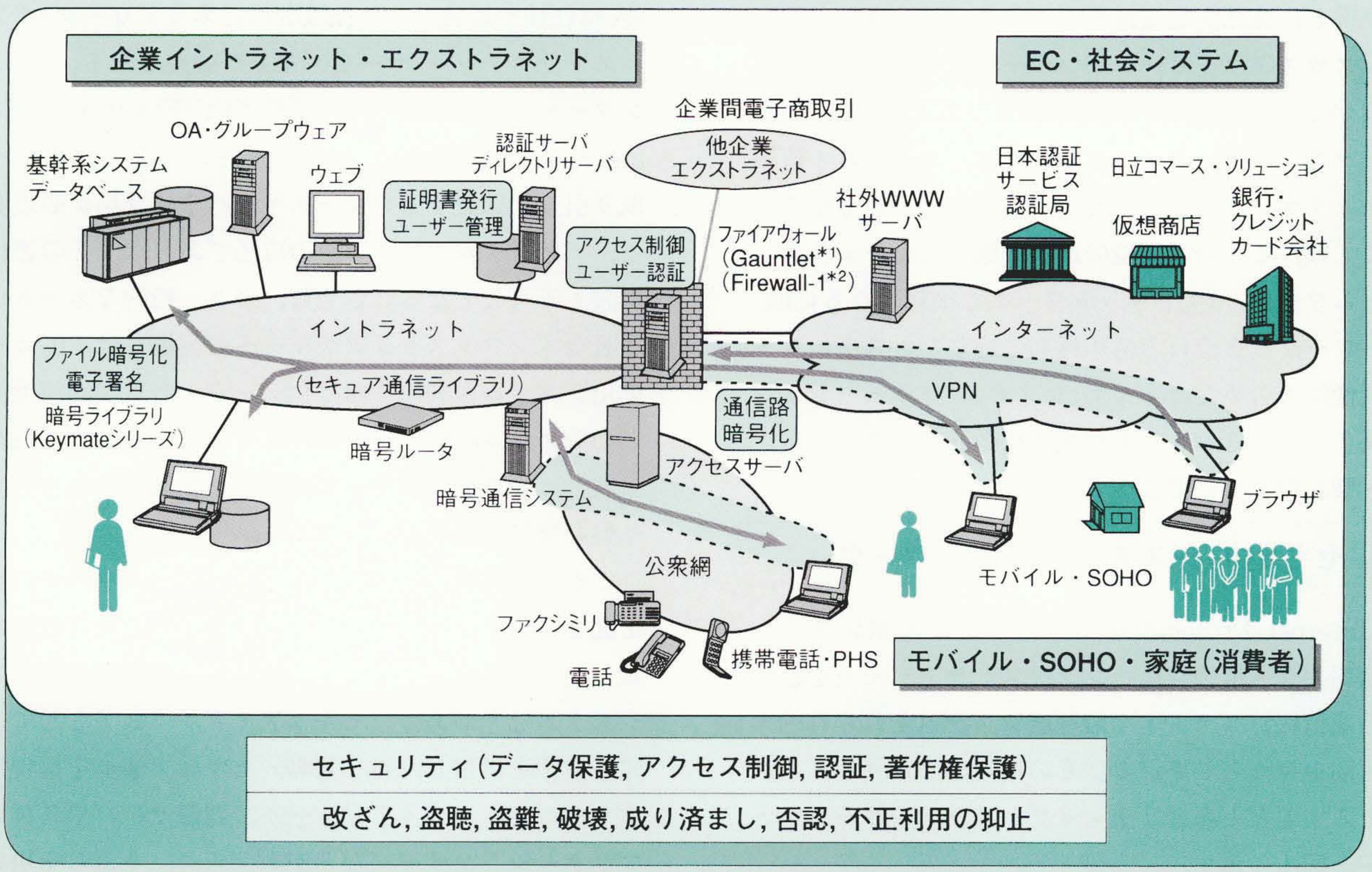
セキュア システム ソリューションとセキュリティ技術

Secure System Solution and Security Technology

金野千里 *Chisato Konno* 久芳 靖 *Yasushi Kuba*
角田光弘 *Mitsuhiro Tsunoda* 手塚 悟 *Satoru Tezuka*



注：略語説明ほか WWW(World Wide Web), EC(Electronic Commerce), SOHO(Small Office, Home Office)
PHS(Personal Handyphone System), VPN(Virtual Private Network), ⟷(暗号通信)
＊1 Gauntletは, 米国Trusted Information Systems, Inc.の商品名称である。
＊2 Firewall-1は, Check Point Software Technology Ltd.の商品名称である。

セキュア イントラネット・インターネット システム コンセプト

企業―家庭―社会をセキュア, シームレス, グローバルなネットワークで接続する, セキュア イントラネット・インターネット システムのイメージを示す。強固でフレキシブルなセキュリティ技術がこの発展を支えている。

学術情報や公開情報などの非商用ネットワークとして発展してきたインターネット技術は, そのオープン・グローバル性と優れた操作性などから, 企業内システム(イントラネット)をはじめとして, 企業間システム(エクストラネット), 企業―消費者間システム〔EC(Electronic Commerce)など〕へとその適用範囲が急速に広がっている。企業―家庭―社会がシームレスなネットワークで接続し, それぞれのユーザーに許可される適正なシステムサービスがどこからでも安全に提供され, 高度情報化社会への展開が期待されている。この巨大な分散環境を実現するためには, ネットワークに接続されているシステムや情報の保護を目的としたセキュリティ技術が不可欠であり, システムの用途や接続範囲の広がりに比例して重要性が増している。

暗号を基盤としたセキュリティ技術は, システムのアクセス制御やネットワーク上のデータ保護をはじめとして, 交信相手の認証, 交信データの正当性の保証, 交信履歴の否認防止などを実現している。一方, 配信されるデータの著作権保護や, システムトータルとしての暗号化データ・暗号鍵の回復手段などが必要となる。

日立製作所は, このイントラネット・インターネットの発展を支えるトータルなセキュア システム ソリューションを提案している。

1　はじめに

イントラネット・インターネットシステムの浸透は急速に進んでいる。企業システムを例にとれば，ウェブによる情報共有・情報発信から始まって，グループウェア，データベースアクセス，既存の基幹システムの情報・処理と連携した意思決定支援やデータウェアハウス，顧客へのマスカスタマイゼーションサービスなど，業務革新につながる幅広い応用が展開されつつある[1]。このネットワークコンピューティングの拡大は，システム・情報のセキュリティ保護が前提になって初めて可能となる。

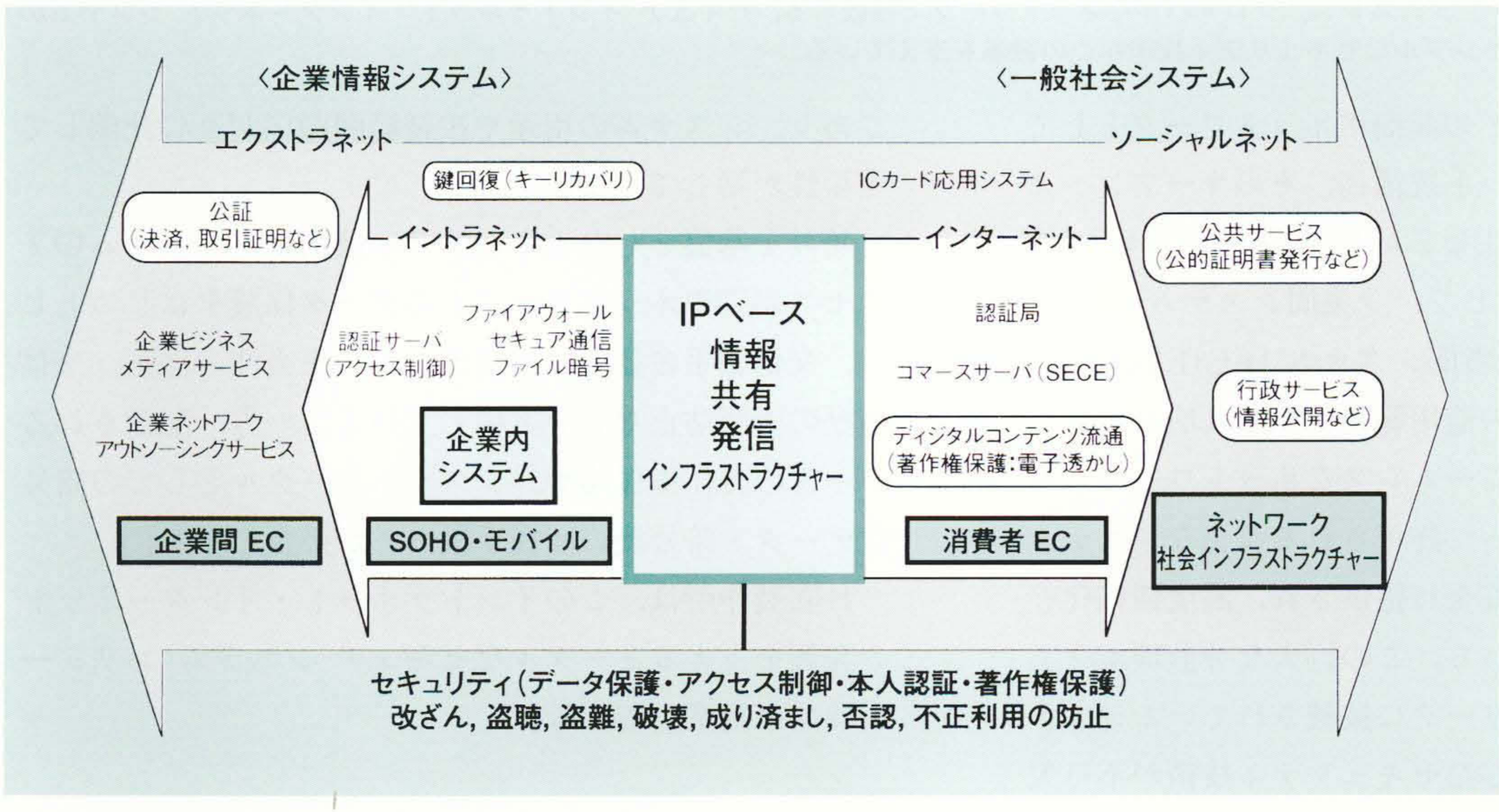
ここでは，この分散環境の進展に則したセキュリティフレームワーク，また，ネットワークで接続される範囲，ネットワーク上を流れる情報種別に応じたシステムコストや利便性も含めたセキュア システム ソリューションの構築手法と，それらを実現する特徴的なセキュリティ技術・製品群について述べる。

2　セキュア システム フレームワーク

IP(Internet Protocol)をベースとした情報システムは，情報共有・情報発信インフラストラクチャーを起点に，企業情報システムと一般社会システムそれぞれへ大きな展開を可能としている。その用途の広がりと，それを支える主要なセキュリティサブシステムやサービスとの対応を**図1**に示す。

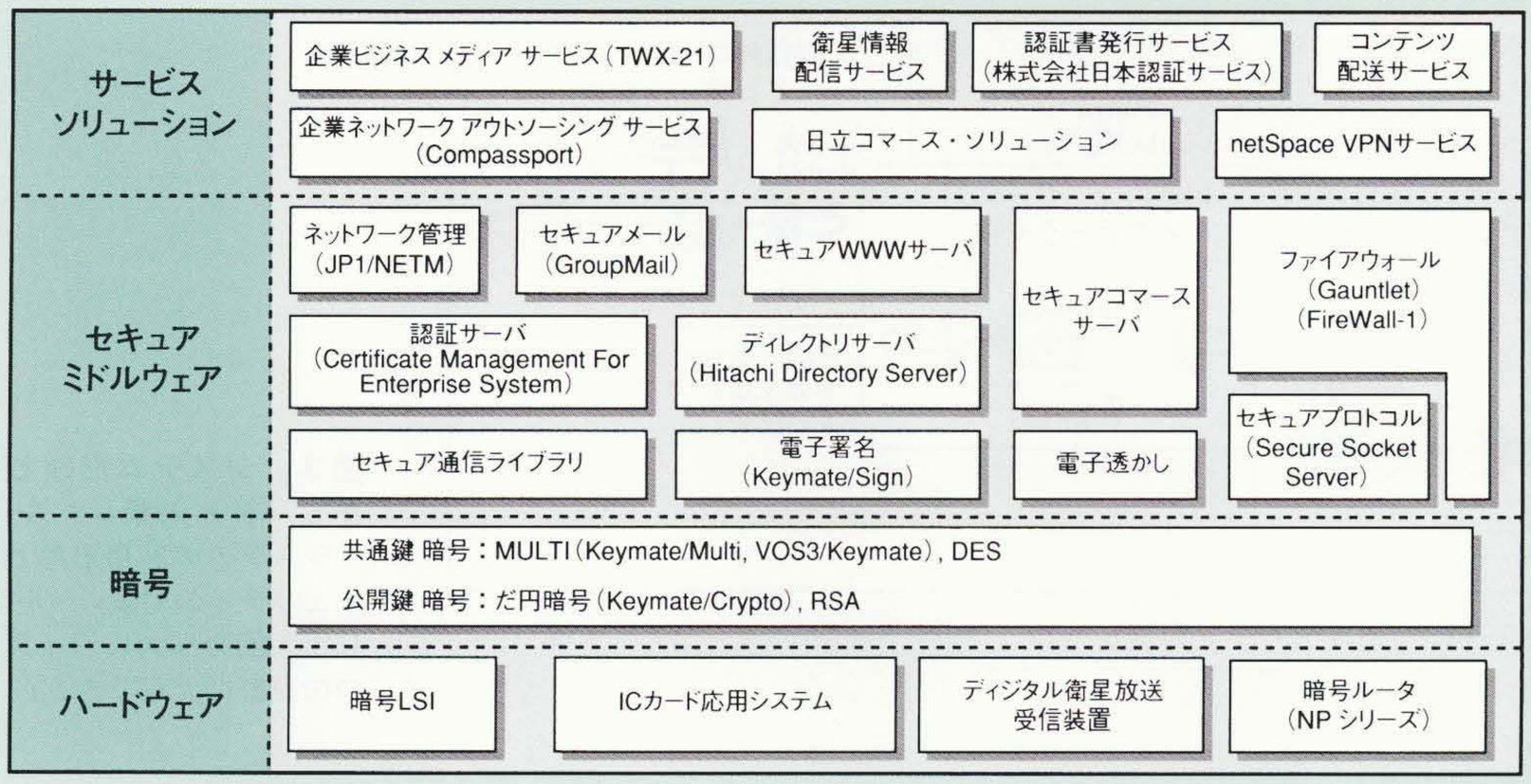
インターネット技術を活用した企業内情報システム(イントラネット)や社外からのアクセスを可能とするSOHO・モバイルシステムでは，ファイアウォール，セキュア通信，ファイル暗号などによるアクセス制御やデータ保護などが必須となる。また，システム内の情報やプログラムの利用にあたって，より精緻(ち)なユーザー認証を実現するために，認証サーバが導入される。さらに，企業間の情報流通や取り引きへの展開である「エクストラネット」では，その受発注や決済に対する公証機能，信頼性や帯域のより保証されたネットワーク インフラストラクチャー サービスなどが必要となる。一方，インターネットの展開では，消費者EC(Electronic Commerce：電子商取引)に対するセキュアなネットワーク取り引きを保証するコマースサーバや認証局が必須であり，ディジタルコンテンツの流通であれば，その著作権保護も不可欠となる。さらに，より一般的なネットワーク社会インフラストラクチャーへの発展には，ICカード応用システムの利用や暗号化データ・暗号鍵回復機能などのシステムのトータルセキュリティを保証する技術，公共サービスや行政サービスなどの公的な社会サービス基盤の整備が必要となってくる。

これらを実現するセキュリティフレームワークの構成を**図2**に示す。セキュリティの基盤である暗号技術を搭載したハードウェアとして，暗号ルータやICカード応用システムなどがある。セキュアミドルウェアとしては，暗号技術を活用した電子署名，セキュア通信を実現するプロトコル，ファイアウォール，認証サーバや各種のアプリケーションサーバなどがあげられ，それらを用いたサービスやソリューション群で構成する。ユーザーの用途に沿ったセキュア システム ソリューションは，これらを組み合わせることによって構築可能となる。



注1：略語説明
EC(Electronic Commerce)
SOHO(Small Office, Home Office)
SECE(Secure Electronic Commerce Environment)
注2：□(今後の展開)

図1　イントラネット・インターネットシステムの進展
イントラネット・インターネットの進展とセキュリティ技術・サービスとの対応を示す。



注1：▭（日立製作所の製品・商品区分）
（　）（日立製作所の製品・商品名称）
注2：略語説明
VPN（Virtual Private Network）

図2　日立セキュリティフレームワーク

用途やシステム形態に適合したセキュリティを，システムトータルで実現可能とする，ハードウェア・ソフトウェアの階層の全体像を示す。

セキュア システム ソリューションの構築手法を3章で，セキュリティ製品群のうち，特徴的な技術と製品を4章でそれぞれ述べる。

3　セキュア システム ソリューション

3.1　セキュリティポリシー

セキュリティポリシーとは，「脅威は何か」，「だれから守るか」，「保護する対象は何か」，「セキュリティに対してどれだけの代償(コスト)を払うか」を抽出，整理し，セキュリティ確保のスタンスを明確化したものである。ソリューションでは，セキュリティポリシーの作成がシステムを設計，導入，運用するうえで重要と思われる。たとえ一つのセキュリティホールでも，分散システム全体としてのセキュリティレベルを低下させるからである。

セキュリティポリシーをベースに構築するセキュアシステムの形態と，その構築手順の考え方の概要を以下に述べる。

3.2　セキュアシステムを実現する機能

セキュアシステムを実現するために必要な機能は，以下のとおりである。

(1)　ネットワーク利用制限

利用できるネットワークを制限する。組織内と組織外(社内と社外)を分ける機能である。

ファイアウォール，ルータによるパケットフィルタリングなどの対策で実現する。

(2)　端末制限

利用できる端末を制限する。利用できる組織や部署を制限する機能である。

(3)　利用アプリケーション制限

利用できる業務を制限する。業務担当や部門外秘の業務のように，制限したいときの機能である。

業務と関係のないアプリケーションを制限(ホームページ閲覧やTelnet利用などを制限)するときにも用いる。

(4)　利用者制限

本来の利用者を確認する。ID(Identification)番号やパスワードのほかに，電子的な証明書を追加し，本人認証を強化する機能がある。特定利用者だけに限定する業務に適する。すなわち部門外秘や関係外秘の業務に有効である。

3.3　セキュアシステムの形態とセキュリティ対策

セキュリティにかけるコストには，費用対効果を考慮した設計が求められる。必要な個所に必要な対策をとることが重要となるが，ネットワーク上を流れるデータの種類や不正利用で想定される被害の度合いにより，必要なセキュリティレベルが決まってくる。

また，一般にセキュリティレベルを上げるとコストは大きくなり，利便性(操作性，性能，機能など)が悪くなる。セキュリティレベルと，必要コストや利便性を考慮し，対策ポイントに必要なセキュリティ対策をいかに適用するかが鍵となる。

システム形態とそのセキュリティ対策の概要を**図3**に示す。

(1)　組織内クローズドネットワーク形態

社内LANで，外部ネットワークとの接続が無く，同じ組織のユーザーが利用する環境である。この形態は組織外にネットワークが接続されていないため，利用サーバ

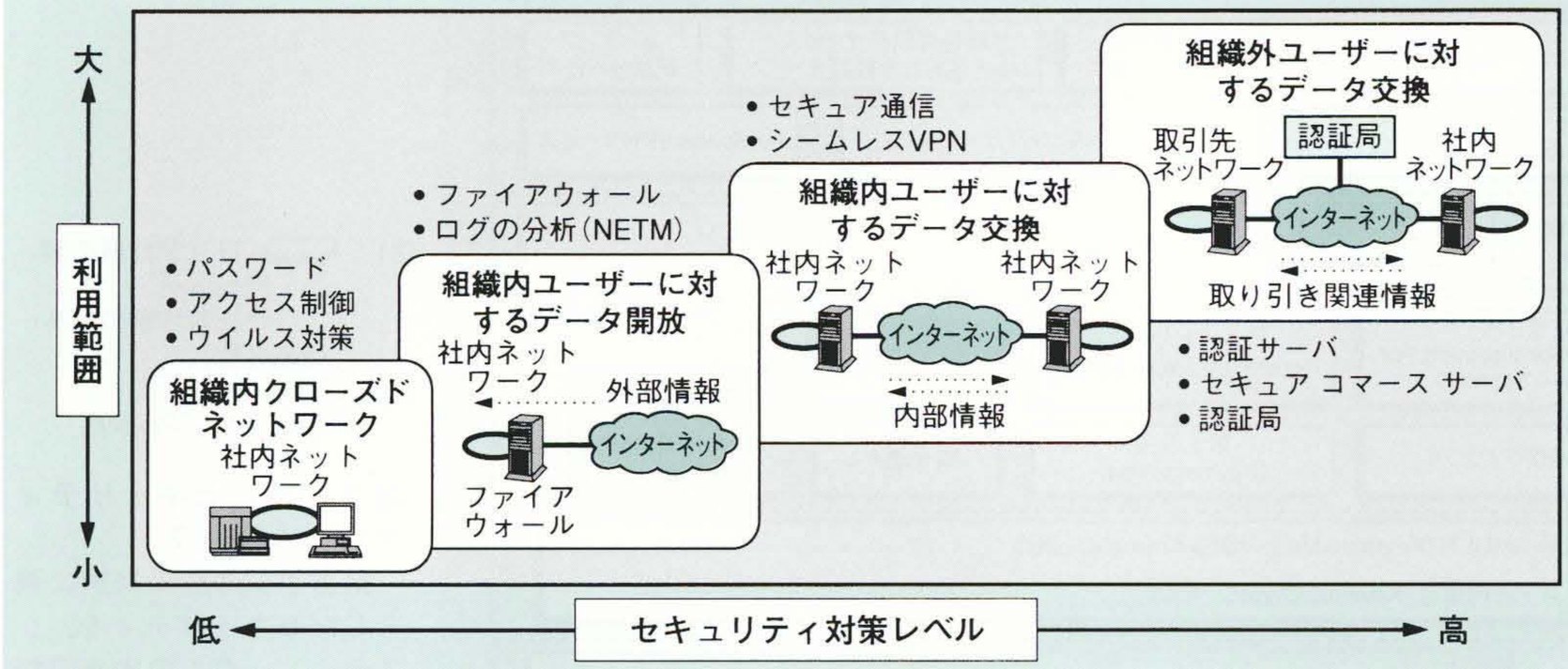


図3　システム形態とセキュリティ対策レベル

システムの利用形態とセキュリティの対策レベルは，利用範囲の拡大に沿って四つの形態に大別できる。

での認証・アクセス制御などの設定や，ウィルス対策ソフトウェア導入でのセキュリティ対策が基本となる。この形態が，セキュリティポリシー策定時の基本単位となる。

組織内不正アクセスを想定すると，利用者の本人確認を強化する必要がある。

(2)　組織内ユーザーに対するデータ開放形態

インターネットと専用線接続し，外部サービスを利用する環境である。この型は，外部からの不正な侵入を新たに考慮する必要がある。特に外部ネットワークとの接続部分はセキュリティ対策での重要なポイントであり，ファイアウォールなどの設置が必須となる。

(3)　組織内ユーザーに対するデータ交換形態

インターネットを介して組織内でデータ交換を利用する環境である。SOHOやモバイルでのアクセスもこの形態に含まれる。この形態では，インターネット上の通信データの盗聴を新たに考慮する必要がある。なお，モバイルでのアクセスについては，利用者の本人確認が必須である。

(4)　組織外ユーザーに対するデータ交換形態

組織外のユーザーとインターネットを介してデータ交換を利用するエクストラネット形態である。この形態では，通信データの改ざんや，成り済まし，一度認めたデータの否認について新たに考慮する必要がある。

事例としては，インターネット上での企業間ECや消費者ECのシステムがある。

3.4　セキュアシステム構築手順

セキュアソリューションでは，システム構築時と運用時のセキュリティ面でのよりどころとなるセキュリティポリシーをベースとしている。このため，サービス〔WWW(World Wide Web)アクセス，メール，ファイル転送などのアプリケーション〕や利用者を規定することにより，アクセス制御のための設定を洗い出し，この設定情報を実装時に生かしながらセキュリティを確保したシステムが設計できるような，標準的な手順を規定している。手順の概要を以下に示す。

(1)　設計項目の整理

実現するサービスや制約事項を抽出，整理し，セキュリティポリシーを作成する。

(2)　基本アーキテクチャの設計

基本となるネットワークを設計し，セキュリティを考慮しながらサービスの実現方法を検討する。

(3)　アーキテクチャの詳細化

サービスを提供するうえで，セキュリティ面での考慮点をチェックし，必要な補強を行う。

(4)　システムの評価

セキュリティポリシーを満たしているかを確認する。評価は定期的に実施する。

4　セキュアシステムを支える基盤技術

前章で述べたセキュアシステムの構築を支えるセキュリティ基盤技術について以下に述べる。

4.1　セキュリティ基盤製品アーキテクチャ

今日の企業情報システムは，インターネット技術を中心としたイントラネット環境を中心に構築されてきており，さらに，分散オブジェクト技術をベースにしたシステム形態になりつつある。しかし，メインフレームやUNIXサーバ※)を中心としたクライアント/サーバ・シ

※)　UNIXは，X/Open Company Limitedがライセンスしている米国ならびに他の国における登録商標である。

ステム形態も広く利用されており，これらのシステム形態を包含したセキュリティアーキテクチャや製品を体系的に提供することにより，システム全体のセキュリティが確保できる。

日立製作所は，(1) 企業情報システム全体を保護するためのセキュリティ(ファイアウォール)，(2) インターネットやモバイル環境での安全な通信を実現する“VPN(仮想プライベートネットワーク)”，(3) イントラネット・インターネット環境での業務やサービス単位でよりきめ細かなセキュリティを確保するためのアプリケーションセキュリティを実現している(**図4**参照)。さらに今後は，分散オブジェクト基盤“Network Objectplaza”に基づいて構築する，基幹業務サーバを中心とするサーバ群の保護を実現していく。

さらに，これらのセキュリティ製品を共通に運用するための機能をインターネットの標準技術に基づいて提供し，セキュリティ運用負担の軽減を図っていく。

4.2　ネットワークセキュリティ

企業情報システムに対する外部からの不正なアクセスを防止するため，ファイアウォールとして“Gauntlet”と“FireWall-1”という二つの製品を提供し，基本的なサイトセキュリティ構築を支援している。

4.3　仮想プライベートネットワーク

専用線の代わりに本社—支社間などを相互接続するネットワークとして，また，モバイル運用や在宅勤務，SOHOといった新たな勤務形態を実現するためのインフラストラクチャーとして，VPNを提供している。

日立製作所は，Gauntletファイアウォールにアドオンして利用が可能な“VPN for Gauntlet”と，公衆ネットワーク経由のモバイルアクセス形態を主な対象とした「Secure Socket Serverシステム」の二つのVPN製品を提供している。いずれのシステムでも高い強度を持つMULTI2暗号[2),3)]を利用した通信が可能である。

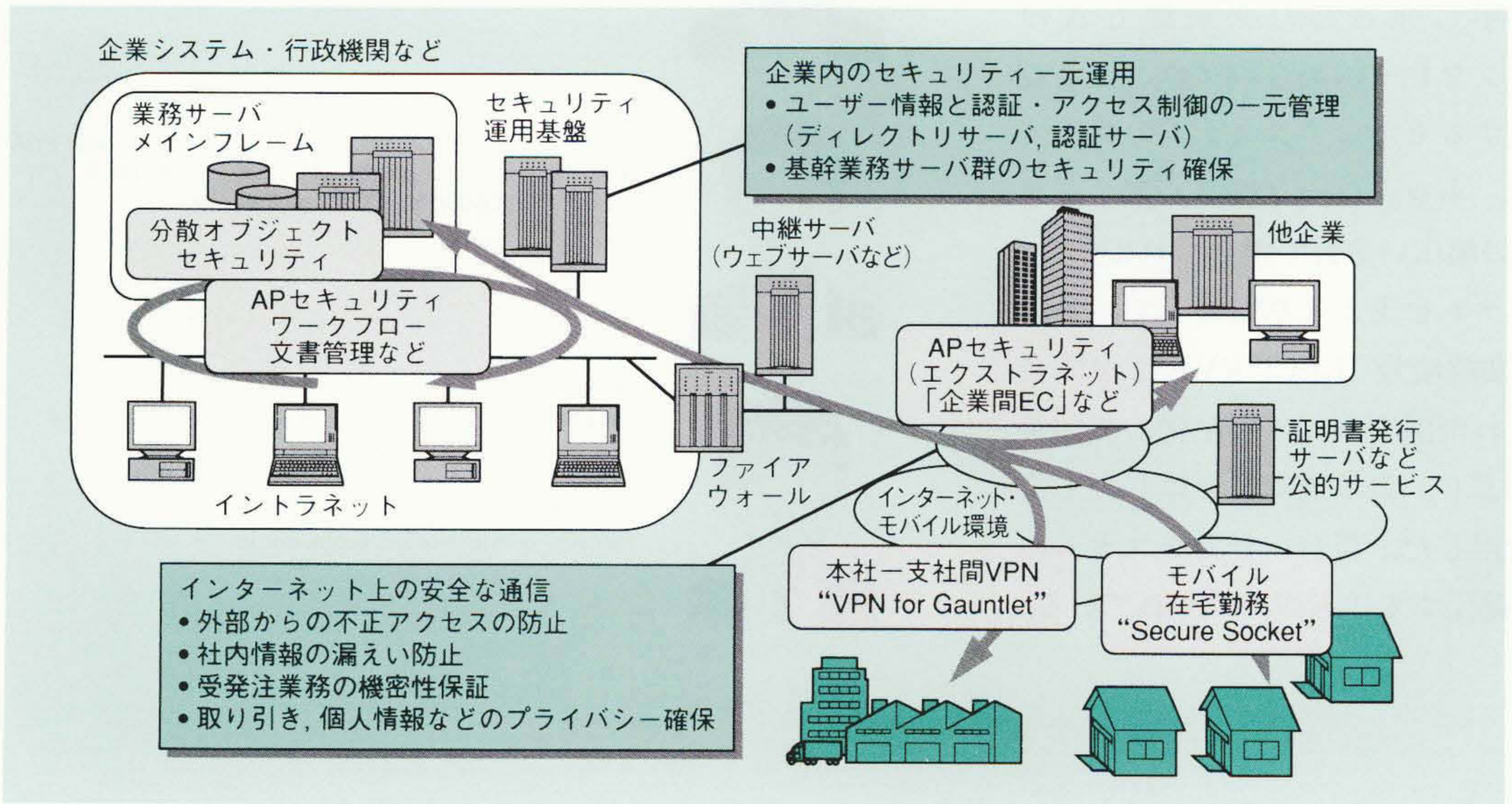
4.4　分散オブジェクト環境のセキュリティ

Network Objectplazaで構築する分散システム環境のセキュリティ基盤として，OMG(Object Management Group)の提唱する“CORBA(Common Object Request Broker Architecture) Security2.0”準拠のセキュリティサービス機能を提供する。

セキュリティサーバで管理するセキュリティドメインに属するオブジェクト間のメッセージを，セキュアプロトコルである“SECIOP”で一律に暗号化して署名付きメッセージとすることができるほか，オブジェクト相互間のアクセスを制御することができ，セキュアな分散システム環境が構築できる。また，セキュリティドメインに属するアプリケーション(オブジェクト)に対するシングルログイン機能も実現する。

4.5　アプリケーションセキュリティ

途中のネットワークの安全性や分散システム環境形態に依存せず，アプリケーション相互間でのセキュアなメッセージ交換とファイル交換を実現する。これらの機能はアプリケーションからセキュア通信ライブラリを利用することによって実現でき，暗号処理や署名などを必要なデータに対して必要なレベルできめ細かく行えるため，ミッションクリティカルな業務に向いている。ECなど，インターネットやエクストラネット環境で展開する



注：略語説明
AP(Application Program)

図4　日立製作所が実現するセキュアな企業情報システム環境

企業間や社会を結ぶシームレスなアプリケーション実現のためのセキュリティインフラストラクチャーを提供する。システム形態や業務目的により，さまざまなレベルのセキュリティを確保できる。

基幹型アプリーションや，人事情報，経理，決済業務を扱うシステムなどに今後積極的に適用していく。

4.6　セキュリティ運用基盤

ユーザーニーズとシステム構築形態に合わせた各種のセキュリティ機能の共通運用を可能にし，運用コストの最小化を図るため，インターネット技術をベースとした共通運用管理を実現する。

セキュアシステム構築では，インターネット環境で広く採用されている「X.509公開鍵証明書」を中心に実現している。イントラネット・エクストラネット向けの証明書発行サーバを提供するとともに，発行した証明書は，そのユーザー情報と合わせてIETF(Internet Engineering Task Force)で規定されるLDAP(Lightweight Directory Access Protocol)に準拠したディレクトリサーバで管理することにより，従来アプリケーションごとに保持していたユーザー管理を一元化し，運用負荷の低減を可能としている。また，証明書の格納媒体としてICカードの利用を可能とすることによって安全性の強化を図るとともに，シングルログインの実現など，エンドユーザーのセキュリティ運用負担の軽減も目指していく。

今後，セキュリティポリシーに基づいてセキュリティ機能が動作しているかどうかを検証するセキュリティ管理(監査)機能，インターネットを経由して接続されるパソコンをLAN環境同様に管理するための，アクセス制御と暗号機能を利用したソフトウェア・コンテンツの配布も実現していく。

4.7　セキュリティ機能を支える暗号技術

日立製作所は，各種のセキュリティ技術，セキュリティ製品の基礎技術である暗号技術の開発に1980年代から取り組んできた。1989年に発表した共通鍵方式の「MULTI2暗号」は，メインフレームからパソコンに至るまで，日立製作所が提案するセキュアシステムの共通技術基盤となっているほか，ネットワーク機器，ディジタル衛星放送システムなどの幅広い分野で用いられている。

また，今後の情報システムを支える基盤として，公開鍵暗号方式の「日立だ円曲線暗号“ELCURVE”」を開発して1997年7月に発表し，わが国で最初に製品化して同年9月に出荷した。これにより，電子商取引をはじめとする，インターネットを活用した，新しい社会システムの安全性を将来にわたって確保することが期待されている。

5　おわりに

ここでは，今後のイントラネット・インターネットシステムの発展の基盤となるセキュア システム ソリューションとセキュリティ技術・製品群について述べた。

企業での情報共有・情報発信や業務間連携による業務革新，家庭での新しいメディア配給インフラストラクチャー，社会での流通・金融・行政ネットワークサービスなどの実現と充実を目指し，今後もよりグローバルでシームレスなネットワークシステムのトータル 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。

参考文献

1) 川上，外：サイバスペース時代における経営および情報システムの新展開，日立評論，**79**，5，416～420(平9-5)
2) 佐々木，外：オープンネットワークにおけるセキュリティ技術，日立評論，**79**，5，459～464(平9-5)
3) 佐々木，外：インターネットセキュリティ，オーム社(1996)

執筆者紹介

金野千里
1977年日立製作所入社，情報事業本部 事業企画本部 システム製品企画部 所属
現在，セキュリティ関連製品の企画に従事
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@comp. hitachi. co. jp

角田光弘
1987年日立製作所入社，情報システム事業部 ネットワークシステム本部 企画部 所属
現在，イントラネット・インターネット ソリューション サービスの開発，拡販に従事
E-mail：tsunoda@system. hitachi. co. jp

久芳　靖
1988年日立製作所入社，ソフトウェア開発本部 計画部 所属
現在，セキュリティ関連製品ほかの製品企画に従事
E-mail：kubayasu@soft. hitachi. co. jp

手塚　悟
1984年日立製作所入社，システム開発研究所 セキュリティシステム研究センタ 所属
現在，セキュリティシステムの研究開発に従事
情報処理学会会員
E-mail：tezuka@sdl. hitachi. co. jp