ネットワーク技術の変遷とネットマークスが提供するソリューション

Transition of Network Technology and NETMARKS-provided Solutions

橘　　伸　俊

要　約　コンピュータ関連技術の発展により，コンピュータを動かし利用する基盤としてのICT基盤も発展してきた．コンピュータ同士，コンピュータと周辺機器，コンピュータと端末を接続するネットワークは，取り扱うデータ量の増大によって高速化・大容量化が求められてきた．また，その重要性も増している．一方でネットワークはオープンシステムにより低価格化・一般化・高機能化が繰り返され，インターネットの普及により利便性・生産性は向上したものの，セキュリティなど検討課題が現れ，対応策が取られてきた．

本論文では，技術要素の観点から，ネットワークインフラ，インターネット・ブロードバンド，ネットワークセキュリティ，ストレージネットワーク，サーバファーム，ユニファイド・コミュニケーションの各技術の変遷を述べる．また，これらに対応した商品を選定もしくは開発・インテグレーションし，顧客に提供するネットマークスの取り組みとソリューションを紹介する．

Abstract　According to the development of computer-related technology, ICT infrastructure also has developed as an infrastructure to run and use computers. For the network technology connecting computer-to-computer, computer-to-peripherals and computer-to-terminals, the increase in speed and bandwidth have been required by the increase in traffic volume. And ICT infrastructure has become more important. Meanwhile, price-reduction, generalization, and high-functionality had been repeated with the open system. Furthermore the spread of Internet makes the conveniences and productivities higher. But the issues such as security have appeared and related measures are taken.

In this article, transition of technology in the field of network infrastructure, Internet/broadband, network security, storage network, server farm and unified communication are described. And it also describes the strategy and the solutions provided by NETMARKS INC. that has selected or developed the products which are used in these fields, and has integrated the products to customers.

1. は　じ　め　に

コンピュータシステムはあらゆる面で発展を続け，その進化によるコミュニケーション手段の多様化，高速化は，我々のライフスタイル，ワークスタイルそして，ビジネスの仕組みにまで大きな変革をもたらしている．コンピュータシステムの進化を支えるICT基盤は高速・大量伝送のニーズが増大するにつれていっそうのオープン化・多様化が進んでいる．ICT基盤の重要性はますます高まっており，データそのものへのセキュリティ対策や災害等への備えとしてのリカバリ対策，環境への配慮など，さまざまな課題も顕在化してきている．

株式会社ネットマークス（以降，ネットマークス）は，ネットワークはもとよりセキュリティやストレージネットワーク，ユニファイド・コミュニケーションなど最先端の技術を取り入れて，顧客にいつでも安全，快適にコミュニケーションできるICT基盤を提供するために，数々

のソリューションとサポートサービスを開発し，体制を整備・強化してきた．

本論文では，2章でICT基盤に求められる課題とそれを解決して発展してきた技術の変遷を概観する．3章ではその変遷の中でネットマークスがどのような商品やサービスをソリューション化しインテグレーションしてきたのかを説明する．この中で注目されている技術要素について取り上げ本特集号所収の各論文につなげる．

なお，通信キャリアのネットワークおよび家庭内ネットワークは本論文の対象外とする．

2. ネットワーク技術の変遷

コンピュータシステムが企業の業務の中で重要性を増すにつれ，高速・大容量・広域・信頼性・安全性・完全性・運用性といったニーズ・課題が発生し，それを解決する技術要素が開発されてきた．本章では，ネットワークインフラ，インターネット・ブロードバンド，ネットワークセキュリティ，ストレージネットワーク，サーバファーム，及びユニファイド・コミュニケーションの各分野でニーズや課題とそれを解決する技術要素や仕様を概観する．図1に一般的な企業におけるコンピュータシステムの物理的構成と，その中での各分野の位置付けを示す．

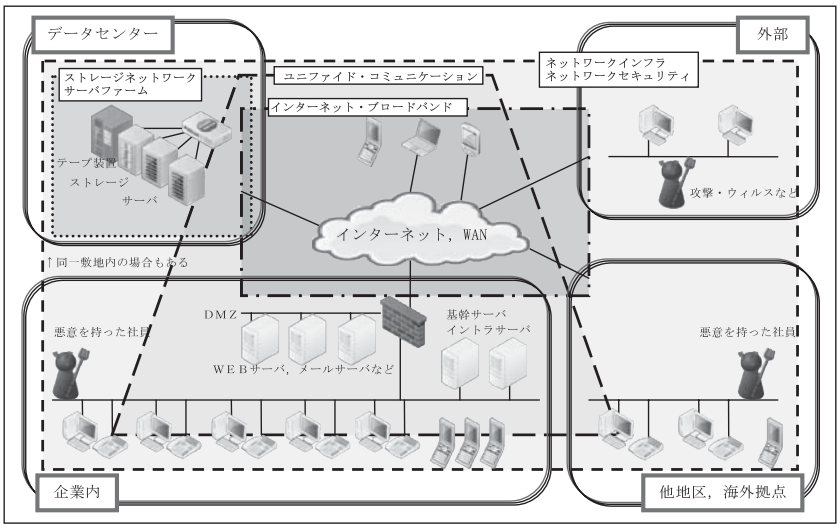

図1　コンピュータシステムの物理的構成とその中での各分野の位置付け

なお，ICT基盤では標準化や相互接続は必須条件であり，メーカ主導・標準化団体主導・デファクトスタンダードとも呼ばれる業界標準など，様々な仕様が検討・提案・審議・承認・公開され，技術要素の普及をいっそう推し進めてきた．IEEE[*1]，ANSI[*2]，IETF[*3]，RFC[*4]，W3C[*5]などその団体や標準仕様も技術変遷の一部として紹介していく．

2.1　ネットワークインフラ

コンピュータで使用されるネットワークは，コンピュータの発展に合わせて進化してきた．当初はホストコンピュータとその周辺機器，ホストコンピュータ間，およびホストコンピュータとそれを使用する端末までの接続のためのものが中心で，それらはホストコンピュータメーカが策定した独自仕様や，業界毎に開発されたものであった．前者にはDCA[*6]，SNA[*7]，HNA[*8]，

FNA[*9]，DINA[*10] などがあり，1970 年代中頃から発表されてきた．後者には全銀協手順[*11]，JCA 手順[*12] があり，1980 年代に規定されたプロトコルである．

1970 年代後半からの小型コンピュータ技術の発展により，一般企業へのコンピュータの導入が広まり，さらにオペレーティングシステムの発展によりアプリケーションが大幅に増えたことで，その普及が加速された．一方，コンピュータ間を接続するネットワークは，仕様を公開した所謂オープンなプロトコルが提案され，普及するとともに業界標準として認知されるようになり，いっそう広まっていった．

企業内のネットワークは同一地区内を対象とする LAN（Local Area Network）と他地区との接続を対象とする WAN（Wide Area Network）に大きく分かれる．また，LAN・WAN 共に工場の生産・制御系データを通信するネットワークと業務・OA 系の情報を通信するためのネットワークが別々に存在している．これらのネットワークは，データや設備の共有のため相互接続されるようになった．異なるネットワーク同士を接続するには，標準化されたプロトコルがきわめて重要な役割を果たした．

1980 年代中頃，LAN のデータリンク層以下には IEEE802.3 委員会，802.5 委員会のそれぞれで規格化された Ethernet や Token Ring などいくつかの種類があった．その中でも LAN の進展は Ethernet の普及によるところが大きい．また，Ethernet 間を高速に，かつ高い信頼性を保って接続するバックボーンネットワークのニーズが発生し，FDDI（Fiber Distributed Data Interface）が ANSI で規格化された．FDDI は 100Mbps のリング形式のネットワークであり，単一箇所の障害に対してはループバックと呼ぶ手法で途切れることのない信頼性を実現した．さらに，マルチメディア通信ニーズに応じて ATM（Asynchronous Transfer Mode）が ATM Forum で標準化された．その後，高速な Ethernet が規格化され，バックボーンでも使用されるようになった．表 1 に Ethernet の主要な規格（伝送速度，ケーブル長，媒体）を示す．

表 1　Ethernet の主要な規格

Ethernet 規格名		IEEE 仕様	伝送速度	ケーブル長	媒体
10Base2（Thin Ethernet）		802.3a	10Mbps	185m	50Ω同軸（5mm 径）
10Base5（Thick Ethernet）		802.3		500m	50Ω同軸（10mm 径）
10Base-T（Twisted Pair Ethernet）		802.3i		100m	UTP（2 対 CAT3）
100Base-T（Fast Ethernet）	100Base-FX	802.3u	100Mbps	2000m	1300nm MMF
	100Base-TX			100m	UTP（2 対 CAT5）
1000Base-X（Gigabit Ethernet）	1000Base-LX	802.3z	1Gbps	550m	1300nm MMF
				5000m	1300nm SMF
	1000Base-SX			550m	850nm MMF
1000Base-T		802.3ab		100m	UTP（4 対 CAT5）
10GBase-X	10GBase-LX4	802.3ae	10Gbps	300m	1310nm MMF（WWDM）
				10000m	1310nm SMF（WWDM）
10GBase-R/W	10GBase-SR/SW			300m	850nm MMF
	10GBase-LR/LW			10000m	1310nm SMF
	10GBase-ER/EW			40000m	1550nm SMF
10GBase-T		802.3an		100m	UTP(4 対 CAT6)

本論分執筆時点（2009 年 9 月）で最速な Ethernet は 10Gbps だが，バックボーンだけでなくサーバ直接でも使用可能である．サーバでの高速通信を実現するために TCP 処理を I/F モジュールにオフロードするなどの工夫がされている．さらに，40Gbps と 100Gbps の規格が既に IEEE802.ba 委員会にて検討されており，2010 年に標準化完了の見込みである．

なお，先の IEEE802.3 委員会では単に速度とメディアに関する規格だけではなく，802.3ac にて VLAN タグが，802.3ad にて Link Aggregation が規格化され，物理的な接続とは独立した仮想的な構成が可能となった．また，802.3af にて Power over Ethernet[*13] が規格化され，LAN ケーブル上で電力が供給できるようになり，対応機器であれば電源の配線が不要になった．これは IP 電話や無線 LAN アクセスポイントの普及に一役買っている．

一方 1990 年代には，配線の手間の解消やモビリティ向上のために無線 LAN も開発された．当初は電波や赤外線を使い独自方式で LAN 間を接続する製品が開発され，その後 IEEE802.11 委員会で電波を使った無線 LAN が規格化された．端末用 I/F も開発され，ノート型 PC にはほぼ標準実装されたことで普及に弾みがついた．表 2 に IEEE802.11 仕様の無線 LAN の主要な規格（伝送速度，周波数帯，使用場所，免許の要否）を示す．

表 2　無線 LAN の主要な規格

IEEE仕様	伝送速度	周波数帯	使用場所	免許・登録の要否
802.11	2Mbps	2.4～2.5GHz	屋内外	免許・登録不要
802.11b	11Mbps/22Mbps	2.4～2.5GHz		
802.11a	最大54Mbps	5.15～5.35GHz	屋内	免許・登録不要
		5.47～5.725GHz	屋内外	免許・登録不要
802.11g	54Mbps	2.4～2.5GHz	屋内外	免許・届出不要
802.11j	54Mbps	4.9～5.0GHz，5.03～5.09GHz	屋内外	登録が必要
802.11n	300Mbps	2.4～2.5GHz	屋内外	免許・届出不要
		4.9～5.0GHz，5.03～5.09GHz	屋内外	登録が必要
		5.15～5.35GHz	屋内	免許・登録不要
		5.47～5.725GHz	屋内外	免許・登録不要

これらの LAN は 1990 年代にオフィス環境においてファイルサーバやプリントサーバの共有目的で普及した．この時に普及したネットワーク OS の一つが Netware であり，NetBIOS，NetBEUI，IPX/SPX などのプロトコルが開発された．また，Macintosh では AppleTalk と呼ぶプロトコルでサーバやプリンタを共有できた．これら複数のプロトコルのパケットを LAN 超えで通信させるマルチプロトコルルーティング機能も開発・実装されたが，各機能が IP 上のプロトコルを使って実現できるようになり，次第に IP に置き換わっていった．

一方，WAN 接続は，回線交換，蓄積交換，専用回線に大別される．最初の回線交換は公衆電話回線や ISDN など，ダイアリングによって通信が可能となるものである．次の蓄積交換はパケット交換やフレームリレー，セルリレーなど，回線は共有するもののデータをパケットなどに分割し細かい単位で伝送するものである．最後の専用回線は 1 対 1 で地区間を接続するためのものである．通信の自由化によって WAN は多くの通信事業者から様々なメニューが提供されている．一般には価格・速度・帯域保証・地域などの条件で選定する．

2.2　インターネット・ブロードバンド

インターネットは日本では 1984 年に JUNET（Japan University NETwork）が始まり，1990 年代前半までは電話回線上で UUCP（Unix to Unix CoPy）プロトコルにて電子メール（RFC976 にて規定）や掲示板などがバケツリレー式に転送される形態で，研究機関・研究部門を中心に利用されてきた[1]．その後通信の自由化が進み，商用の ISP（Internet Service Provider）が事業を始めたことと，マルチメディア情報を出力でき，リンクを張って各 WEB サ

イトを渡り歩くことができるブラウザNCSA Mosaicが出現したことが重なり，1990年代中頃には徐々に企業でもISP事業者と契約してインターネットを利用する素地ができあがってきた．また，電子メールについても，インターネット接続がUUCPからIP化されることによってSMTP（Simple Mail Transfer Protocol：RFC 821）がUUCPに代わって使われている[2]．

それ以降，ISP接続料金の引き下げ，インターネットを意識したOSであるWindows95のリリース，国内外の光回線網の整備によりインターネット利用者が広がった．また，インターネット上のIPパケットを世界中に通信させるためのルーティングプロトコル，名前をIPアドレスに変換するドメインネームシステム（RFC 1034，1035にて規定）が普及のための技術要素として貢献している（2009年8月現在でjpドメインの登録数は110万を超えている）[3][4][5]．1990年代後半以降，OS・ブラウザ・電子メールなどのソフトが高機能化し，PCの価格も低下したことで利用が一層広まった．さらに既存の電話回線の空き帯域を活用するADSL（Asymmetric Digital Subscriber Line）技術が開発された．1999年から商用サービスが開始され，このサービスに始まったブロードバンドの価格競争もあり，日本は世界でも他国に較べ安価に家庭でブロードバンドを利用できる国になっている．

このようにインターネットが普及する一方で，端末に割り当てているIPアドレスがいずれ枯渇するという問題が1990年頃から議論され始めた．これを解決する次世代のアドレス体系・プロトコルが検討され，IPv6として規格化されている．NAT（Network Address Translation）をはじめとするアドレス変換技術の発達の効果で，移行の期限は明確ではないものの，IPv6はコンシューマ市場を中心に広がっている．

2001年以降，ブログなどの普及により個人でも情報を手軽に発信できるようになった．また，インターネット上での決済や広告，ロングテールと言われるような今まではビジネスにならなかった小さな市場の見直しなどビジネスモデルに多くの変化をもたらしている．このようなインターネットの新しい使われ方はWeb2.0とも言われた．

2.3　ネットワークセキュリティ

ネットワークセキュリティの分野をさらにその目的からネットワーク脅威対策，コンテンツセキュリティ対策，アイデンティティ・アクセス管理，システムセキュリティ管理，暗号化に分類して記述する[6][7]．

2.3.1　ネットワーク脅威対策

インターネットと接続するセグメントや極めて機密性の高い情報を取り扱っている部門では特にアクセスを制御し安全性を確保することが求められる．そのためには通信を必要なものだけに絞り，記録することが有効である．これを実現するため，1990年代中頃にFW（Firewall：防火壁）と呼ぶ機能が開発された．また，安全性を高めるためにFWの導入だけでなく攻撃型の通信を検知・防御するニーズがあり，2000年頃にIDS（Intrusion Detection System：侵入検出システム）/IPS（Intrusion Prevention System：侵入防止システム）といった製品が登場した．さらに，WEBサーバを外部に公開している場合には，より高い安全性が求められ，通常のFWよりもWEBに特化した，深いレベルでコンテンツを分析しサーバを守るWAF（Web Application Firewall）製品が2005年頃に開発され，WEBサーバへの外部からの攻撃を防いでいる．これらFW，IDS/IPS，WAFは独立して機能するものであり，製品のメーカ

が独自で開発しているため，標準化要素はない．

一方，地区間をインターネットなど他のネットワーク経由で仮想的に接続するVPN（Virtual Private Network）は1990年代末頃から登場した．IPsec（Security Architecture for Internet Protocol）はVPNを実現するための一つとして標準化されている[8]．これは暗号技術を用いて，IPパケット単位でデータの改竄防止や秘匿機能を提供するプロトコルである．また，PC単体がインターネット経由で社内LANにアクセスするためのモバイルVPN用として，IPsec-VPNの他にも2005年頃にSSL-VPN製品が開発・商品化された．SSL-VPNはWEBサーバとの通信暗号化のために使用されているSSL（Secure Socket Layer）のプロトコルを使ってVPNを実装している．SSLを使うことでFWの設定変更を避けることができるため，気軽に使えるというメリットがある．

2.3.2 コンテンツセキュリティ対策

外部との通信が普及することで課題になったものに，1980年代に登場したウィルスがある．電子メールの添付ファイルやダウンロードしたファイルがウィルスに感染している場合，これを検知・駆除するのがウィルス対策製品である．ウィルスと感染経路は似ているものの自己増殖を特徴とするワーム感染の対策も求められる．

また，WEBサイトは情報収集など業務に不可欠である反面，有害なサイトも乱立しており，WEBのトラフィックをモニタリングし，アクセス先の表示を制限するURLフィルタも数多く製品化され顧客に導入されている．

情報漏えい対策を広くセキュアコンテンツ管理と捉えることもできる．故意による事件と，過失やウィルスによる流出等の事故の両面での対策に分けることができる．入退室管理，印刷管理，アクセス管理，PCの外部デバイス無効化といった方法で物理的に持ち出せないようにするのが事件対策である．また，偽メールや偽WEBサイトを使って銀行口座やクレジットカード情報を得ようとするフィッシング行為を防ぐことも事件対策である．一方，シンクライアント化，ファイルやディスクの暗号化，ウィルス対策などは事故対策と言える．2006年頃には通信内容をモニタリングしてキーワードやデータパターンを用いてフィルタリングするDLP（Data Loss/Leak/Leakage Protection）という製品分野もできている．いずれもISMS[*14]に代表されるような情報セキュリティポリシィと定期的なアセスメント，運用ルールの策定，投資といったトータルな内部統制活動の中で活用することが効果的である．

2.3.3 アイデンティティ・アクセス管理

コンピュータシステムを利用するに当たり，一般的にはIDとパスワードにて利用者を認証し権限を与えるが，単純な固定パスワードは破られる可能性がある．認証をより確かなものにし，信頼性を高めるために，ICカードなど認証デバイスを使った認証，生体認証，ワンタイムパスワードなどの技術が1990年代を中心に開発された．一方，システムのオープン化によって，内部には多くのサーバが存在するようになり，個々のサーバで信頼性の高い認証を行うには，利用者・管理者ともに負担が大きくなってきた．これを解決するために，IDの登録や変更・削除時のワークフローや機器への反映などにおけるミスを防ぎ作業の効率化を図る，ID関連業務に特化した統合ID管理製品が2004年頃から製品化されている．

なお，インターネット経由での取引では，PKI[*15]などによって相手の信用度を確認し通信内

容の正確性を保証する技術が使用されている．

2.3.4　システムセキュリティ管理

システムが複雑化し数多くの機器で構成されるようになると，システム全体のセキュリティ管理が困難になってくる．具体的にはシステム導入後の設定変更や日々の運用，セキュリティの維持業務が特定の個人に依存しないように，システム的な取り組みが必要になってくる．例えば，

- PC の OS パッチ適用状況やアプリケーションのインストール状況および設定などの情報をチェックし，予め定められたポリシィと比較してコントロールするなどの管理を行うためのシステムがある．2004 年頃に登場した検疫ネットワーク[*16]がこれを実現する技術に当てはまり，メーカ主導で決めた手順が複数存在している．
- ウィルス対策や外部アクセス対策など各種機器で検知したアラートの蓄積・分析・通知といった処理をするシステムとして，SIM（Security Information Management）や SEM（Security Event Management）とも呼ばれるログ統合管理ソリューションが注目を集めている．
- 擬似的に外部からの攻撃を行ってシステムの脆弱性を調査するシステムがある．チェックの対象はサーバ，クライアント，ネットワーク機器，WEB アプリケーション，データベースと幅広い．

などが 1990 年代初頭より大手セキュリティ製品メーカからリリースされており，その範囲は広い．企業の情報セキュリティポリシィでは運用面についても規定することが必須で，それにはこれらのツールの活用が効果的である．

2.3.5　暗号化

機密情報が流出した際，被害を最小限に止めるために暗号技術は有効である．最も身近な手法はユーザの使用している端末での暗号化であり，ファイルの暗号化，ファイルシステムの暗号化，ディスクの暗号化の各機能が，1980 年代後半からパソコン OS に搭載され始めたほか，パッケージ製品でもリリースされた．特に社員が持ち出すノート型 PC に対しては，盗難にあっても解読が困難なディスクの暗号化製品を導入するユーザが多い．また，暗号の技術面だけでなく，社員に暗号化を徹底させるための運用面が求められている．

これら単体での暗号化の他に，ネットワーク上の電文の暗号化として，

- S/MIME（Secure/Multipurpose Internet Mail Extensions）や PGP（Pretty Good Privacy）などよる電子メールの暗号化[9][10]
- VPN をはじめとするリモートアクセスや地区間接続通信の暗号化
- 無線 LAN の通信暗号化
- WEB サーバとの通信の SSL による暗号化[11]
- サーバへのリモートログインやファイル転送のための SSH（Secure Shell）による通信の暗号化[12]

などがある．暗号化するには鍵を使用する．暗号化と復号化で同じ鍵を使用する共通鍵暗号方式として，70 年代年に DES[*17]が，80 年代に RC4[*18]が開発された．DES は解読方法が発見され，セキュリティ強化対策版の Triple DES が開発され，さらに 2001 年に AES（Advanced Encryption Standard）が NIST[*19]で制定された．無線 LAN で使用されているセキュリティ

規格の IEEE802.11i（WPA2）では AES をサポートしている．しかし，この共通鍵暗号方式では通信の組み合わせ毎に鍵が必要であり，その鍵の受け渡しや管理が課題であった．これを解決するために Diffie と Hellman が公開鍵と秘密鍵を使う公開鍵暗号方式の概念を 1976 年に発表した．この方式は公開鍵で暗号化し，秘密鍵で複合化するというもので，管理するのは自分の秘密鍵一つになる．その翌年の 1977 年に RSA 暗号が発明され，現在も普及している．暗号化に関しては量子暗号など研究が続いている．共通鍵暗号方式と公開鍵暗号方式はそれぞれ特徴があり，実システムではこれらの両方式を組み合わせるケースが多く見受けられる[*20]．

2. 4　ストレージネットワーク

コンピュータで処理するデータ量は増大を続け，さらに高い信頼性と高速性が求められている．また，サーバが増えることでリソース効率の高いディスク構成が求められている．ストレージやテープ装置を個別にいずれかのコンピュータに接続し専用で使う構成では，障害時の運用やディスクの空きエリアといったリソースの効率化に限界があった．ストレージの可用性を高め，またディスクを共有することで空きエリアの有効利用を可能とするためにストレージ等外部装置をネットワークで接続したのがストレージネットワークである．

従来の接続形態を DAS（Direct Attached Storage）と呼ぶのに対して，ストレージネットワークは SAN（Storage Area Network），NAS（Network Attached Storage）と呼ぶものに大きく分けることができる．SAN はネットワークを介してブロック単位で透過的にアクセスできるもので，NAS はファイル単位でアクセスできるものである．1990 年代中頃に登場した SAN は，サーバに接続する HBA（Host Bus Adapter）や FC（Fiber Channel）スイッチ，FC 対応装置間を FC ネットワークで構成し，その上で SCSI（Small Computer System Interface）のプロトコルを利用することが多い．その伝送速度は 1/2/4/8Gbps と高速な規格が規定されており，16Gbps の規格も策定中である．一方，NAS はファイルサーバとして以前から利用されていたものであり，IP ネットワーク上で CIFS（Common Internet File System）や NFS（Network File System）のプロトコルに対応したサーバで実現する．SAN と明確に区別するために NAS という言葉が使われたが，そもそも SAN と NAS は目的が異なるものであり，これらを組み合わせることも可能である．図 2 に SAN と NAS およびその混在構成の概念図を示す．

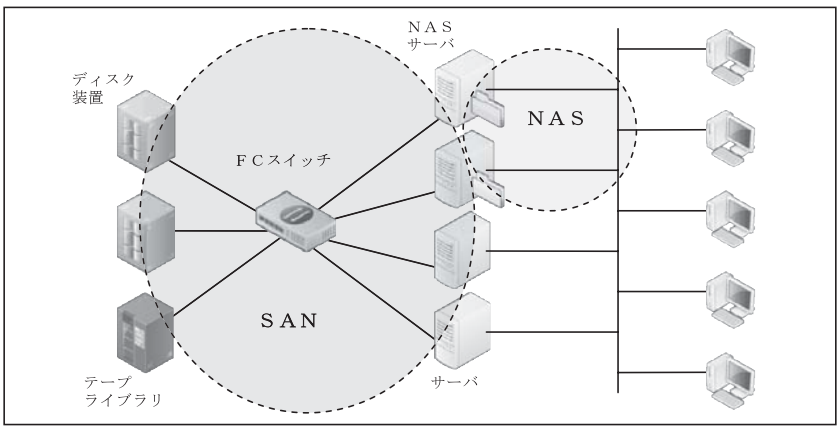

図 2　SAN と NAS およびその混在構成

FC は ANSI INCITS T11 委員会で規格化され 1999 年以降に製品が出始め，現在は高速サーバ周辺で普及している．この FC のネットワークは LAN とは別のネットワークを必要とするため，IP ネットワークと組み合わせる技術が開発された．iSCSI（Internet SCSI）と FCIP（Fibre Channel over IP）である．iSCSI は TCP/IP 上で直接 SCSI ブロックを伝送するもので，専用の HBA などが不要になる技術であり，RFC3385 などで規定されている[13]．FCIP は FC フレームを IP でカプセル化して，SAN 間を IP ネットワークを経由させて通信する技術であり，RFC3821 で規定されている[14]．これらはそれぞれ 2002 年と 2004 年に公開されている．

さらに，データセンターを中心に高速化と集約化の要望が高まっている．FC と Ethernet を同一の物理 I/F を仮想的に共有して使用し，10Gbps の高速 I/F 上で統合化・仮想化・自動化を実現できる技術が FCoE（Fibre Channel over Ethernet）である．FCoE は 2009 年 6 月に，ANSI INCITS T11 で FC-BB-5 として標準化されたばかりだが，既に数社から製品がリリースされている．図 3 に一般的なサーバの高速 I/F と FCoE の I/F の概念図の比較を示す．CNA が FC と Ethernet を論理的に統合しているものであることが分かる．

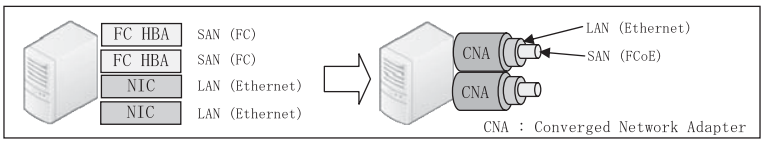

図 3　一般的なサーバの高速 I/F と FCoE の I/F の概念の比較

2. 5　サーバファーム

コンピュータシステムのサーバの配置は，ホストの集中から各種サーバの分散，分散されていても利用者からは統合化されて利用できるクラウドコンピューティングなど大きな変遷があるが，どこかのデータセンター内のサーバファームを利用しているという点は変わらない．高速・大容量・安定稼働が当然求められる中で，運用コストや消費電力の削減を実現する必要がある．そのために統合化（集約化），仮想化，自動化・自律化がキーになっている．サーバファームにおけるサーバ・ネットワーク・運用の三つの分野の技術要素を紹介する．

- サーバ技術：データセンター内の密度を高めるため，2001 年頃からブレードサーバが各サーバメーカから製品化されている．また，2006 年頃からは複数のラック単位で究極的な高密度と高い電力効率，低い発熱量を実現する製品や，早期にデータセンターを実現させるために貨物用コンテナを丸ごとデータセンター仕様にする製品が登場した．
- ネットワーク技術：データセンター内に設置するネットワーク機器はサーバとコアネットワークを接続する高速な I/F を備え，FW 機能などを増設モジュール形式で内蔵し，論理的な構成を組むことで仮想的なネットワークを実現できる．さらに冗長構成を組むことで自動切換を行って高い可用性を実現している．また，サーバの負荷分散装置は暗号化処理のオフロードや WEB サーバなどの同一処理を複数台に分散する機能を備えている．これらの製品は 1990 年代に登場してきた．
- 運用・ソフト技術：複数台で論理的に処理を分散するとともに一台に見せるクラスタソフト，一台で論理的に複数のサーバとして機能する仮想化 OS ソフト，初期設定や動作の状況に応じて設定を変更するといったサーバ運用を自動化するソフトが各運用

管理ソフトベンダーから1990年代より製品化されている．

表3に上記技術要素とそれで対応可能な機能を示す．

表3　技術要素と可能な機能

技術要素	統合化	仮想化	自動・自律化
サーバ			
ブレードサーバ	○		
高密度専用サーバ，コンテナシステム	○		
ネットワーク			
サーバファブリックスイッチ	○	○	○
負荷分散スイッチ	○	○	○
ソフトウェア			
クラスタソフト	○	○	○
仮想化OSソフト	○	○	○
運用自動化ツール			○

現在この分野はコンピュータメーカ，ストレージ機器メーカ，ソフトウェアメーカ，ネットワーク機器メーカが参入しており，大規模買収も活発でありプレーヤーが市場で入り乱れている．導入に当たっては各要素の相性など組み合わせのノウハウや運用面での検討，ロードマップの考慮が今まで以上に求められる．

2.6　ユニファイド・コミュニケーション

企業には既に固定電話，FAX，携帯電話，電子メール，インスタントメッセージ，テレビ会議など多様なコミュニケーション手段が広がっている．ただ，それらは個別のシステムであり，ユーザは時間帯や場所，通信環境，相手の状況などによってそれらを使い分けなければならなかった．ユニファイド・コミュニケーションはこれらの機能をそれぞれの長所を活かしつつ，一つのシステムに統合あるいは既存アプリケーションと連携することによって，オフィスワークの効率や生産性の向上・ワークスタイルの変革を図るものである．

ユニファイド・コミュニケーションの導入は運用コスト削減のためのIP電話に始まる．従来のPBX（Private Branch eXchange）の代わりにIPベースのPBX機能を備えたサーバとIP対応の電話機を使用する．IP電話化することで，配線が一本化され，迅速かつ柔軟なレイアウト変更に対応できる．また，各地区にあったPBXをセンターのIP-PBXに一元化できる．これに通話ログや課金といった付加機能が開発され，従来のPBX機能に置き換わるものになっていった．当然，相互接続性が必要でありG.711の音声符号化やH.264といった動画圧縮，H.323やSIP（Session Initiation Protocol）といったシグナリングなどの規格が策定されている．但し，電話機能の中では転送をはじめとする規格外の多くの機能がメーカ独自で開発され，相互接続が遅れる一つの要因となっている．

さらに，電子電話帳から通話先をクリックすることで自動発呼したり，相手の在席状況（プレゼンスと呼ぶ）を確認してコミュニケーション手段を変更したり，離席時の伝言を電子メールに添付して確認できるなど，電話とシステムを連携させて生産性を向上させるための導入が目立つ．また無線LANをサポートしたデュアルフォンの登場で，それを社内では内線電話として使用し，社外では携帯電話に自動転送させて着信できる率を高めるなど，生産性も向上できるようになってきた．

2007年には通信帯域の広帯域化もあって高解像度の大型ディスプレイ複数台に鮮明な映像を映し出し音声もクリアになり，あたかもディスプレイの向こう側に相手がいるような臨場感

表 4　コンピュータネットワーク技術の年代表

分野	要素技術	1970 年代	1980 年代	1990 年代	2000 年代	2010 年代
ネットワーク	ネットワークアーキテクチャ発表	▲ホストコンピュータメーカが独自のアーキテクチャを発表				
	IEE802.3 規格		▲(83)			
	OSI 参照モデル制定		▲(83)			
	IBM が NetBIOS を開発		▲(84)			
	IBM が NetBEUI を開発		▲(85)			
	IBM が TokenRing LAN 出荷		▲(85)			
	FDDI が ANSI にて標準化		(87)▲			
	ATM フォーラム発足			▲(91)		
	IEEE802.3u(100Base-Tx) 規格			▲(95)		
	IEEE802.3z(1000Base-X) 規格			(98)▲		
	IEEE802.11b, 11a 規格			(99)▲		
	IEEE802.3ae(10Gbps) 規格				▲(02)	
	IEEE802.3ba(40Gbps,100Gbps) 規格				(10 の見込み)▲	
インターネット	JUNET 開始		▲(84)			
	商用 ISP 事業開始			▲(92)		
	NCSA Mosaic 登場			▲(93)		
	NTT の WEB サーバ立ち上げ			▲(93)		
	Netscape 公開			▲(94)		
	Windows95 発売			▲(95)		
	ADSL 開始			(99)▲		
	Web2.0 発表				▲	
	IPv6			(95：仕様決定)▲	IPv4 大元割当枯渇▲	
セキュリティ	DES を NBS が採用	(77)▲				
	RSA を RSA が開発	(77)▲				
	ウィルス登場		(86)▲			
	RC4 を RSA が開発		(87)▲			
	ワーム登場		(88)▲			
	ITU-T が X.509 を公開		(88)▲			
	Firewall 登場			▲		
	SSH 誕生			▲(95)		
	IPsec を RFC で公開			▲(95)		
	PGP を RFC で公開			(96)▲		
	BS7799-2 策定			(98)▲		
	S/MIME を RFC で公開			(98)▲		
	IPsec VPN 登場			▲		
	SSL/TLS を RFC で公開			(99)▲		
	メール感染型ウィルス流行			(99)▲		
	IDS 登場				▲	
	NIST が AES を制定				▲(01)	
	IPS 登場				▲	
	WPA2 で AES をサポート				▲(04)	
	検疫ネットワーク登場				▲(04)	
	SSL-VPN 登場				(05)▲	
	Winny による情報漏洩多発				(06)▲	
	SSH を RFC で公開				(06)▲	
	WAF 製品登場				▲	
ストレージ	FC-PH（ANSI X3.230:1994）			▲(94)		
	iSCSI				▲(02)	
	FCIP				▲(04)	
	FCoE				(09)▲	
サーバファーム	クラスタソフト			▲(94)		
	サーバファブリックスイッチ			▲(95)		
	サーバ負荷分散スイッチ			(96)▲		
	仮想 OS ソフト			(98)▲		
	運用自動化ツール			(99)▲		
	ブレードサーバ				▲(01)	
	DC 専用高密度サーバ				(06)▲	
ユニファイドコミュニケーション	CCITT(現 ITU-T) G.711 音声符号化	▲(72)				
	ITU-T H.323 Ver.1 音声・動画通信			(96)▲		
	ITU-T H.323 Ver.2 音声・動画通信			(98)▲		
	大規模 IP-PBX 導入活発化				▲	
	SIP				▲(02)	
	ITU-T H.264 動画圧縮				▲(03)	
	IP コンタクトセンター活発化				▲	
	デュアルフォン				▲	
	テレプレゼンス				▲	

の高いシステムが実現できるようになった．これはテレプレゼンスと呼ぶ技術で，従来のビデオ会議の延長線上では比べられない程のものである．

一方で電話対応を業務の生業としているようなコールセンターでは従来の PBX だけでは対応できない特殊な機能（具体的には効率的な顧客対応や省力化，分析・レポーティングなど）をコンピュータを利用して実現することが必要であり，この分野を中心に CTI（Computer Telephony Integration）技術が発展してきた．CTI では PBX 機能のほかに ACD（Automatic Call Distribution：コールをオペレータに振り分ける）機能，IVR（Interactive Voice Response：音声による自動応答）機能が代表的な機能であり，コールを最適な応対者に効率的にルーティングすることができる．特に PBX が IP 化されたシステムは IP コールセンターと呼ばれ，IP 化されていれば場所に依存しない柔軟なシステム構成が取れ拡張性に優れている．さらに，センターシステムをデータセンターに集約させることでセキュリティレベルの高い運用が可能であり，これは PBX の IP 化による特徴を生かしたものである．

表 4 に以上紹介してきた要素技術とその出現した年代を示す．

3. ネットマークスの取り組みとソリューション

インテグレータであるネットマークスは，これらの技術の変遷の中で顧客のニーズを理解・分析し，最適な商品を提案・設計・構築し，保守・運用・監視のサービスを提供している．そのために，①世の中の技術動向・商品動向・法令などの情報をウォッチし新規商品を発掘，②メーカの新商品の情報を収集，③商品の評価，④商品化・必要な体制の整備，⑤メーカが保証する品質をチェックする仕組みと体制の整備を行っている．また，システムを稼働させるためのインテグレーションには要求仕様の理解や機器の設定，プロジェクトマネジメントのためのスキルが必要であり，基礎技術の習得とともに，メーカの認定技術者を育てメーカとの連携強化に努めている．図 4 にネットワーク基盤を中心としたネットマークスのソリューションマップを示す．マルチベンダーのネットワーク基盤を中心として，ユニファイド・コミュニケーションソリューション，データセンターソリューション，トータルセキュリティソリューション，アウトソーシングサービス，海外ソリューションを総合的に提供している．

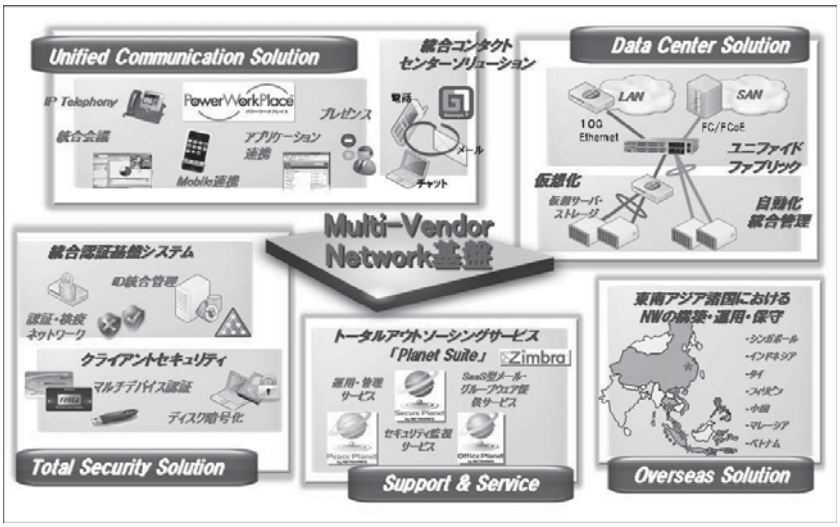

図 4　ネットマークスのソリューションマップ

この章では，2章で述べた六つの分類を一部集約するのに加えて，これらのインテグレーションの観点から，ネットマークスの取り組みとソリューションを解説する．

3.1　マルチベンダネットワーク基盤

マルチベンダーのネットワーク基盤はネットマークスのビジネスのほぼすべてに関係するものである．導入件数でもスイッチやルータが大半を占めており，この他は無線 LAN のアクセスポイントや無線 LAN スイッチ，工事関係で構成される．

ネットマークスはインテグレータとして，顧客の要件に適したネットワークシステムを構築し高速性・安定性・信頼性を実現する．そのためには製品知識やメーカとの強力な関係が必要であり，認定技術者を多く育成している．特に米国 Cisco Systems 社製品の取り扱いが多く，販売・技術・サポートの各局面で外部の審査を受け，2000 年にゴールドパートナーに認定された．なお，顧客ニーズは様々であり，製品の機能面や信頼性から国産製品や特徴ある製品を必要とするケースがあるため，特定のメーカに依存しないという方針で商品化を行っている．

3.2　トータルセキュリティソリューション

ネットマークスでは，ゲートウェイセキュリティ，統合認証基盤，クライアントセキュリティの各分野で，常に最新の技術を取り入れた幅広いセキュリティソリューションを開発し，セキュリティポリシーの策定から運用・構築までトータルに提供している．図5に導入箇所で分類したネットマークスのトータルセキュリティソリューションマップを示す．三つの分類それぞれに製品を Firewall などの機能でグループ化したジャンルを記載している．セキュリティといってもジャンルの広いのが分かる．

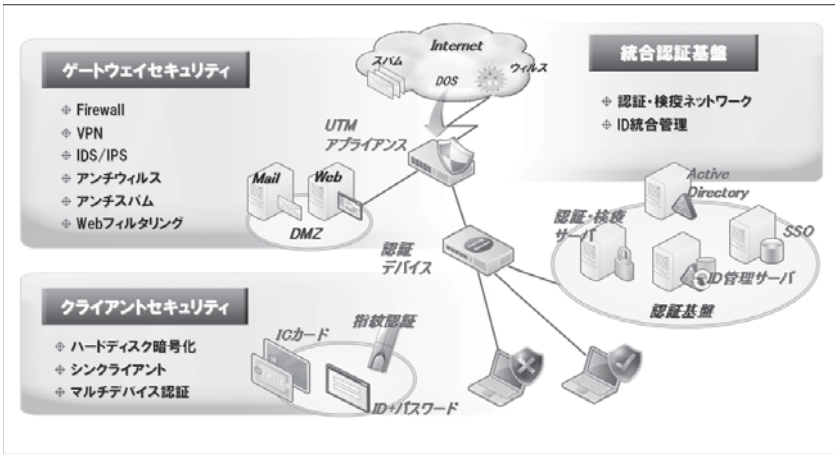

図5　セキュリティのソリューションマップ

業界全体で技術的に未成熟な新しいジャンルにおいては取扱商品は一つだけであるが，技術が成熟してくると同一ジャンルでも機能や特徴の異なる複数製品を商品化し，運用サービスを提供するなど顧客のニーズに応えている．例えば，アクセスポイントやインターネット経由の通信の認証向けに，ワンタイムパスワード製品として二つのメーカの製品を商品化し，幅広いユーザニーズに対応している．二つの製品とは，個人に配布するトークンデバイスに1分毎に

異なる数字が表示される SecurID と，インターネット経由でブラウザに表示される文字配列からユーザ個別にあらかじめ決めた配列パターンでパスワードを決定する SECUREMATRIX である．この他にも認証機能を ASP 型の運用サービスでも提供している．

一方，セキュアログオンソフトウェアとして SecureSuiteV を自社開発している．SecureSuiteV は，IC カード，指紋認証などの本人認証を Active Directory や Citrix XenApp 環境で利用可能にするソフトウェアである．表 5 に，図 5 中の三つの分類と 2. 3 節にて示した五つの技術要素の対応を示す．

表 5　セキュリティソリューションの分類と技術要素の対応

	ネットワーク脅威対策	コンテンツセキュリティ対策	アイデンティティ・アクセス管理	システムセキュリティ管理	暗号化
ゲートウェイセキュリティ	◎	◎	○	○	◎
統合認証基盤	○		◎	○	
クライアントセキュリティ	○	◎	○	○	◎

本人確認のための認証基盤と ID の管理基盤を中心にその技術解説・用途・事例・インテグレーション上の注意点とネットマークスの取り組みに関して，本特集号所収論文「セキュリティと利便性を両立させる統合認証基盤」にて解説する．

3. 3　データセンターソリューション

ネットマークスでは，ネットワーク統合仮想化，統合一元運用，WAN 最適化・高速ファイル転送・情報共有可視化，データセンターコアネットワーク，及びサーバブレード＋仮想マシンの各分野でデータセンターの仮想化・統合を実現するために，ソリューションの開発・提供を行っている．図 6 にネットマークスのデータセンターソリューションマップを示す．

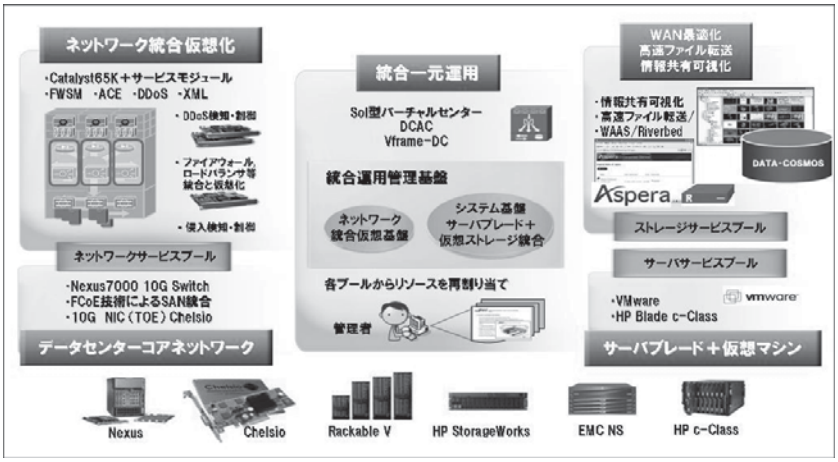

図 6　データセンターのソリューションマップ

まず，ネットワーク仮想化を実現するために，Cisco Systems 社の Nexus や Catalyst6500 および FW や負荷分散などの機能モジュール，Chelsio Communications 社[*21] の 10G Ethernet

を中心に相互接続検証を行って商品化した．これらのおのおのが仮想化に対応している．サーバやストレージは米国 Hewlett-Packard 社，EMC 社[*22]，Rackable Systems 社[*23] の機器をインテグレーションしている．また，WAN 経由の通信では，帯域だけでなく遅延が転送速度の大きな要因になるため，WAN 上の通信を最適化させる機器やソフトウェアをいち早く見つけ取り扱っている．これはデータセンターと国内の拠点との接続はもちろん，海外との接続で効果が高く，海外のネットマークス拠点すべてが注力しているソリューションの一つである．

データセンター内のストレージネットワークではそのインフラに加え，利用・運用支援のためのソリューションとして，グローバルネームスペース，ILM（Information Lifecycle Management），FLM（File Lifecycle Management），バックアップを実現する商品も揃えてインテグレーションしている．特に，長年培った Fibre Channel の技術と FC HBA やファイバチャネルスイッチの製品知識をベースに SAN の設計，構築，テスト，トレーニングなどのプロフェッショナルサービスを行っている．また，2009 年度からはファイルなど情報共有可視化を高速化するソリューションにも取り組んでいる．

ネットワークの仮想化を中心に，その技術解説・用途・事例・インテグレーション上の注意点とネットマークスの取り組みに関して，本特集号所収論文「システム基盤の最適化を実現するネットワーク仮想化」にて解説する．

WAN 高速化を中心に，その技術解説・用途・事例・インテグレーション上の注意点とネットマークスの取り組みに関して，本特集号所収論文「アプリケーションレスポンスを改善する WAN 高速化装置」にて解説する．

ネットワーク化されたストレージを中心に，その技術解説・用途・事例・インテグレーション上の注意点，動向，ネットマークスの取り組みについて，本特集号所収論文「ビジネス継続を実現するストレージソリューション」にて解説する．

ファイルの高速可視化ソリューションを中心に，その技術解説・用途とネットマークスの取り組みに関して，本特集号所収論文「文書を可視化する高速表示ソリューション“DATA-COSMOS”」にて解説する．

3. 4　ユニファイド・コミュニケーションソリューション

ネットマークスではプレゼンス，統合会議，アプリケーション連携，モバイル連携，及び統合コンタクトセンターの各ソリューション分野でコミュニケーションや業務スピードの向上を実現すべく商品の開発・提供を行い，ユニファイド・コミュニケーションソリューションとして推進している．図 7 にネットマークスのユニファイド・コミュニケーションソリューションマップを示す．

ネットマークスは Cisco Systems 社と戦略的な提携を結ぶことで国内でもいち早く IP テレフォニー技術を習得し，2001 年には国内で初めて Cisco Systems 社の IP 電話を使った大規模な IP テレフォニーシステムを構築した．その後も数多くの導入実績を誇るリーディングカンパニーとして市場開拓に取り組み，本論文執筆時点までに 15 万台を超える IP 電話を導入している．自社内にユニファイド・コミュニケーション専用の大型のラボ環境を有し，導入前に顧客の環境に適合させるための様々な評価・検証を行っている．また，日本市場特有の要望に応える各種アプリケーションを独自に開発し，ユーザ環境に合わせた様々なソリューションを提供している．さらに，2007 年 3 月には Cisco Systems 社の認定するユニファイド・コミュニ

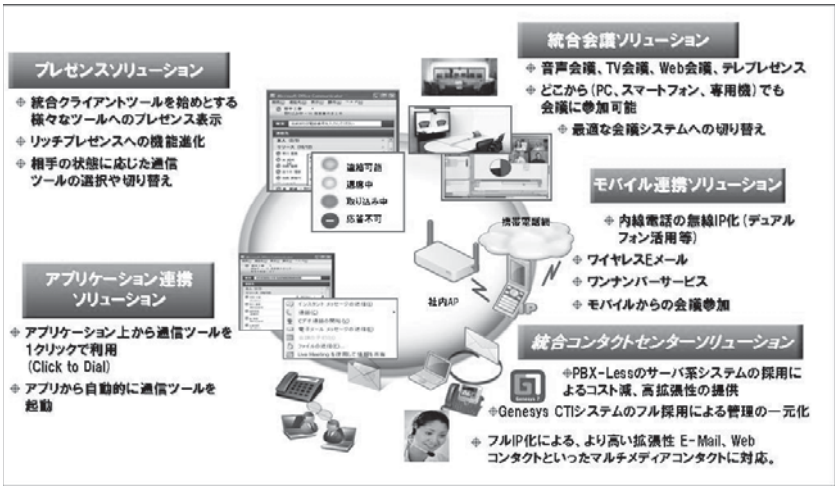

図7　ユニファイド・コミュニケーションのソリューションマップ

ケーションの最高パートナー認定資格である「マスター UCS（Unified Communications Specialization）」を取得した．本資格はネットマークスが国内では初めて，また世界でも 2 番目の取得である．

日本ユニシスグループの一員となった 2007 年の秋には PowerWorkPlace を発表した．PowerWorkPlace は，“コミュニケーションの壁”を取り払うために，ネットマークスの「ユニファイド・コミュニケーション」と，ユニアデックス株式会社の「AiriP（アイリップ）モビリティーソリューション」，そして日本ユニシス株式会社の高品質なシステムインテグレーション力を連携していく，新しいコンセプトである．

一方で，PBX と連携する CTI システムでは，特に UnPBX と呼ぶ非従来型 PBX を大規模コンタクトセンターに適用する市場が広がると判断し，米国 Genesys Telecommunications Laboratories 社の認定パートナーとなり IP コンタクトセンターの市場開拓と技術習得を行い，多くの大規模コンタクトセンターの構築実績を上げてきた．このソリューションでは，電話，FAX，WEB などのマルチチャネル I/F を統合的に受け付けることができる．先のユニファイド・コミュニケーション技術を使って様々なコミュニケーション手段を組み合わせ，受け付けたコールを適した部署にルーティングさせるビジネスプロセスルーティングという業務改善とユーザ情報の活用を可能とする“これからのコンタクトセンター”を提供している．

ユニファイド・コミュニケーションのソリューションは，ネットマークスでの取り組み，導入用途や事例，企業への導入における課題，今後の方向性などを交えて，本特集号所収論文「ワークスタイル改革を実現するユニファイド・コミュニケーション」にて解説する．

IP コンタクトセンターを中心に，その技術解説・用途・事例・インテグレーション上の注意点とネットマークスの取り組みに関して，本特集号所収論文「コールセンター業務を効率化する IP コンタクトセンターシステム」にて解説する．

3.5　インテグレーションサービス

インテグレーションサービスは，顧客のニーズを理解・分析し最適な商品を提案・設計・構築するサービスである．また，障害発生の際にはログやダンプ，ネットワーク上でキャプチャ

したデータから原因を究明することもある．そのためには①ヒアリング能力，②ネットワーク分野の知識，③幅広い製品知識，④設定に関する知識，⑤プロジェクトマネジメント能力が求められるので，エンジニアのスキル向上に日々努めている．一方で，インテグレーションの中では製品に対して高い品質が求められる．そのための品質管理では，

・新規取り扱い製品の選定の際や顧客毎のシステム設計の際には機能や性能の評価・検証を行う．このような機種に依存する品質に対し，以下の分担で取り組んでいる．
  ◇新規商材取り扱い検討時の評価，および，既存取り扱い製品の機能検証や性能測定を製品担当技術部門が実施
  ◇実際の導入構成/設定で動作を確認する導入前システム検証をアカウント技術部門が実施
・また，日々の出荷品である個々の製品に対するハードウェア不良などの検査を品質管理センターが実施し，不具合の撲滅や低減に努めている．

製品担当技術部門が実施する機能検証，性能測定に関しては，本特集号所収論文「高品質システムを実現するネットワーク機器検証手法」にて解説する．

品質管理に関しては，本特集号所収論文「海外メーカー製品に対する品質確保への取り組み」にて解説する．

3.6　アウトソーシングサービス

システムの重要性と高度化が増すにつれ，システムの構築後の安定稼働が求められる．顧客に安心して使用していただくために，以下のサービスを提供している．

1)　保守サービス：システムの異常発生時にコールセンターにて電話の受付から現場出動者のコントロールや障害の切り分け支援を行い，機器の故障の際には対象機器を交換するサービスである．通常は保守契約に基づいて実施する．そのため，顧客の機器情報，構成情報，契約情報，保守対応状況などの管理システムを構築し運用している．

2)　セキュリティ製品の運用代行サービス（SecurePlanet）：セキュリティ製品は操作が特殊で，誤った設定変更はセキュリティホールになりかねない．また，設定変更の依頼・承認・実施といったフロー通りの実施とその記録，装置のログの管理・分析などの運用業務が重要である．さらに設定変更は休日や夜間に実施するケースが多い．このようにセキュリティ製品の運用には十分な体制・スキルが必要だが，これを顧客に代わってリモートから実行する．サービス実施にあたっては，通信の暗号化，プロセスの標準化，オペレーションの記録を行っている．このサービスは Firewall，VPN，認証サーバ，不正アクセス対策機器などに対して提供している．図 8 に Firewall 運用サービスの概念図を示す．

3)　ネットワークやサーバのリモート監視，リモート運用サービス（PeacePlanet）：サーバやネットワーク機器といったインフラは 24 時間 365 日の安定稼働が求められている．これらを監視・運用する体制とスキルを維持するには膨大なコストが発生する．これを軽減させるため，リモートで接続して様々な手法で装置の状態を監視し，障害切り分けやレポートの作成などの運用を代行するサービスである．
  ・顧客との打合せにて監視や運用の柔軟な個別設計
  ・幅広い監視の手順があるだけでなく，対象装置に特殊なエージェントをインストールすることなく安定かつ安価に監視を実現する自社開発のシステム

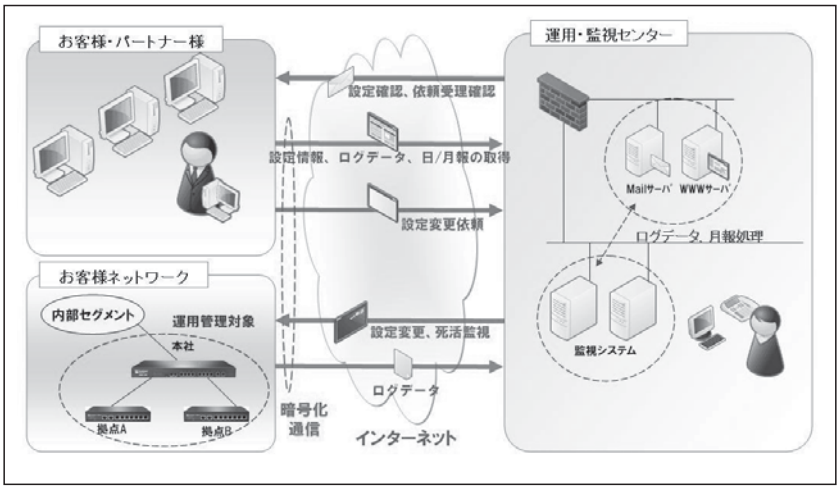

図 8　Firewall 運用サービスの概念図

・状況を共有するための WEB 公開や，レポートやログを分析するといった高度なサービス

が特徴である．これはサービスセンターのシステム化と十分教育されたエンジニアの体制整備によって提供している．

4）　常駐派遣サービス：システムの安定運用のために，オペレーションエンジニアを顧客のサイトに常駐させることが求められるケースがある．この場合には単にエンジニアを派遣するだけではなく，センターから支援する必要があり，そのための教育を行い体制を整備している．

5）　ヘルプデスクサービス：顧客自身が運用するケースにて，操作方法が分からなかったり，設定変更による影響が分からなかったりすることが多い．これを支援するために取り扱い製品の稼働後のヘルプデスクサービスを提供している．そのために，動作確認の機器を準備するとともに対応できるエンジニア体制およびその製品スキルを維持している．

6）　SaaS 型サービス：顧客自身が実施する機器情報の日々の管理業務を ITIL（Information Technology Infrastructure Library）に沿った運用にするための CMDB（Configuration Management DataBase）機能のサービスを提供している他，電子メール機能を WEB の GUI で実現するサービスを提供している．CMDB 機能のサービス提供に関しては本特集号所収論文「システム運用者の管理業務を効率化する CMDB ツール“PLANET-IMAS”」にて解説する．

7）　運用支援サービス（PowerPlanet）：ネットワークシステム構築後に必要となる運用を支援するサービスとして，顧客専用の Web ポータルサイトを通じた情報提供やサービスデスク，ネットワークの設定変更時の影響とその範囲などに関する高度な技術的アドバイスを実施する SE 支援サービスなどを 2009 年から提供している．

4. お　わ　り　に

本稿ではネットワーク技術の変遷とその中でのネットマークスの取り組みを中心に述べた．クラウドコンピューティングをはじめネットワークを前提とした新しいコンセプトへの対応な

ど，システムは複雑になり高度化している一方，顧客からは安定稼働するのが当然として期待される．今後もネットワークインテグレータのトッププレーヤーとして新しい技術への対応，ソリューションやサービスの開発，安定稼働への取り組みを積極的に推し進めていく．本特集号所収の各論文にて，読者の方々にはこの点をご認識いただけることと確信している．

また，ネットマークスの各ソリューションの取り組みは単に個々のソリューションだけではなく，技術部門が部門間の連携を図り，顧客アカウントチームが複数のソリューションを取りまとめ，会社全体での提案・対応を行っていることも書き加えておきたい．

さらに，論文中で述べた PowerWorkPlace のように，ネットマークスが日本ユニシスグループに参画したことにより，日本ユニシス株式会社，ユニアデックス株式会社をはじめとするグループ各社の商品企画部門とともに商材を相互に紹介し取り扱うことで，ソリューションの幅をさらに広げるとともに，効率的な商品の開発に取り組んでいる．

＊ 1　IEEE は The Institute of Electrical and Electronics Engineers, Inc. の略で，アメリカ合衆国に本部を持つ電気・電子技術の学会．
＊ 2　ANSI は American National Standards Institute の略で，アメリカ合衆国の工業的な分野の標準化組織であり公の合意形成のために，さまざまな規格を開発．
＊ 3　IETF は Internet Engineering Task Force の略で，インターネットで利用される技術の標準化を策定する組織．
＊ 4　RFC は Request for Comments の略で，IETF による技術仕様の保存，公開の形式．
＊ 5　W3C は World Wide Web Consortium の略で，World Wide Web で使用される各種技術の標準化を推進する為に設立された標準化団体，非営利団体．
＊ 6　DCA は Distributed Communication Architecture の略で，ユニシスのコンピュータネットワーク・アーキテクチャであり，更にはそれに基づいたプロトコルスタック．
＊ 7　SNA は Systems Network Architecture の略で，IBM のコンピュータネットワーク・アーキテクチャであり，更にはそれに基づいたプロトコルスタック．
＊ 8　HNA は Hitachi Network Architecture の略で，日立製作所のコンピュータネットワーク・アーキテクチャであり，更にはそれに基づいたプロトコルスタック．
＊ 9　FNA は Fujitsu Network Architecture の略で，富士通のコンピュータネットワーク・アーキテクチャであり，更にはそれに基づいたプロトコルスタック．
＊10　DINA は Distributed Information processing Network Architecture の略で，日本電気のコンピュータネットワーク・アーキテクチャであり，更にはそれに基づいたプロトコルスタック．
＊11　全銀協手順とは全国銀行協会連合会が規定した，一般企業や銀行相互間の金融情報交換用の標準通信プロトコル．
＊12　JCA 手順とは日本チェーンストア協会が規定した取引先データ交換標準通信制御手順．
＊13　Power of Ethernet は，電力線を通信路として利用する技術である PLC（Power Line Communication）とは別物である．
＊14　ISMS は Information Security Management System の略で，情報セキュリティを確保・維持するために，ルール（セキュリティポリシー）に基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのこと．
＊15　PKI（Public Key Infrastructure）はインターネット上での安全な取引を実現するために公開鍵証明書，認証局（CA），登録局（RA）を体系立てたモデルであり，1988 年に ITU-T が X.509 で規定している．WEB サーバを立ち上げて SSL で暗号化した通信を行うには自前で CA を立てるかベリサインなどの有償サービスを使うことになる．
＊16　検疫ネットワークとは，PC が物理的にネットワークに接続した際に，まずパッチの適用状況やウィルス対策ソフトのパターンファイルのバージョンを自動的に調べ，ポリシィに適合していればネットワークリソースを利用できるようにする仕組み．不適合の場合は隔離されたネットワークに割り当て，適切な設定を施したのちに再度検査する．
＊17　DES（Data Encryption Standard）は IBM が開発し後の NIST（National Institute of Standards and Technology）である NSB（National Security Branch）により採用された．共通鍵暗号方式でもブロック暗号の代表的なもの．
＊18　RC4（Rivest Cipher 4）は 1987 年に RSA Security 社で Ron Rivest によって開発された．共通鍵暗号方式でもストリーム暗号の代表的なもの．
＊19　NIST は National Institute of Standards and Technology の略で，アメリカ合衆国商務省配

下の技術部門であり非行政機関である国立標準技術研究所.

＊20 SSL や S/MIME では認証や鍵の暗号化で RSA を，データの暗号化で RC4 や DES を採用している．尚，SSL や S/MIME では暗号だけでなく，PKI の電子署名機能を使うことで高い安全性を実現している．

＊21 Chelsio Communications 社は既存のインフィニバンド，ファイバチャネル，イーサネットで利用されるインターフェースを 10 ギガビットイーサネットに統合する NIC，ASIC を提供している．サーバ，ストレージ，ネットワークが 10 ギガビットイーサネットでフラットに接続し，次世代データセンターにおけるユニファイド・コンピューテングの基盤となるものである．

＊22 EMC 社はストレージを中心としたメーカであったが RSA Security 社や VMware 社を買収するなど事業範囲を広げ，情報インフラストラクチャの大手メーカとして成長している．データセンターの仮想化ソリューションにも注力している．

＊23 Rackable Systems 社はデータセンター用高密度（DC 電源）サーバやコンテナ型データセンターを開発しているメーカ．Silicon Graphics 社を買収するなど単に IT インフラメーカとしてのみならず，HPC 分野にも意欲的である．

参考文献

［1］ RFC 976 Mark. R. Horton 他, “UUCP Mail Interchange Format Standard”, Feb. 1986,
http://www.ietf.org/rfc/rfc976.txt（以降，RFC については本サイトのものを参照）
［2］ RFC 821 J. Klensin, Editor 他, “Simple Mail Transfer Protocol”, April 2001
［3］ RFC 1034 P. Mockapetris 他, “DOMAIN NAMES - CONCEPTS AND FACILITIES”, November 1987
［4］ RFC 1035 P. Mockapetris 他, “DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION”, November 1987
［5］ ドメイン名の統計情報 http://jpinfo.jp/stats/
［6］ 日本ネットワークセキュリティ協会教育部会 著，情報セキュリティプロフェッショナル教科書，アスキー・メディアワークス，2009 年 3 月
［7］ 平成 20 年度 情報セキュリティ市場調査報告書 日本ネットワークセキュリティ協会
［8］ RFC 1825 R. Atkinson, “Security Architecture for the Internet Protocol”, August 1995
［9］ RFC 2311 S. Dusse 他, “S/MIME Version 2 Message Specification”, March 1998
［10］ RFC 1991 D. Atkins 他, “PGP Message Exchange Formats”, August 1996,
［11］ RFC 2246 T. Dierks 他, “The TLS Protocol”, January 1999
［12］ RFC 4251 T. Ylonen, “The Secure Shell (SSH) Protocol Architecture”, January 2006
［13］ RFC 3385 D. Sheinwald 他, “Internet Protocol Small Computer System Interface (iSCSI) - Cyclic Redundancy Check (CRC)/Checksum Considerations”, September 2002
［14］ RFC 3821 M. Rajagopal 他, “Fibre Channel Over TCP/IP (FCIP)”, July 2004
［15］ http://www.netmarks.co.jp/

上記参考文献の URL 確認：2009. 11. 4

執筆者紹介

橘 伸 俊（Nobutoshi Tachibana）
2001 年に住友電工(株)より(株)ネットマークスに転籍．技術サポートセンターにて新規取り扱い製品の評価検証を担当した後，マネージメントサービスの事業立ち上げに従事．その後，技術本部とマーケティング部門および国際ビジネスに従事.