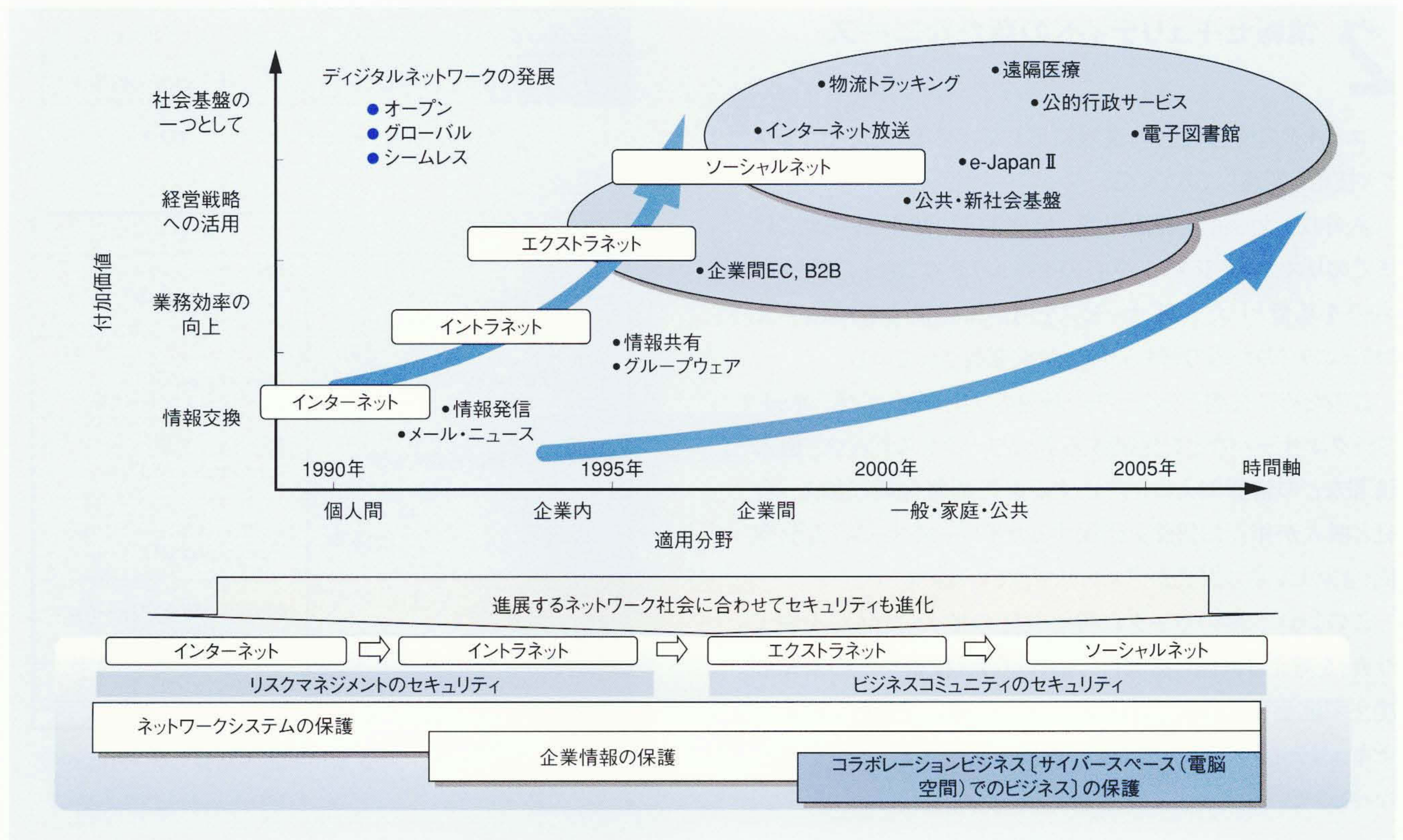


ビジネスと社会におけるセキュリティ維持に貢献する“Secureplaza”

Hitachi's Security Solutions for Safety in Business and Society

中野 利彦 Toshihiko Nakano 森田 光 Akira Morita
山田 知明 Tomoaki Yamada 坪 毅 Takeshi Akutsu



注：略語説明 EC (Electronic Commerce), B2B (Business to Business)

インターネットの進展とセキュリティ技術の進化

デジタルネットワークの発展に応じて必要となる、セキュリティ技術の進展を示す。

デジタルネットワーク技術の普及と進展により、インターネットは、企業や政府、自治体、個人をつなぐソーシャルネットワークとなり、社会基盤の一つとなってきた。このため、情報セキュリティは、信頼性の高い情報ライフラインの基盤として、ますます重要性を増している。

これを受けて日立製作所は、進展するネットワーク社会に対応するセキュリティソリューションとして、

“Secureplaza (セキュアプラザ)”を開発し、提供している。これは、リスクマネジメントとビジネスコミュニティのためのセキュリティという二つの視点から開発したトータルセキュリティソリューションである。このソリューションでは、情報ライフラインの高水準なセキュリティ維持に貢献するために、「システムの広がりに対応したステップ別ソリューション」と、「セキュリティの導入目的に応じた目的別ソリューション」を提案している。

1 はじめに

政府が進めている「e-Japan戦略Ⅱ」などにより、電子政府シ

ステムや、インターネットを活用したビジネス、社会基盤が急速に進展してきており、ユビキタス情報社会が身近なものとなってきている。それに伴い、不正アクセスや情報漏えいなどのリスクが増大し、深刻化している。

具体的には、不正アクセスやウイルスにより、組織の保有財産が脅威にさらされる。また、個人情報など組織内の情報が外部に漏えいすることにより、企業や団体の社会的信用が失墜するおそれがある。

ここでは、ビジネスと社会のセキュリティ基盤を実現するという視点で、情報セキュリティと日立製作所のトータル セキュリティ ソリューション“Secureplaza(セキュアプラザ)”について述べる。

2 情報セキュリティへの新たなニーズ

ユビキタス情報社会の進展に応じて、必要となるセキュリティ技術も変遷してきている。

ネットワークや情報機器保護、情報漏えい防止といったこれまでのリスクマネジメント中心のセキュリティに加え、インターネットを基盤とした各種サービスを円滑に提供する、ビジネスコミュニティのためのセキュリティが重要視されている。

このために必要となるセキュリティのソリューションも、ネットワークやサーバなどを保護するネットワークシステムや、個人情報などの情報漏えいを防止する企業情報保護に加え、会社と個人が相互に信頼を確保するサイバースペース(電脳空間)上のビジネス保護が求められてきている。

このように、ネットワークの利用範囲の拡大に伴い、セキュリティを考える範囲も拡大し、セキュリティ技術やその基準も絶えず進展している。これらの状況を的確に把握し、最適なセキュリティシステムを検討し、構築、運用することが必要となってきた。

3 Secureplazaソリューション

3.1 ソリューション体系

これらのニーズに対応し、日立製作所は、日立グループ関連会社とともにセキュリティ製品やエンジニアリングを統合し、トータル セキュリティ ソリューション“Secureplaza”を提供している。

Secureplazaでは、セキュリティの検討、構築、運用を、(1) ビジネスの経営施策に合わせたセキュリティを検討する「経営策定レベル」と、(2) セキュリティ計画に合致した構築・運用を実現する「構築・運用レベル」の2階層に分けている。さらに、システムやサービスの広がり即したセキュリティ対策を九つのステップで提供する「ステップ別ソリューション」と、顧客が必要としているセキュリティの導入目的に対応した「目的別トータルソリューション」を提案している(図1参照)。

「ステップ別ソリューション」は、セキュリティの検討を始める第一歩となる「セキュリティポリシー策定」から、ネットワークでの

顧客のシステムは?	対 策
ステップ8: 万一の際の金銭的, 対外的な対策	保険
ステップ7: システムの定常的な監査	監査, 教育
ステップ6: 統合的な管理	統合運用管理
ステップ5: サイトを出入りする情報の制御	コンテンツ監視
ステップ4: ネットワークやサーバの監視	不正アクセス監視
ステップ3: 外部からの不特定の相手と交通	認証システム
ステップ2: ネットワークで(秘)データを利用	通信路の暗号化
ステップ1: インターネットに接続	ファイアウォール
ステップ0: 複数でリソースを共有	セキュリティポリシー

(a) 高信頼な情報ライフラインをトータルに支える九つのステップ別ソリューション

目的	ソリューション
セキュリティ状況の総合的診断	診断ソリューション “Secureplaza/HS” 診断サービス
セキュリティシステムの運用委託	アウトソーシング “Secureplaza/HS” アウトソーシングサービス
業務に応じた認証基盤の実現	認証ソリューション “Secureplaza/IM”
サーバのトータルセキュリティの実現	機密情報保全ソリューション “Secureplaza/TZ”
情報漏えい防止の実現	情報漏えい防止ソリューション “Secureplaza/LG”
セキュリティについてのコンサルティング	コンサルティングサービス “Secureplaza/CS”

(b) 導入目的ごとに専門知識、専門組織、製品をパッケージ化した目的別ソリューション

図1 トータル セキュリティ ソリューション“Secureplaza”のソリューション体系

ニーズに合わせたセキュリティソリューションを提供する。

情報利用を進めるうえで必要となる「ファイアウォール」や「通信路の暗号化」、「不正アクセス監視」、「コンテンツ監視」、サイバースペースでのビジネスを保護するうえで不可欠な「個人認証」、「企業認証」、「コンテンツ認証」などの「認証システム」、さらに、規模の拡大に合わせた「統合運用管理」、「監査・教育」、「保険」までを提供するソリューションである。

「目的別トータルソリューション」で提供している目的ごとの個別のソリューションについて、以下に述べる。

3.2 初期診断、アウトソーシングソリューション “Secureplaza/HS”

セキュリティ対策では、一度システムを構築してしまえば安全というわけではなく、セキュリティ情報を収集したり、稼動状況を管理し、最新プログラムへの入れ替えをするなど、日々の運用がきわめて重要である。また、セキュリティのぜい弱性

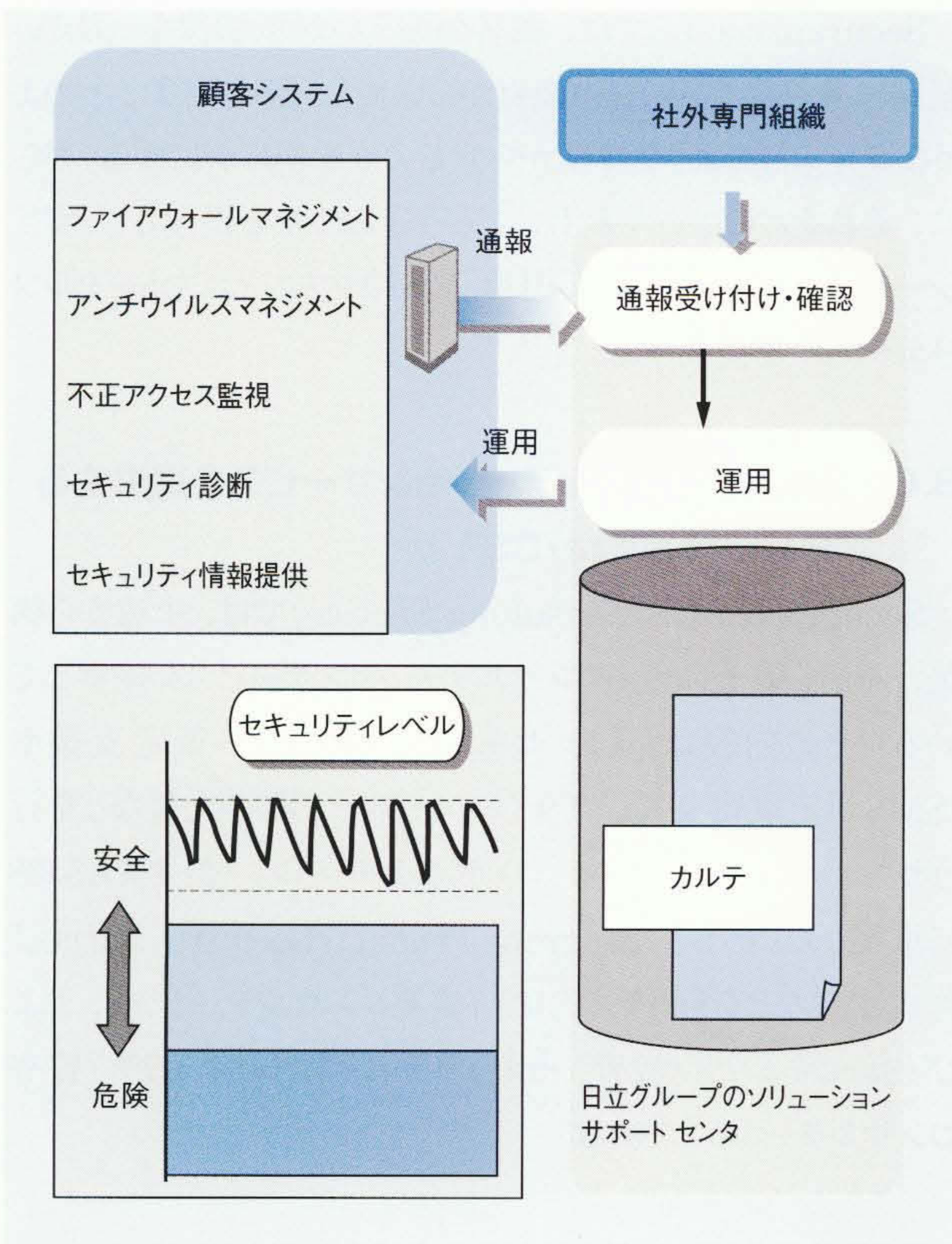


図2 アウトソーシングソリューション

セキュリティシステムの運用を、セキュリティレベル維持とカルテを活用したソリューションで提供する。

が日々報告されていることから、適切な対応を継続的に行う必要があり、運用者の負担はますます増加している。

これらの課題を解決するために、Secureplaza/HS (Healthcare Service)では、診断や導入評価を実施する診断サービスと、各種監視を提供する月次のアウトソーシングサービスを提供している。診断サービスでは、ISMS (Information Security Management System)の管理項目に基づくアセスメントと、各種のセキュリティホール診断を提供する。アウトソーシングサービスでは、継続的な対応を行うために、まずセキュリティヘルスケアカルテを作成し、顧客が利用している機器を把握する。このカルテに基づいて、状況を随時報告し、その対策を提供することで、顧客の運用負担を軽減し、セキュリティ水準の維持を図る(図2参照)。

3.3 真正性保証ソリューション“Secureplaza/IM”

インターネットを利用したサービスの提供や利用を行うためには、相手が確実に本人であることを確認し、正しい内容でのやり取りを保証することが必要である。

このため、ネットワーク上で相手を本人であると確認し、電子的に取り引きされる内容が正しいと証明し、取引時刻や、将来にわたっての真正性を保証することが不可欠である。これらを実現するソリューションが、Secureplaza/IM (Identity Management)である。具体的には、(1) 見えないネットワーク上の個人を証明するための「認証基盤構築ソリューション」、

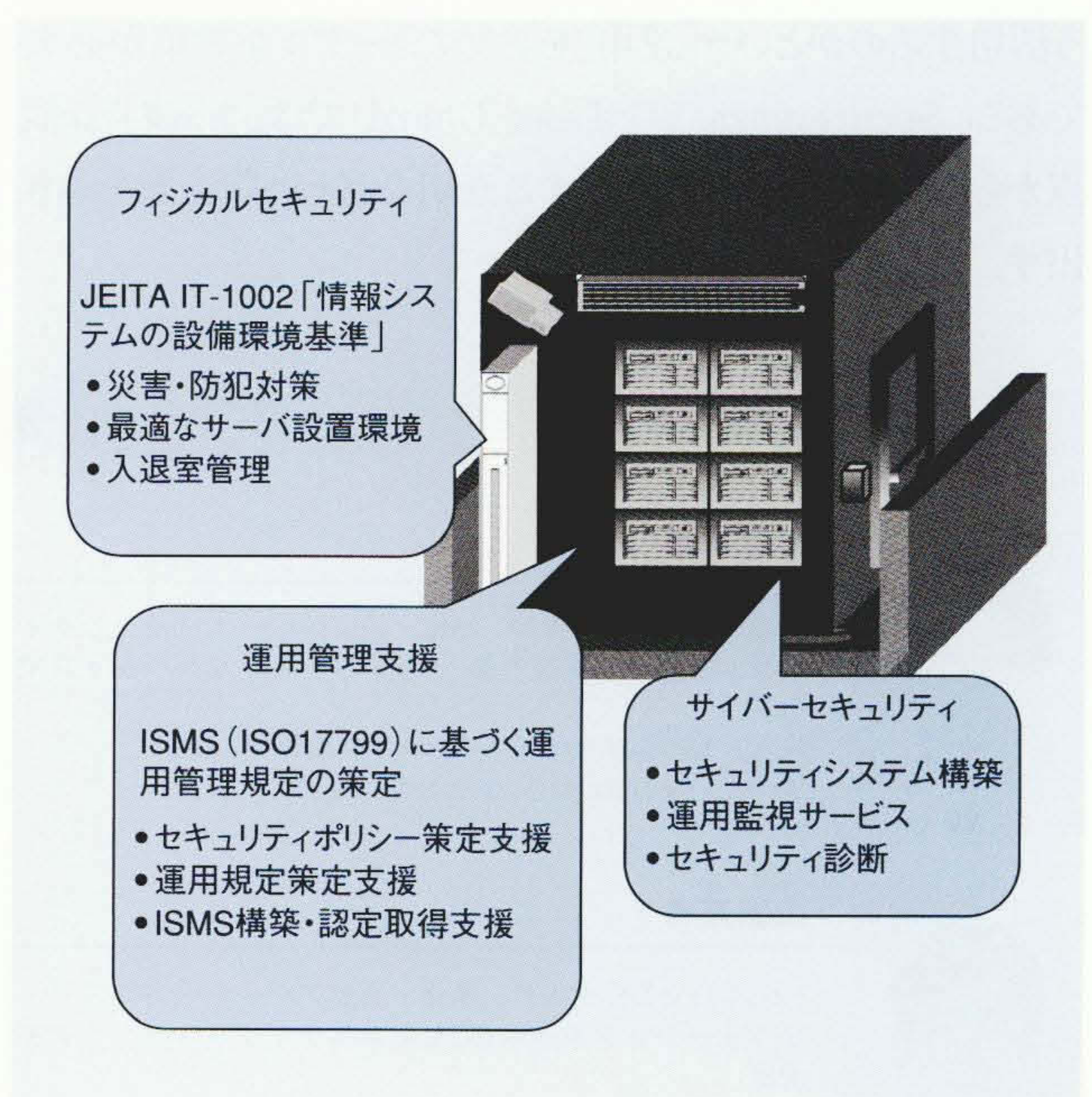
(2) 実印が必要な電子取引の基盤を実現する「署名法対応・GPKI (Government Public Key Infrastructure) 相互認証サービス」、(3) 取り交わされる電子的なデータの時刻を証明する「電子署名・タイムスタンプシステム」、および(4) 電子文書の真正性を長期に証明することができる「ヒステリシス署名システム」を提供している。

3.4 機密情報保全ソリューション “Secureplaza/TZ”

巧妙化する外部攻撃、内部犯罪、自然災害、テロ行為の増加など、多様化する脅威に対して、これまでのような個別かつ一面的なセキュリティ対策では、企業の機密情報や重要なサーバのセキュリティを維持することはきわめて困難になってきている。

Secureplaza/TZ (Trusted Zone)では、ISMS (Information Security Management System)の管理項目に基づき、フィジカル(物理的)セキュリティ、サイバーセキュリティ、および運用管理支援を含むトータルなセキュリティ環境を提供し、迅速・安価に、顧客サイトにセキュアなサーバの設置環境を構築できるようにする(図3参照)。

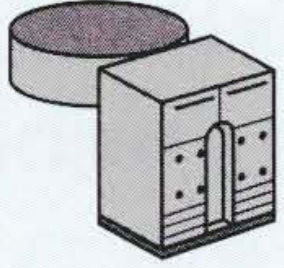
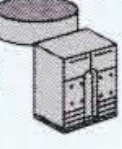
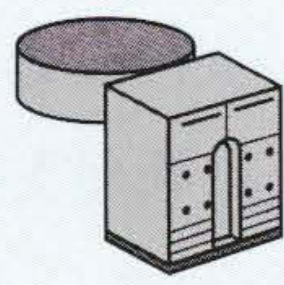
フィジカルセキュリティでは、セキュリティルームとしてセコム株式会社の「セコム情報金庫」を利用し、顧客サイトにiDC (Internet Data Center)レベルの堅ろうな物理スペースを構築する。サイバーセキュリティでは、Secureplazaのソリューションメニューから、顧客の要件に合わせた適切な対策を提供するほか、ディザスタリカバリ(災害復旧)を実現するオフサイトバックアップサービスも提供する。



注：略語説明 JEITA(社団法人電子情報技術産業協会)

図3 機密情報保全ソリューション

サーバを安全に管理するために必要となるフィジカル面、サイバースペース面、および運用管理面をトータルにサポートする。

Who (だれが)	Why (なぜ)	How (どのように)	Where/When (どこで、いつ)	What (何を)
社内派遣者	故意	●不正アクセスのぞき見 盗聴 成り済まし	基幹系システム 	非公開文書 (ファイル)
	認定ミス	●不正侵入 ●盗難	社内LAN 	持ち出し メディア
	パッチ不良 (ホール)	●不正コピー	オフィス ファイルサーバ 	廃棄 メディア
	ポリシー違反	●媒体への不正出力	一般社員 	メール
社外	不注意	●不正持ち出し ●紛失 ●天災	社外公開用サーバ 	持ち出し パソコン 廃棄 パソコン

注：略語説明 LAN(Local Area Network)
図4 情報漏えいの経路
情報漏えい防止のために、5W1Hで漏えい経路を分析する。

3.5 情報漏えい防止ソリューション
“Secureplaza/LG”

個人情報保護法の制定などを契機として、企業からの情報漏えい、特に顧客の個人情報流出をどう防ぐかということが大きな関心を集めている。このような情報漏えいを防止するためには、「ツール(道具)」の導入だけではなく、何を漏えいから守るのかという「ポリシー(方針)」と、ツールをどう活用するのかという「運用」を含めたトータルな対策が必要である。Secureplaza/LG(Leak Guard)では、トータルな観点から、顧客のニーズに合致する適切な漏えい防止策を導き出す。

Secureplaza/LGでは、顧客の漏えい対策状況を、漏えい経路に着目して5W1Hの観点から診断し(図4参照)、どのような資産をどのような脅威から守るのかを明らかにする。さらに、それをどのツールを用いてどう守るのかを提示し、「ポリシー」、「ツール」、および「運用」のバランスのとれたトータルソリューションを提供する。

3.6 3体系のコンサルティングサービスを提供する
“Secureplaza/CS”

Secureplaza/CS(Consulting Service)では、上流から構築、運用、監査に至るコンサルティングサービスを提供している。その内容は、(1) セキュリティポリシー策定支援やISMS認定取得支援、プライバシーマーク取得支援などを行うセキュリティ マネジメント コンサルテーション、(2) ISO15408に準拠したPP/ST(Program Product/Security Target)作成支援などを行うセキュリティ構築コンサルティング、および(3) セキュリティ教育、セキュリティ診断、セキュリティ監査コンサルティングである。

4 おわりに

ここでは、情報セキュリティを維持するためのさまざまな対策を支援する、日立製作所のトータル セキュリティ ソリューション“Secureplaza”について述べた。
ネットワークの利用範囲の広がりとともにセキュリティの範囲も拡大し、セキュリティ技術やその基準も変化している。このような状況を把握したうえで、最適なセキュリティシステムを検討し、構築、運用することが求められている。
日立製作所は、今後も、ビジネスと社会のためにセキュリティソリューションを提案していく考えである。

執筆者紹介



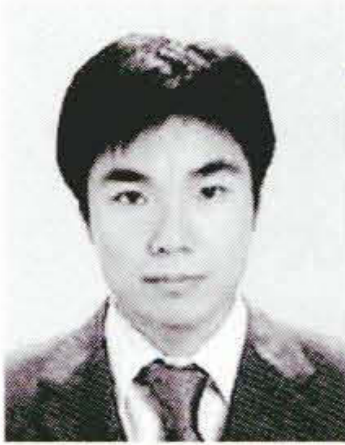
中野利彦
1980年日立製作所入社、情報・通信グループ セキュリティソリューション推進本部 セキュリティソリューション室所属
現在、セキュリティソリューションの開発に従事
E-mail : tos-nakano @ itg. hitachi. co. jp



山田知明
1993年日立製作所入社、情報・通信グループ セキュリティソリューション推進本部 セキュリティソリューション室所属
現在、セキュリティソリューションの開発に従事
E-mail : tyamada @ itg. hitachi. co. jp



森田 光
1996年日立製作所入社、情報・通信グループ セキュリティソリューション推進本部 セキュリティソリューション室所属
現在、セキュリティソリューションの開発に従事
E-mail : amorita @ itg. hitachi. co. jp



坪 毅
1997年日立製作所入社、情報・通信グループ セキュリティソリューション推進本部 セキュリティソリューション室所属
現在、セキュリティソリューションの開発に従事
E-mail : takutsu @ itg. hitachi. co. jp