セキュリティポリシーの機能と効用

～危ないサイトの見分け方～

株式会社アイ・ティ・フロンティア
セキュリティソリューション部
園田道夫

インターネットの危険性

- つまるところ、インターネットは「危険」なインフラである
- 世界中に通じていて、しかも物理的距離が無いに等しい
  - 国籍、思想、宗教、文化などのメンタリティがかなり異なる人々が無造作に集まっている
  - 現実世界での犯罪は、地域で言えばかなり局所的だが、インターネットではブラジルのクラッカーが日本のサイトを攻撃できてしまう

インターネットの危険性2

- 成りすまし、騙り、身元隠しが容易
  - 物理的コミュニケーションを伴わない上、認証データが現実世界並みに貧弱
  - 認証データなどのコピーが非常に簡単で、かつ正確
  - 構造上身元や発信元を追いかけるのにも限界がある

インターネットの危険性3

- 嫌がらせにも弱い
  - 匿名性を悪用した嫌がらせ（ストーカー、迷惑メール）
  - ものすごく多くの人に簡単に情報公開・メール送信できることを悪用した嫌がらせ（掲示板悪用、誹謗中傷ページ、迷惑メール）
  - 接続が誰にでも開かれていることを悪用した嫌がらせ（使用不能攻撃＝DOS攻撃）

今までのインフラは？

- 物理的に遠いところからの各種攻撃は非常に困難、もしくは膨大なコストがかかる
- 認証はインターネットより厳しい？
- 認証データの偽造はインターネットより難しく、コストもかかる
- 嫌がらせに対しても、インターネットよりはまし

そんなインターネットも利用拡大中

- ブロードバンド＆常時接続時代の本格的な家庭への到来
  - 今後数年のうちに、常時接続環境は現在のテレビ並みの普及？
  - 携帯端末（携帯電話含む）もますます普及
  - それどころか、IPv6になると洗濯機や冷蔵庫、電子レンジや風呂湧かし装置までインターネット接続されてしまう？？

そんなインターネットも利用拡大中2

- 社会的インフラもインターネットに接続される時代に
  - 電子政府（もしかして防衛情報？？）
  - 電子お役所（もしかして住民基本台帳？？）
  - そればかりか、大規模プラントも？
  - もしかして、電力・ガス・水道も？
  - もしかして、交通（道路、鉄道、航空）も？？
  - CMには、遠隔地に住む名医が、ネットワークを介して手術する、というのがありました。もしかして、まさか・・・

インターネットは思ったよりも「危険」である

- 再び、インターネット・インフラの基本的な弱さとは？
  - 成りすまし、騙り、身元隠蔽
  - 盗聴
  - 詐欺
  - 嫌がらせ
- 本当は、インターネットが「危険」なのではなく、インターネットのリスクを知らず、理解せず、無視して使うことが危険なのでは？

そんなインターネットも利用拡大中3

- 電子商取引 (e-commerce) の拡がり
  - オークションサイト (情報交換)
  - 物品販売 (地球最大の書店アマゾンの成功？)
- 利用拡大しているが、肝心な決済情報のやり取りはまだまだこれから
- まだまだ立ち上げや運用コストがかかり、インターネットで取引すればそれだけで儲かるという時代ではない

電子商取引とは？

- 電子商取引にはいろいろな形態がある
  - B to B　(企業間取引)
  - B to C　(企業から消費者へのオンライン取引)
  - C to C　(消費者間のオンライン取引)
- いずれもネットワークを介在させる
- クレジットカード決済などの既存のインフラも、補助的に利用する場合もある

電子商取引の決済方法は？

- プリペイド貨幣を使った決済
- クレジット番号のやりとりによる引き落とし
- 電子的な貨幣
- 電子的な銀行の参入

電子商取引のリスク

- またまた、インターネットの基本的なリスク
  - 成りすまし、騙り、身元隠蔽
  - 盗聴
  - 詐欺
  - 嫌がらせ
- リスク対策は？

電子商取引のリスク対策

- 暗号化インフラによる認証の強化
  - お金のやり取りには匿名性は不要
  - 盗聴対策
- サーバーセキュリティ対策
- ネットワーク構成のセキュア化（ファイアウォールなどの導入）
- 銀行や電子貨幣出版者によるリスクヘッジ

電子商取引のリスク対策2

- サービスプログラムのセキュリティを意識した設計・実装
  - フロントに立つWebサーバーのプログラム（CGI、スクリプト、Java、ColdFusionなどなど）が必要最小限の情報以外出さない
  - Webによるサービス（HTTP）の性質を理解した設計
  - プログラム言語の性質を理解した実装
  - 適正なセッション管理

電子商取引のリスク対策3

- 嫌がらせ対策は難しい
  - どこからが嫌がらせなのか？
  - 手口の悪質＆巧妙化
  - パターンの機械的な認識によるフィルタには限界がある？（パケット内容まである程度踏み込んで、ISPなど上流にてフィルタしたい）

リスク対策の効果？

- 暗号化（とそれに伴う認証の強化）は、リスクを根絶できるのか？
  - 成りすまし、騙り、身元隠蔽
  - 盗聴
  - 詐欺
- 成りすまし、騙り、身元隠蔽を「ある程度までは」防げる
- 盗聴も「ある程度までは」防げる
- 詐欺は防げない？身元保証は誰がやるのか？

電子商取引のリスク2

- 人間リスク（かかわるプレイヤーすべて）
  - 実はこれが最大のリスク？
  - 特にエンドユーザーのリスクが大きい
- サービス提供者リスク（脆弱な経営基盤等）
- インフラ提供者リスク（脆弱な経営基盤等）
- 認証局リスク
- 保険リスク（高額な保険＝コスト）

関わる人はどんな人？

- 使う人（エンドユーザー）は知識も見識も普通の人々（企業、団体、一般消費者）
  - 特別な技術的知識を持っている人はごく少数
- サービスを提供する人々（企業、団体、個人）
- システムやネットワーク、サーバーを管理する人々（技術者。非技術者の場合もあり？）
- 決済する人々（銀行など）

エンドユーザーに何を期待できるか？

- 知識も見識も普通の人々には、何も期待できない！
- エンドユーザー自身の利益を守ることすら期待できない？自分の情報などが悪用されても気が付かない？
- まして商取引システムを守る意識などさらさらない？

エンドユーザーの脅威？

- どんなに素晴らしいセキュリティ対策も、エンドユーザーが台無しにしてしまう危険がある
  - セキュアなサーバー、セキュアな暗号化ネットワーク、インフラを使っていても、カギがひとつ漏れたら非常に危険になる
- 意識・無意識にかかわらず、エンドユーザーこそ最大の脅威？

エンドユーザー対策

- エンドユーザーの選別
- 暗号化以外の認証手段（電話番号コールバック、専用回線によるサービスなど）
- あらかじめエンドユーザー負担でリスクヘッジしておく
  - クレジットカードの保険や年会費
  - 利用契約書
- 銀行やクレジット会社とリスクを分担する

エンドユーザーから見た危ないサイトの見分け方

- 今利用しているそのサイトは本当に安全なのか？
  - 主催者はどこの誰か？
  - どのように構築されているのか？
  - どんな情報を要求してくるのか？
  - どんな情報を公開しているのか？
  - どんなセキュリティポリシーを持っているのか？
  - どんなプライバシーポリシーを持っているのか？
  - どんなセキュリティ対策を行っているのか？

電子商取引を主催する人はどんな人？

- 企業（大きいのから小さいのまで）、団体、個人、つまるところ何でもあり
- 国籍不明、信用度も身元も不明
- インターネットにつながっているというだけで、実社会のように確かな（？）身元証明があるわけではない

主催者に
何を期待できるか？

- これまた何も期待できない？
- 主催者自身の利益を守ることすら期待できない？
- 商取引システムを守る意識は、さすがに少しは持ち合わせているかも知れない

(しかし保証はできない)

主催者の脅威？

- どんなに名の通った企業が主催しているサイトでも、セキュリティの対策がちゃんとしているかどうかとは相関しない
  - きちんと費用をかけて管理しているとは限らない
  - 技術力が高いとも限らない
  - 現実世界でのブランド力とインターネットでのブランド力は異なっている
- むしろ有名な会社ほど、名を売りたい攻撃者に狙われやすい (間接的な脅威)

サイトを管理する人はどんな人？

- 片手間、ボランティア、本業以外の仕事として管理している
- たまたまコンピュータ好きで詳しかっただけ
- 若い人
- 問題意識がある人
- ・・・共通するのは、ほぼ「無償」である、ということ
- 無償でない管理者も居るには居るが・・・
- もしかすると、誰も「管理」していない？

(ボランティア) 管理者に何を期待できるか？

- 今のところボランティア管理者に期待するしかない？
- それでなくても多忙なのに、そこまできっちり手が回らない？ (その分報酬貰えるわけでもないし)
- 技術レベルも、かけられる手間隙も属人的 (平準化していないので、保証できない)

(ボランティア) 管理者の脅威？

- 報酬も評価も無いのに、責任だけ負わされている
- 報酬も評価も無いので、責任も無い
- 報酬も評価も無いので、技術力も向上しない (できない)
- 報酬も評価も無いので、体制も作れない
- 報酬も評価も無いので、時間も作れない
- ・・・セキュリティレベルを上げられない

(ボランティアじゃない) 管理者に何を期待できるか？

- 今のところ (ボランティアじゃない) 管理者に期待するしかない？
- 報酬は貰っているが、技術レベルはこれまた属人的
- きちんとした技術情報が見当たらない？ (わけではない。ちゃんと在るところには在るのに、世の中被害は後を絶たない)

(ボランティアじゃない) 管理者の脅威？

- 報酬も評価も有るのに、不当に責任が重い
- 報酬も評価も有るのに、それでも責任が無い
- 報酬も評価も有るのに、技術力が向上しない (できない)
- 報酬も評価も有るのに、地味な仕事なのでやりたがる奇特な人は少ない
- ・・・セキュリティレベルを上げられない

コンテンツ作る人はどんな人？

- エンドユーザーと同じく、知識も見識も普通の人々
  - 特別な技術的知識を持っている人はごく少数
- コンテンツを作って、最新の超便利ツールでばりばりアップしたい！
- アップした後も直に触ってメンテナンスしたい！
- 当然ながら、セキュリティ意識は低く、自分の仕事がやりやすければそれでよい

コンテンツを作る人に何を期待できるか？

- 便利なツールが使えないことに我慢できるか？（煩雑な手順を経て、わけわかなコマンド文字列を叩いてコンテンツ更新する、など）
- 管理者の提示するセキュリティ対策（ポリシー）に従えるか？
- サイトを守る意識を持てるか？
- ・・・やはり期待できない？

コンテンツを作る人の脅威？

- コンテンツやデータ更新には危険がともなう（明らかにサーバー内ファイルや設定などを更新する必要がある）
- サイトやデータを守る（少なくとも与えられた手順に従う）意識が無ければ、最大の脅威

決済などに関わる人はどんな人？

- 銀行、ネット銀行、クレジット会社などに加え、別業界からの新規参入も有り
- モロに経済的なリスクを背負うため、金融的なプロか、それに準じる知識を持った人が多い
- 犯罪的な意図を持った人もごくタマには居る

決済などに関わる人に何を期待できるか？

- 自分たちの力が及ぶ範疇（というより責任範囲か？）については、シビアにかつプロフェッショナルな仕事が期待できる
- しかし、責任範囲の外には決して出ない（当然か）
- 顧客を切り捨ててでも自分たちを守る（これも金融系企業活動の論理から言えば当然か？）

決済などに関わる人の脅威？

- 法律や金融知識による理論武装はほぼ完璧（しかし、必ずしも顧客を守るという原理で動いているわけではない）
- リスクヘッジをエンドユーザー、主催者に巧妙に要求してくる（適正な価格であれば問題は無い）
- ・・・しかし総じてあまり大きな脅威ではない。困っていても助けてくれないことが多いだけ

再び、エンドユーザーから見た危ないサイトの見分け方

- 今利用しているそのサイトは本当に安全なのか？
  - 主催者はどこの誰か？
  - どのように構築されているのか？
  - どんな情報を要求してくるのか？
  - どんな情報を公開しているのか？
  - どんなセキュリティポリシーを持っているのか？
  - どんなプライバシーポリシーを持っているのか？
  - どんなセキュリティ対策を行っているのか？

エンドユーザーからは何が見えるのか？

- エンドユーザーがチェックできること
  - サイトの関連情報
    - INTERNIC,JPNICなどの情報
    - 主催企業、団体などの関連情報（株価、業績、組織体制、業界内での評判、雑誌新聞などの情報、さまざまなメーリングリストでの評判、あまり信用できないが2ちゃんねる情報、スラッシュドットの噂情報）
    - インサイダー情報
    - 取引先からの情報

エンドユーザーからは何が見えるのか？2

- 他にエンドユーザーがチェックできること
  - サイトそのものの情報
    - DNS、メールサーバー、Webサーバーなどの有無、およびバージョンや設定情報などなど
    - ファイアウォールの有無、フィルタの有無などなど
    - どのくらいの頻度でメンテナンスされているか、などなど
    - ポートスキャンによる情報（今は違法ではない）

エンドユーザーからは何が見えるのか？3

- プログラム関連でエンドユーザーがチェックできること
  - クロスサイトスクリプティング？
  - ダウンロードされてくるソースやスクリプト(そもそもどんな開発言語(環境)を使っているのか？
  - URIと引き数
  - Cookie情報
  - SSLなどの認証情報

エンドユーザーからは何が見えるのか？4

- まだまだある、プログラム関連でエンドユーザーがチェックできること
  - 正しくないURI入力などに対する処理結果
  - Hiddenフィールドの内容データ偽造への対処は？
  - Cookie内容偽造への対処は？
  - パスワードのやり取りは？パスワードポリシーは？
  - ・・・しかし、こんなことまでチェックしてもいいのだろうか？（自分の情報やお金を守るため、自己防衛なら良い？それとも行き過ぎか？）

エンドユーザーからは何が見えるのか？5

- 他にもまだある、エンドユーザーがチェックできること
  - プライバシーポリシーの表示 (あまり多くない)
  - セキュリティポリシーの表示 (少ない。見せない・隠す方が多い)
  - そのサイトのものに限らず、主催企業・団体のセキュリティポリシーの表示 (少ない。見せない・隠す方が多い)

エンドユーザーからは何が見えるのか？6

- エンドユーザーがチェックできることはまだまだあるが、このあたりからは、・・・
  - サーバー管理画面 (遠隔管理ツール)
  - Webサーバー管理画面
  - Webサーバーのスクリプトエンジンの管理画面
  - そのほか各種管理ツール用裏口ポートなどをヒントに、いろいろな画面 (ツール用クライアント画面もある)

エンドユーザーに何が見えてしまうのか？

- 今までエンドユーザーの視点であげてきたチェックポイントは、逆に言えば構築側のチェックポイントでもある
- エンドユーザーに対し、適切なアクセスコントロールを行う必要がある
- 管理者やコンテンツメーカーに対しても同様

では、
どうすれば良いのか？

- 実は技術的な対策はそれほど問題ではない？
- 真の問題は、セキュリティポリシー（アクセスポリシー、メンテナンスポリシーなど）が無いこと
- サイトに関わるすべてのメンバーの役割と責任、そしてアクセスポリシーを作る必要がある（現状の整理）

セキュリティポリシーの機能と効用

- セキュリティポリシーを作り、構築、管理運用、コンテンツ更新などの局面で、各メンバーの役割と責任を明文化する
  - 混沌とした現状の整理
  - 主な脅威の洗い出しと認識 (リスク分析)
  - 事後対策の手順も作成し、万が一に備えておく (リスクヘッジ)

セキュリティポリシーの機能と効用2

- 技術的要件はポリシーに従うもの
  - 無駄な投資をせず、効率の良い対策を行う
- 取り扱い情報の資産価値を見極め（というか、「決め」）れば、相応な投資を行うことができる
- プレイヤーが交代してもレベルを落とさないことが可能

セキュリティポリシーのルールとしての要件

- 罰則は必要（＝ポリシー運用者には権限が必要）
- 状況に応じてメンテナンスが必要（手続きのハードルを高くしてしまうと、生きたポリシーにならない）
- サイトの最高責任者のお墨付きが必要（権限という意味でも）
- 広報宣伝が必要（認知されないルールは無いのと同じ
- 多くの関係者を味方につけることが大事

セキュリティポリシーは広報すべき？

- ポリシーを社内だけでなく社外に対しても広報した方が良い？
  - ポリシー、スタンダード（標準）、プロシージャ（手順）というレベル分け
  - ポリシーのレベルであれば社外広報しても危険にはならない。むしろ、ユーザーを安心させるポイントになる（もちろんそれだけの社会的責任を負うことにはなる）

セキュリティポリシーは高い？？

- 企業や団体としてポリシーを作ることは、専門家を一定期間拘束することになるため、高くなってしまう？
- サイトレベルのポリシーならば、そんなに高くはつかない？
- 費用対効果を見ようとしても分かりにくいが、想定される被害や負の宣伝効果に比べれば、けっして高くはない？

セキュリティポリシーは難しい？

- 少なくともセキュリティ関連の一般的な脅威や技術的内容について、広範な知識が必要 (リスクを炙り出すことができる知識)
- リスクに応じた解決策 (技術的、ルール的) に関する知識が必要
- 自前で上記の人材を育てるかどうか？育てないのならどうするのか？

とにかくセキュリティポリシーを作ってみる

- 現状の整理のために、とりあえず、とにかくポリシーを作る
  - 今はポリシーのサンプルやテンプレートなども公開されている
  - 脅威や不正アクセスの手法についても、技術解説書が多数あるし、教育コースやセミナーも多くある
  - メーリングリストやネット上の記事など、セキュリティの文字が無いことはない
  - ・・・関連知識を仕入れるのは、それほど困難ではない

とにかくセキュリティポリシーを運営してみる

- 作ったら、使って（運用して）みよう
- 直すことをためらわない
- 最初から無理にレベルを合わせようとせず、使ってみながら修正していく
- 必要とあれば専門家に聞いてみるといいが、専門家にできることは手助けに過ぎない

セキュリティポリシーの効果を計ってみる

- 使ってみた感想「厳しすぎ？甘すぎ？」
- 今まで検知できなかった不正アクセスの試みを検知できるようになったか？
- 今まで責任者と責任範囲が明らかになっていなかったのが、はっきりしたか？
- 今まで手順がはっきりしていなかったことが、はっきりしてきたか？

セキュリティポリシーの効果を計ってみる2

- 何かが起こったときの対処手順がクリアになったか？
- ポリシーは社員（組織構成員）すべてに知られているか？
- ポリシー作成＆運用前と後では、セキュリティに関する意識が変わったか？

～終わり～