第９部

特集9 Cybersecurity Operations Architecture for Secured Internet Infrastructure

近藤 賢郎

第１章　はじめに

近年台頭する未知のセキュリティ脅威に対応すべく，ネットワークやサーバ機器からのログ情報やエンド・デバイス上のソフトウェアの振る舞い等の情報をもとに，セキュリティ脅威を包括的に検知するセキュリティ運用技術の開発が盛んである．一方でそれらのセキュリティ運用技術はセキュリティ事業者が顧客組織にサービスとして提供する形式が一般的であり，その利用形態はセキュリティ事業者に集約された中央集権的なアーキテクチャに基づいたものといえる．例えばManaged SOC（MSOC）サービスの利用は中央集権的なアーキテクチャに基づいたセキュリティ運用の典型例であり，顧客組織で観測されるIDS（Intrusion Detection System）装置やエンドポイントセキュリティ製品に由来するアラートをMSOCサービスに提供する．中央集権的なアーキテクチャに基づいたセキュリティ運用では，顧客組織で観測された異常事象に関する詳細な脅威分析を実施することで，当該顧客組織が受ける脅威活動の有無の把握に有意義である．しかし，異常事象を示すアラートやログ情報の分析では顧客組織が利用する業務システムや外部サービスの種類や性質までをも参照できない場合も多く，結果的に顧客組織において運用者が実施する具体的な対処の効率化が計れない場合も多い．

これらの問題を解決することを目指して，分散型アーキテクチャに基づくセキュリティ運用技術の開発を目標として，本稿では複数組織に跨がったSOC（Security Operation Center）連携をもとにしたセキュリティ運用手法を提案する．本手法では信頼関係のある複数組織間に跨がって対処に係る知識（対処のインテリジェンス）を交換して解析することで，柔軟で正確なセキュリティ脅威の分析を目指す．

本稿では，まず2章でセキュリティ運用のライフサイクルと，対処のインテリジェンスの生成に必要な一次情報を概説する．次に，3章で対処のインテリジェンスの類型と生成を論じ，4章で対処のインテリジェンスを複数組織間で共有することによるセキュリティ運用について論じる．また，5章ではそのために必要な基盤技術について，具体的な成果である(i)ダークネット分析による脅威活動の予兆検知[25]，(ii)分散アウトライアー検知に基づいた不審度判定[26]，(iii)対処支援[27]を中心に述べる．最後に，6章で関連研究を述べて，7章で本稿を纏める．

第２章　セキュリティ運用のライフサイクル

2.1　情報セキュリティリスク

異常事象の発生を検知した際に検知された順に全ての事象に対する対応を実施するのは困難となるため，対応の優先順位付けを実施することは重要である．具体的には，慶應義塾においては毎日3億件程度の異常事象がネットワーク型のセキュリティアプライアンスで検知される．これらの異常事象の中には組織外から組織内に対する単純なスキャニング相当の活動から，個別具体のマルウェアの組織内における潜伏を示すC2通信などが混在する．

対応に先立つ優先順位付けのための手段として一般に情報セキュリティリスクを用いる．ISO/IEC27000:2018を参照すると，情報セキュリティリスクとは「想定される脅威が情報資産の持つ脆弱性を悪用した結果，組織に対して悪影響を与える潜在的可能性」と定義され，脅威，脆弱性，（情報）資産の3つの要素によって構成される．図1には情報セキュリティリスクを構成する脅威，脆弱性，資

産の関係性を示す模式を示す．

脅威とは，システムや組織に対し害を与える望まないインシデントを発生する潜在的原因のことであり，具体的には脅威行為者が標的組織を宛先として実施する攻撃活動として表象する．このため，脅威行為者が有する能力や標的組織に対する攻撃意図の大小に応じて脅威の程度は変化する．脆弱性とは，技術・プロセスなどに内在するサイバーセキュリティ上の欠点・欠陥のことを指し，脅威行為者の視点から利用可能な標的組織が有する技術的・組織的（プロセス/ヒト）な弱点を指す．プロセス上の脆弱性とは，資産管理が適切に行われずパッチが適用されてないサーバが存在する可能性があるといった，業務プロセス上の欠点・欠陥が挙げられる．ヒトに関する脆弱性は，ソーシャルエンジニアリングやフィッシング攻撃など人間の心理を悪用して攻撃に利用され，標的組織内における構成員に対するセキュリティ教育による改善が求められる．資産とは，セキュリティ施策により守るべき対象を指しており，特に，個人情報，顧客情報・機密情報，認証情報，金融情報，知的資産情報などの情報資産があてはまる．これらの情報資産は実体としては組織内やクラウド環境等の情報システム環境に蓄積されていることから，組織内IT資産（計算機，ネットワーク）のインベントリ管理，ソフトウェアの構成管理，外部（クラウド）サービスの利用管理によって，情報資産の所在が担保される．

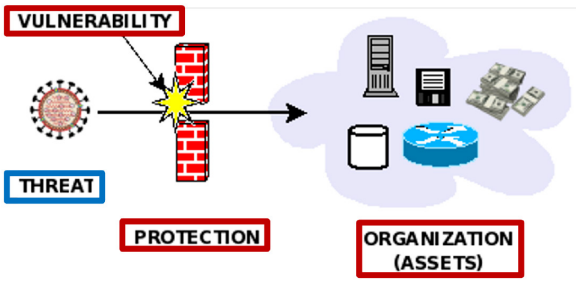

図1 情報セキュリティリスクの定義.

2.2 チケットDBによる対処の状況管理

各組織では，チケットデータベースシステム（チケットDB）など，セキュリティ運用の一環としてインシデント等のセキュリティ事象の対処状況を管理する仕組みを持っている．図2にチケットDBに基づいた異常検知事象への対処手順を示す．異常検知事象を発見した一次対応者は，チケットを起票することでその事象をチケットDB内に登録する．異常事象は平常時の運用の中で発見されるもののため，通常この役割は平常時の環境で情報システム環境を運用するNOC担当者またはその中での異常検知事象の管理を担うSOC担当者が実施する．登録された各チケットはインシデント対応を指揮するディスパッチャによって，その後の対応が必要な場合には対応者（ハンドラー）に割当てられる．ディスパッチャは着目事象以外の事象を含めその時点における全組織的な情報セキュリティ環境を把握していることが求められるため，典型的にはCSIRT担当者がこの役割を担う．ハンドラーは着目事象の性質に基づいて，NOC担当者，SOC担当者，CSIRT担当者の何れかが担う．定常的な運用業務の一環として異常検知事象への対処を実施する場合にはNOC担当者やSOC担当者がハンドラーとして割当てられ，緊急性を要する対処の場面ではCSIRT担当者がハンドラーに割当てられる傾向にある．ハンドラーは対処が進行していく過程をチケットのコメントとして追記する．加えて，主にSOC担当者/CSIRT担当者などセキュリティ事象の検知や対処を主管する者がアドバイザとして，対処に関する助言をチケットにコメントとして追記する場合もあ

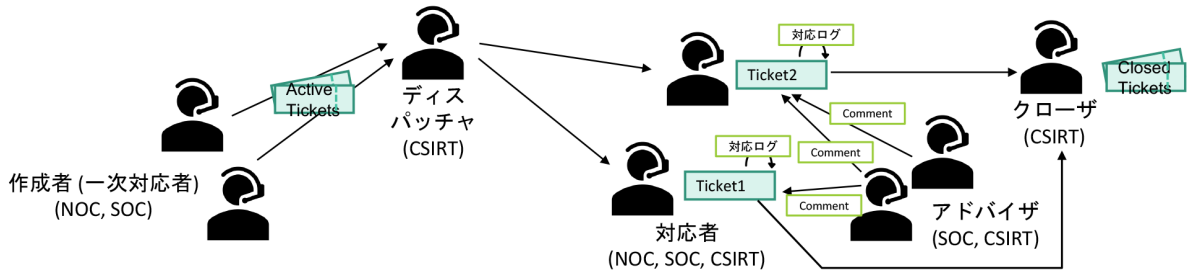

図2 チケットデータベースシステム（チケットDB）に基づいた対処の実施手順.

る．ハンドラーによる対処が完了したら，クローザによって着目事象への対処が必要十分に施されたかの確認を実施して，必要十分な場合には，当該チケットを閉じる．ディスパッチャ同様，クローザにも着目事象以外の事象を含めその時点における全組織的な情報セキュリティ環境を把握していることが求められるため，典型的にはCSIRT担当者がこの役割を担う．

このように各組織ごとのインシデント対処において，調査対象の資産，インシデント発生要因となった脆弱性，調査項目，対応手順，対応者，対応完了までの時間軸等，異常検知事象が認識されてからその対処が完了するまでの対処実績はチケットDBに蓄積される．

本稿では後述する対処に係る知識（インテリジェンス）を生成する際の一次情報の参照先としてチケットDBを想定する．これらの対処実績の中には複数組織にまたがって再利用できない情報（IT資産の構成情報，情報資産の構成情報など）も含まれる場合もある．このため，これらの対処実績の中から再利用可能な情報を抽出する過程が対処に係る知識の生成においては必要となる．

第３章　対処のインテリジェンス

3.1　運用組織で生成される対処のインテリジェンス

セキュリティベンダによって提供される異常検知のための仕組みは，標的組織における様々な異常事象の検知に利用される．そのための仕組みは，シグニチャに基づくパターンマッチやDPIに基づいたL7解析，さらに主にエンドポイント上で観測されるソフトウェアの挙動と攻撃者の振るまいモデル（e.g., MITRE ATT&CK, cyber kill-chain）との比較に基づいた振る舞い検知などである．これらの異常検知のための仕組みは，脅威行為者自身や，標的組織内で観測される脅威行為者の活動の分析に基づいている．このため，検知に係る知識は，広範な脅威行為者の振る舞いを観測可能な脅威インテリジェンス事業者の観測結果に基づくことでスケール性を発揮でき，中央集権的な方法でも効率的に生成可能となる．

一方で，異常検知事象に対する対処は，標的組織ごとに前提となる状況に依存して変化する．つまり，情報セキュリティリスクを構成する技術的/組織的（プロセス，人）な脆弱性や，保護すべき情報資産とそれを蓄積する情報システムの構成，組織ごとの事業継続計画など，標的組織ごとに異なる状況を前提として対処の仕方は変化する．このため，対処に係る知識は基本的に標的組織内で生成されるものとなる．脅威インテリジェンス事業者においても標的組織から情報を集約することで対処に係る知識の生成は可能だが，標的組織毎に前提となる脆弱性や資産の状況が異なるため，それらの前提知識も併せて脅威インテリジェンス事業者に開示する必要がある．これらの前提知識も標的組織ごとに機微な情報資産に当たるため必要以上の情報開示は適切ではない．このため，検知に係る知識の生成と異なり，脅威インテリジェンス事業者における中央集権的な手法に基づいた対処に係る知識の生成はスケール性を発揮できない．

3.2　対処に係るインテリジェンスの類型

対処の優先度付けに係る知識: 主に差し迫った脅威やその脅威に関わる自組織内の脆弱性情報を検知するための知見・ノウハウなどが含まれている．これらの知識は標的組織が実際に享受する情報セキュリティリスクを判断するための知識となるため，運用者がリスク判断の際に利用した脅威行為者に関するアトリビューション情報や，リスク判断の前提となる自組織が保有する守るべき情報資産やIT資産の構成情報が対象となる．これらの知識を分散型SOC基盤を通じて受け取ることで，自組織で生じた嫌疑事象に対する情報セキュリティリスク判定に利用できる．このため迅速な対応が必要なハイリスクな事象の選別を効率的に実施できる点で効果がある．

有事対処の実施に係る知識: 主に有事対応の中で観測された攻撃の具体的な戦略やテクニック，想定される被害の判断，被害に対応した遮断手順といった知見などが含まれる．特に攻撃の具体的な戦略やテクニックは，攻撃者の振る舞いモデル（e.g., MITRE ATT&CK, cyber kill-chain）とマッピングされて示される．これらの知識は攻撃活動が観測された組織で実施される，ダメージコントロールとしての対応手順と，ダメージコントロールの後に実施する詳細な分析を伴う対応手順に関する知見となる．これらの知識を分散型SOC基盤を通じて受け取るこ

とで，着目する事象について自組織への影響度（impact）を判定する際に利用できる．このためインシデントに対する効果的な封じ込め策の選別を効率的に実施できる点で効果がある．

予防手順/事後的な恒久対応に係る知識: 主に（対応が実施された結果）現在は差し迫っていない脅威やその脅威に関わる自組織内の脆弱性情報を検知するための知見・ノウハウなどが含まれている．これらの知識にはサーバ機器やネットワークの管理者向けの情報に加えて，一般利用者向けの注意喚起が含まれる場合もある．

3.3　対処に係るインテリジェンスの生成

各組織ごとのチケットDBに記載された対処実績は通常自然言語にて記録されたものである．これらの対処実績は通常インシデント対処の進行に伴って逐次的に生成されていくもので，3.2節に示された知識が混在した形式で蓄積される．このためチケットDBに蓄積された対処実績から対処に係る知識を生成する仕組みを構築することが必要となる．3.1節では，対処のインテリジェンスを生成するための必要な基本的な情報として，情報資産やIT資産の構成を示すアセット情報と技術面・制度面に跨がった組織の脆弱性情報を示した．本節では，対処実績の中に記載された情報の中から対処に係る知識を生成するために方針として，参照される必要がある具体的な情報を示す．

3.3.1　対処の優先度付けに係る知識の生成

情報資産やIT資産の構成情報以外の点では，対処の優先度付けに係る知識の生成には情報セキュリティリスクを構成する脅威に関する情報が必要となる．重大な脅威として運用者に認識された情報は，脅威インテリジェンス事業者が付与した脅威行為者の名称や，検閲隔離されたマルウェアと既知のIOCとのマッチングの結果などが該当する．さらに異常検知事象が孕む脅威のレベルを判定するための分析手順（e.g., 検閲隔離された検体の静的・動的解析手順）も対処の優先度付けに係る知識に含まれる．

一方で，運用者の視点で有事としての対処と認識された重大な脅威ばかりでなく，有事としての対処を要さないと認識された脅威に関する情報も該当する．例えば，過検知事象として認識されている既知の事象（e.g., セキュリティ製品の特性，複数のセキュリティ製品同士の干渉など），悪性が低い異常検知事象として認識されている既知の事象（e.g., greyware, adwareに対する異常検知判定）などがある．

3.3.2　有事対処の実施に係る知識の生成

3.2節の記した通り，有事対処の実施に係る知識には対処の中で観測された攻撃の具体的な戦略やテクニック，想定される被害の判断，被害に対応した遮断手順といった知見が含まれる．対処実績の中では，攻撃の具体的な戦略やテクニックが具体的に特定される場合（e.g., 総当たり式の認証突破の試行，組織内端末間の横展開の試行，ホスト内の権限昇格の試行）もあるものの，具体的な戦略やテクニックの特定がないままに観測された現象を記録する場合もある．これは有事対処の中で必ずしもすべての観測に対して適切な属性付けが完了しないままに有事対応が進行，収束する場合もあるからだ．前者については攻撃者の振る舞いモデルへのマッピングが容易に実施可能であるものの，後者についてはどのような形式で知識として抽出するかにつきさらなる検討を要する．

想定される被害の判断は，対処の中で観測された事象の中から攻撃者の目的（e.g., 情報流出，サービス妨害）を特定した場合はそれを抽出する．被害に対応した遮断手順は，対処の中で実施した遮断の範囲（e.g., プロセス，エンドホスト，サブネット）を抽出する．

第４章　分散型SOCに基づいたセキュリティ運用

4.1　従来型のセキュリティ運用との比較

図3に分散型SOCに基づくことでセキュリティ運用がどう変化するかの模式を示す．従来よりセキュリティ運用は主にセキュリティ・ベンダが実施した脅威分析の結果を参照して自組織内における異常事象を発見し，それらの事象に対して運用者が対処を実施するものであった．この課程でセキュリティ・ベンダは顧客組織やダークネット等のセンサで観測されたセキュリティイベント情報やアラート情報を対象に脅威分析を実施している．しかし，脅威分析の結果得られるものは異常検知のための

知識であり，顧客組織において運用者が実施する対処自体を効率化する効果は乏しい．

このため，分散型SOCにおいては，運用者が実施する対処から対処に関する知識(インテリジェンス)を生成することを目指し，異常検知と対処の両面に跨がったセキュリティ運用の効率化を目指す．ここでの対処に関するインテリジェンスとは，運用者が実施するセキュリティ運用内の対処に対して再利用可能な知識のことを指す．運用者が実施する対処の中には，表層的なセキュリティイベント情報やアラート情報だけでなく，顧客組織が有する資産情報や脆弱性情報までをも考慮したリスク評価が含まれる．分散型SOCでは，このような運用者がセキュリティ運用する中で暗黙的に実施しているリスク評価の課程をインテリジェンスとして抽出・共有することで，対処の効率化を図る．

4.2　参加組織間の関係

分散型SOCに参加する組織間の関係には密な連携と疎な連携の2種類の類型が考えられる．密な連携は参加組織間の個別の契約所に基づいた契約関係に基づくのに対して，疎な連携は分散型SOCに加入するにあたっての約款同意に基づいた契約関係を想定する．密な連携では分散型SOCに加入する組織間でフルメッシュな契約関係を構築することを想定しているが，既に密な連携を構築しているグループ毎に階層的に契約関係を構築することでスケールアウトさせることが可能となる．これら2種類の関係を想定することで，分散型SOCにおいて共有される情報の種類に柔軟性を持たせるとともに，参加する組織数の拡充を目指す．

密な連携では個別の契約書による契約関係に基づいた関係が想定されることから，分散型SOCにおいて開示される情報の範囲やその開示先における取り扱いについて個別に定義することが可能となる．このため，各組織で観測された情報を生に近い状態で共有することも想定され，そのような情報を活用した早期脅威検知にも積極的に役立てることが可能となる．一方で，疎な連携では，約款同意に基づいた関係が想定されることから，分散型SOCにおいて開示される情報の範囲やその開示先における取扱いについて，個別に定義することが難しい．このため，各組織で観測された情報に機微情報(e.g., 資産情報)が含まれた場合には，それらの情報は原則秘匿化処理を実施した上で共有されることが想定される．

第5章　分散型SOCを実現する基盤技術

図4には分散型SOCを構成する基盤(分散型SOC基盤)の概要を示す．分散型SOC基盤はインフラ部とアプリ部の二つの構成要素から成る．

分散型SOC基盤のインフラ部は(a)他組織との間での対処のインテリジェンスの共有機能を持つデータ共有機能[28]，(b)自組織で生成された対処のインテリジェンスを分散型SOCアプリに提供する際に，インテリジェンス間の相関等の情報を加えるデータ加工機能，(c)分散型SOCアプリが情報を利用する際に利用可能な分散型SOC API，

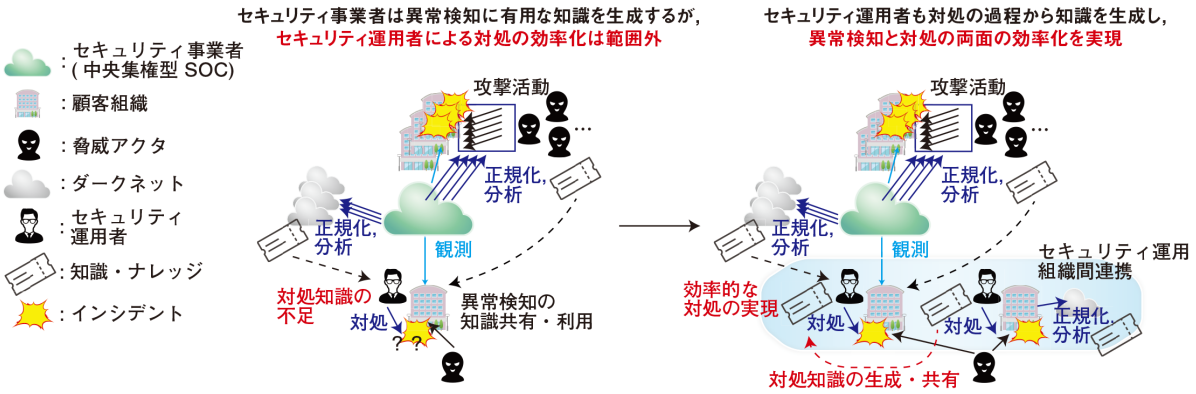

図3　分散型SOC構想に基づいたセキュリティ運用．

(d)自組織で生成された対処のインテリジェンスを他組織に共有する際に加えられる信頼度評価・アクセス制御機能から構成される．分散型SOCアプリは，個々の組織毎に自組織に必要なアプリを選択してそのインスタンスを生成する．現在想定される分散型SOCアプリとしては，(i)ダークネット分析に基づく脅威活動の予兆検知[25]，(ii)分散アウトライアー検知に基づいた不審度判定[26]，(iii)対処支援[27]，(iv)脅威探索がある．3.2節で述べた知識の類型に基づくと，(i)，(ii)，(iv)については対処の優先順位付けにかかる知識を生成し，(iii)については対処手順にかかる知識を生成し，それらを運用者に対して提供する．

5.1　ダークネット分析に基づく脅威活動の予兆検知[25]

研究者やネットワーク運用者は，マルウェア感染，DDoS，脆弱なシステムを見つけるためのスキャンなど，インターネット上の悪意のある活動を理解するために，ダークネットと呼ばれる未使用のインターネット・アドレス空間を定期的に監視している．本研究の目的は，詳細な類似性分析を実施することで，複数の組織にまたがるダークネット監視の有効性を実証することだ．

文献[25]では，業種も第1オクテットのサブネット範囲も異なる2つの組織で観測されたダークネットデータを分析した．1つの組織が組織内で類似性分析を行うようにアドレス空間を複数のブロックに分割し，組織内と組織間の類似性分析結果を比較した。その結果，組織内よりも組織間の方が送信元ホストの類似度が低いことがわかった．また，組織内ではより多くのソースホストを監視した．さらに，送信先のポート/プロトコルによって結果が異なることも報告した．これらの結果から，ダークネットの監視ポイントを複数の組織に分散させることの有効性を明らかにした．

5.2　分散アウトライアー検知に基づいた不審度判定[26]

サイバー攻撃の激化にともない，悪性サイトへの接続を防止する技術が求められている．既存手法としては，ブラックリストやホワイトリストを用いたものがある．しかし，公開されているブラックリストやホワイトリストだけで，インターネット上にあるすべての良性Webサイト，悪性Webサイトを網羅するのは難しい．したがって，これらリストに存在しないサイトが良性か悪性かを判断できないという課題がある．

文献[26]ではこの課題を解決する分散異常検知型AED手法を提案する．提案手法では組織が保有する，サイトへの接続ログを元に接続傾向を分析し，その傾向との乖離度を利用してサイトの良性，悪性を判定する．また，自組織の接続傾向だけでなく，他組織の接続傾向を利用することで判定の精度向上を狙う．さらに，判定で誤って悪性と判断した良性サイトへの接続を即時遮断するのではなく，機械には突破困難な追加認証を課し，突破できなかった場合のみ接続を遮断する．提案システムにより，業務遂行に必要なサイトを誤って悪性と判定した際の業務阻害を緩和しつつ，悪性サイトへの接続を遮断できることが期待できる．

また，評価実験では，他組織の接続傾向を用いることに

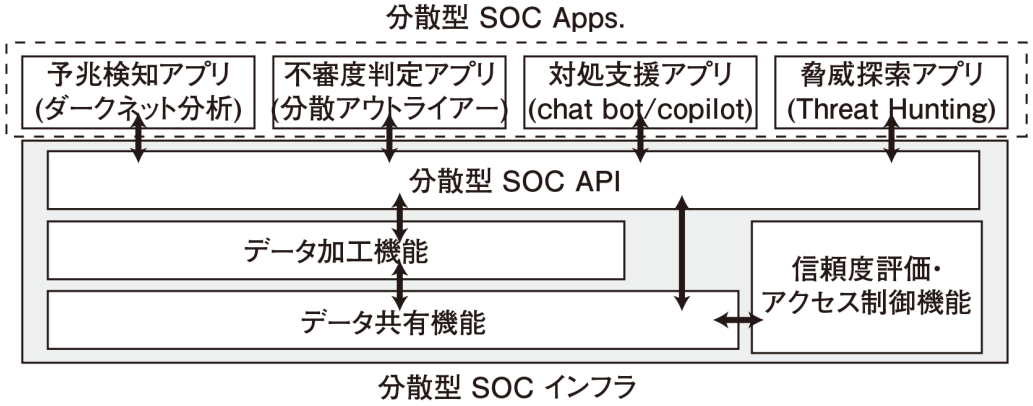

図4　分散型SOCを実現する基盤技術．

よる，不審度検知の精度向上を示した．また，従来方式であるWL型のAEDと比較して，異常検知方式を取り入れることにより，99%以上の検知率を維持した状態で，日々のCAPTCHA発生回数を約3分の1に減らせることを示した．さらに，検知率90，95%以上という，ある程度検知率の低下を許容したケースでは，自組織のみの接続傾向を用いる場合と比較し，他組織の接続傾向を用いることによりCAPTCHA発生回数をさらに削減できることを示した．また，処理性能に関して，処理時間の93.6%が3秒以内であることから，実運用に適応可能だと示した．

5.3 対処支援[27]

サイバー攻撃の増加，高度化にともない，組織では攻撃の見逃しやセキュリティインシデントの対処に膨大な時間を要している．対策の一つとして，複数組織で攻撃関連情報等の情報共有を行い，攻撃への事前対策や事後対応に活用している．情報共有の取り組みは各種存在するが，本研究ではこれまで共有が見られていない，各組織のセキュリティオペレータがセキュリティインシデントに対して実施や検討したやり取りの記録(以下，インシデント対応記録)に着目し，本記録を組織間で共有することの有用性検証と，共有システムの開発について述べる．

先ず，有用性検証では，サイバー攻撃の予防や早期検知，対処中のインシデントの早期解決に有用な情報がインシデント対応記録に存在するのかを，実際の組織のデータを用い評価した．評価の結果，人手による判断により，他組織においても有用であると考えられる情報がインシデント対応記録に含まれていることが明らかとなった．

次に，複数組織間のインシデント対応記録共有システムを設計し，情報共有の主な阻害要因であると考えられている，有用な情報の抽出，及び共有情報内の機微機密情報の保護の手間を，大規模言語モデルを用いることによりどの程度削減可能かを評価した．結果，他組織に共有すべき重要なインシデントに関するインシデント対応記録を，評価者により手動で選別する場合と比較して，正解率72.56%，適合率70.0%，再現率73.7%で自動選別でき，また，インシデント対応記録内のIPアドレスや人名などの機微機密情報を自動で保護できることを確認した．

第６章　関連研究・技術

6.1 組織間に跨がった脅威情報共有

Structured Threat Information eXpression (STIX)[29]はXMLに基づいたセキュリティ脅威を記述するためのフォーマットである．STIXでは観測事象，セキュリティ脅威のインジケータ，攻撃者，脆弱性といった項目を柔軟に記述可能である．STIXではその他のXMLに基づくフォーマット(e.g., Snort[30], Yara[31])を参照することができ，この点でも拡張性に富んだ特性を持っている．Trusted Automated Exchange of Indicator Information (TAXII)[32]はセキュリティ脅威情報を交換するためのプロトコルである．TAXIIを利用することでセキュリティ脅威に関する様々の情報(e.g., IPアドレス，電子メールのヘッダ情報，特定の脆弱性と紐付いたマルウェアの情報)を交換出来る．TAXIIではHTTPやHTTPSを使用した転送仕様をサポートしており，TAXIIで使用するHTTPヘッダが規定されている．このため広範な主体との間でセキュリティ脅威情報の交換が可能となっている．

Incident Object Description Exchange Format (IODEF)[33]はインシデント情報を組織間で交換することを目的としたフォーマットである．IODEFではデータモデルとしての規定がなされている一方でXMLに基づいた利用が想定されており，XML schemaが定義されている．IODEFはインシデントに関わる情報(e.g., 識別子，検知時刻，開始・終了時刻，インシデント評価方法，レスポンス時の連絡先)の柔軟な記述が可能であり，セキュリティ脅威情報の共有の先駆け的な存在とも言える．

6.2 Automted Indicator Sharing

Automted Indicator Sharing (AIS)[34]は米国CISAが提供するサービスで，公共・民間部門の組織間でサイバー脅威指標と防衛策のリアルタイム交換を可能にする．AISはサービス参加者を保護しサイバー攻撃の発生率を減少させることを目的としている．AISコミュニティには民間企業，連邦機関，州・地域・地方(SLTT)政府，ISACs，ISAOs，外国政府パートナーが含まれる．AISは参加者への無料で提供され，敵対行為の試みなど守備策とサイバー脅威指標の共有を可能にし，リアルタイムの洞察に

よりAISコミュニティの他の参加者を保護し、攻撃手法の敵対者による使用を制限する.

AISではサイバー脅威指標と防衛策の情報にはSTIX, マシン間通信にはTAXIIが使用される. これらの標準を使用することで, 参加者間で攻撃のコンテクスト(戦術、技術、手順、脆弱性など)などの情報をプロトコルを介して共有することを可能にする. AIS参加者はSTIX/TAXIIクライアントを使用してCISAと, それに続く他のAIS参加者との間でサイバー脅威指標と防衛策をAIS TAXIIサーバー経由で共有する.

6.3 Security Operations Center: A Systematic Study and Open Challenges

文献[35]では, 文献のシステマティックレビューによってセキュリティ運用を構成する様々な構成要素を人, プロセス, 技術などに分類し, それらの主要な課題を特定している. 具体的には以下のような課題が挙げられている.

1. 人的面での課題: 単調なタスクによるアナリストの燃え尽き症候群, 各組織における専門的な人材の維持
2. プロセス面での課題: プロセスの定義不足, 組織内の他の業務プロセスへのセキュリティ運用の統合の不足
3. 技術面での課題IT環境の複雑性の増加, ツールの多様性と維持管理の困難さ

単調なタスクの処理や多様なツールの維持管理のといった課題はセキュリティ運用業務の自動化によって解消されるため見込みがあるものの, 自動化対象とする業務の取捨選択には組織毎に独自のリスク判断に基づいて実施する必要がある. その過程には, 運用者としての専門的な知見だけでなく, 資産情報等を踏まえた自組織内の他の業務フローとの整合性をも考慮する必要があることから, セキュリティ運用の自動化の前提として本稿が議論する対処に係る知識の生成を踏まえる必要があるものと考える.

第7章 まとめ

本稿では, 分散型アーキテクチャに基づくセキュリティ運用技術の開発を目標として, 複数組織に跨がったSOC(Security Operation Center)連携をもとにしたセキュリティ運用手法を提案した. また, 本稿ではセキュリティ運用を実施する組織による対処に係る知識を, 実運用の中で生成された対処の記録を元に類型化した. その結果, 対処の優先度付けや有事対処を実施する際に, 他組織の運用者が作成した対処ログから再利用可能な知識が生成可能なことを確認した.

さらに, それらの知識を生成する際に必要な基盤技術である分散型SOC基盤の効果を, (i)ダークネット分析に基づく脅威活動の予兆検知[25], (ii)分散アウトライアー検知に基づいた不審度判定[26], (iii)対処支援[27]の3つの機能に関してプロトタイプして検証した. 今後は, 実際のセキュリティ運用環境にプロトタイプを投入して, 分散型SOC基盤に基づいたセキュリティ運用の実現可能性の検証を進めたい.