ＵＴ－ＣＡ　の　構　築

1.はじめに

UT-CA とは、情報基盤センターPKI プロジェクトが、東大規模の大学内での CA(PKI における認証局) の現実的な運用が可能かどうかを調査研究し、あわせて関連するノウハウを蓄積するために構築したパイロット版 CA です。われわれは、大学という「特殊」な組織で CA を運用するときに考慮しなければならない問題の洗い出しからはじめ、世間一般に認知されている電子証明書発行機関での運用との異同を明らかにしたいと考えました。この検討は、東大が PKI を内部で運用できるか、外注が必須かという意思決定をするのに非常に重要になると考えたからです。キーワードは「信頼」と「業務」、さらに「コスト」です。

電子証明書の需要は着実に増加しています。Web の認証、無線 LAN の認証や SSH の認証に電子証明書を用いることは例外的なことではありません。認証のほかに電子証明書を用いるデジタル署名や暗号化メール(S/MIME)を理解できるソフトウェアは普通のものになってきました。Grid の一部では、認証と暗号化に PKI を本格的に使うようになってきました。

このような状況の中、PKI を安定して運用し、組織のメンバーに利便性を安価にしかも安全に提供することの重要性はますますたかまっています。電子証明書を提供することがビジネスになり、実際いくつかの大手のベンダーが存在します。また、仲間内で小規模に PKI を運用して電子証明書を利用するアプリケーションを利用しているシーンも見受けられます。そのためのソフトウェアを含めたパッケージもフリーのものから、少々値の張るものまで出てくるようになりました。この世界で先進国であるアメリカでは、Educause や Internet2 といった組織で、大学で PKI を安定して運用するための研究を後押しし、ソフトウェアとドキュメントを書き続けています。

この中で、東大がどのような方向を取るのかを模索するために、UT-CA の構築と実証実験を通じてセンターは研究成果と運用ノウハウを蓄積してきました。ここでは、UT-CA 構築の動機、経緯について述べ、さらに現在進行中の実証実験について報告したいと思います。

2.UT-CA 構築の動機

PKI の構築の必要性は、セキュリティの強度を高める必要のあるアプリケーションの存在にあります。学内のサーバーの運用を見ても、プライバシーや財産に関係するものは、パスワード認証に加えて IP アドレスの制限などをかけているものが多くあります。今後、学内、または学外におけるセキュリティポリシーの厳格化にともない、パスワード認証が許されないサーバーが多く出てくることが予想されます。PKI の電子証明書による認証は現状の技術水準では（正しく運用されれば）最高水準の強度を提供するとされ、抜本的な解を与えるものと期待されます。アプリケーション側でも証明書認証に対応するものが普通に出てくるようになりました（Web 認証、無線 LAN、SSL-VPN、SSH、…)。

PKI の運用の際に一番問題になるのは、人員の配置を含めた運用体制と、関係するコストです。PKI の生命線は、「信頼」されることです。この信頼を勝ち取るためのコストはそれほど小さいものではないといわれています。この負担を合理的とみなせば内部で PKI を運用することになるし、過大と見積もれば、技術とノウハウを持ったところに外注することが合理的になります。アメリカの例を見ると、MIT や Dartmouth 大学など、著名な大学の一部では内部運用を行っています。また、外注しているところも多く見受けられます。

内部運用するにしても、外注するにしても、どこにコストがかかるかの正確な見積もりが必要です。われわれは、このコスト見積もりをしたいと考えました。

コストには、運用体制の構築と実際の運用が含まれます。特に対利用者窓口（RA: 登録局）を全部外注することは東大のような対学生、対教職員への対応組織がきちんと組織され、運用されている組織にとって必ずしも合理的とはいえません。われわれが知りたいことには、RA の運用についてのノウハウも当然含まれます。

以上のような動機で、われわれはまずパイロット CA を構築しようと考えました。パイロット版の CA を運用しながら、実地にコスト見積もりやノウハウの蓄積を図ろうとしたわけです。2005 年秋には基準と基本的な仕様を定め、発注しました。

3. 構築基準

仕様の策定のときにわれわれの定めた構築基準を以下に説明します。仕様策定までに調査はそれなりに行ってきましたが、それだけでは不十分と考え、コンサルティングを同時に入れることにしました。技術的な問題もさることながら、運用体制という組織の問題を扱うときに、コンサルティングは必須だと考えました。

3.1 大学においては分散 RA Architecture が必須

東大という組織には、複数キャンパスが存在するという意味での物理的な分散が存在します。それ以上に部局が管理の単位になっているという管理的な分散の存在を考慮に入れることが必要です。したがって、RA は部局ごとに分散して運用されなければなりません。

3.2 大学組織にあった RA の運用体制が必須

大学は、従来から学生証をはじめとして、さまざまな証明書を大量に発行してきました。それが大した事故や事件もなく運用されてきたことで、内部に運用に関してのスキルが蓄積されていると考えられます。われわれが考慮すべきは、RA を従来の事務ラインと独立に作るのではなく、教職員の士気とスキルに依存しながら、通常の事務の一環として処理できるように運用体制を構築することです。

そのためには、RA は部局ごとの分散管理が必須です。CA は、その性格上ある程度中央集権的なものですが、対利用者窓口を部局ごとに分散管理できる運用体制が組めれば、全体の業務がスムーズに回っていきます。

3.3 利用者負担を最小にすることが必須

電子証明書発行において利用者に多くを負担させることは、運用上好ましくありません。利用者は、申請したら、最小限の手間で、IC カードなどの安全な媒体に関連データが格納されることが必須です。利用者が鍵ペアを生成したり、（安全性を要求するときに）ハードディスクに格納できるようなインターフェイスを残しておくことはできるだけ避けるべきだと考えました。われわれの CA は、鍵ペアは代理生成することにしました。安全な媒体への鍵の格納に関して、RA の負担をできるだけ少なくする方法については、これからの課題です。

3.4 運用管理規定が大学の実情を反映していること

CA の運用管理規定を CP/CPS といいます。これが CA の信頼を生むもとになっています。外部から信頼を勝ち取るためには、厳格な運用管理規定を定め、さらに外部監査を定期的に受けることが必要とされています。われわれの CA は、ソフトウェアとして、安全性を担保するようなロジックを作りこみました。これには複数人操作の強制や、詳細な記録の採取が含まれます。さらに、設置場所についても、配慮をすることにしました。ただ、たとえば

Web サーバー証明書を発行しているような会社のような厳格な運用管理規定を作るか、大学の実情にあわせて投資を省略できるところはないのか、というところは考えどころです。アメリカの大学でも、ここら辺りは悩ましいところのようで、ゆるめの運用管理規定案がいくつか提案されています。もちろん、「ゆるい」運用管理規定でも、実質的に安全な運用を担保することはもちろん必要です。

4. 構築の経緯

パイロット CA である UT-CA は、前述のように 2005 年秋に設計と発注を行いました。UT-CA のメインは証明書を発行するシステム(IA)よりも、RA と運用体制です。RA は分散型のアーキテクチャと運用体制をとることにしました。IC カードとの連携について当時は良い解が見つからず、後回しにしました（現状もそうです)。証明書の発行体制については、コンサルティングを受けながら、いろいろな可能性を検討しました。UT-CA では、証明書をダウンロードする機能を作りこむことにしました。

構築は 2006 年前半に一段落し、7 月末に各方面へのデモンストレーションを行うことができました。それ以後も、実証実験に向けて小規模のアップデートを行っています。

5. 実証実験の開始

2006 年の後半は、UT-CA の実証実験をすることにしました。

PKI の需要があることは間違いないのですが、それが今すぐなのか、それとも近い将来なのかは、具体的に利用者の声を聞かないと不安なところもあります。そこで、複数の部局の協力を仰ぎ、需要調査を兼ねて実地に使ってもらうことにしました。対象としたアプリケーションは（第一弾として）S/MIME と SSL-VPN です。もうひとつ、われわれの検討した RA の分散運用が本当に機能するのかについての検証もしたいと考えました。さらに、運用管理規定の策定に向けても、どうしても実地に運用しなければならないということもありました。

幸い、情報学環に手をあげていただき、S/MIME（暗号化メール）の利用に UT-CA 発行の証明書を利用してもらうことができました。現在部局単位の RA を情報学環に設置し、具体的に窓口業務を行ってもらっています。さらに情報基盤センターにも RA を設置し、業務を開始しています。実証実験は 2007 年 3 月まで続きます。現在も、次回の UT-CA の改良に反映しなければならない、ポジティブな改善意見をもらっています。実証実験の結果は近いうちに報告できると思います。

6. おわりに

本稿では、大学における PKI の運用のために設計した UT-CA について、その構築の動機から構築基準と現在の実証実験にいたるまでの経緯を述べました。

内部統制と、セキュリティポリシーの強制、またセキュリティ強化といった自発的な動機によっても PKI のインフラとしての提供は待ったなしになってきました。今後東大でも PKI の構築が本格化すると考えていますが、その際に UT-CA の技術とノウハウの蓄積が活用できることを願っています。

（佐藤周行）