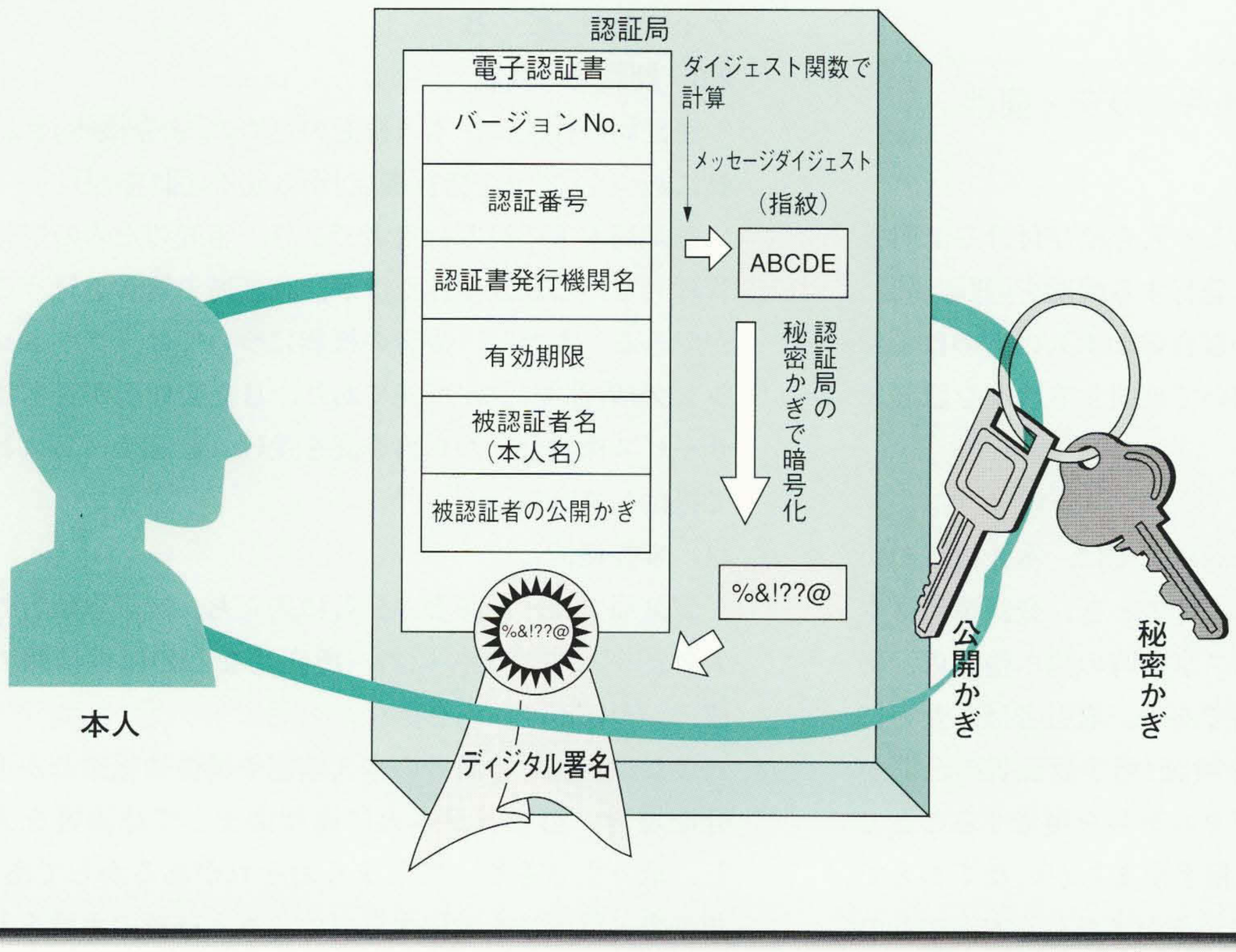
セキュア エレクトロニック コマースを支える認証サービス

Certificate Service for Secure Electronic Commerce

滝田誠一郎　*Seiichirô Takita*　森山将治　*Shôji Moriyama*
田川　豊　*Yutaka Tagawa*　米田英央　*Hideo Yoneda*



電子認証書の役割

認証局の発行する電子認証書は，本人と，本人の持つかぎペアの一つである公開かぎを結び付ける役割を持つ。電子認証書には，認証局のディジタル署名が付与されている。

インターネットの世界的な普及とイントラネット・エクストラネットの進展に伴い，インターネットを利用した多種多様なビジネスが急速に商用化，実用化されつつある。特に，企業一消費者間EC(Electronic Commerce：電子商取引)や企業一企業間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。しかし，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技術が必要である。暗号を基盤としたセキュリティ技術は，暗号による盗聴防止と，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，および安全性の高い電子認証書(公開かぎ)の配布を実現している。

電子認証書は，認証局の秘密かぎによってディジタル署名が付与されており，電子認証書の真正性は，このディジタル署名を検証することで確認することができる。もし仮に認証局の秘密かぎが漏えいした場合，不正者によって偽りの電子認証書が作成可能となり，今まで発行した認証書，ひいては電子認証書に基づいた電子商取引すべてが信用できないものとなる。こうしたことから，公開かぎ基盤の中核を成す認証局のセキュリティがきわめて重要となる。

日立製作所は，SET(Secure Electronic Transaction)認証局で，VISA International社とMasterCard International社のセキュリティ監査を受査した。今後，“SECE(Secure Electronic Transaction/Secure Electronic Commerce Environment)”や“SSL”，“S/MIME”など，さまざまな分野の認証局・公証局にこのセキュリティ技術を適用し，安全性の高い認証サービスを提案していく。

1　はじめに

日立製作所は，インターネット環境での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，消費者EC(Electronic Commerce：電子商取引)と，企業間ECのセキュリティ基盤となる「認証局」を構築した。特に消費者ECについては，1997年10月に，日本認証サービス株式会社から電子認証書発行サービスを受託し，提供している。

インターネット上での電子商取引で，目に見えない相

手が本当に正しい取引相手であることを信用する最も安全な手段が，公開かぎ基盤に基づいた認証局の発行する電子認証書を用いる方法である。

ここでは，セキュア エレクトロニック コマースを支える認証局の役割と，認証局にかかわるセキュリティ技術について述べる。

2　認証局の必要性とセキュリティ要件

2.1　認証の定義

公開かぎとその持ち主である本人を結び付ける証明書を「認証書」と言い，認証書を発行する機関を「認証局」と言う。言いかえれば，公開かぎ自体が本人のものにまちがいないことを，認証書を用いて証明する機関を認証局という。

2.2　役　　割

インターネット上での電子商取引では，本人認証のためにディジタル署名を用いる。このとき，登録情報は本人の公開かぎであり，サービス享受時の提示情報は，秘密かぎによるディジタル署名である。取引者は，互いに取引相手のディジタル署名を検証(相手認証書の公開かぎにより，取引相手のディジタル署名を復号することで検証)することによって取引相手がまちがいなく本人であることを確認するが，公開かぎがまさしく本人のものであることが保証されないと，正しい本人認証とは言えない。

ディジタル署名を用いる本人認証では，本人認証の確実性は，公開かぎの持ち主を証明する認証書と，さらにそれを発行する認証局の信頼性，言いかえるとセキュリティにかかっている。

2.3　認証局の機能

認証局の機能は，本人確認のための「審査機能」と，それに基づく「認証書発行機能」から成る(**図1**参照)。

認証局本来の役割は前者であり，審査のための情報を管理している認証主体だけが，認証局の運営を行うことができる。ただし，後者の機能については，アウトソーシング(外部委託)が可能であり，日立製作所が日本認証サービス株式会社から再委託を受け，認証サービスとして提供している。

(1)　審査機能

認証局では，認証書の発行に先立ち，認証申請者の本人確認や，申請者の氏名，所在地などの属性情報の確認，いわゆる「審査」を行う。

これは，認証申請者の本人確認や属性情報確認が不十分な場合，第三者が本人に成り済まして認証書を入手し，取り引きを行ってしまうおそれがあるからである。認証書の信頼性を確保するには，本人確認の手段をどのように講じるかが重要である。

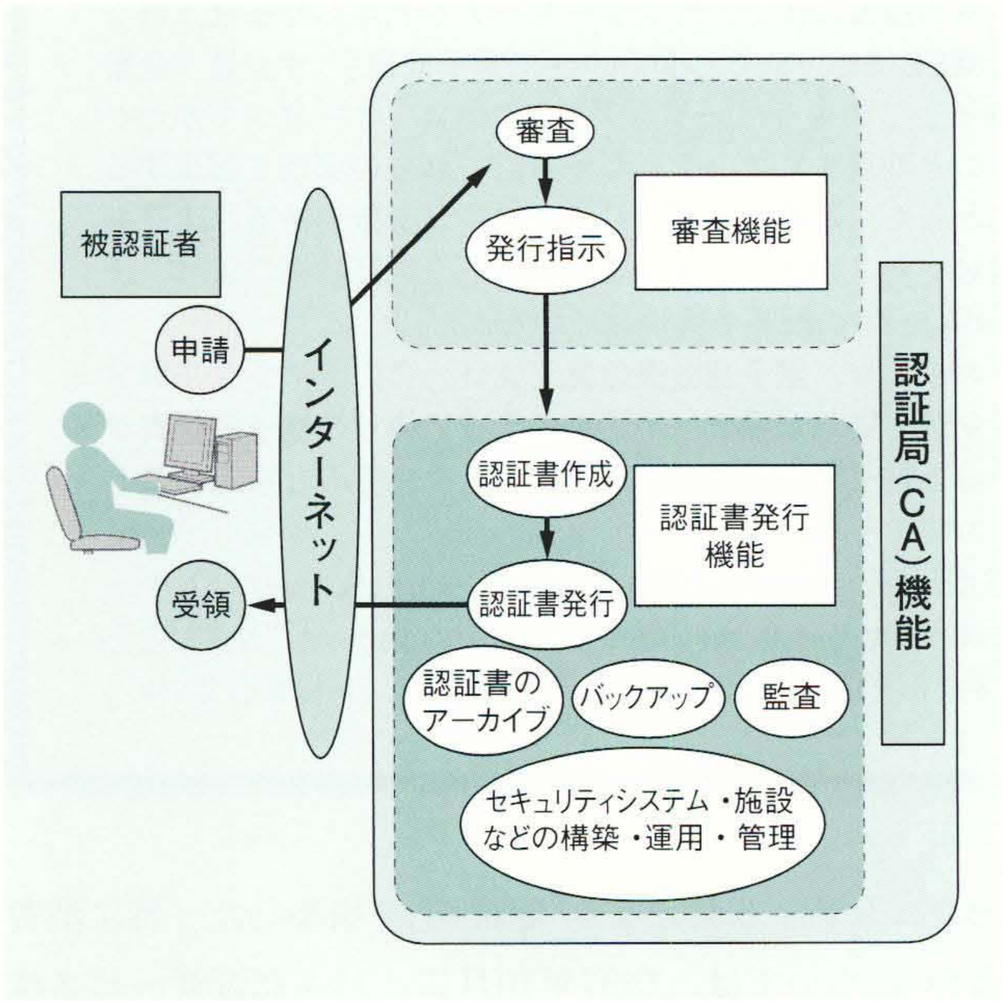
インターネットバンキングでは，本人の個人情報(住所，氏名，電話番号など)，およびその人に事前に郵便で送られ，その人しか知ることのない「契約者番号」により，本人を確認して認証書を発行する。

(2)　認証書発行機能

認証局が発行する認証書には，認証局自身が保有する秘密かぎでサインしたディジタル署名が添付されている。認証書の真正性は，秘密かぎでサインした，この認証局のディジタル署名で保証される。認証書の改ざんは，認証局のディジタル署名で検証することができる。

認証局の秘密かぎが外部に漏れたり，危殆(たい)化のおそれがある場合は，認証書に信頼を置いて行動する利用者に大きな損害を与えるおそれがある。仮に，不正者が認証局の秘密かぎを入手すると，この不正者は認証局を装って偽りの認証書を発行することができるようになる。秘密かぎの漏えいの事実が判明しないかぎり，不正に発行された認証書が本物として通用してしまう。

このように，認証書発行上の問題は，故意，過失のいずれによっても社会に及ぼす影響がきわめて大きい。



注：略語説明　CA(Certification Authority)

図1　認証局を構成する機能

被認証者は，インターネット経由で認証局に認証書の発行を申請し，事前登録情報を基に審査を受け，認証書を受領する。

3 認証局実現のためのセキュリティ技術

日立製作所が日本認証サービス株式会社から受託している認証局では，VISA International社とMasterCard International社それぞれからその運用要件が提示されており，運用に際しては，認証局階層構造の中で，これら2社からの認定を必要とした。1998年10月にセキュリティの自己監査を実施した後，1998年12月と1999年1月にそれぞれの会社の現地査察を受けた。

セキュリティシステム実現には，「(1) 脅威分析，(2) セキュリティポリシー策定，(3) ポリシーに沿ったセキュリティの実行(ビジネスプロセスの実行)」のステップで，(1)→(2)→(3)→(1)のフィードバックサイクルが必要となる。それぞれの会社の受査には高いレベルの(1)，(2)，(3)が要求され，日立製作所は，その現地査察を受けることで，高度なセキュリティシステムの構築，運用，管理を実現している。

セキュリティの実現には，次の項目を順守することが重要である。

(1) 機密性(不当に参照されないこと)
(2) 完全性(不当に破壊，改ざんされないこと)
(3) 可用性(不当な理由で，情報，コンピュータが使用できなくなること)
(4) 証拠性(事実，内容が否認されないこと)
(5) 原本性(不正にコピーされないこと)

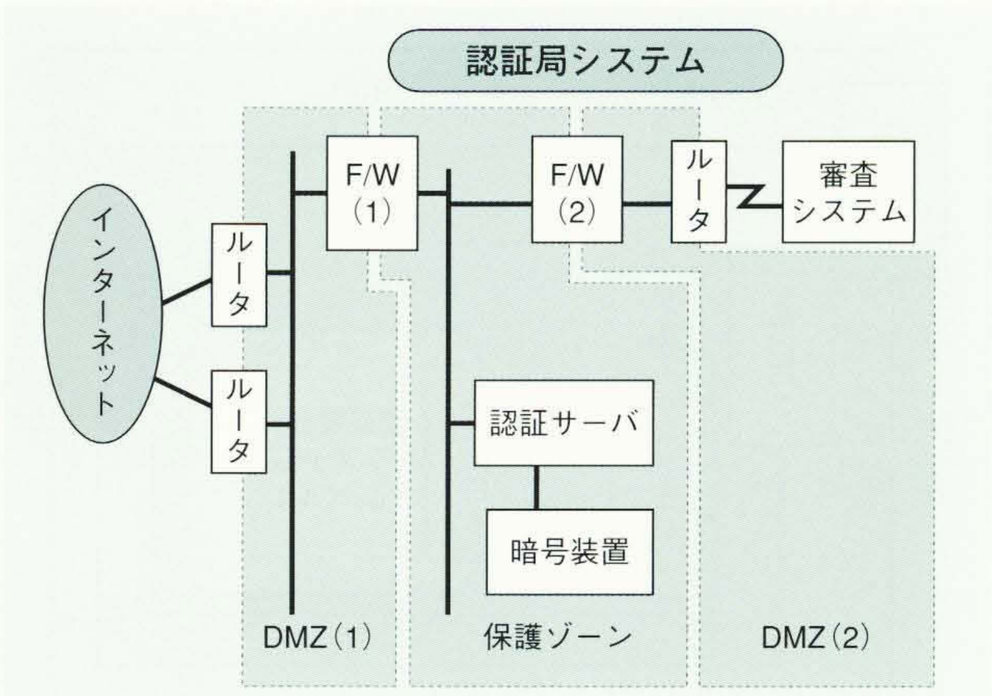
認証局から見た場合，脅威が外部からの要因だけではなく，内部要因に起因する場合も検討する必要がある。セキュリティ実現にあたっては，まず認証局の秘密かぎが漏えいした場合(コピーや盗聴，紛失)に想定される現象・影響を分析することから開始した。その結果，認証局に求められるセキュリティでは，外部からの脅威に対するガードとしての物理的な対策に加え，認証局が保有する各種の情報についても，論理的または内部不正に対してもガードする必要があると考え，各種のセキュリティ機能を設定した。その例について以下に述べる。

3.1 外部脅威に対するセキュリティポリシー

3.1.1 ネットワーク

インターネットや審査システムが接続される専用線経由での，不正な認証書発行の申請を図るアクセスを防止するため，認証書発行システムの前後にファイアウォールを設置する。ファイアウォールでは，不正アクセスの履歴を取得し，定期的に検証する。

認証局を構成するネットワークの概念を**図2**に示す。



注：略語説明　DMZ(Demilitarized Zone；非武装地帯)

図2　ネットワークの構成概念
認証書発行機能をつかさどる認証サーバや暗号化装置は，F/W(Firewall)によって外部アタックから保護される。

認証局システムは，(1) 保護ゾーン，(2) DMZ(1)〔Demilitarized Zone(1)〕，および (3) DMZ(2)に分けられる。

(1) 保護ゾーン

認証サーバや暗号化装置などが設置される，最も高いセキュリティ保護が必要なネットワークである。インターネットからのアタックにはF/W(1)〔Firewall(1)〕で，審査システム側からのアタックにはF/W(2)でそれぞれ保護を行う。

(2) DMZ(1)

インターネットからの通信をすべて受け付ける。フロントサーバと監視用端末を要塞(さい)ホストとして，セキュリティーガードを施す。保護ゾーンへのアタックに対する防御はF/W(1)によって行う。

(3) DMZ(2)

審査システム側ネットワークからのF/W(2)への特定通信だけを受け付ける。

ファイアウォールのポリシーとしては，各ファイアウォールでの他のホストからの操作(例えば，Telnetからの遠隔ログインによる操作)を禁止する。このほかに，各ルータとサーバのセキュリティポリシーを個別に設定している。

3.1.2 設備・施設

認証施設には，さまざまなレベルを持つセキュリティエリアを設けることにより，認証書発行システムを設置する専用室を物理的に安全な環境とするようにくふうしている(**図3**参照)。

各セキュリティレベルに応じて，入退出管理やモニタ

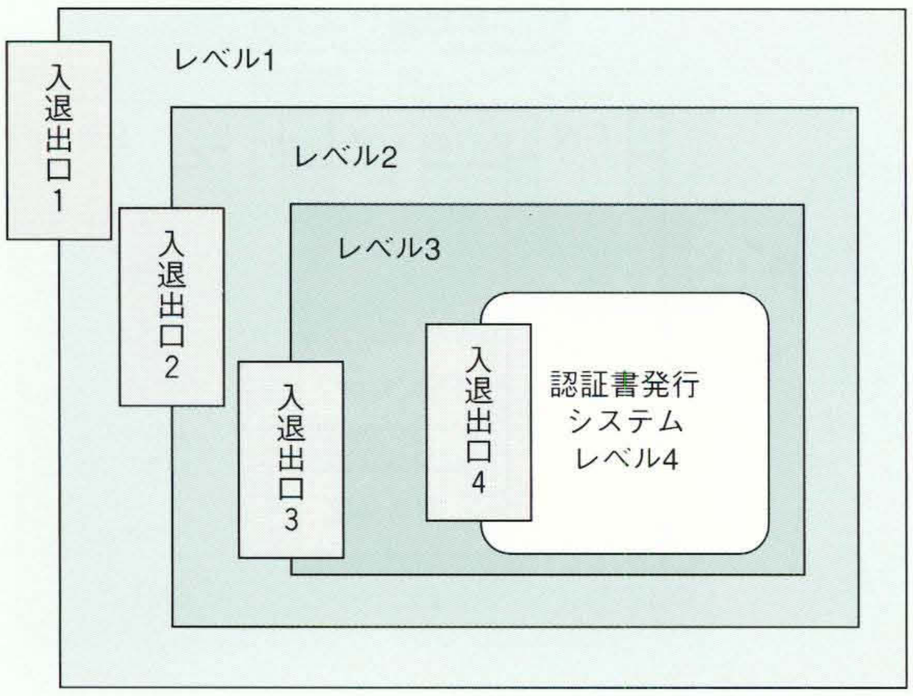


図3 認証施設のセキュリティレベル
認証書発行システムは，最もセキュリティレベルの高いレベル4の専用室に設置している。

リング，センシングなどを行い，その記録は内部規定で定める期間保管し，電子データについてはディジタル署名を施して保管している。また，これらの施設・設備は，財団法人日本品質保証機構の検査に合格している。

3.2 内部脅威に対するセキュリティポリシー

3.2.1 かぎ管理

認証局セキュリティのかなめとなるのが，この「かぎ管理」である。SET／SECE認証局は，かぎ管理について，かぎのライフサイクルを考慮した，以下のような観点からのセキュリティポリシーを設定している。

(1) 暗号装置へのアクセス，(2) かぎの生成，(3) かぎのロード(保管されているかぎを暗号装置に移動)，(4) かぎの活性・非活性化，(5) かぎの使用，(6) かぎの保管，(7) かぎのバックアップ，(8) かぎの破棄，(9) かぎのアーカイブ

具体的なかぎ管理ポリシーの設定では，上記の各観点で操作者の権限を明確にし，単一人による操作を自動的に排除する機能，耐タンパ性，検知・追跡機能(証拠性)を設けた。

3.2.2 自己監査

3年に一度の自己監査を実施する。監査は，社内の認証事業に携わらないセキュリティの専門家が実施する。現時点での監査項目数は353件である。また，監査のない年には，変更のあった部分だけの自己監査を実施する。

3.3 セキュリティの評価

現在，CC(Common Criteria)，ISO(国際標準化機構)，IPA(財団法人情報処理振興協会)などでその評価基準を作成中である。日立製作所は，これに先立って，VISA International社とMasterCard International社のセキュリティ基準に準拠する認証サービスを実現した。

今後，ISOで標準化されると思われるセキュリティ評価基準に照らした再評価が必要と考える。

4 おわりに

ここでは，インターネット上でのビジネスを展開していくうえで，そのかなめとなる認証局の役割と，認証局にかかわるセキュリティ技術について述べた。

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し，認証サービスのいっそうの充実に努めていく考えである。

参考文献

1) 松本，外：電子商取引のセキュリティ技術，日経BP社(1998)
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)

執筆者紹介

滝田誠一郎
1968年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 金融第一システム本部 電子決済システム開発センタ 所属
現在，認証局システム，電子マネー，ICカードシステムの開発に従事
E-mail：takita @ system. hitachi. co. jp

田川 豊
1984年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 金融第一システム本部 電子決済システム開発センタ 所属
現在，認証局システムの企画・開発に従事
E-mail：y-tagawa @ system. hitachi. co. jp

森山将治
1985年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 金融ビッグバン推進本部 商品開発第2センタ 所属
現在，金融系のエレクトロニック コマース システム・認証システムの企画・開発に従事
E-mail：smoriya @ system. hitachi. co. jp

米田英央
1993年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 ネットワーク&サービス本部 アウトソーシング部 所属
現在，アウトソーシングサービス企画・運用に従事
E-mail：yoneda @ system. hitachi. co. jp