情報科学（二）講義資料-12　情報セキュリティ対策　　大島正毅

2001.07.09　改訂

情報セキュリティ対策（安全性、信頼性）

計算機やネットワークは大規模で複雑であり、組織活動・社会活動に大きな影響を及ぼしているため確実に動作することが求められる。計算機やネットワークの特性をよく理解して対策を立てる必要がある。

安全

　セーフティ　自然災害が主

　セキュリティ　人為的が主

RAS（Reliability, Abailability, Servicability）信頼性、可用性、保守性

IS（Integrity, Security）一貫性維持、セキュリティ、A（Auditability）監査性

（初期には RAS と呼ばれていたが、現在は RASISA という）

大別して、自然災害等の外部要因、システム構成要素の障害、人為的障害（外部・内部）に対処できる必要あり。

自然災害等

・火災、水害、地震、停電、通信回線の障害

　対策：消火設備（計算機用にはハロン等が使われる。しかし人が窒息する危険がある）、設置場所（水害が予想される場合、高い位置に設置、水（給・配水管、エアコンダクト出口などの）を近づけないように配置する）、機器を十分固定する・耐震構造にする（地震対策）、無停電装置、自家発電、給電の二重化、ケーブルの確保など。通信回線の二重化（例通常専用回線、予備に ISDN 回線）

・システム構成要素の障害

　ハード（ディスク、CPU）の故障、ソフト的障害、誤操作、ファイルの容量オーバなど

　2 重化・冗長化（システム全体（デュアル接続、デュプレックス接続）、ディスクのミラーリング（データを2 重に持つ）、RAID ディスク、フォールトトレラント計算機）、ファイルのバックアップ（システム全体としても、個別ユーザにも重要　システムに関しては定期バックアップ計画を作り計画的にバックアップを行う。フルダンプ（全体のバックアップ）とインクレメンタルダンプ（変化のあった部分だけをバックアップ）を組み合わせることが多い）

・人為的障害（Integrity、Security に関わる）

　　内部　誤操作、悪意

　　外部　侵入

外部からの悪意の侵入（クラッカー）がクローズアップされやすいが、全体のバランスが重要　内部の悪意への対応難しい（職掌分離、操作を単独でしない、人事を固定化しない、退職時には在職時の秘密保持誓約書にサイン）

機密情報、重要情報の類別、保護方針

機密情報とバイタル情報は特に重点的に対策する、マニュアル化するのがよい

バイタル（vital）情報：組織活動継続に特に重要な情報（売掛金・買掛金情報、在庫情報、顧客情報など）

建物・部屋の入出管理、鍵管理、端末操作の途中で席を立たない、ネットワークからの遮断、ファイアウォール、パケットフィルタリング

ファイアウォール

組織内部のネットワークと外部ネットワークの間に関門となるファイアウォールを置く。内部では自由に通信できるが、外部との通信は制限する。

パケットフィルタリング

たとえば、telnet について IP アドレスが内部のものは通過させるが、外部は通過させないようにパケットを識別して処理する。TCP wrapper などが使われている。

ssh (Secure Shell)

ssh は rsh(リモートシェル) と同様にネットワークを介して遠隔地のコンピュータにログインしてコマンドを実行するプログラムで、（rsh とは異なり）強力な認証システムによって安全ではない経路を通じての安全な通信を提供するために使われる。

ユーザ識別　ログイン・ファイルアクセス時のパスワード確認、ID カード、生体計測（指紋、声紋、手形、掌紋、眼底パターン、キーストローク等）による本人確認

単純なパスワードは避け時々変更する、管理者用パスワードは特に注意。パスワードに期限を設けたり、使い捨てにすることもある。

リソース管理　ユーザ毎にアクセスできるファイル、可能な操作を規定する　UNIX ではユーザをデータの作成者、同一グループ、他者について、それぞれファイルの保護機能（r, w, x）がなされている、簡単で実効がある

組織では担当部署のデータは読み書きでき、他部署データは読むだけ、機密データはいずれも許可されないなどとする。

システムの情報をみだりに公開しないこと（ネットワークアドレス、リモートアクセス用電話番号等）

セキュリティホール

セキュリティ対策上の穴。計算機の保守用・検査用に出荷時に用意されているユーザアカウントが残されている場合セキュリティホールとなりやすい。パスワードの変更はシステムレベルでしか行えないが、自分のパスワード変更は可能なようにプログラム実行ファイルに setuid ビットを付ける。同様の目的で setuid ビットを付けるプログラムはセキュリティホールになりやすい。

ウィルス

ほかのプログラムに寄生し、プログラムの動作を狂わせるプログラム。

ワーム

独立したプログラムで、ネットワークを介して増殖する。
トロイの木馬
外観上は役に立つプログラムとして配布されるが、内部に不正な機能が隠されているプログラム。
爆弾
一定の日時が来ると不正な操作を行うプログラム。
trap door（落とし戸）
システムの保守用に設計時に作りこまれる秘密の入り口。通常の手続きを無視して特権を得られるようになっていることが多い。
ソーシャルエンジニアリング
管理者や上役のふりをして電話で重要な情報を聞きだしたりする手法の総称。
コンピュータ緊急対応センター
コンピュータセキュリティに関わる事件の情報を集め、対策を教示する団体、JPCERT/CC の略称で知られる（http://www.jpcert.or.jp/）。
システム監査
誰がどんな操作をしたか記録
普段と異なる操作、重要な操作の記録
　ただしこれらを徹底すると処理速度が遅くなったりファイル容量を食ったりする
（c.f.　C2 セキュリティ=国家安全保障局）

・暗号

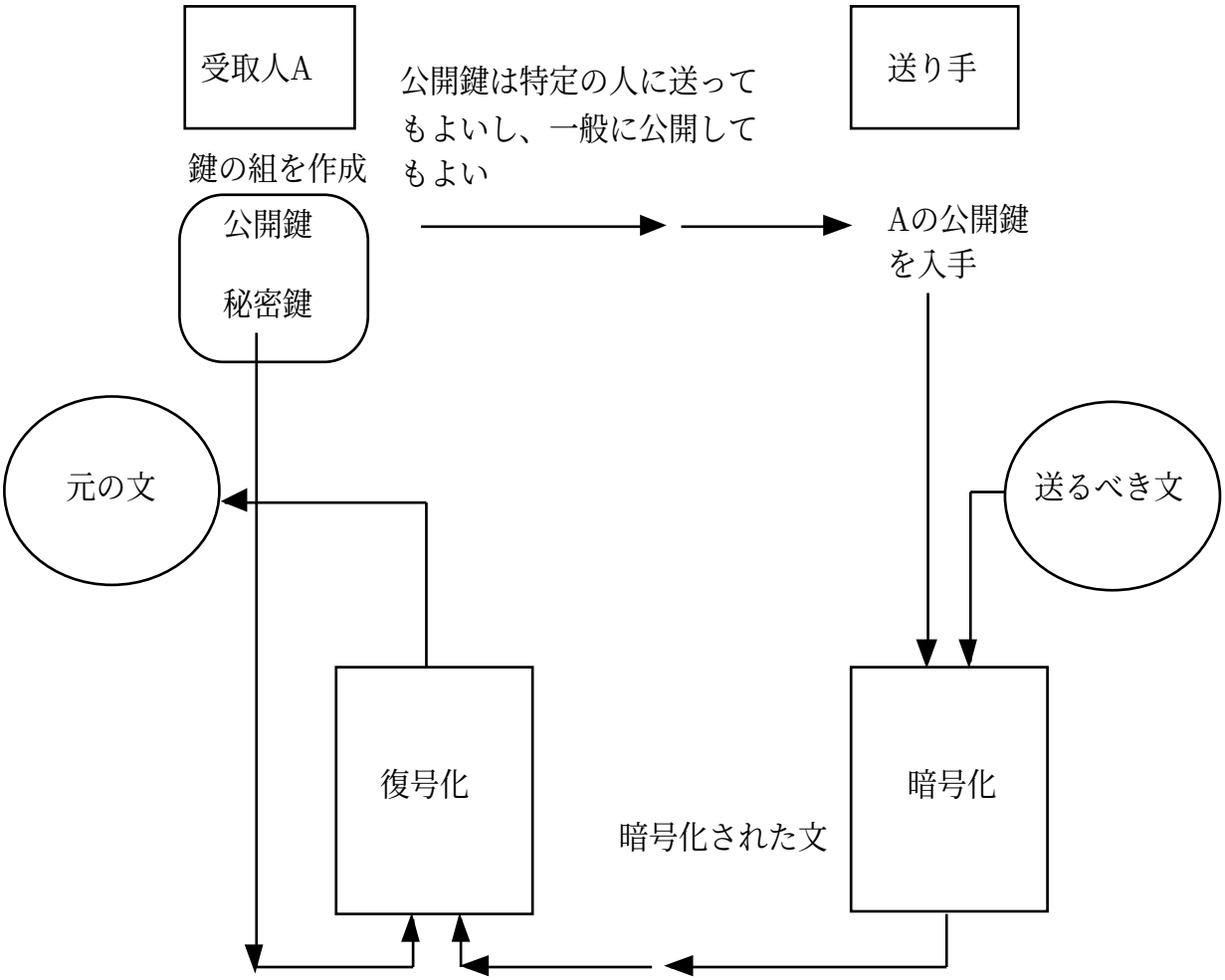
古くから使われているのは秘密鍵方式。暗号化も復号も同じ鍵を用いる。秘密鍵の受け渡しはじかに行うのが原則。

DES（Data Encription Standard、米国で標準化されている秘密鍵方式）

公開鍵暗号

RSA アルゴリズムが著名。暗号化と復号を別の鍵で行う。暗号化は公開鍵で行ない、復号は秘密鍵で行う。ある人が自分の鍵をきめ、公開鍵と秘密鍵を作成する（ペアになっている）。公開鍵は一般に公開してもよいし、非公開でも秘密にしなくてよい。送りたい人は公開鍵で送りたいデータを暗号化し、受け取った側は秘密鍵で復号する。秘密鍵は本人だけしか知らないので、他人は復号できない。

公開鍵方式の方が安全性が高いが、処理効率が悪いので、公開鍵と秘密鍵の併用（秘密鍵を公開鍵方式で送り、正味のデータを秘密鍵方式で送るなど）も行われる。



公開鍵による送信と受信

・リスク分析
　管理統制
　物理的セキュリティ
　信頼性
　不測事態対応計画
　適用業務保全性
　アクセス管理
　データ伝送の保護

参考文献

1.上園忠弘：情報システムのセキュリティ、トッパン、2,400 円
2.Deborah Russell/G.T. Gangemi Sr.著、山口　英監訳：コンピュータセキュリティの基礎、アスキー出版局、4,800 円
3.長島洋一：はじめて学ぶ情報セキュリティ、工業調査会、1,854 円
4.E. Guttman, L. Leong, G. Malkin：一般ユーザのためのセキュリティハンドブック、UNIX MAGAZINE, 1998.8