京都大学の情報セキュリティ対策について

2014年９月18日
京都大学　情報環境機構
斉藤康己

ゲーテの言葉

- 『一人一人が自分の家の前を掃けば、町中がきれいだ。』
- もとの言葉は：

「銘々自分の戸の前を掃け、
そうすれば町のどの区も清潔だ。
銘々自分の課題を果たせ、
そうすれば市会は無事だ。」

インターネットって何ですか？

- 世界の政治、経済、人々の日々の生活の全てを支える一番重要なインフラ！
- 何かに例えるとすると？
  - 道路交通網？ハイウェイ？
  - 私の答えは：

インターネットって何ですか？

- 世界の政治、経済、人々の日々の生活の全てを支える一番重要なインフラ！
- 何かに例えるとすると？
  - 道路交通網？
  - 私の答えは：
    - 昔、立花隆が「Global brain」と言っていた。
    - 体の中のネットワーク、神経系や血管系に例えられる。
    - 日々新陳代謝している。
      - RFCの改訂を繰り返して。
      - Programの総体も猛スピードで進化している。
    - ロバスト（強靭）で、もろいが、壊れにくい。
    - しかし、Bugや脆弱性は必ず入る。人間の弱さ？

「セキュリティ」って何ですか？

- 面倒くさくてできればやりたくないもの
  - インターネットの負の側面。
  - 昔はもっと「おおらか」だったのに．．．
- 交通規則のようなものか？
  → ちょっと違う．．．

規則というよりは、インターネットを快適に利用し、思わぬセキュリティ事故を起こしたり、事故に巻き込まれたりしないための、「安全運転の心得」のようなもの。

情報セキュリティの侵害から情報を守る事

情報を守ると言うことは：
情報資産の機密性、完全性、可用性を維持する事。

- PCがウイルスに感染して個人情報が漏出してしまった！（機密性の侵害）
- 外部からの不正アクセスにより大学のホームページが改竄されてしまった！（完全性の侵害）
- メールサーバが故障して電子メールが届かず仕事にならない！（可用性の侵害）

目次

1. はじめに
2. インターネットの基本的な考え方
   - 歴史
   - コンセンサス
   - ガバナンス
   - なぜセキュリティ・インシデントは増え続けるのか？
3. 具体的なセキュリティ・インシデントの紹介
4. 事例から得られる教訓
5. 京都大学のセキュリティを守る仕組み
6. 安全運転の心得（一人一人に実践して欲しいこと）

1．はじめに

- 今日、伝えたい事
  - インターネットは便利な道具。おおいに使いましょう。
  - セキュリティの脅威は交通事故のようなもの。
  - 危険の存在を知って、しっかり対処すれば怖くない。

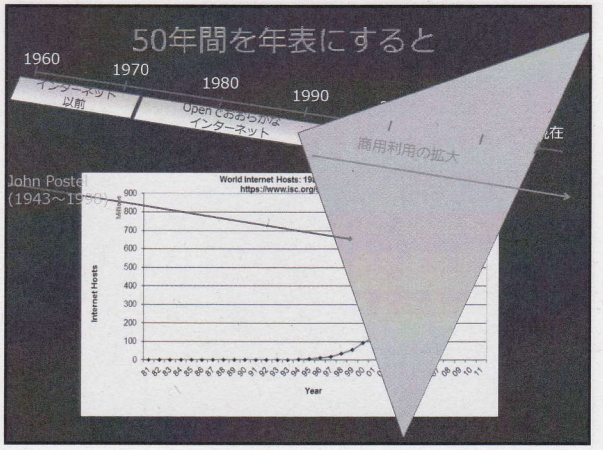
2．インターネットの基本的な考え方

- インターネットって何？セキュリティって何？
- インターネットの歴史
- インターネットの基本的な考え方
  - コンセンサス（はどう作られるか？）
- インターネットは誰のもの？
  - インターネット・ガバナンスの話
  - 悪者はどこにいるか？
- どういうセキュリティ・インシデントが増えているのか？
  - 愉快犯、金儲けのプロ集団、政治的目的の人

2－1：インターネットの歴史

- 大学中心の大らかでオープンなインターネットの時代。メールやTelnet、FTPの利用中心（1960年～1990年）
  - Paul BaranやDonald Davies: よるパケット通信の論文（1960年代前半）
  - 最初のRFC（Request for Comment）（1969年）
  - ARPANet開始（1969年）
  - Unixをベル研が開発（1969年）
- 商用利用の開始（1990年頃？）
  - 世界初の商用ISP（米国PSINet）（1989年）
  - 初めてのWebページ（WWW by Tim Berners-Lee@CERN）（1991年）
- 商用利用の急拡大（1995年～2005年）
  - Amazon(1995), Google(1998), Wikipedia(2001), Skype(2003), Facebook(2004), YouTube(2005), Twitter(2006), mixi(2004), LINE(2011)
- インターネットバブル（2000年）
- 世界中に利用が広がりセキュリティ事故だらけに？！（現在）

50年間を年表にすると



日本におけるインターネットの発展と歴史

- 古いドキュメントだが
  - http://www.soi.wide.ad.jp/class/20000001/slides/12/2.html参照。
- 日本ではUUCPでのバケツリレーネットワークからスタート。
- 今では：
  - https://www.nic.ad.jp/timeline/#jpnic
  - この年表は良くできているのでお勧め。

脱線：HackerとCracker

- 昔は私もHackerと呼ばれた…
- 'Hacker' by the Hacker's Dictionary :
  - A person who enjoys learning the details of computer systems and how to stretch their capabilities – as opposed to most users of computers, who prefer to learn only the minimum amount necessary.
- 'Cracker' by an old Dictionary :
  - Thin flaky, dry biscuit
  - Firework that makes cracking noises when set off
- Happy.exeの話で違いを述べると…

脱線：Happy.exeの話

- 古き良き時代（1984年頃？）の昔話。
- 99年に流行ったHappy99.exeとは別の話。
- 研究所で使っていたDEC2060という計算機は米国のAI研究者が良く使う計算機で標準でついてくるOSの中に<games>とか<unsupported>という名前のディレクトリがあり、その中にdungeonとか、山のようにたくさんのゲームプログラムがころがっていた。
- ある日、その中にhappy.exeという名前のファイルを発見。さっそく実行してみると…

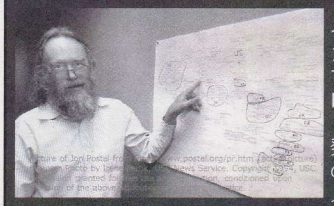
Happy.exeの話（続き）

- 「Delete *.*.*」を実行し始めた！
  - ✓これは現在のディレクトリの中の全てのファイルを削除するコマンド。
- 真っ青になって、Control-Cを連打するも、強制終了は受け付けられず、ただただ今までの努力の結晶である自分のファイルが削除されていくのを呆然と見守るのみ。
- はっと、気がついて「undeleteがある！」と思った矢先、計算機は「expunge」を実行しだした！
- 万事窮す！

Happy.exeの話（続き）

- と思ったら、「expunge」が終了してしばらく経った所で、茫然自失状態の私の目の前に：
  - ✓「ただいまあなたがご覧になったコマンドはどれも実際には実行されていません。どうです、Happyになったでしょう！！！」というメッセージが表示されて、おしまい。
- これには本当にハッピーな気分になった。
- ちょっと悪質なイタズラかもしれないが、実害は無く、ユーモアたっぷり。
- Hackerはこの程度のことはするが、それ以上の悪さはしない。それに対してCrackerは悪質。

John Postel



インターネットの父
1998年に突然亡くなるまで、この人が [redacted] だった！
RFCという仕組みを長年（30年！）に渡って維持・発展させ、インターネットの「やり方」を定着させた人。

ICANN = Internet Corporation for Assigned Names and Numbersは、
国際的な民間非営利法人。

= Internet Assigned Numbers Authority
インターネット上の共有資源：ＩＰアドレス、ドメイン名、プロトコル番号などを管理し、重複などが起こらないようにする役目を果たす。
2000年にICANNという組織にこの機能は吸収された。

2－2：インターネットの基本的な考え方

- オープンであること（Openness）、
- 自助の精神（Self Help）、
- 大まかな同意と動くコードによる実現（rough consensus and running code）、
- 自立分散で強靭なシステムなど（autonomous, distributed and robust system）
- 現在のインターネットは更に進化して…
  - 止まる事を知らない商用利用、BitCoinとか。

2－3：インターネット・ガバナンスとは？

- Internet Governance
  - Governance = 管理、制御、統治
  - 本来は「分散・自立システム」であるはずのInternetに管理や統治が必要か？
  - 管理しないと、どうしようもないリソースがある：
    - IPアドレス
    - ドメイン名
    - プロトコル番号、ポート番号、AS番号、MIB識別子

  などなど。
  - そもそもの発端は「ドメイン名紛争」。

インターネット・ガバナンスの基本

- Private Operation
- Bottom-Up Coordination
- Rough Consensus and running code
- Open and Transparent

- ICANNの運営の基本方針ともなっている。

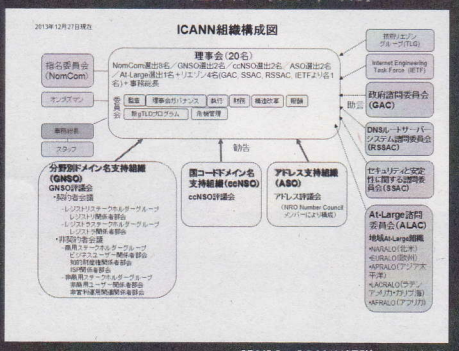
ICANNの役割

- IPアドレス空間の割り振り
- プロトコル識別子の割り当て
- gTLDおよびccTLDの名前システム管理
- ルートサーバのシステム管理

などを行う国際的に組織された民間非営利法人。

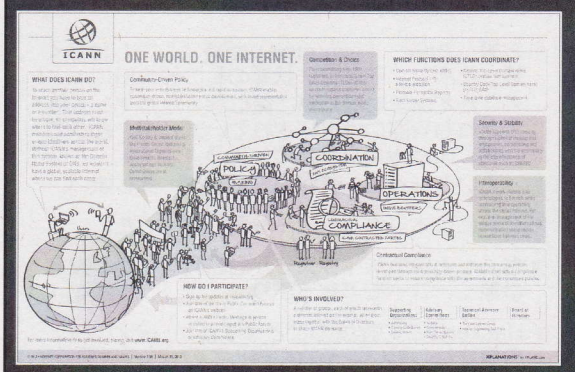
- https://www.nic.ad.jp/ja/icann/about/organization.html

ICANNの組織（日本流）

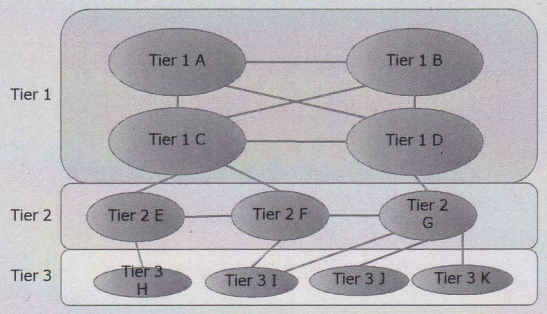


JPNICのICANN解説ページから

ICANNのイメージ図（米国流）



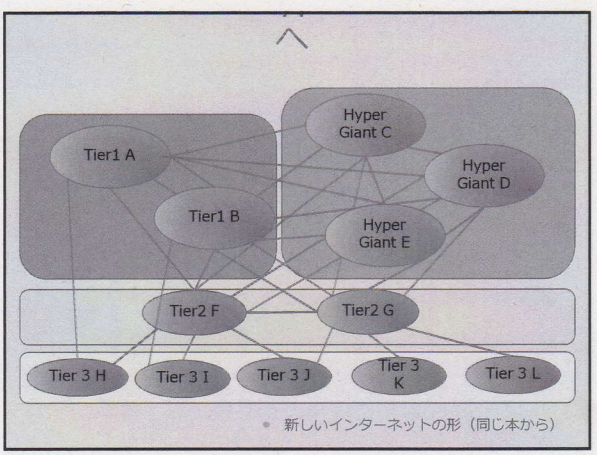
2－4：Internet全体のちょっと前までの構造



- あきみち、空閑洋平：「もろさが織りなす粘り強い世界 インターネットのカタチ」、オーム社、2011年、p.194から。

Hyper Giantsの登場

- Hyper Giants
  - ✓ Google, Facebook, YouTube (Google), Microsoft, Yahoo, Akamaiなど、Internet上で大きなトラヒックを発生させているプレイヤ
- 2010年でちょっと古いデータだが：
  - ✓ Google一社だけでインターネット全体の１割以上（数字は要確認！）のトラヒックを生成している！
  - ✓ http://www.arbornetworks.com/asert/2010/10/google-breaks-traffic-record/

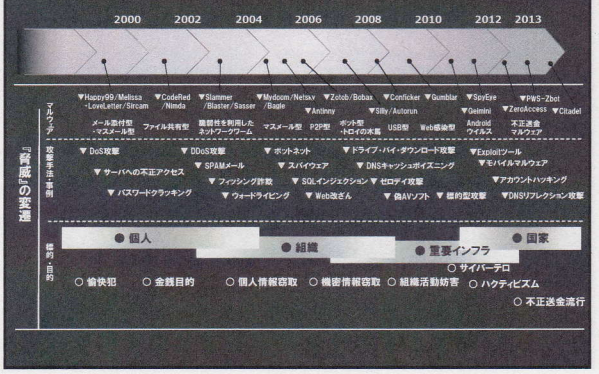


- 新しいインターネットの形（同じ本から）

2－5：どういうセキュリティ・インシデントが増えているのか？

- 昔は愉快犯
- 最近は：
  - 金銭目的のプロ集団
  - 政治的なプロパガンダ目的の行為
    - サイバーテロ、ハクティビズム

ネットワーク上の脅威の変遷年表



2－5：どういうセキュリティ・インシデントが増えているのか？

- 昔は愉快犯
- 最近は：
  - 金銭目的のプロ集団
  - 政治的なプロパガンダ目的の行為
    - サイバーテロ、ハクティビズム
- とりあえず、最近の具体例をいくつかみてみる事にしましょう。

3．具体的なセキュリティ・インシデントの紹介

1. 韓国大規模IT障害事件
2. ロリポップ（Word Press利用サイト）で不正アクセスによる改竄事件
3. BaiduIME Shimejiの情報送信問題
4. Adobeのアカウント情報流出事件
5. ゆうちゃん事件（パソコン遠隔操作事件）
6. ネットバンキング不正送金事件
7. LINEのアカウント乗っ取り事件
8. ベネッセの顧客情報漏洩事件

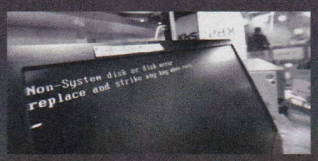
京大で実際に起こったインシデント

9. フィッシング詐欺
10. SPS-IDの漏洩、大量スパムメール送出事件
11. Google Groupで個人情報漏洩

3－1：韓国大規模IT障害事件

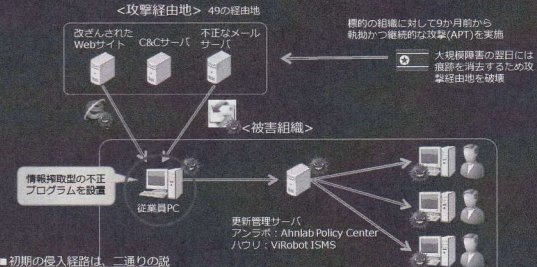
- 2013年3月20日午後2時(UTC+9)に、韓国の放送事業者(KBS, KMC, YTN)の社内イントラネット(通信網)とPC/サーバ、金融機関(新韓銀行 他)のATMに障害が相次いで発生。
- 原因は、PC/サーバへの不正プログラムの感染により起動障害、システム破壊が発生したためである。
- 金融機関のATMは3月20日午後4時に8割程度復旧し、9日後の29日に被害組織のシステムが完全復旧した。

韓国 大規模IT障害の概要



- 主要放送局と金融機関でPCとサーバ合計3万2千台が被害を受けた。
- 韓国合同対応チームは4月10日に攻撃元は北朝鮮の偵察総局と推定されると発表。

不正プログラムの侵入経路



■初期の侵入経路は、二通りの説
改ざんされたWebサイトに接続した従業員のPCが不正プログラムに感染(TrendMicro、F-Secure)
マルウェアが添付されたメールを開いた従業員のPCが不正プログラムに感染(Avast、IssueMakersLab)
■感染した従業員PCがウイルス対策ベンダの更新管理サーバに破壊型の不正プログラムを設置。
アンラボのAhnlab Policy Centerの認証バイパスの脆弱性を利用して不正プログラムを設置。ViRobot ISMSは不明。
■更新管理サーバ経由で組織内の様々なPC/サーバが破壊型の不正プログラムに感染。

この事例から見えてくる組織の課題

- 攻撃者/侵入経路の特定と対策方法の醸成は困難
- 集中管理サーバ全般のセキュリティ対策が必要
- 大規模なシステム破壊への備え
- 国のインフラを標的としたサイバー攻撃への備え
  - 攻撃者は、韓国のウイルス対策ソフトだけを停止するウイルスを作成。今回のサイバー攻撃では、[illegible]とし、[illegible]に及んだ。国として重要インフラ事業者のセキュリティ対策を推進する施策が必要である。
- 結局、[illegible]最初の侵入経路は個人のPCだった！
  - [illegible]

3－2：ロリポップ、WordPress利用サイトで不正アクセスによる改竄事件

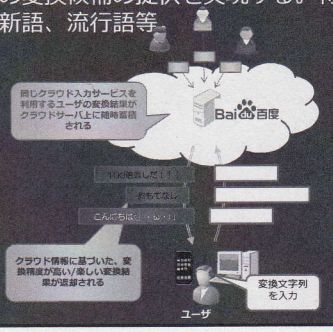
- 株式会社paperboy&co.（ペパボ）の個人向けレンタルサーバサービス「ロリポップ！」利用者のHPが8000件以上改竄された事件。
- http://internet.watch.impress.co.jp/docs/news/20130829_613274.html
- WordPressというCMSを利用していた。
- WordPressの脆弱性もあるが、ペパボの設定不備も原因。
- 植林した自然でない森林は脆弱（水害とか病気に対して脆い）というのに類似。

3－3：BaiduIME Shimejiの情報送信問題

- 2013年12月26日に、読売新聞・NHKがBaidu社の無料の日本語入力ソフト「Baidu IME」の情報送信の問題を報道。
- クラウド入力機能のBaidu IMEを利用して文字を入力すると、全角文字・変換結果等の入力内容がBaidu社(日本法人)のクラウドサーバに送信される点を指摘。
- NISCが、Baidu IMEを利用しないように各省庁に注意喚起を実施。Baidu IMEの利用状況の調査の結果、複数の官公庁・県・市・国立大学がBaidu IMEをインストールしていたことが判明し、アンインストールを実施。
- また、Baidu社の無料のAndroid向け日本語入力アプリ「Simeji」においても、同様の問題が存在していた。Simejiは、2013年8月時点で600万回のダウンロードが実施されている。

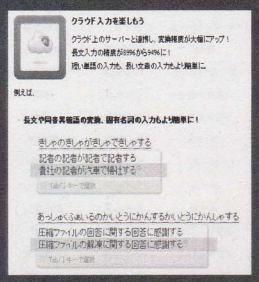
クラウド利用による高度なサービスの実現

- Baidu IME/Simeji などのクラウド入力IMEは、クラウドサーバと通信を行い、高精度な変換、大量の変換候補の提供を実現する。特に、顔文字、新語、流行語等。

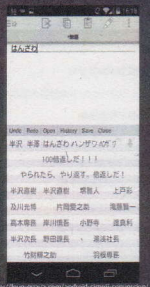


Baiduの入力変換例

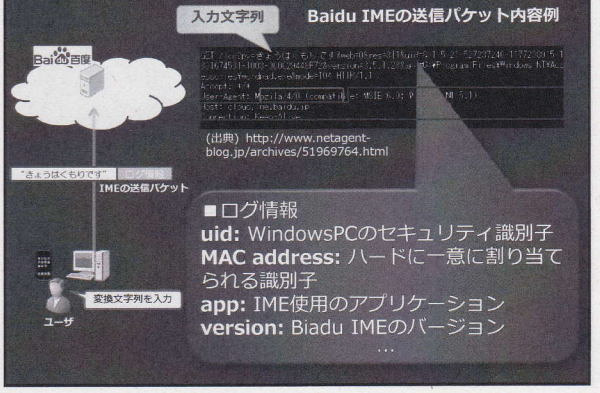
Baidu IME 入力変換例



Shimeji 入力変換例

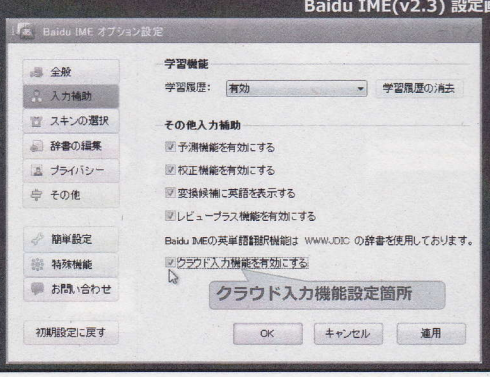


Baidu IME/Simejiの問題点(情報送信方式)

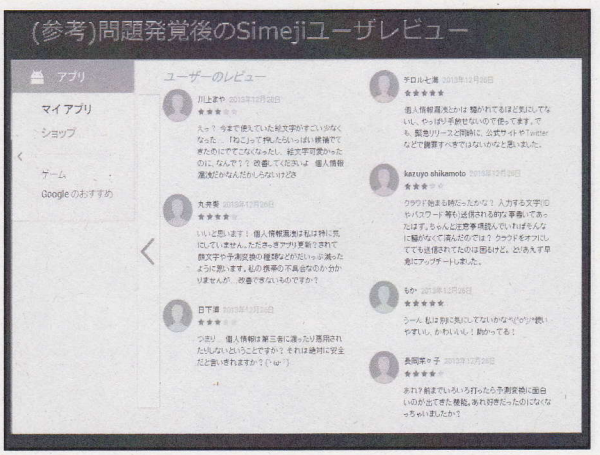


Baidu IME/Simejiの問題点 (デフォルト設定とユーザ同意の確認)

Baidu IME(v2.3) 設定画面



(参考)問題発覚後のSimejiユーザレビュー



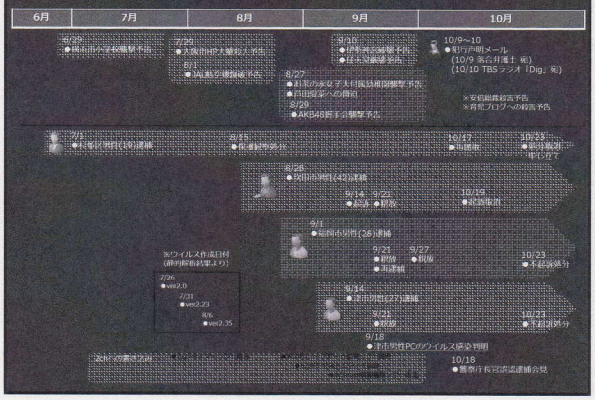
3－4：Adobeのアカウント情報流出事件

- 昨年10月頃、Adobe社の顧客情報流出
  - Adobe社の公式HPでの説明（日本語）
  - http://blogs.adobe.com/japan-conversations/%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E9%87%8D%E8%A6%81%E3%81%AA%E3%81%8A%E7%9F%A5%E3%82%89%E3%81%9B/
  - Brad Arkin CSOの英語のページでは：
  - http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html
- よくある、危ないパスワード
  - Adobeからユーザ情報が漏洩した後（昨年10月頃）のニュース記事から：
  - http://www.itmedia.co.jp/enterprise/articles/1311/06/news040.html

3－5：ゆうちゃん事件（パソコン遠隔操作事件）

- 2012年6月末～9月にかけて、インターネットを通じた襲撃・殺害予告が次々に発生し、東京都・大阪府・福岡県・三重県の4人が逮捕される事件が発生。
- その後、4人のパソコンが遠隔操作ウイルスに感染しており、実際には第3者にパソコンが乗っ取られ、踏み台として使われて、襲撃や殺人などの犯罪予告の書き込みが遠隔操作により行われていた事が判明。
- 4人は釈放されたが、真犯人は見つからず。
- 2013年に入り、真犯人を名乗る者からの「江ノ島の猫にチップを預けた」メールをきっかけに片山祐輔被告が逮捕される。
- しかし、片山被告は１年以上犯行を否定し続け、2014年裁判が始まっても裁判の行方は不透明だった。
- 2014年5月16日に真犯人を名乗る者からのメイルをきっかけに事件は急転直下、片山被告が「全て自分がやりました」と言って犯行を認めた。

事件の経過・時系列（2012年）



犯行予告

<犯行声明で関与が記載された犯行予告事件>

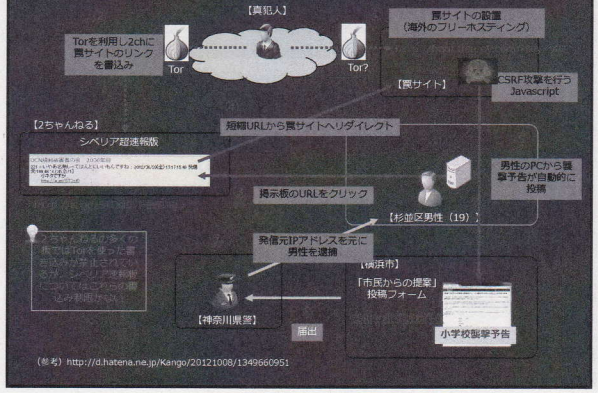
	日時	犯行予告対象	遠隔操作の対象	犯行予告先	手法	捜査担当
1	6月29日	横浜市 市立小学校襲撃予告	杉並区男性(19)	メールフォーム	CSRF	神奈川県警
2	7月29日	大阪日本橋 大量殺人予告	吹田市男性(42)	メールフォーム	ウイルス	大阪府警
3	7月29日	皇居ランナー大量殺人予告	〃	不明	ウイルス	届出なし
4	8月1日	日本航空機爆破予告	〃	メールフォーム	ウイルス	警視庁
5	8月9日	コミックマーケット大量殺人予告	愛知会社員	2ちゃんねる	ウイルス	不明
6	8月9日	天皇陛下殺害予告	〃	2ちゃんねる	ウイルス	不明
7	8月27日	お茶の水女子大付属幼稚園襲撃予告	福岡市男性（28	メール	ウイルス	警視庁
8	8月27日	芸能プロダクション脅迫	〃	メール	ウイルス	警視庁
9	8月27日	学習院初等科襲撃予告	〃	メール	ウイルス	届出なし
10	8月27日	部落解放同盟襲撃予告	〃	メール	ウイルス	届出なし
11	8月29日	AKB48握手会襲撃予告	〃	2ちゃんねる	ウイルス	警視庁
12	9月10日	伊勢神宮破壊予告	津市男性(27)	2ちゃんねる	ウイルス	三重県警
13	9月10日	任天堂本社破壊予告	〃	2ちゃんねる	ウイルス	三重県警

（参考）http://d.hatena.ne.jp/Kango/20121008/1349660951　※水色部分は犯行声明で明らかになったもの

その後の経過・時系列（2013年以降）

- 2013年1月1日と5日、複数の報道機関等へ以前と同じメールアドレスからメールが届く。
- 2013年1月5日のメールでは、「江ノ島にいる猫にソースコードや犯人の主張を記録したチップを預けた」と記述があり、捜査は急展開。
- 2013年2月10日、片山被告が威力業務妨害容疑で逮捕される。
- 片山被告は犯行を否認し続け、2013年3月3日一旦釈放されるも、警察は数回の再逮捕を繰り返す。
- 2014年3月5日、ほぼ1年ぶりに片山被告が保釈される。
- （さて裁判はどうなるかと皆が注目していると．．．）
- 2014年5月16日、真犯人を名乗る者からのメールの発信をきっかけに、この発信に使われた携帯電話が荒川河川敷から回収され、保釈が取り消され、片山被告は東京拘置所へ。
- 2014年5月22日の公判の罪状認否にて、「全部事実で、すべて自分がやった」と告白。

CSRFの犯行手口（横浜市のケース）

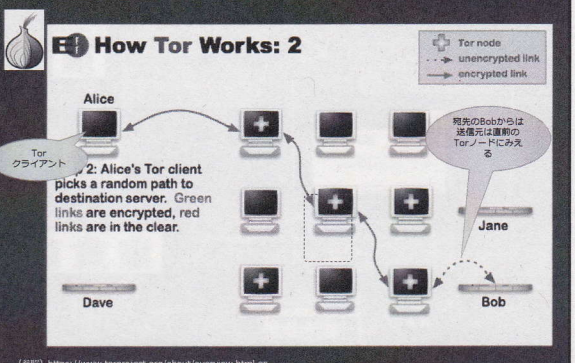


（参考）http://d.hatena.ne.jp/Kango/20121008/1349660951

事件からみる課題など

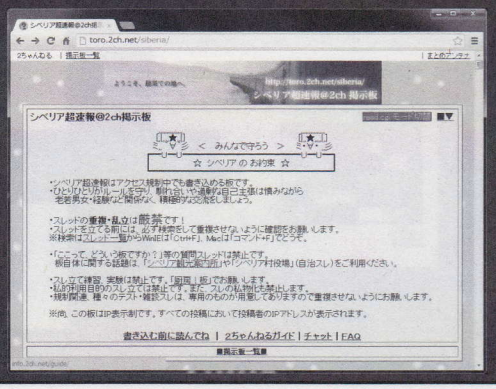
- ネット犯罪における　　の危険性。
  　　の限界、サイバー犯罪捜査の課題が浮き彫りに。
  「犯行声明」が出されなかったら、逮捕された人たちの冤罪を晴らすことができたのか？
- サイバー犯罪の取り締まりのあり方。
  　　密室での取り調べ。
- なりすましによる犯罪予告ーこれまでにないタイプの犯罪
  だれでも　　・　　になる恐怖
- 遠隔操作ウイルスは
  マルウェアの世界では目新しいものではなく、バックドア型やトロイの木馬に分類されるもの。
  「シマンテック」によると、昨年１年間に世界中で作られた遠隔操作ウイルスは　　に上る。（出典）
  http://mainichi.jp/select/news/20121029k0000m040162000c.html
- 被害を生まないための個人の　　も必要。

（参考）Tor「The Onion Router」



（参照）https://www.torproject.org/about/overview.html.en

（参考）シベリア超速報@2ch掲示板



警察庁からの注意喚起

出典：http://www.npa.go.jp/cyber/warning/

遠隔操作ウイルスの被害に遭わないために！

○ パソコンのＯＳを含むプログラムを最新の状態にアップグレードしましょう。
○ あやしいサイトにアクセスしないようにしましょう。
○ 信頼のおけないプログラムをダウンロードしないようにしましょう。
○ ウイルス対策ソフトを必ず導入し、最新の状態にアップデートしましょう。
○ ファイアウォールの設定をしましょう。

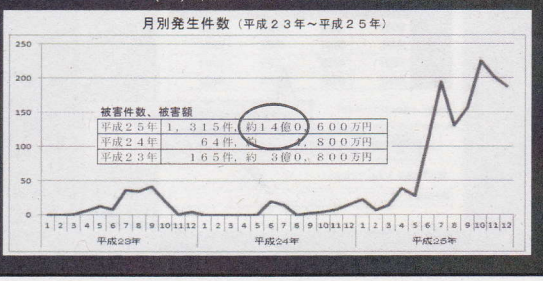
３－６：ネットバンキング不正送金事件

- 2013年6月以降、国内においてネットバンキング不正送金事件多発。
- 預貯金が勝手に送金される被害が１～１１月に　　
- 不正送金の件数が2013年６月に急増して以降、６月１１１件、７月１９４件、８月１３０件、９月１５０件と高い水準で推移している。被害額は６月に約９５８０万円、７月以降は１億円を超え続けており、「異常な増え方」。
- 増加の背景として、個人情報詐取目的のマルウェア　　等の流行があると見られており、マルウェアに感染した顧客のパソコンから顧客が気付かないうちにＩＤ、パスワード、取引ごとに使い捨てで利用する「ワンタイムパスワード」等を詐取しているものとみられている。

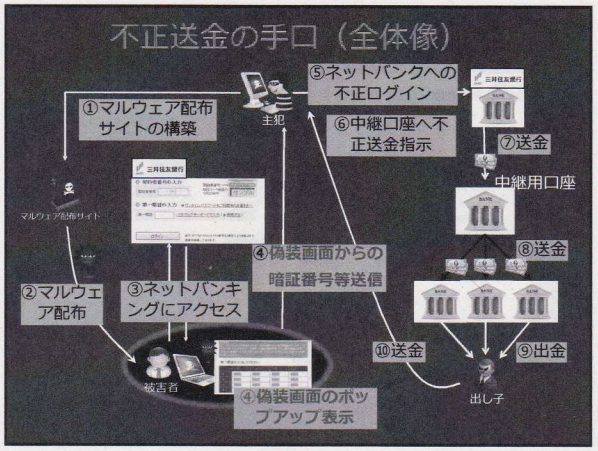
被害発生状況(2014年4月警察庁発表)

- ネットバンキングに係る不正送金被害（警察庁）
  - 犯行等の状況
    - 被害口座は個人名義がほとんど。
    - 被害口座に係るパスワード等を入手する方法は、

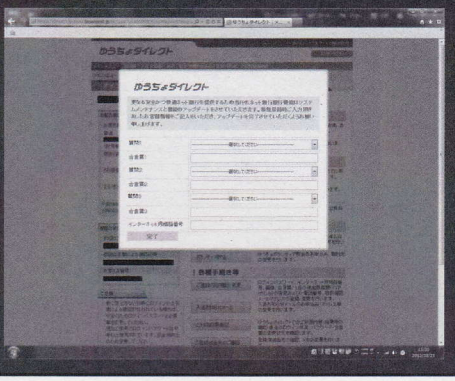
(出典) http://www.nikkei.com/article/DGXNZO71282200W4A510C1CR8000/



不正送金の手口（全体像）

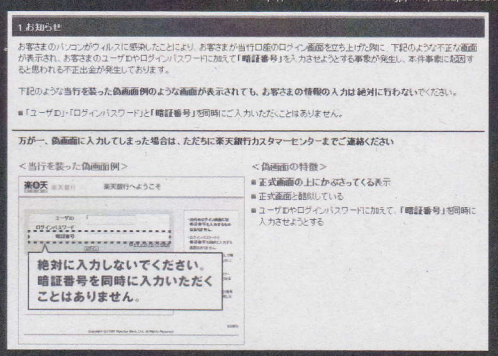


偽装ポップアップ画面例（ゆうちょ銀行）

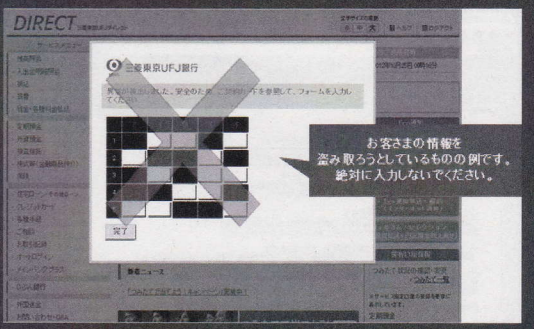


偽装ポップアップ画面例（楽天銀行）

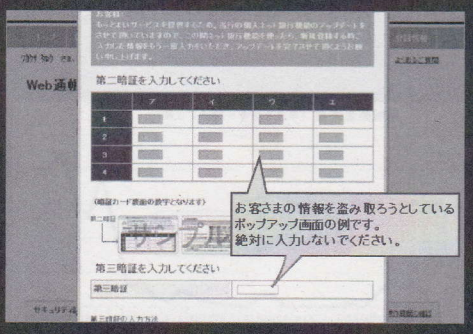
出典：http://www.rakuten-bank.co.jp/info/2012/121030-2.html



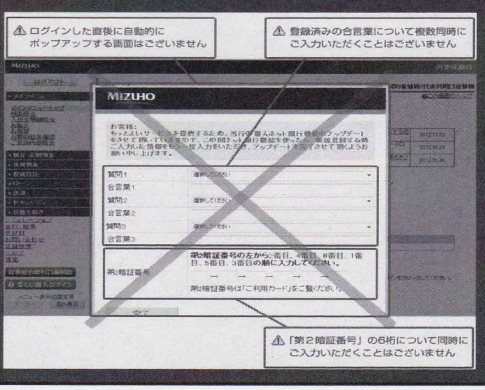
偽装ポップアップ画面例（三菱東京UFJ）



偽装ポップアップ画面例（三井住友）



偽装ポップアップ画面例（みずほ）



オンライン銀行詐欺ツールの流行

出典：
2013/7/23 トレンドマイクロ セキュリティブログ
http://blog.trendmicro.co.jp/archives/7547

7月 23

オンライン銀行詐欺ツール「Citadel」：日本での被害増加を確認、国内で2万台以上の感染

by シニアスペシャリスト 岡本 勝之

(2 投票, 平均値/最大値：4.00 / 5)　ブックマークへ追加　3 users　この記事を印刷

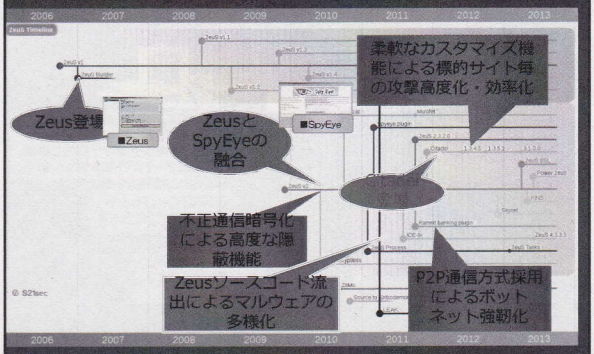
トレンドマイクロの脅威調査組織である「Forward-looking Threat Research(FTR)」では、さまざまな調査を行っていますが、その調査の中で、日本での被害が 96%以上をしめるオンライン銀行詐欺ツールの攻撃キャンペーンを確認しました。オンライン銀行詐欺ツールとは、オンライン銀行口座のID/パスワードによる金銭詐取を最終的な目的とするマルウェアプログラムの総称です。現在では、正規オンライン銀行Webページ上で各種認証情報の入力を促すためのポップアップ表示や、情報を盗聴する手口が中心となっています。日本に特化したオンライン銀行詐欺ツールの攻撃については、2012年10月29日のブログ記事、2013年2月14日のブログ記事、「2013年第1四半期セキュリティラウンドアップ」などで触れていますが、今回確認された攻撃は、その後も継続して日本を狙う攻撃が拡大傾向にあることを示すものと言えます。

この攻撃で利用されたオンライン銀行詐欺ツールは「Citadel」ファミリ(「TSPY_ZBOT」などとして検出)です。これらのツールが詐取情報をやりとりする際に使用の C&Cサーバは、現時点でだけでも、9つの IPアドレスを特定しており、地理的ロケーションでは、アメリカなどに分散していました。これらの C&Cサーバについてアクセス状況を監視したところ、アクセス元の96%以上が日本からのものと確認されました。この C&Cサーバへのアクセス発生は、既にユーザ環境に感染したオンライン銀行詐欺ツールの存在を示すものであり、感染被害のほとんどが日本国内で発生していることを意味します。

また、これらの C&Cサーバへアクセスするオンライン銀行詐欺ツール検体とその設定ファイルの解析から以下のことが確認できました。

- 情報詐取対象の 6つの金融機関はすべて日本国内のものであり、アクセス元の情報と併せて日本のみを狙った攻撃であることが明らかと言える
- 金融機関以外にも、Gmail、Yahooメール、Windows live(Hotmail)など、有名 Webメールも情報詐取対象となっている

個人情報詐取マルウェア(開発ツール)の変遷

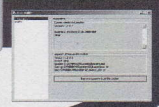


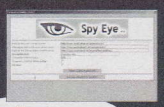
(出典) S21sec http://securityblog.s21sec.com/2013/11/zeus-timeline-i.html

個人情報詐取マルウェア(開発ツール)の変遷

キーロガー、画面キャプチャ等の情報詐取機能を持つ。
2011年5月にソースコードがネットに流出し、亜種マルウェアが一気に拡大した。

Zeus





SpyEye

後継ツール→機能の進化

Zeusとならぶ代表的な個人情報収集マルウェア作成ツールキット。中間者(MITB)攻撃の機能等を提供。

Citadelは自身の**高度な隠蔽化機能**を持つほか、「ダイナミック・コンフィグ」機能を含む**高度なボットネット管理・制御機能**を持つなど、従来のマルウェアに比べさらに洗練度が増しているという。
また、本ツールはアンダーグラウンドにおいて強固な開発環境・サポート体制を持っていると見られており、急拡大の一因に結び付いていると見られている。

Citadelの流行

CitadelはZeusを元に開発されたマルウェア開発ツール。口座情報を詐取するために多く利用されている。海外においては欧米を中心に既に500万台以上のPCへ感染、90カ国以上で5億ドル以上の被害が発生しているという。

Citadelの感染拡大状況

出典: http://www.mcafee.com/us/resources/white-papers/wp-citadel-trojan.pdf

オンライン銀行詐欺ツールの急増

オンライン銀行詐欺ツールの被害を受けた国：トップ 10

国名	割合
米国	23%
ブラジル	16%
日本	12%
インド	6%
オーストラリア	3%
フランス	3%
ドイツ	2%
ベトナム	2%
台湾	2%
メキシコ	2%
その他	29%

TrendLabs 2013 年第 3 四半期セキュリティラウンドアップ

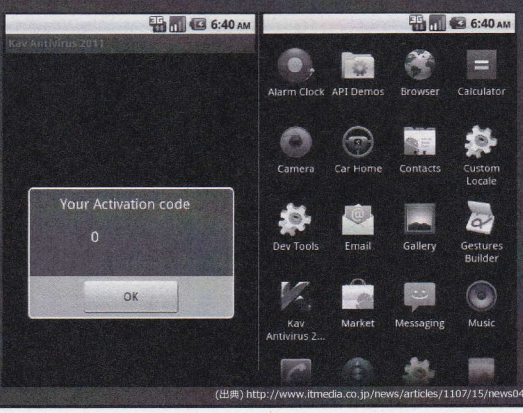
サイバー犯罪

オンライン銀行詐欺ツールがスパムメール経由で最も拡散された不正プログラムに

米国とブラジルが、オンライン銀行詐欺ツールによる感染被害が最も多い国内としてランクインしています。一方、日本が前四半期の第 5 位から今四半期は第 3 位に上昇しています。これは、主に不正プログラム「Citadel」の感染増加に起因しています。

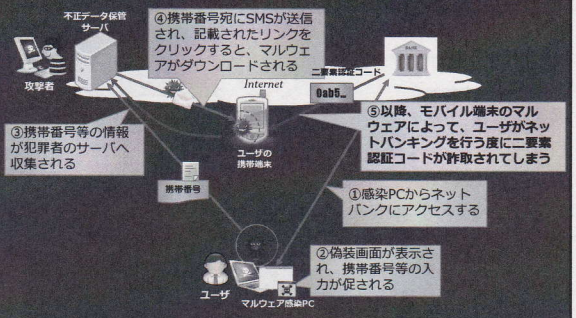
(出典) TrendLabs 2013 第3四半期セキュリティラウンドアップ

スマートフォンで動作するZeus



(出典) http://www.itmedia.co.jp/news/articles/1107/15/news046.html

海外で発生している モバイルマルウェアを利用した不正送金の例



PCと同様に、携帯・スマホのセキュリティ対策も重要である。

3－7：LINEのアカウント乗っ取り事件

2014年6月27日のLINEのブログでの正式アナウンスは：

- http://official-blog.line.me/ja/archives/1004331596.html
- いわゆるID、PWの使い回しが原因との記述。

- 乗っ取りの多発を受けてのニュース：
  - http://weekly.ascii.jp/elem/000/000/230/230157/
  - ユーザ向けに対策を親切に解説してある。

3－8：ベネッセの顧客情報漏洩事件

- 2014年7月9日、ベネッセコーポレーションは、760万件の顧客情報が外部に漏洩した事を確認したと発表。
  - 発表文は以下：
  - http://www.benesse-hd.co.jp/ja/about/release_20140709.pdf
- 2014年7月17日、内部犯行であることが判明し、下請け業者のSEが逮捕される。
- 持ち出された件数は2260万件に上り、ベネッセは顧客への金銭補償に200億円の原資を投入する考えを示した。
  - http://www.tsuhanshinbun.com/archive/2014/07/post-1914.html

3－9：京大の事例から：フィッシング詐欺の被害

- 2012年度に4回の大規模な攻撃があった。次第に巧妙化。
  - 2012年5月、8月、12月、2013年1月。
  - 1月の攻撃では学生用メール(KUMOI)そっくりの画面でECS-IDとパスワードの入力を要求。パスワードを奪取された例があった。具体的な被害は未確認。
  - 他大学ではパスワードを奪われSPAM発信などの踏み台に利用された事例も発生！

3－9：フィッシングメールと偽造HPの例

- フィッシングメールの件名と本文　(2012年8月に実際に送られて来たメール)

Subject:　UNIVERSITY OF KYOTO
本文：
弊社のセキュリティシステムは，誰かがあなたの許可なく電子メールアカウントにアクセスしようと示している,あなたのアカウントへの侵入に気づいた．我々は原因でこの問題にあなたのアカウントへのアクセスを制限しました．あなたは，あなたのアカウントを確認することをお勧めします．あなたのアカウントを確認するには，
ログインしてください．
<http://xxxxxxx.com/kyotoforum>
ありがとうございました
システム管理者だけです．

3－10：SPS-IDの漏洩、大量スパムメール送出事件

- 2013年8月13日、全学メイルの高負荷状態が発生しました。原因は一人の教職員のSPS-IDが何らかの手段で盗まれたこと。
- それを使って、あるメールサーバが踏み台にされ、大量のスパムメール（25通/秒、9万通/1時間）が流されたためでした。
- これは京都大学全体の1日のメイル処理量の約１０分の１に当たる多さです！遮断しなければ、メイルサーバがダウンする危険性もありました。

3－11：Google Groupで個人情報漏洩事件

- ある部局でGoogle Groupを情報共有に利用。閲覧できる人をメンバ限定とする設定をしていなかったために、個人情報等が誰でも見える状態になっていました。それを外部から指摘され、2013年8月24日付けの新聞等にも取り上げられました。
- その後全部局への調査を昨年9月初旬に実施し、110部局中17部局で業務上の機密情報をGoogle Groupで実際に扱っていることが判明。その内3部局が外部からも内容が見える状態であった（対処済み）。

4．事例から得られる教訓

- 事例から得られる教訓
- 穴（脆弱性）はどこにあるか？
  - 個人、組織、NW、PC、スマホ？
- なぜ、セキュリティ・インシデントは起こり続けるのか？（増え続けるのか？）
- どうすればセキュリティ・インシデントを防げるか？（被害に会わずに済むか？）

4－0．事例から得られる教訓

- 3－1：韓国大規模IT障害事件：
  - 最初は1人のPCから。
- 3－2：ロリポップ、Word Press利用サイトで不正アクセスによる改竄事件
  - インターネット上のサービスが安全とは限らない。
- 3－3：BaiduIME　Shimejiの情報送信問題
  - 善意のサービスも時として悪さをする？
  - 要は使い方次第。
- 3－4：Adobeのアカウント情報流出事件
  - Passwordは丁寧に作ろう！
- 3－5：ゆうちゃん事件（パソコン遠隔操作事件）
  - 人間が悪さをしている。
- 3－6：ネットバンキング不正送金事件
  - やっぱりお金が目当て！
- 3－7：LINEのアカウント乗っ取り事件
  - Passwordの使い回しが原因？
- 3－8：ベネッセの顧客情報漏洩事件
  - 人間が穴だということ。

4－0：京大の事例から得られる教訓

- 3－9：フィッシング詐欺の被害
  - メールに注意！
- 3－10：SPS-ID漏洩
  - IDとパスワードは大切！
- 3－11：Google Groupで個人情報漏洩
  - デフォールトをチェックしよう！
  - 何が、誰に見えるか？をいつも意識。

4－1：穴（脆弱性）はどこにあるのか？

- 個人
- PC
- NW
- システム
- 組織

4－2：なぜセキュリティ・インシデントは起こり続けるのか？

- ソフトウェアには必ず脆弱性がある。
- そして、インターネットの世界にそれを利用する悪い連中（Cracker）が居る限り、
- 無くならない．．．

ソフトウェアの脆弱性は？

- 想定外の使われ方をした場合に、想定外のかつ良からぬ動きをしてしまうコードの部分を「脆弱性」と言う。
- バグとは違うが、ほとんどのソフトウェアは何らかの脆弱性を含んでいると考えるべき。
  - →人間の弱さに起因
- だから、バグも脆弱性も無くならない！

人間八則（Law of Man）

by 高橋秀俊

人間は…

きまぐれ	whimsical
なまけもの	lazy
不注意	careless
根気がない	no patience
単調をきらう	hate monotony
のろま	dull
論理的思考に弱い	weak in logical thinking
何をするかわからない	unpredictable

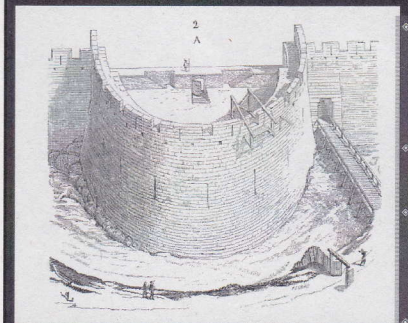
4－3：どうすればセキュリティ・インシデントを防げるか（被害に会わずに済むか）

4－4：ネットワークセキュリティ対策は危機管理の一部

- リアルワールド(現実世界)でやっている危機管理と考え方は同じ。
- HRO、High Risk Organizationを見習って。
  - 金融の例
  - 原子力発電所（東日本大震災の例）。
- ReactiveとProactive
  - 危機を認識する。
  - 危機発生時の被害を予測し、危機に陥らないよう対策を実施する。
  - 危機に陥った時は状況を分析し、最小限に被害を押える措置を講じる。
  - 危機から最短で復旧する方法を考える。

5．京都大学のセキュリティを守る仕組み

5－2：企業でセキュリティを守るモデルは城塞型

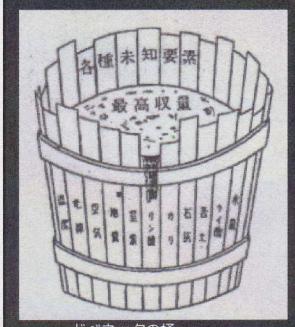


- 城塞型（企業型）：
  - 外壁で外からの攻撃を防御。
  - 中からできる事も制限される。
- 城塞型は完璧か？
  →
- メイルとWebの出入り口は開けておかざるを得ない。ウィルスでも何でも、全てそこから入って来る。
- それを最初に迎え撃つのは結局「個

京都大学のセキュリティを守るモデルは？

- セキュリティは、「自ら守る！」のが基本。
- 組織はそれをサポートする。
- ゲーテ型（大学型）：
  - 大学のNWは、（セミ）オープンなNW。
  - 個々のユーザが自分で注意する。
- 京都大学は

5－3：水は低きに流れ．．．



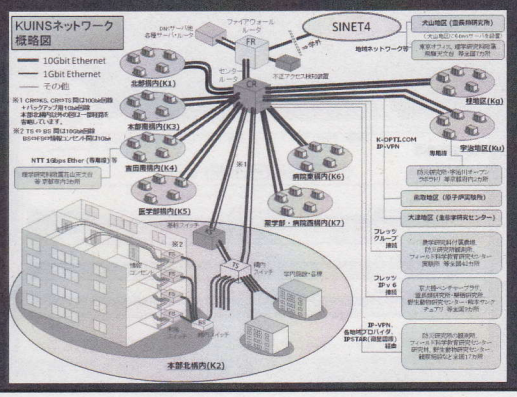
ドベネックの桶

- ある組織全体の「セキュリティのレベル」はその組織の中で　　！
- つまり、一人一人のセキュリティレベルが全体のレベルを決めてしまう！
- さらに、インターネットはものすごい　　なので、一人でも穴を開けてしまうとオオゴトに！

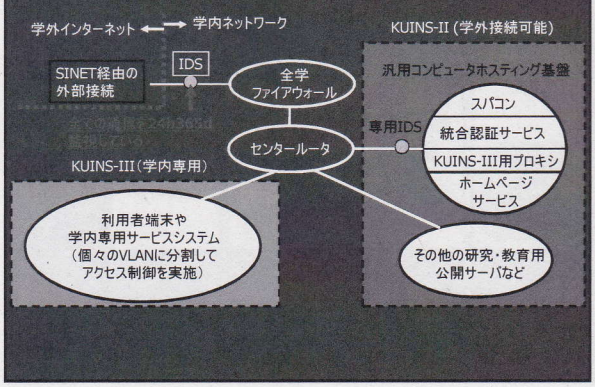
5－4：京都大学の全学情報システムとNW

- システムの規模：
  - 統合認証システム（ICカードとその機能の実現）
    - 教職員（SPS-ID）：
    - 学生（ECS-ID）：
  - （京都大学の学内ネットワークの略称）。
    - Kyoto University Integrated Information Network System
    - 隔地接続: 91箇所 / 情報コンセント数:
    - KUINS-II（学外向けサーバなどで使用）
      - IPアドレス: 約2550 / サブネット数: 約360
    - KUINS-III（学内端末で使用，外部はプロキシ経由）
      - VLAN数: 約4250
      - 無線LANアクセスポイント数：

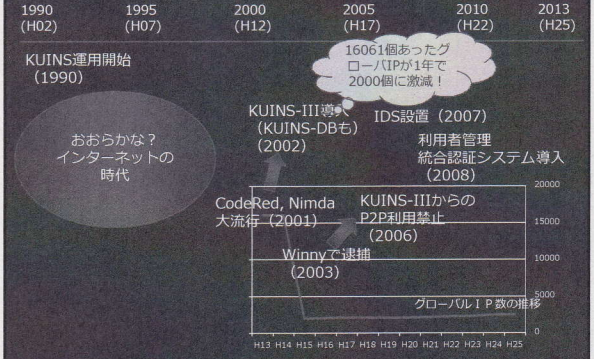
5－5：KUINSネットワーク



5－6：KUINSネットワークのセキュリティ監視

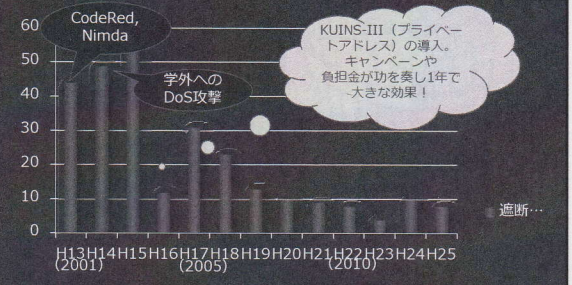


5－7：KUINSのセキュリティ対策の歴史



5－8：危機管理委員会による通信遮断件数の推移

- 京都大学では、学外に大きな影響を与えるインシデントや学内に影響が広がる恐れのあるインシデントに対して、緊急措置として通信の遮断を行って来た。その経年推移を見ると：



5－9：NWセキュリティは頑張って確保している

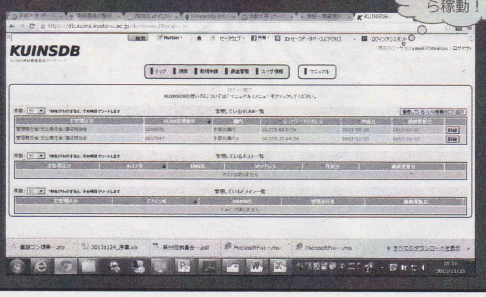
- KUINS-III（プライベートアドレス利用）の導入が大きな効果を発揮。
- 同時に、各居室へのVLANによる情報コンセント設置でインシデントの影響範囲を小さくした事も重要。
- 情報コンセントは全部で32000個。
- KUINS-III VLANは4250個。
- KUINSDB（次頁）も威力を発揮！
  - インシデント発生時も対策が容易に。
- 現在ではグローバルアドレスは１２年前の約1万6千個から約2500個（1/5以下）に激減した。


情報コンセント

5－10：KUINSDBも威力を発揮！

- KUINSDB（KUINS接続機器登録データベース）は、VLAN・ホストの登録申請や、機器・IPアドレス・情報コンセントの管理を行うためのシステム。
- 単なるDBではなく、利用申請、設定変更、承認の手続きや、利用するネットワーク・機器の管理を全てWebブラウザ上で行うことが出来る。
  - DBと実際の設定との齟齬を防止。

2003年から稼動！



5－11：京都大学全体のルールと仕組み

Policy　Standard　Procedure

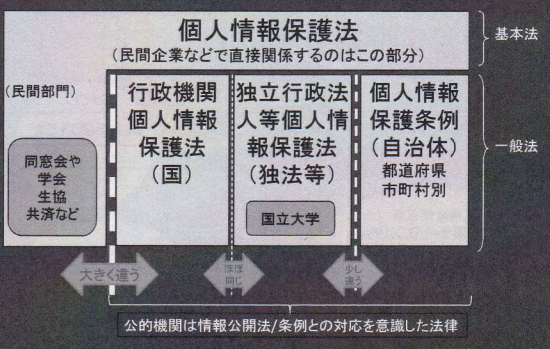
- 全体は、基本方針、対策基準、実施手順の3階層構成：詳細は下記参照：
  http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/regulation/index.html

「京都大学における情報セキュリティの基本方針」　(Policy)
「京都大学の情報セキュリティ対策に関する規定」　(Standard)
「京都大学情報セキュリティ対策基準」
「京都大学情報資産利用のためのルール」
「京都大学情報格付け基準」
「京都大学情報セキュリティ監査規程」
「京都大学情報セキュリティポリシー実施手順書」
「京都大学情報の格付け及び取扱い手順書」
「京都大学における個人情報の保護に関する規程」
「京都大学全学情報システム利用規則」
「パスワード、不正プログラム対策、無線LAN設置ガイドライン」など。　(Procedure)

5－12：京大のルールと仕組みの中から．．．

- 今日ご説明する内容は（ごく一部）：
  - 個人情報保護法と関連法令
  - 情報資産の格付け基準
  - 全学情報セキュリティ体制
  - 各部局の情報セキュリティ体制
- もしあなたの部局でインシデントが起こったら？
- 詳細は下記参照：
  - http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/regulation/index.html

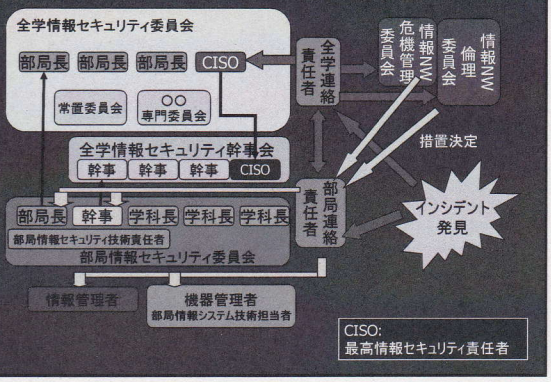
5－13：個人情報保護法と関連法令



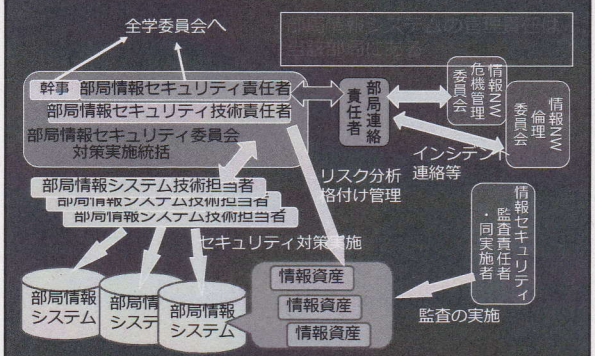
5－14：情報資産の格付け基準

- 要機密情報（特定の人にしか見せてはいけない情報）
  - - 秘密情報（機密性3）
    - Ex. 実施前の入試問題，未発表の人事関連情報など。
  - - 学内限りの情報（機密性2）
    - Ex. 学内勉強会の資料，部局長会議等の協議事項など。
  - その他（機密性1）
- 要保全情報（改ざんされないようにする必要がある情報）
  - 完全性2： 情報が改ざんされると支障をきたす。
  - その他（完全性1）。
- 要安定情報（いつでもその情報にアクセスできるようにする必要がある情報）
  - 可用性2： 情報が使えないと支障をきたす。
  - その他（可用性1）。

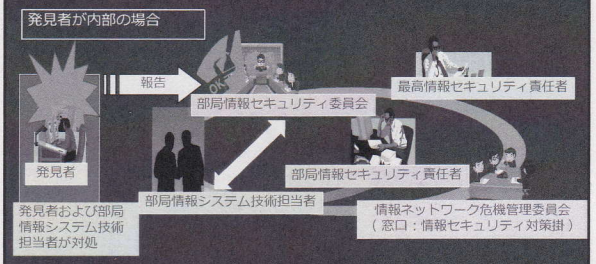
5－15：全学情報セキュリティ体制



5－16：各部局の情報セキュリティ体制



5－17：もしあなたの部局でインシデントが起こったら？



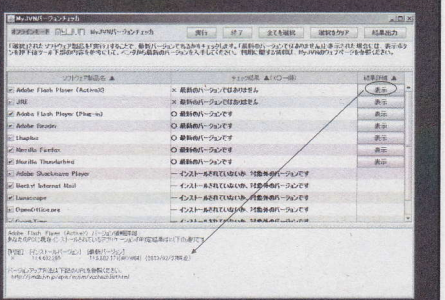
外部へ迷惑をかけている場合、内部に影響が広がりそうな場合などに、情報ネットワーク危機管理委員会から遮断措置が行われる場合があります（指示に従ってください）。

6：安全運転の心得

- 一人ひとりに最低限守ってもらいたい事
- セキュリティ対策ソフト（ウィルススキャン）の導入と最新版への更新。Macも、できたらスマホも！
  - OSも、各種アプリも常に最新版に！
  - アプリが最新かどうかの確認方法は次ページで。
- メールやWebでのウィルス対策。
- パスワードの安全確保。

6－1：アプリが最新かどうかの確認方法

- 情報処理推進機構（IPA）www.ipa.go.jpに便利なツールあり
  http://jvndb.jvn.jp/apis/myjvn/



6－2:メールやWebでのウィルス対策

- メールで注意すべき事：
  - ウィルスは「添付ファイル」とともにやってくる。添付ファイルは無用心に開かない。
  - 特にファイル名が「～.exe」となっているものは絶対に開かない。
  - ウィルス対策ソフトがあるから安心ではない！
  - 最近の「標的型」「ゼロデイ」等と呼ばれる攻撃は
  - 添付ファイル付きメールを送るときも相手のことを考えるべし！
  - 圧縮してファイルを送る場合は前もって相手に伝える。
  - 「自己解凍ファイル」形式では送らない。

  などなど。
- Webで注意すべき事：
  - 改竄されたWeb経由に注意。
  - 不用意にリンクをクリックしない。
  - 証明書で安全なサイトかどうかを確かめる（最近はこの機能がついたウィルス対策ソフトやブラウザも多い）。

6－3：パスワードの安全確保

- 最近、リスト攻撃などによって、パスワードが漏洩し、思わぬ事故に繋がるケースが増えている。

  パスワードは：
  - 8文字以上で、英大小文字、数字、記号をすべて含むように！
- パスワードはシステム毎に分ける！
- 3ヶ月（90日）に1回は更新する。
- パスワードの強度を簡単にチェックできるサイト:
  - https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx

Tips: 覚えやすいパスワードの作り方

- ストーリーのあるパスワード（作り方を覚えておく）。
  - 忘れても、再度「同じ方法」で作り出せるように。
  - 自分の身の回りでしか使わないような言葉を使う。
  - ex. 奥さんと子供に関係のある事。例えば、あだ名、趣味に関する事など。
- いくつかの「パーツ」を組み合わせて長くする！
  - ex. 奥さんのあだ名＋あなたの好きな数字列＋飼っている犬の名前とか。
  - 並べる順番を変えると別のパスワードにもなる！
  - そのサービスを表わす記号をどこかに入れてもいい。
  - ex.「xyz123ABC」が上記で作ったPWならば、
    - 「facebook-xyz123ABC」とするなど。
  - こんな面白いやり方もある！
    - http://tabi-labo.com/32665/password/

6－4：ABC

- A: 当たり前の事を
- B: 馬鹿にしないで（馬鹿正直に）
- C: ちゃんとやる！

6－5：情報セキュリティのe-Learning

- 必ず受講してください（京都大学構成員の義務です）。
  - 格付けやセキュリティポリシーなど一通り学ぶ事ができます。
  - 受講した事実は所属の各部局長に通知されます（成績は通知しません）。
- 教職員グループウェアからアクセスできます：
  - リンクインデックス→「各種e-learning」→「情報セキュリティe-Learning」→「学認連携Moodle講習サイト」に入り、

    「京都大学の情報格付け」と
    「京都大学情報システム利用規則とセキュリティ」
    の両方を受講してください。テスト終了で受講したとみなされます。

参考になるサイトなど

- 総務省：国民のための情報セキュリティサイト
  http://www.soumu.go.jp/joho_tsusin/security/index.html
- 警察庁：セキュリティポータル @police
  http://www.cyberpolice.go.jp/
- 情報処理推進機構（IPA）
  http://www.ipa.go.jp/security/
- 情報セキュリティ対策室セキュリティ情報
  http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/

情報セキュリティについての問い合わせ先

まず各部局の情報セキュリティ担当者に相談を：
部局情報システム技術担当者
部局情報セキュリティ委員会

情報セキュリティ対策室Webページ
http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/

情報セキュリティ対策掛
電話　075-753-7490
E-mail：i-s-office@iimc.kyoto-u.ac.jp

まとめ

- 今日、伝えたかった事
  - インターネットは便利な道具。
  - 使わない手はない。
  - セキュリティの脅威は交通事故のようなもの。
  - 危険の存在を知って、しっかり対処すれば怖くない。

ゲーテの言葉（再掲）

- 『一人一人が自分の家の前を掃けば、町中がきれいだ。』

↓

- 一人一人がセキュリティの心得を守れば、大学全体が安全（セキュア）だ．．．

Credit

- 「3. 具体的なセキュリティ・インシデントの紹介」では、Telecom-ISAC Japanの西部康喜さんから提供して頂いたコンテンツを手直しして使わせて頂きました。

The End

感想　　『京都大学の情報セキュリティ対策について』：斉藤康己教授

・全体を守るのは結局個人だという事を改めて認識しました。
・身近ではあるがよく理解していない部分の説明が多く有りとても興味深い内容であった。事例の説明等にもう少し時間が長くあればよかったと思う。
・情報化社会における個人のセキュリティに対する意識改革は常に更新を促される必要があると思われるので最近の事例を挙げたお話を伺えてとても良かったです。自分自身の業務内容での注意点についても最新のものと比較する必要性を感じました。
・コンピューターが一般に利用される前からのご使用経験など、これまでのインターネットも歴史的な背景や利用方法・状況などをご説明頂き、またご自身の経験からくる丁寧な理解しやすいご説明が非常に良かったです。
・情報セキュリティに対する考え方やインターネットのことがよく分かった。インターネットについては、その歴史等、あまり知らなかったので、大変興味深く聞くことができた。人が使うものなので、使用する一人一人がモラルを持つことが必要なのだと感じた。
・セキュリティというと堅い話になるかと思いきや、受講者の身近な問題まで落とし込んだ内容にまで噛み砕いてくださっていたので、楽しく受講することができました。個人PCのセキュリティを再確認しておきます。
・ニュースや記事では騒動や犯人などが主となる情報で、次はセキュリティには注意しましょうと、肝心の知るべき原因などの情報が断片的かつ少ないように思います。セキュリティインシデントの事例として最近世間を騒がせた事件がどのような手口、経路で生じたのか紹介していただき、各事例騒動の全景がつかめたように思います。そして、インシデントを防ぐためには自己防衛が大切であること再認識することができました。
・インターネットの情報セキュリティについて改めて考えることができ良かった。様々なネット被害を知ることができ、またそれらにあわないように気をつけたい。パスワードの考え方を教えてもらい、参考になった。今までパスワードの変更をしたことがなかったが、今後はその方法を参考にしてパスワードを時々変更していこうと思った。
・様々なセキュリティインシデントの事例を紹介して頂き、大変勉強になった。ちょうど同じ週に友人のLINEのアカウントが乗っ取られたところであったので他人事ではないことを改めて認識した。今後、自分の周りのセキュリティの再確認を行っていきたい。
・セキュリティについて「自らが守る」が基本であり、組織はそれを「サポートするもの」であるということについて、よく勉強になりました。
・インターネットの歴史から、今後の課題まで詳しく講義を聞けて本当に面白かった。
もともと性善説によって運用されていたインターネットが、悪質な利用者によって整備されていく経緯がよくわかった。自分自身がルールを守り、組織に迷惑を掛けない情報対策に努めたいと思います。
・情報セキュリティは大学（組織）任せになるのではなく、個人としても注意を払わなけ

ればならないものであることが分かりました。

・京都大学の情報セキュリティの基本は自ら守ること。そのために個々が使用するパソコンのセキュリティソフトは最新にしておくこと、パスワードはいろいろな文字を組み合わすことなどが紹介された。しかし、世の中には様々なネット犯罪が横行しているようで講義でも幾つか紹介されたが、そういう話を聞くと情報セキュリティを例え万全にしたとしてもクラッカーと呼ばれる人がセキュリティを破ってくるのではという気がした。新種のコンピューターウイルスが新たに開発された場合、最新のセキュリティソフトでも歯が立たないのではと思った。講義では 50 年経ったらネット犯罪は無くなるのではと予期されていたが、実際はどうなるのか誰にも分からないなと思った。

・様々な具体例を紹介していただき、とてもわかりやすく、面白く、参考になった。個人の PC を守ることが基本であるということを肝に銘じたい。

・インターネットの歴史や考え方の講義は、これまでは「何となく」知っていることが多かったので、その詳細について知ることができて有意義でした。ハッカーとクラッカーは同じ意味に捉えていたので、その違いがよく分かりました。

インターネットセキュリティに関してユーザー側でできることについては、概ね実践できていたので、安心しました。一人一人の心構えが大事だと思うので、今後も当たり前のことを続けていきたいと思います。

・非常に有意義な講義だった。 便利に使っているグーグル等のプロバイダは果たして業務に使って良いのか悪いのか分からず使用していた。しかし斉藤先生より個人がしっかりと管理を行えば、どんどん使ってくださいと言われ、安心した。また、インターネットの歴史やセキュリティ管理をすることになった経緯やさまざまなハッカーによる事件などを講義いただき、セキュリティ対策の関心が高まった。今後はしっかりとパスワード管理などをしていこうと思う。また忘れにくいパスワードの作り方をお教えいただいたのでさっそく実行して行こうと思う。

・インターネットの歴史から実際の事件などから得られる教訓など、大変解りやすい講義だった。インターネットとは何か、セキュリティとは何かについての問いかけについて理解が深まり、「ゲーテの言葉」などプレゼン技術についても学ぶ事が多数あった。

・そもそも京大ネットワークに接続しているユーザー一人一人が意識して対策を行っていかなければ意味が無いという事を改めて認識する事が出来た。

・セキュリティの実例について、具体的にわかり易くご説明いただきありがとうございました。

・情報セキュリティの重要さは認識しているつもりなのですが、コンピューターは多くの人にとってその仕組みをよく知らないままにとにかく使い始める事がほとんどだろうと思いますし、何をどう気をつければいいか誰からも教わらないまま使い続ける事が普通となっていますので、今後もずっとセキュリティ問題は続いてゆくだろうなと思いました。

・インターネットの歴史やウィルスの脅威などとても興味深い話ばかりだった。機会があれば、ぜひもう一度受講したいと思った。
・人が皆善人なら、セキュリティの問題も考える必要もないが、そうでないから何かセキュリティ対策が必要になってくる。そういうことがここ数年で特に大事になってきている。大学内でもいろんな事件があったりして、改めて対策をしなければならないことに気づかされた。ただ、人任せでなく、自分から被害リスクを上げるようなことをしないことが何より重要だということが分かった。
・インターネットの歴史から始まり、近年のネットより発生した犯罪の話やなどを興味深く拝聴した。パスワードに関してはなるべく同じにしないように気を付けてはいるものの、一度決めてしまったら定期的に変えたりすることをしていないので今後気を付けようと思った。また、安易にサイトに入ることで大学全体に被害を与えることもあることを今まで以上に念頭に置いていきたいと思った。
・組織のセキュリティ対策として、各個人の意識・作業が重要だという話が印象に残った。また、パスワード設定についての話も非常にためになった。
・インターネットにおけるセキュリティについて、非常に噛み砕いた面白いお話が聞けてとても役に立ちました。特に京都大学に対するネット攻撃の凄さは、色々と情報ではお聞きしていたのですが、それに対抗するセキュリティ技術には脱帽する思いです。完璧なセキュリティはないので、結局、一人一人のセキュリティ意識を高めるしかなく、パスワードもしっかり管理しなければどんなに素晴らしいセキュリティ対策でも意味が無くなってしまう事を、改めて痛感しました。今後、巨大素数積の暗号も破られる時代になる可能性もあるので、ABC（当たり前の事を、馬鹿にしないで（馬鹿正直に)、ちゃんとやる！）を意識して実施します。
・具体的な内容で、わかりやすく話してくださり、インターネットがどう発展してきてどのようにして情報セキュリティ問題が生じ、深刻化していったのかを知ることができた。ゲーテの引用を用いたメッセージは肝に銘じたい。
・インターネット創成期から、現在の様々なセキュリティにまつわる犯罪事例まで解説していただきとても参考になりました。パスワードはもう少し頻繁に変えようと思います。
・この話を聞いて、インターネットセキュリティについて楽しく勉強することが出来た。特に、最近の実際にあった事件を題材にしてその原因を聞くことでそれに対してどのような対策をとればよいかということを考えるきっかけとなったので、この講義を聞くことが出来て非常に有意義であった。今後も新しい事件などがあれば、その原因について是非知っておきたいと思っている。
・情報セキュリティについて、身近な例を交えてご説明があり、大変わかりやすかった。
・全学生が共用で使用する教育用 PC 端末を管理しているので、セキュリティをどう考え、どう保護するのか大変興味があります。講義ではエンドユーザーよりの話でしたが、管理者が今後どう考えていくべきかといった話もお聞きしたかったです。

・一時間半という中で，非常にボリュームのある内容であった。とても興味深く聞かせていただき、時間が足らないほどに感じた。組織がどんなに強固な仕組みを構築しても、個人の行いにより簡単にどうとでもなってしまうことが理解でき、個々の利用に大きな責任がありことを自覚した。
・セキュリティについて再確認できた。
・古い時代のインターネットはオープンであったという話が印象的でした。
・最新事例がわかりやすく紹介され、大変勉強になった。

講義：斉藤教授