PKI構築サービスとPKIカードシステム TARGUSYS™

PKI Construction Services and TARGUSYS™ PKI Card System

能勢　健一朗　NOSE Ken-ichiro
麻野間　利行　ASANOMA Toshiyuki
西岡　満　NISHIOKA Mitsuru

PKI（Public Key Infrastructure：公開鍵（かぎ）基盤）は，公開鍵暗号方式を利用したセキュリティインフラストラクチャ（インフラストラクチャは，以下，インフラと略記）であり，インターネットを利用した電子商取引（EC）などで，盗聴，改ざん，なりすましといったリスクを回避する有効な手段として注目されている。PKIシステムのかなめとなるのが電子証明書を発行する認証局だが，信頼できる認証局を構築・運用するのは簡単なことではない。当社では，認証局を中心としたPKI構築サービスを提供するとともに，電子証明書をICカードに格納することで，より強固なセキュリティソリューションを提供するPKIカードシステムTARGUSYS™を開発した。

Public key infrastructure (PKI) is a security infrastructure using the public key cryptosystem. It is considered an effective way to avoid risks such as unauthorized interception, modification, and fabrication in electronic commerce via the Internet. A certification authority is an important entity which issues a certificate on PKI systems. It is not easy to construct and operate a reliable certification authority.

Toshiba provides PKI construction services for the construction of a certification authority. We have also developed the TARGUSYS™ PKI card system, which provides a highly secure solution by a certificate stored in a smart card.

1 まえがき

近年，インターネットが急速に普及し，個人だけでなく企業間においてもECがあたりまえのように行われるようになってきている。しかし，その便利さの一方で，インターネットを利用することにより，盗聴，改ざん，なりすまし，否認などのリスクを伴うことになる。

これらのリスクを回避する方法として，情報の暗号化や電子署名が有効であるとされ，公開鍵暗号方式を基に，暗号化や電子署名を利用したセキュリティインフラであるPKIが注目されている。日本でも政府による電子政府構想(注1)により，政府認証基盤GPKI（Government PKI）や2001年4月に施行された電子署名法など，社会的にもPKIの重要度が確実に高まってきている。

ここでは，当社が提供するPKI構築サービスとPKIカードシステムTARGUSYS™について述べる。

2 PKIの仕組み

2.1 公開鍵暗号方式と電子署名

公開鍵暗号方式は，同じ鍵で暗号化・復号を行う共通鍵暗号方式に対し，暗号化と復号で異なる二つの鍵を使用する暗号方式である。あらかじめ秘密鍵，公開鍵と呼ばれる一対の鍵ペアを生成し，公開鍵で暗号化したものは秘密鍵で復号ができ，秘密鍵で署名したものは公開鍵で検証ができるという特徴を持っている。秘密鍵は本人だけが保管し，公開鍵は第三者へ公開することで，複数の相手と暗号通信する場合でも管理する鍵は一つでよい。暗号通信する相手の数だけ鍵を管理しなければならない共通鍵暗号方式に比べ，インターネットのようなオープンなインフラに適している。

電子署名は，秘密鍵は本人しか保持していないことを前提に，公開鍵暗号方式の秘密鍵を利用して情報が改ざんされていないことを保証する技術である。送信者がメッセージといっしょに，本人の秘密鍵で送信するメッセージに署

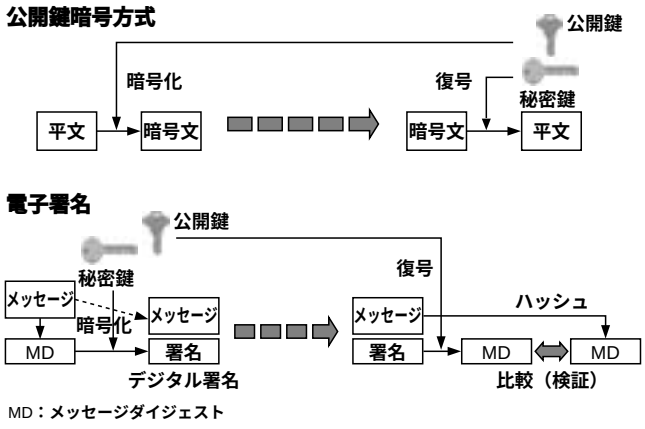

図1．公開鍵暗号方式と電子署名　公開鍵で暗号化し，秘密鍵で署名する。
Public key cryptosystem and digital signature

（注1）　行政を効率化し国民負担の軽減を図るため，申請届出手続きや政府調達など，行政手続きの電子化を実現するシステムの構想。

名したものを相手に送付する。受信者が送信者の公開鍵で署名を検証して正しければ，送信者以外の第三者によって改ざんされていないことになる。実際の電子署名は，秘密鍵より小さいデータに対して行うことが効果的であるため，一方向性ハッシュ関数と組み合わせて行われる（**図1**）。

2.2　電子証明書と認証局

通信相手と暗号通信を行うには相手の公開鍵が必要であるが，インターネット上では通信相手が見えないので簡単に身分を偽ることができてしまう。本人だと言って送付してきた公開鍵が，本当に本人のものであるという保証はなく，公開鍵の真正性を保証する仕組みが必要である。PKIでは，この保証を信頼できる第三者機関が行い，保証を裏付けるものとして公開鍵の証明書を発行する。発行される証明書を電子証明書（又は，公開鍵証明書）と呼び，信頼できる第三者機関を認証局（又は，認証機関）と呼ぶ。

電子証明書を発行する認証局サービスに加入するものは，電子証明書を発行してもらうために認証局へ自分の情報と公開鍵を送付し，電子証明書の申請を行う。認証局は，加入者情報の真正性を審査して確かに本人であると確認した場合に，加入者の電子証明書を発行する。電子証明書を発行することで認証局は加入者から信頼され，かつ加入者の公開鍵が認証局に登録されていることを保証する。

電子証明書の中には，登録された公開鍵に対応する秘密鍵保持者の情報，登録された公開鍵，証明書を発行した認証局の情報，認証局の署名などの情報が含まれている。したがって，電子証明書を入手した者はそれらの情報を得ることができ，認証局の署名を検証することでその証明書が改ざんされていないか（正しい証明書であるか）を確認することができる。

インターネット上で通信をする者は，自分の秘密鍵は厳重に保管して第三者が入手できないようにし，公開鍵は信頼できる認証局に登録する。お互いが信頼できる認証局から発行された電子証明書を入手すれば，見えない相手を確認することができ，正当な者どうしが安全な通信を行うことができる。これを相互認証と呼び，なりすましや否認を防止することができる（**図2**）。

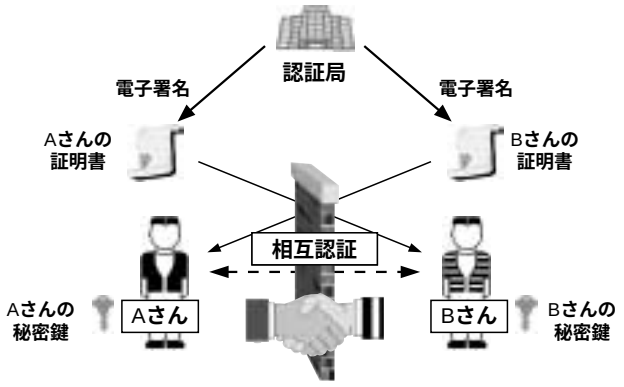

図2．電子証明書と認証局　信頼できる認証局に公開鍵を登録し，電子証明書を発行してもらうことにより，見えない相手との相互認証ができる。
Certificate and certification authority

3　PKI構築サービス

PKIでは，認証局を信頼することが電子証明書を信頼することになり，認証局がPKIにおける信頼の基盤となる。

つまり，信頼できる認証局を構築・運用することが，PKIを成功させる重要な鍵と言っても過言ではない。それだけに，信頼の基盤である認証局が満たさなければならない要件には様々なものがあり，これらを満たすために充分な検討が必要である。主な要件を次に示す[1]。

(1)　マネジメント要件
- (a)　認証局自身の安全性と信頼性の確保や，加入者による秘密鍵の保護
- (b)　認証局の責任と保証に関するポリシーの策定，開示
- (c)　経営情報や技術情報，認証局運用規定などの情報開示

(2)　運用要件
- (a)　加入者の本人確認と情報の真正性確認などの証明書発行時の審査
- (b)　暗号モジュール内部での鍵生成，秘密鍵の保管などの認証局秘密鍵の管理
- (c)　証明書の登録，保管，開示などの証明書の管理
- (d)　証明書失効リスト（CRL：Certificate Revocation List）の生成，保管，開示などの管理

(3)　システム・設備要件
- (a)　品質，開発環境，実運用システムなどのシステム管理
- (b)　システムセキュリティの確保
- (c)　暗号鍵管理モジュールの選定
- (d)　認証システム設置室のセキュリティ確保

このように，信頼できる認証局を構築・運用していくのは，そう簡単なことではない。そのため，当社では，認証局ソリューションとしてPKI構築サービスを提供している。主なサービス内容を次に示す。

(1)　PKI導入コンサルテーション　　要求定義の確認，認証局基本方針策定，スケジュール策定支援

(2)　認証局サービス設計支援　　サービスレベル，サービスモデルなどの設計支援

(3)　認証局運用設計支援　　証明書発行手順（新規，更新，破棄などの証明書ライフサイクル管理），運用体制などの設計支援，及び証明書ポリシー，認証局運用規定などの策定支援

(4) 認証局システム設計支援　システム機能設計，セキュリティ要件などのシステム設計支援，試験仕様作成支援

(5) 認証局構築支援　認証局システムセットアップなどの認証局構築支援

(6) Webセキュリティ構築支援　Webサーバセキュリティポリシー策定，Webサーバ構築，SSL（Secure Sockets Layer）設定支援

(7) ディレクトリサーバ連携支援　ディレクトリ構造設計，ディレクトリサーバ構築，SSL設定支援

(8) エンドユーザー教育支援　管理者へのトレーニングなど

これらのサービスを提供することで，お客さまが購入された認証局ソリューションにおいて，認証局の導入から構築までをサポートし，信頼できる認証局の運用に寄与している。

当社で販売している認証局ソリューションには，VeriSign社のOnSiteとNetscape Communications社のCertificate Management System(注2)（CMS）がある。また，Microsoft® Windows®(注3) 2000 Serverにも認証局ソリューションがあり，これによる構築も可能である。

OnSiteは，認証局機能の登録局と発行局のうち，発行局をVeriSign社へアウトソーシングする認証局サービスである。認証局秘密鍵の管理，証明書の管理やCRL発行など，運用コストが掛かる部分がアウトソーシングされるので，電子証明書が多数発行される大規模なPKIシステムに向いている。

また，OnSiteには，パブリックサービスとプライベートサービスがある。パブリックサービスを利用した認証局を導入した場合，認証局証明書があらかじめブラウザに格納されているため，暗号・署名メールS/MIME（Secure/Multipurpose Internet Mail Extensions）の利用に適した認証局と言える。プライベートサービスは会員向けサービスなど，加入者が限定されている場合に適している。

一方，CMSは，認証局の機能をすべて自前で構築する認証局ソフトウェアパッケージである。電子証明書の発行枚数が比較的少ない小中規模なPKIシステムに向いており，これはプライベートサービスとなる。

4 PKIカードシステム TARGUSYS™

4.1 ICカードによる加入者秘密鍵の保護

PKIシステムを構築した場合，加入者秘密鍵の保護をどうするかという問題がある。秘密鍵が悪意を持った第三者に盗まれてしまうと，暗号メールを解読されてしまったり，自分になりすまされてしまう可能性がある。PKIにおいては，信頼できる認証局が強固なセキュリティにより，安全に運用していたとしても，加入者の秘密鍵は加入者の責任で守らねばならない。

代表的なブラウザ及びメーラであるMicrosoft®社のInternet Explorer(注4)，Outlook™ Express(注5)やNetscape Communications社のNetscape Navigator®(注6)，Netscape Messenger(注7)の場合，標準の秘密鍵保護方法はハードディスク上にファイル若しくはレジストリの形で保存し，パスワードで保護するというものである。そのため，パスワードの脆弱（ぜいじゃく）性から抜け出すことはできない。

そこで，注目されているのがICカードである。PKI対応のICカードでは，秘密鍵と公開鍵の鍵ペア，及び電子証明書を格納することができる。秘密鍵を使用して暗号化処理することはできるが，カード内の秘密鍵を盗み出すことは極めて難しい。

カード自体の盗難に対しても，カード使用時に入力するPIN（Personal Identificaiton Number）が，連続して一定回数まちがえるとICカードがロックして使えなくなる機能により，高い確率で第三者による悪用を防ぐことができる。

また，ICカードは簡単に持ち歩くことができ，ICカードリーダライタが接続されている他のパソコン（PC）で安全に使用できる利便性を持っている。

4.2 PKI対応ICカードTARGUSYS™

このようにPKI対応ICカードは，加入者秘密鍵をより高いセキュリティで保護し，PKIのシステムセキュリティを更に強固なものにすることができる。

このため，当社では，2001年3月にPKIカードシステムTARGUSYS™を開発した（**図3**）。

図3. TARGUSYS™**カード**　秘密鍵を，高いセキュリティで保護することができる。
TARGUSYS™ smart card

TARGUSYS™には以下の特長がある。

(1) 代表的なブラウザ及びメーラに対応　カードに格納された秘密鍵，及び電子証明書を代表的なブラウザ及びメーラであるInternet Explorer，Outlook™ Express

(注2) Certificate Management Systemは，Netscape Communications 社の商標。
(注3)，(注4)，(注5) Microsoft，Windows，Internet Explorer，Outlookは，米国Microsoft Corporationの米国及びその他の国における登録商標。
(注6)，(注7) Netscape Navigator，Netscape Messengerは，Netscape Communications 社の登録商標又は商標。

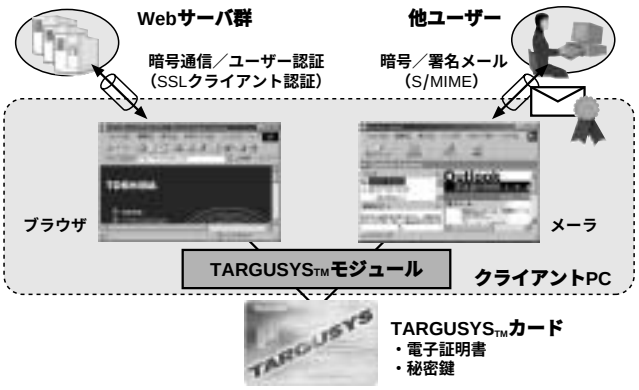

図4．ブラウザ及びメーラからTARGUSYS™の利用　ICカードに格納された秘密鍵，電子証明書を利用したSSL，S/MIMEを実現する。
Use of TARGUSYS™ via Web browser and mail client

やNetscape Navigator®，Netscape Messengerで共通に使用することができ，SSLやS/MIMEを実現する（図4）。

ICカードへアクセスするインタフェースとして，Internet Explorer，Outlook™ ExpressはWindows®の暗号API（Application Programming Interface）であるCryptoAPIを，また，Netscape Navigator®，Netscape Messengerは，RSA Security社が標準化しているPKCS#11を採用している。TARGUSYS™では，PCにインストールされるソフトウェアモジュール部分がどちらのインタフェースもサポートし，内部でその差異を吸収することにより，どちらからでも同じ秘密鍵や電子証明書を利用できる（図5）。

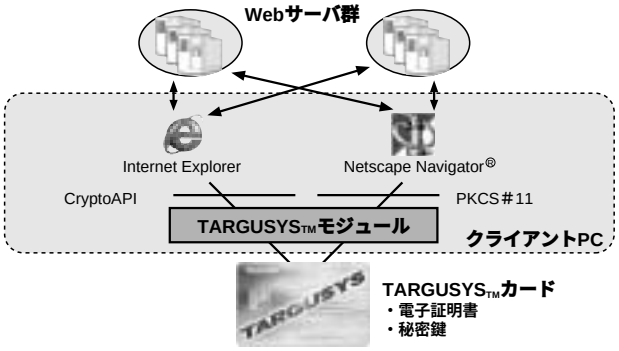

図5．Internet Explorer，Netscape Navigator®からTARGUSYS™の利用　どちらのブラウザからでも同じ秘密鍵，電子証明書を利用できる。
Use of TARGUSYS™ via Internet Explorer and Netscape Navigator®

⑵ Windows®2000スマートカードログオンに対応

TARGUSYS™はPKIだけでなく，Windows®2000スマートカードログオンにも対応している。通常，スマートカードログオン用として市販されているカードは，電子証明書が1枚しか入らないため，ログオン専用カードとなりPKI用として利用するには大きな制限がある。このため，通常はログオン後にICカードを差し替えて利用することになる。

TARGUSYS™では，PKI用とWindows®2000スマートカードログオン用の両方の電子証明書を1枚のカードに格納することができるため，ログオンしたカードでそのままSSLやS/MIMEなどPKIとしての利用ができる。また，この間，ICカードを抜き差しする必要がないため，ICカードでしかログオンを許可せず，カードを抜くと自動的にログオフするような，セキュリティの高いWindows®2000のオプションを選択することができる。

5 あとがき

インターネット上での通信を安全なものにするPKIだが，PKIの信頼の基盤となる認証局を構築するには，サービスレベルの検討や運用方針の策定，システム構成，運用管理などの様々な検討が必要である。そのため，当社では認証局の構築を中心としたPKI構築サービスを提供している。これにより，お客様が信頼できる認証局の構築・運用をすることが可能となる。また，加入者秘密鍵の保護についてもPKIカードシステムTARGUSYS™を開発することにより，より強固なセキュリティソリューションを提供している。

今後は，当社の認証局ソリューションとPKIカードシステムTARGUSYS™とを連携させた，統合管理ソリューションを開発していく所存である。

文　献

⑴ 認証局運用ガイドライン．電子商取引実証推進協議会（ECOM）認証局検討ワーキンググループ．http：//www.ecom.or.jp/qecom/about_wg/wg08/index.htm

能勢　健一朗　NOSE Ken-ichiro
e-ソリューション社 SI技術開発センター SI技術担当。
情報セキュリティ技術の開発に従事。情報処理学会会員。
Systems Integration Technology Center

麻野間　利行　ASANOMA Toshiyuki
e-ソリューション社 SI技術開発センター SI技術担当。
情報セキュリティ技術の開発に従事。情報処理学会会員。
Systems Integration Technology Center

西岡　　満　NISHIOKA Mitsuru
デジタルメディアネットワーク社 メディアカード事業部 ICカード販売推進部主務。ICカード商品技術に従事。
Media Card Div.