インターネット セキュリティ (I)

岡田 高 (JPCERT/CC)

JPCERT/CCへのアクセス

- WWW
  http://www.jpcert.or.jp/
- 情報提供用メーリングリスト（登録方法）
  http://www.jpcert.or.jp/announce.html
- 電子メール:　info@jpcert.or.jp
- 電話:　03 (5575) 7762
- FAX:　03 (5575) 7764

今日の予定

- 不正アクセスの現状
- セキュリティの考え方
- サービス利用者のセキュリティ
- 一般的なサービスのセキュリティ
- 各種サービスのセキュリティ
- 非常事態への対応

JPCERT/CC

- (主に) 日本国内を対象としたIRT
  - 不正アクセス届出への対応
    - 傾向の把握
    - 技術的なアドバイス
    - 攻撃元への連絡
  - 啓発活動
- 中立、民間、非営利
  - 特別な権限は有していない
- 1996年8月発表/1996年10月事務所開設

不正アクセスの現状

JPCERT/CCへの届出

- 約400件
  1996年10月～1997年9月
  未遂の攻撃についての報告を含む

不正アクセスの動向

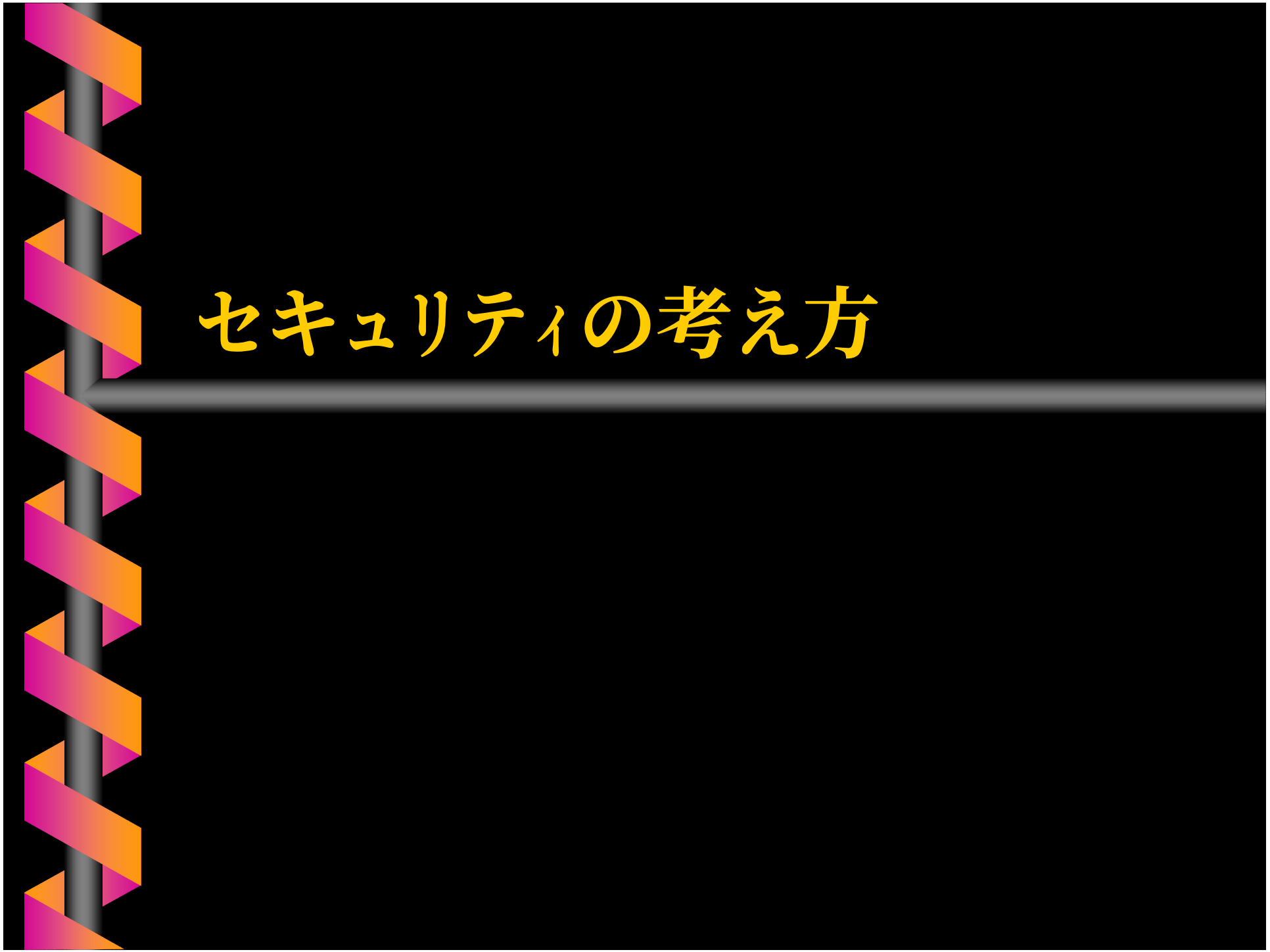
- ソフトウェアのセキュリティ・ホールへの攻撃
  sendmail, INN, phf, IMAPサーバー
- 電子メールの不正な中継と電子メール爆撃
- パスワード推測，パスワード破り
- 侵入

不正アクセスの動向

- 侵入後の行動
  - ルート権限の不正入手
  - トロイの木馬の設置
  - パケット盗聴プログラムの設置
    - 認証情報（パスワード）の取得
  - 踏み台アタック

スキャン型の攻撃

- 特定のセキュリティ・ホールへの攻撃を
- 多数のホストに対して
- 機械的に試行
  - /etc/passwdの取得
  - その他重要ファイルの取得


セキュリティの考え方

セキュリティへのステップ

- 条件の明確化
- ポリシーの決定
- 設計
- 実装、構築
- 検証
- 運用、評価
- 繰り返し

ポリシー

- 明確化が重要
- 理想は
  ドキュメント化されたポリシーが
  組織的に支持され
  タイムリーに更新される
- 現実は...?

構成要素の選定

- システムへの習熟度は？
- 投入できる労力は？
- 出荷時設定
  - 機能性重視の傾向
  - 使わない機能は無効化

フリーソフトウェア

- 商業製品にもベースにしているものがある
  - そのものの安全性に差はない？
    - 実験的なものはともかく...
- 商業製品のメリット
  - セキュリティ・パッチ
    - 実行形式での提供
  - サポート
- 投入できる労力は？

セキュリティの要素技術

- 認証
- アクセス制御
- 監査記録、ログ
- データ保全
- データ秘匿
- 否認防止

ユーザー認証

- パスワード，パスフレーズ
- ワンタイム・パスワード
  - S/Key，OPIE
  - 各種トークン・カード製品
- etc ...

ユーザー認証

（高度な認証システム）

ワンタイム・パスワード

パスワード認証

認証なし

アクセス制御

- ファイアーウォール
- パケット・フィルタリング
- tcp_wrappers
- xinetd
- 各種サーバー機能
- etc ...

アクセス制御

許可するもの以外は拒否

拒否するもの以外は許可

すべて許可

ログ

- プライバシーに配慮
  ユーザーの理解が得られる範囲で
  なるべく詳細に記録する
  - ディスク領域の確保
  - ローテーションの調整
  - 設定の調整

ファイアーウォール

- 対策の局所化
  - 防御できない不正アクセスもありうる
  - 他の対策もあわせて検討、実施
  - 積極的なアクセス制御をしない場合も有効
- 活用のポイント
  - ポリシーを反映した設定
  - 機能・特性の把握
  - 日々のメンテナンス

VPN

- 接続先が侵入されると危険
- 対策
  - 適度な認証
  - 適度なアクセス制御
    - 接続先は、やはり外界

セキュリティ情報とデマ

- そのままフォワードしない
- まず自分で確認
  - 信頼できる情報源でチェック
  - 教えるときは一次情報へのポインタを中心に
    - http://ciac.llnl.gov/ciac/CIACHoaxes.html
    - http://www.ipa.go.jp/SECURITY/index-j.html

サービス利用者のセキュリティ

コンテンツによるリスク

- 問題のあるデータの受領をきっかけに
  - WWW，電子メール（添付ファイル），...
- 不都合な動作が行われる
  - マクロウィルス
  - ディスクの初期化
  - ローカル情報の送信
  - etc ...
- ソフトウェアや設定、ユーザーの習慣に依存

コンテンツによるリスク

- 対策
  - 関連ソフトウェアのバージョン・アップ
    - かえって「便利」な新版は危険か？
  - ブラウザー設定の調整
  - 安全なファイル形式の選択
  - ウィルス検索・駆除ソフト
  - ファイアーウォールでの検出、排除
  - “検疫所”の設置

WWWのリスク

- コンテンツによるリスク
- プライバシーの漏洩
- ネットワーク盗聴
- 電子掲示板（チャット）ページ

WWWとプライバシー（1）

- サーバーへの情報伝送
  - IPアドレス（マシンネーム）
  - 使用ブラウザー
  - 参照したページ
    - プロキシー・サーバーにもログが残る
- プロトコルのデザイン上の事実
  - 信頼できるサイトだけをアクセス

WWWとプライバシー (2)

- ブラウザーの問題に由来する情報漏洩
- 対策
  - 最新版ブラウザーの利用
    - しかし、継続的に同種のバグが発見されている
    - 常に最新情報に注意
  - ブラウザーの交換

電子掲示板（チャット）ページ

- 問題のある投稿
  - 猥褻、誹謗中傷、個人攻撃、いやがらせ ...
- 対策
  - HTMLタグの制限
  - アクセスログの監視
  - 投稿者の事前登録
  - リスクの自覚
    - 不特定多数や匿名での情報交換

電子メール

- 本質的なリスク
  - 送信ミス（内容, 宛先）
  - 不達
  - トラフィック解析
  - 窃視
- 電子メールのデザイン上の事実
  - ユーザーの自覚
  - 暗号技術の利用（部分的な解決）

SPAM, 電子メール爆弾

- 対応は慎重に
  - 偽造ヘッダーが使われている
    - Received: や From:
  - 直近の Received: なら信頼できる？
  - 発信源のプロバイダーに連絡してみる
- 予防
  - アドレスを不特定多数に開示しない
    - メーリングリスト等は別のアドレスで参加する
  - 中継システム側の対策

メーリングリスト

- 典型的なリスク
  - WWWゲートウェイ経由でのアドレスの開示
  - 他の参加者へのアドレスなどの開示
  - メーリングリスト経由でのSPAM，電子メール爆撃
- 対策
  - 参加前の確認
    - 運営ポリシー、運営内容
  - 別アドレスからの参加

一般的なサービスのセキュリティ

セキュリティ・ホール

- 典型的なリスク
  - 設定情報の漏洩
  - 侵入
  - 侵入後の特権の獲得
- 対策
  - アクセス制御
  - 最新版ソフトウェア（パッチ）の利用
  - 一時的な使用停止
  - 利用の放棄

パスワード認証

- 典型的なリスク
  - ネットワーク盗聴による取得
  - 辞書攻撃
  - ブルートフォース攻撃
    - 短くなりつつある8文字
    - 各種 crack ツールの存在
  - パスワードファイルの漏洩
    - サイト外でのパスワード破り

パスワード認証

- 対策
  - ユーザーの自覚
    - 英大小文字、数字、記号をすべて混ぜる
    - 辞書攻撃に強いパスワードを選ぶ
    - 8文字(以上)の長さにする
  - シャドウ・パスワードの導入
  - システム管理者によるcrack
- 必要であれば、より強力な認証機構を導入

ネットワーク盗聴

- 対策
  - 暗号通信
  - ネットワーク・インタフェースの監視
    - promiscuousモード
  - スイッチの導入（1マシン1ポート）
- パスワード盗聴への対策
  - 盗聴に強い認証方式の使用
    - ワンタイム・パスワード，APOP，...

IP spoofing

- 始点アドレスを偽造
  - IPパケットに含まれる
  - アドレスベースのアクセス制御を不正に通過
- 対策
  - パケットフィルタリングの実施
    1. 内部アドレスを始点に持つパケットの
    1. 外界からの侵入
  - 外界のアドレスは設定に記述しない

DNS spoofing

- DNSの登録情報を偽造
  - ホストネームベースのアクセス制御を不正に通過
- 対策
  - 最新版ソフトウェアの利用
  - 信頼できる情報を利用
    - 手元のオーサライズド・サーバーの情報のみ使用
    - または、ホストネームを設定に記述しない

ログ

- 典型的なリスク
  - 領域の不足
  - 偽造
  - 改ざん
- 対策
  - ディスク領域の確保、ローテーションの調整
  - ファイルのアクセス権設定
  - syslogパケットのフィルタリング
  - （ハードコピー、専用マシンの導入）

メール配送サービス

- 典型的なリスク
  - 中継地点としての使用
  - sendmailへの攻撃
- 対策
  - 最新版ソフトウェアの使用
  - 中継利用の禁止
    - http://www.jpcert.or.jp/tech/97-0001/
  - SMTPサーバーの停止 （発信のみのホスト）

メールの自動処理

- 典型的なリスク
  - 設定ミス
  - 誤った権限での起動
  - ソフトウェア，設定のセキュリティ・ホール
- 対策
  - 最新版ソフトウェアの使用
  - smrshの使用
  - decodeエイリアスは管理者あてにしておく

メールボックスサービス

- 典型的なリスク
  - ネットワーク盗聴
  - IMAPサーバーへの攻撃
- 対策
  - 最新版ソフトウェアの使用
  - アクセスの規制、記録
  - ネットワーク盗聴対策の実施

情報提供サービス一般

- 典型的なリスク
  - 不正アクセスの標的
    - ホスト名から明らかにそれとわかる
    - インターネット全域を対象に公開している
    - 侵入
    - アンダーグラウンド情報交換
    - コンテンツの改ざん
  - WWWロボットによる不本意な情報開示

情報提供サービス一般

- 対策
  - 最新版ソフトウェアの使用
  - 外部プログラム（CGI，SITE EXEC, ...）
    - 不要なものは削除
    - 作成、設定は慎重に
  - アクセスログの保存

情報提供サービス一般

- 対策
  - 遠隔ログインの制限
  - パケットフィルタリング等による防御
  - ファイアーウォールの背後に隠蔽
    - 人気サーバーの場合、処理能力に注意
  - 専用サーバーへの切り分け

WWW サーバー

- 対策
  - まずphfを起動不可能にする
  - 使用するプログラムのみ導入
    - CGIプログラム
  - cgi-binディレクトリ
    - 最小限必要な実行形式だけを置く
    - 置いてはいけないものの例
      - perl, sh, ...

Anonymous FTP

- 典型的なリスク
  - セキュリティ・ホール，設定ミスへの攻撃
  - 書き込み可能ディレクトリの悪用
- 対策
  - 最新版ソフトウェアの利用
    - 古いftpdは問題あり
  - 書き込み可能ディレクトリの監視
  - サービスの変更
    - HTTPサーバーのほうが守りやすいか？

WWWロボットによる情報開示

- 対症療法
  都度、ロボットの管理者に連絡する
- 対策
  robots.txt
    http://info.webcrawler.com/mak/projects/robots/norobots.html
  ファイル単位のアクセス制御
    - ヒューマン・エラーの回避
      → 独立したサーバー、独立した運用

遠隔ログイン

- 侵入口の一つ
- ネットワーク盗聴
- 対策
  - アクセスの規制、記録
  - ネットワーク盗聴対策の実施
- クライアントのサーバー機能に注意

各種サービスの
セキュリティ

メーリングリスト・サービス

- 典型的なリスク
  - メールのリスク一般
    - 影響は参加者数に比して大
  - 加えてリスト・サーバーのセキュリティ・ホール
- 対策
  - 投稿を登録アドレスのみに制限
  - 登録時に確認メールの交換を行なう
  - 最新版ソフトウェアの使用

Samba

- 随時バージョンアップされている
- 外界からのアクセスは適宜規制
- 関連トピック
  - クライアント環境のリスク
    - NetBIOS over TCP/IP
  - パスワード・キャッシュ

rコマンド群

- 典型的なリスク
  - セキュリティ・ホールへの攻撃
  - DNS spoofing，IP spoofing による侵入
  - 有効なユーザー名のprobe（rexecd）
  - /etc/hosts.equiv, ~/.rhosts の設定ミス
- 対策
  - アクセス制御またはサービスの無効化
  - ツールの導入
    - tcp_wrappers，logdaemon，rdist，...

Sun RPC （NIS, NFS, ...）

- 典型的なリスク
  - サイト外からの情報取得（NIS，rup，rusers, ...）
  - rexd経由の攻撃
  - NFSマウント
- 対策
  - rexdの無効化
  - パケットフィルタリング、アクセス制御
  - portmap（rpcbind）の置換
  - /var/yp/securenetsの記述

NTP

- 不正な時刻情報の挿入
  - ログの混乱、タイムベース認証の欺瞞
- 対策
  - 認証機能の利用
  - アクセス制御
  - 信頼できる時刻サーバーの指定
  - 複数の時刻サーバーの指定

X Window System

- 典型的なリスク
  - 既知セキュリティ・ホール多数
  - セッションの盗聴
- 対策
  - 最新版ソフトウェアの利用
  - ユーザー認証（xauth）の使用
  - ホストベース認証（xhost）の使用
  - アクセスの規制、記録

非常事態への対応

監視

- 平時の状態を把握
  - 正規ユーザーの挙動
  - システムの動作
- 常に異変に注意
  - 定期的にログをチェック
  - 抽出、報告ツールの利用

IRT, 他サイトからの連絡

- 冷静に対応
  - 欺瞞情報かもしれない
  - IRTは真実の場合に備えて連絡を中継する
- 事実関係の調査からスタート
  - 「踏み台」にされているおそれがある

攻撃者の追跡について

- リスク
  被害の拡大，他サイトからの苦情，...
- 必要なもの
  運
  交渉力
  技術力
  労力、時間
  etc ...
- リスクのほうが上回らないか？

状況の把握

- 運用マニュアル類を参照
  - 組織の運用基準があれば準拠
    - 対応手順，内容
    - プレス対策，顧客対策，...
- 本当に攻撃（侵入）されているのか？
  - 事故？ 障害？ 攻撃？
- 「今すぐ」行動する必要があるか？
  - 侵入者を刺激しないように注意する

一般的な対応

- 責任者、担当者への連絡
- 被害の拡大防止
  - ネットワークからの遮断
- 証拠の保全
  - ネットワーク接続状況の記録
  - 稼動中のプロセスの記録
  - 完全バックアップの作成
  - ...

攻撃元サイトへの連絡

- 踏み台にされている可能性がある
  - 警告
  - 調査依頼
    - 「抗議」は避けるほうが無難
- 注意事項
  - プライバシーの保護
  - 機密漏洩の防止
- 攻撃者の視線に注意

IRTへの連絡

- 大局的な対策、対応
  - 勧告文書のリリース
  - etc ...
- 大規模な不正アクセスへの対応
- 一般的な技術アドバイス
- 攻撃元への連絡（直接できない場合）

復旧作業

- 被害状況の把握
  侵入経路
- バックアップからの回復
  → 信頼性に注意
- 配布メディアからの回復
- 再発防止策の導入
  設定の改善，全パスワードの変更, ...

アフターフォロー

- 詳細な調査･分析
- 記録，ドキュメンテーション
- システムの見直し
  - ポリシー
  - 運用マニュアル
  - 設定


まとめ

まとめ

- 現実に不正アクセスは存在する
- すべてのサイトは狙われている
- 心当たりの有無にかかわらず攻撃される
- 対策を！

情報提供のお願い

- 実害のない場合もぜひご一報を
- 届出様式

  http://www.jpcert.or.jp/form.html

  1.不正アクセスを受けたサイト

  2.あなたの連絡先

  3.影響を受けたホストの情報

  4.不正アクセスの内容

参考情報

JPCERT/CC提供情報

- Web
  http://www.jpcert.or.jp/
- 情報提供用メーリングリスト（登録方法）
  http://www.jpcert.or.jp/announce.html
- 参考文献リスト
  http://www.jpcert.or.jp/ref.html
- 初心者のためのセキュリティー講座
  http://www.jpcert.or.jp/magazine/beginners.html

FTPミラー

- CERT/CC
  ftp://ftp.jpcert.or.jp/pub/cert/
- AUSCERT
  ftp://ftp.jpcert.or.jp/pub/auscert/
- CIAC
  ftp://ftp.jpcert.or.jp/pub/ciac/

ツール

- CERT/CCアーカイブ （ミラー）
  ftp://ftp.jpcert.or.jp/pub/cert/tools/
- CIACアーカイブ
  http://ciac.llnl.gov/ （Tools）
- COASTアーカイブ
  http://www.cs.purdue.edu/coast/archive/index.html

Assigned Numbers

- RFC 1700
- 最新情報

  http://www.iana.org/iana/　(General Assignments)

  ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers

RFC

- Internet Draft

  http://www.ietf.org/ (Internet-Drafts Index)

  - "Users' Security Handbook"

- RFC 2196

  "Site Security Handbook"

- RFC 1281

  "Guidelines for the Secure Operation of the Internet"