デジタル世界の身分証明書その 4　ー情報基盤センターPKI プロジェクトー

1. はじめに

今回は UT-CA[1][1]の電子証明書の発行・運用体制についてお知らせしようと思います。キーワードは「信頼性」です。前回(Vol8)[2]、前々回(Vol7)[3]の記事で何度も「信頼」という用語がでてきますが、それは CA[Certification Authority：PKI における認証局]の根幹となるものが「信頼性」であるからです。

一般的に CA は、運転免許証を発行する都道府県の公安委員会（運転免許センター）やパスポートを発行する外務省などに例えられます。つまり CA は、電子証明書を発行する発行機関であるといえます。

ところで、皆さんは「運転免許証」や「パスポート」を様々な場面で身分証明書として活用されていると思います。それはその発行機関を、身分証明書を確認する側である金融機関、会員制のレンタルビデオ店、携帯電話販売店などが信頼[2]しているから可能なことです。それでは身分証明書である電子証明書が、信頼できない機関から発行されたとしたらどうでしょうか？もちろん誰も信頼しないですし使えません。

そこで今回は、UT-CA を信頼していただくような根拠をできるだけ分りやすくご説明します。ただし、認証局業務の性質上、具体的に記述できないこともあります。その点はご容赦願います。

2. UT-CA の運用体制とセキュリティ

2.1 相互牽制による運用体制

UT-CA の運用体制のポリシは CA サーバ操作担当者（以下、操作者といいます）同士の相互牽制（2-person rule）です。操作者一人の不正を許さないために、サーバの操作についてはすべて 2 人による相互牽制を行っています（図 1）。

図 1　CA 操作者による相互牽制

図はイメージです（実際の操作者、セキュリティルームではありません）

1　PKI プロジェクトによる東大規模の認証局構築のためのパイロット版 CA[Certification Authority：PKI における認証局]。

2　信頼のほかにいわゆる「本人確認法」（平成 14 年法律第 32 号）などといった法的根拠は当然必要です。

また、CA 内で運用されているサーバ群（以下、CA サーバ群）を管理している保管庫の鍵も適正に管理しています。CA サーバ群の操作者は保管庫の鍵を持つことができません。一方 CA サーバ群保管庫鍵管理者は､CA サーバ群のオペレーションをすることができません(表 1)（図 2)。さらに、CA サーバ群保管庫鍵管理簿を作成し、鍵の使用開始時間、終了時間、鍵持出者、セキュリティルーム入室者を逐一管理簿に記録しています。

表 1　操作者 A、操作者 B、CA サーバ群保管庫鍵管理者のマトリックス

	CA サーバ群の操作	操作者 A の牽制	CA サーバ群保管庫の鍵管理
操作者 A	○	×	×
操作者 B	×	○	×
保管庫鍵管理者	×	×	○

図 2　UT-CA サーバ群
(現在は専用の保管庫で厳重に管理しています)

それでは具体例を挙げて CA 操作者の相互牽制をお知らせします。図 3 は UT-CA の概念図です。UT-CA の操作者は IA[Issuing Authority：発行局]サーバと RA[Registration Authority：登録局]サーバの操作を担当しますが、例えば、操作者 A が証明書発行の元になるマスタデータの更新を行った場合は、操作者 B が確認作業を行います。

ところで、図 3 に「CA がない」と気付かれたと思います。実は CA とは IA と RA およびリポジトリ（証明書データベース）を包括した総称です。

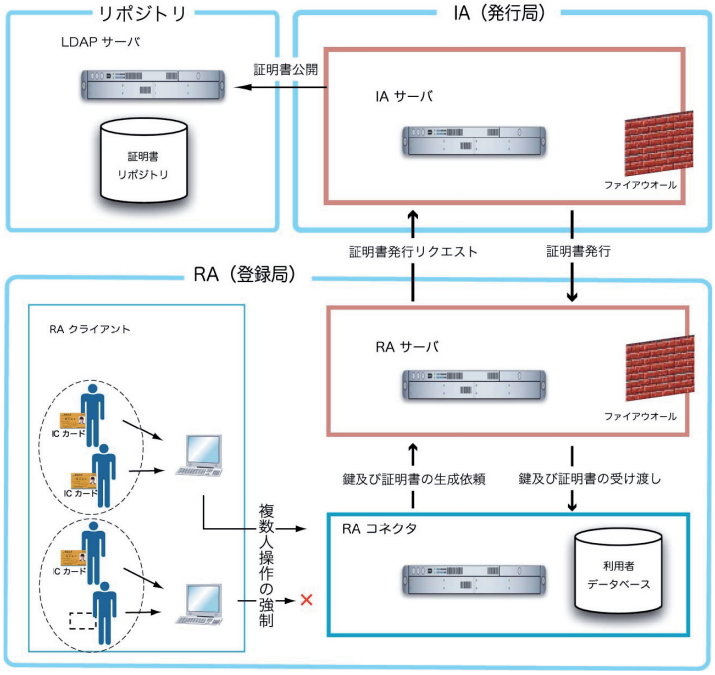

図 3　UT-CA の概念図

2.2 セキュリティ管理

CA のセキュリティ管理は、「物理的セキュリティ管理」と「技術的セキュリティ管理」があります。ここでは気軽に読めて、かつ普段知ることがないであろう「物理的セキュリティ管理」（＝セキュリティルーム）についての情報をお知らせします。ちなみに「技術的セキュリティ管理」である鍵ペアの生成、鍵サイズ、暗号モジュール技術などの話を書くとそれだけで紙面が尽きてしまうので割愛します。

それでは UT-CA の物理的セキュリティ管理についてお知らせします。

・入室するには IC カードが必要（図 4）
・さらに入室するためには、秘密のキーが必要
・複数の監視カメラで 24 時間の監視、記録を取っている（図 5）
・CA は専用の保管庫で厳重に管理し、容易に複製できない鍵を用い施錠している

また、この他の物理的な管理としては、

・水害対策のためセキュリティルームは 2 階以上に設置している
・火災対策のため火災報知機を設置している
・防犯対策のためセキュリティルームには窓がない

などといった対策[3]をしています。

3 本稿でお知らせした物理的セキュリティ管理は、認証局業界では半ば常識的になっているものです。

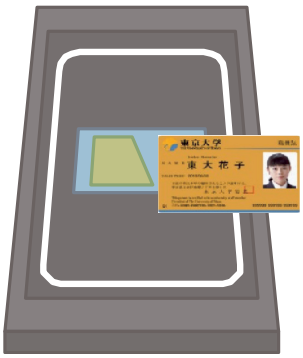

図4　IC カードとリーダ

図5　監視カメラ

図はすべてイメージです（実物とは異なります）

2.3 UT-CA の電子証明書発行・運用体制報告@名古屋大学

「面倒ではないですか？」

2007 年 3 月に名古屋大学で「総合技術研究発表会」という、大学共同利用機関および各大学・高等専門学校の技術系職員が日常業務の成果を発表する機会があり、UT-CA の電子証明書発行・運用体制の報告をしました。その発表を終えた後の質疑応答で、冒頭のような質問をされました。ここまで読まれた皆さんも同じような疑問を持たれたと思います。

答えは簡単で「そのとおり」です。ただし、次の説明も付け加えました。「電子的な身分証明書である電子証明書を発行するということは利用者に対して非常に責任のあることであり、簡単に誰にでも発行してしまえるような体制では信用問題になります。そこで誰に対しても説明ができる体制を構築する必要がありました。つまり、複数人による相互牽制や、オペレータ以外の人が CA サーバ群の保管庫の鍵を管理するなど、不正を許さない体制です。」といった回答をしました。

3. おわりに

これまでの説明は電子証明書発行局（IA）の話題が中心となりましたが、「正しい人（要件は本稿では述べませんが）に正しい手順で電子証明書利用者を登録する」という業務を行う登録局（RA）についても、ここまで説明してきたような厳格な運用をしております。

最後に繰り返しになりますが CA の根幹は「信頼性」です。容易に電子証明書が発行されたり不正が入り込む余地があったりすれば誰も信頼しません。PKI プロジェクトには、大学の特性や実情を考えた、実質的な厳格さを保証した上で合理的な体制を構築する、という課題があります。例えば予算を考慮せずに商業認証局と同等のコストをかけるならば、最も厳格な体制が構築できるでしょうが、それが大学の許容できないコストになってしまっては現実的ではありません。その見極めも PKI プロジェクトの重要なミッションの一つです。

この結論は、PKI プロジェクトが現在進行中の実証実験で得るノウハウを元に検討を重ね、最終的な UT-CA の体制をデジタルライフまたは別の広報手段でお知らせすることになります。

参考資料：

[1]http://www.pki.itc.u-tokyo.ac.jp/
[2] Digital Life Vol.8, http://www.itc.u-tokyo.ac.jp/DigitalLife/Vol8/Digital_Life_vol.8.pdf, pp36-38

[3] Digital Life Vol.7,http://www.pki.itc.u-tokyo.ac.jp/pdoc/digital_life/DL_V7_pp36-37.pdf

(大島大輔)