事業活動報告 NO. 2

平成25年度 大学情報セキュリティ研究講習会 開催報告

1. 概要

サイバー戦争とも言われる最近の状況下、政府機関及び企業の重要な情報が窃取・流出する事態が頻発している。大学においても昨年国立大学の５大学で論文・研究報告・教職員のメールアドレスなどが国際ハッカー集団に窃取され、その情報が公開される事件も発生している。

そこで、本協会では私立大学・短期大学における情報セキュリティの危機管理能力の強化を推進するため、サイバー攻撃への対策と情報資産の保全および業務継続に向けた対応について、講演や実習およびディスカッションを行う講習会を、８月27日(火)に学習院大学（豊島区目白）で開催した。本協会の加盟・非加盟の大学・短期大学から参加を募集し、74名（58大学）の参加があった。

本講習会では、上記のような脅威への対策を踏まえた情報セキュリティの探究を目的に講演を中心とした全体会、および実習を中心とした二つのコースを設けた。

2. 全体会

全体会は、「サイバー攻撃への対策」と「災害時を想定した対策」の２部構成とした。

本講習会の運営委員会としては、第１部の問題意識として、常態化する情報の窃取・流出の背景にある「**攻撃の手口のステルス化**」と「**大学の情報資産管理の組織的対応への遅れ**」に警鐘を鳴らすことを挙げた。第１にサイバー攻撃情報及び対処方法などの最新情報を理解すること、第２に企業を中心に先行して実施されている政府関連機関との攻撃手法情報の共有の仕組みについて知見を高めることを目標に三つの講演を実施した。

まず、前者については**名古屋大学教授**の**高倉弘喜氏**より「**サイバー攻撃の脅威と攻撃パターン**」と題して講演していただいた。

様々なサイバー攻撃のうち、深刻視される標的型攻撃に対しては、一般的に「攻撃・被害の全貌把握」と「被害システムに対する完全なセキュリティ対策措置」が叫ばれる。しかし、高倉氏の指摘によれば、実際の事例では攻撃被害の発覚から半年以上も前から侵入を許していることが多く、その全貌の把握となれば１年程度の時間が必要である。これらの状況を鑑みれば、標的型攻撃の被害に合った場合、被害状況を調査継続しながら、その途中経過を公表するといった対応にならざるを得ないことが示された。一方、標的型攻撃対策としては、昨年度の大学情報セキュリティ研究講習会で紹介された「出口」対策の概念が誤解されて流布されている点にも警鐘を鳴らし、学内ネットワークの細かいVLAN分割やアクセス制御、認証サーバーのアクセス制御といったオーソドックスではあるが徹底することが難しい対策についても、段階を追って導入する努力を行うよう改めて主張された。

また、今後の新たな脅威として、個人持ち込み機器を経由した意図しない通信経路問題やOA機器・情報家電・自動車といった様々なデバイスに存在する脆弱性の悪用にも注意するべきことが指摘された。これらの困難な状況を踏まえながら、今後に期待されている標的型攻撃対策としてクライアントやネットワークの仮想化による効果的な防御態勢の展望を紹介した。

次に、後者について、「**サイバー攻撃対策の情報共有組織「J-CSIP」の取り組み**」題して、**独立行政法人情報処理推進機構**（以下、IPAと表記）の**松坂志氏**より講演いただいた。松坂氏は、官民連携によるサーバー攻撃に関する情報共有の取組み「Initiative for Cyber Security Information sharing Partnership of Japan」（以下、J-CSIPと表記）を推進している。現在の参加企業は５業界、45組織とのことであるが、特に重工業界からも多数参加していることでもよく知られている。実績として、標的型攻撃メールの収集に関して、2012年度で201件、

2013年度もこれまでの４半期で64件とのことで、J-CSIP発足以前の収集数に比して大幅な伸びを示している。

また、大学を対象とした本講演のために、実際に大学で観測された標的型攻撃メールの例も提示し、危機意識を持つよう警告を発した。

J-CSIPが運用する情報共有スキームのポイントは、IPAが参加組織とのNDAを結んだ上で情報の集約点・発信源となることである。IPAの監督官庁は経済産業省であるが、参加組織から提供された攻撃情報はIPAから経済産業省に報告されずに機密が守られることも参加企業の情報提供を促す意味で重要であろう。

J-CSIPの運用の結果、標的型攻撃は特定の企業のみではなく、特定の業界に類似の攻撃がなされることが明確になった。これにより、J-CSIPが類似攻撃の早期発見による被害の回避に有用であることも認識され、現在は参加企業によるスムーズで活発な情報提供がなされるようになったという。

本協会としても、加盟校を中心に大学への標的型攻撃の情報共有を行う仕組みを立ち上げるか検討中であり、本講演で示されたスキームは大変参考になるものであった。

第２部では、「**災害時を想定した対策**」をテーマに据えた。

日本では、大規模な地震の発生が予測されており、いつ震災が起きても不思議ではない状態にある。大学の社会的責任を果たすためには、教育・研究活動の成果としての情報資産及び災害時での情報通信体制の確保が課題である。しかし、今回の本協会が実施したアンケート調査（７月実施、P.57参照）でも、実際の対策を行っている大学は２割程度に過ぎず、ほとんどが計画を策定する段階のままである。

そこで、本講習会の運営委員会では遠隔地の大学との情報資産の相互補完及び業務継続性の可能性について検討するにあたり、大学間による補完の範囲や方式および条件合わせなどが先進的に進められている実践例として、今年度初頭に宇都宮大学と横浜国立大学によって締結された情報戦略協定に着目した。本協定について**宇都宮大学学長補佐、総合メディア基盤センター長**の**永井明氏**より「**大学間業務継続連携事業によるIT-BCP基幹システム**」と題して講演いただいた。

冒頭に配慮すべき点として指摘されたのは、大学の業務継続の必要性は災害時のみでないということである。その点を、全職員が日常から意識する必要があると述べられていた。言葉では簡単であるが、実現が難しいこのテーマに対し、宇都宮大学ではISMSやBCMSなどの認証制度を学内に上手く定着させることで、職員の能力を伸ばすことによって実現に成功した点を強調されていた。

実は、この大学間業務継続連携事業は、その発端から数えて10年に亘る準備がなされており、その時系列も丁寧に説明された。また、本協定が実現できた大きな要因として、何よりも両大学の学長が直接扱う案件であったことを挙げられていた点が印象強い。両大学の学長は、「情報は資産である」という明確な意識を持っていたことが、双方の大学の合意形成に寄与している。大学の情報戦略にとって、ガバナンスが如何に大切であるかを示す例と言える。

もともとは大学間でのデータバックアップというレベルから発足したこの計画も、現在では、両大学の仮想化基盤を共有して、相互の仮想サーバーを運用し、トラブル時の相互運用補助、更にはシステム購入の際の共同調達といった運用面での連携まで高い完成度で実施されていることが発表された。

また、この連携の真の目的である職員の能力育成であるが、宇都宮大学との職員交流と相互の運用提携により両大学の運用能力が伸びたことも報告された。

「人が財産である」という明確なメッセージが、大学の情報システム運用にも結実した成果を示した大変素晴らしい講演であった。

3. 情報セキュリティ対策技術部門コース

本コースでは、標的型攻撃の攻撃手法や攻撃を受けた場合の対処方法を演習などによって理解を深めることを目標とした。また、災害対策の一環として日常平常時から大学情報システムの業務継続性を確保するために、最低限必要な情報の優先度を決定するための大まかな指針を示した。

まず、標的型攻撃の攻撃手法と防御方法については、図１に示す架空の標的型攻撃シナリオを作成し、それに基づいて下記の（１）～（５）の講義・演習を行った。

（１）標的型攻撃とインシデントレスポンス

標的型攻撃の攻撃手法の基礎知識を講義で確認し、本コースにおけるインシデントレスポンスの演習範囲を明確にした。

具体的には、標的型攻撃の目的の確認、RATやPass the Hash 攻撃といった要素技術の概要、攻撃痕跡の調査ポイントの紹介を行い、標的型攻撃のインシデントレスポンスフローの内、初動対応を演習で取り扱うことを説明した。

（2）遠隔操作ツール(RAT)の機能とリスク

標的型攻撃の攻撃者側を体験するために、標的型攻撃で使われる攻撃の要素技術の内でRATを取り挙げた。RATの作成、感染パソコンのリモート操作によるパソコン内やネットワーク情報などの収集を演習した。

この実習により、標的型攻撃の脅威を具体的にイメージすることができた。

（3）標的型攻撃メールと添付ファイルのマルウェア（静的）解析

インシデントレスポンスの初動対応の一つとして、標的型攻撃メールへの対策を演習した。

標的型攻撃メールの特徴としては、「実在の人物名を騙る」、「添付ファイルの開封やURLのクリックを誘発する文面」、「メールヘッダー情報の不自然さ」が挙げられる。本セッションでは、標的型攻撃メールの典型例を提示し、上記の特徴に当てはまる箇所の確認を演習した。

また、標的型攻撃メールの添付ファイルには、マルウェアの混入が疑われるため、その安全性調査が必須である。そこで、本セッションの後半では、OfficeMalScanner やVirusTotalなどの利用によるマルウェアの静的解析を実習して、安全性調査の基本的テクニックの習得を図った。

（4）標的型攻撃の痕跡調査

インシデントレスポンスの初動対応としては、マルウェアに感染した疑いのあるパソコンについて調査・隔離・再インストールの前に、該当パソコンの複製の取得が重要である。

そこで、本セッションでは、まずFTK Imger Liteでパソコンのハードディスクとメモリの複製を取得する演習を行った。

さらに、メモリダンプイメージから、疑わしいプロセスの特定、不正サイトへの通信などを調査する一連のマルウェア痕跡調査を体験した。

この実習により、標的型攻撃の被害の疑いがある場合、セキュリティベンダーへの調査依頼を掛けるために必要な基礎知識が習得できた。

（5）標的型攻撃へのセキュリティ対策

標的型攻撃の攻撃手法と防御方法について扱う最後のセッションでは、講義形式で実習内容の体系的にまとめ、更に、補足として、Pass the Hash 攻撃の概要と標的型攻撃が確認された場合のセキュリティ

持続的標的型攻撃対策演習ストーリー

1．導入

A教授のもとに、大学職員から議事録を添付したメールが届いた。添付ファイルはWordファイルであったが、特に議事録を要求した覚えがないため、情報センターに届け出た。

情報センターでは、メールの送信先、メールの送信元が実在の人物であること、添付ファイルがWordであったことを重要視して調査を開始した。

2．攻撃者の攻撃活動シナリオ

<6ヶ月前>
- 某国より、原子力開発委員を務めている○○大学のA教授が保持する機密情報を搾取する依頼があった。
- 攻撃者は、【苦情】をSubjectに記入したメールを、大学の問い合わせ先に送信。その際に、Wordに偽造したRTF 脆弱性悪用Dropperを添付した。
- 総務課長が件のメールを受信し、添付ファイルを開封しDropperに感染、RATをダウンロードした。

<3ヶ月前>
- RATを使って、ネットワーク設定情報（IPアドレス、DNS、メールサーバ）を入手した。
- RATを使って、教職員名簿、委員会名簿を入手した。これらのファイルは総務課長のPC内に保存。また、該当ファイルを学外へ転送。
- 学内のメールサーバを直接指定して、事務系アカウントにマルウェア付メールを送信した。組織内のマルウェア検知機能を調査した。

<2ヶ月前>
- 課長PCからのSMB接続を悪用して、学内のファイルサーバにネットワークログオンしてRATを配置した。教務系ネットワークへのRATダウンロードに使う目的。
- 学内のメールサーバに直接SMTP接続して、教務系アカウントにRTF 脆弱性悪用Dropper(ファイルサーバからのRATダウンロード機能付き)を添付したメールを送信した。感染成功。

<当月>
- A教授への議事録を装ったRTF 脆弱性悪Dropper(ファイルサーバからのRATダウンロード機能付き)添付メールを送信した。

【標題】：Re: 議事録再送依頼
【本文】：A先生
総務課の植木です。
ご要望の委員会議事録を再送します。
ご査収下さい。
> 植木さま
> 理工学部のAです。
> 先程の委員会の議事録ファイルを紛失しました。
> 再送願います。
【添付ファイル名】議事録.doc

図1　標的型攻撃シナリオ

対策のポイントを説明した。

本コースの最後のセッションでは、大学情報システムの事業継続性の確保という観点で、本協会の平成24年度大学情報システム研究会報告書から、「業務分析ワークシート」を紹介し、平常時から大学の情報サービスの優先度を確認しておくことが重要であることを確認して終了した。

受講者アンケートからは、「情報担当者への啓蒙を進めたい」、「職員の意識を変えていきたい」、「学内のネットワーク利用者講習会に内容を盛り込みたい」などの記述があり、講習会の目的が実現できていることが分かった。

その一方で、標的型攻撃の脅威については具体的なイメージが掴めたものの、対策事例の説明時間が少なく、その点の改善を求める声もあった。

今後の技術部門コースの題材としては、実際の事例をベースに、標的型攻撃、仮想化技術、クラウド、スマホ、無線LAN、IPv6トンネルなどへの対応を挙げている受講者が多かった。

また、講習会を２日間開催でレベル別でコースの提供を求める意見もでた。今後の検討課題にしたい。

4．情報セキュリティマネジメントコース

本コースでは、大学の教育・研究・経営に関する情報資産を守るための情報セキュリティマネジメントという観点から、喫緊の課題であるサイバー攻撃の対策、災害を想定した対策をテーマに取り上げた。講習では、サイバー攻撃や災害の脅威やリスクの重要性を確認するとともに、教職員による協力体制の構築や大学間及び外部組織との連携による情報資産保護の仕組みについてグループで討議された。これにより、情報セキュリティに対して、大学組織として今後求められる対応を見据えた検討が行われた。

コースには36名の参加があった。所属は約６割が情報システム部門であり、他には教務部門、図書館、事務部門（総務）等であった。役職は、管理職もしくは教員が約７割を占めた。また、過去に本コースに参加したことのある方が２割弱おり、情報セキュリティ関連の研修として、本講習会が継続的に活用されていることが分かった。

（１）情報セキュリティ対策の自己点検・評価の結果分析と活用について

本協会が加盟校に対して平成22年度から継続して実施している「情報セキュリティ対策の自己点検・評価」の結果について公表し、今年度のテーマであるサイバー攻撃の対策及び災害を想定した対策という観点から、現状と経年の変化について報告した。また、今年度に併せて実施されたサイバー攻撃及び情報セキュリティ関連規程の対応状況の調査アンケートの結果も報告を行った。

（２）サイバー攻撃への危機意識の共有と連携体制の検討

大学で実際に発生した情報セキュリティインシデントの事例を紹介し、身近な所でサイバー攻撃が発生していることを認識して危機意識を共有するとともに、ケーススタディとして学内でインシデントが発生した際に求められる対応について、グループワークを行った。また、インシデントの内容や対応に関する情報を、大学間で共有する仕組みやそのために求められる体制について、グループディスカッションによる検討を行った。

（３）災害を想定した情報セキュリティ対策の検討

東日本大震災により甚大な被害を受けた石巻専修大学から、当時の状況を振り返るとともに、被災後２年を経過した大学の現状とその間に検討・実施された災害対策について報告された。その後、本協会の大学情報システム研究委員会がまとめた業務分析ワークシートを用いて、災害時に備えた大学の情報システムの復旧の優先度やデータ保護についての個人研究、グループディスカッションを行った。特に、大学が守るべき重要情報資産について、二重化やバックアップ等の対策を大学間での協定・連携による実現やデータセンターの活用を踏まえた議論が行われた。

参加者のアンケートによると、それぞれのテーマについてほとんどの参加者が「理解できた／概ね理解できた」と回答している。一方で、所属校に持ち帰り対策を検討したい旨の記述も散見される。サイバー攻撃対策や災害対策をはじめ、情報セキュリティの重要性が理解されつつも、実践のためにはまだまだ余地が残されていることが浮き彫りになった。当コースとしても、今後の更なる改善と継続的な取り組みが望まれる。

文責：情報セキュリティ研究講習会運営委員会