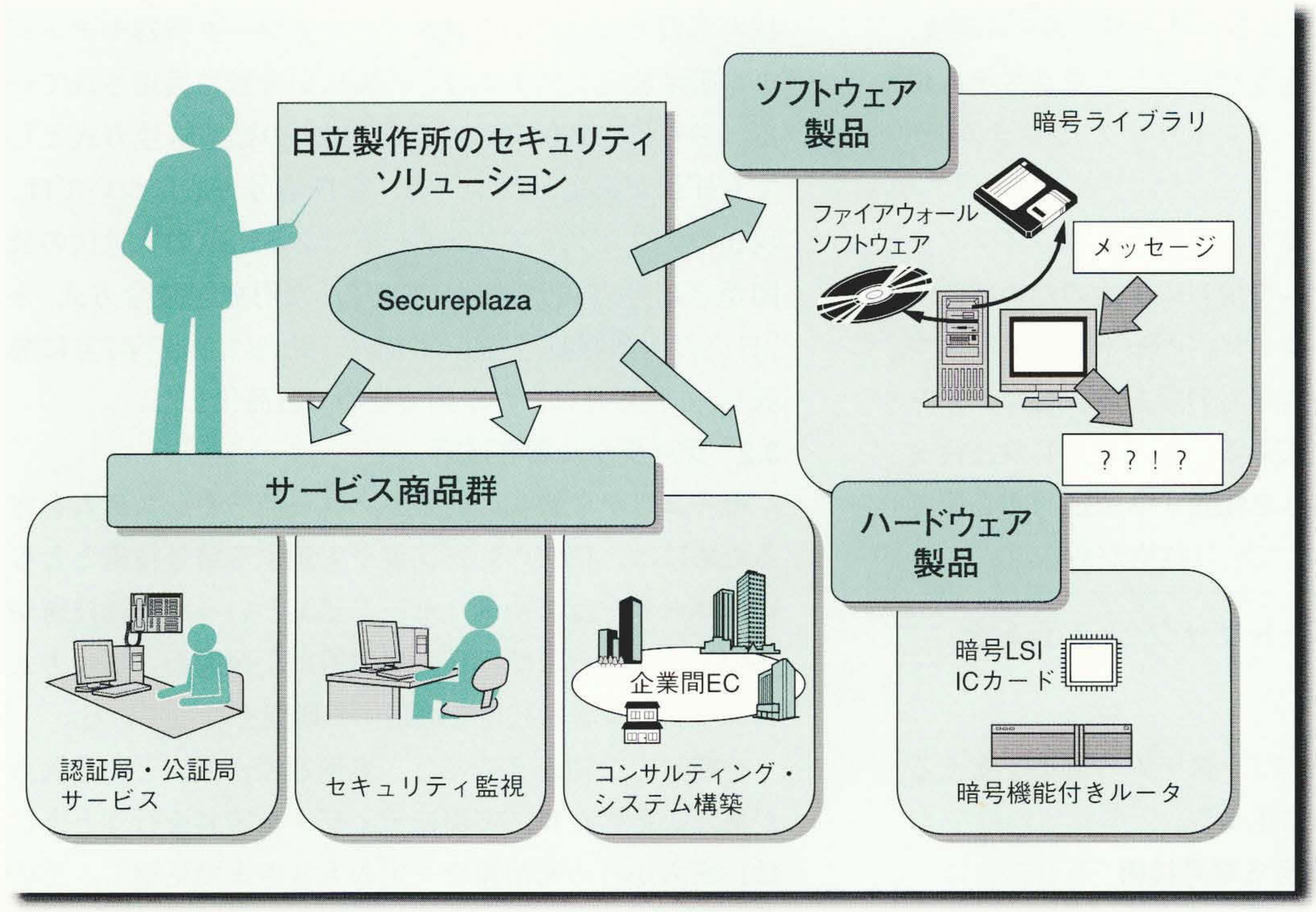
情報技術におけるセキュリティ セントリック システム

Security Centric Systems as an Information Technology

手塚　悟　*Satoru Tezuka*　　光永　聖　*Satoshi Mitsunaga*
中上昇一　*Shôichi Nakagami*　　北嶋弘行　*Hiroyuki Kitajima*



注：略語説明
EC（Electronic Commerce；電子商取引）

「セキュリティ セントリック システム」を実現するためのセキュリティ ソリューション“Secureplaza”の構成

Secureplazaは，日立製作所のトータルセキュリティ技術のソリューションを示すものである。

インターネットの世界的な普及に伴い，インターネットを利用した多種多様なビジネスが提案されるようになった。特に，企業ー消費者間EC(Electronic Commerce：電子商取引)や企業ー企業間ECはその代表的なものであり，社会の仕組みとして認知されつつある。このように，インターネットは，オープンでかつグローバルなネットワーク環境を提供し，高度情報化社会を構築するものと期待されている。これらの環境を実現するためには，インターネットに接続されたシステムや情報の保護を目的とした，高度なセキュリティ(安全性)技術を駆使した「セキュリティ セントリック システム」が不可欠である。

暗号を基盤としたセキュリティ技術は，公開かぎ暗号ベースのディジタル署名を用いた認証技術により，データの改ざんや成り済ましの防止，および安全なかぎの配布を実現している。

日立製作所は，インターネットでのビジネスを展開するにあたり，セキュリティソリューションとして“Secureplaza”を提案し，セキュリティ セントリック システムを支える暗号などの基盤技術の研究開発，さらに，これらの基盤技術を駆使して，電子認証公証システムや企業間ECなどの応用システムの研究開発に取り組んでいる。

1　はじめに

オープンでかつグローバルなインターネットの急激な普及とともに，その環境下での多種多様なビジネスが提案されている。EC(Electronic Commerce：電子商取引)を例にとれば，消費者対応，企業対応ビジネスがともに急速に立ち上がっており，ソフトウェアや旅行，自動車などの幅広い商品がネット上での取引シェアを拡大している。このような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(安全性)保護が前提になって初めて可能となる。

日立製作所は，このようなインターネット環境ではセキュリティ技術がますます重要になるとの認識の下に，セキュリティソリューションとして“Secureplaza”を提案している。

ここでは，このインターネット上でのビジネスを展開していくにあたって必要とされる，高度なセキュリティ技術を駆使したセキュリティ セントリック システムの基盤技術と，その技術を活用した応用システムについて述べる。

2 セキュリティ セントリック システムの概要

インターネット技術は，今日の企業情報システムに対して，「イントラネット」という環境を提供している。ここでは，これまでのクライアント—サーバシステム環境，さらに分散オブジェクト技術をベースとしたシステム環境も包含する「セキュリティ セントリック システム」が必要とされている。

このセキュリティ セントリック システムは，インターネットに接続されるシステムや情報の保護のために，サービスやシステム，ソフトウェア，ハードウェアなどすべての商品や製品に展開されるものである。特に，インターネット上でのECを考えてみると，主要な基盤技術としては，セキュアな取り引きを保証する認証局が必須であり，これらの基礎技術として暗号技術がある。

3 セキュリティ セントリック システムを支える基盤技術

セキュリティ セントリック システムの構築を支える主要基盤技術について以下に述べる。

3.1 セキュリティ機能を支える暗号技術

暗号方式のうち，共通かぎ暗号方式“DES(Data Encryption Standard)”と公開かぎ暗号方式“RSA(Rivest, Shamir, Adelman)”が，ECで使われる暗号方式の事実上の世界標準(デファクトスタンダード)になっている。

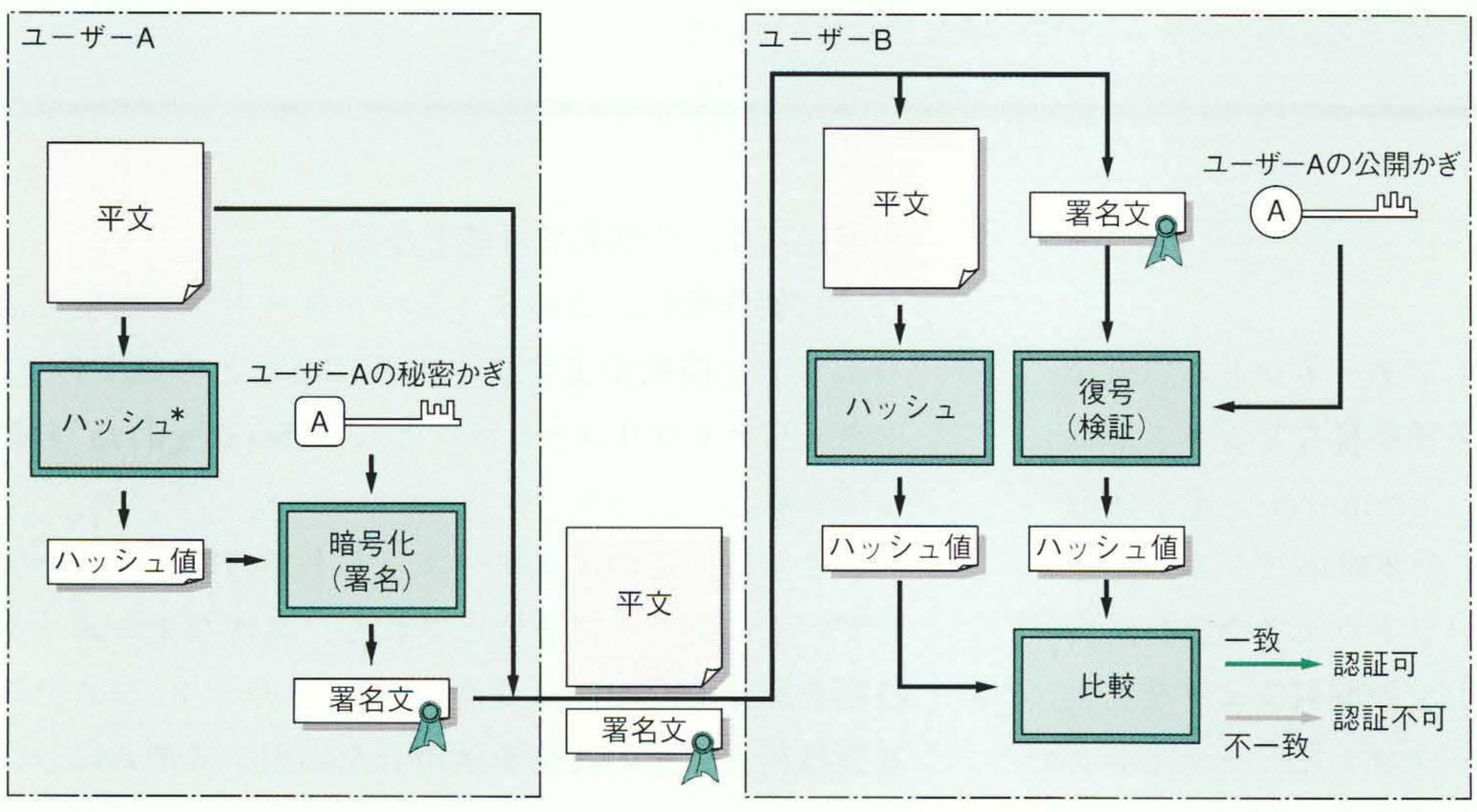
これに対して日立製作所は，セキュリティ技術・セキュリティ製品・セキュリティ商品の基礎技術である暗号技術に1980年代の初めから取り組んでいる。1989年にはDESよりも安全性の高い共通かぎ方式の「MULTI2暗号」を発表した。この暗号は，メインフレームからパソコンに至るまで，日立製作所のセキュリティシステムの共通技術基盤となっているほか，ネットワーク機器やディジタル衛星放送システムなどの幅広い分野に適用されている。さらに，1998年にはIEEE1394の標準暗号方式としても採用が決定した。一方，公開暗号方式については，現在のデファクトスタンダードであるRSAの次世代の公開かぎ暗号方式と言われている「だ円曲線暗号方式」を「日立だ円曲線暗号“ELCURVE”」として1997年7月に発表し，同年9月に，わが国で初めて製品化した。

3.2 ディジタル署名技術

セキュリティ喪失の脅威からユーザーやシステムを守るためには，情報の秘密保護や実現する暗号技術とともに，ユーザー認証やメッセージ認証といった認証技術が必要である。そこで，日立製作所は，公開かぎ暗号方式にディジタル署名技術を適用する研究を行っている。

一般に，公開かぎ暗号は，処理速度が遅いという欠点がある。そのため，実際にディジタル署名を行うときには，あらかじめ元情報を一定の大きさまで圧縮し，その圧縮結果に対して署名をするようにした(**図1**参照)。

ユーザーAがユーザーBに署名付き情報を送る場合，ユーザーAは自分の秘密かぎで平文のハッシュ値を暗号化し，平文と暗号文(署名文)とを組にしてユーザーBに送る。ユーザーBは，受け取った署名文をユーザーAの公開かぎで復号し，その復号結果とユーザーAから受け取った平文とを比較する。それら二つのデータが一致し



注：＊ハッシュとは,データの高速読み出しの方法を意味する。

図1 ディジタル署名の手順
公開かぎを利用したディジタル署名の手順を示す。
インターネット上での目に見えない相手の確実な認証と送られてきた内容の改ざんを防止することができる。

ていれば，受け取った署名文はユーザーAの秘密かぎで暗号化されていることになる。ユーザーAの秘密かぎを知っているのはユーザーA本人しかいないはずなので，ユーザーBは，ユーザーAが署名したということ(ユーザー認証)と，平文が何ら改ざんされていないということ(メッセージ認証)を検証することができる。ただし，上記の手順では，平文の機密性については考慮していない。機密情報に署名を施す場合などでは，平文の暗号化も別途行う必要がある。

4 セキュリティ セントリック システムに基づく応用システム

前章で述べたセキュリティ セントリック システムの基盤技術を駆使した，特に重要な応用サービスシステムとして，電子認証公証局と企業間ECサービスについて以下に述べる。

4.1 電子認証公証局

ECの普及・発展には，セキュリティの確保が必須である。セキュリティ機能の一つとして，取り引きをしようとする相手が，自分が意図し，また名乗っているとおりの相手かを確認する「本人確認」の機能がある。ECでは，暗号技術を利用して，公開かぎ証明書とディジタル署名を組み合わせて本人を確認する方式を適用する。

この場合，公開かぎの所有者がだれであるかを，公開かぎの使用者に証明する「認証」が必要になる。この認証行為を行う機関が，CA(Certification Authority：認証局)と呼ぶTTP(Trusted Third Party：信頼できる第三者機関)であり，CAが発行する公開かぎ証明書を認証書(Certificate)と言う。この枠組みは，ITU(国際電気通信連合)の勧告X.509で規定されている。

日立製作所は，利用が想定される金融機関や関連するベンダ約50社とともに，日本認証サービス株式会社(JCS)を設立し，1997年10月からサービスを開始した。JCSは，認証書発行サービスを複数企業に提供するため，高い信用力とともに社会的な中立性が求められている。

一方，電子認証システムが，「だれと」「だれが」電子商取引を行ったのかということを証明するシステムであるのに対して，電子公証システムは，「いつ」「どのような内容の」電子商取引を行ったのかということを証明するシステムである(**図2**参照)。

4.2 企業間ECサービス

日立製作所は，企業間ECを支援する会員制サービス「企業間ビジネス メディア サービス“TWX-21(Trade Wind on Extranet-21)”」を，1997年10月から開始している(**図3**参照)。

TWX-21では，企業間の電子商取引全般にわたる一貫したアプリケーションと，会員間の自由な取り引きを実現する取り引きの場を提供しており，企業活動のマーケティング，設計，製造，検査，販売，物流，支払い，保守，廃棄という一連の業務にかかわる各種サービス機能を順

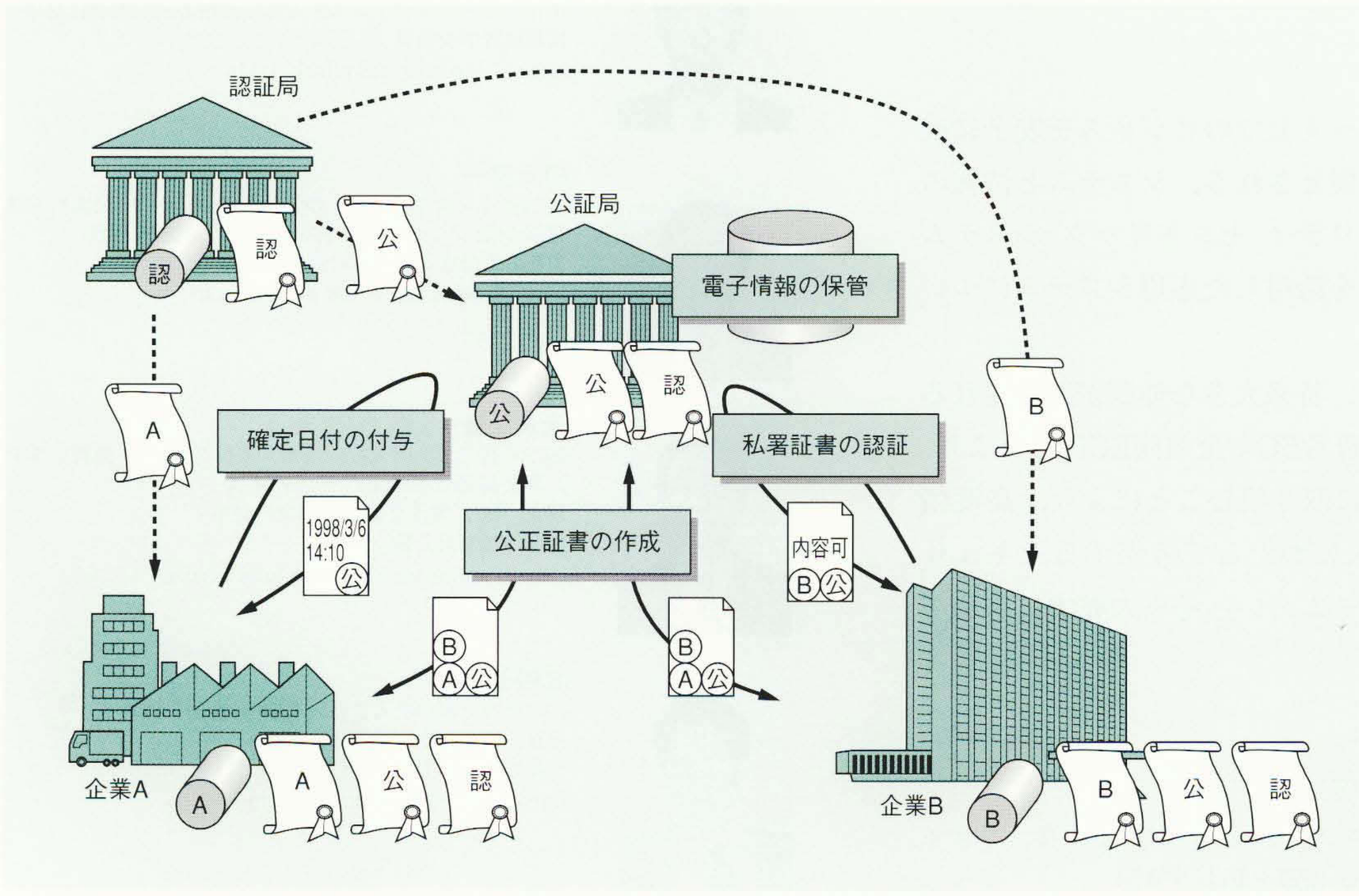


図2 「電子公証システム」の仕組み

電子公証システムの機能と処理手順を示す。電子公証の利用者(企業A，企業B)は事前にみずからの認証書を取得する(点線矢印)。

その上で，公証局に依頼する内容(確定日付の付与など)に応じて公証局や取り引き相手の認証書を利用する(実線矢印)。

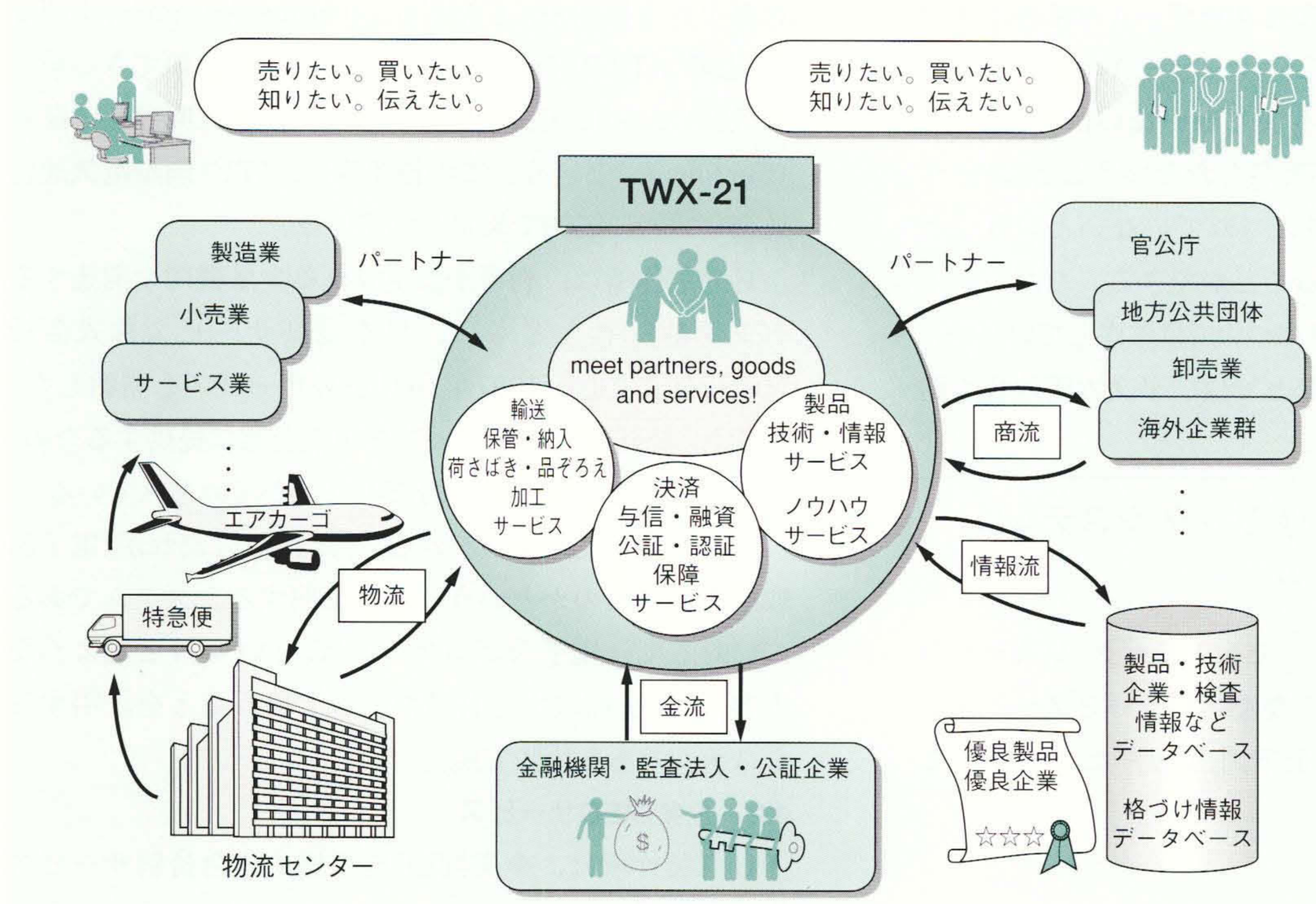


図3　企業間ビジネス メディア サービス“TWX-21”の機能概要

企業間の電子商取引を実現するサービスとして，TWX-21会員間の，セキュアでかつ自由な商取り引きを可能とする取り引きの場を提供する。

次提供していく予定である。

TWX-21センタに設置した各種のビジネス アプリケーション サーバと，取り引きを公正，正確，安全，高効率に進めるためのMC(Master of Ceremonies)サーバの構成でサービスを提供し，前章で述べた暗号技術やディジタル署名技術などの基盤技術を駆使したセキュリティ セントリック システムを構築している。

5　おわりに

ここでは，インターネット上でのビジネスを安全に展開していくにあたって必要とされる，システムと情報の保護を目的としたセキュリティ セントリック システムの基盤技術と，その技術を活用した応用システムについて述べた。

日立製作所は，今後も，将来大きな伸びが期待されるインターネット上での消費者ECや企業間ECはもとより，公共分野ECにも積極的に取り組むことにより，高度情報化社会の安全性を将来にわたって確保するセキュリティ セントリック システムのいっそうの充実に努めていく考えである。

参考文献

1) 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)
2) 佐々木，外：インターネットセキュリティ，オーム社(1996)
3) 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)

執筆者紹介

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応用技術の研究開発に従事
情報処理学会会員
E-mail：tezuka @ sdl. hitachi. co. jp

中上昇一
1979年日立製作所入社，情報・通信グループ 公共情報事業部 官公システム本部 官公システム第五部 所属
現在，官公庁システムの開発に従事
E-mail：nakagami @ jkk. hitachi. co. jp

光永　聖
1979年日立製作所入社，情報・通信グループ 情報システム事業部 商品開発第二センタ 所属
現在，EC，電子認証局の開発に従事
情報処理学会会員
E-mail：mitunaga @ system. hitachi. co. jp

北嶋弘行
1971年日立製作所入社，企業間EC推進本部 所属
現在，TWX-21の研究開発に従事
情報処理学会会員，IEEE会員
E-mail：kita @ ebs. hitachi. co. jp