本資料について

- 本資料は下記書籍を基に作成されたものですが、内容を正確に示せているかどうかは保証できません。正しく知りたい方は、書籍の方を参照してください。

書籍名：体系的に学ぶ　インターネットセキュリティ

著者：神埼洋治・西井美鷹

発行者：瀬川弘司

発行日：2008年1月28日

発行：日経BPソフトプレス

インターネットセキュリティ

2

070427641
加藤諒

背景

- インターネットの普及、生活に不可欠なものに
- 不正侵入や詐欺など危険性の心配
- インターネットの危険と安全の理解が必要

ファイアウォール

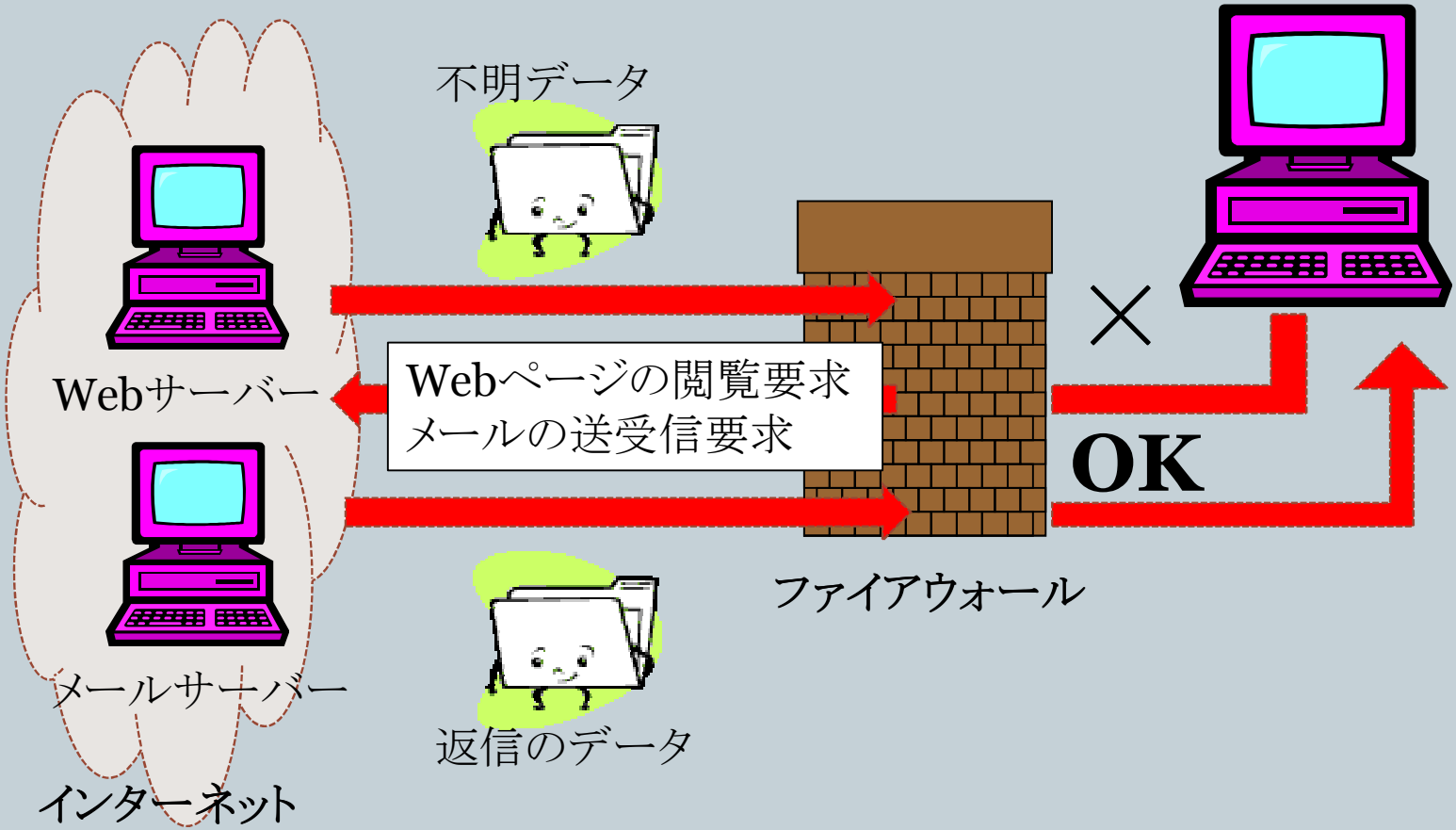
- ファイアウォールとは
  - 直訳すると「防火壁」、実際は「セキュリティ機能付きの扉」の役割
  - 外部からやってくるデータをチェックし、内部ネットワークに不正に侵入するのを防止する
- 「ファイアウォール機器」と「パーソナルファイアウォール」
  - ファイアウォール機器

    →ルータなどの専用機器にファイアウォールが搭載された機器。外部と内部ネットワークとの境目におかれ外部から内部への不正侵入を防ぐ役割を担う。
  - パーソナルファイアウォール

    →ファイアウォールの役割をするソフトウェア。コンピュータが外部に向けて勝手にデータを送信して情報流出しないよう監視することが主な目的。

ファイアウォール

- ファイアウォールの基本的なしくみ



ファイアウォール

- ファイアウォールが不正を見分けるしくみ
- セキュリティポリシー・・・セキュリティに関する組織内の基本的な方針や指針
- 「パケットフィルタリング」と「アプリケーションゲートウェイ」

・パケットフィルタリング

「アドレスフィルタリング」＋「ポートフィルタリング」

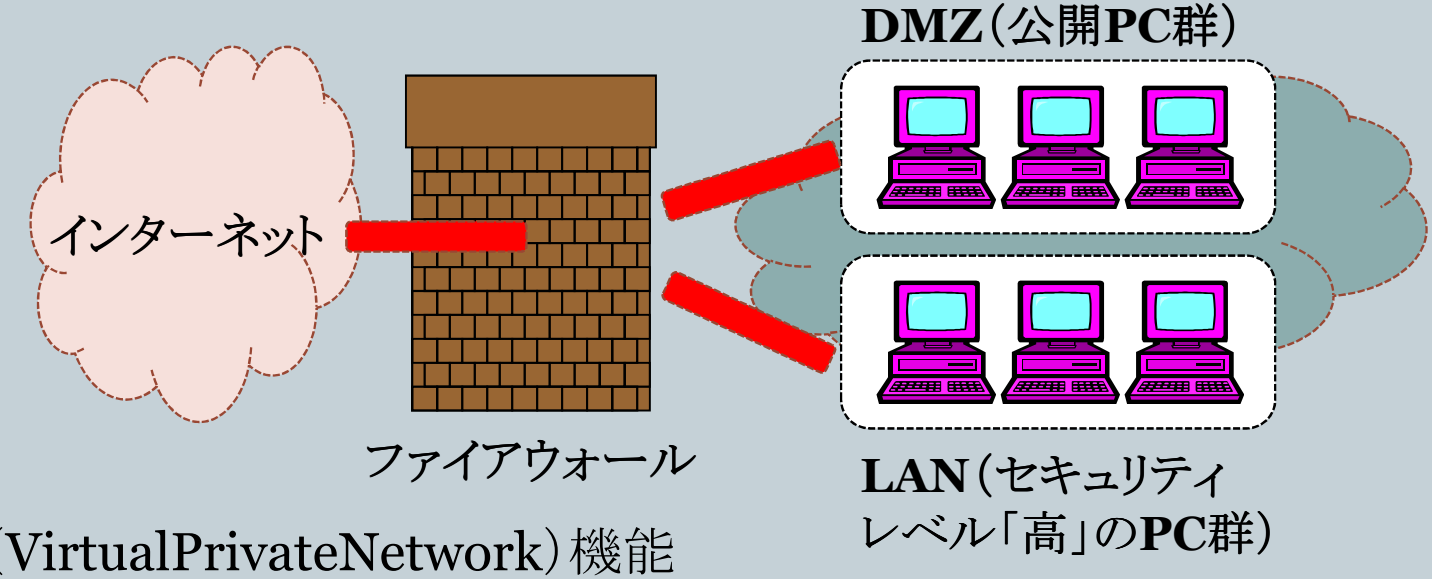
・アプリケーションゲートウェイ(プロキシ)

「プロキシサーバー」を設置する

方式	メリット	デメリット
パケットフィルタリング	・制御処理が高速 ・設定がシンプル	・細かなパケット制御が難しい ・パケットのデータの内容まではチェックできない
アプリケーションゲートウェイ	・プロトコルごとに詳細な設定可能 ・データの内容までチェックできる	・チェックが複雑になると処理 ・システムが連携しやすくなってしまう

ファイアウォール

DMZ（DeMilitarizedZone）機能
DMZは「非武装地域」と訳され、Web、ワークとは隔離する領域である。インターネットから不正な攻撃から内部ネットワークを守る役割がある。



VPN（VirtualPrivateNetwork）機能
これはインターネット回線に認証や暗号化技術を用いて、仮想的な専用回路を創りだすものである。VPNの構築によりコストのかかる専用回線の設置が不要となり、インターネット上で支社間との重要なデータのやり取りもセキュアに行うことができる。

クラッカー

- クラッカーとは

  •クラッキング・・・インターネットから内部ネットワークに勝手に侵入する、侵入しようとする行為

  •クラッカー・・・クラッキングする人

- ハッカー≠犯罪者

  ハッカー・・・コンピュータなど専門的な知識に長けた人

  アタッカー・・・アクセス制限のかかったネットワークに侵入しようと攻撃を試みる人

- ファイアウォールがない場合、

  クラッカーはすべてのポートにアクセスし（ポートスキャン）、どんなサービスが動いているか、どのポートが利用可能状態になっているか調べる。ポート番号によって稼働しているサービスがわかる。やたらポートが開いていたり、セキュリティの隙間、穴（セキュリティホール）から侵入してくる。

クラッカー

- さらに詳しく侵入手口を説明する。

開いているポートを探し出して侵入する

(1)Webサイトに対してポートスキャン→利用可能なポート番号がわかる

(2)ポート番号から稼働しているサービスの種類が分かる

(3)稼働中サービスに対してデータを送り返信が見る→起動中サービスのソフトとバージョンがわかる

(4)知り得たソフトの中でセキュリティホールがあるもの、セキュリティチェックが甘いものを調べる。

(5)クラッキングを仕掛ける

セキュリティホール、脆弱性

- セキュリティホール・・・

  「安全性の落とし穴」と訳され、ソフトウェア上のバグや設計上のミスなどの不具合のうち、安全面で問題となるものを指す。

- 脆弱性・・・

  セキュリティホールのうち本来確保されていなければならない安全性に対して設計が甘い場合に呼ばれる言葉である。

- セキュリティホールを塞ぐには、対策パッチをインストールするしかない

  →定期的なソフトのメーカーHP、またハードウェアのメーカーHPも目を通すことが大切

クラッカー

- クラッカーが無差別に侵入してくる理由
  - ゲーム感覚でのハッキング
  - 情報を盗み出し、売る
  - 踏み台、ボット

踏み台：クラッカーがシステム管理者に気づかれぬようにコンピュータをのっとり、不正アクセスやスパムの大量配信などの中継地点に利用すること

ボット：コンピュータにボットソフトウェアを侵入させ普段はひ　そませておき、遠隔操作によって一斉に特定のサーバーを攻撃するDos攻撃や大量のスパムの配信にコンピュータやサーバーなどネットワークそのものを利用する

コンピュータウィルス

- コンピュータウィルスとは

  →コンピュータを誤作動させる、プログラムとデータを破壊する
  コンピュータ使用者の意志とは異なった動きをし、不利益をもたらすプログラム

  誤動作しなくとも不正ならウィルスである

- ウィルスはと大きく3つに分類できる

  •トロイの木馬：他のコンピュータに感染しない。

  •ワーム：他のコンピュータに感染し、単体で動作する。

  •狭義のコンピュータウイルス：

  　他のコンピュータに感染し、プログラムやコードに寄生して動作する。

Nimda（ニムダ）

- 名称：W32/Nimda-Mm
- 別名：Nimda、Conceput、CodeRainbow
- タイプ：実行ファイル感染型、自動自己実行型、ワーム型、JavaScript型、トロイの木馬の機能も
- 活動場所：Windows、メール、HP、IISサーバー
- 発見日：2001年9月

・セキュリティホールを放置したままのIISサーバーを探して侵入する。

・ウイルスファイルを作成後、ウイルス実行のためのJavaScriptをHPに埋め込む。これにより、HPにアクセスしたユーザーは閲覧しただけでNimdaに感染してしまう。アドレス帳やブラウザの履歴からメールアドレスと思われる情報引き出し、ウイルスコードを埋め込んだ添付ファイルをこれらのアドレスに送信し感染を増やしていく。Nimdaは独自のメール送信機能も装備しているため、送信した履歴が残らない。

・ネットワークで共有されているほかのコンピュータにも寄生して感染を増やしていく感染は爆発的に増え続ける。

・被害は複数ある。多くのファイルやレジストリが破壊されたり上書きされるので、コンピュータの動作が不安定になる。セキュリティが大幅に低下する。大量のウイルスメールを送信する。ブラウザの履歴から検索したアドレスにまで送信してしまうため、多大な規模の迷惑となる。発生から数日間は膨大なトラフィックに耐え切れずダウンしてしまうサーバーもある。

ウイルス侵入ルート

- ウイルス侵入ルート
  - メールに添付されて侵入
  - バックドアから侵入
  - HP閲覧によって感染
  - Windowsのせいでウイルス蔓延

ウイルス感染防止と対策

- ウイルス感染の防止と対策
  - ウイルス対策ソフトを導入することが一番
  - 大きく2つの機能を持つ

    （1）ウイルスに感染してしまったファイルからウイルスのコード部分を取り除き、さらなる感染や増殖を防ぐ機能

    （2）コンピュータ内のウイルスを検出する機能
- ウイルス対策ソフトは、ウイルスを探し出すのでウイルススキャンソフト、感染を防ぐことができるのでワクチンソフトとも呼ばれる。

ワクチン

- ワクチン・・・生物学におけるワクチンと同様に、免疫記憶を利用してウイルスの検知や削除を行う
- 免疫記憶＝ウイルスのコードやプログラム内の特長的な部分をデータベース化してたもの

- このデータベースを利用してウイルスを探し出す方法を「パターンマッチング」という。パターンマッチングには3つの方法がある。
  - ウイルスコードと完全に一致するか比較→ウイルスのすべてのコードをワクチンのウイルスデータベースに記憶させておき、これをウイルスと思われる部分と比較する
  - チェックサムを使用した比較→チェックサムとはコードを数値として扱い、このうちのいくつかの合計値を求め、それを比較する。
  - コードの一部だけ抜き出しての比較→コードの一部を抜き出して比較する。
- すでにウイルスの構造が解析されているものにしか通用しない。

ワクチン

- 「ヒューリスティック」という方法もある
- ウイルスの行動パターンを解析し、ワクチンのデータベースに登録しておいて、同じような行動パターンをするファイルやプログラムがないかコンピュータの中を監視しておくしくみ
- 数多くの未知のウイルスにも対応できるが、ウイルスの行動パターンに似た通常ファイルを感染ファイルと誤認してしまう場合がある。そのため数多くの行動パターンを登録する必要がある。

ウイルスに感染したら

- ウイルス感染後の処理
  - ウイルスコードを取り除く(コードを削除するか、影響のないコードに書き換える)
  - ウイルスに感染したファイル自体の削除
  - 特殊なフォルダ(ウイルス対策ソフトが作成したフォルダ)への起動
  - 何もしない、放置する
- 最良はファイルの削除だが、重要なファイルが感染している場合はこれをしてはいけない。ので、無難にウイルスコードを取り除くのがよい。

ネット詐欺

- ネット詐欺
  →インターネットやメールを利用した詐欺行為のこと
  さまざまな種類がある
  ・不正請求（架空請求）
  ・ワンクリック詐欺
  ・フィッシング詐欺
  ・ネットオークション詐欺

  ここ数年、急激に被害数が増加している

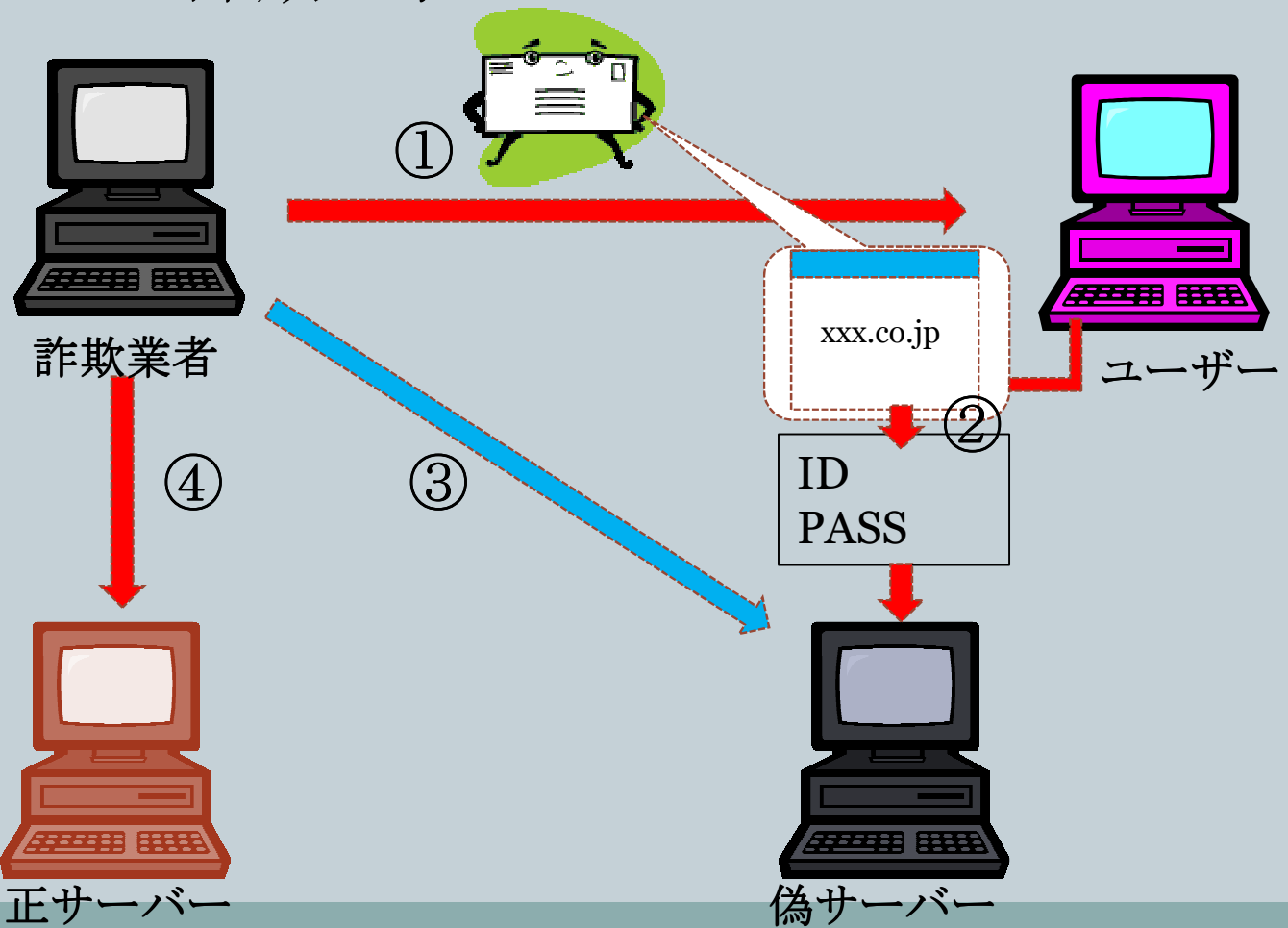
フィッシング詐欺

- 概要
  - フィッシング詐欺

    ……銀行やクレジット会社など金融きかんや、Yahoo！などのようにインターネットでの決済システムを持った大手企業を装い、偽のメールやHPを作って、クレジットカードの情報やID、パスワードなどの個人情報を不正に入手し、それを悪用して金銭を勝手に引き出したり、騙し取る犯罪
  - 2004年の調査で、過去1年間に被害者数はアメリカだけで198万人、被害総額にして約24億ドルに上る。
  - フィッシングは「Phishing」と書き、釣りを意味する「Fishing」と「洗練された、高尚な」を意味する「Sophisticated」の合成語といわれている

フィッシング詐欺

- フィッシング詐欺の手口



フィッシング詐欺

- 見破る方法
- URLでさえうまく偽装する＝見ただけじゃ見分けにくい
  これは、HTML形式のメールを悪用することで偽装できる。

  zzz.co.jp

  このようにタグを入力するとURLにはxxx.co.jp、表示は zzz.co.jpの内容と異なったものにできる。
- HTML形式メールを受信拒否する設定のユーザーが増えている。

- セキュリティ対策ソフトの使用
- IE7のフィッシング詐欺検出機能

おわり