〈製品/ハードウェア〉

マルチレイヤスイッチ「UNIVERGE IP8800/700シリーズ」

Technology of IP8800/700 as UNIVERGE-IP Series

中牟田竜也* Tatsuya Nakamuta
秋山智律* Tomonori Akiyama
阿部裕司** Yuji Abe
谷川智彦*** Tomohiko Tanikawa
市橋将孝† Masataka Ichihashi
永田泰史† Yasufumi Nagata

要　旨

パソコンでのGigabit Ethernet標準装備によって高速LANの普及とともに安価なネットワーク構築への需要が高まり，国内LANスイッチ市場は成長を続けています。一方，システムを構築する上で，よりセキュアなネットワーク機能がLANスイッチにも求められるようになってきています。

IP8800/700シリーズは，ES4000という専用ASICによるチップセットを搭載することにより，マルチレイヤスイッチとしての機能，性能を高めているとともに，利便性の高い認証サービスを提供する認証機能を実装するなど，信頼性に配慮したレイヤ3スイッチとして，UNIVERGE-IPシリーズを構成します。

As the recent PCs generally support Gigabit Ethernet, the demand for inexpensive networks increases and high-speed LAN technologies become popular. This is the reason why the domestic market of LAN switches is growing up. On the other hand, more secure features are required for the next-model LAN switches.

IP8800/700 series are the Layer 3 switches that contain the ES4000 in-house developed ASIC chip set. It achieves high level features and performance. It also allows the user-friendly security services with its authentication functions. UNIVERGE-IP series consists of this IP8800 series focused on such high reliability.

1．まえがき

インターネットの普及にともない，ネット上での電子取引は急増し，自治体や公共施設への申請手続きなどを電子化する“電子政府”計画もスタートしています。このような環境下で，今後，個人情報の漏洩に対する防御が重要な課題になってきます。加えて，2005年4月1日に個人情報保護法案が施行されることで，顧客情報を中心とした情報セキュリティ管理は企業にとっていっそう重要性を帯びてきています。また，市町村合併が進む地方自治体のネットワーク再編でも住民情報の保護への対策需要が高まっています。

特にネットワーク内部からの不正アクセス行為は対策が難しく，相次いで起こった大手インターネットプロバイダの顧客情報流出のケースを始めとして情報漏洩の7割は内部犯行によるともいわれていることからも，強固なセキュリティ機能を有することが，今後のスイッチ機器選びの大きなポイントになっています。

1.1　装置概要

IP8800/700シリーズは，ネットワーク接続時にユーザや端末の識別を行い，本人であることを認証した上で接続を許可するといった認証サービスを実現するスイッチ認証機能を提供します。

セキュリティ対策だけでなく，ハードウェアのインフラ管理面においてもIP8800/700シリーズは電源・CPU（Central Processing Unit）などの基幹部分二重化構成，VRRP（Virtual Router Redundancy Protocol）による装置冗長構成，RSTP（Rapid Spanning Tree Protocol）による高速復旧などの機能で高い信頼性を保証しています。さらに，上位モデルでは構築されたセキュアなシステム上で10Gbpsの大容量バックボーンや10/100/1000Mbpsの3speed対応高収容オプションも利用可能です。

1.2　製品仕様

IP8800/700シリーズは**図1**に示すとおり，フロアLAN向けの下位モデル3機種，バックボーンLAN向け上位モデル3機種というラインナップからなり，かつこれらはすべてES400チップセットを搭載し，同じアーキテクチャで動作

＊ IPネットワーク事業部
IP Networks Division
＊＊ 第一コンピュータソフトウェア事業部
1st Computer Software Division
＊＊＊ NECソフト静岡支社
NEC Soft, Ltd. Shizuoka Branch Division
† NECエンジニアリング
NEC Engineering, Ltd.

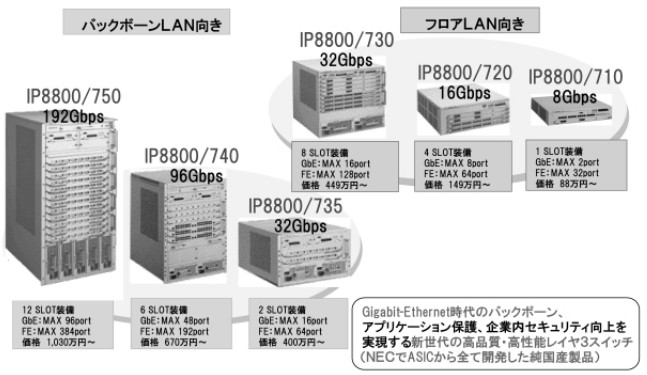

図1　IP8800/700シリーズ概要
Fig.1　IP8800/700 Series Lineup.

するため高いシステム親和性を有しています。

モデルごとの本体，およびオプションカードの諸元はそれぞれ**表1**，**表2**のとおりとなります。これらを組み合わせることで多様なネットワーク環境に対応します。

2．IP8800/700シリーズハードウェアの特徴

IP8800/700シリーズは，自社製ASIC（Application Specific Integrate Circuit）によるスイッチチップセットES4000を全モデルに採用することでスイッチング容量8Gbpsのエントリーモデル710Bから，192Gbpsの最上位750まで6モデルを統一アーキテクチャで構成しています。

これによりネットワーク規模に適したモデルを選択できるとともに，統一した管理手段により運用コストの大幅削減を実現することができます。

ES4000は，8レベルのQoS（Quality of Service）制御を実現するパケットスイッチ・エンジンPSE（Persistent Storage Engine），IPv6をハードウェア制御するフォワーディング・エンジンPFE，クロスバスイッチ・エレメントXSEの3種類のチップセットから構成されます。

表1　本体諸元
Table 1　IP8800/700 Specifications.

項　目	下位モデル			上位モデル		
	710B	720	730	735	740	750
拡張スロット数	1	4	8	2	6	12
性能（Mpps）	6	12	24	24	72	144
IPホストテーブル	47万	47万	120万	120万	280万	280万
ルーティングテーブル	47万	47万	120万	120万	280万	280万
MACテーブル	24万	48万	96万	96万	288万	576万
定格電力（W）	150	350	650	650	1300	2600
重量（kg）	9.8	20	50	30	80	170
ルーティングプロトコル	IPv4 （RIP/RIP2，OSPFv2，BGP4，Static） IPv6 （RIPng，OSPFv3，BGP4+，Static）					
サポートVLAN	ポートベースVLAN，MACベースVLAN， IPサブネットVLAN，プロトコルベースVLAN， TAG-VLAN，プライベートVLAN，Extended-VLAN					

表2　オプション諸元
Table 2　Option Module Specifications.

下位モデル	10/100BASE-TX 16portモジュール
	1000BASE-X 2portモジュール
上位モデル	10/100BASE-TX 32port+SFP4portモジュール
	1000BASE-X 8portモジュール
	10GBASE-LR モジュール
	10/100/100BASE-Tx 20portモジュール

2.1　様々な形態のEthernetをサポート

IP8800/700シリーズは，レガシーインタフェースである10/100BASE-Tに加えて，GigabitインタフェースにGBIC（Gigabit Interface Converter）を採用し，1000BASE-SX，1000BASE-LX，1000BASE-LH（長距離70km）をサポートします。また，昨今のサーバネットワークの強化に対応して，カテゴリ5ケーブルによるGigabitEther規格である1000BASE-Tのサポートも行っています。さらに高速なバックボーンネットワークとして，10GbitEthernetをサポートした10G-BASE-LRモジュールもサポートしています。これにより，10Mbps～10Gbpsまでの速度を同一のEthernetアーキテクチャ上で構成することができます。

2.2　10GbitEthernetモジュール

図2に示すように，IP8800/700の10G-BASE-LRモジュールはエンジンモジュールと10G-BASE-LRラインモジュールから構成されています。

エンジンモジュールには，フルワイヤ速度でルーティング，キューイング処理を行うES4000チップセットが実装されています。

10G-LRラインモジュールには，このエンジンモジュールを利用し，10Gbpsで受信したパケットを8+2本のGigabit Etherに分散/集約させるMUX-10GエンジンをFPGAで開

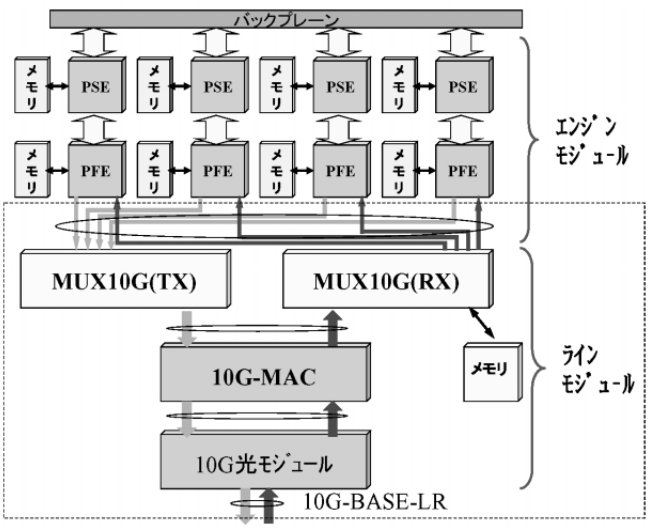

図2　10G-BASE-LRモジュールブロック図
Fig.2　10G-BASE-LR Module Block diagram.

発，実装したことで，従来のES4000チップセットの特徴であるIPv6対応，QoS機能，ハードウェアによる高速フィルタリング機能などを10Gbpsのワイヤ速度で実現しています。

2.3 10/100/1000BASE-Tモジュール

よりフレキシブルなネットワーク構築要求に応えるため，今回IP8800/700シリーズでは20ポートの10/100/1000BASE-Tポートを持つ新規モジュールの開発を行いました。

この10/100/1000BASE-Tモジュールにより既存のカテゴリ5ケーブルにより，10MbpsのレガシーLANからGigabit Etherまでを1つのモジュールで収容することが可能となります。また，20ポートの多ポート収容を実現できるので，ポート単価を下げシステム構築コストの削減にも寄与することができます。さらに今秋には本モジュールの機能強化として，20ポートのうち任意のポートに対して，2レベルの優先度を備える付加価値を追加予定です。これにより，サーバ接続ポートには高い優先度を，クライアントPCには通常の優先度を与え，スイッチの帯域を有効に活用することを可能とします。

2.4 Ethernetの信頼性向上

IP8800/700シリーズはこれら高速，大容量化するとともに高い信頼性が要求されるネットワークに対して，IEEE802.3adリンクアグリゲーションやIEEE802.1w RSTPといった冗長化技術を装備し，これらEthernetの信頼性を向上させています。

10G-BASE-LRモジュールでの最大4本のリンクアグリゲーションを実現することにより，最大40GbpsまでのEthernetをシームレスに高い信頼性で構成することが可能です。

また，装置単体での信頼性向上施策として「活線挿抜によるオンライン保守機能」「電源，制御部二重化による冗長化機能」などを備え，ハードウェア上での信頼性向上も実現しています。

3．ソフトウェアソリューション

IP8800/700シリーズでは，強固なユーザ管理機能や拡張機能を有する認証VLANと，比較的簡易でかつ世界標準機能でもあるIEEE802.1Xの2つの認証機能を実装しています**図3**。これにより，ユーザ環境に合わせて最適な認証サービス環境を選択することができます。

3.1 IEEE802.1Xによる認証機能

IEEE 802.1X認証機能では，**図4**で示すとおり，IP8800/700シリーズを介して，RADIUSサーバとWindows XP などに標準装備されているSupplicantと呼ばれるクライアントソフトウェアを用いた，比較的手軽な認証ネットワークの導入が可能になります。

さらに，IEEE 802.1X認証では，様々な認証方式を選択することが可能なEAP（Extensible Authentication Protocol)という認証プロトコルを用いるため，ID/パスワードを用いた単純なネットワーク認証から，電子証明書を用いたPKI（Public Key Infrastructure）認証などのセキュリティレベルの高いものまで，用途に応じた幅広いネットワークセキュリティ環境の構築が可能になります。

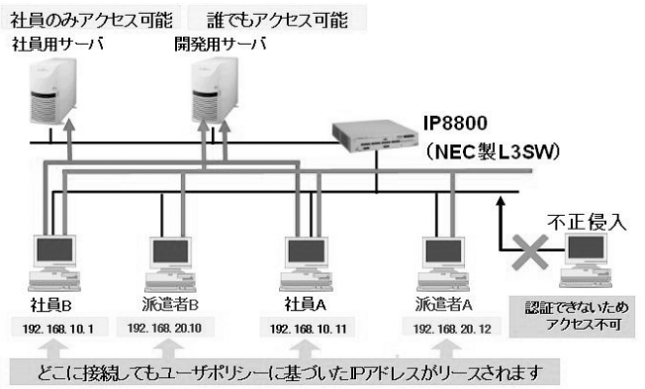

図3 IP8800/700による認証ソリューション
Fig.3 Authentication Solution with IP8800/700.

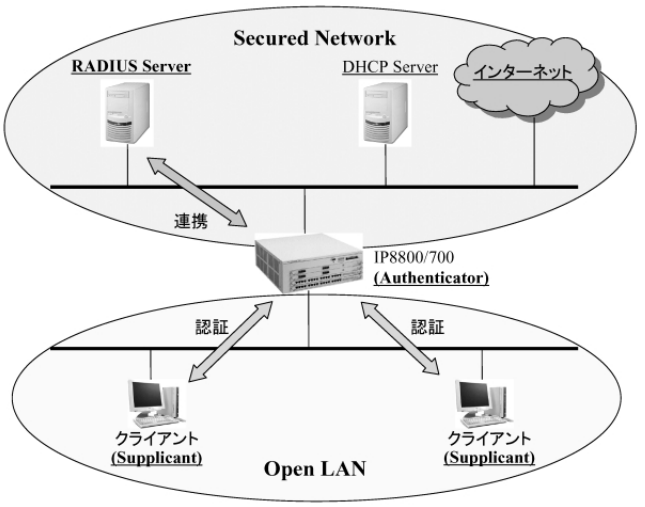

図4 IEEE802.1ｘ認証機能
Fig.4 IEEE802.1x Authentication Function.

また，認証済ポートにおいて複数端末の通信を許可するMultiple Host機能や，端末ごとに認証状態を管理するMultiple Authentication機能により，IEEE 802.1X認証フレームを透過するスイッチやハブを経由して同一ポートに接続する，複数端末の認証制御を実現しています。

その他，IEEE 802.1X 認証の拡張的な機能として，認証用RADIUS（Remote Authentication Dial-In User Service）サーバのユーザ情報にVLAN情報を付加することによって，ユーザ認証情報とVLANを対応付けたネットワークを構成することを可能とする自動VLAN割り当て機能や，RADIUSサーバに送信される認証セッション情報によって，ユーザ追跡を行うことを可能にするRADIUS Accounting機能も備えています。

3.2 認証VLANによる認証機能

認証VLANは，IP8800/700シリーズにVLANaccessAgent機能を実装し，NECの認証サービス用サーバであるVitalQIP

との連動によって，アクセス権限の管理を可能とするなど，ユーザニーズに合わせた，きめ細かいソリューションを提供する高機能な認証機能です。

認証VLANでは，ユーザIDとパスワードをチェックし，その照合を求めて認証を受けるためのネットワークと認証後にのみアクセス可能とする業務用のネットワークとをVALNで分離しておき，認証が完了した端末のMACアドレスを業務用ネットワークのMAC Address Based VLANに動的に登録することにより，認証システムを実現します。

認証VLANは，その高い拡張性から企業や自治体への導入に適し，またマルチレベルのアクセシビリティが設定可能な点で学術機関や医療機関などで高い評価を得ています。

3.3 認証VLAN機能を用いたPC検疫システムの構築

PC検疫システムとは，セキュリティパッチの適用状況が最新でないマシン，ウイルス対策ソフトのデータファイルが最新でないマシンなどを，業務用のネットワークに接続させず，ウイルス対策の処置をするためだけの特殊なネットワーク（クリーンLAN）に閉じ込めるシステムです。

クリーンLANでウイルス対策を行うことにより，業務用のLANにアクセスできるようになります。

このPC検疫システムの構築に認証VLAN技術が着目されています。認証VLANは以下のような理由により，PC検疫システムの構築に適しています。

- 認証用のVLAN＝検疫用VLANとして環境を構築することができます。
- ユーザID，パスワードのチェックに加え，認証を行った端末の機器固有情報（MACアドレスなど）からその端末のウイルス対策状況を動的にチェックする仕組みを組み込むことにより，簡単にPC検疫システムの構築が可能になります。

このたび，IP8800/700シリーズの認証VLAN機能を提供するソフトウェア製品「VLANaccessController」に，サイバーテロ対策製品「CapsSuite」と連携する機能を開発致しました。**図5**に示すとおり，CapsSuiteが保持するウイルス対策状況をユーザ認証時に動的に参照することにより，PC検疫システムを実現しています。IP8800/700シリーズを用いたPC検疫システムには以下のような特徴があります。

- イントラネットに接続されるすべての端末のウイルス対策状況（セキュリティパッチの適用状況，ウイルス対策ソフトエンジン，DATファイルのバージョンチェックなど）の一元管理が可能です。
- ウイルス対策状況の完全でない端末を正規のVLANに接続させないことが可能です。
- 不正接続端末を排除することが可能です。
- ウイルス対策状況が完全でない端末についても，ネットワークケーブルを差し替えることなく，ウイルス対策の実施が可能です。

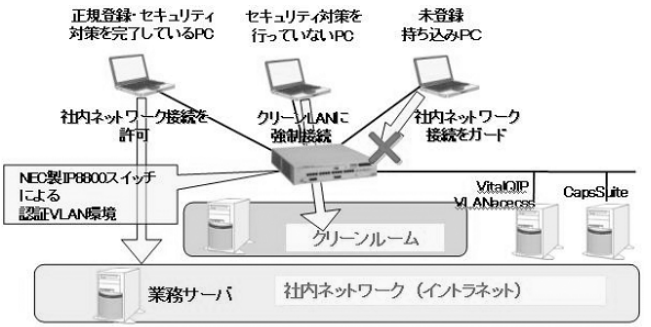

図5 PC検疫システム
Fig.5 Quarantine System for PC.

4．むすび

以上述べたとおり，ネットワークの高速・大容量化に加え，多様化の要求に応えるべく，NECではさらなる製品強化に対応していくとともに，検疫ソリューションなどを中心とした連携ソリューション展開にも注力していきます。

＊イーサネット（Ethernet）は，XEROX社の登録商標です。

参考文献

IEEE802.3ae Media Access Control Parameters, Physical Layers and Management Parameters for 10 Gb/s Operation

筆者紹介

Tatsuya Nakamuta
中牟田竜也（なかむた たつや） 1987年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部マネージャー。

Tomonori Akiyama
秋山 智律（あきやま とものり） 2000年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部勤務。

Yuji Abe
阿部 裕司（あべ ゆうじ） 1999年，NEC入社。現在，コンピュータソフトウェア事業本部第一コンピュータソフトウェア事業部勤務。

Tomohiko Tanikawa
谷川 智彦（たにかわ ともひこ） 1987年，静岡日本電気ソフトウェア入社。現在，NECソフト静岡支社ITソフトウェアビジネス部マネージャー。

Masataka Ichihashi
市橋　将考（いちはし　まさたか）　1997年，NECエンジニアリング入社。現在，IPビジネス事業部第二システム商品技術部勤務。

Yasufumi Nagata
永田　泰史（ながた　やすふみ）　1999年，NECエンジニアリング入社。現在，IPビジネス事業部第二システム商品技術部勤務。