Internet Week 2009 - *H1 インターネットセキュリティ2009* -

脅威のトレンド 2009 Webサイトの動向

2009年11月24日

NRIセキュアテクノロジーズ株式会社

テクニカルコンサルティング部
セキュリティコンサルタント
櫻井 厚雄

目次

1. 2009年のWebサイト被害状況
2. Webサイトのセキュリティ実態
3. 対策
4. 今後の展望

1. 2009年のWebサイト被害状況
手口その1 マルウェア頒布への悪用

改竄サイトを基点とした
大規模なマルウェア感染

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、2009年6月および2009年上半期のコンピュータウイルス・不正アクセスの届出状況をまとめました。
（届出状況の詳細PDF資料はこちら）

1. 今月の呼びかけ

「 あなたのウェブサイト、改ざんされていませんか？ 」
― ウイルスばらまきサイトに仕立て上げられているかもしれません ―

最近、企業や個人が運営しているウェブサイトを改ざんされる事例が多く発生しています。改ざんされたウェブサイトには、閲覧した利用者のパソコンをウイルスに感染させる仕掛けが組み込まれている場合があります。その結果、改ざんされたウェブサイトの利用者から、「ウイルスを検知した」、「ウイルスに感染した」といった届出や相談がIPAに寄せられています。
改ざんされたウェブサイトの運営者は、被害者に留まらず、ウェブサイト利用者のパソコンにウイルスを感染させてしまう加害者となります。このような被害の拡大を防ぐため、ウェブサイトの管理者は、管理しているウェブサイトが改ざんされていないか確認し、ウイルスの"ばらまきサイト"に仕立て上げられないようにしてください。

印 刷

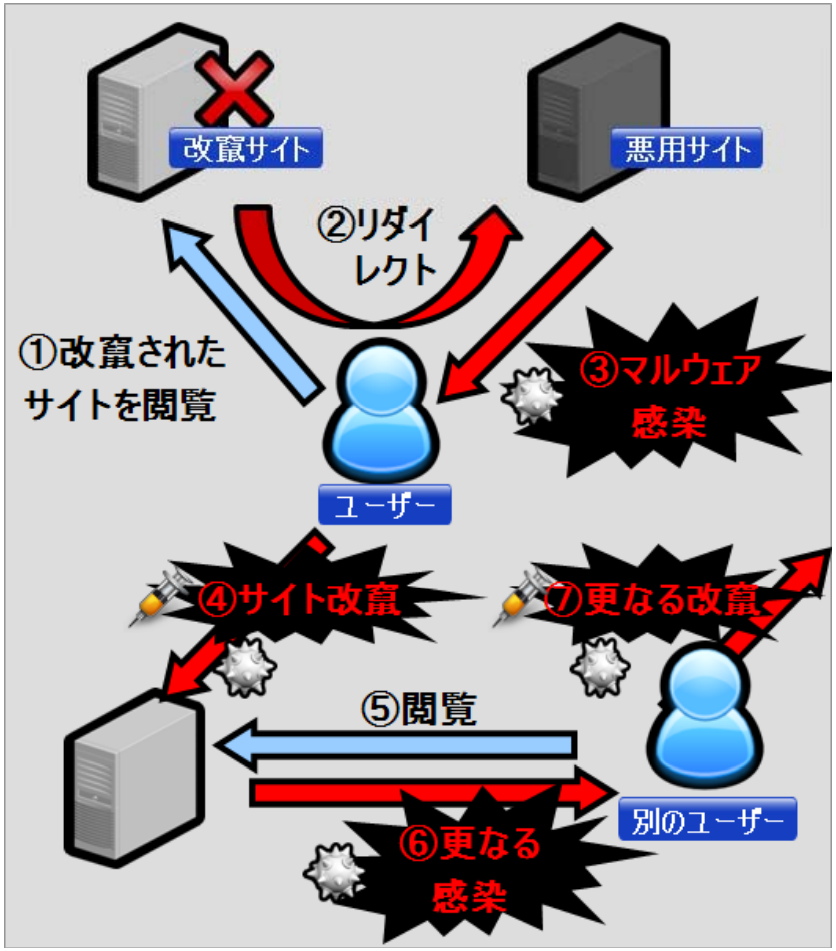
2009年5月12日

弊社サイトの改ざんに関するお詫びとご説明

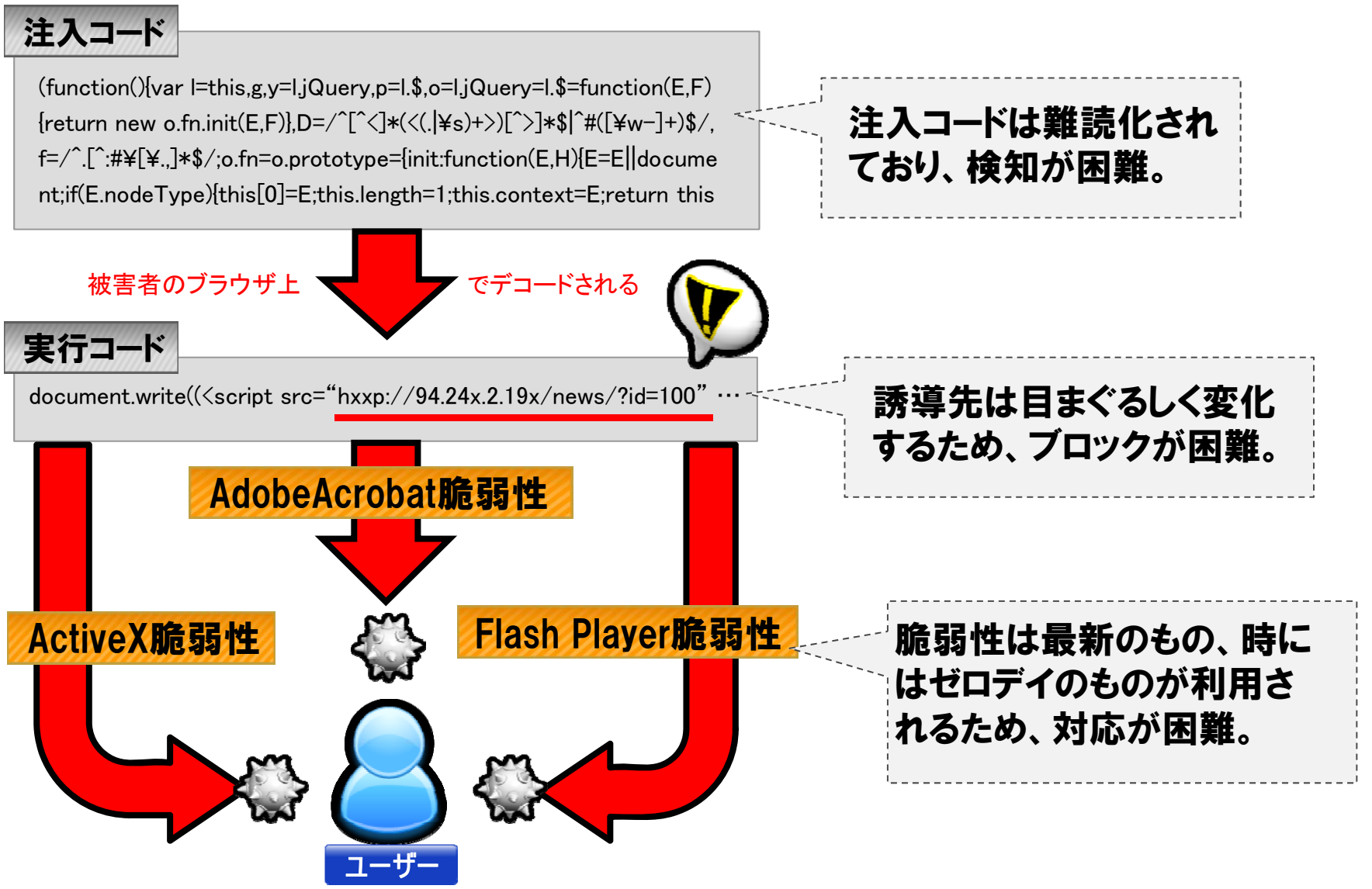
[redacted]株式会社

いつも[redacted]株式会社のホームページをご覧いただきありがとうございます。

この度、弊社サイトの一部において第三者による改ざんが確認され、当該期間に下記サイトを閲覧された方にウイルス感染の恐れがあることが判明いたしました。平素から弊社サイトをご覧いただいている皆様にご迷惑をおかけしましたこと、心よりお詫び申し上げます。



1. 2009年のWebサイト被害状況
手口その1 マルウェア頒布への悪用



注入コードは難読化されており、検知が困難。

誘導先は目まぐるしく変化するため、ブロックが困難。

脆弱性は最新のもの、時にはゼロデイのものが利用されるため、対応が困難。

1. 2009年のWebサイト被害状況
手口その2 SQLインジェクション

NRI SECURE TECHNOLOGIES

今年も発生した大規模SQLインジェクション被害

対象サイト	時期	件数	被害内容、漏洩した情報
カカクコム	2005年5月	約22,500件	メールアドレス
ワコール	2005年11月	5,188件	個人情報(クレジットカード情報を含む)
中略			
ホッタ株式会社	2008年9月	1万8000件	顧客情報（クレジットカード情報含む）
アスマート （含む同系列サイト）	2009年8月	約14万5000件	個人情報 （クレジットカード情報を含む）
イーサプライ	2009年8月	約5600件	個人情報 （クレジットカード情報を含む）
デジタルダイレクト	2009年8月	約16万1000件	個人情報 （クレジットカード情報を含む）

（出所）
各種報道記事から
NRIセキュアテクノロジーズ作成

1．2009年のWebサイト被害状況
Webサイト攻撃に悪用される脆弱性

- Webサイト侵入によるコンテンツ改竄
  ⇒アクセス制御やパスワード管理等、愉快犯主体の時代からあった問題
- SQLインジェクションによる情報漏洩や改竄
  ⇒SQLインジェクションの国内メジャーデビューは4年以上も前

▼

Webサイト攻撃に悪用される脆弱性は新しい問題ではない

▼

Webサイトには昔からある手口がいまだに通用する！

2. Webサイトのセキュリティ実態
2009年度上半期の診断結果より

- **35%のWebサイトに致命的な欠陥が存在**
  - 計98の企業のWebサイトに実施したセキュリティ診断サービス結果※

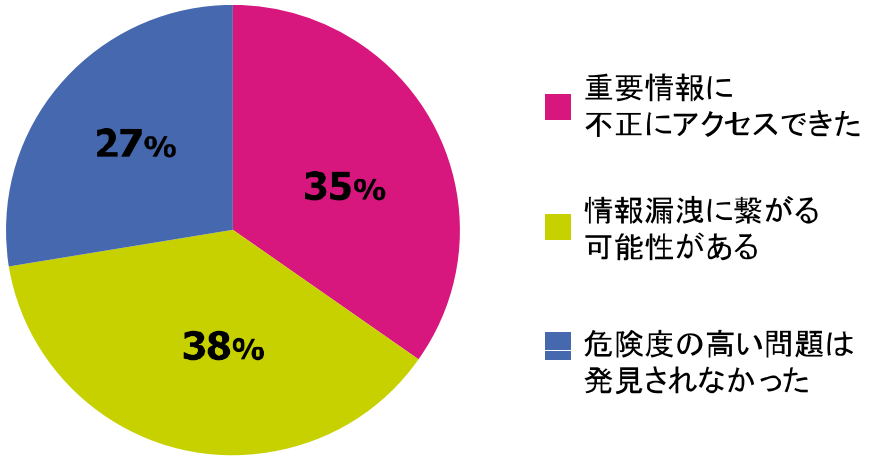
※ NRIセキュアの2009年度上半期（2009年4月1日～9月30日）
Webアプリケーション診断サービス実績より

セキュリティ診断結果

- 35%のWebサイトで、実際に重要情報を不正に取得できる致命的な欠陥が見つかった

- Webアプリケーション診断とは
  - ✓ Webサイトのセキュリティ欠陥を発見する商用サービス
  - ✓ 第三者(いわゆる「ハッカー」)と同じ条件で、外部からセキュリティ上の問題点を探す
  - ✓ サイト公開前もしくは既存サイトへの追加機能リリース前の最終チェック段階で診断するケースが大半

セキュリティ診断の実施結果
（2009年度上半期）

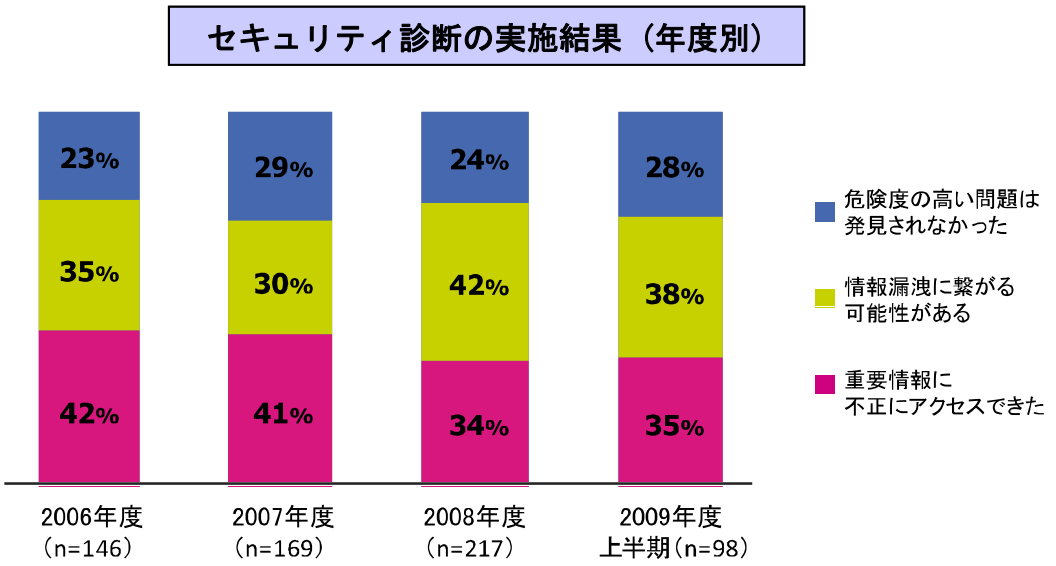


2. Webサイトのセキュリティ実態
2009年度上半期の診断結果より

- これまでと比較しても致命的な問題を抱えるWebサイト割合に大きな変化はない

セキュリティ診断結果の経年分析

- 2009年度になってもWebサイトのセキュリティレベルが大きく向上しているわけではない
  - ✓ 相変わらず3割強のWebサイトで、実際に重要情報を不正に取得できてしまう
  - ✓ 危険度の高い問題が発見されなかったサイトは、2割台にとどまる



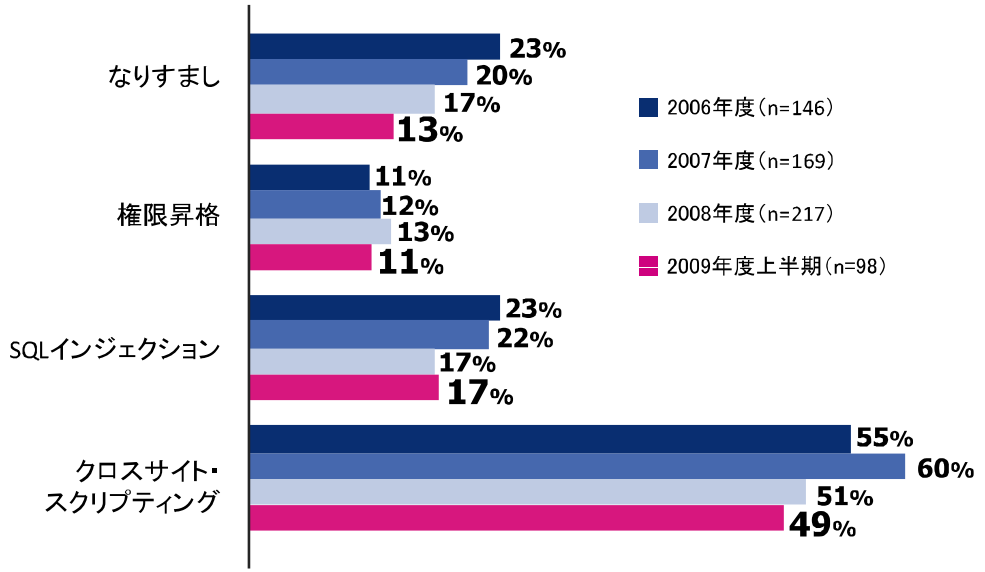
2. Webサイトのセキュリティ実態
2009年度上半期の診断結果より

- 主要な脆弱性の発見割合にも大きな変化はない

主要な脆弱性の発見割合

- 重要情報に不正にアクセスできたケースでは、毎年以下の3つの脆弱性が比較的多く発見されている
  - ✓ 関連チェック不足による　なりすまし
  - ✓ 権限昇格による管理者機能へのアクセス
  - ✓ SQLインジェクションによるデータベースへの不正操作
- 減らないクロスサイト・スクリプティング脆弱性
  - ✓ 相変わらず半数近くのWebサイトで発見される

セキュリティ診断の実施結果（年度別）

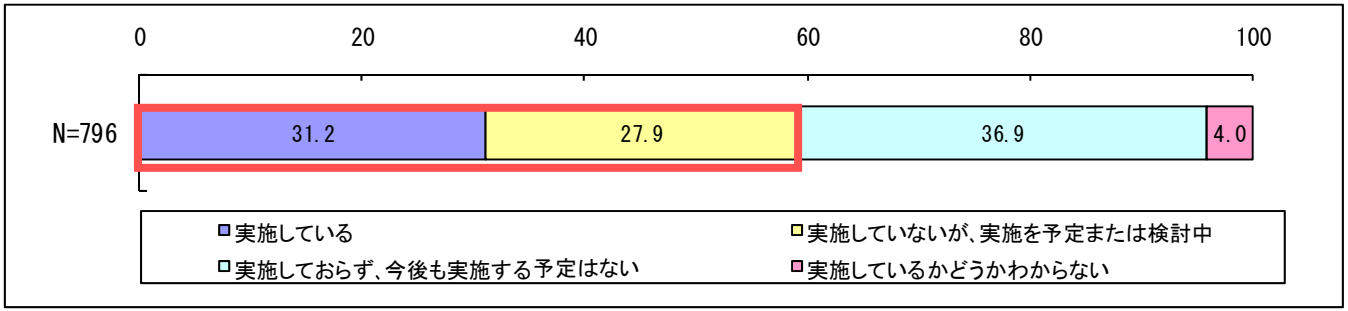


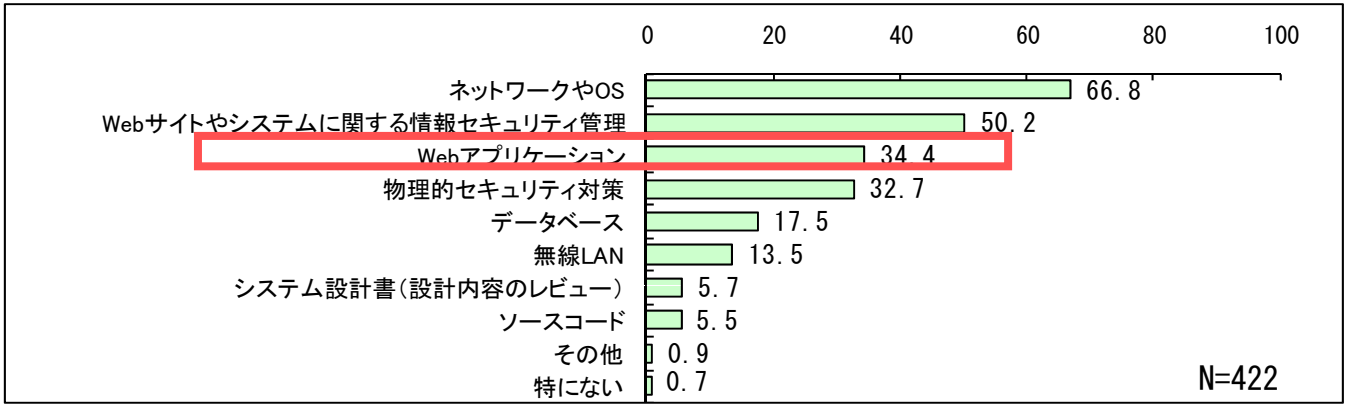
2. Webサイトのセキュリティ実態
2009年 アンケート結果より

- 世間一般におけるセキュリティ診断の実施割合はおよそ2割程度

NRIセキュアテクノロジーズが実施したアンケート調査

- Webアプリケーションのセキュリティ診断を実施している企業は20.3%





【出所】
NRIセキュアテクノロジーズ
「企業における情報セキュリティ実態調査2009」

2. Webサイトのセキュリティ実態

- セキュリティ診断を実施している企業は、20.3%
- セキュリティ診断の結果、35%のWebサイトに致命的な欠陥が発見される
  ⇒コストを掛けて診断を実施している意識の高いサイトでもこの数値

▼

多くのWebサイトが危険な状態のまま運営されていることが懸念される

▼

■不正アクセスのリスクは日々増加
- 高度化・広範化する攻撃手法
- 金銭目的によるインターネット犯罪の増加

▼

数多くのWebサイトがいつ被害にあってもおかしくない状況

3. 対策
安全なWebサイトを真面目に構築しましょう

- 要件定義段階において、セキュリティガイドラインを設定
  - システム開発において守るべきセキュリティ対策をまとめたガイドラインを作成
  - ガイドラインを軸としたマネジメントサイクル(PDCAサイクル)を構築
  - 漏れのないセキュリティ要件定義を行う
- ガイドライン/セキュリティレビューを利用したセキュア設計
  - セキュリティ要件を適切に設計に落とし込む
- 実装工程でソースコードレビューを実施する
  - 網羅的なレビューにより対策漏れを排除
  - 問題が見つかったら同工程内で直ちに修正に着手

- 各フェーズで多層的にチェックを行う
  - 工程が下流に進むに従って、潜在する問題が排除されてゆくようなアプローチ
  - 公開直前には、これまでの工程で漏れが生じた箇所のみ対策するだけで済む
  - 結果、トータルでの費用を低く抑えられコスト効率の高いセキュリティ対策が可能

4. 今後の展望
ハッカー視点から見たWebサイトセキュリティ

■2009年度上半期セキュリティ診断の結果から
- 診断対象はこれからオープンもしくは運用が本格的になっていくサイト
  ⇒既存のサイトと比較してセキュリティレベルは大して向上していない

▼

脆弱なWebサイトが日々作られ続けている

▼

- 多くのユーザクライアントアプリが脆弱なのは既知だが、一気に狙うには？
  ⇒サイトを改竄すれば、カモが向こうからやってくる。マルウェア配布のための電波塔
- 通常ファイウォール等で阻止され、DBにはダイレクトアクセスできない
  ⇒SQLインジェクションを悪用すれば、WebアプリがDB攻撃のための便利なインターフェースに

▼

脆弱なWebサイトは攻撃者にとって色々と便利な攻撃ツール

「今後も美味しくいただきます」

お問い合わせは下記まで

NRIセキュアテクノロジーズ株式会社

〒 105-7113　東京都港区東新橋1-5-2　汐留シティセンター

TEL： 03-6274-1011　E-mail：info@nri-secure.co.jp

Home Page：http://www.nri-secure.co.jp