

N+I Tokyo 2004

C20: SSL VPNの真価を探る

# SSL VPNへの取り組み

2004/7/1

日本電気株式会社

則房 雅也, CISSP

# SSL VPNとの関わり

- **米国でインターネット、セキュリティの技術・製品開発を10年あまり**
  - SOCKS、ファイアウォール製品、VPN製品、イントラネット構築・運用、セキュリティ技術、ネットワークアプリケーション
  - ファイアウォールの課題、インターネットの課題などに直面
- **SSL VPNアプライアンスの開発に着手**
  - SAFEBORDER AP100、派手さはないが実益を提供できる製品
  - ファイアウォール、インターネットの課題が克服できると信じている
- **海外の製品が多いが、日本の市場に根付かないことも多いことを懸念**
  - enNetforum SSLVPNリモートアクセス分科会発足に協力
  - 日本のSSL VPN市場のすそ野を広げる
- **啓蒙活動**
  - SSL VPNに関するセミナー、雑誌記事、本など

# SSL VPNが必要とされる背景

## コンピューティングのモデル

1. 端末-ホスト型
2. クライアント-サーバ型
3. 三層クラサバ型
4. Thinクライアント型

70年代

80' ~

90' ~

90' 初

## ネットワーキングのモデル

1. 専用線
2. LAN
3. 広域につながったLAN
4. オンラインネットワーク

このあたりからプライベートIPとNATが使われファイアウォールも浸透

5. ウェブ型

90' 中

5. 商用インターネット

ここから先のコンピューティングモデルが広がらない、利用も浸透していかない

6. ストリーミング型

90' 後

6. 広帯域インターネット

7. P2P型

00' ~

7. モバイル

8. グリッド型

将来

8. ユビキタス

# SSL VPNの本質は何か

<本人確認、アプリケーション確認、セッション管理、アクセス制御>を一連の流れの中で統合的に行う

- IPパケットを見ても情報不足、IP層の技術では難しい
- VPN実現方式は違ってもSSL VPNとしての共通要件

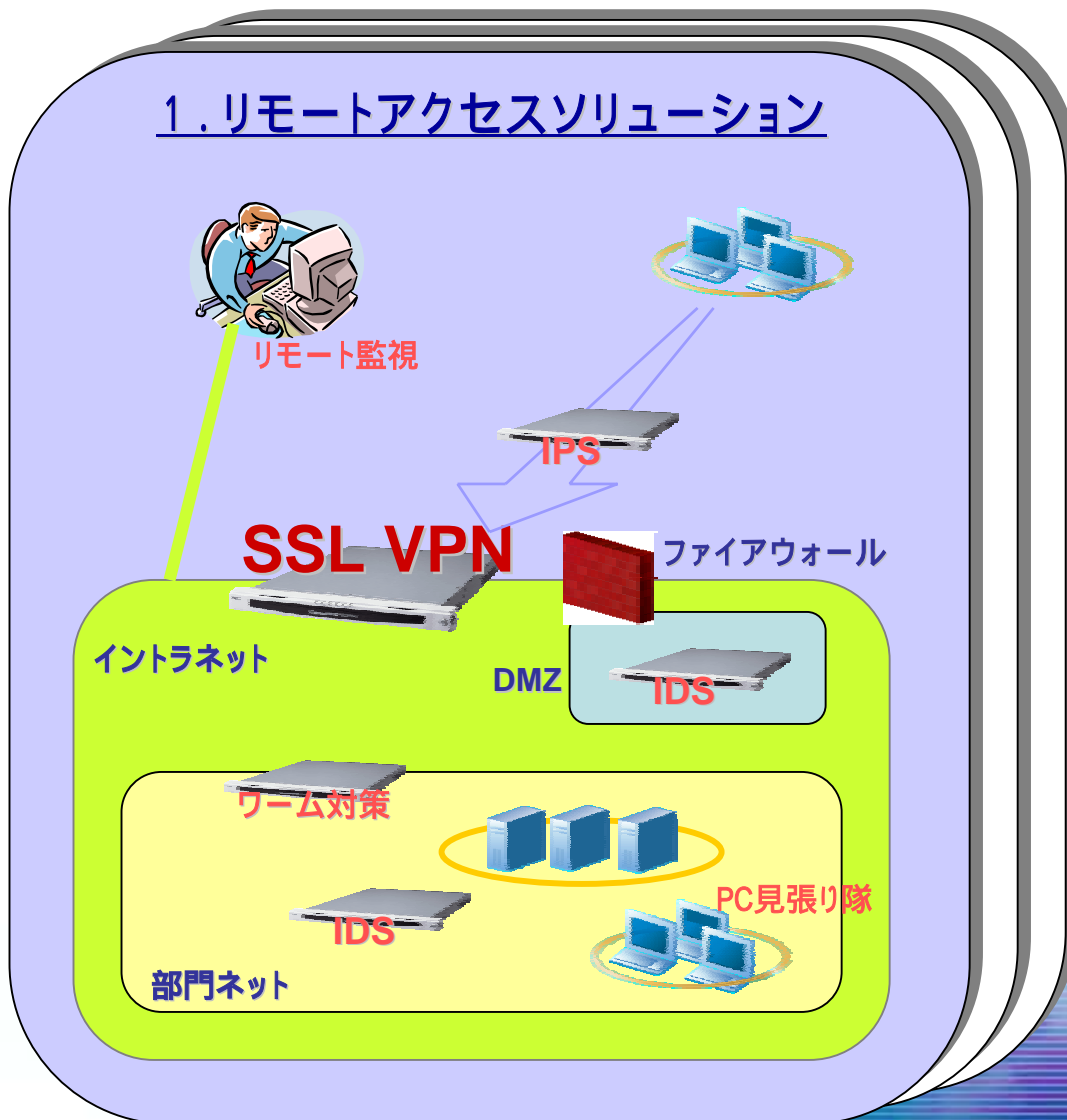
	リバースプロキシ (HTTPS)	フォワードプロキシ (SSL化SOCKS)	SSLトンネル(Java利 用、アプリケーション データ)	SSLトンネル(ActiveX 利用、L2フレーム)
本人確認	ブラウザ、証明書、 HTTPベーシック認証、 OTPなど他の認証シス テム	ブラウザ、専用モジュ ール、証明書、UN/PW、 OTPなど他の認証シス テム	ブラウザ、証明書、 HTTPベーシック認証、 OTPなど他の認証シ ステム	ブラウザ、証明書、 HTTPベーシック認証、 OTPなど他の認証シス テム
アプリケー ション確認	ブラウザ	アプリケーションリスト	アプリケーションリスト	アプリケーションリスト
セッション 管理	HTTPSセッション+別 のHTTP/HTTPSセッシ ョン	多段SSL化SOCKSセッ ション+TCP/UDPセッ ション	2点間SSLトンネル+ アプリケーションセッ ション	2点間SSLトンネル+ IPルーティング
アクセス制 御	(通信先) ウェブサー バ名、URL (通信元) ユーザ/グ ループ	(通信先) ネットワー ク名(FQDN)、IPアドレ ス、ポート番号 (通信元) ユーザ/グ ループ	(通信先) アプリケー ションサーバ名 (通信元) ユーザ/グ ループ	(通信先) IPアドレス、 ポート番号 (通信元) ユーザ/グ ループ

# SSL VPNの価値、優位性、可能性

- **新しいネット利用、サービスを展開する鍵**
  - IPルーティング、名前解決の問題が少ない
  - イン트라ネットの業務アプリをインターネットに持ち出して使える
  - セキュリティ機能のないアプリでも、変更せずにセキュリティ(認証、暗号化、アクセス管理)を追加できる
  - ユーザ認証後アプリケーションを選択するので、限られたアクセスを厳密管理できる
- **かつ、広域(グローバルも含め)に展開する鍵**
  - クライアントレスでエンドユーザの手をかけない
  - 途中のIPインフラに影響を受けない
  - DMZまわりのIPインフラを変更しなくても導入できる
- **ファイアウォールの束縛から逃れる鍵**
  - 特定ユーザ、特定アプリのトラフィックをファイアウォールから切り離してSSL VPNで管理
  - ファイアウォールの変更なし

# NECが考えるSSL VPNとネットワークセキュリティ

- **SSL VPN**  
SAFEBORDER
  - 業務アプリを安全につなく
- **IPS**  
S@FEGUARD
  - 不信なアクセスを止める
- **ワーム対策**  
WORMGUARD
  - ワーム拡散を止める
- **PC見張り隊**  
CAPS
  - PCの安全状態を監視
- **リモート監視**  
ActSecure
  - 24/365セキュリティ監視サービス



# SSL VPNに対するNECの取り組み

- **社員にリモートアクセスサービス開始**
  - － ワンタイムパスワードとの連携
  - － 海外駐在社員数千人がイントラネットアクセス可能に
- **今後の強化方向**
  - 認証連携： ワンタイムパスワード、PKI (ICカード、USBキー)、など
  - アプリケーション連携： グループウェア、マルチメディアアプリケーション、業務アプリケーション
  - セキュリティ製品連携： PCセキュリティツール  
ファイアウォール非依存
- **NWとITを融合するツール**
  - － Nler、Sler両方へのソリューション提供

# enNetforum SSL VPNリモートアクセス分科会

## 設立の目的

本分科会は、SSL VPNを活用したユーザにとって利便性が高く、かつセキュアなリモートアクセス環境を実現するための指針を提供する事を目的として、下記の活動を行う。

- (1) SSL VPNの利点と現状の課題の整理
- (2) SSL VPNを実現する多様な技術方式の分類と整理
- (3) SSL VPNの利用事例の検討、分析
- (4) SSL VPNが目指すべき方向の検討

設立趣意書(2003年10月3日)

- (主査) 則房 雅也 日本電気(株)  
(副査) 三浦 竜樹 (株)アイ・ティ・アール  
(事務局) 干場 久仁雄 (株)インターネット総合研究所

## 連携・協力組織

NPO日本ネットワークセキュリティ協会  
インターネットVPNワーキンググループ

## これまでの活動

enNetforum SSL VPNセミナー  
N+I NETWORK GUIDE 2004年2月～6月号 連載記事  
N+I NETWORK GUIDE 2004年8月号 特集記事  
N+I TOKYO 2004 SSL VPN製品展示コーナー、パネルディスカッション

## ステアリングメンバ(五十音順)

臼井 公孝 ソフトバンクパブリッシング(株)  
大須賀 浩 テクマトリックス(株)  
岸部 貞治 (株)ネットマークス  
則房 雅也 日本電気(株)  
犬塚 昌利 ノーテルネットワークス(株)  
三浦 竜樹 (株)アイ・ティ・アール

## ディスカッションメンバ(五十音順)

広川 智理 (株)アイ・ティ・アール  
田中 定明 (株)インターネット総合研究所  
武堂 貴宏 F5 ネットワークスジャパン株式会社  
西村 豊雄 企業通信システムエンジニアリング(株)  
福永 啓蔵 シスコシステムズ(株)  
松島 正明 新日鉄ソリューションズ(株)  
野尻 佐智子 ソフトバンクBB(株)  
濱田 久志 高千穂交易(株)  
伊藤 吉也 テクマトリックス(株)  
飯島 正行 日本オフィス・システム(株)  
世良田 照治 日本電気(株)  
相原 敬雄 日本ベリサイン株式会社  
吉田 次男 ジュニパーネットワークス(株)  
三家本 賢三 富士ゼロックス(株)  
橋口 昌弘 横河電機(株)