サイバー脅威を検知するセキュリティ・オペレーション・センター

Security Operation Center that Detects Cyber Threats

石　黒　　怜，木 埜 由紀子

要　約　Security Operation Center（SOC）とは，情報システムへのサイバー脅威の検知や監視，分析をするための重要な機能である．SOC はその導入形態により，プライベート SOC，パブリック（商用）SOC，ハイブリッド SOC の三種類に分類される．運用体制としては，インシデント対応を行う CSIRT と協調することで，組織の防衛能力向上を図ることができる．実際の運用では，業務一覧の整理，アクティビティの整理といったプロセスの明文化や検証が重要となる．今後は外部サービスの利用が中心となるので，それらを正しく活用する能力が求められる．

Abstract　Security Operation Center (SOC) has important functions which to detect, monitor and analyze cyber threats for information systems. SOCs are classified into three types, private SOC, public (commercial) SOC, and hybrid SOC, according to the form of installation. As an operation system, it is possible to improve the defense capability of the organization by coordinating with the CSIRT that handles incidents. In actual operation, it is important to clarify and verify processes such as organizing work lists and organizing activities. Since the use of external services will increase in the future, the ability to utilize them correctly is required.

1. は　じ　め　に

いまや情報システムは社会インフラの一つで，企業や組織の運営に欠かせないものとなり，情報資産の価値の高さも広く認識されるようになった．これに伴い，セキュリティインシデントにより情報システムの停止や顧客情報の漏えい等が発生すると，自組織の損失やブランドイメージの失墜だけでなく，取引先や顧客等の関係者にも大きな被害や影響をもたらす状況となっている．

近年，サイバー犯罪は価値の高い情報資産（技術/個人情報等）の窃取等を目的としたものとなり，攻撃方法も高度化/複雑化している．そのため，インターネット境界やエンドポイントにセキュリティ製品を導入するだけでは攻撃を 100％防ぐことは不可能であるという認識が広がっており，侵入されることを前提としたセキュリティ対策として CSIRT や SOC を組織する企業が増加している．この「侵入を前提としたセキュリティ対策」において重要なことは，いかに早い段階で侵入に気が付くか，つまり，いかに早くセキュリティインシデントの発生を「検知」できるかである．なぜなら，インシデント対応は時間との勝負であり，検知が早ければ早いほど，被害の発生や影響範囲を抑えることができるためである．ただし，たとえ「検知」する機能が十分であっても「対応」する機能が不十分であれば，セキュリティ対策全体としては脆弱であるため，セキュリティ対策に必要な機能を理解し網羅的に対応することが重要である．

本稿では，サイバー脅威を検知するための組織である SOC に焦点を当て，日本ユニシス株式会社とグループ会社（以降，日本ユニシスグループ）の SOC 運営の経験を踏まえて，セキュリティ対策機能における「検知」の位置づけや SOC 運営における役割等を整理する．まず 2 章でセキュリティインシデントを検知する機能の要件をサイバーセキュリティフレームワークを基にまとめ，次いで 3 章で SOC の導入形態や運用体制，そして監視システムについて述べる．本稿が各企業や組織における SOC 運営の一助となれば幸いである．

2. 検知機能の要件

セキュリティ対策機能の全体像と検知機能の要件については，米国国立標準技術研究所（National Institute of Standards and Technology：NIST）が公開しているサイバーセキュリティフレームワーク（Cyber Security Framework：CSF）[1][2]で詳細を確認することができる．CSF は「重要インフラのサイバーセキュリティを改善するためのフレームワーク」ではあるが，「予防」策にとどまらずにサイバー攻撃対策を中心とした「検知」や「対応」に言及し，広く企業に適用できるように要件が汎用化されていること等から，重要インフラのみならず活用されているフレームワークである．本章では，CSF の一部であるフレームワークコアを用いて，検知機能の要件を挙げる．なお，CSF の詳細に関しては，本特集号の掲載論文「サイバーセキュリティフレームワークを応用したアセスメント」[3]を参照されたい．

2.1 フレームワークコアの五つの機能

CSF の構成要素の一つであるフレームワークコアは，すべての重要インフラ分野に共通となるサイバーセキュリティ対策，期待される成果，適用可能な参考情報をまとめたものであり，「識別（Identify）」，「防御（Protect）」，「検知（Detect）」，「対応（Respond）」，「復旧（Recover）」の五つのセキュリティ対策機能により構成されている．フレームワークコアを用いた評価を行うことで，自組織における各セキュリティ対策機能の担当部門や対応状況を整理することができる．

2.2 フレームワークコアに見る検知機能の要件

フレームワークコアにおいて，各機能はカテゴリとサブカテゴリに細分化され，検知機能では三つのカテゴリと 18 のサブカテゴリに細分化される．サブカテゴリではより詳細な機能要件が定義されているため，具体的な対応に落とし込むことができる．表 1 に，検知機能におけるカテゴリおよびサブカテゴリの内容と相当する対応例を示す．

表 1　フレームワークコアにおける検知機能と相当する対応の例

カテゴリ	サブカテゴリ	相当する対応（例）
異常とイベント（DE.AE） 異常な活動は，検知されており，イベントがもたらす潜在的な影響が，把握されている．	ネットワーク運用のベースラインと，ユーザとシステムで期待されるデータフローが，定められ，管理されている．（DE.AE-1）	・通信要件 ・URL フィルタリング[*1] 等

	検知したイベントは，攻撃の標的と手法を理解するために分析されている． (DE.AE-2)	・SIEM（Security Information and Event Management）[*2] ・OSINT（Open Source Intelligence）[*3] ・Sandbox 解析[*4] 等
	イベントデータは，複数の情報源やセンサーから収集され，相互分析されている． (DE.AE-3)	・SIEM ・Proxy ログ ・ファイアウォールログ ・メールログ ・DNS ログ ・IDS・IPS[*5] ログ ・ウイルス対策製品ログ 等
	イベントがもたらす影響が，判断されている． (DE.AE-4)	・OSINT ・Sandbox 解析 等
	インシデント警告の閾値が，定められている． (DE.AE-5)	・SIEM 等
セキュリティの継続的なモニタリング (DE.CM) 情報システムと資産は，サイバーセキュリティイベントを識別し，保護対策の有効性を検証するために，モニタリングされている．	ネットワークは，サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている． (DE.CM-1)	・SIEM ・ログ分析 等
	物理環境は，サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている． (DE.CM-2)	・入退館記録 等
	人員の活動は，サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている． (DE.CM-3)	・Proxy ログ ・OS ログ ・動画記録 等
	悪質なコードは，検知されている． (DE.CM-4)	・パケット分析 等
	不正なモバイルコードは，検知されている． (DE.CM-5)	・パケット分析 等
	外部サービスプロバイダの活動は，潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている． (DE.CM-6)	・外部サービスアクティビティ監視 等
	権限のない人員，接続，デバイス，ソフトウェアのモニタリングが，実施されている． (DE.CM-7)	・資産管理 ・ID 管理 等
	脆弱性スキャンが，実施されている． (DE.CM-8)	・脆弱性診断 等

検知プロセス（DE.DP） 検知プロセスおよび手順が，異常なイベントに確実に気付くために維持され，テストされている．	検知に関する役割と責任は，説明責任を果たせるように明確に定義されている．（DE.DP-1）	・定義の明文化 ・定義内容の維持，継続的な検証と見直し ・定期/臨時の報告書 等
	検知活動は，該当するすべての要求事項を準拠している．（DE.DP-2）	
	検知プロセスが，テストされている．（DE.DP-3）	
	イベント検知情報が，周知されている．（DE.DP-4）	
	検知プロセスが，継続的に改善されている．（DE.DP-5）	

2. 3　検知機能の他機能との連携

フレームワークコアの検知機能は，単純に脆弱性や攻撃等のサイバー脅威を検知するだけではなく，検知した結果を基に「防御（PR）」機能および「対応（RS）」機能と連携する．連携イメージを図 1 に示す．

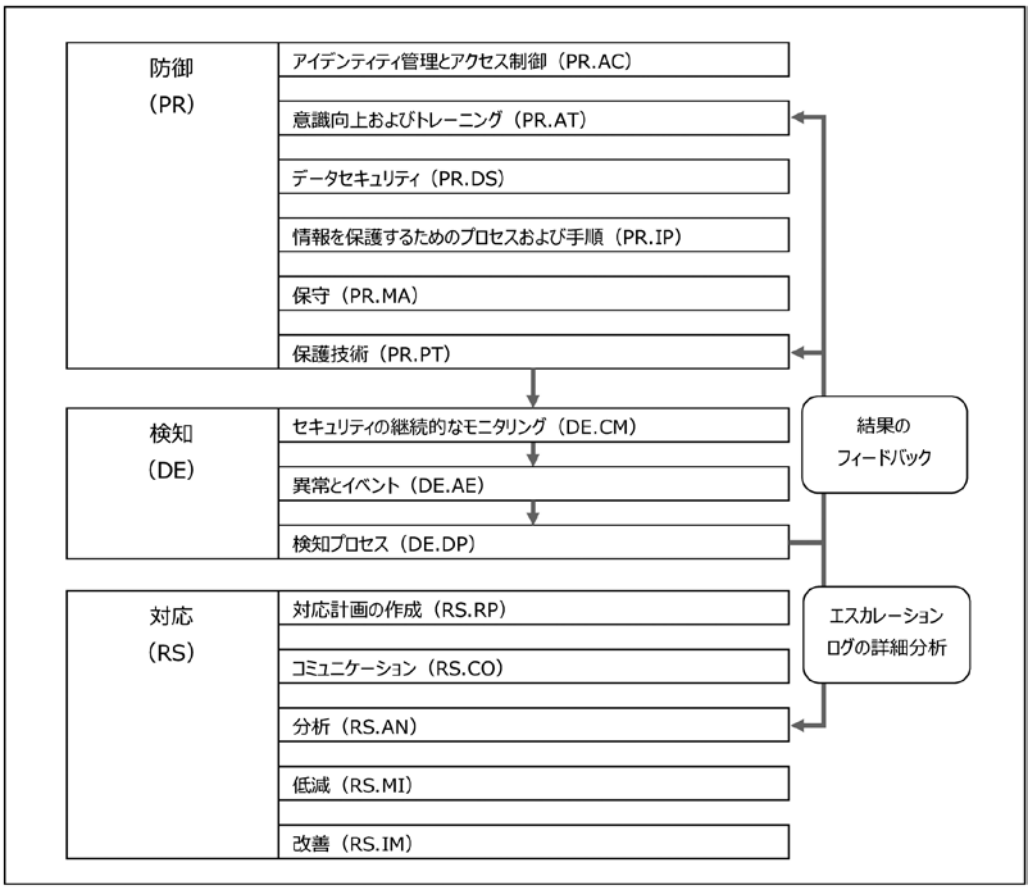

図 1　検知機能の他機能への連携イメージ

「防御（PR)」機能との連携においては，「セキュリティの継続的なモニタリング（DE.CM)」から「異常とイベント（DE.AE)」を検知し，「検知プロセス（DE.DP)」に基づいて「防御（PR)」機能にフィードバックを行い，フィードバックした「防御（PR)」機能の下で「セキュリティの継続的なモニタリング（DE.CM)」を行う，といった循環の仕組みがある．例えば，フィッシング詐欺情報や，ばら撒きメールのような脅威情報を検知した際に防御機能におけるカテゴリ「意識向上およびトレーニング（PR.AT)」部分にフィードバックを行うことで，セキュリティインシデント発生のリスクを低減することができる．

「対応（RS)」機能との連携という点では，「異常とイベント（DE.AE)」から「検知プロセス（DE.DP)」に基づいてセキュリティインシデント発生と判断した際には，同じく「検知プロセス（DE.DP)」の手順に基づいて速やかに「対応（RS)」機能へと連携し，モニタリングの情報から「分析（RE.AN)」を担うという関係性がある．

3.　セキュリティ・オペレーション・センター

セキュリティ・オペレーション・センターはSOCと略され，情報システムへの脅威の監視や分析等を行い，検知機能の役割を担う．本章では，導入形態によるSOCの分類とその特徴，SOCの運用体制と人材，運用プロセス，監視システムについて整理する．

3.1　SOCの導入形態と分類

SOCはその導入形態により三種類に分類することができる．監視装置の設置や監視システムの構築，並びにログやアラートを自組織で一元管理するSOCをプライベートSOCと分類する．これに対して，監視装置の設置やSOC運営をフルアウトソースするものをパブリック（商用）SOCと分類し，両者の複合的なものをハイブリッドSOCと分類する．それぞれの分類によって運営者やメリット/デメリット，監視範囲の深度が異なるため，整理したものを表2に示す．

表2　SOCの分類

分　類	導入形態	運営者	監視深度	メリット	デメリット
パブリック（商用）SOC	監視装置の設置や監視基盤の構築・運用等をアウトソースする	セキュリティオペレーション事業者	浅い	・セキュリティオペレーション事業者の専門要員を利用することができ，自組織での人材育成や要員確保が軽減できる ・短期導入できる	・プライベートSOCに比べてカスタマイズが困難 ・情報連携や機密保持が容易ではない
プライベートSOC	自組織で監視装置の設置や監視基盤の構築を行い，監視や分析，基盤運用も自組織で行う	自組織	深いが限定的	・自組織に応じてカスタマイズできる ・自組織内で完結するため機密保持が容易	・構築や運用に関するノウハウが必要 ・人材育成に時間と費用がかかり容易ではない ・短期導入が困難

ハイブリッド SOC	監視装置の設置を自組織で行い，監視等の運用をアウトソースする	自組織＋セキュリティオペレーション事業者	深い	・プライベート SOC とパブリック SOC，両方のメリットを享受できる	・自組織とアウトソース先で役割分担と責任範囲の明確化が必要

SOC 運用をアウトソースする際は，機密上の理由等によりファイアウォールログや Proxy ログ等のネットワーク境界部分のログ監視が主となるため，監視深度が浅くなる傾向がある．一方，プライベート SOC は自組織内で完結するために機密上の制限が少なく，全範囲を監視できるが，主に人的リソースがネックとなり監視深度が限定的となる傾向がある．また，十分なリソースを割り当てることができずに中途半端になることや，形骸化する恐れもある．ハイブリッド SOC は自組織内の限られたリソースを分散させずに集中させることができるため，リソースを要所に注力し，有効活用することができる．

SOC 運用の何をアウトソースすべきか判断が難しい点ではあるが，内部（組織内，または被害者）/外部（組織外，または攻撃者）と専門性の高/低のベクトルで分類することで優先度を付けやすくなる．アウトソースを優先すべき部分は専門性の高さが最優先であり，次いで組織外や攻撃者側の情報といった外部領域である．昨今では次世代ファイアウォール等が専門性の高いパケット分析や検体解析等の機能を有していることや，専門ベンダのアナリストによる最新の脅威情報や攻撃キャンペーン情報，ディープ Web[*6] の分析情報等，多くの脅威情報をサービスとして入手することができるため，専門性の高い外部情報等の収集や整理をアウトソースしやすい状況となっている．そのため，今後，セキュリティ専門ベンダではない組織の SOC 運用においては，サービスや機能を使いこなし，得られた情報を正しく理解し判断する能力が求められる．

3. 2　SOC の運用体制と人材

SOC の運用体制と人材について，日本セキュリティオペレーション事業者協議会（Information Security Operation providers Group Japan：ISOG-J）が公開している「セキュリティ対応組織の教科書 v2.1」[4]を参考にその役割，求められるスキルを確認したものを表 3 と以下 1）から 7）に挙げる．インシデント対応を行う CSIRT（Computer Security Incident Response Team）と協調することで，組織の防衛能力向上を図ることができるので，SOC とは別に CSIRT を組織している日本ユニシスグループにおける役割分担も例として付加した．なお，日本ユニシスグループの情報セキュリティ推進体制に関しては，本特集号の掲載論文「日本ユニシスグループのサイバーセキュリティ戦略」[5]を参照されたい．

表 3　SOC の運用体制と CSIRT 運営組織での役割分担

役　割	作業概要	必要なスキル	日本ユニシスグループでの分担
一次分析担当（ティア 1）	アラート監視 イベントの一次調査	SIEM や調査用ツールの使用 手順の整理 ログの分析	SOC

二次分析担当 (ティア 2)	イベントの二次調査 イベントの対応情報管理 エスカレーション	ログの分析 脅威情報分析 プロセス策定	SOC
インシデント 対応担当	ログの詳細分析 インシデントハンドリング	インシデントハンドリング 社内外調整	CSIRT
リサーチ 解析担当	脅威情報等の収集・解析	脆弱性情報や脅威情報の収集と分析 情報の周知，伝達	SOC
脆弱性管理・ 診断担当	システムの脆弱性管理 脆弱性診断	脆弱性情報収集 脆弱性知識 脆弱性診断ツールの使用	脆弱性診断チーム
フォレンジック 担当	フォレンジック調査	フォレンジック知識 フォレンジックツールの使用	CSIRT 外部フォレンジック サービス
システム運用・ 管理担当	サーバの運用管理 ツールの保守開発	OS やネットワーク知識 使用ツールの知識	SOC

1）一次分析担当（ティア 1）

SIEM によるアラート通知を監視し，イベントの一次調査を行う．イベント内容を精査し，ログを分析するためにツールの特性や使用方法に精通していることが要求される．そのため，ログの調査方法やツールの使用等における手順の整理・標準化も求められる．

日本ユニシスグループの場合は，この役割は SOC が担当している．アラート監視については，SIEM やイベント監視系のソリューションを用いて自動化することが多く，イベント管理において通知を自動化する仕組みを採用している．

2）二次分析担当（ティア 2）

一次分析担当が判断できないイベントの二次調査や，セキュリティインシデントの発生を検知した際のエスカレーション等を行う．ログや脅威情報の分析に加えて，2.3 節に記載の他セキュリティ機能との連携を行うためのプロセス作りや社内連絡ルートの整理といったスキルも要する．

日本ユニシスグループの場合は，この役割は SOC が担当している．一般的な SOC 運用と同様に一次分析担当者と二次分析担当者をティア 1，ティア 2 と明示的に役割を分けている．

3）インシデント対応担当

セキュリティインシデントが発生した際に優先順位付けといった状況判断や，社内外組織との調整を担う．セキュリティスキルとロールの相関を整理した「セキュリティ知識分野（Security Body of Knowledge：SecBok）2019」[6]のロールに照らすと，社内外の連絡窓口となりそれぞれ情報連携を行う「PoC（Point of Contact）」や，インシデントの全体統括や優先順位を判断する「コマンダー，トリアージ」，組織内調整を行う「ノーティフィケーション」等に関連したスキルが要求される．

SOC とは別に CSIRT を運用している組織の場合は，CSIRT 要員がこの役割を担うのが一般的である．日本ユニシスグループの場合も，本役割は SOC ではなく，CSIRT が担当している．

4）リサーチ・解析担当

日々新しい脆弱性や攻撃が明らかとなる中で，最新の情報を収集し，必要に応じて検知・防御機能へ反映するために解析を行う．SecBok2019 のロールに照らすと，セキュリティイベントや脅威情報，脆弱性情報，攻撃者のプロファイル情報，国際情勢の把握，メディア情報などを収集する「リサーチャー」に関連したスキルが要求される．専門性の高いスキルが要求されるため，アウトソースする優先度の高い役割である．

日本ユニシスグループの場合，OSINT の利用や外部団体の共有情報に加えてセキュリティベンダの提供する脅威情報サービスを利用することで，最新の脅威情報のリサーチ・解析を省力化している．

5）脆弱性管理・診断要員

守る対象のシステムに関する脆弱性情報の管理や診断を行う．SecBok2019 のロールに照らすと，ネットワークや OS，ミドルウェア，アプリケーションがセキュアプログラミングされているかどうか検査し，診断結果の評価を行う「脆弱性診断士」に関連したスキルが要求される．ネットワークやアプリケーションの脆弱性の知識に加えて，専用の脆弱性診断ツールにも精通していなければならず，専門性の高い役割である．

日本ユニシスグループの場合は，脆弱性診断をセキュリティ技術主管部署の脆弱性診断チームが実施している．システムに関する脆弱性管理は自組織で行うが，脆弱性診断の実施に関しては専門性の高い分野であるため，アウトソースする優先度の高い役割である．

6）フォレンジック担当

主にセキュリティインシデント発生時において，フォレンジック調査を行い証拠の確認や保全を行う．SecBok2019 のロールに照らすと，証拠保全とともに，消されたデータを復活させて足跡を追跡し，システム的な鑑識，精密検査，解析，報告を行う「フォレンジックエンジニア」に関連したスキルが要求される．脆弱性診断と同様に専用ツールの使用を含めて高いスキルが要求されるため，アウトソースする優先度の高い役割である

日本ユニシスグループの場合，自社で開発・運用・保守等を行っているシステムに対するフォレンジック調査では，客観性を担保するために外部フォレンジックサービスを利用するケースもある．

7）システム運用・管理担当

SOC 運用におけるサーバ等の運用に加えて，SIEM や関連システムの運用・保守や調査・分析ツールの開発を行う．使用する SIEM 等の製品知識に加えて，サーバ運用・保守等に関わる一般的な知識が要求される．

日本ユニシスグループの場合は，一次分析担当が SIEM の運用・保守と調査・分析ツールの開発を兼務し，二次分析担当にてサーバ運用等を兼務している．SIEM 等による分析をアウトソースする場合は，ツール開発等の役割もアウトソースできるメリットがある．

3. 3　SOC の運用プロセス

SOC の運用プロセスについては，プロセスの明文化や検証が重要となる．運用プロセスは，以下に挙げる手順で整理する．

3.3.1　業務一覧の整理

SOC 運用における業務内容を項目に分けて一覧化する．例えば，SOC のログ監視や調査に関わる運用の業務内容を整理するにあたっては，大きく「監視」「調査対応」「報告」という大項目に分けることができる．また，「調査対応」に関しては，検知した脅威が「既知の脅威」か「未知の脅威」かにより関連するアクター（SOC，CSIRT，情報システム部門）や必要となるアクティビティが変わるため，小項目として既知か未知かで分けることができる．さらに，調査対応は内部的なログの監視とイベント検知だけとは限らず，CSIRT といった SOC 以外の部門からの依頼によるものもあるため，外部からの問い合わせ対応も分けるべきである．

本作業における最終的な目標は，次にアクティビティを整理するために業務を漏れなく抽出し，関連するアクターを洗い出すことである．本作業の成果物として，業務内容一覧を表 4 に示す．

表 4　業務内容一覧

業務名称				作業概要	関連するアクター	アクティビティNo
大項目		小項目				
1	監視	1	監視	監視対象センサーから取得するログをSIEMの検知ルールと照合し、不審な操作や通信を自動で検知する。	SOC担当者（ティア1）	SOC-01-01「ログ監視（自動）」
2	調査対応	1	既知の脅威	SIEMで検知した不審な操作や通信をもとに過去の事象を参照し、事象の特定および脅威の有無を判断する。	SOC担当者（ティア1）	SOC-02-01「脅威の識別（既知の脅威）」
		2	未知の脅威	SIEMで検知した不審な操作や通信が過去の事象に一致しない場合、事象の特定および脅威の有無を判断する。調査に際し、情報システム部門と協力する。	SOC担当者（ティア1） SOC担当者（ティア2） 情報システム部門	SOC-02-02「脅威の識別（未知の脅威）」
		3	外部からの問い合わせ対応	CSIRTからの連絡により認識したイベントについて、ログ情報の詳細分析を行い、原因の発生箇所や発生日時、影響範囲等を調査し、結果を問い合わせ元に報告する。	SOC担当者（ティア1） SOC担当者（ティア2） CSIRT	SOC-02-03「CSIRTからの問い合わせ対応」
		4	インシデント情報管理	脅威情報、インシデント情報を「インシデント管理システム」に登録、原因、影響度、対応状況を追跡・把握し管理する。	SOC担当者（ティア1） SOC担当者（ティア2）	SOC-02-04-1「インシデント情報管理（ティア1）」 SOC-02-04-2「インシデント情報管理（ティア2）」
3	報告	1	定期報告書の作成・提示	監視の結果、問い合わせ内容・回答結果、インシデント対応状況、ログ分析レポートを纏め、CSIRTへ報告を行う。また、定期報告書に関する問い合わせ対応を行う。	SOC担当者（ティア1） SOC担当者（ティア2）	SOC-03-01「定期報告」
		2	臨時報告書の作成・提示	検知内容の確認・調査の結果、セキュリティインシデントが発生したと認められた場合に、臨時報告書を作成の上CSIRTへエスカレーションを行う。また、臨時報告書に関する問い合わせ対応を行う。	SOC担当者（ティア1） SOC担当者（ティア2）	SOC-03-02「臨時報告」

3.3.2　アクティビティの整理

業務内容の一覧化により，対象の業務概要と関連するアクターが整理される．アクティビティの整理においては，業務内容一覧で整理した業務の単位で，それぞれのアクターが何をどういった順番で行い，それぞれのアクターがどう関連するかを図 2 のようなアクティビティ図等を用いて整理する．

この作業で最も重要な点は，条件分岐における判断基準やアクター間の連携方法および手順を明確化することである．例えば，脅威の識別において「既知の脅威」であるか「未知の脅威」であるかを判断するといっても，過去のイベント情報におけるマルウェアの可能性があるファイル名やハッシュ値，C&C サーバ[*7] 等の通信先の URL といった複数の情報から，どの情報が一致したら「既知の脅威」とするかを明確にしておかなければ正しい判断はできない．そのため，アクティビティの整理では「Yes」「No」の条件分岐を明示するだけではなく，「Yes」「No」を判断するための判断基準が明示されているかを確認することが重要である．また，アクター

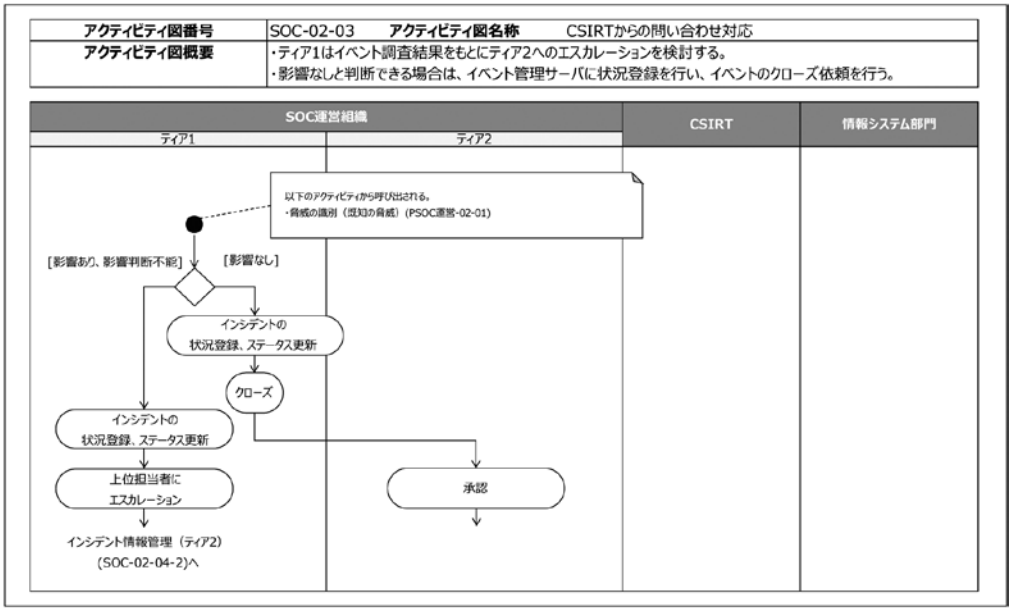

図 2　アクティビティ図

間の連携については，アクティビティ図等によりアクター間の連携の必要性や流れを明確にするだけではなく，連携方法や手順も明確にするべきである．

アクティビティのフローや条件分岐，関連するアクター等は，ある程度は他の情報を参考もしくは流用できる部分もあるが，判断基準や連携方法および手順は各々の企業や組織で異なるため，アクティビティの整理においては，自組織に適した基準や情報を確認した上で明文化することが重要である．また，2.2 節表 1 の検知プロセス（DE.DP）に記載の通り，継続的に検知プロセスをテストすることにより定義したアクティビティや関連する判断基準，アクター間の連携方法や手段等の実効性を確認し，改善していかなければならない．

3. 4　SOC の監視システム

本節では，SOC 運用に欠かせない監視システムについて，監視対象とするセンサー，ログの収集と各種ログの分析を行う SIEM，検知イベントを記録し状況のトレースや調査・分析結果の情報蓄積と検索を行うためのイベント管理に分けて整理する．

3. 4. 1　監視対象とするセンサー

SOC が監視対象とするセンサーは，インシデントを検知するために必要な情報を出力する機器や装置である．そのため，SOC が監視対象とするセンサーは，2.2 節表 1 の「DE.AE-3」の相当する対応（例）に記載されているような機器を対象としており，一般的なネットワーク機器だけでなく，ネットワーク上やエンドポイント機器に導入されているセキュリティ対策製品，ファイアウォールや IDS 等，ネットワーク境界部分に設置されたセンサーが主な監視対象となる．加えて，メールゲートウェイや，DNS 等の各種サーバログ，エンドポイントに導入されたセキュリティ対策製品のログ等，収集・分析対象とするセンサーは数多くあるが，全ての機器を対象とすることは現実的ではないため，目的やリソース等によって対象を選定する．

また，近年ではクラウド利用や外部サービスの利用が増加していることから，パブリッククラウド等が提供するクラウドの利用状況や外部サービスから提供されるログ等も分析を要するなど，監視対象として検討すべきセンサーは増加し続けている．

3. 4. 2　ログ分析を行う SIEM

SOC 運用の監視システムの中心は SIEM である．セキュリティベンダが提供する有償の SIEM には，各種センサーが出力するログをデフォルト設定で取り込むことができ，かつ，デフォルトの検知ルールセットが豊富であり，ベンダによるサポートや機能開発等があるといったメリットがある．OSS（Open Source Software）の SIEM は，構築や設定，運用やトラブルシューティングを自身で行わなければならず，高度な知識やスキルが要求されるが，ライセンス費用やベンダ保守費用がかからずコストメリットが大きい．技術やスキルが十分である場合は，OSS の SIEM を選択することも検討すべきだろう．

3. 4. 3　イベント管理

SIEM が各種センサーのログを分析し発生したイベントを管理することで，発生したイベントとその調査状況，また，イベントに対する調査内容や調査結果，対応内容等を記録することができる．SOC 運用を行う中で，過去に調査を行ったイベントの情報を蓄積しておけば，以後の調査において必要な情報を検索でき，調査の効率化を図ることができる．

日本ユニシスグループの SOC 運用においては，SIEM とイベント管理の役割を分け，それぞれの役割を担当するサーバも分けている．

3. 4. 4　SOC の運用するセキュリティ監視基盤イメージ

本節で述べたシステム基盤の内容を踏まえた，日本ユニシスグループが運用するセキュリティ監視基盤のイメージを図 3 に示す．

まず，SIEM においてインターネット境界の NGFW[*8] やプロキシサーバ，メールゲートウェイのログを取得し，エンドポイントセキュリティ製品（NGAV[*9]）のログはエンドポイントセキュリティの管理サーバを経由して取得する．取得したログはログ受信・分析サーバにて検知ルールへの照合を行い，検知ルールに合致した場合はイベント管理に情報連携し，イベントを作成する．また，調査・分析のために，項目毎に分解した情報をログ保管・検索サーバに保持する．

イベント管理では，SIEM から連携された情報を基にして送信元や送信先の情報を予め補完した状態でイベントを作成し，ティア 1 にイベント発生を通知する．ティア 1 はイベント管理サーバを参照し，必要に応じて OSINT 等を活用して一次調査を行い，一次調査結果や二次調査依頼をイベント管理サーバに入力する．一次調査結果が入力されると，イベント管理サーバはティア 2 に一次調査結果の確認，または二次調査の開始を通知する．ティア 2 は一次調査結果の確認や二次調査を行い，必要に応じて CSIRT へのエスカレーションや，防御機能に反映するための情報システム部門へのフィードバックを行う．また，近年では NGFW や NGAV が持つ脅威インテリジェンスサービス（Cloud Sandbox 解析機能）への情報連携と自動的な防御への反映機能を活用することで，新たに確認した脅威に関する対策をセンサーへ効率的に反映することができる．

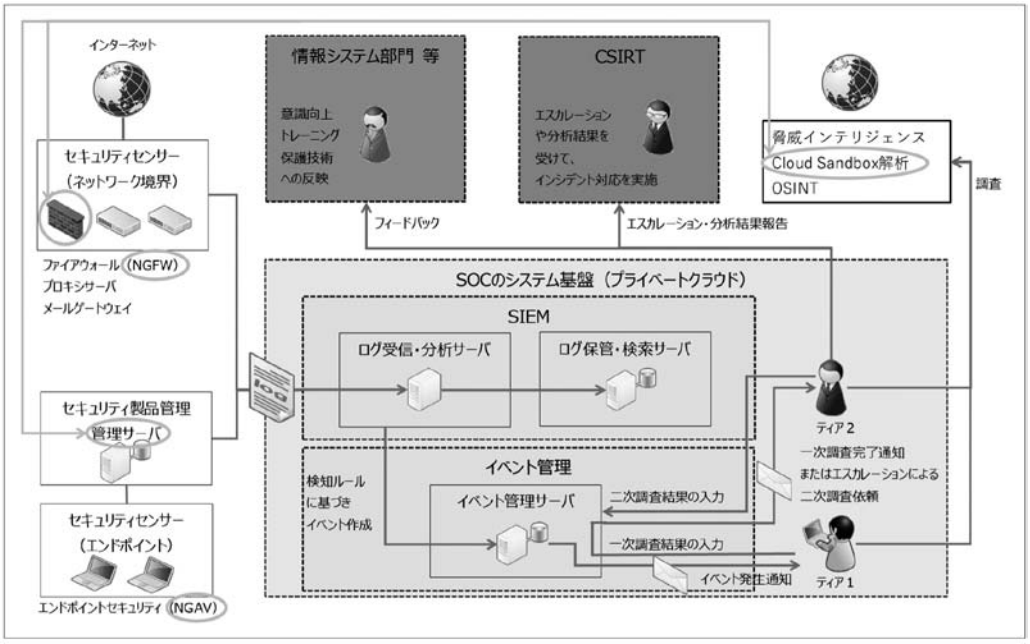

図3　日本ユニシスグループが運用するセキュリティ監視基盤イメージ

3.5　セキュリティ監視基盤と運用の今後

セキュリティ監視基盤が監視すべきセンサーの対象は，3.4.1項に記載の通り，今後も増加することが予測される．時間や場所にとらわれない働き方が進むにつれてネットワーク境界は曖昧となり，今までのネットワーク境界に設置されたセンサーの監視だけでは不十分になることが予想でき，今後はエンドポイントやネットワークトラフィックの監視もより重要性が増すであろう．監視すべきセンサーが増加するということは，センサーが出力するログを保管するストレージ領域が増加することを意味する．また，大量のログの複雑な分析や検索をする際は，高スペックのサーバを準備したり，AIや機械学習といった新しい技術も取り入れなければならない．

このような加速度的に進むセキュリティ監視の状況変化に対応するためには，体制の面では，3.1節に記載のアウトソースすべき分野を整理・認識した上で，自組織のリソースを必要な箇所に集中し有効活用する．また，システム基盤の面では，AIや機械学習等の新しい技術を迅速に取り入れ，安価で柔軟なシステムリソースを確保するために，パブリッククラウドやセキュリティベンダの提供するクラウドサービス型の分析機能を有効活用すべきであろう．

これらのことから，今後はセキュリティ監視基盤も他のサービス等と同様に，運用やシステムの中心はパブリッククラウドに移り，分析機能も外部サービスの利用が中心になると予想される．そのため，企業や組織のセキュリティ監視基盤の運用においては，アウトソースすべき機能の選定に加えて，アウトソースした機能やサービスを正しく理解し活用する能力が求められてくると考えられる．

4.　お　わ　り　に

近年，様々な部分のセンサーログを監視する必要性があることを受けて，各種センサーのロ

グをクラウド上で集約し，クラウドサービスにより各種センサー間のログを AI や機械学習を用いて相関分析する仕組みが登場し始めている点が非常に興味深い．極論ではあるが，このような流れがスタンダードになった際は，それぞれの組織において SIEM そのものや SIEM のためのサーバを保持しなくてよくなる可能性もあり，今後もセキュリティ監視領域の技術動向を注視するべきだろう．

＊1　URL フィルタリングとは，公序良俗に反するサイトやマルウェア等に感染させられる悪質なサイトにアクセスさせないための技術の一つである．閲覧を許可あるいは拒否する URL を列挙し，該当する URL を制限，あるいは逆に該当しないものを全面的に排除することで実現する．

＊2　SIEM（Security Information and Event Management）とは，情報システムを構成する様々な機器やソフトウェアの動作状況の記録（ログ）を一元的に蓄積・管理し，保安上の脅威となる事象をいち早く検知・分析するものを指す．

＊3　OSINT（Open Source INTelligence）とは，オープン・ソース，すなわち一般に公開され利用できる情報を情報源に，機密情報を収集することを指す．

＊4　Sandbox 解析とは，サンドボックス（砂場）と呼ばれる攻撃されても問題のない仮想環境を構築し，その環境内でプログラムを実行することでプログラムの挙動を動的に解析する技術を指す．砂場以外の環境に影響を与えないため，不審なプログラムの挙動を解析する有用な手法として知られている．

＊5　侵入検知システム（Intrusion Detection System：IDS），侵入防御システム（Intrusion Prevention System：IPS）は，通信を監視し，侵入の試みなど不正なアクセスを検知（Detection）または防御（Prevention）する製品や仕組みを指す．

＊6　ディープ Web とは，深層 Web（しんそうウェブ）とも表現され，World Wide Web 上にある情報のうちで，通常の検索エンジンが収集できない情報である．通常の検索エンジンで収集可能な情報は，表層 Web，サーフェス Web，またはビジブル Web と呼ばれる．

＊7　C&C（Command and Control）サーバとは，ボットネットや感染コンピュータのネットワークに対し，不正なコマンドを遠隔で頻繁に送信するために利用されるサーバを指す．

＊8　NGFW（Next Generation Fire Wall）とは，アプリケーションコントロール（L7）の機能を実装し，各アプリケーション固有のトラフィック情報などを解析する機能によりトラフィック内のアプリケーションを識別し可視化，制御することができるファイアウォールを指す．

＊9　NGAV（Next Generation Anti-Virus）とは，エンドポイント上のプロセス等を AI や機械学習といった新しい技術を用いて検査することにより，攻撃者が従来型のパターンマッチングによるアンチウイルス防御をすり抜けるために使用する悪意のあるツールや手法を検出し防御することができる製品を指す．

参考文献

［1］ NIST Cybersecurity Framework, National Institute of Standards and Technology https://www.nist.gov/cyberframework

［2］「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版（頁対訳）」，独立行政法人情報処理推進機構（IPA），2019 年 1 月 https://www.ipa.go.jp/files/000071204.pdf

［3］ 福田　俊介，「サイバーセキュリティフレームワークを応用したアセスメント」，ユニシス技報，日本ユニシス，Vol.39 No.2，通巻 141 号，2019 年 9 月

［4］「セキュリティ対応組織（SOC/CSIRT）の教科書～機能・役割・人材スキル・成熟度～　第 2.1 版」，日本セキュリティオペレーション事業者協議会，2018 年 3 月 https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1.pdf

［5］ 澤田　雅広，「日本ユニシスグループのサイバーセキュリティ戦略」，ユニシス技報，日本ユニシス，Vol.39 No.2，通巻 141 号，2019 年 9 月

［6］「セキュリティ知識分野（Security Body of Knowledge：SecBok）2019」，特定非営利活動法人日本ネットワークセキュリティ協会，2019 年 3 月 https://www.jnsa.org/result/2018/skillmap/data/02_SecBoK2019.xlsx

※　上記参考文献に含まれる URL のリンク先は，2019 年 7 月 24 日時点での存在を確認．

執筆者紹介　石　黒　　怜（Rei Ishiguro）

2006年日本ユニシス(株)入社．金融部門にて地銀勘定系パッケージの適用開発，保守に取り組む．2016年よりセキュリティサービス部にてプライベートSOC運用と米国Unisys社製セキュリティ製品の販売支援に従事．情報処理安全確保支援士．

木 埜　由紀子（Yukiko Kino）

2015年日本ユニシス(株)入社．セキュリティサービス部にて，プライベートSOC運用と脆弱性診断に従事．セキュリティ人材育成など社内セキュリティ啓蒙活動にも取り組む．情報処理安全確保支援士．