CAにおける特権クライアント

4T－2

藤原 豊
NTT情報流通プラットフォーム研究所
e-mail: yutaka@isl.ntt.co.jp

1. はじめに

改ざん，なりすましなどのネットワーク上の脅威を防ぐため，公開鍵暗号方式[1]が，セキュアな情報流通を実現する上で，いっそう重要になってきている．

CA(Certification Authority)は，公開鍵暗号方式における公開鍵の持ち主を証明する公開鍵証明証(以下，単に証明証という)を発行，管理するシステムであり[2]，セキュアなイントラネット，エクストラネットを構築する際に必須のものになってきている．

本稿では，CAをイントラネット，エクストラネットに適用する場合に，CAが備えるべきクライアント識別機能について，特に企業ユースの観点から考察する．

2. 企業ユースを考えた際の課題

CAは利用者からの申請に基づき，本人であることを確認した上で，証明証の発行，無効化を行う．通常，利用者の証明証が勝手に変更されてはならないので，CAは，他の利用者の証明証を登録や無効化する行為を許さないようにしている．

しかし，企業ユースを考えたとき，組織改変などの場合に，個々の利用者が証明証の変更(無効化，登録)をCAに対して行なうのは，ネットワークトラヒックの集中によるレスポンスの悪化や，変更忘れによる新旧証明証の混在をまねく可能性があり問題である．個別に処理を行うよりは，例えば，総務担当者が，まとめて証明証の変更を行う方が効率的と考えられる．

このためには，「総務担当者」のように，CAから承認を受けたエンティティからの申請に限り，他の利用者の証明証を操作できるようにする必要がある．本稿では，他の利用者の証明証の登録・無効化ができるエンティティを特権クライアントと呼ぶこととする．

3. 特権クライアント

3.1 クライアントの識別方法

CAが一般クライアントと特権クライアントの申請を識別する方法としては，申請元のIPアドレスを用いる方法が考えられる．特定のIPアドレスからの申請であれば特権クライアントからの申請として扱う．しかし，CAをイントラネット・エクストラネット等，企業で用いることを考えたときには，組織改変に伴うネットワーク構成の変更や担当者の異動などにより，特権クライアントを物理的に固定するのは難しいことから，必ずしも有効とはいえない．また，パスフレーズを入力させることにより特権クライアントを識別する方法も考えられるが，クライアントとCA間のプロトコルを変更しなければならず，影響範囲が大きくなるという欠点がある．

そこで，このような状況に対処するため，申請者の識別名(DN: Distinguished Name)で特権クライアントを識別することとする．申請書には申請者の識別名とディジタル署名が付与されるため，ディジタル署名が検証できれば，確実に特権クライアントを識別することが可能となる．特権クライアントの公開鍵をあらかじめCAに登録しておくことにより，CAは自ら保持している証明証を用いてディジタル署名の検証が可能である．特権クライアントを変更する際には，特権クライアント

Specially authorized clients on a CA system
Yutaka FUJIWARA
NTT Information Sharing Platform Laboratories.

の証明証を無効化し，新たに公開鍵を登録すればよい．特権クライアントの公開鍵の登録は一般クライアントの公開鍵とは別の手段で登録する必要があるが，これは次節で述べる．

3.2 特権クライアントの登録と管理

特権クライアントの公開鍵を登録する際には，厳密な認証が必要である．このため，複数人による本人確認を行うなどした後，オフラインで CA に登録することが望ましい．このとき，図１に示すような管理テーブルに，識別名(DN)と他の利用者の証明証に対する操作権限を定義することとする．図１の例では，特権クライアントＡは他の利用者の公開鍵登録と証明証参照を，特権クライアントＢは証明証の無効化と参照を，そして，特権クライアントＣは，登録と無効化と参照のすべてが許可されている．また，その他のクライアント，すなわち，一般クライアントは，他の利用者の証明証に対しては，参照のみ行えるということを示している．

識別名 (DN)	証明証に対する操作		
	登録	無効化	参照
A	○	×	○
B	×	○	○
C	○	○	○
その他	×	×	○

図１　管理テーブルの例

このような管理テーブルを用いることにより，特権クライアントごとに与える権限を変えることが可能である．さらに，操作できる証明証の条件を本テーブルに付加すれば，より細かい権限付与も可能になる．例えば，操作可能な証明証の所有者の所属(識別名に含まれることが多い)を条件とすることにより，事業部ごとに特権クライアントを設けることも可能になる．

3.3 処理の流れ

クライアントより申請を受け付けた場合に，CA が証明証に対する操作を許可するか否かを判定する際の処理の流れを図２にまとめる．

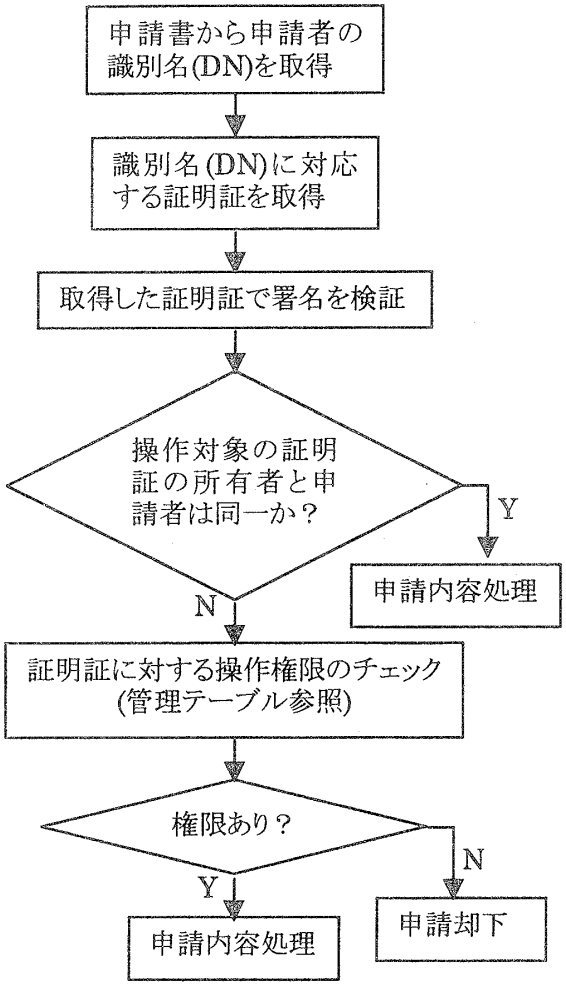

図２　処理の流れ

4. おわりに

本稿では，CA を企業内で利用するとき，組織改変などの際にも効率的な運用を可能とする「特権クライアント」について述べた．

参考文献

[1] W.Diffie and M.Hellman, "New Directions in Cryptography", IEEE Tran. on Information Theory, Vol.IT-22, No.6, pp.644-654, 1976.

[2] 中尾昌善，中原慎一，“イントラネットの実現に向けた認証システム構築技術”，NTT R&D Vol.46 No.9, pp.951(59)-958(66), 1997.