第6章 認証局ソフトウェアの要件検討

内容

- 機能分離の実現
- 権限分離の実現
- ユーザ環境の対応状況
- 業務システムとの連携

6. 認証局ソフトウェアの要件検討

6.1. はじめに

本調査研究の一環として認証局の検討を行うにあたり、運用とシステムの両面の検討を行うことに留意した。これは安全性の確保を目的としたシステムは、SI ベンダに構築の一切を任せるような手法が向いていないと考えたためである。例えば、戦国時代に活動拠点となる城を構築することを考える。運用を行う主体が、敵の侵入を遅くする、跳ね上げ橋や入り組んだ道路といった基本的な知識を持たずに、城を持つことは危険ではないだろうか。運用者が、設計者のいう通りに構築をして、城を維持し敵から身を守ることができるだろうか。また、城は防衛と同時に活動拠点でもあるため、城を守る武士は何名いるのか、何を目的とする城なのかといった要件を意識して構築しなければならない。認証局の構築においても、構築を人任せにすることで運用レベルが想定していたものと著しく異なるか、非現実的な運用コストを発生させてしまう恐れがある。

そこで本調査研究では、認証局のシステムの根幹である認証局ソフトウェアに関して、国内外のベンダ 6 社に協力を依頼し、評価・検討を行った。認証局ソフトウェアを実際に試験導入することで、そのソフトウェアが想定している環境や運用形態を理解するためである。その結果判明してきたことは、価格とともに、利用形態、想定する環境などがソフトウェアごとに様々だということである。価格が高い製品であれば適用可能性が広がるかといえば、そうではない。逆に自社の環境に適合する製品を導入すれば、開発部分を最小化させ、場合によっては設定変更だけで導入が可能になる場合があると考えられる。

本章では、認証局ソフトウェアがどのような運用や環境を想定しているのか、認証局ソフトウェアを選ぶ際のポイント、また運用の想定のために検討しておくべき点について、下記の項目に重点をおいて述べる。

- 機能分離の実現
- 権限分離の実現
- ユーザ環境の対応状況
- 業務システムとの連携

特に二番目の権限分離の実現は、安全な認証局の重点だと考えられるため、JPNIC における検討方法をまじえて説明する。また PKI の適切な普及を考えた場合に、業務システムとの連携は認証局ソフトウェアにとっての課題だと考えられるため、考察事項を交えて述べる。

また本章の最後に、一部のソフトウェアベンダに対して回答を依頼した質問表を掲載する。この質問表は CP/CPS 策定の際に作成した業務モデルを元に、ソフトウェアの構成要素ごとの質問を集めたものである。評価に先立ってこのような質問表を用意したことで、ソフトウェアの概要把握に役立った。

6.2. 機能分離の実現

認証局ソフトウェアにおける機能分離とは、概念的な認証局の機能をシステムの中で分離させることである。概念的な機能は、ITU-T の X.509 や IETF の RFC3280 における定義に加えて、慣例的な概念も使われている。

認証局の機能を分別していくとそれぞれの機能に要される安全性の要素が異なることがわかる(表 6-1)。

表 6-1 認証局の概念上の機能

機能体	役割	安全性の要素
RA	EE の登録と発行申請を受け付ける。	申請者の本人性(個人とは限らない)や申請内容に対する適切な方針の適用が要求される。受け付け機能のサービルレベルに影響する。
IA	RA によって受け付けられた発行申請を受け取り、適切なフィールドを持つ証明書の発行を行う。狭義に CA と呼ばれることがある。	恣意性を排除して証明書発行のポリシに従うことが要求される。秘密鍵の保護を担う。
PA	証明書や CRL を公開する。リポジトリとも呼ばれる。検証者や公開鍵を得ようとする EE の要求に応じて動作する。	サービスレベルに応じた公開機能の維持が要求される。CRL の配布が遅れると、失効情報の伝達が遅れ、無効な証明書を無効だと判断できない恐れがある。
VA	検証者の要求に応じて証明書の有効性を判定する。	サービスレベルに応じた検証機能の維持が要求される。検証結果に署名を行うため、鍵の管理等が必要となり、PA よりもサービスレベルの向上を図りにくい。

簡略に書くと、RA は要求をきちんと受け付けることができるか、IA は認証局の信頼に足る発行を行うことができるか、PA と VA はサービスを維持し続けることができるかといった要件を持つ、ということになる。

これらの機能の分離が、運用を検討している認証局にどこまで必要であるのかを決定する必要がある。機能の分離によって、RA は受け付け業務に専念し、IA は鍵の保護に専念するといった、保護機能の専門化を行うことができる。例えば IA はハードウェアセキュリティモジュール（以下、HSM と呼ぶ）のような特殊な機器を使って鍵を保護し、暗号鍵の漏洩やそれによる不慮の証明書発行が起こらないようにする。

一方、機能を分離しないことで生まれるメリットもある。管理の容易さ・管理人員の削減・機器の維持にかかる費用の削減といったものである。社内利用のように閉じた環境で認証局を運用したり、迅速な発行処理が必要とされたりする場合に有効である。

商用認証局ソフトウェアのうち、比較的高価なものはより細かい機能の分離を実現することが出来る。逆に比較的安価なソフトウェアは機能が一体化しているという傾向がある。

6.2.1. 機能分離の影響

認証局ソフトウェアの検討にあたり、機能分離は運用と技術の面で下記の二つの点に影響する。

- 機能を機器(または仮想的なクライアント)ごとに分離しているかどうか
- 機能間の通信プロトコルに何を利用しているか

6.2.1.1. 機能の機器ごとの分離

「機能の機器ごとの分離」は、認証局ソフトウェアの運用に影響する。運用形態を分類すると表 6-2 のようになる。

表 6-2 認証局ソフトウェア運用形態の分類

運用形態	概要
一体型	認証局が持つ全ての機能を単一のソフトウェアや機器で実現するもの。
RA-CA 型	EE の登録管理を RA で行い、特殊で高価な機器を利用する CA を分離するタイプ。
RA-IA-PA 型	RA-CA 型に加えて PA(リポジトリ)を別途に管理するタイプである。
RA-IA-PA-VA 型	VA を設けて、失効情報の伝達遅延を短縮させたり、利用者端末の単純化を図ったりしたものである。

一体型では、発行する証明書の種類の変更や証明書の状態管理に関して小回りが利く運用が可能である。技術的に複雑な設定や開発を行う必要がある場合には、一体型が向いている場合が多い。一方、登録業務と発行業務の分離といった、安全性のレベルを上げる運用には向かない。発行対象に関する情報管理や利用者ごとの発行要求の管理は別のソフトウェアで行うような場合に向いている。

次に機器の分離の型と特徴を述べる。

- RA-CA 型
  RA-CA 型では、登録管理業務を一般のオフィスで行い、HSM を利用した CA をセキュアデータセンターで管理する、といった運用形態である。
  認証局の運用を EE の登録管理であると捉え、IA や PA といった運用要件の厳しい機能を専門業者に委託するような場合にも該当すると考えられる。
  ソフトウェアの中には単一の RA で複数の CA に接続することができ、少数の管理者が複数の認証局を管理することができるものがある。

- RA-IA-PA 型
  RA-IA-PA 型では、リポジトリを別途管理することで、利用者のメンバ管理に PA を用いることができる。商用認証局ソフトウェアの典型的な型である。PA で LDAP を利用し、証明書以外の情報も一緒に管理することで社員名簿や連絡簿、社内システムのユーザデータベースとして応用することが考えられる。
  PA の運用は可用性(availability)の確保が重要である。特に失効処理の遅延に影響する。しかし、実際の運用の場では運用者の主体的な可用性の確保よりも現実的な検討が行われることが多い。つまり利用者に対して提示したサービスレベルを如何に適切なコストで維持するか、という検討方法である。このことは、次の RA-IA-PA-VA 型にも当てはまる。

- RA-IA-PA-VA 型
  RA-IA-PA-VA 型は、証明書の検証者が複雑な検証処理を行わずに、VA に任せる場合に使われる。商用認証局ソフトウェアに VA が付属していることは少なく、他製品の購入が必要なることが多い。しかし大量の証明書を発行するような大規模な運用の場面では、VA を設けるよりも PA を使った CRL の配布の方がサービス停止を避けやすく、かつ失効情報の伝達遅延が短いことがある。
  証明書検証を一手に担う VA は、求められるサービスレベルが高くなりがちである。例えば証明書検証者が 24 時間 365 日アクセス可能なサーバを用意することは容易ではない。

機器の機能ごとの分離に関する要件検討のポイントは、まず要求されるサービスレベルから認証局の型を想定し、その型で運用が可能な認証局ソフトウェアを利用することである。

6.2.1.2. 機能間の通信プロトコルの採用方法

後者の「機能間の通信プロトコルの採用方法」は、それぞれの機能がどのようなプロトコルを使って通信を行うか、という点である。

RA-IA 間でどのようなプロトコルが使われているのか、PA はどのプロトコルを利

用可能か、といったことを事前に調べておくことは、業務に合わせた認証局ソフトウェアを採用する際に有効である。

RA-IA が標準的なプロトコルを用いていると、RA に機能を付加して社内システムと連携するような開発を行うことが比較的容易にできる。RA-IA 間で使われる代表的なプロトコルに CMP(Certificate Management Protocol)がある。CMP のように、証明書の管理に適したプロトコルが利用できると RA 端末の開発が行いやすい。証明書のバルク発行のために、RA 端末プログラムが開発されていることがある。商用認証局ソフトウェアでは CMP が利用されることが多い。

PA は一般的に LDAP を用いることが多い。PA で LDAP のような標準化されたプロトコルを用いることで、オープンソフトウェアの利用など、ソフトウェアの選択の幅ができる。LDAP の他に HTTP や FTP などが利用されることもある。一方、LDAP でデータの格納に使われるオブジェクトクラスは、ベンダごとに違いがあることがある。オブジェクトクラスとは、一塊のデータが持つ値の種類を定義したものである。LDAP ではアクセスする際にオブジェクトクラスを指定して検索やデータの格納を行うため、プログラム間で共通したオブジェクトクラスを想定していないと、データの交換ができない。利用者のエントリ person 等についてはソフトウェア毎に共通している事が多い。

Web ブラウザやメールソフトの中には、電話帳のような共有データベースのために LDAP を使うことがある。Web ブラウザなどのクライアントプログラムから PA へのアクセスがある場合には、クライアントプログラムがどのようなオブジェクトクラスを想定しているのか、調査しておく必要がある。

機能間の通信プロトコルに関する要件検討のポイントは、まず RA システムや証明書発行システムの開発を行う必要があるかどうかを決めることである。開発の必要がない場合にはあまり重点をおいて検討を行う必要はない。証明書発行システムや RA にある程度の機能を実装する必要がある場合には、標準的なプロトコルを採用していて、かつその開発環境を用意できることが望ましい。

6.3. 権限分離の実現

認証局ソフトウェアの中には、証明書の管理するための権限や、認証局のシステム管理のための権限といった、権限分離の仕組みを実装しているものがある。例えば認証局のシステム管理の権限ではシステムの起動や終了等の操作しか行うことができず、証明書の発行ができない。逆に証明書の発行を承認する権限だけでは、他の操作、例えば認証局の設定が行えないなどである。変更同一内容の権限でも、複数のオペレータが揃わないと操作できない、といった合議制操作のための権限を実現したものもある。

権限の分離によって、不正の抑止／防止といった認証局の運用レベルの向上を図ることができるが、管理に要する人員が増えるなどのデメリットがある。認証局ソフトウェアがどのような権限分離に対応しているのか、それが必要十分であるかを予め調べておくことが有効である。いくつかの認証局ソフトウェアが実装している操作の権限分離機構では、下記のような役割が存在している。

- **システムの起動と終了**

  認証局システムの起動に必要な権限と、証明書の操作に必要な権限とが異なっているようなケースである。RA と PA などのサーバ毎に異なるパスワードを設定することができるものもあり、実質的に管理の分担を行うことが可能である。

- **RA 業務**

  証明書の発行や失効など、RA 業務を行う権限が設けられるケースである。

  単一の RA 端末で複数の RA 業務を行うことができるソフトウェアの場合、RA サーバが RA 端末の接続時に認証と権限の確認が行われる。

  複数の認証局の RA 業務を、単一の部署で担当し、その代わりに IA の鍵の保護をセキュアデータセンターで行うといったことが可能である。

- **監査**

  記録の監査のみを行うことができる権限が設けられるケースである。

  監査権限だけでは、RA 業務も認証局システムの設定変更を行うこともできない。認証業務の外部監査を受ける場合などに、監査人に対して監査権限のみを与えるといったことが可能である。

- **バックアップ**

  認証局の運用に関連するファイルのバックアップのみを行うことができる権限が設けられているケースである。

  バックアップの権限だけでは、RA 業務やシステムの起動や終了を行うことができない。データの遠隔地保管を行う場合など、認証業務の担当とは異なる部署でデータを

扱う必要があるときに有効である。

これらの機能の中で、運用を検討している認証局が必要としているものは何かという検討が必要である。操作の機能分離は、認証局ソフトウェアの基本的な設計方針に依存している場合が多く、特殊な役割を増やしたり操作を単純化する変更を行ったりすることは難しい。

権限分離の機能を利用するには、ソフトウェアの設定を行う前に、実際の担当者の役割を決めておく必要がある。本調査研究では下記のような手順で担当者の役割を検討した。

1. **運用レベルを決める**

   自然人の認証を可能にする認証局なのか、Web を使った商取引に利用する認証局なのか、社内で利用するローカルな認証局なのか、といった運用のレベルを決める。

   運用レベルの検討には、2002 年度の「IP アドレス認証局のあり方に関する調査研究報告書」の第 4 章が参考になる。WebTrust for CA、ECOM の認証局運用ガイドライン、特定認証業務のガイドラインを RFC2457 の目次に揃えて比較している。

2. **役割を列挙する**

   運用責任者、鍵管理者、オペレータ、監査者などの役割を列挙する。過度に詳細な役割を設けると、業務負荷が増大するだけでなく、担当者が自分の役割を忘れてしまうことがある。

   認証業務の運用にどのような役割があるかは、本報告書の第 5 章が参考になる。

   認証局ソフトウェアが規定値として設定している役割を参考にすることは有効な方法である。

3. **兼務の可能性を検討する**

   兼務ができない排他的な役割は存在するが、兼務を検討することでトレーニングコストを下げたり役割を自覚できたりするような円滑な運用を図ることができる。

   担当する部署の、具体的な人員を当てはめると検討しやすい。

   JPNIC において検討した、構成人数や兼務の可能性については本報告書の第 5 章で述べた。

4. **担当者の役割と操作体制を決定する**

   各担当者に割り当てられた役割に応じて、認証局ソフトウェアの操作の体制を決める。決定された体制に従って、権限を持つユーザをそれぞれ登録する。

以上の手法はあらゆる場面で適用可能であるとは考えにくいが、認証業務を始めるにあたって業務配分の際に参考になるものではないかと考える。

権限分離の実現に関する要件検討のポイントは、認証局の運用レベルよって異なっている。比較的高い安全性を要求される認証局の場合は、まず前述したような方法で運用体制を想定しておき、その体制を実現できるソフトウェアを利用する。限定的な発行対象しか持たない認証局の場合は、むしろ認証局ソフトウェアで実現可能な権限の分離方法を調査した方が早い。認証局ソフトウェアの中には、OS の機能等を利用してより細かい操作の権限分離ができるものがあるためである。

6.4. ユーザ環境の対応状況

高価な認証局ソフトウェアを使って発行した証明書でも、ユーザ環境で効果的に利用できなければ意味がない。想定しているユーザ環境で利用できる証明書や CRL を、認証局ソフトウェアを使って発行することができるのかどうかを、検討しておくことは重要である。

ここでいう証明書の効果的な利用とは、利用環境に適したセキュリティトークンに証明書を格納できるか、そしてアプリケーションが証明書を解釈できるか、ということである。ここでは特にユーザ環境に関係するセキュリティトークンについて述べる。

セキュリティトークンには、ハードウェアトークンとソフトウェアトークンがある。これらは実現方法がハードウェアか、ソフトウェアかという違いにとどまらず、認証局ソフトウェアに必要とされる機能が異なってくる。認証業務の形態を交えながら、違いについて述べる。

ハードウェアトークンは IC カードに代表される小型の機器である。FIPS140-1 等の安全要件を満たす製品の場合、一度 IC カードに保存された秘密鍵を外部から読み出すことが非常に難しい。証明書を IC カードという機器に結び付けて捉えることができるため、証明書と鍵ペアのコピーが作られてしまう危険を避けることができ、また鍵ペアを紛失したことを物品である IC カードの紛失によって知ることができる。

ハードウェアトークンを利用するには、鍵ペアをどこで生成し、認証局によって発行された証明書をどこで格納するかという検討を行う必要がある。社員証や学生証のような認証に用いる証明書の場合には、認証局側で IC カードを管理し配布する"センター発行モデル"が考えられる。この場合は、認証局ソフトウェアが IC カードを使った鍵生成や、IC カードにエンコードするためのデータイメージを作成することができればよい。商用の認証局ソフトウェアのいくつかは、このどちらの用途にも対応している。

ユーザ側で鍵ペアの生成を行う必要がある場合には、そのハードウェアトークンの受け渡しに留意する必要がある。ユーザ側で鍵の生成を行った後にネットワークを利用して認証局側から証明書を転送し、ハードウェアトークンに書き込む方法があるが、この方法では、ユーザが本当にハードウェアトークンを利用しているのかどうかを、認証局側から確認することができない。

遠隔地のユーザと本人確認の上でハードウェアトークンを受け渡しするには、本人確認書類と共に IC カードを持参してもらうか、本人特定郵便などを利用して、ユーザ本人が IC カードを利用する状況を作る必要がある。

ソフトウェアトークンはハードウェアトークンの機能をソフトウェアで実現したもので、SSL/TLS に対応した Web ブラウザで"証明書ストア"などと呼ばれているもの

である。予め設定したパスフレーズを入力しないと格納された鍵ペアを利用できないなど、利用方法はハードウェアトークンに似ている。しかしソフトウェアで実現されているため、データのコピーが可能であり、また認証局側から"秘密鍵をエクスポートできない"といった設定を強制することができない。

一方、ソフトウェアトークンはハードウェアトークンの利用に必要なカードリーダといった機器やドライバソフトウェアが必要ないため、多くの種類のユーザ環境で利用できる。導入コストが低く Web ブラウザを使った鍵生成と証明書の格納に対応しているため、Web インターフェースを持つ認証局ソフトウェアと通信を行って証明書の利用に使われることが多い。

Web ブラウザを使った鍵生成と証明書の格納には、認証局ソフトウェアがそのための Web サービスを提供できる必要がある。Web ブラウザ毎に対応方法が異なるため、ユーザ環境で使われる Web ブラウザに対応した認証局ソフトウェアが必要になる。

ユーザ環境の対応状況に関する要件検討のポイントは、ユーザの利用環境の中で、鍵ペアの生成と管理をどう行うか決めることである。ユーザに鍵生成をさせるか、生成された鍵はどこに保存されるか、証明書の上書きは可能か、オフラインでの受け渡しを実現する業務体制を持つかなどを決定しておくことで、どのタイプのセキュリティトークンを使用するかなどが必然的に決定されるようになる。

6.5. RA の業務システムとの連携

認証局がユーザとの接点を持つ業務は、RA 業務である。ユーザサービスの向上や業務効率の向上を考えると、RA 業務でユーザ登録や既存のユーザ情報の参照などが行われることが考えられる。つまり既存の業務システムにあるユーザ情報と認証局の持つ証明書の情報を一元的に扱う場面が、今後現れてくると考えられる。

既にグループウェアの中にはユーザ情報と証明書を連動させたものがあり、また証明書が格納された IC カードを使った社員証の発行サービスがある。

今後、PKI がより一般化するに従い業務システムと融合し、業務システムにおける認証情報の一つとして、透過的な形態で証明書を利用する場面が現れると考えられる。

本調査研究で検討したクライアント認証用の証明書は、RA 業務とアドレス資源管理業務が連携したシステムで管理することを検討している。このようなシステムを検討するには、RA と業務システムがどのようなインターフェースで連携をするのかを定めることが重要である。ここでは、RA 業務と業務システムの連携の例として、ユーザグループの扱いについて述べる。

6.5.1. ユーザグループの扱い

業務システムにおいて、あるユーザ（例えば人事課の担当者）が他のユーザ（例えば総務課の社員）のユーザ情報を作成する場面は一般的である。グループ企業の中で転勤ないし異動があれば、両企業の人事担当者が所属変更の手続きを行い、異動したユーザの業務システムにおける扱い（認証情報）を変更する。

これは、システム管理者による一元的なユーザ情報の管理とは形態が異なる。ユーザ情報の変更が人事担当者によって申請され、システム管理者によって処理されることは考えられるが、システム管理者が本人確認を行っているわけではない。

認証局における認証業務の観点でみると、これは人事課の担当者が RA 業務を行っていることになる。一つの認証局に対して複数の RA が設けられた状態である。しかしこの RA は、他の RA の担当であるグループのユーザ情報を変更することはできない。

このように、ユーザのグルーピングが行われた場面で PKI を活用するには、認証局による一つのユーザ管理ではなく、複数の RA によるグループ毎のユーザ管理が行われる必要がある。

6.5.2. 業務システムと認証局のインターフェース

証明書を業務システムにおける認証情報として利用することを考えると、証明書の発行がユーザ情報の作成であり、証明書の失効がユーザ情報の削除という意味になる。

これを実現するには、業務システムにおけるユーザ管理のユーザインターフェースにおいて RA 業務が行えるような工夫が必要である。単なる RA 端末のカスタマイズではなく、役職や担当、連絡先といった属性と共に管理できるような透過的な連携が必要である。

多くの認証局ソフトウェアは、業務システムとの連携の面で課題を持っている。グループウェアや業務システムのミドルウェアにおいて PKI を統合的に利用できるようなれば、強固な認証機能を利用した社内業務システムや、関連企業との取引に使われるシステムにおいて広範囲に普及すると考える。

認証局ソフトウェアの中には、いくつかの試みを行っているものがあり、企業ユーザによるフィードバックによって、より適切なコストの PKI が普及していくことが望まれる。

6.6. 要件検討のポイント

今回の検討を通じて得られた要件検討のポイントを項目ごとにまとめると、下記のようになる。

- 機器の機能ごとの分離
  　要求されるサービスレベルから認証局の型を想定し、その型で運用が可能な認証局ソフトウェアを利用する。

- 機能間の通信プロトコル
  　RA システムなどの開発を行う必要がない場合は、VA や PA、RA の設置に関する条件がない限り、重点をおいて検討する必要はない。RA システムや証明書発行システムの開発の必要がある場合には、標準的なプロトコルを利用しているかどうかを調べ、またその開発環境が用意できることを確認する。

- 権限分離の実現
  　高い安全性が要求される認証局の場合は、まず運用体制を想定する。その体制を実現できるソフトウェアを利用する。限られた発行対象を持つ認証局の場合は、認証局ソフトウェアで実現可能な権限の分離方法を調べ、それに合わせた運用体制を検討する。

- ユーザ環境の対応状況
  　鍵ペアの生成と管理をどこで、どのように行う必要があるかを決める。オフラインでの受け渡しがある場合には、その業務体制が確保できるかを検討する。

6.7. 質問表について

　認証局ソフトウェアの機能概要を調査するため、機能ごとの状況をたずねた質問表を作成した。これは第 4 章で述べた業務モデルに基づいて作成されており、想定した業務に適合する認証局ソフトウェアを検討するために有効であった。

　質問表は、対象別と観点別の二種類が作られた。参考のため、ここに掲載する。