情報インフラセキュリティの現在と明日

園田道夫
vp5m-snd@asahi-net.or.jp
http://www.asahi-net.or.jp/~vp5m-snd/sec/
http://d.hatena.ne.jp/sonodam/

自己紹介

- 1962年生まれ厄年
- 2004年1月1日よりフリー
- 情報処理機構（IPA）研究員
- 日本ネットワークセキュリティ協会（JNSA）研究員
- SISS（日本セキュリティ情報流通協議会）監事
- JNSAハニーポットWG、セキュリティスタジアムWGリーダー
- **技術者教育をテーマに、教育講座企画中**
- セキュリティ夜話（http://www.asahi-net.or.jp/~vp5m-snd/sec/）
- 極楽せきゅあ日記（http://d.hatena.ne.jp/sonodam/）
- vp5m-snd at asahi-net.or.jp

基本的な紐解き

- インフラとは何か？
  - Infrastructure＝インフラ、基盤[設備・構造]、（電気・ガス・水道・鉄道・道路などの）生活の基礎となる設備、経済基盤、構造基盤、社会資本
  - ・・・こうして見てみると、無いとか止まっているとかいう状況では困るものが多い
- インフラとは**基盤**である。しかも止まったら{けっこう、かなり}困る
- ・・・では情報インフラとは？

情報インフラはインフラなのか？

- 情報インフラ（ITインフラ）とは？
  - 情報の流通基盤、インターネット、ネットワーク、その上のアプリケーション（イントラネット、掲示板、メール、Webサービス、Wiki、日記、WebDAV、XOOPS、グループウエア、メッセンジャー、IRC、電話、テレビ電話、P2Pなど）
  - 多くのアプリ、ネットワークはTCP/IPというベースの上に構築されている
    - ご存知のとおり、TCP/IPというのはもともと軍用のプロトコルであり、戦場であってもとにかく通信が届くように作られている
  - しかし、これがとてもインフラであると威張れないほどに、**弱い！**

情報インフラはどこが弱いのか？

情報インフラ	水　　道
よく止まる	めったに止まらない
よく渋滞する	渋滞することはほとんどない
修理の技術が確立されていない、浸透していない	専門家の手を安価で借りることができるほど、技術は確立されている
各部品の欠陥が多い	部品に欠陥はほとんどない

インフラとしての成熟度や安定度が違うことがよくわかる

情報インフラの問題点

- 構成する部品に欠陥がどうしようもなく多い
  - 相次ぐパッチ、欠陥修正
  - メンテナンスプログラムにも不備
  - 道路で言えば信号機が始終故障しているようなもの？
- DNS、ルーターをやられたらおしまい
  - ルートDNSサーバーが攻撃されると影響が大きい（2002年10月の攻撃例有り）
  - 基幹に近いところのルーターが攻撃されると、これも影響が大きい
- メンテナンス部隊があまりにもパワー不足
  - 技術的知識の不足
  - 人手（技術者）不足

しかし、「問題点」はどこ吹く風？

- 情報インフラの利用はますます進む
  - 電話（音声、テレビ）やラジオ・テレビ放送、映画やヴィジュアル番組の配信
  - テレビ会議、スクール
  - ゲームネットワーク
  - ファックス、コピー
- 新しい形のコラボレーション、コミュニケーションも出てきている
  - ドキュメントの共有開発（Wiki、WebDAVなど）
  - P2P（これは何もファイル交換だけでなく、グループウエアなどへの応用例もある）

さらに進む情報インフラの利用

- 投票
- 役所の手続き、書類発行
- 銀行
- 鉄道や飛行機など交通機関の利用
- そして、ウ[illegible]ネットも？

情報インフラへの脅威の正体

- 普通「インフラ」と言うのならば、無いと困ることが多い
  - 水道、電気、ガス、交通機関などは、無いと日常生活に支障が出る
- しかし、情報インフラはほんとうに**無くて困るものなのか？**
- 言い換えると、ほんとうに代替できないものなのだろうか？

代替手段について考えてみよう

Q:組織内ネットワークがおしゃかになったとしたら？

A:組織外のネットワークを通信手段に使えば良い

Q:組織外も含めて近傍の（例えば日本の）ネットワークがおしゃかになったとしたら

A:電話（固定、携帯）をかければいいし、FAXもあります

Q:電話ネットワークも含めておしゃかになったとしたら？

A:そんな日はどうせ仕事にならないんだから、あきらめる。というより、そういうときは仕事云々って言ってる場合ではない？

最大の問題点は

- 脆弱な基盤の問題を解決せず、利用ばかりしようとしていることにあるのでは？
- **というよりも、依存しすぎているのではないか？**
- よく見かける、IP網に電話もテレビ会議も基幹システムもメールもWeb閲覧もグループウエアも乗せてしまう例は、IPコケたらみなコケる
  - トラブルにかかるコスト（これだけ相乗りしていると、トラブルも増える）を組み込むと、**ちっともコストダウンになっていない**のでは？

「依存しすぎ」の例

- 某グループウエア
  - メールと掲示板、会議室など情報流通がすべてこのグループウエア上で行われる
  - このサーバーがコケたら上記すべてのサービスがコケる。当然サービス負荷が集中するため、よくコケる。まったくよくコケる

バランスの取れたシステムの例

- Webである商材を見積もり、発注するシステム（3年前に構築されたもの）
  - 会員制のサイトで、そもそも会員は受注側でもある（マーケットプレイス）
  - 見積もり、注文はWebインタフェースで行う
  - 見積書、注文書はWeb上で確認するが、必ずFAXでも送付される
  - FAXが来なければ電話などで確認するし、FAXだけが来てもおかしい＝相互に見積もりと発注行為を確認できる仕組み
- 情報インフラに過度に依存していない、バランスの取れたシステム

依存しすぎ状態への移行

- せっかく既存のインフラで代替が利くのに、IPネットワークにすべて集中させようとしている
  - 電話網の移行
  - 公共サービスの移行
- わざわざ依存しすぎ状況を招き、自らリスクを集中させていっているようだ
- しかもそれは、単に「依存しすぎ」になるというだけでなく、**新たな脅威**を生み出している

IPネットワークの新たな脅威

- 電話が以前より簡単に盗聴できるようになる
- ドキュメント共有型の開発は、ひとつの認証を破ると妨害工作がしやすくなる
- 衛星回線によるテレビ中継会議はまず妨害できないが、IPならばこれも妨害しやすくなる
- 公共サービスや銀行などがIPに乗ると、嫌がらせしやすくなり、経済的被害（利益）などを引き起こしやすくなる
  - 公共サービスの場合は、以前からソーシャルエンジニアリングしやすかったみたいですが・・・
- 何より、**侵入経路が増える！**

そして、脆弱さが未解決なまま、新たな脅威は組織内にまで入り込みはじめる

組織内、組織外の安全度の差（昔編）

- その昔、組織内は清潔で安全だった
  - 出入り口はひとつかふたつだった
  - ノートPCを持ち込むヤツも居なかった（高いから）
  - 家庭環境がそもそも安全だったので、家庭で「風邪を引く」可能性はほとんどなかった
- 組織外ではさすがにあやしい通信が飛び交うことも少なくなかった
  - だが、組織内までなかなか入ってこなかった
- 情報インフラの弱さは変わっていないが、昔は（少なくとも組織内は）「保護」されていた

組織内、組織外の安全度の差（今編）

- 今、組織内は外にとても近くなっている
  - 出入り口が増えた。とにかく増えた
  - いまどきノートPCを持ち出し持ち込みしない組織など無い
  - 家庭でも常時接続に晒されて、風邪を引きっぱなし
  - 組織外のあやしい通信が｛家庭、ホットスポットなど｝経由で入り込む可能性が高くなっている
- 組織内を隔離し、守るというモデルは、そろそろ破綻しかかっているのでは？
  - 隔離によって「保護」されなくなってきているので、情報インフラの弱さの影響をそのまま受けてしまう

縮まりつつある組織内外の差

- 内部は無菌室だから安全、とはもはや言えない
  - あまりに増えてしまった出入り口
  - あまりにも非専門家さんたちへの依存度を増してしまった
- 家庭内も視野に入れて守らないとならない
  - 下手すると家庭内は外と変わらない
  - 家庭で常時接続を利用する人々が、すべて技術の専門家であるわけがない→ファイアウォールだ、ルーターだ、と言われても限界がある
  - ・・・しかし、家で仕事をするのを止めろ、とは言えない

増えすぎた出入り口on情報インフラ

- グループウエア
- メッセンジャー
- IRC
- 電話(テレビ電話も)
- P2P
- トンネル
- VPN
- 新しいWeb利用
- そしてもちろん、メール
- Web閲覧
- ftp
- DNS参照

その出入り口を守っているのは

- ファイアウォール！
  - インターネット接続の最大のボトルネックとなりつつある
  - それこそここがコケたら全てコケるが、その割りにあまり性能などが重視されていないし、冗長化も考慮されていない
  - もともと処理効率が良いものではないのに、機能はどんどん重厚長大化しつつある
- ほぼ同じようなリスク集中例として、ルーターもある

今更ですが、ファイアウォールだけでは守れない

- トンネル、VPNなどはいったん認証されてしまうと、使い方いろいろ使い放題
  - IPsecはまだしも、SSL-VPNとかトンネルは認証が弱い実装もある
  - SSL-VPNなどは、Webアプリの弱点を抱えていることもあるし、なにしろSSL（多くはOpenSSLとか）である
  - トンネルもSSLを使っていたりすることもあり、同じ弱点を抱える可能性がある
- 暗号化通信は、通信の内容を隠すというメリット以外に、より強固な認証ができる、というメリットもあるが、それを生かさないと逆に脆弱になることもある

既存のソリューションが役立たずになる日

- ネットワーク型IDSは（導入がけっこう進んでおりますが）そのままでは廃れていってしまう
  - 外からのアクセスをゲイトウエイのようにして受けて、そこで侵入を検知するというのが発展形？
    - しかし、いかにもボトルネックになりそう
- コンテンツフィルターなど、データの中身を見張るソリューションはトンネルで迂回されてしまいそう
  - トンネル経由で禁止されているサービスなども利用されてしまう（モラルの問題も大きいが）
- 集中ゲイトウエイタイプのソリューションにとっては厳しい時代になる

現実的になりつつある、個別防衛時代

- 複合的、複雑なインフラの発達と、リスクの増大と多様化に対抗するには、リスクを個々で管理する
  - まずは個々の端末を個々で守る
  - パーソナルファイアウォールの導入と、管理スイッチ（遠隔からその端末の通信を遮断できる仕掛け）の導入
  - 家庭、出張先のホテルLAN、出向先、ホットスポットでの汚染に対し、個々で抵抗力をつける
  - 個々の端末に導入するファイアウォールは、外からの通信を（一部UDP以外）受け取らない、とすれば、自発的通信による脅威のみに絞り込むことができる

では、既存には無いソリューション例

- トラフィック異常検知と解析
  - トラフィック（通信量）の異常を、定量化して捉える方法
  - シグネチャー（既存の通信パターン）によらない検知ができる
  - トンネルも捕捉できる
  - 詳しくは某日経BP社主催NET&COMにて

ディレクトリサービス等による プロファイル、ポリシー管理

- セキュリティポリシー（ここでは、ルール体系ではなく、個々の端末の設定、アクセスポリシーなどを意味する）を配信し、プロファイル違反やポリシー違反を管理する仕組みが必要
  - トンネルや違反通信を、そもそもさせない
  - 重要なパッチなどの適用管理も同時に行う
  - さらに高機能化させて、マシンリソース（CD,DVD,メモリスティック、USBなど）の管理や、ファイルアクセス管理を行うソリューションもある（ディレクトリサービスが必須ではないが）

組織はそれでいいかもしれない が、社会的な問題は？

- 頼むから公共サービスとかをWebでやろうなんて止めてくれ
- 銀行も同上
- 決済も取引も、バランスの取れたリスクヘッジ（既存インフラの取り込み）が無く、IPネットワークに依存したものはお願いだから止めてくれ
- 通信文を暗号化すればいい、とか言わないで欲しい。最も大きな問題は**認証問題**

（対社会問題）自衛策はあるのか？

- 使わないことが最大の防御
  - しかし、基本的にそのサービスが安全かどうか見極めることはできない（いろいろな意味で）
  - であれば、既存の形態のサービスを極力利用する
    - Webで振込みとかすると、もしそのサービスが弱かったら口座自体が危険だが、ATMならせいぜい一定時間止まったり間違い振込みとかあるだけ（それも大きいが）。どちらの方が安全か、と問われれば、保守的に既存の実績がある方をお勧めする

再び、弱さの強調

- 現在の情報インフラは、そもそも技術的な基盤からして弱い
  - ベンダーの多くが提供提案するソリューションは、現在のインフラの根本的な弱さを補完すべく開発されたものではなく、後追いの対策がほとんど
  - どこかで抜本的な改善が必要でしょう
    - みんなDNSSECするとか（DNSネック対応）
    - ルーティングプロトコルを増強するとか（DOS対応）
    - IPv6を本気で導入するとか

まとめ

大きなインフラ	プロトコルや仕組みそのものの改良が必要 調整機関、第三者機関が必要？
組織のインフラ	既存のソリューション以外にセキュリティインシデントを捉えることが可能な仕掛けが必要 IPの新たな脅威を捕捉できることが必要
個々のPC	パーソナルファイアウォールとウイルス対策を基軸とした、個別防衛が必要

※まだまだやるべきことは山積みのようです（ため息）

付録:バランス感覚

- ひとつのインフラがおしゃかになったときのことを考える(業務継続計画)
  - 既存のインフラ(電話、FAXなど)を含む総合的なインフラとしてとらえ、何らかの情報伝達手段を残す
    - (A)メールサーバー経由のメール
    - (A) Webサーバーからメールサーバー経由のWebメール
    - (A) Webサーバーによる告知
    - (B)外部ISPのメール
    - (B)外部サーバーの掲示板
    - (C)携帯電話のメール
    - (C)携帯電話
    - (D)電話
    - (D)FAX

(A)～(D)はインフラの種類

参考

- インターネット情報インフラ防護のための技術調査（最終更新日：2003年 5月21日）
  - http://www.ipa.go.jp/security/fy14/reports/internet/infrastructure.html
- RFC3013：推奨されるISPセキュリティサービスと手順
  - http://www.ipa.go.jp/security/rfc/RFC3013JA.html
- 「インシデントレスポンス」
  - Kevin Mandia / Chris Prosise著
  - エクストランス株式会社訳、坂井順行 / 新井悠監修
  - ISBN 4798102954
- 「不正アクセスの予防とリスク管理」
  - Cathy Cronkhite / Jack McCullough 著
  - 夏目 大 訳、武藤 健志 監修
  - ISBN: 4883373436

THE END