xSP のオペレータが知っておくべき セキュリティの基礎知識

2003 年 7 月 7 日

佐野　晋

㈳日本ネットワークインフォメーションセンター

1. インシデント

研究社 新英和・和英中辞典 より

in・ci・dent /ins ∂ dnt/

出来事; (特に，重大事件に発展する危険性をもつ)付随事件，小事件， 紛争, 事変 《★【類語】 「アクシデント」 は思いがけなく起こる事故; 「イベント」 は重要な出来事や行事》.

2. コンピュータ セキュリティ インシデント

- コンピュータのセキュリティのインシデント
  - コンピュータセキュリティの
  - 重大事件に発展する危険性をもつ事象または現実化した事象で
  - 特にインターネットを経由したもの
- JPCERT/CC FAQ より
  コンピュータセキュリティに関係する人為的事象で、意図的および偶発 的なもの (その疑いがある場合) を含みます。例えば、リソースの不正 使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さ らにそれらに至るための行為 (事象) などがあります。

3. CSIRT

- コンピュータ・セキュリティ・インシデント・レスポンス・チーム
- コンピュータのセキュリティの「インシデント」に対応するチーム
- 対応:関係者との連係をとって，インシデントの防止を行い，発生した際のインシデントの沈静化をはかり，復旧を支援し， 再発を防止する一連の組織的活動.
  - 関連する情報の収集，発信
  - 警告
  - 関係者，関係組織間との連絡
  - 啓発・普及

4. セキュリティに関連する言葉

- リアイアビリティ
- トラストネス
- セイフィティ
- :

5. C.I.A.

OECD（経済協力開発機構）のセキュリティガイドラインで示された用語で, 情報セキュリティの基本概念.

- **Confidentiality −機密性, 守秘性(，秘匿性)**
  許可されないユーザ/プロセスからのデータ/情報システムをアクセスを防止する
- **Integrity −完全性(，保全性)**
  データ/情報システムが正確で完全であること
- **Availability − 可用性**
  データ/情報システムを必要なときにアクセス可能な状態を確保すること

6. いろいろなインシデント

- **不正利用**
- **アタック**
- **クラック**
- **侵入**
- **攻撃**
- **不正侵入** - 侵入は不正なのでおかしい
- **不正アクセス** - 法律により定義.
- **無権限アクセス**
- **改ざん** - 権限なしに/悪意をもってデータを変更すること
- **偽造** - 権限なしに/悪意をもってデータを作ること
- **サイバーテロ** - 政治的な目的/意図によるコンピュータシステムへの攻撃
- **盗聴**．悪意を持った傍聴．cf．盗聴法
- **消去**
- **破壊**. 悪意をもってデータを消去したり，サービスやシステムを壊すこと.
- **スパム**. 情報を繰り返し執拗に送ること
- **なりすまし**
- **妨害**

- クラッカー（cracker）
- 攻撃者（attacker）
- 侵入者（intruder）
- ハッカー (hacker).

7. 不正アクセス行為

「不正アクセス行為の禁止等に関する法律(2000年2月13日施行)」で定義. 要約すると，ネットワークに接続しアクセス制御されたコンピュータに対する

- なりすまし行為
- セキュリティ・ホールを攻撃する行為

（目的）
第一条 この法律は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のため の都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機 に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高 度情報通信社会の健全な発展に寄与することを目的とする。

（定義）
第二条 この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定 電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。 ）につき当該特定電子計算機の動作を管理する者をいう。
２ この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係 るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項に おいて「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区 別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれ かに該当する符号とその他の符号を組み合わせたものをいう。
一 当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
二 当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法 により作成される符号
三 当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号
３ この法律において「アクセス制御機能」とは、特定電子計算機の特定利用

を自動的に制御するために当 該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を 介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者に より当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用い て当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含 む。次条第二項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又 は一部を解除するものをいう。

（不正アクセス行為の禁止）
第三条 何人も、不正アクセス行為をしてはならない。
２ 前項に規定する不正アクセス行為とは、次の各号の一に該当する行為をいう。
一 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人 の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特 定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当 該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）
二 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定 利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電 子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能 を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号にお いて同じ。）
三 電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用 を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令 を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

8. 本当のハッカー - お約束

Eric S. Raymond 編，福崎俊博訳，アスキー出版局「ハッカーズ大辞典」より

0. もともとは，斧で家具を製作する人
1. プログラム可能なシステムの細かい部分を探ったり，その 機能を拡張する方法を探求したりするのに喜びを感じる人． 最小限のこのしか勉強したがらない大半のユーザとは対象的
2. 熱中して(さらには取り付かれたように)プログラミング する人．または，プログラミングを単に論理化するのでは なく，プログラミングを楽しむ人．
3. ハック価値(hack value)を評価できる人
4. 手早くプログラミングするのが得意な人
5. あるプログラムのエキスパート．または頻繁にそれを使っ て仕事をする人．たとば「UNIXハッカー」
6. あらゆる種類のエキスパートまたは熱狂的なファン．たと えば天文ハッカーなどという．
7. 創意工夫を発揮して打破したり回避したりするという知的 な難問を楽しむ人
8. [誤用] あちらこちら調べ回って情報を機密情報を探り出 そうとする悪意の詮索好き．このことからパスワードハッ カー，ネットワークハッカーなどといわれる．ただしい用 語はクラッカー．

9. 脆弱性(vulnerability)，セキュリティーホール

組織を含む情報システムのセキュリティ上の

- 欠陥
- 開発者，管理者の意図しない弱点
- 予想されなかった利用方法
- 情報セキュリティリスクを誘発する要因

プログラムの場合，以下のような原因で発生:

- 仕様の誤り
- プログラミングの誤り
- インストレーションの誤り
- 設定の誤り
- 想定された利用状況と違う状況での利用

10. なりすまし

正当なユーザ/プロセス/コンピュータのふりをすること
- 他人の名前，ID/パスワード を利用
- 発信元IPアドレスを偽造
- メールのFromアドレスの偽造
- フリーメール等を利用した第3者のふり
- ものまね，こわいろ

11. ソーシャル・エンジニアリング・アタック

- ×社会工学的攻撃
- 技術的でない，または低技術による攻撃
  - ものまね，声色(こわいろ)，演技
  - ぺてん
  - 買収
  - 恐喝
  - 脅迫
  - 窃盗
  - 詐欺
  - 内通者

12. ショルダーハック

- 肩越しにユーザのキータイプやディスプレイを盗み見て、 重要な情報を盗み出すこと

- 人の情報セキュリティ管理の甘さを示す事例

13. トロイの木馬

- 正しいプログラムに見せかけて，不正な機能を含めたプログラム
- ギリシャ神話に登場する「トロイの木馬」に由来
- スパイウエアもトロイの木馬の一種

14. バックドア，裏口

- 正規でない(禁止されている)アクセス経路，アクセス可能とするたの仕掛け
- 侵入者が再侵入しやすくするため仕掛けることがある．例えば:
  - ユーザのパスワードの変更，ユーザの追加
  - トロイの木馬付きのコマンドの追加
  - 正規コマンドをトロイの木馬付きのコマンドに置き換え

- “.rhost”, “.ssh” など，アクセス制御設定ファイルの改ざん
- “/etc/rc”, “.cshrc”などの改ざん
- 侵入用サーバの追加
- cron, atなど周期プログラムの追加
- ルータの設定変更
- モデム，TTYの設定変更

• バックドア，トロイの木馬が仕掛けられると発見は面倒． システムの再インストール，再設定の必要あり

15. システムログ

• システム履歴，動作記録
• オペレーティングシステム，サーバプロセス，アプリケーションなどが イベントごとに記録
• 記録例
  - ログインの成功記録，失敗記録
  - 特権ユーザへの移行の成功記録，失敗記録
  - 認証失敗記録
  - サーバの起動/停止記録
  - ハードウエアエラー
  - :
• アカウンティング情報(コマンド実行，資源利用履歴)
• メールログ

• 壊し方
  - システムログ機能を(一時)停止
  - ログファイルの消去
  - ログファイルの当該情報のみを抹消
  - 無用なシステムログを大量発生

16. スクリプトキディ

- クラックツールに頼った侵入者/攻撃者
- 非技術的クラッカーに対する蔑称
- 年齢によらない

侵入者/攻撃者の大衆化を表す．技術がなくても高度な技術を必要とする 侵入，攻撃が可能となる．

17. DoS（Denial of Service）攻撃

- サービス妨害攻撃
- 大量のデータや不正パケットを送りつけるなどして，正常なサービスを妨害.
  - 高い負荷，レスポンスの低下
  - 脆弱性を攻撃
- 可用性に対する攻撃

18. DDoS（Distributed Denial of Service）攻撃

- 分散サービス妨害攻撃
- 一つのターゲットに複数の地点から，DoS攻撃を行う
- DDoS攻撃のためのツールが流通
- 直接の攻撃元は踏台の可能性が高い
- 防御
  - IPフィルタリング
  - 帯域制御
  - 関連組織との連係し経路から攻撃地点をさがし除去.

19. ポートスキャン

- コンピュータのポートを検索して，起動しているサービスを調べる
- 脆弱性のあるサービスやソフトウエアの発見

- 侵入や攻撃の事前準備
- ポートスキャンを検出することで，侵入や攻撃を事前に察知
- 防御
  - 不要なサービスは起動させない
  - 脆弱性のあるソフトウエアの除去
  - 途中経路のルータによるポートフィルタリング
- ポートスキャン検出されにくいスキャン方法も．別アドレス

20. Q: ポートスキャンをとめたいので何か方法を教えて欲しい

(JPCERT/CC FAQより)

ポートスキャンなどの弱点探索のアクセス自体を完全に止めることは、 技術的に困難です。したがって、これらのアクセスが行われたとしても、 各サイトで運用されているサービスに影響がないように対策を施してお くことが望まれます。また一般論として、あるアクセスについて接続を 拒否したログが記録されていたとしても、その他のすべてのアクセスが 拒否されているとは限りません。監視の対象から外れているサービスや アクセスが行われた形跡がないか、ご確認ください。

21. 踏み台

- 侵入したコンピュータや脆弱性のあるコンピュータを経由して，他に再侵入，攻撃すること
- 逆探知を面倒に
- 利用方法
  - ログインの踏台．攻撃元の逆探知を面倒に
  - ファイアウオールを踏台にした裏口
  - メイル，WEBアクセスの匿名化
  - スパムメールの中継基地
  - DDoS 攻撃基地
- コンピュータだけでなく，ルータ，ネットワーク装置も踏み台になる可能性あり．

22. ブルートフォースアタック

- Brute Force = 力ずくで、強引に
- ex. パスワードの辞書攻撃
- 回線の高帯域化に従い注目したい

23. セッションハイジャック

- 確立した他人の通信を横取りすること
  - TCPのハイジャック
  - DNSのにせ応答

24. バッファオーバラン

- 正規のデータ領域を越えてデータを書き込み，そのデータに実行を移し， 不正にプログラムを実行，または，プログラム/システムの停止.
- バッファーオーバフロー，スタックオーバフローとも
- 例

```
void worse(dest, src) {
 char work[32];
 strcpy(work, src); /* XXX */
   :
}
```

```
while (gets(line) != NULL)  /* XXX */
puts(line);
```

```
sprintf(line,"%s %d", str, val);  /* XXX */
```

- ユーザからみると，長い文字列を入力
  - 長いタグ
  - 長いURI
  - 長いパラメータ
  - 構文に違反する入力データ
  - :

25. Internet Worm 1988

- 1988年11月2日
- 隣接する計算機を侵入しながら増殖する Worm プログラム
  - Robert Morris @ Cornell大学
  - VAXとSUNワークステーションが対象
- インターネットが数日停止
- 完全修復に1週間
- セキュリティホールに対する関心が高まる
  - ソフトウエアの脆弱性への理解
  - 対策ツール (例. Crack, COPS, ...)の開発
  - セキュリティ関連情報の流通
  - CERT/CCの発足へ
- 基本的なアイデアがそこに :-(
  - 隣接ホストを発見
    - **/etc/hosts.equiv**
    - **/.rhosts**
    - ルーティング表
  - ユーザの発見
    - **/etc/passwd**
    - **~/.rhosts**, **~/.forward**
  - 相手ホストに侵入
    - パスワード予測と rsh, rexec の遠隔実行
    - sendmail の DEBUGコマンド
    - fingerd の **gets()**オーバフロー
- 相手ホストに自分の複製をつくり繰り返す

26. IDS

• Intrusion Detection System ― 侵入検知システム
• 侵入を自動的に検出し管理者に警告を発する.

二つの検出方法

• ミスユース検出(misuse detection)
  - 不正を検出
  - 侵入パターンのデータベース(シグネチャ)と比較
  - 知られた侵入に対して確実に警告
  - 知らない侵入方式には無力

• アノマリ検出（anomaly detection）
  - 例外，通常ではない状況を検出．異常検出.
  - (主に)統計的処理
  - 知らない侵入にも対応できるかも
  - 誤検出，過剰検出，すなわち，無用な警告の多発の可能性

二つのタイプ

• ネットワーク型
  - ネットワークのトラフィックを監視
• ホスト型
  - システムログ等を監視

使って悪くないが，過剰な信頼は禁物.

27. 分散協調IDS

• ネットワークの複数の地点での侵入情報を集め，広域での侵入を検出
• 影響範囲が広域の侵入に対応

28. インシデント情報交換フォーマット

- CSIRT間の情報交換
- IETF inch(Extended Incident Handling) WG
  - IODEF(インシデント・オブジェクト・記述フォーマット)
  - XMLベース

  ☞ *http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-01.txt*

29. ハニーポット

- 蜂蜜の壷
  - 脆弱性のあるように見せかけたシステムを公開
  - 侵入者/攻撃者をおびきよせる
  - 意図的に侵入/攻撃させる
  - 侵入/攻撃を検出して，行動を記録し，管理者に警告
- 侵入方法を知ることができる
- 素人には危険．法律的，倫理的問題も．

- ホスト型IDSの一種とも

- The Honeynet Projec

  ☞ *http://project.honeynet.org/*

30. 疑似アタック，

- ペネトレーションテスト(penetration test)，侵入テストとも
- 外部から侵入を試みるテスト
- ツールによる方法，人が侵入を試みる方法
- 専門(有料)のプロフェッショナルサービスも

- セキュリティ対策ができていないシステムにとっては
  - 問題点が明確になる
- セキュリティ対策ができているシステムにとっては

- 設定の再チェックができる
- 外部監査的な意味あいも

• 抜きうちで行うことも

31. 防火壁 - Firewall

• ポリシの界面での調整機構
• 前提条件
  - ポリシとネットワークトポロジが一致していること
  - 通信は，全部*ここ*を通ること.
• 新しいポリシ調整機構への期待．防火壁では対応しにくい環境.
  - 個人利用
  - ターミナルが直接ネットワーク接続
  - ユービキタス・コンンピューティング

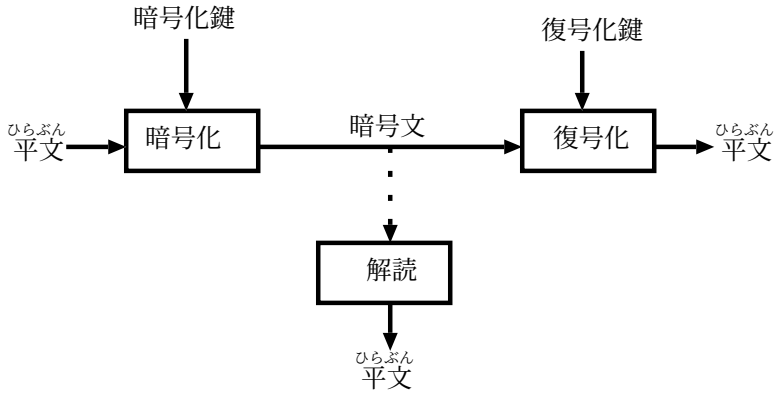
32. DMZ

• 非武装地帯 (DeMilitarized Zone)

33. 暗号基礎講座

- 暗号
  - 暗号文をつくって機密を守る．通信時，蓄積，保存 .
  - 発信者の認証を行う.
  - 改ざん(不正な書き換え)を検出する.
- 鍵交換
  - 公開鍵証明書
  - PKI(Public Key Infrastructure, 公開鍵基盤)
- 応用
  - IPSec
  - DNSSEC
  - SSL, TLS
  - SMIME, PGP

34. 暗号系



- 暗号(cryptography)
- 平文(ひらぶん，plaintext)
- 暗号文(ciphertext)
- 暗号化(encryption)
- 暗号化鍵(encryption key)
- 復号化(decryption)
- 復号化鍵(decrytion key)
- 解読(cryptoanalysis)
- 暗号系(cryptosystem)

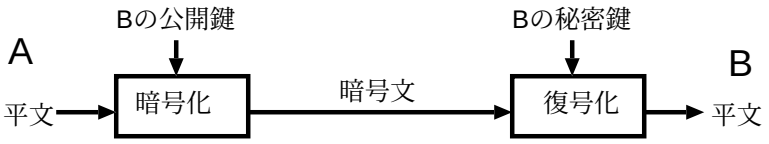
35. 暗号アルゴリズム

• 対称暗号系(慣用暗号系，共通鍵暗号)
  - 暗号化鍵と復号化鍵が同じ
  - 非対称鍵暗号系に比べて高速に処理
  - 例
    - DES(Datat Encryption Standard, 54ビット)，すでに弱い
    - AES(Advanced Encryption Standard, Rijindael, 128ビット)
    - トリプルDES

• 非対称暗号系(公開鍵暗号系)
  - 暗号化鍵と復号化鍵が異なる
  - 片方の鍵が知られても他方の鍵を知るのが困難
  - 計算が容易でない数学的問題を利用
  - 対称暗号系にくらべて処理が遅い
  - 署名，守秘に利用
    - 例
    - RSA(RSA暗号アルゴリズム)
    - ECDSA(楕円曲線暗号アルゴリズム)

36. 公開鍵暗号系による暗号化

- 受信者(B)の暗号化鍵を公開とする
- 発信者は公開されたBの暗号化鍵で暗号化
- 受信者は自らの秘密鍵で復号化
- 暗号文を復号化できるのは，Bだけ

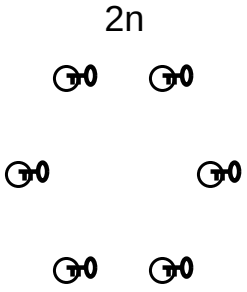


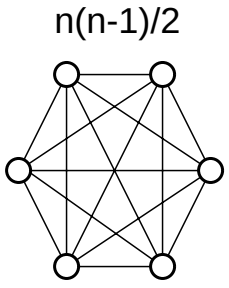
37. 公開鍵暗号系による署名，改ざん検出

- 発信者(A)の復号化鍵を公開とする
- 発信者は自らの秘密鍵で暗号化
- 受信者は公開されたAの復号化鍵で復号化
- 復号化がうまくいけば，Aからのものであることが確認でき，改ざんのないことも確認

38. 鍵の数

- n人がそれぞれ互いに暗号通信を行うとき
- 共通鍵暗号系の場合，それぞれが，他の(n-1)人分の秘密鍵を共有しなければならない． 全体で，n(n-1)/2.
- 公開鍵暗号系の場合，それぞれが，鍵の対をもち，一方を公開する． 全体で，2n.





39. CRYPTREC(暗号技術評価プロジェクト)

- 電子政府における調達のための推奨すべき暗号(電子政府推奨暗号)
- 今後10年間は安心してつかえる暗号技術
- リスト2003年2月公開
- 継続して評価改定を行う

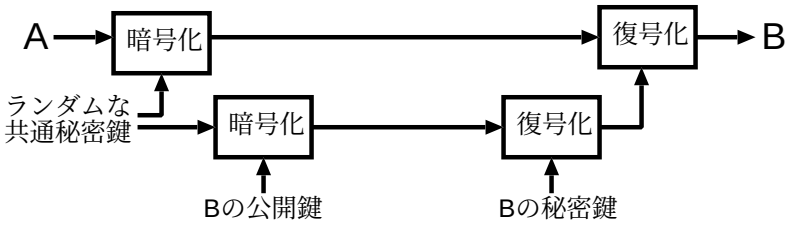
☞ *http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030604_press.html*

40. 電子政府推奨暗号リスト (2002年2月20日，総務省/経済省)

- 公開鍵暗号
  - 署名
    - DSA, ECDSA, RSASSA-PKCS-v1_5, RSA-PSS
  - 守秘
    - RSA-OAEP, RSAES-PKCS-v1_5
  - 鍵共有
    - DH, ECDH, PSEC-KME
- 共通鍵暗号
  - 64ビットブロック暗号(128ビットブロック暗号を推奨)
    - CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3-key Triple DES
  - 128ビットブロック暗号
    - AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000
  - ストリーム暗号
    - MULTI-S01, MUGI, 128-bit RC4
- その他
  - ハッシュ関数
    - RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512
  - 疑似乱数生成系
    - PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1， PRNG based on SHA-1 for general purpose in FIPS186-2(+change notice 1)Appendix 3.1，PRNG based on SHA-1 for general purpose in FIPS186-2(+change notice 1)reviced Appendix 3.1

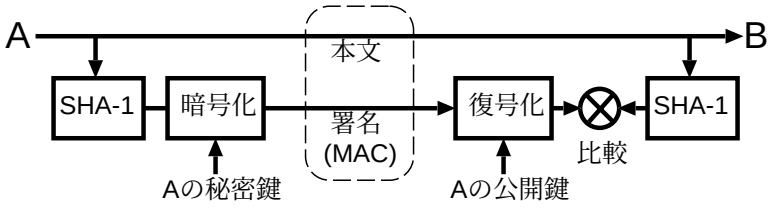
41. 公開鍵と共通鍵を組み合わせた暗号化

- 一時的に利用する共通秘密鍵を乱数を用いて生成
- 受信者(B)の公開鍵で共有秘密鍵を暗号化して送る
- 文書を共有秘密鍵で共通鍵暗号で暗号化して送る
- 受信者は自らの秘密鍵で暗号化された共有秘密鍵を復号化する
- 復号化された共有秘密鍵で文書を復号化する



42. 公開鍵と共通鍵を組み合わせた署名

- 文書をハッシュ関数(たとえばSHA-1)にかけ固定長データにハッシュ化する
- ハッシュデータを自らの秘密鍵で暗号化する．これを MAC(Message Authentication Code)と呼ぶ.
- MACを本文と共におくる.
- 受信者は，MACを発信者の公開鍵で復号化する
- 上記データと本文をハッシュ化したデータを比較して，一致していれば， 発信者からのものであることが確認でき，改ざんのないことも確認

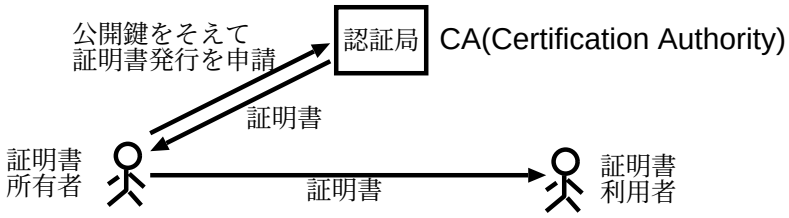


43. ハッシュ関数

- 可変長のデータを固定長データに変換
- セキュリティ向けのハッシュ関数をセキュアハッシュ関数と呼ぶ
  - 入力データの長さが違ってもダイジェスト長は一定
  - 入力データが少しでも異なれば，ダイジェストは大きく異なる
  - ダイジェストから入力データの算出は困難
  - 同じダイジェストの異なった入力データを見つけるのは困難
- 例えば
  - MD5．RFC1312．128ビットを出力．弱点がみつかっている
  - SHA-1，RFC3174．160ビットを出力．主流．

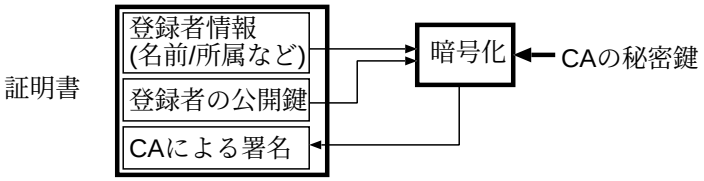
44. PKI

- Public Key Infrastructure, 公開鍵基盤
- 公開された公開鍵が本当に本人のものであることを保証する
- 信頼できる第3者(TTP： Trusted Third Party)に公開鍵の署名を受ける
- このTTP を認証局(CA)と呼ぶ



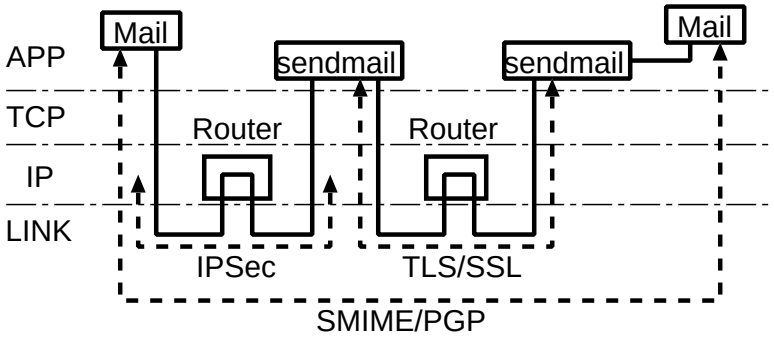
45. 証明書

- CAによって署名された公開鍵
- X.509 証明書．ITUのX.509で規定され，RFC2459でインターネットでの利用が規定.



46. プロトコル階層と暗号

- エンドトゥーエンド
- トランスポートレベル
- IPレベル
- リンクレベル
- 物理レベル



47. 「セキュリティ文化」

• 2002年8月 改定 OECDガイドライン で登場

- 情報システムやネットワークにおけるセキュリティの意識の促進（啓発）をはかる
- セキュリティを十分考慮してシステム構築を行うべきこと

情報システム及びネットワークのセキュリティのためのガイドライン セキュリティ文化の普及に向けて

☞ *http://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl_a.html*

☞ *http://www.oecd.org/pdf/M00033000/M00033182.pdf*

I. セキュリティ文化の普及に向けて

このガイドラインは、セキュリティ文化（すなわち、情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること）の発展を促進することによって、絶えず変化を続けるセキュ リティの環境に対応するものである。このガイドラインは、ネットワーク及び システムの安全な設計及び利用が後知恵の結果であったことが余りにも多かっ た時代との明確な決別の合図である。参加者は情報システム、ネットワーク及 び関連するサービスに一層依存するようになっており、これらすべてが信頼で き、かつ安全なものであることが必要となっている。すべての参加者の利益、 並びにシステム、ネットワーク及び関連するサービスの性質を適切に考慮した アプローチのみが、効果的なセ キュリティを提供し得る。各参加者は、セ キュリティを確実にするための重要な担い手である。参加者は、自らの役割に 応じて、関連するセキュリティリスクと予防の手段を認識し、責任を持って、 情報システム及びネットワークのセキュリティを強化するための措置をとるべ きである。

セキュリティ文化を普及させるためには、リーダーシップと広範な参画の双方が必要となる。また、セキュリティ文化の普及により、すべての参加者の間

でセキュリティの必要性が理解されるとともに、セキュリティの計画及びマネジメントに高い優先順位が与えられるべきである。セキュリティの課題は、政府及び企業のすべてのレベルにとって、またすべての参加者にとって関心を持ち、責任を持つべき事項である。このガイドラインは、社会全体でセキュリティ 文化の普及に向けた取り組みが行われるための基礎をなすものである。これに より、参加者がすべての情報システム及びネットワークの設計及び利用にセキュ リティを組み込むことが可能になる。このガイドラインは、すべての参加者が、 情報システム及びネットワークの運用について考え、評価し、影響を与える方 法として、セキュリティ文化を取り入れ、普及することを提案する。