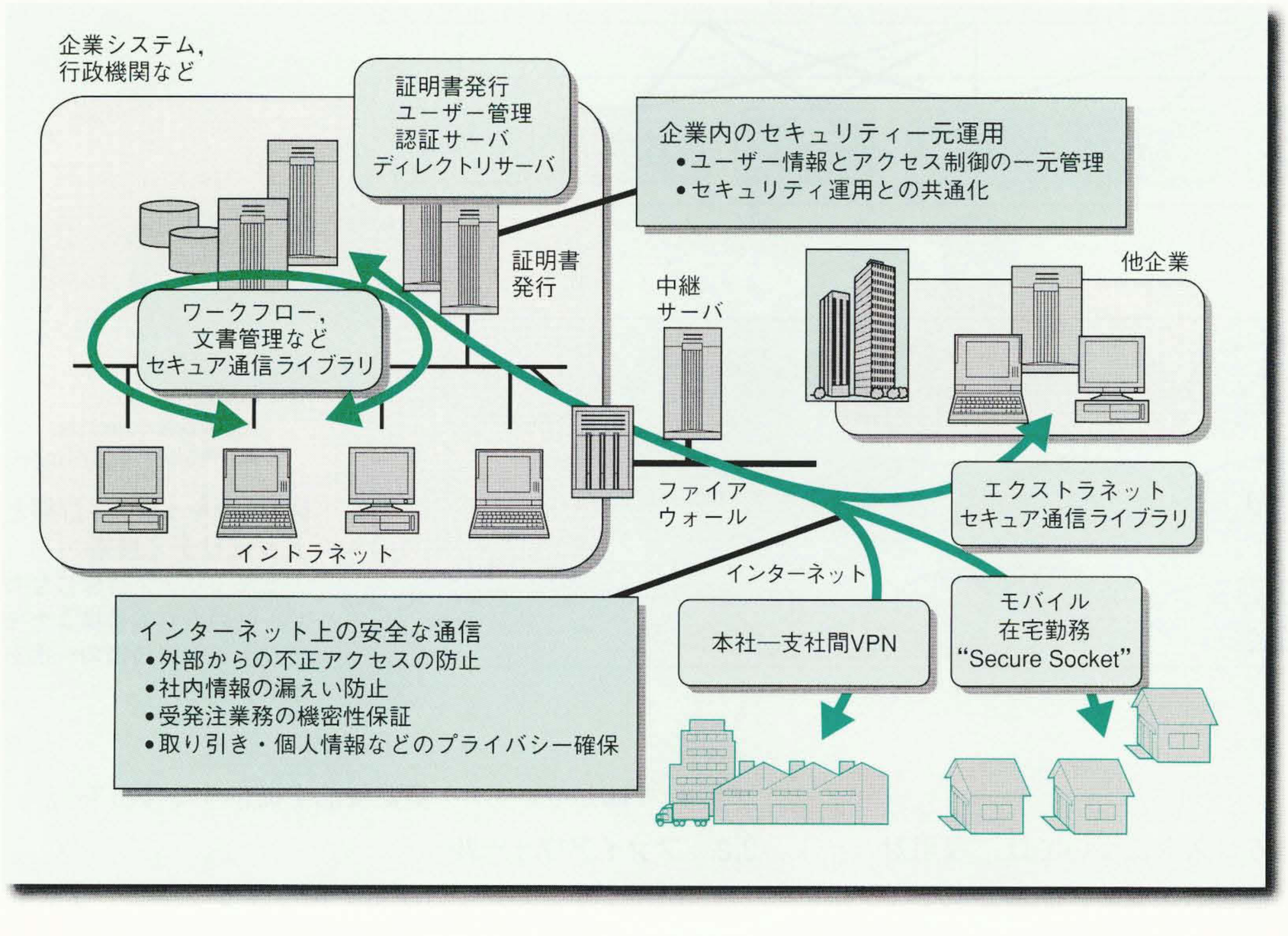
セキュアな情報システムを実現する Secureplazaのソフトウェア製品とその特徴

Software Products for Secured Information Systems

重田明男　*Akio Shigeta*　　池内　学　*Manabu Ikeuchi*
久芳　靖　*Yasushi Kuba*



注：略語説明
VPN（Virtual Private Network）

Secureplaza製品が支える情報システムセキュリティ

企業間や社会を結ぶシームレスで安全な情報システムを実現するために，Secureplaza製品は，システム形態や業務形態に適合したさまざまなセキュリティレベルの確保を可能にする。

最近のコンピュータネットワークの目覚ましい進展に伴い，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，そのオープン性やグローバル性と操作性などから，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）や企業—消費者間システム〔EC（Electronic Commerce：電子商取引）など〕へとその適用範囲を急速に拡大し，企業のビジネス形態を変ぼうさせつつある。一方，その利便性の裏側として，企業システムでは，情報の保護を目的としたシステム構築や，運用でのセキュリティ対策が重要なテーマとして注目されている。

日立製作所は，このような変ぼうを遂げつつあるコンピュータネットワークでのセキュリティ喪失への脅威の解決手段として，暗号技術を基盤としたネットワーク上のデータ保護やシステムのアクセス制御，さらに交信相手の認証などのセキュリティ製品を開発し，セキュリティサービスと合わせたセキュリティ トータル ソリューションを提案している。

1　はじめに

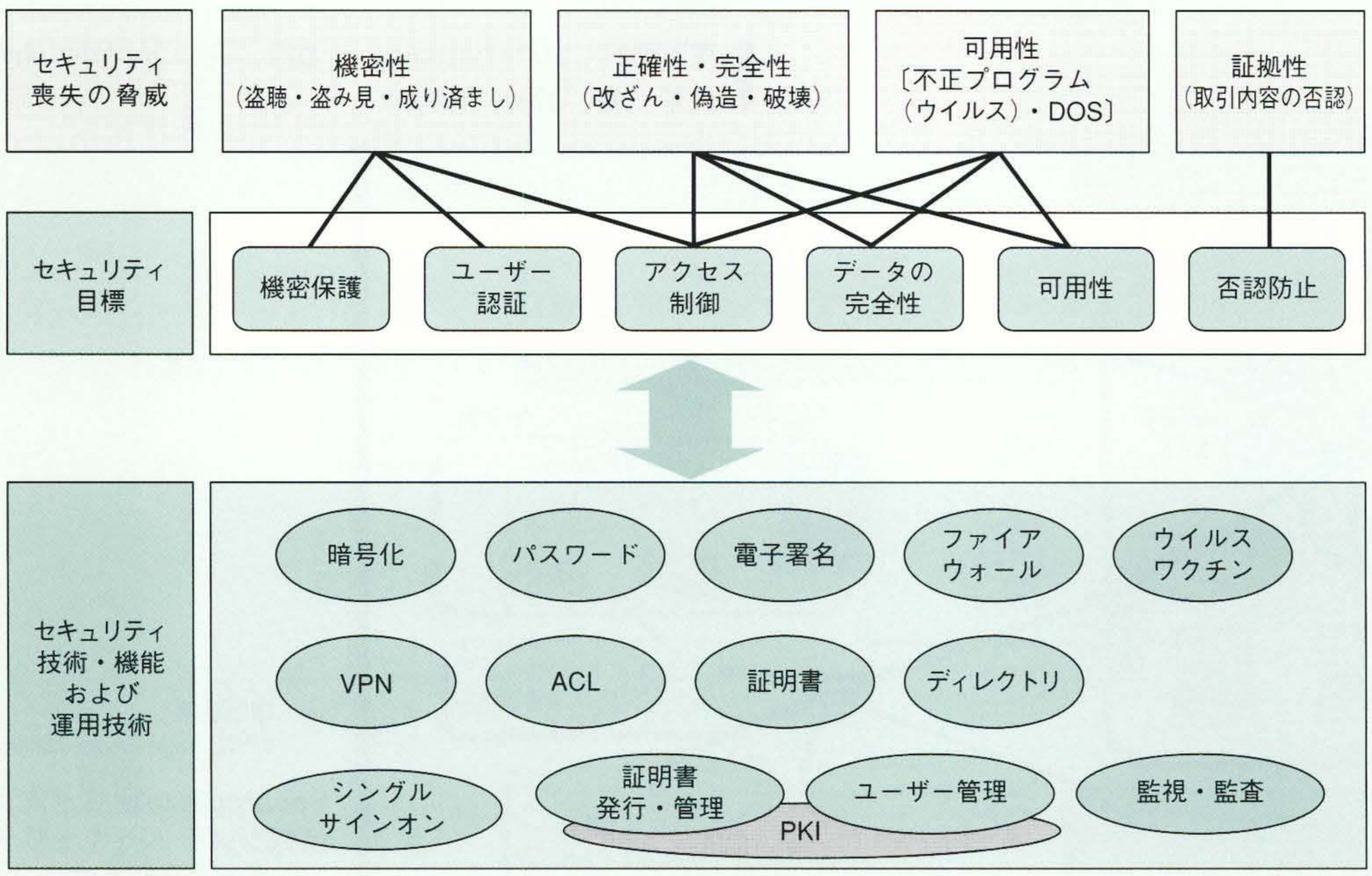
インターネット技術の発展に伴い，情報システムが急速に変ぼうしている。企業システムを例にとれば，Webによる情報共有・情報発信から始まって，グループウェア，DB（Database）アクセス，既存の基幹システムと連携したシステムへとその利用範囲が拡大し，企業でのビジネス形態も多様化している[1]。しかし，このインターネット技術の拡大による情報システムの変ぼうは，システム・情報へのセキュリティ保護を前提として存在しなければ，企業の存続にかかわる危険性をはらんでいる。

ここでは，変ぼうしつつある情報システムに対するセキュリティ喪失の脅威とその解決手段，それを実現するセキュリティ製品群と製品を支えるセキュリティ技術について述べる。

2　情報システムでのセキュリティ喪失の脅威と対策

2.1　セキュリティ喪失の脅威とセキュリティ目標

インターネット技術を活用した情報システムを構築するにあたっては，想定されるセキュリティ喪失の脅威を明らかにし，それらの脅威に対するセキュリティ目標を定め，目標を達成するために適切な技術・機能を選定するプロセス[2]が必要である（**図1**参照）。



注：略語説明
ACL(Access Control List)
PKI(Public Key Infrastructure)

図1 セキュリティ目標とセキュリティ技術

セキュリティ目標に合わせ，利用される多様なセキュリティ対策技術の一例を示す。

2.2 セキュリティ対策

セキュリティ対策にかけるコストについては，費用対効果を考慮する必要がある。必要な個所に必要な対策を施すことは重要であるが，必要なセキュリティレベルは，ネットワーク上を流れるデータの種類や不正利用によって想定される被害の度合いに応じて決める必要がある。

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)は悪くなる。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設計のポイントになる。

2.3 セキュリティの運用

セキュリティシステムを運用面から見たとき，個々のセキュリティ技術や機能を独立に実現するのではなく，PKIを中心とした，共通的なセキュリティ運用基盤の上に業務システムを構築することが必要である。さらに，管理者の運用コストだけでなく，利用者の利便性を考慮した，複数のアプリケーションの利用でも一度のパスワード入力で済む「シングルサインオン機能」の採用なども重要である。

3 セキュアシステムを支える基盤製品

3.1 Secureplazaでのセキュリティ基盤製品

情報システムで想定されるセキュリティ喪失の脅威に対するセキュリティ対策として，Secureplaza(セキュアプラザ)ではセキュリティ基盤製品を提供する(**表1**参照)。

3.2 ファイアウォール

今後の情報システムの構築では，インターネットを抜きにして考えることは難しい。このような，インターネットを含む環境で，外部の不正なアクセスから情報システム(サイト)を防御するのが「ファイアウォール」である。

ファイアウォールの基本的な役割は，外部(インターネット)との出入り口を1か所に絞ることにより，情報の流入出をコントロール(アクセス制御)することであり，コンピュータ室の入退室制限といった従来の物理的対策に相当する。また，アクセスのログを取得することにより，不正なアクセスがなかったかどうかを検証し，アクセス制御ルールの監査・検証を行うことができる。

アクセス制御では，組織のセキュリティポリシーに基づいて，だれにどの情報(サーバ)へのアクセスを許可するのかということを定義する。ネットワークレベルでは，発信IP(Internet Protocol)アドレス，着信IPアドレス，アクセスの方向性(外部に向けてか，外部からか)，プロトコル種別，ポート番号といった項目を設定することにより，アクセス制御を構築する。「Gauntletファイアウォール」のような，アプリケーションゲートウェイ型と呼ばれるタイプのファイアウォールでは，アプリケーション層に「プロキシー機能」と呼ばれるゲートウェイ機能を持たせることにより，プロトコルやデータ構造を意識した，よりきめ細かなアクセス制御が可能である。

表1　セキュリティ喪失の脅威に対するセキュリティ基盤製品
日立製作所はさまざまのセキュリティ喪失の脅威に対する製品をラインアップしている。

攻撃方法	セキュリティ上の脅威	対策項目	対応するSecureplaza製品
外部ユーザーによる不正アクセス	サーバへの不正侵入 データの盗難・破壊	サーバの保護 ネット上のアクセス制御	Gauntletファイアウォール*1, FireWall-1*2
	社内ユーザーへの成り済まし	厳密なユーザー認証	セキュリティライブラリ*3,*4, 認証サーバ*4
	不正侵入の見逃し	監査ログの追跡	JP1 Security Investigator
	ネット上の盗聴	データ暗号化	Secure Socket Serverシステム*3,*4, 仮想プライベートネットワーク支援機能 for Gauntlet
	データの改ざん	署名付き通信	セキュリティライブラリ
社内ユーザーによる不正アクセス	他人への成り済まし	ユーザー管理	Hitachi Directory Server JP1/User Administration
		ユーザー認証	認証サーバ, セキュリティライブラリ
	権限外のシステム, データ利用	アクセス制御	Hitachi Directory Server, CORBA Security Service
	機密データの漏えい	データ暗号化	Keymate/Crypto*3, セキュリティライブラリ　ほか
偶発的な攻撃・不正	コンピュータウイルス	ウイルスワクチン	Gauntlet，Groupmaxでのワクチンソフトウェア連携
	悪質なWebコンテンツ	コンテンツフィルタリング	Gauntletファイアウォール

注：＊1　Gauntletは，米国Network Associates, Inc.の商標である。
＊2　FireWall-1は，CheckPoint Software Technologies, Ltd.の商標である。
＊3　Keymate/Crypto，セキュリティライブラリ，Secure Socket Clientは，情報処理振興事業協会(IPA)が推進する「創造的ソフトウェア育成事業」の一環として技術開発された内容を含んでいる。
＊4　認証サーバ，セキュリティライブラリ，Secure Socket Clientは，情報処理振興事業協会(IPA)が推進する「エレクトロニック・コマース推進事業」の一環として技術開発された内容を含んでいる。

さらに，組織内のネットワークをプライベートアドレスとインターネットのグローバルアドレスに使い分けるためのNAT(Network Address Translation：ネットワークアドレス変換)機能を利用することにより，組織内のネットワークアドレスを外部ネットワークから隠ぺいすることが可能である。

これらのネットワークレベルのアクセス制御機能に加え，「Gauntletファイアウォール」と“FireWall-1”は，有害なプログラムがコンテンツ(情報の内容)の形で侵入するのを防止するための「Javaアプレット」※1)や「ActiveXコントロール」※2)のフィルタリング機能と，ウイルス ワクチン ソフトウェアと連携したコンピュータ ウイルス フィルタリング機能も持ち，これらの機能で多様化するセキュリティ喪失の脅威に柔軟に対応することなど，常にエンハンスが加えられている。

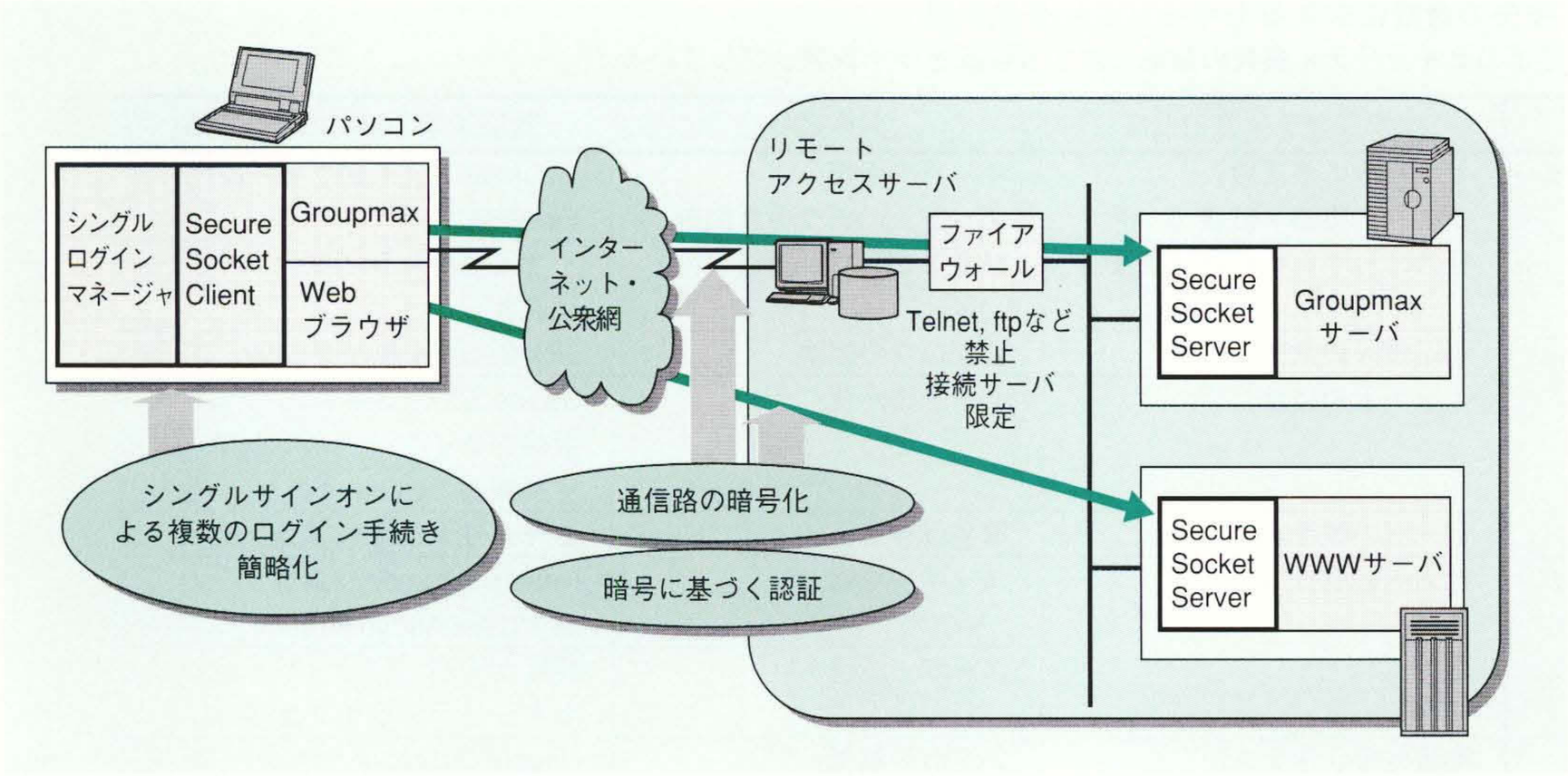
※1) JavaおよびすべてのJava関連の商標およびロゴは，米国およびその他の国における米国Sun Microsystems, Inc.の商標または登録商標である。
※2) ActiveXは，米国およびその他の国における米国Microsoft Corp.の商標である。

3.3　VPN機能

VPNは，二つのネットワーク間や2地点間の安全な通信路として，インターネットや公衆網を利用するための技術である。暗号化技術を用いてプロトコル上のデータをカプセル化して相手に送信することにより，セキュリティが保たれていないネットワークを経由する場合でも，安全な通信路を確立することができる。

日立製作所は，Gauntletファイアウォールにアドオンして利用できる「仮想プライベートネットワーク支援機能 for Gauntlet」と，ファイアウォールとは独立して運用が可能な「Secure Socket Serverシステム」という二つのタイプのVPN製品を提供している。どちらもTCP(Transmission Control Protocol)レイヤとアプリケーション層の間に位置するソケットでアプリケーションデータをカプセル化して中継する方式を採用しているため，VPNを利用した通信を行う場合でも，外部に対して内部ネットワークを隠ぺいできるという特徴がある。さらに，暗号アルゴリズムとして日立製作所が開発した「MULTI2暗号」[3]を利用しているので，VPN製品としてトップレベルの暗号強度を持つ。

ファイアウォールとは独立に構成できる「Secure



注：略語説明
WWW(World Wide Web)

図2 リモートアクセス環境でのVPN機能の活用
VPN機能を活用することにより，モバイルやSOHOでのリモートアクセス環境で高度のセキュリティを実現する。

Socket Serverシステム」は，モバイルやSOHO(Small Office, Home Office)に対応して運用する，公衆網を利用したリモートアクセス環境の構築(**図2**参照)や，異なるファイアウォールを運用する企業間でのエクストラネットの構築ができるほか，X.509公開かぎ証明書(後述)を利用したICカードによるユーザー認証ができるなど，今後のビジネス形態にいち早く対応した製品である。

3.4 セキュリティ共通運用基盤

情報システムのセキュリティ対策を個々のシステムやアプリケーションごとに進めていくと，セキュリティレベルのばらつきが生じるほか，ユーザー管理や認証情報管理，暗号かぎ管理といった面での運用コストが増大する。ユーザー管理と公開かぎ証明書の発行・運用管理を一元的に行うことによってセキュリティ運用コストの低減とセキュリティ方針の統一的な実施をねらいとしているのが，“PKI”と呼ばれる公開かぎ運用基盤である。PKIは，LDAP(Lightweight Directory Access Protocol)に基づくディレクトリサービスや，X.509公開かぎ証明書といったインターネット標準技術をベースに運用できることから，EC(Electronic Commerce：電子商取引)などのインターネット対応システムですでに標準的に採用されているほか，今後は，イントラネットでのセキュリティ共通運用基盤の機能を持つようになるものと予想する。

3.4.1 ユーザー管理

ディレクトリサービスは，システム運用のための情報を統合管理し，ミドルウェアやアプリケーションからその情報の高速検索・参照を可能にする技術であり，インターネット技術としては，IETF(Internet Engineering Task Force)でLDAPとして標準化されている。ディレクトリサービスでは，アクセスプロトコルだけでなく，ディレクトリで管理する対象データ定義も標準化されているので，製品間での相互運用性に優れている。

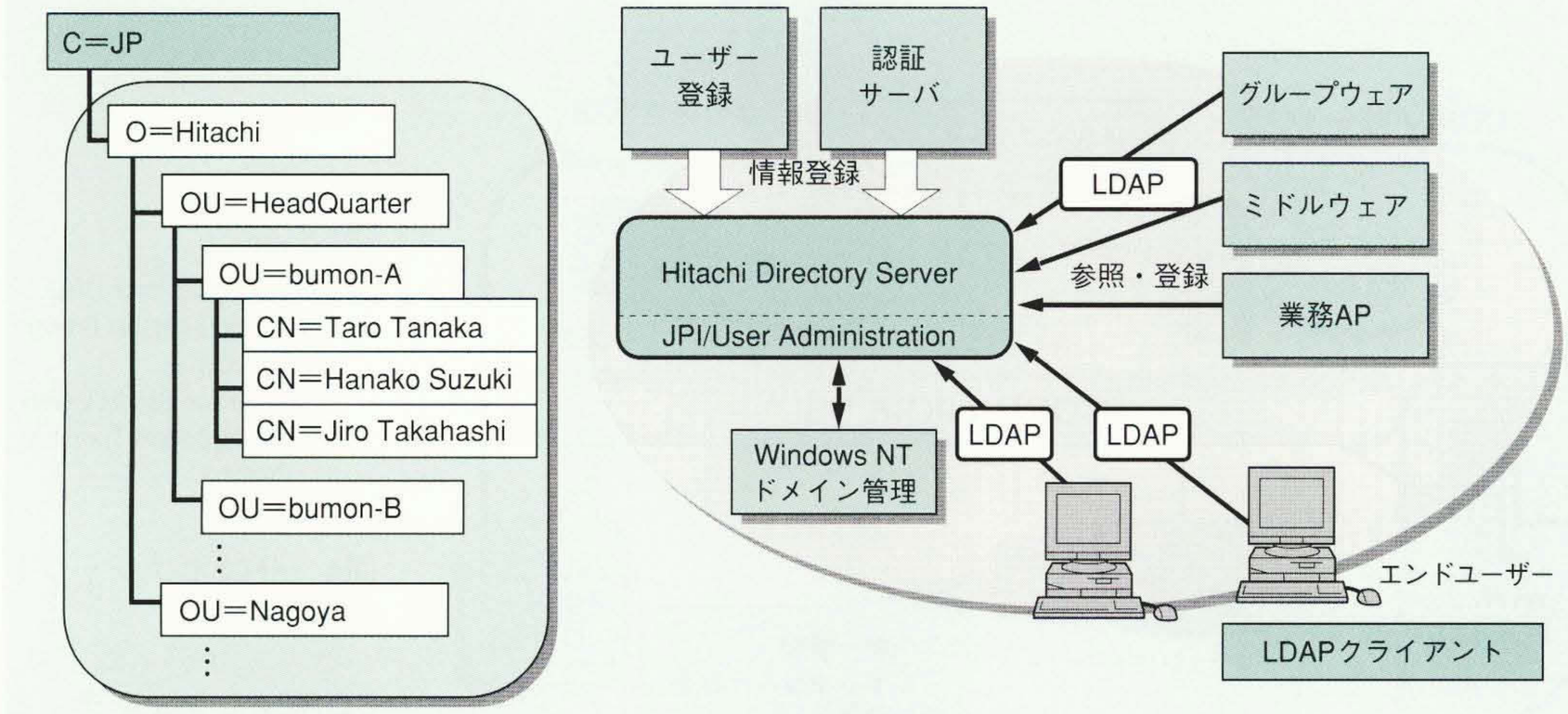
ディレクトリサーバには，メールやグループウェアで参照するメールアドレスのほか，セキュリティ運用で利用される公開かぎ証明書，アクセス制御に必要となる所属・役職などの情報を格納することができる。また，属性の拡張により，ユーザーグループなどを定義することも可能である。これらのユーザー情報を，各ミドルウェアやアプリケーションごとではなく，ディレクトリで一元管理することにより，管理コストの低減を実現することが可能となる。

“Hitachi Directory Server Version 2”では，さらに，認証サーバと連動した公開かぎ証明書の格納やユーザーグループ定義機能などのセキュリティ運用のための機能のほかに，米国Netscape Communications社のディレクトリサーバ製品との相互運用性，日立製作所のスケーラブルデータベース“HiRDB”を利用した信頼性向上のためのオプション機能などを持たせている。また，JP1/User Administrationを使用すれば，Windows NT※3)やGroupmaxで管理するユーザー情報と相互に同期をとる機能により，ユーザー管理の利便性をいっそう高めている(**図3**参照)。

3.4.2 電子証明書によるユーザー認証

ユーザー認証には，長い間パスワードが広く利用され

※3) Windows NTは，米国およびその他の国における米国Microsoft Corp.の登録商標である。



注：略語説明
AP（Application Program）

図3　ディレクトリを利用したユーザー管理
LDAP環境と既存業務AP（非LDAP）環境で，ユーザー管理を統合することができる。

てきた。しかし，インターネットのようなセキュリティ面で不安定なネットワークを経由する場合には，固定的なパスワードによるユーザー認証は，盗聴や成り済ましといったセキュリティ喪失の脅威に対して無防備である。そのため，ワンタイムパスワードや暗号技術を利用した，より安全な認証方法が必要となる。その中でもインターネット技術をベースとするのが，公開かぎ証明書を利用した認証方法である。

公開かぎ証明書は，認証サーバ（認証局）が発行するディジタル証明書であり，本人だけが知りうる秘密かぎの情報と組み合わせて利用することにより，同期型の接続でも，メールのような非同期型のシステムでも，ユーザー認証（発信者の認証）を確実に行うことが可能となる。

日立製作所の「認証サーバ」では，企業などの組織内でこの公開かぎ証明書を発行，運用することができる。また，Hitachi Directory Serverとの連動により，ユーザー管理と連動したセキュリティ運用基盤が確立できるほか，「セキュリティライブラリ」を利用することにより，証明書に基づくセキュリティ運用やメッセージの暗号・復号化処理を提供し，セキュアなアプリケーションの構築を可能としている。さらに，ファイル暗号化機能により，ファイル署名を利用した，ファイルへのアクセス制御が実現できる。

3.4.3　シングルサインオン

日立製作所のディジタル証明書による認証やディレクトリサービスを利用すれば，エンドユーザーが複数のアプリケーションを利用するたびにパスワードを入力しないで済む「シングルサインオン」環境を構築することができる。また日立製作所は，ディジタル証明書やディレクトリサービスに対応していない，既存のアプリケーションを含むシングルサインオンを実現するための「シングルログイン マネージャ」を提案している（**図2**参照）。さらにICカードと組み合わせることにより，いっそう強固で使いやすいユーザー認証システムを構築することができる。

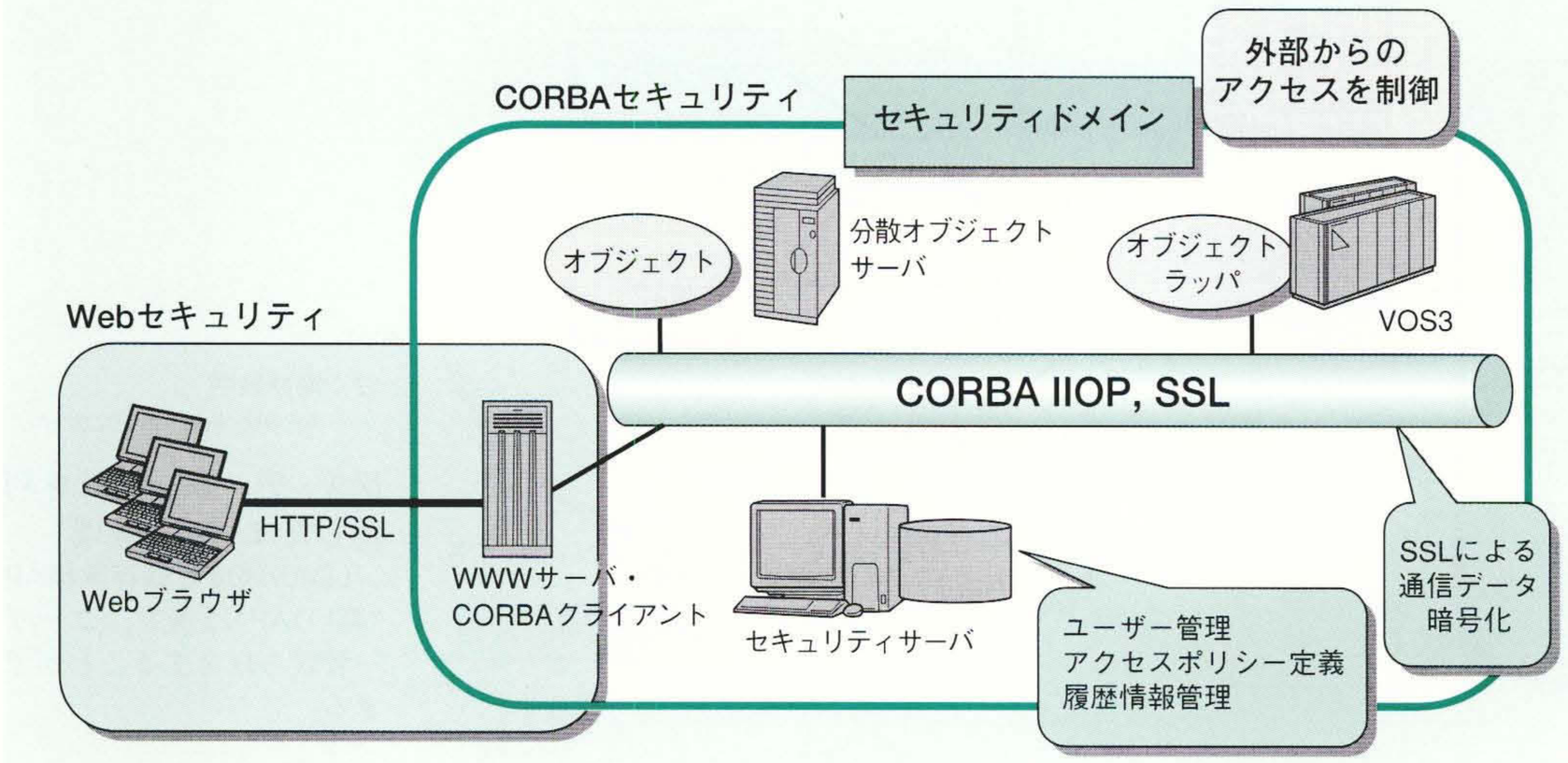
3.5　セキュリティ機能を支える暗号技術

日立製作所は，各種のセキュリティ技術や，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年代初頭から取り組んでいる。1989年に発表した共通かぎ方式の「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，ネットワーク機器や衛星放送システムなどの幅広い分野で実際に用いられている。

また，今後の情報システムを支える基盤として，公開かぎ暗号方式の「だ円曲線暗号」[3]を開発し，1997年7月に発表した。これをさらに発展させてEC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していく考えである。

4　今後の課題

Network Objectplaza[4]による分散オブジェクト型システム構築の中核を成すCORBA（Common Object Request Broker Architecture）環境に対しても，日立製作所は，OMG（Object Management Group）が提唱する“CORBA Security Service”に標準準拠した“Security Service”を提案した。分散オブジェクト環境では，シームレスなオブジェクト間接続が構築できるという利便性がある反面，だれでもオブジェクトを透過的に参照できるというセキュリティ上の課題があり，“Security



注：略語説明
IIOP〔Internet Inter-ORB (Object Request Broker) Protocol〕
SSL(Secure Socket Layer)
HTTP(Hypertext Transfer Protocol)

図4　分散オブジェクトセキュリティ
セキュリティにより，CORBAセキュリティとWebセキュリティの連携が拡大していく。

Service"はこれを解決する。CORBAセキュリティドメインを構築することにより，ドメイン内のユーザー管理やユーザー認証，アクセス制御，暗号通信などの各種のセキュリティ機能をセキュリティサーバで統合的に運用できるほか，ドメイン内のオブジェクトへのドメイン外からのアクセス制限や，ドメインのセキュリティ方針に基づくアクセス履歴の取得が可能である(**図4**参照)。

今後の情報システムの課題としては，分散オブジェクト環境と既存のクライアントサーバ環境で，システム連携上のシームレスなセキュリティシステムを提供することがあげられる。

5　おわりに

ここでは，インターネット技術を用いた企業情報システムでの，セキュリティ脅威に対する解決手段としてのセキュリティ技術と製品について述べた。

急速に変ぼうする社会情勢に合わせて，情報ネットワークも急激な変化を遂げつつあり，セキュリティ喪失への脅威は多様化している。今後も，Secureplazaでは，セキュリティ技術をセキュリティソリューションとしていち早く製品化し，提案していく考えである。

参考文献

1) 佐々木，外：インターネットセキュリティ，オーム社(1996)
2) 金野，外： セキュア システム ソリューションとセキュリティ技術，日立評論，**80**，5，397～402(平10-5)
3) 佐々木，外：電子商取引を支える基本技術，bit，No.391，65～74，共立出版(1999-4)
4) 斉藤，外：これからの情報システム"Network Object-plaza"，日立評論，**80**，5，391～396(平10-5)

執筆者紹介

重田明男
1981年日立製作所入社，情報・通信グループ ソフトウェア事業部 基本ソフトウェア本部 第4OS設計部 所属
現在，セキュリティ関連製品の開発・拡販に従事
E-mail：shigeta @ soft. hitachi. co. jp

久芳　靖
1988年日立製作所入社，情報・通信グループ ソフトウェア事業部 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

池内　学
1981年日立製作所入社，情報・通信グループ ソフトウェア事業部 基本ソフトウェア本部 第4OS設計部 所属
現在，セキュリティ関連製品の開発に従事
E-mail：ikeuchi @ soft. hitachi. co. jp