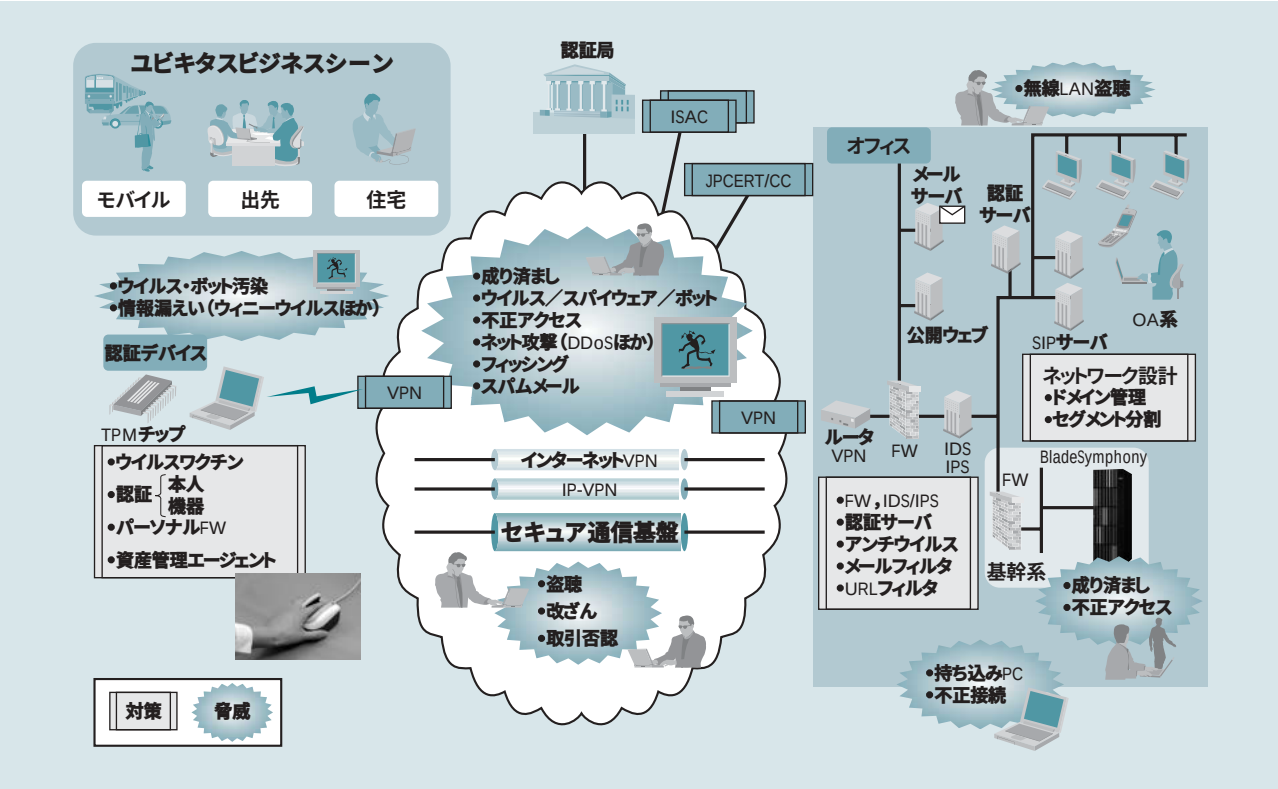
トータルネットワークセキュリティソリューション

Total Network Security Solution

金野 千里 Chisato konno
坏 毅 Takeshi Akutsu
山田 知明 Tomoaki Yamada
瀬野尾 修二 Shûji Senoo



注:略語説明 TPM(Trusted Platform Module)，ISAC(Information Sharing and Analysis Center)，JPCERT/CC(Japan Computer Emergency Response Team/Coordination Center)，FW(Fire Wall)，VPN(Virtual Private Network)，IDS(Intrusion Detection System)，IPS(Intrusion Prevention System)，DDoS(Distributed Denial of Services)，SIP(Session Initiation Protocol)，IP(Internet Protocol)，URL(Uniform Resource Locator)

図1 ネットワークの脅威とセキュリティ対策のイメージ
社内外のネットワークに存在するさまざまな脅威に対して，クライアント，ネットワーク上，サイトにおけるセキュリティ対策全体のイメージを示す。

1. はじめに

近年のブロードバンドの普及，パソコンの性能向上，IP(Internet Protocol)テレフォニーとの融合などを背景に，オフィスでの業務形態の変化やワークプレイスのユビキタス化が進んでいる。いつでも，どこでも，タイムリーな処理や情報へのアクセスが可能となり，業務のスピード・効率も飛躍的に向上してきている。その一方で，ネットワークは，成り済まし，ネット攻撃，感染力の強いウイルスの出現，不正アクセス，盗聴などに加え，フィッシングといった人間工学的な攻撃まで，さまざまな脅威にさらされており，さらには2005年4月に施行された個人情報保護法への対応なども，組織にとっては大きな課題となってきている[1)]。

ここでは，ネットワークのセキュリティ上のさまざまな脅威と，それに対するトータルなセキュリティソリューション，ユビキタスアクセスで重要となる確実な認証や検疫ネットワーク，および安全なネットワークソリューションについて述べる(**図1**参照)。

2. ネットワークにおける脅威と対策

2.1 ネットワークにおける脅威

ネットワークの利用には以下のようなさまざまな脅威が存在する(**図2**参照)。

(1) 成り済まし:クライアント，サイト双方

オフィス業務形態の変化やワークプレイスのユビキタス化の進展に伴い，業務のスピードや効率は飛躍的に向上し，インターネットを介した商取引やサービスも活況を呈してきている。一方，ネットワークには，成り済まし，ネット攻撃，不正アクセス，盗聴，ウイルス，フィッシングなど，さまざまな脅威が存在している。個人情報保護法への対応なども含め，ネットワークのセキュリティ対策は組織にとって大きな課題となってきている。

（2）不正アクセス:セキュリティホール利用など
（3）ネット攻撃:DoS（Denial of Services）系攻撃による大量パケット送付など
（4）ウイルス，スパイウェア，ボット
（5）盗聴:公開ネットワーク上や無線LAN（Local Area Network）など
（6）不正接続:サイト内ネットワークへの持ち込みPC（Personal Computer）など
（7）メール経由情報漏えい:個人情報ファイル添付など
（8）スパムメール:業務外やフィッシングメールなど
（9）フィッシング:ウェブサイトの成り済ましなど
（10）ウェブ経由情報漏えい:掲示板投稿，ウェブメールなど
（11）ウェブ業務外利用:汚染サイトアクセス含む
（12）データ改ざん，取引否認など

これらのいずれもが，攻撃手法の巧妙化，攻撃源の広域分散化，強い感染力，被害情報量の増大など深刻な問題となっており，以下の多面的な被害を生じさせている。
（1）ウイルスやネット攻撃などイベント・インシデント系のネットワーク正常利用への妨害
（2）盗聴や情報漏えいをはじめとした組織情報への被害
（3）スパムメールや業務外利用などの業務効率の低下

それぞれのシステムやサービスには，これらの脅威に対する適切なリスク評価に基づいた対策が重要となる。

2.2 セキュリティ対策の全体像

ネットワークのセキュリティ対策は，（1）ネットワークの利用規約やポリシーの策定，（2）ネットワーク設計と構築，（3）脅威に対するツールの選択と対策，および（4）運用管理・監視・改善対策の実施から成る。

このうち（3）に関する最近の動向として以下があげられる。
（a）IEEE 802.1x系のネットワーク認証機構，TPM（Trusted Platform Module）などによる端末認証，生体を活用した本人認証など，認証レベルの強化
（b）複数の脅威に対応する複合アプライアンスサーバ
（c）セキュリティ機能を持ったインテリジェントスイッチ
（d）認証，暗号化などを備えたネットワークインフラ
（e）イベント・インシデント情報の共有による対応体制を国や業界として整備〔Telecom-ISAC（財団法人日本データ通信協会テレコム・アイザック推進会議）など〕

セキュリティ上の脅威はネットワークを介してくるが，対策は

脅威		セキュリティ対策 クライアント	ネットワーク	サイト内
インシデント&イベント	成り済まし	認証デバイス〈ユーザー認証〉〈機器認証〉	認証局サーバ	認証サーバ〈RADIUS〉〈PKI認証〉
情報漏えい	不正アクセス	P-FW, P-IDS/IPS	インシデント情報提供サービス	運用監視 FW, IDS/IPS
業務妨害	ネット攻撃			アンチウイルスゲートウェイ
	ウイルス スパイウェア・ボット	ウイルスワクチン P-FW, P-IPS		セキュリティパッチ対策 検疫ネットワーク
	盗聴	データ暗号化	VPN〈SSL, IPsec ほか〉	データ暗号化
	不正接続	−	−	不正PC／汚染PC排除ツール
	メール経由情報漏えい スパムメール	−	−	メールフィルタ スパムフィルタ
	フィッシング	認証プラグイン	サイト認証サービス	サイト／メール真正性保証
	ウェブ経由情報漏えい ウェブ業務外利用	−	URLフィルタリングサービス	URLフィルタ
	データ改ざん・否認	PKI電子署名	真正性保証・タイムスタンプサービス	PKI電子署名

注:略語説明　VPN（Virtual Private Network），SSL（Secure Socket Layer），IPsec（Security Architecture for Internet Protocol），P（Personal）RADIUS（Remote Authentication Dial In User Service），PKI（Public Key Infrastructure）

図2　ネットワークにおける脅威と対策の一覧
縦軸に脅威を，横軸に対策個所と対策内容を示す。

クライアント，ネットワーク上，サイト（内のサーバ類）に対して，それぞれの部分で実施することになる。脅威と対策の全体像を**図2**に示す。

日立製作所および日立グループは，セキュリティのトータルソリューション体系として「Secureplaza」[2),3)]をそろえており，常に最新技術を取り込んで，脅威群へのトータルなセキュリティ対策を提供している。この対策にかかわるソリューションには以下の三つがある[4)]。

（1）Secureplaza/HS（Healthcare Service）

セキュリティマネジメント，不正アクセス監視と対策，セキュリティ情報提供などから成るセキュリティレベルの維持・管理サービス群

（2）Secureplaza/PB（Pollution Block）

既知のウイルス対策，未知のウイルス対策，持ち込みPCからの感染防止，サイト内の感染拡大抑止などから成るトータルなウイルス汚染防止対策

（3）Secureplaza/EI（Event Incident & Action）

セキュリティオペレーションセンターで，サイバー，フィジカルの両面からイベント・インシデントを統合監視，分析を行い，事前予防と速やかな対策を実現するソリューション

3. 認証およびセキュアネットワークソリューション

ここでは，2.2節で述べた最新の動向に対応した主なソリューションについて紹介する。

3.1 認　　証

認証は，オープンなネットワークでのセキュリティ対策の鍵となる機能である。ネットワークでの利用における認証には，「ユーザー認証」と「機器（クライアント，サーバ，サイト）認証」の二つがある。

認証の実現には以下の情報が用いられる。

（1）ID/パスワードなどの記憶情報

（2）USB（Universal Serial Bus）キー，ICカード，MAC（Media Access Control）アドレス，PKI（公開鍵暗号認証基盤）における暗号鍵などの所持物情報

（3）バイオメトリクスなど本人自身の情報

これまで，ユーザー認証については（1）と（2）が主に用いられてきたが，最近では（3）が用いられ始めている。ただし，ネットワークを通しての本人認証は，ネットワーク上で安全に認証が実現できるPKIなどと連携して，ローカルで本人認証を指静脈認証などによって実施し，その認証結果をもって有効となるPKIでネットワーク上での認証を実現することが可能である。また，機器（クライアント，サーバ，サイト）認証には，これまで（2）が用いられてきたが，USBキーやICカードなどでは盗難が，MACアドレスなどでは詐称が脅威となっている。こうした中で，PCやネットワーク装置などの機器にセキュリティチップを搭載する動きが始まっており，今後の大きな流れになることが予想される。

3.2 TCGおよびTPMソリューション

TCG（Trusted Computing Group）は，日立製作所をはじめ120社以上の企業が参加するセキュリティに関する標準仕様を検討する業界団体である[4)]。TCGの目的は，TPM（Trusted Platform Module）と呼ばれるPCプラットフォームに埋め込まれたセキュリティチップを信頼の要とした，信頼できるコンピューティング環境の実現である。TCGの技術，およびTPMについて以下に述べる。

（1）エンドポイントセキュリティの強化

現在，ネットワークに接続されているさまざまな端末・デバイスはウイルス，スパイウェア，不正アクセス，また情報漏えいなどセキュリティの脅威に常にさらされており，ネットワーク全体のセキュリティ確保のためにもエンドポイント（クライアント端末）におけるセキュリティ強化が不可欠である。TCGでは，ウイルス，スパイウェアなどによるプラットフォームの改ざんのリスクに対して，耐タンパなハードウェアデバイスであるTPMを利用し，プラットフォームの信頼性を保証する仕組みを提供している。すでに多くのPCにTPMが搭載され出荷されており，今後これらを有効に活用したセキュリティソリューションの展開が重要となってくる。TPMを活用したソリューションのメリットは四つある。

（a）システム構成の完全性保証

（b）ハードウェアによるデータ保護（情報漏えい防止）

（c）ハードウェアによる鍵管理・暗号処理環境

（d）TCO（Total Cost of Ownership）の削減

TCGの技術は，既存のセキュリティソリューションの強化策としても有効であることから，日立グループでは，すでに指静脈認証装置とも連携しており，今後もTPMの耐タンパ性を有効に活用した製品・ソリューションを展開していく。

（2）ネットワークセキュリティへの展開

ネットワークセキュリティへの活用として，まずPCプラットフォームに埋め込まれたTPMを利用した端末認証があげられる。現在，端末認証にはMACアドレスやIPアドレスが利用されているが，いずれも容易に改ざんすることが可能である。いっそう確実に端末を識別・認証する技術として，TPMに埋め込んだPKI証明書を用いた認証が有効である。Secureplaza/IM（Identity Management）では，以下の端末認証ソリューションをそろえている。

（a）リモートアクセス時の端末認証〔SSL-VPN（Secure Socket Layer-Virtual Private Network）/IPsec（Security Architecture for Internet Protocol）〕

(b) 社内LANの端末認証〔IEEE 802.1x EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)〕

また，TCGの技術を利用することにより，エンドポイントのソフトウェア構成をリモートから検証することが可能となる。すなわち，社内のネットワークに接続される端末が企業のセキュリティポリシーに適合しているかをチェックし，アクセス制御に利用することが可能である。これらの技術はTNC(Trusted Network Connect)としてTCG内で標準化が進められており，今後さまざまなネットワークセキュリティ製品に組み込んでいく。

3.3 日立セキュア通信基盤ソリューション

社内ネットワークに潜むさまざまな脅威に対して，認証，通信路保護，アクセス制御，利用履歴の一元管理などをそれぞれに実現することは，事前検討やツールの選定，構築などを含め，期間やコストが掛かることになる。日立グループは，組織内における本来のセキュアネットワークインフラとして，これらをオールインワンでパッケージングしたセキュア通信基盤ソリューションを提供している。このソリューションによって既存ネットワークを堅強なセキュリティ環境に変えることが可能で，運用管理も容易になる(54ページ参照)。

3.4 検疫ソリューション

近年，業務ニーズにより，社外や自宅へPCを持ち出して使用するモバイルアクセスが増えてきている。そうした環境下では，再度そのPCが持ち込まれ，社内ネットワークへ接続されることがサイトにとって大きな脅威となる。それに対する対策である検疫ソリューションのフローを図3に示す。インテリジェントスイッチ，ネットワーク監視ツール，資産管理ツール，ウイルスワクチン機能などを組み合わせることによって，それぞれのサイトのネットワーク環境に合わせたさまざまなレベルの検疫を実現することができる。一例として，日立グループは，総合システム運用管理ツール「JP1」と不正PC接続抑止／切断ツールである「NX NetMonitor」[5]と連携することにより，検出・隔離・治療・再接続を一貫して行うソリューションを提供している。

4. おわりに

ここでは，現在のトータルなネットワークセキュリティソリューションの全体像について述べた。

オフィスの業務形態の変化やワークプレイスのユビキタス化が進展している反面，脅威やコンプライアンスへの備えがますます重要となってきている。

日立グループは，今後も，ユビキタスオフィスなど，利用シーンの多様化と高度なネットワークサービスの進展に向けて，安全・安心なネットワークの利用環境を実現するトータルセキュリティソリューションに取り組んでいく考えである。

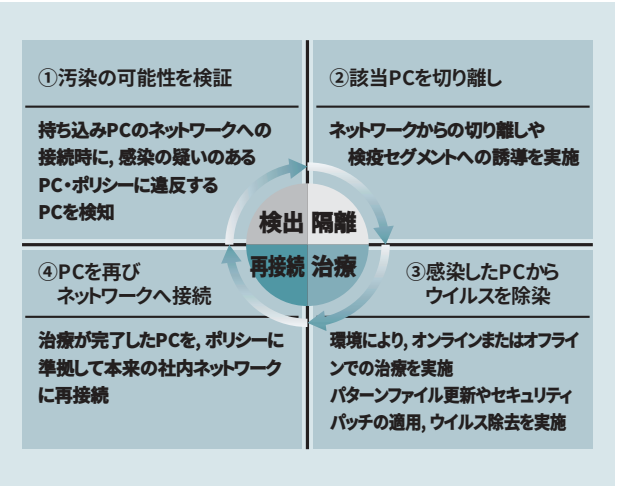


図3　検疫ソリューションのトータルフロー
検知，ネットワーク切り離し，除染，再接続を一貫して行う。

参考文献

1) 小林，外：よくわかる企業セキュリティ入門 事業継続(BCM)とSOX法，日刊工業新聞社(2006.2)
2) 金野：情報セキュリティの動向とトータルセキュリティソリューション，情報処理学会誌(2002.10)
3) 金野，外：セキュアなサービスプラットフォームを実現するセキュリティソリューション" Secureplaza "，日立評論，86，6，437～442(2004.6)
4) TCG(Trusted Computing Group)，https://www.trustedcomputinggroup.org/
5) 日立セキュリティソリューションSecureplaza，http://www.hitachi.co.jp/Secureplaza

執筆者紹介

金野 千里
1977年日立製作所入社，情報・通信グループ セキュリティ事業部 セキュリティソリューション推進本部 セキュリティマーケット開発部 所属
現在，セキュリティソリューションの企画と事業展開に従事
理学博士
日本応用数理学会会員，情報処理学会会員

坏 毅
1997年日立製作所入社，情報・通信グループ セキュリティ事業部 セキュリティソリューション推進本部 セキュリティシステムソリューション部 所属
現在，セキュリティソリューションの開発と事業展開に従事

山田 知明
1993年日立製作所入社，情報・通信グループ セキュリティ事業部 セキュリティソリューション推進本部 セキュリティシステムソリューション部 所属
現在，セキュリティソリューションの開発と事業展開に従事

瀬野尾 修二
1984年日立製作所入社，情報・通信グループ セキュリティ事業部 セキュリティソリューション推進本部 セキュリティシステムソリューション部 所属
現在，セキュリティソリューションの開発と事業展開に従事