みんなで探そう！セキュリティ対策のおとしどころ

九州大学大学院・システム情報科学府
上本　悠貴

セキュリティ運用の実情

情報システムへの依存度が高まるにつれて、そのシステムを狙うサイバー攻撃からの防御、システム自身のセキュリティを維持することは非常に重要な課題となっている。現在では、それらの課題に対して技術的に取り組んでいたとしても、全てのインシデントを未然に防ぐことは困難になっている。

各組織の予算や人員は異なるので、セキュリティ対策も組織によって異なるが、セキュリティ対策をどこまで行うべきかは共通した悩みの種である。

システム技術分科会合 2018 概要

2019 年 2 月 1 日に中之島ダイビル１０階にある富士通株式会社　富士通 DTC（Digital Transformation Center）大阪にて開催された、サイエンティフィック・システム研究会（以下、SS 研）システム技術分科会会合では、『みんなで探そう！セキュリティ対策のおとしどころ』の題のもと、セキュリティ対策の現状と課題についての講演と意見交換が行われた。

１名の講演者による、SOC の運用事例や、そこから浮上してきたセキュリティ対策の課題、今後インシデント対応で求められる能力についての講演が行われた。

セキュリティ対策状況の共有と討論

講演後に行われた討論、意見交換は、ワールドカフェ形式で２部行われた。各グループでテーブルマスターを中心に、参加者の所属する組織の実情を踏まえた意見が飛び交う。テーマを事前に定めず行われた１部では、インシデント対応や教育を中心に産学で様々な意見交換がなされた。１部を踏まえたテーマで実施した２部は、テーマに沿った各組織の実情にまで踏み込んだ密度の濃い討論が行われた。

NII-SOCS の運用から浮上してきたセキュリティ対策の課題

～高度化するサイバー攻撃にどう向き合うか～

国立情報学研究所　高倉　弘喜氏

サイバーセキュリティ基本法により、大学その他の教育研究機関は、自主的かつ積極的にサイバーセキュリティ対策を行い、重大なインシデントに対しては内閣府への説明が求められる。しかしながら、すべての大学が個別で上記に対応することは現状困難である。

NII-Security Operation Collaboration Services(以下、NII-SOCS)では、NII が構築、運用する学術ネットワーク(SINET)と商用系の通信を監視している。加えて、大学に設置された NII のセンサーから上がってくる警報の簡易解析や、セキュリティベンダとの情報共有から、注意喚起をしている。

上記の運用を続けていく中で、様々なことが分かってきた。まず、大学毎のインシデント発生率のギャップである。多くの大学は、インシデントは月に 1 件弱であるのに対し、数百ものインシデントが月毎に発生している所もある。要因に、大学の規模によるガバナンスの効きにくさが挙げられる。次に、インシデントの原因である。そのほとんどがマルウェアであり、ほぼ全てのマルウェアは学生の Android スマートフォンであることが分かった。日本語での感染活動に留学生が引っかかり感染が多発している。C&C サーバと通信を確立させるマルウェアも比較的多く、スマートフォンの扱いには注意が必要である。

注意喚起時、大学側のよくある誤った対応がある。まず、VirusTotal に反射的にマルウェアを参照させる場合である。昨今の標的型攻撃は、本物のメールにマルウェアを添付することがある。VirusTotal は、条件を満たす全ての人に収集したウイルスを提供する。そのため、機密情報の漏洩の危険がある。また、マルウェアのハッシュ値のみではお手上げで、対応を諦めてしまう場合がある。しかし、通信先ドメイン名が分かれば、類似マルウェアに関する情報が得られることがある。

IT 依存度が急速に高まる大学で、「インシデントが発生したら対処」というもぐらたたきのサイクルを改善する必要がある。攻撃によってシステムが止まった場合に、被害の大きなものから格付けし、どのランクへの攻撃かで対応をかえる「ダメージコントロール」が非常に重要となる。重要システムへの攻撃は、早急に対応が必要だが、そうでない場合、対処せずあえて監視のみとすることで、攻撃者の情報が得られるかもしれない。現状、大学ではシステムの停止と被害の大きさを紐づけできていない。

これからは、セキュリティ対策を学内だけでするのでなく、他組織との連携が重要である。また、急速に進む AI 化、自動化によって、ある程度の攻撃は AI が対処することが想定される。そのため、これからの大学に求められるのは、学内外の連携が取れる組織(全学実施責任者、CSIRT など)や、全体を俯瞰して意思決定ができる人材ではないだろうか。

高倉　弘喜氏

(Takakura Hiroki)

国立情報学研究所

ワールドカフェ形式でのグループ討論

講演後、ワールドカフェ形式でのグループ討論が２部行われた。具体的には、６つのテーブルにそれぞれテーブルマスターがおり、参加者が各テーブルを回りテーブルマスターを中心に意見交換や討論を行った。第一部では、予めテーマを決めることなく、参加者の所属する組織毎での対応の情報交換を中心に討論が行われた。テーブルには画用紙やポストイットがあり、セキュリティ対策やインシデントを書き出し、分類することによって、互いの理解をより深める意見交換となった。第一部の各テーブルの概要は以下の通りである。

表１．グループ討論第一部の概要

テーブル１	大学で起きているインシデントを理解することで、産学で連携のとれた対策が可能となる。そのために、大学目線でインシデントに重要度をつけ、人員や予算に合わせた対策に関した意見交換が行われた。
テーブル２	セキュリティ対策には、教育が必要である。組織毎に守るものは違うため、各々で確認が必要である。また、入出力を VDI で絞ることでセキュリティインシデントを抑制できている。
テーブル３	各組織のセキュリティ対応を共有した。その中でも、ペナルティの重さからくるインシデントの隠蔽といった、人の心理面に関する対処方やアイディアが討論された。
テーブル４	組織内でセキュリティの意識付けを行う効果的な手法が複数話されていた。

テーブル５	一律的に対策をとることは難しいため、セキュアなネットワークの構成法や、セキュリティ対策を浸透させる為の様々な対策が討論された。
テーブル６	大学組織に対するセキュリティベンダからの警告は多く、クローズにならないものある。それらに対しての管理や対処を中心に討論された。

第二部では、一部で行われた内容を踏まえて、テーブル毎にテーマを決めて討論が行われた。テーマに沿った各組織の事例も多く共有され、それに対しての是非や改善案が多く議論された。第二部の各テーブルのテーマと概要は以下の通りである。

表２．グループ討論第二部のテーマと概要

テーブル１ 偉い先生問題	セキュリティの認識が広がってきたこともあり、多くの先生が従うようになった。ごく一部の、理解が得られない先生達に対しての対策が複数挙げられた。
テーブル２ インシデントの 終了判定	インシデントの終了判定を、文書化しておくことは非常に難しい。PC がウイルス感染した場合は、OS をクリーンインストールし、１週間経過観察をするのが落としどころだろう。
テーブル３ 教育は実施した けれど…	教育の評価は、実施率だけでいいのか。教育後の意識付けの為に、ディスカッションを設ける、帰属意識を高めるなどの、手法が提案された。教育を実施する側と受講側の気持ちの折り合いが重要である。
テーブル４ インシデントの入り口 (トリアージ)	重大な場合には報道される。ネガティブな報道をされない為の対策が必要である。情報漏洩があったかも重要な点である。様々な重大インシデントの想定をしておくべきである。報告しやすい組織づくりが早期対応に繋がる。
テーブル５ 私のインシデント対応 はこれでよかったの？	FW では検知されたが、アンチウイルスでは検知されなかった。 →重要データがあるかどうかで対応を変えるべき 利用しているクラウドサービスの IP が、別ドメインでマルウェアを配布していた。IP を FW で遮断していいか。 →遮断してよい。安くても不審なところからサービスを買うべきでない。
テーブル６ 学生問題	留学生の PC にマルウェアが入っていたり、C&C サーバと通信する事例が多い。そのため、e-Learing や事前の講習が必要である。注意喚起の多国語化も重要である。また、学生の SNS による情報漏洩等は落ち着いてきている。