

安心・安全なネットワークを支える技術と富士通のソリューション

Network's Roles in Security Enhancement

あらまし

インターネットを中心とした情報インフラへの依存度を増す現代社会では、安心・安全なインフラを設計・構築し、それを日々最適に維持・運用することが至上命題となっている。インターネットに依存する社会は、利便性を飛躍的に向上させたが、一方で、一瞬にして多大な損害を被る、あるいは、危機的な事態に遭遇する危険性を増大させている。

本稿では、このような脅威に対して社会の安心・安全を確保し、向上させるためにネットワークがどのような役割を果たすことができるかを述べる。具体的には、ネットワークの信頼性や品質を高めるとともに、ネットワーク上の脅威から企業や個人を守るために取り得る安心・安全への対策・技術について述べる。また、ネットワークへの対策・技術を実際に企業のインフラに導入し、お客様の情報資産を守る富士通のソリューションを紹介する。

Abstract

Modern society now heavily depends on the Internet-based infrastructure. Along with dramatic improvements in the level of convenience, this infrastructure also brings the risk of serious disruptions to society. We must therefore ensure that this infrastructure is secure and optimally operate and maintain it. This paper describes how network technologies enhance security and help protect our society from various threats. Specifically, it outlines measures and technologies that can be applied to the network infrastructure to increase the reliability and quality of services and protect enterprises and individuals from network threats. This paper also introduces some Fujitsu products and services that apply these measures and technologies so that customers' information assets and infrastructures are protected.



今林 徹(いまばやし あきら)
FENICSシステム統括部サービス企画部 所属
現在、企業向けのネットワークサービスの企画・開発に従事。



石田健司(いしだ けんじ)
FENICSシステム統括部サービス企画部 所属
現在、企業向けのネットワークサービスの企画・開発に従事。

まえがき

インターネットを中心とした情報インフラへの依存度を増す現代社会では、安心・安全なインフラを設計・構築し、最適に維持・運用することが至上命題となっている。インターネットに依存する社会は、利便性を飛躍的に向上させたが、一方で、一瞬にして多大な損害を被る、あるいは危機的な事態に遭遇する危険性を増大させている。

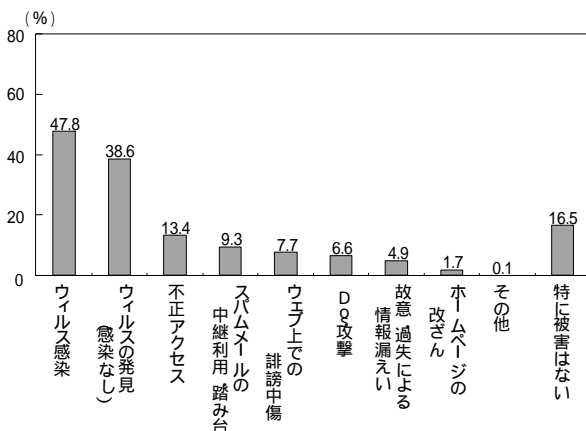
本稿では、このような脅威に対して社会の安心・安全を確保し向上させるためにネットワークがどのような役割を果たすことができるか、また、そのためにどのような対策を講じるべきかを述べる。さらに、ネットワークの対策技術を実際に企業のインフラに導入しお客様の情報資産を守る富士通のソリューションを紹介する。

ネットワークの重要性の高まりと脅威の増加

まず、インターネットを中心とするユビキタス社会がいかにネットワークに依存し、また、脅威や不確定さが増加しているかを本章では述べる。

ユビキタス社会におけるネットワーク依存

DSL (Digital Subscriber Line) や光アクセスなどの有線ネットワーク、携帯電話やモバイル無線などの無線ネットワークインフラの拡充によって、いつでもどこでも必要な情報へのアクセスが可能となるユビキタス社会が現実のものとして進展している。企業の社員や一般個人はあらゆる場所でWebや社内



(出典)総務省:平成17年版 情報通信白書 第1章第5節図表[2]より作成

図-1 企業の情報セキュリティ被害状況 (複数回答)
Fig.1-Information security damage of enterprise (two or more answers allowed).

情報資産へのアクセスを行っている。

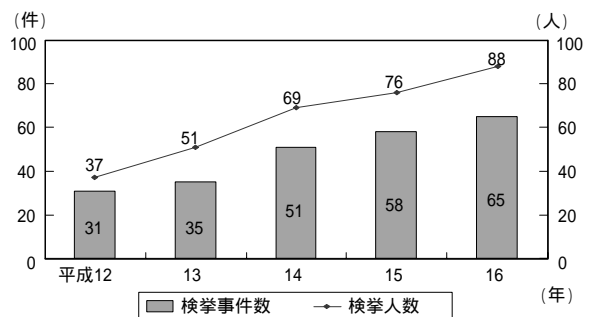
このような社会では、自然災害、人工災害、機器・回線の故障といった事象によってネットワークが利用できない場合、情報へのアクセスが失われることになり、業務や個人利用に大きな支障をきたす状況が生まれている。このため、ネットワークの信頼性への要求は以前にも増して高まっている。

また、現代人の生活は、エレベータ、発電機、自動販売機、家庭の家電機器といった社会/家庭インフラへの依存度が年々高まっている。このようなインフラが止まる、あるいは故障することによって、社会の生活は多大な不便さと損害を経験することとなり、場合によっては、人命が危険にさらされる。このようなインフラを、ネットワークを介して確実に遠隔監視・保守する重要性は日増しに強まっている。

インターネットの普及による脅威と不確定さの増加

従来のTDM (時分割多重装置) や交換機を使った通信ネットワークでは、特定場所にいるユーザだけが特定経路を通じて社内の情報インフラを利用することができた。しかし、インターネットの普及により、不特定多数の利用者が多数の経路を通じて企業の情報インフラにアクセスすることが可能となり、不正な情報アクセスやWinnyなどの共有ソフトにより情報漏えいが起こりやすい環境が作られている。このために、企業やその利用者が多大な損害を被る事態が数多く発生しており、その数は、図-1および図-2に示すように年々増加している⁽¹⁾

さらに、従来の通信回線では時分割多重方式を用



国家公安委員会・総務省・経済産業省報道資料により作成

(出典)総務省:平成17年版 情報通信白書 第1章第5節図表[5]

図-2 不正アクセス禁止法違反事件の検挙状況 (重複計上あり)

Fig.2-Number of arrests due to Anti-Unauthorized Access Law violation.

いて各情報が決められた伝送帯域を使って通信を行っていたため、各通信の品質は一定に保たれ、互いに影響することがなかった。しかし、インターネットの世界では、ベストエフォートがデフォルトとなっており、重要な通信についてはこれを間違いなく決められた時間や速度で伝送するための特別な手段を講じない限り品質が保証できないという弱点、言い換えると、ベストエフォートによる不確定さが存在している。

ネットワークにおける安心・安全対策

本章では、前章で述べた状況のもとで、ネットワークの信頼性や品質を高めるとともにネットワーク上の脅威から企業や個人を守るために、どのような安心・安全への対策が取り得るのかを述べる。

ネットワークの可用性・安全性の向上

通信回線の冗長化やバックアップといった通信手段の高信頼化を行うことにより、万一、事故や故障などによって一つの通信手段が可用でなくなったとしても、別の通信手段で情報へのアクセスを継続可能とする。この際、複数のキャリアや複数の通信経路を用いることが有効である。

また、インターネットのように不特定多数の利用者が使用するネットワークを安心・安全に使用するための技術の一つとして、二つの通信ノード間で仮想的に専用線と同等なセキュリティレベルを確保する仮想専用線（VPN：Virtual Private Network）がある。VPNを実現するための方法の一つとしてIPsecが広く利用されている。IPsecは通信の際に認証処理や、通信内容の暗号化処理を実施することにより、「機密性の確保」「完全性の確保」「送信元の認証」などを実現する。暗号化を施すことにより、例えば情報が他者に渡ったとしても容易に判読できないようにすることが可能となる。

ネットワーク越しに存在する脅威の防御

ネットワーク越しに企業のインフラに不正なアクセスを試みたり攻撃を加えたりしようとする悪意の利用者やウイルスから企業が身を守るためには、ネットワークにおいて脅威を防御する対策を施す必要がある。このような対策としては、以下の手法・技術が挙げられる。

（１）利用者や端末の制限

許可されない不正な端末によるアクセスを拒否す

る。また、ネットワークにアクセスできる利用者を認証することにより、あらかじめ許可された利用者からのみのアクセスを許容する。さらに、セキュリティレベルの低い端末のネットワークへの接続を防止する。

（２）攻撃への対策

ポートスキャン、DoS/DDoS（Denial of Service/Distributed Denial of Service）攻撃、ワーム拡散などを遮断する。

（３）不適切な通信の遮断

ファイアウォール機能を用いることにより、WinnyなどのP2P通信を検知し必要に応じて遮断する。

（４）内部ネットワークの隠蔽（NATの利用）

NAT（Network Address Translation）機能の利用により、内部アドレスを隠蔽し、外から攻撃対象となりうる内部ネットワークを見えなくする。

ネットワーク上での品質確保

帯域制御や優先制御といった機能を用いることにより、重要な情報や優先させるべき情報を、必要な時間や速度で伝送する。これによって、音声や動画といったリアルタイム性を要求されるメディアの品質を保った伝送が可能となる。

セキュアなインターネットを用いた遠隔監視

エレベータやオフィス、家庭などの遠隔監視・保守は、企業の従業員や個人の安心・安全を確保する重要な要素であり、ホームセキュリティなどのビジネスも年々拡大している。遠隔接続を行うためのネットワークとしては、安価でどこでも使えるインターネットが利用されることが望まれる。この際、機器監視やホームセキュリティは、扱う情報の秘匿性を保つことが要求されるため、VPNにより暗号化することが望まれる。

富士通のソリューション

前章で述べたネットワークにおける対策技術を実際に企業のインフラに導入し、お客様の情報資産を守るため、富士通では以下のようなソリューションを提供している。

ネットワークの可用性・安全性の向上

（１）マルチキャリア接続

富士通のFENICSサービス⁽²⁾では、複数のキャリアの回線により冗長化構成を取るマルチキャリア環

境を提供することが可能である。異なるキャリアの回線を利用することにより、あるキャリアがダウンした場合でも、他キャリアの回線が同時にダウンする可能性は低いいため、高信頼なネットワーク環境を構築することができる。このような冗長化構成は、後述の富士通のIPCOM Sシリーズ[®]やSi-Rシリーズ[®]製品を用いることにより実現可能である。

(2) 機器/通信経路の2重化

IPCOM SシリーズやSi-Rシリーズでは、VRRP (Virtual Router Redundancy Protocol) などによる機器/通信経路の2重化機能を実現しており、通信経路の障害あるいは装置障害を検知し、自動的に通信を継続可能とするネットワークを構成することが可能である。

また、図-3のように、広域イーサネットやIP-VPNなどの回線を主系回線、インターネットVPNを従系回線とし、回線障害あるいは装置障害発生時の従系回線への自動切換/復旧時の自動切戻しを実施することが可能である。複数種のネットワークを利用した通信経路の2重化により、より高信頼なネットワークを実現することも可能である。

(3) 暗号化

前章で述べたIPsecの処理は暗号化をしない通常の通信よりも複雑であり、相応のCPU能力を必要とする。Si-Rシリーズでは、そのIPsec通信に必要な各種暗号処理 { 通信暗号, IKE (Internet Key Exchange) のネゴシエーションに必要な認証と鍵の演算処理 } をハードウェアで高速処理することにより、安価な機種であっても、高い処理性能を提供している。

さらに、Si-Rシリーズの上位機種 (Si-R570/370) では通信暗号処理とIKE処理をそれぞれ独立したASICで処理することにより、各拠点とのIKEネゴシエーションが一斉に重なった場合でも安定した通信ができるように設計されている。

(4) ネットワーク機器の鍵情報の安全な保管

Si-Rシリーズ (Si-R260B/180) では、拠点ルータとして世界で初めてTCGv1.1b[®]準拠のセキュリティチップを搭載した。セキュリティチップは、認証や通信暗号化に使用する鍵情報の安全な保管機能をハードウェアで処理する。このため、外部からの攻撃に強く、高いセキュリティレベルを実現するものであり、秘密情報の第三者への流出を防止することができる。

ネットワーク越しに存在する脅威の防御

【利用者や端末などの制限】

(1) 不正なアクセスの制限

IPCOM Sシリーズでは、通過するパケットを検査することによって様々な不正アクセスを遮断することができる。MACアドレス、IPアドレス、ポート番号、メディアタイプ、アプリケーションコマンド、アクティブコンテンツ (Javaなど)、パターンマッチなどを条件としたアクセス制御を行うことによって、許可されない端末・メディア・アプリケーションの遮断が可能となる。

また、IPCOM Lシリーズ[®]では、利用者 (PC) のWeb認証を行うことによって、許可された利用者 (PC) 以外からのネットワークおよびその配下の情報資産の利用を止め、不正なアクセスを防ぐことが可能である。例えば、IPCOM L 1400では、

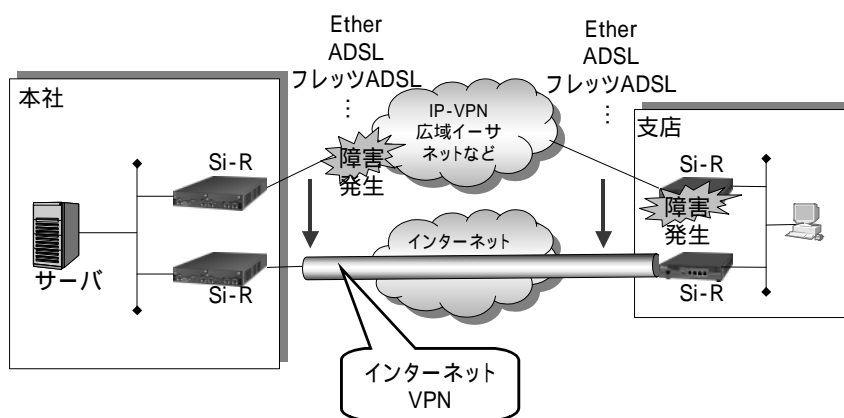


図-3 通信経路の2重化
Fig.3-Circuit redundancy.

500台の端末の認証が可能である。また、富士通のRADIUS認証サーバであるSafeauthor[®]との組合せにより、ActiveDirectoryとの連携も可能である。

(2) 不適切なPCのアクセス制限 (WinnyなどのP2P通信ソフトなどへの対策を含む)

IPCOM Lシリーズを富士通の検疫サーバであるSystemwalker Desktop Inspection (DTI) ⁽⁷⁾と連携して用いることにより、セキュリティ対策レベルの低いPC (WindowsなどのOSのパッチレベルの低いPC、ウイルス対策ソフトのインストールがされていないPC、WinnyなどのP2P通信ソフトを搭載したPC、など)のネットワークへの接続を防ぐことが可能である。IPCOM Lシリーズは、PCがネットワークに接続される際に、Webブラウザなどを通してDTIとの間で認証を行うことにより、不適切なPCのアクセス制限を実施する (図-4)。許可するセキュリティ対策レベルの設定は、DTIへのチェックポリシーの適用により行う。チェックポリシーの適用により、WinnyのようなP2P通信ソフトを検疫するウイルス定義ソフトの最新版の適用を万全にすることができ、その結果、情報漏えいを未然に防ぐことが可能となる。

【攻撃に対する防御】

(1) サービス妨害 (DoS/DDoS) 攻撃への対策

IPCOM Sシリーズでは、TCP/UDPポートスキャン攻撃、SYN Flood、UDP Flood、Smurfなど

の遮断を行う。これによりDoS攻撃を防御するとともに、DDoS攻撃の前段階として悪意者が行うであろう踏み台化攻撃を防御しDDoS攻撃自体の起こる可能性を下げる効果が期待できる。

(2) ワーム拡散防止 (通信フィルタリング)

ワームは、Eメール型ワーム、ネットワーク探索型ワーム、WebやP2P通信を利用し感染するワームに分類が可能である。IPCOM Lシリーズではこのうち、SQL SlammerやMSBlasterといったような「ネットワーク探索型ワーム」を検知の対象とする。

IPCOM Lシリーズは、独自の「ワーム振る舞い検知専用ハードウェア」を搭載し、従来方式では防げない未知ワームの初期拡散の防止に効果を発揮する。ネットワーク探索型ワームに感染した場合、大量に新しいフローが発生することによってネットワーク機器の負荷が上がったり、ネットワークの輻輳^{ふくそう}が発生したりする。ネットワーク探索型ワームは、脆弱性が発見されてから十分な対処が施される前に一瞬で感染を広げてしまうため (0-day attackという)、近年最も問題視されているワームであるが、従来方式であるシグニチャ方式ではこのような新しいワームを検知できない。IPCOM Lシリーズはこの拡散防止に効果を発揮する。さらに、全パケットを10 Gbpsフルパケットでモニタリングすることが可能である。装置内部で全パケットを10 Gbpsフルキャプチャしてワームを検知するため、

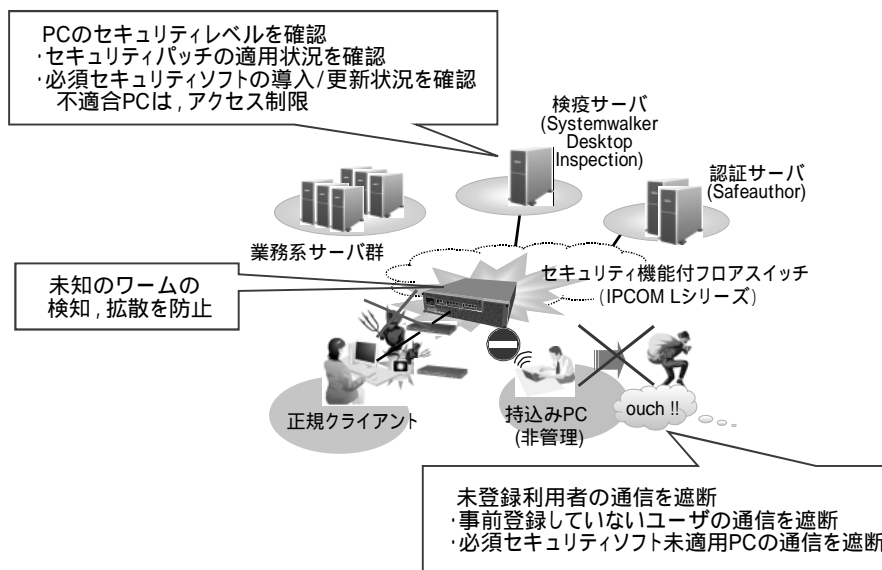


図-4 アクセスセキュリティのソリューション
Fig.4-Solution for access security.

トラフィック量に依存することなく、ワームを検知することができる点も特長である。シグニチャ方式の不正侵入防止システム（IPS：Intrusion Prevention System）の場合は、トラフィックが増えた際、検知率が下がる、あるいは中継性能が劣化する傾向にあるが、IPCOM Lシリーズのアーキテクチャはその問題を解決している。

【不適切な通信の遮断（WinnyなどのP2P通信の遮断）】

IPCOM SシリーズやIPCOM Lシリーズのファイアウォール機能を用いることにより、WinnyなどのP2P通信を検知し、これを遮断することが可能である。

また、IPCOM Sシリーズの帯域制御機能を利用すれば、通信を許可されたP2P通信の帯域を制御し抑圧することもできる。この機能により、P2P通信を用いて大容量のデータファイル（映像など）が交換されることでサービスプロバイダや企業のネットワークが逼迫することを防ぐことが可能となる。IPCOM Sシリーズでは、P2Pアプリケーションがデータ通信に使用するTCP/UDPポート番号を追跡しP2Pアプリケーションのデータ通信トラフィックを定義されたトラフィック・クラスとして自動的に認識する。この機能により、ダイナミックなTCP/UDPポート番号を意識することなくトラフィック・クラスにアプリケーション種別を指定するだけで簡単に帯域管理ができる。

【内部ネットワークの隠蔽】

IPCOM SシリーズやSi-Rシリーズでは、NAT機能によるアドレス変換を用いて内部ネットワークを隠蔽することが可能である。すなわち、外から見えるアドレスは内部の端末のアドレスとは異なる体系となっているため、外部から攻撃先の端末を指定することができない。

ネットワークの高品質の確保

IPCOM SシリーズやSi-Rシリーズの帯域制御機能を用いることで、回線を通る情報を音声・ビデオ・データといった種類に応じて優先付けし、また、それぞれの種類の情報が回線の中で使用する帯域を設定することができる。これによって音声・ビデオのリアルタイム性を保ち品質を確保することが可能となる。帯域制御方式は、IPCOM Sシリーズでは双方向に帯域制御を行える独自方式のBTC

（Bi-directional Traffic Control）を用い、Si-RシリーズではWFQ（Weighted Fair Queuing）を適用している。

遠隔監視におけるVPNの利用と管理性の向上

FENICSのビジネスVPNサービスを用いることにより、インターネットを用いた遠隔監視・保守などにおける通信の秘匿性を保つことができる。さらに、ビジネスVPNのサービス状況はFENICSのセンタにより常時監視されているため、インターネットを用いながら管理性を向上させることが可能となる。

む す び

本稿で述べたように、富士通では、インターネット社会の各種の脅威や不確定さから企業や個人を守るため、様々な製品やサービスをお客様に提供している。今後、インターネットやユビキタス環境は一層の速度をもって進展し、新しい脅威が生まれることが予想される。富士通は、これらの脅威からお客様の情報インフラを未然に、あるいは迅速に守るためのネットワーク製品およびサービスの提供を積極的に進めていきたい。

参考文献

- (1) 総務省：平成17年版 情報通信白書 第1章 「u-Japan実現に向けた課題」第5節，2005，p.100-114 .
- (2) 富士通：ネットワークサービス .
<http://fenics.fujitsu.com/networkservice/index.html>
- (3) 富士通：ネットワークサーバIPCOM（アイピーコム）.
<http://primeserver.fujitsu.com/ipcom/>
- (4) 富士通：PアクセスルータGeoStream Si-Rシリーズ .
<http://fenics.fujitsu.com/products/sir/>
- (5) Trusted Computing Group (TCG) .
<https://www.trustedcomputinggroup.org/>
- (6) 富士通：ユーザ認証ソフトウェアSafeauthor（セーフオーサー）.
http://segroup.fujitsu.com/secure/catalog/files/Safeauthor_CZ4056-4.pdf
- (7) 富士通：Systemwalker Desktop Inspection（デスクトップ インスペクション）.
http://systemwalker.fujitsu.com/jp/desktop_inspection/