(3)「情報セキュリティ」講義資料の作成

末吉　豊

「情報セキュリティ読本 三訂版」(情報処理推進機構，実教出版，2009，144ページ，500円）を安全工学教育の教材として用いることができるように，講義資料としてパワーポイントファイルを作成した。

情報処理推進機構（Information-Technology Promotion Agency，IPA）は経済産業省所管の独立行政法人として，情報処理の振興を図るための様々な事業を行っている機関である。具体的には，IPA セキュリティセンターを中心に，情報セキュリティに関する普及啓発活動，ウイルス・不正アクセス対策，情報システムの脆弱性への取り組み，IT セキュリティ評価・認証，暗号技術調査・評価，暗号モジュールの試験および認証制度などの事業に取り組むほか，情報セキュリティに関する最新の情報を IPA セキュリティセンターのホームページ（http://www.ipa.go.jp/security/）で提供している。

「情報セキュリティ読本 三訂版」は小冊子であるが，

第１章　今日のセキュリティリスク
第２章　情報セキュリティの基礎
第３章　見えない脅威とその対策－個人レベルのセキュリティ対策－
第４章　組織の一員としてのセキュリティ対策
第５章　もっと知りたいセキュリティ技術
第６章　情報セキュリティ関連の法規と制度
第７章　IPA セキュリティセンターの活動

からなり，今日の情報化社会におけるセキュリティリスクと様々な攻撃手法，それらに対する個人レベルおよび組織の一員としてのセキュリティ対策が，技術的な側面も含めてわかりやすく説明されている。また，情報セキュリティ関連の法規や制度についての解説や情報セキュリティに関する用語集も付いていて，手元においておくと便利である。

講義資料のパワーポイントは，上記の内容をコンパクトにまとめたもので，テキストと併用して使用することを想定している。すべての内容を授業で扱えば，５回分くらいの分量となるが，第１章，第２章，第３章，第４章（または第５章）に絞れば，３回の講義でも使用可能である。なお，今後授業で活用しながら，図表やイラストを挿入するなど，よりわかりやすい内容に変えていきたいと考えている。

情報セキュリティ

講義資料

1

情報セキュリティの教科書・参考書

□ 情報処理推進機構，情報セキュリティ読本
実教出版，500円

参考書

・情報処理推進機構，情報セキュリティ教本
実教出版，2500円

・長崎大学工学部「安全安心工学入門」編集委員会編，安全安心工学入門 第4章
古今書院，2625円

2

第1章 今日のセキュリティリスク

1-1. 今日のセキュリティリスク

1-2. 危険の認識と対策

3

1-1. 今日のセキュリティリスク(1)

□ 手口の多様化

・ボット，フィッシング詐欺，ワンクリック請求など

① 狙われるWebサイト-正規のサイトも要注意-

・Webサイトが改ざんされ，Webサイトを訪れたユーザが被害に遭う事例が多発(2008年)

4

1-1. 今日のセキュリティリスク(2)

② 巧妙化するフィッシング詐欺-うっかりしていると騙される?-

・偽のWebサイトにユーザを誘導し，個人情報やクレジットカード番号などを盗み取る

・2003年頃から社会問題化，手口も巧妙化

③ 増加する金融取引被害-便利と危険は隣り合わせ-

・返品を装い，オンラインショップをスパイウェアに感染させ，ネットバンキング用のパスワードを盗み取る

・ネットカフェのパソコンにキーロガーを仕込む

・フィッシング詐欺で取得した暗証番号で不正送金

5

1-1. 今日のセキュリティリスク(3)

④ P2Pファイル交換ソフトを介した情報漏えい

-知らない間に情報漏えい-

・P2Pファイル交換ソフトのWinny，Shareによる情報漏えい事件が多発

・漏えい後，時間が経つほど，情報が拡散

・2004年頃から始まり，原発，自衛隊，病院，警察，刑務所など公共機関の情報が漏えい

・2006年に漏えい件数が増加，現在も増加中

6

1-1. 今日のセキュリティリスク(4)

⑤ 犯罪に使われるインターネット-共犯者募集中-
- 犯罪者がインターネット掲示板で知り合う
- 携帯サイトやインターネット掲示板で，殺人の依頼，強盗・窃盗の共犯者募集
- 携帯サイトへの犯罪予告(秋葉原事件)
- 出会い系サイトでのトラブル

7

1-2. 危険の認識と対策(1)

① インターネットに潜む危険
- Webページを閲覧するだけで感染
  Webサーバにウイルス，スパイウェアが仕込まれている危険がある
- リンクをクリックするだけで，不正請求される
  ワンクリック不正請求，個人情報の盗難
- 不正なプログラムを誤ってダウンロード
  Webサイトに不正なプログラムが置かれている

8

1-2. 危険の認識と対策(2)

② メールに潜む危険
- スパムメール(迷惑メール)
  スパムフィルタの利用，スパムメールは削除
  掲示板やブログにメールアドレスを書かない
- マルウェア(ウイルス，スパイウェア，ボット)
  多くは，メールの添付ファイルで感染拡大
- フィッシングメール
  メールを使って，フィッシングサイトに誘導

9

1-2. 危険の認識と対策(3)

③ 日常業務に潜む危険
- 会社からの資料持ち出し時に情報漏えい
- 不要書類の破棄から情報漏えい
- 歓談時の何気ない会話から情報漏えい

10

1-2. 危険の認識と対策(4)

④ 危険への対処法
- セキュリティリスクを知る(第2章)
- マルウェアについて理解する(第3章)
- 効果的なセキュリティ対策を施す(第3，4章)
- 情報セキュリティ技術について知る(第5章)
- 情報セキュリティに関する法律について知る(第6章)

11

第2章 情報セキュリティの基礎

2-1. 情報セキュリティとは
2-2. 外部のリスク要因
2-3. 内部のリスク要因
2-4. 情報リテラシーと情報倫理

12

2-1. 情報セキュリティとは(1)

① 情報セキュリティの基本概念

・機密性

許可された者だけが情報にアクセスできる

IDやパスワードの設定で情報漏えいを防ぐ

・完全性

情報や情報の処理方法を正確で完全にする

ホームページや情報システムの改ざんを防ぐ

13

2-1. 情報セキュリティとは(2)

・可用性

必要なときに情報にアクセスできる

ウイルス感染やシステムダウンを防ぐ

(役所や銀行のシステムダウンは影響大)

14

2-1. 情報セキュリティとは(3)

② 情報資産とリスク・インシデント

・情報資産

財務, 人事, 顧客, 戦略, 技術等の資産

・リスクとインシデント

リスク(情報資産を脅かす内外の脅威)

インシデント(情報資産が損なわれた状態)

・リスクの要因

組織外部からの攻撃, 組織内部の脆弱性

15

2-2. 外部のリスク要因(1)

① マルウェア

・ウイルス

他のファイルやプログラムに寄生し, 不正な行為を行う

・スパイウェア

利用者や管理者の意図に反してインストールされ, 個人情報やアクセス履歴を収集する

16

2-2. 外部のリスク要因(2)

・ボット

コンピュータに感染し, 感染したコンピュータを外部から操作

・マルウェアは2000年代に急増

・最近は巧妙化・凶悪化し, 気付きにくい

17

2-2. 外部のリスク要因(3)

② 外部からの侵入(不正アクセス)

・攻撃用ツール

スニファ(ネットワークを盗聴)

ポートスキャン(ポートの状態を調べる)

パスワードクラッキング(パスワードを破る)

・侵入行為(第5章)

事前調査, 権限取得, 不正実行, 後処理の4段階. 攻撃用ツールをパッケージ化

18

2-2. 外部のリスク要因(4)

・不正行為の種類
情報漏えい, 盗聴, 改ざん, なりすまし, 破壊, コンピュータの不正使用
不正プログラムの埋め込み, 踏み台

19

2-2. 外部のリスク要因(5)

③ サーバへの攻撃(サービス妨害)
・サーバへの攻撃は影響が大きい
・DDos攻撃(分散Dos攻撃)
Dos攻撃(Denial of Services):サーバに大量のデータを送り, 機能低下させる攻撃
DDos攻撃:多数のコンピュータからDos攻撃
DDos攻撃を仕込むウイルス, ボットも登場

20

2-2. 外部のリスク要因(6)

・メール攻撃
メールサーバに大量のメールを送りつける
メールサーバの転送機能を悪用

21

2-3. 内部のリスク要因(1)

① 情報システムの脆弱性
・ソフトウェアの脆弱性
・ID, パスワードのずさんな管理
・侵入されやすいシステム(セキュリティホール)
・OS(オペレーティングシステム)の脆弱性
対策:Windowsなどのセキュリティパッチ(修正プログラム)を適用し, 脆弱性を解消

22

2-3. 内部のリスク要因(2)

・Webブラウザやメールソフトの脆弱性
Internet ExplorerやOutlook Expressの脆弱性を解消しておく
・Webアプリケーションの脆弱性
システムの開発時から脆弱性を除く必要
・脆弱性を悪用する攻撃(第5章)
クロスサイトスクリプティング, SQLインジェクション, DNSキャッシュポイズニング

23

2-3. 内部のリスク要因(3)

② 組織に内在する脆弱性
・外部からの攻撃(1割程度)より, 内部の脅威(紛失・盗難, 漏えい, 誤送信, 内部犯行)が8割強で多い
・紛失・盗難(記憶媒体の持ち出しによる)
・P2Pファイル交換ソフト経由の漏えい(自宅で)
・誤公開・誤送信(誤ったファイルを公開, 送信)
・内部犯行(個人情報の持ち出し)

24

2-3. 内部のリスク要因(4)

・組織の情報セキュリティ対策(第4章)
経営者の関与とリーダーシップ
従業員の理解と協力
守りやすいルール(基準と手順をはっきりと)

25

2-4. 情報リテラシーと情報倫理

・情報リテラシー
情報機器やネットワークを活用する基本能力
(コンピュータの操作, データの作成や整理,
情報検索能力, 情報セキュリティの知識)
・情報倫理(情報モラル, 情報マナー)
1) 他人の誹謗中傷をしない
2) 他人のプライバシーを侵害しない
3) 著作権について知り, 侵害をしない

26

第3章 見えない脅威とその対策
-個人レベルのセキュリティ対策-

3-1. マルウエア-見えない化が進む
3-2. 共通の対策
3-3. 標的型攻撃と誘導型攻撃への対策
3-4. フィッシング詐欺への対策
3-5. ワンクリック不正請求への対策
3-6. 無線LANに潜む脅威とその対策

27

3-1. マルウエア-見えない化が進む(1)

① マルウェアとは?
・コンピュータウイルス, スパイウェア, ボット,
ワーム, トロイの木馬

② マルウェアに感染するとどうなるのか?
・P2Pファイル交換ソフトによる情報漏えい
W32/Antinny, W32/Exponny ウイルス
企業や公的機関から内部資料が流出

28

3-1. マルウエア-見えない化が進む(2)

・パソコンの中の情報をまるごと公開
山田オルタナティブウイルス
パソコン内にWebサーバを立ち上げ, 全ファ
イルをWebページとして公開(暴露ウイルス)
・スパイウェアによる情報の盗みだし
実在の組織名をかたり, 添付ファイル付きメー
ルで感染させる. キーロガーがよく使われる

29

3-1. マルウエア-見えない化が進む(3)

・サイトへの誘導やマルウェアのダウンロード
脆弱性攻撃によりダウンローダに感染
→ マルウェアを次々にダウンロード
(シーケンシャルマルウェア)
・DDos攻撃
ボットネットワーク(数千～数十万台)から攻撃
知らない間にDDos攻撃に加担

30

3-1. マルウエア-見えない化が進む(4)

・ウイルスメールの大量送信やアドレスの詐称
ユーザが気付かないうちに，ウイルスメールを大量に送信，感染を広げる
添付ファイルを開くと感染
・ウイルス対策ソフト停止やアクセス妨害
W32/Sober亜種：ウイルス対策ソフトを停止
W32/Downad：ウイルス対策ソフトベンダーのWebサイトへのアクセスを妨害

31

3-1. マルウエア-見えない化が進む(5)

・その他の症状
インターネットにつなぐだけでウイルスに感染
W32/SQLSlammer：大量のパケットを発信
W32/MSBlaster：コンピュータが再起動を繰り返し，使えなくなる
W32/Mimail亜種：フィッシング詐欺を行う
データファイルの破壊
コンピュータを起動させない

32

3-1. マルウエア-見えない化が進む(6)

③ マルウェア感染の原因
・USBメモリの接続による感染
USB内のプログラムの自動実行機能を悪用
USB→パソコン→USB→…と感染が拡散
USBの自動実行機能を無効化しておく

33

3-1. マルウエア-見えない化が進む(7)

・ファイルのオープンによる感染
メールの添付ファイル，Webサイトからダウンロード，外部媒体など
気を引くファイル名，拡張子，アイコンの偽装
公的機関を装ったメールの添付ファイル
・Webページの閲覧による感染
脆弱性を解消していないとWebページをみるだけでマルウェアに感染することがある

34

3-1. マルウエア-見えない化が進む(8)

・メールの開封・プレビューによる感染
メールソフトやOSの脆弱性を悪用
・ネットワークへの接続による感染
OSの脆弱性を悪用
W32/Downad，W32/Deloderなど

35

3-2. 共通の対策(1)

① 脆弱性の解消
・Windows Updateを自動的に行う
・修正プログラム(パッチ)を手動で実行
・ソフトウェアを最新版にバージョンアップ

② ウイルス対策ソフトのインストールと更新
・ウイルス対策ソフトをインストール，自動更新

36

3-2. 共通の対策(2)

③ パーソナルファイアウォールの活用
・4-4参照

④ Webブラウザのセキュリティ設定
・Internet Explorer で設定
[ツール]→[インターネットオプション]→
[セキュリティ] (設定はできるだけ高く)
不要なサービスや機能は無効にする

37

3-2. 共通の対策(3)

⑤ ネットサーフィンの危険性とその対策
・不審なサイトには近づかない
・安易にダウンロード, インストールしない
・個人情報をむやみに入力しない
・SSL方式接続(https://と鍵アイコン)を確認
・クレジットカードの請求書, 金融機関の利用
履歴をこまめに確認

38

3-2. 共通の対策(4)

⑥ メールソフトのセキュリティ設定
・Outlook Express で設定
[ツール]→[オプション]→[セキュリティ]
・不要な機能やサービスはオフにする

⑦ 不審な添付ファイル, 迷惑メールの取り扱い
・不審なメールや添付ファイルは開かない
・迷惑メールはそのまま削除, スパムフィルタ

39

3-2. 共通の対策(5)

・添付ファイルは開く前にウイルス検査
・拡張子exe, pif, scr, bat, comは要注意
・アイコンの偽装に注意
exeをdocに見せかけ, 二重の拡張子など
・エクスプローラーで「拡張子を表示」に設定
・メールの暗号化とディジタル署名の利用
PGP, S/MIME など

40

3-2. 共通の対策(6)

⑧ その他の注意点
・アプリケーションのセキュリティ機能の活用
Word, Excelでマクロの自動実行を不可に
・自分以外のパソコンに個人情報を入力しない
・USBメモリの利用における注意点
他人のUSBメモリは自身のパソコンに接続しない
他人のパソコンに自身のUSBメモリは接続しない
USBメモリの自動実行機能を無効化する

41

3-2. 共通の対策(7)

⑨ いざという時のために
・万が一のために, データは必ずバックアップ
・ウイルス感染の兆候を見逃さない
・マルウェアに感染したら, 落ち着いて対処する
1) コンピュータ使用を停止, システム管理者の指示を仰ぐ
2) 最新のウイルス対策ソフトで, ウイルス名を特定
3) ウイルス対策ソフト, 駆除ツールでウイルスを駆除
4) データを破壊されたときは, バックアップから復旧
5) 最新のウイルソフトでもう一度検査を行う
6) 感染経路を特定し, 再発防止の予防策を講じる
・初期化, 再インストールが最も安全確実

42

3-3. 標的型攻撃と誘導型攻撃への対策(1)

① 標的型攻撃とその対策

・標的型攻撃:主に電子メールを用いて，特定の組織や個人をねらう攻撃
・ウイルス対策ソフトが対応しにくい
・事例:苦情メールにスパイウェアを仕込む
・公的機関をかたり，添付ファイルを開かせる
・メールの件名，本文，添付ファイルに注意する

43

3-3. 標的型攻撃と誘導型攻撃への対策(2)

② 誘導型攻撃とその対策

・誘導型攻撃:利用者を攻撃者の仕掛けた罠に誘導する攻撃(受動的攻撃)
・興味を引くメールを送り，罠を仕掛けたWebページに誘導し，ウイルスを送り込む
・安易にリンクをクリックしない
・脆弱性を解消しておく

44

3-4. フィッシング詐欺への対策(1)

① フィッシング詐欺とは

・フィッシング詐欺:メールなどで，偽サイトに誘導し，個人情報を盗み取る
・巧妙な手口で個人情報を入力させる

② フィッシング詐欺への対策

・メールの送信元，内容を安易に信用しない
・リンクを安易にクリックしない

45

3-4. フィッシング詐欺への対策(2)

・入力前に本物のサイトかどうか確認する
正しいURLかどうか確認する(偽装に注意)
SSL接続を示す鍵アイコンがあるか確認する
フィッシング対策用のソフトウェアを使用する

③ ますます巧妙化するフィッシング詐欺

・特定の相手をねらう標的型攻撃
・DNSレコードを改ざんし，偽サイトへ誘導

46

3-5. ワンクリック不正請求への対策(1)

① ワンクリック不正請求とは

・出会い系サイトなどを装い，リンクをクリックしただけで，ユーザに料金の支払いを求める
・ユーザの不安を煽り，料金を支払わせる

② ワンクリック不正請求への対策

・信頼できないサイトへ気軽にアクセスしない
・契約は成立していないので，連絡を取らない

47

3-5. ワンクリック不正請求への対策(2)

・しつこく請求される場合は，消費生活センター，無料弁護士相談所，警察等へ相談する

③ スパイウェアによる不正請求

・スパイウェアにより，メールアドレスが盗まれ，支払い請求が送られて来ることがある
・ウイルス・スパイウェア対策ソフトでチェック
・OSの再インストールかシステムの復元で対処

48

3-6. 無線LANに潜む脅威とその対策(1)

① 無線LANの危険性
- 無線LANの電波は簡単にキャッチできる
- セキュリティ対策を怠ると，思わぬ被害

② 無線LANのセキュリティ対策
- データの暗号化(WPAまたはWPA2の設定)
  機器がサポートする最強の暗号方式を選択
  推測しにくいパスワードを設定

49

3-6. 無線LANに潜む脅威とその対策(2)

- ESS-IDの設定
  アクセスポイントのESS-IDは機器や使用者を推測しにくい値に変更
  ANYクライアントの接続を拒否するよう設定
  ESS-IDの通知(ビーコン)を無効化する

- MACアドレスフィルタリングの設定
  MACアドレスフィルタリングを有効にする

50

3-6. 無線LANに潜む脅威とその対策(3)

- 公衆無線LANのアクセスポイントを使用するときは，セキュリティに十分注意する

③ 無線LANの設定は難しい？-WPSで自動設定-
- WPS(Wi-Fi Protected Setup)を用いれば，無線LANのセキュリティ設定は簡単

51

第4章 組織の一員としての情報セキュリティ対策

4-1. 組織のセキュリティ対策
4-2. 従業員としての心得
4-3. 気を付けたい情報漏えい
4-4. 終わりのないプロセス

52

4-1. 組織のセキュリティ対策(1)

□ 情報セキュリティマネジメントシステム
(ISMS: Information Security Management System)
- 組織は経営層を中心に，技術的，物理的，人的，組織的な視点からの対策を体系的かつ系統立てて情報セキュリティに取り組む
- 計画(Plan)，実行(Do)，点検(Check)，処置(Act)のPDCAサイクルに沿って推進

53

4-1. 組織のセキュリティ対策(2)

① 計画(Plan)-体制の整備とポリシーの策定-
- 組織内の体制の確立
  経営陣を頂点とするトップダウン管理体制
- セキュリティポリシーの策定
  基本方針，対策基準
  「何を守るか」「どのようなリスクがあるか」
  最高責任者は組織の長
  社員はセキュリティポリシーをよく理解する

54

4-1. 組織のセキュリティ対策(3)

・対策事項の立案
リスク分析に従い，具体的な対策事項を立案
(ウイルス・不正アクセス対策，アクセス権限)
・実施手順(マニュアル)の策定
電子メールソフトの設定内容とその手順
ID，メールアドレス，パスワードの管理
私的利用や自動転送の禁止
インシデント発生時の対策方針と手順など

55

4-1. 組織のセキュリティ対策(4)

② 実行(Do)-導入と運用-
・導入フェーズ
(1) 構築と設定
ウイルス対策ソフトの導入
ファイアウォールの設定(アクセス制御)
OSやアプリケーションのセキュリティ設定
(2) 設定における留意点
不要なサービスを停止し，リスクを軽減

56

4-1. 組織のセキュリティ対策(5)

(3) 脆弱性の解消
サーバの構築・設定の際には，最新の修正
プログラムを適用
(4) レベルに応じたアクセス制御
組織のメンバーごとにアクセスレベルを設定
個人情報・機密情報の厳密なアクセス制御

57

4-1. 組織のセキュリティ対策(6)

・運用フェーズ
(1) セキュリティポリシーの周知徹底と教育
各人の役割と責任を明確に
セキュリティ上の脅威と対策を教育
(2) 脆弱性対策
脆弱性の報告に対し，速やかにパッチ適用
(3) 異動／退職職員のフォロー
異動・退職者のアカウントは確実に削除

58

4-1. 組織のセキュリティ対策(7)

③ 点検(Check)-監視と評価-
・監視と評価
通信，不正アクセスの監視
異常検知，不正アクセス検知
脆弱性検査
自己点検
情報セキュリティ対策ベンチマークによる診断
第三者による情報セキュリティ監査

59

4-1. 組織のセキュリティ対策(8)

・セキュリティ事故への対応
計画段階で緊急時対応計画を定める
事故の際はセキュリティポリシーに従い，対応
被害状況の調査，2次災害を防止
原因を特定し，再発防止策を徹底
対応策を記録，時系列の報告書にまとめる
必要ならば，各種届け出を行う
対応窓口を設け，正確な情報を提供

60

4-1. 組織のセキュリティ対策(9)

④ 処置(Act)-見直しと改善-

・事故の教訓を生かし，セキュリティポリシーを見直し，改善点を検討

・セキュリティ評価に基づき，改善

セキュリティマネジメントのサイクルを回しながら，組織に適した情報セキュリティ対策を高めていく

61

4-2. 従業員としての心得

・規則を知り，遵守する

基本方針，対策基準，実施手順を理解し，順守

・情報セキュリティ上の脅威とその対策を知る

・「自分だけは」，「これぐらいなら」は通用しない

例外的なケースなど，必ず上司，管理者に相談

ミスの際は，速やかに報告する

・情報漏えいに気を付ける(次節参照)

62

4-3. 気を付けたい情報漏えい(1)

・情報漏えいの経路と原因

情報の管理，漏えい防止が重要

情報漏えいの経路と原因

情報漏えいの経路：PC本体，外部記憶媒体，紙媒体P2Pファイル交換ソフトなど

情報漏えいの原因：紛失・盗難，P2Pファイル交換ソフト経由，誤送信，内部犯行など

人為的ミスの占める割合が大きい

63

4-3. 気を付けたい情報漏えい(2)

・情報漏えいを防止するためのポイント

・ファイル交換ソフトは使用しない

・私物パソコンをやむを得ず使用する場合は，使用上のルールや管理について定める

・やむを得ず，情報を外部に持ち出す場合には，持ち出しのルールを決めて，厳重に管理する

64

4-3. 気を付けたい情報漏えい(3)

・組織の一員としての情報セキュリティ心得

(1) 情報や機器を許可なく持ち出さない

(2) 私物のパソコンなどを許可なく持ち込まない

プログラムを許可なくダウンロードしない

(3) 書類，機器，メモリなどを放置しない

クリアデスクトップポリシー(机上の整理)

クリアスクリーンポリシー(離席するときは，パソコンをシャットダウン)

65

4-3. 気を付けたい情報漏えい(4)

(4) 情報や機器を未対策のまま廃棄しない

専用ソフトでデータ消去，書類はシュレッダー

(5) 個人の権限を他人に貸与，譲渡しない

IDやパスワードは他人に教えない

(6) 業務上知り得た情報を公言しない

居酒屋での何気ない会話，出張時や帰宅時のパソコンでの仕事に，情報漏えいの危険

(7) 情報漏えいを起こした場合は速やかに報告

66

4-4. 終わりのないプロセス

セキュリティ対策は，導入すれば終わりではない
対策の配備，運用，教訓のフィードバックが必要

技術的対策と管理的対策の両輪が必要不可欠

67

第5章 もっと知りたいセキュリティ技術

5-1. アカウント，ID，パスワード
5-2. 攻撃手法
5-3. 脆弱性を悪用する攻撃
5-4. ファイアウォール
5-5. 暗号とディジタル署名

68

5-1. アカウント，ID，パスワード(1)

□ ネットワークやシステムは，ユーザごとに利用範囲(権限)を定める

・アカウント：ユーザの利用権限
・ID：個人を識別する番号
・パスワード：正しいユーザであることの証明

69

5-1. アカウント，ID，パスワード(2)

① パスワードの重要性
・正しいパスワードを入力した人を本人と認める
・パスワードの漏えいは，本人だけでなく，システム全体，ネットワーク全体に被害をもたらす

② パスワードクラッキング
・本人から入手(ソーシャルエンジニアリング)
本人を騙して，言葉巧みに聞き出す

70

5-1. アカウント，ID，パスワード(3)

・パスワードを推測する
生年月日など，ユーザの情報から推測する
・パスワードを解析する
サーバのパスワードファイルを入手し，解析
ブルートフォース攻撃，辞書攻撃など
・盗聴する
・LAN上のデータを監視し，パスワードを抽出

71

5-1. アカウント，ID，パスワード(4)

③ パスワードを保護するための対策
・強度が高い(推測しにくい)パスワードを使用
英文字，数字，記号で8文字以上
推測しにくく，自分が忘れないパスワード
・定期的にパスワードを変更
・パスワードは絶対に他人に教えない
パスワードを聞かれることはない
・同一のパスワードを使い回さない

72

5-1. アカウント, ID, パスワード(5)

④ さまざまな認証方式

・パスワードは, 情報資源にアクセスする人が本人であることを確認する手段(認証という)

1)本人しか知らない知識(パスワード)で確認

2)本人固有の持ち物で確認

ワンタイムパスワード, スマートカードなど

3)本人の身体的特徴, 行動的特徴で確認

指紋や署名など(バイオメトリック認証)

73

5-2. 攻撃手法(1)

□ 外部からの侵入は, 事前調査, 権限取得, 不正実行, 後処理の4段階で行われる

① 事前調査

・ターゲットとなる組織のシステム情報(IPアドレス, サーバ名, サーバソフトウェア, OS, 提供サービス, 侵入検知システムなど)を調べる

・開かれているポートを調べる(ポートスキャン)

74

5-2. 攻撃手法(2)

② 権限取得

・パスワードを解析し, アクセス権限(一般ユーザ, 特権ユーザ)を不正に取得

③ 不正実行

・情報の盗みだし, 盗聴, 改ざん, なりすまし, 破壊, 不正プログラムの埋め込み, 踏み台

75

5-2. 攻撃手法(3)

④ 後処理

・不正行為を行った後, ログの消去などにより, 証拠隠滅工作を行う

・次回に侵入するための裏口(バックドア)作成

76

5-3. 脆弱性を悪用する攻撃(1)

① ポートと脆弱性

・ポート:インターネットにおいて特定のサービスを通信させるための認識番号

・プロトコル:サービス提供のための約束ごと

例:Webページ用のポート番号は80番, Webサービス提供のためのプロトコルがHTTP

メール受信用のポート番号は110番, メール受信のためのプロトコルがPOP

77

5-3. 脆弱性を悪用する攻撃(2)

・ポートの脆弱性を悪用する攻撃がある

・「使わないポートは閉じておく」のが有効

② 脆弱性を悪用する攻撃

・バッファオーバーフロー攻撃

コンピュータが処理しきれない大量のデータを送り込み, システムを操作する権限を奪う

78

5-3. 脆弱性を悪用する攻撃(3)

・クロスサイトスクリプティング攻撃
罠を仕掛けたサイトでユーザが不用意にリンクをクリックすると，別のサイトに飛ばされ，用意されたスクリプトが実行され，被害に遭うCookieが読み取られ，個人情報(IDやパスワードが含まれる)が盗まれることが多い

スクリプト：機械語への変換を省略して実行できるようにした簡易プログラム

79

5-3. 脆弱性を悪用する攻撃(4)

・SQLインジェクション攻撃
WebアプリケーションにSQLの脆弱性があるとき，不正なコマンドをSQL文を埋め込んで，データベース内のレコードを不正に操作する個人情報が漏えいするなどの被害が生じる

SQL：データベースの操作やデータの定義を行うための問い合わせ言語

80

5-3. 脆弱性を悪用する攻撃(5)

・DNSキャッシュポイズニング攻撃
DNSサーバの脆弱性を悪用し，偽のドメイン管理情報をキャッシュ(一時記憶)させる攻撃
ユーザが偽のWebページに誘導され，情報漏えいなどの被害に遭う

DNS：インターネット上のIPアドレス(192.168.170.255)とドメイン名(www.ipa.go.jp)を対応させる仕組み

81

5-4. ファイアウォール(1)

① ファイアウォールとは？
・インターネットとLAN(内部のネットワーク)の境界に設置し，アクセス制御を行う仕組み
・外部との出口を絞る
・LANの内部構造を外部に見せない
・外部からの不正なアクセスを排除する
・必要なアクセスだけを通過させる

82

5-4. ファイアウォール(2)

② パケットフィルタリング，アプリケーションゲートウェイ，プライベートアドレス
・パケットフィルタリング
パケットのヘッダ情報(送信元IPアドレス，相手先IPアドレス，送信元ポート番号，相手先ポート番号，パケットの連番など)の情報に基づき，アクセスを制御する仕組み

パケット：インターネットやLANなど，TCP/IPネットワークで送られるデータの単位

83

5-4. ファイアウォール(3)

・アプリケーションゲートウェイ
HTTP，FTP，POP，SMTPなどのアプリケーションプロトコルに基づき，アクセス制御を行うプロトコルごとに制御が可能

・プライベートアドレスの割り当て
組織内のみで通用するIPアドレス
外部からアクセスできないので，安全

84

5-4. ファイアウォール(4)

③ ネットワークアドレス変換技術(NAT)

・NAT:プライベートアドレスをグローバルアドレスに1対1に変換する技術

・NAPT:ポート番号も変換して，1つのグローバルアドレスに複数のプライベートアドレスを対応させる技術

・内部情報を隠蔽しつつ，外部へアクセス可能

85

5-4. ファイアウォール(5)

④ DMZ(DeMilitarized Zone:非武装地帯)

・外部ネットワークと組織内ネットワークの緩衝地帯で，ファイアウォールの内部に置く

・Webサーバ，Mailサーバ，DNSサーバなどの公開サーバ群をDMZにおく

⑤ ファイアウォールの落とし穴

・万全ではないので，過信は禁物

86

5-4. ファイアウォール(6)

⑥ パーソナルファイアウォール

・個人ユーザのコンピュータを守る手段

・低価格で，初心者でも簡単に使える

・ウイルス対策を組み合わせた製品もある

87

5-5. 暗号とディジタル署名(1)

① 暗号技術とは？

・一定の法則に基づいてデータを変換し，元のデータを第三者に知られないようにする技術

・暗号化，復号，アルゴリズム，鍵

暗号化：平文→暗号文

復号：暗号文→平文

アルゴリズム：変換法則

鍵：変換の量，変換に用いる数値

88

5-5. 暗号とディジタル署名(2)

・共通鍵暗号方式

送信者と受信者が共通鍵でデータの暗号化，復号を行う．高速だが，鍵の受け渡しが困難

DES，AES，MISTY1，Cameliaなど

・公開鍵暗号方式

秘密鍵と公開鍵のペアを用いる．一方の鍵で暗号化すると他方の鍵でしか復号できない

89

5-5. 暗号とディジタル署名(3)

秘密通信の仕組み

Bさん:鍵のペアを作成し，公開鍵を公開

Aさん:Bさんの公開鍵で暗号化し，送信

Bさん:自分の秘密鍵で復号

鍵の受け渡しは容易だが，アルゴリズムが複雑なため，低速

RSA，ElGamal，楕円曲線暗号など

90

5-5. 暗号とディジタル署名(4)

・ハイブリッド暗号方式
共通鍵暗号と公開鍵暗号の利点を組合せる
1. Bは鍵のペアを作成し，公開鍵をAに送信
2. Aは共通鍵を作成し，Bの公開鍵で暗号化
3. Aは暗号化した共通鍵をBに送信
4. Bは暗号文を復号し，共通鍵を取り出す
5. 以後，A，Bは共通鍵で秘密通信を行う

91

5-5. 暗号とディジタル署名(5)

② ディジタル署名方式
・署名者は署名用の秘密鍵と公開鍵のペアを作成し，公開鍵を公開
・データを秘密鍵で暗号化したものは，対応する公開鍵でしか復号できない．公開鍵に対応する秘密鍵をもっている人が，署名者である
・署名サイズを小さくするため，ハッシュ関数を用い，メッセージダイジェストに署名する

92

5-5. 暗号とディジタル署名(6)

③ 認証局とは？
・公開鍵と本人の結びつきを証明する仕組み
・認証局(CA)は，ユーザからの申込を受けてディジタル証明書(公開鍵証明書)を発行
・証明書はユーザの登録者情報，公開鍵，有効期限，認証局のディジタル署名などを含む
・ユーザは通信相手にディジタル証明書を送信
・通信相手は，認証局のディジタル署名を確認

93

5-5. 暗号とディジタル署名(7)

④ 身近に使われている暗号技術
・WWWでの暗号化(SSL)
Webサイトは，認証局から公開鍵証明書を受け取り，SSL通信を行えるようにする
1. ユーザがSSLサイトにアクセスすると，サイトは公開鍵証明書を送信
2. ユーザはブラウザにあるCAの公開鍵で証明書の署名を検証し，公開鍵を取り出す

94

5-5. 暗号とディジタル署名(8)

3. ユーザのブラウザは共通鍵を生成し，Webサイトの公開鍵で暗号化して送信
4. 以後は，共通鍵方式で秘密通信を行う
セッション鍵(共通鍵)は使い捨てにする

・暗号化メール
盗聴防止，改ざんの検証，なりすまし防止
PGP，S/MIME：ハイブリッド暗号方式を使う

95

5-5. 暗号とディジタル署名(9)

(1) PGP
メーラとともに使用し，メールの暗号化とディジタル署名が可能．公開鍵の交換に認証局を使用せず，本人同士が相互認証
(2) S/MIME
S/MIMEのプロトコルを実装したメーラを使うことで，暗号化，ディジタル署名が可能
認証局から公開鍵証明書の交付が必要

96

5-5. 暗号とディジタル署名(10)

・携帯電話やICカードで利用される暗号技術

携帯電話の機種によっては，SSL対応の
WWWサーバへのアクセスが可能

ICカード(スマートカード)は，暗号処理機能
を持つことができ，磁気カードより安全

住民基本台帳カードやクレジットカードに利用

97

第6章 情報セキュリティ関連の法規と制度

6-1. 情報セキュリティの国際標準
6-2. 情報セキュリティに関する法律
6-3. 知的財産を守る法律
6-4. 迷惑メール関連法
6-5. 情報セキュリティ関連制度

98

6-1. 情報セキュリティの国際標準(1)

① 情報セキュリティマネジメントの国際標準
27000シリーズ

・ISO/IEC 27000シリーズは，組織として情報
セキュリティ確保に取り組むための国際規格
・ISO/IEC 27001:要求事項
・ISO/IEC 27002:実践規範
・ISO/IEC 27001，27002はJIS規格化され，
JIS Q 27001，JIS Q 27002となっている

99

6-1. 情報セキュリティの国際標準(2)

② セキュリティ製品の評価認証のための国際
標準ISO/IEC 15408

・セキュリティ製品やシステムが適切に設計され，
正しく実践されているかどうかを評価
・機能要件:製品やシステムが備えるべきIT
セキュリティに必要な機能を網羅
・保証要件:セキュリティ機能が確実に実現され
ていることを保証するための要件

100

6-1. 情報セキュリティの国際標準(3)

・ISO/IEC 15408のJIS規格化:JIS X5070
・ITセキュリティ評価及び認証制度
ISO/IEC 15408(CC)に基づき，IPAが認証
・CCによる認証書は国際的に相互認証される
(CCRA:2009年6月現在，26カ国が参加)
・2008年4月以降は新しい国際標準CC V3.1
を用いる

101

6-1. 情報セキュリティの国際標準(4)

③ OECD情報セキュリティガイドライン

・1992年，OECD(経済開発協力機構)が制定
・米同時多発テロを受け，2002年に全面改正
・新ガイドラインで情報セキュリティ文化を提唱
・責任の原則，リスクアセスメントの原則，
セキュリティマネジメントなど9原則を記載

102

6-2. 情報セキュリティに関する法律(1)

① 刑法

・1987年の改正で，コンピュータ犯罪防止の規定を追加．刑事罰が可能

・電子計算機損壊等業務妨害罪

・電磁的記録不正作出及び共用罪

・電子計算機使用詐欺罪

103

6-2. 情報セキュリティに関する法律(2)

② 不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）

・不正アクセスや不正アクセスを助長する行為が処罰の対象．以下の3点を規定

・他人のIDやパスワードを無断使用

・セキュリティホールを突いた直接侵入攻撃

・セキュリティホールを突いた間接侵入攻撃

・システム管理者に予防に必要な対策を求める

104

6-2. 情報セキュリティに関する法律(3)

③ 電子署名及び認証業務に関する法律（電子署名法）

・電子署名に署名や押印と同じ効力を持たせる

・電子署名，電子証明書とは何かを規定

・電子的に認証を行う認証業務や認証事業者について規定

105

6-2. 情報セキュリティに関する法律(4)

④ 個人情報の保護に関する法律（個人情報保護法）

・個人情報（特定の個人を識別可能な情報）の漏えいや不正利用などに対し，個人情報を取り扱う事業者の遵守すべき義務を規定

・5000件を超える個人情報を有するデータベースを使用する組織が対象

・本人の了解なしに個人情報を流用，売買，譲渡することを規制

106

6-2. 情報セキュリティに関する法律(5)

・個人情報保護の基本原則

1．個人情報の利用は収集目的の範囲内で

2．事業の範囲内で，収集目的を明確にする

3．正確性，最新性を維持する

4．不正アクセス，紛失，改ざん，漏えいなどに対し，合理的な安全対策を講ずる

5．開示，訂正，削除を求められた場合は，原則として応じる

107

6-3. 知的財産を守る法律(1)

□ 知的財産は，著作権，トレードシークレット，産業財産権（特許，意匠，商標）の3つに大別され，「著作権法」，「不正防止法」，「特許法」などで守られている

① 著作権法

・「創作性」のある思想や表現などの著作物や著作者の保護が目的

108

6-3. 知的財産を守る法律(2)

・プログラムやデータベースは保護の対象
・プログラム言語，アルゴリズム，規約，統計情報等は保護の対象にならない
・著作者人格権：公表権，氏名表示権，同一性保持権
・著作財産権：複製権，上演権，公衆送信権，口述権，展示権，貸与権，翻訳権など
・著作財産権の侵害が多くなっている

109

6-3. 知的財産を守る法律(3)

② 不正競争防止法
・トレードシークレット(企業のノウハウや営業秘密などの有用な機密情報)の保護が目的
・トレードシークレットの不正入手，不正使用に対し，差し止め請求権，損害賠償請求権が認められている

110

6-4. 迷惑メール関連法

・迷惑メール関連法
「特定商取引に関する法律」，「特定電子メールの送信の適正化等に関する法律」
・宣伝や勧誘のメールには，「未承諾広告※」，送信者の氏名，住所の表示を義務づけ
・受信を拒否する人には送信してはならない
・同意した人にのみ送信が認められる
・架空メールアドレスへの送信禁止

111

6-5. 情報セキュリティ関連制度(1)

① ISMS 適合性評価制度
・組織の情報セキュリティマネジメントシステム(ISMS)が基準に適合しているかどうかを，第三者機関が客観的に評価する制度
・JIS Q 27001の基準に準拠し，評価する

② IT セキュリティ評価及び認証制度
・ISO/IEC 15408に基づき，セキュリティ製品やシステムの保証レベルを評価・認証する

112

6-5. 情報セキュリティ関連制度(2)

③ 暗号モジュール試験及び認証制度
・暗号モジュールが，JIS X 19790に示されたセキュリティ要求事項に適合しているかどうかを第三者機関が客観的に試験・認証する制度

④ プライバシーマーク制度
・JIS Q 15001に基づき，個人情報保護の取り組みが適切であるかどうかを認定する

113

6-5. 情報セキュリティ関連制度(3)

⑤ 情報セキュリティ監査制度
・独立・専門的な立場の監査人が，組織の情報セキュリティ対策の状況を客観的に検証・評価し，適切性を保証したり，助言を与えたりする
・「情報セキュリティ管理基準」，「情報セキュリティ監査基準」に準拠して監査を実施する

114

6-5. 情報セキュリティ関連制度(4)

⑥ コンピュータウイルス及び不正アクセスに関する届出制度
- ・コンピュータウイルス対策基準，コンピュータ不正アクセス対策基準に基づき，ウイルスや不正アクセスの届出と相談を受け付ける制度

⑦ 脆弱性関連情報に関する届出制度
- ・ソフトウェア等脆弱性関連情報取扱基準に基づき，ソフトウェア等の脆弱性に関する情報の届出を受け付ける制度

115

第7章 IPAセキュリティセンターの活動(1)

□ IPA(独立行政法人情報処理推進機構)
- ・経済産業省所管の独立行政法人として，情報処理の振興を図るための事業を行っている

□ IPAセキュリティセンター
- ・経済産業省の情報セキュリティ政策を実行に移すため，情報セキュリティ関連の各種事業に取り組んでいる

116

第7章 IPAセキュリティセンターの活動(2)

・情報セキュリティに関する普及啓発活動など
情報セキュリティに関する対策実践情報の掲載
情報セキュリティに関する各種セミナーの開催
情報セキュリティに関する調査報告書の公開
情報セキュリティに政策立案のための情報分析
情報セキュリティに関する技術開発の公募

117

第7章 IPAセキュリティセンターの活動(3)

・ウイルス・不正アクセス対策
ウイルス・不正アクセスの届出と相談の受付
ウイルス・不正アクセスのための資料作成配布
インターネット定点観測システムを構築・運用
脅威の発生状況の把握と情報提供

118

第7章 IPAセキュリティセンターの活動(4)

・情報システムの脆弱性への取り組み
情報システムの脆弱性，攻撃手法の検証・解析
警告情報の公表
「情報セキュリティ早期警戒パートナーシップ」

・IT セキュリティ評価・認証
ISO/IEC 15408に基づき，セキュリティ製品やシステムの評価結果の認証を行う

119

第7章 IPAセキュリティセンターの活動(5)

・暗号技術調査・評価
暗号技術評価(CRYPTREC)の推進
電子政府推奨暗号リストの公表，継続的評価
暗号モジュールに対する要件の作成

・暗号モジュールの試験および認証制度
暗号モジュールがJIS X 19790のセキュリティ要求事項に適合しているかどうかを確認する

120