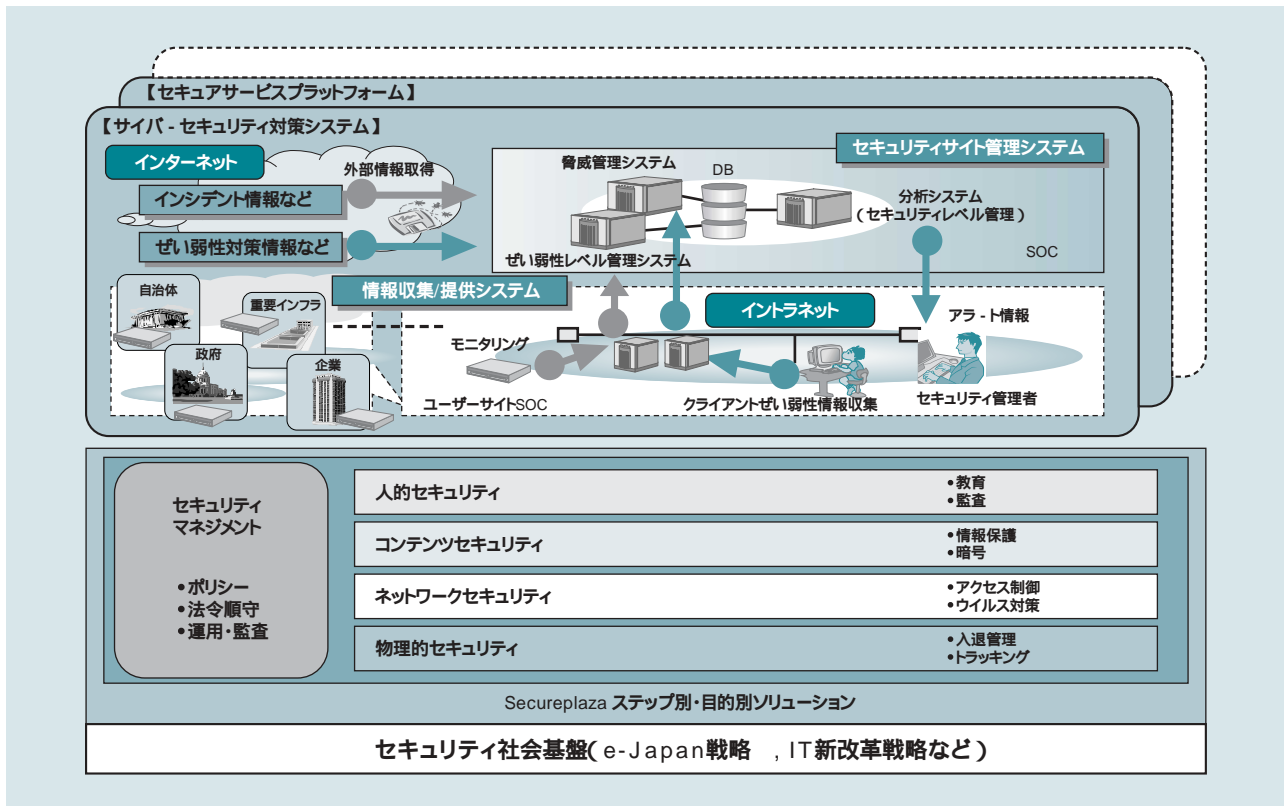


重要な情報を守る日立セキュリティソリューション 「Secureplaza」

Hitachi's Total Security Solution for Protecting Important Information

二本松 勝 Masaru Nihonmatsu
金野 千里 Chisato Konno

瀬野尾 修二 Shūji Senoo
洲崎 誠一 Seiichi Susaki



注:略語説明 DB(Database),SOC(Security Operation Center)

図1 日立的取り組みをセキュリティソリューションとそれを支える「Secureplaza」

「重要な情報を守るため、日立グループは「Secureplaza」コンソーシアムを結成し、情報セキュリティにかかわる多くの製品・サービスを準備し、あらゆるセキュリティソリューションに対応している。

1.はじめに

近年、ITの爆発的な普及に伴い、いっそうの利便性、効率性が求められているが、一方でマイナスの面も指摘されるようになってきた。新聞紙上を頻りに騒がせている情報漏えい問題やサイバーテロも身近な問題としてとらえられてきており、ITに関するセキュリティ、あるいはITを用いたセキュリティはますます重要性を増している。ITはもはや単なるツールではなく、人命から国の存続までを左右するものとなり、政府からマスコミまで「情報セキュリティ」を大きな課題として取り上げている。

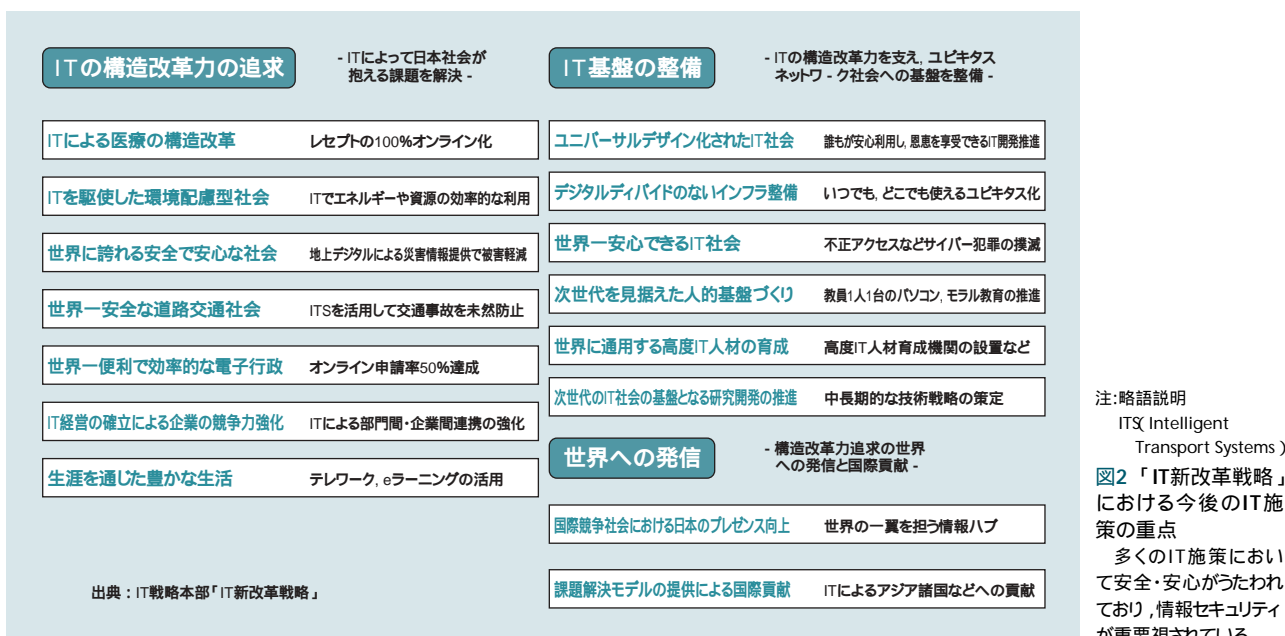
ここでは、情報セキュリティに関する国の施策、日立グループの取り組みと「トータルセキュリティソリューション」Secureplaza(セキュアプラザ)について述べる(図1参照)。

2.情報セキュリティについての国家施策

「e-Japan戦略」でも、すでに情報セキュリティの重要性は強調されていたが、2006年1月に出された「IT新改革戦略」では、アプリケーション面での「IT構造改革力の追求」と基盤面での「IT基盤の整備」において、直接、間接を含め多くのセキュリティに関するガイドラインが示されている(図2参照)。また、ほぼ同時期に、セキュリティに絞り込んだ施策として、IT戦略本部情報セキュリティ政策会議から「第1次情報セキュリティ基本計画」、内閣官房情報セキュリティセンター(NISC)から「政府機関の情報セキュリティ対策のための統一基準(2005年12月版(全体版初版))」、および「重要インフラの情報セキュリティ対策に係る行動計画」が打ち出されている。こ

2003年7月にIT戦略本部から発表された「e-Japan戦略」でも情報セキュリティの重要性は打ち出されていたが、2006年1月の「IT新改革戦略」では、各種IT施策の中でもセキュリティの比重がさらに増大している。また、ほぼ同時期に出された情報セキュリティ政策会議の「第1次情報セキュリティ基本計画」などではきたるべき時代の情報セキュリティのあり方をうたっている。

このような中、日立グループは、IT基盤や顧客の情報システムなどに関わる情報セキュリティに積極的に取り組み、顧客の重要な経営資産を守るためのトータルなセキュリティソリューション「Secureplaza」を強化し、拡充を図っていく。



の背景には、米国同時多発テロから大きく変わった世界情勢や天災・人災による重要インフラ障害、また不祥事や情報漏えいなどを防止するための組織の内部統制・IT統制の必要性が増大したという面があることも考えられる。きたるべき日本の将来に対し、特に情報セキュリティが重要な要素であることを意味するものである。

これらのガイドラインでは、政府・自治体、重要インフラ事業者、一般の会社組織などに、ある程度の期限を設けてセキュリティについての施策や対策をとるように具体的な提言がなされている。それは「第1次情報セキュリティ基本計画」で述べている「情報セキュリティ先進国」となり、世界をリードすることを目指そうとするものである。

日立グループは、これらのガイドラインを具体化し、実現していくために、保有する技術・サービスを駆使して貢献していく考えである。

3. 情報セキュリティについての取り組み

日立グループは、情報セキュリティへの取り組み方針として、IT基盤と重要インフラを構成する領域での対応を重視し、

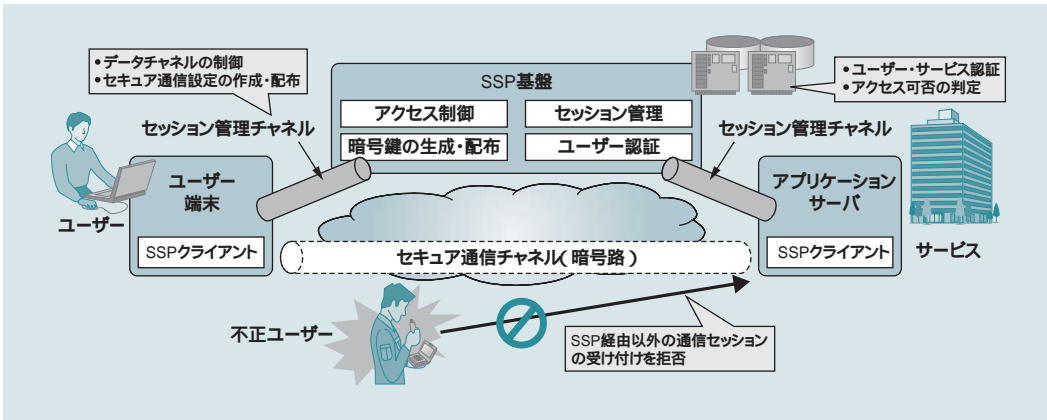
国・自治体(電子政府・電子自治体)や重要インフラ(電力、交通、通信、金融など)には、セキュリティ共通基盤(暗号、電子署名、PKI(Public Key Infrastructure)など)を用い、関係業界と連携して、技術開発・サービス提供を行っている。e-Japan戦略なども勘案した主なソリューションは以下のとおりである。

(1) サイバーセキュリティ対策システム

総務省および情報通信研究機構(NICT:National Institute of Information and Communications Technology)対応の国家プロジェクトなどへの参画を基に、インターネットでの広域的な情報収集手法と、イントラネットでの独自の解析ノウハウを研究し、総合的な判断情報を提供するSOC(Security Operation Center)連携システムを実現する。LAN(Local Area Network)を対象としたイベントやインシデント管理により、ネットワークセキュリティ確保策を管理者に提供できることが特長である。

(2) セキュアサービスプラットフォーム

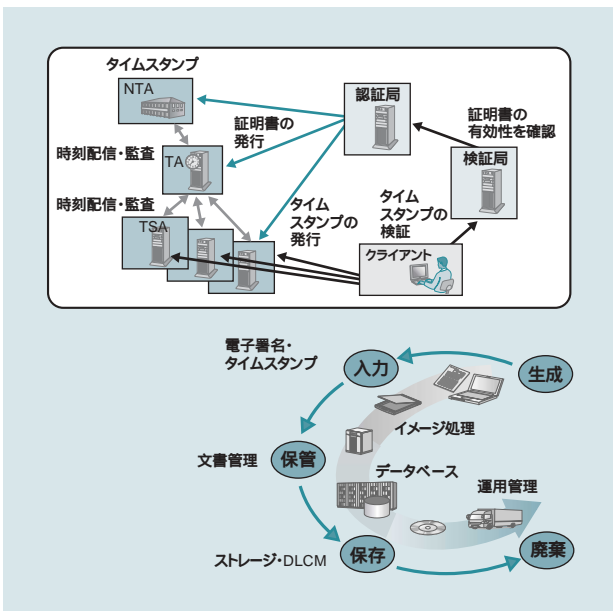
第三者認証をコアとするセキュアな通信サービスプラットフォーム環境(認証・VPN(Virtual Private Network)・アクセス制御システム)を提供し、ネットワークインフラのレベルで、セキュリティ機能や一元管理された通信の運用管理環境を実



注:略語説明

SSP(Secure Service Platform)

図3 セキュアサービスプラットフォーム
第三者認証を核とするセキュアな通信サービスプラットフォーム環境を提供する。



注:略語説明 NTA(National Time Authority), TA(Time Authority)
TSA(Time Stamp Authority)
DLCM(Data Life Cycle Management)

図4 タイムスタンプとそれを活用したe文書ソリューション
長期間有効なタイムスタンプを活用し、長期保存や改ざん防止を実現するe文書ソリューションを提供する。

現する。従来は、システム個々にセキュリティ対策を行っていたことを一元化することにより、作業が大幅に軽減できることが特長である(図3参照)。

(3) 時刻認証基盤(タイムスタンプ)およびe文書ソリューション

これまでより安全な鍵長(暗号化の際に用いられるビット列である「鍵」のけた数)で高負荷時にも十分な処理能力を持つタイムスタンプ技術を開発し、長期間有効なタイムスタンプを実現した。これにより、日本標準時を利用して正確かつセキュリティの高いタイムスタンプを付与するとともに、このタイムスタンプを活用し、文書の生成から廃棄に至るまでのライフサイクル管理を実現するe文書ソリューションが構築できる。長期保存や改ざん防止・非改ざん証明など各種セキュリティ対策を施すと同時に、業務分析を行い、電子化されない文書を含めた文書管理経費の削減やBPR(Business Process Reengineering)による業務効率化を実現する(図4参照)。

(4) 監査・認定

ISO15408「情報技術セキュリティ評価基準」などにに基づき、セキュリティポリシー策定や、セキュリティ監査、ISMS(Information Security Management System)取得を支援する。

4 .日立セキュリティソリューション「Secureplaza」

Secureplazaは、「ステップ別ソリューション」と「目的別ソリューション」の二つのソリューション体系に大別できる。それらを構成するツールは、日立グループの製品群の中から要件に適したものを選択する体系としている。

4.1 ステップ別ソリューション

Secureplazaのステップ別ソリューションは、あらゆる規模をカバーするセキュリティシステムを九つのステップに分類し、その実現をサポートするものである(図5参照)。

顧客のシステムは?	対策	典型的な顧客層
Step8 : 万一の際の金銭的、対外的な対策が必要なら...	保険	大規模インターネット 商取引システム 中規模インターネット
Step7 : システムの定期的な監査が必要なら...	監査・教育	
Step6 : 大規模システムで、統合的な管理が必要なら...	統合運用管理	
Step5 : サイトを出入りする情報の制御なら...	コンテンツ監視	
Step4 : ネットワークやサーバの監視が必要なら...	不正アクセス監視	
Step3 : 外部からの不特定の相手と交信するなら...	認証システム	
Step2 : ネットワークで(秘)データなどをやり取りするなら...	VPN	
Step1 : インターネットに接続しているなら...	ファイアウォール	
Step0 : 複数でリソースを共有しているなら...	セキュリティポリシー	

注:略語説明 VPN(Virtual Private Network)

図5 「Secureplaza」ステップ別ソリューション
高度な情報セキュリティシステムを九つのステップでトータルに支えていく。

セキュリティマネジメントへの第一歩 Secureplaza/CS(Consultation Service)	セキュリティポリシー・策定やISMS認証取得などを、経営策定の観点から支援する。
セキュリティレベルの維持・把握を行う。 Secureplaza/HS(Healthcare Service)	時間とともに低下しがちなセキュリティレベルを、定期的な診断・検査により、目標レベルに保つ。
組織全体をウイルス感染から守る。 Secureplaza/PB(Pollution Block)	ウイルス感染から組織を守るため、組織形態に最適な感染予防策などをトータルに支援する。
内部からの情報の持ち出しを防ぐ。 Secureplaza/LG(Leak Guard)	情報漏えいのさまざまな可能性を検証・診断し、適切なツール導入や監視により、リスクを解消する。
企業活動記録の保全を対策する。 Secureplaza/FS(Forensic Solution)	企業の活動記録を保全、収集し、監査対応や事件・事故の際の証拠保全の対応を支援する。
外部アクセスから情報資産を守る。 Secureplaza/US(Ubiquitous Access Security)	さまざまなユビキタスアクセスの形態に、多様なレベルの認証、通信路保護、情報保護を実現する。
情報や利用者の正当性を判別・保証する。 Secureplaza/IM(Identity Management)	ネット取引などの安全性を確保するため、PKIなど最新技術を駆使した仕組みを提供する。
外部からの脅威に備える。 Secureplaza/TZ(Trusted Zone)	堅ろうな物理セキュリティと情報セキュリティの提供により、物理的脅威とネット上の脅威、双方に備える。

注:略語説明 ISMS(Information Security Management System)
PKI(Public Key Infrastructure)

図6 「Secureplaza」目的別ソリューション

顧客の脅威対応、法制度対応の目的に合わせ、日立独自の技術や製品を用いて付加価値を提供する。

4.2 目的別ソリューション

Secureplazaの目的別ソリューションは、セキュリティ対策の目的や課題に対応してパッケージ化したもので、オフィスなどでのあらゆる情報リスクを全方位からカバーするものである。各ソリューションは、診断やコンサルテーション、ポリシー策定、システム構築、運用管理までをメニューとしている。現在、ニーズの高い八つのソリューションを、図6に示す。

日立は、Secureplazaにより、多くのオフィスやサイトで抱えているセキュリティに関する課題やインターネットサービスに伴う各種問題に対応し、目的別ソリューションをそろえ、トータルなセキュリティソリューションとしていっそうの充実を図っていく。

5. おわりに

ここでは、重要性を増した情報セキュリティについての最近の国家施策、また日立的取り組みと、そのベースとなるトータ

ルなセキュリティソリューション「Secureplaza」について述べた。

日立グループは、従来からセキュアな情報基盤と重要インフラに取り組んできたが、今後も国家的な視野に立ち、ますます求められる情報やそれに伴うサービスの安全性に対応し、さまざまな情報セキュリティソリューションを充実していくとともに、フィジカルセキュリティや生体認証などと組み合わせ、いっそう幅広い分野でのセキュリティソリューションの提供を目指す考えである。

参考文献など

- 1) 高度情報通信ネットワーク社会推進戦略本部(IT戦略本部),
<http://www.kantei.go.jp/jip/singi/it2/>
- 2) 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



二本松 勝

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
E-mail:masaru.nihommatsu.sq@hitachi.com



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
情報処理学会会員、日本応用数理学会会員
E-mail:chisato.konno.hy@hitachi.com



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・開発と事業展開に従事
E-mail:shuji.senoo.uz@hitachi.com



洲崎 誠一

1991年日立製作所入社、システム開発研究所 第七部 所属
現在、サイバー攻撃対策技術の研究開発に従事
工学博士
情報処理学会会員
E-mail:susaki@sdl.hitachi.co.jp