情報セキュリティ　本学の事例と対応

企画・情報部　情報基盤課　セキュリティ対策掛
片　桐　　統

１．　はじめに

教育・研究・業務などの環境の電子化が発達するに伴い、その情報をいかに守るかという情報セキュリティも、大学の安定的な運営に非常に重要なファクターとなっている。個々の教職員の観点で見ても、ひとたび情報セキュリティインシデントに巻き込まれると、自身の業務に影響するだけでなく、最悪の場合は懲戒の対象となる可能性もある。

本講義では、情報セキュリティの予備知識を簡単に紹介した上で、京都大学の不正アクセス連絡体制を説明する。そして、本年度話題となっている標的型攻撃の概要、使用するPCのウィルス感染疑いが通知された際の対処手順と日常的に行っておくべき対策、セキュリティ事案の事例を紹介する。

２．　情報セキュリティの予備知識

情報セキュリティとは、「情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。」（ISO/IEC27001 より）となっている。機密性、完全性および可用性について、本学では情報セキュリティ対策基準において、表 **1** のように定義している。

表 1 機密性，完全性および可用性の定義

用語	定義
機密性	情報に関して、アクセスを認可された者だけがこれにアクセスできる状態を確保すること。
完全性	情報が破壊、改ざん又は消去されていない状態を確保すること。
可用性	情報へのアクセスを認可された者が、必要時に中断することなく、当該情報及び関連情報資産にアクセスできる状態を確保すること。

また、本学では情報セキュリティ対策規程において、機密性、完全性及び可用性に関し、「意図的又は偶発的に生じる、本学の諸規程又は法律に違反する事故若しくは事件」を、情報セキュリティインシデントと定義している。

３．　京都大学の不正アクセス体制

本学における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)やコンピュータウィルス、その他により被害が発生(以下「不正アクセス」という.)した場合の連絡体制は「コンピュータ不正アクセス対応連絡要領」

に定められている。連絡体制の概要を図 1 に示す。

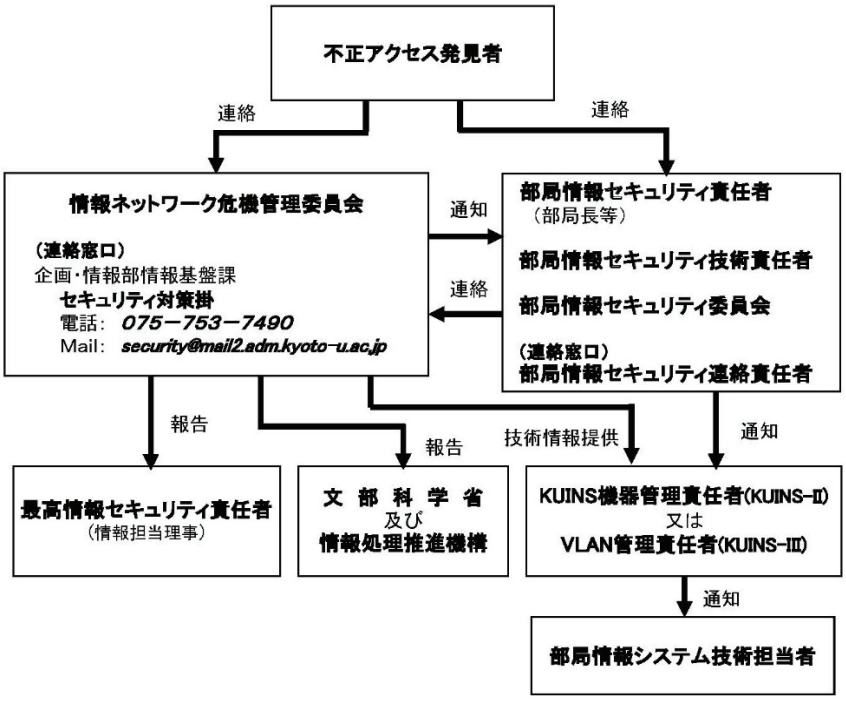

図 1

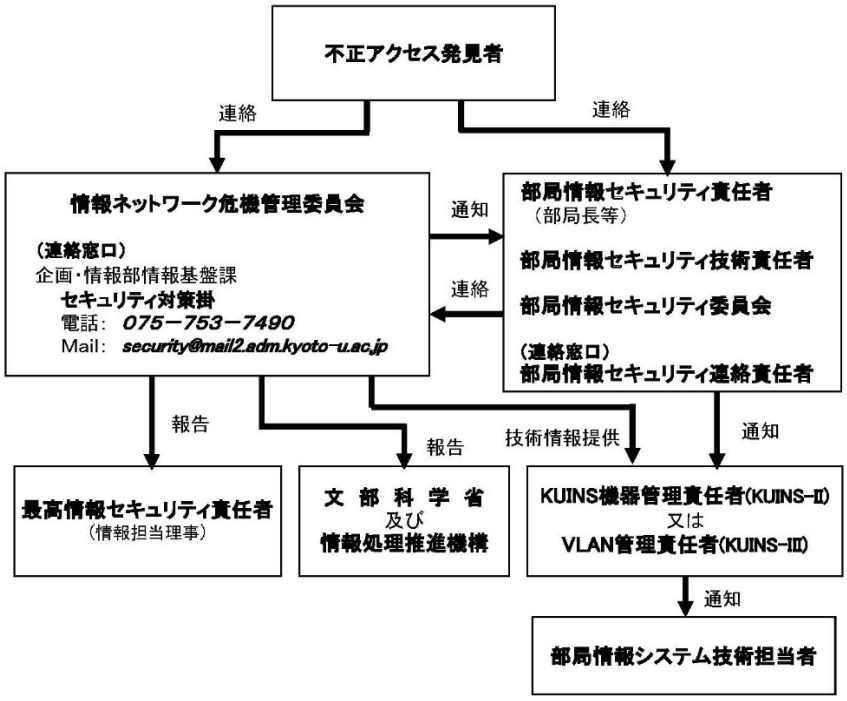

図 1 不正アクセス発生時の連絡体制

４． ウィルス感染疑いの安全確認への対処

本学に設置する IDS（侵入検知装置）での検知等、ウィルス感染の疑いがある場合、情報ネットワーク危機管理委員会の連絡窓口であるセキュリティ対策掛から部局に通知を行う。ウィルス感染疑いの通知を受け取った場合の対処は、一般的に以下の手順で

行う。複数名でお互いに確認しながら行うことを推奨する。

1） 機器の特定（VLAN 管理責任者）
2） 機器のウィルス対策ソフトウェアの定義ファイル更新（機器の使用者）
3） 完全スキャンの実施（機器の使用者）

ウィルス感染が確認されなかった場合
4） 情報ネットワーク危機管理委員会へ、ウィルス感染が確認されなかった旨を報告（VLAN 管理責任者等）

ウィルス感染が確認された場合
4） 部局情報セキュリティ連絡責任者へ報告（VLAN 管理責任者）
5） ネットワークケーブルを外す。無線 LAN の場合、機能を停止（機器の使用者）
6） PC 内に保存されている、個人情報・機密情報の確認
7） 可能であれば、感染経路（メール、WEB、USB など）の特定や、感染ファイルの特定と保存（VLAN 管理責任者）
8） 必要に応じて、OS のクリーンインストールを実施
9） 不正アクセス等報告書（ウィルス感染）提出

5． 日常的に実施が必要な対策

情報セキュリティインシデントに巻き込まれるリスクを低減するためには、パソコンの使用者は、日常的に以下の実施に注意を払う必要がある。

1） OS のアップデート、ウィルス対策ソフトウェアの定義ファイル更新、各種アプリケーションのセキュリティパッチの適用。
2） ID とパスワードの管理の徹底（パスワードガイドラインに準拠したパスワードの使用）。
3） 不用意にメールの添付ファイルを開かない。リンクをクリックしない。
4） 業務に無関係な WEB アクセスは行わない。
5） 他人から預かった USB メモリを使用する際は、まずウィルス対策ソフトでスキャンする。
6） 出所不明のフリーウェア等は使用しない。

6． 標的型攻撃とは

標的型攻撃とは、ターゲット（標的）を定めて、機密情報などを得るために、ターゲットに合わせて行う攻撃の総称である。また、標的型メールとは、サイバー攻撃の一種で、攻撃や機密情報漏洩などを目的として、特定の組織や個人を対象に送り付けられる電子メールである。一般的な標的型攻撃の概要を、

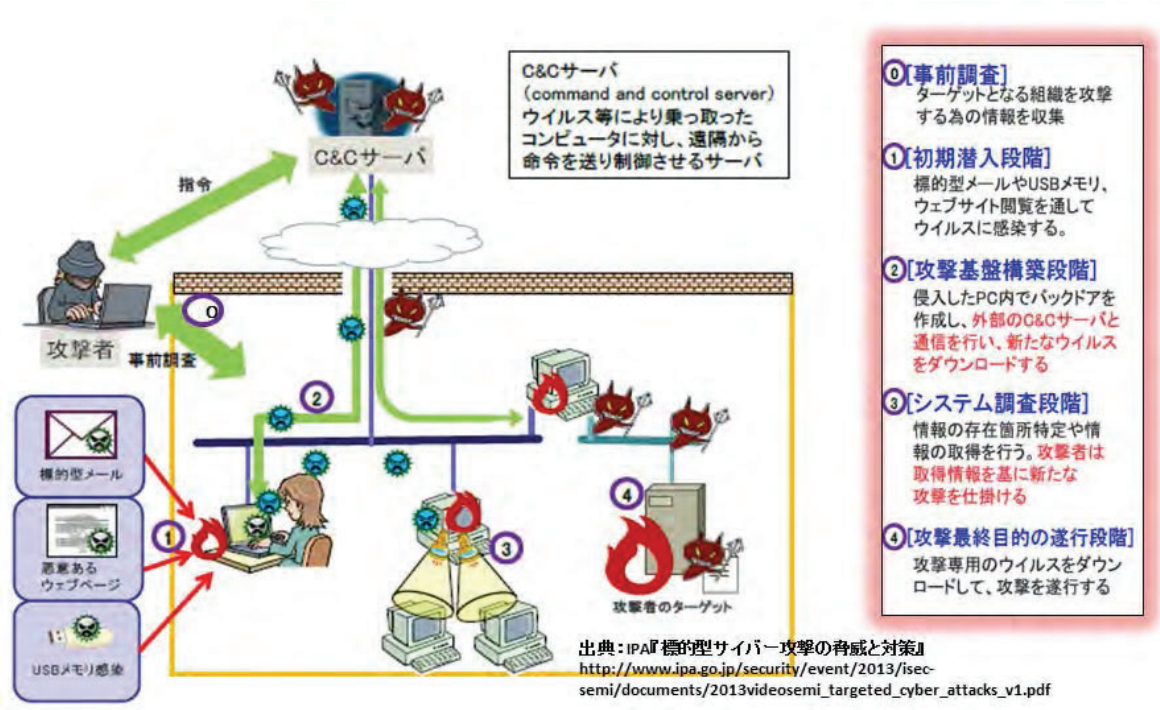

図 **2** に示す。

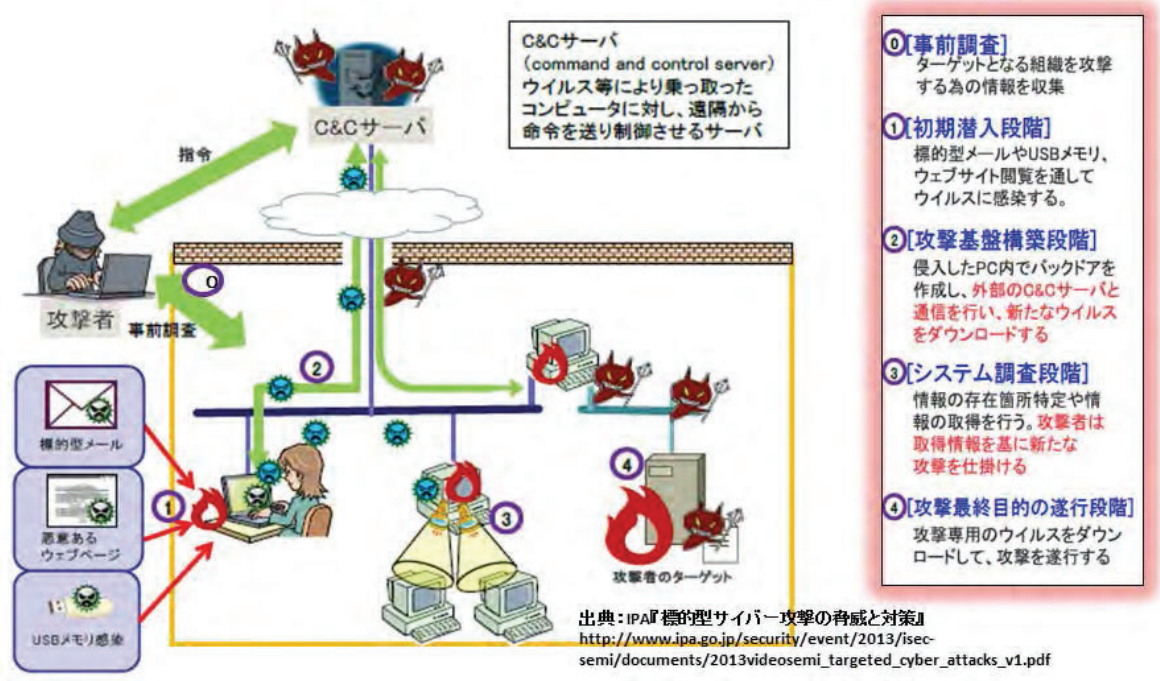

図 2 標的型攻撃の概要

7． 本学および他機関のインシデント事例

1） SPS-ID とパスワードが悪用され、全学メールから大量のスパムメールを送信された。（9 万通／1 時間）

2） Google Groups で、閲覧権限を適切に設定していなかったため、個人情報がイ

ンターネット上に公開された。

3） 他機関において、業務用 PC がウィルスに感染し、大量の個人情報が漏洩。

4） 他機関において、PC がマルウェアに感染し、業務用アカウントが流出。そのアカウントを悪用されて、大量の個人情報が漏洩した可能性。

8． おわりに

標的型攻撃に代表されるような攻撃は、ネットワークへのセキュリティ対策だけでは防ぎきれない。ユーザの日々の情報セキュリティに対する意識を向上することが重要となっている。

情報セキュリティの維持・管理について、より一層理解を深め、日頃から注意を払う必要がある。

『情報セキュリティ　本学の事例と対応』: 感想（抜粋）

・非常に分かりやすく、かつ話を聞き入ってしまう講義だった。
綺麗事ではない、実務レベルでの脅威を分かりやすく丁寧に解説されているので、セキュリティ対策として、情報を守るために何をすべきか、が分かりやすい。大学の組織の一員として、確実に守らなければと改めて思った。

・何かあった際に、いつでも相談できる人を事前に想定しておくことは必要だと感じました（セキュリティ問わず）

・質問形式で行われ最初の方は分かりやすかったが、その分時間を消費してしまい後半が端折り気味になったのが残念であった。情報セキュリティについて、これまで当たり前のように思っていた事が以外と知らなかったという事に気づかされた。

・メールが使えないとストレス貯まるとみたいに言われていたけれど、自分が一日中机に向かっている職場で無いので正直それはどうかなと思った。また、万が一ウイルスに掛かり秘密情報が盗まれても個人では盗まれたかわからないのは難しい問題だなと思った。何か対策ソフトがあればよいのにと思う。

・ウイルスなどに関してはある程度の知識を持っていたつもりでいたが、不正アクセスなどで侵入されたときに厳しい罰則が科されてしまうといったことに関しては知らなかったので今後もっと気をつけて対応をしていきたいと思わせる内容でした。プレゼンテーションも非常に上手で、飽きない講義でした。

・現在は専らユーザーだが、一時期サーバー管理者をしていたことがあり、今回の講義で久しぶりに管理者としての立場で物を考えることができたのはいい刺激になりました。
PC を使うことが当たり前となっているにも関わらず、ブラックボックス化が進んでいるためによりユーザーがより無頓着、無防備になっていっているのが気になります。
また、侵入者の悪意もエスカレートかつ高度化している割に、管理者の役割も責任も実態に合っていないように思います。このあたりの改善は必要なのでしょうね。

・情報セキュリティ。昔はそんな情報欲しい人はいないし、使い道もない。それが昔の考え方であったが、今では情報が外に漏れること自体が懲罰の対象になった。ボーナスが減る、昇進に響くなど一生を棒に振ることになる。そんなことが冒頭で述べられ『うーん』と考えてしまった。特に懲罰の実例としてウイルス感染で年金情報を漏えいしてしまった職員の話がなされ危機感を感じるようになった。というのも、もしウイルス感染したら自

分だけでなく組織全体のパソコンにも感染が拡大して大ごとになり、最後はその責任を取って自分自身が罰せられる、その実例ができてしまったと思ったからだ。そして、ウイルス感染したらどうしたら良いかということで考える時間が別途設けられ、当日に配布されたマニュアルに加えて各部局の最高責任者である所長に通報することが大事という結論で講義は終了した。なお、講義の途中で考える時間を別途作ったのは講師としてうまいなあとその時思った。講義をただ聞いているだけでは考えないからで、今後自分が何かプレゼンテーションをしなければならなくなった時は参考にしたいと思った。

・情報系から送られてくる情報はたいて難しく敬遠するけど、今回の講義は理解でしました。もう少し長時間講義してほしかった。

・毎年 e-learning を受講しているが今回の講義を聞いて情報セキュリティについて分かっていないことが多いことがよく分かった。今後も e-learning を積極的に受講するなどして知識を深めていきたいと思った。

・情報セキュリティ関連のお話を聞くことが時々ありますが、常に身近なことのような遠いことのような不思議な感覚になります。色々と対策は施すのですがどこか実感が伴わない感じがあります。

・e ラーニングなどで情報セキュリティーに関してはある程度知識はあるつもりであったが、改めて講義を聞くと忘れていることも多く再教育の場の充実の必要性を感じた。講義自体は演者のテンポの良い話やスピーカーに質問を振るなど楽しく聞くことができた。今後のプレゼンの参考にしたい。

片桐係長の講義