IT事業におけるIPネットワークソリューションの展望

Scope of IP Network Solutions in IT Business

井 出 大 史*1　　武 智 洋*1
IDE Hirofumi　　TAKECHI Hiroshi

インターネットが社会の情報通信インフラストラクチャーに進化しつつある。このインターネットを，社会や産業の情報通信基盤とする為には，モラルや法制度，可用性(アベイラビリティー)やセキュリティ等の課題を解決する必要がある。

本稿では，この中で技術的に解決すべきテーマを抽出し，産業構造の中に当てはめ，機能のセグメンテーションを行うと共に，その機能のあるべき姿について記述し，本稿以降に掲載する論文がシステム全体の中のどの機能となるか，及び，相対関係を明らかにした。

The Internet has been grown a vital information infrastructure in today's society. The Internet, however, is necessary to overcome various issues in order to be the true winner that can support society and industries as viable information infrastructure -- such as establishment of socially acceptable ethics and laws, and further improvement of availability and security. This paper lists up some technical issues to be solved, and categorize them into several functional segments that constitute industrial structure. This paper also describes what is desirable for each function, along with classifying the subsequent papers in the whole system to which function they correspond, and clarifying how they are intertwined.

1. はじめに

当社では，IT(Information Technology)分野におけるシステムインテグレーション，システム構築に必要なプロダクト，システムを運用して行くためのサービスの事業化を図っている。本特集号では，インターネットの先端的研究プロジェクトであるWIDEプロジェクトへの参画を通して培ってきた，IPネットワーク技術を基盤とするIP(Internet Protocol)ネットワークソリューション事業について紹介させていただく。

情報通信技術の進歩に伴い，様々な社会変革が起きつつある。その中でも顕著な変化が，インターネットの社会インフラストラクチャー化である。これまでは広域でオープンのネットワークとは言え，情報環境や使うためのスキルの問題もあり，モラルを有した限られた人々が参加者であった。しかし，最近ではプロバイダーのサービス機能の多様化，機器の取り扱いの容易性向上，コンテンツの充実等から，多くの人々がプレーヤーとなりつつある。また，単なる情報伝達の手段から，電子商取引(Electronic Commerce：EC)と言われる商取引き関係にも使われるようになり，まさに社会の重要なインフラストラクチャーとなりつつある。

インターネットを推進し，これからもその発展に尽力されている方々にとっては，バーチャルからリアルに全てのものがインターネット上で展開できる真の情報社会の実現が間近である確信を抱かれていると思われる。

インターネットの目指す環境は，n：nのコミュニケーションを世界規模で実現する事であり，従来のマスコミュニケーションとしてのブロードキャストコミュニケーション(１：N)や，電話による１：１コミュニケーションに対して，コミュニケーションの範囲が飛躍的に増大する。また，情報が電子化され，即時性が加わっている為，これまで人類が経験し得なかった新たな価値観が創造される。しかし，社会の基本インフラストラクチャーとなるには，影の部分をクリアして行く必要がある。モラルや法制度，弱者を生まない為の工夫，産業構造の転換等社会科学側面の整備も不可欠であり，ネットワークの機能・性能の向上，運用維持，セキュリティの確保等技術レベルで解決すべき課題も多く存在する。

このために，今後も多くの個人，企業，団体が支援育成を行ってゆくことになる。当社では，これまでの生産財の分野から，IPネットワークインフラストラクチャー

*1 IT事業部　ビジネス開発センター

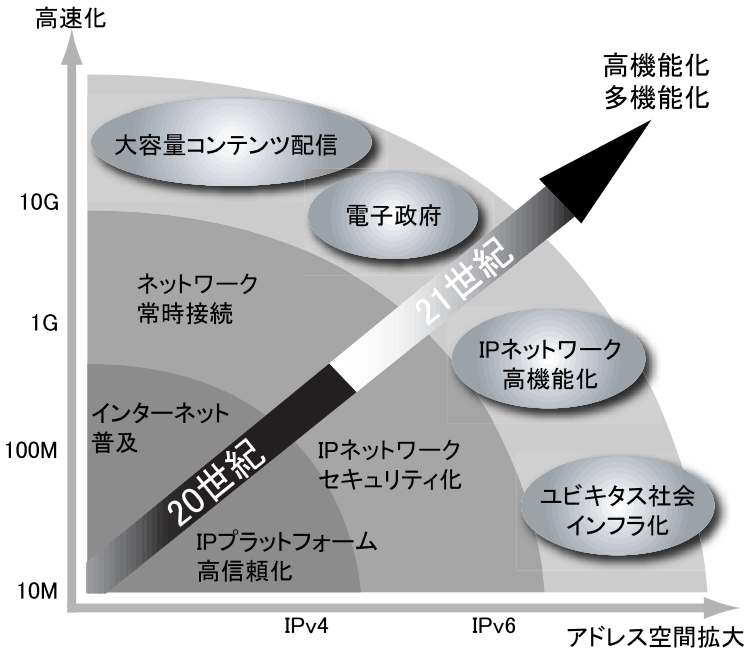

図１　IPネットワークの進化

の分野でもサプライヤーの役割を担う事で，社会への貢献を果たしたいと考えている。

2.　IPネットワークソリューションのコンセプト

マクロ視点のネットワーク進化の概要を，**図１**に示す。社会の多くの人々と，産業や社会の機能に役立つ為には，通信の高速化と常時接続環境の実現，及び，IPv4からIPv6へのアドレス空間の拡大，それに伴うネットワークの機能的な進化が必要になる。当社の“IPネットワークソリューション”は，このベクトル方向に視点を置き，ネットワーク関連の機器・システムの機能・性能向上を図る分野，可用性(アベイラビリティ)確保のためのネットワークサイト監視，運用支援の分野，及び，セキュリティに関する監視，運用，コンサルティングといった分野に注力して行く。

3.　IPネットワークシステムの運用管理

これまで述べた範囲の内，急速な情報化，ネットワーク化で，ECサイトで急速にニーズが顕在化してきた分野にサイトの可用性の確保がある。IPネットワークサイトでは多くのベンダー，システムインテグレータが協力してシステム設計，構築，維持運用を行っている。この階層を図式化したものが**図２**である。

ネットワークレイヤーが提供する高速情報通信機能と，アプリケーションレイヤーの間には，エンジニアリングが必要なレイヤーが存在する。従来は，システムインテグレータが案件単位に対応してきた部分である。しかし，IPネットワークがインフラストラクチャー化するためには，アプリケーションを構築する場合，IPネットワークの仕組みを意識せず，自由に使いこなせることが必要である。アプリケーションレイヤーと，ネットワークレイヤーをつなぐこの階層を，当社ではサービス・サポート・レイヤー(SSL)と名付け，この階層での仕組みを総称してアプリケーション・サービス・インフラストラクチャー(ASI)と呼んでいる。このASIの内容は，現状ではマネージメントサービスプロバイダ(MSP)とセキュリティサービスプロバイダ(SSP)から構成される。

MSPはサーバやネットワーク機器の運用管理であり，機器の異常検知や負荷管理が主体となる。また，SSPはウィルス攻撃，セキュリティホールからのアタックや不正侵入，分散型サービス不能攻撃等への対応が主体である。(この中の不正侵入監視に付いては，「ネットワーク不正侵入監視システムIS1000シリーズ」として，横河技報vol. 44，no. 4，2000で既に紹介している。)このMSPとSSPは機能上別けているが，サイトの可用性の確保というユーザニーズからは密接不可分の機能であり，監視と運用管理機能の統合支援機能となる。顧客にとって，この部分を外部に委託する最大のメリットは，ネットワーク人材確保と経済性である。なぜならば，IPネットワーク機器は日進月歩が続いており，セキュリティ対応も同様に，次々と新たな攻撃が発生し，１ユーザがこれらの突発事象に対応する為に，高度のネットワークエンジニアを24時間365日常時待機させ，かつ，監視システムやログ解析TOOLを保持しつづける事は，個々の企業にとっては大きな負担となり，事実上不可能だからである。

また，iDC(Internet Data Center)にサイト設定する場合は，iDCの機密機構とスペース上の制約から，遠隔監視・運用管理が不可欠となり，様々な分野のエキスパートを揃え，通常の対応は極力自動化した監視・運用支援が不可欠となる。この可用性確保のサービスを提供するシステムとして，本特集号では「統合リモート監視システム」を紹介する。

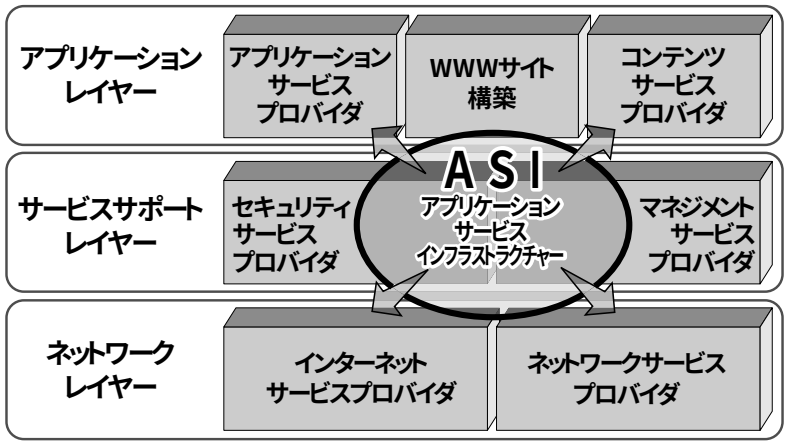

図２　IPネットワークソリューションサービスの位置付け
― ASIの充実が急務 ―

4.　IPネットワークシステムのセキュリティ

4.1 IPネットワークシステムのセキュリティ研究開発

インターネットが社会的基盤(クリティカルインフラストラクチャ)としての重みを増すに連れて最重要になるのが，セキュリティの確保である。セキュリティは“セキュリティポリシー”，“個人認証”，“暗号化”といった全般的な対応と，“ウィルス”，“アタック”，“クラッキング”のような外部攻撃への対応に大別される。今回はこの中の外部からの攻撃に対するセキュリティについて紹介を行う。

外部からの攻撃に関しては，次に示すような4つの段階の脅威があると言われている。

ネットワークに迫る脅威の４分類

1. 個人による悪戯や攻撃
2. 集団によるサイバー犯罪
3. 集団によるサイバーテロ
4. 国家による情報戦争

現状，セキュリティ対策としては上記 １，２に分類されるものを想定したセキュリティプロダクトやサービスが一般的である。これは，しかしながら，最近では，他国から日本に向けて行われたクラッキング予告を伴うWEB ページ改竄などが発生しており，年々増加するサイバースペースでのクラッキングが既に上記 １，２の段階から３のサイバーテロに近づきつつあることを示している。また，インターネットなどのサイバースペースにおけるこれらの脅威が通常の実社会とは異なる点として，全ての段階においても利用される技術がほぼ同じであるという点が挙げられる。この特性から，上記3の段階で使用された技術がすぐに，１，２の段階に普及し，クラッキング技術は加速度的に洗練されることが予想される。

当社では一般へのセキュリティソリューションの提供を行うと共に，セキュリティ技術は，上記４つの段階に共通する可能性があるという認識で取り組んでいる。

そのため活動として，国の研究機関などとサイバーテロ対策についての共同研究も行っており，その研究の中から，開発されたものが，本稿以降の論文に紹介する

「DDoS Attackシミュレータ」

「脆弱性情報データベース」

である。

セキュリティを確保する上で，クラッカーがどのように攻撃を仕掛けてくるのかを知ることは非常に重要である。実際の手口を再現することで，どのような対抗手段を講じるべきかを予め検討しておき，実際に攻撃が行われた場合にどのような手段が使用されているかを把握し，迅速且つ的確な対応処置を講じることが出来るように，準備しておく必要がある。

このような観点から，2000年当初から実ネットワークで被害が出始め，その被害が甚大となる分散型サービス不能攻撃(DDoS : Distributed Denial of Service)に注目し，その攻撃方法の研究や実際の攻撃ツールがどのように動作するか，及びその際の被攻撃側システムがどのような挙動を示すのかを調査してきた。そのための装置として，分散型サービス不能攻撃を模擬する「DDoS Attackシミュレータ」の開発を行った。

さらに，クラッカー側の手段だけではなく，守るべきシステム側にどのような弱み・脆弱性があるかを十分に知っておくことも重要である。クラッカーよりいち早く脆弱な点を知り，対策を施すことで常に強固なシステムを保持することが可能となる。そのための基礎的なデータを保持し，自由な検索ができるシステムとして「脆弱性情報データベース」を開発した。

4.2 IPネットワークシステムのセキュリティ製品・サービス

一般にセキュリティ製品・サービスがどのような機能を提供しているかを，家の安全を確保するモデルに置き換えて説明すると，理解し易い。

- まず，家の門をしっかり守るという意味では，ファイアウォールの設置が該当すると思われる。
- 監視カメラを設置したり番犬を放って，外部からの侵入者を監視することは，侵入検知システム設置が該当する。
- 何かあった時に対応するために守衛などを配置するこ

とは，リモート監視サービスに当る。
・さらに，家全体の戸締まりが十分であるかをチェックすることは，セキュリティスキャンサービス或いはペネトレーションテストを行うことと考えられる。
・また，家全体の安全対策が十分であり，バランスがとれているかを検討することは，システム全体のセキュリティポリシーを策定することと同じである。

家の安全確保を考えるのと同じように，IP ネットワークシステムの安全性・安定性を確保するためには，ただ単にファイアウォールを設置しただけで良いというものではない。それぞれの特性を考えて，必要なセキュリティプロダクト・サービスを組み合わせて設計し，それらが総合的に機能するように構築することが重要である。

現在，主なセキュリティプロダクト・サービスとして以下のものを提供している。
・システム全体のセキュリティの品質を高めるための「セキュリティポリシーサービス」
・各種セキュリティプロダクトの設置・設定，セキュリティシステムの設計を行う「セキュリティプロフェッショナルサービス」
・侵入検知システムアプライアンスサーバ「IS100, IS700, IS1000」
・運用・監視サービス「統合リモート監視・運用サービス pilotEye」
・システム内部からの情報漏洩監視装置「パケットブラックホール」(販売元レーザファイブ社)

当社では，IPネットワークシステムのセキュリティを確保するために，核となるこれらセキュリティプロダクトと，それらを総合的に結び付けるサービスを提供し，顧客にソリューションとしてセキュリティ技術を提供している。また，インターネット上で実際に起っている各種攻撃やクラッカーについて調査・研究活動を行い，より確実で常に最先端のセキュリティソリューションを提供できるようにしていきたいと考えている。

5. IPv6への展開

次世代のインターネット環境は，IPv6を活用し，且つ，高速・常時接続となる。しかし，IPv4から，IPv6への移行は突然転換される訳ではなく，既存のIPv4の利用形態を活かしながら，これまでネットワーク化が図られてこなかった分野，例えば，自動車や家庭で使用される様々な機器から普及が始まると考えられる。

5.1 IPv6／IPv4トランスレーション

IPv6への移行をスムースに行うためには，IPv6の利用形態から，既に多数あるIPv4のコンテンツ資産をアクセスできるトランスレーション機能が不可欠である。このために開発された商品が「IPv6／IPv4トランスレータTTB」である。この技術についての詳細は，本特集号掲載の「IPv6／IPv4トランスレータTTB」を参照いただきたい。

5.2 IPv6利用技術の開発

IPv6環境では，いわゆるコンピュータではないネットワーク機能を保有した多くのノードが接続され，このノードが相互にコミュニケーションをするようになる。IPv6に関しては，当社はこれまでの国家プロジェクトへの参画を通して，多くの技術と経験を積ませて頂いた。そこで，これらを活かして，株式会社ワイドリサーチとの合弁企業であるインターネット・ノード株式会社(INI)を設立し，IPv6を活用したマイクロノード(サーバー機能を内蔵した機器)を開発し，これを活用したアプリケーション開発にも取り組んでいる。本特集号では，世界初のIPv6マイクロノードである「温度測定マイクロノード」についての詳細を掲載している。また，アプリケーション開発の過程で，インターネット経由の大量情報をどの様にハンドリングするか，セキュリティ確保をどの様にするか，データのマイニング方法等，解決すべき課題が明らかになりつつある。本件については，今後，実施される実証試験後に，成果を詳細に報告する。

6. おわりに

当社はIPネットワーク時代の新たな産業ニーズに対応すべく，ASI(Application Service Infrastructure)の部分にリソースを集約し，高度情報社会の産業基盤に貢献したいと考えている。各項目の詳細は，本特集号の各論文に述べられている。

また，当社のインダストリアル・オートメーション分野における工場の制御システムと管理コンピュータ，及びそこに接続されるオープンネットワーク環境でのセキュリティの考え方と実証結果は，「プラントネットワークセキュリティ」として，横河技報vol. 45, no .1, 2001に紹介されている。この技術も同一の思想の下で開発されたものである。今回の報告は，主にインターネット環境下における可用性の確保を主眼としてご紹介させて頂いた。

* 本文中の製品名，名称は，各社の商標もしくは，登録商標です。