「マルチメディア，分散，協調とモバイル
(DICOMO2018) シンポジウム」 平成30年7月

分散型 SOC アーキテクチャに基づいた複数組織間における セキュリティ・オペレーションの連携

近藤 賢郎[1]　細川 達己[1]　重本 倫宏[2]　藤井 康広[2]　中村 修[3]

概要：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・オペレーション技術の開発が盛んである．一方でそれらのセキュリティ・オペレーション技術はセキュリティ・ベンダ (Security Provider) がカスタマ組織 (Customer) 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 Security Provider 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．その結果，Customer が利用するネットワーク・サービスの性質やそれらのログ情報を考慮したセキュリティ・オペレーションが困難となり，Customer の数に応じてスケーラビリティ上の問題を生じうる．これらの問題を解決することを目指して，本稿では分散型アーキテクチャに基づくセキュリティ・オペレーション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・オペレーション手法を提案する．本手法では信頼関係のある複数組織間に跨がってセキュリティ・オペレーションに必要な情報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が可能となる．本稿では，提案する手法の実効性を実運用される学術系バックボーンネットワークのトラフィック・トレースを元に複数組織に跨がるセキュリティ・オペレーションを実施して検証する．

A Mechanism of Inter-organization Cooperation for Security Operation based on Decentralized SOC Architecture

Takao Kondo[1]　Tatsumi Hosokawa[1]　Tomohiro Shigemoto[2]　Yasuhiro Fujii[2]　Osamu Nakamura[3]

1. はじめに

近年インターネットに接続する情報環境は標的型攻撃の登場やマルウェア亜種の発生速度の増加に見られるように，未知のセキュリティ脅威に対する対策が課題となっており，その対応のためにセキュリティ・オペレーション技術の開発が盛んである．従来セキュリティ脅威に対してはユーザが持つエンド・デバイスにエンドポイント・セキュリティ・ソフトウェアをインストールした上で，脅威を示すシグニチャとのパターン・マッチを実施することで検知・駆除してきた．しかし未知の脅威に対しては未だシグニチャが生成されていないために，パターン・マッチによる脅威検知は原理的な限界を抱える．そこでネットワーク・トラフィックや各種サーバ機器のログやユーザが持つエンド・デバイス上のソフトウェアの振る舞いを解析することで，セキュリティ脅威を包括的に検知する機構をさしてセキュリティ・オペレーション技術という．

セキュリティ・オペレーション技術は，セキュリティ・オペレーション・センタ (SOC) を抱えるセキュリティ・ベンダ (*Security Provider*) がその顧客となる組織 (*Customer*) に対してサービスとして提供される場合が多い．Customer にはそのネットワーク内に L7 ファイアウォール等のプロトコル解析可能なゲートウェイやネットワーク・センサを配置する．また Customer に属するエンド・デバイスには

[1] 慶應義塾インフォメーションテクノロジーセンター本部
Headquarters of Information Technology Center, Keio University
[2] 株式会社日立製作所
Hitachi, Ltd.
[3] 慶應義塾大学環境情報学部
Faculty of Environment and Information Study, Keio University

そのデバイス上のソフトウェアの振る舞いを監視するエンドポイント・セキュリティ・ソフトウェアがインストールされる．これらのゲートウェイ，ネットワーク・センサ，ソフトウェアから収集される情報は，Security Provider が提供する解析エンジンにて解析され異常がある場合には Customer に通知される．

しかし，Customer から収集される情報には Customer が利用するサービスの性質やそのログ情報が必ずしも含まれておらず，それらの情報を踏まえない振る舞いの解析は非効率である．また Security Provider が一極集中型で SOC 機能を有するモデルでは Customer が増えたときにスケーラビリティ上の問題が生じる．

以上のような問題意識の元，本稿では単一の Security Provider のみにセキュリティ・オペレーションを依存するのではなく，Security Provider と Customer 及び Customer が利用するサービスの事業者 (*Service Provider*) との連携を通じたセキュリティ・オペレーション手法を提案する．本稿で提案するセキュリティ・オペレーション手法は一極集中型でなく分散型の SOC アーキテクチャに基づいた手法といえる．本稿が提案する手法では信頼関係のある複数組織間に跨がってセキュリティ・オペレーションに必要な情報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が可能となる．また SOC 機能を複数組織間で役割分担して持ち合うことで，一極集中型の SOC アーキテクチャがはらんでいたスケーラビリティ上の問題も解消する．

本稿は以下の構成を取る．2 節では既存研究として単一組織内における部門間のセキュリティ・オペレーション連携 [1] を取り上げる．3 節は一極集中型の SOC アーキテクチャと比較する形で分散型 SOC アーキテクチャを定義する．4 節は分散型 SOC アーキテクチャに基づく複数組織に跨がったセキュリティ・オペレーションの連携手法について述べて，5 節にてその実効性を実運用される学術系バックボーンネットワークのトラフィック・トレースを元に検証する．6 節にて複数組織に跨がったセキュリティ脅威情報の共有手法に関する関連研究を述べる．7 節にて今後の方向性を示して 8 節にて本稿を纏める．

2. 既存研究: 単一組織内における部門間セキュリティ・オペレーション連携

2.1 キャンパス・ネットワーク環境におけるセキュリティ・オペレーション

[1] では分散型 SOC アーキテクチャに基づくセキュリティ・オペレーションのための情報基盤を慶應義塾大学矢上キャンパスをモデルとして構築した．このモデルでは大学の教育研究系ネットワークを対象としたセキュリティ・オペレーションを想定している．つまり，ネットワーク資源の運用・管理権限が大学の情報基盤部門から下位接続組織に委譲され，passive monitoring に 基づく SOC 活動を大学の情報基盤部門が実施する環境を想定している．慶應義塾の場合には情報基盤部門としてインフォメーションテクノロジーセンター (ITC) [2] が設置されており，全学的な SOC 機能は ITC が担う．

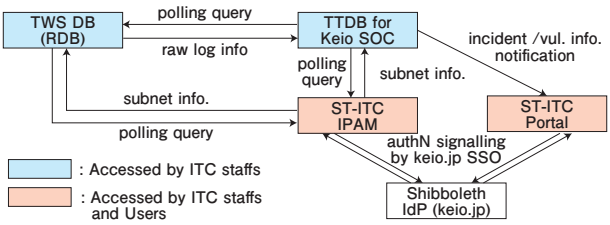

図 1 構成モジュール

ITC では 2003 年頃からトラフィック情報提供システム (TWS) [3] を開発しており，継続的にセキュリティ・オペレーションに取り組んでいる．現在の TWS では学内の主要各キャンパス毎に設置された L7 ファイアウォールからのログ情報，DNS リゾルバにおけるクエリログ情報，主要キャンパス間を接続するバックボーン・ネットワークにおけるフロー情報等を収集して，それらの情報を解析して検知した異常を利用者である下位組織に対して通知する．しかし現状の TWS では (i) ITC と委譲先組織間の双方向のコミュニケーション，(ii) 委譲先組織でのアドレス資源の利用実態の把握，(iii) 生の log 情報からのインシデント情報の抽出が実現されておらず，これらの問題を解決することを目指した情報基盤を [1] では提案する．

2.2 構成モジュール

図 1 に提案した情報基盤の構成モジュールを示す．この情報基盤は (i) ネットワーク・サーバ機器から出力される生のログ情報の蓄積機構 (*TWS DB*), (ii) 生のログを元に抽出されたインシデント情報の蓄積機構 (*TTDB for Keio SOC*), (iii) 委譲されたアドレス資源の管理する IPAM 機構 (*ST-ITC IPAM*), (iv) ITC と委譲先組織とのセキュリティ脅威に関する情報共有のフロントエンドであるポータルサイト (*ST-ITC Portal*), (v) 学内共通認証基盤 (Shibboleth[4], [5] IdP) から構成される．TTDB for Keio SOC は Interop Tokyo Shownet NOC[6] にて開発されたチケットデータベースを改良して，ST-ITC IPAM は Rails アプリケーションとして，ST-ITC Portal は Goole Classroom[7], [8] により構築した．TWS DB と TTDB for Keio SOC は ITC のスタッフのみがアクセスするのに対して，ST-ITC IPAM と ST-ITC Portal は ITC のスタッフに加えてアドレス資源の委譲先組織に属するメンバもアクセスする．従って ST-ITC IPAM と ST-ITC Portal は学内共通認証基盤による認証を踏まえたアクセスとなる．

TWS DB にセキュリティ脅威に関するログ情報が登録されるとポーリングを経てインシデント情報が TTDB for

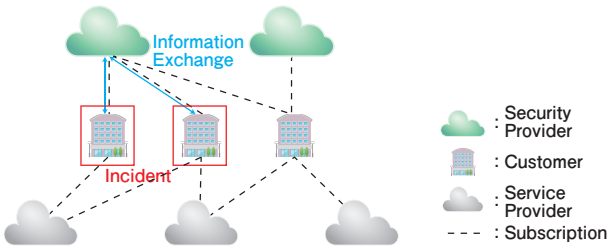

図 2　中央集権型 SOC アーキテクチャ

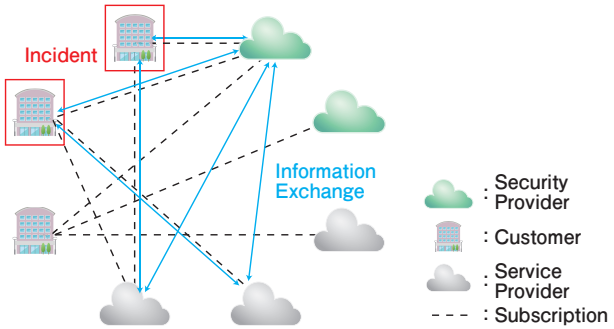

図 3　分散型の SOC アーキテクチャ

Keio SOC に登録される．TTDB for Keio SOC にインシデント情報が登録されると ST-ITC IPAM に登録された情報に従って該当するインシデントがどの委譲先組織が管轄するネットワークで発生したものかが確認されて，ST-ITC Portal の該当組織のページにインシデント情報が配信される．その後のインシデント・レスポンスは ST-ITC Portal を介して ITC と委譲先組織が共同して実施する．

2.3　既存研究と本研究との関係

[1] が想定する教育研究系ネットワークでは，情報基盤部門からアドレス資源の委譲先組織毎にネットワークの運用権限を委譲する．またインシデント発生時のレスポンスは情報基盤部門と共同しつつ基本的には委譲先組織にて実施する．その意味でインシデント・レスポンスの点では自律分散的な運用が取られているといえる．

一方で定常的な SOC 機能については情報基盤部門が一極集中的に実施する想定に立っている．本稿ではこの SOC 機能を複数組織に跨がって役割分担する自律分散型のアーキテクチャに拡張する．自律分散型アーキテクチャに従ったセキュリティ・オペレーションを実施することにより，Customer が利用するサービスやそのサービスの Service Provider が保有するログ情報の特性を生かした SOC 機能を単一障害点なしに実現することが目標である．

3.　分散型 SOC アーキテクチャ

3.1　中央集権型 SOC アーキテクチャの問題点

中央集権型の SOC アーキテクチャに基づくセキュリティ・オペレーションを図 2 に示す．Customer は利用するサービスの Service Provider と SOC 機能を提供する Security Provider との間に subscription を保有しており，Service Provider と Security Provider に対して対価を支払う．結果的に Customer と Service Provider，Customer と Security Provider との間には subscription に基づく信頼関係がある．Customer は Security Provider が提供するセキュリティ・アプライアンス製品を自ネットワークやエンド・デバイスに設置する．設置されたセキュリティ・アプライアンスは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に関する情報を収集して，Security Provider が提供する解析エンジンにて分析する．

Customer にてセキュリティ・インシデントが発生した場合，Security Provider の解析エンジンは Customer のもとで収集できる情報をもとに当該インシデントを分析する．また全ての分析は Security Provider が提供する解析エンジンを元に実施される．しかし，このようなアーキテクチャに基づいたセキュリティ・オペレーションでは Customer が利用するサービスの性質やそのログ情報をもとにした振る舞い解析が実施できない．Service Provider には自身のサービスに関するセマンティクスであったり他の Customer から収集できるログ情報が蓄積されているが，Security Provider はそれらの情報を利用した振る舞い解析を実施することが困難である．また中央集権的なアーキテクチャに起因して全てのセキュリティ・オペレーションは Security Provider にて実施される．結果的に Security Provider が単一障害点となると同時に Customer の数に応じたスケーラビリティ上の問題を孕んでいる．

3.2　分散型 SOC アーキテクチャ

一方で自律分散型の SOC アーキテクチャに基づくセキュリティ・オペレーションを図 3 に示す．この場合も 3.1 節の場合と同様に，Customer は利用するサービスの Service Provider と SOC 機能を提供する Security Provider との間に subscription を保有しており，Customer と Service Provider，Customer と Security Provider との間には subscription に基づく信頼関係があるものとする．

Customer にてセキュリティ・インシデントが発生した場合，Security Provider は Customer のもとで収集した情報を元に当該インシデントを解析出来る．加えて，そのインシデントが Customer が利用するサービスに関わるものである場合，Service Provider にはそのサービス内でやりとりされるメッセージのセマンティクスや他の Customer に関わるログ情報が蓄積されている．分散型 SOC アーキテクチャに基づくセキュリティ・オペレーションでは，これらの情報を含んだ解析を実施する．解析を実施する主体としては Service Provider 自身や Customer が subscription を持つ Security Provider が挙げられる．Security Provider

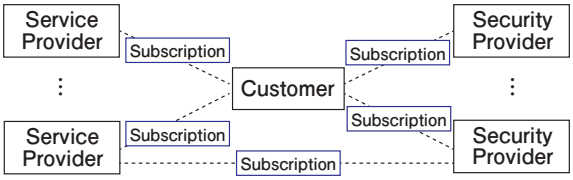

図 4　想定する環境

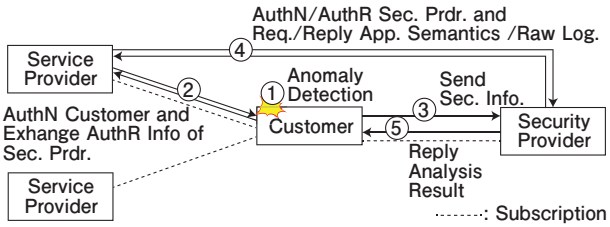

図 5　Customer を起点とするセキュリティ・オペレーション

が解析を実施する場合は，必要に応じて Service Provider から Security Provider に解析に必要な情報が共有される．

Security Provider と Service Provider は何れも Customer との間で subscription を前提とした信頼関係を持つ一方で，両者は直接的には信頼関係を有しない場合がある．従って分散型 SOC アーキテクチャに基づくセキュリティ・オペレーションでは，どの主体がどの情報を利活用できるかについてマルチ・ドメインに跨がった認証認可機構 [9], [10] の利用を前提とする．また Service Provider が保有する他の Customer に関するログ情報を Security Provider との間で共有する場合には，明示的に Customer からの承認が必要となる．セキュリティ・オペレーションを実施する度に個々の Customer から承認をとるのが煩雑な場合は，Service Provider から subscription を購入する際に当該 Customer に関わるログ情報を利用する旨の了承を取る．その場合もログ情報の利活用があった場合には，どのような Security Operation に利用するためにどの情報をどの主体と共有したのかについてのアカウンティング情報が Customer に通知される．

4. 分散型 SOC アーキテクチャに基づくセキュリティ・オペレーション連携

4.1 想定する環境

図 4 に本稿が想定する複数組織に跨がったセキュリティ・オペレーション連携を実施する環境を示す．*Security Provider* とはセキュリティ脅威に関する解析を生業とし，それをサービスとして提供する主体のことを指す．サンドボックス環境といったプロプライエタリなセキュリティ・アプライアンス製品をサービスとして提供する主体や，セキュリティ脅威に関する分析をレポートとして提供する主体が挙げられる．

Service Provider とは，アプリケーションやネットワーク接続性を定常的に運用することを生業とし，それをサービスとして提供する主体のことを指す．Service Provider はアプリケーションを提供する *Application Service Provider* (*ASP*) とネットワーク接続性を提供する *Network Service Provider* (*NSP*) とに大別される．Service Provider は自身が提供するサービスの性質やシグナリング・メッセージのセマンティクスを把握しており，自身が運用するサービスに関する全てのログ情報を保有する．Service Provider は生業としてサービスを継続的に運用する立場にあることから，自力でのセキュリティ・オペレーションを実施する場合も多い．一方で専門的な見地を求めて Security Provider から subscription を購入する場合もある．

Customer は ASP, NSP といった主体からサービスを購入して利用する主体のことを指す．Customer は ASP や NSP が提供するサービスを利用する主体であり，何らかのサービスを生業として継続的に運用する立場にない．このため自力でのセキュリティ・オペレーションは制約を受けることが多いので，その場合には Security Provider から subscription を購入する．

4.2 Customer を起点とする連携

Customer を起点とするセキュリティ・オペレーション連携を図 5 に示す．この事例では Customer と Service Provider，Customer と Security Provider との間にそれぞれ subscription が存在し，両者の間には信頼関係があるものとする．図 5 では Customer が利用するサービス内で検知した異常につき Security Provider にその分析を依頼すると同時に，当該サービスを提供する Service Provider に対しても関連するログ情報の調査と必要に応じて Security Provider への提供を依頼している．Service Provider は Customer からの求めに応じて自身が持つログ情報を調査して，必要があると判断した場合には当該ログ情報を Security Provider に送信する．Service Provider は Customer を認証した後に Customer からの要求を受け付け，Security Provider を認証認可した後に当該ログ情報を Security Provider に送信する．Security Provider の認可に関わる情報は Customer が Service Provider に送信する．

例えば Customer に設置されたメール・アプライアンス機器にて不明な送信元からのメールが検出されたとする．そのメールには添付ファイルがついているものの，メール・アプライアンス機器で実施したシグニチャによるパターン・マッチではマルウェア判定が陽性とならなかったとする．このとき Customer は当該添付ファイルを Security Provider が保有するサンドボックス環境で実行してその振る舞いを検証しつつ，自身が subscription を持つ NSP に対して同じ送信元からのメールが同時期に他の宛先宛に送信されていなかったか調査を依頼する．NSP は Customer からの依頼に応じて調査を実施して流行を確認して，必要

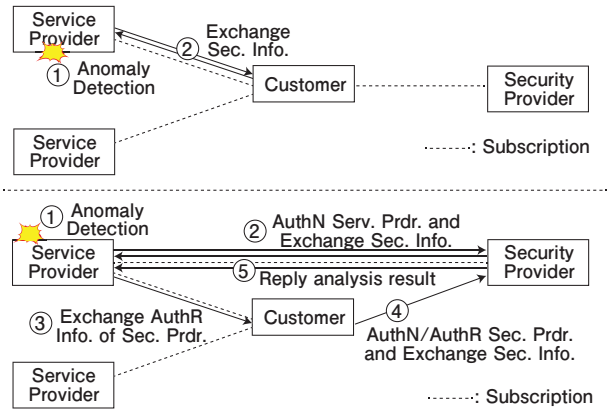

図 6 Service Provider を起点とするセキュリティ・オペレーション

に応じてその調査結果を Security Provider に対して提供する．

4.3 Service Provider を起点とする連携

Service Provider を起点とするセキュリティ・オペレーション連携を図 6 に示す．Service Provider は Customer との間に subscription を保有するものとする．この事例では Service Provider が実施する Security Operation の範囲によって場合分けされる．Service Provider が Security Provider との間で subscription を持っておらず自力でセキュリティ・オペレーションする場合，Service Provider で検知された異常は自身の Customer との間で共有される (図 6 上段)．この場合 Service Provider の視点で Customer は自身の subscription を購読する相手なので，追加での認証認可の手続きは必要ない．

一方 Service Provider が Security Provider との間で subscription を保有する場合には，Service Provider は 検知した異常につき Security Provider にその分析を依頼すると同時に，自身の subscription を購読する customer に対して検体の提供を依頼する場合が考えられる (図 6 下段)．このとき Customer は Service Provider からの依頼に応じて検体を Security Provider に送信して，Security Provier は Service Provider とその Customer の双方からの情報を分析したレポートを Service Provider に返信する．Security Provider は Service Provider を認証した後に Service Provider からの要求を受け付ける．Customer は自身が subscription を持つ Service Provider を経由して Security Provider の認可情報を受信して，検体を送信する前に Security Provider を認証認可する．

図 6 上段について，例えば Customer が subscription を購入する NSP が運用するダークネットにて異常が観測された場合が考えられる．ダークネットで観測されるスキャニングの変化を検知することで未知のセキュリティ脅威に対する早期警戒情報を形成し，それを Customer との間で共有するといった場合である．図 6 下段について，例えば NSP で観測されたフロー情報を元に Security Provider に対して解析を依頼した場合に，Security Provider にて NSP 配下の Customer を標的にした Advanced Persistent Threat (APT) 攻撃の疑いが判明した場合が挙げられる．このとき NSP にはフロー粒度のログ情報しか残っていないために，メール等の検体の提供を当該 Customer に依頼するといった場合である．

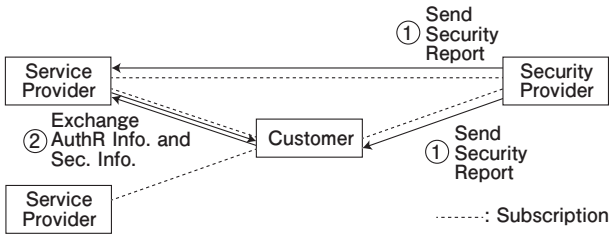

図 7 Security Provider を起点とするセキュリティ・オペレーション

4.4 Security Provider を起点とする連携

Security Provider を起点とするセキュリティ・オペレーション連携を図 7 に示す．Security Provider は Service Provider と Customoer との双方の間に subscription を持つものとする．この事例では Security Provider が提供するセキュリティ・アナリストによるレポートの送付が起点となる．Security Provider が提供するレポートの内容が自組織で該当するかを確認するためには，自組織でのセキュリティ・オペレーションによって実際に観測して検証する必要がある．その観測結果を Service Provider と Customer 間で共有することで，観測結果の流行を確認することが出来る．Service Provider と Customer との間での観測結果を共有する前に，互いに Security Provider からのレポートに関する subscription を保有を確認する必要がある．このため観測結果の共有に先立って Service Provider と Customer との間で認可情報が交換される．

5. 慶應・WIDE・日立間のセキュリティ・オペレーション連携

慶應義塾 ITC 及び慶應義塾大学サイバーセキュリティ研究センター [11] と株式会社日立製作所 [12] は複数組織に跨がった SOC 間連携を実施するための運用技術に関する協同研究を実施している．本節では 4 節で示した複数組織に跨がったセキュリティ・オペレーション連携を，慶應義塾大学を Customer，慶應大学にインターネット接続性をサービスとして提供する WIDE Project[13] を NSP，Security Provider を日立製作所と想定して検証する．特に 4.2 節で述べた Customer を起点としたセキュリティ・オペレーション連携を取り上げる．

慶應義塾 ITC に設置されたメール・アプライアンス機器にて，不明な送信元からのメールが検出された．このアプライアンス機器が実施したシグニチャのパターン・マッ

チに基づく判別ではメールの添付ファイルに対するマルウェア判定が陽性とはならなかった．そこで慶應義塾 ITC は 日立製作所に対して動的解析環境 [14] における当該添付ファイルの実行および振る舞いの検証を依頼すると同時に，WIDE Project に対して当該メールを受信した時刻から 1 時間遡ったトラフィック・トレース [15], [16] を対象に同じ送信元から他の宛先に対しても同様のメールが送信されているかの調査を依頼した．その結果，日立製作所からは当該添付ファイルがフィッシング・サイトに誘導するマルウェアであるとの報告を受けるのと同時に，WIDE Project からは慶應義塾以外の宛先に対しても同様のメールが多数送信されていたとの報告を受けた．これらの結果を併せることで，このメールは慶應義塾を殊更標的としない悪意を持ったメールであると判別された．

6. 関連研究

本節では複数組織に跨がったセキュリティ脅威情報の共有手法に関する関連研究として STIX/TAXII[17], [18], CVE/CVSS[19], [20], IODEF[21] について述べる．

6.1 STIX/TAXII

Structured Threat Information eXpression (*STIX*) 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[22], Yara[23]) 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*) 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．

6.2 CVE/CVSS

Common Vulnerabilities and Exposures (*CVE*) は発見されたなセキュリティ脅威に関する一意な識別子を提供する．この識別子を用いることでベンダ間に跨がってセキュリティ脅威を一意に特定することができ，当該脅威自体の評価やその対策ツールの開発に役立つ．*Common Vulnerability Scoring System* (*CVSS*) は CVE によって一意に特定されたセキュリティ脅威の重篤度を評価するためのフレームワークである．CVSS はセキュリティ脅威に対するオープンで包括的，汎用的な評価手法の確立と普及を目指して提案され，現在では CVE と同様にベンダ間を跨がって広く用いられている．

6.3 IODEF

Incident Object Description Exchange Format (*IODEF*) 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．

7. 今後の方向性

(i) 共有される情報の抽象化: 本稿で述べたセキュリティ・オペレーションでは，セキュリティ脅威情報を交換し合う主体間において subscription を根拠とする信頼関係を前提としている．この信頼関係を根拠として生のログ情報を含んだセキュリティ脅威情報の共有を想定して，複数主体に跨がって分散した SOC 機能によるセキュリティ・オペレーションを実現する．しかし subscription を前提とした信頼関係を前提としたときも，共有されるセキュリティ脅威情報の中にどの情報が含まれるかは共有する相手によって区別すべきである．このためセキュリティ・オペレーションを共同する主体の信頼関係をクラス分けして，そのクラスに応じた共有情報の抽象化を実施する必要がある．

(ii) 組織間に跨がったマルチドメイン環境での認証認可: 3.2 節で述べたとおり，分散型 SOC アーキテクチャに基づいた複数主体に跨がったセキュリティ・オペレーション連携を実現するためには，マルチドメイン環境での認証認可 [9], [10] を実現する必要がある．このような認証認可機構を前提とすることで，subscription を前提とした SOC 機能を分散して担う主体間の信頼関係を構築することができる．

(iii) ASP を含んだセキュリティ・オペレーション連携: 本稿では Service Provider として主に NSP を想定したセキュリティ・オペレーション連携を述べた．このため ASP との連携を含むセキュリティ・オペレーションについても検討する必要がある．特に ASP が展開するサービスの特性やシグナリング・メッセージのセマンティクスを踏まえた上でのセキュリティ脅威分析について検討の余地が残る．

図 8 に 2 節で述べた既存研究で提案する情報基盤に複数組織に跨がったセキュリティ・オペレーション連携を実現する機構を加えたモジュール構成を示す．既存研究で提案した情報基盤 (図 1) と比較すると，SOC 間連携を仲介するエージェント (*InterSOC Agent*) と SOC 間連携時の認証認可機構 (*AAA for InterSOC Comm.*) がモジュールと

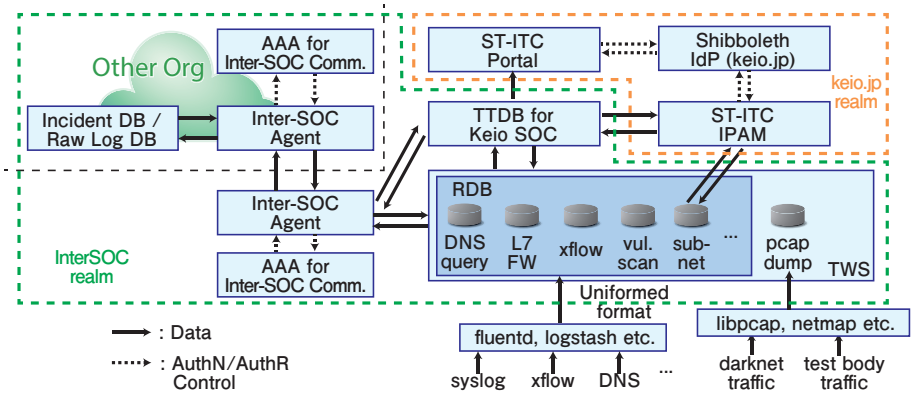

図 8　複数組織間の SOC 機能連携を前提とした情報基盤

して追加されている．SOC 間に跨がった情報交換は全て InterSOC Agent を介して行われる．TWS DB や TTDB for Keio SOC といった生のログ情報データベースやインデント情報データベースは SOC 間連携時には InterSOC Agent の内側に隠蔽される．また学内共通認証基盤である Shibboleth IdP とは別に SOC 間連携用途の認証認可機構を AAA for InterSOC Comm. として配置する．これは Shibboleth IdP が学内のシングルドメインを前提とした IdP なのに対して AAA for InterSOC Comm. はマルチドメインに跨がった認証認可を実現する必要があるからである．

8. 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・オペレーション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・オペレーション手法を提案する．本手法では信頼関係のある Customer, Service Provider, Security Provider の間でセキュリティ・オペレーションに必要な情報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が可能となる．本稿では分散型 SOC アーキテクチャに基づくセキュリティ・オペレーション手法を起点となる主体によって分類した後に，その実効性を実運用される学術系バックボーンネットワークのトラフィック・トレースを元に検証した．

参考文献

[1] 近藤賢郎, 中島春香, 細川達己, 藤井康広, 藤井翔太, 林直樹, 鬼頭哲郎, 重本倫宏, 鍛忠司, 鈴木茂哉, 中村修, 砂原秀樹. 大学ネットワーク環境における SOC/CSIRT 活動に用いる情報共有基盤の提案. In *Proc. of IPSJ IOT40 WKSHP*, 2018.

[2] 慶應義塾 ITC. `http://www.itc.keio.ac.jp/ja/top_itc.html`.

[3] 細川達巳, 金子康樹. 大学ネットワークにおけるサブネット管理者とのネットワークセキュリティ・トラフィック情報の共有. In *Proc. of AXIES '17*, 2017.

[4] W. Jie, A. Young, J. Arshad, J. Finch, and R. Procter. A Guanxi Shibboleth based Security Infrastructure. In *Proc. of IEEE EDOC WKSHPS'08*, pp. 151–158, 2008.

[5] R. O. Sinnott, J. Jiang, J. Watt, and O. Ajayi. Shibboleth-based Access to and Usage of Grid Resources. In *Proc. of IEEE/ACM Int. Conf, of Grid Resources '06*, pp. 136–143, 2006.

[6] Interop Tokyo. `https://www.interop.jp/`.

[7] G Suite for Education. `https://edu.google.com/intl/ja/`.

[8] Google Claassroom. `https://edu.google.com/intl/ja/products/productivity-tools/classroom/`.

[9] Y. Atsuya, K. Kaneko, and F. Teraoka. Yamata-no-Orochi: an Authentication and Authorization Infrastructure for Internet Services (in Japanese). *IPSJ Journal*, Vol. 55, No. 2, pp. 849–864, 2014.

[10] S. Ben Ayed and F. Teraoka. Collaborative Access Control for Multi-Domain Cloud Computing. *IEICE Trans. on Info. and Sys.*, Vol. E95-D, No. 10, pp. 2401–2414, 2012.

[11] サイバーセキュリティ研究センター - 慶應義塾大学 先導研究センター. `http://www.karc.keio.ac.jp/center/center-54.html`.

[12] Hitachi Global. `http://www.hitachi.com/`.

[13] WIDE backbone. `http://two.wide.ad.jp/`.

[14] 仲小路博史, 鬼頭倫宏, 林直樹, 寺田真敏, 菊池浩明. 多種環境マルウェア動的解析システムの提案および評価. 情報処理学会論文誌, Vol. 56, No. 9, pp. 1730–1744, 2015.

[15] MAWI Working Group Traffic Archive. `http://mawi.wide.ad.jp/mawi/`.

[16] K. Cho, K. Mitsuya, and A. Kato. Traffic data repository at the wide project. In *Proc. of USENIX ATC, FREENIX Track*, 2000.

[17] S. Barnum. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX). Technical Papers, *MITRE*, 2012.

[18] J. Connolly, M. Davidson, M. Richard, and C. Skorupka. The Trusted Automated eXchange of Indicator Information (TAXII) . Technical Papers, *MITRE*, 2012.

[19] CVE - Common Vulnerabilities and Exposures. `https://cve.mitre.org/`.

[20] Common Vulnerability Scoring System SIG. `https://www.first.org/cvss/`.

[21] R. Danyliw. The Incident Object Description Exchange Format Version 2. RFC 7970, *IETF*, 2016.

[22] Snort - Network Intrusion Detection & Prevention System. `https://www.snort.org/`.

[23] YaraRules Project. `http://yararules.com/`.