Microsoft

Your potential. Our passion.™

Web 時代に現れた脅威

Eiji Yoshida
Security Response Team
Microsoft Asia Limited

Summary

Web 時代に入り、数多くの Web アプリケーションや Web クライアントが企業や個人を問わずに製作され続けています。これらが製作され続けて普及するとともに、Web 時代だからこそ注目されるような新たな問題も現れています。

本セッションではクロスサイト・スクリプティングや受動的攻撃などを取り上げて、Web 時代に現れた脅威の紹介と対策を説明します。

Your potential. Our passion.™

Microsoft

本セッションの Topic

- Web 時代に現れた脅威の分類
  - Web Application Side の脅威
  - Web Client Side の脅威
  - Web Server Side の脅威
- Web 時代では、この3つに分類された脅威それぞれについてセキュリティ対策が必要

Your potential. Our passion.™

Microsoft

Web Application Side の脅威

Web Application Side

Your potential. Our passion.™

Microsoft

Web Application とは

- Web Client との通信に HTTP を使うアプリケーション
- Web Client との通信をもとに動的にコンテンツを生成するアプリケーション
- HTTP を使い Web Client にオンラインで機能を提供するアプリケーション

Your potential. Our passion.™

Microsoft

Web Application の代表例

- **Web Application の代表例**
  - インターネット・ショッピング
  - サーチ・エンジン
  - インターネット掲示板
  - **Blog**（ダイアリー）
- **URL で拡張子が .asp や .cgi と書かれているアプリケーション**

Your potential. Our passion.™

Microsoft

Web Application のメリット / デメリット

- **Web Application のメリット**
  - **Web Application は、Web Client から受け取った情報をもとにコンテンツを生成できる**
- **Web Application のデメリット**
  - **Web Application はコンテンツの生成に Web Client から受け取った情報の影響を受ける**

Your potential. Our passion.™

Microsoft

Web Application のデメリット

- Web Application のデメリットは結果として
  - Web Client から送られた悪意のある情報に誘導されて、 Web Application が悪意のあるコンテンツを生成してしまう

Your potential. Our passion.™

Microsoft

Web Application Side の脅威

- **Web Application のデメリットによる脅威**
  - クロスサイト・スクリプティング (Cross-Site Scripting)

    CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests
    http://www.cert.org/advisories/CA-2000-02

Your potential. Our passion.™

Microsoft

クロスサイト・スクリプティングとは

- **Web Application** などの動的にコンテンツを生成する仕組みの問題
- スクリプトがサイトからサイトへとクロスして実行

Your potential. Our passion.™

Microsoft

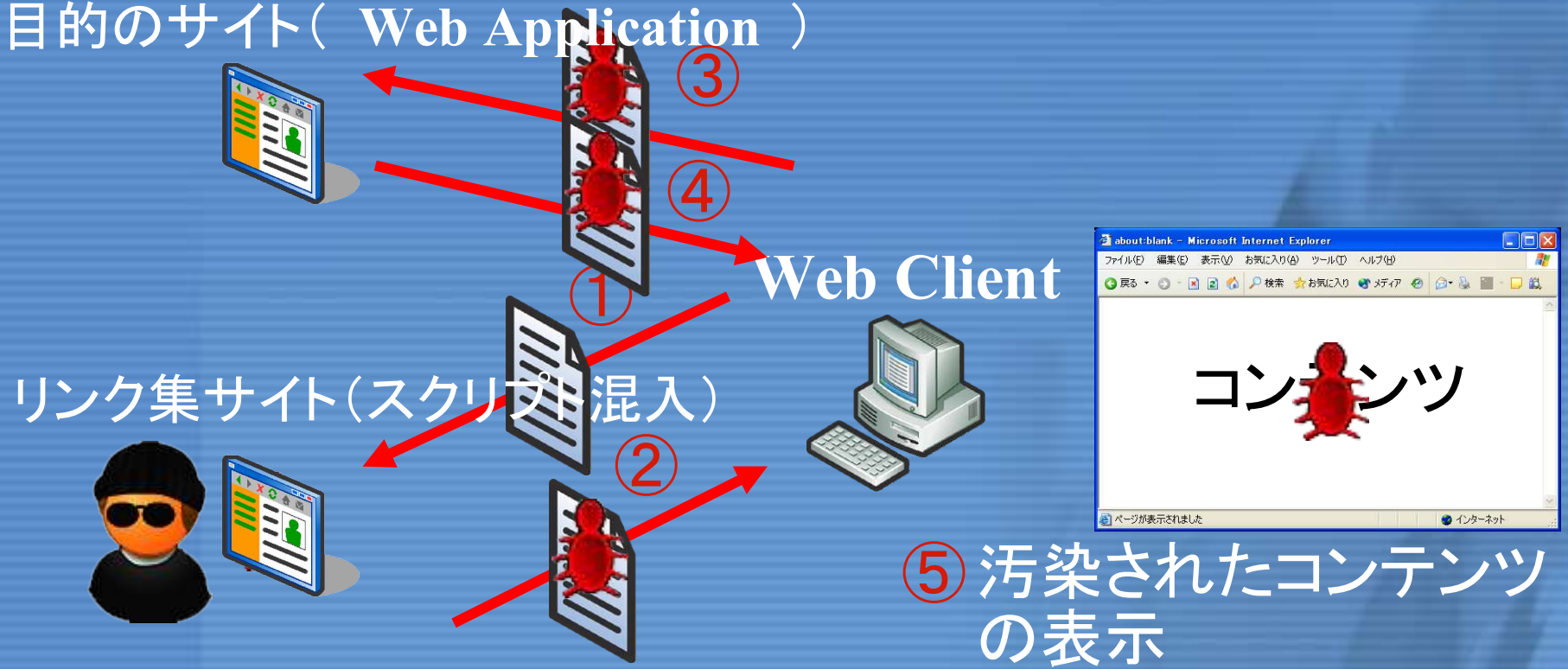
クロスサイト・スクリプティングによる問題

- 不本意なコンテンツの生成
  - 提供情報の操作
  - スクリプトの実行
    - **Cookie** の操作
- アクセス制限（セキュリティ ゾーン）の回避

Your potential. Our passion.™

Microsoft

不本意なコンテンツの生成



Your potential. Our passion.™

Microsoft

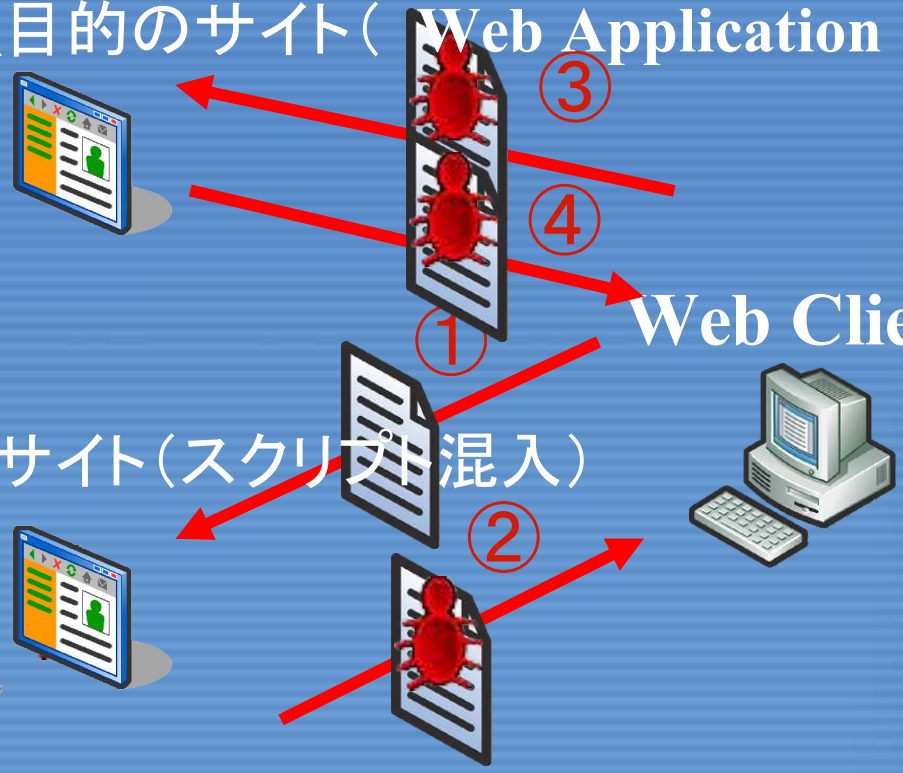
セキュリティ ゾーン

Your potential. Our passion.™

Microsoft

アクセス制限の回避

信頼する目的のサイト（ Web Application ）



信頼するサイトの
スクリプトは有効

⑤ 埋め込まれていた
スクリプトを実行！

Your potential. Our passion.™

Microsoft

クロスサイト・スクリプティング対策

- スクリプトの無効化（サニタイジング）
  - メタ文字を置換して無効化
    - 「 < 」→「 < 」
    - 「 > 」→「 > 」
    - 「 & 」→「 & 」
  - 埋め込む場所にあわせて入力情報を無効化（タグ属性やURL属性などで必要な処理が異なるため）
  - 無効化判定と無効化処理はコンテンツ出力時

Your potential. Our passion.™

Microsoft

Web Client Side の脅威

Web Client Side

Your potential. Our passion.™

Microsoft

Web Client とは

- Web ブラウザと呼ばれるアプリケーション
- Web Application や Web Server との通信に HTTP を使うアプリケーション
- HTML を解釈して Web コンテンツを表示するアプリケーション

Your potential. Our passion.™

Microsoft

Web Client の代表例

- **Microsoft Internet Explorer (Microsoft Corporation)**
- **Opera Web Browser (Opera Software ASA)**
- **Netscape Navigator (Netscape Communications Corporation)**

Your potential. Our passion.™

Microsoft

Web Client のメリット / デメリット

- **Web Client のメリット**
  - **Web Application や Web Server から送られてきた情報を Web Client が処理して、Web コンテンツとして表示する**
- **Web Client のデメリット**
  - **Web Application や Web Server から送られてきた情報を Web Client が処理する際に、問題が発生しやすい**

Your potential. Our passion.™

Microsoft

Web Client Side の脅威

- **Web Client のデメリットによる脅威**
  - 受動的攻撃

受動的攻撃検証サイト
http://zaddik.hp.infoseek.co.jp/

Your potential. Our passion.™

Microsoft

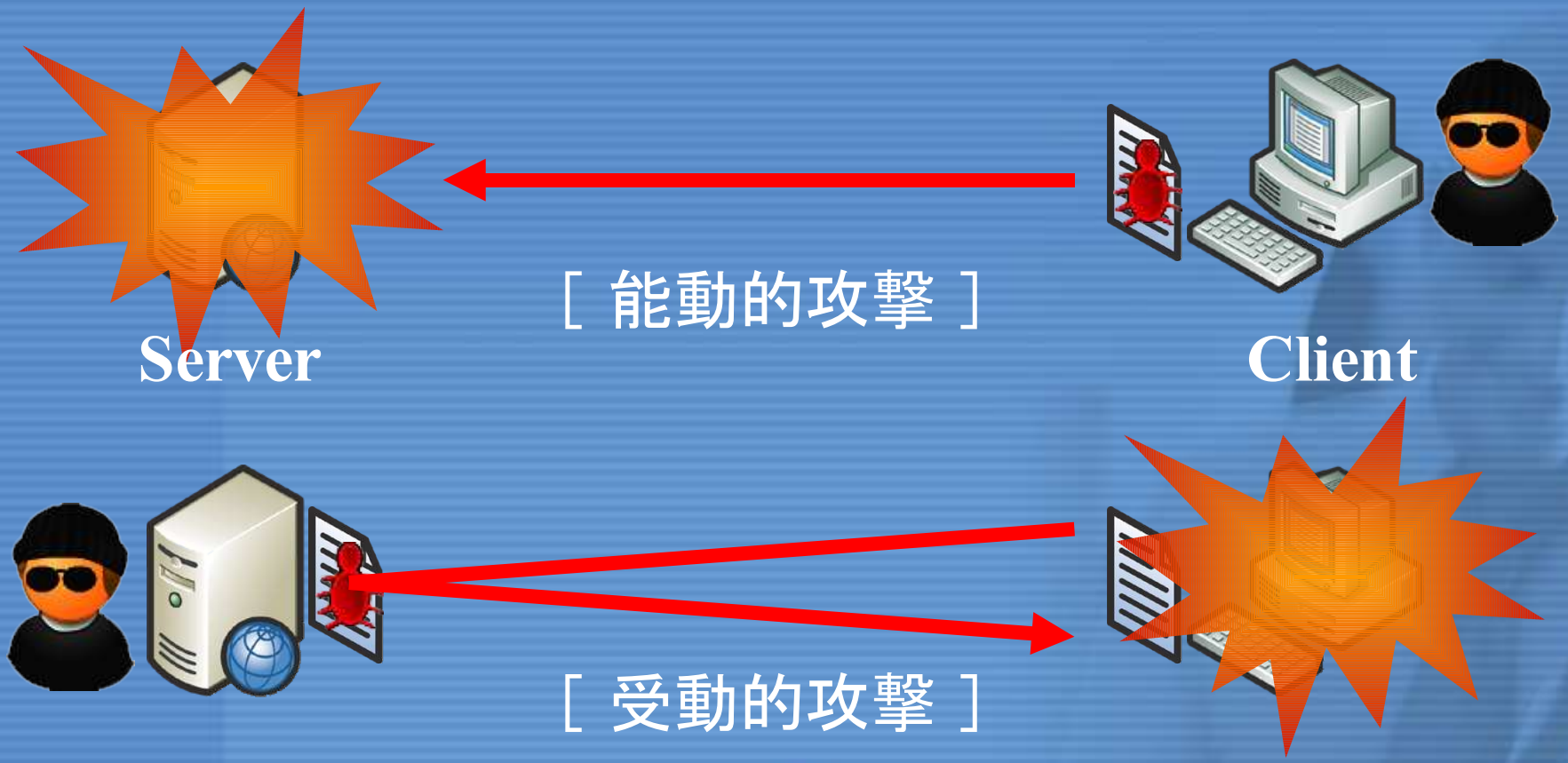
受動的攻撃とは

- ユーザからの要求に対して悪意のある情報を送り込む攻撃
  - 能動的攻撃（従来の攻撃）
    攻撃側が起点となる攻撃
  - 受動的攻撃
    攻撃対象が起点となる攻撃

Your potential. Our passion.™

Microsoft

能動的攻撃と受動的攻撃



Your potential. Our passion.™

Microsoft

受動的攻撃による問題

- Web ページや HTML メールの表示による被害の発生
  - ウイルスの感染
  - コマンドの実行
- アクセス制限の回避
  - ファイアウォールの無効化
  - 社内ネットワークの侵入

Your potential. Our passion.™

Microsoft

Web ページ表示による被害発生

- 「不適切な MIME ヘッダーが原因で Internet Explorer が電子メールの添付ファイルを実行する (MS01-020) 」を悪用し、Web ページや HTML メールを表示するだけで添付ファイルを実行
  - Nimda ワーム (2001/9)
  - Swen ワーム (2003/9)

※ 修正プログラム MS01-020 (2001/4)

Your potential. Our passion.™

Microsoft

アクセス制限の回避

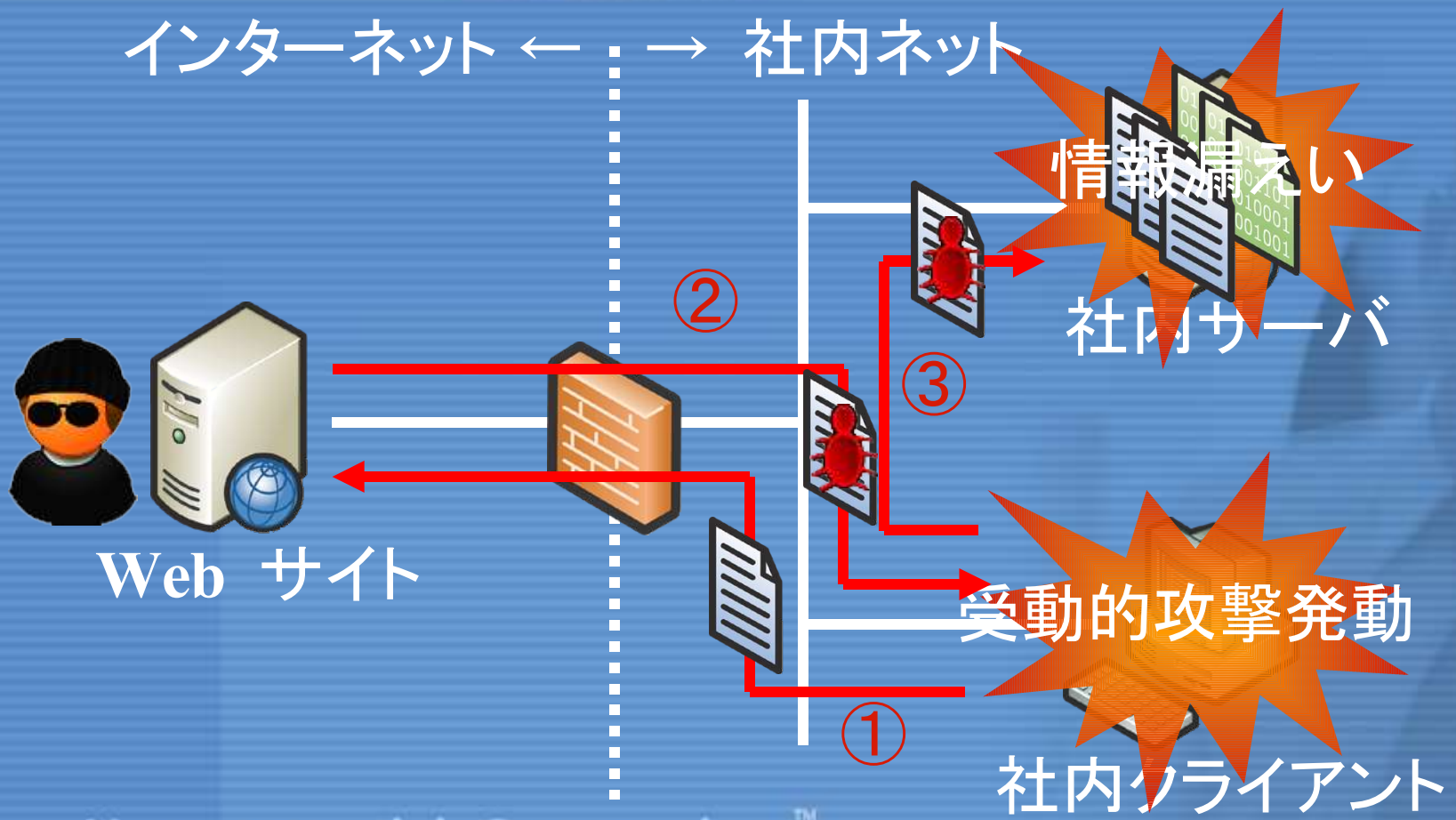
- 攻撃対象を起点として攻撃を開始することで、ファイアウォール等に登載されているパケットフィルタリングを回避
  - ファイアウォールのアクセス制御設定

インターネット → 社内ネット	×
社内ネット → インターネット	○
社内ネット → インターネット → 社内ネット	

Your potential. Our passion.™

Microsoft

アクセス制限の回避



Your potential. Our passion.™

Microsoft

受動的攻撃対策

- 修正プログラムを適用する
- ブラウザのセキュリティ設定を使い各種機能を厳しく制限する
- **Administrator** などの管理者ユーザで **Web** ページを閲覧しない
- ウイルス対策ソフトウェアをインストールする

Your potential. Our passion.™

Microsoft

Web Server Side の脅威

Web Server Side

Your potential. Our passion.™

Microsoft

Web Server とは

- Web Application や Web Client との通信に HTTP を使うサービス
- Web ページ や Web Application といったリソースを管理するサービス

Your potential. Our passion.™

Microsoft

Web Server の代表例

- Microsoft Internet Information Services (Microsoft Corporation)
- Apache HTTP Server (The Apache Software Foundation)
- Netscape Enterprise Server (Netscape Communications Corporation)

Your potential. Our passion.™

Microsoft

Web Server Side の脅威

- FrontPage Server Extensions の設定ミスを悪用した Web コンテンツの改ざん
  - FrontPage Server Extensions

    FrontPage Server Extensions
    http://msdn.microsoft.com/library/en-us/d

Your potential. Our passion.™

Microsoft

FPSE とは

- Web Server にリモートでのコンテンツ作成や管理といった機能を拡張するプログラム
- Microsoft Office FrontPage やネットワーク プレースを使ったコンテンツ管理が可能
- FrontPage やネットワーク プレースと FrontPage Server Extensions 間は HTTP による通信

Your potential. Our passion.™

Microsoft

FPSE の設定についての注意点

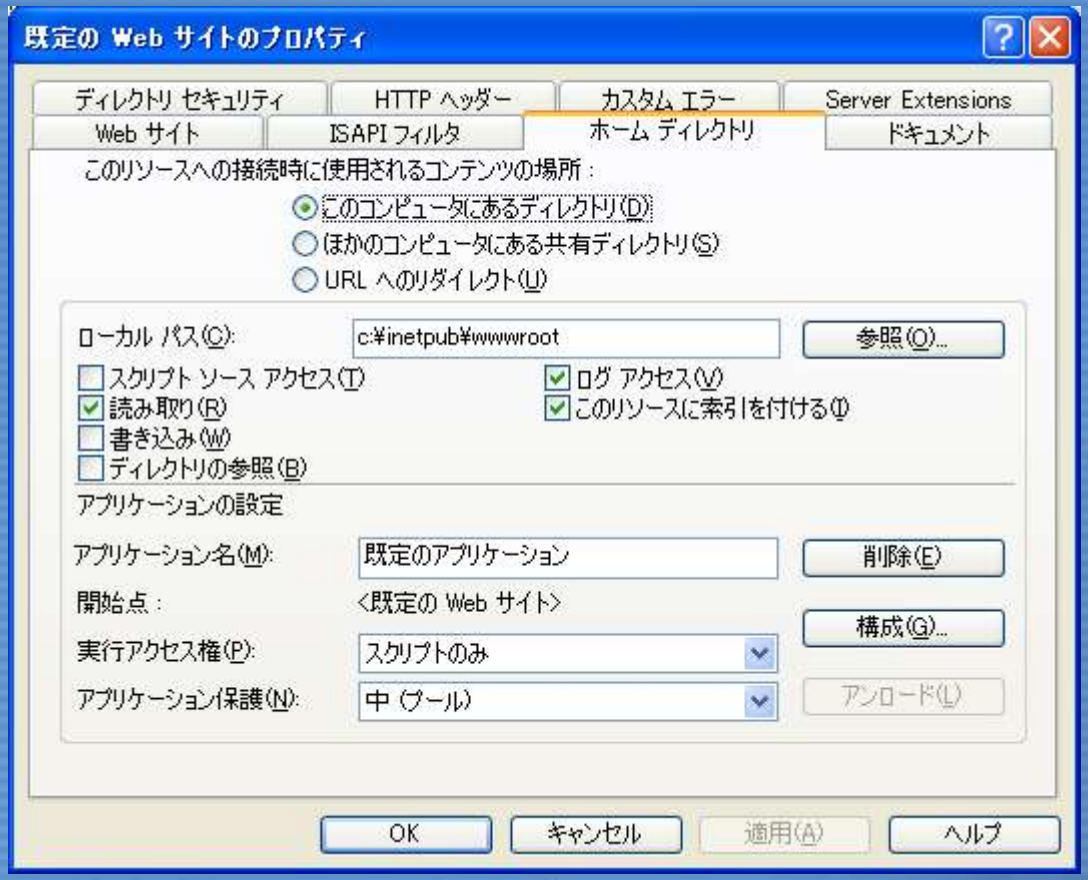
- リモートでのコンテンツ作成や管理といった FPSE の機能を悪用したコンテンツ改ざん
  - コンテンツの作成や管理に必要なアクセス権

FPSE	NTFS アクセス権
WebDAV	NTFS アクセス権 IIS アクセス権（書き込み）

Your potential. Our passion.™

Microsoft

IIS アクセス権



Your potential. Our passion.™

Microsoft

対策の注意点

- HTTP 通信を通すように設定されたパケットフィルタリングでは FPSE の設定ミスを悪用した改ざんは防ぐことができない
- IIS のアクセス権で「書き込み」を外しても FPSE の設定ミスを悪用した改ざんは防ぐことができない
- 全ての修正プログラムをインストールしても FPSE の設定ミスを悪用した改ざんは防ぐことができない

Your potential. Our passion.™

Microsoft

FPSE 設定ミスによる改ざんの対策

- FPSE を使用しないならアンインストール
- Web コンテンツとなるフォルダやファイルに適切な NTFS アクセス権を設定
  - IIS のディレクトリ セキュリティで匿名アクセスを許している場合は、匿名で使用するユーザーに NTFS アクセス権で「書き込み」や「変更」を与えない
    ※ 初期設定では与えられていない！

Your potential. Our passion.™

Microsoft

まとめ

- Web 時代では、従来のように Web Server だけをセキュアにするのではなく、Web Application や Web Client もセキュアにすることが必要
- Web 時代では、 Web Server の管理者だけではなく、 Web Application を作成するプログラマーも、 Web Client を使う一般ユーザーもセキュリティを勉強することが必要

Your potential. Our passion.™

Microsoft

行っていただきたいこと

- コミュニティなどに参加して、セキュリティ業界の人と交流を
  - セキュリティに関する情報や考え方に注目
- あとでセキュリティではなく、まずはセキュリティを
  - セキュリティは付け足すよりも、セキュアに設計するほうが効率的かつ効果的

Your potential. Our passion.™

Microsoft

行っていただきたいこと

- セキュアだと「思う」のではなく、セキュアであることの「確認」を
  - 確認をせずにセキュアだと思い込むことは危険

Your potential. Our passion.™

Microsoft

ぜひ読んでください！

- セキュリティ管理 - 基本のトレードオフ：
  http://www.microsoft.com/japan/techn
- Windows2000 セキュリティ強化ガイド：
  http://www.microsoft.com/japan/techn

Your potential. Our passion.™

Microsoft

ぜひ読んでください！

- マイクロソフト の Securing Windows 2000 Server ソリューション：
  http://www.microsoft.com/japan/techn
- Windows Server 2003 Security Guide：
  http://www.microsoft.com/japan/techn

Your potential. Our passion.™

Microsoft