



SANCTUM

Webアプリケーションセキュリティ

HINET

株式会社 日立情報ネットワーク

Webアプリケーション・ハッキングの 最新の事例



税務サイトe1040リー
ブス顧客の情報と
SSNが暴露される
— CNET News.com,
2001年2月12日

ナスダック改ざんされ、他に
季節的な落書きも
— SecurityWatch.com
2000年11月27日

Ameritechの電子決算システ
ムの欠点が露呈
Chicago Tribune, 2001年4月6日

IPlanetサーバのセキュリティ
ホールがオンラインバ
ンキングに影響
— The Register, 2001年4月28日

AP通信社サイト
ハッキングされる
— Interactive Week
2001年5月20日

民主党サイトでドナー情報
が暴露される
— MSNBC 2001年4月5日

Microsoftサーバパッ
チの提供延期

— Zdnet 2001年5月9日

IRS電子ファイリングシステ
ムにセキュリティの緩みが
発見される
— LA Times, 2001年5月15日

クラッカー、ショッピングソフ
トの脆弱性を利用し、カー
ド情報を盗み出す
— Newsbytes,
2001年4月10日

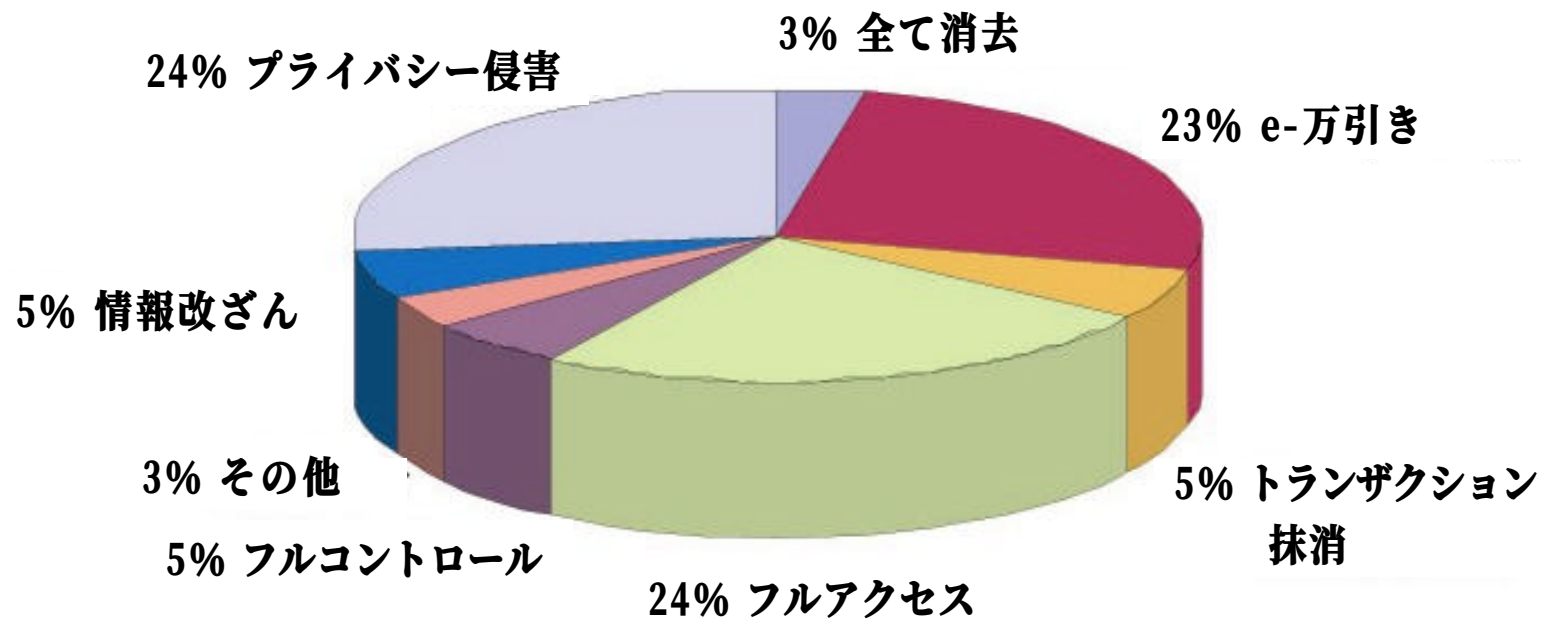
米 海軍ハッキングされる
— SecurityWatch.com,
2001年3月30日

俗説

- “自分のサイトは安全”:
 - ファイアウォールを導入している
 - データを暗号化している
 - 定期的に監査している
 - 独自のポリシーを制定している



現実 - 97% のサイトで脆弱性が認められる



*The results of over 75 AppAudits
conducted by Sanctum Inc.*

何故それが問題なのか

- 本当の脅威:
 - ハッカーとは
 - 一般的なハッカーとは髪を紫にそめた14才の少年ではなく、電子犯罪者である。
 - 自動化されたスキャナーなどのツールを使用し、パッチの当てていないサイトを見つけだす。
- 環境の現実:
 - それぞれセキュリティのノウハウのレベルが異なる、引き伸ばされたチームによって構築されている。
 - サードパーティ製品と自社開発コードとの組み合わせ。
 - 平均3日で、新しいセキュリティホールが発見される。
 - 時間がない - サードパーティ製品の最新のパッチをまだ当てていない。
- 現在の対応:
 - 機能性がつねにセキュリティに優先される。
 - Webアプリケーションレベルのセキュリティ対策は手動が最善の方法である。

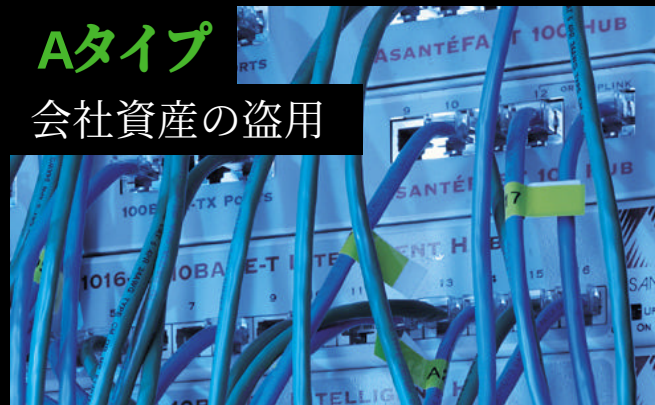
ビジネスの抱える問題 - Webアプリケーションハッキング



Webアプリケーションにおける不正行為

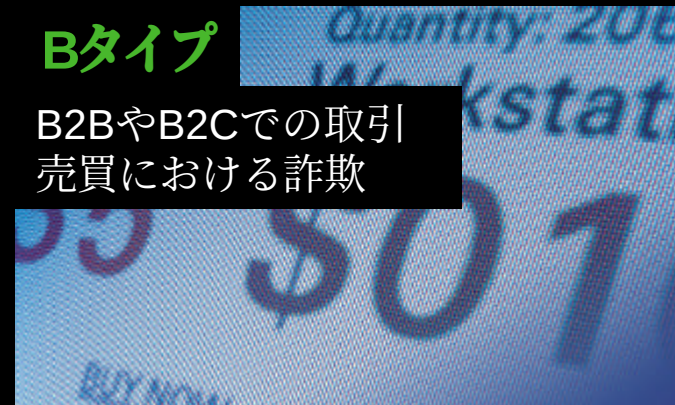
Aタイプ

会社資産の盗用



Bタイプ

B2BやB2Cでの取引
売買における詐欺



Cタイプ

顧客情報の入手

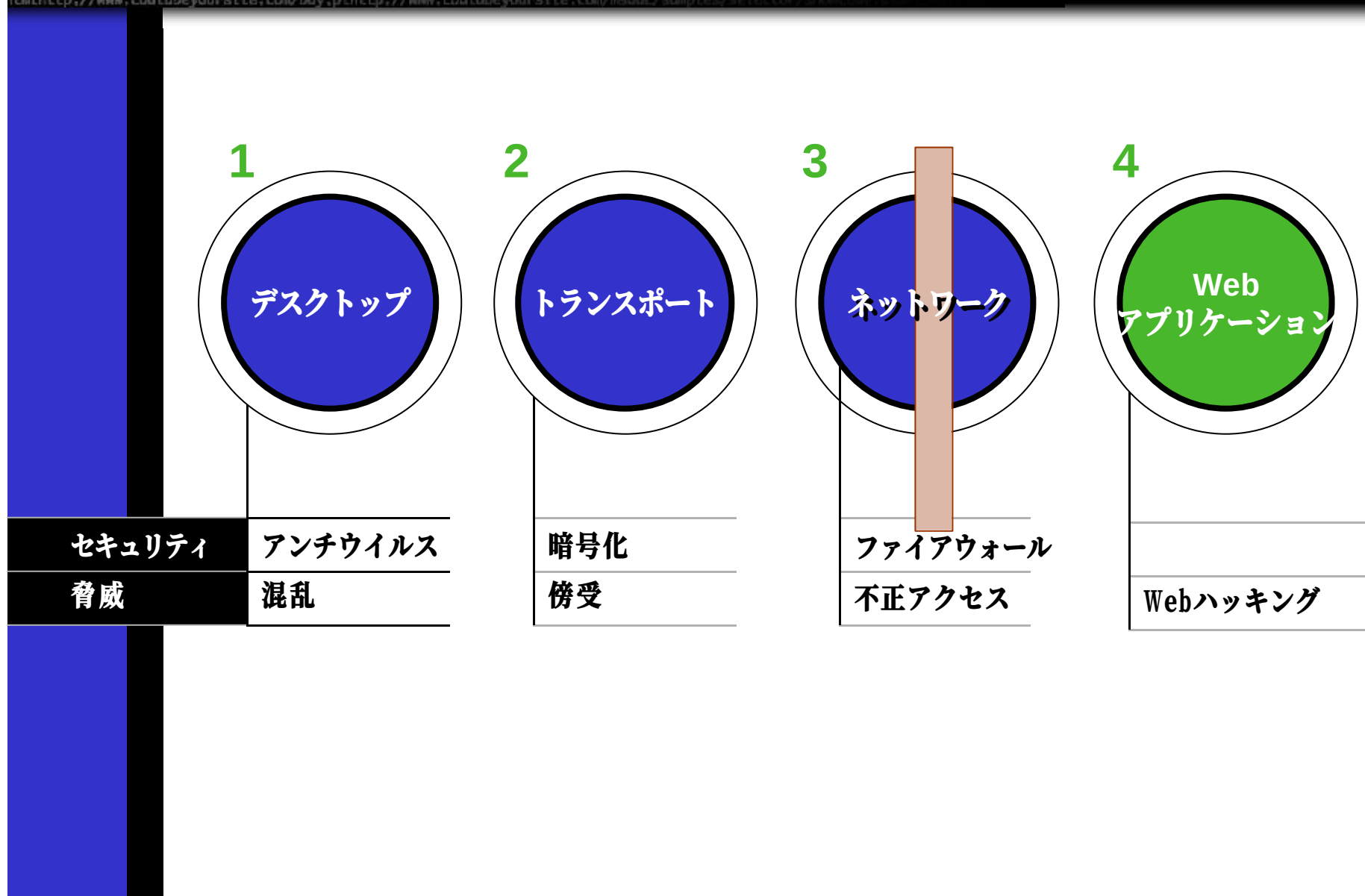


Dタイプ

サイトの改ざん



Webセキュリティにおける4つのレベル



デスクトップレベル

- アンチウイルスソフト
 - Symantec
 - Network Associates
 - Trend Micro
- パーソナルファイアウォール
 - Symantec
 - Network Ice

1

デスクトップ

セキュリティ

アンチウイルス

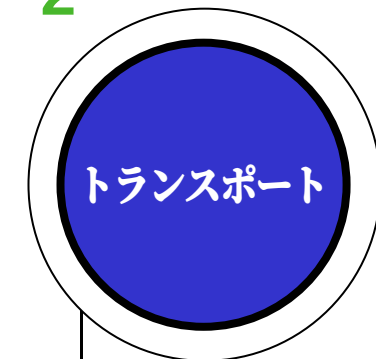
脅威

混乱

トランスポートレベル

- 暗号化
 - Virtual Private Network (VPN)
 - Entrust, Cisco, CheckPoint
 - Secure Socket Layer (SSL)
 - Netscape
- 認証局
 - デジタル証明書
 - Entrust, Verisign

2

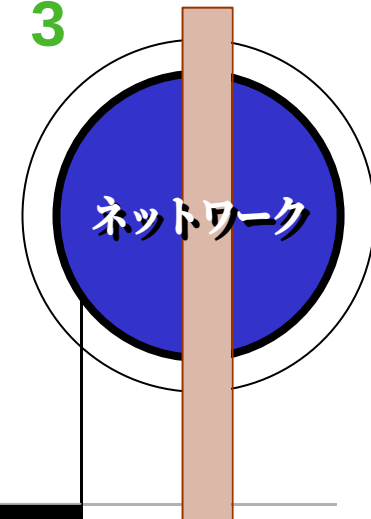


セキュリティ	暗号化
脅威	傍受

ネットワークレベル

- ファイアウォール
 - CheckPoint, Cisco, WatchGuard
- 不正侵入検知
 - ISS, Cisco, CA
- 脆弱性スキャン
 - NAI, ISS.

3



セキュリティ

ファイアウォール

脅威

不正アクセス

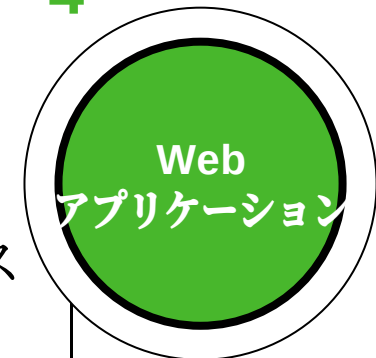
Webアプリケーションレベル

内側にある聖域:

- コンテンツ
 - スタティック、ダイナミック (アプリケーションサービス)
- データ
 - 顧客、関連企業 ...
- 自社開発コード
- サードパーティ構成要素
 - Webサーバ、アプリケーションサーバ、データベースサーバ、OS、 ...

ハッキングの60%はアプリケーションレベルで行なわれている (Gartner Group調べ)

4



セキュリティ

脅威

Webハッキング

Webアプリケーションレベルの脅威

デスクトップ

トランスポート

ネットワーク

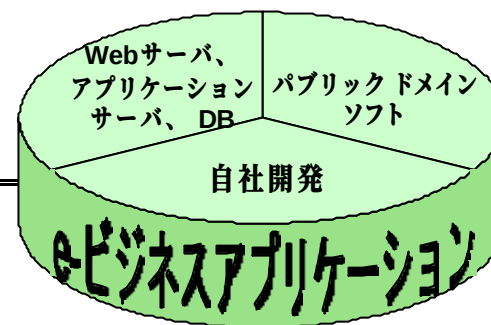
アプリケーション

アンチウイルス
(Symantec, NAI,
Trend)

デジタル証明書
(Verisign, Entrust)

SSL
(Netscape, RSA)

ファイアウォール
&
不正侵入検知
(Cisco, ISS,
Checkpoint,
Axent)



ブラウザ



Internet



一般ネットワーク
サービス
(email, ftp, nfs, ...)

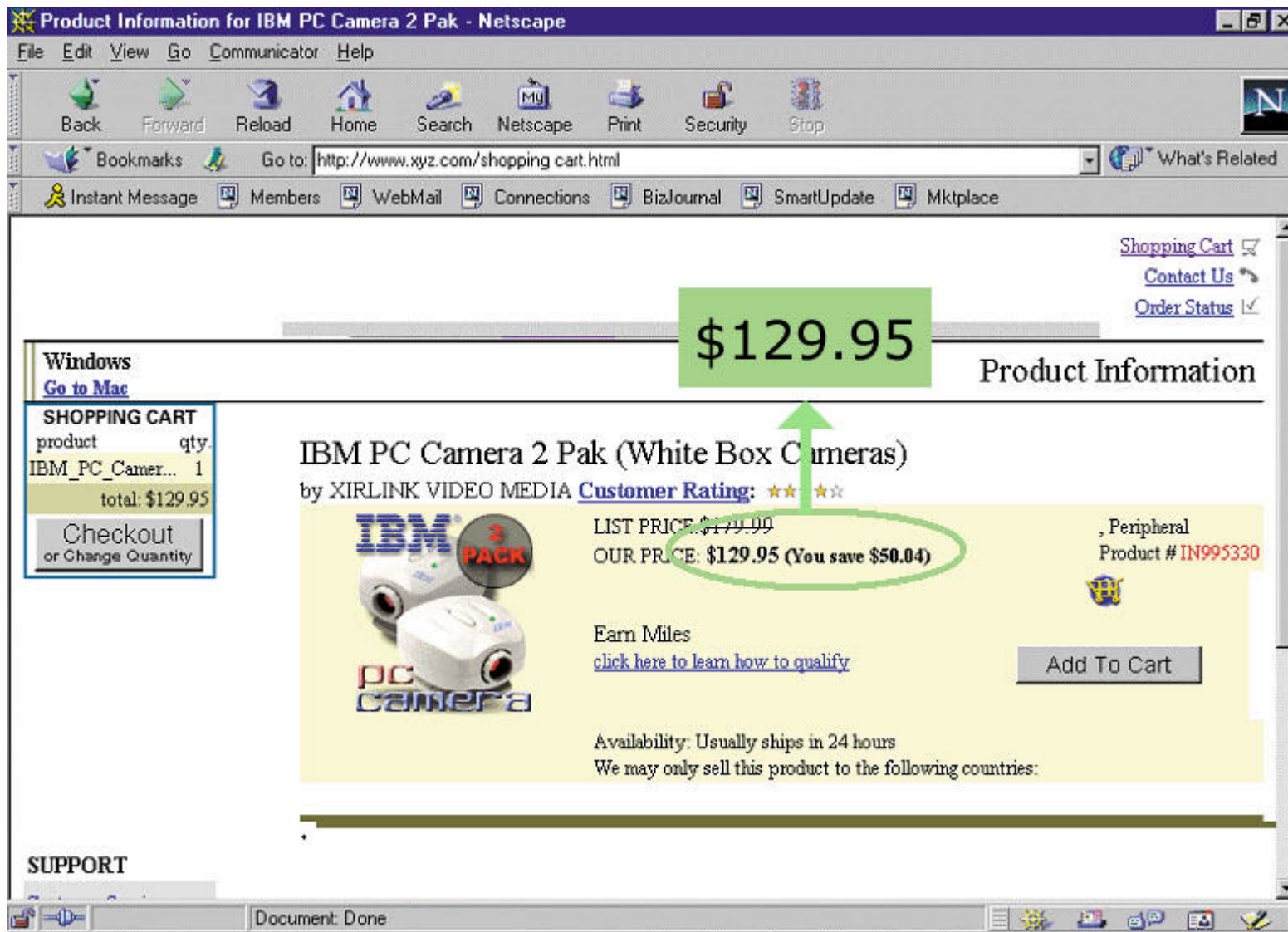


例1: 隠しフィールド

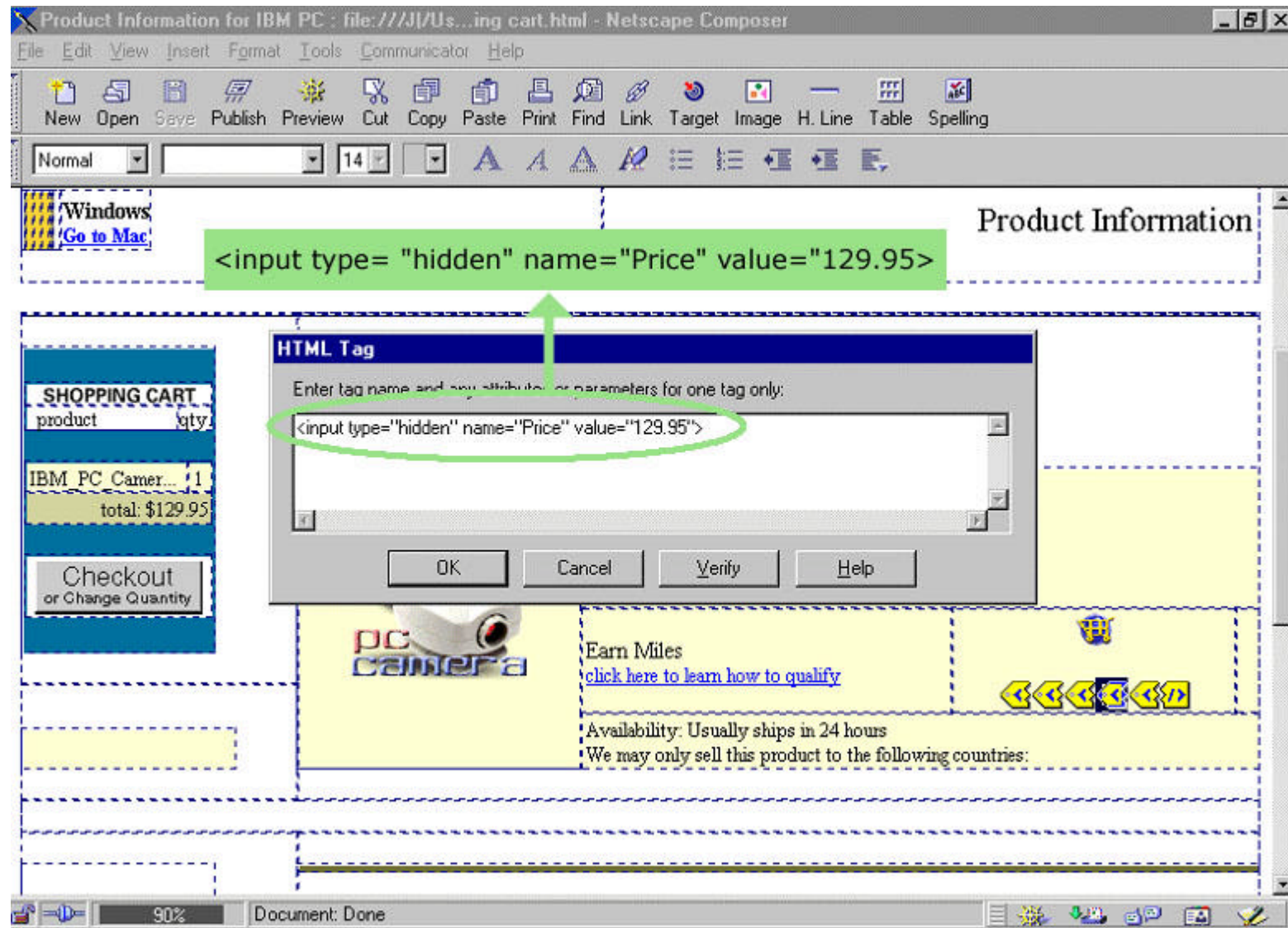
- フォームのフィールドが変更され、壊れたデータをWebアプリケーションに渡すことを許してしまう。
- オンラインショッピング
 - 価格を改ざんし商品を盗む
 - サードパーティのショッピングカートソフトでの隠しフィールド(Hidden field)のハッキング



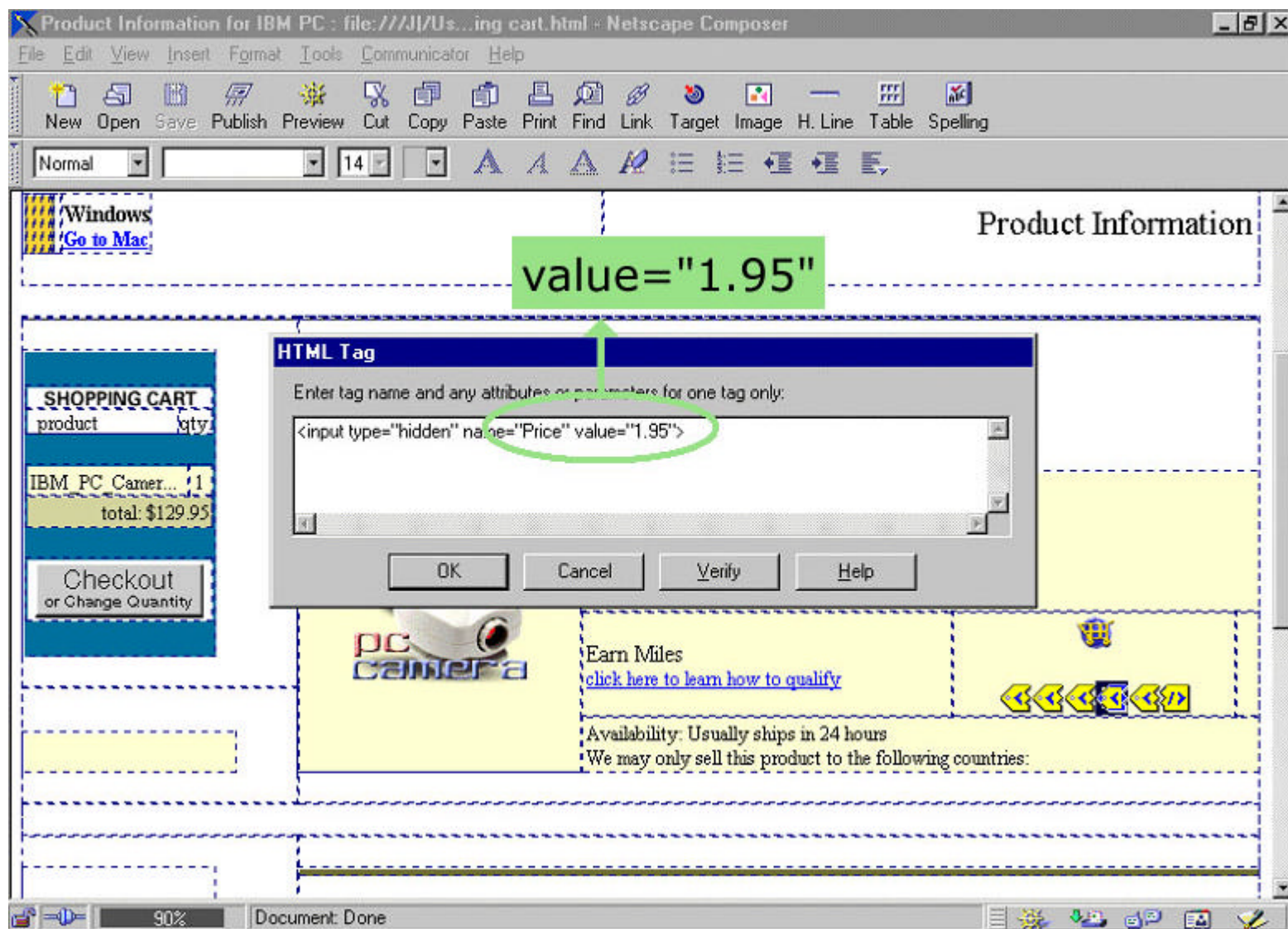
隠しフィールド - 例



隠しフィールド - 例



隠しフィールド - 例



隠しフィールド - 例

Shopping Cart

SEARCH

Your Shopping Cart Contains

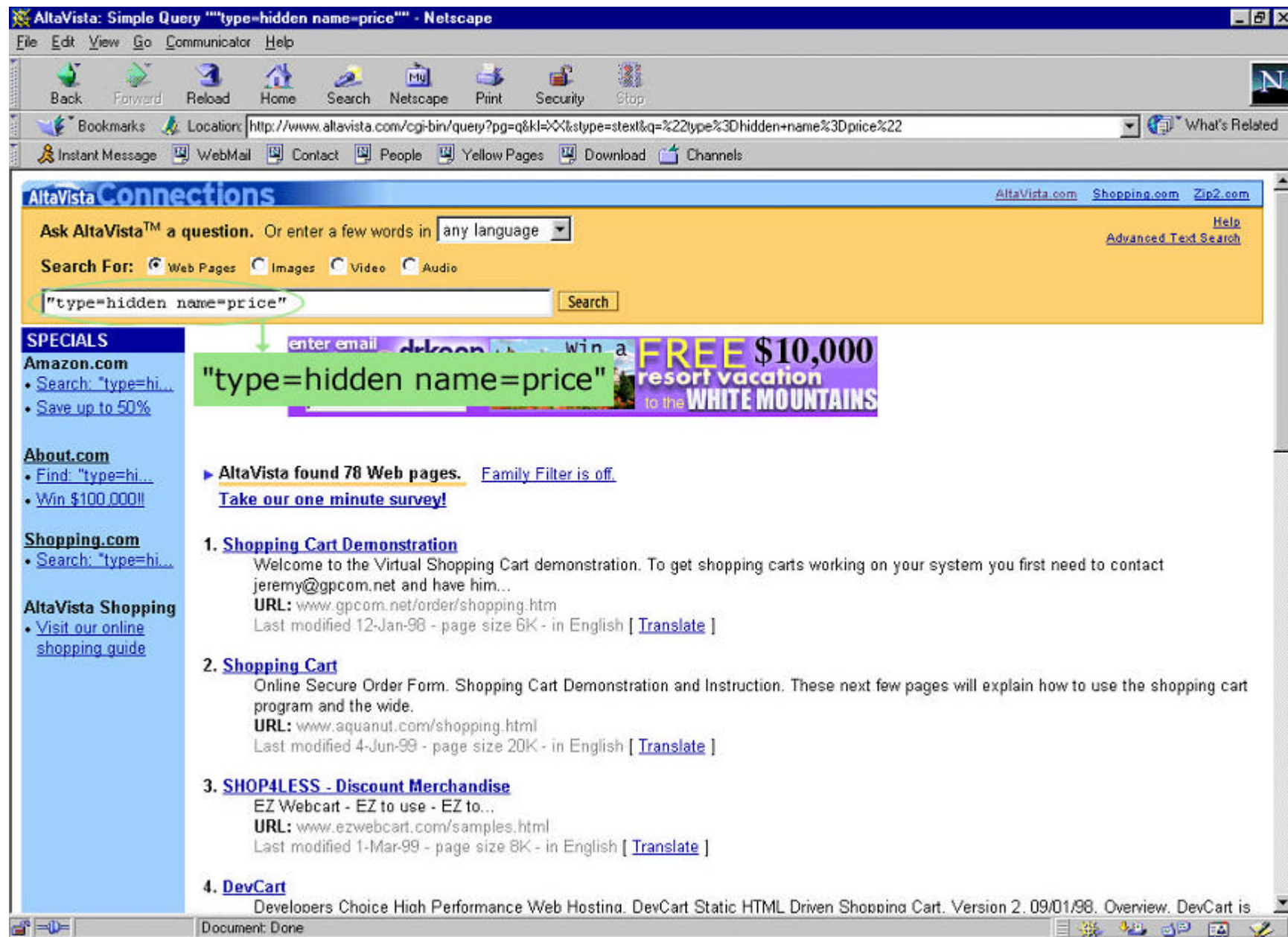
Title	Availability	Qty.	Unit Price	Total Price
IBM PC Camera 2 Pak (White Box Cameras) Peripheral	Usually ships in 24 hours	1	\$1.95	\$1.95

[Recalculate subtotal after Qty. Change.](#)

Subtotal: \$1.95

If you get an error when you try to check out, you may be behind a firewall that does not support secure transactions. If this happens, you can use our [regular server](#).

隠しフィールド - 例



バックドアとデバックオプション



- 内部開発コードに残された脆弱性が利用される。
- オンラインバンキング
 - 金銭盗難
 - デバックオプションの利用

バックドアとデバックオプション - 例

Online Banking - Account Summary - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Go to: <http://www.xxx.com/per/acctInfo/acctSum/>

Instant Message WebMail Contact People Yellow Pages Download Channels

Account Summary

Account Summary provides a snapshot of your finances.

Liquid Accounts	Account Numbers	Available Balance
Pam's Checking	9876-543XXX	\$1,916.18
John's Checking	8765-432XXX	\$1,317.10
Money Market	7888-564XXX	\$7,655.25
• Not FDIC insured • No bank guarantee • May Lose Value		
Total		\$10,888.53

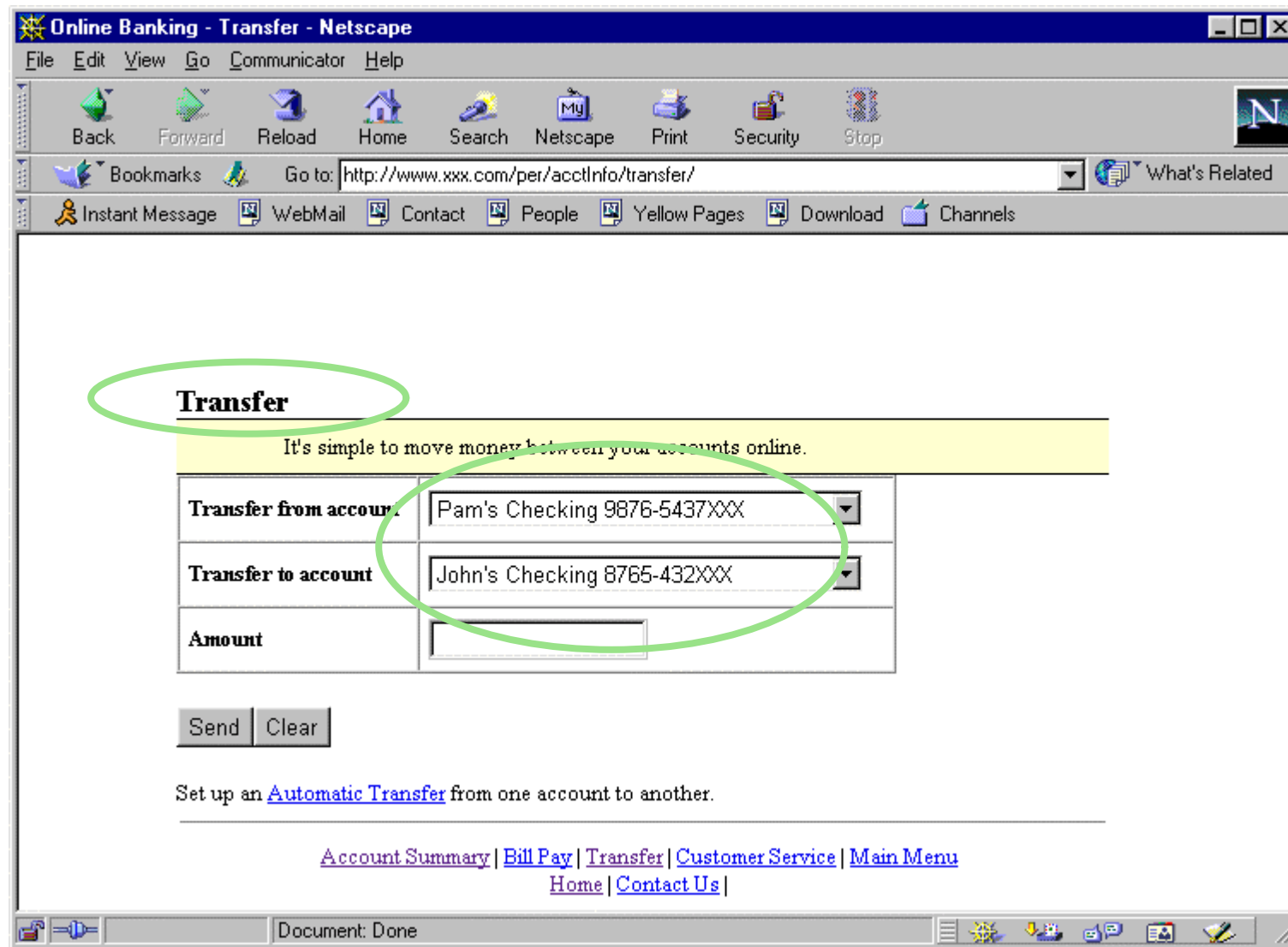
Credit Accounts	Account Numbers	Available Balance
VISA	3456-7890-XXXX-XXXX	\$4,650.49
MASTERCARD	9876-5432-XXXX-XXXX	\$1,287.52

To end your banking session, be sure to Sign Off.

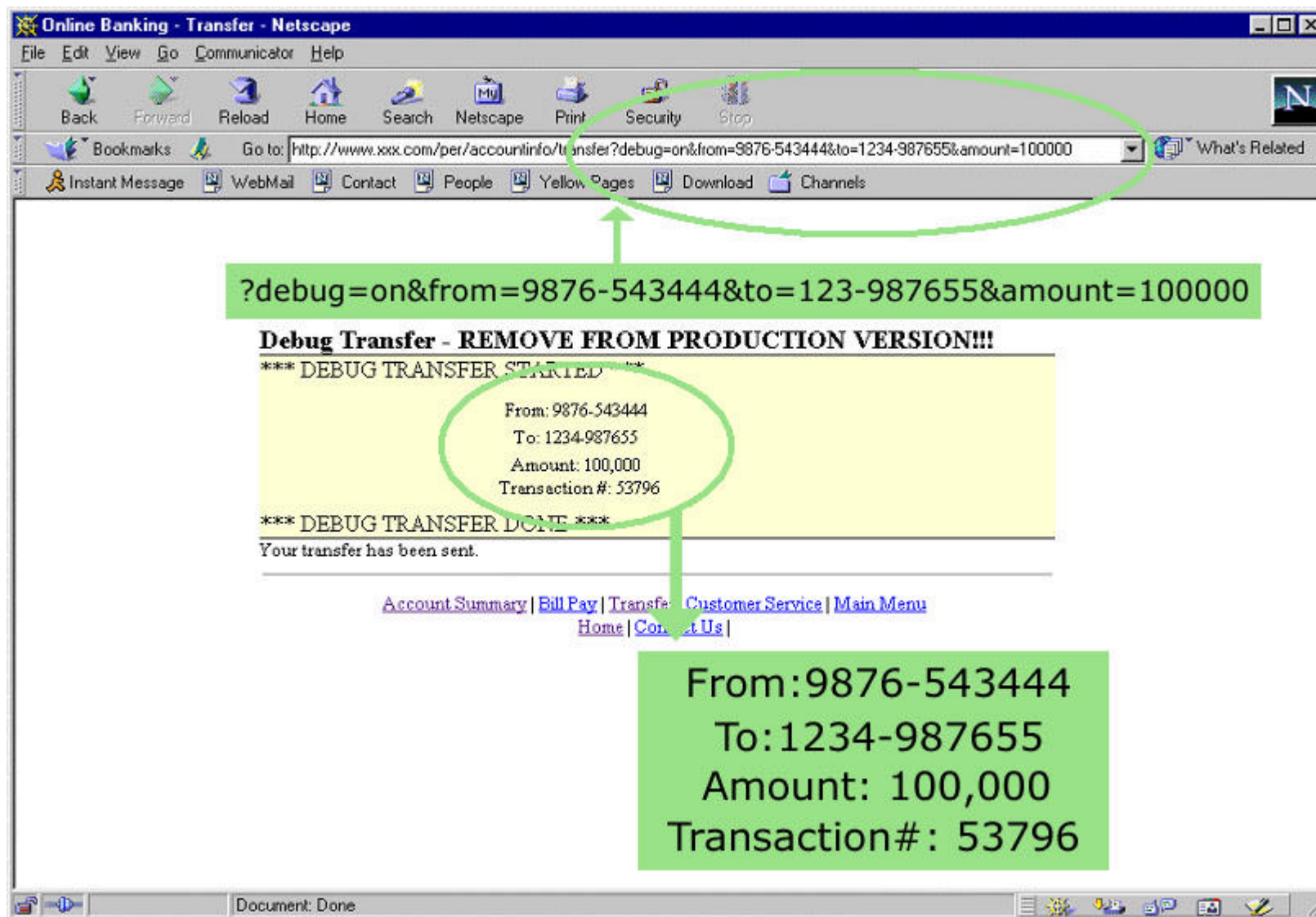
[Account Summary](#) | [Bill Pay](#) | [Transfer](#) | [Customer Service](#) | [Main Menu](#)
[Home](#) | [Contact Us](#)

Document: Done

バックドアとデバックオプション - 例



バックドアとデバックオプション - 例

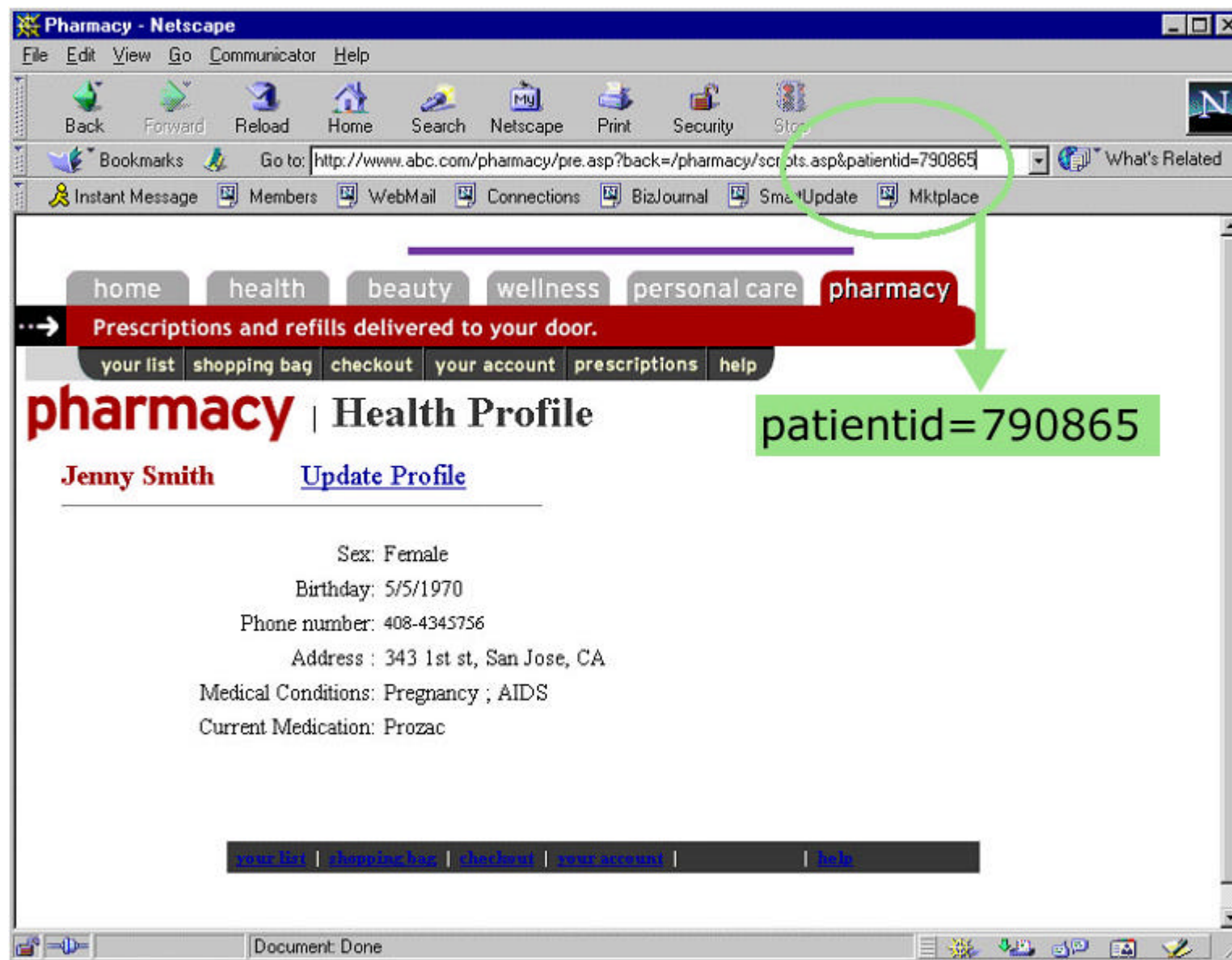


パラメータ改ざん

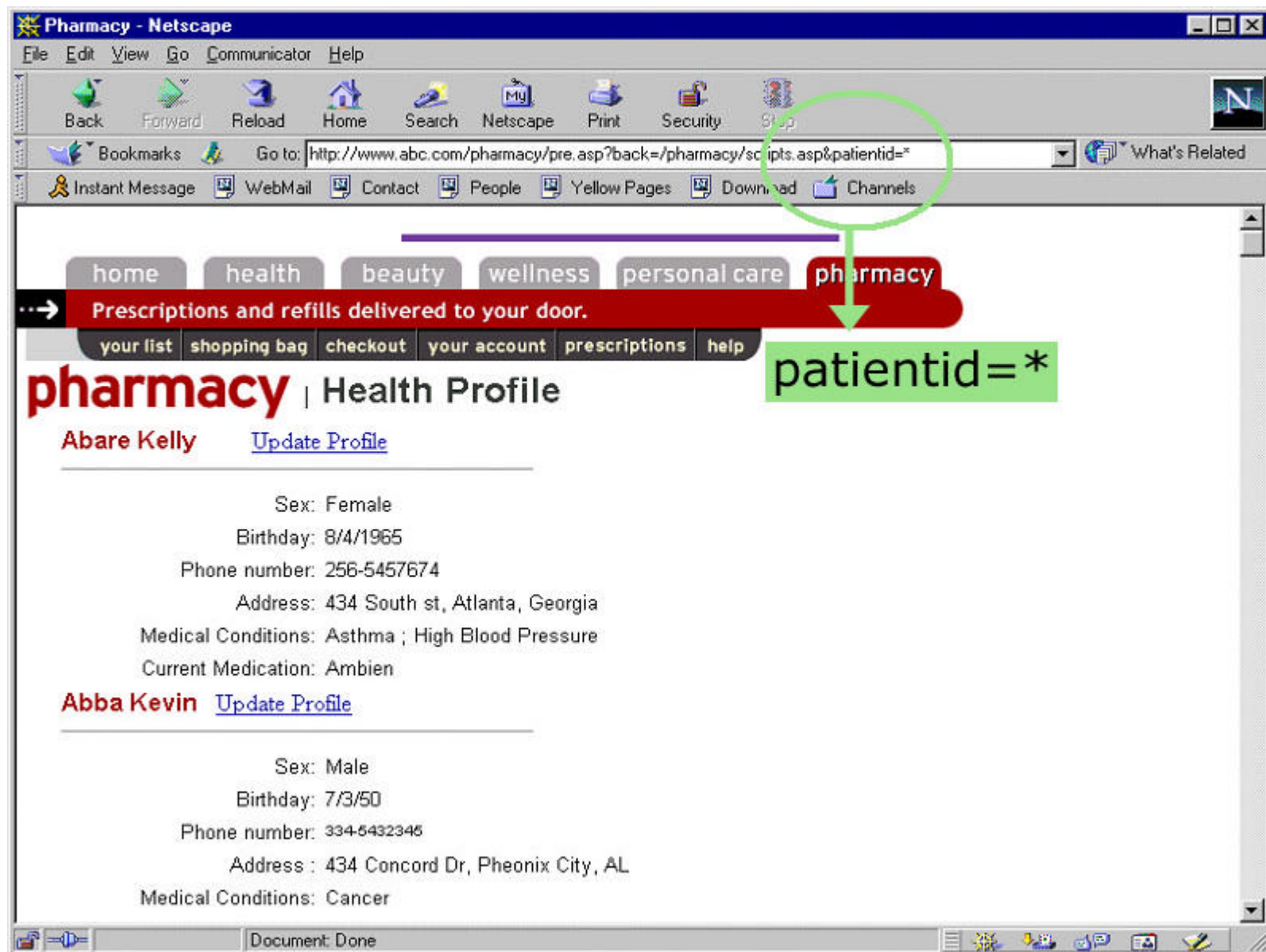


- URLの一部として送られるパラメータの改ざん
- オンライン病院（薬局）
 - メディカルレコードへのアクセス
 - CGIパラメータを使用したSQLクエリーの実行

パラメータ改ざん - 例



パラメータ改ざん - 例



アプリケーションレベルでの攻撃

- Hidden Field Manipulation (隠しフィールド)
- Parameter Tampering (パラメータ改ざん)
- Cookie Poisoning (クッキーの汚染)
- Stealth Commanding (コマンドの隠蔽)
- Forceful Browsing (強制的ブラウズ)
- Backdoors and Debug options (バックドアとデバッグオプション)
- 3rd Party Misconfiguration (サードパーティによる設定ミス)
- Cross Site Scripting (クロスサイトスクリプティング)
- Buffer Overflow (バッファオーバーフロー)
- Published Vulnerabilities (公開された脆弱性)

手動でのパッチ当て - 今日の課題

果てしない、労力と費用！

- 多岐に渡る人為的ミスの可能性
 - 開発、品質保証、オペレーション、ベンダーソフト、アウトソーシング
- 毎日のように発見されるサードパーティのバグ
 - パッチが公開されるまでサイトは危険にさらされる
- サイトの複雑性
 - 何行ものコードや、いくつかのアプリケーションの組み合わせ
- 開発者のジレンマ
 - 圧縮されたアプリケーションの開発工程
 - 市場の必要とするインパクトのある製品開発と品質保証との時間
 - 良いプログラムの実行を安全なコードでできる確率

Sanctumのソリューション

デスクトップ

アンチウイルス
(Symantec, NAI, Trend)

ブラウザ



トランスポート

デジタル証明書
(Verisign, Entrust)

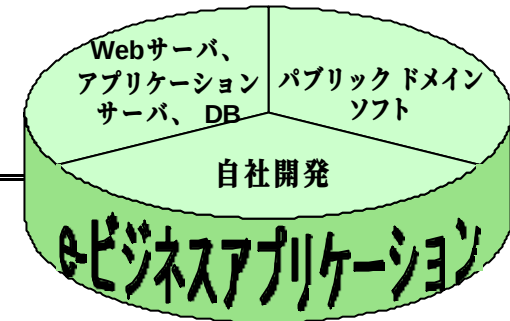
SSL
(Netscape, RSA)

Internet

ネットワーク

ファイアウォール & 不正侵入検知
(Cisco, ISS, Checkpoint, Axent)

アプリケーション



“防御”



Webアプリケーションへの不正アクセスを防御する 知性的セキュリティ基盤ソフト！

- アプリケーションレベルの全ての攻撃に対して防御し、ログを取り、アラートをあげます。
- 企業の成長しつづける電子資産を守るための、企業クラスの拡張性、運用性、相互運用性を提供します。
- 新しいサービスプロバイダーのビジネスモデルとして、信頼性と経済性の優れたアプリケーションレベルのセキュリティを提供いたします。
- すでにお持ちのファイアウォールや暗号化のテクノロジーを補完いたします。

AppShieldの仕組み

AppShieldのセキュリティポリシーとは：
Dynamic Policy Recognition (DPR)を使用しての自動作成
Policy Enforcement mechanismによる施行。

ブラウザ



Policy Recognition

Policy Enforcement

Webサーバ



Sanctumソリューション概要



- **強固な防御** – サイトをハッカーから守り、運用者に侵入試みのアラートをあげます。
 - ダイナミック vs スタティック防御
 - 自動化された**24時間×7日間**の防御
 - サードパーティ製品と自社開発コードの防御
 - 現行の開発実行に影響を与えることなくサイトの防御を可能にします。
 - 機能性にセキュリティを追加

ソリューション vs. テクニック

	教化サーバ	ホスト用 IDS	アクセス コントロール	コンテンツの 完全性	AppShield
APP. BUFFER OVERFLOW					●
COOKIE POISONING					●
CROSS SITE SCRIPTING					●
HIDDEN MANIPULATION					●
STEALTH COMMANDING					●
3 RD PARTY MISCONFIG.	●	●			●
KNOWN 3 RD PARTY VULNERABILITIES	●	●			●
PARAMETER TAMPERING					●
BACKDOORS & DEBUG OPT.					●
FORCEFUL BROWSING			●		●

結論



- 2002年には、セキュリティに対する懸念から1800万ドルのセールス損失が予測される。(連邦取引委員会の発表)
- 攻撃の60%はアプリケーションレベルで行なわれている (Gartner Group 調べ) - ファイアウォールと暗号化は必須だが、十分ではない。
- Webアプリケーションはビジネスの中心である。
- セキュリティがビジネスを加速させる！

SANCTUM はWebアプリケーションに対する不正アクセスに対して、サイトにたとえ知られていないセキュリティホールや欠陥があったとしてもそれを防衛する、始めてで唯一のセキュリティソリューション基盤です。

HINET