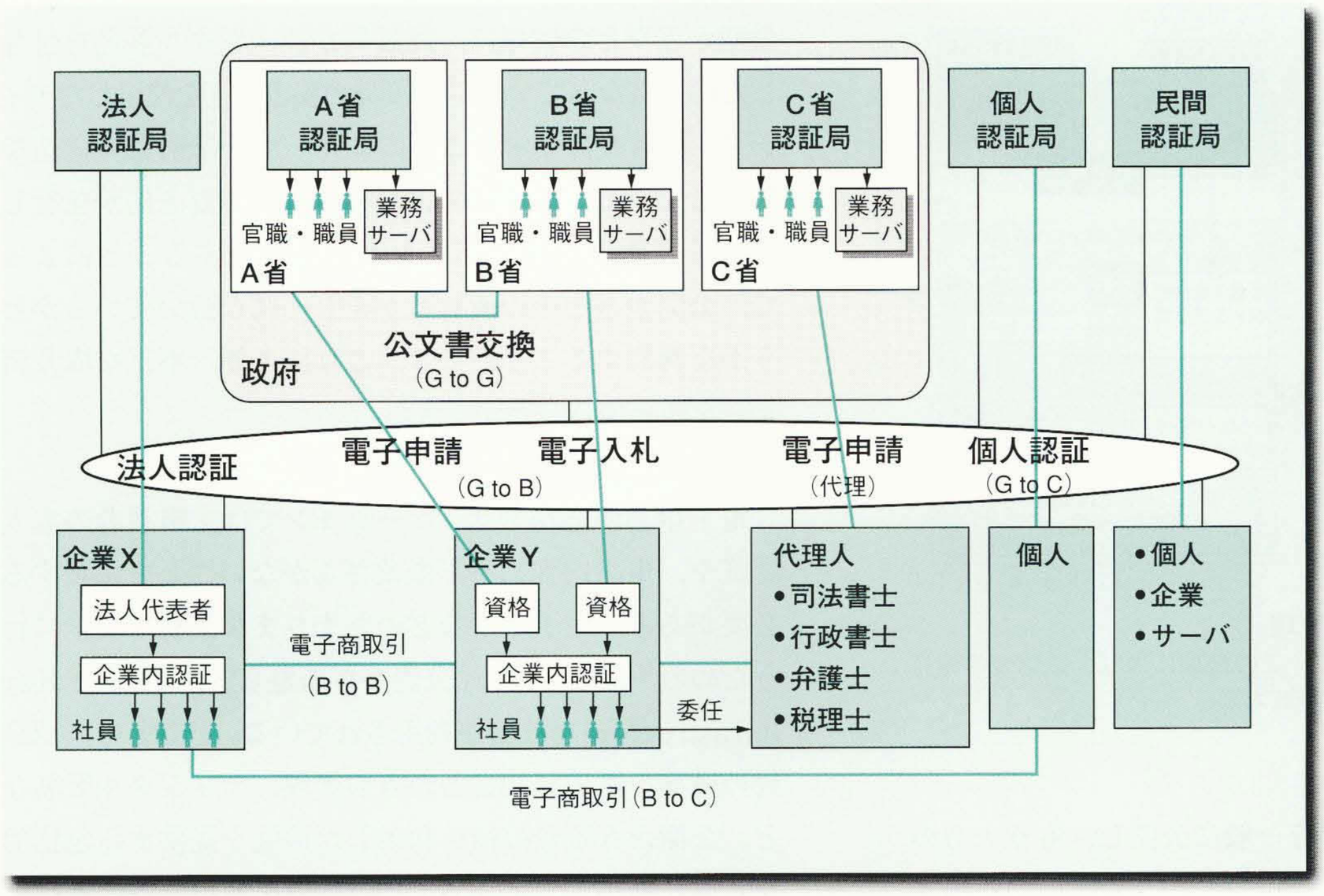
特集　21世紀の豊かな社会を支える電子行政ソリューション

# 電子行政を支えるセキュリティ基盤技術

## Security Infrastructure Technologies for Cyber Administration

中上昇一　*Shôichi Nakagami*　手塚　悟　*Satoru Tezuka*
菊田篤史　*Atsushi Kikuta*　松永和男　*Kazuo Matsunaga*




注：略語説明
G to G（Government to Governmrnt）
G to B（Government to Business）
G to C（Government to Consumer）
B to B（Business to Business）
B to C（Business to Consumer）

**電子行政の全体イメージ**
電子行政の今後の発展のイメージを示す。公文書交換や電子申請，電子入札などの業務から電子商取引まで，さまざまな電子的取り引きがインターネット上で行われる。

電子行政では，インターネット上で行う公文書交換や電子申請，電子入札などの業務から，さらに，民間にかかわる企業間電子商取引，企業と個人間電子商取引まで，さまざまな電子取り引きを安全かつスムーズに行う必要がある。このような電子行政を実現するためには，情報インフラストラクチャーの整備が必須であり，中でも，「改ざん防止」や「成り済まし防止」，「原本性・真正性の保証」，「否認防止」，「盗聴防止」，「プライバシー保護」などに細心の注意が必要になる。
このような課題を解決するために，(1) 公開かぎ基盤(PKI：Public Key Infrastructure)による電子認証技術，(2) ソフトウェア技術としての暗号アルゴリズムやビジュアル認証技術，(3) ハードウェア技術としての暗号装置やICカード，(4) システム技術としてのファイアウォールやセキュリティシステム要件を満たす運用技術などを，有効に組み合わせて適用する必要がある。日立製作所は，これらの基盤技術を「行政サービス基盤ソリューション」として提案している。

## 1　はじめに

時間や空間にとらわれない電子行政サービスを実現するには，万全のセキュリティ(安全性)対策をとることが前提となる。インターネットを使ってさまざまな電子取り引きを行うためには，取引相手とは非対面となることから，「改ざん防止」や「成り済まし防止」，「原本性・真正性の保証」，「否認防止」，「盗聴防止」，「プライバシー保護」などに十分配慮する必要がある。

ここでは，このような要件に対応する「セキュリティ基盤技術」について述べる。

## 2　電子認証技術

### 2.1　ディジタル署名

ネットワークを使用して電子取り引きを行う場合，送信相手の本人確認や送信情報の不正な改ざんを検出するための技術として，「ディジタル署名」が用いられる。ディジタル署名は，「公開かぎ暗号」を利用したものである。

公開かぎ暗号は，ある情報を暗号化する際に使用するかぎと復号化する際に使用するかぎとが異なっており，一方のかぎで暗号化すると，もう一方のかぎでしか復号化できない仕組みになっている。

また，一方のかぎから他方のかぎを算出することが困

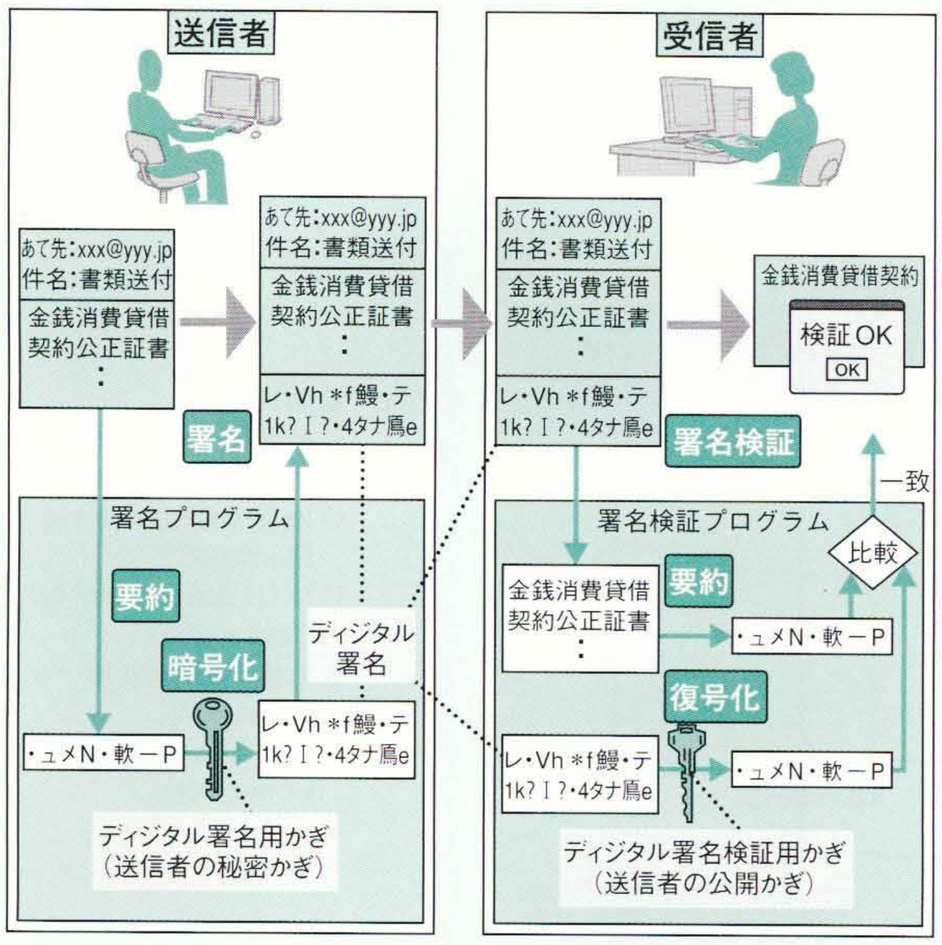



**図1　ディジタル署名技術の原理**
ディジタル署名の原理を示す。この技術により，送信者の確認や改ざんの検知を行うことが可能になる。

難なことから，一方のかぎを一般に公開し，もう一方のかぎは他人に知らせないように秘密に保管して使用する。公開するかぎを「公開かぎ」，秘密に保管しておくかぎを「秘密かぎ」と呼ぶ。

公開かぎ暗号を用いたディジタル署名の原理を**図1**に示す。まず，送信者は，自分の秘密かぎにより，送信情報にディジタル署名を付与し(秘密かぎによる暗号化)，それを受信者に送る。そして，受信者は送信者の公開かぎによってディジタル署名を検証する(公開かぎによる復号化)。署名検証に使用した公開かぎが署名に使用した秘密かぎと対になっているものであれば，情報を正しく復元できる。情報が正しく復元できなかった場合は，送信情報が改ざんされているか，別の秘密かぎによってディジタル署名が付与されていることになる。

### 2.2　電子証明書と認証局

ディジタル署名では，署名検証に問題がない場合は，公開かぎに対応した秘密かぎを使用して署名されていることがわかる。しかし，本人認証を行うためには，取引相手の公開かぎであると思っているかぎが，ほんとうに本人のものであるということを確認する必要がある。公開かぎの所有者の身元確認を行い，公開かぎとその所有者が結び付いていることを保証する役割を担う第三者機関が「認証局(CA：Certification Authority)」である。

認証局は，公開かぎとその所有者が結び付いていることを保証するために，「電子証明書(公開かぎ証明書，「認証書」とも呼ばれる。)」を発行する。電子証明書のフォーマットはITU(国際電気通信連合)のX.509で標準化が進められており，認証局名や公開かぎの所有者名，公開かぎなどの情報に，認証局がディジタル署名を付与した構造となっている。認証局の秘密かぎを使用したディジタル署名を付与することにより，電子証明書の偽造を防止している。電子証明書の利用者は，認証局が発行した電子証明書のディジタル署名を検証することによって，公開かぎとその所有者が正しく結び付いているかどうかを判断することができ，これにより，不正な成り済ましを防止することができる。

### 2.3　PKI

電子申請の業務アプリケーションでは，申請者の本人認証や，申請内容に不正な改ざんがないことを保証する必要がある。電子申請などのさまざまな業務を安全に行うための手段として，「公開かぎ基盤(PKI：Public Key Infrastructure)」技術が利用されている。PKIとは，認証局の構築や電子証明書とかぎの管理，ディジタル署名など，公開かぎ暗号技術を利用した機能を提供する包括的な基盤技術のことである。PKI技術を使用することにより，電子メールやウェブブラウジング，電子取り引き〔EC(Electronic Commerce)，EDI(Electronic Data Interchange)など〕，アクセス管理，VPN(Virtual Private Network)などの多様なアプリケーションで，電子証明書を用いた本人認証や暗号通信が容易に行えるようになる。

### 2.4　今後の課題

今後，PKI技術をベースとして多くの認証局が開設されると予測されるが，これに対応する認証局間の相互認証や，電子証明書の有効性確認方式などが重要なポイントとなる。また，認証局間のセキュリティレベルのマッチングやX.509証明書における日本語など2バイトコードの対応の標準化も必要となる。これには，国内に限らず，海外との接続も当然含まれる。電子取り引きなどを急速に普及させるためには，技術や制度面でのこれらの整備が重要な課題となる。

## 3　ビジュアル認証技術

### 3.1　背　　景

インターネット上のホームページでは，一部で不正な商取引や情報発信などが行われ，また，悪意を持った情報改ざんによって利用者が被害を受けるケースが生じている。

インターネット・マーク技術は，このような状況を未然に防ぐための対策として，ホームページにはられたマーク画像により，ホームページの内容や発信者情報などを利用者が視認し，確認する手段を提供する技術である。これは，通信・放送機構の委託研究として，1998年9月から2000年3月の期間で日立製作所が研究し，開発したものである。

### 3.2　インターネット・マーク技術

インターネット・マーク技術は，高密度電子透かし技術とディジタル署名技術を用い，小さな画像データに認証情報を埋め込んだ画像マークを用いることにより，ホームページの真正性を検証する技術である(**図2**参照)。これにより，画像マークやホームページに対する不正コピーや改ざん，成り済ましの検出など，高度なセキュリティを実現している。検証結果や有効期限などを画像マークのデザイン変化により，ビジュアルに表現できるため，使い勝手と視認性にも優れている。

インターネット・マーク技術の特徴は，小さな画像マークに多くの情報を埋め込む「高密度電子透かし技術」にある。画像マークのデザインを保ちつつ，ホームページに関する情報を画像マークに埋め込むことが可能である。高密度電子透かし技術で埋め込む情報にはディジタル署名技術による改ざん防止が施されているため，万一画像に埋め込まれた情報を書き換えられた場合でも，その検出を可能としている。

インターネット・マークがはり付けられるべきホームページ以外に不正にはられている場合や，インターネット・マークに付与した有効期限が切れている場合などは，その検証結果をマーク画像上に「検証NG」などの文字で表示し，視覚的に表現することが可能である。

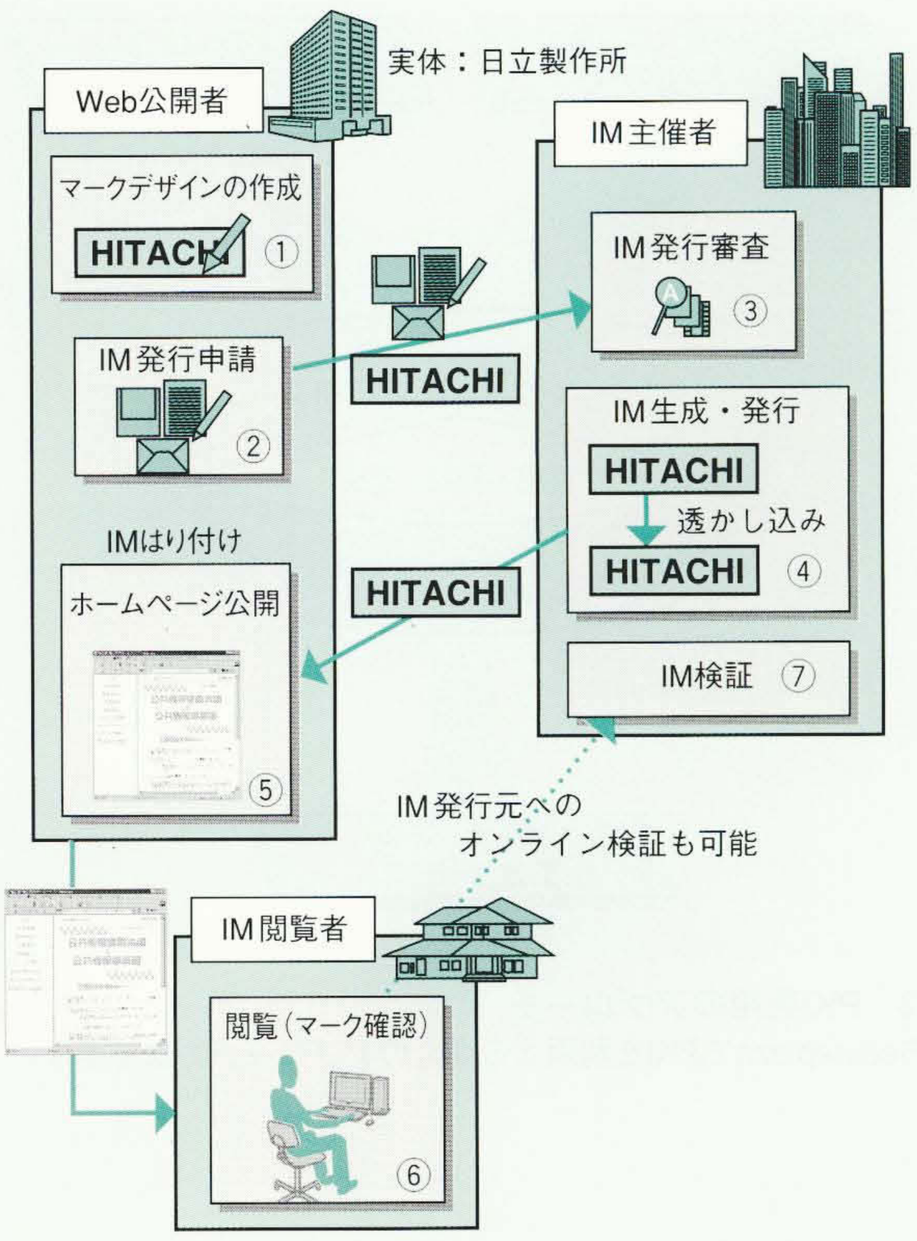
### 3.3　ホームページの真正性証明以外への適用

日立製作所は，インターネット・マーク技術のネットワークコミュニティ活動への適用を検討しており，安全かつ使いやすいネットワーク環境の構築に取り組んでいる。

また，ホームページ以外でも，文書管理システムなどとの連携により，ネットワーク上を流通する電子データの真正性を検証でき，かつ利用者にわかりやすいシステムの実現を図っていく。

### 3.4　世界標準への採用の働きかけ

現在，GBDe※)などにより，いわゆる「トラストマーク」についての標準化が世界レベルで検討されている。日立製作所は，インターネット・マーク技術が標準として採択されるように積極的に提案活動を展開している。




注：略語説明ほか　IM(Internet-Marks)
丸中数字は，運用の流れを示す。

**図2　インターネット・マークのホームページへの適用例**
インターネット・マーク技術をホームページに適用した例を示す。高密度電子透かし技術とディジタル署名技術を用いることにより，ホームページの真正性が検証できる。

## 4　Secureplaza

日立製作所は，総合的な情報システムセキュリティを実現する製品・サービス体系として“Secureplaza”を提案している。電子行政を実現するために必要なセキュリティ技術としては，不正アクセス対策に代表されるようなネットワークセキュリテを含めて，あらゆる面からセキュリティに対する脅威を分析し，計画的な対策をとる必要がある。特に，ネットワークを中心に多様なサービスを実現する電子政府には，電子認証を含む，PKI技術を応用した強固なセキュリティが欠かせない。

日立製作所は，セキュリティ技術の動向に対応してSecureplazaの製品・サービスを充実，拡張している。これにより，PKIについても最先端の技術を備えた製

※) GBDe：Global Business Dialogue on e-commerceの略で，電子商取引に関する世界共通のルール作りの実現を目的とする世界規模のNGO

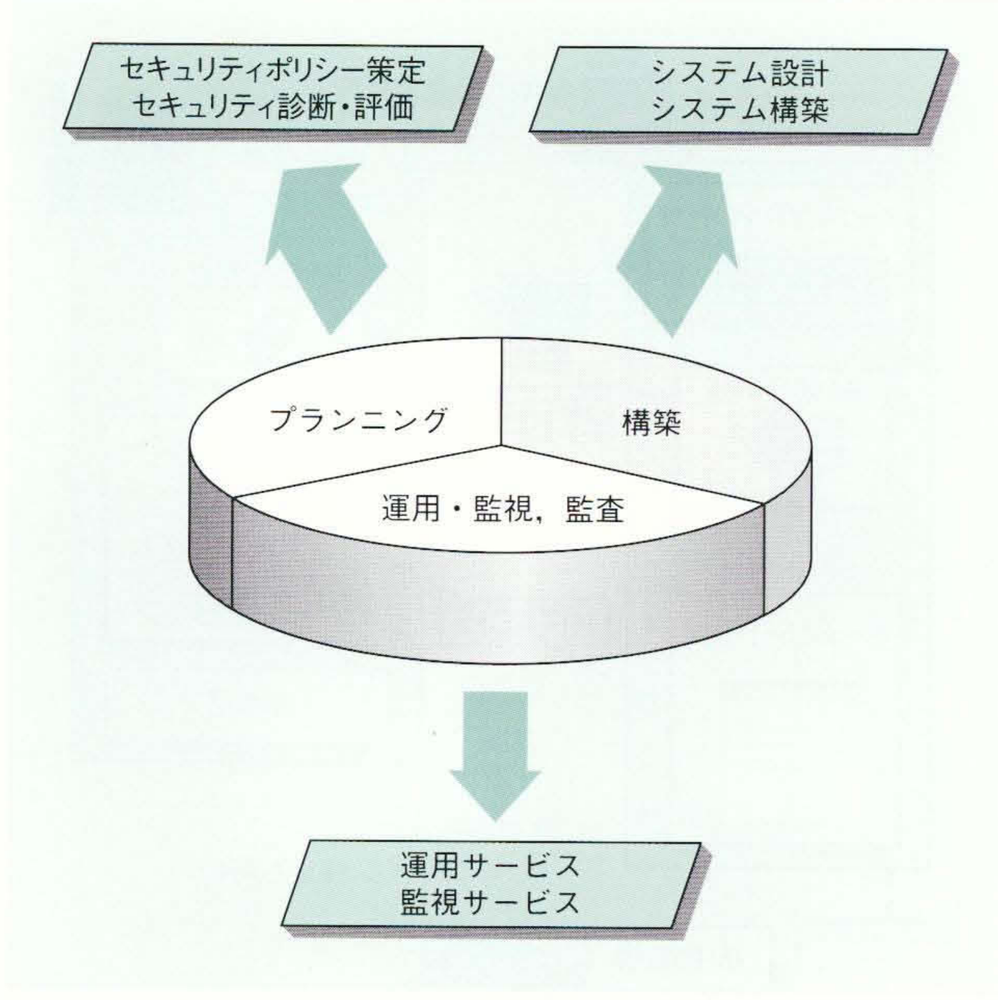



**図3　PKI利用のアプローチ**
SecureplazaでPKIを利用する場合のアプローチ方法を示す。

品・サービスを提供することができる。

さらに，セキュアな情報システムを実現するためには，プランニングの段階から計画的なセキュリティ設計が必要であり，PKIを利用する場合にも以下のようなアプローチが必要となる(**図3**参照)。

(1) プランニングフェーズ

セキュリティポリシー策定を行うフェーズで，セキュアなシステムを実現するためのセキュリティの基本方針を明確にする。この段階で構築するシステムのセキュリティ脅威の分析・要件の定義を行い，目的とするセキュリティレベルを定める。特に，認証システムのように高度なセキュリティを必要とするシステムを運用する場合には，使用するソフトウェアやハードウェアのセキュリティだけでなく，運用者や設備に対するセキュリティを含めて体系的に行う。さらに，セキュリティ診断と評価により，セキュリティの弱点がないかを確認することも重要である。

(2) 構築フェーズ

セキュリティポリシーに基づいて，具体的なシステムの設計と構築を行う。PKIを利用する場合は，かぎ管理・証書形式の設計・証書管理(発行，配布，失効)などを設計し，運用するためのシステム構築を行う。Secureplazaでは，構築するシステムの規模に応じて，スケーラブルな提案を可能とする製品・サービス群をそろえている

特に高度なセキュリティを必要とする場合には，ハードウェアを利用した安全性の高いかぎ管理や，ICカード，指紋認証などを利用することも可能としている。

(3) 運用・監視，監査フェーズ

システム構築後の運用フェーズでも，セキュリティを維持するためには，ポリシーに従った運用を行うだけでなく，不正アクセスなどの監視も怠ることができない。Secureplazaでは，監視サービスや運用サービスも体系的にメニュー化することにより，さまざまな運用に合わせて最適なサービスを提供している。

さらに，わが国でもJIS化に伴い，セキュリティの国際評価基準として"ISO15408"が普及する見込みである。今後は，このような評価・認証制度に基づく，客観的なセキュリティへの取組みが求められることになる。Secureplazaでも，このISO15408に対応するサービスを提供している。

## 5　おわりに

ここでは，電子行政サービスを実現するうえで必要不可欠なセキュリティ基盤技術について述べた。

今後も，アジア・米国・欧州との相互接続を視野に入れて，インターネットを使ってさまざまな電子取り引きを安全かつスムーズに行うことができるように，セキュリティ基盤技術の開発に注力していく考えである。

### 執筆者紹介

**中上昇一**
1979年日立製作所入社，公共システム事業部 GPKI事業推進センタ 所属
現在，中央官庁系システムの開発，認証局基盤技術関連システムの開発に従事
E-mail：nakagami @ jkk. hitachi. co. jp

**菊田篤史**
1987年日立製作所入社，公共システム事業部 インターネットマークス事業推進センタ 所属
現在，インターネット・マーク技術関連の事業推進に従事
E-mail：atu-kiku @ jkk. 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
工学博士
情報処理学会会員
E-mail：tezuka @ sdl. hitachi. co. jp

**松永和男**
1982年日立製作所入社，ソフトウェア事業部 ネットワークソフトウェア本部 第3ネットワークソフト設計部 所属
現在，セキュリティ関連製品の開発に従事
情報処理学会会員
E-mail：matsun_k @ gm. soft. hitachi. co. jp