HP IceWall技術レポート:

HP IceWall SSOでのE2EEソリューション
– ジェムアルト「Ezioサーバー」との連携

1. はじめに

インターネット経由でサービスを提供するシステムでは、利用者にユーザーIDとパスワードの入力を求めることがあります。特にパスワードは高い機密性が要求されるデーターであり、扱いについては第三者に盗まれることがないように高いセキュリティが求められます。
そのため一般にはクライアントとサーバー間の通信にSSL等を使って暗号化し、通信路での漏洩を防止しています。

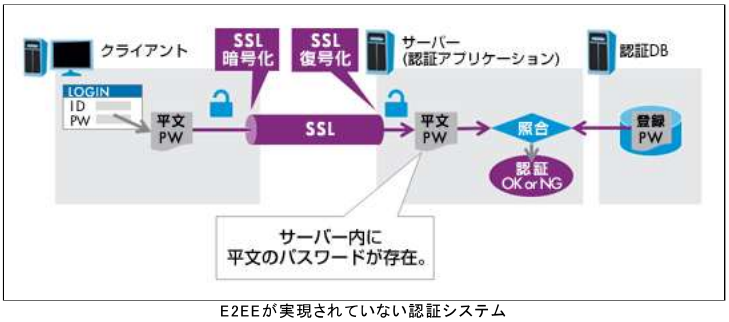
さらに、通信路だけでなくサーバー上での漏洩も防止し、より高度なセキュリティを確保するのがE2EE(End-to-End Encription)です。
シンガポール金融管理局(MAS)のガイドラインでは、インターネットバンキングのシステムにおいてE2EEが必須と定められています。(MAS規制)シンガポールは金融先進国としていち早くE2EEを義務化しましたが、将来的には他の地域でも必要となる可能性が考えられ、E2EE対応の重要度は高まることが予想されます。

ジェムアルト社の製品「Ezioサーバー」はE2EEを実現するためのアプライアンスで、金融機関を中心にグローバルに導入されています。
本レポートでは、HP IceWall SSOがEzioサーバーと連携してE2EEを実現する認証システムのソリューションをご紹介します。

2. E2EE(End-to-End Encryption)とは

E2EEとは、End(ブラウザー)からEnd(DBもしくはその入力値を検証するモジュール)まで暗号化を維持したまま通信や処理を行う方式です。途中の通信路やネットワーク機器、サーバー上で暗号化を維持し、重要なデーターの漏洩を防止します。

まず認証におけるE2EEについて説明するために、SSLを使った通信路の暗号化のみで、E2EEまでは実現していない一般的な認証システムの概念図を以下に示します。

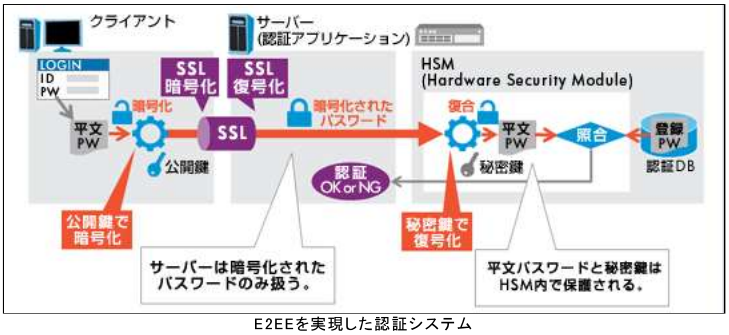


E2EEが実現されていない認証システム

ユーザーがブラウザーで入力したパスワードはSSLで暗号化されてサーバーに送信されます。サーバー側ではSSLの復合化を行ってパスワードを平文にし、あらかじめ認証DB等に登録されていたパスワードと照合して認証を行います。
実際は認証DBに暗号化やハッシュ化されたパスワードが登録されていますが、この図では省略しています。

ここで問題になるのはパスワードの復号がサーバー上で行われる点です。つまり平文パスワードがサーバーのメモリー上に存在するので、悪意のあるプログラムやウィルスに読み取られる可能性が非常に低いもののゼロではありません。

次にE2EEを実現した認証システムの例を以下に示します。



E2EEを実現した認証システム

ユーザーがブラウザーで入力したパスワードに対して、SSLの通信を行う前に暗号化を行います。
サーバー上ではSSLの復合化は行いますが、パスワードは暗号化されたまま後段のHSM(Hardware Security Module)へ送られます。HSMはデーターが漏洩しないような様々な対策が施されたハードウェアで、パスワードの復合化や照合を全てこの中のみで行うことで漏洩を防止します。つまり、End(ブラウザー)からEnd(HSM)の間で暗号化を維持することでE2EEを実現します。

3. ジェムアルト「Ezioサーバー」とは

Ezioサーバーはジェムアルト社より提供されているアプライアンス製品です。

サーバー内には、パスワード検証に使用するHardware Security Module(HSM)が内蔵されています。HSMでは秘密鍵が漏洩しないように管理されており、外部でパスワードの復号化が行えない仕様となっています。
また、Ezioサーバー内部には専用のデータベースも用意されており、パスワードは暗号化された状態で格納されます。パスワード検証時には、Ezio連携モジュールから受け取ったパスワードとデータベースに格納されているパスワードをHSM内で復号化し、照合します。

4. HP IceWall SSOとEzioサーバーの連携によるE2EEソリューション

今回ご紹介するE2EEソリューションは、大きく分けるとHP IceWall SSOシステム、Ezioサーバー、Ezio連携サ

ーバーで構成されます。

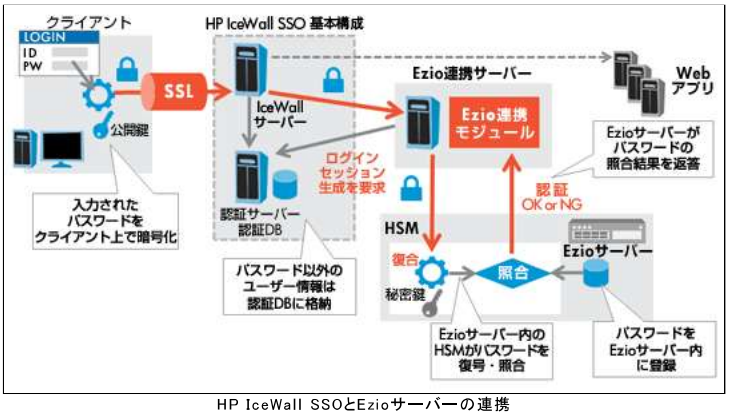
HP IceWall SSOシステム	SSO(シングルサインオン)を実現するためのシステムです。 IceWallサーバーや認証サーバー、認証DBといったHP IceWall SSOの標準的なコンポーネントで構成されます。 パスワードの管理についてはEzioサーバーでおこなうため、認証DBにはパスワード以外のユーザー情報を格納します。 ログインセッションの管理は通常のHP IceWall SSOシステムと同様に認証サーバーで行います。 アクセス制御などパスワード検証を伴わない処理については、Ezioサーバーや Ezio連携サーバーを使用せず、HP IceWall SSOシステムのみで行います。 IceWallサーバーはリバースプロキシーとして動作し、通常のシステムと同じくアクセスの認可処理を行います。
Ezio連携サーバー	HP IceWall SSOとEzioサーバーを連携させるためのソフトウェアを作成して配置します。(以降、作成するソフトウェアを「Ezio連携モジュール」と記述します) Ezio連携モジュールは、ログインやパスワード変更といったパスワードの検証を伴う処理において動作します。 ログインの際には、Ezioサーバーに対してパスワードの検証を要求し、検証がOKであれば認証サーバーに対してログインセッションの発行を要求します。 ユーザーがパスワードを変更する際は、Ezioサーバーに対してパスワードの検証と登録されているパスワードの変更を要求します。
Ezioサーバー	Ezio連携サーバーからの要求を受けてパスワードの検証や変更を行います。 Ezioサーバー内のHSMにはパスワードの暗号化/復号化のために使用する秘密鍵が格納されています。 Ezioサーバーに内蔵されているDBにはユーザーIDと暗号化されたパスワードが格納されていて、パスワードの復号化と検証がHSM内で閉じて行われ、復号化されたパスワードが外に漏洩しないようになっています。

下図は、HP IceWall SSOとEzioサーバーの連携例を示しています。この図を基に、E2EEが実現されていることを説明します。

処理の例としてログインを考えます。

1. まずユーザーがログイン画面に入力したパスワードはEzioサーバーの公開鍵を用いてクライアント上で暗号化されます。この暗号化は、ブラウザー～IceWallサーバー～Ezio連携サーバー～Ezioサーバーに至るまで維持されます。
2. Ezioサーバーに送られた暗号化されているパスワードは、HSMの中で秘密鍵を用いて復号化されます。
3. さらにEzioサーバー内のDBに暗号化されて登録されているパスワードもHSM内で復号化され、検証が行われます。
4. 検証結果としてOK/NGの情報のみがEzio連携サーバーに返却されます。
5. OKの情報が返却されると、Ezio連携サーバーから認証サーバーに対してログインセッションの生成が要求されます。
6. ログインセッションが生成されると、認証の処理が完了します。

結果として、復号化されたパスワードがHSM外部に渡ることはなく、認証が完了します。



HP IceWall SSOとEzioサーバーの連携

5.まとめ

本レポートでは、HP IceWall SSOとEzioサーバーを連携させることでE2EEを実現した認証システムソリューションを説明しました。E2EEは悪意のある管理者やウィルスなどによるパスワードの漏洩を厳密に防ぐために有効な仕組みです。

今後、政府当局によるE2EEの義務付けはシンガポール以外の国にも広がる可能性があります。
また、政府の規制の有無にかかわらず、より厳密なセキュリティが要求されるシステムに必要となっていくソリューションだと考えられます。

6. 参考URL

» ジェムアルト社

2015.6.15　　新規掲載

執筆者　　日本ヒューレット・パッカード テクノロジーコンサルティング事業統括　テクニカルコンサルタント 山岡 義史
日本ヒューレット・パッカード テクノロジーコンサルティング事業統括　スペシャリスト 佐藤 義昭