セキュリティ入門

Internet Week 2000

（株）電通国際情報サービス
e-テクノロジー統括部
熊谷誠治
kuma@isid.co.jp

なぜセキュリティなのか？

- インターネットの普及で意識が高まる
  - 利用者が増えれば犯罪者も増える
  - 犯罪だという認識がない犯罪者も
- 実際に被害が急増中
  - 守らないとやられる
  - 守りが弱いとやられる
  - 守り方がわからない管理者も急増
- しっかり守れといわれても…
  - 守れといわれても予算はつけてもらえない
  - 独学では限界も
  - 素人が学ぶスピードよりも犯罪者の進歩が早い

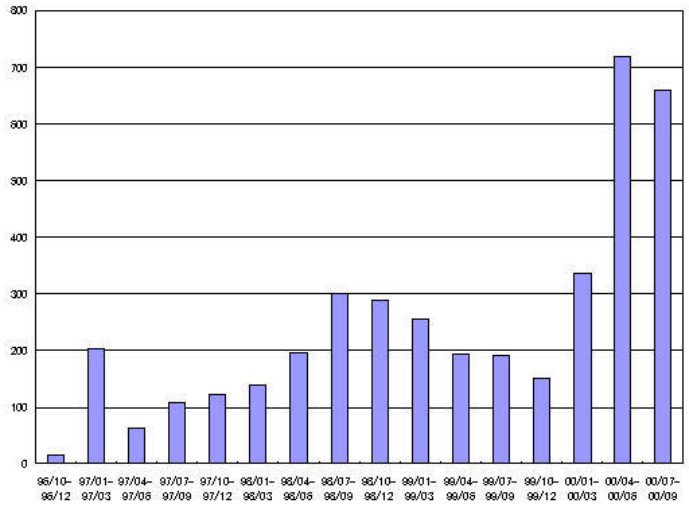
IW2000-B3
3

官公庁Web改ざん事件

- 2000年1月に発生
  - 官公庁のホームページをつぎつぎと改ざん・消去
  - 海外からの攻撃だといわれている
- 守りが不十分なサイトが多数存在
  - ファイアウォールがないもの
  - セキュリティ・ホールをついたもの
  - 外部からアクセス可能なもの
- 被害は
  - 信用失墜
  - 緊急対応費用
- 原因は
  - 危険性認識の甘さ
  - 守るしくみが用意されていなかった

IW2000-B3
4

インシデント報告件数の推移



JPCERT/CCが受け付けた報告件数(3が月ごと)
http://www.jpcert.or.jp/stat/reports.html より

IW2000-B3
5

不正アクセスによる被害

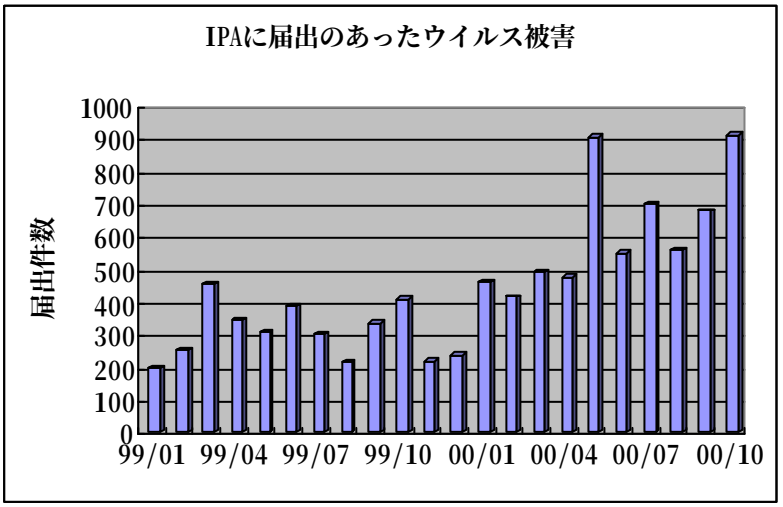
- コンピュータに侵入
  - 侵入そのものが犯罪 → 不正アクセス防止法
  - トロイの木馬をしかける
- ファイルを破壊
  - データが消失
  - コンピュータを再インストール
- ファイルを窃盗
  - 盗んだファイルを公開
  - 盗んだクレジットカード番号を悪用
- SPAMメールの中継に使用
- 踏み台にしてほかに侵入

Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
6

多発するウイルス被害



http://www.ipa.go.jp/security/txt/2000_11outline.html などからデータを入手

Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
7

ウイルスによる被害

- 届出があるのはほんの一部
  - 実体は不明
  - 企業内で広がると一気に
- ウイルスはどこからやってくるのか？
  - 他人からもらったプログラム
  - メール
- ウイルスが大きく進化
  - 勝手にウイルス付きのメールを送る
  - しかも、アドレス帳を参照して
- 被害は甚大
  - ファイルの破壊、知人にも被害が及ぶ

iSiD

IW2000-B3
8

ダウンロードによる被害

- ウイルスに感染
- 勝手に電話をかけられる
  - ダイヤルQ2
  - 国際電話
- ハードディスク内のデータを破壊
- 外部の第三者がコンピュータを操作
  - 破壊、窃盗
  - 踏み台
- コンピュータ内のファイルを窃盗
  - 外部に送出

iSiD

IW2000-B3
9

詐欺による被害

- 購入した「はず」の商品が届かない
  - 売り主に連絡が取れない
  - 売り主の連絡先がわからない
  - 売り主が倒産
  - オークション・サイトが責任をとってくれない
- 「試用」は無料といわれたのに課金された
  - 「試用」でカード番号を教えてしまった
  - キャンセルする方法がわからない
- クレジットカードに身に覚えのない課金
  - カード会社はとりあってくれない

IW2000-B3
10

なりすましによる被害

- 身に覚えのない「クレーム」のメール
  - だれかが名をかたって掲示板に悪口
  - だれかが名をかたってSPAMを送信
- エラーメールが大量に届く
  - SPAMの発信人としてメールアドレスをかたられた
  - ひどいときには何万通も
- 身に覚えのない商品が届く
  - だれかが名をかたって注文
- おかしな電話がかかったりメールが届く
  - 電話番号やメールアドレスを公表された
  - 個人情報が流出している !!

Information Services International - Dentsu, Ltd.

IW2000-B3
11

盗聴による被害

- メールを読まれる
  - なぜそのことを知っているの？
  - どうもおかしい
- パスワードを盗まれる
  - いろいろと悪用が可能
  - メール、コンピュータ、…
- クレジットカード番号を盗まれる
  - 勝手に使われてしまうと
- 盗聴されても分からない
  - 証拠が残らない

IW2000-B3
12

被害にあった人はいるのか？

- 知人が被害にあったとは聞いたことがない !?
  - というひとが多い
  - 運が悪いだけ？
  - 気づかないだけ？
- 本当に事件は起こっているのか？
  - IPAやJPCERTの発表は少ない
  - ウイルスは月に1000件程度？
    - » 数千万台のコンピュータ使われているのに？
  - 不正アクセスが数十件程度？
    - » 数十万のサイトがあるのに？
- 現実には起こっている !!
  - 被害にあうと損害は甚大

IW2000-B3
13

インターネットは危険なのか？

- インターネットだから危険ということはない
  - それなら安全なのか？
  - インターネットは安全ではない
- 実社会と同じ !!
  - 実社会の危険性を理解できていない人も多い
  - 危険を理解していないのが一番危ない
- 実社会は危険なのか？
  - 大変危険
  - それを理解していないともっと危険
- だからインターネットも危ない
  - 実社会の延長だから

iSiD

IW2000-B3
14

実社会の危なさ

- テロ
  - 国際テロ
  - 犯罪組織
- 強盗
  - ハイジャック
  - 集団スリ
  - おやじ狩り
- 窃盗
  - ピッキング
  - 置き引き
  - ケチャップマン

iSiD

IW2000-B3
15

実社会の危なさ(つづき)

- 詐欺
  - 集団催眠、宗教まがい団体
  - ネズミ講、高配当投資、M資金
  - 取り込み詐欺
  - ワイン・マン
- カード詐欺
  - 偽造カード
  - スキミング、番号窃盗
  - 盗難カード利用
- ぼったくり
  - 店
  - タクシー

IW2000-B3
16

実社会の危なさ(つづき)

- 盗撮・盗聴
  - トイレ、更衣室
  - 会議室、役員室
- 事故
  - 火災
  - 衝突
  - 墜落
- 落書き
  - 建物
  - 乗り物
- 通り魔

Information Services International - Dentsu, Ltd.

IW2000-B3
17

インターネット上で身を守る

- 実社会で身を守れない人は…
  - インターネットでも身を守れるわけがない
- 危険を認識できないと被害は拡大
  - 自分だけは大丈夫？
  - 手口がわければ防ぎ方もわかるはず
- 「身を守る」と「運がいい」とは意味が違う
  - でも、結果は同じ
  - 身を守る心構えが重要
- かならず被害に遭うとは限らない
  - 運がよければ被害に遭わない
  - 今日は大丈夫でも明日は不明

iSiD

IW2000-B3
18

インターネットの犯罪者

- プロ
  - 極秘情報を目的とした産業スパイ
  - 軍事情報、先端技術情報を目的とした国際スパイ
  - 情報破壊・システム破壊による営業妨害
- アマ
  - 技術力の誇示
  - 他人につられて
  - 楽しみのひとつ
- 社内
  - 不満分子 → 「いつかはこういうことになると…」
  - 金銭に困って → 「えっ、あの人が」
  - 派遣社員・アルバイト

iSiD

IW2000-B3
19

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

iSiD

IW2000-B3
20

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？

iSiD

IW2000-B3
21

ポート・スキャンが襲う

- サーバで動いているプログラムを探し出す
  - プログラムが稼働していないと攻撃は不可能
  - 稼働しているプログラムの弱点をつく
  - プログラムごとに利用するポートが違う
- ポートを探すからポート・スキャン
  - 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
- 攻撃用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
  - 自分のサイトをスキャンしてチェック

iSiD

IW2000-B3
22

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

iSiD

IW2000-B3
23

ファイアウォールとは？

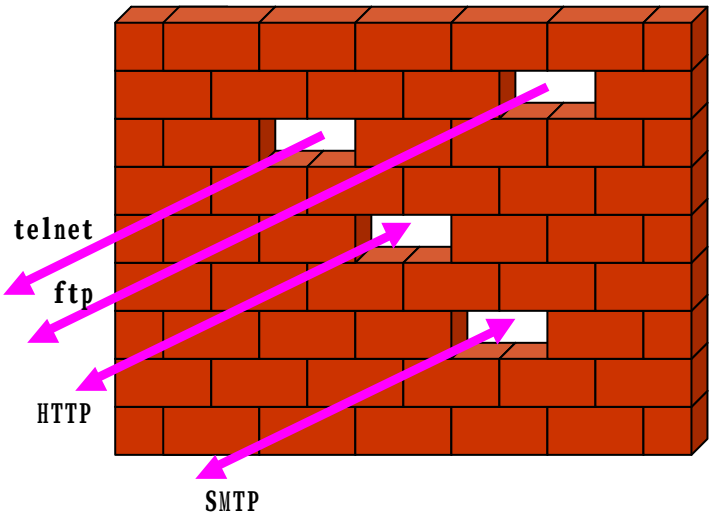
- 防火壁
  - 火災が発生するとそこでくい止める
  - 普段は楽に通れる
  - 何も通さない壁では意味がない
- インターネットから社内LANを守る
  - つながないのが一番安全
  - つながないとインターネットが使えない
  - インターネットを安全に使うための解決策
- どこに設置して何を通す(止める)かが問題
  - 管理者がしっかりと判断して設定する
  - 使い易さと安全性のトレードオフ

Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
24

必要な通信のみを通す

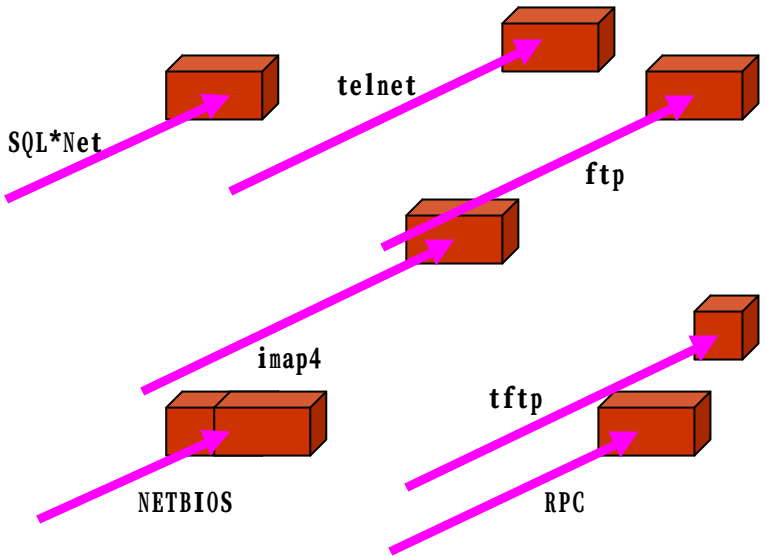


Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
25

危険な通信を止める



Information Services International - Dentsu, Ltd.

iSiD

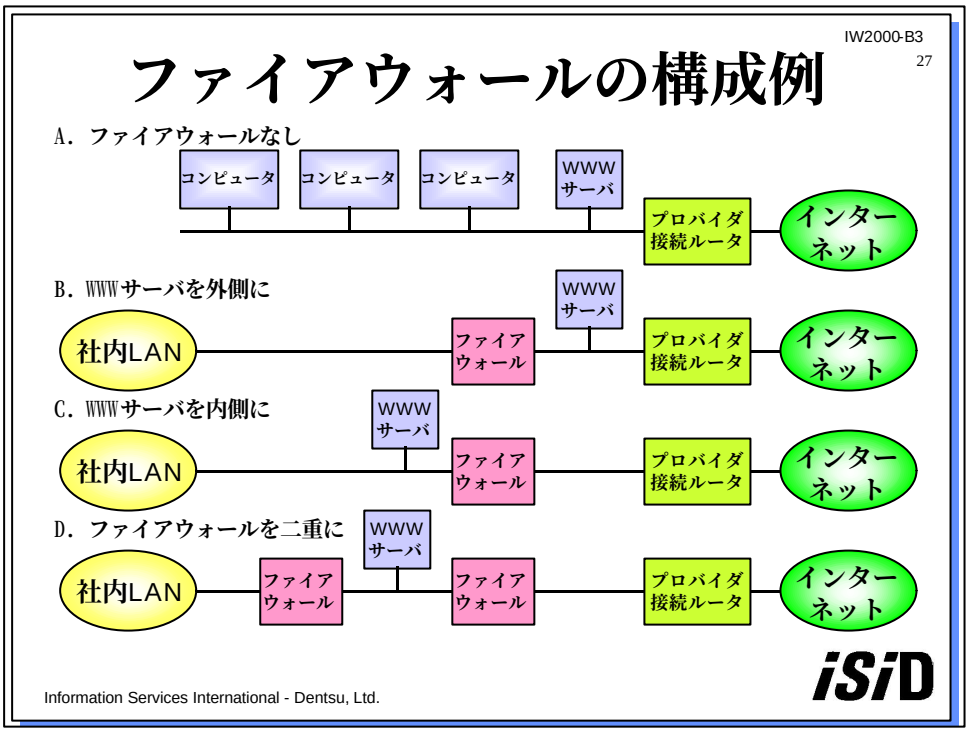
IW2000-B3
26

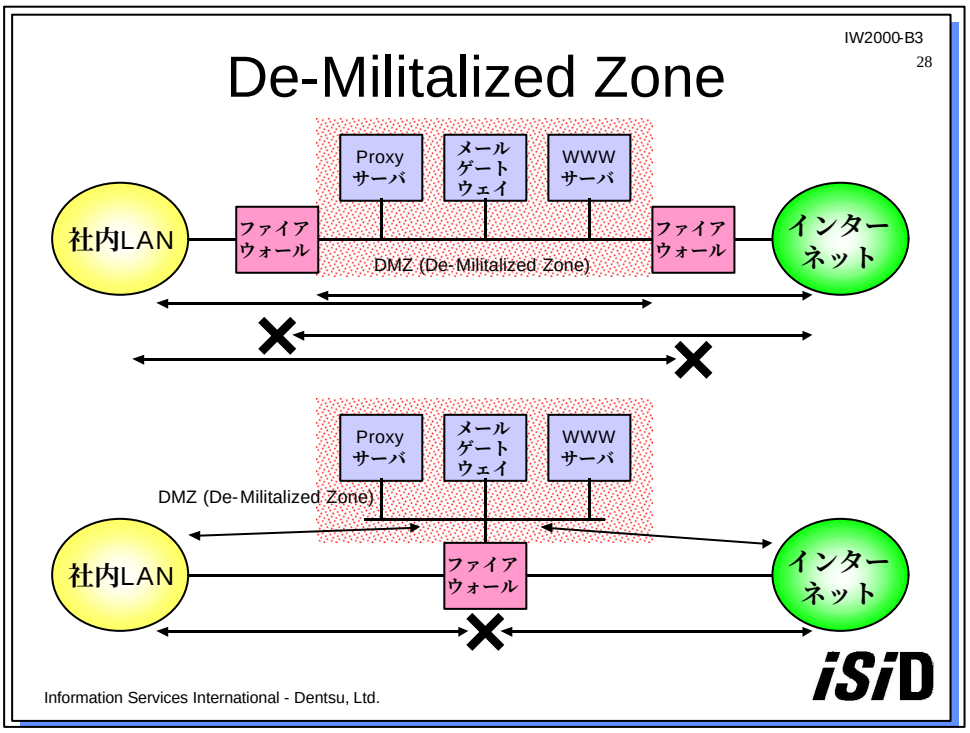
社内からの犯罪を防止する

- 社外に対する不正行為
  - 社内から社外にポートスキャン
  - 社内からの不正アクセス
- 違法行為
  - 社外の不法ダウンロードサイトを利用
  - 著作権を侵害したコンテンツの公開
- 社内システムの不正利用
  - SPAMの送信
  - 個人的ビジネス
- これらもファイアウォールで防げる
  - 社内からのアクセス・発信も制限する

Information Services International - Dentsu, Ltd.

iSiD





IW2000-B3
29

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・セイフ**という考え方を忘れずに

iSiD

IW2000-B3
30

Intrusion Detection System

- 侵入検出システム (IDS)
  - 不正アクセスを検出するために通信を監視
  - 侵入を検出すると関係者に伝える
  - 調査分析に必要な情報を保存・提供
- 通信をリアルタイムで監視
  - 通信速度に適合した処理能力のコンピュータが必要
  - 通信内容を確認して異常を検出
  - 通信を切断
  - ファイアウォールの設定を動的に変更してブロック

iSiD

IW2000-B3
31

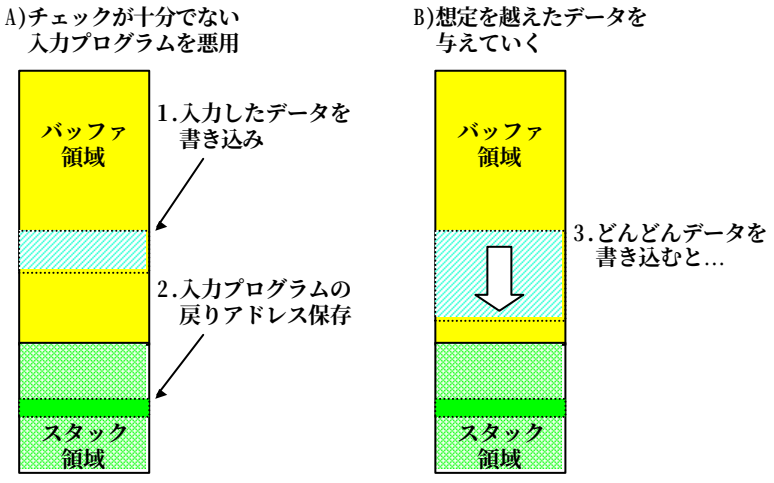
セキュリティ・ホール

- 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
  - 安全教育が十分に行われていない
  - プログラムの規模が大きいと確認・検査が難しい
  - ハッカーはこの「穴」を探している
- 「穴」が見つかると…
  - 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

iSiD

IW2000-B3
32

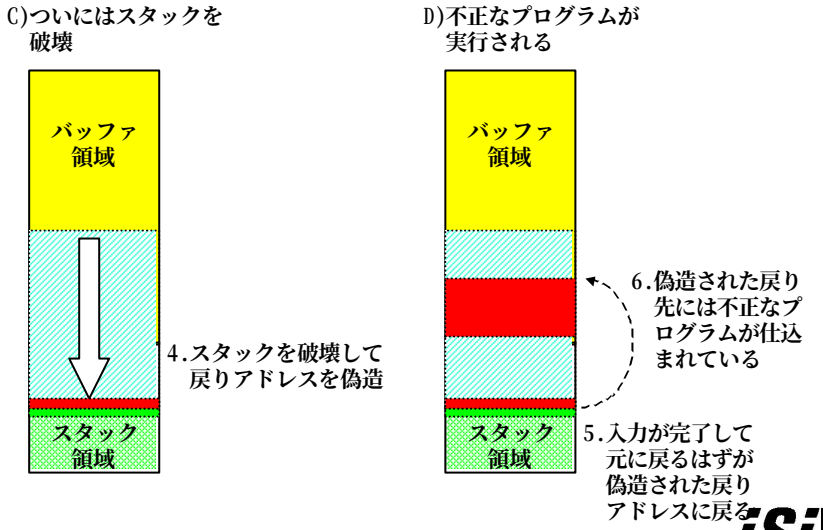
バッファ・オーバー・フロー



iSiD

IW2000-B3
33

バッファ・オーバー・フロー



IW2000-B3
34

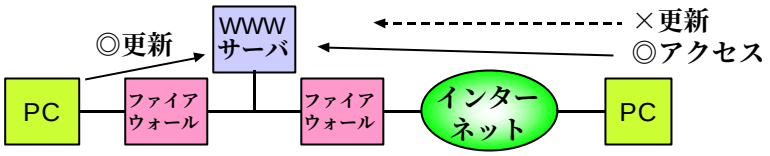
コンテンツを更新する

- 社内に設置したサーバなら社内で更新可能
  - iDCに設置するとそうはいかない
  - ISDNなどでインターネットでない通信路を確保
    - » 発信者番号通知機能でアクセス制限
- インターネットから更新したい
  - メンテナンスを社外に委託
  - iDCにサーバを設置
- telnetやftpを使いたい
  - インターネットからアクセスできると便利
  - 第三者がアクセスする危険が生まれる

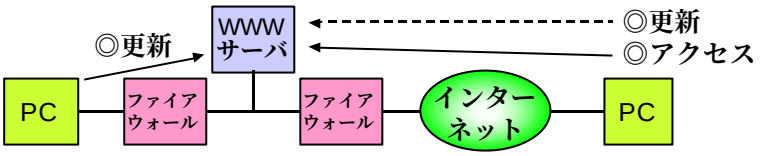
IW2000-B3
35

Web上のコンテンツを更新する

A. 社内に設置、社内で更新



B. 社内に設置、社外からも更新 (非常に危険)



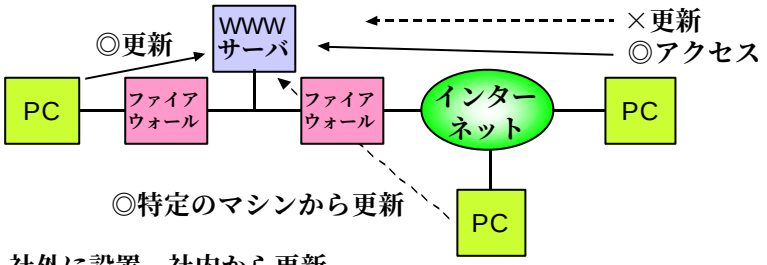
Information Services International - Dentsu, Ltd.

iSiD

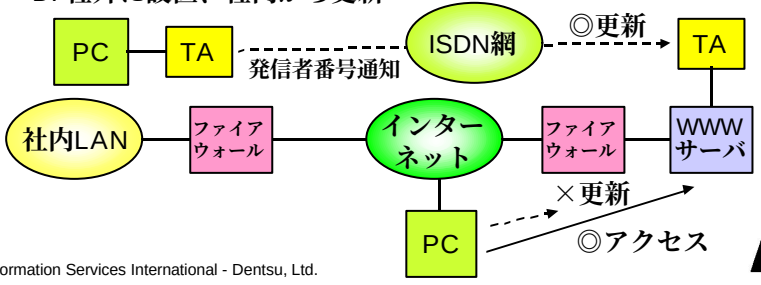
IW2000-B3
36

Web上のコンテンツを更新する

C. 社内に設置、社外から更新



D. 社外に設置、社内から更新



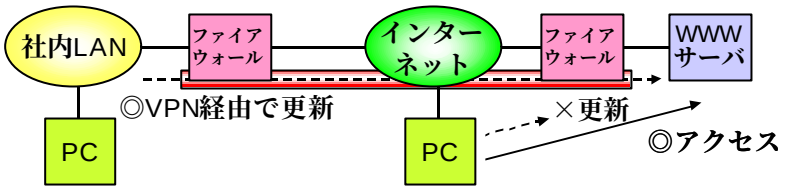
Information Services International - Dentsu, Ltd.

iSiD

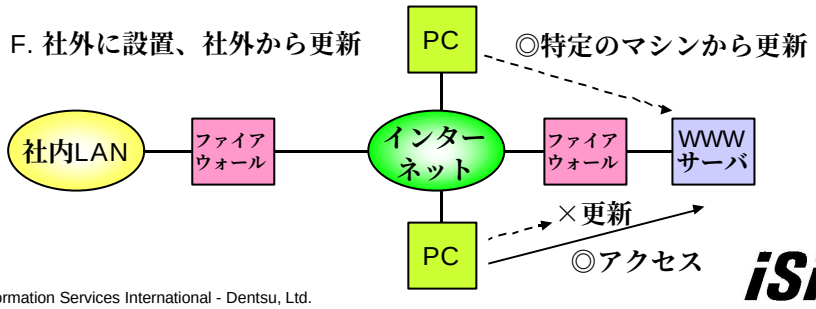
IW2000-B3
37

Web上のコンテンツを更新する

E. 社外に設置、社内から更新



F. 社外に設置、社外から更新



Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
38

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？
  - 現実はこういう人が多い

Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
39

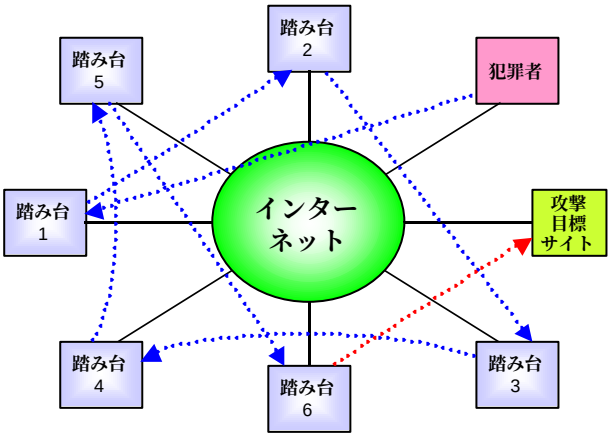
踏み台に注意

- 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

iSiD

IW2000-B3
40

踏み台の実際



iSiD

IW2000-B3
41

Denial of Service

- DoS
  - サービス妨害
  - サービス不能攻撃
  - 過負荷などでサービスを提供できなくする
- DDoS
  - Distributed DoS
  - 複数のコンピュータからDoSをしかける
  - 負荷が大きくなる
  - 高帯域ネットにつながっていても被害を受ける
- 通常、踏み台を利用して攻撃
  - 踏み台にされないことが重要

IW2000-B3
42

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

IW2000-B3
43

インターネットで使う暗号技術

- 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
- 共有鍵暗号方式
  - 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
  - 認証と共有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

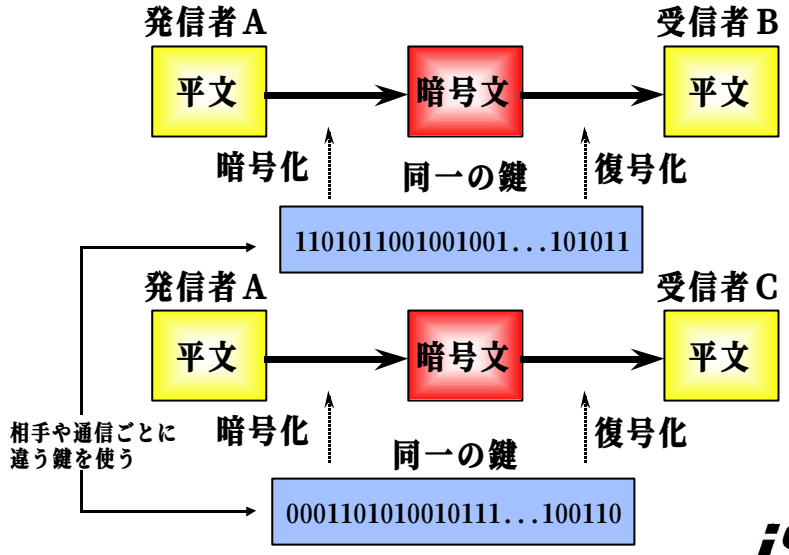
IW2000-B3
44

共有鍵暗号方式

- 送信者と受信者は暗号、復号に同じ鍵を使う
  - 鍵を共有するから「共有鍵暗号」
- 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

IW2000-B3
45

共有鍵暗号方式



Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
46

暗号鍵の長さと組み合わせの数

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
	(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

IW2000-B3
47

公開鍵暗号方式

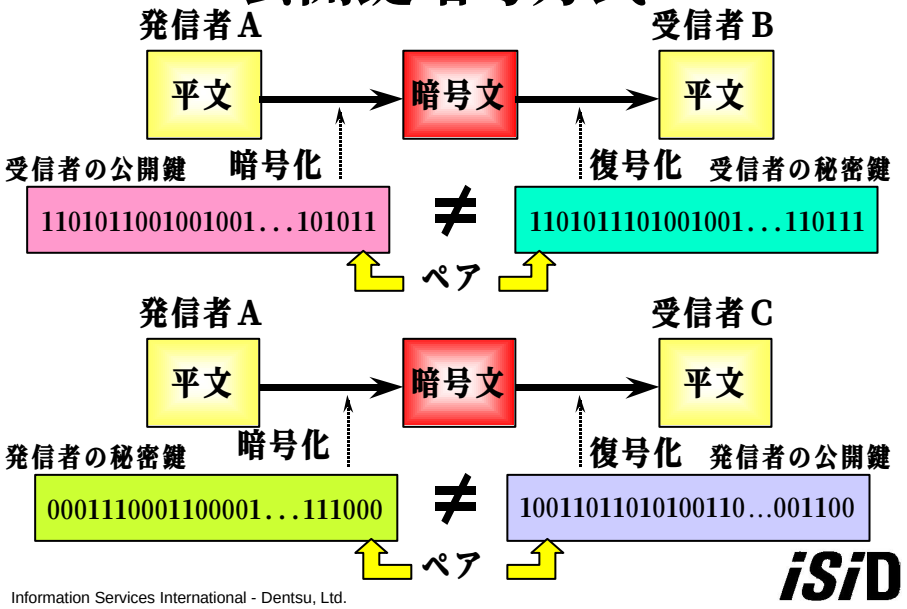
- 暗号化鍵と復号化鍵が異なる
  - ふたつの鍵(公開鍵と秘密鍵)がペアになっている
  - 片方を公開(公開鍵)し、片方を秘密(秘密鍵)に
  - 公開鍵で暗号化 → 秘密鍵でのみ復号可能
  - 秘密鍵で暗号化 → 公開鍵でのみ復号可能
- 処理速度は遅い
  - メッセージ全体の暗号には不向き
- こちらも強度が問題
  - 1024ビット程度の鍵が用いられる
  - 認証局では、2048～4096ビット

Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
48

公開鍵暗号方式



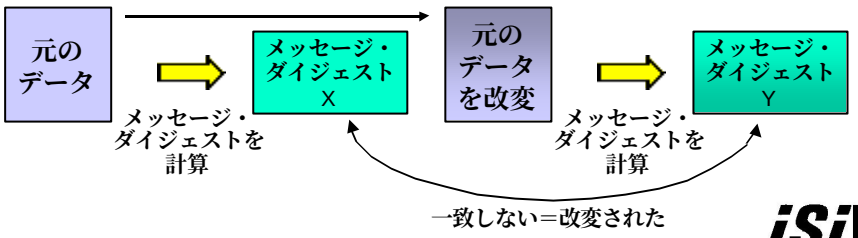
Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
49

メッセージ・ダイジェスト

- データに計算処理を行ってある値を得る
  - 特定の長さの結果を得る
    - » SHA-1　160ビット
    - » MD5　　128ビット
- 同じ計算結果を得られれば…
  - 同一結果になるようにデータを変更するのが難しい
  - データを変更すれば計算結果が変化する



iSiD

IW2000-B3
50

Virtual Private Network

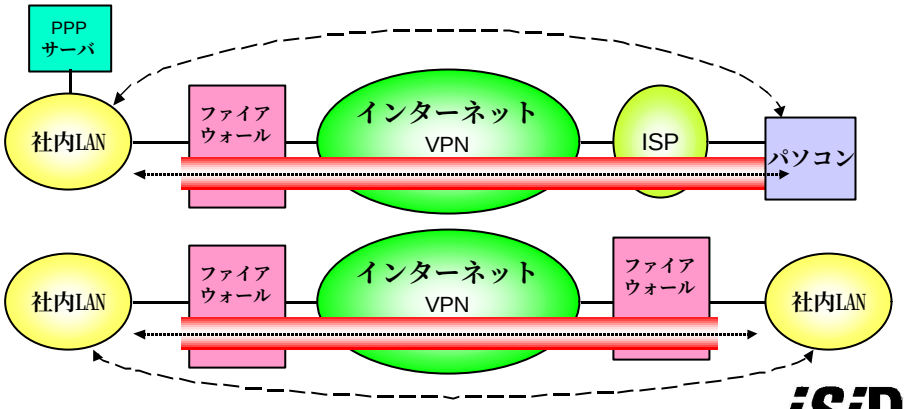
- 実質的なプライベート・ネットワークを作る
  - インターネットを使って
  - 暗号技術で盗聴を防ぐ
  - 「仮想」ではなく「実質的な」
- あたかも専用線のように
  - いくつかのパターンが存在
    - » ネットワーク ⟷ ネットワーク
    - » ネットワーク ⟷ コンピュータ
    - » コンピュータ ⟷ コンピュータ
- メリットは
  - 通信費の削減が可能
  - 社外から安全に通信可能

iSiD

IW2000-B3
51

Virtual Private Network(つづき)

- デメリット
  - 接続相手のリスクがそのままやってくる
  - VPNの中にもファイアウォールを設けよう



IW2000-B3
52

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…
  - 155Mbpsなら1時間で72Gバイト(1.7TB/日)
  - 流れるデータを選択的に取り込む
- 絶対に不可能ということではない
  - 国家レベルで取り組めば
  - 探偵に頼まれた通信会社職員が荷担すれば
- 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

IW2000-B3
53

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

IW2000-B3
54

相手の顔が見えない

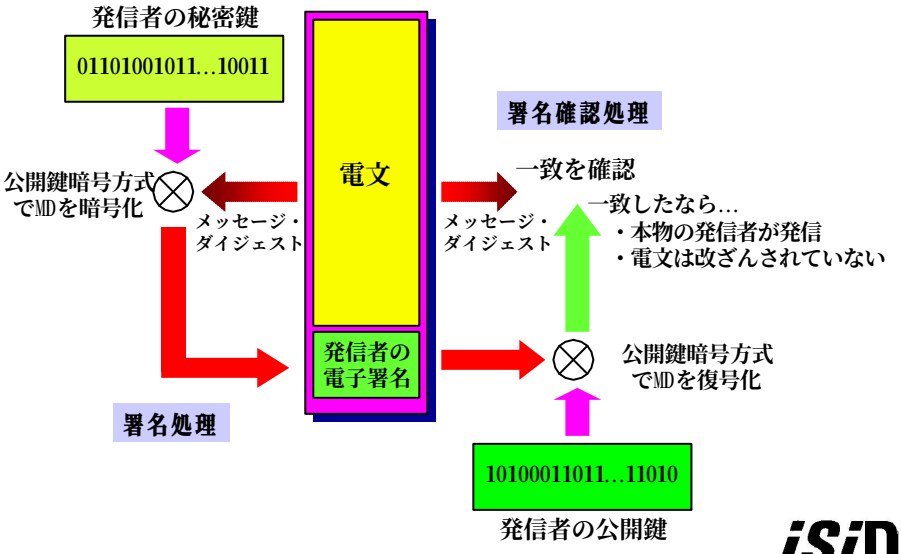
- ネットワークの向こうはモモンガかもしれない
  - 顔も見えないし声も聞こえない
  - 顔が見えても相手を知らなければ偽物かもしれない
- 契約書に印鑑を押してもらうわけにもいかない
  - 物理的に「もの」を交換できない
  - なにを信じればいいのかが難しい
- 電子的な情報で相手を確認する手段が必要
  - そこで登場するのが電子署名
  - 暗号技術を駆使することで解決できる

自分自身を証明する

「わたしは“くまがい”です」と宣言する
- 誰にでも宣言することは可能
- 本物であることを示したことにはならない

- 何を根拠に証明するのか？
  - 免許証 → 公安委員会が証明
  - パスポート → 外務省が証明
  - 指紋 → どこにも登録されていない？
- 本物であることを示すしくみが重要
  - 信頼のおける人に保証してもらう
  - 信頼のおける組織に保証してもらう
  - 印籠を持っていることを確認する

電子署名のしくみ



IW2000-B3
57

Public Key Infrastructure

- PKI
  - 公開鍵暗号基盤 と訳す
  - 電子認証のためのインフラ
- 公開鍵暗号技術を利用して本人証明
  - 利用者の公開鍵を認証局の秘密鍵で暗号化
  - 配布されている認証局の公開鍵で復号できれば本物
  - 印鑑証明書に押された市長印のようなもの
- 認証局とは
  - 英語ではCA (Certificate Authority)
  - 印鑑証明書の発行組織のようなもの
- 証明書とは
  - 利用者の公開鍵に認証局が電子署名したもの

iSiD

IW2000-B3
58

PKIを利用する

- 認証
  - Webサーバが本物である
  - 電子メールの発信人が本物である
  - ネーム・サーバ情報の発信人が本物である
  - ルーティング情報の発信人は本物である
  - ドライバの作成者が本物である
  - VPNの相手が本物である
- インターネット経由のあらゆる認証で使われる
  - 利用はどんどん広がる
  - ますます重要なものになっていく

iSiD

IW2000-B3
59

証明書の信頼性は？

- 確実な認証にはコストがかかる
  - 簡単な認証でいい場合もある
  - 完璧な認証を求める場合もある
- 完璧さとコストを秤にかけて複数のレベルを
  - クラス１ メールアドレスが正しい(誰かに届く)
  - クラス２ 第三者機関を通して個人情報を確認
  - クラス３ 戸籍謄本など公的書類で確認
  - クラス４ 所属組織も含めて調査し確認
- レベルによって発行料金が違う
  - 1,500円/年 ～ 数千円/年
  - ちょっと高すぎないか !!

iSiD

IW2000-B3
60

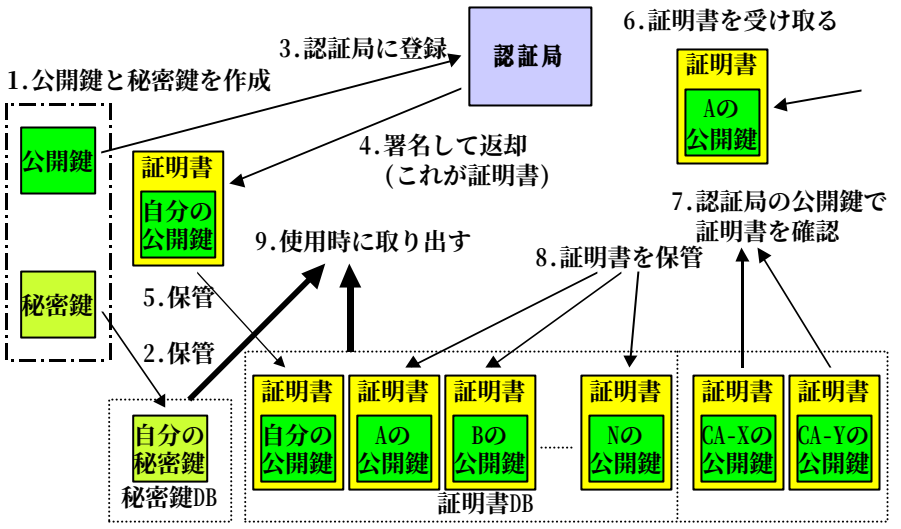
いろいろな認証局

- 証明書発行機関
  - 公開鍵が正しいことを証明書
    - » 印鑑証明書
- 商用サービス
  - 日本ベリサイン などなど
- プライベート認証局
  - 自社で運営する認証局
  - 誰の権限で証明書を発行するか？
  - 他の認証局に認証を受けるのか？
- 認証局の秘密鍵管理が重要
  - 盗まれると大問題に

iSiD

IW2000-B3
61

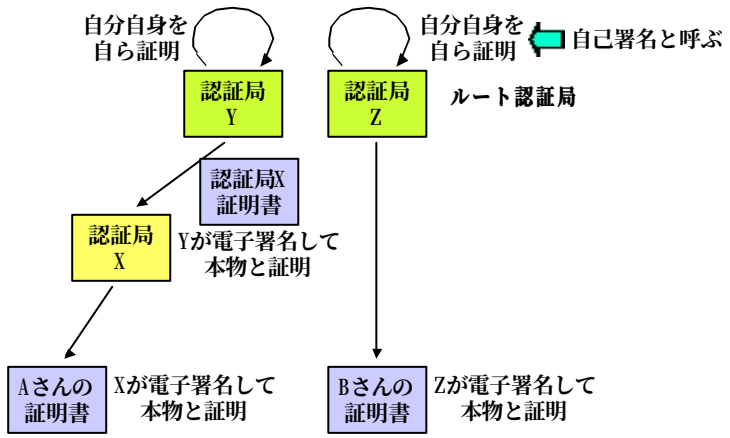
認証局のしくみ



iSiD

IW2000-B3
62

認証局の構造

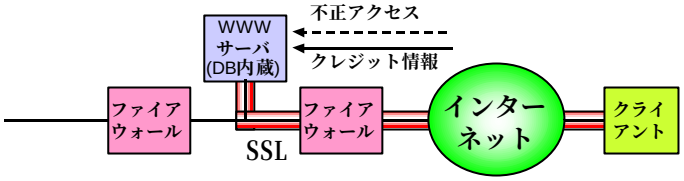


iSiD

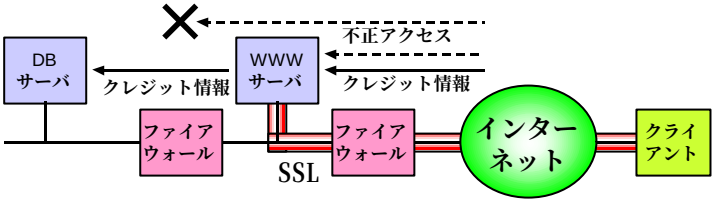
IW2000-B3
63

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



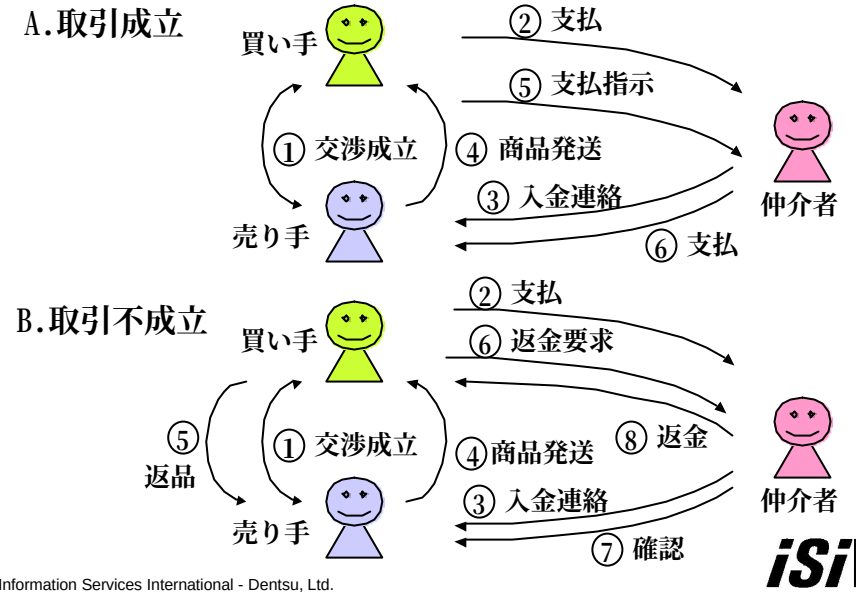
IW2000-B3
64

SSLを使えば安心？

- 「当サイトはSSL対応なので安心です」
  - Secure Sockets Layer
    - » サーバとクライアント間の通信を暗号化する
    - » クレジットカード情報などを暗号化して送る技術
- 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
  - インターネットで買わないといけないのか？
  - 相手が個人ならなおさら
    - » たとえばオークション

IW2000-B3
65

エスクロウのしくみ

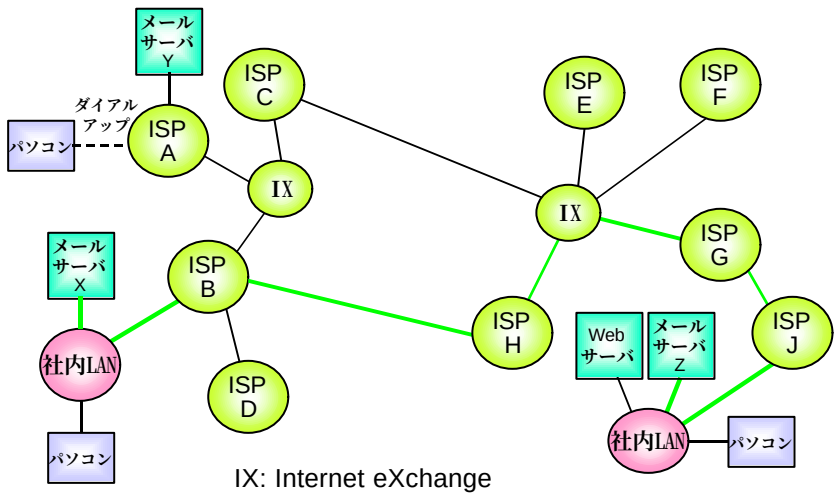


Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
66

メール転送のしくみ

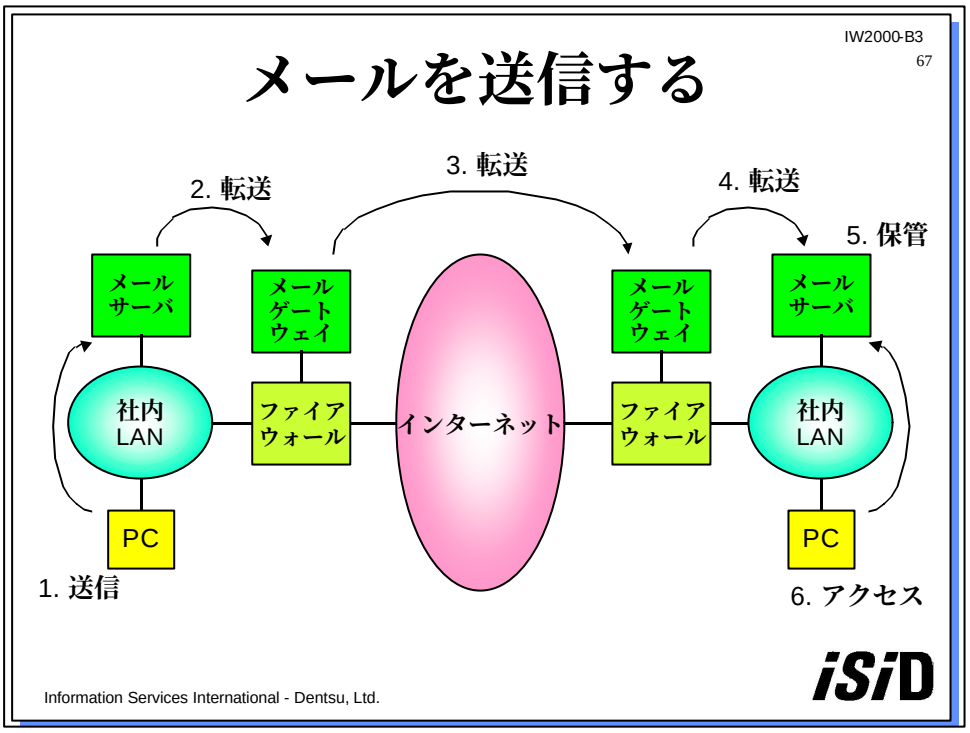


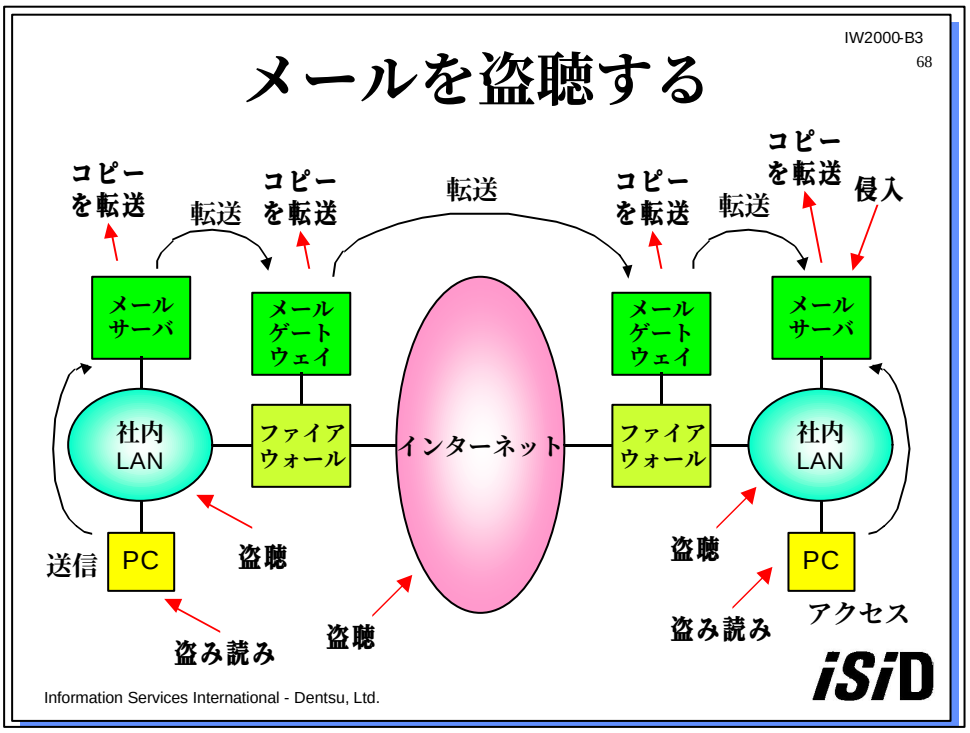
IX: Internet eXchange

ISP: Internet Service Provider

Information Services International - Dentsu, Ltd.

iSiD





IW2000-B3
69

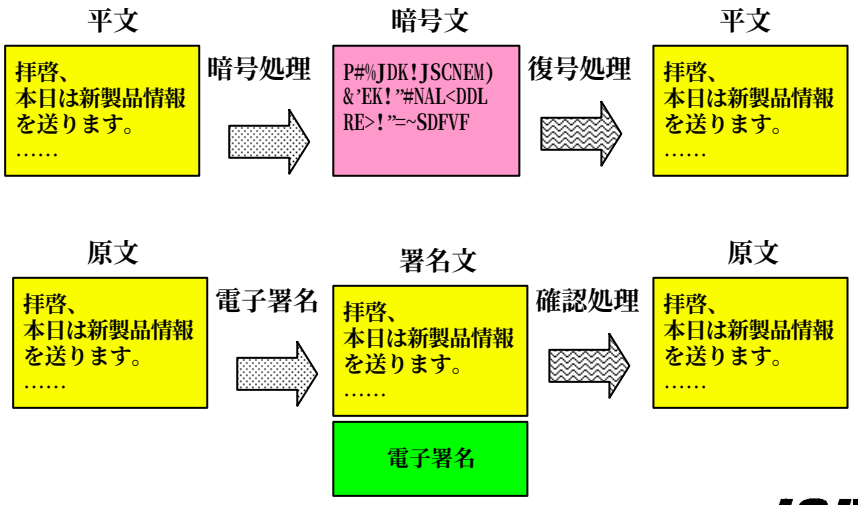
メールシステムは脆弱

- 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
  - 管理者なら読めてしまう
- 暗号電子メールもあるが普及していない
  - PGP(Pretty Good Privacy)
  - S/MIME(Secure/MIME)
    - » MIME → Multipurpose Internet Mail Extensions
- メーラで暗号処理
  - 電文の暗号化
  - 電子署名で発信人確認と改ざん検出

iSiD

IW2000-B3
70

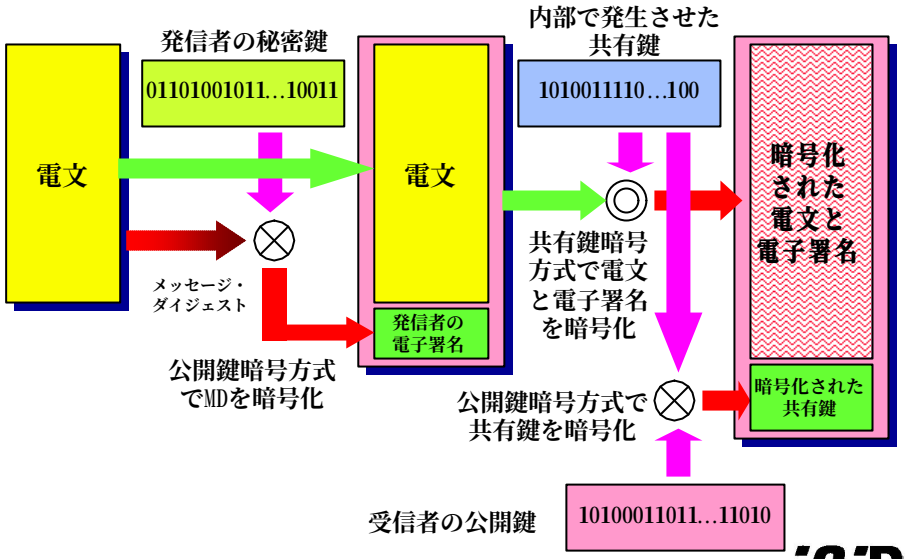
暗号メールの使い方



iSiD

IW2000-B3
71

暗号化メールのしくみ



Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
72

キーリカバリとキーエスクロウ

- キーリカバリ
  - 共有鍵、秘密鍵をなくても復号可能
  - 安全性とプライバシーは？
  - しかし、どうしても復号したい場合もあるのでは？
- キーエスクロウ(鍵寄託)
  - 第三者に復号可能な鍵を預ける
    - » 部分的な預託もありうる
    - » 使うときのルールが重要
  - 会社等では必要？
    - » 社員が退職した時
    - » 鍵を紛失してしまった
    - » 検閲

Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
73

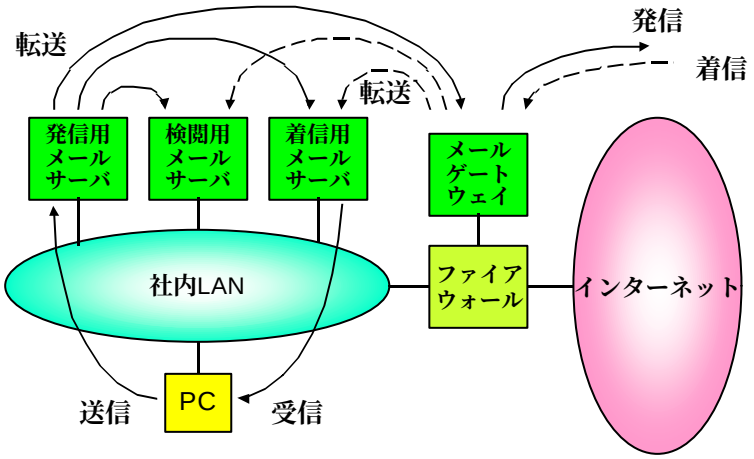
メールを検閲する

- 電子メールは情報流出の危険が大きい
  - 簡単に情報を流してしまうことも
  - 防ぐ方法を考えておくことは危機管理のひとつ
- 企業のメールは企業のもの
  - 業務のための通信手段
  - 会社の電話を個人が使うと業務上横領
- プライバシーの侵害にはあたらないのか？
  - 個人利用の禁止と検閲を通告しておく
  - 通告がないと誤解する人も現れるはず
- 検閲ということばがきついのなら
  - 内容チェックと呼びましょう :-)

iSiD

IW2000-B3
74

検閲のためのシステム



iSiD

IW2000-B3
75

恐ろしいウイルス

- 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
- 最近はメールクライアントを悪用
  - アドレス帳に登録された相手に勝手に送る
  - 知人からウイルス付きのメールが届く
  - 添付されるファイル形式もいろいろ
  - HTMLメール+添付ファイル自動実行も
- 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

iSiD

IW2000-B3
76

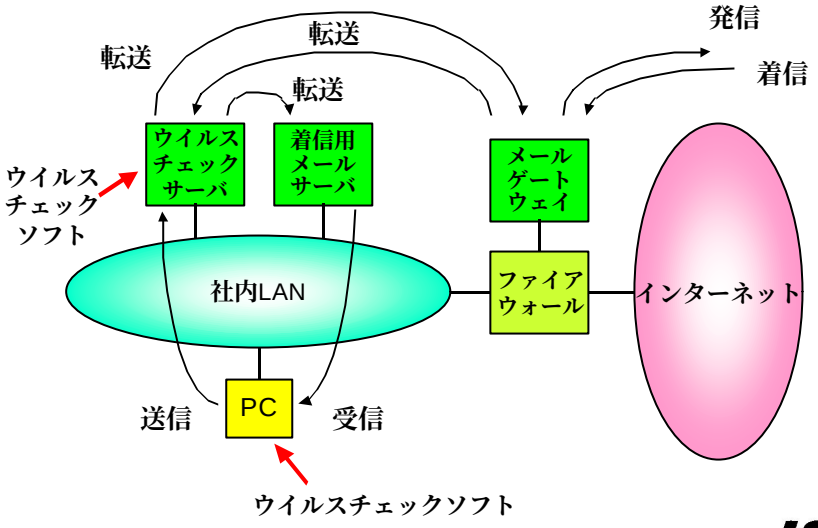
ウイルスを防ぐ

- メールゲートウェイなどでチェック
  - 企業内に入る前に感染していないか調べる
  - 社外から届く前に確認
- パソコンでチェック
  - 届いたメールやファイルが感染していないか
  - 読む前に確認
- ウイルスチェックソフトが存在
  - 新たに生まれるウイルスに関する情報を更新
  - 更新されるのはウイルスが出回ってから
- 完璧ではない
  - 怪しいメールはしばらく寝かしてから読む

iSiD

IW2000-B3
77

メールのウイルスチェック



Information Services International - Dentsu, Ltd.

iSiD

IW2000-B3
78

プライバシが狙われている

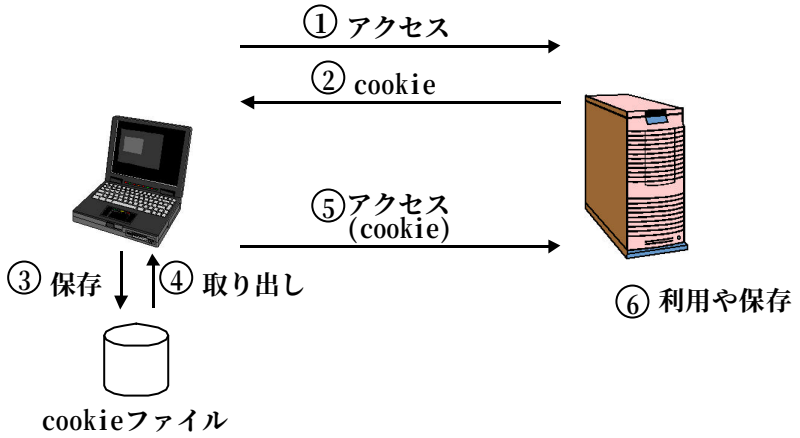
- クライアントを特定するためのしくみ
  - Cookieがクライアントを特定
  - Webをアクセスするとクライアントに送られる
  - 拒否できるがdefaultでは受け付ける
- どうなるの？
  - アクセス状況をサーバ保有者に把握されてしまう
  - アンケートなどに答えて氏名を明かしていると…
    - » アクセス状況が個人にひもづけされる
- 拒否したほうがいいの？
  - プライバシに関する考え方次第
  - 拒否するとアクセスできないサイトもある

Information Services International - Dentsu, Ltd.

iSiD

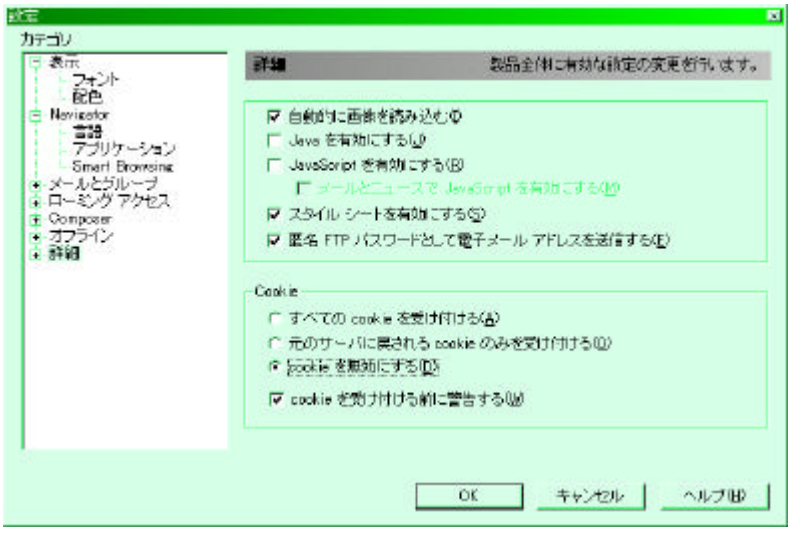
IW2000-B3
79

クッキーのしくみ



IW2000-B3
80

ブラウザ側で扱いを決める



IW2000-B3
81

プライバシと無料サービス

- 日本人はプライバシに無頓着？
  - 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…
  - MLでの発言からメールアドレスを収集も
- 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かも
  - 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となり得る
  - 個人情報がどんどん流出することも

iSiD

IW2000-B3
82

利用者のプライバシを守る

- 個人情報を守るための方針や方法を決める
  - どのような組織体制で守るのか
  - どのように監査していくのか
  - 問題をどのように見直していくのか
- プライバシ・マーク制度
  - (財)日本情報処理開発協会が制定
  - http://www.jipdec.or.jp/security/privacy/
  - 個人情報保護に関するガイドライン

iSiD

IW2000-B3
83

プライバシ・ポリシーとは

- プライバシを守るための方針
  - どのような情報を集めるのか
  - どのような情報は集めないのか
  - どのような目的で情報を集めるのか
  - どのような手段で情報を集めるのか
  - その情報をどのように利用するのか
  - 集めた情報をどのような危機から守るのか
  - 利用し終わった情報はどのように廃棄するのか
  - その企業が存続しなくなったときにどう扱うのか

IW2000-B3
84

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

IW2000-B3
85

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

iSiD

IW2000-B3
86

SPAMを送らないように

- SPAM(スパム)とはハムの缶詰
  - 勝手に送られてくる電子メールの広告を意味
  - Unsolicited Commercial Emailとも呼ぶ
- 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
- 悪質業者に広告を依頼しない
  - 「メールアドレス売ります」
  - 「1000万人に広告を送ってあげます」
- 中継に使われることも
  - http://www.ipa.go.jp/security/ciadr/antirelay.html

iSiD

IW2000-B3
87

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

iSiD

IW2000-B3
88

危機管理も忘れずに

- セキュリティは危機管理の一部
  - 危機を認識する
  - 危機発生時の被害を予測する
  - 危機に陥らない方法を考える
  - 逃れられない危機であれば，被害を最小限に抑える方法を考える
  - 危機に陥ったなら状況を分析する
  - 危機に陥ったなら被害を最小限に抑える措置を講じる
  - 危機から最短で復旧する方法を考える

iSiD

IW2000-B3
89

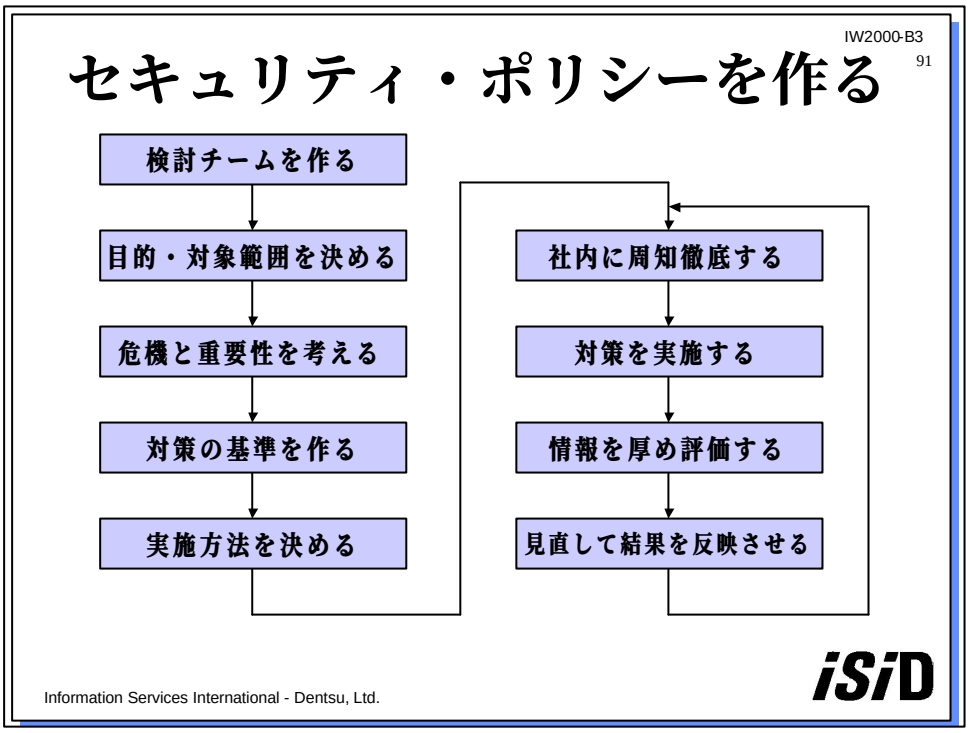
人の弱さに備える

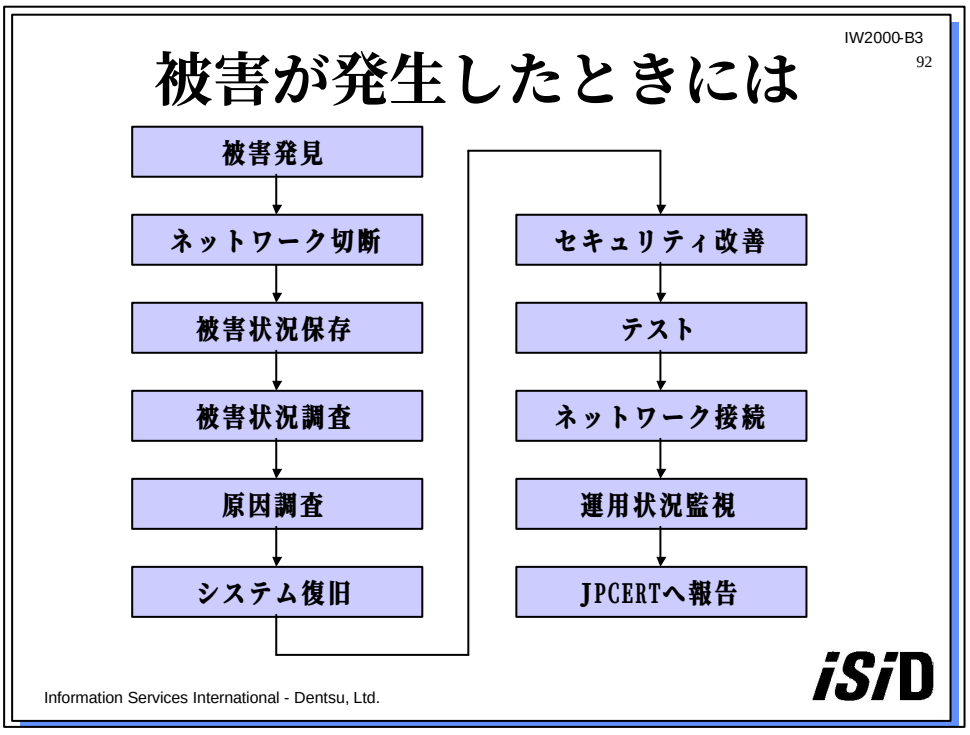
- 人が絡むとファイアウォールや暗号も効果なし
  - 転職時の「おみやげ」
  - 脅しによる強要
  - 金銭による誘惑
- 抑止効果と相互監視
  - 信用していると止められない
    - » 権限のある人が犯罪に走る
  - 罰を明確に示す
  - 罰を強化する
- ソーシャル・エンジニアリング
  - ひとをだまして情報を入手
  - プロにかかるといちころらしい

IW2000-B3
90

セキュリティ・ポリシー

- セキュリティに関する考え方を統一する
  - インターネットだけを考えていても意味がない
  - 情報を守るなら、誰が触れられるかも含めて
  - 持ち出しを制限するならFDや紙の含めて
- 「セキュリティ・ポリシー」もひとつではない
  - 人によって意味が違う
    - » セキュリティの基本方針
    - » ファイアウォールの設定方法
    - » インターネット・セキュリティの運用方針
  - まずは意味の統一が重要





IW2000-B3
93

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/

IW2000-B3
94

犯罪から身を守るために

- 危険な場所を知る
  - 国、地域
  - 都市、地区
  - 店、部屋、トイレ
- 危険な手口を知る
  - ケッチャップ・マン、ワイン・マン
  - 路地に引きずり込む
  - ホテル客室の金庫にドリルで穴
- ことば巧みに
  - 「いい品物ですがお金が必要なので安く売ります」
  - 「もうかりまっせ」、「当社は絶対安全です」

Information Services International - Dentsu, Ltd.

IW2000-B3
95

法律は守ってくれない !?

- 「情報」を盗んでも罪を問えない
  - プリントアウトした紙、コピーに使ったFD
  - ネット経由なら、不正アクセス防止法が適用
- にせクレジットカードの保有もOK
  - 偽造団が日本に押し寄せる
- 個人情報を漏らしても罪に問われるのは一部
  - 国家公務員やNTTの社員などのみ
  - 金融機関などは法制化に反対しているらしい
- 相談する相手もいない
  - 警察も消費者センターもあてにならない？
- 自分の身は自分で守るしかない

iSiD

IW2000-B3
96

社会情勢の変化に対応する

- 海外へ出かける人が増加
  - 危険な地域が多い
  - 海外の危なさを認識していない人が多い
- 海外から流入する犯罪組織
  - 「国内は安全」という認識を逆手に
  - 海外の手口を国内に
  - 密入国が増加中
- 国内の犯罪組織も過激化
  - 海外からの流入組に負けられない
  - 資金源の確保のために
- インターネットも同じ

iSiD

参考URL

- **情報処理振興事業協会セキュリティセンター**
  - http://www.ipa.go.jp/security/index.html
- JPCERT/CC
  - http://www.jpcert.or.jp/
- **首相官邸高度情報社会推進本部**
  - http://www.kantei.go.jp/jp/it/security/index.html
- **通産省情報セキュリティ政策関連のページ**
  - http://www.miti.go.jp/kohosys/topics/10000098/
- **セキュリティ@日経インターネットテクノロジー**
  - http://nit.nikkeibp.co.jp/security/index.html