HP IceWall SSO

HP IceWall技術レポート：セキュリティ対策特集（2）

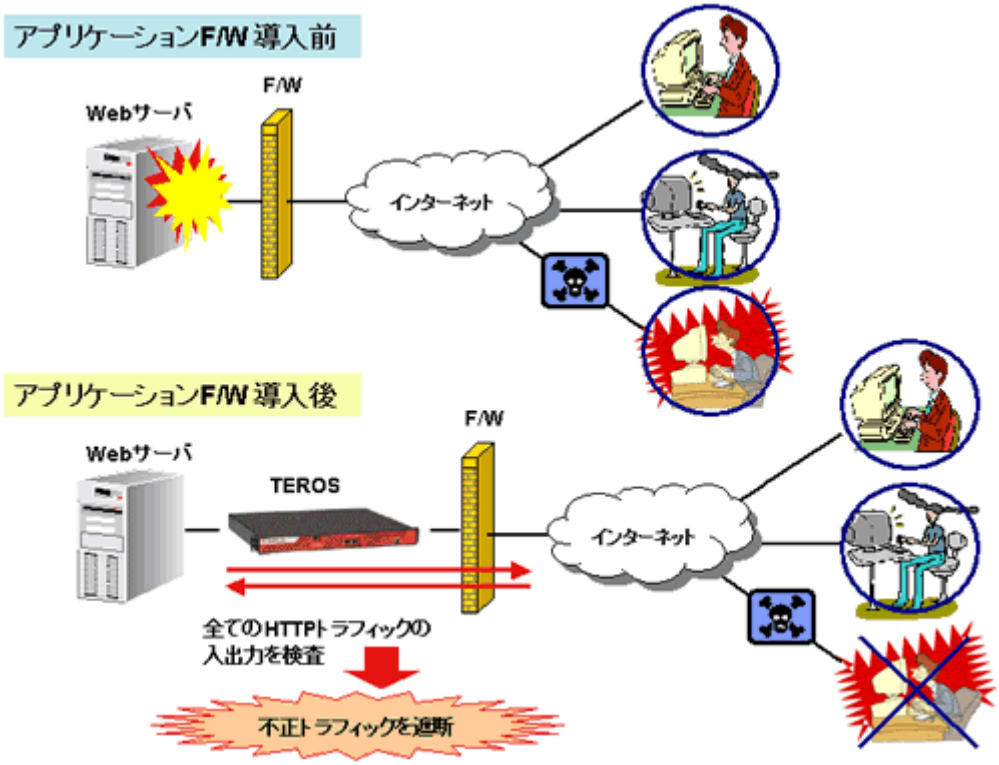
多数のWebアプリケーションを運用している場合、ユーザの個人情報がそれぞれのアプリケーションに分散していて十分な保護がされていなかったり、OSおよびアプリケーションのセキュリティホールへの対処が遅れているサイトが存在するといった危険があります。それらに個別に対応していくのは大変手間がかかりますが、2005年4月より全面施行される個人情報保護法では、社内で保有する個人データの「安全性の確保」が求められますので、しっかりとケアする必要があります。また、ユーザの立場からすると、アプリケーション毎にユーザIDとパスワードを覚えておくのが大変、といった悩みもあるのではないでしょうか。
今回ご紹介する、HP IceWall SSOとTEROS Secure Application Gatewayの連携で実現する「セキュア・シングルサインオン」では、HP IceWall SSOによってアクセスコントロールを、TEROSによってWebアプリケーションへの攻撃防止を行い、磐石のセキュリティと、ユーザに対しては利便性を提供いたします！

ビジネスの拡大と共に重要さが増していくWebアプリケーションへの対策

Webアプリケーション保護の必要性

Webアプリケーションの保護は「行うべき」事項から「行わなければならない」ものへと変わりました。Webサーバでは既に多くのWebアプリケーションが実行されており、個人情報を扱っていたり、各種の売買取引を行っていたり、様々な機密情報を取り扱っています。
これらは企業のビジネスにとって非常に重要な情報であり、万一そのような情報が外部にさらされるようなことがあれば会社の信頼に関る問題となります。このようなWebアプリケーションはしばしば大規模かつ複雑であり、全てのWebアプリケーションの状態を把握することは困難を極めます。また、コストを掛けて大規模なセキュリティ対策を行ったにも関らず、未知の脆弱性が存在するということは考えたくないと思います。しかし実際にはほとんどのWebアプリケーションは何らかの脆弱性を含んでおり、さらに問題なことはこのような脆弱性に対する不正（クラッキング行為）は通常のWebアクセスと同様に80番ポート（又は443番ポート）を通じて行われてしまうという点です。

セキュリティ監査会社から監査を受けることにより、セキュリティ監査レポートを受け取ることができます。監査レポートはしばしば膨大な量となります。いくつかの脆弱性は簡単な変更で修復が可能かもしれませんが、その問題がアプリケーションのロジックの内部にかかわるような問題だったらどうでしょうか。Webアプリケーション構築に利用しているサードパーティツールに脆弱性がある場合はどうでしょうか。この脆弱性が企業内に存在する全てのWebサーバに関る問題であったら。しばしばその脆弱性（バグ）を修正するのは大変な工数がかかったり、実際問題として不可能であったりするでしょう。また監査ツールでは見つけられない問題も潜んでいることを忘れてはいけません。



個々のアプリケーションの入力チェックを十分に行い、チェック漏れが無いように手作業でのテストを繰り返し行うことは非常にコストが掛かると共に、人手で行っている限り個人差が発生する為、一定レベルのセキュリティを確保することはできません。そこでWebアプリケーションファイヤーウォール（WAF）を活用することになります。

TEROS Secure Application Gateway

TEROSは、Webサーバとファイヤーウォールの間に設置するアプライアンス型のWAF製品です。すべてのWebトラフィックを監視することにより、HTTP/HTTPSデータの内部に含まれる各種不正攻撃からWebアプリケーションを強固に守ります。また、学習機能搭載によりセキュリティポリシーの設定が容易にでき、管理者に負担をかけずにセキュリティを強化できます。

- 豊富なチェック機能
  バッファオーバーフロー、クロスサイトスクリプティング、Cookieの改ざん、Dos攻撃などのWebアプリケーションの脆弱性を狙った不正攻撃に対して各種のチェックを行います。また、入力データだけではなく、Webサーバからの出力データに対しても禁止語チェックやクレジットカード番号のマスキングなどのフィルタリング機能を標準搭載しています。また、全ての管理はブラウザにより、リモートでの設定管理

が可能です。

フィルタリングの流れ

- 学習機能
  通過するトラフィックをTEROSが学習することにより、最適なポリシーを自動的に生成することができ、管理者は生成されたポリシーの中から適用したいものを選択するだけで設定できます。運用開始後もポリシーを取捨選択していくことで最適化していくことが可能です。

- セッションフェイルオーバー（VRRP対応）
  ミッションクリティカルな環境下では、複数台のTEROSを設置し、冗長構成をとることが可能です。セッションフェイルオーバー機能を備えているため、ハードウェア障害などに対してもユーザは全く意識することなく、継続したサービス提供が可能です。

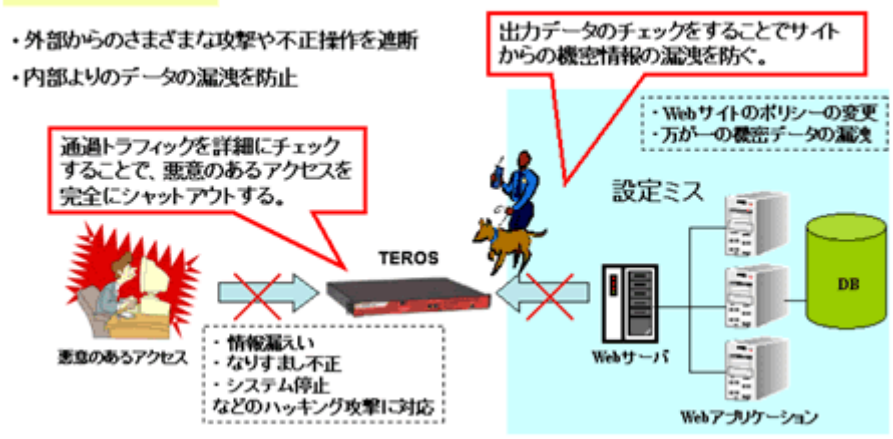
- 通知およびロギング
  不正トラフィックを検出した場合の動作は以下の通りです。
  - 不正な通信を遮断します。（可能な場合は不正な内容を無害化して通過させます。）
  - ユーザにエラーページを表示し、不正な通信の内容をログへ記録します。
  - 必要に応じて管理者へメール通知やSNMPトラップの送出が可能で、HP OpenView製品との連携も可能です。

- 2種類の設置モード
  TEROSはProxyモードとBridgeモードの2つの設置方法を採用しています。

- ファイヤーウォール製品との連動
  FireWall-1、Netscreenとの連携が可能で、指定したIPアドレスからの接続を拒否することができます。

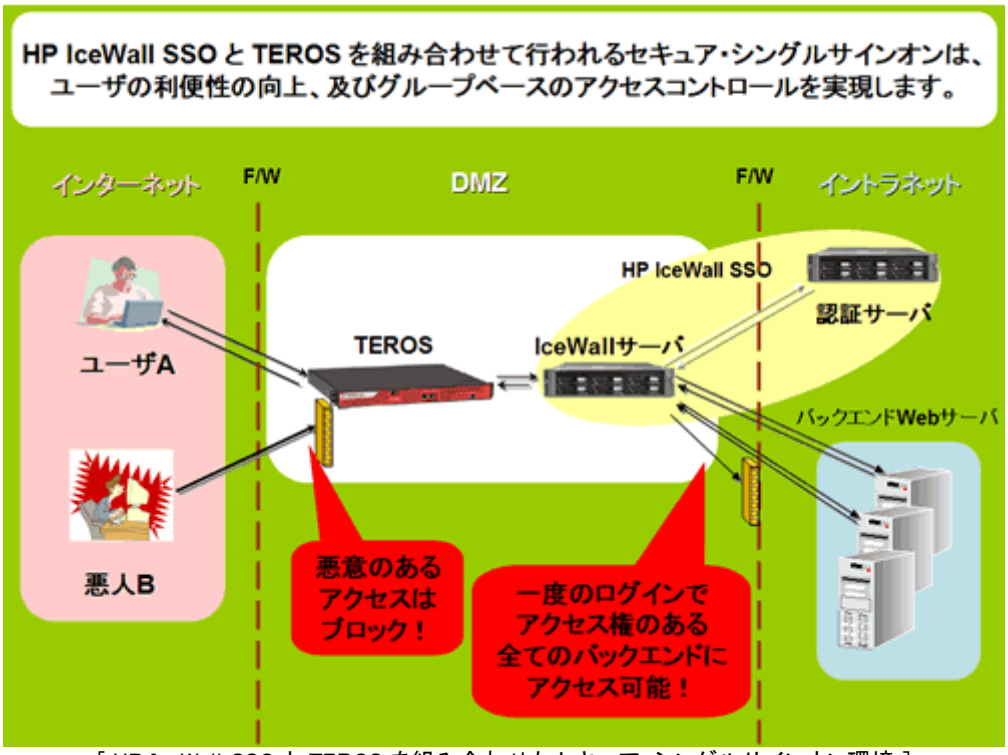
- XMLチェック
  Webサービスに対しても効果を発揮します。WSDL の設定をすることによりWebトラフィックの監視ができます。

TEROSの導入効果



HP IceWall SSOとTEROS の連携による セキュア・シングルサインオン

ビジネスチャンスの拡大に伴い、企業が維持・管理しなければならないWebアプリケーションは増加して行きます。それに伴い、ユーザが管理しなければならない認証情報も増加します。HP IceWall SSOによってユーザ情報を一元管理することにより、ユーザは一度ログインするだけで、アクセス権を持つ全てのWebアプリケーションへのアクセスが可能になります。この環境をTEROS と組み合わせて運用をすることにより、全てのアプリケーションに対するセキュリティを一定レベルに確保しながらも、ユーザはシームレスにアプリケーションにアクセスすることが可能になります。バックエンドWebアプリケーションへのアクセス可否はHP IceWall SSOによって判断され、アクセスの内容はTEROSとHP IceWall SSOによって判断されるのです。
では、HP IceWall SSOはアクセスコントロールだけなのかというと、そうではありません。HP IceWall SSOが提供するセキュリティ機能ももちろんございます。それは次の項でご説明します。



［ HP IceWall SSO と TEROS を組み合わせたセキュア・シングルサインオン環境 ］

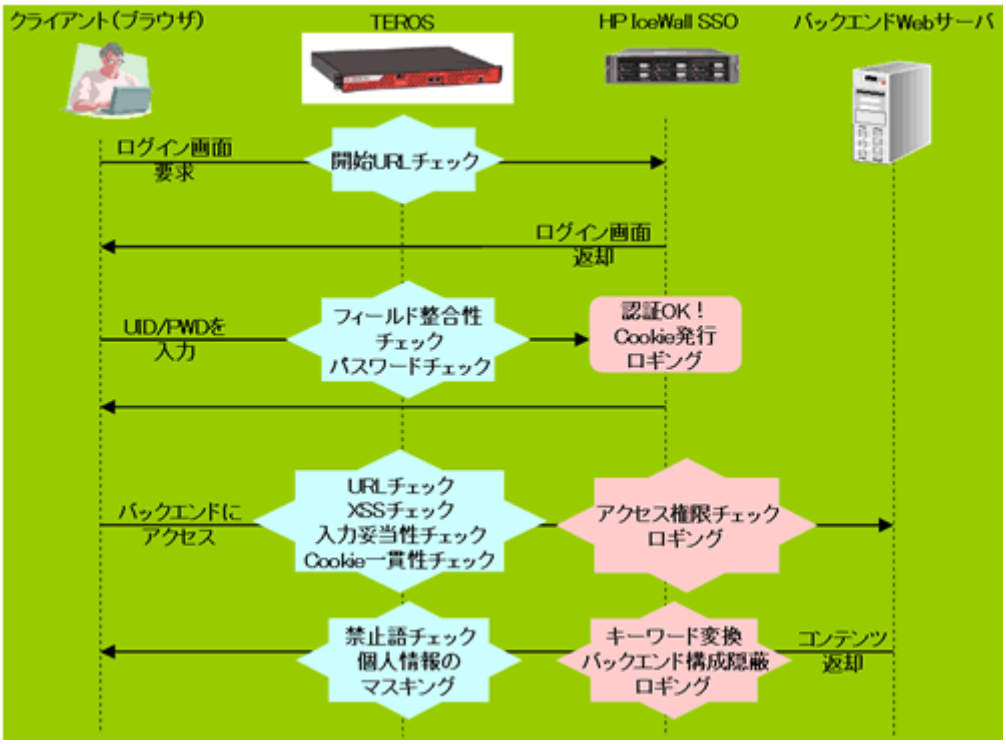
HP IceWall SSOとTEROS連携時のアクセスフロー

TEROS Secure Application Gateway によって、HP IceWall SSO の IceWall サーバに転送されたユーザ情報を用いて、認証サーバが認証を行います。ユーザ認証後の、Webアプリケーションへのアクセス内容はTEROSとHP IceWall SSOによって逐一チェックされます。

HP IceWall SSOが提供する主なセキュリティ機能は以下の通りです。

- 詳細ロギング
  ユーザのソースIP、ログイン経過時間等をロギングできます。
- バックエンドの構成隠蔽
  リバースプロキシ機能により、バックエンドWebアプリケーションのURLを隠蔽することができます。
- キーワード変換
  外部に流出させたくない情報（言葉）を変換して、ユーザにレスポンスを返すことができます。

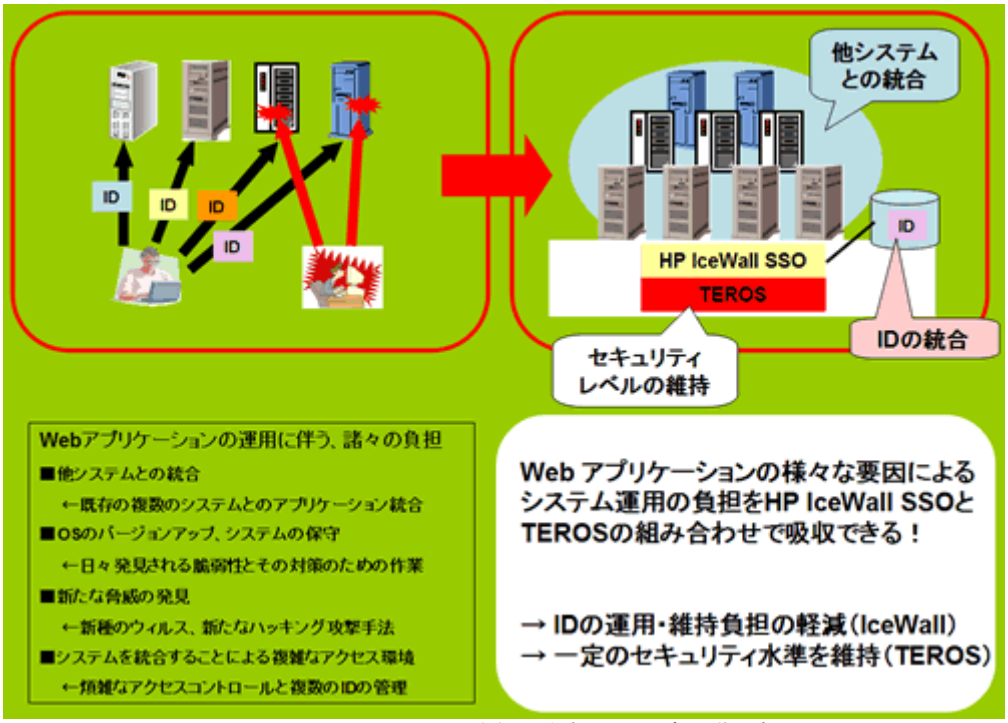
さらに、HP IceWall SSOと TEROSの連携は、それぞれの設定に特別な変更を施さずに行うことが可能です。



[HP IceWall SSO + TEROSの認証およびアクセスフロー]

セキュア・シングルサインオンの導入効果

HP IceWall SSOを用いたシングルサインオンによって、ユーザの利便性は向上し、またTEROSを用いることによって、全てのバックエンドWebアプリケーションサーバのセキュリティを、企業のセキュリティポリシーレベルに維持することが可能になります。利便性と安全性という相反する2つの性質を統合したソリューション、それがセキュア・シングルサインオンなのです！



[HP IceWall SSOと TEROS を組み合わせた環境の導入効果]

2004.11.26

・ビジネスの拡大と共に重要さが増していくWebアプリケーションへの対策

株式会社日本システムディベロップメント
ソリューション本部 担当　森田 知浩 氏
お問い合わせメールアドレス： teros@nsd.co.jp
株式会社日本システムディベロップメントホームページ： http://www.nsd.co.jp/teros/

・HP IceWall SSOとTEROSの連携によるセキュア・シングルサインオン
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 林 理絵

●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)
≫ セキュリティ特集(1) - 撃退!!FireWallを越えるアプリケーションレベル攻撃
≫ セキュリティ特集(2) - HP IceWall SSOとTEROSを使用したセキュア・シングルサインオンの実現（本トピックス）