HP IceWall SSO

HP IceWall技術レポート：セキュリティ対策特集（1）

HP IceWall SSOのCrossSite Scripting,バッファオーバフロー、セッションハイジャック対策

» 守りを固めるTurn Key Solution !! – HP IceWall SSO＆PKI(Onsite) –
撃退!!FireWallを越えるアプリケーションレベル攻撃

»

HP IceWall SSOはミッションクリティカルな都銀のインターネットバンキング、企業間金融商取引でも使用され、そのセキュリティ機能に絶大な信頼を頂いております。その理由はどこにあるのでしょうか？今回はアプリケーションレベルの攻撃対策という観点から、HP IceWall SSOをご紹介します。

アプリケーションレベルWeb攻撃の猛威

昨今Webの世界を騒がせる、FireWallも通過してしまうアプリケーションレベルでのWeb攻撃。「FireWallを導入している、データを暗号化している、セキュリティ診断を受けた、不正アクセスを監視している」もはや、こうした対策だけでは容赦のない攻撃にされされる時代が訪れ、管理者の頭痛の種となっていることと思います。

聞き覚えのあるこれら。全てFireWallを越える攻撃なのです！！

Hidden Field Manipulation（隠しフィールド）
Parameter Tampering（パラメータ改ざん）
Cookie Poisoning（クッキー改ざん）
Stealth Commanding（コマンドの隠蔽）
Forceful Browsing（強制ブラウズ）
Debug Option(デバッグオプション)
Buffer Overflow（バッファオーバフロー）
CodeRed, Nimda（Webサーバウィルス）
CrossSite Scripting（クロスサイトスクリプティング）

例えば、ポート80への攻撃。Nimda。
HP IceWall SSOがなければ、最新のセキュリティパッチを当てるしかありません。
Nimdaに感染したWebサイトへアクセスしたPCは、Nimdaに感染したPCはメールソフトのアドレス帳の宛先に自動でウィルスメールを送付、PC同士に感染させます。また、PCがネットワークに接続していると、共有ドライブに接続しているネットワーク内PCやサーバ、セキュリティパッチの当たっていないIISがあるとその脆弱性につけこんでNimdaに感染させます。また、IISがCodeRed Ⅱに感染していた場合はそのバックドアを利用し、Nimdaに感染させます。
つまり、FireWallだけではWebサーバを守りきれないのです。

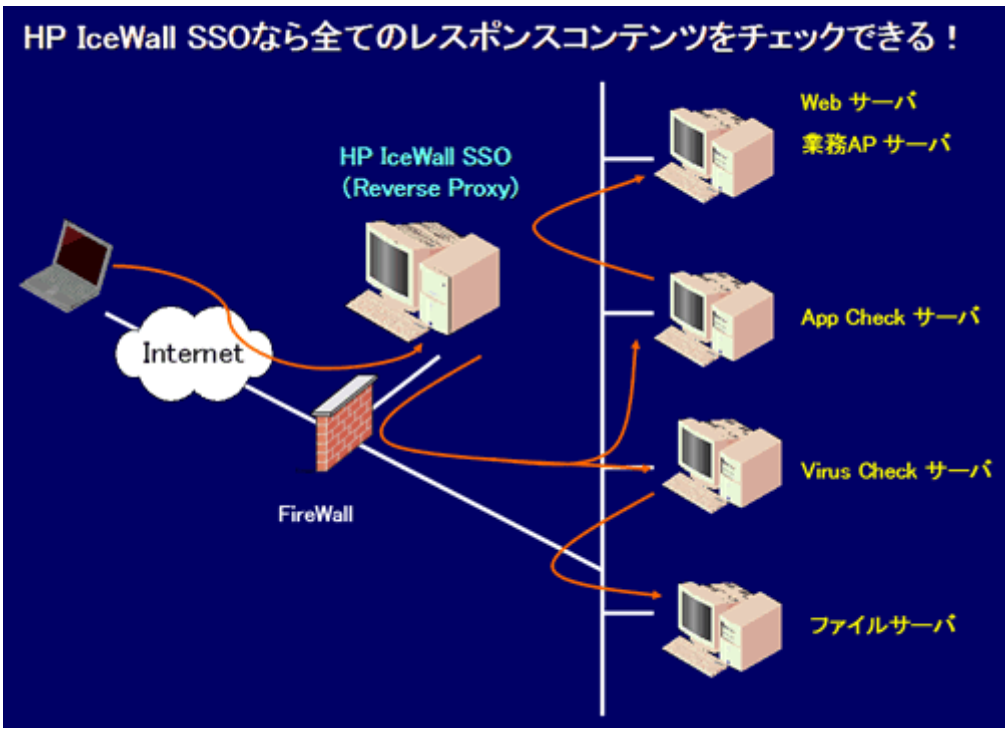
次に、クロスサイトスクリプティング（CSS）。
例えば、クッキーを奪うスクリプトを埋め込んだリンクを書き込んだ悪意のあるサイトにユーザがアクセスすると、クッキーがPCのハードディスクに保存され、再度そのリンクをクリックするとスクリプトが実行され、PCのハードディスクに保存されているクッキーが悪意のあるサイトに送られてしまいます。
FireWallは、CSSに全く効果を発揮することができません。
これらを防ぐには、アプリケーション側で全ての入力フィールドのチェックを行う必要があります。

金融商取引にも採用されるセキュリティ。だからHP IceWall SSO！！Nimdaもクロスサイトスクリプティングも防ぎます

1. HP IceWall SSOなら全てのレスポンスコンテンツをチェック＆変換できる！
2. リクエストヘッダー、レスポンスコンテンツ内の悪意スクリプトを検知
3. 4つのフィルタ機能がクロスサイトスクリプティングからWebサイトを保護！
4. データサイズ制限機能で、バッファオーバフロー対策も万全！
5. セッションハイジャック対策？HP IceWall SSOにお任せください

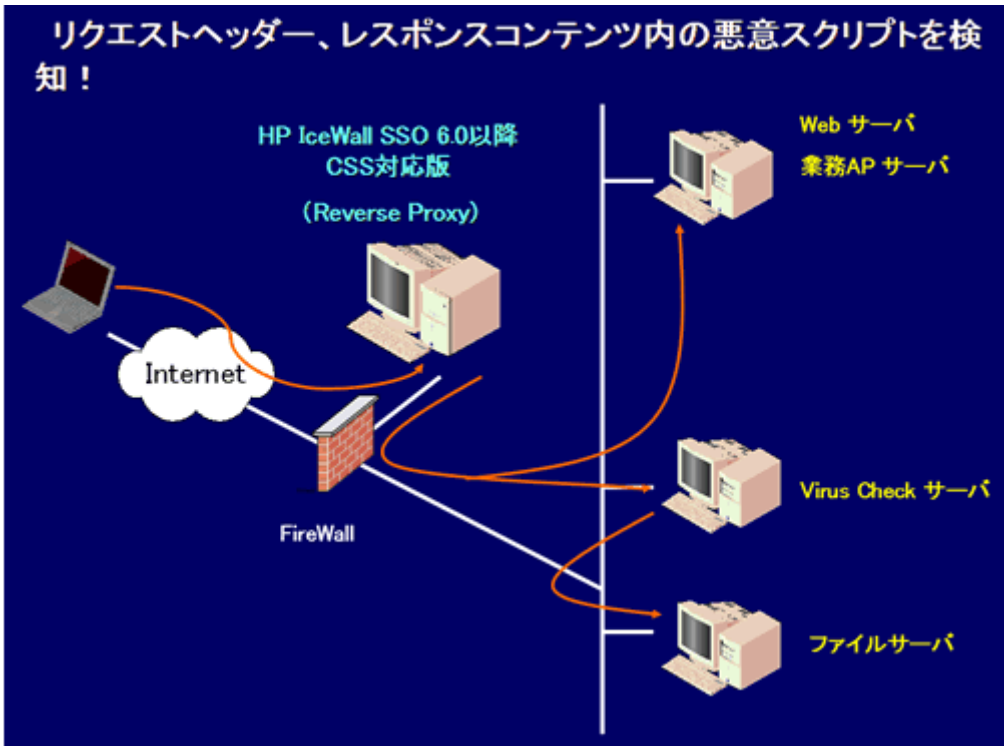
1. HP IceWall SSOなら全てのレスポンスコンテンツをチェック＆変換できる！

HP IceWall SSOは、リバースプロキシ型のシングルサインオン製品。
アプリケーション側で全ての入力フィールドをチェックしなくても、HP IceWall SSOを前段に配置することで全てのトランザクションがHP IceWall SSOを経由するようになり、HTTPリクエストやHTMLなどのレスポンスコンテンツをチェック、変換することが可能です。



2. リクエストヘッダー、レスポンスコンテンツ内の悪意スクリプトを検知！

既にご紹介した通り、HP IceWall SSOはHTTPリクエストやHTMLなどのレスポンスコンテンツをチェックすることができます。
この機能を使用し、リクエストヘッダーやレスポンスコンテンツ内の悪意のあるスクリプトを検知することが可能。クロスサイトスクリプティング（CSS）防御対策としても有効です。（HP IceWall SSO ver.6.0以降）アップロード＆ダウンロードするファイルのウィルス検知については、ウィルスフィルタリング機能を有する製品と組み合わせてご使用頂くと効果的です。
また、アプリケーションチェックサーバを併用し、機能を補完することをお勧めします。



3．4つのフィルタ機能がクロスサイトスクリプティングからWebサイトを保護！

HP IceWall SSO ver.6.0より、CSS対応として4つのフィルタ機能が追加されました。

1. GET送信データフィルタ （QUERY_STRING規制）
   GETリクエスト内のタグ(Script等)にフィルタをかけることが可能

2. POST送信データフィルタ(POSTDATA規制)
   POSTリクエスト内のタグにフィルタをかけることが可能

3. HTMLフィルタ(タグ規制)
   バックエンドWebサーバから受信するコンテンツ内のタグにフィルタをかけることが可能

4. ホストフィルタ(ホスト規制)
   バックエンドWebサーバから受信するコンテンツ内のURLにフィルタをかけることが可能

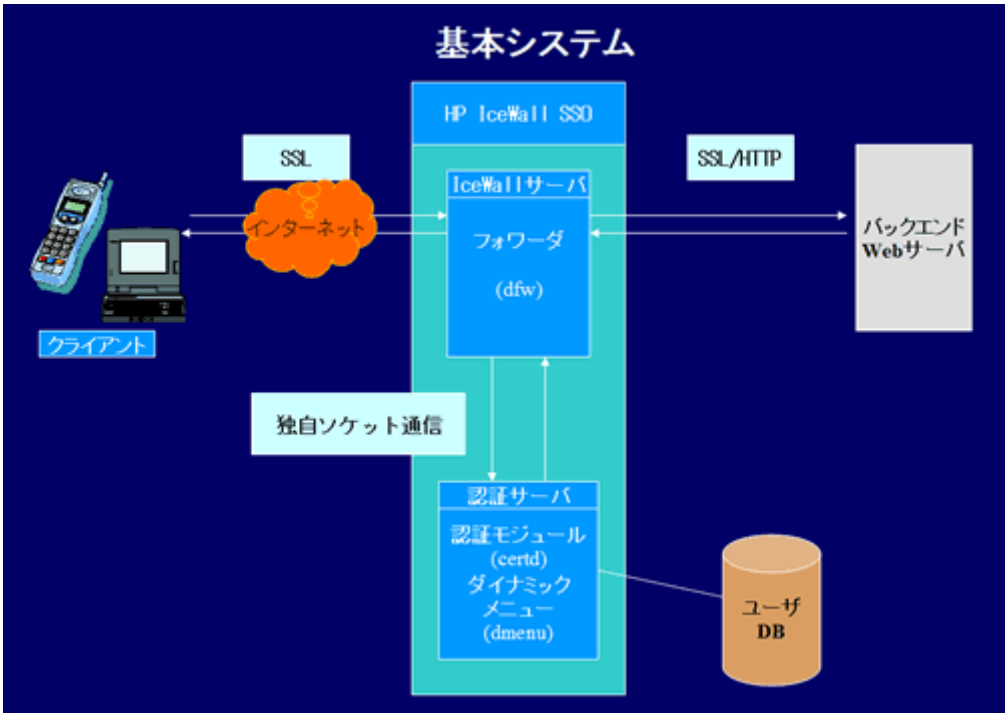
4．データサイズ制限機能で、バッファオーバフロー対策も万全！

HP IceWall SSO ver.6.0より、バックエンドWebサーバ(IIS等)へのデータサイズ制限機能が追加されました。CodeRed等のバッファオーバフロー対策も万全です。

1. バックエンドWebサーバへのリクエストURLの長さを制御できる(PATH_INFOの最大長を設定できる: MAXURL)
2. バックエンドWebサーバへのQueryStringの長さを制御できる(QUERY_STRINGの最大長を設定できる: MAXQUERY)

5．セッションハイジャック対策？HP IceWall SSOにお任せください！

セッションIDを盗まれ、本人に成り済まされ、不正行為が行われるのがセッションハイジャック。HP IceWall SSO ではすべての通信をHTTPS化して行っているため、セッションハイジャックをされる心配はありません。また、次期バージョンではクッキーにセキュア属性を付加することも可能に。



HP IceWall SSO構築にあたっては、経験豊富なセキュリティコンサルタント、技術者が万全の体制でサポートいたします。セキュリティでも実績のあるHP IceWall SSO。評価版で是非お試しください。

2003.8.25 日本ヒューレット・パッカード コンサルティング事業部テクニカルコンサルタント 染井さやか

●関連技術レポート
» セキュリティ特集(1) - 守りを固めるTurn Key Solution !! - HP IceWall SSO＆PKI(Onsite)