セキュアネットワークソリューション

大多和　篤夫　　辻　秀幸
飯島　勝　　八木　勇

はじめに

e-Japan重点計画をはじめ行政分野や一般社会にIT（Information Technology）が普及し，ITによる社会の基盤形成が急速に進んでいる[1) 2)]。反面，知らず知らずのうちに「IT依存」，「ネットワーク依存」の傾向が高まり，脆弱な情報セキュリティ対策や低いセキュリティ意識が横行する現在，社会の安全確保への懸念も増しつつある。政府主導のセキュリティ施策も進められているが，我が国の安全保障の点で，より高いレベルの情報セキュリティの確保が喫緊の課題である。

本稿では，日本のセキュリティ施策の動向やネットワーク社会の課題を踏まえ，当社のセキュアネットワークソリューションを，中核である広域ネットワーク防護システムを中心に紹介する。

日本政府のセキュリティ施策

日本のセキュリティ施策は，平成12年1月に起きた政府機関のホームページ連続改ざん事件に端を発し，

- 情報セキュリティポリシーに関するガイドライン（平成12年7月18日）
- 重要インフラのサイバーテロ対策に係る特別行動計画（平成12年12月15日）
- 欧州評議会「サイバー犯罪条約（Convention of Cybercrime）」へ署名（平成13年11月23日）
- 内閣官房NIRT（緊急対応支援チーム:National Incident Response Team）発足（平成14年4月1日）
- OECD（経済開発協力機構）情報セキュリティガイドライン改訂（平成14年7月25日）
- 情報セキュリティ総合戦略の策定（平成15年10月10日）

等々の諸施策が推進されてきた（**図1**）。

一方，平成9年より霞が関WAN，住民基本台帳ネットワーク，総合行政ネットワーク（LGWAN），政府認証基盤（GPKI），地方公共団体組織認証基盤（LGPKI），公的個人認証基盤といった日本の行政分野の要となるさまざまな基盤システムの整備が進んできている。

これまで急速に進められてきた，いわゆる電子政府，電子自治体の基盤システムの整備施策であったが，情報セキュリティ確保という点においては，各府省個別の対策という範囲から政府横断的な対策へと，現在見直しが進められている。たとえば，経済産業省が昨年10月10日に策定した「情報セキュリティ総合戦略」[3)]には，“しなやかな「事故前提社会システム」の構築”なども盛り込まれ，サイバーテロ対策などへの具体施策に拍車がかかると予想される。

ネットワーク社会の課題

現代社会は，ネットワークこそ人間の知的活動を行う上で必須となる“知的ツール”と捉え，IT基盤の構築を推進し，ネットワークのオープン化や，インターネットの普及とともに接続を広げ，コンピュータ資源を有効に活用する術を創造してきた。そして，ネットワークを介してさまざまな情報を伝達・共有・処理を行うためには，セキュリティの確保が必要であることも学んできた。

たとえば，情報の機密性を確保するには暗号化すればよいが，情報を共有，処理するためには復号が必要である。

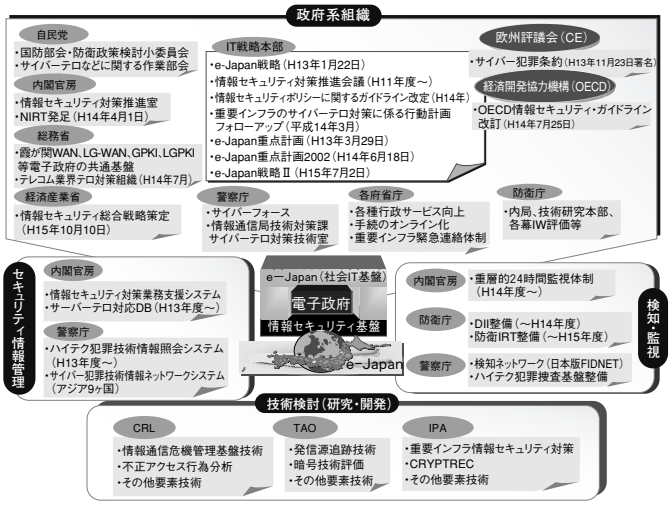

図1　e-Japanセキュリティ施策の動向

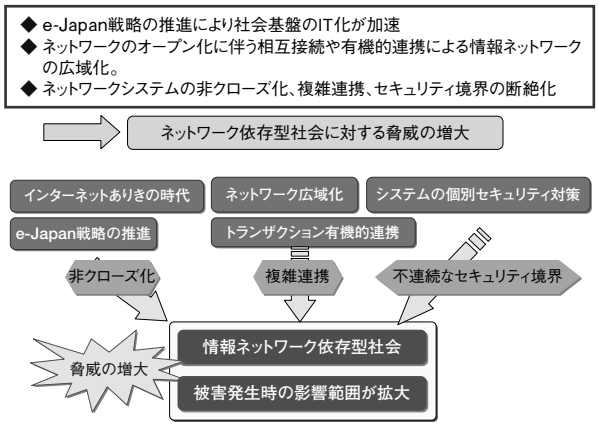

図2　情報ネットワーク依存型社会の課題

情報を扱う当事者同士が必要に応じて機密性を確保できることが理想だが，物理的な制約，論理的な制約から情報を非クローズ（オープン）にせざるを得ない段階が必ず存在し，そこが脆弱性を生むことになる。

一方，これらの流れは情報セキュリティという観点では，情報の“非クローズ化”やシステム同士の複雑連携による“セキュリティ境界の断絶”を招いており，セキュリティ上の隙間を生じさせている（**図2**）。

悪意を持った攻撃者がネットワーク越しにサーバを探索し，脆弱性が対策されないまま放置されたWebサーバやメールサーバ等を狙ったサービス妨害やホームページの改ざんといった不正アクセス事件，昨年8月に猛威を振るったBlasterワームなどコンピュータウィルスの蔓延による被害が日常茶飯事で発生している。このような昨今の情報セキュリティに関わる事件や社会的不安を鑑みると，

- September11以降のテロ事件の多発
- 顧客情報や機密情報の漏えい事件の多発
- 住民基本台帳ネットワークの本格始動
- 日本的な性善説は格好の標的になり得る

など，安全担保を懸念する事柄が多い。

また，一般社会におけるセキュリティ対策状況や国家レベルの安全対策の点では，

- Webサイトに対するサイバー攻撃，コンピュータウィルスによる被害は日常化し，もはや一般的なセキュリティ対策では不十分。（技術の陳腐化）
- 世界各国で起こるテロ行為，国交異常や緊張の高まりにより，国家安全保障といったナショナルセキュリティの強化が必要。（ナショナルセキュリティ）
- 経済の低迷とIT神話の崩壊から，あらゆる企業活動の分野で生き残りをかけて競っており，マクロ経済の視点に立ったリスク管理が必要。（リスクマネジメント）

といった課題がある。

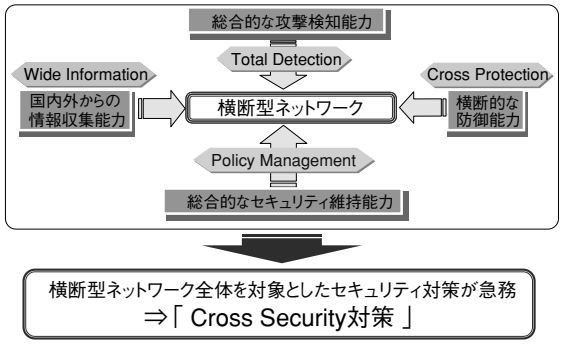

図3　横断型ネットワークのセキュリティの対策

極端な場合，企業活動や諜報活動といった断面では，従来の方法では競争相手に勝ることができないとなると，「手段を問わない」といった方法をとることも考えられる。このように考えると，利益中心主義的な企業活動，諜報活動が新たな脅威を生む可能性すらうかがえる。

まさに今，社会インフラの防護といった視点で，ネットワークインフラを狙った所謂“サイバーテロ”までをも想定した“横断型ネットワーク防御の仕組み”が必要になってきている（**図3**）。

電子政府のネットワーク基盤を例にとると，霞が関WANで各府省の行政システムが相互接続された電子政府システムは，複数の外部接続点を有する広域のIPネットワークで接続された“広域イントラネット”として捉えることができる。

一般的に，この形態では各々個別にシステムのセキュリティ領域を管理することになり，セキュリティ境界の断絶化が起こり易い。このため，相互接続点に位置付けられる各拠点で，セキュリティ事案（たとえばサイバーテロのような一斉攻撃）発生時のポリシーを明確にする必要がある。ポリシーの共有やメンテナンスなどを考慮すると，システム規模によっては相互接続されたシステム全体で新たなセキュリティ境界を設けるほうが合理的な運用管理が可能になる。

セキュアネットワークの基本概念

当社が提供する「セキュアネットワーク」の基本概念を述べる。

インターネット等の外部ネットワークとの接続点のセキュリティ対策においては，不正アクセスの有無をIDS（IDS：Intrusion Detection System）と呼ばれる侵入検知システムで監視し，ファイアウォールによって不要なトラフィックの流入を防ぐといった方法が一般的である。しかし，ネットワークを流れるデータフローやシステムの動作履歴から不正なアクセスを見極める際の不正アク

セス検知機能と捕捉した当該データフロー（不正アクセスと判別したトラフィック）に対する遮断機能が十分でないため，機能上の信頼性を欠く問題が指摘されている。

このため，侵入検知システムやファイアウォールを導入しただけでは十分とは言い難く，システム管理者によるログの分析など，セキュリティに関する運用の負担を強いる結果となっている。

また，たとえ侵入検知システムやファイアウォールの扱いに精通していても，攻撃者の動機が悪戯なのか，別の目的なのかまでの判別は困難極まりなく，その上“サイバーテロ”が突如として起こる事などの予測は極めて困難と言える。即ち，いざという時の緊急対応がシステムの可用性に大きく影響を与え，放っておけばシステムダウンや誤動作を招きかねないという危険性をはらんでおり，システムのアラート認識がセキュリティ管理の課題となっている。

当社では長年のシステム構築経験，研究開発成果をもとに上記の課題を解決し，お客様が安心して利用できるネットワークを実現するためのセキュリティ基盤「セキュアネットワーク」を実現した。

「セキュアネットワーク」では，ネットワークの運用に主眼を置き，従来技術だけでは不十分なセキュリティ機能を向上させ，セキュリティ管理の負担を軽減する統合化されたソリューションを提供している。

相互接続によって形成された“広域イントラネット”など横断型ネットワークにおいては，ネットワーク全体の安全を保つため，

- 統一的ポリシー制御
- 不正トラフィック遮断，横断的アクセス制御
- 高度な侵入検知，攻撃追跡
- 防御情報の有効活用

といった，新技術が強く望まれている。「セキュアネットワーク」では，これらの各機能が互いに連携してネットワーク全体で効率的なセキュリティの管理が行えるようになっている。**図4**に「セキュアネットワーク」の基本概念を，**図5**にセキュアネットワークソリューションの概要を示す。

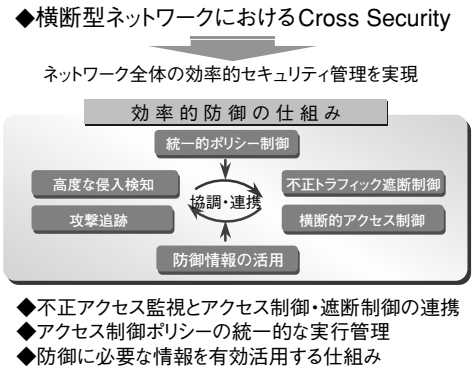

図4　セキュアネットワークの基本概念

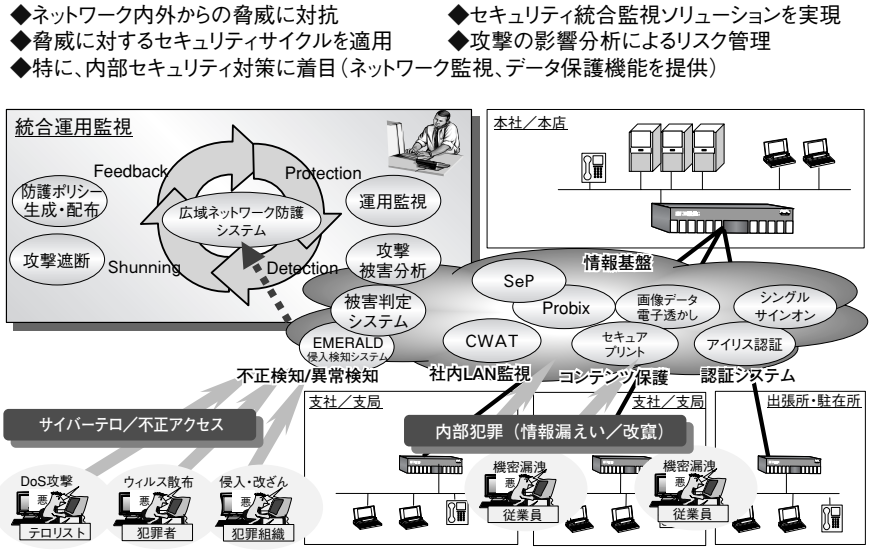

図5　セキュアネットワークソリューションの概要

広域ネットワーク防護システム

セキュリティ機能を実現する上で，運用管理が重要であることは言うまでもない。運用管理においては，業務システムのセキュリティ機能が何を対象としたか，その動作が正しく処理されたか，業務システムの状態が危機的状態に陥ってないかなど，業務システムの運用継続の可否に係る判断をしなければならない。

また，更にネットワークの安全性と可用性を最大限にするためのシステム要件として以下が挙げられる。

- Protection：通常状態において，業務システムが最低限必要なセキュリティポリシーで保護されていること
- Detection：通常状態のセキュリティポリシーでは回避できない攻撃を被った場合，それを検知できること
- Shunning：業務システムに対する影響が最低限の範囲に抑止できるよう回避できること

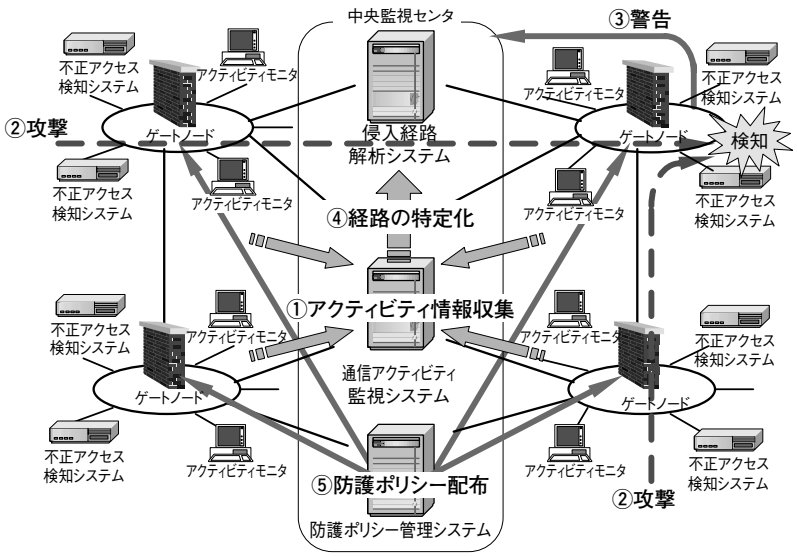

図6　広域ネットワーク防護システム

●Feedback：業務システムが影響を被った場合，当該攻撃に対する抵抗力を持つこと

上記のシステム要件を有機的に機能させるためには，各プロセスが閉じた系として連携することが重要である。たとえば，マルチサイトのネットワークにおけるShunningプロセスにおいては，影響の抑止（システムの切り離し）範囲を特定化することで被害の最小化が実現でき，Feedbackプロセスを当該攻撃を被ったサイト以外に適用することで，「Protection→Detection→Shunning→Feedback→Protection・・・」といったネットワーク全体の運用継続性を重視した学習型のセキュリティ管理機能を実現することができる。

我々は，これらをセキュリティサイクル化し，ネットワーク全体の強度が自律的に進化できるよう適応型セキュリティを目指している。

図6に，広域イントラネットを「セキュアネットワーク」によって実現した“広域ネットワーク防護システム”を示す。

本システムは，広域ネットワークの各拠点に不正アクセス検知システム，アクティビティモニタ，およびファイアウォールを分散配置し，これらを中央監視センターから一括で統合管理する構成になっている。

中央監視センターでは各拠点を通過する通信パケットに対して，発信元，宛先等の情報から通信のパス情報（「アクティビティ情報」という）をアクティビティモニタで監視し，通信経路の特定化を行うための通信アクティビティの識別を行う（**図6**①）。

各拠点に配置した不正アクセス検知システムが不正アクセスを検知した場合，もしくは複数の経路を使って攻撃を行うような分散型の不正アクセスを検知した場合，中央監視センターのアクティビティ識別により，当該通信アクティビティを観測したネットワーク上の位置情報から侵入経路を特定化する（**図6**②，③，④）。

中央監視センターの防護ポリシー管理システムでは，発信元からのアクセスを禁止するなどアクセス制御命令を生成し，侵入経路となったファイアウォールやその他のファイアウォールに対し防護ポリシーとして配布する（**図6**⑤）。

“広域ネットワーク防護システム”はマルチサイトにおけるシステム全体の統一的セキュリティ管理を実現した事例である。**図6**に示すシステム構成で，攻撃検知機能は不正アクセスに限定した構成であり，不正アクセス検知システムに他の検知機能を有するセンサシステムを付加することで，さまざまな脅威に対抗することが可能である。

ま と め

当社が提供する「セキュアネットワーク」の基本概念と，その中核である“広域ネットワーク防護システム”を中心に紹介してきた。

我々は，お客様が安心して利用できるネットワークソリューションを提供することにより，社会の発展に寄与したいと考える。 ◆◆

■参考文献

1）e-Japan重点計画，IT戦略本部，平成13年3月29日
2）e-Japan戦略Ⅱ，IT戦略本部，平成15年7月2日
3）情報セキュリティ総合戦略，経済産業省，平成15年10月10日

●筆者紹介

大多和篤夫：Atsuo Ootawa.システムソリューションカンパニー 社会情報ソリューション本部 セキュアネットワーク推進プロジェクト プロジェクトリーダ
辻秀幸：Hideyuki Tsuji.システムソリューションカンパニー 社会情報ソリューション本部 セキュアネットワーク推進プロジェクト ステアリングコミッティー
飯島勝：Masaru Iijima.沖ソフトウェア株式会社 東京第2支社 システム1部
八木勇：Isamu Yagi. システムソリューションカンパニー 社会情報ソリューション本部 セキュアネットワーク推進プロジェクト