情報科学入門

#14 セキュリティ

Yutaka Yasuda


お問い合わせ
全国情報セキュリティ啓発キャラバン
インターネット安全教室
経済産業省
JNSA
文字サイズの変更 小 大
インターネットの安全な使い方を学びましょう♪
CHECK PC!
全国の安全教室
みんなで学ぼう!!
安全教室の教材
Web版
インターネット安全教室
あなたの地域は？
全国の安全教室
みんなで学ぼう！
安全教室の教材
"Web版"インターネット
安全教室
まずはこちらから！
安全教室とは？
共催団体
関連リンク
全国連絡会議
メンバーページ
あなたの町や学校で「インターネット安全教室」を開催しませんか?
出前講座を希望する団体、学校等を募集中です！
無料
What' New 新着情報
12.10.30 Web版インターネット安全教室サイトを公開しました！⇒
12.10.30 HPをリニューアルしました。
12.05.11 2011年度版インターネット安全教室の字幕付き
Topics トピックス
Web版インターネット安全教室サイトを公開！
経済産業省：http://www.net-anzen.go.jp

情報セキュリティ

- 安全な情報サービスのために維持すべき性質
- 機密性： Confidentiality

  誰がその情報にアクセスして良いか
- 完全性： Integrity

  情報（やソフトウェア）が真正のものか
- 可用性： Availability

  必要な時に確実に情報にアクセスできるか

セキュリティ管理

- 他者との接触によっておびやかされる

  機会の増加：データのやりとり

  状況の変化：オープンなネットワークへの接続

- これら要素別にそのリスクを検討し、対策する

  事故・悪意のある処理によって破られない

  破られた場合の影響を許容範囲に収める

前提

- この場では余り重点的に扱わない事も多い

  物理セキュリティ

  社会工学 (social engineering)

  （内部者による）データ改ざんなどに伴う犯罪行為

  デジタルフォレンジック digital forensics

- 現実には安全管理は一般に総力戦であることを忘れず

  教育も行う（直接的なものだけでなく情報倫理も含め）

脅威

- 機密性・完全性の側面から

  データの改ざん、漏洩、なりすまし、Phishing

- 可用性の側面から

  サービスの妨害、資源の浪費

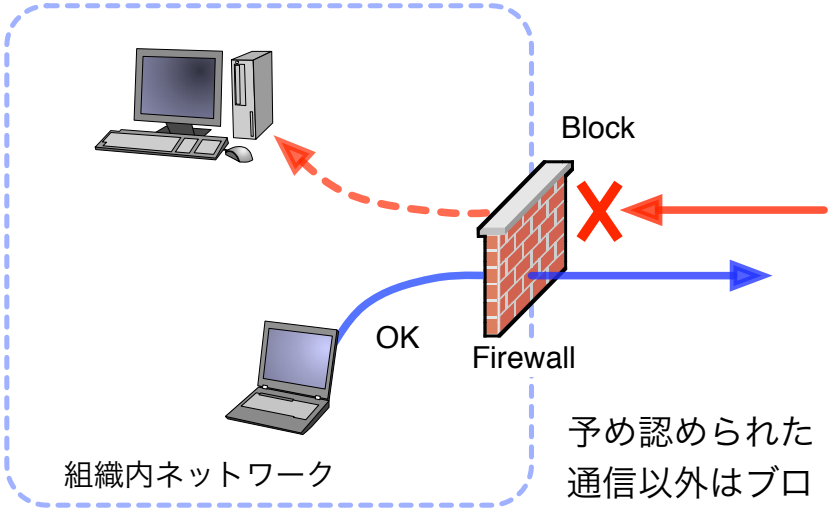
- 対策

  ウィルス検知ソフト、ファイアウォール、etc.

ウィルス検出ソフト

- PC が自身の処理内容を監視
  - ネットワーク、ファイルのアクセス等
  - Malware を検出・検疫・削除
- 問題
  - アップデート vs 亜種
  - ゼロディ攻撃
  - システム負荷（パフォーマンスへの影響）

ファイアウォール



- ネットワーク越しの侵入を防ぐ
  - セキュリティ・ホールを狙った攻撃
  - 漏洩した・推測されたパスワードによるアクセス
  - 予め認められた通信以外をブロックする etc.
- インターネット接続点に設置
  - いまどきは各マシンごとに設定
  - default で on に（Windows なら XP SP2 以降）
- 内と外の区別が無くなった
  - ウィルス感染した内部のPCが攻撃する

侵入口

- セキュリティホール（exploit：脆弱性）

  不正パスワード取得にしてもその後の権限昇格が問題

- 本来はソフトウェアの欠陥（バグ）

  従来から存在する問題だが近年脅威が増しつつある

  インターネット接続＋再攻撃可能なOSの普及

- 実際に多い（報告されているだけでも）
- 基本的にはアップデートで対応

  ゼロディ問題（再び）


IPA
独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan
Google™カスタム検索
検索
IPAについて
サイトマップ
お問合せ
ENGLISH
HOME
情報セキュリティ
ソフトウェア・エンジニアリング
IT人材育成
情報処理技術者試験
未 踏
国際標準の推進
HOME >> 情報セキュリティ >> 緊急対策情報・注意喚起 一覧
情報セキュリティ
ENGLISH
読者層別
個人の方
経営者の方
システム管理者の方
技術者・研究者の方
緊急対策情報
届出・相談
ウイルスの届出
不正アクセスの届出
脆弱性関連情報の届出
情報セキュリティ対策
制御システム
ウイルス対策
ボット対策
不正アクセス対策
脆弱性対策
対策実践情報
暗号技術
セキュリティエコノミクス
情報セキュリティ認証関連
JISEC
JCMVP
セミナー・イベント
緊急対策情報・注意喚起 一覧
2012年度
12月12日掲載 Adobe Flash Player の脆弱性対策について(APSB12-27)(CVE-2012-5676等)
11月07日掲載 Adobe Flash Player の脆弱性対策について(APSB12-24)(CVE-2012-5274等)
10月17日掲載 Oracle Java の脆弱性対策について(CVE-2012-5083等)
10月09日掲載 Adobe Flash Player の脆弱性対策について(APSB12-22)(CVE-2012-5248等)
09月24日更新 【緊急対策情報】Internet Explorer の脆弱性の修正について(MS12-063)(CVE-2012-4969等)
08月31日掲載 【緊急対策情報】Java の脆弱性の修正について(CVE-2012-4681)
08月22日掲載 【緊急対策情報】Adobe Flash Player の脆弱性の修正について(APSB12-19)(CVE-2012-4163等)
08月15日掲載 【緊急対策情報】Adobe Flash Player の脆弱性の修正について(APSB12-18)(CVE-2012-1535)
08月15日掲載 【緊急対策情報】Microsoft Office 等の脆弱性の修正について(MS12-060)(CVE-2012-1856)
07月11日掲載 【緊急対策情報】Microsoft Office 等の脆弱性の修正について(MS12-046)(CVE-2012-1854)
07月11日更新 【緊急対策情報】Microsoft Windows 等の脆弱性の修正について(MS12-043)(CVE-2012-1889)
06月13日掲載 【緊急対策情報】Internet Explorer の脆弱性の修正について(MS12-037)(CVE-2012-1875等)
05月25日掲載 「LAN-W300N/R」シリーズにおけるセキュリティ上の弱点（脆弱性）の注意喚起
05月23日掲載 Android OSを標的とした不審なアプリに関する注意喚起
05月07日掲載 【緊急対策情報】Adobe Flash Player の脆弱性について(APSB12-09)(CVE-2012-0779)
04月24日掲載 複数のジャストシステム製品におけるセキュリティ上の弱点（脆弱性）の注意喚起
04月11日掲載 【緊急対策情報】
http://www.ipa.go.jp/security/index.html

コンピューターとインターネット セキュリティ | Microsoft セーフティとセキュリティ センター

www.microsoft.com/ja-jp/security/default.aspx

Microsoft
セーフティとセキュリティ センター
コンピューター セキュリティ, デジタル プライバシー, オンライン セーフティ

日本 変更 | すべての Microso

Microsoft Security を検索

ホーム | セキュリティ | プライバシー | 家族 | リソース

ワールドワイド | サポート | ニュースレ

コンピューターを無料で保護!

保護
Microsoft Security Essentials の無料ダウンロード
コンピューターをウイルス、スパイウェアなどのマルウェアから守ります。

更新
Windows Update を起動
最新のセキュリティ更新プログラムをダウンロードしてインストールし、オンラインのコンピューターの安全性を高めます。

修正
Microsoft Safety Scanner を実行
ウイルスやスパイアなどのマルウェ感染している可能ある場合は、コンーターをスキャンください。

7月の？

目的別メニュー

- セキュリティ更新プログラム、ツールをダウンロードする
  - Microsoft Update でセキュリティ更新プログラムをダウンロードする
  - 無料のウイルス対策プログラムをダウンロードする

マイクロソフト セキュリティ アドバイザリ 2982792 を公開
2014 年 7 月 11 日に マイクロソフト セキュリティ アドバイザリ 2982792「不適切に発行されたデジタル証明書により、なりすましが行われる」を公開しました。

最新のセキュリティ更新プログラムをインストール
2014 年 7 月 9 日に 6 件のセキュリティ情報を公開しました。更新プログラムをインストールするには

7 月のセキュリティ更新プログラム

"http://www.microsoft.com/ja-jp/security/default.aspx" のメニューを表示

http://www.microsoft.com/japan/protect/default.mspx

誤：感染する機会が無ければ良いのではないか？

- IPA 2010/12/6 【今月の呼びかけ】

  ウェブサイトを閲覧しただけでウイルスに感染させられる “ドライブ・バイ・ダウンロード” 攻撃に注意しましょう!

- ドライブ・バイ・ダウンロード

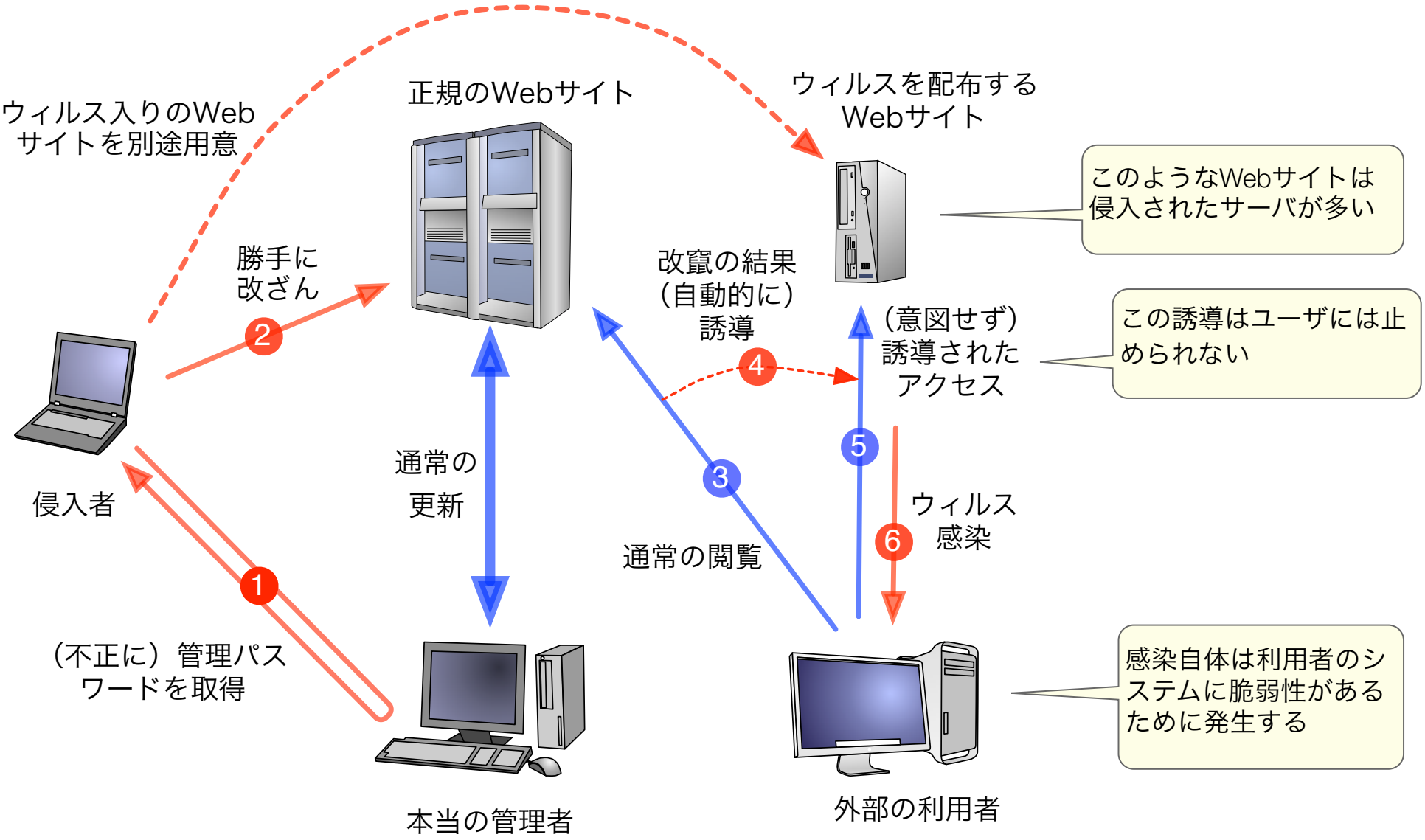
  悪意のあるWebサイトを閲覧しただけで感染させられる手法（セキュリティ・ホールを衝く）

- 誤：怪しいサイトを意図して閲覧しなければ良い

  正当なWebサーバの改竄もあり得る（ガンブラー）

- 標的型攻撃の増加（2011年）

事例：ガンブラー（手法）

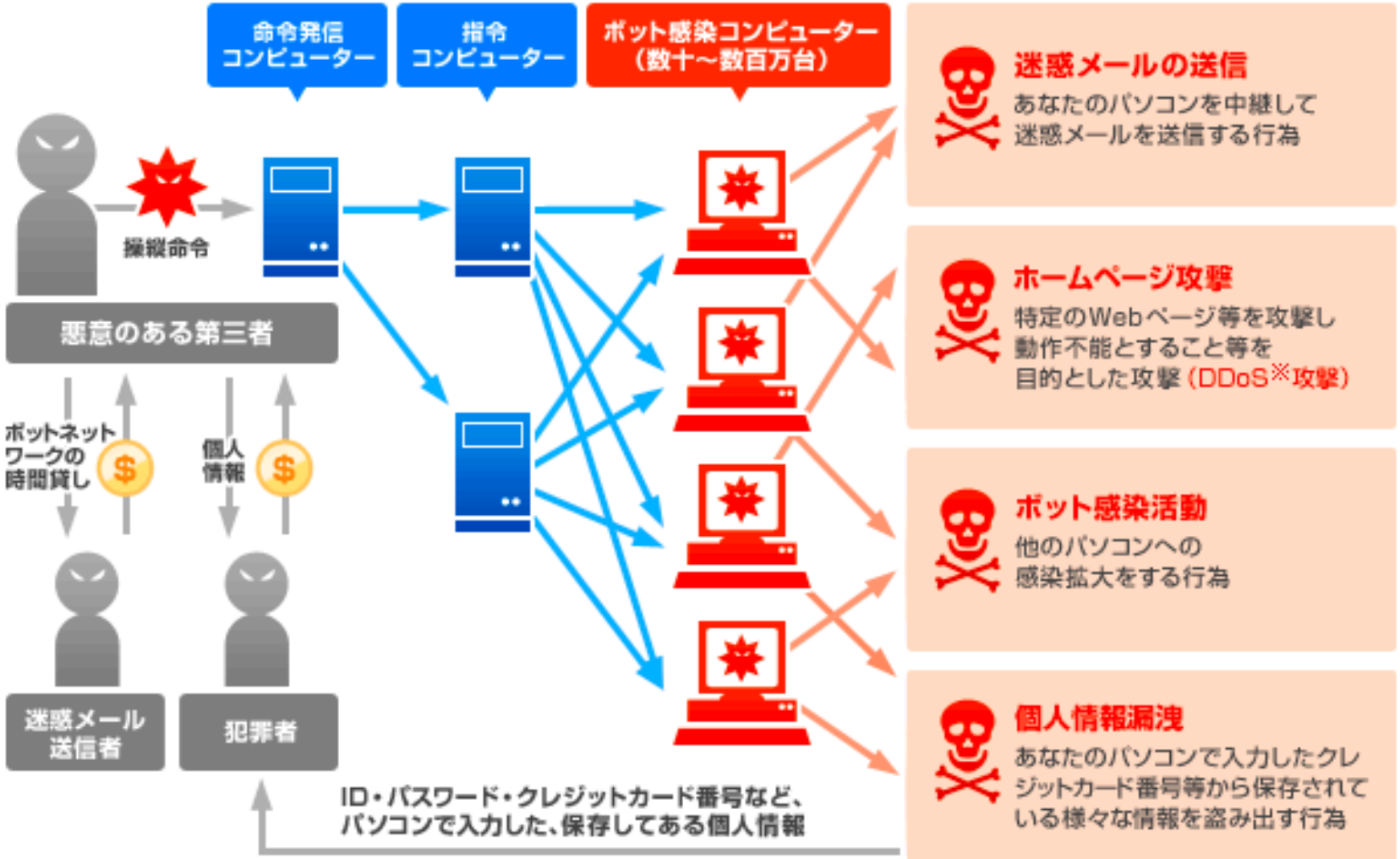

ウィルス入りのWeb
サイトを別途用意
正規のWebサイト
ウィルスを配布する
Webサイト
このようなWebサイトは
侵入されたサーバが多い
勝手に
改ざん
2
改竄の結果
（自動的に）
誘導
4
（意図せず）
誘導された
アクセス
この誘導はユーザには止
められない
侵入者
通常の
更新
3
5
ウィルス
感染
6
通常の閲覧
1
（不正に）管理パス
ワードを取得
感染自体は利用者のシ
ステムに脆弱性がある
ために発生する
本当の管理者
外部の利用者

Botnet

- ボット(Bot)
  - 悪意を持った誰かによってネットワーク越しにコントロールされているマシン
  - 持ち主が知らない間に遠隔操作用のプログラムを仕込まれてしまう
  - そのうちに他のマシンの攻撃に加担
  - そのような状態にあっても持ち主は気づかない
  - ネット上に大量に存在し、組織的に利用 → **Botnet**
- 愉快犯ではなく犯罪目的

サイバークリーンセンターによる2008年6月の国内ボット感染者数調査（推定）
「ブロードバンドユーザ約3000万人のうち約30万人（感染率約1%）」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/ippan19.htm

ボットネットによる脅威



https://www.ccc.go.jp/ サイバークリーンセンター

感染経路

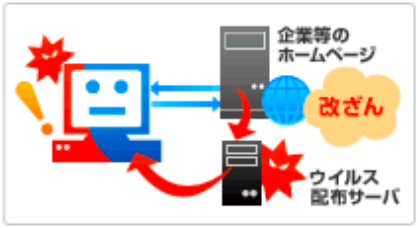
- 多様な経路
- 脆弱性が侵入口
- 既に利用者の不注意といった問題ではない

経路1 ネットワーク感染型

Windows等の基本ソフトや、その他のプログラムのセキュリティホール（ぜい弱性）や設定の不備を悪用し感染するタイプ。インターネット等のネットワークに接続するだけで感染する。

経路2 メール添付感染型

メールの添付ファイルをクリックし感染するタイプ。

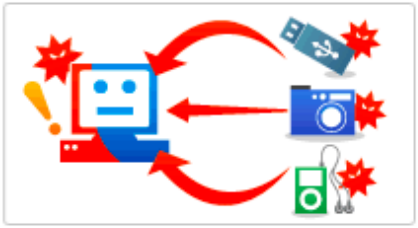


経路3 Web閲覧感染型

ブラウザで閲覧したホームページに埋め込まれたウイルスをダウンロードして感染するタイプ。ホームページを見ただけで感染することもある。

経路4 Web誘導感染型

迷惑メールのURL等をクリックしアクセスしたホームページからウイルスをダウンロードして感染するタイプ。



経路5 外部記憶媒体感染型

USBメモリ、デジタルカメラ、ミュージックプレーヤーなどの外部記憶媒体を介在して感染するタイプ。

https://www.ccc.go.jp/ サイバークリーンセンター

不正・犯罪行為への加担

- SPAM 送信
- DoS 攻撃（Denial of Service）
- さらなる感染
- ついで(?)にキースキャンなど

行動管理

- 私たちは何をすればよいか
- 「インターネットの歩き方」とは何だ

IPA 情報セキュリティ「個人の方」http://www.ipa.go.jp/security/personal/

知る

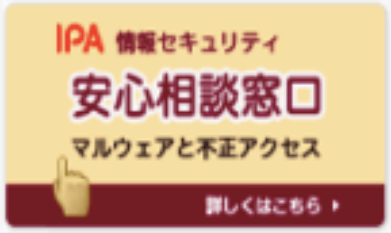
- 情報セキュリティ・ポータルサイト「ここからセキュリティ！」
- これだけはやろう！セキュリティ対策
- オンラインゲームを楽しむ前に--3つのセキュリティポイント
- ウイルス感染を防ぐためのポイント
- 情報漏えいを防ぐためのポイント
- 侵入を防ぐためのポイント
- 知っておきたい注意点
- ウイルスの届け出状況
- コンピュータウイルス用語集
- 届出ウイルス一覧

守る

- ウイルス対策
- ファイル交換ソフト(Winny等)による情報漏えい防止策
- スパイウエア対策
- フィッシング対策
- 送信メールの情報漏えい防止策
- ワンクリックによる料金請求の防止
- 一般家庭における無線LANのセキュリティに関する注意

相談する（無料）

- 情報セキュリティに関して困った場合は、お気軽に



入手する

- 情報セキュリティ対策教材のご案内
- 情報セキュリティ関連コンテンツ
- 出版物のご案内
- 普及啓発資料のご案内

行動管理

- オンラインゲーム設定
  - パソコン購入直後のセキュリティ設定
  - インターネット利用時のセキュリティ設定
  - メイル利用時のセキュリティ設定
- ウィルス感染を防ぐ
- 侵入対策
- 情報漏洩防止
- スパイウェア対策
- Phishing 詐欺対策
- ワンクリック詐欺防止
- 無線LAN設定
- etc. etc.

IPA 情報セキュリティ「個人の方」http://www.ipa.go.jp/security/personal/

Phishing 詐欺（手法）

- 例：
  1. 銀行を装ってオンライン口座にアクセスさせるようなメイルを送る（「住所の確認をしています」etc.）
  2. 書かれていたURLをクリックすると全然違うサイトへ
  3. しかし見た目はいつもの login 画面そっくり
  4. いつものユーザ名とパスワードを入力（これを取得）
  5. あたかもパスワードを打ち間違えたかのようなメッセージを出して、本物の銀行の login 画面に移動させる
- 予備知識

  メイルの送信者欄は全く信用できない（擬装可能）

IPA 情報セキュリティ「個人の方」フィッシング対策 http://www.ipa.go.jp/security/personal/protect/phishing.html

Phishing 詐欺（対策）

- アクセス先の確認

  そもそもパスワードを入力させるような作業がメイルで来ることはない

- メイルの URL を信用しない

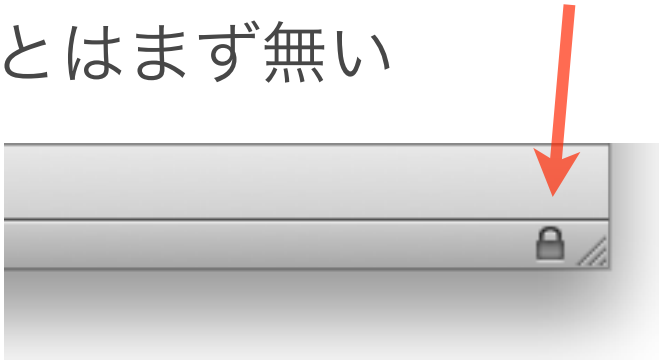
  ブックマークなり信頼できるリンクからアクセス

  URL のドメイン名を確認

- HTTPS によるアクセス

  パスワードを暗号化無しで入れることはまず無い

  https://... なら電子証明書を確認



IPA 情報セキュリティ「個人の方」フィッシング対策 http://www.ipa.go.jp/security/personal/protect/phishing.html

まとめ

- ネットワーク越しの攻撃
  - 侵入（データの取得やコントロール目的）
  - DoS （サービス妨害）
  - ボット
- 対策
  - システムアップデート、ウィルス検出ソフト、ファイアウォール、etc.
  - 個別対応の積み重ねしかない
  - 技術・教育・社会制度（法）も含めて前進
- 加害者とならないよう