同居型複数論理CAの運用に関する一考察

6H－05

金岡　文彦　　政本　廣志
NTT情報流通プラットフォーム研究所
e-mail:{kaneoka,masamoto}@dsa.isl.ntt.co.jp

1.はじめに

近年、国内でも電子署名及び認証業務に関する法律[1]やGPKI相互運用性仕様書[2]、省庁認証局CP/CPSガイドライン[3]にCAの運用に関する方針が各省庁によって示され、認証局（CA）の正式運用が始まりつつある。[1][3]では認証局（CA）を運用するための登場人物と役割を表1にまとめたように想定されている。

表1　登場人物とその役割

登場人物	役割
CA責任者	・CA運営方針の決定 ・認証業務の統括 ・CA秘密鍵危殆化の対応統括 ・CA操作員等への操作指示及び作業結果確認 ・CAの運営及び運用の統括
CA鍵管理者（複数人）	・HSMの機能を制御する鍵（管理鍵）の保管管理 ・CA秘密鍵のバックアップ媒体の保管管理 ・CA秘密鍵生成、自己署名鍵の更新時におけるHSMに対する鍵操作 ・CA秘密鍵の更新時におけるHSMに対する鍵操作 ・CA秘密鍵のバックアップ、リストア時のHSMに対する鍵操作及び媒体セット
CA操作員	・CA秘密鍵（HSM）の活性化、非活性化 ・CAシステムの起動・停止 ・CAシステムの動作に関する設定変更管理 ・CAシステムのDBバックアップに関する諸設定並びにバックアップ、リストア、アーカイブ操作
監査人	・監査ログの検査 ・不要な監査ログの削除

A study on the operation over the multi-CAs with the different management policy
Fumihiko KANEOKA, Hiroshi MASAMOTO
NTT Information Sharing Platform Laboratories

2.現状と問題点

現状、認証局（CA）は設置場所の広さや導入費用等の要因から、一台のサーバマシンに複数の論理CAを同居させた構築が行われ運用されることがある。

しかし[1][3]では、そもそも一台のサーバマシンで動作する複数の論理CAは同じCP（Certificate Policy）の元で運用されることを想定して作成されているため、表1に示されるように、同じCPの元で運用される場合は、従来「CA責任者」が全ての複数論理CAの運用を統括していた。

そのため、複数の論理CAがCA毎に異なるCPを用いて運用を行うと、それぞれのCPが干渉しあって、マシンリソースを食いつぶしたり、他のCAの証明書発行を妨げたり、他のCAのログを参照できたりする等の新たな問題点の発生が考えられる。そこで、それぞれのCPが他のCAに干渉しないポリシ設定の範囲を統括できる人格を新たに設定する必要がでてくる。

本論文では、一台のサーバマシンに複数の論理CAを同居させた場合をモデルに構築及び運用を行っていく際、新たに発生する問題点である最低限設定すべき役割とその操作権限に関して論述する。

3.新たな人格の定義とその役割

異なる運営方針のCAの統括を行うことができる人格を新たに「サーバ管理者」として登場させる。この「サーバ管理者」が各CAの運用の統括を行うために、主に次の2つの役割を新たに持たせる事にする。

・各CAの運用の統括
・サーバマシンの維持管理

ただしこの2つの役割のうち、後者は「マシ

ン管理者」として切り出すことも可能である。

また表2に示すように、「CA 責任者」「CA 鍵管理者」「CA 操作者」「CA 監査人」も各 CA 毎に異なる CP に基づいて、それぞれ独自の役割を設定できるようにする。

表2　CP の異なる CAs の運用を行う時の役割

登場人物	役割
サーバ管理者	・異なる運営方針の CA の統括 ・サーバ root 権限の管理 ・サーバの維持管理
各 CA 責任者	・各 CA 運営方針の決定 ・各 CA の認証業務の統括 ・各 CA 秘密鍵危殆化の対応統括 ・CA 操作員等への操作指示及び作業結果確認 ・CA の運営及び運用の統括
各 CA 鍵管理者（複数人）	・HSM の機能を制御する鍵（管理鍵）の保管管理 ・CA 秘密鍵のバックアップ媒体の保管管理 ・CA 秘密鍵生成、自己署名鍵の更新時における HSM に対する鍵操作 ・CA 秘密鍵の更新時における HSM に対する鍵操作 ・CA 秘密鍵のバックアップ、リストア時の HSM に対する鍵操作及び媒体セット
各 CA 操作員	・CA 秘密鍵（HSM）の活性化、非活性化 ・CA システムの起動・停止 ・CA システムの動作に関する設定変更管理 ・CA システムの DB バックアップに関する諸設定並びにバックアップ、リストア、アーカイブ操作
各 CA 監査人	・各ＣＡの監査ログの検査 ・不要な監査ログの削除

4.各役割を実行するための操作権限の設定

CA 毎に異なる CP を用いて運用を行う場合、表2で示した「サーバ管理者」の役割を新たに加えた。そこでこの「サーバ管理者」の役割を実行するための操作を、異なる運営方針同士が干渉しあわないようにすることを想定し、表 3 にまとめる。また CA 毎に異なる CP を用いて運用を行うことで、従来[1][3]で想定されている操作のうち、各 CA 毎に複数設定可能となる操作について、表4にまとめる。

表3　サーバ管理者が行う操作

役割	操作
異なる運営方針の CA の統括	各 CA が設定する運営方針の設定範囲の確認
	各 CA の DB 等のリソース割り当て
サーバ root 権限	PWD 更新
サーバの維持管理	サーバ起動・停止
	システムバックアップ、リストア、リカバリ

表4　各 CA 毎に異なる権限設定が可能な操作

役割	操作
各 CA 運営方針の決定	発行する証明書ポリシ
	相互証明書発行ポリシ
	RL 発行間隔
	鍵更新間隔
	バックアップ、アーカイブの取得
各 CA 秘密鍵危殆化の対応統括	鍵発行、失効ポリシ
各 CA の監査ログ検査	ログ取得、検査

5.まとめ

一台のサーバマシンに異なる CP を持った複数の論理 CA を同居させた場合の構築及び運用を行う際、新たな人格である「サーバ管理者」を定義し、その人格が持つ役割を実行させるための操作権限について提案した。また従来から想定されていた操作のうち、各 CA 毎に設定変更可能な操作についてまとめた。

＜参考文献＞

[1] 電子署名及び認証業務に関する法律、http://www.meti.go.jp/policy/netsecurity/digitalsign.htm

[2] GPKI 相互運用性仕様書、http://www.gpki.go.jp/session/010514_2.pdf

[3] 省庁認証局 CP/CPS ガイドライン、http://www.soumu.go.jp/gyoukan/kanri/010514_5.pdf