

HP IceWall SSO

HP IceWall技術レポート:セキュリティ対策特集(1)

<p>守りを固めるTurn Key Solution !! - HP IceWall SSO & PKI (Onsite) -</p>		<p>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</p> <hr/> <p>»</p>
---	---	--

Webシステムにおけるリスクを回避し、安全性を確保する標準技術 : PKI

インターネットが急速に普及し、商取引のインフラとしても当たり前のように使われるようになってきている現在、Webシステムにおいてセキュリティを保ち、その安全性をどう確保するのが、大きな課題になっています。

Webシステムにおけるリスクとはなんですか？

代表的なものでは、インターネット上に飛び交うデータを他人が盗み見る「盗聴」、データを書き換えてしまう「改ざん」、また、第三者が正当な取引主体に成りすまして、取引をおこなってしまう「なりすまし」などが存在します。

このような、リスクを回避し、インターネット上で安全な商取引を行うためのインフラとして注目されているのが、PKIです。PKIとは、“Public Key Infrastructure”の略で、公開鍵暗号方式という暗号技術を使用したセキュリティ・インフラのことを指しています。

本人認証の方式として、このPKI技術を利用した電子証明書による認証をWebサービスに実装し、より強固な認証をおこなうことは、BtoBを始めとする電子商取引サービスのサイトからイントラネットまでの幅広いWebシステムにおいて、もはや標準的な技術となっています。

HP IceWall SSO+PKI : No.1 ソリューション

HP IceWall SSOは、早くからこのPKI技術に注目し、クライアント証明書を使用したさらに強固な本人認証技術のオプションを用意しました。

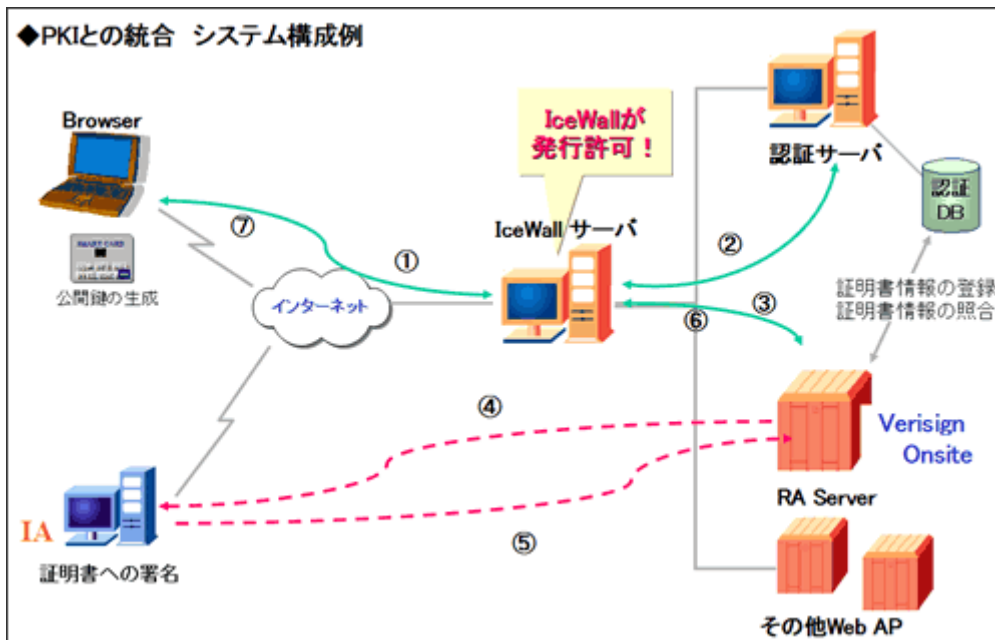
さらに認証局(Certificate Authority, CA)としての機能を提供するVerisign社のOnsiteと組み合わせたソリューションを実システムとして1997年に構築しました。

このソリューションはその後、HP IceWall SSO PKI対応版として電子商取引を始めとした大規模なBtoBシステムにおいて数多く採用されており、パートナーであるVerisign社からは、昨年、2001年Verisign Onsite販売実績第一位として、感謝状を頂戴しております。

また、最近では、NTTドコモの“FirstPass”(FOMAにてクライアント証明書が使用できるサービス)への対応も開始したり、アイデンティティ認証サービスを提供するIdentrusとの組み合わせで導入した実績もございます。

このように、HP IceWall SSO+PKIの組み合わせは、Webシステムの認証におけるベストソリューションとして、様々なお客様からの支持を受けています。

Verisign Onsiteとの接続事例



1. ブラウザからIceWallへ証明書発行要求を送信
2. IceWallがユーザ認証とユーザの証明書発行権限を確認
3. IceWallは許可されたユーザの証明書発行リクエストをRAへ送信
4. RA → IAへ証明書発行依頼
5. IA → RAへ証明書発行
6. IAから発行された証明書情報をRAがフォワーダ経由でブラウザへ送信
7. ブラウザは証明書のインストールを実行

ではHP IceWall SSO+PKIが、なぜ上記のように多くの支持を受けているのでしょうか。Verisign Onsiteとの接続事例から、その理由をご理解いただきましょう。

<PKI技術実装に関する問題>

安全性を確保するために当たり前のよう利用され始めたPKI技術ですが、実際にPKIを利用した認証システムを実装し、運用、管理をおこなうには、多くの手間とコストがかかるのも事実です。電子証明書を利用した認証システムに関しても、自社で認証局(CA)を構築し、証明書の発行、更新、失効、失効リストの新などの業務をおこない、管理を続けていくには、非常に多くの手間がかかります。HP IceWall SSOでは、第三者信頼機関として一般によく知られているVerisign社が提供したOnsiteサービスとの組み合わせにより、クライアント証明書を利用したシステムを容易に構築、運用することができる機能を提供しております。

<Verisign Onsite>

Verisign社のOnsiteは、認証局(Certificate Authority, CA)としての機能を提供するサービスです。CAは、ユーザの身元確認業務を行うRA(Registration Authority)と、証明書の発行業務を担当するIA(Issuing Authority)の2つから成り立ちます。RAの登録承認機能はOnSite導入企業で管理し、IAの証明書発行業務はVerisign社が受け持ちます。アウトソース認証局という形で運用される VeriSign OnSite を利用することにより、企業は迅速かつ容易にPKIを導入し、PKIバックボーンを設計/準備/運用/維持するために必要となる多額の出費を節約することができます。

<HP IceWall SSO+Verisign Onsiteのメリット>

HP IceWall SSOをOnsiteサービスと組み合わせる最大のメリットは、証明書発行までのプロセスを自動化し、運用の負担をさらに削減が可能となることです。通常、証明書の発行にはユーザの本人性の確認が必要となるため、ユーザは事前に詳細なユーザ情報を認証局に提出し、認証局はその情報に基づいてユーザに証明書発行を許可するかの判断をおこなう必要があります。

発行する証明書情報だけでなく、発行を許可するユーザ個人情報も管理しなければならず、証明書発行側の管理者の負担は多大なものとなります。

このソリューションでは、IceWallの基本機能であるユーザ認証をおこなうと共に、許可されたユーザのみ証明書発行システムへアクセスさせることによって、本人性の確認、証明書の発行を自動化しています。

また、[RA構築サービス](#)を利用する事で、ユーザにひもづけられた証明書情報を自動的に取得し、IceWallの認証データベースに保存する機能が加わります。そのため、発行局であるVerisign社のIAに問い合わせることなく、ユーザの証明書ライフサイクルの状態を管理者が把握することが可能です。

このように、HP IceWall SSO+Verisign Onsiteのソリューションでは、PKI技術を導入した強固なセキュリティ機能を提供しておりますので、金融商取引のインフラとしても安心してご使用いただけます。

また、その信頼性の高さから、すでに金融機関を始めとする多くのBtoBシステムにて導入いただいております。

HP IceWall SSO+PKIで、Webシステムに強固な認証を！

システムのセキュリティレベルを保つためには、多くの手間やコストが必要となります。
コストを削減するだけでなく、安全性の高いWeb認証サービスと利便性の高いシステム運用をご提供するHP IceWall SSO+PKIの組み合わせをどうぞご検討ください。

2003.8.25 日本ヒューレット・パカード コンサルティング事業部テクニカルコンサルタント 藤間朝子

2013.1.31 文面の加筆修正

●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\(Onsite\)\(本トピックス\)](#)
- » [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](#)