大学における外部 SOC 有効活用の一考察

A study on Effective Utilization of External SOC at University

佐藤 由章†，辻井 高浩†，藤川 和利†
Yoshiaki Sato†, Takahiro Tsujii†, Kazutoshi Fujikawa†

yosiaki@itc.naist.jp, tsujii@itc.naist.jp, fujikawa@itc.naist.jp

†奈良先端科学技術大学院大学 総合情報基盤センター

†Nara Institute of Science and Technology Information Initiative Center

概要

昨今のサイバー犯罪の急激な増加により企業や国の機関において個人情報もしくは機密情報の漏洩という重大インシデントを防ぐことが急務となっている．奈良先端科学技術大学院大学（以下，本学）においては，情報セキュリティ対策の重要性を鑑み，CSIRT(Computer Security Incident Response Team：情報セキュリティ緊急対応チーム)を 2016 年 10 月 1 日に設置した．CSIRT の構成員は，全学の情報環境をサポートする総合情報基盤センターの運用に関わるスタッフが兼務しており，既存部署による従来のセキュリティ対応よりも厳密な対応が要求され負担増となっている．CSIRT において業務軽減のためにセキュリティに関するシステム強化を諮るも，CSIRT 構成員がシステムからの多数のアラートから対応すべき重要インシデントを抽出するスキル・経験・知識は充分ではない．一方，情報環境の高度化にともない，従来業務も増加しており，CSIRT 構成員がセキュリティ業務に専念することは難しい状況である．

本稿では，本学の従来のセキュリティ対応と CSIRT 設置後におけるシステム強化策を述べ，CSIRT スタッフのセキュリティ業務軽減と CSIRT の本来の目的であるインシデント発生時の迅速対応のために本年度より開始した本学における外部 SOC 連携の現状と効果について報告する．

キーワード

CSIRT，セキュリティ，外部 SOC

1. はじめに.

我が国の情報セキュティを取り巻く環境はサイバー犯罪の急激な増加および手口の巧妙化により，セキュリティリスクは増幅しており，企業や国の機関においても社会問題となる情報漏えい等の重大インシデントが発生している．各機関では組織内のセキュリティリスクを排除するため，情報セキュティ問題を専門に扱う CSIRT 設立の動きが活発化している [1].

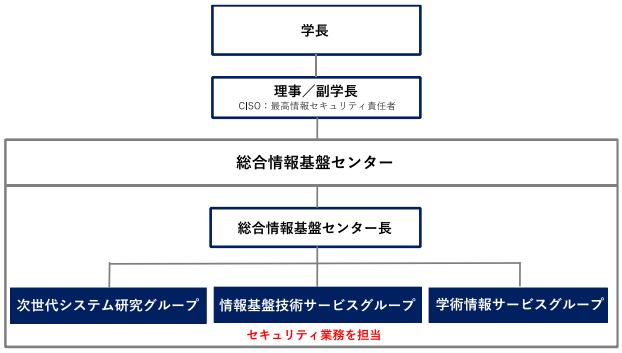
本学においても 2016 年 10 月に CSIRT を設立したが，CSIRT の構成員は，全学の情報環境をサポートする総合情報基盤センターの運用に関わるスタッフが兼務しており，既存部署による従来のセキュリティ対応よりも厳密な対応が要求され負担増となっている．CSIRT 設置後，業務軽減のためにセキュリティに関するシステム強化を実施したが，システムからの多数のアラートから対応すべき重要インシデントを抽出することが必要不可欠となっている．一方，情報環境の高度化にともない，従来業務も増加しており，CSIRT 構成員がセキュリティ関連業務に専念することは難しい状況である．

本稿では，本学の従来のセキュリティ対応と CSIRT 設置後におけるシステム強化策を述べ，CSIRT スタッフのセキュリティ業務軽減および CSIRT の本来の目的であるインシデント発生時の迅速対応のために本年度より開始した本学における外部 SOC 連携の現状と効果について報告する．

2. 平成２９年度までのセキュリティ対策

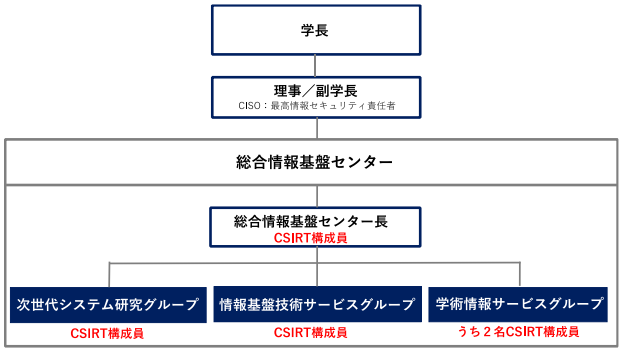
2.1. 組織

2016 年 9 月まで，本学におけるセキュリティ業務は図−1 で示すように総合情報基盤センターが実施しており，総合情報基盤センターの情報基盤技術サービスグループのスタッフ 7 名で通常業務の一部として対応していた.



図−1　2016 年 9 月までの組織図

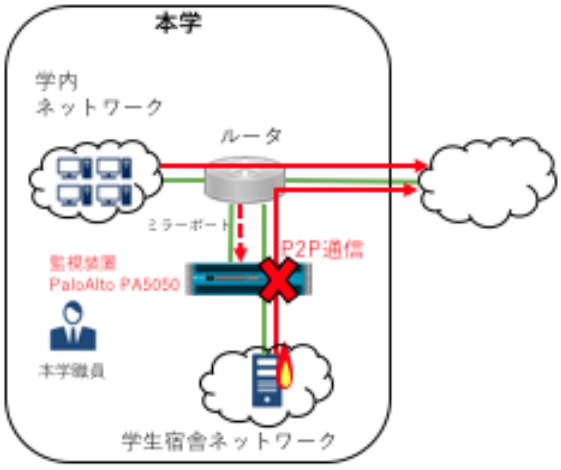
2016 年 10 月以降，CSIRT がセキュリティ業務を担当することになった． CSIRT の構成員は，図−２で示すように総合情報基盤センターの情報基盤技術サービスグループのスタッフ７名に総合情報基盤センター長，次世代システム研究グループのスタッフ５名，学術情報サービスグループのスタッフ２名が加わり１５名体制に増員されたが全員が兼務している状況である.



図−２　2016 年 10 月以降の組織図

2.2. システム構成

本学における平成２９年度までのセキュリティ対策のシステム構成を図−３に示す.



図−３　システム構成図

セキュリティ監視装置としては Palo Alto 社製 PA5050（以下，装置 A）を使用していた．装置 A は，マルウェアや不正アクセスにおける攻撃の特徴的なパターンであるシグネチャ [2]ベースでのアラート検知機能を持っており，シグネチャに一致する通信を検知すると，アラートが検出される仕組みとなっている．装置 A においては最新のウイルスや攻撃に対してシグネチャの更新が遅れる場合がありゼロデイ攻撃 [3]に対しては対応できない.

本学では装置 A を学内ネットワークにおけるインターネット境界ルータのミラーリングポートに接続し，学内

から学外への通信モニタリング用として活用していた.

学生宿舎ネットワークにおいては装置Aをファイアウォールとして活用しており，学生宿舎ネットワークセグメントからの通信においては，装置 A を経由するシステム構成により学生宿舎からの P2P 通信については自動通信断を実施していた.

2.3. 運用体制

セキュリティ関連の利用者からの報告，CSIRT 構成員の通常業務内で検知できる異常および外部セキュリティ機関からの連絡等により装置 A のログを確認し，インシデントに該当すると判断された場合は必要な対応を実施していた. 通常時は，装置 A のアラート数が膨大なため全てアラートへの対応が不可能であり，学生宿舎ネットワークについては装置Aによる自動通信断設定に依存していたため，装置 A のログをインシデント発生後の調査のみに活用していた.

2.4. 問題点

2.4.1. インシデント検知

インシデント検知における問題点を以下に示す.

- 装置 A の膨大なアラート件数
  装置 A のアラート件数が膨大であり，全てのアラートに関して対応することは不可能であった.
- 標的型攻撃・ゼロデイ攻撃への対応
  装置 A はシグネチャベースのアラート検知機能によりインシデント検出を行なっているため，特定の企業や団体を狙った攻撃および未知の攻撃についてはシグネチャが存在しないため対応することができない.

2.4.2. 人的リソース

人的リソースに関する問題点を以下に示す.

- スキル・経験・知識
  セキュリティシステムを有効に活用するためには担当者のスキル・経験・知識が必要である.
- 業務量の増加
  本学情報セキュリティ緊急対応チーム (NAIST CSIRT) は，既存の総合情報基盤センターのスタッフが兼務している．既存部署による従来のセキュリティ対応よりも厳密な対応が要求され負担増となっている．一方，情報環境の高度化にともない，従来業務も増加している.

3. 解決方針

2.4 節で述べた平成２９年度までのセキュリティ対策に関する問題点を解決するために以下の方針を立てた.

3.1. 監視装置の更新

平成 29 年度まで設置してきた装置 A を 2018 年 3 月 1 日に後継機種に置き換えるとともに，新たなセキュリティ監視装置を設置することにより従来未対応となっていた標的型攻撃･ゼロディ攻撃への対応を図ることとした. 更新機器を以下に示す.

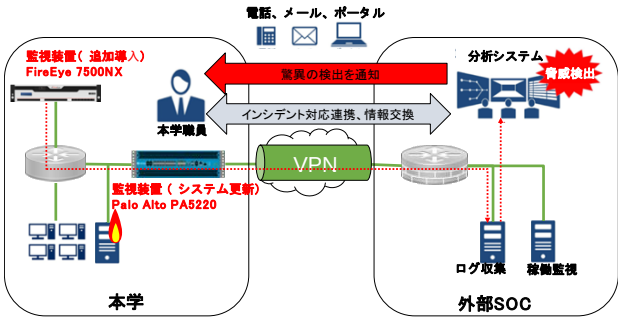
- Palo Alto 社製 PA5220（以下，装置 B）
  マルウェアや不正アクセスにおける攻撃の特徴的なパターンであるシグネチャベースでのアラート検知機能を持っており，シグネチャに一致する通信を検知すると，アラートが検出される仕組みとなっている. 装置 B においては最新のウイルスや攻撃に対してシグネチャの更新が遅れる場合がありゼロデイ攻撃に対しては対応できない. 既存の装置 A よりもスループット機能が向上している.
- FireEye 社製 7500NX（以下，装置 C）
  シグネチャに依存しないセキュリティ監視装置であり，外部から受け取った通信やプログラムを装置内の保護された仮想領域であるサンドボックスで解析することによって，標的型攻撃となる悪意のある通信であるかどうかを判断する仕組みとなっている. シグネチャを持っていないため既知の脅威には対応できない場合がある.

3.2. 外部 SOC サービスとの連携

本学では，平成 30 年 5 月 1 日よりセキュリティ機器のアラート分析を外部 SOC(Security Operation Center)である株式会社インフォセックに委託し，各機器の膨大なアラートのうち外部 SOC が抽出したアラートを CSIRT 構成員がインシデントとして対応している.

3.2.1. システム構成

外部 SOC との連携サービスにおけるシステム構成図を図−４に示す.



図−４　外部 SOC との連携サービス

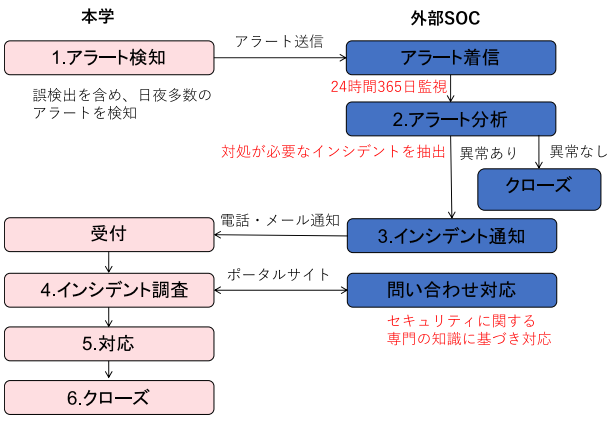
本学設置の装置 B および装置 C のアラートは，本学と外部 SOC 間で接続された VPN を経由して外部 SOC に送信される．外部 SOC は受けとったアラートを表−１に示すようにレベル１からレベル４までの４段階の重大度に分類し，重大度に応じた連絡手段（電話，メールまたはポータルサイト）により本学に通知する．

重大度	通信内容	連絡手段
レベル１	アドレススキャン・ポートスキャン等の調査通信	ポータルサイト
レベル２	攻撃行為であるが失敗が確認された通信	ポータルサイト
レベル３	攻撃がおこなわれているが成否が確認できない通信	電話・メール・ポータルサイト
レベル４	攻撃の成功が確認された場合などの通信	電話・メール・ポータルサイト

表−１インシデントのレベル

3.2.2. 運用体制

外部 SOC 連携サービスの流れを図−５に示す．



図−５外部 SOC 連携サービスの流れ

外部 SOC が本学専用のポータルサイトを用意しており，すべてのアラートの分析結果はこちらに登録される．

外部 SOC がレベル２以下と分析したアラートについては対応が終了した状況であるクローズとして登録されるので，本学の CSIRT 構成員は対応が不要となる．

レベル３以上と分析したアラートについては，外部 SOC が分析結果をポータルサイトに情報を登録した後，本学にメールによる通知をするとともにリスト（経験値の高い者を上位）に従い CSIRT 構成員の個人所有携帯電話にも連絡する．外部 SOC の対応は２４時間３６５日であるため，業務時間内であれば当日の担当者が，リーダーとなり対応を実施し，業務時間外であれば電話連絡を受けた者がリーダーとなり対応をするが，緊急度によっては全員参集の場合もある．

本学 CSIRT 構成員は外部 SOC が用意した本学専用のポータルサイトのインシデントを確認することができる．ポータルサイトの確認は当番制としており業務負荷の平準化を図っている．外部 SOC が登録したインシデントを適切な検索条件により一覧表示することができる．各インシデントの記載内容は以下のとおりである．

- 発生日時
- イベントの概要
- 詳細情報
  通信元，通信先 (IP アドレス，ポート番号，URL)
- 分析結果

CSIRT 構成員はポータルサイト記載の内容，各監視機器のログを確認し，インシデントを発生させた該当者へ事実確認および対応依頼を行う．対応依頼は基本的にメールで実施するが，緊急度が高い場合は，インシデントを発生させた該当者本人が所属する部署に直接訪問して確認する．確認後，CSIRT 構成員は対応内容や質問をポータルサイトの各インシデントのコメント欄に登録し外部 SOC と CSIRT 構成員との間で情報共有している．

重大インシデントの可能性がある場合は，速やかに CISO への連絡・相談を行うとともに外部機関への連絡および組織内への通知を実施している

外部 SOC との連携サービス開始後は各 CSIRT 構成員の対応内容の妥当性を確認するため毎日打ち合わせを実施し，各インシデントの対応状況をクローズにする際には，CSIRT 構成員の合意により決定している．

4. 結果と考察

4.1. 外部 SOC サービス導入後の状況

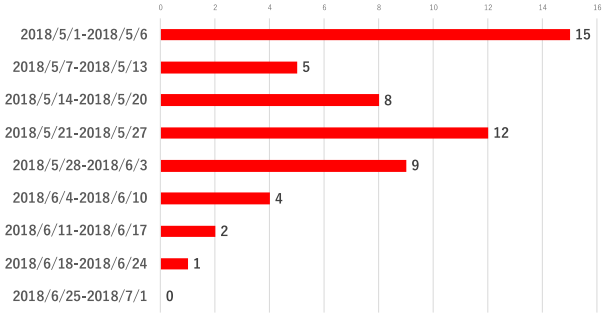
4.1.1. 具体例

外部 SOC との連携サービス導入後，外部 SOC と連携したインシデント対応の具体例を紹介する．

- 装置 B でのみ検出された事例
  学外から脆弱性のある Apache を使用していた本学サーバに対するディレクトリトラバーサル攻撃で手法も一般的であったが，装置 C では検出できなかった．脆弱性をつく不正アクセス通信が試みられ，攻撃に成功していることが検出されたが，装置 B のログには HTTP メッセージの内容も全て記録されているため，不正アクセスの内容を詳細に調査することにより，サーバの設定ファイルにはアクセスされたものの，研究データや個人情報の漏洩はなかったことを確認できた．
- 当初は装置 C でのみ検出されたが，その後の調査では装置 B も併用した事例
  学生が学内ネットワークで利用中の PC でマルウェアをダウンロードしており，ダウンロードファイルが ZIP 形式で圧縮されていたため装置 B のシグネチャでは検出されなかったが，装置 C のサンドボックス解析で検出できた．当該マルウェアを実行するとさらに別のマルウェアをダウンロードすること，およびダウンロードサイトへの通信先を装置 C で自動解析できた．装置 C の解析結果に基づいてさらに 装置 B のログを調査したところ，マルウェアの実行には至っていなかったことを確認できた．
- 装置 C でのみ検出された事例
  装置 C に置いて学生が利用中の PC から仮想通貨のマイニングを行うマルウェアのコールバック通信が検出された．装置 B ではシグネチャにコールバック通信先が C&C サーバ [4] として登録されていなかったため検出されなかった．利用者へ連絡し，セキュリティツールによるマルウェア駆除を試すよう指示したところ，実際にマルウェアが検出・駆除され，駆除後はコールバックが停止することを確認できた．

4.1.2. 統計情報

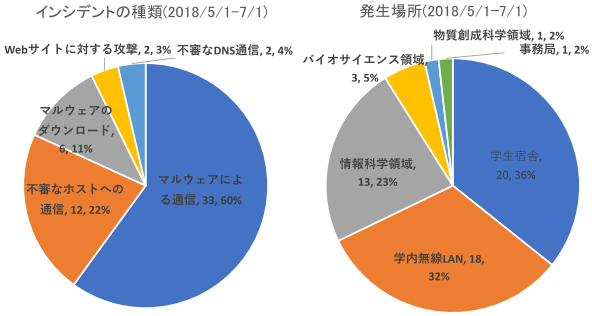
図−６にサービス開始時からのインシデント件数を示す．



図−６インシデント件数(2018/5/1-2018/7/1)

サービス開始時はインシデント検知数が多かったが，外部 SOC が抽出したインシデントのみに専念することで確実にインシデントをクローズの状況にすることにより件数を減少させることができた．レベル３以上のアラートへの適切な対応により，重大インシデントを未然に防いでいると推測している．

また図−７にインシデントの種類と発生場所を示す



図−７インシデントの種類と発生場所

インシデントの種類はマルウェア感染に関する通信だけでインシデント発生件数全体の７０％を占めている．学生宿舎，学内無線 LAN 接続端末だけでインシデント発生件数全体の７０％を占めている．

4.2. 考察

4.2.1. インシデント検知

本学のセキュリティ監視装置に 装置 C を追加し，装置 B と併用する事で以下のことが実現できたと考える．

- インシデント検知能力の向上
  装置 B のシグネチャベースによるアラート検知機能，ログ収集，解析機能にあわせて 装置 C のサンドボックスによる通信解析が補完されることによりインシデント検知能力が向上した．
- 追跡調査機能の向上
  装置 B と装置 C のログを合わせて調査することによりインシデント追跡機能が向上した．

外部 SOC によるログ解析により以下のことが実現できたと考える．

- 対応すべきインシデントの明確化
  外部 SOC がログ解析することにより，対応すべきインシデントが明確化され，本学担当者は必要な対応に専念できるようになった．
- 確実な対応

外部 SOC によるログ解析開始までは，監視装置の不定期なモニタリングの実施もあって２年（２０１６／４／１ー２０１８／４／３０）で１８件の対応件数であったが，ログ解析開始後は２ヶ月（２０１８／５／１ー７／１）では５７件となり対応件数が大幅に増加し，確実な対応が実施できていると考えている．

確実なインシデント対応により重大なインシデントに進展する前段階で予防できていると考える．

4.2.2. 人的リソース

外部 SOC 連携によるインシデント対応により，確実なセキュリティ対応をとれるようになり，効率的な業務を遂行していると考えている．しかしながら，重大インシデントに繋がる事案が発生すると，セキュリティ関連以外の既存業務に支障をきたすことは予測できており，専任の職員が必要であると考える．

4.2.3. 今後の課題

3 節で述べた対策により，本学におけるインシデントの対応についての問題点が改善されたが，引き続き以下の課題が残っている．

- 業務時間外におけるインシデント対応
  現在は業務時間外の連絡手段として個人の携帯電話を利用しており，電話代も個人負担となっている．CSIRT 構成員に対して別途携帯電話もしくはタブレットの支給を行う対応の検討が必要と考えている．
- BYOD 端末の取扱
  学内無線 LAN 接続端末は，学内ネットワークであるため，個人の所有端末（BYOD）を含む全ての接続端末において初期化を含めた厳格な対応をしている．しかしながら個人の所有端末に対してそこまで強制力を持って対応すべきか，検討する必要があると考える．
- CSIRT 構成員のさらなるスキル向上
  CISRT 構成員のさらなるスキルの向上は必要であり，外部 SOC との意見交換会や他組織との勉強会を定期的に開催する予定である．
- インシデント履歴の参照
  ポータルサイトではクローズ（対応済）となったインシデントが検索しづらいといった課題がある．このため過去の対応済インシデント履歴を用意に閲覧するためのシステム構築を検討している．
- SIEM [5]の活用
  現在，標的型メールに関するインシデント発生時の追跡調査において複数のシステムログを調査する必要があり，かなりのコストを要している．メール，DNS および認証に関するログを収集する SIEM を導入し標的型メールに関するインシデント発生後の追跡を容易することを検討している．

5. まとめ

監視装置の追加，外部 SOC サービスとの連携を実施することで的確なインシデント対応ができるようになり，重大インシデントの予防にも繋がっている．CSIRT 構成員の監視装置の操作スキルの向上といった二次的な効果も得られた．CSIRT 構成員のさらなるスキル向上は必要と考えており，外部組織との意見交換会もしくは勉強会を定期的に実施していく予定である．

現時点においてはインシデント履歴の参照や，メールインシデント発生時の追跡調査に課題があるため SIEM の活用および新たなシステム構築の実施により，本学におけるセキュリティのさらなる向上を検討していく予定である．

参考文献

[1] 情報処理推進機構，「情報セキュリティ 10 大脅威 2018」，https://www.ipa.go.jp/security/vuln/10threats2018.html

[2] 情報処理推進機構，「侵入検知・予防システム」，https://www.ipa.go.jp/security/fy18/reports/contents/remote/Chapter7/8.htm

[3] 情報処理推進機構，「修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について」，https://www.ipa.go.jp/security/virus/zda.html

[4] トレンドマイクロ，「C&C サーバ」，https://www.trendmicro.com/vinfo/jp/security/definition/command-and-control-c-c-server

[5] キヤノン IT ソリューションズ，「SIEM（Security Information and Event Management）」，https://eset-info.canon-its.jp/malware_info/term/detail/00036.html