◇◇◇◇◇◇
特 集 2
◇◇◇◇◇◇

九州工業大学における
情報セキュリティ対策の取り組みについて

中村 豊[1]
佐藤 彰洋[2]
福田 豊[3]
和田 数字郎[4]

1 はじめに

九州工業大学では 2006 年 4 月に P2P アプリケーションを用いた著作権違反や不正なソフトウェアダウンロードに起因する情報セキュリティ・インシデントの全学的な対応を目的として，全学情報基盤室が設置されました．また現場での対策組織とは別に，国立情報学研究所が公開している高等教育機関の情報セキュリティ対策のためのサンプル規定集を元に，本学情報セキュリティポリシー作成 WG によるインシデント対策フローの整備を行いました．2013 年には，戸畑，飯塚，若松各キャンパス毎に行われていたネットワーク整備，管理業務を一体的運用に変更し，また情報セキュリティ対策強化を目的として全学情報基盤室を発展的に改組し，情報基盤機構情報基盤運用室を設置しました．情報基盤運用室の主業務は以下の通りです．

1. 学外ネットワークへの接続及び学内情報ネットワーク並びにそれらを構成する機器等の運用管理に関すること．
2. 学内情報ネットワークに係る資源割当及びサブネットワークの申請等に関すること．
3. 学内サブネットワークの技術支援に関すること．
4. 情報セキュリティの確保及び情報セキュリティ・インシデント対応に関すること．
5. 情報セキュリティ・インシデントの発生時に初動対応として行う学内情報ネットワーク接続からの強制的な遮断に関すること．
6. 情報機器のデジタル・フォレンジック（物理的なアクセス，持ち帰り，証拠保全，調査及び個人情報を含むログの解析等）の運用管理に関すること．

この様な業務内容を円滑に遂行していくために，第 2 章で情報基盤運用室が実際に行っている機器の整備や規則の整備について説明します．

[1]情報科学センター　准教授　yutaka-n@isc.kyutech.ac.jp
[2]情報科学センター　助教　satoh@isc.kyutech.ac.jp
[3]情報科学センター　助教　fukuda@isc.kyutech.ac.jp
[4]情報科学センター　技術職員　swada@isc.kyutech.ac.jp

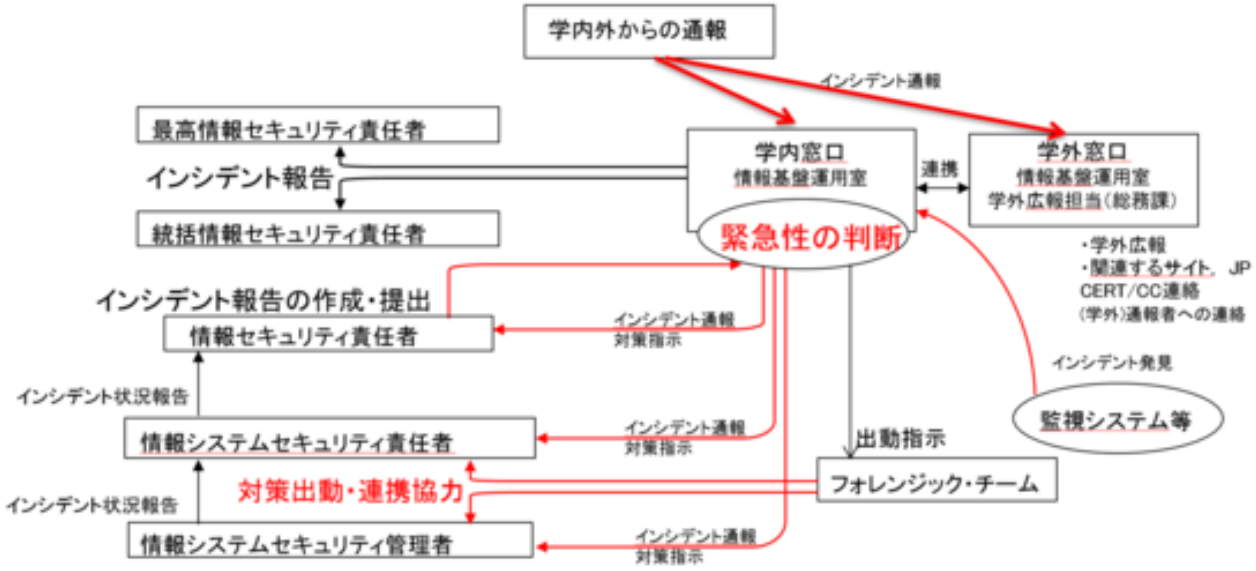


図 1: 情報セキュリティインシデントフロー

2 対策リスト

2.1 組織

組織としては，2013 年から情報基盤運用室が全学ネットワークの管理・運営・情報セキュリティ対策を担う形として整備されました．情報基盤機構内に，情報科学センター，情報基盤企画室，情報基盤運用室が置かれ，それぞれの業務範囲が定義されました．2016 年に文部科学省から通知された「国立大学法人等における情報セキュリティ強化について」に基づいて，九州工業大学では情報基盤運用室員を中心とした,「フォレンジック・チーム」を新たに設置しました．フォレンジック・チームはインシデント発生時の初動対応を専門に扱うチームとしてデジタル・フォレンジックの権限を CIO/CISO より直接移譲を受けます．また，チームメンバーの訓練を定期的に実施する必要があるので，訓練のための予算措置を要求しています．自組織内だけでのインシデント対応では，最新の攻撃情報や脆弱性情報などの取得が困難であることから，日本シーサート協議会 [1] への参加について準備を進めています．

図 1 に実際にインシデントが発生した際のフロー図を示します．本学情報セキュリティポリシー作成 WG によるインシデント対策フローから実際に稼働しているフローを抽出しています．組織の整備だけではなく，インシデント発生時の業務フローを明確化するために対応フローが整備されました．外部からの通報は情報基盤運用室もしくは総務課広報担当によって受理され，当該部局への連絡および初動対応は情報基盤運用室が担う体制となっています．フォレンジック・チームは情報基盤運用室からの指示を受けて，インシデントが発生した当該端末を当該部局の管理者と共に調査します．

2.2 基幹ネットワーク

基幹ネットワークとしては，全学セキュア・ネットワーク [2] として，2014 年 9 月からサービスを開始しています．情報セキュリティ対策の主な装置としては，境界ファイアーウォール, 各キャンパスファイアーウォールです．また，全学で利用可能な無線 LAN 環境 [3],[4] も整備しており，本学統合 ID (九工大 ID) を用いて IEEE 802.1X 認証を経由して利用可能です．

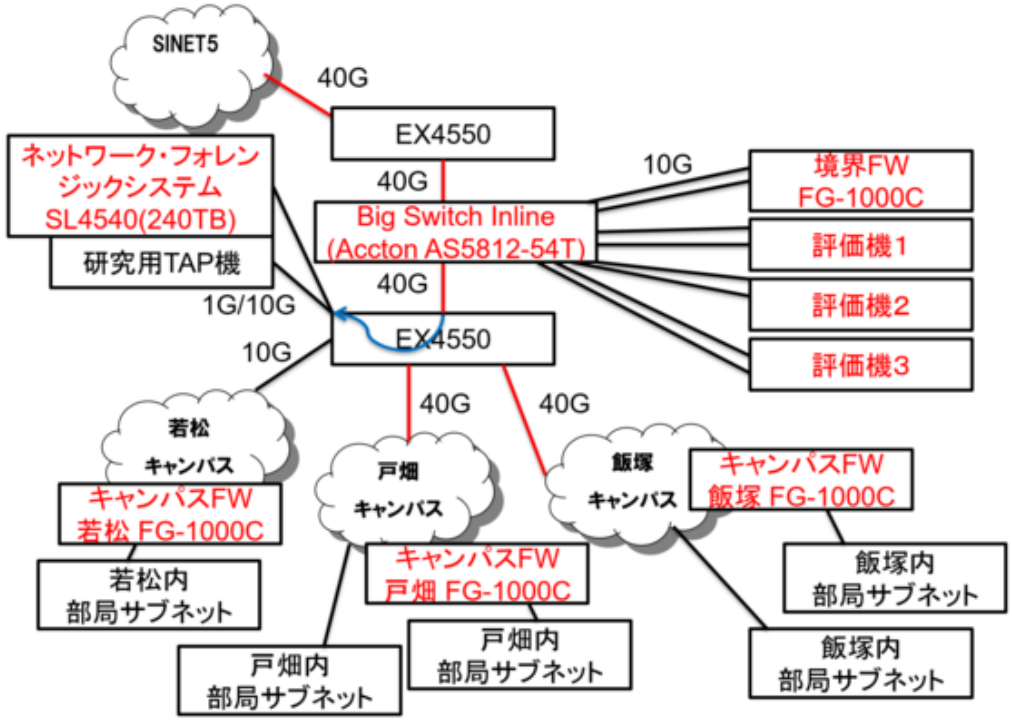


図 2: 九工大ネットワーク概要図

無線 LAN 接続後，無線 LAN のコントローラで端末間や一部の学内サービスを除き外部からの通信は廃棄しています．また，インシデント発生時はコントローラのログ (2.8.1 節で詳述) からユーザ ID 及び使用場所，使用端末を特定し，重要度に応じて一時的な無線 LAN 接続禁止等の措置を行っています．その他，アプリケーションコントロールやフィルタリングは 2.3.2, 2.3.3 節で述べる枠組みを適用しています．

図 2 に九工大ネットワーク概要図を示します．境界ファイアーウォール，キャンパスファイアーウォール，ネットワーク・フォレンジックシステムなどが図 2 に示される様な形で接続されています．具体的な内容はそれぞれの項目で詳述します．

全学ネットワークの管理では，zabbix[5] を用いた死活監視を運用しており，ネットワーク機器に障害が発生した場合は，メールにて運用室構成員に通知されます．また，一部のフロアスイッチにはループ検知の設定を投入しています．フロアスイッチには Juniper 社の EX2200 を導入しており，BPDU を検出すると自動的にポートを閉塞する設定を投入しています．EX2200 では BPDU を検知するとトラップを通知する設定も投入しており，管理アプライアンスである JunosSpace がトラップを受け取り，運用室員にメールを通知するフローを構築しました．例年，年度の切り替わりのタイミングで研究室内のレイアウト変更に伴うケーブル配線ミスによるループが頻発したことから，これらの設定を投入することになりました．

2.3 境界ファイアーウォール

境界ファイアーウォールでは，様々なセキュリティ対策を実施するために，以下の各小節で述べている機能を有効にしています．境界ファイアーウォールとして Fortigate 社 FG-1000C が導入されています．FG-1000C ではダッシュボード上に Fortiview と呼ばれる統計情報を表示する機能が装備されています．しかし，本学の環境で運用を続けていくうちに Fortiview の表示に問題が発生したため，2017 年

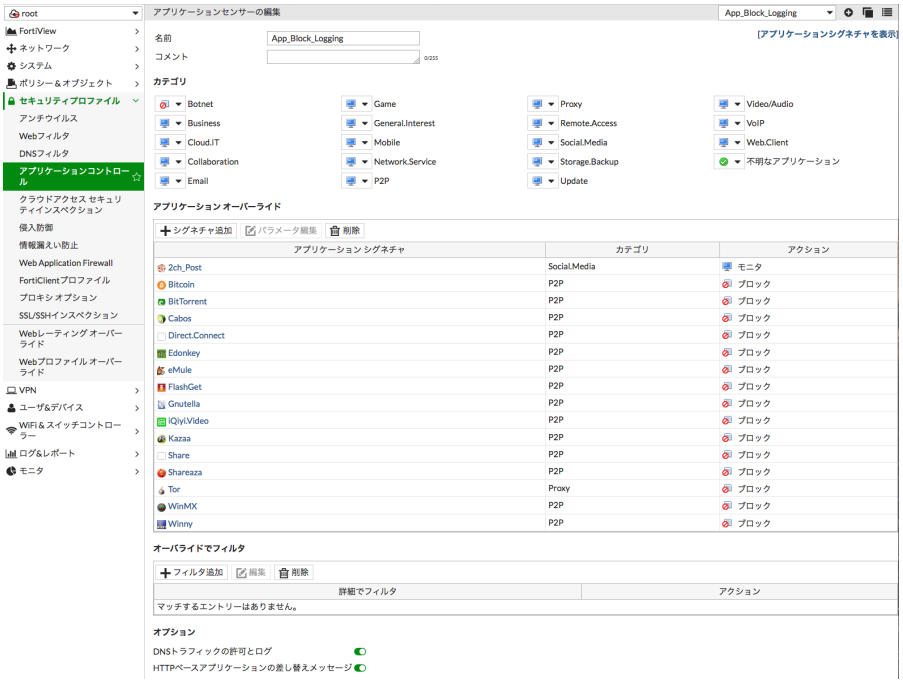


図 3: アプリケーションコントロールプロファイル例

3 月に FortiAnalyzer-1000E を導入し，Fortigate のログを転送する設定を投入しました．これによりログ解析とファイアーウォール運用を分離することが可能となりました．

FortiAnalyzer では，以下の各小節で述べている機能に関するログを蓄積，検索が可能です．インシデントが発生した際には，FortiAnalyzer を用いて，アプリケーションの通信ログ，Web Filtering における通信ログ，メール受信の内容等の確認を行います．

2.3.1 学外公開 IP アドレスの制御

九州工業大学では，2017 年 9 月 1 日現在で，3873 個の学外公開 IP アドレスが設定されています．これらは Web システムにより申請されたものに対して，後述する脆弱性診断を実施し，申請された IP アドレスに対して全てのポートを解放する仕組みとなっています．

今年度中には，セキュリティ強化の一環として，公開 IP アドレスに対して解放ポートも制御する様に仕様変更を行う予定です．

2.3.2 アプリケーションコントロール

アプリケーションコントロールでは主に学内から学外への通信で，大学の規則に違反している通信をブロックするポリシーを適用しています．アプリケーションコントロールは全学セキュア・ネットワークシステム導入当初から設定を投入しています．これは，それまで規則として禁止していた P2P 通信を遮断することを目的としていたからです．

実際の設定ではプロファイルのカテゴリとして，セキュリティ対策として「Botnet」に含まれる通信をブロックしています．また，P2P アプリケーションの一部をブロックする設定を入れています．ブロック以外にも，全てのカテゴリのモニタリングを実施しているため，全学的なアプリケーションの利用傾向の把握にも役立っています．図 3 にアプリケーションコントロール設定プロファイル例を示します．

図 4: Web Filtering プロファイル例

2.3.3 Web Filtering

Web Filtering は 2016 年 8 月 1 日よりポリシー適用を開始しました．2016 年 6 月より試験運用を開始し，学内からの Web 通信（このタイミングでは宛先ポート 80 番のみ）に Web Filtering のモニタリングポリシーを適用し，通信状態の観測を行いました．その結果，カテゴリとして，「Malicous site」，「Porno」など，教育，研究に不必要かつ，マルウェアのダウンロードを誘引する可能性のあるサイトへのアクセスが確認されました．現在のブロックポリシーは「ヌード（裸体）」「ポルノ」「スパム URL」「フィッシング」「悪意のあるサイト」の 5 つのカテゴリをブロックしています．図 4 に Web Filtering の設定プロファイル例を示します．

Web Filtering では，HTTP の 80 番だけではなく HTTPS の 443 番ポートも合わせてポリシーの適用を行っています．443 番ポートのポリシー適用は 2017 年 7 月頃から運用を開始しています．マルウェアの C&C 通信が 443 番ポートを用いられている現象が確認されたことや，443 番ポートのアダルトサイトがブロックされていないことが確認されたため，443 番ポートへの Web Filtering の設定を投入することになりました．

当初は deep-inspection を実施していたが，カテゴリ分類でのブロックに不具合が生じたため，性能劣化の少ない，certificate-inspection のポリシーに変更しました．certificate-inspection では，証明書内の CN を参照し，FortiGuard[6] への問い合わせを行います．このため，URL パス等のログを収集することはできません．deep-inspection ポリシーを適用した場合は，境界ファイアーウォール内のローカル CA 証明書を外部からの証明書と入れ替えてユーザへ提供するため，ユーザからは Fortinet の自己署名証明書を取得した様に見えます．大学での運用としては，これは望ましい挙動ではないため，deep-inspection での運用は見送りました．Active Directory を用いた一括端末管理を実施している環境では，事前に Fortinet のローカル CA 証明書をユーザ端末に強制的にインストールすることで，この様な問題を回避することが可能です．

2.3.4 アンチウィルス

学外からメール添付によるウィルス感染を予防することを目的として，学内のメールを受信しているサーバの IP アドレス情報を収集し，それらのアドレスグループに対して，ウィルスを除去するためのプロファイルを作成しました．試験運用を 2015 年 12 月頃より開始し，一部のサーバに対してウィルス除去のテストを実施しました．テスト運用では大きな問題が発生しなかったため，本番運用を 2016 年 6 月 1 日より開始し，学外から学内への SMTP セッションに対してウィルス除去を行うアンチウィルスプロファイルを適用しました．

Fortigate 上での設定では FortiGuard へのシグネチャ更新は 1 時間に 1 回が最短時間です．しかし 1 時間の間にアンチウィルスシグネチャが複数回更新され，ウィルス付きメールが学内に侵入する現象が確認されたので，外部サーバより 15 分毎にアンチウィルスシグネチャを強制的に更新するスクリプトを実行しています．

2.3.5 情報漏洩対策

2017 年 7 月アメリカ学会を騙る標的型攻撃メール [7] が本学において観測されました．2.3.4 節で述べたアンチウィルスログによって発見できたが，これは添付メールを用いた標的型攻撃メールのためでした．URL を用いた標的型攻撃メールではアンチウィルスログでは検出できないため，情報漏洩対策 (DLP) プロファイルを作成し，学外から学内へのメールに対してポリシーを適用しました．図 5 に情報漏洩対策プロファイル設定例を示します．

DLP 対策を実施後，8 月 20 日頃に九州工業大学の生命体工学研究科を騙るフィッシングサイトへ誘導するメールが本学へ接到しました．本対策により接到メールは 56 通で，宛先メールアドレスの確認もできたため，メール到着後の対策が容易となりました．

実際に構築されたフィッシングサイトを図 6 に示します．図 6 に示すように，weebly.com を用いた偽サイトであったため，フィッシング対策協議会 [8] への連絡と並行して，weebly.com の問い合わせサイトへ直接連絡を行い，偽サイトの閉鎖を要求しました．これらの連絡に加え，Web Filtering ログを用いて学内からフィッシングサイトへアクセスした形跡について調査しました．幸いにして，この事例ではフィッシングサイトへのアクセスは確認されませんでした．

図 5: 情報漏洩対策プロファイル例

問題点としては，学外からアクセスしていた場合はこれらのシステム上でも確認することが不可能な点です．大学での端末の利用形態を考えると，学外からのアクセスも容易に発生するため，利用者へのフィッシング対策の啓蒙活動も併せて進めていく必要があります．

2.4 キャンパスファイアーウォール

図 2 に九工大ネットワークの概要図を示しています．図 2 に示すように，戸畑キャンパス，飯塚キャンパス，若松キャンパスにも Fortigate-1000C が導入されています．キャンパスファイアーウォールでは，各キャンパスおよび部局においてアクセス制限を設定するための機能を有効にしています．境界ファイアーウォールは大学の境界での学外公開の制御を実施しているが，キャンパスファイアーウォールでは大学内の通信に対して，制限をかけることを目的としています．複数の部局がそれぞれでファイアーウォールポリシーを記述できる様に，それぞれ仮想ドメイン毎に論理分割された構成となっています．

戸畑キャンパス及び飯塚ャンパスでは，各学科およびセンター毎に仮想ドメインを割り当てており，それぞれ独自でのポリシー適用を依頼しています．若松キャンパスは導入時より 1 ドメインでの運用となっていたため，それを継承した形での運用となっています．2017 年 9 月現在で，戸畑で 19 ドメイン，飯塚で 15 ドメインを収容しています．既存で収容されていない部局や教室があるため，順次キャンパスファイアーウォールへの収容を調整しています．

2.5 ネットワーク・フォレンジックシステム

図 2 中の SL4540 と表記されている装置がネットワーク・フォレンジックシステムです．HP 社 ProLaint SL4540 Gen8 サーバが導入されています．OS として CentOS7 が稼働し，tcpdump コマンドにより大学の出入り口のすべてのパケットをペイロードも含めて保存しています．ストレージの物理容量は 4TB ニアライン SAS が 60 個入っており，240TB となっています．これを RAID6 構成とし，100TB のパーティション 2 つに分割しています．それぞれのパーティションで奇数日，偶数日と振り分けを行い，ディスク障害対策としています．ネットワークインタフェースは 10Gbase-T インタフェースを 2 口準備し，キャンパス間スイッチからのポートミラーでトラヒックをキャプチャしています．本システムで九州工

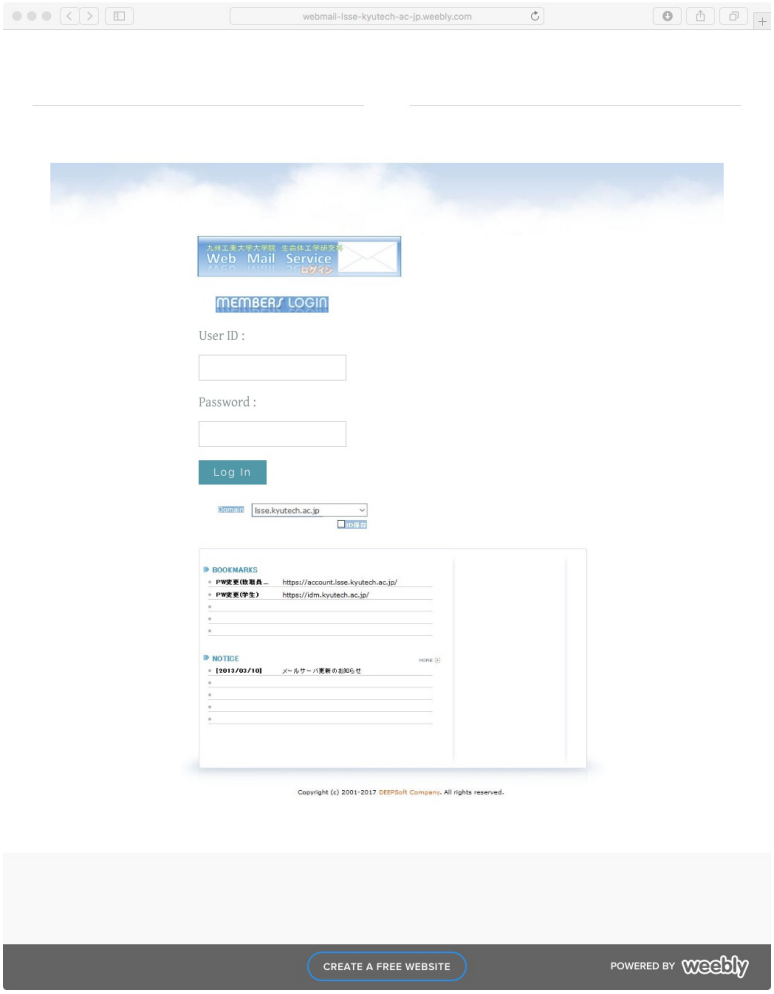
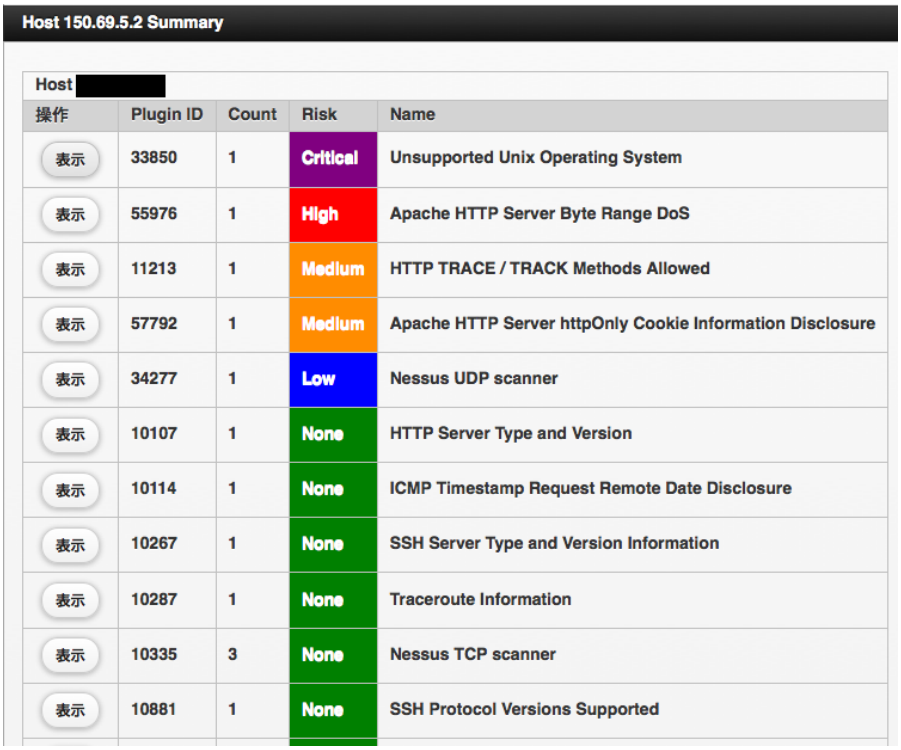


図 6: フィッシングサイト

業大学ではおおよそ 3ヶ月間のトラヒックを保存することが可能となっています．3ヶ月以内であれば，遡って通信履歴を追跡することが可能となっているため，ネットワーク・フォレンジックの重要な設備となっています．

2.6 脆弱性診断

九州工業大学では，2.3.1 節で述べた境界ファイアーウォールにおける学外公開 IP アドレスに関して，実際に公開される前に脆弱性診断を実施します．脆弱性診断には tenable 社の nessus[9] を用いて行います．図 7 に脆弱性診断実行例を示します．本学では Risk medium 以上が出た場合は公開を認めない方針で運用しています．実際にサーバの脆弱性によりインシデントが発生した場合，境界ファイアーウォールでのアクセス遮断および，当該サーバの脆弱性診断を実施し，当該管理者へ対策を促します．Risk medium の対策が実施されるまでは，学外公開は停止されます．



Host 150.69.5.2 Summary

Host [redacted]

操作	Plugin ID	Count	Risk	Name
表示	33850	1	Critical	Unsupported Unix Operating System
表示	55976	1	High	Apache HTTP Server Byte Range DoS
表示	11213	1	Medium	HTTP TRACE / TRACK Methods Allowed
表示	57792	1	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure
表示	34277	1	Low	Nessus UDP scanner
表示	10107	1	None	HTTP Server Type and Version
表示	10114	1	None	ICMP Timestamp Request Remote Date Disclosure
表示	10267	1	None	SSH Server Type and Version Information
表示	10287	1	None	Traceroute Information
表示	10335	3	None	Nessus TCP scanner
表示	10881	1	None	SSH Protocol Versions Supported

図 7: 脆弱性診断実行例

2.7 全学 DNS キャッシングサーバ

本学では 2016 年 12 月より，全学 DNS キャッシングサーバの運用を開始しました．これは，以下に述べる 2 点を目的としたセキュリティ向上の対策の一環です．物理サーバとして Dell PowerEdge 1950III を用い，ハイパーバイザーとして esxi6.0.0 を導入しています．ゲスト OS として CentOS7 を導入し，bind により DNS キャッシングサーバをサービスしています．物理 CPU 2 個 (総計 8 コア)，メモリ 32GB を実装しています．

- DNS 権威サーバと DNS キャッシングサーバを分離することで DNS キャッシュポイズニング攻撃 [11] の回避を図る
- DNS キャッシングサーバのクエリログを保存することで，DNS プロトコルを用いた学内からの不正通信の検出を可能とする

戸畑キャンパス，飯塚キャンパスにそれぞれ 3 台の物理サーバを準備し，仮想環境を構築したのちに DNS キャッシングサーバの構築を行いました．クエリログを 2.8.2 節で述べる syslog サーバへ転送することで，全ての DNS キャッシングサーバのクエリログを保存することが可能な環境を構築しました．平日の 1 日のクエリ数は戸畑，飯塚共に約 300 万クエリでログの総量はそれぞれ約 600MByte でした．

全学 DNS キャッシングサーバの構築により，早期警戒情報 [10] に含まれる C&C サーバの FQDN を用いた学内端末の調査が容易となり，学内セキュリティの向上に寄与しています．

2.8 ログ保存

本学ではログ保存のために 3 系統の syslog サーバを運用しています．以下にそれぞれの役割について説明します．

2.8.1 syslog1 号機

syslog1 号機は全学セキュア・ネットワーク [2] で導入されたスイッチの syslog を保存するためのシステムです．syslog1 号機はスイッチだけではなく，キャンパス間の WDM や無線 LAN コントローラのログなど 200 以上のデバイスのログを保存しています．仮想環境上に構築されています．

2.8.2 syslog3 号機

syslog3 号機は 2.7 節で述べた DNS キャッシングサーバの DNS クエリログを保存するためのシステムです．syslog3 号機は 2TB ストレージを 12 個搭載し，RAID6 で構成してログ保存容量として 16TB を確保したサーバです．6 台の DNS キャッシングサーバのログは本システムでの保存だけではなく，FortiAnalyzer-1000E へ転送することで，簡易検索を実行可能にしてます．インシデント発生時の初動対応では FortiAnalyzer を用い，定常的な検査では本システムに構築したスクリプトを daily で実行することで不審な FQDN へのクエリが発生していないかどうかの検査を行っています．また syslog3 号機では DNS キャッシングサーバのログ以外に事務局が管理している AD サーバの認証ログや無線 LAN および VPN 認証に用いている AD サーバの認証ログも保存しています．AD サーバから認証ログを syslog サーバへ転送するために nxlog[12] を用いています．

2.8.3 syslog4 号機

syslog4 号機は境界ファイアーウォールのログを保存するためのシステムです．syslog4 は DNS キャッシングサーバのログを保存しているシステムと同様のスペックです．境界ファイアーウォールでは 2.3 節で述べたように様々な機能を有効にしているため，ログ量が膨大です．1 日のログ量はおおよそ 10GB ～40GB で推移しています．

2.9 エンドポイント

本学ではネットワーク上での対策だけではなく，エンドポイントのソリューションも合わせて導入しています．本学ではトレンドマイクロの包括契約であるキャンパスアグリーメントを契約しており，教職員だけではなく全ての学生の端末にも利用可能です．各キャンパスにコーポレート配信サーバを導入しており，それぞれのキャンパス毎で管理されています．ログ，検知などの全学的な集約がされていないため，全学での統一的な運用はされていません．今後はコントロールマネージャの導入も含めた全学的な統一的な運用に向けた作業が必要であると考えています．エンドポイントのライセンスにスマートフォンやタブレット端末も含まれているため，スマートフォンやタブレット端末へも実験的に導入を進めています．

2.10 評価機

情報基盤運用室では図 2 に示される九工大ネットワーク環境を用いて，様々なセキュリティ機器の評価，検証 [17] を行ってきました．2017 年 3 月に導入された，SDN スイッチ Big Monitoring Fabric[16] の導入により，これまではミラートラヒックによる評価しかできなかったものが，インライン環境で評価することが可能となりました．Big Monitoring Fabric の導入により，評価機の導入，撤去が容易になったこと，また，運用機においても同一メーカーで HA 構成による冗長化ではなく，異なるメーカーで冗長構成を構築することが可能となりました．しかし，こうした構築ではポリシーの同期など問題点も存在します．

3　インシデント対応例

本節では実際にインシデントが発生した際に図 1 のフローに基づいてどのような対応を行うかについて述べます.

8/31 16:55 頃，本学工学部のある部局の公開 Web サーバが広告の書き込みが可能な状態で放置されている旨の通報を学外者から受けました．直後に中村が当該 Web サイトを閲覧，通報通りであることを確認しました．このタイミングでインシデントであると判断し，当該 web サーバの学外公開ポリシーを停止し，外部からのアクセスの遮断を実施（17:13 頃）．同時に学内からはアクセス可能であるので，インシデント対応の事務的な手続きを進めることを，事務方に指示を出しました．事務方から当該部局へのインシデント発生の通知は 17:50 頃でした.

学外公開サーバであったため，対策が実施されて，かつインシデント対応報告書が提出され内容に不備がないかどうかの確認が完了した後に，学外公開遮断の解除が行われます.

統括情報セキュリティ責任者や最高情報セキュリティ責任者へは，提出されたインシデント報告書に基づいて報告が行われます.

4　標的型攻撃メール訓練

情報基盤運用室では，2015 年から標的型攻撃メールを疑似送信し組織構成員の訓練を図るとともに，標的型攻撃メールへの啓蒙活動を行ってきました．実際の送信作業や偽装サイトの構築に関しては株式会社キューデンインフォコム [13] の標的型攻撃メール訓練サービスを利用しています．2015 年度に実施した訓練は最初のメール送信であったため，どの程度のデータが取得できるか？を主眼において訓練を行いました．2016 年度では 2015 年度の結果を踏まえて，e-learning にアンケートを付加して，訓練者からの情報取得に努めました.

4.1　事前準備，調査

キューデンインフォコムの標的型攻撃メール訓練サービスを用いて訓練を実施するに当たり，事前に決定しておかなければならない項目が複数あります．次節以降で，各項目について述べます.

4.2　メール受信者の範囲の決定

予算との兼ね合いも考慮する必要があるが，メール受信者の範囲を広げると必要な予算は多くなります．限られた予算の範囲内で訓練を実施するために何名程度に対して訓練メールを送信するのか？を決定する必要があります．本学での訓練の場合，常勤教職員および非常勤職員としました．非常勤講師は含まれていません．この理由は本学の教職員用ポータルサイトにおけるアカウント配布者と同等程度が望ましいという判断からです．実際のメール送信数は約 900 アカウントでした.

4.3　メール送信日時の決定

2015 年度は初回であったため，業務的な繁忙期は避け，かつ，情報セキュリティに対して意識を高めるために，本学で行っている「情報モラル向上週間」の期間中に実施しました．2015 年度の訓練では，登録されたアカウントへの一斉送信であったため，メール受信を不審に思った職員が他の職員に口頭で確認するなどの事象が確認されました．2016 年度以降では，実際に教職員への一斉通知を装った内容の文面としたため，メール送信に関しては全教職員に対して一斉に送信しました.


ID管理者 <sysid.manager@gmail.com>
【重要】認証IDシステムパスワード更新のお願い
宛先: 中村 豊 <yutaka-n@isc.kyutech.ac.jp>

※このメールは対象者にのみ自動送信しています。

認証IDシステムに登録されている、一部の利用者のパスワード情報が外部に
漏洩した疑いがあり、現在、影響範囲を調査中です。

このメールを受信した方は、悪意のある第三者に漏洩した情報を悪用される
恐れがありますので、以下のＵＲＬの手順に従って至急パスワードを更新して
ください。
（クリックすると手順が表示されます。）

http:/[redacted]/password/password.h[redacted]

図 8: 2015 年度の訓練メール文面

4.4 メールの文面の決定

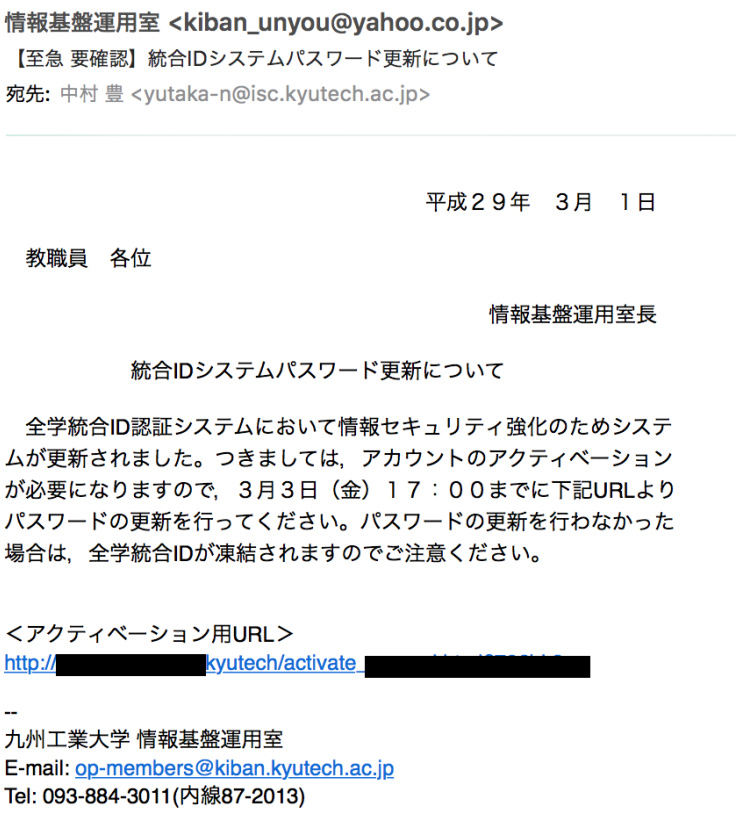
メール受信者に共通で，かつ注意を引きそうな話題を選択する必要があると考え，2015 年度では統合アカウント管理システムからの情報漏洩疑いに関する文面での訓練を行いました．図 8 に実際に送信されたメール文面を示します．From 行に関しては，置換機能を用いて「ID 管理者」とし，実体のメールアドレスは gmail を用いました．また，添付ファイルではなく URL 型としました．キューデンインフォコムのサービスの制限で添付ファイルの場合はワードファイルに限定されることや，ポップアップでのブロックがかかるかもしれない，という問題を回避するためです．

2016 年度では，日本学術振興会を装った不審なメール [14] の様な事件が発生していたため，文面の難易度を高度化し，From 行以外は全て実際に業務で用いられている情報を用いて文面を作成しました．図 9 に実際に送信されたメール文面を示します．

4.5 クリック率，クリック後

2016 年度の訓練では，3 月に送信したこと，アカウントに関係し締切を設けた文面であったことから，全体のクリック率は 41.4%と非常に高い数値となりました．図 10 に職種毎のクリック者数，クリック率の内訳を示します．2015 年度の訓練では，非常勤職員と常勤職員で 2 倍程度のクリック率の差が見られました．しかし，2016 年度の訓練では，文面の難易度が上がったため，職種による有意な差は見られませんでした．

URL をクリックすると，図 11 に示される画面が表示されます．クリックした後に，サイボウズガルーン [15] への報告を促しているが，2016 年度の訓練ではクリック後の報告は 17.2%と低調でした．実際にインシデントとして発生している文面と同程度の難易度であることを考えると，クリックを防止する教育を行うと共に，クリック後に報告・連絡を行うことが重要である旨の啓蒙を続けていく必要があります．



情報基盤運用室 <kiban_unyou@yahoo.co.jp>
【至急 要確認】統合IDシステムパスワード更新について
宛先: 中村 豊 <yutaka-n@isc.kyutech.ac.jp>

平成２９年　３月　１日

教職員　各位

情報基盤運用室長

統合IDシステムパスワード更新について

全学統合ID認証システムにおいて情報セキュリティ強化のためシステムが更新されました。つきましては，アカウントのアクティベーションが必要になりますので，３月３日（金）１７：００までに下記URLよりパスワードの更新を行ってください。パスワードの更新を行わなかった場合は，全学統合IDが凍結されますのでご注意ください。

＜アクティベーション用URL＞
http://[redacted]kyutech/activate_[redacted]

--
九州工業大学 情報基盤運用室
E-mail: op-members@kiban.kyutech.ac.jp
Tel: 093-884-3011(内線87-2013)

図 9: 2016 年度の訓練メール文面

5　まとめ

本報告では，九州工業大学情報基盤運用室がこれまで実施してきた情報セキュリティ対策について，それぞれの項目毎に詳述しました．セキュリティ対策の実働部隊として情報基盤運用室が機能していくためには，組織のあり方の整備，規則の改訂，装置の導入，チューニング，対外的な情報収集と必要項目等，整備していかなければならない事項は多岐にわたります．CIO からの権限移譲を規則として制定したとしても，実際の機器の操作が伴わなければ，その規則の効果を得ることはできません．

今後の課題として次期ネットワークシステムの調達に関するセキュリティ機器の調査，検討や運用体制の見直しなど引き続き実施していく必要があります．

参考文献

[1] 日本シーサート協議会, http://www.nca.gr.jp/

[2] 中村 豊 , 福田 豊 , 佐藤 彰洋: 九州工業大学における全学セキュア・ネットワークの導入について, 研究報告インターネットと運用技術 (IOT), 2015-IOT-28(20), 1-6 (2015-02-26)

[3] 福田 豊 , 中村 豊 , 佐藤 彰洋: 九州工業大学・全学セキュアネットワーク導入における無線 LAN 更新, 研究報告インターネットと運用技術 (IOT), 2015-IOT-28(21), 1-6 (2015-02-26)

[4] 福田 豊 , 中村 豊: 九州工業大学・全学セキュアネットワークにおける無線 LAN 利用について, 研究報告インターネットと運用技術 (IOT), 2016-IOT-32(1), 1-8 (2016-02-25), 2188-8787

職種	開封者数	対象者数	開封率
事務職員	127	316	40.2%
うち事務補佐員	62	146	42.5%
事務補佐員除く	65	170	38.2%
教育職員	173	387	44.7%
うち特任教授等	6	18	33.3%
特任教授等除く	167	369	45.3%
技術職員	44	116	37.9%
うち技術補佐員	6	29	20.7%
技術補佐員除く	38	87	43.7%
研究職員等(※)	17	54	31.5%
合計	361	873	41.4%

※研究職員，継続研究員，支援研究員，科学研究支援員，産学官連携研究員，技術移転アソシエイト，教務補佐員

図 10: 2016 年度の職種毎のクリック者数・クリック率の内訳

[5] ZABBIX, https://www.zabbix.com/jp/

[6] FortiGuard Labs, https://fortiguard.com/

[7] アメリカ学会 緊急不審メール情報ーアメリカ学会を騙ったなりすまりのメール, http://www.jaas.gr.jp/blog/2017/07/post-284.html

[8] フィッシング対策協議会, https://www.antiphishing.jp/

[9] Nessus, https://www.tenable.com/products/nessus-vulnerability-scanner

[10] JPCERT/CC 早期警戒情報, https://www.jpcert.or.jp/wwinfo/

[11] DNS Cache Poisoning Vulnerability, https://www.iana.org/about/presentations/davies-viareggio-entropyvuln-081002.pdf

[12] NXlog, https://nxlog.co/

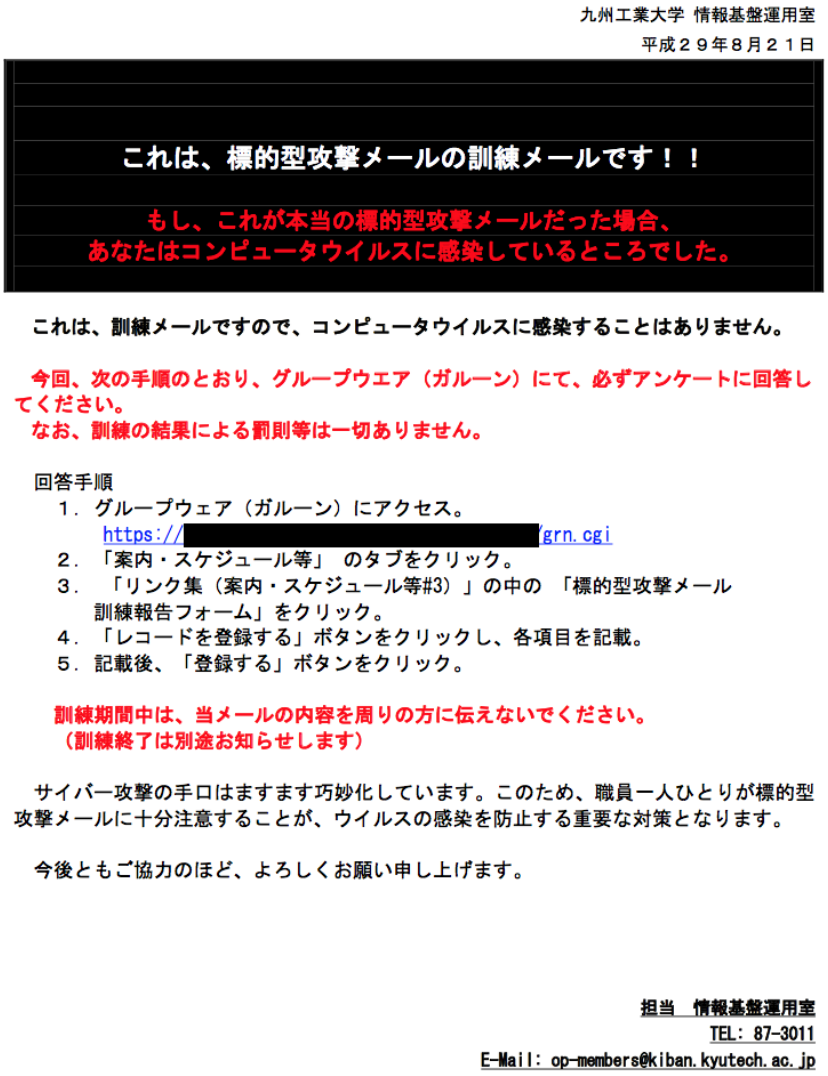
[13] 株式会社キューデンインフォコム, https://www.qic.co.jp/

[14] 日本学術振興会を騙った標的型攻撃メール, https://csirt.ninja/?p=1103

[15] サイボウズガルーン, https://garoon.cybozu.co.jp

[16] Big Monitoring Fabric, http://www.bigswitch.com/sdn-products/sdn-products/big-monitoring-fabric/overview

[17] 中村 豊 , 佐藤 彰洋: 次世代ファイアーウォール機器の評価検証について, インターネットと運用技術シンポジウム 2016 論文集,2016,106-106 (2016-12-01)



九州工業大学 情報基盤運用室
平成２９年８月２１日

これは、標的型攻撃メールの訓練メールです！！

もし、これが本当の標的型攻撃メールだった場合、
あなたはコンピュータウイルスに感染しているところでした。

これは、訓練メールですので、コンピュータウイルスに感染することはありません。

今回、次の手順のとおり、グループウエア（ガルーン）にて、必ずアンケートに回答してください。
なお、訓練の結果による罰則等は一切ありません。

回答手順
１．グループウェア（ガルーン）にアクセス。
https://[redacted]/grn.cgi
２．「案内・スケジュール等」 のタブをクリック。
３．「リンク集（案内・スケジュール等#3）」の中の 「標的型攻撃メール訓練報告フォーム」をクリック。
４．「レコードを登録する」ボタンをクリックし、各項目を記載。
５．記載後、「登録する」ボタンをクリック。

訓練期間中は、当メールの内容を周りの方に伝えないでください。
（訓練終了は別途お知らせします）

サイバー攻撃の手口はますます巧妙化しています。このため、職員一人ひとりが標的型攻撃メールに十分注意することが、ウイルスの感染を防止する重要な対策となります。

今後ともご協力のほど、よろしくお願い申し上げます。

担当　情報基盤運用室
TEL: 87-3011
E-Mail: op-members@kiban.kyutech.ac.jp

図 11: クリック後の画面