セキュリティリスクとは何か？

2003/03/22 NT-Committee2
緊急コンピュータセキュリティ研究会
園田道夫
vp5m-snd@asahi-net.or.jp
あやしいサイト展開中
http://www.asahi-net.or.jp/~vp5m-snd/sec/

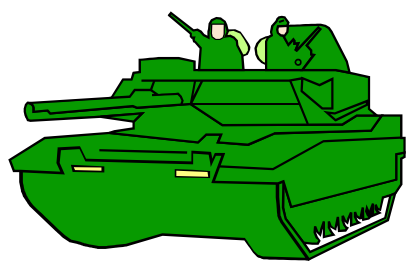
前口上

- 何か行動するときは、すべてリスクを伴う
  - サーバー立てると、サーバーのリスク
  - Webアプリ作ると、アプリのリスク
  - 人に頼むと、人のリスク
- そもそもコンピュータとかOSとかサーバーソフトウエアなんて、自動車だったらリコールものの欠陥だらけ。それを使おうってんだから・・・

そもそも、コンピュータとは

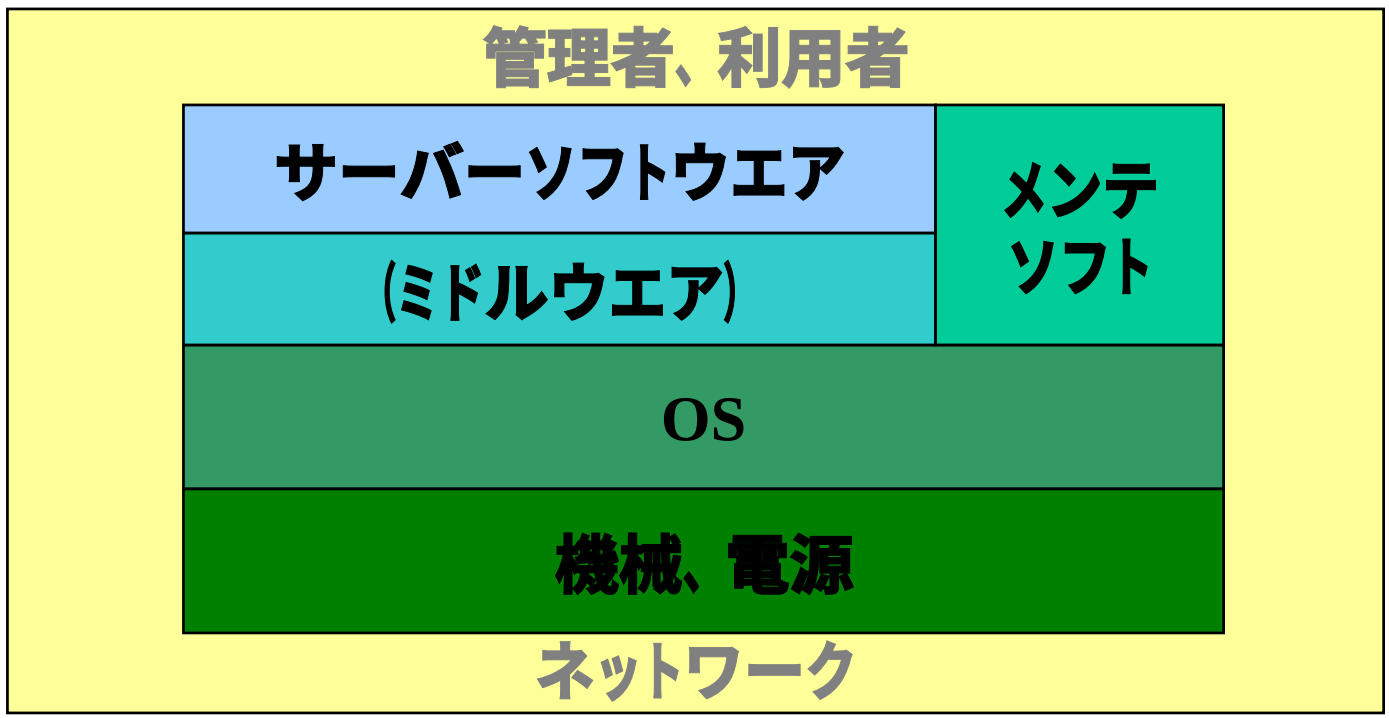
- 機械よわい
- OS弱い
- サーバー弱い
- アプリ弱い (作る人知らなすぎ)
- ミドルウエア弱い
- 管理する人知らなすぎ
- 使う人暴力的
- 愉快犯多し
- ・・・という**だめだめ**なシロモノです
  - ったくこれで家電なんて笑っちゃうぜ

どこ撃っても
やれちゃうので、
かえってどこから
やったら良いか
選択に困るぞ (苦笑)



サーバー動かすのに必要な要素

- どの要素にもリスクがある



・・・どのリスクの管理がおろそかになっても、セキュリティのダムはそこから**決壊（がが～ん）**する

なんと言っても一番厄介なのは人間

- 人はミスする
- 人はヨコシマになる
- 人は借金で鬼になる
- 人は携帯電話、携帯端末を使って情報を漏らせる持ち出せる
- 人はUSBメモリで情報を持ち出せる
- 人は利用するシステムの穴を本能的に探す（ほんとか？）
- 人は悪用してくださいといわんばかりのシステムは必ず悪用する（ほんとか？）

リスクの別の顔

- 業務が続けられるのか？という視点
  - 機械が壊れたり停電したらみなこける
  - OSがコケたらみなこける
  - サーバーソフトウエア、ミドルウエアこけてもなんとかなる
  - メンテソフトこけても当面支障無し
- 扱うネタが暴露・破壊・漏洩するとビジネスにどれだけインパクトがあるか？という視点
  - 個人情報が漏れたら会社の終わりor賠償金お一人1万5千円（最低額）
  - 事後対応間違えたら会社の終わり
  - サーバーの設定情報が漏れても、扱う情報が無事ならやりなおしがききます（ほんとか？）

ネタに着目しライフサイクルを追いかける

- お客様情報第一ならば、お客様情報が生まれてから消去されるまで（ライフサイクル）を追いかけて、できればすべてのプロセスを保護しよう

ライフサイクル追いかけ例：Webアプリへのユーザー登録情報

	媒体・サーバー	生誕	コピー	お亡くなり
1.	Web	ユーザー入力	無し	DB登録後削除
2.	DB	ユーザー入力	バックアップディスク	ユーザー削除
3.	紙①社内資料	DBから出力	月1ミーティングで配布	ミーティング後裁断
4.	紙②広報資料	3. から広報サマライズ	マスコミに配布	←
5.	紙③広報マーケ資料	3. から広報サマライズ	広報部署内利用	キャビネット保管

リスクは変化に敏感

- 今まで安全だったとしても、リスクは変化する
  - 管理する人が変わると、目配り可能エリアが極小化
  - 某OSのように3年に1回メジャーバージョンが変わると、管理・設定方法で考慮すべきポイントが変化する
  - ある日突然グループウエアにワークフローが追加されました
  - ある日突然ポート80なメッセンジャーが出てきました
  - 常時接続もそろそろ底値で、社員が家で仕事する比率が高くなってきました
- それまでの管理方法で良いのか？と、常に周囲にイヤな目を向けておく

新種のリスク

- 新たなリスクもどんどん出てくる
  - 昨日まで誰も気にとめていなかった？SQL狙いなスラマ-とか
  - 昨日まで誰も気が付いていなかった**だめだめ**なインターネットプリンタサービスとか (笑)
  - 昨日まで影も形もなかった新たなチャットソフトがいきなり大流行とか
  - 昨日まで影も形もなかった新たなファイル交換ソフトがいきなりトラフィック食いまくってるとか
- とにかく**情報収集**しないと・・・。もし情報収集が手に余るなら管理をあきらめるしかない？

変化や新種のリスクを逃さない

- いつもの状態を数量化する手段を持ち、総量チェック
  - ポイントごとのトラフィックデータ、アクセスログ、エラーログ、システムログ、検出されるウイルス数、クレーム件数、かかってくる電話の数、メールの数、入退出数などを「解析」せず、総量で変化を見る（トラフィック解析で侵入検知という方法論もある）
- いつもの状態を手順書、フローなどに記述しておく
  - 手順どおりに事が運んでいるか？をたまに監査してみる
  - 手順どおりにやってどうなのか？を自分でチェックしてみる
- ルール違反や無視、サボタージュなどを分析する
- 一般的なセキュリティ情報の収集を継続的に行う
  - アンテナ使ったらちょっとは楽かも。オカネで買う手もある
  - メーリングリストの総量でチェックという手もある

リスクの3つの鉄則

Check!

- リスクは一面的ではない。多面的に分析しリスクをチェックしよう！
  - サーバーに着目
  - 人に着目
  - 物理的環境、機械に着目
  - 情報（ネタ）に着目

- リスクは変化する。環境や状況の変化に敏感になろう！
  - ある日突然昨日までの方法論は通用しなくなる
- そのリスクで終わりではない。新しいリスクをトレースする**情報源**を確保しよう！
  - 昨日まで誰も気にとめていなかったリスクが出現する

まとめ：リスク分析の意味

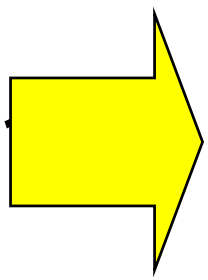
- リスク分析結果はそのままリスク管理策の裏返し

危ない状態（リスク）	望ましい状態
管理手順書が無いので、現場の人の目配りに依拠している	ぱりっとした手順書を作る
データがどこにもバックアップされていない	バックアップすりゃいいじゃん
今度のOSは新しいUpdate機能が入ってばりばり使えます（でも外に繋ぐ）	やたら外に繋いでUpdateせず、社内のUpdate用サーバーを使ってもらう

❖ リスク分析をしっかり行えば、リスク管理策（リスクヘッジ）も見えてくる（ハズ）

リスク分析（管理）参考資料

- BS7799（ISO/IEC 17799）
  - 10のカテゴリー、127のリスク管理項目によって、リスク管理方法の要件が列挙されているテンプレート
    - 1．セキュリティポリシー
    - 2．セキュリティ組織
    - 3．資産の識別と管理
    - 4．人に対するセキュリティ
    - 5．環境や物理面のセキュリテ
    - 6．通信と運用の管理
    - 7．システムの開発と保守
    - 8．アクセス管理
    - 9．業務の継続のための管理
    - 10．準拠



必要なところだけ抜き出して、必要で可能な要件だけ満たすようにする

それが満たされているかどうか分析する

番外：そのまんまリスク管理・対策

- サーバー（OS、サービス）、アプリ、ネットワークのリスクやインシデント対応、監視などは・・・詳しくはこの後のセッションにて
- 人のリスク管理にはこんな対策があります
  - 誰でも見れば何とかなる手順書
  - 手順書を作る手間が割けないならせめてダブルキャスト
  - ダブルキャストすら無理っぽいならせめて記録（を取ることによる抑止効果、ミス防止）
  - 記録もダメなら監視カメラ（笑）
  - カメラ高いならNetBus（笑）
  - NetBusあざといなら契約書（雇用契約、賠償してねのお約束（裁判沙汰用））
  - 契約書敷居が高いならモラル＆技術教育でもしますか
  - モラル＆技術教育するネタもお金も無いならあきらめましょう

番外：逃げのリスク対策

- **だめだめじゃない人に（有償で）頼む**（ex.某港139さん @15000円/1h）
- **頼めなくても例えばSecureIISを導入する**
- **ホスティング、アウトソース、コンテンツ預かりに頼む**
- **こうしてみると、オカネでいろいろ対策できますね**
  （逃げのためにもオカネが必要、ということか）
  - **それでも人件費に比べたら安いもの？**
  - **一番高くつくのは、**
    役割を明示的に振らずに管理させること？

エンドタイトル(出演順)

- リコール;http://www.motnet.go.jp/carinf/ris/Default.htm (自動車)
- だめだめ;人気沸騰中！だめだめ日記
- だだ漏れOS;W*ndows,L*nux,S*laris,A*Xなど
- よわよわサーバー;I*S,*pache,send*ail,B*ND
- 呆れたミドルウエア; (以下略)
- 京都府宇治市関連 (一人1万5千円)
  http://www.mainichi.co.jp/digital/netfile/archive/200102/26-2.html
- TBC関連;http://homepage3.nifty.com/tbc-higai/ (ご参考)
- 事後対応; http://www.shoeisha.com/book/Detail.asp?bid=1406
- リスクの別の顔; http://www.asahi-net.or.jp/~vp5m-snd/sec/human/secpolicy-6.html

エンドタイトル(出演順)

- **情報のライフサイクルネタ;近日公開予定**
- **リスクの変化ネタ;近日公開予定**
- **トラフィック解析**; http://www.seshop.com/detail.asp?pid=2600
- NetBus; http://netbus.org/download.html
- **某港**139**さん@**15000**円**/1h; http://www.port139.co.jp/services.htm
- Secure IIS; http://www.isquare.co.jp/product/security/secureiis.html
- **オカネ使う対策;近日公開予定@日経**ITPro
- **効率良く情報収集するには;近日公開予定**
- **リスク分析テンプレート; 近日公開予定**
- **プラスセックよろしこ;**http://www.itfrontier.co.jp/sec/
- **ノーウォー**; http://www.votenowar.org/