

# HP IceWall SSO

HP IceWall技術レポート: モバイル ソリューション

モバイル端末からのアクセスを  
考慮したセキュアなシステム  
構築を簡単に実現



デバイスの違いを越えて、いつでも、どこからでも、情報ネットワークにアクセスできる環境、「ユビキタスコンピューティング」の概念が広く普及されている現在、携帯電話やPDAなどを利用したモバイルアクセスに対応したサービスの提供はWebアプリケーションサービスの構築にあたって、もはや基本的な要件とされております。

すでにPCから利用しているWebアプリケーションを、PDAや携帯からもアクセスしたいというユーザのニーズに合わせて、システム開発者、管理者側で、新たに携帯用コンテンツを作成し、サービスの拡張を測るケースも増えております。

このように、モバイル端末を使ったシステムが普及し始めている現在、その構築の際にまず必要とされるのがシステムのセキュリティ対策です。これまで、モバイル端末からのアクセスを考慮したシステム構築例があまり紹介されてきていないことから、システム管理者の方々にも、その構築に興味はあるが、セキュリティ面の具体的対策にはどのようなものがあるのか、という疑問を持たれている方が多いようです。

- ▶ モバイルアクセスを考慮したシステム構築におけるセキュリティリスク
- ▶ HP IceWall SSOを利用してモバイルアクセスを考慮したセキュアなシステム構築を容易に実現
- ▶ HP IceWall SSO ver7.0の拡張機能を使ってさらに便利なモバイル用システムを構築！日本での開発・サポート体制を生かして、多くの携帯端末機種に対応
- ▶ 日本での開発・サポート体制を生かして、多くの携帯端末機種に対応
- ▶ 動作確認済モバイル一覧

▶

今回の特集では、モバイル端末からのアクセスを考慮したセキュアなシステム構築を簡単に実現する、HP IceWall SSOの機能をご紹介します。

## モバイルアクセスを考慮したシステム構築におけるセキュリティリスク

例えば、モバイル端末から、社内のWebアプリケーションを利用することができるようなシステムを構築した場合、経路は以下ようになります。

1. 携帯端末 — キャリア通信網 — インターネット — LAN
2. 携帯端末 — キャリア通信網 — 専用線 — LAN
3. 携帯端末 — 電話回線網 — LAN

1.のように、インターネットを経由してアクセスさせる場合、モバイルアクセスでも、盗聴・改ざん・なりすましといった、通常のインターネット経由でのアクセスに伴うリスクが考えられます。

また、2.、3.のようにインターネットを経由しない場合は、不特定多数からのアクセス可能なネットワークではないので、盗聴、改ざんなどの心配は少なくなります。不正アクセスに関しては、通常のPCからのアクセスと同じように注意をしなければなりません。

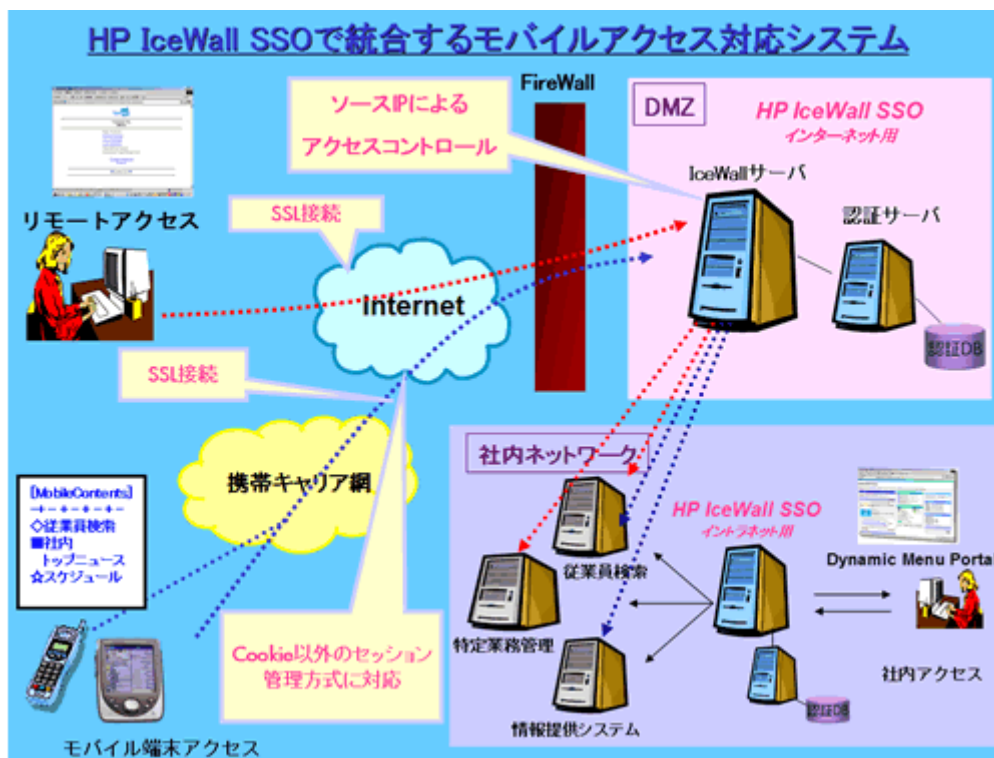
モバイル端末という便利なものからのアクセスを許可する以上は、社内の重要な情報に対する認証や、アクセスコントロールを万全におこない、社内のWebサーバに直接攻撃されないような手段を考えなければなりません。

## HP IceWall SSOを利用してモバイルアクセスを考慮したセキュアなシステム構築を容易に実現

このように、モバイルアクセスに対応したシステムには様々なセキュリティリスクがつきものですが、HP IceWall SSOを利用することでセキュリティリスクを軽減し、モバイルアクセスに対応したシステム構築を容易に実現することができます。

HP IceWall SSOでは、2年前にリリースされたバージョン5.0iより、モバイルアクセスに対応した様々な機能を提供し、すでに多くのお客様のモバイル対応サービスに活用いただいております。

以下の図は、HP IceWall SSOを導入いただいた場合のアクセス経路の例になります。



この図のように、HP IceWall SSOでは、機種によってCookieによるセッション管理が不可能な携帯電話アクセスでも、Cookie以外の独自のセッションを管理方式を使用することで、携帯端末からのアクセスにも容易に認証ロジックをつけることができます。

また、SSL通信の設定に対応しておりますので、インターネット経由のアクセスでも安心してご利用いただくことができ、通信回線費用の確保に必要なコスト削減にもつながります。

このように、HP IceWall SSOを活用いただくことにより、いつでも、どこからでもセキュアに必要な情報を手に入れていただくことのできる便利なシステムを容易に構築することができるのです。

#### HP IceWall SSO ver7.0の拡張機能を使ってさらに便利なモバイル用システムを構築！

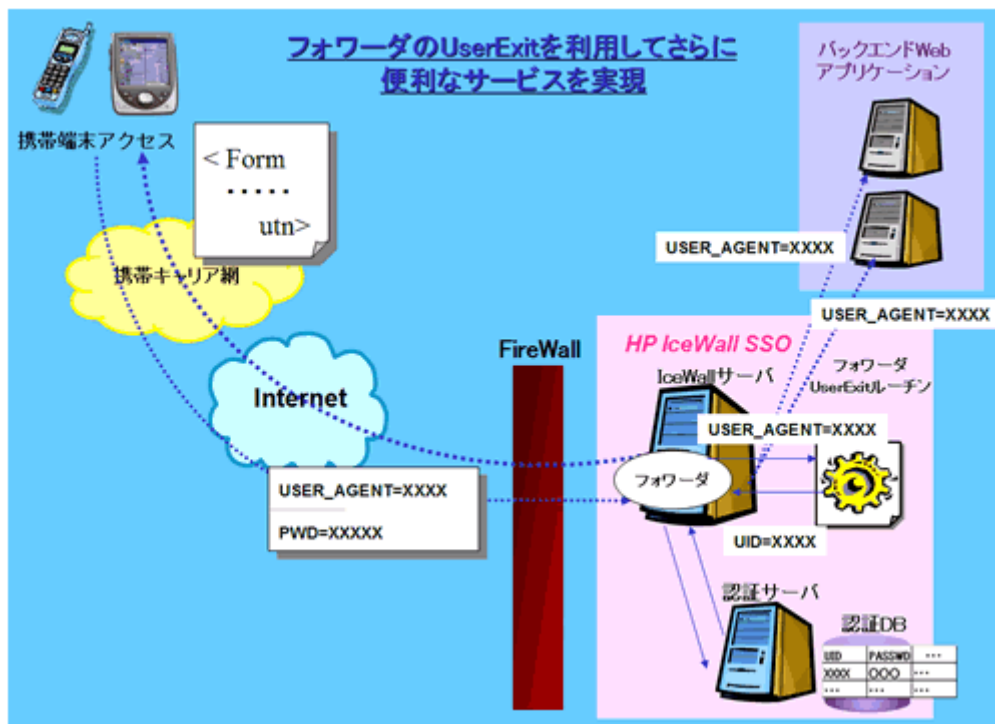
ここまでは、モバイルアクセスを考慮したシステム構築を容易にする様々なIceWallの基本機能をご紹介して参りましたが、HP IceWall SSO ver7.0で搭載された拡張機能により、さらに便利な認証サービスの構築が可能になりました。

HP IceWall SSO ver7.0からのフォワーダのUserExitルーチンを利用することにより、HP IceWall SSOは、認証データベースに登録されている情報だけでなく、クライアントの端末から送られてくる情報を認証情報として利用したり、バックエンドのWebアプリケーションサーバに引き渡したりすることができます。

これによりユーザは、ユーザIDを持たなくても、自分の携帯電話に割り振られている端末の製造番号により、認証をすることが可能となります。

また、携帯用のコンテンツは、キャリアごと、またメーカーごとに、HTMLの仕様が若干異なっていることがありますが、このような機能を使うことにより、アクセスしてきた携帯端末の製造IDを取り出し、バックエンドに配置された、コンテンツサーバに送ることによって、コンテンツサーバはキャリアを判定し、それにあつたコンテンツを生成することができるようになりました。

以下の図は、このように利便性の高いUseExitルーチンを利用した場合のシステムの簡単な通信の流れを示しています。



※UserExitルーチンに関する細かい解説については、“UserExitルーチン特集”をご参照ください。

日本での開発・サポート体制を生かして、多くの携帯端末機種に対応

このように、HP IceWall SSOでは、モバイル端末によるアクセスを考慮したシステム構築を視野に入れた様々な機能を実装しております。

そして日本で開発・サポートしている強みを生かして、携帯電話、PDAの数多くの機種で検証を実施し、すでに多くの接続実績を持っております。

対応検証済みの携帯機種の一覧についてはこちらをご覧ください。(動作確認済モバイル一覧へ)

また、NTTドコモ様から、モバイル端末からのアクセスを考慮したシステムをセキュアに構築するための認定パートナーとして、LinktoDoCoMoのロゴの使用許可を取得している他、NTTドコモ様及びNTTドコモグループ様8社による、FOMAによるクライアント認証サービス「FirstPass」サービス提供に関するパートナー企業としても認定をいただいているなど、パートナー様との連携もごございます。

モバイルアクセスによるサービスの拡張をお考えの方、また、モバイルアクセスのセキュリティに関する疑問等をお持ちの方は、是非一度お問い合わせください。

2003.12.19 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 藤間 朝子