電子政府のセキュリティ技術

Security Technologies for Electronic Government Systems

丹羽　朗人 NIWA Akito
石原　達也 ISHIHARA Tatsuya
島田　毅 SHIMADA Tsuyoshi

電子政府の実現には，情報セキュリティ技術が不可欠である。電子政府のシステムは，適切なセキュリテイ対策なくしては，申請文書の盗聴・改ざん，申請者へのなりすまし，コンピュータウィルスなどの様々な脅威に対して脆弱（ぜいじゃく）である。当社は，こうしたクリティカルな脅威からシステムを保護するため，暗号，署名，公開鍵（かぎ）認証基盤（PKI：Public Key Infrastructure），公印付与などのセキュリティコンポーネント開発や，セキュリティに焦点を当てた新しいシステム開発技術の確立に取り組んでいる。

Information technology (IT) security technologies are indispensable for electronic government systems. Without proper security countermeasures, such systems are vulnerable to various threats such as unauthorized access to application documents, illegal modification of documents, falsification of applicants' identities, and computer viruses.

Toshiba provides security technologies such as cryptography, digital signatures, public key infrastructure (PKI), granting of official seals, and system development methodologies focusing on IT security to protect systems against critical threats.

1 まえがき

電子政府の構築は，行政の効率化や国民負担の軽減を目的として，行政手続きの電子化を実現するものであり，その情報セキュリティの確保が不可欠である。電子政府のセキュアな基盤構築に向けて，国は，暗号技術の整備，プロテクション技術の開発，情報機器・システムのセキュリティ評価技術の整備などの施策[(1)]を実施している。

当社は，情報セキュリティ技術の全般にわたって研究・開発を行っているが，ここでは特に，電子政府に向けて進めているセキュリティ技術について紹介する。前述した国の施策に対応させて，暗号技術，電子署名技術，PKI技術，公印付与技術，セキュリティ確保のためのシステム開発技術に焦点を当てて述べる。

2 電子申請・認証のためのコンポーネント技術

政府は電子政府の構築のため，電子認証基盤の構築と各種申請手続きの電子化に積極的に取り組んでいる。

この電子申請の場面においては，申請者本人の確認や文書内容の改ざんの防止，秘匿化などが必要となる。

当社は，こうした場面に適用可能なセキュリティコンポーネントの開発を行っている。アプリケーションシステムの開発において，品質の確保された部品化コンポーネントの再利用により，新たに開発するソフトウェアの量の削減と品質の向上が可能になる。ここでは，こうしたセキュリティコンポーネントについて説明する。

2.1 暗号・署名関連

よく知られているように暗号には共通鍵暗号と公開鍵暗号があり，一般的にはデータ秘匿のために共通鍵暗号，電子文書のデジタル署名作成のために公開鍵暗号を用いる。

当社は共通鍵暗号として独自の暗号Hierocrypt$_{TM}$（ヒエロクリプト）[(2)]を開発し，2003年開始予定の電子政府向けにIPA（情報処理振興事業協会）とTAO（通信・放送機構）によって推進されている暗号技術評価事業（CRYPTOREC）ほか，各種標準化への提案を進めている。

Hierocrypt$_{TM}$は主要なプラットフォーム上での高速処理とコンパクトな実装が可能であり，C言語，Java[(注1)]による実装のほか，ICカードにも搭載されている。

公開鍵暗号としては，当社は標準方式であるRSA（Rivest-Shamir-Adleman）から今後標準となることが予想される楕円（だえん）曲線暗号までを実装しており，種々の環境における高性能な処理を目標の一つとして開発を行っている[(3)]。

当社では，これまで必要に応じて個別にライブラリを開発・蓄積してきたが，今後は世の中の技術動向を見据えながら，アプリケーションからの使いやすさを考慮した体系的な整備を行い，電子政府をはじめとするシステム構築への利用を促進していく。

2.2 PKI関連

前節で述べた公開鍵暗号の仕組みが正当に機能するようにするためには，鍵ペアの真の所有者を確認する必要があり，このための一つの解がPKI技術である。

（注1）Javaは，米国SunMicrosystems社の商標

行政機関において，国民などとインターネットを介して申請・届出や結果の通知を行う場合などには，それを作成した名義人や，申請書，通知文書の内容が改ざんされていないかの確認が必要であり，そのために民間や各行政機関の間で共通のインフラストラクチャを整える必要がある。これを実現する仕組みとしてGPKI（Government Public Key Infrastructure）が進められている。

こうした動向のなか，PKI関連ライブラリの開発を進め，現在次のものが，当社電子申請システムなどでコンポーネント技術として活用が進められている。

⑴ 各種PKCSライブラリ　RSA Security Inc.の提唱する規格PKCS（Public Key Crypto Standard）[4]に基づくPKI関連ライブラリ

⑵ OCSP（証明書の有効性即時確認）機能　公開鍵証明書が失効していないことを認証局の発行するCRL（証明書廃棄リスト）を使わずにオンラインで即時に確認する機能

⑶ XML署名プラグイン[2]　W3C（World Wide Web Consortium）での規格に従ったXML（eXtensible Markup Language）フォーマットによる電子署名（XML署名）をWebブラウザにて付与

⑷ ICカードによるPKI　秘密鍵や公開鍵証明書をICカードに格納し保護。当社PKIカードシステムTARGUSYS$_{TM}$[2]によりInternet Explorer，Netscape NavigatorのいずれからもICカード内の同じ秘密鍵，証明書を利用可能

これらコンポーネントを用いた電子申請としては，例えば次のような手順が考えられる。

ⓐ 申請者はブラウザにて公開鍵ペアを生成し，秘密鍵をICカードに保存（上記（4））

ⓑ PKCS#10公開鍵証明書発行リクエストを当該認証局に送付（上記（1））

ⓒ 認証局発行の申請者の公開鍵証明書をインターネットでブラウザにて取得，ICカードに保存（上記（4））

ⓓ 行政機関への電子申請をブラウザからICカードの秘密鍵を用いて，XML署名を付与して実施（上記（3））

ⓔ 申請受付の行政機関は申請書の署名検証を行うが，OCSPにて公開鍵証明書の有効性を確認（上記（2））

PKCS#12ライブラリ，OCSPリクエスト機能は商業登記に基づく電子認証制度に対応して，当社が開発した申請受付端末利用者ソフトウェアパッケージにも組み込まれた[2]。

2.3 公印付与ライブラリ

2.1及び2.2節で挙げたコンポーネントは，業務非依存なものであったが，業務関連のコンポーネントも開発している。その一例として，ここでは公印付与ライブラリを紹介する。

当社は電子申請システムにおけるコンポーネントの一つとして公印付与サーバを提案している。

公印付与サーバの役割を簡単に述べると，公印を管理し，文書に公印（デジタル署名）を付与することである。公印は，サーバにてHSM（Hardware Security Module）により保護され，公印付与の履歴もサーバで保存される。

公印付与ライブラリは，公印付与サーバの実装に必要な機能をライブラリ化したものである。

公印付与サーバのシステム構成を**図1**に示す。処理の流れは次のようになる。

⑴ 申請者は申請文書に署名を付与し行政機関へ送信

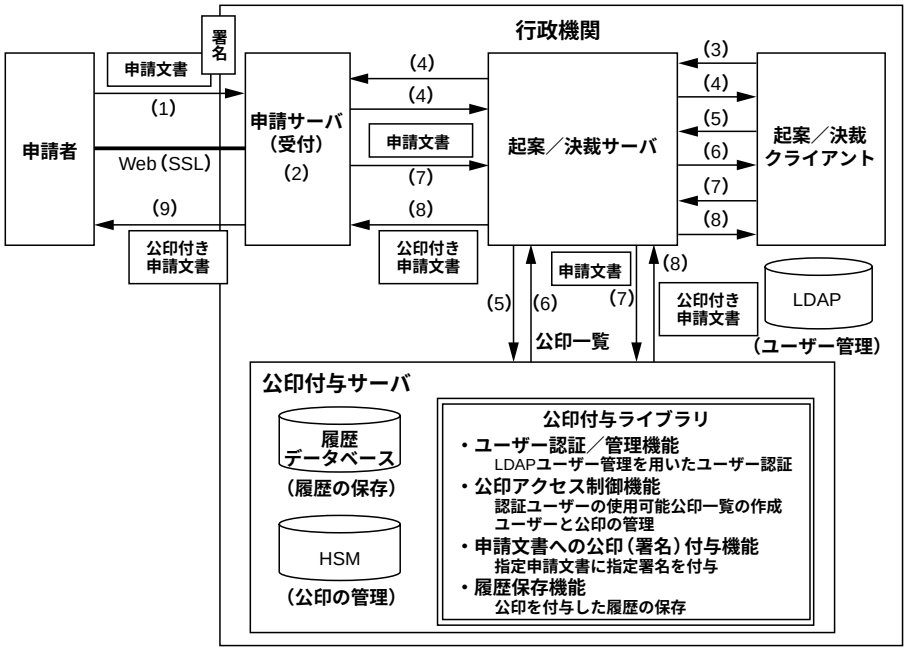

図1．公印付与サーバのシステム構成
公印付与サーバと関連要素の構成及び各構成要素間でやり取りされるデータを示す。
System configuration of official seal grant server

⑵ 申請文書は申請サーバが受け付け，保存／管理
⑶ 公印付与者は起案／決裁クライアントから起案／決裁サーバに申請文書の確認を要求
⑷ 起案／決裁サーバは申請サーバから一覧を取得し，起案／決裁クライアントに表示
⑸ 申請文書を選択，ユーザー管理 LDAP（Lightweight Directory Access Protocol）によるユーザー認証
⑹ 公印付与者の使用可能な公印一覧を表示
⑺ 申請文書を公印付与サーバに送り公印を付与
⑻ 結果を表示し公印付き申請文書を申請サーバに保存
⑼ 申請者は公印付き申請文書を受信

3 ISO15408によるシステムセキュリティの実現

3.1 IT セキュリティ評価基準

今日の情報システムは，ネットワークに接続され，ホームページの改ざんやコンピュータウィルスといった脅威に常にさらされている。電子政府の情報システムは，社会基盤の一部であり，特に強い対抗力を備えなければならない。政府は，中央省庁のシステム構築にセキュリティ評価などのプロセスを有機的に組み込み，セキュリティに関する信頼性がより高いシステムの構築を図る方針[5]を決定した。セキュリティ評価は，1999年に国際標準として制定されたIT（情報技術）セキュリティ評価基準ISO/IEC15408[6]（JIS X5070）（ISO：国際標準化機構，IEC：国際電気標準会議）に基づいて行われる。これは，成立の経緯からCC（Common Criteria for information technology security evaluation）とも呼ばれる。

3.2 システムセキュリティの実現

従来，システムセキュリティを扱うフレームワークは，一部の特殊な用途のものを除けば見当たらなかった。CCは評価の基準であるが，その基準を満たす方法論の実現を通して，包括的なフレームワークとして活用できる。

図2は，活用方法を概念的に表したものである。最初の作業であるセキュリティ設計仕様書（ST：Security Target）の作成は，セキュリティに焦点を当てた基本設計と言える。ここでは，まず評価対象である開発物を定義した後，保護すべき情報資産を明らかにし，その資産に対するすべての脅威を洗い出す。ついで，洗い出した脅威に対して，どんなセキュリティ対策方針で対抗するかを定め，更にこの対策方針を具体化するセキュリティ機能や管理運用ルールを決定する。セキュリティ機能は，CCパート2“セキュリティ機能要件”から選択する。パート2には機能間の依存関係が明記されており，セキュリティ機能の有機的な連携を，自然な流れで設計に盛り込むことができる。

ST作成が終わると，セキュリティ機能仕様書（FSP）及びセキュリティ上位レベル設計書（HLD）の作成，開発物の実装，テストへと進む。ST，FSP，HLDなどはいずれも，セキュリティの保証を示すエビデンスである。これらエビデンスに対して，CCパート3“セキュリティ保証要件”が厳格な基準を定義している。例えば，STで規定したセキュリティ機能がHLDの設計項目へ正確にブレークダウンされていること，セキュリティ機能と設計項目との対応が完全に取れていることを示す証拠の提示が，要件として課せられる。

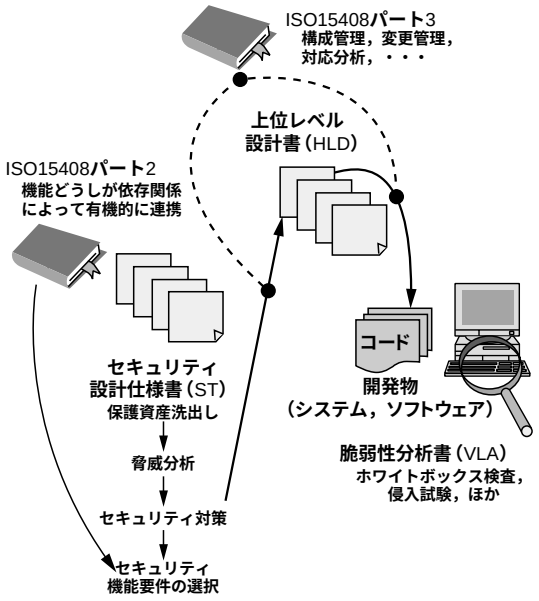

図2．活用の方法　包括的なセキュリティを実現するためのフレームワークとして活用できる。
Application concept of ISO/IEC15408

3.3 ISO15408準拠の設計開発

開発部門にとっては，どのような開発方法によれば成果物やエビデンスが要件を満足するようにできるのかということが，最大の関心事である。しかしながら，CCそのものは評価の基準であり，開発方法については何も規定していない。われわれのグループは，IPA，JEITA（電子情報技術産業協会）などにおけるCC準拠セキュリティ評価の技術開発に参画してきた。その経験や知見を基に，セキュリティに焦点を当てた新しい開発方法論を整備している。

例えば，CCの要件を現行の開発工程に組み込む必要がある。**図3**は，共通フレーム[7]の“開発プロセス”に，CCパート3の保証要件を整合させた開発モデルの例を示している。図中，CC準拠工程の各成果物は通常工程にフィードバックされるものだが，見やすさのため図にはその関連を書き入れていない。また，脆弱性分析では，基本ソフトウェア（OS）やWebサーバ，DBMS（DataBase Management System）など，よく使われる製品について，あらかじめ詳細に脆弱性分析の対象項目を洗い出して，標準分析セットを開発し，作業の精密化，効率化を図っている。

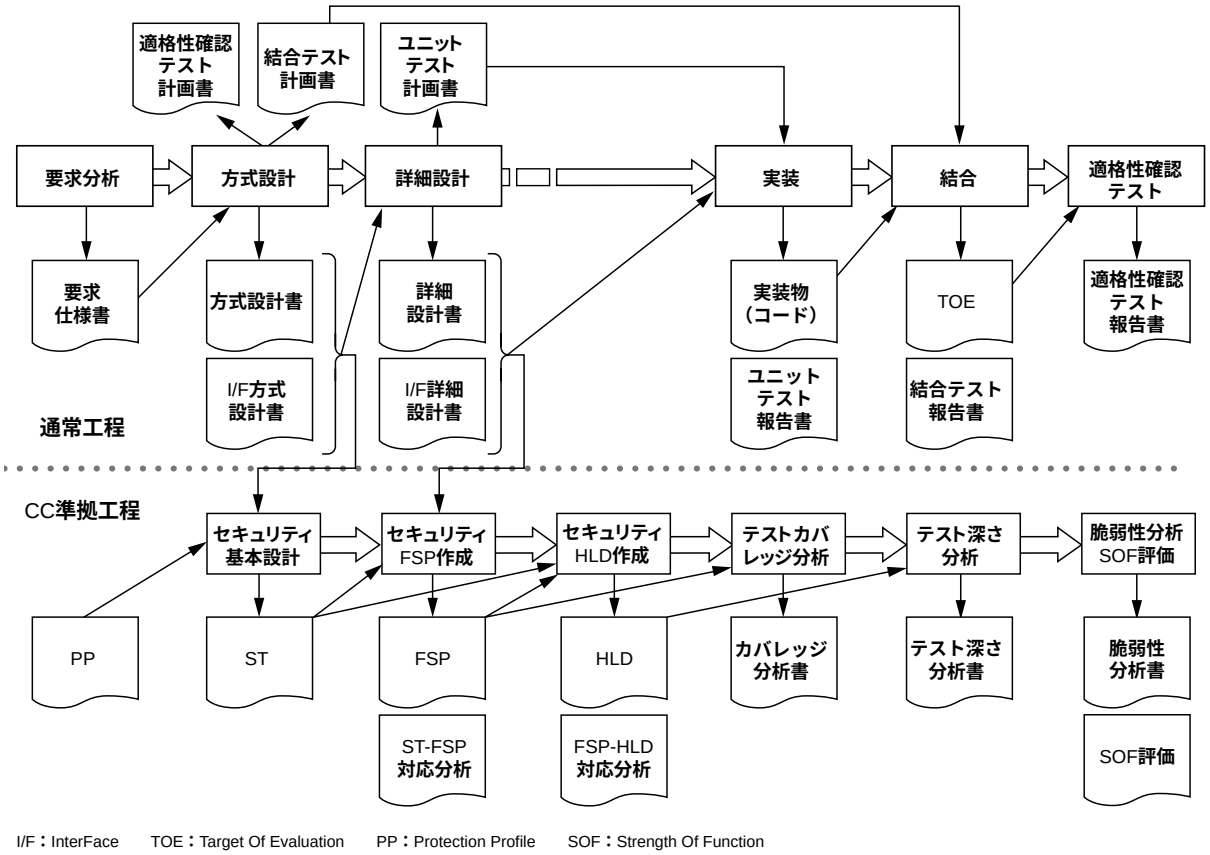

図3．ISO/IEC15408準拠の開発モデル例　共通フレーム準拠の従来工程とISO/IEC15408準拠工程との整合を示す。
Development process model based on ISO/IEC15408

4 あとがき

当社では，電子政府関連システムの企画・開発部門，セキュリティ技術の研究・開発部門など関係者が一体となって，電子政府におけるセキュリティ実現へのアプローチを展開しており，中央省庁，地方自治体などのニーズに的確にこたえる技術開発を続けている。ここで紹介した技術成果は，いずれも，電子政府のセキュアな情報システム構築に大きく寄与できるものと期待している。

文　献

(1) 通商産業省．"情報セキュリティ政策実行プログラムの位置付け"．情報セキュリティ政策実行プログラム．2000，p.2.
(2) 東芝レビュー，情報セキュリティ特集の各該当記事．**56**，7，2001，p.1－57.
(3) 新保　淳，ほか．暗号技術と鍵回復システム．東芝レビュー．**54**，7，1999，p.8－11.
(4) http://www.rsasecurity.com/rsalabs/pkcs/
(5) 経済産業省．“各省庁の調達におけるセキュリティ水準の高い製品等の利用方針”．ISO/IEC15408を活用した調達のガイドブック Version1.02．2001，p.13.
(6) ISO/IEC．ISO/IEC15408：1999 Information technology -Security techniques-Evaluation criteria for IT security．1999.
(7) SLCP-JCF98委員会．共通フレーム98-SLCP-JCF98-(1998年度版)．東京，通産資料調査会，1998，p.350.

丹羽　朗人　NIWA Akito
e-ソリューション社 SI技術開発センター SI技術担当主務。暗号技術・応用システムの研究・開発に従事。情報処理学会会員。
Systems Integration Technology Center

石原　達也　ISHIHARA Tatsuya
e-ソリューション社 ネットワークインテグレーションサービス事業部 営業技術第二担当。情報セキュリティ技術及び同応用システムの研究・開発に従事。情報処理学会会員。
Network Integration Service Div.

島田　　毅　SHIMADA Tsuyoshi
e-ソリューション社 SI技術開発センター SI技術担当主務。システム・セキュリティの研究・開発に従事。IEEE，米国プロジェクト管理協会，人工知能学会会員。
Systems Integration Technology Center