電子政府・電子自治体とセキュリティ技術

e-Government and Security Technologies

北折　昌司　■KITAORI Shoji
中村　宏　■NAKAMURA Hiroshi
河本　高文　■KOMOTO Takafumi

電子政府・電子自治体の構築において，セキュリティは重要な課題である。
東芝ソリューション（株）は電子政府・電子自治体のセキュリティを確保するために，セキュアなシステムを構築する手法，組織の情報セキュリティを管理する仕組みの確立方法，及びPKI（公開鍵基盤）を用いたソリューションを開発した。

Security technologies are a key aspect of the establishment of e-government. The ISO/IEC15408 specifications of the International Organization for Standardization and the International Electrotechnical Commission define how to develop systems in a secure manner, whereas information security management systems (ISMS) specify how an organization is to keep its information assets secure.

Toshiba Solutions Corp. has developed system development methodologies focusing on information technology security with respect to ISO/IEC15408 and ISMS. A public key infrastructure (PKI) smart card issuing system has also been developed as a typical example of application systems utilizing our security technologies.

1 まえがき

インターネット上で重要な情報を取り扱う電子政府・電子自治体の構築において，セキュリティは重要な課題である。

ここでは，セキュアなシステムを構築する手法としてのISO/IEC15408（国際標準化機構／国際電気標準会議規格15408）の取組みと，組織のセキュリティを確保する仕組みとしての情報セキュリティマネジメントシステム（ISMS）の取組みについて述べる。併せて，システム事例の中から特定認証対応ICカード発行ソリューションの事例を説明し，東芝ソリューション（株）のセキュリティに対する取組みと考え方について述べる。

2 ISO/IEC15408によるセキュアなシステム構築手法

2.1 セキュアな電子政府構築のための制度と施策

政府は，電子政府の構築に必要なIT（情報技術）製品やシステム（以下，ITシステムと言う）のセキュリティ水準を確保するために，ISO/IEC15408に基づき，評価機関によってITシステムのセキュリティ機能とその品質を評価する“ITセキュリティ評価・認証制度”を創設し，既に運用を開始している。そして各省庁は，信頼できるITシステムを調達するために，可能な限り評価・認証されたITシステムの利用を推進することに合意している。

政府調達へのITセキュリティ評価・認証制度の適用に関しては，2002年7月に公表された“情報システムの調達に係る総合評価落札方式の標準ガイド”[(1)]の中で，ITセキュリティ評価・認証制度に基づく評価に関する項目を設定することが示されたのをはじめ，2003年10月には，世界最高水準の高信頼性社会の構築のために策定された“情報セキュリティ総合戦略”[(2)]の具体策の中にも，ITセキュリティ評価・認証制度の普及強化が取り上げられており，今後，更に適用範囲が拡大することが見込まれる。

2.2 ISO/IEC15408認証取得支援サービス

このような状況に対処するため，当社はISO/IEC15408認証取得支援サービスを開発し，サービスの提供を進めている。支援サービスは，セキュリティ設計支援，セキュリティ設計技術者養成支援，及び保証要件適合化支援の三つから成る。これらのうち，ここではセキュリティ設計支援について述べる。

セキュリティ設計支援には，ST（Security Target）作成支援が含まれ，ISO/IEC15408で要求されている，保護資産洗い出し～脅威分析～セキュリティ対策方針策定～セキュリティ機能要件選定～サマリ仕様設計～必要十分性分析，といった一連のST作成の流れに基づく技術支援を行う。

2.3 ST作成手順

当社が提供するISO/IEC15408認証取得支援サービスのST作成支援を，官公庁や地方自治体の行政文書を電子的に管理する行政文書管理システムのST作成に適用し，評価機関によるST評価に合格した。現在，認証機関がST評価報告を確認中である。

ST作成手順を**図1**に示し，行政文書管理システムの事例に沿ってST作成のポイントを以下に述べる。

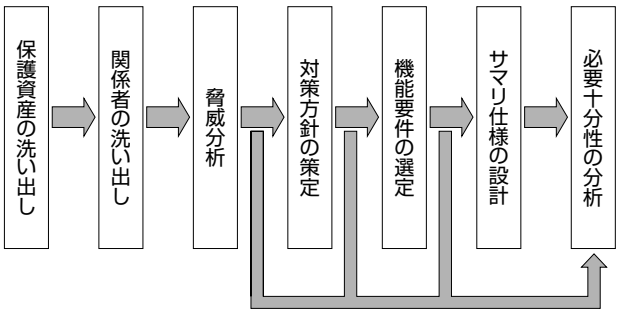

図1．ST作成手順 ― 保護資産を想定される脅威から守るための対抗策を策定する。
Security target development process

なお，今回ST評価を行った行政文書管理システムをベースに商品化してきたものが，当社の行政文書管理システムArcFort™である。

⑴ 保護資産の洗い出し　　行政文書管理システムにおける文書データといった保護すべき資産の洗い出しを行う。保護資産が決まったら，これ以降の分析や対策は，保護資産を効果的に守ることができるかどうかの観点から実施する。保護資産を明確にすることで，過剰な対策を見直すことができるようになる。

⑵ 関係者の洗い出し　　業務担当者やシステム管理者などのシステム運用・操作者だけでなく，システムにかかわる人をすべて洗い出す。例外的にしかシステムにアクセスしない保守員や，ネットワーク経由でアクセスできる人も含めて洗い出す。誰が操作，運用するかを常に考えることで，システムの利用イメージが浮かび上がってくる。

⑶ 脅威分析　　誰が，どの保護資産に，どのような手段で損害を与える可能性があるかを分析する。漠然とした脅威では対策の検討が難しくなるので，極力具体的に記述する。

⑷ セキュリティ対策方針の策定　　想定される脅威に対して対抗できる対策を検討する。対策は，システム的に実現できることだけでなく，運用で実現できることも含めて検討する。想定するシステム機能や運用環境を超えている脅威については，前提条件とすることも検討する。

⑸ セキュリティ機能要件の選定　　ISO/IEC15408（パート2）に挙げられている多数のセキュリティ機能要件から選択する。セキュリティ機能要件の関連は依存性としてリンクされているため，関係のある機能要件を芋づる式に抽出することができる。

⑹ サマリ仕様の設計　　システム構築につながる部分であるため，実装を考慮に入れて検討する必要がある。

⑺ 必要十分性の分析　　想定した脅威に対して対応できていることを，脅威～対策方針，対策方針～機能要件，機能要件～サマリ仕様のそれぞれの間で必要性と十分性を検証することで確認する。

3 ISMSによる組織としてのセキュリティの確立

3.1 ISMS

電子政府・電子自治体システムを運用する組織の情報セキュリティマネジメントも重要課題である。情報セキュリティマネジメントには，ISMSという考え方がある。

ISMSは，組織が策定した情報セキュリティポリシーに基づいて，その組織が情報セキュリティに対するプロセスを継続的に改善していく仕組みの確立を目指すものである。プロセス改善のアプローチは，いわゆるPDCAサイクル（Plan（計画）→Do（実施）→Check（点検）→Act（処置））を回していくことである。

ISMSを確立し維持していくのに必要なベストプラクティスを集めたガイドラインとして，ISO/IEC17799という国際規格がある。ISO/IEC17799には，ISMSを確立する際に管理すべき10の領域に対して，36の管理目的と127の管理策が設定されている。現在，ISMSの認証基準には，英国規格のBS7799-2と日本情報処理開発協会（JIPDEC）によるISMS適合性評価制度がある。

ISMS認証基準と詳細管理策の関連を**図2**に示す。

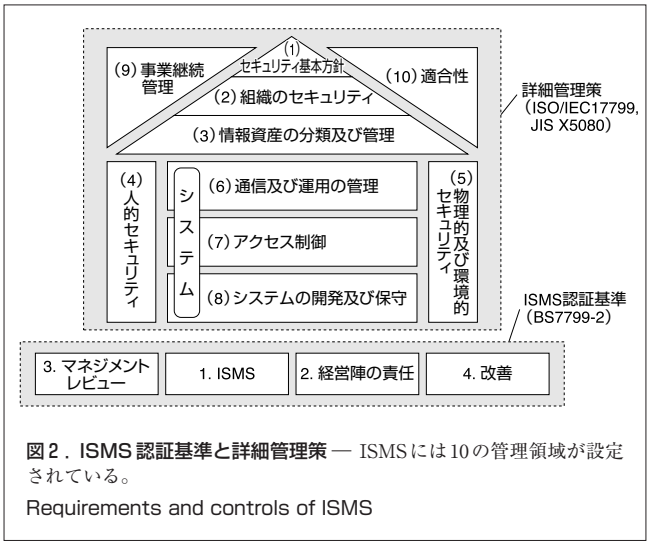

図2．ISMS認証基準と詳細管理策 ― ISMSには10の管理領域が設定されている。
Requirements and controls of ISMS

3.2 電子政府・電子自治体の情報セキュリティマネジメント

電子政府の情報セキュリティマネジメントについては，2003年7月にCIO（情報化統括責任者）連絡会議決定として公開された“電子政府構築計画”の中で，情報システムの

安全・信頼性を確保するために，各省庁は情報セキュリティポリシーに基づき，必要な対策を実施することとされている。

電子自治体においては，全国の自治体がネットワークで接続されることで，一部自治体のぜい弱性問題が全体に波及することを防ぐために，2003年8月に総務省自治行政局から公開された“電子自治体推進指針”の中で，情報セキュリティポリシーの策定と運用，及び情報セキュリティ監査の推進が示された。

情報セキュリティ監査制度は，2003年4月から運用が開始されており，組織の情報セキュリティ対策について専門知識を持つ外部専門家により，客観的に評価するものである。電子政府・電子自治体での利用が想定されており，電子政府情報セキュリティ監査基準モデルや，地方公共団体情報セキュリティ監査基準が策定されている。

3.3 当社のISMS関連サービス

当社では，ISMS関連サービスとして，組織のセキュリティへの取組みを簡易に診断する“セキュリティ初期診断サービス”，ISMSの基礎となる情報セキュリティポリシーを組織の現状に合わせて適切に策定支援する“情報セキュリティポリシー策定サービス”，BS7799-2やJIPDECのISMS認証基準に基づく認証取得を支援する“ISMS認証取得支援サービス”を提供している。

また，情報セキュリティで重要となる人の問題やシステムのセキュリティホールなどのぜい弱性に対処するために，“情報セキュリティ教育サービス”と“システムセキュリティ診断サービス”を提供している。

これらのサービスを，当社の官公情報システム部門に適用し，短期間にISMS認証を取得した。

4 特定認証対応ICカード発行ソリューション

電子政府構築計画は“利用者本位の行政サービスの提供”と“予算効率の高い簡素な政府”の実現を目指したものであり，ここで示された基本方針に沿って，各省庁が行政手続きの電子化を中心としたアクションプランを公表している[3]。中でも入札及び各種申請手続きは，電子政府構築計画の効果が十分に発揮できる分野として期待され，ほとんどの省庁は2004年度中には本格運用を計画している。特に国土交通省では，2003年度に実施が計画されていた入札の100％電子化を目標として，4月から電子入札の全面実施を開始した。こうした動きは地方自治体にも広まりつつある。

電子入札の前提となるのは，入札業者からインターネットを介して送られる入札金額などの情報を暗号化などの手段によって守り，かつ入札業者に偽りがないことを確認することができる認証基盤技術である。このため政府は“政府認証基盤（GPKI）”の構築に早期から着手し，この論文を執筆した時点では，1府10省3庁と民間事業者（団体を含む）16社の認証サービスがこの共通の認証基盤との相互認証を完了し[4]，更に地方公共団体が行う公的個人認証へと拡大している[5]。

民間業者が電子入札に参加するためには，電子署名法に基づいて認定され（特定認証事業者）かつ政府認証基盤との相互接続ができる民間認証サービス事業者から電子証明書の発行を受ける必要があり，その電子証明書を使って電子入札を行うことになる。このようにして，全国どこからでもインターネットを介して，すべての省庁あるいは地方自治体に対して入札を行うことが近い将来に可能となる。入札に用いた電子証明書が政府認証基盤と連携するようすを**図3**に示す。

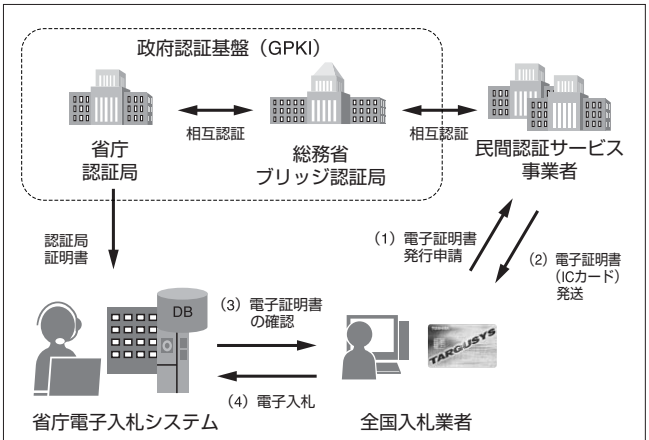

図3．政府認証基盤と電子証明書による電子入札— 総務省ブリッジ認証局と民間認証局とが相互接続することにより，民間認証局が発行したICカードで，政府が運営する電子入札システムを利用することができる。
Government PKI and electronic bidding system

当社では，独自に開発したPKI/ICカードソリューションTARGUSYS$_{TM}$[6]を使って民間認証サービス事業者向けに“特定認証対応ICカード発行ソリューション”を開発し，電子入札用ICカード発行サービスを行っている帝国データバンクの“TDB電子認証サービスTypeA[7]”において運用されている。TDB電子認証サービスTypeAは，既に15,000枚のICカード発行実績を持ち，建設業を中心として，日本全国の民間企業の電子入札で使われている。最近では，国税庁の国税電子申告・納税システムへの対応も発表され，その用途はしだいに広がりつつある。

特定認証対応ICカード発行ソリューションは，日本品質保証機構（JQA）[8]などの指定調査機関が電子署名法に基づいて行う，監査基準に適合したセキュリティ機能を持ち，かつ民間認証事業者がその認証設備を外部に委託することで，比較的短期間に電子入札向けのICカード発行サービスを開始できる点に特徴がある。

全体のシステム構成を**図4**に示す。処理の流れは次のようになる。

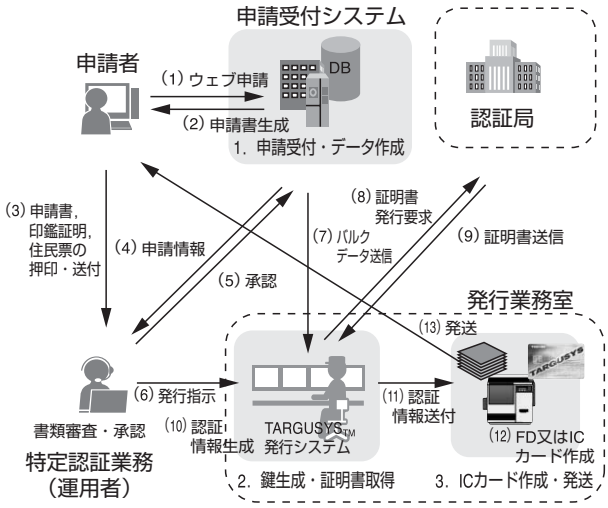

図4．特定認証局対応ICカード ソリューションシステムの構成 ― 申請受付システム，認証システム，ICカード発行システムなど，特定認証業務としてのトータルなシステムを提供する。

Authentication server smart card issuing system

⑴　申請者はインターネットにより申請受付システムにアクセスして電子証明書の発行をウェブ申請する。

⑵　申請受付システムは申請情報をデータベース化すると同時に申請書生成を行い申請者へ返す。

⑶　申請書を印刷して押印を行い申請書，印鑑証明，住民票を送付する。

⑷　特定認証サービス事業者はインターネットを介して申請受付システムのデータベースにアクセスし，申請情報を参照して書類審査を行う。

⑸　承認する。

⑹　認証設備室内にあるTARGUSYS$_{TM}$発行システムに発行指示を出す。

⑺～⑿　鍵の生成，電子証明書の発行及びICカードの作成が一括して行われる。

⒀　それを受取人限定郵便で発送する。

以上により，電子入札を行う申請者本人にICカードを確実に渡すことができ，またこのICカードに格納された署名鍵を取り出す手段はないため，安全確実に電子入札を行うことができる。

今後，電子入札はもちろん各種行政手続きの電子化が進むにつれて，政府や地方自治体が行う電子入札のように，公的な目的に使われる認証手段の用途はますます拡大していくことは確実である。また，電子契約や電子調達といった分野において，これを民間利用する試みも活発になっていくと見込まれる。

5　あとがき

住民基本台帳ICカードの不正利用が新聞紙上をにぎわすなど，電子政府におけるセキュリティの重要性は増すばかりとも言える。当社は，システムセキュリティ技術の開発に積極的に取り組み，電子政府・電子自治体の実現に貢献するとともに，その成果を民間に活用することで，安全で安心できるIT社会の実現に少なからず貢献できるものと考えている。

文　献

⑴　経済産業省．“加算方式による総合評価落札方式の導入について（情報システムに係わる政府調達制度の見直し）”．＜http://www.meti.go.jp/kohosys/press/0002961/＞，（参照2004-04-06）．

⑵　経済産業省．“情報セキュリティ総合戦略”．＜http://www.meti.go.jp/policy/netsecurity/strategy.htm＞，（参照2004-04-06）．

⑶　総務省行政管理局．“電子政府構築計画について”電子政府の総合窓口．＜http://www.e-gov.go.jp/doc/scheme.html＞，（参照2004-04-06）．

⑷　総務省行政管理局．政府認証基盤（GPKI）．＜http://www.gpki.go.jp/＞，“官職等の証明書を発行する認証局”．＜http://www.gpki.go.jp/cas/index.html＞，“申請者の証明書を発行する認証局”．＜http://www.gpki.go.jp/cas/ee.html＞，（参照2004-04-06）．

⑸　総合行政ネットワーク運営協議会．地方公共団体における組織認証基盤（LGPKI）．＜http://www.lgpki.jp/＞，（参照2004-04-06）．

⑹　能勢健一朗，ほか．PKI構築サービスとPKIカードシステムTARGUSYS$_{TM}$．東芝レビュー．**56**，7，2001，p.34－37．

⑺　帝国データバンク．TDB電子認証サービスTypeA．<http://www.tdb.co.jp/typeA/>，（参照2004-04-06）．

⑻　(財)日本品質保証機構（JQA）．“電子署名・認証”．＜http://www.jqa.jp/11it/denshininsho.html＞，（参照2004-04-06）．

北折　昌司　KITAORI Shoji

東芝ソリューション（株）プラットフォームソリューション事業部 プラットフォームソリューション第三部参事。セキュリティプラットフォームサービス業務に従事。

Toshiba Solutions Corp.

中村　宏　NAKAMURA Hiroshi

東芝ソリューション（株）官公情報システム事業部 技術管理部主任。技術管理業務に従事。

Toshiba Solutions Corp.

河本　高文　KOMOTO Takafumi

東芝ソリューション（株）官公情報システム事業部 電子政府ソリューション部主任。情報セキュリティサービスの開発に従事。情報処理学会会員。

Toshiba Solutions Corp.