Vol.2018-IOT-40 No.30
2018/3/6

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

近藤 賢郎[1,a)]　中島 春香[2]　細川 達己[1]　藤井 康広[5]　藤井 翔太[5]　林 直樹[5]　鬼頭 哲郎[5]
重本 倫宏[5]　鍛 忠司[5]　鈴木 茂哉[2]　中村 修[4]　砂原 秀樹[3]

概要：本研究では，大学の教育研究系ネットワークを対象とした SOC/CSIRT 活動に用いるための情報共有基盤を提案し，実際のキャンパス・ネットワーク環境をモデルとして実装・構築する．本基盤は (i) 大学の情報基盤部門における SOC 活動から得られた生のログの蓄積機構，(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，(iii) 情報基盤部門から委譲されたアドレス資源を管理するための IPAM 機構，(iii) 情報基盤部門と委譲先組織間でセキュリティ脅威の情報共有のためのポータルサイト機構から構成される．これらの基盤を通して情報基盤部門から委譲されたアドレス資源の使用実態に基づいた SOC 活動と，情報基盤部門と委譲先組織間での日常的なセキュリティ脅威情報の共有やインシデント発生時に両者間で途切れることのない意思疎通が可能となる．本研究は慶應義塾大学における実際のキャンパス・ネットワーク環境をモデルとして実装・構築された．(i) は本学 SOC 活動のために慶應義塾 ITC で開発された TWS (トラフィック情報提供システム) を用いた．(ii) は Interop Tokyo Shownet NOC で開発された TTDB と呼ばれるチケットデータベースに改変を加えて構築した．(iii) は Rails アプリケーションとして，(iv) は Google Classroom により実装・構築した．また本研究では単一組織による SOC 活動の限界を取り除くために複数組織に跨がる SOC 間連携の検証を行った．

キーワード：セキュリティ・オペレーション，セキュリティ・オートメーション，教育研究系ネットワーク

A Proposal of Information Exchange Infrastructure for SOC/CSIRT Activities in Campus Network Environment

Kondo Takao[1,a)]　Nakashima Haruka[2]　Hosokawa Tatsumi[1]　Fujii Yasuhiro[5]　Fujii Shota[5]
Hayashi Naoki[5]　Kito Tetsuro[5]　Shigemoto Tomohiro[5]　Kaji Tadashi[5]　Suzuki Shigeya[2]
Nakamura Osamu[4]　Sunahara Hideki[3]

1. はじめに

大学のネットワーク環境は広大なアドレス資源を有しており，一般に業務部門と教育研究部門の二つのネットワークから構成される．業務部門系ネットワークは大学内の業務部門が学内向けに展開するサービスを展開したり，業務部門に属する職員がアクセス線として利用する．教育研究系ネットワークは学生や教員がアクセス線として利用したり，対外的な研究業績等の情報公開に加え学術研究活動を支える情報基盤としての役割も担う．慶應義塾インフォ

[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] 慶應義塾大学大学院政策・メディア研究科
Graduate School of Media and Governance, Keio University
[3] 慶應義塾大学大学院メディアデザイン研究科
Graduate School of Media Design, Keio University
[4] 慶應義塾大学環境情報学部
Faculty of Environment and Information Studies, Keio University
[5] 株式会社日立製作所
Hitachi, Ltd.
[a)] latte@itc.keio.ac.jp

メーションテクノロジーセンター (ITC)[1] は弊学におけるキャンパス・ネットワーク環境の構築・運用を担う組織であり，近年台頭するセキュリティ脅威に対応すべく弊学におけるセキュリティ・オペレーション・センタ (SOC) 活動も担う．

慶應義塾における教育研究系ネットワークは教育研究活動を尊重するとの目的から ITC はその運用を学部・学科や研究室等の組織に委譲している．ITC における SOC 活動に関しても利用者からの申請なしには過度な traffic filtering は実施せず，原則 passive monitoring に留めている．Passive monitoring に基づく監視で学内外向けの攻撃トラフィックを発見した場合は，委譲先組織の利用者に通知して対応を依頼・管理する．

本研究はこのように (i) ネットワーク資源の運用・管理権限が下位接続組織に委譲され，(ii) passive monitoring に基づく SOC 活動を実施するといった特徴をもつ教育研究系ネットワークを対象に，SOC/CSIRT 活動に用いるための情報基盤を提案する．本基盤は (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，(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，(iii) 委譲されたアドレス資源の管理する IPAM 機構，(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から構成される．これらの基盤を通して ITC から委譲されたアドレス資源の使用実態に基づいた SOC 活動と，ITC と委譲先組織間での日常的なセキュリティ脅威情報の共有やインシデント発生時に両者間で途切れることのない意思疎通が可能となる．

本研究は慶應義塾大学における実際のキャンパス・ネットワーク環境をモデルとして実装・構築された．(i) は弊学 SOC 活動のために ITC で開発されたトラフィック情報提供システム (TWS)[2] を用いた．(ii) は Interop Tokyo Shownet で開発された TTDB と呼ばれるチケットデータベースに改変を加えて構築した．(iii) は Rails アプリケーションとして，(iv) は Google Classroom により実装・構築した．

2. 既存技術: トラフィック情報提供システム (TWS)

本章では慶應義塾 ITC において開発されたトラフィック情報提供システム (TWS)[2] について概説する．TWS は慶應義塾 ITC が所有するネットワーク・サーバ機器からのログを収集して解析し，必要に応じてその結果をネットワーク資源の委譲先組織等に提供するシステムである．

2.1 TWS が構築された経緯

TWS は慶應義塾においてファイル共有ソフトウェア利用に関するポリシを導入した 2003 年頃にから開発が始まったシステムである．当初は慶應義塾のキャンパス間ネットワークを構成する基幹ルータが生成する access control list (ACL) のログを元に解析を実施していた．2012 年に L7 ファイアウォールを導入して以後は TWS への情報ソースの中心は L7 ファイアウォールとなり，アプリケーション可視化まで範疇となった．加えて TWS 内の情報の記録・検索用途に RDBMS を導入した．TWS の開発により学内のインシデントの発見や発生後の原因究明が容易に実施できるようになった

2.2 TWS の現在の構成

2016 年 - 2017 年にかけて TWS の改修が実施された．主な改修事項は以下の通りである．(i) 準リアルタイムな DB への格納: 従来 TWS 内 RDBMS への同期頻度はは一日に一回であったが数分毎に一回に改修された．

(ii) ログ増大に対応した高速化 (二次記憶の SSD 化が中心): L7 ファイアウォールの導入が契機となり 2012 年には 1000 万行 / 日であったログの入力が 2016 年には 9000 万行 / 日にまで増加していた．それに対応するために主に二次記憶の SSD 化を中心とした高速化を実施した．その結果，学内基幹ルータが出力するフロー情報や DNS フルリゾルバが出力するのクエリ LOG といったさらなる情報ソースの追加が可能となった．結果的に 2017 年現在 1 日に約 5 億行，100 GB の情報が TWS には保存されている．

(iii) アドレス資源の割当情報 DB との連携: アドレス資源が ITC から下位接続組織に委譲・割当される教育研究系ネットワークでは，ITC 内の SOC 活動にて発見されたセキュリティ脅威に対する対応も原則的にアドレス資源の割当を受けた委譲先組織が行うポリシに基づく．このため SOC 活動で発見したセキュリティ脅威がどの下位接続組織に割り当てられているセグメントで発生したのかを特定する仕組みが導入された．

(iv) アドレス資源の委譲先組織への通知機能: 2017 年 1 月より希望があった委譲先組織に対して，ITC が実施する SOC 活動の中でその組織が割当を受けたネットワーク資源に対するセキュリティ脅威が見つかれば自動的にメール通知される機構が導入された．大学組織の性質上，委譲先組織にコンピュータ・セキュリティの専門家が在籍するとは必ずしも限らないので，偽陽性が少なく理解しやすい項目に関する通知を実施している．例えば学外向けセッション (SSH, RDP, SMTP etc.) に関するセッション数の異常上昇，L7 ファイアウォールが判定できなかった大量トラフィック，学外への脅威トラフィック等である．

3. 本研究における問題意識

本研究ではこれまで TWS をもとに実施していた SOC 活動に対して以下の問題意識を提起している．(i) ITC と委譲先組織間の双方向のコミュニケーション: TWS では

アドレス資源の希望する委譲先組織に対して自ネットワークに関するセキュリティ脅威情報の通知を実施している．しかし，セキュリティ脅威が発見された後にその対応に関する ITC と委譲先組織との間のコミュニケーションは基本的にメールに基づくものとなる．SOC 活動によって発見されたセキュリティ脅威に関して委譲先組織でどのような対応がなされたかを ITC の視点で正確に把握し管理するためには，両者間でメールで記されるより細かな粒度でインタラクティブに情報を交換する必要がある．

(ii) 委譲先組織でのアドレス資源の利用実態の把握: ITC から下位接続組織に対してネットワーク資源を割り当てる際には，一定のアドレスレンジ毎に委譲が割り当てされることが多い．従って ITC の視点では割り当てたアドレス資源に含まれる個々のアドレスがどのような用途で使用されているのかを把握するためにはは逐一ヒアリングを実施する必要がありコストが大きい．ITC による SOC 活動の精度を省コストで実現するためには委譲されたアドレス資源がどのような用途で利用されているのかの実態を把握する必要がある．

(iii) 生の log 情報からのインシデント情報の抽出機構: 2017 年現在，TWS が収集する ITC が保有するネットワーク・サーバ機器から収集される情報は 5 億行 / 日にも及ぶ．2.2 節にて例示して言及したように，現在の TWS にもこれらの膨大な log 情報から有意味なインシデント・セキュリティ脅威情報を抽出する機構は含まれているものの，その網羅率には課題が残る．これら収集された膨大な生の log 情報から現実のインシデント・セキュリティ脅威情報を抽出し，その単位で ITC 内の教職員や下位接続組織内の利用者に対して情報を提示する必要がある．

4. 情報基盤の設計と実装

本研究では 3 節で述べた問題意識に基づき，教育研究系ネットワークにおける SOC/CSIRT 活動に用いるための情報基盤を提案する．また本研究では慶應義塾大学矢上キャンパスの環境をモデルとして本基盤を実装した．矢上キャンパスには理工学部を構成する 11 学科のそれぞれに 10 - 20 個の研究室が所属する．このような矢上キャンパスにおける多種多様な下位接続組織形態を踏まえ，本学内における教育研究系ネットワークのモデルとして矢上キャンパスを選択した．

4.1 ITC による SOC 活動の実施環境

図 1 に慶應義塾におけるネットワーク環境として KEIO-NET (AS38635) の概要を示す．KEIO-NET は慶應義塾の主要 6 キャンパス (日吉，三田，矢上，信濃町，芝，藤沢) を中心に展開されるバックボーン・ネットワーク (BB ネットワーク) を持つ．BB ネットワークにおけるキャンパス間の隣接関係は Layer 3 に基づく．各キャンパスに広

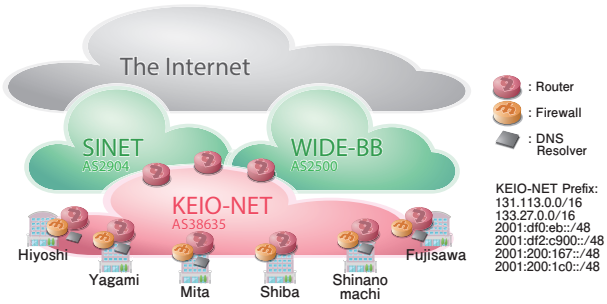

図 1 KEIO-NET (AS38635) のネットワーク環境

がる教育研究系ネットワークは BB ネットワークのスタブ・ネットワークとして構成される．また KEIO-NET は上流 ISP に対して複数 (SINET に対して 2 箇所，WIDE に対して 1 箇所) の接続を持つ．このため KEIO-NET と対外組織との間の通信は非対称な経路によって基づく場合がある．

ITC では L7 ファイアウォールやフロー情報，DNS リゾルバ内のクエリ log 等の passive monitoring を実施している．L7 ファイアウォールは各キャンパス毎に BB ネットワークとの接続境界点に設置されている．このように上流 ISP との接続点でなく各キャンパス毎に L7 ファイアウォールを設置することで，上流 ISP との接続点が複数あることに由来する非対称な経路が L7 ファイアウォールのセキュリティ脅威の検知に影響しなくなる．フロー情報についても各キャンパス毎に BB ネットワークとの接続境界点で収集されている．さらに芝共立キャンパスを除く主要 5 キャンパスにおいて学内向け DNS リゾルバが設置されており，それらのリゾルバからクエリ log が収集されている．

教育研究系ネットワークでは ITC から学部・学科，研究室等の下位接続組織に対してアドレス資源が割り当てられ，その運用を該当組織に委譲される．特に，ITC から学科に対して割り当てられたアドレス資源の一部が再度学科から研究室に割り当てられるといったような，ITC からの視点でアドレス資源の再委譲もポリシ上許容される．このようなポリシを前提として ITC での SOC 活動を精度良く遂行するためには，委譲先組織との連携を通じて個々のアドレス資源の利用実態を ITC にて把握することが必要である．

4.2 構成モジュール

図 2 に矢上キャンパスをモデルとした際の提案する情報基盤のモジュール群をしめす．(i) 生の log 情報の格納機構 (TWS DB)，(ii) インシデント情報の抽出・格納機構 (TTDB for Keio SOC), (iii) 委譲されたアドレス資源の管理機構 (ST-ITC IPAM), (iv) ITC と委譲先組織間のセキュリティ脅威情報共有のためのポータルサイト (ST-ITC Portal), (v) 慶應義塾共通情報基盤 (keio.jp)[3] である．

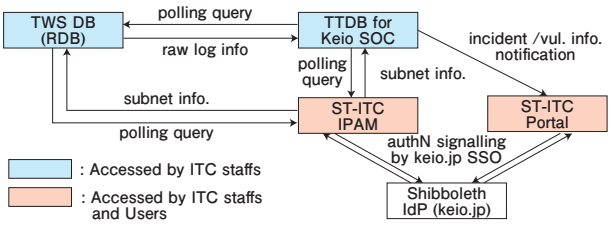

図 2　提案する情報基盤の構成モジュール

4.2.1　TWS DB

TWS DB は既存技術として 2 節であげたトラフィック情報提供システム (TWS) が収集する情報を格納する機構である．矢上キャンパスを含む全キャンパスの教研系ネットワークを対象に L7 ファイアウォールの log 情報，フロー情報，DNS クエリ log 情報を準リアルタイムに格納する．これらの情報は RDB に格納されるのでセキュリティ脆弱性の発見やインシデント発見後の原因究明の場面で SQL クエリによる検索が可能である．

4.2.2　TTDB for Keio SOC

TTDB for Keio SOC は TWS DB に蓄積される生の log 情報からインシデント・セキュリティ脅威情報を抽出して格納するチケット・データベース機構である．本研究では一つインシデントやセキュリティ脅威情報を一つのチケットとして取り扱う．TWS DB の log 情報から抽出したインシデントやセキュリティ脅威情報は一つのチケットとして起票される．起票されたチケットは委譲先組織の担当者に割り当てられる．当該担当者がインシデントやセキュリティ脅威に対する対応を完了した旨を ITC の教職員が確認すると，当該チケットは閉じられてアーカイブされる．

TTDB とは Interop Tokyo[4] Shownet NOC にて開発されている会場ネットワーク (Shownet) の設定やトラブル対応のためのチケットデータベースである．Shownet NOC では Interop 出展社組織に対してネットワーク資源を割り当ててその運用を委譲する．出展社組織は割り当てられたアドレス資源を Interop 会期中にわたって自ら運用しつつ，その上で自社ネットワーク・システム製品を展示する．Shownet の構成上ネットワーク資源を下位接続組織に対して委譲して運用するモデルのため，TTDB にはアドレス資源管理やその委譲先組織といった要素に基づくデータモデリングがなされている．Shownet のこのような環境が大学における教育研究系ネットワークを取り巻く環境と類似することから本研究ではチケットデータベースとして TTDB を採用した．TTDB を SOC 活動でも活用するために本研究では TTDB に対してインシデントやセキュリティ脆弱性情報に関するデータ構造を追加した．また SOC 活動に必要にないデータ構造 (出展社情報など) や機能を削除した．追加したデータ構造としては例えばインシデントやセキュリティ脆弱性のイベントがある．そのデータ構造には，イベントの発生・発見・収束日時，severity, イベント ID，委譲先組織 ID などが含まれる，

4.2.3　ST-ITC IPAM

ST-ITC IPAM は矢上キャンパス内の学科や研究室等に委譲されたアドレス資源を管理するための IPAM 機構である．この IPAM 機構では，ITC の教職員及びアドレス資源の委譲先組織に属するものが当該アドレス資源に関する管理権限を有している．

ST-ITC IPAM は ITC 内で Rails アプリケーションとして開発された．IPAM アプライアンス製品は市場に数多くあるものの，本研究の範囲では DNS 権威サーバや DHCP サーバとの連携といった機能は余剰な要素となる．また ITC における SOC 活動の変化等により本研究において提案・実装する情報基盤内のデータ構造や API が今後変化する可能性も残される．このような利用に基づき ST-ITC IPAM は ITC 内で内製するという意思決定に至った．

ST-ITC IPAM はネットワーク資源の論理側面と物理側面の両面において表現する．論理的側面には委譲先組織に割り当てられたアドレス範囲，VLAN ID，Default GW，個々のアドレスで稼働するサービス名などの情報が含まれる．物理的側面にはキャンパス内における棟番号，階数，部屋番号，ネットワークコンセント番号といった情報が含まれる．これらの情報は委譲先組織の ID を以て結合される．

4.2.4　ST-ITC Portal

ST-ITC Portal は ITC とアドレス資源の委譲先組織の間でセキュリティ脅威情報を共有するためのポータルサイトである．このポータルサイトは慶應義塾にてライセンス契約する G Suite for Education[5] に含まれる Google Classroom[6] を用いて実装された．Google Classroom ではその参加者間で教師役と生徒役のロールプレイが可能である．この教師役は生徒役に対して課題を提示して，その課題の進捗状況を管理することが出来る．また教師役からの課題の投稿毎に，教師役と生徒役の両者が参加するフォーラムを形成することが出来る．このフォーラムの中では教師役と生徒役の両者が参加する議論の展開ができる．

ST-ITC Portal ではアドレス資源の委譲先組織毎に Classroom を開設し，ITC の教職員が教師役，委譲先組織に所属するものが生徒役として参加する．教師役の ITC の教職員は，委譲されたアドレス資源に関わるインシデントやセキュリティ脆弱性イベントの発生に併せて課題を Classroom に投稿して，その対応状況の進捗を管理する．その対応の中で問題が生じた場合はフォーラム機能を用いて Classroom 内で議論を展開する．アドレス資源の委譲先組織の担当者が対応を完了した場合は，課題の完了を Classroom 内で報告する．報告を受けた ITC の教職員は適切な対応がなされていることを確認した上で課題の提出を受け入れる．

4.2.5 慶應義塾共通認証システム (keio.jp)

keio.jp[3] は慶應義塾内に設置された Shibboleth[7], [8] IdP をバックエンドに持った学内シングルサインオン (SSO) 基盤である．4.2.3 節，4.2.4 節で示した通り，ST-ITC IPAM と ST-ITC Portal は ITC の教職員に加えてアドレス資源の委譲先組織に所属するものが利用する．慶應義塾に所属する教職員及び学生は慶應 ID を用いた keio.jp 上で SSO が利用可能であるため，ST-ITC IPAM と ST-ITC Portal の両サービスの利用者の認証機構として keio.jp を用いた．

ST-ITC Portal については Google Classroom を含む G Suite for Education が既に keio.jp の SP として登録されていた．ST-ITC IPAM は内製 Rails アプリケーションのため，本研究の中で keio.jp の SP として登録した．

4.3 モジュール間連携に基づくオートメーション

図 2 には 4.2 節で示した 5 つのモジュール間の連携が示されている．アドレス資源の委譲先組織に対するインシデントやセキュリティ脆弱性等のイベント発生通知は ST-ITC Portal を介してなされる．ST-ITC Portal にイベント発生通知が到達するのはインシデント・データベースである TTDB for Keio SOC に対するチケット操作に連動する．

TTDB for Keio SOC は TWS DB と ST-ITC IPAM に対して定期的にポーリングして両者に対する更新差分を取得する．TWS DB からは ITC 保有機器からの log 情報の更新を受けて，新規のセキュリティ・イベントの発生を検知する．ST-ITC IPAM からはアドレス管理情報の更新を受けて，セキュリティ・イベントが発生した委譲先組織の特定に利用する．結果的に，TTDB for Keio SOC におけるポーリングを調整することが ITC によるオートメーションの制御に紐付く．

5. 複数組織に跨がった SOC 間連携の検証

4 節までで，大学の教育研究系ネットワークを対象にした SOC/CSIRT 活動に用いる情報基盤を提案・実装して，それに基づく SOC/CSIRT 活動について述べてきた．しかし単一組織による SOC 活動には，人的・技術的資源の両面の跨がる制約がボトルネックとなり限界がある場合がほとんどだ．組織ごとに人的・技術的資源の事情は異なるので SOC 活動に含まれる要素ごとに組織間で得手不得手があるとの前提に立ち，信頼関係の保てる組織間での SOC 活動の連携を実施することは安全な情報環境を実現する上で有意義である．

そのような問題意識のもと，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 [9] と株式会社日立製作所 [10] 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．本節ではその中で実施した複数 SOC に跨がった チケットシステム間連携の検証事例について紹介する．

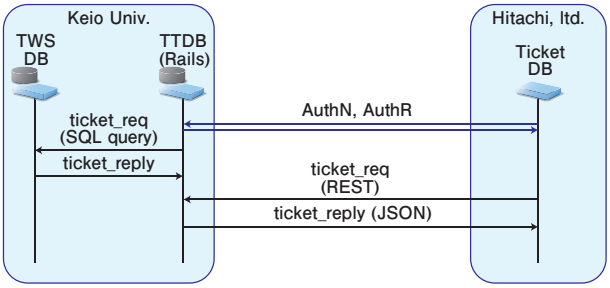

図 3 SOC 間連携事例: チケットシステム間連携

図 3 には SOC 間連携の検証のために実施したチケットシステム間連携の概要が示されている．まず両組織間に認証認可に基づいた暗号化されたセッションが開設される．その後，慶應内 TWS DB に対する SQL クエリをもとに TTDB 内にセキュリティ・イベントに関するチケットが生成される．セキュリティ・イベントの種類は TWS DB に対して発行される SQL クエリにて制御される．その後日立内のチケットシステムはあらかじめ確立していた暗号化セッションを通して TTDB が用意した REST API を通じて生成されたチケット内の情報を要求する．TTDB は要求されたチケット内の情報を JSON の形式に整形して返信する．

チケットシステム間連携のユースケースとしては検体検査の連携があげられる．例えば慶應内で見つかったマルウェアの被疑があるファイルを安全なファイルストレージに保存してその URL を TTDB に記す．日立側はチケットシステム間連携を通じて該当 URL にアクセスして自社のサンドボックス環境内でその挙動を検査する．

6. 今後の課題

6.1 セキュリティ・イベント情報の抽出方法

TWS DB に蓄積された生の log 情報からインシデントやセキュリティ脆弱性等のセキュリティ・イベント情報を抽出する方法に関してさらに検討を進める必要がある．2 において何例かの具体例を提示しているものの，生の log 情報の種別やその組み合わせ方に応じた体系化立てた手法の確立を目指すべきと言える．

6.2 SOC 間連携を前提にした情報基盤

5 節で示した SOC 間連携を前提としたで情報基盤の構築が必要である．図 2 で示した情報基盤を SOC 間連携を前提に拡張すると図 4 が得られる．このモデルでははは現在の TWS DB に保存されている L7 ファイアウォールの log 情報，フロー情報，DNS クエリ log 情報に加えて，さらに収集する情報の種類が増えていくことを前提としている．RDB に格納される情報については種類増加に容易に対応

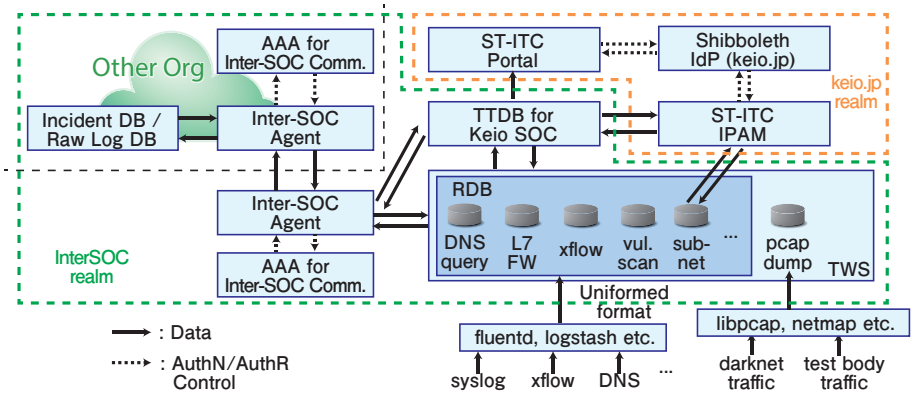

図 4　SOC 間連携を前提にした情報基盤

できるよう fluentd 等を介した共通フォーマット化を踏まえている．また RDB に格納されない pcap 形式の dump ファイルの保存も想定している．

SOC 間に跨がった連携では直接各 SOC が持つ生の log 情報やインシデント DB にはアクセスせず，Inter-SOC Agent を介した連携となる．また複数 SOC に跨がった SOC 間連携ではマルチドメイン環境の認証認可を前提とした機構 [11], [12], [13] が求められる．図 4 では学内向けの SSO サービスである keio.jp realm と SOC 間連携の為の InterSOC realm が併存する構成となっている．

7. まとめ

本研究ではネットワーク資源の運用・管理権限が下位接続組織に委譲され，passive monitoring に基づく SOC 活動を実施する教育研究系ネットワークを対象とした SOC/CSIRT 活動のための情報基盤を提案した．また本研究では多種多様な組織構造を持った本学矢上キャンパスを教育研究系ネットワークのモデルケースとして選択して本基盤を実装した．

その知見を前提に単一組織による SOC 活動の限界を取り除くために，本研究では複数組織に跨がる SOC 間連携の検証を行った．今後の課題として，生の log 情報からセキュリティ・イベントを抽出する手法の体系化と複数 SOC 間の連携を前提とした情報基盤の構築が挙げられる．

参考文献

[1] 慶應義塾 ITC. http://www.itc.keio.ac.jp/ja/top_itc.html.
[2] 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.
[3] keio.jp マニュアル. http://www.itc.keio.ac.jp/ja/keiojp_manual.html.
[4] Interop Tokyo. https://www.interop.jp/.
[5] G Suite for Education. https://edu.google.com/intl/ja/.
[6] Google Claassroom. https://edu.google.com/intl/ja/products/productivity-tools/classroom/.
[7] 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.
[8] 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.
[9] 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/endcenter/center-54.html.
[10] Hitachi Global. http://www.hitachi.com/.
[11] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn. Diameter Base Protocol. RFC 6733, *IETF*, 2012.
[12] C. Neuman and T. Ts'o. Kerberos: An Authentication Service for Computer Networks. *IEEE Communications Magazine*, Vol. 32, No. 9, pp. 33–38, 1994.
[13] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. The Kerberos Network Authentication Service (V5). RFC 4120, *IETF*, 2005.