

セキュリティ入門

Internet Week '99

株)電通国際情報サービス

デジタルキャンパス

熊谷誠治

kuma@isid.co.jp

Copyright © 1999 All Rights Reserved, by Seiji Kumagai

Information Services International - Dentsu, Ltd.

セキュリティって何？

- 辞書(EXCEED 英和辞典)で引くと...
 - se · cu · ri · ty
 - n.安全(from); 安心; [古]油断; 确实; 保護, 保安; 防衛(策) (against; from);
 - 【コンピュータ】安全保護(無断でデータにアクセスできないようにすること); 保証(金・人); 担保(品); 借用証(for); (pl.)証券, 証書, 債券.
- 安全を守ることらしい
 - 安全といわれると重要かと思うが...

Information Services International - Dentsu, Ltd.

何から何を守るのか？

- 何を守るのか？
 - 人命
 - 企業
 - 財産
 - 名誉
 - 情報
 - 人権
- 何から守るのか？
 - 天災から
 - 事故から
 - 犯罪者から
 - 一般人から
 - 運命から

どのように守るのか？

- それが問題
 - 対象物による
 - コストはどの程度かけられるのか
- 守る必要はあるのか？
 - コストをかける価値があるのか
 - それによって何が得られるのか
- 失うものを知ることが重要
 - 会社の存続に関わる情報
 - 一度失うと回復が難しい信用
 - 失ってもいいものばかりなら守る必要がない

発生している事件

- 盗聴
- 侵入
- なりすまし
- 情報の改ざん
- 情報の破壊
- 情報の盗みだし
- ウイルス
- ワーム
- SPAM

発生している被害

- 誹謗・中傷
- 不法品売買
- 猥褻(わいせつ)図画陳列
- クレジットカード盗用
- 脅迫
- アクセス妨害
- 業務妨害
- 詐欺
- プライバシー侵害
- 著作権侵害
- いたづら

具体的なトラブルの例

- 私の名前で掲示板に第三者の悪口を投稿された
- 私のメールアドレスで宣伝メールを送られた
- プロバイダの請求額が予想よりも多い
- 掲示板に自宅の住所と電話番号が掲載された
- 宣伝メールがどんどん送られてくる
- 身に覚えのないクレジットカードの請求がきた
- 私が送ったメールを第三者が知っているようだ
- パソコンに変な表示が出たあと動かなくなった
- NASAからアタックはやめろと抗議メールがきた
- Webを勝手に書き替えられた

Information Services International - Dentsu, Ltd.

iSiD

インターネットだけの問題か？

- 実社会でも起こっている
 - 怪文書
 - 注文していないピザが届く
 - クレジットカード偽造
 - キャッチセールス
 - ニセ通販
 - カード請求金額不正増額
- インターネットの登場で...
 - 犯罪がより手軽に実行できるようになった
 - 顔が見えないので安心してしまう
 - 追跡手段があるので検挙率は向上しているのでは？

Information Services International - Dentsu, Ltd.

iSiD

クレジットカードは危ない!?

- サインだけで確認
 - カードはカード会社が保証
 - » 発行時点で身元確認
 - 限度額が信用範囲
- インターネットではサインが送れない
 - 電話番号で確認する程度
 - » 電話番号は簡単に調べられる
 - 名義人以外を受けつける業者は要注意
- 暗証番号に注意
 - たったの4桁
 - キャッシングされると...
 - 保険があっても安心できない
- ほかに危険がいっぱい
 - でも大量に使われている

結局は利用者の意識の問題

- 暗証番号の管理
 - 暗証番号を難しくすると忘れる
 - 全部同じ暗証番号にすると被害が拡大する
- 利用結果の確認
 - 利用控の保存
 - 毎月の利用明細の確認
- 利用ルールの確認
 - 誤請求の処理手順
 - カード会社の責任範囲
- 購入先の確認
 - リスクの判定が重要

インターネットは危険 !!

- 現実にトラブルが起こっている
 - マスコミが大きく取り上げる
 - つぎの被害者は自分かもしれない
 - よく分からないので怖い
- 技術の進歩が早すぎる
 - 社内に分かる人がいない
 - 勉強しても追いつけない
 - いつもハッカーが先行している
- 専門家が少なすぎる
 - 知識が私 < 相手 なら、信じるしかない
 - しかし、相手 < 世間の常識 ということもあり得る

インターネットは安全 !!

- 現実にみんなが使っている
 - そんなに危なければだれも使わないはず
 - 利用者が多いので犯罪にあう確率は低い
 - 安全のためのしくみがたくさん販売されている
 - 専門家に任せているから大丈夫
- インターネットで最新情報が届く
 - ちゃんと見張っていれば危険な状況が把握できる
 - 最初に攻撃されるとは考えにくい
- 使わないとビジネスにならない
 - 使う以上、危ないとはいえない
 - どう安全に使うかが問題

本当はどっち？

- 安全だと思っている人には「危険」を説く
 - 安全だと思ふことは危険
 - 安全だと思つて使つてはいけない
- 危険だと思っている人には「安全」を説く
 - 危険だと思つている人には安全
 - 危険だからと使わなければビジネスができない
- どうすればいいの？
 - 危険さを理解し、
 - 十分な対策をとり、
 - 常に「危険」を意識しながら使う

法整備の遅れる日本

- 「情報」を盗んでも罪を問えない
 - プリントアウトした紙
 - コピーに使つたFD
- にせクレジットカードの保有もOK
 - 使つて初めて罪になる
 - 偽造団が日本に押し寄せる
- 国家権力には通信の盗聴が許される
 - 手続きなどがいいかげん？
 - 通信以外の盗聴は？
 - » 盗聴器を仕掛けるために侵入すると不法侵入
- 自分の身は自分で守るしかない

何を守るべきなのか

- 自身の持つ情報
 - パスワードだけで守られているといえるのか？
- 外部からの侵入
 - 侵入口をふさぐ
 - 侵入を検知する
- 外部からのコマンド実行
 - 侵入しなくてもできてしまう
 - セキュリティ・ホールからプログラムを送り込む
 - CGIで実行する
- コマンドが実行できると...
 - システムの破壊、情報の持ち出しが可能

プライバシーが狙われている

- Cookieを食べますか？
 - クライアントを特定するためのしくみ
 - Webをアクセスするとクライアントに送られる
 - 拒否できるがdefaultでは受け付ける
- どうなるの？
 - アクセス状況をサーバ保有者に把握されてしまう
 - アンケートなどに答えて氏名を明かしていると...
 - » アクセス状況が個人にひもづけされる
- 拒否したほうがいいのか？
 - プライバシーに関する考え次第
 - 拒否するとアクセスできないサイトもある

プライバシーと無料サービス

- 日本人はプライバシーに無頓着？
 - 電話帳に電話番号を載せている人は？
 - 同窓生名簿も要注意
 - 自分の名前をWebで検索してみると...
- 年賀状サイト
 - 送りたい相手のメールアドレスを伝えると届く
 - メールアドレスを集める手段
 - 利用すると相手に迷惑がかかることも
- プレゼントやアンケート
 - これもメールアドレスを集める手段
 - 個人情報がどんどん流出する

ウイルスに注意していますか？

- システムを破壊する伝染性のあるプログラム
 - メール添付のプログラムやデータに寄生
 - コンピュータに伝染しシステムを破壊
 - データの転送などでどんどん感染
- ウイルスチェックで万全か？
 - パターンファイルは配布が遅れる
 - だから受け取ってすぐには開かない
 - » 他の人が開いて問題のないことを確認する
 - » 新しいパターンファイルがくるまで待つ
- 他人を信用しないことが重要
 - 「信じるものはだまされる」
 - 自分の安全は自分で守る

Unsolicited Commercial Email

- 一般にはSPAMと呼ばれている
 - SPAMはハムの缶詰
 - インターネットとどう関係があるのか？
- 勝手にどんどん送られてくる宣伝・広告メール
 - メールアドレスが販売されている
 - 効果があると勘違いしている
- 受信者に通信コスト負担を強いる
 - 発信コストは安いが受信者は迷惑
 - FAXによるDMと同じように問題
- 勝手に広告を送りつける企業からは買わない
 - 効果がなければなくなるはず？
- ある程度はシステムで防げるが...

Information Services International - Dentsu, Ltd.

iSiD

パスワードで守れるのか？

- やさしいパスワードは危険
 - 辞書に載っている文字列
 - 人名、製品名、グループ名なども
- 難しいパスワードも実は危険
 - 総当たりすればいずれ当たる
 - 総当たりには時間がかかるが...
- ひとつのパスワードを流用しない
 - 目的にあわせてパスワードを変える
 - 重要度にあわせてパスワードを決める
- パスワードを共有しない
 - ひとつのIDを共有すると責任が不明確に

Information Services International - Dentsu, Ltd.

iSiD

より安全なパスワード

- パスワードを使い捨てる
 - 毎回、違うパスワードを入力するしくみ
 - これなら盗聴されてもつぎは違うパスワードが必要
 - 総当たりで試そうとしても、総当たりにならない
- どんなシステムがあるのか
 - S/Keyというフリーウェア
 - SecurIDなどのトークン・カード
- 使うのが面倒？
 - S/Keyは毎回計算が必要
 - SecurIDなどはPINの入力が必要
 - » Personal Identification Number



改ざんされても大丈夫

- ハッカーが侵入してコンテンツを改ざん...
 - 重要な内容じゃないから消えても大丈夫
 - コピーがあるからすぐに元に戻せる
 - だれも読んでないから大丈夫
- ほんとに大丈夫なの？
 - 商売敵の悪口に書き替えられたら
 - ダウンロード用プログラムにウイルス仕込まれたら
 - 新聞に大きく取り上げられたら
 - 踏み台にされてNASAに侵入されたら
- 問題の大きさに気づかず「大丈夫」では？
 - 現実はこの人が多い



踏み台に注意

- 踏み台って何？
 - 誰かが侵入するが、破壊も盗みもしない
 - そこからさらにほかへ侵入する
- 被害はないのか？
 - 踏まれただけでは表面的な被害はゼロ
 - これだけでは痛くもかゆくもない
 - だから気づきにくい
- それで...
 - つぎに侵入されたところからは侵入者に見える
 - 犯人扱いされてしまう 告訴される危険もある
 - 他の組織に大きな迷惑をかけることになる

ハッカーがうじゃうじゃいる？

- プロと行き過ぎた研究者と模倣犯
 - それぞれが活動中
- 産業スパイ
 - 冷戦の終了で産業界へ移行か
 - 国家安全保障局が手を貸すといううわさも
- 研究の果てに
 - 技術を試したくなる
 - 名前が残ることもある
- できるといわれればやってみたくなる人も
 - 情報はたくさん流れている
 - 犯罪という意識が薄い

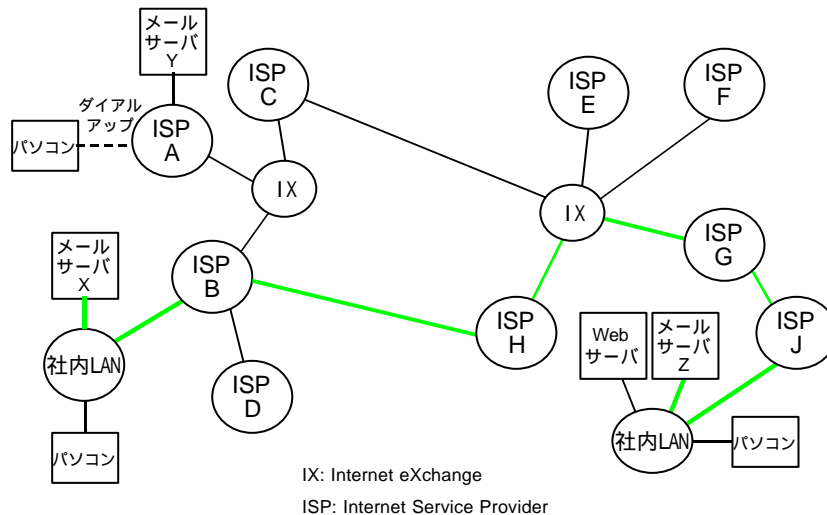
盗聴されている？

- 巷のうわさ
 - ハッカーがたくさんいる
 - インターネットはバケツリレー
 - 国家レベルで監視されている
 - 社内LANの盗聴は簡単
- 今と昔は全然違う
 - ネットワークの造り方
 - 商用化
 - 管理体制
- それで、安全性は...

isiD

Information Services International - Dentsu, Ltd.

インターネットのしくみ



isiD

Information Services International - Dentsu, Ltd.

盗聴は可能なのか？

- 何を盗聴するのか？
 - メール
 - クレジットカード番号
 - すべての通信
- 盗聴場所は
 - 社内LAN
 - 接続しているISP
 - 経路のISP
 - 相手の社内LAN
 - 通信会社
 - サーバ

バケツリレーってほんと？

- インターネットはバケツリレー？
 - これは昔の話
 - いまはバケツリレーなんかしていない
 - end-to-endの通信
- 途中の盗聴は難しい
 - 電話の盗聴に比べるとはるかに難しい
 - 保存されるメール・サーバが狙われる
 - 途中では保存されない

社内LANは危ない

- Ethernetは共有メディア
 - 1本のケーブルにみんなの通信が流れる
 - その気になれば簡単に盗聴できる
 - 盗聴データを解読するソフトも存在する
- お金をかければ解決できる
 - スイッチング・ハブで不要なデータを流さない
 - ルータでネットワークを分割する
 - ルータでアクセス制限をかける
- 生のデータが見えると...
 - メールが盗聴される
 - パスワードが盗聴される

盗聴に備える

- インターネット通信路上の盗聴は難しいが...
 - 国家がやればできてしまう
 - 探偵に頼まれた通信会社職員が荷担すれば
- 絶対に不可能ということではない
 - 盗聴に備えなければならない
 - 海外との通信は特に注意が必要
- どのように備えるのか
 - 重要な情報をインターネットで送らない
 - » 電話はもっと危ない
 - 通信路を暗号化する
 - 電文を暗号化する

Virtual Private Network

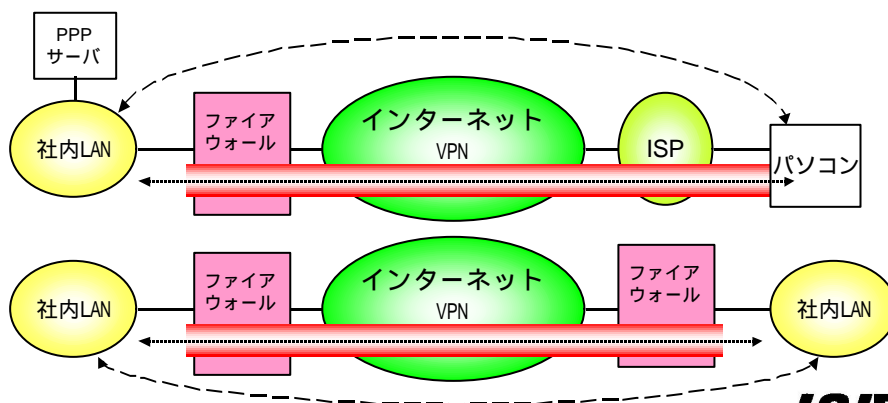
- 実質的なプライベート・ネットワークを作る
 - インターネットを使って
 - 暗号技術で盗聴を防ぐ
 - 「仮想」ではなく「実質的な」
- あたかも専用線のように
 - いくつかのパターンが存在
 - » ネットワーク ←→ ネットワーク
 - » ネットワーク ←→ コンピュータ
 - » コンピュータ ←→ コンピュータ
- メリットは
 - 通信費の削減が可能
 - 社外から安全に通信可能

Information Services International - Dentsu, Ltd.

iSiD

Virtual Private Network(cont'd)

- デメリット
 - 接続相手のリスクがそのままやってくる



Information Services International - Dentsu, Ltd.

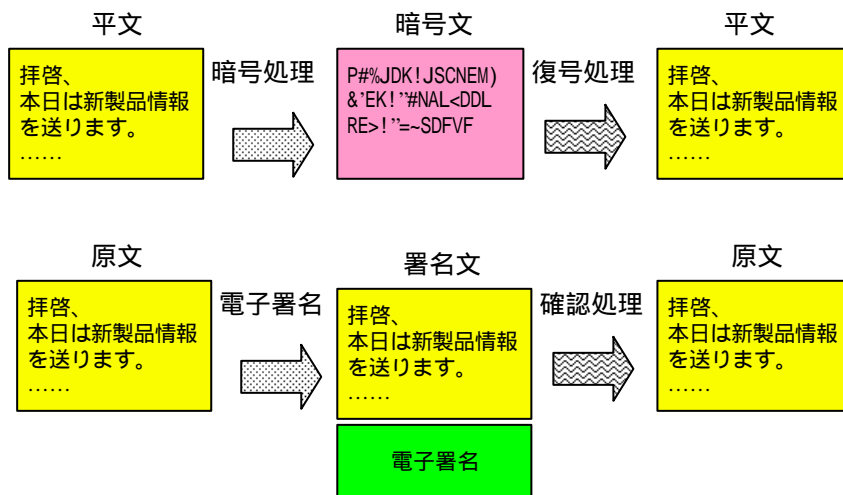
iSiD

脆弱なメールシステム

- メールに多くのリスクが存在
 - 暗号化されていないから盗聴される
 - 発信者を確認できないからなりすまされる
 - 書き替え可能だから改ざんされる
- 暗号電子メール
 - PGP(Pretty Good Privacy)
 - S/MIME(Secure/MIME)
 - » MIME Multipurpose Internet Mail Extensions
- メールで暗号処理
 - 電文の暗号化
 - 電子署名で発信者確認と改ざん検出



暗号メールの使い方



暗号メールに使う暗号技術

- 暗号の利用方法
 - 通信経路で盗聴されても分からない - 暗号
 - ネットワーク越しは相手が見えない - 認証
 - 電子情報は書き換えても分からない - 改ざん発見
- 共通鍵暗号方式
 - 電文の暗号化に利用する
 - » DES, TripleDES, ISEA, RC2, RC4, MISTY, FEAL, CAST
- 公開鍵暗号方式
 - 認証と共通鍵の暗号化に利用する
 - » RSA, Diffie-Hellman, ElGamal
- メッセージ・ダイジェスト
 - 改ざん発見に利用する
 - » SHA-1, MD5

Information Services International - Dentsu, Ltd.

iSiD

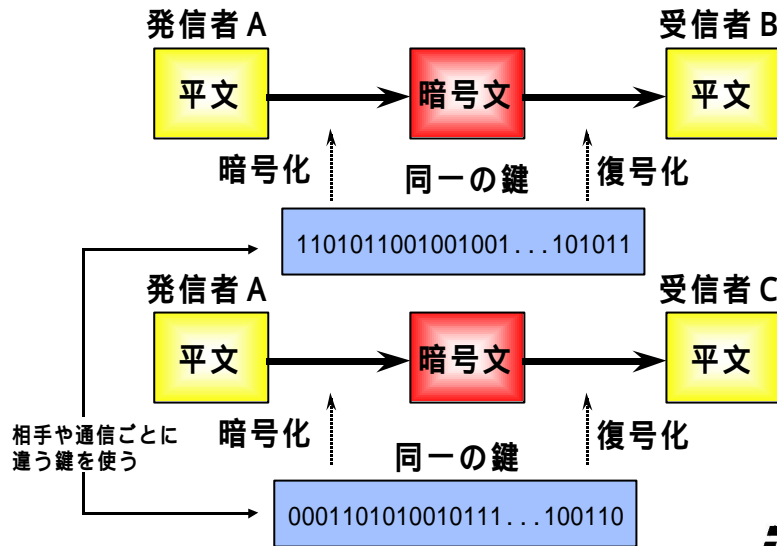
共通鍵暗号方式

- 送信者と受信者は暗号、復号に同じ鍵を使う
 - 共通の鍵だから「共通鍵暗号」
- 処理速度が速い
 - 大量のデータを処理可能
- 送信者と受信者の間で鍵を受け渡す
 - 相手ごとに違う鍵が必要
 - » 同じ鍵を使うと暗号化の意味がない
 - 安全な鍵交換の方法が問題
 - » 鍵が盗まれては意味がない
- 鍵の強度が問題
 - 総当たりで試せば必ず破れる

Information Services International - Dentsu, Ltd.

iSiD

共通鍵暗号方式



Information Services International - Dentsu, Ltd.

iSiD

暗号鍵の長さとお組み合わせの数

40ビット	1,099,511,627,776
56ビット	72,057,594,037,930,000
64ビット	18,446,744,073,710,000,000
128ビット	340,282,366,920,900,000,000,000,000,000,000,000,000,000,000

(有効数字13桁)

暗号解読コンテストでは、56ビットが22時間で解読されている

Information Services International - Dentsu, Ltd.

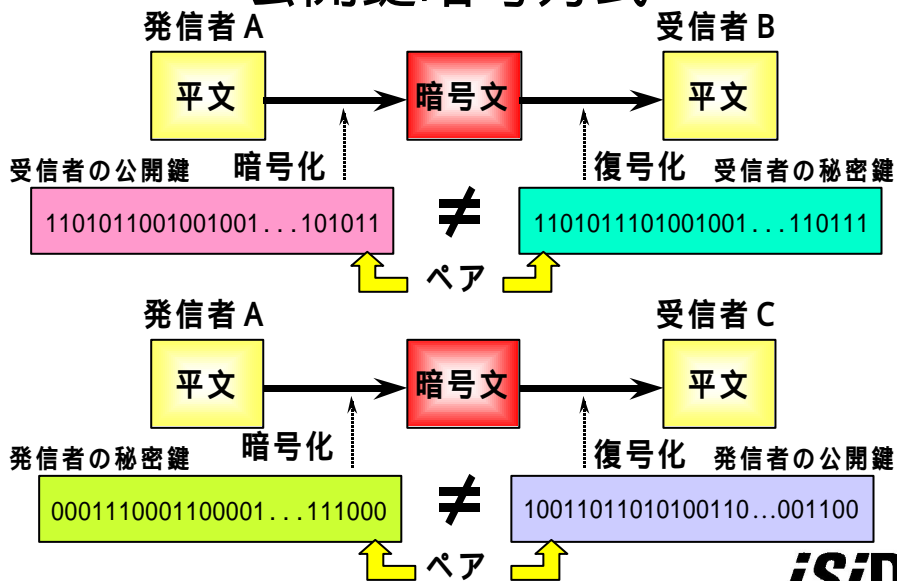
iSiD

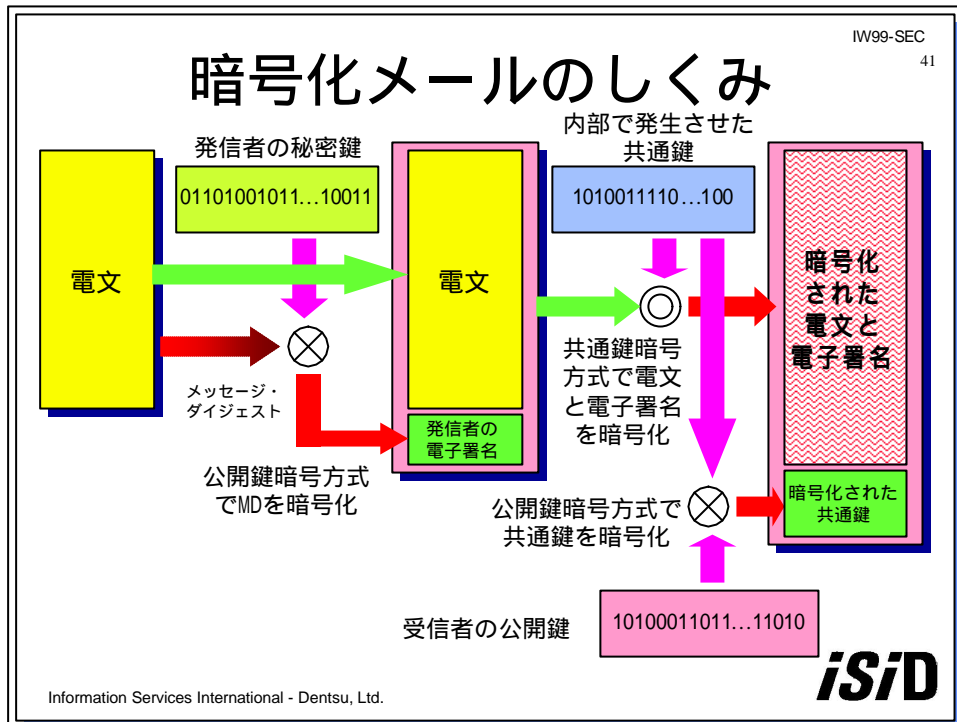
公開鍵暗号方式

- 暗号化鍵と復号化鍵が異なる
 - ふたつの鍵(公開鍵と秘密鍵)がペアになっている
 - 片方を公開(公開鍵)し、片方を秘密(秘密鍵)に
 - 公開鍵で暗号化 秘密鍵でのみ復号可能
 - 秘密鍵で暗号化 公開鍵でのみ復号可能
- 処理速度は遅い
 - メッセージ全体の暗号には不向き
- こちらも強度が問題
 - 米国内では1024ビットが使われている
 - 米国から日本向けに輸出できるのは512ビット
 - 704ビット以上必要といわれている



公開鍵暗号方式





- IW99-SEC
42
- ## 公開鍵を配布する
- 公開鍵をどのように配るかが問題
 - メールでは送れない
 - 対面で手渡しでは配布範囲に限られる
 - 相手の公開鍵を第三者の電子署名で確認
 - 電子署名されていれば本物と証明できる
 - 誰が証明してくれるのか
 - » 特定の企業、地方自治体、ボランティア組織、自社
 - 第三者の証明組織をどのようにして信用するのか
 - » その組織の本物の公開鍵をみんなが持つことが重要
 - CA(Certification Authority)
 - 証明書発行機関 = 認証局
 - CAが発行した証明書を信用する
 - 認証局が別の認証局を証明することも
- Information Services International - Dentsu, Ltd. **iSiD**

暗号技術は軍事兵器

- 暗号は犯罪者やテロリストの情報も守る
 - これでは国家の安全が守れない
 - 軍事的な意味も大きいので軍事兵器扱い
 - 技術の国外持ち出しや利用には大きな制限
- 一般利用者が使えない
 - 米国政府が輸出を制限
 - » 抜け穴も存在する
 - インターネット・ビジネスの普及を妨げる
- 日本から持ち出すのも問題
 - 外国為替及び外国貿易管理法違反の可能性はある
 - 通商産業省貿易局安全保障貿易管理課に聞く
 - » 03-3501-2800

Information Services International - Dentsu, Ltd.



SSLを使えば安心？

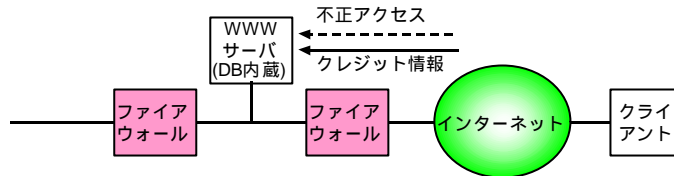
- 「当サイトはSSL対応なので安心です」
 - ショッピング・サイトでよく見かける
 - クレジットカード情報などを暗号化して送る技術
- Secure Sockets Layer
 - Netscape社が開発した暗号通信技術
 - サーバとクライアント間の通信を暗号化する
 - » 暗号化が開始されればブラウザに鍵のマークが現れる
- 通信路での盗聴は難しいが...
 - ショッピング・サイトに届いてからが問題
 - » 侵入や攻撃によるファイルの窃盗
 - » 従業員による顧客DBの持ち出しなど
- 企業としての信用とそれなりの技術力
 - どうしても買いたければそれなりの覚悟で

Information Services International - Dentsu, Ltd.

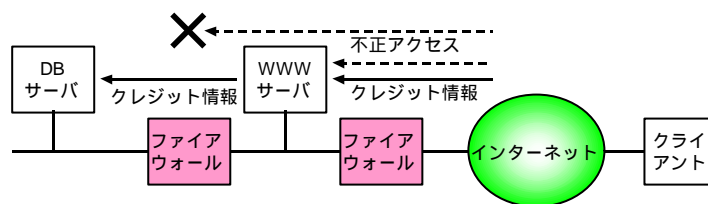


ショッピング・サーバの構成例

A. 危険な構成



B. 一般的な構成



ショッピングの心得

- クレジットカードは嗜好を収集される
 - 買い物内容までカード会社に流れる
 - その情報を売っている会社もある
- クレジットカード伝票に電話番号は必要か？
 - 電話番号を書いた伝票が流出すると危ない
 - 本当に必要なときは「要確認」となるはず
- 同じサイトで買い物を続けると...
 - やはり個人情報が収集される
 - その扱いが問題になる
 - その情報をもとに嗜好を探り出して「おすすめ」へ
 - 便利な反面怖い

サーバは狙われている

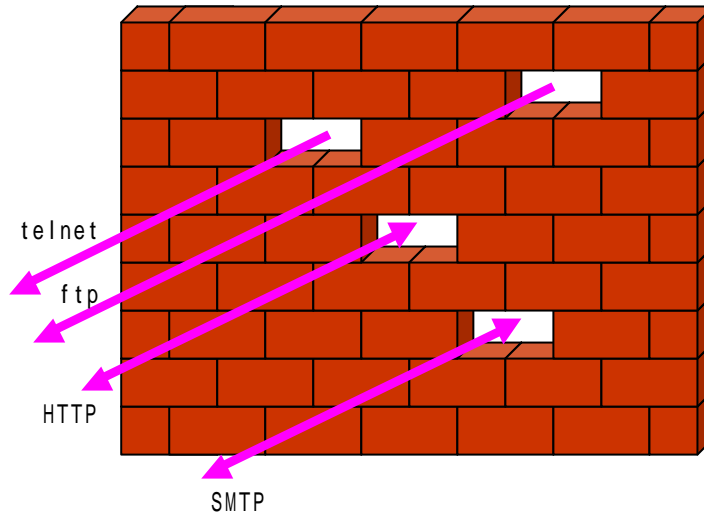
- 外部からアクセスできるので危ない
 - ファイアウォールの内側のマシンは攻撃しにくい
 - 特定のポートしか開いていなくてもそこから攻撃
- 攻撃のパターン
 - セキュリティ・ホールを突く
 - 設定ミスを突く
 - 甘いCGI(Common Gateway Interface)を攻める
- ファイアウォールだけでは防ぎきれない
 - 正しい設定
 - 確実な監視
 - それなりの知識が必要

ファイアウォールとは？

- 防火壁
 - 火災が発生するとそこでくい止める
 - 普段は楽に通れる
 - 何も通さない壁では意味がない
- インターネットから社内LANを守る
 - つながないのが一番安全
 - つながないとインターネットが使えない
 - インターネットを安全に使うための解決策
- どこに設置して何を通す(止める)かが問題
 - 管理者がしっかりと判断して設定する
 - 使い易さと安全性のトレードオフ

必要な通信のみを止める

IW99-SEC
49

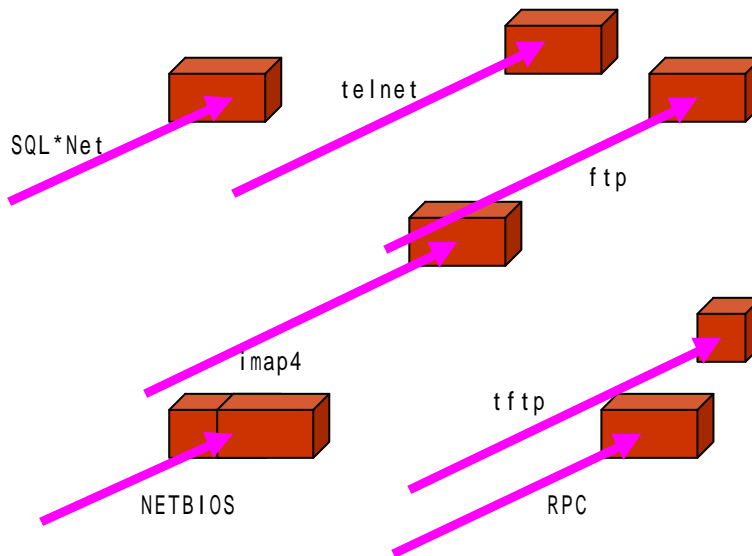


Information Services International - Dentsu, Ltd.

iSiD

危険な通信を止める

IW99-SEC
50



Information Services International - Dentsu, Ltd.

iSiD

サーバと社内LANを守る

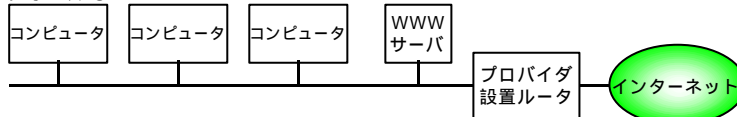
- サーバ類はインターネットとの通信が必須
 - 必要最低限の通信を許す
 - » SMTP、DNS、HTTP、HTTPSなど
 - それ以外は原則通信不可
 - » telnet、ftpなど
- 社内からもインターネットをアクセスしたい
 - かならずProxyを通し、直接通信を認めない
 - かならずログを残して、トラブル発生に備える
- 社外からのメンテナンス用の経路が必要
 - 通信路の暗号化
 - 接続時のワンタイムパスワード
 - IPアドレスによるフィルタリング

Information Services International - Dentsu, Ltd.

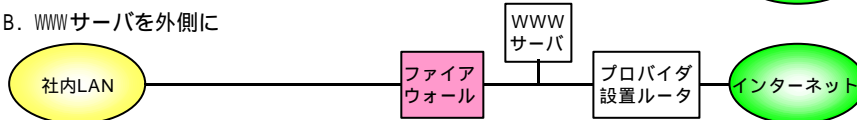


ファイアウォールの構成例

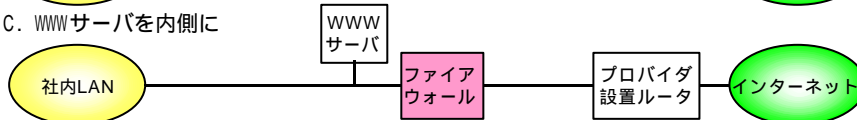
A. ファイアウォールなし



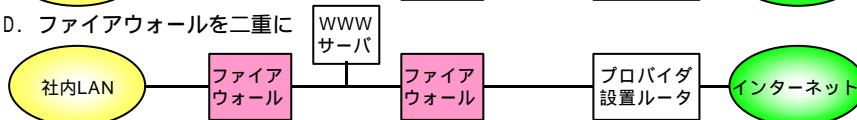
B. WWWサーバを外側に



C. WWWサーバを内側に



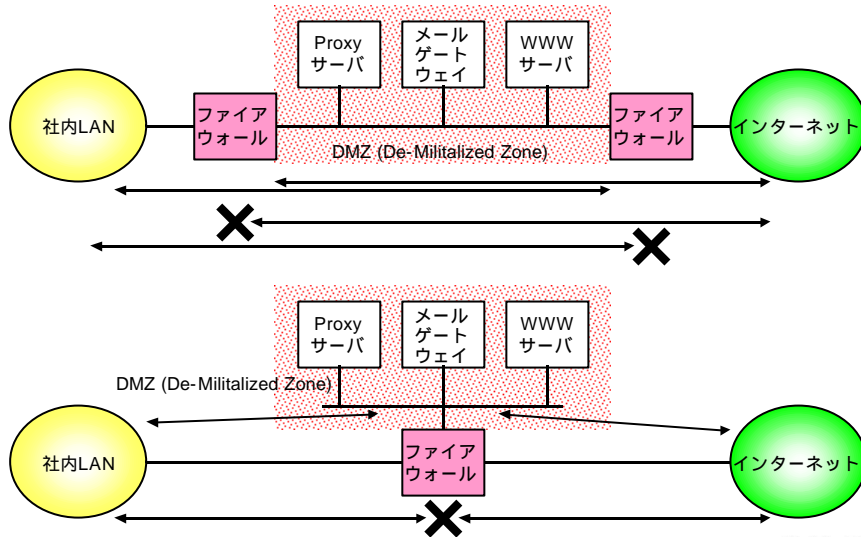
D. ファイアウォールを二重に



Information Services International - Dentsu, Ltd.



De-Militalized Zone



ファイアウォールで安心？

- 設置しただけでは安全は守れない
 - 攻撃手段はどんどん進化する
 - ファイアウォールでの守り方も進化させる必要あり
- セキュリティホールのあるファイアウォールも
 - どの製品を使うかは重要な選択
 - 機能、性能、使い勝手、信頼性などで判断
- それでも安心してはいけない
 - つねにセキュリティ情報に注目しておく
 - ログを調べて大丈夫なことを確認する
 - 自分たちでできなければ専門家に任せる
- **フェイル・セーフ**という考え方を忘れずに

なんでもできるとうれしい

- 利用者はいろいろ楽しみたい
 - RealPlayer
 - IRC
 - telnet
 - NetMeeting
- ファイアウォールに「穴」を開けることに
 - アタックされる危険が増す
 - 外部に対するアタックを起こす危険も
- 楽しいものは高帯域
 - ネットワークを圧迫する
 - 肝心の仕事に影響が出ることも

ポート・スキャンが襲う

- ファイアウォールに開けられた穴を探すツール
 - DNSでサーバを見つける
 - ポートに順番にアクセスして答えるポートを探す
 - そこに攻撃を仕掛ける
- ファイアウォールに穴がないと通信できない
 - 通信するには答えるサーバが必要
 - そのサーバが何に答えるかを探し出す
- フリーウェアが配布されている
 - だれでもが簡単にポート・スキャンできる
 - スキャンされた方にとっては攻撃と見られる
 - 管理者なら自分のサイトをスキャンすることも

危ないサーバたち

- ファイアウォールが機能していない
 - 予算がないのでファイアウォールが買えない
 - 買ったけれど設定方法が解らない
 - 4年前に購入してからさわったことがない
- リモートでログインできる
 - telnetとftpができないと内容を更新できない
 - » ちゃんとパスワードはつけている
 - » 5人で更新するのでみんな同じパスワードを使う
- 監視のしかたが解らない
 - ログファイルを見ても何が書かれているか解らない
 - ログファイルを見たこともない
 - トロイの木馬って、大きな木製の馬ですか？

ちゃんと動くのもセキュリティ

- 侵入や破壊だけがセキュリティではない
 - システムが止まれば仕事にならない
 - 安定して使えることが重要
 - セキュリティ上、重要な課題
- システムは動いていて当たり前
 - だれも止まるとは思っていない
 - だから止まると大変
- 機械は壊れる
 - それに備えることが重要
 - 壊れにくい機械と壊れても止まらないしくみ
 - 短時間で復旧するしくみや手順

インターネットは止まらない？

- 核攻撃にも耐えられる
 - インターネット開発の動機
 - » 集中型は中心がやられると全滅
 - » 分散型で複数の経路を用意して対応
 - どこかがやられてもどこかが生きている
- 商用インターネットは？
 - お金が絡むために簡単ではない
 - 新幹線のトンネルが崩落しても、その切符では飛行機には乗せてくれない
 - どこが壊れるとどうなるのか
- 日本は東京に集中
 - 関東大震災が発生すると...

システムを止めないために

- 壊れる部分を二重化する
 - 完全に二重化すれば費用も二倍
 - 壊れにくい部分と壊れやすい部分を見極める
 - 壊れにくい部分でも壊れることがある
 - 確率と費用対効果
- たとえばどこ？
 - 機器の電源
 - 電源回路
 - 無停電電源装置
 - ネットワークの迂回路
 - サーバのホットスタンバイ
 - サーバの完全二重化

セキュリティ・ホール

- プログラムの「穴」
 - 本来は存在しないはずのバグの一種
 - 特定のデータを送り込むと予定されていない動き
 - これを利用してハッカーが侵入や命令実行
- なぜ「穴」が存在するのか
 - 安全設計が不十分だと開発時に潜り込んでしまう
 - プログラムの規模が大きいと検査が難しい
 - ハッカーはこの「穴」を探している
- 「穴」が見つかる...
 - すぐには公表されない
 - 「穴」のふさぎ方がわかってから公表

CERT/CCとJPCERT/CC

- CERT/Coordination Center
 - コンピュータの犯罪に緊急対応するチーム
 - 24時間、週7日対応
 - <http://www.cert.org/>
- JPCERT/CC
 - 同様な組織が日本にも
 - コンピュータ緊急対応センター
 - » 被害の受け付けと対応
 - » 被害の実態調査、被害状況・侵入手口の分析
 - » 再発防止のための対策の検討と助言
 - <http://www.jpCERT.or.jp/>

ログを残す

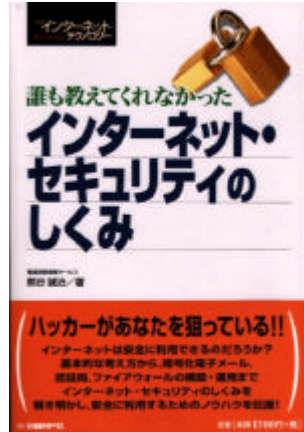
- アクセス状況を記録しておく
 - PPPアクセス
 - メール送受信
 - Webアクセス
 - 機密情報アクセス
 - 管理権限アクセス
- どんな役に立つのか
 - 利用状況の確認
 - 混雑状況の把握
 - 不達メールの確認
 - 不正利用の犯人特定

安全を守るために

- パスワードを守る
- パスワードを共有しない
- 必須な利用に留める
- 危険な使い方を避ける
- 外部からのアクセスは最低限しか許さない
- セキュリティ・ホールをふさぐ
- アクセス・ログを残す
- セキュリティ情報を常時把握しておく
- 危険を発見したらすぐに対応する

参考文献

- 誰も教えてくれなかったインターネット・セキュリティのしくみ
 - 日経BP社刊 熊谷誠治著
 - 初版 1999年5月1日
 - ISBN4-8222-2306-X C3055
 - [1700円 + 税]



Information Services International - Dentsu, Ltd.

(株)電通国際情報サービス

- Information Services International-Dentsu, Ltd.
 - URL=<http://www.isid.co.jp/>
 - 設立 1975年 12月 11日
 - 資本金 6億9570万円
 - 売上高 464億4500万円 (1999年3月期)
 - 従業員数 861名 (1999年4月1日現在)
 - 営業拠点
 - » 東京、大阪、名古屋、広島、ニューヨーク、ブラッセル、ロンドン、香港、シンガポール、マレーシア
- 事業内容
 - 国際ネットワーク(特別第二種通信事業者)
 - システム・インテグレーション、ソフトウェア開発
 - CAD/CAM/CAEソフトウェア販売 など

Information Services International - Dentsu, Ltd.