Internet Week 2003 <B3>
2003/12/2

インターネットセキュリティ 30の疑問

ネットワンシステムズ(株)
白橋明弘

重要性増すセキュリティ

- インターネットの普及・拡大と共に、セキュリティの重要性が増している
- 特に2000年前後からのブロードバンドの本格的な普及は、質的な変化をもたらした
- ブロードバンドの普及→脅威の増幅
- ネットの重要性増大→影響の深刻化
- 社会インフラ化したインターネットでは、<提供者の責任>と<利用者の常識>が重要

30の疑問

1. 今時の常識編 (9問)
2. 構築・運用編 (8問)
3. ワーム対策編 (3問)
4. 法律・制度編 (5問)
5. 新技術・新製品編 (5問)

(1) 今時の常識編

第１問

銀行のATMの暗証番号は4桁の数字、だったら、インターネットバンキングで使うパスワードも4桁で十分？

相手の見えないインターネット

- 銀行のATMには、
  - 監視カメラ
  - 3回暗証番号を間違えるとロック

  などの対策がある。
- インターネットは、
  - 不特定の(匿名の)相手からのアクセスを受ける
  - 対面などによる抑止力が期待できない
  - 不正行為に時間をたっぷりかけられる

  などの特性があるので、強固な認証が必要

第2問

銀行サイトなどでよく見られる「SSL 128bitの高度な暗号化技術を用いているので安全」は本当か？

SSLで守れるのは一部のみ

- 暗号化で守れるのは、通信内容の秘匿(と完全性検査)だけ
- OSのセキュリティ・ホールが放置されてたら？
- Webサーバにセキュリティ・ホールがあったら？
- Webサーバのアクセス制御がいい加減だったら？
- Webサーバに重要な顧客データを格納してたら？

第3問

SSLで暗号化されていれば、
固定パスワードでも安全？
(パスワード自体は、推測されにくい安全なものが使われているとして)

盗聴の危険は無い、しかし...

- SSLで保護されるので、通信路の途中で盗聴される心配はない。
- 通信路のはじ(端末および人間)での危険は、SSLでは防げない
  - パスワードを肩越しに覗かれる
  - キーロガーを仕掛けられる
  - その他、利用者の不注意でパスワードが漏れる
- 固定パスワードの弱点は「reuseによるなりすまし」で、通信路を暗号化してもこの点は変わらない
  - 例えば、ワンタイム(使い捨て)パスワードなら、安全

第4問

インターネットカフェやホットスポットを利用するのは、安全ですか？

危険がいっぱいです

- 備え付けPCの場合
  - PCに何が仕掛けられているかわかりません。個人認証をするサイトの利用や、個人情報の入力などは一切してはいけません。
- 自分のPCを持ち込む場合
  - 重要な情報は、SSLやVPNなどで必ず暗号化して送受信しましょう。

第5問

無線LANは、情報漏洩や社内ネットワークへの侵入などの可能性があり、危険だというのは本当ですか？

正しく使えば、大丈夫です

- 無線LANのセキュリティの問題には、
  次の2つの側面がある
- 誤った使用法による問題
  → 例えば、暗号化無しで使用は酷い
  → 正しい知識を普及させる必要あり
- 無線LANの規格や仕様の不備・不足
  → 長期的には、新規格の整備に期待 (後述)
  → 今ある技術や製品をうまく使いこなす

第6問

インターネットカフェでネットバンキングを利用して、1600万円を詐取されるという事件が起こりましたが、これは利用者が不注意ということで仕方ないのでしょうか。

無知を笑うのは易しいが...

- インターネットカフェのPCで、ネットバンキングを利用するなど、自殺行為に等しい
- キーロガーの類の格好の餌食に
- キャッシュカードと暗証番号を使われたに等しいので、責任は全て利用者に帰される
- 「セキュリティの常識」の普及が急務
- しかし、サービス提供者も、より安全なシステムを提供する責務があるのではないか？

第7問

サービス提供者にセキュリテイ対策をやってもらいたいのですが、そのために使い難くなったり、利用料金が上がったりするのは嫌なのですが。

利用者はわがまま？

- それは「わがまま」です。そういう利用者が多いと、サービス提供者も、セキュリティ強化にコストをかけるインセンティブが働きません。セキュリティの強化で、利用者が減るのでは、話になりません。
- セキュリティと使い易さを両立させるのが技術ですが、コストの問題は難しい。
- 「セキュリティの文化」を広める必要がある。

第8問

フリーメールや、各種のサイトに登録する場合、気をつけることはありますか？

安易なパスワードに注意

- まず、信用できるサイトを選ぶのは当然
- 安易なパスワードだと、第３者に推測される
  - ネット犯罪の多くが、盗用アカウントを悪用
  - 登録している個人情報が漏れる可能性も
- パスワード忘れの際に使う、「リマインダー」もしっかりと設定する。
- パスワード代わりに、メールアドレスを打ち込むだけで利用できるようなサイトは使用しない

第9問

様々な所で使うパスワードが多くなりすぎで、覚えきれません。やはり、パスワードをメモに記録してはいけないのでしょうか？

パスワードはメモするな？

- 多数のパスワードが覚えられない。でもメモはできない→簡単なパスワードを付けてしまうでは、全く逆効果
- パスワードをメモして、そのメモを(暗号化するなど)しっかり管理する、が合理的
- Single Sign On は、こうした問題を解決してくれる技術だが、インターネット上で使えるようになるのは、まだ先のこと

(2) 構築･運用編

第10問

ファイアウォールで、Webサーバへの攻撃を防ぐことはできますか？

できるものとできないものがある

- 防げるもの
  - http, https(SSL) 以外の通信による攻撃
  - ファイアウォールでフィルタリングすることで、例えサーバに(パッチ未適用の・未知の)脆弱性があっても、攻撃をブロックできる
- (一般に)防げないもの
  - http, https(SSL) による、Webサーバの脆弱性に対する攻撃 → サーバのパッチ適用が重要

第11問

ルータのアクセスリストとファイアウォールのアクセスリストで、設定上注意すべき違いはありますか？

ルータとファイアウォールの違い

- ルータの ACL (Cisco の場合)
  - 静的な Packet Filtering である
  - 行きの Packet と、戻りの Packet に対するルールは別々に記述する
  - Network I/F 毎にアクセス・リストを記述する
    - あるI/Fを通過する Packet に対するルール
- ファイアウォールの ACL (多くの製品で)
  - 動的な Packet Filtering or Appl. GW である
  - 行きと戻りは、ワンセットでルールは1つだけ
  - 通常I/Fを区別するという概念は無い(アドレスのみ)

第12問

ファイアウォールのDMZ(非武装地帯、緩衝地帯)の使い方について、注意点を教えてください。

DMZは使用ポリシーが重要

- ファイアウォール・ポリシーの原則
  - 危険度の高いエリアから低いエリアへは、最小限の通信しか許可しない
  - 危険度の低いエリアから、高いエリアへの通信も、よく必要性を検討する
- ありがちな駄目な例
  - DMZ→社内が管理上の都合で、穴だらけ
  - DMZ→インターネットを、宛先anyで httpを許可している

第13問

リモートアクセス用のVPNの導入を検討しています。注意すべき点について教えてください。

LAN間VPNとの違いに注意

- リモートアクセスVPNは、拡張機能が必要
  - IPsecは、もともとHost間、LAN間中心の設計
  - リモートアクセス用には、認証機構の拡張、IPアドレスの配布、DNSサーバアドレスの配布などの機能が必須
  - 標準化は進められているが、ベンダ独自の実装多く、互換性は期待できない
  - 上記理由で、専用クライアントソフトが必要、OS標準のIPsecは「使えない」

第14問

VPN利用のリモートアクセスの認証強化に、OTP・PKI・生体認証のいずれかの導入を考えています。選択のポイントを教えてください。

認証手段の選択は悩ましい

- OTP (One Time Password)
  - 「時代遅れ」と思われがちだが、手堅いソリューション
- PKI (Public Key Infrastructure)
  - インフラを作る気なら、本気の取り組みが必要
  - 意外に大きい運用コストに注意
  - 単目的のお手軽導入には？
- 生体認証 (or USB認証デバイス)
  - 人気高いが、意外に普及進まず
  - ネットワーク認証として使う標準の欠如がネック
  - PKIとの組み合わせでは、さらにコスト高に

第15問

Windows Update を頻繁に実行していれば、パッチ適用の点では、安全と思っていいでしょうか？

対象外のものに要注意

- WindowsのOS自体、IE、IISなどのパッチは Windows Update でカバーされる
- クライアントPCは、Widnows Update励行を推奨
- しかし、Back Office 系 (SQL Server、Exchange Server等) は、個別パッチが必要
- Back Office 系など入れていないと思っていても、アプリケーションの一部として SQL Server (MSDE2000) が入っていたりするので要注意
- サーバーの場合、パッチをあてると動かなくなることもあるので、悩ましい

第16問

Webサーバーの防御に、ファイアウォールの導入、サーバへのパッチ適用以外に、良い手段はありませんか？

転んだ後の対策も重要です

- セキュリティ対策に「万全」はありません。どんなにしっかり管理をしても、公開サーバーが侵入されたり、ワームに感染する可能性はあります
- やられてしまった後の被害を広げないことを考えて設計することも、セキュリティでは重要です
- 公開サーバーを、ファイアウォールのDMZ(非武装地帯・緩衝地帯、第3セグメント)に置いて、危険を封じ込めるのが、良く取られる手法です
- バックアップなど、復旧の手順も定めておきます

第17問

最近、メールなどで個人情報のファイルなどが流出する事故・事件が良く起こっています。これを防止する良い方法はないでしょうか？

システムだけでは限界がある

- 添付ファイル名や、本文中のキーワードでメールをチェック(保留)するツールはあり、上手く使えば、ミスの防止には役に立つ
  - ルール策定や、運用手順の確立が肝心
  - 社員教育も重要
  - 悪意ある内部犯行に対しては、効果が無い
  - メール以外の漏洩ルートも管理する必要有り

(3) ワーム対策編

第18問

今年のN+I幕張では、会場のShowNet でワームが蔓延したというのは、本当ですか？

本当のようです

- 持ち込まれたPC、レンタルで借りたPCがShowNetにつないだ瞬間に、Windows Updateを適用する間もなく、ワームに感染するといった事件が起こったようです。
- CodeRed や Slammer の攻撃は、今でも、インターネット中に降ってきています。パッチのあたっていないPCは、あっという間にやられます。
- 「グローバルIPアドレス」=「危険」と思いましょう。

第19問

MS Blaster が、Code Red や Nimda と異なり、個人や家庭で大きな被害を出したのは、何故ですか？

MSBlast の特徴まとめ

- 攻撃対象OS: Windows 2000/XP
- 攻撃対象サービス: RPC/DCOM
- 攻撃対象ポート: 135/TCP
- 利用された脆弱性: RPC インターフェースの buffer overrun
- 感染手段: 上記脆弱性に対する攻撃の反復
- 感染対象: ランダムなIPアドレス、近傍をより攻撃
- 副作用: リブート (バグによる)
- DoS攻撃: 特定サイトに一斉にパケット送信 (不発)
- 特徴: クライアントにも広く感染

4つのワームの比較

ワーム	攻撃サービス	攻撃ポート	副作用(直接的)	DoS攻撃	特徴
Code Red	IIS	TCP 80	(バックドア)	有(不発)	
Nimda	IIS	TCP 80	ファイル上書き	無	複合型
SQL Slammer	SQL Server	UDP 1433	無	無	感染スピード
MS Blast	RPC DCOM	TCP 135	無	有(不発)	Client感染

第20問

毎回のように大きな被害をするワームへの対策に、決め手はないのでしょうか？

ワーム対策: 基本の対策

- 予防
  - パッチの適用 (基本)
  - クライアントに対する脆弱性検査
  - Personal Firewall の利用 (感染拡大防止に効果)
- 検知
  - 内→外へのトラフィックの監視が重要に
  - ファイアウォールのログ、IDSの利用
- 被害拡大防止
  - ファイアウォールの利用 (DMZ利用で封じ込め)
  - 危険なネットワークは分離する

ワーム対策: 今後の動向

- パッチ管理の自動化・強制が次第に進む
- 脆弱性検査が、クライアントにも拡大
- システムに新たに接続したPCを検査する
- パッチを適用してないPCはシステムに接続させない
- Personal Firewall のデフォールト装備
- PC管理体制の見直しが進む

(4) 法律・制度編

第21問

個人情報の安易な漏洩事件が多発しています。個人情報保護法が出来て、このような状況は改善するでしょうか？

漏洩防止対策の義務化

- これまでの事件は、個人情報のセキュリティに対する意識の薄さと、基本的なセキュリティ対策の欠如によるものです。
- 個人情報保護法では、個人データが漏洩しないように、安全管理措置(20条)、従業者の監督(21条)、委託先の監督(22条)を求めているので、長期的には改善につながると期待されます。

第22問

自サイトが不正侵入されて、踏み台にされ第3者のサイトに被害を与えてしまった。
訴えられてしまうのか？

踏み台サイトの責任は

- 損害賠償請求をされる可能性があります。
  米国では、実際にそういう事例があります。
  日本では、まだ無いようです。
- 責任が認められるかどうかは、過失の程度にもよります。
- インターネットに接続する責任として、踏み台にされないよう注意しなくてはなりません。

第23問

M社のOSのセキュリティ・ホールで、甚大な被害を被った。M社に損害賠償請求することはできますか？

ソフトウェアのバグは免責

- ソフトウェアは、動産ではなく、PL(製造物責任)法の対象外であり、契約上、瑕疵が免責されているので、訴えることはできません。
- 情報家電はPL法の対象になるのか？ユビキタス社会での、製造者の責任は?
- しかし、組み込みシステムのソフトウェアはPL法の対象になるという解釈が有力です。

第24問

ISO 15408 (Common Criteria) は有用ですか？

15408はフレームワークです

- 15408 (Common Criteria) は、セキュリティ・システムや、製品が、きちんとしたセキュリティの枠組みの上で、設計・製造されていることを確認する仕組みです。
- ただ、認定を取っているというだけは、形式が整っているというだけで、意味はありません。(馬鹿HUBだって15408の認定を取れる)
  どういう内容で認定をうけているかが肝心です。
  (例えば、EAL4+ の <+> の内容)

第25問

ISO 17799 (BS7799)、あるいはその日本版である ISMS (情報セキュリティマネジメントシステム)は有用ですか？

ガイドライン・チェックリストとして有用

- 6月17日現在で、179社がISMS認証を取得済み(本家英国のBS7799取得～90社)
- BS7799/ISMS の考え方は有用と思います。
- セキュリティ・ポリシーや運用ルールを策定する際に、リファレンスあるいはチェックリストとして、役に立ちます。
- 認証を取る過程で、見落としていた対策・対応に気づくことが多々あります。

(5) 新技術・新製品編

第26問

無線LANの新しい規格 WPA (WiFi Protected Access) や、802.11i は、無線LANのセキュリティの問題点を解決してくれるでしょうか?

無線LANセキュリティの改善

- WEP(Wired Equivalent Privacy)の問題点
  - 暗号プロトコルが脆弱で、解読される危険性がある
  - 鍵設定が手動で、かつ全ユーザに共通
- この夏から製品化されている WPA (WiFi Protected Access)や、IEEEで標準化が進んでいる802.1iで、大きく改善の見込み
  - ユーザ毎に異なる鍵を生成、定期的に変更
  - RADIUSと連携し、認証の集中管理が可能
- 現状の課題は、認証方式の乱立
  - EAP-TLS, LEAP, PEAP, EAP-TTLS

第27問

IDSを導入しましたが、無意味がアラートばかりでとても運用できません。IDSの運用性・有効性を高めるという新しいアイデアについて、教えてください。

IDSの新しい動向

- IDSは、入れたけど使えてないことが多い
  - 運用が手にあまる
  - 誤検知、誤報(False Positive)多すぎ
  - 使えるようにするチューニングが大変
- 管理性を向上させる新しい動向
  - 脆弱性監査と、IDSの連携
    →チューニングの自動化と誤報の低減の実現
  - 統合管理ツール(SIMS)により、複数のデバイス(FW,IDS,…)のイベント相関を取り、誤報を低減する

第28問

IDP (Intrusion Detection & Prevention) という技術を最近耳にしますが、どうなのでしょうか。

IDP という方向性

- IDP (Intrusion Detection & Prevention)
  - IDS を通信が通過する形で置き、攻撃を検知したセッションをリアルタイムで遮断
  - かつては、「インライン型IDS」と分類
  - FWとIDSの連携機能は、「使えなかった」が一体化して、高速・密に連携することで実用化
  - たとえ無意味な攻撃でも、攻撃は攻撃、止めてしまえばよい、という発想
  - パフォーマンスなどが課題

第29問

今話題の新製品として、SSL-VPN がありますが、今の IPsec VPN に替わって、将来これが主流になっていくのでしょうか。

SLL-VPNは、製品を見極めて

- クライアントは、Webブラウザ中で動作する (IPsec のようなクライアントソフトウェアが不要)
- プロトコルはSSLなので、どこでも使える (IPsec の NAT Traversal のような問題が起こらない)
- 但し、ブラウザベースなので、アプリケーションが限定される (IPsec のように透過的ではない)
  - Webアプリケーション、SMTP/POP, ターミナル系

第30問

IPv6 が普及すると、セキュリティの技術や考え方がかわるのでしょうか？

いずれ、変わるでしょう

- 企業ネットワークにおいては、セキュリティに関して、これまでのIPv4と全く同じやり方を採用することも可能です。
- IPv6の特長を生かした P2P (End to End)のアプリケーションや、End to End の IPsec が広く利用されるようになると、セキュリティ対策も変わってくるでしょう。
- 情報家電的な応用に関しては、ホームゲートウェイがセキュリティの「関所」になるかもしれません。
- ユビキタスのセキュリティは、まだわかりません。

ご清聴ありがとうございました。

Any Questions ?