e-ビジネス情報技術講座
第9回
コンピュータウイルス対策

講師:片岡　信弘

教科書第11章

ポイント

- 悪意のあるソフトウェアはコンピュータウイルスやマルウェアなどとよばれる
- コンピュータウイルスの感染の経路
- コンピュータウイルスの被害
- コンピュータウイルスの対策
- サイバーテロの実態と対策

11.1.コンピュータウイルスとは

悪意のあるプログラムを全て含めて
広義のコンピュータウイルスと呼ぶ

コンピュータウイルスの種類

- マルウェア
  - 悪意のプログラムの総称であり，不正プログラムを総称してマルウェアとよぶ
  - コンピュータウイルス(広義)ともよばれる.
- コンピュータウイルス(狭義)
  - 他のプログラムやファイルに寄生して，ファイルの破壊やコンピュータに異常な動作をさせる
  - マルウェアの中では最も古くから存在するタイプ

コンピュータウイルスの種類(続き)

- ワーム
  - ウイルス(狭義)のように寄生する他のプログラムを必要とせず単独で活動
  - スクリプト言語やマクロなど簡易的技術で作成.
- スパイウェア
  - 利用者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集
- ボット
  - コンピュータを攻撃者が外部より操作
  - 感染したコンピュータは，攻撃者の指令に従い，情報の盗み出しや，迷惑メールの送付やサーバ攻撃などを行う

11.2.コンピュータウイルス
感染経路

USBメモリ経由，Webサイト経由
，メール経由，マクロ機能を利
用した感染が存在する

Quiz1

- 道端にUSBメモリが落ちていたらどうするか
  - 拾ってPCに挿して内容から持ち主を確認し持ち主に届ける
  - 無視する
  - 拾って警察に届ける

USBメモリ経由の感染

- USBメモリやSDメモリカードなど可搬型のメモリ経由で感染
- パソコンにUSBメモリなど接続すると，USBメモリ内のプログラムが自動実行される機能を悪用
- 自動実行機能によりウイルスをダウンロードするプログラムが実行される
- ウイルスに感染したパソコンにUSBメモリを接続すると，そのUSBメモリにウイルスが感染

Webサイト経由の感染

- ウイルスに感染したWebサイトを閲覧することにより，そのパソコンの脆弱性をついてウイルスに感染
- 正規のWebサイトが不正アクセスにより**改竄**(改ざん)されウイルスがしかけられていることもある
- メールで悪意のあるWebサイトに**誘導**しWebサイト経由の感染も多い

メール経由の感染

- ウイルス感染の95%を占める
- メールの添付ファイルにより感染するケース
- メールマガジンだと思いそこの掲載URLをクリックしたらウイルスに感染
  - 多数の人にこのウイルス付きのメールが転送され大きな迷惑をかける事例あり
- スパムメールやインスタントメールに存在する怪しげなURLは絶対にクリックしない

ウイルスを持った添付ファイルのメール事例

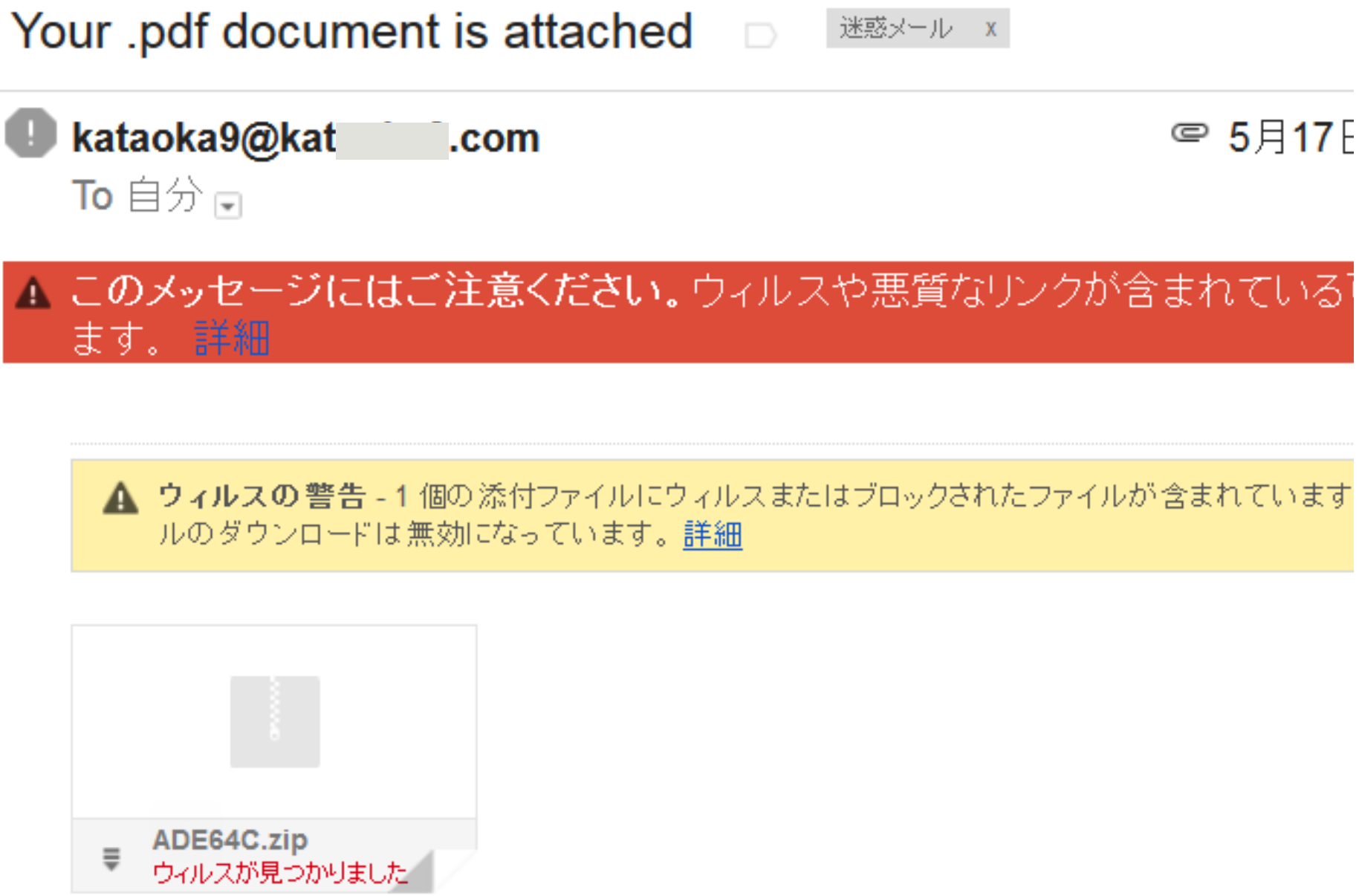
Ron Jensen	**Re:** - Hey kataoka9, I hope you're doing well. I'
自分	Your .pdf document is attached
Amazon.com	Your Amazon.com order has dispatched (#245
Corine Velasquez	**Re:** - hi kataoka9 I have attached a revised spr
Imelda Franks	**Re:** - hi kataoka9 I have attached a revised spr
epson85148396748	**Attached File**

Amazon.com <auto-shipping@amazon.com> 5月

To 自分

⚠ このメッセージにはご注意ください。ウィルスや悪質なリンクが含まれてます。 詳細

⚠ **ウィルスの警告** - 1 個の添付ファイルにウィルスまたはブロックされたファイルが含まれてルのダウンロードは無効になっています。詳細


Your .pdf document is attached
迷惑メール x
kataoka9@kat .com
5月17日
To 自分
このメッセージにはご注意ください。ウィルスや悪質なリンクが含まれている
ます。 詳細
ウィルスの警告 - 1 個の添付ファイルにウィルスまたはブロックされたファイルが含まれています
ルのダウンロードは無効になっています。詳細
ADE64C.zip
ウィルスが見つかりました

マクロ機能を利用した感染

- Wordの文書ファイルやExcelの表計算ファイルのマクロを開くと感染するもの
- Windowsがファイルを開くとき「マクロを有効にしますか」と聞きいてくるのはこのため

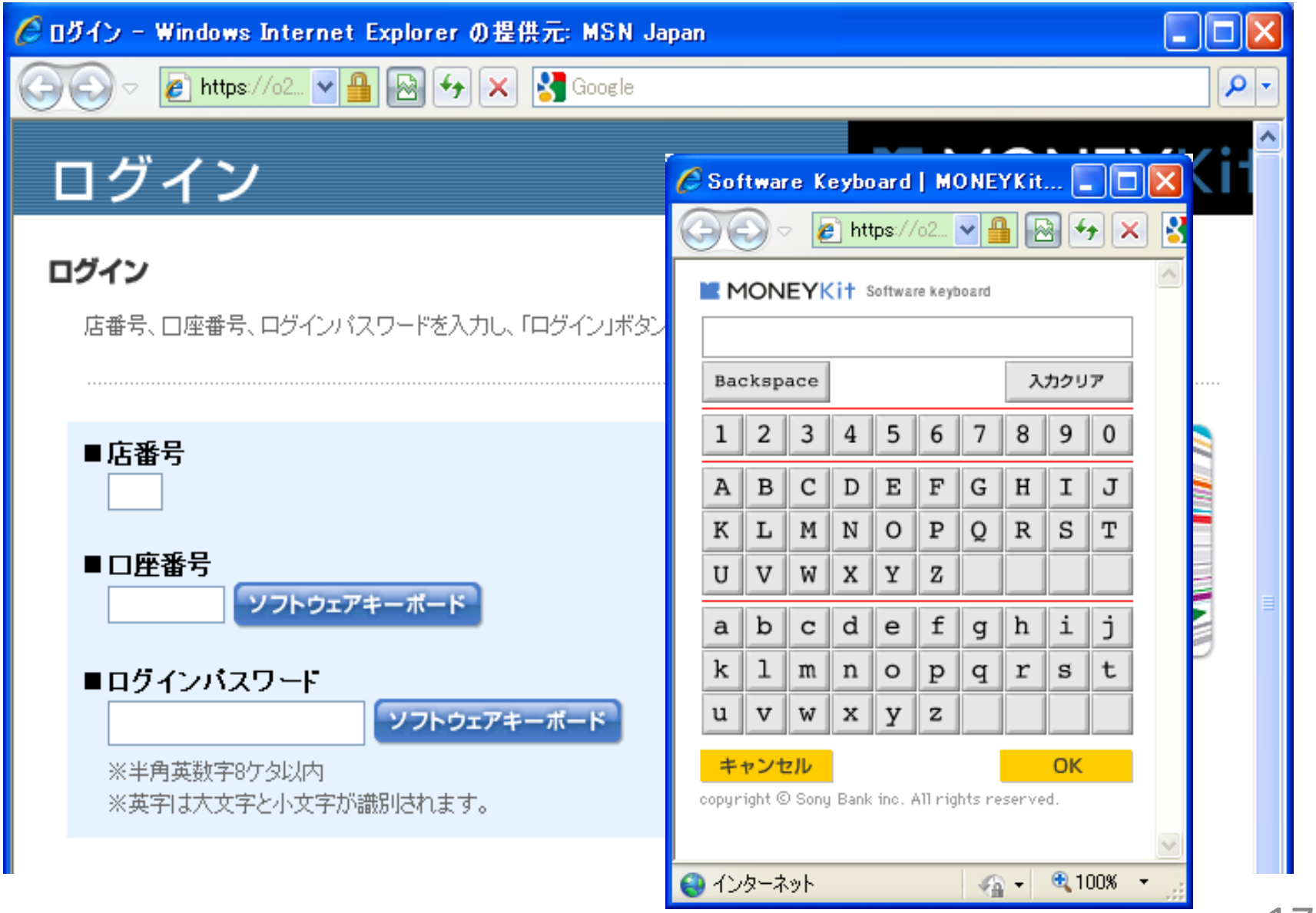
11.3. コンピュータウイルス による被害内容

パスワード盗取，コンピュータ外部からの操作，コンピュータ破壊やデータ漏えい，身代金要求，知らぬ間に他人への攻撃

キーロガーによるパスワード盗取

- キーボード入力を監視し記録するウイルスによりユーザIDやパスワードが盗み出される
- 防ぐ1つの手段がソフトキーボード
  - ログイン画面でキーボードを利用せず，ソフトウェア入力を行う
  - キーボードの代わりに画面をクリックすることにより入力を行う

図11.1 ソフトキーボード入力　p130



バックドアによるコンピュータの外部からの操作

- バックドアウイルスに感染すると，コンピュータを外部から操作できるようにされる

- 侵入口(バックドア)を用意することによりユーザに気づかれずコンピュータを外部から操作可能となる

トロイの木馬によるコンピュータ破壊やデータ漏えい

- 正体を偽りコンピュータに侵入し不正を行うウイルス
- コンピュータの破壊やデータの外部漏えいなどがおこる
- 感染によりカウントダウンが始まりハードディスクの初期化がされてしまう事例もある
- トロイの木馬とは
  - トロイとギリシャの戦争でギリシャ軍の計略
  - 戦争の原因は何?

番外　トロイの木馬

- ギリシャ神話に登場する巨大な木馬で長年続いた**トロイ戦争**でギリシャ軍が計略に利用した

- ラーオコーン

- 遺跡発見者はシュリーマン
- 戦争の原因は?

ウイルスによるコンピュータ破壊の事例

- MaAfeeウイルス体験擬似サイト
- http://www.mcafee.com/japan/home/demo/report/index1.html

特定のファイルの暗号化による身代金要求

- ランサムウェアに感染するとコンピュータ内の特定のファイルが暗号化される
- これを解読するためのプログラムを売りつけられる
- 対応策
  - ネット非接続デバイスにバックアップを取る

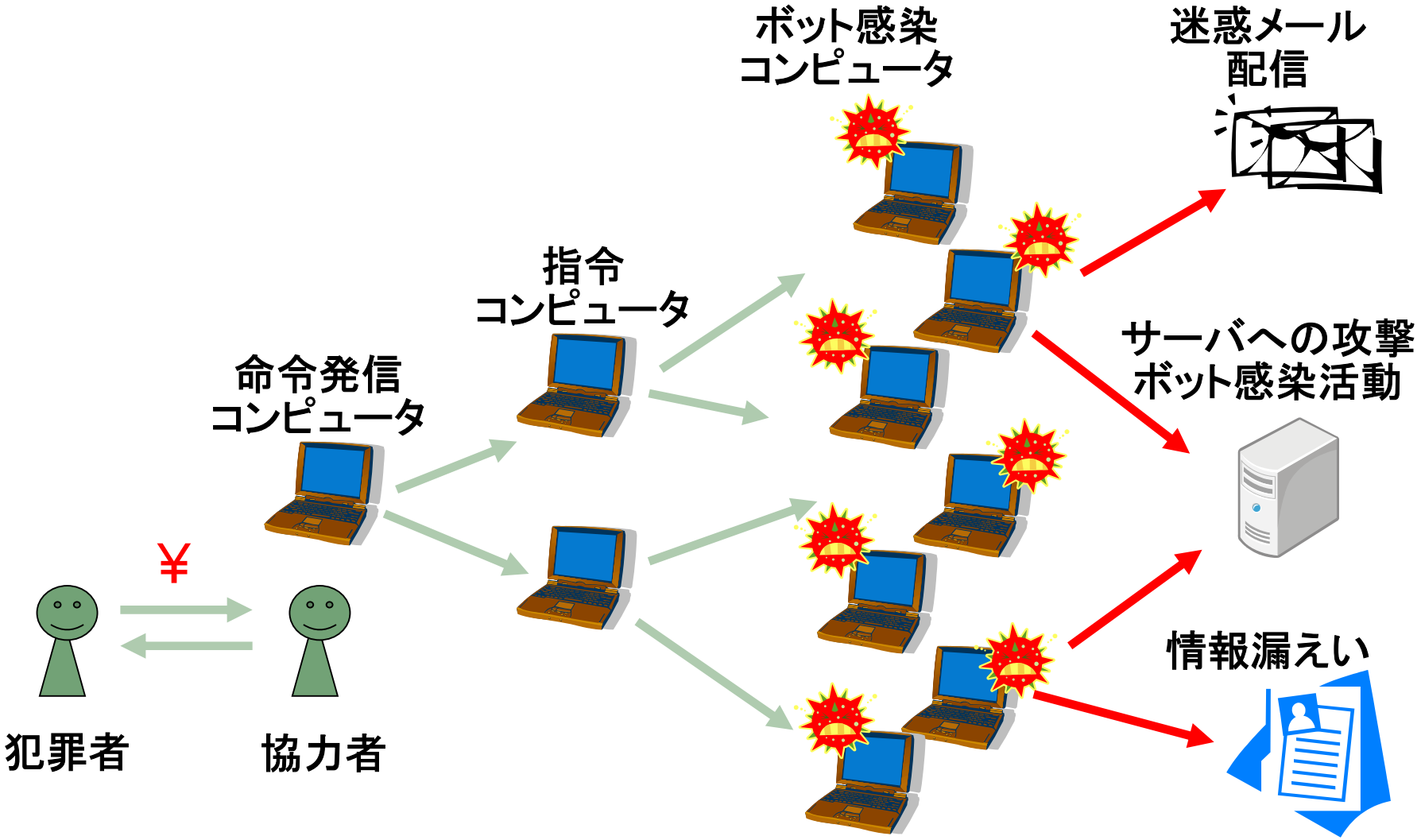
スパイウェアによる個人情報漏えい

- スパイウェアは利用者の個人情報やWebサイトのアクセス履歴などを収集し送付する
- ユーザの意図に反してインストールされている場合は不正な行為
- 他アプリケーションとセットで配布しそのソフトと一括して利用条件として承諾を求めるものもある
- 意識しない内に承諾しており不正ではないが注意が必要.

ボットによる他人への攻撃

- ボットに感染すると他のコンピュータに操られ他人のコンピュータを攻撃する
- 犯罪者は協力者に金銭などを支払って作業を依頼
- 協力者は指令コンピュータを使い脆弱性のあるコンピュータをボットに感染させる
- ボット感染が成功すれば，命令発信コンピュータは，指令コンピュータに指示し攻撃させる
- 指令コンピュータは迷惑メール発信，サーバへ攻撃，情報漏洩指令をボット感染コンピュータ行わせる.

図11.3　ボットによる攻撃模式図　p132



11.5. コンピュータウイルス対策

ウイルス対策ソフトの利用の他，コンピュータの脆弱性をなくすことが重要

ウイルス対策ソフトの利用

- ウイルス対策ソフトを導入する
- ウイルスは常に新種が発生しているためこれの対策のため，定義ファイルを常に更新する
- 一定周期でパソコン全体のウイルス検査と駆除
- 無料のウイルス対策ソフトも存在する有料のものは多数の付加機能を有する
- Winows10のウイルス対策
  - ウイルス検知率は他の有料ソフトと同等

ウイルス対策ソフトの付加機能

- 有料ウイルス対策ソフトの機能例
  - パーソナルファイアウォール機能
  - フィッシングサイトをブロック機能
  - 迷惑メール対策機能
  - 個人情報漏洩対策
  - 有害サイトブロック
- 機能をよく調べた上で導入する必要あり
- ウイルス対策ソフトの企業のHPではセキュリティ対策の事例や解説があり参考となる

スマホのためのウイルス対策

- iPhoneアプリに対してAndroidアプリは誰でも作成公開が可能.
  - 危険なアプリが作成される可能性よりが高い
- パソコンと同等に考えてウイルス対策を行う必要
- ウイルス対策ソフト
  - アバスト，ESET，ノートン，ウイルスバスター，マカフィーなどが出ている

コンピュータの脆弱性をなくすこと

- ウイルスはコンピュータ脆弱性を利用して侵入
  - ◆キュリティホールを塞ぐことが必要
- WindowsなどのOSやソフトウェアの修正情報の適用を確実に行う
  - ◆WindowsXPやOffice2007の使用は速やかに止める
  - ◆Windows7は来年初めでサポート停止
- Adobe Acrobat，Office関連ソフト，圧縮/解凍ソフト(+Lhaca)，音楽管理ソフト(iTunes)等々

パーソナルファイアウォール

- パーソナルファイアウォール
  - 不正な外部からのアクセスや意図しない外部へのアクセスを遮断
  - ボットなどのウイルスの活動を防止

11.6.ウイルスに感染した時の処置

パソコン上からの駆除

- 各種の対策を行っていてもウイルスに感染する場合がある．この場合下記の処置を行う
  - 他のパソコンへの感染を防ぐためまずネットワークから切り離す
  - パソコン全体のウイルス検査し駆除
  - 検知できても駆除できないものが存在する場合感染しているファイルを削除，ごみ箱からも削除
  - 削除もできない場合はOSの再インストール実行

番外　サイバー攻撃その他

1.サイバーテロとは

	サイバーテロ	サイバーインテリジェンス (Cyber Espionage)
用語の意味	重要インフラの基幹システムに対する**電子的攻撃**	サイバー空間での**諜報活動**
目的	基幹システムの**機能障害**	機密情報の**窃取**(せっしゅ)
対象	重要**インフラ事業者**等	**政府機関**や先端技術を有する事業者等
主な手段	**不正プログラム**への感染 コンピュータへの**不正アクセス**	
事例	2010年イランの**ウラン濃縮施設**への攻撃 2013年3月20日の**韓国へのサイバ**攻撃	

ZDnet Japanセキュリティセミナー2013秋　警察庁　山本貴之氏　資料より作成

(1)イランのウラン濃縮施設への攻撃

- 利用されたのは，Stuxnet(スタックスネット)
- 産業用，制御用システムを狙ったマルウェア
  - 5件のWindows の脆弱性を利用し独シーメンスのシステムを攻撃
  - 30人以上が関わり組織的に開発
  - ネット接続されたシステムとクローズネットワークは時々情報の交換を行う
  - まずネット接続されたシステムを攻略，USB経由でクローズネットワークに入り込む
- 犯人は誰

(2)韓国320サイバーテロ2013年3月

- 農協ATM 1万6,000台停止、新韓銀行でインターネットバンキング停止、済州銀行で業務用PCが動作不能
- 放送局、KBSテレビ、MBCテレビ、YTNテレビの情報システムのダウン
- パッチマネージメントサーバ 乗っ取りアップデートファイルとして悪性コードをばらまいた
- 悪性コードは14時まで待機．マスターブートレコード(MBR)を書き換え，Shutdownコマンドで強制終了．MBRが書き換えられているため，OSを見つけることができずPCは再起動不能
- 犯人はだれ

http://techtarget.itmedia.co.jp/tt/news/1306/05/news02.html

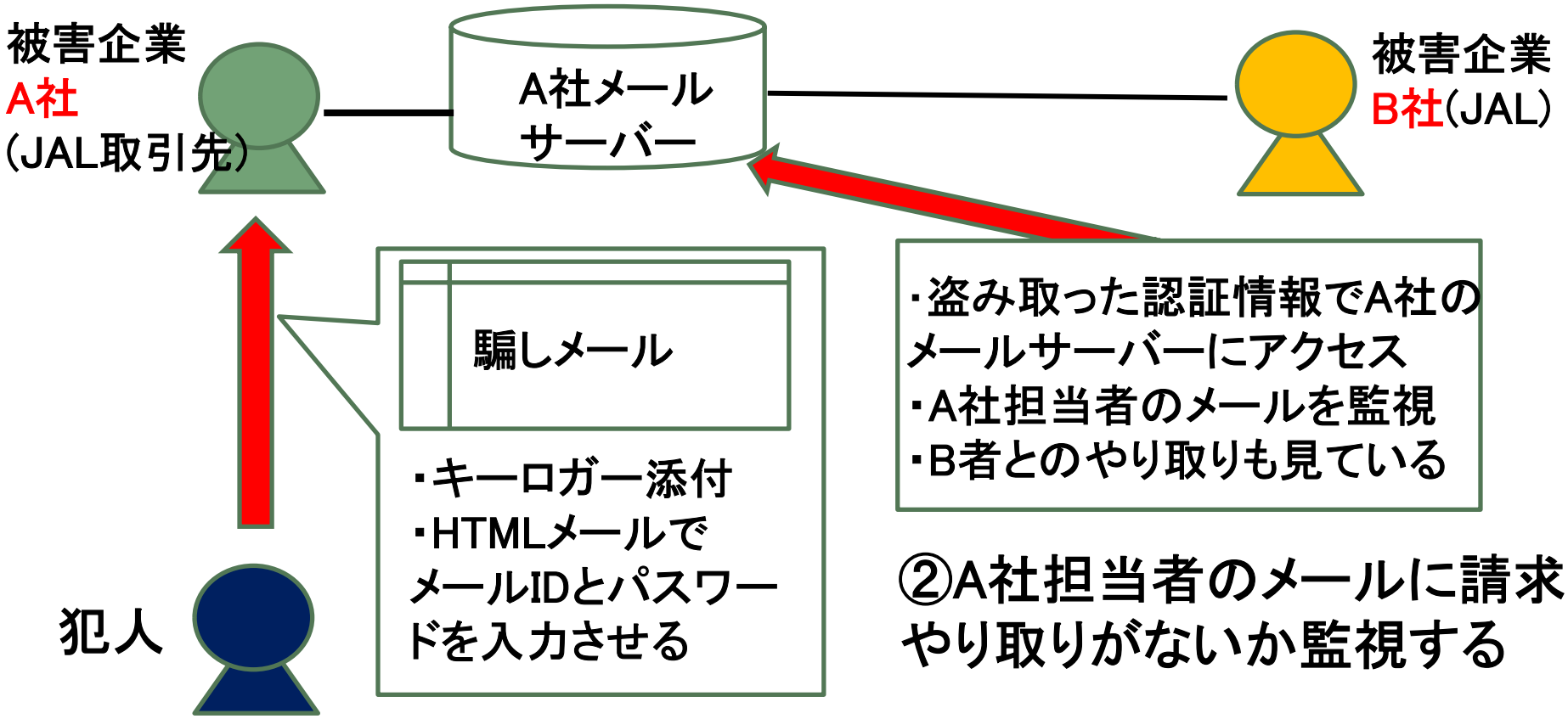
(3)JALビジネスメール詐欺被害

- JAL国内事務所→香港偽口座に3億6千万円、
- JAL米国事務所→香港偽口座に2400万円
- 実際のやりとりに割込む形で請求書変更・口座変更
- メールアドレスはそっくりのもの（CCを含む）
- スカイマークでも未遂事件

- 参考URL
- BEC＝ビジネスメール詐欺は「メール監視」から始まっている
- https://www.nec-solutioninnovators.co.jp/ss/insider/column10.html

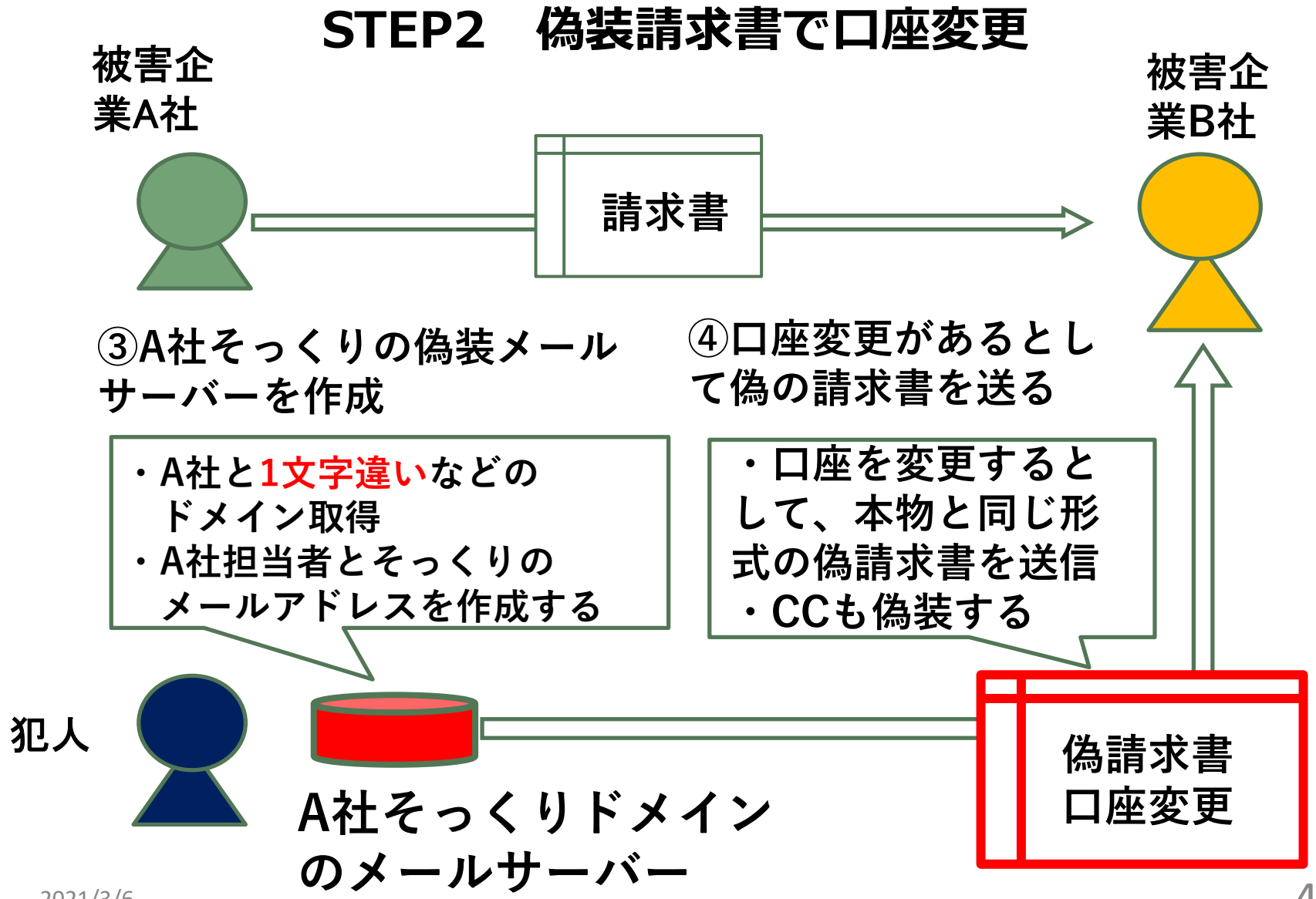
ビジネスメール詐欺の手口

STEP1　メール認証情報の盗み取り



①詐欺メールを送ってメール認証情報を盗み取る

ビジネスメール詐欺の手口2



ビジネスメール詐欺実態（BEC）

- BEC : Business Email Compromise
- 米連邦捜査局（FBI）レポート
  - 2013年10月から2016年5月
  - 1万5668件の被害
  - 損失額は10億5384万9635ドル
- 米国が約9割，米国以外に100カ国
- 日本は3%程度

(4)史上最悪のランサムウェア被害「WannaCry」

- 150カ国35万台以上の被害
- 日本でも日立製作所、川崎市上下水道局、JR東日本高崎支社など600か所・2000端末以上が感染
- http://d-giken.net/kc004/kiji.php?id=KJ000062

ビジネスとしてのランサムウェア

- 「1ファイルお試し復元」「ヘルプデスク」
- 復旧依頼よりも払ったほうが低コスト？と思わせる
- 払うことで犯罪集団の利益になってしまう
- メール対策、脆弱性対策で予防する
- ファイルバックアップの重要性

まとめ

- 悪意のあるソフトウェアはコンピュータウイルスやマルウェアなどと呼ばれる
- コンピュータウイルスの感染
  - 一番危険なのはUSBメモリ
  - 一番多いのはメール及び添付ファイル
  - Webサイトは危険がいっぱい
- コンピュータウイルスの対策
  - ウイルス対策ソフト導入
  - 一定周期でPC全体のスキャン
  - OS，その他の修正情報の適用

FIN