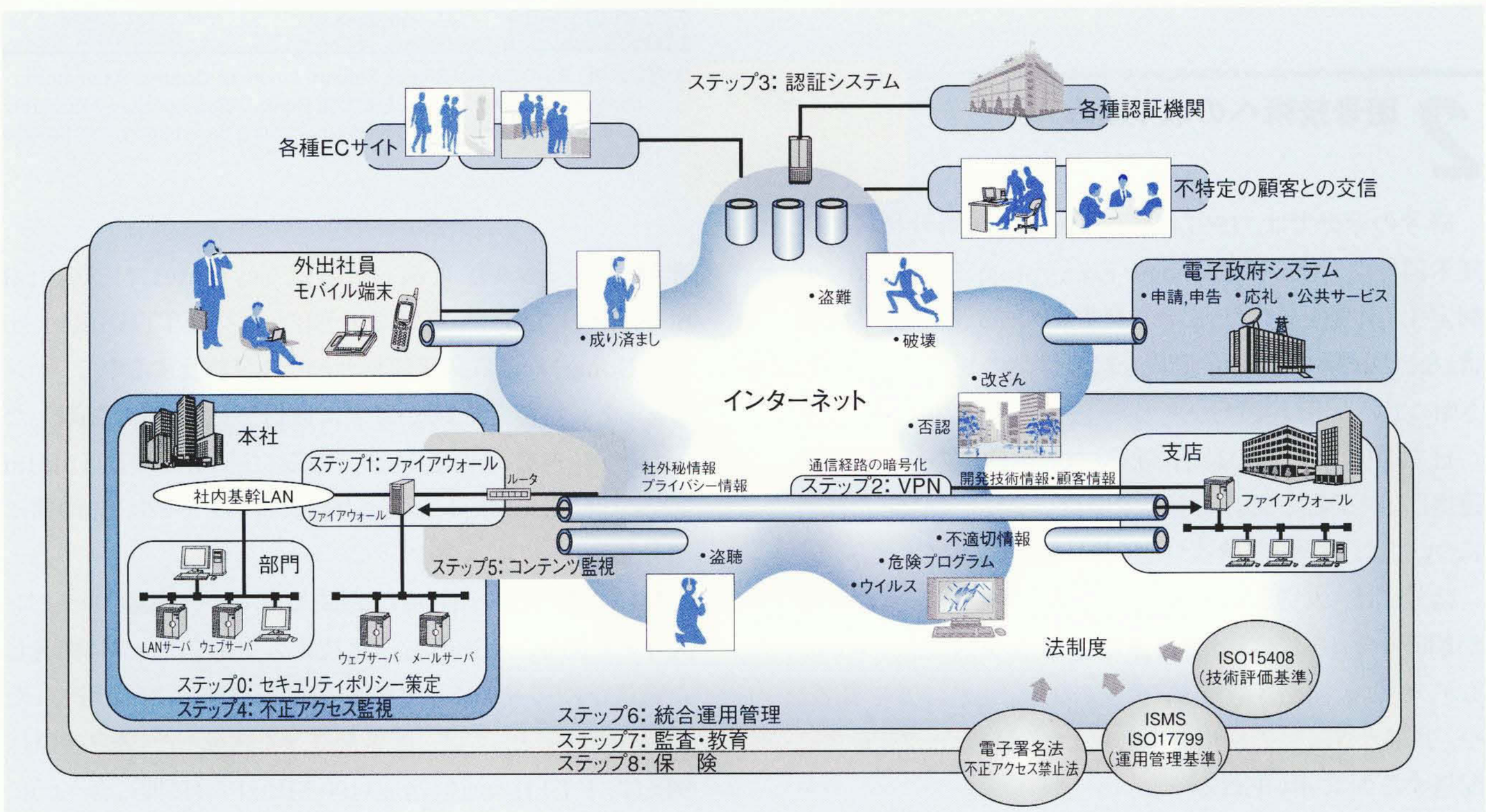
情報ライフラインを支えるトータルセキュリティソリューション“Secureplaza”

Hitachi's Total Security Solution for the Information Lifeline

金野千里 *Chisato Konno*　中野利彦 *Toshihiko Nakano*
宝木和夫 *Kazuo Takaragi*　長谷川大造 *Daizô Hasegawa*



注:略語説明　EC(Electronic Commerce), VPN(Virtual Private Network), ISMS(Information Security Management System), ISO(国際標準化機構)

インターネットシステムのセキュリティ対策の概要
インターネットを活用した典型的な情報システムの構成で，システムやサービスの広がりに応じたSecureplazaのステップ別セキュリティソリューションの全体像を示す。

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，不正アクセス，ウイルス感染，情報漏えい，詐欺行為など，さまざまなリスクが増大し，大きな脅威となってきた。そのため，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，“Secureplaza”において，セキュリティポリシー，ファイアウォール，VPN(Virtual Private Network)，認証，アクセス監視などの多岐にわたるセキュリティ対策を，実際のシステムやサービスの広がりに即した九つのステップで提案している。Secureplazaは，Harmonious Computingのコンセプトに基づくサービス プラットフォーム ソリューションの信頼性を支える構成要素の一つである。

日立製作所は，Secureplazaにより，情報ライフラインのハイレベルなセキュリティ維持に貢献するため，アウトソーシングサービス，認証，情報漏えい対策などの目的に対応したトータルソリューションを提案している。

1 はじめに

ユビキタス情報社会の到来とともに，電子政府システムやインターネット バンキング システムに象徴されるように，インターネット上でのサービスも急速に高度化してきた。それに伴い，不正アクセス，ウイルス感染，情報漏えい，詐欺行為などのリスクが増大し，深刻化している[1]。

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，踏み台にされて他サイトを攻

撃したり，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いる。そのため，サービスの停止や信頼の失墜など，組織活動に多大な影響を与えかねない状況も起きていることから，技術面での対策に加え，法制度面での整備やセキュリティの評価基準が進められている[2]。

ここでは，情報セキュリティにおける最新動向の一つとしての次世代暗号技術と，日立製作所のトータル セキュリティ ソリューション“Secureplaza”について述べる。

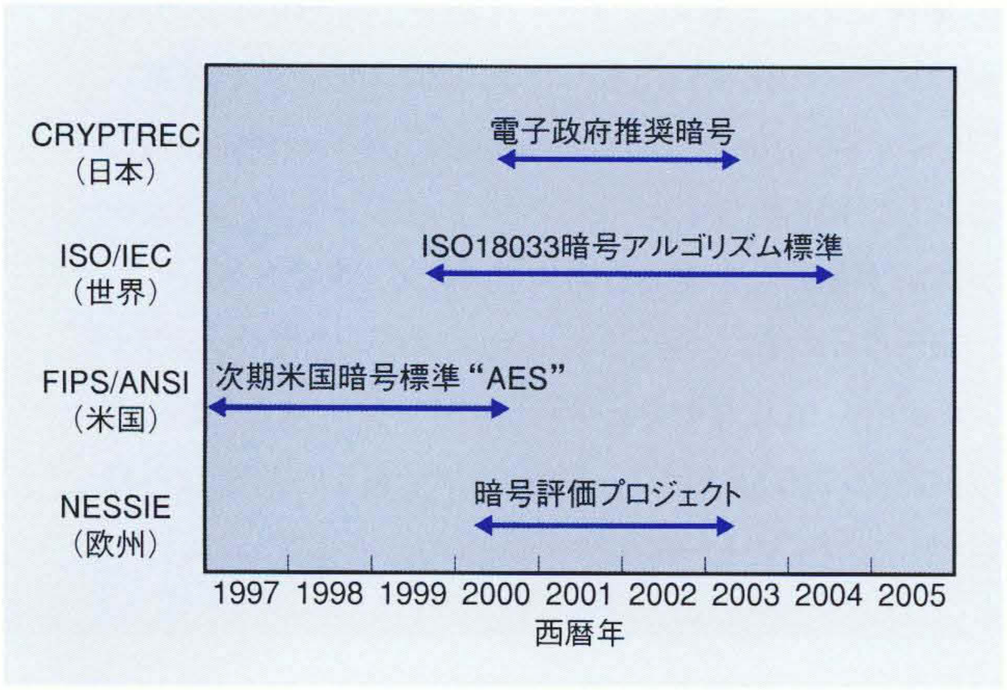
2 暗号技術への取り組み

暗号の分野では，1997年に，米国政府が暗号技術の次期米国標準“AES(Advanced Encryption Standard)”を制定する作業を始めた。これを契機に，ISO(国際標準化機構)などの標準化団体も，新たな暗号標準の制定に向けて動き始めている(**図1**参照)。

日立製作所は，この動きに呼応して，国内外の研究機関と連携しながら特徴ある暗号技術を開発してきた。開発した技術については，標準化に関連づけて製品化する方針をとっている。

暗号には，大別して2種類がある(**表1**参照)。一つは共通かぎ暗号で，主にデータを高速暗号化するのに用いられる。もう一つは公開かぎ暗号で，データの認証(ディジタル署名)や，共通かぎ暗号の使用時に必要となるかぎデータを安全に配送することに用いられる。

このうち共通かぎ暗号については，ストリーム暗号と呼ばれる高速処理に優れた原理を採用し，MULTI-S01(Multimedia Encryption−Stream No. 01)[3]，およびMUGI(Multi Gigabit Cypher)[4]という2方式を開発した。ストリーム暗号は，



注:略語説明　CRYPTREC(Cryptography Research and Evaluation Committee)，ISO/IEC(International Organization for Standardization/International Electrotechnical Commission)，FIPS/ANSI(Federal Information Processing Standards/American National Standards Institute)，NESSIE(New European Schemes for Signatures, Integrity and Encryption)

図1 暗号技術標準化の動き

暗号では，次期米国暗号標準“AES”制定の動きを契機に，ISO(世界)，CRYPTREC(日本)，NESSIE(欧州)などで新たな標準化の動きが生じた。

表1 共通かぎ暗号と公開かぎ暗号

暗号には共通かぎ暗号と公開かぎ暗号の2種類があり，前者はデータの高速暗号化に，後者はディジタル署名やかぎ配送などにそれぞれ用いられる。

	共通かぎ暗号	公開かぎ暗号
代表的な技術・製品	米国:AES 日立製作所:MULTI-S01，MUGI	米国:RSA-OAEP，ECDSA 日立製作所:HIME(R)
暗号かぎの関係	暗号かぎ＝復号かぎ	暗号かぎ≠復号かぎ
秘密かぎの配送	必要	不要
安全な認証(ディジタル署名)	困難	容易
暗号化速度	速い	遅い
主要な用途	データの暗号化	ディジタル署名 かぎの配布

注:略語説明　RSA-OAEP(Rivest-Shamir-Adleman Optimal Asymmetric Encryption Padding)，ECDSA(Elliptic Curve Digital Signature Algorithm)，HIME(R)〔High-Performance Modular Squaring Based Encryption Scheme (Revised Version)〕

非対称ディジタル加入線(ADSL:Asymmetric Digital Subscriber Line)や家庭で使う光ファイバ(FTTH:Fiber to the Home)などの高速通信サービスが普及する中で，コンピュータへ負荷をあまりかけずに通信データを暗号処理したいというニーズにこたえるものである。さらに，DVD(Digital Versatile Disc)などに記録された大量のデータを，短時間に暗号処理するのにも適している。

MUGIは，AESの開発者でもあるベルギー王国のルーベン大学と共同で，AESの高速化技術の一部をベースに開発した高速なストリーム暗号であり，公的な標準として採用された共通かぎ暗号としては，世界最高速を達成した(**表2**参照)。例えば，FTTHの通信速度(100 Mビット/s)に間に合うようにMUGI(800 Mビット/s)で暗号化する場合，コンピュータ(650 MHzのCPU使用の場合)にかかる負荷は12.5%程度で済む。一方，AES(358 Mビット/s)の場合，コンピュータの負荷は28%に増大する。また，DVDの17 Gバイトのデータを暗号処理するのに，MUGIでは170秒で済むのに対して，AESでは380秒程度かかる。

MULTI-S01では，世界で初めて，守秘機能に加え，従来の共通かぎ暗号にはなかった改ざん検知機能も実現した。この機能は，例えば電子商取引での金額情報など，通信路上で改ざんされては困るデータを送信する場合に効力を発揮する。一方，AES単独ではこの機能は効力を発揮することができず，もし守秘とともに改ざん検知も行おうとすると，MAC(Message Authentication Code)などの別処理を行う必要

表2 MULTI-S01とMUGIの性能

従来のブロック暗号と今回開発したストリーム暗号の処理性能比較を示す。

	従来方式	日立製作所の新技術	
暗号名	ブロック暗号 AES	ストリーム暗号	
		MUGI	MULTI-S01*2
速度(Mビット/s)*1	358	800	348

注: *1　650 MHzのCPU換算　*2　秘匿機能＋改ざん検知機能付き

が生じ，処理時間が2倍近くかかる。

MULTI-S01とMUGIは，CRYPTREC（電子政府推奨暗号）として採用された[5]。また，現在，ISOで標準化について審議中であり，第2段階のCD（Committee Draft）に進んでいる。

日立製作所はこのように，基盤技術として標準化に沿った，世界最高レベルの暗号技術を開発している。

3 ステップ別セキュリティソリューション

本来，セキュリティは，それぞれのシステムやサービスの安全性を保証するための対策である。セキュリティソリューション体系“Secureplaza”[6]では，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，大別して九つのステップで構成している[2]。95ページの図では，本社，支社，モバイルの社員，さらに第三者の顧客や公的機関などがインターネットを経由して接続された典型的な構成の中で，LAN接続，インターネット接続からスタートし，業務の広がりに応じて段階的に対策を講じていくステップを示している。

4 目的別セキュリティソリューション

基本的なステップ別のセキュリティ対策に加えて，日立製作所は，顧客のニーズにきめ細かくこたえる目的別のソリューションも提案している。

4.1 セキュリティコンサルティング

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として，Secureplaza/CS（Consulting Service）では，(1) セキュリティ マネージメント コンサルテーション，(2) セキュアシステム構築コンサルテーション，および(3) セキュリティ診断・監査コンサルテーションの体系を用意している。

これらには，セキュリティポリシー策定支援，ISMS（Information Security Management System）認定取得支援，プライバシーマーク取得支援，ISO15408準拠PP/ST（Program Product/Security Target）作成支援なども含まれる。

4.2 セキュリティレベル維持ソリューション

セキュリティ対策は一度行えば万全という性質のものではない。セキュリティの脆（ぜい）弱性は日々報告され，対策ツールの設定も適正に保たれているとは限らず，利用規則の順守も保証の限りではない。また，内外からのアクセスに対する運用監視も常時実施し，アクセスログの解析やアラームに対する適切な処置が必要となる。このような対応を継続的に行い，維持管理サイクルを実現することが，セキュリティ維持に不可欠

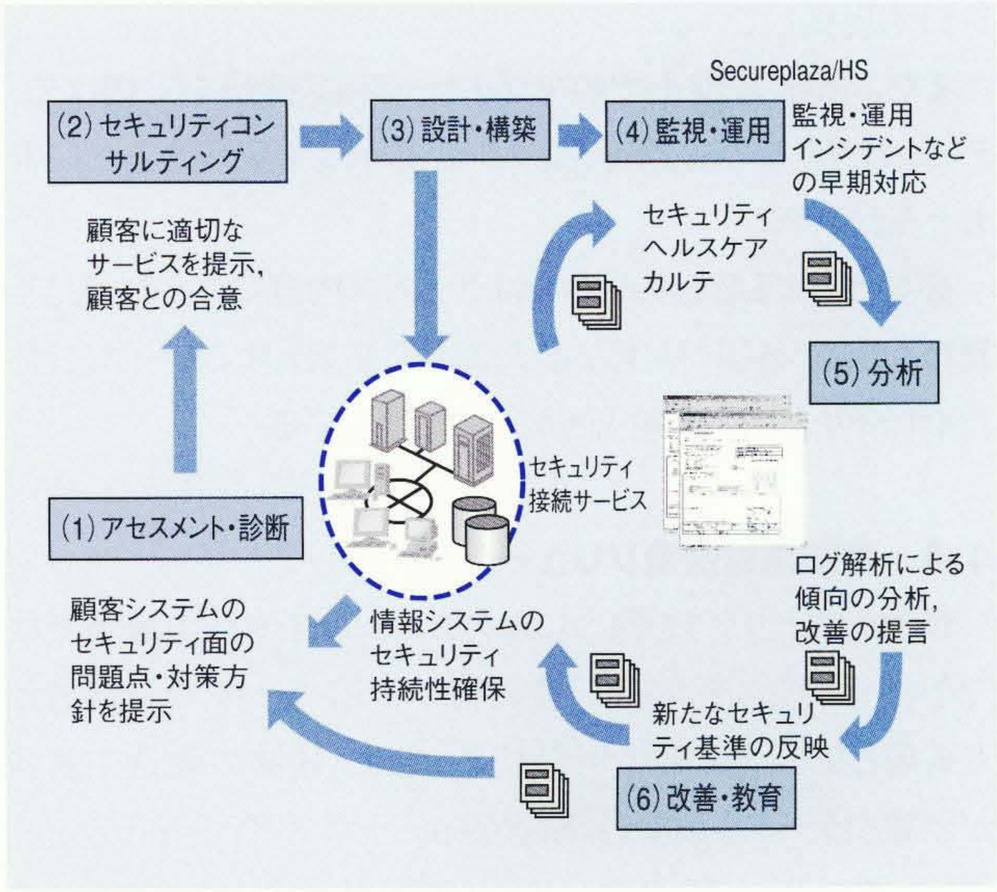


図2 セキュリティ維持管理サイクル
セキュリティライフサイクルに沿ったサービス体系により，企業の持続性をトータルにサポートする。

である（**図2**参照）。Secureplaza/HS（Healthcare Service）では，この維持管理サイクルをアウトソーシングサービスとして提供する。ユーザーサイトのセキュリティ ヘルスケア カルテを作成し，状況報告と必要な対策サービスを随時に提供する。基本的なサービスは，(1) セキュリティ方針策定コンサルティング，(2) セキュリティ診断サービス，(3) 各種セキュリティ サーバ マネジメント サービス，(4) 不正アクセス監視サービス，(5) 情報漏えい防止サービス，(6) セキュアルーム監視・運用サービス，(7) セキュリティ情報提供サービス，および(8) セキュリティ教育支援サービスのメニュー群から成る。

サービスの典型的な提供形態は，初期診断や導入評価を実施する初期サービスと，各種監視や定期診断を組み合わせた月次の基本サービスから成る。

4.3 認証ソリューション

PKI（Public Key Infrastructure）は，インターネットシステムやイントラネットシステムで認証を行うための基盤技術である。PKIでは，認証に加えてVPN（Virtual Private Network）や電子署名なども実現でき，電子政府システムをはじめ，多くの実サービスがこの基盤の上に構築されている。Secureplaza/IM（Identity Management）では，このPKI認証局の構築サービスとして，(1) サイト内に独自に構築する自営認証局と，(2) 電子証明書発行サービスを受けるアウトソーシングの両形態の認証局構築を提供しており，システムやサービスの諸条件をコンサルティングによって選択することができる。

さらに，法制度面での対応として，電子署名法の認定や政府認証基盤接続などを必要とするシステムを構築するためのソリューションも用意している。サービスによっては，交信の時刻を保証するタイムスタンプや，電子文書の原本の長期保存を必要とする業務向けのヒステリシス署名[6]などに対応するソリュー

ションも提供している。

また，認証基盤上でのアプリケーション構築を支援する，ディレクトリサーバ連携やシングルサインオンを実現する商品群もそろえている。

必要とされる認証のレベルはサービス内容によっても大きく異なるので，さらに確実な本人認証を必要とするケースには，バイオメトリックスとの組合せによって対応する。

4.4 機密情報保全ソリューション

情報セキュリティを保つには，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数多い。Secureplaza/TZ(Trusted Zone)では，そのようなサイトに，サーバを格納するセキュアルーム(情報金庫)を導入する(**図3**参照)。地震対策や防火対策はもちろんのこと，ルーム内への出入り管理やネットワーク経由での侵入監視を行う。このソリューションでは，管理が必要なサーバ群を格納するセキュアルームの構築に加え，各種セキュリティツールの設置と運用・監視サービスもそろえている。さらに，運用管理ポリシーを併せて提供することにより，このルーム内を対象としたISMSの評価認定取得も支援する。

4.5 情報漏えい防止ソリューション

情報漏えい被害による訴訟なども多くなってきていることから，情報漏えいの防止は，ブランドイメージの維持や，組織の存続にもかかわる大きな課題となっている。組織内のインターネットの伸展は逆に情報漏えいのリスクを高めており，情報の不正アクセスだけでなく，メディアやパソコンでのコピー，メールによる外部への情報送付，廃棄マシンによる情報漏えいなど，多様な漏えいルートが存在する。Secureplaza/LG(Leak Guard)では，(1) 情報漏えいリスク評価，(2) 情報管理ポリシーの策定，(3) 漏えい防止システム構築，(4) アクセス制御，メールフィルタリング，廃棄ディスクホワイトニングなどの，各種ツールによる対策，および(5) 情報漏えいの監視，監査のようなトータルな情報漏えい防止ソリューションをそろえている。

5 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。

日立製作所は，今後も，ユビキタス情報社会の情報ライフラインを安全に支える，最新の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。

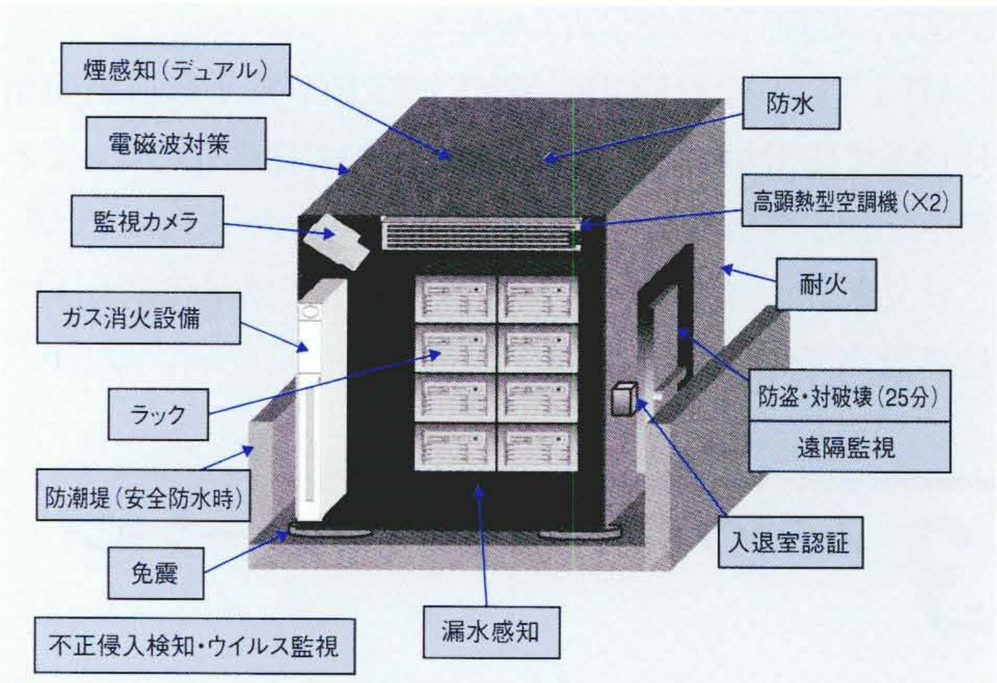


図3 分散型セキュアルーム(情報金庫)による情報保全
セキュアルームの構成諸元と利用イメージを示す。

参考文献など

1) http://www.ipa.go.jp/security/
2) 金野:情報処理学会誌，Vol.43，No.10，pp. 1178～1084(2002.10)
3) S. Furuya, et al. : Integrity-Aware Mode of Stream Cipher, IEICE Trans. Fundamentals, Vol. E85-A, No.1(Jan. 2002)
4) D. Watanabe, et al. : A New Keystream Generator MUGI, Proceedings of 9th International Workshop, FSE 2002(Feb. 2002)
5) 情報処理振興事業協会 通信・放送機構:暗号技術評価報告書(2002年度版)，CRYPTREC Report 2002(2003.3)
6) 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

宝木和夫

1977年日立製作所入社，システム開発研究所 所属
現在，情報セキュリティ技術の研究に従事
工学博士
IEEE会員，電子情報通信学会会員
E-mail：takara @ sdl. hitachi. co. jp

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

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 セキュリティソリューション室 所属
現在，事業マーケティングに従事
E-mail：d-hasegawa @ itg. hitachi. co. jp