〈ソリューション〉

セキュアリモートアクセスソリューション

Secure Remote Access Solutions

早野慎一郎* 則房雅也* 坂本秀紀**
Shin-ichiro Hayano Masaya Norifusa Hidenori Sakamoto

要　旨

ブロードバンド通信環境の進展とともに、外部からインターネットを通して組織内部の情報に安全にアクセスし（リモートアクセス），それをビジネスに活用しようという動きが加速しています。本稿では，まず，リモートアクセスによってビジネスの効率を上げられる例とそれに対する課題，要件を具体的に示しました。次に，課題を解決し，要件に対応するソリューション例を示しました。ソリューションとしては，SSL-VPN技術，モバイルIP技術を中心として使用したUNIVERGEセキュアリモートアクセス らくモデルが効果的に適用できることを示しました。

As broadband communications environment becomes common infrastructure for business, remote access to the intranet through the Internet is expected to accelerate the business processes. At first, this paper shows actual business scenes that can take advantage of the remote access technology. And it also lists up the issues and problems to overcome for the technology. At last, new solutions “UNIVERGE Secure Remote Access RAKU Model” based on SSL-VPN and mobile IP technologies are explained how they solve the problems.

1. まえがき

近年，ネットワーク接続環境の進展により，社内情報を社内だけではなく，社外からアクセスして業務に利用するという形態が色々な場面で現実的になっています。端的な例は，第3世代の携帯を用いて，高速に情報にアクセスできるようになったことです。他にも，ADSLやFTTHといった安価なブロードバンド回線が容易に使用できるようになったこと，公衆無線LANサービスが提供されだしたことにより，企業外でも高速な情報アクセス手段が複数提供されるようになりました。

一方，企業外から企業情報に安全にアクセスする方法としては，従来，IPsecと呼ばれる暗号化方式が一般に使われていましたが，SSL-VPN，モバイルIPという技術を使うことにより，より効果的なソリューションを構築することができることを示します。

2. ネットワークを活用したビジネスの進展

従来，情報の流通は，組織内部のイントラネットとインターネットである外部を明確に区別して行われてきました。外部から組織内部へのアクセスは厳しく制限されていましたが，イントラネット内部では自由に情報の流通をすることができるようにシステムが構築されていました。

近年，企業活動の広がり，ワークスタイルの変化に対応して，インターネットからあるポリシーに応じて安全に組織内部のイントラネットにアクセスすることが求められるようになりつつあります。1つの例は，社員のリモートアクセスです。外出先からオフィスに戻ることなく，イントラネットに接続し，報告書を送ったり，業務指示を出したりすることにより，すばやいアクションを可能とし，移動時間の無駄をなくす試みがなされています。また，オフィス外で働くということも行われるようになってきました。オフィスと同じような環境で在宅勤務が可能になれば，働き方に幅を持たせることができるようになり，組織と個人の要求条件をマッチさせやすくなります。

一方で，図1に示すように，複数の企業がお互いの強み

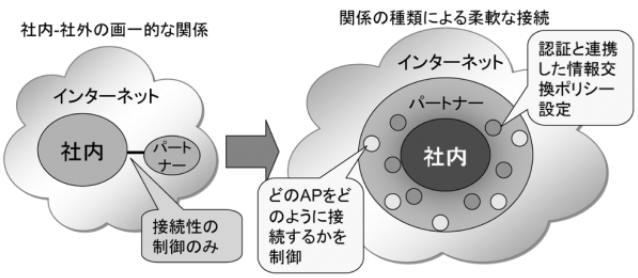

図1　パートナーとの情報交換でのセキュリティ
Fig.1　Security policy for partner relations.

＊ ビジネス開発本部
Business Development Division

＊＊ ブロードバンドプロダクト推進本部
Broadband Products Promotion Division

を活かして連携し，事業を営むことが盛んになり，サプライチェーンマネジメント（SCM）などを通して迅速に情報を交換することが必要になってきました。このような特定の企業間では，特定の情報，たとえば，売上予測のデータを組織内と同じように流通させる必要が出てきました。ただし，この場合でも人事情報など，企業連携に必要ない情報は確実にアクセスが制限されている必要があります。

また，数名程度の小さなオフィス，小規模な販売店などとの情報交換は，従来，ISDN回線や低速な専用線で行われていましたが，ADSL，FTTHなどのブロードバンド回線が安価に利用できるようになり，それらを利用して，大きなオフィスと高速に情報交換が可能になっています。この場合でも，適切なアクセスポリシーに基づいたセキュリティの確保が必要です。

今後，企業連携での情報流通をポリシーに応じて柔軟に制御できる手段を持つことにより，企業活動の幅が広がるものと期待されます。以下では，従来の問題点，SSL-VPN，モバイルIP技術を用いた，上記の課題を解決するソリューションを提案します。

3. セキュアリモートアクセス

3.1 従来の問題点

今まで，インターネットを通してイントラネットへセキュアな接続を行うためには，IPsecという技術が一般に使われていました。この技術はセキュアな通信を行うクライアントと組織内のイントラネットの間に，IPレベルの暗号化によりトンネルを設けるものです。この方式では，クライアント側にドライバソフトウェアをインストールし，その設定を行う必要がありました。また，IPsecでは一度ユーザ認証が行われてしまうと，すべてのIPレベルの通信が可能となるため，アプリケーションレベルでのアクセス記録を行うことや，アクセス制限が難しいという欠点がありました。

3.2 リモートアクセスへの適用

外出先から公衆無線LANサービスなどのブロードバンド環境，ダイアルアップを用いてイントラネット内の情報にアクセスするシステムとして，重要なポイントが4つあります。

(1) 通信路の安全性
(2) 認証の安全性，コスト
(3) ユーザ操作の容易性
(4) 管理の容易性

(1) はIPsec，SSL-VPNなど，標準的な暗号化方式が使用されていれば，大きな問題とはなりません。(2) は安全性とコスト，管理の容易性がトレードオフの関係になっています。IDとパスワードでの認証は簡易ですが，覗き見への対応が難しく，さらに，良いパスワードをユーザに使わせることが難しくなっています。逆に，PKI（Public Key Infrastructure）証明書を使用すると，高い安全性を持った認証を行うことができますが，証明書の認証局が必要になるなど証明書発行のコストが大きくなります。ここでは，パスワード方式の簡便さを持ちながら，その欠点を補う，マトリクス認証方式をSSL-VPN方式と組み合わせたシステムをUNIVERGE セキュアリモートアクセス らくモデル（SSL-VPN）として構築しました。SSL-VPNアプライアンスとしてはUNIVERGE SAFEBORDERという製品を用いています。

SAFEBORDERの特徴を以下にあげます。

① クライアントレスで管理コストが低い
② 利用アプリケーションの管理が可能
③ 広い認証方式へ対応可能

マトリクス認証方式とは，図2に示すように，認証画面に表示されるマトリクスの位置と順番を暗証とするものです。パスワードとしては，マトリクスに表示された数字を暗証となっている位置と順番に従って入力します。マトリクスの各位置に表示される数字は毎回異なるため，暗証とした位置と順番で作られる数字列は認証ごとに異なるものとなります。このため，1つのパスワードが長く使われる単純なパスワードより数段強固なワンタイムパスワードシステムを大きな運用コストの増大なく構築することができます。さらに，マトリクスはWebブラウザを通して表示されるため，特別なワンタイムパスワード生成デバイスを必要とせず，クライアントレスでリモートアクセス機能を提供するSSL-VPN方式とともに，クライアントの管理コストを低減しています。本システムではクライアント側の運用，管理コストが低いため，数千人のユーザをサポートするシステムも容易に構築することができます。また，SAFEBORDERでは他のSSL-VPN装置とは異なり，アプリケーションを認識しているため，アプリケーションの利用制限を行ったり，ユーザがどのアプリケーションを使ったかを記録に残すことができます。

図3にはシステムの概要を示します。ユーザがGSBサーバの持つホームページをアクセスすると，マトリクス認証のデータがGSBサーバにて生成され，ユーザにWebベースでマトリクスが提示されます。ユーザがマトリクスから得

図2 マトリクス認証
Fig.2 Matrix authentication method.

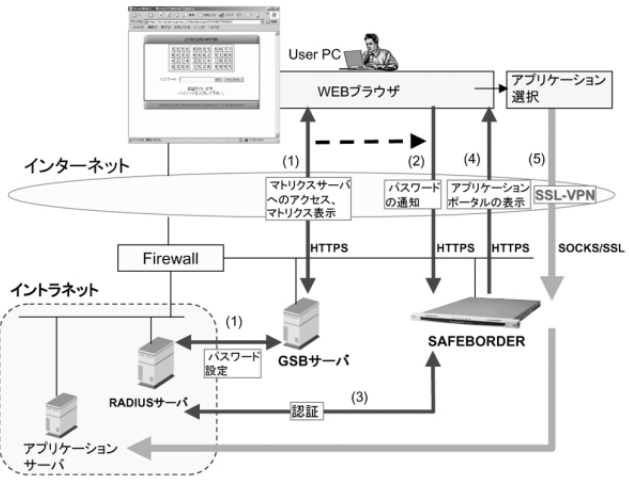

図3　SAFEBORDERでのマトリクス認証の概要
Fig.3　Matrix authentication system with SAFEBORDER remote access.

られるパスワードを入力するとアクセスはSAFEBORDERに移動します。一方，GSBサーバはRADIUSサーバへユーザの認証情報を送ります。SAFEBORDERはユーザが入力するワンタイムパスワードと，RADIUSサーバから提供される認証情報を用い，ユーザを認証します。認証が終わると，SAFEBORDERがSSL-VPN機能をユーザに提供します。

3.3　パートナー企業間情報交換への適用

近年，企業連携による事業の推進が一般化し，パートナー企業間でのフレキシブル，かつ，安全な情報流通システムの構築が求められています。パートナー企業との情報交換では，複数の同時に進行している案件ごとに相手も，どのような情報を交換するか，交換しないかというポリシーも異なります。したがって，案件ごとに異なる情報交換ポリシーを適切に設定でき，管理できること，また，どのアプリケーションによってどのような通信が行われたかを確実に記録に残しておけるようになっていることが重要です。

IPsecを用いたシステムだけではイントラネットをリモートサイトに延長する形となるため，セキュリティポリシーの異なるパートナー企業との情報交換には適しません。また，通信を行おうとする相手先企業との間でIPのプライベートアドレスが重複している環境でもIPsecは使用することができません。そこで，アプリケーション単位でアクセスを制御できるSSL-VPNアプライアンスSAFEBORDERとオーディットサーバを組み合わせたシステムを構築しました。

図4にはSAFEBORDERを用いた企業間情報交換システムの構成を示します。企業間ではSCMシステムのように，マシン-マシンの通信となることが多いため，本システムではPKI証明書を認証に用い，人が介在することなく自動的に情報交換ができるようにクライアントソフトをインストールしてアプリケーションと連携を取っています。SAFEBORDERはSOCKS技術を用いているため，Webの通信に使われるHTTP以外のプロトコルにも対応できること，アプリケーションを区別し，情報交換のポリシーをアプリケーションごとに変えることができるという特徴があります。さらに，オーディットサーバではアプリケーションまで含めた膨大な通信ログを理解しやすい形にまとめて出力するため，通信の専門家でなくてもパートナー企業との情報交換が正しく行われているか，常にチェックをすることが可能です。通信路は，要求される通信信頼性に応じてIP-VPN，既存のインターネット回線，インターネット経由の通信品質が悪化したときのバックアップとしてISDN回線を組み合わせて使います。

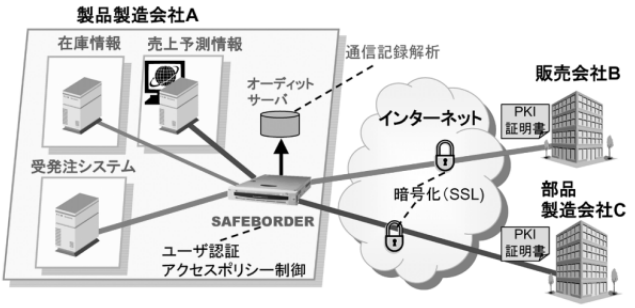

図4　パートナー企業間での情報交換
Fig.4　Data communications among partner companies.

3.4　小規模オフィスとの情報交換

小規模オフィス，販売店などとの情報交換システムでは，クライアント側に通信の専門家を置くことができないため，クライアントの管理が簡単である必要があります。また，初期導入コストも小さくなければなりません。

こういった用途には，図5に示すように，モバイルIP技術を用いたUNIVERGE セキュアリモートアクセス らくモデル（IPsec）を用意しています。モバイルIP技術を実現する機器としてはUNIVERGE MBシリーズを用いています。さらに，モバイルIPの特徴を活かして，VoIPとの連携を示しています。UNIVERGE MBシリーズを用いた場合の特徴として，以下があげられます。

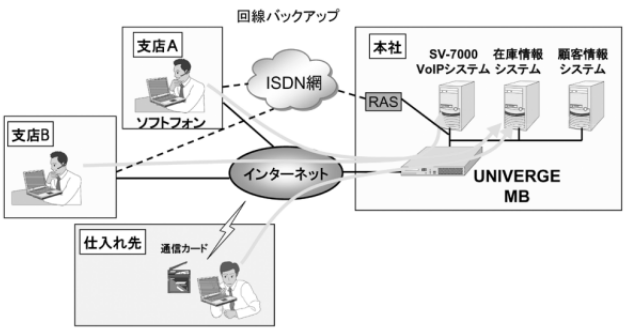

図5　UNIVERGE MBシリーズを用いた小規模オフィスの接続
Fig.5　Communication method of small branch offices using UNIVERGE MB series.

(1) イントラネットと同じ設定がリモートで使える
(2) イントラネットからリモート側へのアクセスが可能
(3) ネットワーク遅延を小さく抑えることができる
(4) アプリケーションの対応幅が大きい

このような特徴をもつため，イントラネットとまったく同一の設定，使い勝手を実現することができます。さらに，イントラネット内で接続をテストしておけば，そのまま，なにもPCの設定を操作することなく，リモート側で使用することができます。これにより，利用者のミスにより，接続できなくなるということが大幅に減り，管理コストを下げることができます。また，VoIPの利用においても，リモートであることを気にすることなく使用することができ，イントラネットからのVoIP電話を受けることもできます。このとき，VoIP電話をかける側も相手がどこにいるかを意識することなく，イントラネットでの番号でリモート側を呼び出すことができます。回線はADSLのような低コストだが品質の保証されないベストエフォートの高速回線を主として使用し，ISDN回線を通信品質が悪化したときのバックアップとして使うことにより，パフォーマンスと信頼性のバランスを取ることができます。

4．むすび

以上，リモートアクセスとして構築された新しいソリューションの紹介を行いました。大規模なリモートアクセス構築，新しい企業間の情報交換システム構築，小規模なシステム構築の3つの例を示し，それぞれ，新しい技術を導入することにより，柔軟に，かつ，安全に管理されたシステムを構築できるようになったことを示しました。今後，携帯電話などの携帯デバイスのサポートなどを含め，ブロードバンド環境をさらに広い領域で利用できるようにしていきたいと考えています。

＊SECURE MATRIXは，（株）シー・エス・イーの登録商標です。

筆者紹介

Shin-ichiro Hayano
早野慎一郎（はやの しんいちろう） 1983年，NEC入社。現在，ビジネス開発本部グループマネージャー。

Masaya Norifusa
則房　雅也（のりふさ まさや） 1980年，NEC入社。現在，ビジネス開発本部エキスパート。

Hidenori Sakamoto
坂本　秀紀（さかもと ひでのり） 1977年，NEC入社。現在，ブロードバンドネットワーク事業本部ブロードバンドプロダクト推進本部マネージャー。