HP IceWall SSO

HP IceWall SSOが提供する個人情報保護ソリューション

2005年4月から、個人情報の保護に関する法律（以下、個人情報保護法）が施行されます。各省庁からも具体的なガイドラインが定められつつあり、個人情報を扱っている企業は、その個人情報の扱い方について早急に見直しを行い、個人情報保護の対策として、社内教育や業務運用改善、ファシリティのセキュリティ強化などを講じていかなければなりません。

ここでは、個人情報保護対策において特に必要性が求められているアイデンティティ&アクセス・マネジメント分野で、優位性・実績のある自社製品「HP IceWall SSO」が実現する個人情報保護ソリューションについてご紹介していきたいと思います。

個人情報保護について

個人情報保護の対策を検討する上で、以下の3つの点についてはよく誤解されがちです。

- 個人のセンシティブな情報だけが、個人情報の対象ではありません。個人を特定するデータは全て個人情報の対象となります。
- 消費者の情報だけが個人情報の対象ではありません。従業員情報や関連会社の社員情報なども個人情報の対象に含まれます。
- 個人情報の漏えいを防止することだけが個人情報保護対策ではありません。以下の表1の3～5のように、個人情報を最新の状態に維持することや、個人情報へのアクセスを制御することも対策として必要です。

個人情報保護法 5原則	Webサービスでの実現方法
1. 利用方法による制限	サービスを提供するための個人情報の利用目的が特定されており、必要範囲を超えてはならない。
2. 適正な方法での取得	ユーザから直接個人情報を取得する場合、ユーザのどの情報がどのような目的で利用されるのか、ユーザの同意を得なければならない。
3. 最新正確性の確保	ユーザの個人情報の内容が正確で且つ最新の内容を保たなければならない。
4. 安全管理	サービスで利用する個人情報が、漏えい、滅失、き損されないよう、措置（暗号化、アクセス制御など）を施さなければならない。
5. 情報への本人の関与	個人情報が、利用者の知り得る状態に置かれており、本人からの求めに応じて訂正、利用停止ができるものとしなければならない。

表1 Webサービスにおける個人情報保護

1、2については、運用や契約によって実現が可能です。3、4、5も同様に、基本的にはITや運用・管理によってすべて対応は可能ですが、人手による作業は、コスト増大や人的ミスによるリスクを伴います。一方で、「データの暗号化」「OSパッチの適用」「認証」「アクセスコントロール」などの個別技術は、局所的なリスクを抑えるものに過ぎません。したがって、全体的なリスクを抑え、なおかつ効率良く対応するためには統合ITソリューションが必要です。

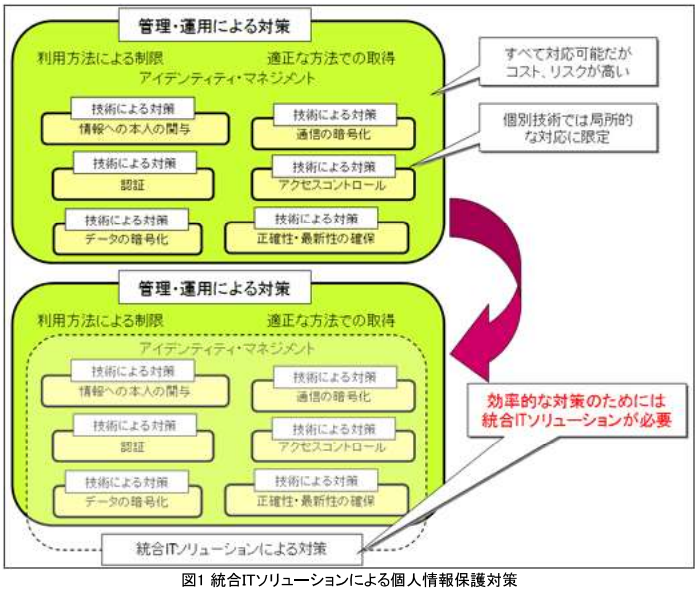

図1 統合ITソリューションによる個人情報保護対策

HP IceWall SSOやHP IceWall Identity Managerは、日本ヒューレット・パッカードが提供する統合ITソリューションのひとつとして、「3.最新正確性の確保」「4.安全管理」「5.情報への本人の関与」の問題をすべて解決します。

HP IceWall SSOが提供する個人情報保護ソリューション

既存のWebサービスシステムが問題となるようなケースを、企業内イントラネット上にある複数の業務Webアプリケーションを利用する場合を例にとって、説明していきましょう。（下記図2参照）

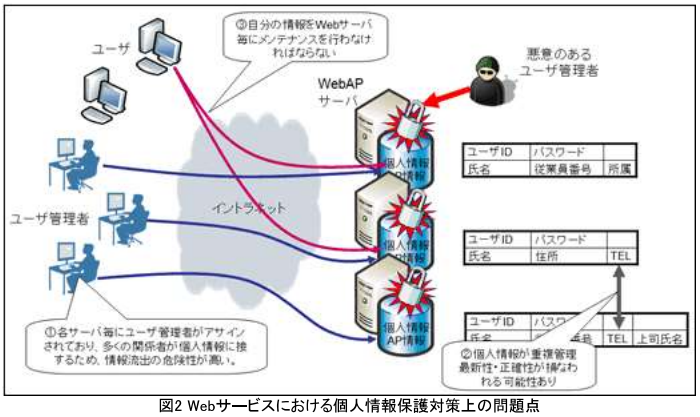

図2 Webサービスにおける個人情報保護対策上の問題点

1. 個人の同じ情報が、複数のDBで重複して管理されていませんか？
2. 個人情報の管理がそれぞれのユーザ管理者、WebAP開発者に一任されていませんか？
   管理者は直接DBにアクセスができるようになっていませんか？
3. ユーザが自分の情報をメンテナンスするために、複数の箇所でインタフェースが実装されているような、開発コスト・運用管理コストのかかるシステムになっていませんか？

このようなシステムに対し、HP IceWall SSO、IceWall Identity Managerを導入すると、以下のような構成になり、各々の問題点を解決します。

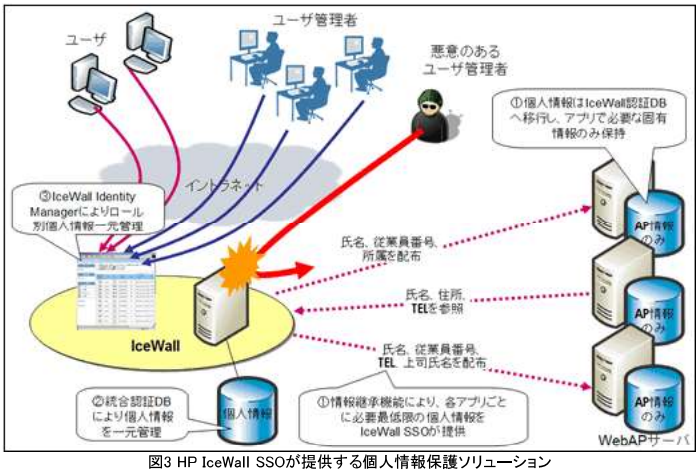

図3 HP IceWall SSOが提供する個人情報保護ソリューション

1. 個人情報の移行と情報継承機能

   既存の複数のDBには個人情報を置かず、IceWall認証DBに集約し、アプリケーション情報だけを残すことが個人情報の最適な安全管理対策と考えられます。IceWallでは個人情報にアクセスするための認証・認可・セキュリティの機能を提供しているため、適切な管理者だけが適切な範囲のみに対して個人情報のアクセスを可能にします。

   ですが、個人情報を一箇所に統合した場合、各WebAPサーバは何らかの方法で個人情報を受け取らなければ、サービスを提供することはできません。そこでIceWall の「情報継承機能※」を使用します。この機能は、IceWall認証DBに含まれている情報であれば、バックエンドのWebAPサーバに必要な情報だけを送信します。

   ※情報継承機能
   ユーザのログイン情報や認証DB上の情報をHTTPヘッダに付加し、環境変数としてバックエンドWebサーバに引き渡す機能

2. 個人情報の一元管理

   また認証DBを一箇所に統合することで、個人情報の追加・更新・削除は一箇所のみで行えばよくなり、WebAPサーバ毎に行う必要がなくなります。これにより、個人情報の正確性、最新性も確保します。

3. HP IceWall Identity Manager※によるセルフサービス機能

   Identity Managerでは、GUIを用いて、認証DB上にある個人情報のメンテナンスをユーザ自身の手によって行うことが可能です。これによりユーザは効率的に自身の個人情報に関与することができ、かつ管理コストを大幅に削減します。

※HP IceWall Identity Managerの詳細については、こちらをご覧ください。

より先端的な個人情報保護ソリューション

たとえば関連会社の従業員が、自社のWebアプリケーションにアクセスする場合、自社の認証DBには関連会社の従業員の個人情報を登録しなければなりませんでした。これでは管理コストも増大しますし、個人情報保護の観点からも、他社の個人情報を預かることはセキュリティ上のリスク増大につながります。

IceWallの「GSSO※機能」は、この問題を解決します。
GSSOには、信頼関係のあるサイト間でSAMLによる認証連携を行う「SAML Gateway方式」があります。（下記図4参照）

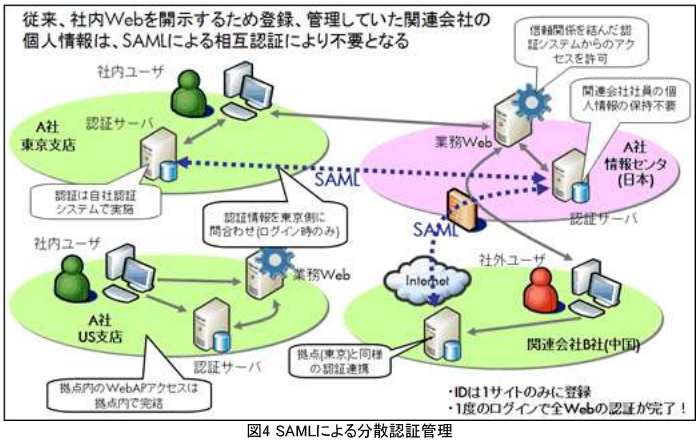

図4 SAMLによる分散認証管理

関連会社B社の従業員が、A社情報センタにあるWebAPを利用したい場合、B社で認証が完了していれば、自動的にB社からA社に対して認証連携を行い、A社での認証が完了します。A社の認証DBにB社の個人情報を登録することなく、GSSOを実現します。

※GSSO＝グローバル・シングルサインオン

日本ヒューレット・パッカードが提供する個人情報保護ソリューション

日本ヒューレット・パッカードでは、個人情報保護ソリューションとして、セキュリティポリシーの策定から、ネットワークセキュリティ、セキュリティデバイス、システム運用管理まで、様々な局面のお客様に柔軟に対応できる統合ITソリューションを用意しています。

- アイデンティティ・アクセスマネジメント
- ログ収集、監視システム
- 不正プログラム・ウィルス対策
- 暗号化、持ち出し制御、コンテンツセキュリティ
- セキュリティコンサルテーション

HP IceWall SSOやHP IceWall Identity Managerも同様にアイデンティティ・アクセスマネジメントの一製品として、より安価に、より迅速に、より安全性の高いWebサービスと利便性の高いシステム運用をご提供します。どうぞご検討ください！

2005.1.11 日本ヒューレット・パッカード コンサルティング・インテグレーション統括本部　IceWallソリューション部
部長　小早川 直樹