京都大学における情報セキュリティ対応の体制と IDS の活用

斎藤 紀恵　尾形 幸亮　片桐 統　石橋 由子

京都大学 企画・情報部 情報基盤課
i-s-office@iimc.kyoto-u.ac.jp

1　はじめに

京都大学では，約 3 万名の構成員が在籍し，学内ネットワークにはサーバ等のグローバル IP アドレスの機器が約 2,400 台，研究室，事務室などの単位で構築している VLAN が約 4,000 個接続されている．

多数の機器を情報セキュリティに関する脅威から守るため IDS（侵入検知装置）を設置しネットワークの監視を行うとともに，情報セキュリティに関する事案に対応する体制を構築している．

本稿では，京都大学における IDS の活用方法と，IDS やその他の情報により入手したインシデントへの対応体制について，事例を交えて紹介する．

2　セキュリティ対応の体制

本学の情報セキュリティ対応の体制を図 1 に示す．最高情報セキュリティ責任者（情報担当理事）のもと，全学の情報セキュリティ確保に必要な事項の検討を行う全学情報セキュリティ委員会（委員：全部局の 部局情報セキュリティ責任者）が設置されている．また，情報ネットワークに関わる危機管理を行うため，最高情報セキュリティ責任者の下に情報ネットワーク危機管理委員会（以下，「危機管理委員会」という．）が設置されている．危機管理委員会や各部局との連絡窓口は，企画・情報部 情報基盤課 セキュリティ対策掛が担当している．さらに，情報ネットワークにおける人権侵害，著作権侵害等に該当するおそれのある情報の発信防止等に関する事項に対応する情報ネットワーク倫理委員会が設置されている．

なお，全学情報セキュリティ技術連絡会（以下，「技術連絡会」という．）は，情報セキュリティに関する全学及び部局間の技術的な連絡調整を行うために 2015 年度より新たに設置されたものである．

各部局においても，部局情報セキュリティ責任者（部局の長）のもと，部局における情報セキュリティに関する事項を扱う部局情報セキュリティ委員会が設置されているなど必要な体制が構築されている．

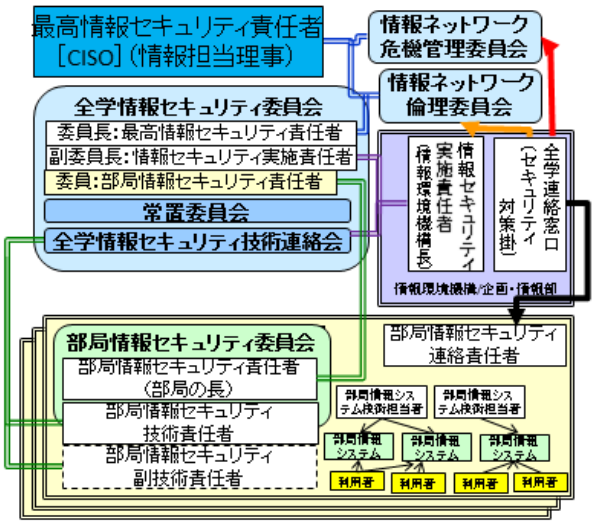

図 1 情報セキュリティ対応の体制

本学情報システムへの不正侵入（データ破壊，ホームページ改ざん，メール不正中継（迷惑メール）等）やマルウェア，その他によって被害が発生した場合（被害の恐れがある場合も含む）の連絡網を図 2 に示す．発見者から連絡があった場合，危機管理委員会が中心となって対応に当たる体制になっており，CSIRT の機能を果たしている．

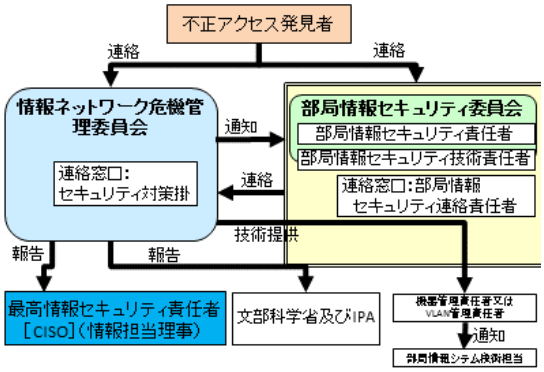

図 2 不正アクセスなどの連絡網

3　IDS の構成

本学の IDS の構成を図 3 に示す．IDS は，対外接続ルータの通信をミラーリングして分析し，攻撃等のパターンにマッチするパケットをアラートとして検知している．

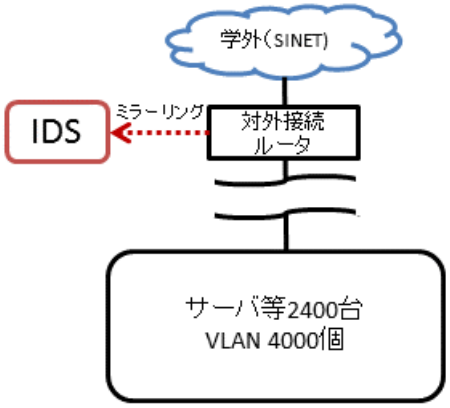

図 3 IDS の配置

4　IDS の監視委託と定期的な確認

IDS で検知したアラートは，1 日あたり 10 万件程度あり，全てを職員が確認することは不可能である．そこで，2010 年度より，24 時間 365 日の体制で，所定の条件に合致するアラートを本学の担当者にメールで通知するよう監視業務を外部委託している．通知対象となるのは，所定の日数内で初めて検知したアラート，検知件数が急増したもの，学外への加害が疑われる通信を行ったもの等となっている．委託業者からのメール通知は 1 日あたり 3 通程度となっている．また，本学の利用規則で禁止している P2P ファイル転送の疑いがあるものについても，1 日分の状況をまとめて通知されるようになっている．委託業者からのメール通知は，原則として職員が勤務時間内に確認し必要な処置を行っている．

また，委託業者からのメール通知対象とならないアラートについても対応が必要なものがないかについて，職員が可能な範囲で状況を確認しており，処置が必要なものがあった場合は対応を行っている．

5　IDS のアラート等への対応

IDS で検知したアラートについて確認等が必要な場合や，外部機関等からセキュリティ事案に関する連絡があった場合，内容に応じて図 4 の対応を行っている．

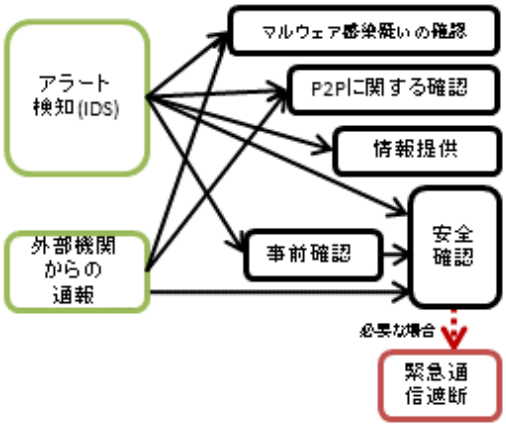

図 4　アラート等への対応

最近 3 年間の分類ごとの対応件数（2015 年 10 月 13 日時点）を表 1 に示す．2014 年度は，OpenSSL の脆弱性（Heartbleed）や Bash の脆弱性（ShellShock）の影響で，「情報提供」，「事前確認」，「安全確認」の件数が多くなっている．5.1 章以降で，それぞれの分類の概要を説明する．

表 1 アラート等への対応状況

分類	2013 年度	2014 年度	2015 年度
マルウェア感染疑いの確認	72	167	60
P2P に関する確認	31	38	6
情報提供	0	622	0
事前確認	19	97	21
安全確認	63	104	16
緊急通信遮断の件数	11	5	2

5.1 マルウェア感染疑いの確認

本学の PC 端末等がマルウェアに感染した疑いのある通信を IDS が検知した場合，プロキシサーバ等のログから当該機器が接続されている VLAN 等の情報を特定し，部局に対してセキュリティソフトを使用した完全スキャンの実施を依頼している．

完全スキャンを実施した結果，マルウェアの感染が確認された場合は，必要な措置を行った上で，当該部局のセキュリティ委員会より危機管理委員会宛てに報告するよう依頼を行っている．

5.2 P2P に関する確認

本学の規則において，ファイル公衆送信機能を有する P2P ソフトウェアの使用は禁止されている．禁止ソフトウェアの使用の疑いのある通信を IDS で検知した場合，マルウェア感染の場合と同様に部局に対して状況の確認を依頼している．P2P に関する確認を行う機器のほとんどは学生が使用しているものである．

5.3 情報提供

学内の機器に網羅的な攻撃を検知した場合等，大量の機器に関して対応が必要な場合は，確認結果の回答を求めない「情報提供」を行う．最近では，2014 年 9 月に発覚した ShellShock に関して，約 600 台の機器の管理者に対して「情報提供」行った．

また，IDS で検知した攻撃に関する状況確認を行った際に，当該攻撃には直接関係のない問題（最新のセキュリティパッチが適用できていない可能性等）を発見した場合にも「情報提供」を行っている．

5.4 事前確認

アプリケーションの特定のバージョンを狙った攻撃などを検知した場合で，当該バージョン等を使用しているか判断できない場合には，機器管理責任者に対して「事前確認」を行い確認結果の回答を依頼している．確認の結果，狙われた脆弱性を含むバージョンを使用していることが判明した場合は「安全確認」にエスカレーションする．

また，特定の機器に対して，成功の可能性が低いと思われる攻撃を多数検知した場合等，念のため確認しておく必要があると判断される内容についても，この「事前確認」を行っている．

5.5 安全確認

IDS で検知したアラートのうち，攻撃の影響を受ける可能性が考えられる場合や，外部機関からの通報で確認が必要と判断される内容の場合，当該機器を管理する部局に対して正式な「安全確認」を行い，当該部局のセキュリティ委員会より危機管理委員会宛てに報告するよう依頼を行っている．

5.6 緊急通信遮断

安全確認を行った機器は，危機管理委員会で状況等の確認を行う．被害の拡大のため必要と判断される場合は，当該機器の学外通信を対外接続ルータ緊急遮断する対応を行っている．

緊急遮断の解除は，必要な対応の実施後，部局から危機管理委員会宛てに提出される対応の報告書の内容等を確認し，問題ないと判断される場合に実施する．

6 発生したインシデントの事例

6.1 不正ファイルのアップロード検知

2015 年 5 月に，本学で管理する 1 台の Web サーバに対して，不正なファイルのアップロードを試みる通信があった旨のアラートを IDS で検知した．試みが成功したかどうか，機器管理者に対して，念のため「事前確認」を行いログ等の確認

を依頼した.

確認の結果，アップロードが成功しているログが確認されたとの第一報があったため，「安全確認」を部局に対して行った．危機管理委員会での審議の結果，当該機器の措置が完了するまでの間，通信を遮断することとなった．最終的には，機器管理部局による調査の結果，アカウント盗用により不正なアップロードは成功したものの，実質的な被害はないことが確認された.

この事例は，実質的な被害はなかった（通信遮断に伴って Web ページが参照できなかった点は除く）が，アカウントが盗用された状態を放置していれば，他の攻撃に悪用される等の可能性もあり，IDS を活用することで問題を発見し対応することができたといえる.

6.2 マルウェア感染疑いの早期対応

IDS でマルウェア感染疑いのある通信を検知した場合，内容を確認し必要と判断した場合は速やかに部局に対応を依頼している.

本学のネットワークには多数の機器が接続されており，外部機関（JPCERT 等）からマルウェア感染に起因する疑いのある通信について連絡がある事例もある．そのような事例についても，通報以前に IDS で検知したアラートをもとに VLAN 等を確認し，部局に対応を依頼済である場合が多くを占めている.

7 おわりに

京都大学における情報セキュリティ対応の体制と IDS の活用について事例を交えて紹介した.

体制については，継続的に見直しを行っており，2015 年度は技術連絡会の新たな設置等を行った．今後の見直しの候補としては，構築から年数が経過している危機管理委員会を中心とした CSIRT 機能について，より効果のある対応ができるよう機能の整理・分類等の実施を検討している.

また，IDS については，現在は，監視業務を委託することで，限られた人員でもアラートを確認可能な体制を構築している．今後は，Web 閲覧時等の暗号化や，BYOD（Bring your own device）の推進に伴う学内ネットワーク接続機器の多様化等がさらに進むことが考えられる．セキュリティ上の効果を十分に得られる IDS の活用方法について，継続して検討し必要に応じて見直しを行っていきたい.