発	コミュニケーション能力 脆弱性や攻撃手法の知識
	内部への把握している情報の公開	コミュニケーション能力、文書力 脆弱性や攻撃手法の知識
	セキュリティコンサルティング	コンサルティングのスキル セキュリティの全般の知識
	外部への脅威情報の公開	コミュニケーション能力、文書力 脆弱性や攻撃手法の知識

まとめ

- セキュリティの対応をする組織の役割を大きく8つに分類し、日本におけるSOC,CSIRTにおける分担や、全体像を組織図としてまとめた
- 分析官がどの程度の規模でどの程度必要であるかをまとめた
- それぞれの役割について必要と思われるスキルをまとめた
- セキュリティに特化したスキルについては継続的な学習により補強すると考えると、ベースとなるコンピュータサイエンス全般や既にあるOS,NW,アプリケーションやプログラミングといったスキルが重要であり、どの役割で活用できそうか参考として頂きたい

参考文献

- 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
- 脆弱性診断士(Webアプリケーション)スキルマップ (ISOG-J)
  - http://isog-j.org/output/2014/about-pentester-web-skillmap-201412.pdf
  - http://isog-j.org/output/2014/pentester-web-skillmap-201412.pdf