SSL-VPN を用いた
リモートアクセスシステムの導入

エムジーシーコンピュータサービス株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

越田　直文

1993 年　三菱ガス化学株式会社　入社
2004 年　財務経理センターシステムグループ所属
　　イントラシステム担当
2004 年　エムジーシーコンピュータサービス株式会社
　　出向
　　現在　ネットワークサポートチーム所属

池田　守人

1994 年　エムジーシーコンピュータサービス株式会社
　　入社
1994 年　基幹系ホスト運用業務を担当
1999 年　基幹系インフラ保守業務を担当
2004 年　運用全般のサポート業務を担当
　　現在　運営管理グループ所属

石橋　正照

1994 年　エムジーシーコンピュータサービス株式会社
　　入社
1994 年　基幹系インフラ保守業務を担当
2004 年　ネットワークシステム全般の保守業務を担当
　　現在　ネットワークサポートチーム所属

中谷　英二

2001 年　三菱ガス化学株式会社　入社
2004 年　エムジーシーコンピュータサービス株式会社
　　入社
2004 年　ネットワークシステム全般の保守業務を担当
　　現在　ネットワークサポートチーム所属

■ 論文要旨 ■

三菱ガス化学株式会社では，社外から社内システムへのアクセス方法としてダイヤルアップ接続，リモートアクセスサービス，及びメール転送システムを許可していたが，利便性，コスト，回線速度，セキュリティなどで各々問題を抱えていた.
これらの問題を解決し，またより一層の利便性，セキュリティ向上を目的に SSL-VPN を用いたリモートアクセスシステムを構築した.
このシステムの導入により，
(1)国内・海外を問わない，安価なインターネット環境からのアクセス
(2)国内・海外の関連拠点からの業務システム利用
(3)国内・海外出張中のメール，社内ウェブの利用
(4)PDA・携帯電話などの携帯端末からの利用
をより安全な環境で可能とし，またセキュリティのより一層の向上のため
(1)ワンタイムパスワードによる個人認証
(2)利用目的による，ユーザーごとのサーバ・アプリケーションへのアクセス制御及び監視
を行うシステムとした.

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要

エムジーシーコンピュータサービス株式会社（以下 MGCCS という）は，平成６年に三菱ガス化学株式会社（以下 MGC という）からシステム部門が分離独立した関連会社である．主に MGC 及び関連会社におけるコンピュータ及びネットワークシステムの企画，開発，保守及び運用管理を行っている．

１．２　リモートアクセスシステムの特徴

リモートアクセスとは，文字通り電話回線などを利用して社外からコンピュータやネットワークに接続するシステムである．出張先や自宅または少人数の拠点から社内 LAN へ接続を行う際に大変有用である．このシステムの導入にはコスト面だけでなくセキュリティ面を十分考慮する必要がある．

２．旧リモートアクセスシステムの問題点

MGC には，図１のとおり，旧リモートアクセスシステムとして

①自社 RAS へのダイヤルアップ接続（利用ユーザー：約 20 名）

②リモートアクセスサービスの利用（利用ユーザー：約 10 名）

とがあり，また本来リモートアクセスとは異なるが，社内メールサービスの利用として

③メール転送システム（利用ユーザー：約 120 名）

を稼動していた．

次にこれらの旧リモートアクセスシステムにおける問題点を挙げる．

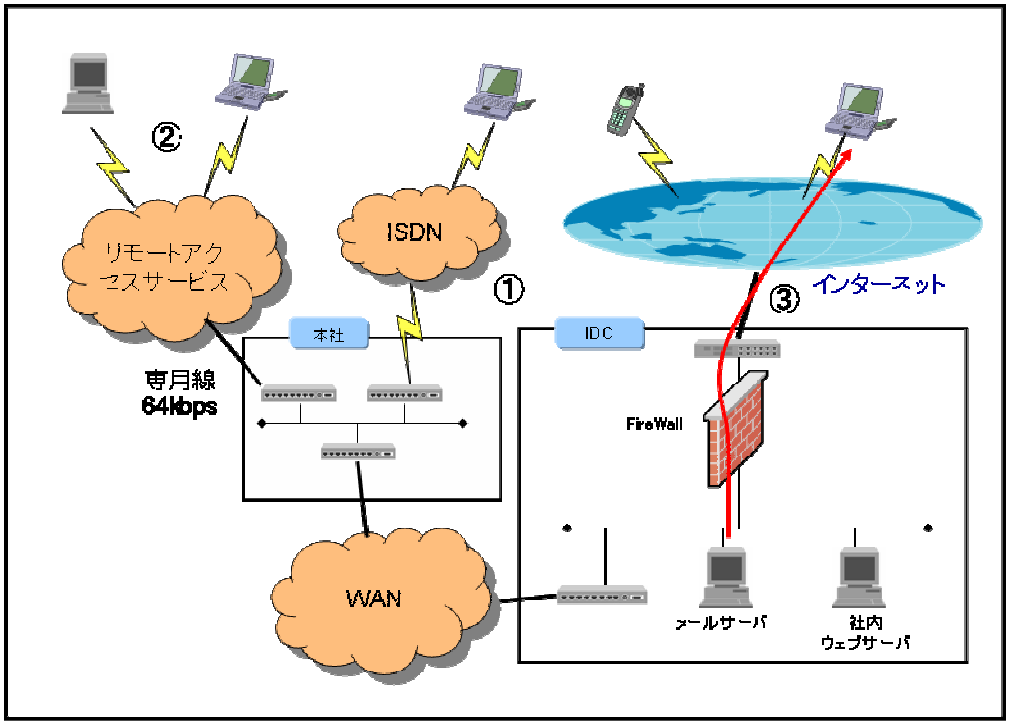


図１．旧リモートアクセスシステム概要

２．１　自社 RAS へのダイヤルアップ接続における問題点

このシステムの問題点としてまず挙げられるのが回線速度と同時アクセスである．接続媒体として PHS を利用していたため回線速度は 64kbps であり，同時接続数も INS 回線を 2 回線利用していたため最大で 4 接続となっていた．

また，RAS を自社設置していたため，障害対応などの運用面でのデメリットもあった．

２．２　リモートアクセスサービスの利用における問題点

MGC は，N 社が提供するリモートアクセスサービスを利用していた．このサービスでは，アクセスポイント設備と認証サーバ設備を提供しており，運用及びセキュリティ面ではよいのだが，回線速度とコスト面での問題があった．

このサービスと MGC との間では，DA 64kbps の専用線で接続していたため，最大でも 64kbps であり，複数人が同時にアクセスするとレスポンスが悪化する．コスト面では，基本サービス料と専用線利用料といった利用者数に依存しない費用があり，利用者数を増加しないと一人当たりの利用料を低下させることができない．しかし，利用者数を増加させると回線速度が低下するといった悪循環が発生していた．

また，アクセス制御及び監視に関しても十分なシステムではなかった．

２．３　メール転送システムにおける問題点

メール転送システムでは，上記の２システムと比較して低コストであり，回線速度もシステム自体に依存しないため，比較的多くの利用者がいた．

しかし利用していたシステムでは，基本的に自社のメールアドレスに届いたメールをすべて転送していたため，転送する必要のないもの，また転送してはいけないものまでも社外へ転送するといったセキュリティ面で問題があった．この問題を解決するためには，メールの振り分けを行う必要があるのだが，当時のシステムでは，容易に対応することが難しかった．

３．新リモートアクセスシステムの選定ポイント

旧リモートアクセスシステムの問題点及び利便性の向上を目的に，以下のポイントで新リモートアクセスシステムの選定を行った．

(1)高速・広範囲のアクセス環境

(2)クライアントレス（PC，PDA，携帯電話など）

(3)広範囲な利用可能アプリケーション

(4)高セキュリティ

次にそれぞれポイントについて説明をする．

３．１　高速・広範囲のアクセス環境

旧リモートアクセスシステムの最大の問題点に低速回線があった．また，基本的にアクセスポイントも国内にしかなく，海外からの利用は実質不可能であった．

これらの問題点を解決するために，新システムのアクセス環境としてインターネット VPN を利用することとした．インターネット VPN であれば，国内・海外を問わず接続可能であり，回線速度に関しても利用状況にあった速度を自由に選択可能となる．

３．２　クライアントレス（PC，PDA，携帯電話など）

現在インターネット VPN を構成する手段として，「IPsec VPN」と「SSL-VPN」の二つがある．これらにはそれぞれメリット・デメリットが存在するが，今回は「SSL-VPN」を選定した．選定した理由の一つにクライアントレスといったポイントがあった．

旧システムにおける利用方法の多くに，メール転送による携帯電話や PDA でのメール確認があった．「IPsec VPN」では専用ソフトウェアを導入する必要があるのに対し，「SSL-VPN」では，基本的に Web ブラウザさえあればよいため，携帯電話や PDA の利用が可能となる．

また，PC を利用する場合でも，ホテルなどに設置されているインターネット端末を利用することが可能となり，常に端末を持ち歩く必要が無くなる．

３．３　広範囲な利用可能アプリケーション

今回のシステム導入では，メールや社内ウェブだけでなく，国内・海外の関連拠点からの業務システム利用を可能にしたいと考えた．「IPsec VPN」と比べ「SSL-VPN」で利用可能なアプリケーションがやや限定されるが，ポートフォワーディングやレイヤー２接続といった機能により上記システムの利用が可能と判断した．

３．４　高セキュリティ

「SSL-VPN」を利用した場合，アプリケーションレベルまでアクセス制御が可能であることから，セキュリティの面でもメリットがあった．

また，更なる高セキュリティ化を目指し，ワンタイムパスワードによる認証システムを導入することとし，このシステムの選定には，運用面及び利用者の側面から「SSL-VPN」との連携に重点を置いた．

４．システムの導入及び運用手順

次に，実際にシステムを導入し，運用を開始するまでの手順を説明する．

４．１　デモ機によるテスト（2004 年 10 月頃）

前項における選定ポイントから２社の SSL-VPN アプライアンス製品（以下 SSL-VPN サーバという．）にしぼり，実際にデモ機によるテストを行った．テストの主な目的としては，SSL-VPN サーバの持つ機能の確認である．

SSL-VPN サーバの機能として主に以下の三つがある．

機能① リバースプロキシ：Web ブラウザを用いるアプリケーション

機能② ポートフォワーディング：固定 TCP ポートを利用するアプリケーション

機能③ レイヤー２接続：上記以外のアプリケーション

これら機能の違いとしては，下にいくほど利用できるアプリケーションは増えるが，アクセス制御などのセキュリティ面でマイナスとなる傾向がある．

まず，テストで用いるシステムを選定し，その通信内容（IP アドレス，ポート番号など）と利用する機能を検討した（表１）．

表１．利用システム及び機能

利用システム	IP アドレス	ポート	機能①	機能②	機能③
社内ウェブ	xxx.xxx.xxx.xxx	TCP80	○	○	○
グループウェア （ウェブ）	xxx.xxx.xxx.xxx	TCP80	○	○	○
メール	xxx.xxx.xxx.xxx	TCP25 TCP110	△*1	○	○
リモート デスクトップ	xxx.xxx.xxx.xxx	TCP3389	×	○	○
ホスト FNA エミュレータ	xxx.xxx.xxx.xxx	TCP747	×	○	○
業務サーバ （メタフレーム）	xxx.xxx.xxx.xxx	TCP1494 UDP1604	×	×	○

○：利用可，△：一部利用可，×：利用不可

*1：ウェブブラウザにて表示

次にデモ機を図２のように実際の環境と同じく DMZ に配置し，それぞれのシステムへの接続確認を行った．

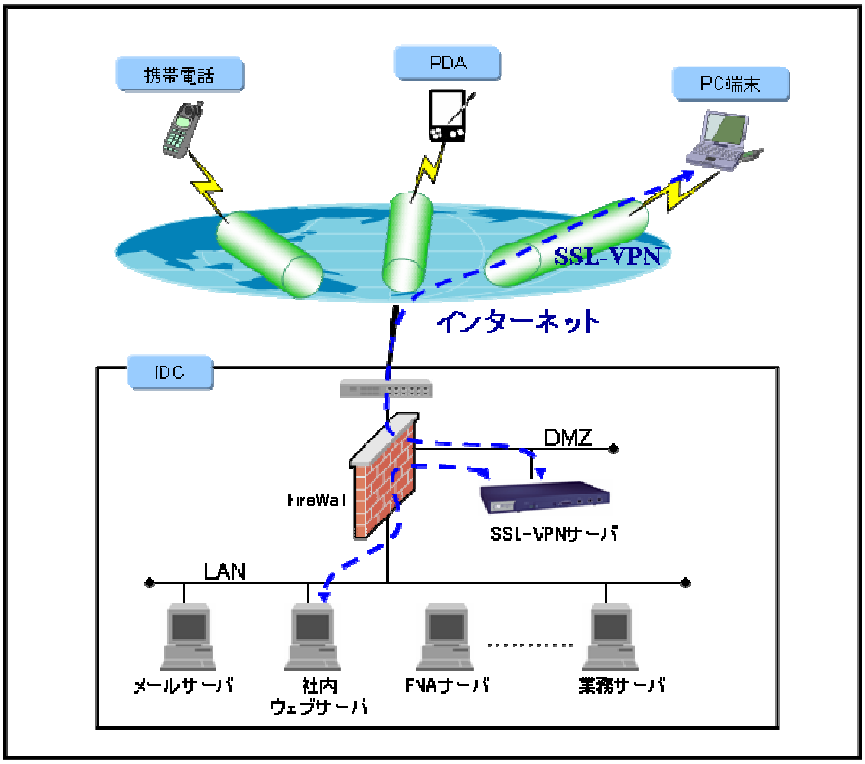


図２．デモ機テスト環境

ここでは，実際の接続可否はもとより，各利用システム・各機能の設定方法の容易さといった点においても注目した．またセキュリティ面では，各ユーザーごとに利用システムを制限できることも確認した．テスト期間は２週間程度であったが，接続及び設定手順の確認を行うのにちょうどよい期間であったと思われる．

４．２　実機導入及びテスト運用（2004 年 11 月下旬～2005 年１月上旬）

デモ機によるテストから F 社の SSL-VPN サーバを，またこの製品との連携から C 社のワンタイムパスワード認証システム（以下認証システムという）を選定し導入した．この認証システムでは，特定のハードウェアトークンを使用せず，Web ブラウザのみで利用可能というユーザー利便性も導入のポイントとなった．

実機導入に先駆け，まずリモートアクセスにて利用するシステムとその通信内容をすべて洗い出した．すでにデモ機によるテストを実施していたので，それぞれのシステムが SSL-VPN サーバのどの機能により利用できるかが比較的容易に想定できた．

続いて実機によるテスト運用を開始し，この段階では，主に SSL-VPN サーバと認証システムの連携確認と以下の運用管理手順の確立を行った．

○利用ユーザー管理

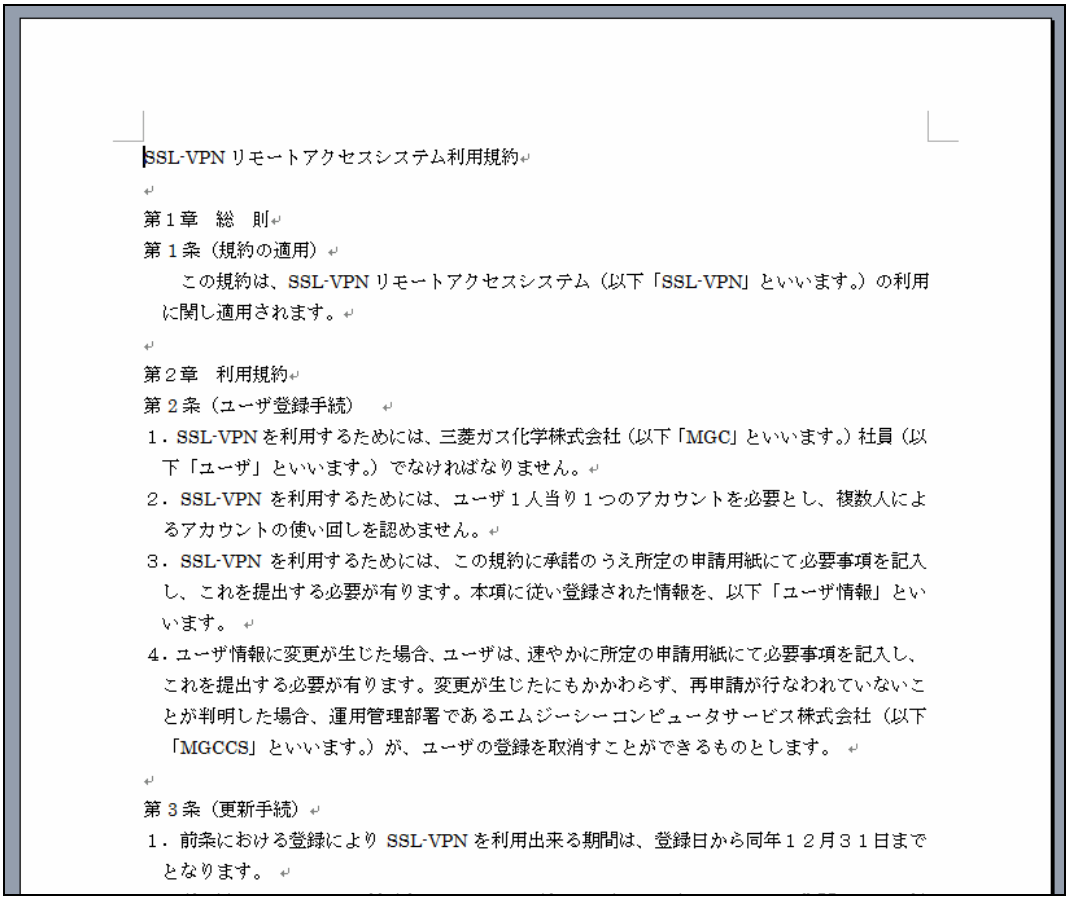
○利用サーバ管理

○管理ファイル運用方法

４．３　利用規約の作成と説明会実施（2005 年１月中旬～下旬）

テスト運用にてほぼ運用管理手順が確定したのち，説明会実施に先駆け，利用規約の作成を行った（図３）．この中では，利用可能なユーザー・サーバの範囲・申請方法，アカウントの有効期間と更新方法，起こりうるトラブルとその責任の所在を明確化した．

続いて利用ユーザーへの説明会を実施した．対象利用ユーザーを MGC 全社員としたことから，全国 17 拠点のイントラ運用者に連絡し，本社にて 2 度説明会を行った．また当日参加できなかった拠点に関しては，現地に赴いて説明会を実施した．説明会の内容としては，新システムの概要，ユーザーインターフェースの説明，利用規約の説明などを行った．



SSL-VPN リモートアクセスシステム利用規約

第１章　総　則

第１条（規約の適用）

この規約は、SSL-VPN リモートアクセスシステム（以下「SSL-VPN」といいます。）の利用に関し適用されます。

第２章　利用規約

第２条（ユーザ登録手続）

１．SSL-VPN を利用するためには、三菱ガス化学株式会社（以下「MGC」といいます。）社員（以下「ユーザ」といいます。）でなければなりません。

２．SSL-VPN を利用するためには、ユーザ１人当り１つのアカウントを必要とし、複数人によるアカウントの使い回しを認めません。

３．SSL-VPN を利用するためには、この規約に承諾のうえ所定の申請用紙にて必要事項を記入し、これを提出する必要が有ります。本項に従い登録された情報を、以下「ユーザ情報」といいます。

４．ユーザ情報に変更が生じた場合、ユーザは、速やかに所定の申請用紙にて必要事項を記入し、これを提出する必要が有ります。変更が生じたにもかかわらず、再申請が行なわれていないことが判明した場合、運用管理部署であるエムジーシーコンピュータサービス株式会社（以下「MGCCS」といいます。）が、ユーザの登録を取消すことができるものとします。

第３条（更新手続）

１．前条における登録により SSL-VPN を利用出来る期間は、登録日から同年１２月３１日までとなります。

図３．SSL-VPN リモートアクセスシステム利用規約例

４．４　本格運用開始と旧システムの停止（2005 年２月～）

以上のような過程を経て，2005 年 2 月から本格運用を開始した．テスト運用をすでに行っていたため，トラブル無くスタートすることができた．

今回のシステム概要を図４に示す．利用者はインターネットに接続後，まず認証用ゲートウェイサーバにアクセスし（①），このゲートウェイサーバ上にログイン ID とパスワードを入力し（②），認証サーバにて正規ユーザーと認証される（③）と SSL-VPN サーバ上から利用者ごとに設定された各システムにアクセス可能となる（④）．

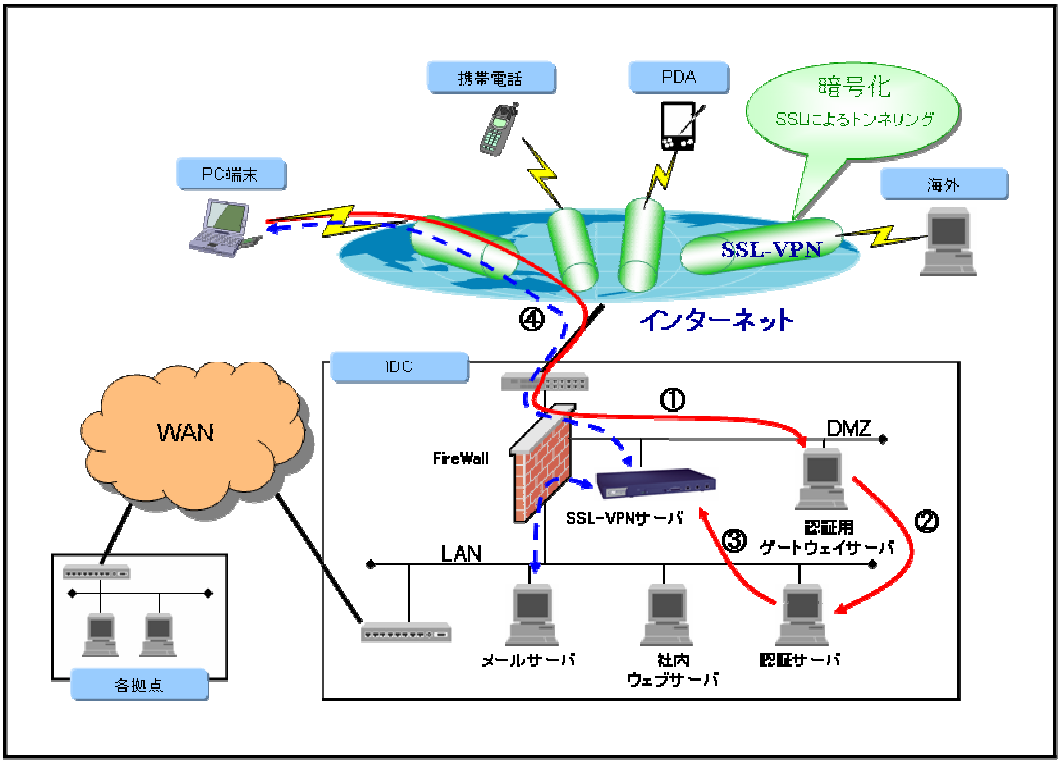


図４．SSL-VPN リモートアクセスシステム概要図

なお旧システムは，一定の重複期間をとった後，2005 年 4 月末ですべてのシステムを停止した．

５．評価と今後の展開

新リモートアクセスシステムは，本格運用開始後，安定した運用を継続している．2005 年 6 月現在，利用ユーザー数は 200 名をこえ，現在も増加中である（旧システム利用者はトータルで 150 名程度）．約 5 ヶ月を経過したがトラブルによるシステム停止は発生していない．

導入目的であった(1)高速・広範囲のアクセス環境，(2)クライアントレス，(3)広範囲な利用可能アプリケーション，(4)高セキュリティにおいて，すべて実現することができた．またコスト面においても，システム自体が大きく異なるため比較しにくいが，旧システムのリモートアクセスサービスの利用と比較して一人当たり１／１０以下のコストとなっている．

今後の展開として，現在，利用者を MGC 社員に限定しているが，今後は出向者を含む関連会社や海外拠点への展開を行う予定である．

６．おわりに

SSL-VPN リモートアクセスシステムの構築により，より多くの利用者の利便性を向上することができただけでなく，リモートアクセスの入り口を一本化したことにで，個人情報・機密情報などの漏洩対策としても十分に効果があるものと思われる.

最後に，このようなシステム構築の機会を提供していただいた会社関係者，及びシステムの設計構築に携わっていただいたすべてのスタッフ及び関係会社の皆様に感謝を申し上げます.