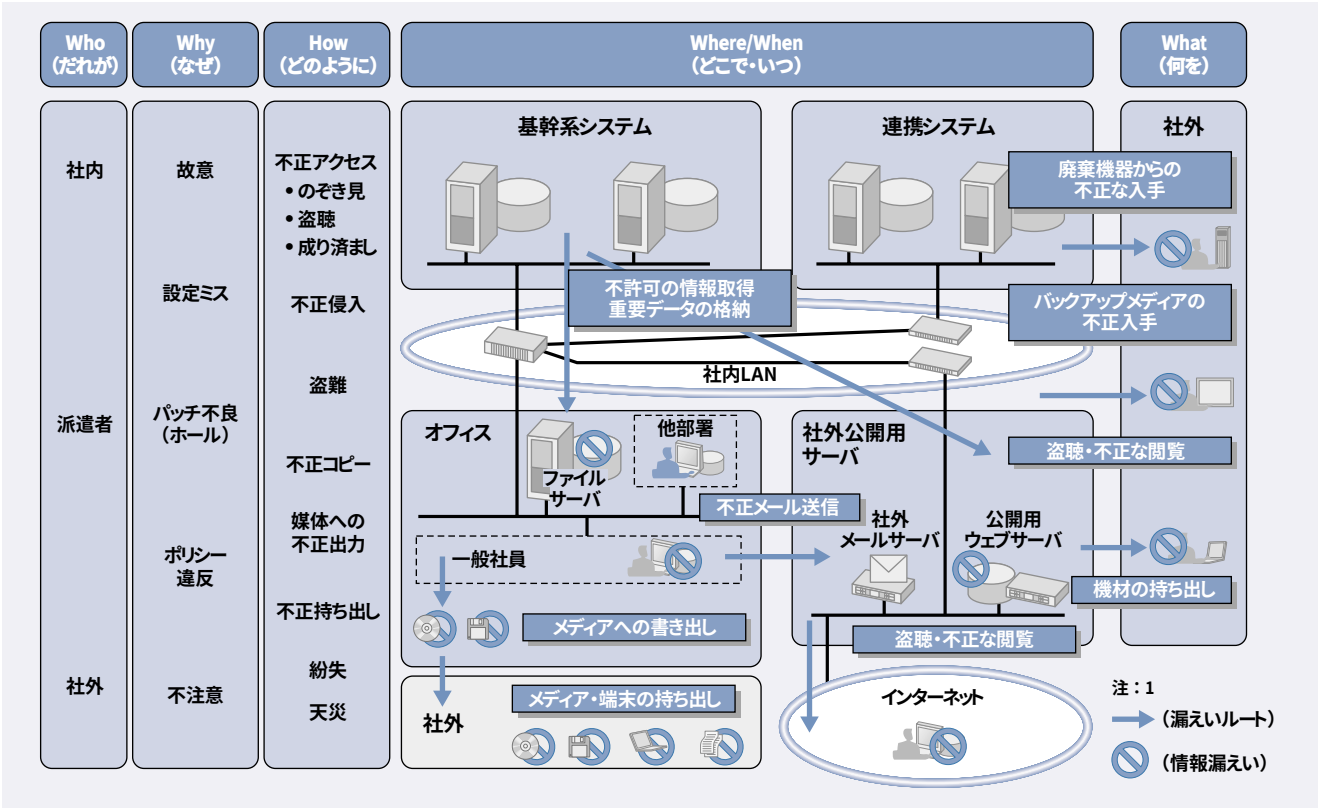
セキュアなサービスプラットフォームを実現するセキュリティソリューション“Secureplaza”

Hitachi's Total Security Solution for Establishing Reliable Service Platforms

金野千里 Chisato Konno　本多義則 Yoshinori Honda
二本松勝 Masaru Nihonmatsu　長谷川大造 Daizô Hasegawa



注2：略語説明　LAN（Local Area Network）

企業システムでの情報漏えいリスクの概要

システム内から情報が漏えいするルートとリスクの全体像（5W1H）を示す。業務の流れにおける情報漏えいリスクの明確化と対策が，Secureplazaの目的別ソリューションの一つである「情報漏えい防止ソリューション」である。

ブロードバンドの普及や，インターネットを利用した新たなサービスの急速な広がりに伴い，ウイルス感染，不正アクセス，情報漏えい，詐欺行為などのリスクは深刻度を増している。日立製作所は，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考え，それに対応するセキュリティソリューションを提案している。

“Secureplaza”は，サービス プラットフォーム コンセプトHarmonious Computingの信頼性を支える重要な構成要素の一つであり，セキュリティポリシー策定，ファイアウォール，VPN，認証，不正アクセス監視，コンテンツ監視，運用管理，監査・教育，保険など統合管理ができるトータル セキュリティ ソリューションである。さらに，情報漏えい防止，ウイルスによる汚染防止など，目的や火急の課題に沿ったソリューションもそろえている。

1 はじめに

高速なネットワークの普及や新たなサービスの急速な広がりとともに，増大するリスクは大きな脅威となってきている。インターネットでは，組織の保有情報資産が脅威にさらされ，被害者となるリスクだけではなく，踏み台として使われ，他サイトへの攻撃や，情報の漏えいによって他者に多大な迷惑をか

けるなど，加害者となるリスクも併せ持っており，サービスの停止や組織の信頼の失墜など，組織活動に多大な影響を与えかねない状況になっている。

ここでは，このようなリスクに対する，日立製作所のトータルセキュリティソリューション“Secureplaza（セキュアプラザ）”と，高度なインターネット社会の推進をけん引する「e-Japan戦略II」の動向，および先行的なセキュアシステム構築への取り組みについて述べる。

2 トータル セキュリティ ソリューション “Secureplaza”[1)]

Secureplazaには，セキュリティ対策についてのさまざまな要求にこたえるため，大別して二つのソリューションの体系がある。ソリューションを構成するツールは，日立グループの商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。

Secureplazaでは，サービス プラットフォーム コンセプト Harmonious Computingの上に構築されるアプリケーションシステムやサービスにおいて，各セキュリティソリューションがコンポーネントとして活用される。

2.1 ステップ別ソリューション[2)]

Secureplazaのステップ別ソリューションは，システムやサービスの広がりに即して考慮していくべきセキュリティ対策を，九つのステップに大別してそろえている（**図1**参照）。

2.2 目的別ソリューション

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が，Secureplazaの目的別ソリューションである。各ソリューションは，診断やコンサルテーション，システム構築，運用管理までをメニューとしている。現在，ニーズの高い六つのソリューションは以下のとおりである。

（1）コンサルテーションサービス“Secureplaza/CS”

Secureplaza/CSでは，セキュリティを実現する各種コンサルテーションをそろえている。セキュリティレベルやホール（不良）の診断から，セキュリティポリシーの策定，運用管理基準であるISMS（Information Security Management System）の構築と認証取得，監査までをメニュー化している。さらに，セキュリティの技術基準であるISO15408準拠のセキュアシステム構築，個人情報保護法への対応など，幅広いコンサルティングメニューを提供している。

（2）ヘルスケアサービス“Secureplaza/HS”

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，一定のセキュリティレベルに維持するのがヘルスケアサービスである。“Secureplaza/HS”では，診断やセキュリティコンサルテーションから成る初期サービスと，定常的なセキュリティ維持を実現する運用，監査，分析から成る基本サービスを提供している。

（3）アイデンティティマネジメント“Secureplaza/IM”

“Secureplaza/IM”は，PKI（Public Key Infrastructure：公開かぎ基盤）をベースとした認証基盤システムの構築をはじめ，ディレクトリサーバおよびシングルサインオンとの連携によるセキュア イントラネット システム構築を実現する。また，認証局の用途や目的に合わせて，署名法対応・GPKI（Government PKI：政府認証基盤）相互認証対応の認証局構築にも対応している。さらに，認証局の上に高付加価値なサービスシステムを実現するために必要となる，電子署名・タイムスタンプ，長期原本性保証，属性認証など，最先端のPKIソリューションをそろえている。

（4）トラステッドゾーン“Secureplaza/TZ”

情報セキュリティでは，システム自体への対策だけでなく，そのシステムを覆う建設物やマシン室への入退室なども重要となる。しかし，サイトによっては，建物の改造や補強が困難なケースも多々存在する。Secureplaza/TZは，既存の建築

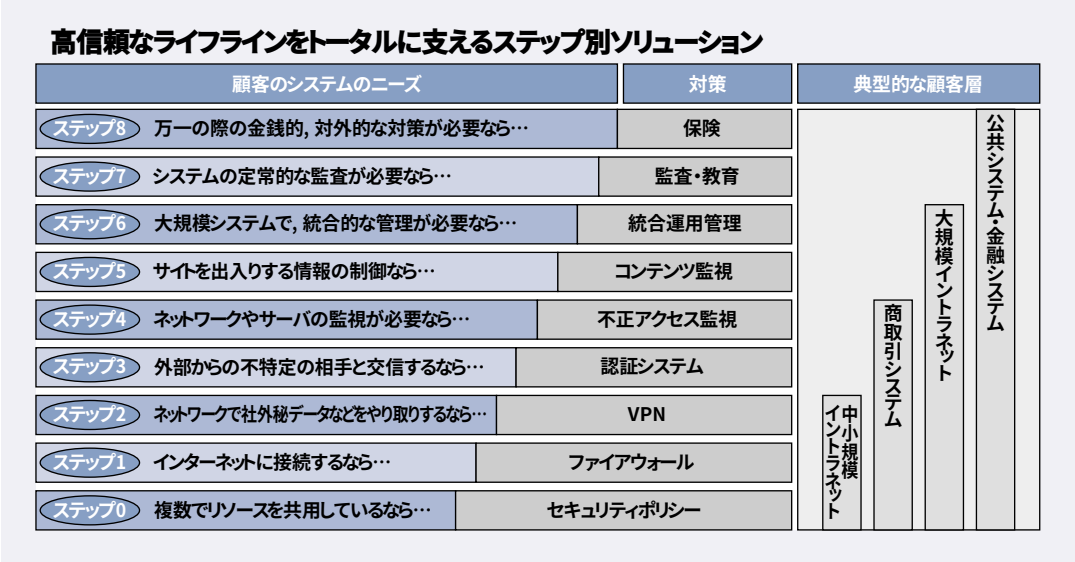


図1 Secureplazaのステップ別ソリューションの概要

システムやサービスの広がりに即して考慮すべきセキュリティ対策をそろえたSecureplazaのステップ別の対策を示す。

注：略語説明
VPN（Virtual Private Network）

物の中にセキュリティ強度の高いエリアを情報金庫として構築する機密情報保全ソリューションである。個人情報データなど，情報資産の中でも特に機密性の高いものを，災害や盗難といった脅威から，物理・サイバー両面でセキュリティを実現する。さらに，運用管理ポリシーを併せて提供することにより，この情報金庫内を対象としたISMSの評価認定取得も支援する。

(5) リークガード“Secureplaza/LG”

情報漏えいのリスクが高まっており，また，個人情報保護基本法を含めた対応は，組織にとって重要な課題となっている。Secureplaza/LGは，情報漏えいのさまざまな可能性を業務の流れに照らして検証，診断し，「いつ・どこで・だれが・何を・何の目的で・どのように」の5W1Hの考え方により，漏えいのリスクをトータルに分析し，分析結果に基づいた対策を提案するソリューションであり，以下のメニューから成る(45ページの図参照)。

(a) リスク分析と業務改善提案
(b) 情報管理ポリシーの策定
(c) 幅広いツール群の中から最適な対策の計画，構築
(d) 運用監視，監査

(6) ポリューションブロッグ“Secureplaza/PB”

2003年に発生したBlasterウイルスをはじめ，セキュリティホールを突いた新種の出現や高い感染力による急速なまん延など，ウイルスは，これまでにない大きな脅威となってきている。ウイルス対策ソフトウェアやファイアウォールを取り入れていても，システムやネットワークにはさまざまな感染経路や媒体が存在しているため，最近では，感染したパソコンの社内への持ち込みによる被害も多発している(**図2**参照)。

業務形態や業務の流れとシステムおよびネットワーク構成を分析し，それぞれのサイトにおける感染リスクの明確化が重要である。また，(a) 既知ウイルス，(b) 未知ウイルス，(c) 不正パソコン接続，(d) 感染パソコン接続，(e) 感染後の局所化や外部への排出抑止，(f) 感染後の復旧など，それぞれへの対策では，さまざまなレベルが考えられる。

汚染防止ソリューションSecureplaza/PBでは，感染リスクの評価やコンサルティングから，ネットワーク設計・構築，インシデント情報提供，診断，監査，被害時の復旧までトータルなソリューションをそろえている。

日立製作所は，多くのサイトが抱えている課題や新しいインターネットサービスへの要求にこたえるために，目的別ソリューションをそろえ，トータル セキュリティ ソリューションの充実を図り，Harmonious Computingの信頼性を確保している。

3 e-Japan戦略IIと日立製作所の取り組み

3.1 e-Japan戦略IIとセキュリティ

「e-Japan戦略Ⅱ」は，2003年7月に，内閣総理大臣を本部長とする「高度情報通信ネットワーク社会推進戦略本部」(略称：IT戦略本部)から打ち出された。主旨は，ITの利活用による，「元気・安心・感動・便利」社会の実現を目指してというものであり，21世紀を迎え，きたるべきわが国の姿を描こうとするものである[3]。

そこには，「医療」，「食」，「生活」，「中小企業金融」，「知」，「就労・労働」，「行政サービス」といった国民にとって身近で重要な七つの分野における先導的取り組みが示されており，特筆すべきは，従来にも増してセキュリティに重きが置かれていることである。それにのっとって2003年10月には，経済産業省によって「情報セキュリティ総合戦略」[4]がまとめられ，世界最高水準の「高信頼性社会」の実現による，経済・文化国家としてのわが国の競争力の強化と総合的な安全保障の向

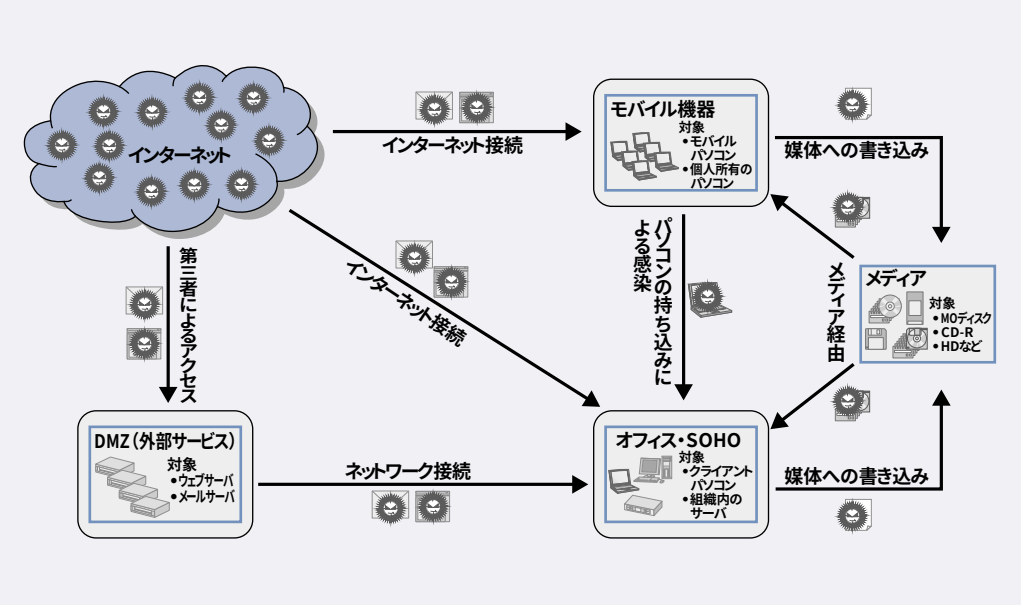


図2 ウイルス感染経路と感染形態の全体像

組織システム内の防御対象に対する感染経路と感染リスクの全体像を示す。

注1：
(メール送受信)
(ホームページ閲覧，ダウンロード，アップロード)
(各種メディアへの書き込み)
(ノートパソコン経由)
(各種メディアの使用)
(防御対象)
(ウイルス感染経路)

注2：略語説明
DMZ(Demilitarized Zone)
SOHO(Small Office, Home Office)

表1「情報セキュリティ総合戦略」の主な項目
しなやかな「事故前提社会システム」の構築や「高信頼性」を強みとするための公的対応の強化が述べられている。

1．事前予防策の強化
●国，自治体の情報管理体制の見直しとそれに伴った技術開発およびシステム構築
●重要インフラストラクチャーの情報セキュリティ監査の実施，サイバーテロ対策技術開発
●ぜい弱性への対処のためのルールと体制の整備，コンピュータウイルスなどの警戒情報提供
●暗号の安全性評価の強化，暗号・認証技術を用いた安全な情報流通体制の確立
●情報セキュリティ監査の実施やISMS認証取得の促進，情報セキュリティ格付け検討
●安全性向上に向けた技術・製品・サービスの開発ほか
2．事故対応策の抜本的強化
●国・自治体における情報共有・活用体制の見直し
●重要インフラストラクチャーにおける情報共有・活用体制の設置
●IT事業者間における情報共有・活用・協力体制の設置
●サービス継続・復旧計画の策定ガイドラインの整備ほか
3．全体を支える基盤の強化
●情報収集・解析機能の整備
●一極集中・依存リスクを回避したIT基盤の形成
●ソフトウェア製造技術の高度化，セキュアプログラミング手法の確立と実用化ほか

注：略語説明　ISMS（Information Security Management System）

上がうたわれている（表1参照）。

e-Japan戦略Ⅱの「情報セキュリティ総合戦略」は，国家全体の総合的な安全保障向上という観点からスタートし，すべての製品，サービスにセキュリティを作り込むというスタイルで進んでいくと考えられる。

3.2　日立製作所としての取り組み

日立製作所は，わが国の政府から大きな指針が出た中で，これまで取り組んできた電力，交通，通信，金融などの重要インフラストラクチャーや電子政府も視野に入れ，ITにかかわるセキュリティ全般に積極的に取り組み，その成果をセキュリティソリューション体系Secureplazaの新しい先行的なソリューションとして加えていく考えである。

e-Japan戦略IIの「情報セキュリティ総合戦略」に対応する日立製作所のセキュリティシステムは，「イベント・インシデント管理ソリューション」であり，ソリューション基盤・フレームワークとしては，「セキュア サービス プラットフォーム（SSP）」，「文書電子化（ペーパーレス）ソリューション」，および「認証基盤ソリューション」があげられる。また，システム運用としては，「監査・認定制度ソリューション」がある（図3参照）。

さらに，Harmonious Computing上で構築される今後のアプリケーションシステムやサービスにも，この戦略への対応を取り込んでいく予定である。

e-Japan戦略IIに対応する具体的なソリューションの一つである「文書電子化」について以下に述べる。

4　文書電子化ソリューション

文書電子化（ペーパーレス）ソリューションは，紙文書と電子文書のライフサイクルを通じてデータの原本性を確保することを目的とし，官公庁・自治体，金融，医療，製造，流通など各分野での利用が想定されている。

このソリューションは，紙文書の真正性を保ちつつイメージデータへの変換を行う「電子化プロセスソリューション」，電子文書の原本性を保証しつつ長期保存を実現する「セキュアアーカイブ ソリューション」，および印刷後の原本性を保証する「セキュア プリント ソリューション」の三つのソリューションで構成する（図4参照）。

4.1　電子化プロセスソリューション

法的，または慣習上の理由により，業務上の紙文書を紙

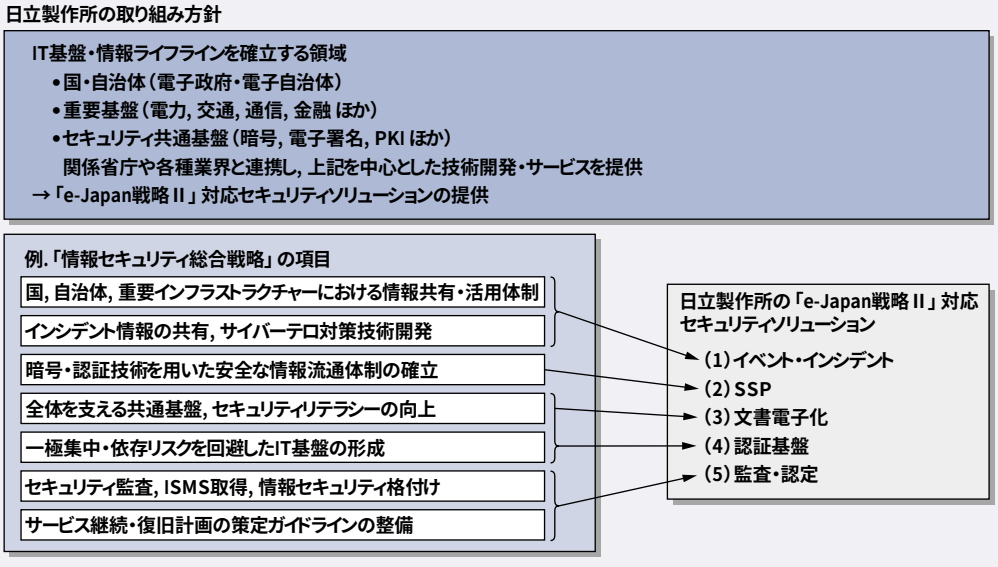
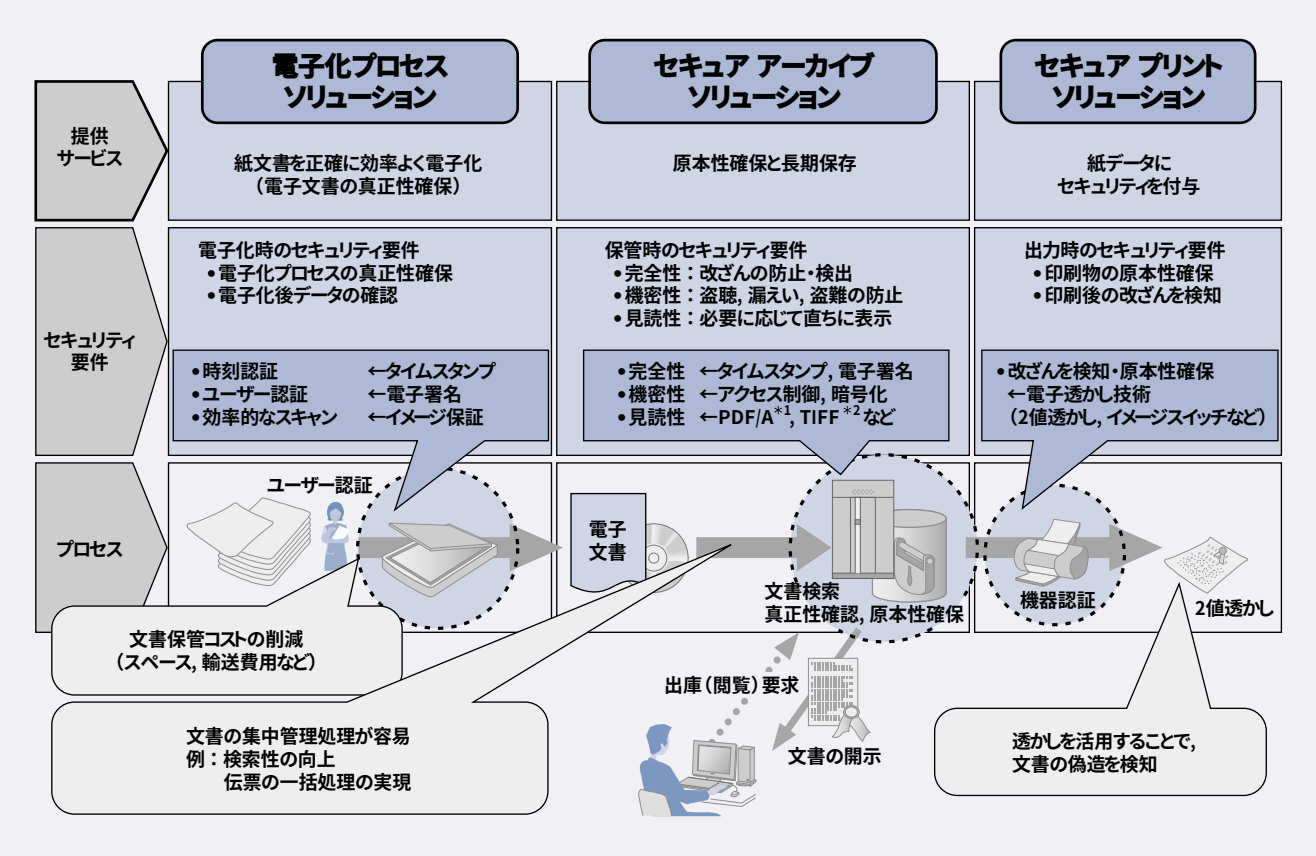


図3　日立製作所のセキュリティへの取り組み方針と内容
「e-Japan戦略　」と「情報セキュリティ総合戦略」を踏まえた日立製作所のセキュリティへの具体的な取り組みを示す。
注：略語説明
PKI（Public Key Infrastructure）
SSP（Secure Service Platform）



注：略語説明ほか　PDF/A（Portable Document Format/Archive），TIFF（Tagged Image File Format）
＊1 PDFは，米国およびその他の国におけるAdobe Systems, Inc.の商標である。
＊2 TIFFは，米国Aldus Corp.が開発したフォーマットの名称である。

図4 文書電子化（ペーパーレス）ソリューションの概要
紙文書の電子化，電子文書の長期保管，印刷後の文書などのライフサイクル全体にわたってセキュリティを確保する。

のまま保存しなければならない例が民間企業には見られる。このような紙文書の保管コストの削減と，電子化による業務効率化を図るのが電子化プロセスソリューションである。

これまでは，紙文書が持つ筆跡，紙質，紙の厚さ，印影など電子文書にはない特徴がイメージデータへの変換によって失われる，またはイメージデータがそのままでは改ざんが容易であるという危ぐにより，紙文書の電子化が認められないケースがあった。このソリューションでは，これらの課題を解決するために，高性能のスキャナの使用と，電子署名およびタイムスタンプといったPKI技術を使用する。

スキャナはA4版など定形の紙文書を高速に電子化する場合にはシートフィーダ型高速スキャナを，領収書などの不定形の紙文書を1枚ずつ電子化する場合には，日立製作所のオーバヘッド型スキャナ“ Blinkscan ”をそれぞれ使用する。これにより，紙が持つ特徴の多くをイメージデータに変換した後も保つことが可能となる。

電子化後にイメージデータが改ざんされるおそれへの対策としては，電子化作業者による電子署名をイメージデータに作成し，さらに，電子署名には信頼の置ける第三者機関によるタイムスタンプを作成する。これにより，「だれが」，「いつ」電子化したのか，また，それ以降イメージデータが改ざんされていないことを第三者に証明することが可能となる。

また，電子化作業のプロセスをJIS Z 6016「紙文書及びマイクロフィルム文書の電子化プロセス」などのガイドラインに沿って運用することにより，イメージデータの原本性を強固にすることができる。

4.2 セキュア アーカイブ ソリューション

電子文書を保存する場合には，原本性を確保することが重要である。このソリューションでは，日立製作所の原本性保証システム“ DP1/Proofbox2 ”を使用することにより，旧総務庁の研究会が定めた原本性の確保要件（完全性，機密性，見読性）を確保する[5]。

DP1/Proofbox2では，電子署名，書き換え・消去不可の制御，および原本への操作履歴管理について，バックアップ・リストアによってデータの完全性を，アクセス制御と暗号化によってデータの機密性をそれぞれ確保する。さらにPDF（Portable Document Format），TIFF（Tagged Image File Format），XML（Extensible Markup Language）などの標準的なフォーマットでデータを保存することにより，見読性を確保する。

データを長期保存する際は，これらの原本性を長期にわ

たって確保する必要がある。セキュア アーカイブ ソリューションでは，ヒステリシス署名を採用することにより，これまで困難であった電子署名の有効性の長期保証を図った。ヒステリシス署名の特徴は，再署名方式に比べて定期的なタイムスタンプ生成が不要であることである。

文書管理機能はDP1/Proofbox2と連携する文書管理システムによって実現し，文書の閲覧，電子署名，タイムスタンプの検証などを行う。

4.3 セキュア プリント ソリューション

電子文書をプリンタで印刷する場合，(1) 不正な印刷，(2) 電子文書の属性情報［文書ID（Identification），作成者IDなど］が紙に反映されない，(3) 印刷物の不正流出，(4) 印刷物の改ざん，(5) 紙に印刷後の追記情報があとで区別できない，および(6) 正本とコピーの区別がつかないというセキュリティ上の課題がある。

セキュア プリント ソリューションでは，これらの課題を解決するために，「電子証紙システム」を使用する。電子証紙システムでは，ICカードによる印刷員数制御，紙文書にトレース情報を埋め込む「2値電子透かし」，紙文書の改ざん検知やコピー識別を行う「電子証紙技術」により，不正な紙文書の流通を防止することができるようになる。

5 おわりに

ここでは，トータル セキュリティ ソリューション“Secureplaza”と，「e-Japan戦略II」，「情報セキュリティ総合戦略」の全体像，およびこれらに対する日立製作所の取り組みについて述べた。

日立製作所は，セキュアな情報ライフラインの実現により，「いつでも，どこでも，だれでも」，「安心・安全」に情報やサービスが利用できる社会を目指し，今後も，最新のトータル セキュリティ ソリューションの提案により，サービス プラットフォーム コンセプトHarmonious Computingの信頼性を支えていく考えである。

参考文献など

1) http://www.hitachi.co.jp/Secureplaza

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，Vol. 43，No. 10，pp. 1078～1084（2002.10）

3) http://www.kantei.go.jp/jp/singi/it2/kettei/ejapan2/030702gaiyou.html

4) http://www.meti.go.jp/policy/netsecurity/strategy.htm

5) 小林，外：電子文書への不正なアクセスや改ざんを防止する原本性保証システム“DP1/Proofbox2”，日立評論，**85**，12，769～774（2003.12）

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，「e-Japan戦略II」関連セキュリティ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：c-konno @ itg. hitachi. co. jp

本多義則

1991年日立製作所入社，システム開発研究所 第7部 所属
現在，セキュアアーカイブの研究開発に従事
E-mail：y-honda @ sdl. hitachi. co. jp

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，「e-Japan戦略II」関連セキュリティの企画と事業展開に従事
E-mail：m-nihonmatsu @ itg. hitachi. co. jp

長谷川大造

1991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 セキュリティマーケット開発部 所属
現在，「e-Japan戦略II」関連セキュリティの事業マーケッティングに従事
E-mail：d-hasegawa @ itg. hitachi. co. jp