帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

2016年度 国際理解公開講座【後期】
「米国を読む」

サイバー攻撃の現在
–米国、中国、そして日本–

中野秀男

帝塚山学院大学

情報メディア学科/ICTセンター長

大阪市立大学名誉教授、堺市情報セキュリティアドバイザー

今日の話

- 自己紹介と参考にした本や資料
- サイバー攻撃
  - 国や組織同士だとサイバー戦争
  - 個人だと標的型攻撃や標的型攻撃メール
- サイバー攻撃の事例
- アメリカでは、中国では、日本の体制は
- 標的型攻撃、標的型攻撃メール
  - zipファイルの添付にご注意
- ソーシャルアタック
- リスクマネジメント
  - 受容レベル

軽く自己紹介

- 大阪大学、大阪市立大学、帝塚山学院大学
- 現在は
  - 帝塚山学院大学情報メディア学科特任教授
    - 兼ICTセンター長
  - 堺市情報セキュリティアドバイザ
    - 3月までは5年間、大阪市ITアドバイザ
- 自治体のIT化
  - 大阪市、堺市、豊中市、奈良の三郷町
- インターネットとインターネット技術の普及
- IT人材の育成(KOF:関西オープンフォーラム)
- 専門はインターネット、インターネット技術、セキュリティ

参考にした本や資料

- 「標的型攻撃/セキュリティガイド」岩井博樹(ラック)
  - Softbank Creative, 2013年3月
- 「ソーシャル・エンジニアリング」Christopher Hadnagy
  - 日経BP, 2011年
- 「サイバー戦争論:ナショナルセキュリティの現在」
  - 伊藤寛, 原書房
- NISC(内閣サイバーセキュリティセンター)調査研究
  - サイバー空間における諸外国の施策動向調査報告書
  - 重要インフラ防護に関する諸国の枠組み等に関する調査報告書
- 「クラウドセキュリティ:クラウド活用のためのリスクマネジメント入門」河野省二他
  - 翔泳社, 2014年5月

情報セキュリティの変遷

- 歴史的に
  - 1980年ぐらいまでは暗号(慣用暗号)
  - 公開鍵暗号の登場で電子署名などビジネスや暮らしに
  - 1990年代のインターネットの普及でセキュリティが重要に
- 今
  - 国や企業を狙ったインシデントが
  - コンピュータ犯罪からサイバー犯罪へ
  - 国と国などとのサイバー攻撃合戦(第5軍)
  - 標的型攻撃/標的型攻撃メール

サイバーの今

- サイバー
  - コンピュータとインターネットに関わることの総称
- 情報は無体物
  - サイバーは有体物も含む
- 今
  - 多くの人がスマホを持って、ネット接続している
  - メールやウェブやSNSで繋がっている
    - フェースブックは17億人
      - http://media.looops.net/news/2016/11/29/2016q3_facebook_instagram_twitter_line/

コンピュータウィルス

- メールで添付ファイル(Excelやexe)が送れるようになった。
  - １９９０年台前半にメールにMIME形式採用
- 最初はパソコンのデータ破壊
- 徐々にパソコンに住みついて
  - 情報を外に出したり
  - 遠隔から操作できるように
- Spyware　や　Adware
- Bot
  - コンピュータやインターネットにある自動プログラム

サイバー犯罪の特徴

- 遠隔地からの犯行
  - 例: 遠隔操作ウィルス(遠隔でかつなりすまし、または踏み台)
- 調査が難しい→アナログ犯罪より易しい？
- 被害が甚大である
- 犯人の罪悪感が乏しい
- 処罰が軽い→みせしめの逮捕
- 愉快犯から特定目的、特定対象に
- コンピュータ犯罪からサイバー犯罪に

サイバーテロ

- 重要インフラに対して、ネットワークなどを利用した電子的な攻撃で、国民生活や社会経済活動に重大な影響を及ぼす可能性のあるもの
- 低コスト、専門的知識、匿名、無痕跡
- 地理的制約なし、時間的制約なし
- 情報通信、金融、航空、鉄道、電力、ガス
- 政府・行政サービス

サイバー犯罪の事例(1)

- 2007年4月：エストニア政府などへのウェブサイト攻撃
- 2008年8月：グルジア政府などへのウェブサイト攻撃
- 2009年7月：米国及び韓国の国防部を含む政府機関へのウェブサイト攻撃
- 2009年12月：Google社等への不正アクセス
- 2010年8月：イランのウラン濃縮制御システムがOSの脆弱性を利用したウィルスに感染
- 2011年3月：韓国の国防部を含む政府機関へのウェブサイト攻撃
- 2013年3月：韓国の複数の放送局や金融機関などの情報システムへの攻撃

サイバー犯罪の事例(2)

- 2012年8月：サウジアラビアのサウジ・アラコム社の3万台に上るコンピュータがウィルスに感染
- 日本
  - 2009年4月：政府機関などのウェブサイト改ざん
  - 2011年9月：防衛関連企業への不正アクセス
  - 2012年6月：裁判所や行政機関、大学病院などのウェブサイトへの攻撃
  - 2015年5月：年金機構への標的型攻撃メール
    - 日本年金機構の情報漏えいについてまとめてみた - piyolog
    - http://d.hatena.ne.jp/Kango/touch/20150601/1433166675

サイバー戦争(1)

- 軍事システムにサイバー技術が
  - 指揮統制システム
  - 通信システム
  - センサーシステム：IoT(Internet of Things)もののインターネット
  - 兵器システム
  - 誘導システム：GPS
  - 兵站システム: 無線タグ

サイバー戦争(2)

- 交戦距離を無限大に
  - インターネットで繋がっていればどこまでも
- 新しい戦闘方式
  - サイバー戦
- 新しい軍事革命
- 新しい戦場を追加
  - 陸、海、空、宇宙、サイバー
- 戦争の性格を変える
- 新たな戦争理論の始まり
- 戦争自体の概念が変わる
  - 軍事力、経済力、情報力

日本での体制

- サイバーセキュリティ戦略本部
  - NISC:内閣サイバーセキュリティセンター(2015年1月)
  - IT総合戦略会議、国家安全保障会議と緊密連携
- 各府省等
  - 金融庁：金融機関
  - 総務省：地方公共団体、情報通信
  - 厚生労働省：医療、水道
  - 経済産業省：電力、ガス、化学、クレジット、石油
  - 国土交通省：鉄道、航空、物流
  - 文部科学省：セキュリティ教育
- 警察庁セキュリティポータルサイト@police
  - インターネット定点観測

アメリカの場合

- NISC(内閣サイバーセキュリティセンター)調査研究より
  - サイバー空間における諸外国の施策動向調査報告書
  - 重要インフラ防護に関する諸国の枠組み等に関する調査報告書
- ホワイトハウス
- 国防総省(DOD)、国土安全保障省(DHS)、商務省
- FBI, CIA, NIST(国家標準技術研究所)
- ネットの監視・情報収集
  - 米国では、国家安全保障局(National Security Agency:NSA)が電子機器を使った情報収集 活動を行っている。組織の人員は、30,000 人以上と言われており、年間予算は機密扱いとなって いる
- 大統領選挙でのメール暴露合戦

中国の場合(1)

- NISC(内閣サイバーセキュリティセンター)調査研究
  - サイバー空間における諸外国の施策動向調査報告書より
- 通信の秘密
- 言論の自由
- インターネットの事前検閲
  - インターネット上のニュースの 掲載許可、不許可を決めているのは、国務院新聞弁公室網絡宣伝管理局
- ネットの監視・情報収集
  - 公安省や中共中央宣伝部等の機関が活動を行い、インタ ーネットを監視
  - インターネット検閲システム「金盾工程」(通称:グレイト・ファイヤー・ウォール)を運用しており、インターネットユーザーのアクセス制限

中国の場合(1)

- 中国は、サイバー犯罪条約に反対しており、加盟していない
- 中国国軍に関する白書
  - 「宇宙およびサイバー空間の国家安全 保障の利益を守る」と指摘した上で、「我々は攻撃されない限り攻撃することはない。しかし我々 は攻撃を受けたら確実に反撃をする」
- サイバー攻撃が業務？
- 五毛党(「いいね」で報酬？）

最近のサイバー攻撃(1)

- 陸自システムにサイバー攻撃、情報流出か　国家関与も　被害の全容不明 －　産経ニュース
  - http://www.sankei.com/smp/affairs/news/161128/afr1611280003-s1.html
- 韓国軍のサイバー司令部、先月サイバー攻撃被害-Chosun online 朝鮮日報
  - http://www.chosunonline.com/site/data/html_dir/2016/10/01/2016100100504.html
- 韓国のサイバー戦事情に見る戦後日本の欠落（Wedge）- Yahoo!ニュース
  - http://zasshi.news.yahoo.co.jp/article?a=20160903-00010002-wedge-kr
- 米軍、ISISにサイバー攻撃開始　指揮系統など妨害
  - http://www.cnn.co.jp/m/usa/35081175.html
- 仏へのサイバー攻撃が１万９千件 「前例のない規模」と軍幹部 - スマホ版 - 47NEWS（よんななニュース）
  - http://www.47news.jp/smp/CN/201501/CN2015011601000689.html

最近のサイバー攻撃(1)

- 記者の眼 - 日本は北朝鮮からのサイバー攻撃に対抗できる？ 対岸の火事ではない「ソニー事件」: ITpro
  - http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/122500149/?n_cid=nbpitp_itptw_top&ST=smart
- サイバー戦争が制御不能になる可能性　WEDGE Infinity(ウェッジ)
  - http://wedge.ismedia.jp/articles/-/8186?layout=b
- ＜中国サイバー攻撃＞米NSA、作戦データを入手（毎日新聞） - Yahoo!ニュース
  - http://headlines.yahoo.co.jp/hl?a=20150922-00000004-mai-int
- アメリカ陸軍、サイバー攻撃分析ソフト「Dshell」をオープンソース化 | OSS TOPICS | OSSNEWS - オープンソース総合情報サイト
  - http://www.ossnews.jp/oss_info/article.html?oid=4849

標的型攻撃(1)定義と目的

- 組織はそこそこ強くなったので、まず弱い個人から攻めよう
- 定義
  - 明確な意志と目的をもった人間が、特定のターゲットに対して、特定の目的で行う、サイバー攻撃の一種
  - 欧米ではAPT(Advanced Persistent Threat)
- 目的
  - 政治的活動(Anonymous, WikiLeaks)
  - サイバー犯罪
  - サイバーテロ
  - サイバー戦争(サイバー空間は第5の戦場)
  - 業務妨害(DDoS攻撃によるサーバ停止)
  - 政治的駆け引き
  - 個人的な動機による攻撃

標的型攻撃(2)目的(続)

- サイバー犯罪
  - オンラインバンクを利用しての不正送金
    - 最近は二重認証の方向へ
  - フィッシング詐欺
  - ランサムウェア(Ransomware)による脅迫：身代金ウィルス
  - 個人情報の売買
  - DDoS攻撃
- 個人的な動機による攻撃
  - 愉快犯
  - 恨みつらみ
  - サイバーストーカー

標的型攻撃(3)攻撃者

- 政府、軍関係者
- 民間企業
  - アングラ企業
  - ライバル会社を攻撃
- マフィア、反社会勢力
- 学生
- その他
  - ネットストーカー
  - 上司や女性社員のPCにRAT(遠隔操作ツール)

標的型攻撃(4)インシデント事例と標的型メール

- RAT(遠隔操作ツール)がPCに
  - メールやメッセージのURLのクリックで
  - 届いたUSBをPCに
- 標的型メール
  - 個人情報の収集
    - Facebook, Twitter, 検索エンジンで写真、住所、勤務先情報を
  - 攻撃するPCが標的
  - RATを組み込ませる
  - パスワードやアドレス帳などを入手
  - 接続元の隠蔽工作
  - 破壊

標的型攻撃(5)ソーシャルエンジニアリング

- 狙われる情報
  - 氏名
  - メールアドレス
  - 会社名
  - 役職
  - 人間関係
- 上記の情報から「なりすましメール」
- SNSやウェブから情報を

標的型攻撃(6)標的型メール

- 実体
  - 業務連絡を装ったメール
  - 取引先を装ったメール
  - 冠婚葬祭を装ったメール
  - 時事ニュースを装ったメール
  - 人材募集を装ったメール
  - グリーティングカードを装ったメール
- 不正プログラムの実行
  - 添付ファイル
  - URLのクリック(不正サイトへの誘導リンク)

情報について

- 以前は
  - 情報開示
  - 説明責任
- 今は
  - 嘘は必ず暴露る
  - 情報は漏れる

Facebook(1)

- 実名主義:なりすまし
- 個人とFacebookページ
- 友達になる
- Facebookページ
  - ホームページとして
  - ホームページの補完として
- 中野秀男:友達870名(July/7/2015)
  - 2011年6月26日から
- 3名が結託されると情報が抜かれる
- 標的型攻撃の情報源

Facebook(2)

- 中野はOpinion Leader的な友達が多いので情報収集に
  - URLを拾って自分宛にメール
  - URL
- TwitterやFacebookの情報は売買されている
- 今はFacebookやLINEの次のSNSが見えない
- Facebookの新しいプライバシーポリシー
- 写真がスキャンされて顔認識

LINE

- 国籍は韓国
  - Twitter, Facebookはアメリカ
- LINEのアカウントの乗っ取り
  - PCでも使っているとあぶない
  - 乗っ取り犯のマニュアル
- なぜ広まったのか
  - 手軽に友達に
  - スタンプ効果

事故を発生させないための対策

- リスクの要因は「脅威」と「脆弱性」
- 「脆弱性」は管理下にあるが、「脅威」はほぼ外部
- 発生することが予想または起こった事象「インシデント」
- 脅威と脆弱性が合致してインシデントができる
- 対策は「脆弱性」にするのが効率的
- 事故の発生に関するリスクアセスメント
  - インターネットなどで脅威情報を収集
  - 収集した脅威に対する脆弱性を洗い出す
  - 洗い出した脆弱性が自組織で起こるか判断

脅威

- IPAの2015年10大脅威
  - https://www.ipa.go.jp/files/000044680.pdf
  - 1.インターネットバンキングやクレジットカードの不正利用
  - 2.内部不正により情報漏洩
  - 3.標的型攻撃による諜報活動
  - 4.ウェブサービスへの不正ログイン
  - 5.ウェブサービスからの顧客情報の窃取
  - 6.ハッカー集団によるサイバーテロ
  - 7.ウェブサイトの改ざん
  - 8.インターネット基盤技術を悪用した攻撃
  - 9.脆弱性公表に伴う攻撃
  - 10.悪意のあるスマートフォンアプリ

事故の影響を最小にするための対策

- 事故の発生をゼロにするのは難しい
  - 技術的に、費用的に
- コストパーフォマンスに合わないものは対策しない
  - 技術者からすると辛いけど、経営的には正しい
- リスク受容レベル
  - 受け入れることのできる損失のレベル
  - 損失
    - サービスの停止だけであく顧客対応、企業の評判
- 機密性：情報を見られたり盗まれた場合の損失
- 完全性：改ざんなどによる影響
- 可用性：サービス停止やパーフォマンス不足による影響

リスクの受容レベルを設定する

- 「予防」や「検知」を組み合わせた「階層防御」
- 予防：事故が起こらないための対策
- 検知：事故の発生に気付くための対策
- 例：ホームページの改ざん
  - 予防：
    - 関係ソフトウェアを最新バージョンに
    - 最新セキュリティパッチの適用
  - 検知
    - アクセスログからの異常発見
  - 影響：利用者にウィルスが。フィッシングサイトへのクリック
  - 受容レベル：改竄後回復または停止までの時間
    - 利用者の利用頻度

対策が実施されていることを保証する

- 「しないこと」のルールから
- 「すること」のルールへ
- ルールも明快に
- 例：パスワード
  - 「パスワードを破られないこと」
  - 「複雑なパスワードにすること」
  - 複雑なパスワードの定義やルールを策定
  - 定義やルールの作成が受容レベルを作ったことになる
    - それで破られたら仕方がないという受容レベル
    - 破られた場合の速やかな処置体制

VOD(Video/Voice On Demand)

- 中野秀男研究室
  - 担当の講義に「情報セキュリティ論」