「電子申請業務における X.509 属性証明書を用いた資格確認技術の開発」

平成 13 年度年次総括報告書

塚田孝則　鮫島吉喜　國廣篤史　日高智美　小野崇　三瀬修一　宮沢徹　宮崎博

日立ソフトウェアエンジニアリング株式会社

概　要

民間から行政への申請業務の多くでは、申請するための資格が必要であり、事前にその資格申請手続きを行っている。さらに申請は当事者本人が申請するとは限らず、申請者から依頼された代理人や業務担当者が申請業務を行っている場合が多い。また、官公庁や自治体での調達においては、指定業者による入札や入札基準に達した業者による入札など、資格が必要な入札がある。このように電子政府の主たる目標の一つとなっている申請業務の電子化では、申請資格や入札資格などを確認することが不可欠である。しかしながら、資格・権限確認は、これまでの公開鍵基盤（PKI）の公開鍵証明書を用いた本人確認や真正性確保では見逃されていた。本研究開発では、資格・権限確認を権限管理基盤（PMI）と属性証明書を用いて電子的に安全、確実に行う資格確認技術の開発を目指し、資格権限および属性証明書に関する調査と、属性証明書を利用した電子申請業務を行うためのシステムの設計を実施した。

1. はじめに

政府は、e-Japan 重点計画において、2003 年度末を目処に行政の効率化や国民負担の軽減を目標に行政手続きを電子化する電子政府の基盤を構築することを目指している。電子政府の構築に向けては信頼性・安全性確保のための技術や情報セキュリティ分野における基盤的ソフトウェア技術の開発が重要な課題である。

電子政府では、企業から行政への申請は電子化される。申請業務には資格が必要なものがある。例えば、道路占有許可申請には、事業免許証を持っているという資格が必要である。資格が必要な申請を電子化する場合、電子的な資格確認技術が必要となる。

図 1 に資格が必要な申請業務の流れを示す。申請を行う企業は電子的に資格申請書を行政に提出し、行政から申請された資格が付与される。業務申請においては当事者本人が申請するとは限らず、代理人が業務申請を行っている場合が多い。この場合、資格が付与された者から業務申請を行う代理人への権限委譲が必要となる。

現在の政府認証基盤で採用されている公開鍵基盤（PKI）技術では、電子的な本人確認に公開鍵証明書が用いられている。この公開鍵証明書を使って個人の認証・特定はできるが、資格や権限の認証および権限委譲の確認を行うことはできない。

この資格や権限の認証の問題を解決する技術として、権限管理基盤（PMI）と属性証明書がある。属性証明書は個人を証明するものではなく、個人が保持する資格や権限を証明する。PMI を用いた資格・権限確認技術により、申請業務の効率化と情報セキュリティの向上といった効果が期待できる。

資格確認は、これまでの情報セキュリティでは見逃される傾向にあった。現状のまま電子政府の運用が開始した場合、資格確認漏れが生じ、資格を持たない者による不正な申請が発生する恐れがある。電子政府において従来以上のセキュリティを確保しつつ、効率的な行政を実現するには、

本研究開発の成果を実際に電子政府に適用して資格確認の電子化・自動化を行うことが不可欠である。

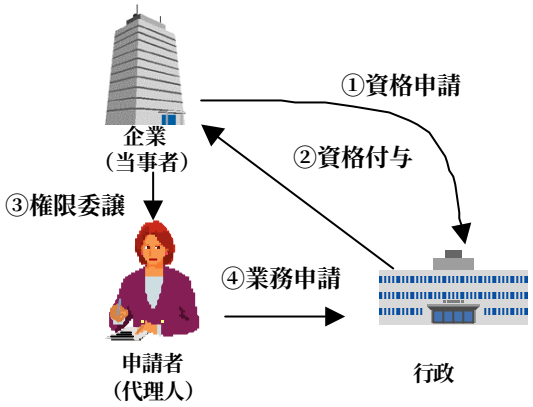

図 1 申請業務

2. 研究目標と内容

本研究開発では電子政府における安全な電子申請業務の実現にむけて、属性証明書を用いて資格を表現し、資格付与、権限委譲および資格確認を行う方式を開発することを目標としている。そこで以下の項目に重点を置き活動した。

① 電子申請業務における資格確認に必要なセキュリティ要件の明確化
② 属性証明書管理・利用ツールの方式設計
③ セキュリティ評価
④ 属性証明書管理・利用ツールの機能設計

各項目の概要を以下に示す。

2.1 電子申請業務における資格確認に必要なセキュリティ要件の明確化

資格確認の方式を設計するにあたり、現在行政で行われている申請における資格・権限の種類、資格付与や権限委譲を調査し、資格付与、権限委譲および資格確認の手続きを電子化する際に必要なセキュリティ要件を明確にすることを目標とした。

2.2 属性証明書管理・利用ツールの方式設計

属性証明書を利用した申請業務を実現するシステム「属性証明書管理・利用ツール」の設計を目標とした。調査に基づいて要件を定義し、電子申請業務のモデル化を行った。本研究開発では ITU-T・ISO で標準化されている X.509 規格にある属性証明書を採用し、申請業務における資格付与および権限委譲、資格確認方式の設計を目標とした。

2.3 セキュリティ評価

本研究開発で設計した属性証明書管理・利用ツールシステムのセキュリティ評価を受けるために、ISO/IEC 15408（コモンクライテリア）に準拠したセキュリティ要求仕様書（PP）を作成し、評価を受けることを目標とした。

2.4 属性証明書管理・利用ツール機能設計

属性証明書管理・利用ツールの機能設計を目標とした。システムを構成する各コンポーネントの機能は以下のように設計することを目標とした。

① 調査結果から導き出したセキュリティ要件を満たす
② PP で選択したセキュリティ機能を網羅する

3. 本年度の活動状況

3.1 活動内容

研究目標に挙げた活動内容の関連を図 2 に示す。

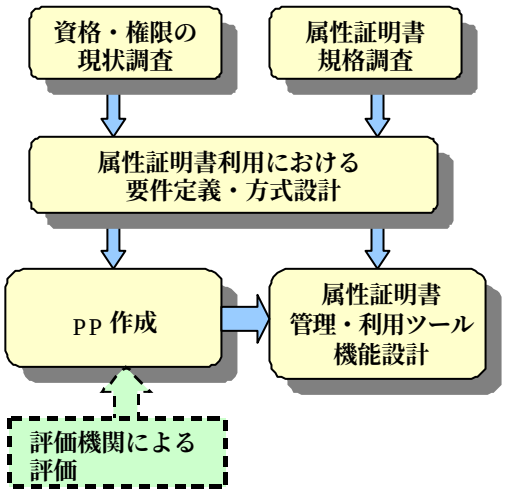

図 2 活動内容

現在行政で行われている申請業務における資格・権限の調査、属性証明書の規格調査をもとに属性証明書管理・利用ツールシステム方式設計を行った。設計したシステムの PP を作成し、さらに機能設計を行った。PP については評価機関による評価を受けた。

3.2　活動スケジュール

本年度の活動スケジュールは図 3 の通りであった。

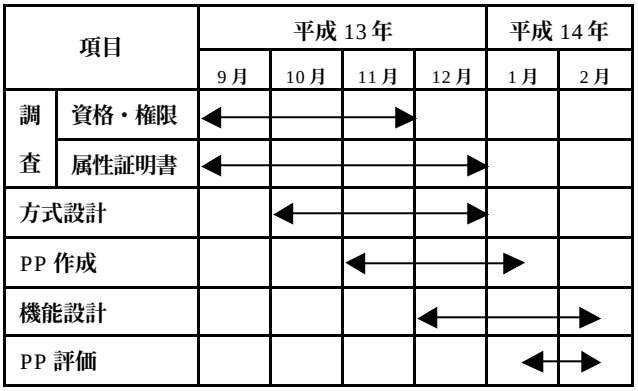

図 3 活動スケジュール

3.3　資格・権限・権限委譲の現状調査

3.3.1　調査項目

電子政府の基盤を構築するために必要なセキュリティ要件を明確にするという観点から、行政における申請業務に必要な資格・権限の種類、権限委譲および資格確認の現状について以下の項目を調査した。

① 行政への申請業務
② 行政組織間における権限委譲
③ 企業におけるワークフロー・アクセスコントロール

3.3.2　行政への申請業務

行政への申請業務のうち、電子化されているもの（表 1 項番 1-5）および電子化されていないもの（表 1 項番 6-8）について、そこで利用される資格・権限の種類、付与、確認手順を調査した。本研究開発の成果を広く電子政府へ適用するため、調査では可能な限り管轄省庁の異なるシステムを調査した。

表 1 調査した申請業務

項番	管轄省庁	システムの名称	申請の内容
1	特許庁	特許出願におけるペーパーレスシステム	特許・実用新案の出願
2	国土交通省	道路占用許可電子申請システム	道路占用許可の申請
3	国土交通省	公共調達共通基盤 電子入札システム	競争参加資格の確認申請、入札
4	法務省	債権譲渡登記オンライン申請制度	法人による金銭債権譲渡の登記申請
5	経済産業省	貿易管理オープンネットワークシステム	輸出申請
6	国土交通省	－	建設業許可申請
7	厚生労働省	－	障害者雇用調整金の申請
8	厚生労働省	－	一般労働者派遣事業許可申請

現状の申請業務を調査した結果、電子申請を行うために必要なセキュリティ要件は大きく分けると以下の 4 点になると考えられた。

① 資格付与手続きにおける被付与者の本人性確保
② 申請文書の原本性確保（完全性確保）、機密性確保
③ 申請者に与えられた資格を証明するデータ（識別番号・識別ラベル、ID/パスワード、電子証明書）の機密性確保
④ 権限を委譲した場合の権限の真正性確保

本研究開発は①と②を PKI で実現し、③と④を PMI で実現することを目指すものである。

3.3.3　行政組織間における権限委譲

行政への申請にかかわる企業内での権限委譲以外に、行政間の権限委譲というものがある。これに関しては下記の事例を調査した。

① 東京都から区への権限委譲
② 都道府県から特例市への権限委譲
③ 都道府県から市町村への権限委譲

調査・検討した結果、行政組織間における権限委譲は電子申請でいう権限委譲ではなく、権限の完全な移行であると判断し、今回設計するツールの適用は行わないこととした。

3.3.4 企業におけるワークフロー・アクセスコントロール

電子申請データのフロー制御と、データへのアクセスコントロールに関連して、システム例と製品を調査した。ワークフローに関しては、既に企業で利用しているシステム 3 例と、既存 2 製品について調査した。アクセスコントロールに関しては、既に企業で利用しているシステム 3 例と、既存 3 製品について調査した。

この調査の範囲では権限委譲の機能は見つからなかった。ワークフローでは一般に申請・審査・承認という 3 つの権限が存在していることが判明した。しかし、権限委譲の機能はワークフローやアクセスコントロール製品では実現されていないことが判明した。

3.4 属性証明書調査

3.4.1 規格調査

規格調査では X.509 で規定されている権限管理のモデルと属性証明書フォーマットについてまとめた。X.509 規格のほか、RFC やインターネットドラフトなどの調査を行い、権限利用を規定した権限ポリシー、属性証明書の属性や拡張項目（エクステンション）の定義と利用方法をまとめた。

その結果､属性証明書には以下の 3 種類があり、電子政府での資格・権限の定義、付与、委譲、確認の枠組みに利用できることが判明した。

① 属性記述証明書
② 属性証明書（権限の委譲なし）
③ 属性証明書（権限の委譲あり）

属性証明書は所有者の権限を証明する権限証明や、所有者の権限を他者へ委譲するための委任状として用いることができる。図 4 に属性証明書利用モデルを示す。ルート権限局（SOA）は属性証明書を発行し、権限局に権限を付与する。同時に、SOA は権限を定義する属性記述証明書を発行する。権限局は属性証明書を発行し、エンドエンティティ（図 4 の権限所有者）に権限を委譲する。権限所有者は権限検証者に属性証明書を提示し、権限を証明する。属性証明書利用モデルを電子申請に適用すると、権限所有者は申請者、権限局は行政となる。また権限（属性証明書）の付与・委譲・確認の基準を権限ポリシーとして定める。権限ポリシーは属性証明書から参照され、権限利用の際は権限ポリシーに従う。

場合によっては企業が行政への申請資格を失ったり、権限を委譲された従業員が退職するといった場合もある。このような場合、属性証明書が無効になる。そのため、権限検証者（行政）側では属性証明書の有効性を確認する手段が必要となる。属性証明書の有効性を確認するには権限局から発行する証明書破棄リスト（CRL）を利用する。

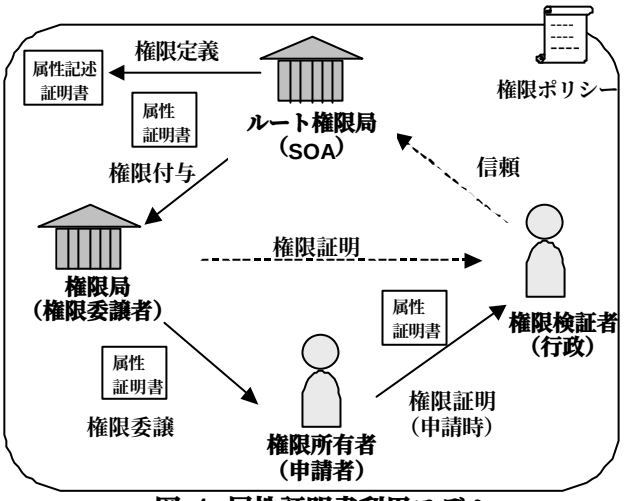

図 4 属性証明書利用モデル

3.4.2 属性証明書利用調査

属性証明書関連の製品と属性証明書の利用状況について調査を行った。現在、属性証明書を発行できる製品（権限局）は 2 製品がリリースされているが、認証局製品に比べ少ない状況であった。また、証明書破棄リストを発行する機能は持っていなかった。3.3.4 節で調査したアクセスコントロ

ール関連 3 製品では、属性証明書の利用はなかったが、他に属性証明書を利用したアクセスコントロール製品が既に 2 製品あり、どちらも情報資源へのアクセス制御を目的とした利用であることが判明した。

3.5　属性証明書利用における方式設計

3.5.1　申請業務のモデル化

3.3 節に挙げた資格・権限の調査で明確になったセキュリティ要件をもとに、資格確認方式における要件を定義し、申請業務のモデル化を行った。行政における申請業務は、業務を行う資格を取得するための資格申請と、その資格を使用して業務を行うための業務申請の 2 つに分けることができる。モデル化した申請業務の概要を図 5 に示す。

① 企業は資格申請書を作成し、行政へ提出する。
② 行政は資格申請書を受け取り、審査を行う。
③ 審査合格の場合、行政は企業へ属性証明書を発行し、資格を付与する。
④ 行政から資格を付与された者（資格保持者）と業務申請者が異なる場合、資格保持者は属性証明書を発行し、業務申請者に権限委譲する。
⑤ 資格保持者または委譲された者（業務申請者）は業務申請書を作成し、業務申請書と属性証明書を行政へ提出する。
⑥ 行政は、業務申請書と属性証明書を受け取り、資格確認と申請内容の審査を行う。

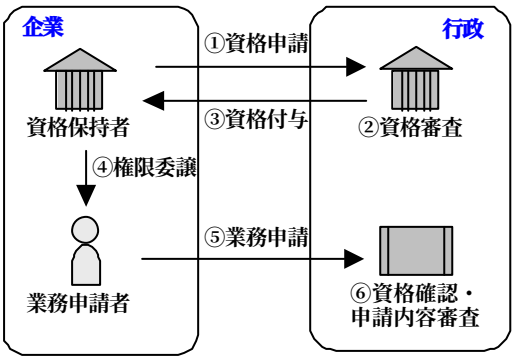

図 5 申請業務モデル

属性証明書は資格付与と権限委譲に用いられ、行政では属性証明書を検証することで業務申請者の資格を確認することができる。本人性確保のために、属性証明書は公開鍵証明書とともに用いる。

3.5.2　属性証明書フォーマットと資格表記

属性証明書の規格調査資料をもとに、属性証明書フォーマットに記述する項目と使用するエクステンションを決定した。

資格は属性証明書の属性項目（attribute）に記述する。資格表記方法については以下の 3 通りの方式を検討した。

① Role 属性（役割）を使用する方式
② Group 属性（グループ）を使用する方式
③ 独自に定義した属性タイプを使用する方式

検討の結果、府省の中で資格・権限を一意に識別する方法として③の方式を採用した。

③の方式を用いた電子政府における資格表記のために新たな属性として Privilege 属性を定義した。この Privilege 属性では行政での各資格・権限を Object Identifier（OID）で指定する。そこで、電子政府における申請業務の資格・権限表記のための OID 体系を提案した。

一方、資格・権限の申請・付与・利用に関する規定として権限ポリシーというものがある。上記 OID の体系とあわせて、この権限ポリシーの体系を定め、権限とも対応付けられるよう規定した。これら OID 体系は政府認証基盤（GPKI）政府認証基盤相互運用性仕様書にある OID 体系を拡張したものとなっている。

3.6　属性証明書管理・利用ツール機能設計

3.6.1　属性証明書を用いた資格権限確認

公開鍵証明書は認証局が発行するのに対し、属性証明書は「権限局」が発行する。また属性証明書が証明する資格の定義はルート権限局（SOA）が属性記述証明書を発行することによって行う。資格申請の結果、行政の権限局から企業の権限局に資格が付与され、企業の権限局から申請者へ権

限が委譲される。電子申請での資格権限確認では、属性記述証明書からの一連の属性証明書（属性証明書パス）と一連の公開鍵証明書（公開鍵証明書パス）の有効性を確認する。図 6 に資格確認の方式を示した。

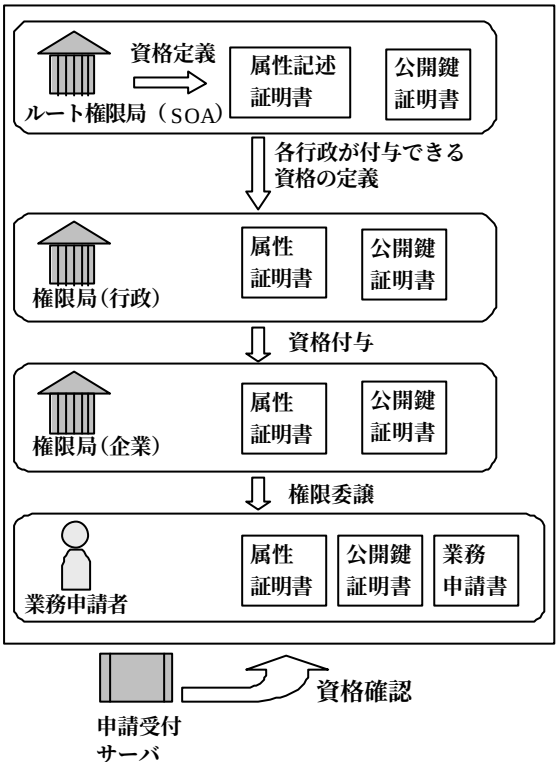

図 6 資格確認の方式

3.6.2 システム構成

モデル化した申請業務を行うシステムとして、属性証明書管理・利用ツールの機能を設計した。システムの構成を図 7 に示す。

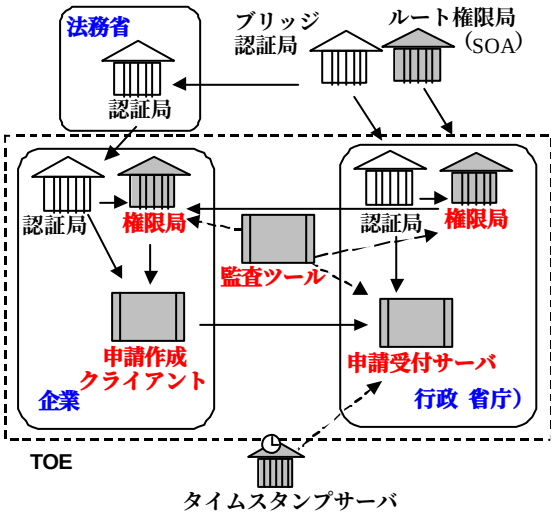

図 7 システム構成

本研究開発では権限局、申請作成クライアント、申請受付サーバ、監査ツールをセキュリティ評価における評価対象（TOE：Target of Evaluation）として、その機能を表 2 のように定義し、設計した。

表 2 コンポーネントの機能

項番	コンポーネント	機能
1	ブリッジ認証局	省庁にある認証局に公開鍵証明書を発行する。
2	ルート権限局（SOA）	省庁にある権限局に属性証明書を発行する。 属性記述証明書を発行する。
3	認証局（法務省）	認証局（企業）に公開鍵証明書を発行する。
4	認証局（行政）	権限局（行政）と申請受付サーバに公開鍵証明書を発行する。
5	認証局（企業）	権限局（企業）と申請作成クライアントに公開鍵証明書を発行する。
6	**権限局（行政）**	企業の権限局に属性証明書を発行する。
7	**権限局（企業）**	申請作成クライアントに属性証明書を発行する。
8	**申請作成クライアント**	申請受付サーバへ業務申請を行う。
9	**申請受付サーバ**	業務申請を受け付け、資格を確認する。
10	**監査ツール**	監査ログのレポートを作成する。
11	タイムスタンプサーバ	申請データのタイムスタンプを生成する。

3.6.3 セキュリティの実現

本研究開発では安全な電子申請業務の実現のための機能設計を目指した。このため機能設計では、電子申請機能の他に、PP にある各セキュリティ機能要件を実現するための機能を盛り込んだ。特に監査機能については、PP の各機能要件が要求する監査項目についても記述した。また権限局へ送付する属性証明書発行要求のフォーマットも設計書の中で規定した。

3.7 PP 作成

本研究開発で設計した属性証明書管理・利用ツールシステムについてコモンクライテリアに準拠した PP（EAL4）を作成した。作成した PP は評

価機関である電子商取引安全技術研究組合（ECSEC）による評価に合格している。

4. 外部発表及び成果物

4.1 外部発表

なし。

4.2 成果物

本年度の IPA に対する納入物件を以下に列挙する。

① 属性証明書を利用した資格権限確認方式調査報告書
② 属性証明書を利用した資格権限確認方式ガイドライン
③ 属性証明書管理・利用ツール機能仕様書
④ 属性証明書管理・利用ツール　セキュリティ要求仕様書
⑤ ④に対する評価報告書

5. 今後の課題

本研究開発は非常に広範囲に渡るシステム開発であったため、いくつか検討できなかった課題が残っている。主な課題として以下の 5 件が挙げられる。

① 検証側の権限確認
② 受信記録
③ 証明書の有効性確認
④ 申請費用の課金
⑤ 実証実験

以下に詳細を記す。

5.1 検証側の権限確認

行政組織の権限委譲にあるように、行政が法に基づいてサービス提供や許可を行っているかを国民の側が確認できる手段が必要となっている。属性証明書を用いて次の 2 つの確認に利用できる。

① 申請受付サーバの申請受付資格の確認
② 申請の審査官の審査資格の確認

まず、電子申請において申請者側にその資格や権限が存在するのと同様に、申請受付側にもその資格や権限が存在すると考えられる。申請者側から見ると、公開鍵証明書を用いて接続先の受付サーバを認証することはできるが、受付サーバがその申請を受け付ける資格や権限があることを証明するものはない。この問題を解決するために、企業側に受付サーバの資格を確認する技術として属性証明書を用いることが考えられる。

また、行政内での申請審査ワークフローにおける審査官にも属性証明書を発行し、審査記録の真正性を確認するという応用も考えられる。

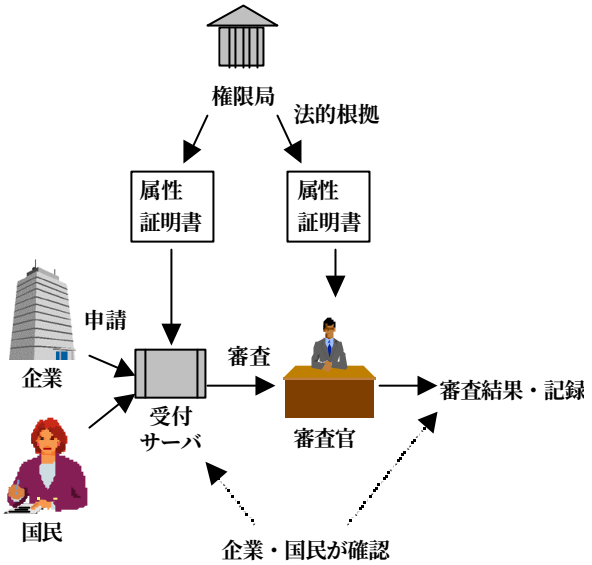

図 8 属性証明書の適用

5.2 受信記録

受信の否認防止策として、機能仕様書ではタイムスタンプサーバ（TSS）を使用することを提案している。不正な申請記録証明が行われないためにも TSS は送信側と受信側の双方から独立した第三者機関であることが望ましいと思われ、そのような機関の整備が要求される。

また、契約の成立を登録するために電子公証という仕組みがある。この電子公証の利用も検討に入れる必要もある。

5.3 証明書の有効性確認と一時失効

CRL を利用した証明書の有効性確認は、証明書破棄が多いシステムや有効性確認のリアルタイ

ム性が重要なシステムでは実用的ではない。代替手段として証明書の有効性をオンラインで確認するプロトコルである OCSP（Online Certificate Status Protocol）の利用が有効である。今後 OCSP サーバの導入も考慮に入れるべきである。

入札などの資格は一時的に資格が無効になる場合が考えられる。この場合、一旦、無効にしたい資格の属性証明書を破棄して、有効になった時に属性証明書を再発行する方法と、一時的に属性証明書を無効にする方法が考えられる。これらの方式の比較・検討が必要である。

5.4 申請費用の課金

電子化されていない申請では、手数料として証紙が貼付されるものがある。このような申請業務が電子化された場合、証紙の貼付に替わる課金方法が必要である。属性証明書に課金先を指定する方法として、Charging Identity 属性を使用することもできるが、本研究開発では課金の仕組みについて方式設計を行っていない。課金方法は電子政府の実現に向けて重要な課題になると考えられる。

5.5 実証実験

調査結果にあるように、現在、属性証明書の発行や利用が可能な製品は限られており、本研究開発で提案しているシステムを実現するには不十分な状況にある。このため、電子政府での実用性を検証するには本研究開発で設計した各ツールを開発し、実証実験を行うことが急がれる。

また、実際の電子政府への適用を考えると、法的な検討も含め、申請および申請のための資格・権限の体系化、資格・権限付与にかかわる基準の検討・整備が必要である。

6. まとめ

本研究開発を通じて、以下の成果を挙げることができた。

① 電子申請業務における属性証明書を利用した資格・権限確認方式を設計し、必要なセキュリティ要件を定義した。
② 電子政府での権限の表記方法案を規定した。
③ 属性証明書管理・利用ツールの機能仕様書を作成した。
④ 属性証明書管理・利用ツールのセキュリティ要求仕様書を作成し、評価に合格した。

本年度の活動では電子申請業務における資格確認技術の開発と題し、属性証明書の利用を前提に、資格確認方式を標準化し、属性証明書管理・利用ツールシステムの設計を行った。信頼できる安全な電子政府の実現に向け、今後残された課題に取り組んでいく必要がある。

7. 参考文献

[1] ITU-T, “Information technology - Open systems interconnection - The directory: Public-key and attribute certificate frameworks,” Recommendation X.509, March 2000.

[2] Farrell Stephen and Russell Housley, “An Internet Attribute Certificate Profile for Authorization,” Internet Draft (Work in Progress), August 2000.

[3] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, D., Holdrege, M. and D. Spence, “AAA Authorization Framework,” RFC 2904, August 2000.

[4] 塚田孝則,「企業システムのための PKI」, 日経 BP 社, 2001 年 12 月.

[5] 総務省,「政府認証基盤（GPKI）政府認証基盤相互運用性仕様書」, 2001 年 4 月.

[6] Peter Yee, “Attribute Certificate Request Message Format,” Internet Draft (Work in Progress), January 2001.

[7] 情報技術セキュリティ評価のためのコモンクライテリア　パート 1：概説と一般モデル　バージョン 2.1 CCIBM-99-031, 1999 年 8 月.

[8] 情報技術セキュリティ評価のためのコモンクライテリア　パート 2：セキュリティ機能

要件　バージョン2.1, CCIBM-99-032, 1999年8月.

[9] 情報技術セキュリティ評価のためのコモンクライテリア　パート3：セキュリティ保証要件　バージョン2.1, CCIBM-99-033, 1999年8月.

[10] ISO/IEC 15408, “Information Technology - Security techniques – Evaluation criteria for IT security - Part2: Security functional requirements,” December 1999.

[11] ISO/IEC 15408, “Information Technology - Security techniques – Evaluation criteria for IT security - Part3: Security assurance requirements,” December 1999.

[12] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1, CCIMB-99-032, August 1999.

[13] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1, CCIMB-99-033, August 1999.

[14] 情報処理振興事業協会, 「電子政府向け電子申請システムプロテクションプロファイル」, Version 1.0, 2001年6月.

[15] Annabelle Lee, NIST; et. al., “Certificate Issuing and Management Components Family of Protection Profiles,” Version1.0, National Security Agency (NSA), October 2001.

[16] Darryl Stal, “Security Target Entrust/Authority 5.1,” Version 1.4, Entrust Technologies, December 2000.

[17] 塚田孝則, 「企業を守るセキュリティポリシーとリスク評価」, 日経BP社, 2001年7月.