特集

統合をコンセプトにネットワークの安定性・安全性を実現するIPCOM EXシリーズ

IPCOM EX Series for Realizing Network Stability and Safety

あらまし

企業システムに対する安定性・安全性に対する要求はますます高まってきている。
本稿では，企業システムを構成しているネットワークの立場から，まず，安定性・安全性を実現するWANエッジ領域とサーバフロント領域を説明し，それぞれの領域における安定性・安全性を阻害する要因とそれへの対策となる機能について述べる。つぎに，富士通のネットワークサーバIPCOM EXシリーズにおいて，「統合」の基本コンセプトの基で，従来機種で培った安定性を実現する機能に加えて，導入・設計の簡素化と運用・トラブルシューティングの簡素化を図ったことを述べ，さらに本シリーズにおいて強化した安定性，シンプル性，安全性について述べる。最後に，本シリーズのWANエッジ領域とサーバフロント領域への適用事例について紹介する。

Abstract

Safety and stability are essential requirements in today's corporate systems. This paper discusses network safety and stability in the WAN-edge and server-front areas from the viewpoint of network infrastructure. Then, it describes the obstacles to achieving safety and stability in these areas and how these obstacles can be overcome. Next, this paper discusses the concept of integration for the NETWORK SERVER IPCOM EX series from the viewpoints of design, installation, and troubleshooting. Lastly, it shows how the IPCOM EX series provides safety and stability by using several examples of their application in WAN edge and server-front areas.

天満尚二（てんま　しょうじ）
システムフロント事業部 所属
現在，IPCOM製品の企画開発に従事。

ま え が き

企業システムは，新たなビジネス，M&A，アライアンスなどにスピーディに対応していかなければならない。そのためには，ネットワークを介した安定したシステム間連携は不可欠である。さらに，インターネットの一般化は，企業システムに，今まで以上に，24時間365日止まることのない安全なサービスを提供し続けることを求めている。このように，企業システムへの安定性・安全性に対する要求はますます高まるばかりである。

本稿では，企業システムを構成しているネットワークの立場から企業システムに求められる安定性・安全性の実現方法について述べ，安定性・安全性を容易に実現することを目指して開発した富士通のネットワークサーバIPCOM EXシリーズの役割，機能について，適用例を交えて紹介する。

ネットワークにおける安定性・安全性

本章では，ネットワークにおいて安定性・安全性を実現する領域を定義し，それぞれの領域に求められる安定性・安全性について，阻害要因とその対策のためのネットワーク機能を示す。

● 安定性・安全性を実現する領域定義

ネットワークにおいて安定性・安全性を実現する領域を**図-1**に示す。

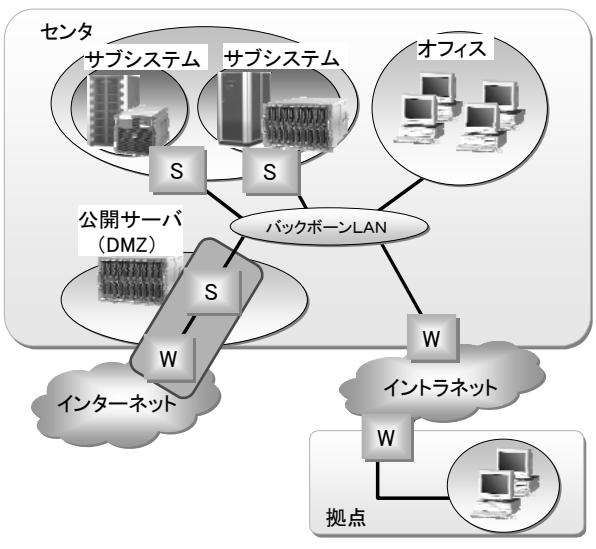


図-1　安定性・安全性を実現する領域
Fig.1-Key area for stability and safety.

(1)　WANエッジ領域（W）

WANエッジ領域は，インターネットやイントラネットなど，広域ネットワークと企業システムを接続する領域である。この領域では，広域ネットワークを介したアプリケーションとの通信の安定性・安全性が求められる。また，とくに，インターネットとの接続においては，アクセスの急増や不正なアクセスから企業システムを守る安全性の確保が求められる。

(2)　サーバフロント領域（S）

サーバフロント領域は，サーバ群とバックボーンLANとの接続など，サーバ群にアクセスする入り口領域である。この領域ではサーバ群が提供するアプリケーションに対するアクセスの安定性・安全性が求められる。

以下では，各領域における安定性・安全性を阻害する要因とその対策のためのネットワーク機能を示す。

● WANエッジ領域における安定性・安全性

【WANエッジ領域における安定性】

WANエッジ領域において求められる安定性は，前述のように，ネットワークを通したアプリケーションとの通信の安定性である。

トランザクションデータのみならず画像や音声など，様々なデータが行き交うIPネットワークでは，専用線以上に通信の安定性が阻害され得る。以下，その要因例と対策のための機能を示す。

(1)　安定性を阻害する要因例

・回線やルータなど，ネットワークと接続する機器の故障
・アクセス回線の異常
・特定のアプリケーションによる通信量の急激な増加

(2)　安定性を実現する機能

上記阻害要因が発生しても企業システムに影響を与えない（換言すると，サービスが停止しない）ためには，以下の機能が必要となる。

・リンク負荷分散機能

企業システムを複数の回線を通してインターネットやイントラネットと接続し，接続した複数の回線すべてを常に利用することで，ルータなどの機器の故障やインターネットやイントラネットの異常により通信が不通となった場合に，残った正常な経路を

使って通信を継続する機能である。

・レイヤ7帯域制御機能

回線を利用しているアプリケーションごとに通信量を監視し，特定のアプリケーションの通信量が急激に増加した場合，あらかじめ定められた通信量に制限し，ほかのアプリケーションの通信を保護する機能である。ルータなどが提供するQoS機能（シェイピング機能とも呼ばれる）は，広域ネットワークに出力する通信量のみを制御するのに対し，本機能は広域ネットワークとの入出力（双方向）の通信量を制御するため，入力データの急激な増加に対しても対応することが可能である。

【WANエッジ領域における安全性】

前述のように，インターネットとの接続において特に安全性が要求されることから，以下ではインターネット接続を前提に，安全性を阻害する要因と対策のためのネットワーク機能について示す。

(1) 安全性を阻害する要因例

・サーバなどへの認められていないアクセス（不正アクセス）

・不正を働くプログラム（ウイルスなど）の外部からの送り込み

・認めていないインターネット（Webサーバ）への内部からのアクセス

・通信データをのぞかれたり（盗聴），書き換えられたりされる行為（改ざん）

(2) 安全性を実現する機能

前記阻害要因に対して，以下の機能により企業システムを保護することができる。

・ファイアウォール機能

認めていないアドレスやポートへのアクセスを遮断することにより，サーバなどへの不正なアクセスからシステムを防御する機能

・アンチウイルス機能

コンピュータウイルスの特徴など（パターン）を記録したデータファイルと通信データを照合し，内部にウイルスが検知された場合，除去もしくは警告を行う機能

・Webコンテンツフィルタ機能

インターネットで不適切な情報にアクセスしないように閲覧に制限をかけることで，Web経由での情報漏えいを防御する機能

・VPN（Virtual Private Network）機能

センタと拠点間，もしくは拠点内のPC間で暗号通信を行うことにより，仮想的に専用線とし，ほかからの盗聴や改ざんから通信データを保護する機能

● サーバフロント領域における安定性・安全性

【サーバフロント領域における安定性】

サーバフロント領域において求められる安定性は，サーバが提供するアプリケーションに対するアクセスの安定性である。

(1) 安定性を阻害する要因例

・サーバの故障や定期保守などによる停止

・特定のサーバに対する処理要求の集中による負荷の増大から生じるレスポンスの悪化

・動画配信などの特定アプリケーションによる通信量の急激な増加から生じるレスポンスの悪化

(2) 安定性を実現する機能

前記阻害要因が発生してもアプリケーションの応答性を維持するためには，以下の機能が必要となる。

・サーバ負荷分散機能

特定のサーバにアクセスが集中しないように，サーバ状態を監視しながら，負荷の軽いサーバにアクセスを振り分ける機能

本機能はサーバの状態を監視していることから，サーバの故障や保守によりサーバが停止した場合に，ほかのサーバにアクセスを振り替えることができ，サービスの停止を回避することができる。

また，本機能により，サーバへのアクセス数に制限を加えることで，サーバの負荷上昇を抑え，よりアクセスを安定化することが可能となる。

・アクセラレータ機能

負荷が高い処理をサーバ上で実行した場合，アクセスの集中により，サーバ負荷が急激に上昇する。このようなサーバで処理した場合に，高いサーバ負荷を必要とする機能をネットワーク機器にオフロードすることをアクセラレータ機能と言う。例えば，SSL（Secure Socket Layer）通信など，暗号処理はサーバ負荷の高い処理であり，SSL通信処理そのものをネットワークにオフロードすることにより，安定したレスポンスを実現することができる。

【サーバフロント領域における安全性】

(1) 安全性を阻害する要因例

・サーバなどへの認められていないアクセス（不正アクセス）

・不正を働くプログラム（ウイルスなど）の内部からの送り込み
・認められていないインターネット（Webサーバ）への内部からのアクセス
・通信データをのぞかれたり（盗聴），書き換えられたりされる行為（改ざん）

(2)　安全性を実現する機能

前記の阻害要因は，WANエッジ領域における安全性の阻害要因と同じである。したがって，安全性を実現する機能も同様の機能が必要とされる。

今や，安全性を阻害する要因の発生は，外部からのみではないため，内部に対しても対策が必要とされている。実際，社会システムなどでは，業務システムごとにファイアウォールを設置したり，データセンタ内の通信を暗号化したりするシステムが構築され始めている。

以上述べた，WANエッジ領域とサーバフロント領域に求められる安定性・安全性，および実現する機能を**表-1**にまとめて示す。

IPCOM EXシリーズのアプローチ

前章で述べた安定性・安全性を実現する様々な機能は，企業システムを構築・運用する上で基本的に必要とされるものである。IPCOMは，これらの多くの機能を簡単にスピーディに利用できるように，「統合」を基本コンセプトに実現してきた（**図-2**）。

IPCOM EXシリーズでは，従来機種で培ったレイヤ7帯域制御機能やリンク負荷分散機能，サーバ負荷分散などの安定性を実現する機能を基盤[1),2)]に加えて，安定性の実現に不可欠となってきているアンチウイルス機能やWebコンテンツフィルタ機能など，安全性を実現する機能を新たに統合した。

さらに，製品ラインナップにおいては，前述の安定性と安全性を実現する領域と機能の関係に着目し，適用領域と使用用途ごとに製品ラインを設け，購入後も段階的に拡張できる製品構成とすることにより，適用のしやすさを追求した。

IPCOM EXのラインナップを**図-3**に示す。

●　統合の目的

統合の目的は大きく，導入・設計の簡素化と運用・トラブルシューティングの簡素化の2点である。

以下，それぞれについて説明する。

(1)　導入・設計の簡素化

安定性・安全性を実現するためには前述のように，多くの機能を必要とする。そのため，従来は，多くの機器を組み合わせる必要があった。設計や導入に

表-1　安定性・安全性を実現する領域と機能

		WANエッジ	サーバフロント
安定性・安全性を実現する領域		インターネットやイントラネットなど，広域ネットワークと接続する領域	サーバ群にアクセスする入り口領域
安定性	求められる安定性	ネットワークを通したアプリケーションとの通信の安定性	アプリケーションへのアクセスの安定性
安定性	安定性を実現する機能	リンク負荷分散機能 レイヤ7帯域制御機能	サーバ負荷分散機能 アクセラレータ機能
安全性	求められる安全性	不正アクセスやデータの盗聴，改ざんからシステムを保護	
安全性	安全性を実現する機能	ファイアウォール機能，アンチウイルス機能，Webコンテンツフィルタ機能，VPN機能など	

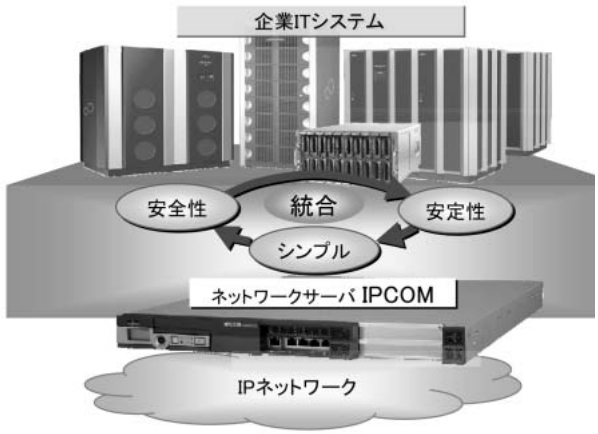


図-2　IPCOMの基本コンセプト「統合」
Fig.2-“Integration” - IPCOM basic concept.

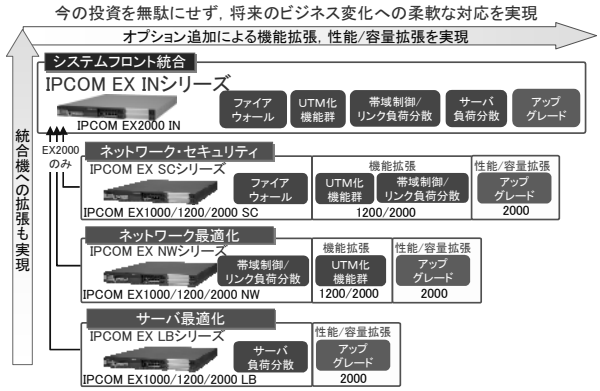
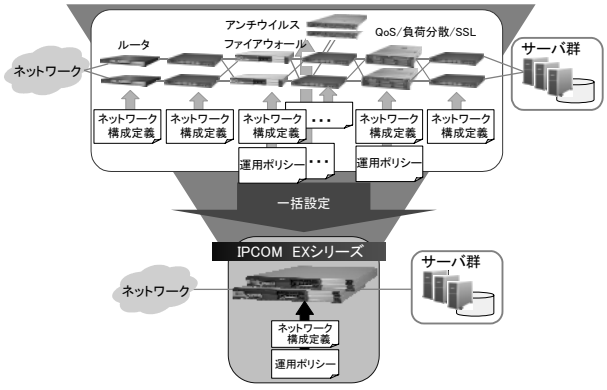
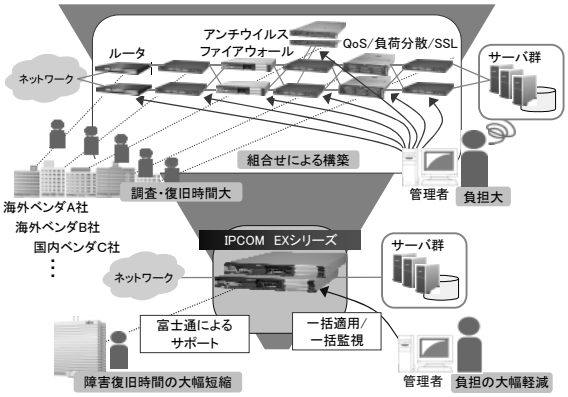


図-3　IPCOM EXシリーズラインナップ
Fig.3-IPCOM EX series lineup.



(a) 設計・作業の工数削減



(b) 運用・トラブルシューティングの簡素化

図-4 「統合」の目的
Fig.4-Merit of "Integration" on design and/or installation.

当たっては,
・機器が提供する機能間の整合性の確保
・機器が故障した場合の迂回路の確保
・様々な機器の設定，操作方法の習得
などが必要であり，多くの機器を組み合わせることで複雑な設計，複雑な検証作業など，工数の増加を招くとともに，かえって安定性を欠くシステムとなりかねなかった。そこで，必要とされる機能を統合することによって,
・機能間の整合性は機器が保証
・迂回路を考慮することなく簡単な設計
が可能となり，設計工数，作業工数を削減できる{**図-4** (a)}。

(2) 運用・トラブルシューティングの簡素化

機器の組合せにより安定性・安全性を確保しようとすると，機器数が増えるため,
・機器故障時の影響範囲の特定が困難
・トラブルシューティングが複雑
・機器のベンダが異なった場合，ベンダ間で共同調査が必要となるが，ベンダ間の調整などによる共同調査は更に困難となる，といった問題が生じる。
統合された場合，1ベンダで1装置となるため，このような問題は解消される{図-4 (b)}。

● **段階的拡張の目的**

前節で述べた観点から，IPCOMでは製品の初期出荷より統合を基本コンセプトとし，製品を展開してきた。以下では，IPCOM EXシリーズにおける統合について述べる。

企業システムは，事業の発展に合わせ，計画的に発展させていくことが望ましい。このような企業システムにとって，初期のシステム構築の段階から必要と思われる機能をすべてそろえることは初期投資の増大や計画変更が発生した場合に投資の無駄を生むことにつながる。また，企業システムのネットワークインフラにおいて，新たに必要となった機能の増強を行う場合に，長時間のサービス停止を伴うことは許されない。

IPCOM EXシリーズは，このような問題を解決するために，一度導入した装置を段階的に機能拡張できる仕組みを設けることで対応した。

ファイアウォールを最初に導入し，アンチウイルス機能の追加，サーバ負荷分散機能の追加と段階的にシステムを拡張させた例を**図-5**に示す。

他社製品の場合には，機能を追加する都度，機器の追加が必要となり，設置スペース，電力などの確保から始まり，既存システムと新規に導入する機器が提供する機能との整合性の確認まで，システムの新設計に匹敵する作業工数が必要となる。

一方，IPCOM EXシリーズの場合，ライセンスを追加設定するだけで必要とされる機能を活性化でき簡単に，また，短期間でシステム増強を行うことができる。

IPCOM EXシリーズの強化ポイント

本章では，IPCOM EXシリーズの強化ポイントについて述べる。

(1) 安全性の強化

WANエッジ領域で企業システムが対応しなければならないセキュリティ脅威は多様化してきており，IPCOM EXシリーズではファイアウォール（一部IPS機能を含む）に加え，従来対応できていなかっ

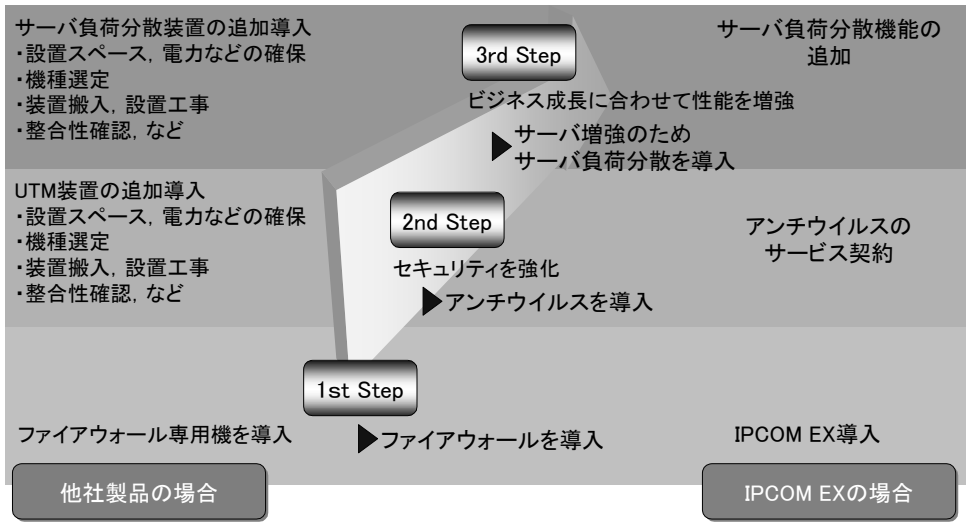


図-5　段階的な成長の適用例
Fig.5-Example of step by step upgrade.

たアンチウイルス機能，Webコンテンツフィルタ機能にも対応し，UTM（Unified Threat Management）として必要とされる機能をカバーした。

(2)　シンプル性の強化

ブレードサーバの登場を契機に，サーバのセンタ統合が進んでおり，それとともに，セキュリティの脅威も1箇所に集中してきている。したがって，脅威が集中するサーバフロント領域において集中した脅威対策を実施することは，効率的，かつ効果的である。IPCOM EXシリーズでは，これに対応すべく，サーバフロント領域におけるセキュリティ対策機能の強化・充実を図るため，業界で初めてサーバ負荷分散機能とUTM機能を統合した。

(3)　安定性の強化

24時間365日無停止のサービスが求められる中，セキュリティ対策などの機能強化の作業のために，長時間にわたってシステムを停止することは許されない。IPCOM EXシリーズは，このような機能強化においてもあらかじめインストールされている機能モジュールをライセンス（オプション）により活性化するだけで，装置を停止することなく機能追加ができるようにすることで，安定性を強化した。

以上で説明したように，IPCOM EXシリーズでは，統合のコンセプトのもとで前記の三つの強化を図ることにより，

・初期費用を40%減
・設置スペースと消費電力をそれぞれ1/8へ
・サポート費用を1/2へ

（いずれも，当社比）を実現してきた。

IPCOM EXシリーズ適用例

本章では，WANエッジ領域とサーバフロント領域それぞれへのIPCOM EXシリーズの適用例を紹介する。

(1)　WANエッジ領域へのIPCOM EXシリーズ適用

オフィスとインターネットを接続するネットワークにおいて，IPCOM EXシリーズを適用した例を**図-6**に示す。これは，IPCOM EXシリーズの

・リンク負荷分散
・レイヤ7帯域制御機能

により，アクセス回線の異常や通信量の急増に備えた安定性を確保し，さらに，UTM機能（ファイアウォール，IPS，アンチウイルス，Webコンテンツフィルタ）により，インターネットからのセキュリティ脅威に備えた安全性を確保した例である。IPCOM EXの統合コンセプトにより，上記機能を1台で実現し，シンプルにシステムを構築した。

(2)　サーバフロント領域へのIPCOM EXシリーズ適用

メールシステムにIPCOM EXシリーズを適用した例を**図-7**に示す。これは，従来，サーバで実現していたアンチウイルス機能やアンチスパム機能と

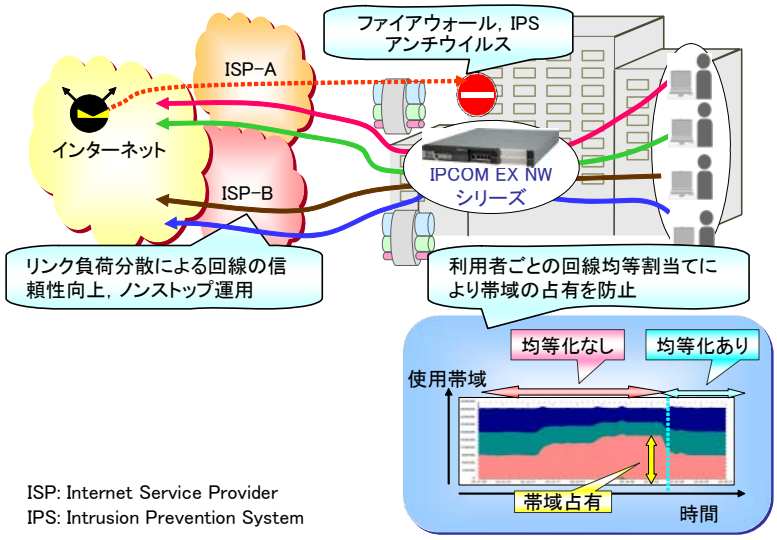
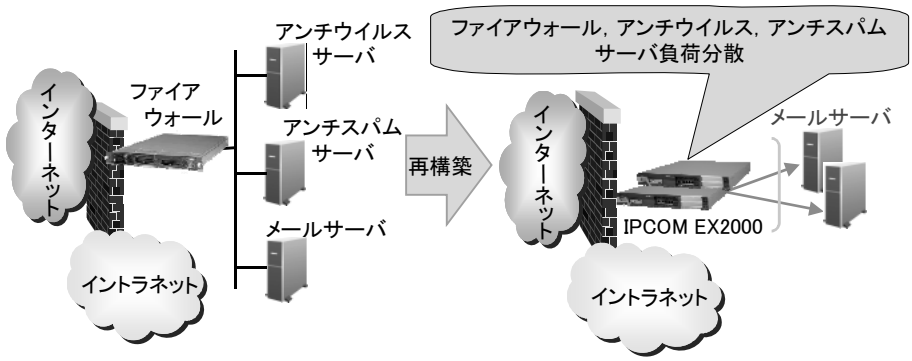


図-6　WANエッジ領域へのIPCOM EXシリーズの適用例
Fig.6-IPCOM EX series case study at WAN edge area.



（a）既存システム　　（b）IPCOM EX2000を導入したシステム

図-7　サーバフロント領域へのIPCOM EXシリーズの適用例
Fig.7-IPCOM EX series case study at serverfront area.

ファイアウォール機能を，IPCOM EXの統合コンセプトにより，1台で実現した例である。IPCOM EXシリーズの導入により，複数台にまたがるサーバの設定，カスタマイズ作業などがIPCOM EXシリーズ1台に簡素化され，さらに，今後，メール量が増加し，サーバ増設が必要となった場合も，メールシステムを止めることなくサーバ増設を可能とした。

むすび

以上，ネットワーク機能による企業システムの安定性・安全性についてIPCOM EXシリーズを例に述べた。

IPCOMは，今後も，統合を基本コンセプトに，さらなる強化を進め，企業システムの安定性と安全性に貢献すべく，継続的に進化をさせていく。

参考文献

(1)　天満尚二：シンプルで高信頼なネットワークサーバ．*FUJITSU*，Vol.56，No.1，p.47-53（2005）．
(2)　日経BP：富士通 新たなる挑戦．東京，日経BP，2004，p.111-116.