（通信プロトコル・セキュリティの検討）

相互セキュリティ基盤に関する検討・認証局構築

認証局構築　調査報告書（2）

第二部　PKI を用いた総合セキュリティ基盤構築に向けた対応

平成 18 年度　経済産業省委託事業

流通システム標準化事業

目次

1. 総合セキュリティ基盤を構成する認証局の認定制度の必要性

本章では、本報告書の第一部の検討結果を受け、総合セキュリティ基盤における認定制度の必要性についての検討を行う。

1.1. 認定制度の必要性

本節では、認証局の認定制度の必要性についての整理を行う。

1.1.1. 認証局の相互運用性に関するその他の課題

本報告書の第一部においては、総合セキュリティ基盤における認証局の相互運用性について、証明書の検証についての観点のみから検討を行った。

本報告書の第一部の検討の結果のように、信頼モデルとしてマルチトラスト方式を採用することで、総合セキュリティ基盤において全ての依拠当事者が全ての利用者の証明書の検証を行うことができる。ただし、認証局の相互運用性については以下のような問題が解決されていない。

(1) 認証局の信頼性の相違

それぞれの認証局が全く異なった利用者の認証手続きを採用した場合や、それぞれの認証局が全くレベルのかけ離れたシステムセキュリティの保護を行う場合は、それぞれの認証局の信頼性は全く異なる。そのような状態では依拠当事者はそれぞれの認証局を同様に信頼することはできない。

(2) 認証局の技術仕様の相違

それぞれの認証局が全く異なった証明書プロファイルやCRLプロファイルを採用した場合や、それぞれの認証局が全く異なったCRLの配布方法を採用した場合は、依拠当事者は、それぞれの認証局が発行した証明書に同様の手続きで依拠することができない。

このような理由により、十分な相互運用性確保のために総合セキュリティ基盤で証明書を発行する認証局は、認証基準、技術仕様等の必要な部分については共通化されている必要があると考えられる。

1.1.2. 認証局を認定する機関、及びガイドラインの必要性

1.1.1項に記載したとおり総合セキュリティ基盤の認証局の相互運用性の確保のためには、認証局の認証基準、技術仕様等の共通化が必要である。ただし、認証局の運用に関わる要件については各関係者の利害等が絡むため、以下のような観点へのバランスのとれた考慮が必要と考えられる

(1) 依拠当事者が十分に認証局を信頼できる要件でなければならない

(2) 認証局が実現可能な要件でなければならない

(3) 既存の認証局を積極的に排除するような要件であってはならない
(4) 認証局に過度の負荷をあたえ、結果的に利用者に過度のコスト負荷をかける要件であってはならない

このため、全体的な観点から総合セキュリティ基盤の関係者の要望を調整し、共通化された要件を作成及び管理する機関が必要であると考えられる。

また、当該機関は、どの認証局が共通化された要件を満たす認証局なのかを利用者または依拠当事者に明確に伝える必要がある。このため、共通化された要件を満たす認証局を信頼できる認証局として認定する制度が必要であると考えられる。

なお、共通化された要件については、認定制度を円滑に運用するために、標準的なフレームワーク等に基づいて作成され、ガイドラインとして公開されるのが望ましいと考えられる。このようなガイドラインは PKI の世界では後述の CP と呼ばれるものに相当し、CP のフレームワークとしては後述の RFC3647 等が存在する。

1.2. 認定制度に関係する PKI の概念

本節では認定制度に関係する PKI の概念の整理を行う。

1.2.1. CP/CPS

PKI の世界では、認証局は、CPS(Certification Practice Statement）と呼ばれる文書を作成しこれを公開することが一般的である。CPS とは、認証局が認証業務を提供するにあたり、自身、利用者、依拠当事者等が実施すべき、または守るべき事項を定めた規程である。CPS が作成される目的には以下のようなものが含まれる。

(1) 各参加者の行動範囲の明確化
　利用者の証明書の利用範囲を明確に制限することで、利用者が認証局が想定していない分野において証明書を使用することを制限する。また、依拠当事者に証明書への依拠に関する条件を課すことで、依拠当事者の証明書への過度な信頼を抑制する等。
(2) 各参加者への技術・手続きに関する情報を提示
　証明書の形式等を開示することで、アプリケーション開発者が、証明書を利用したアプリケーションを作成することが出来るようする。また、証明書発行の際に必要となる手続きを明確に開示することで、利用者が証明書を容易に取得できるようにする等。

CPS は各認証局が個別に構成を検討して作成するのではなく、一般に IETF が作成した CP 及び CPS のためのフレームワークに従って作成される。当該フレームワークは RFC2527 と RFC2527 をアップデートした RFC3647（「証明書ポリシーと認証実践の枠組み」: Certificate Policy and Certification Practices Framework）が存在する。フレームワ

ークとしてはRFC3647の方が新しいが、既存の認証局の幾つかは構築時にRFC2527をベースとしてCPSを作成しているため、現在でもRFC2527 に準拠しているCPSにて運用を行っているところが存在する。

RFC3647が採用している構成を章レベルで以下に示す。なお、RFC3647においては章・節・項（例：1.4.1項 「適切な証明書の利用用途」）のレベルまでCP及びCPSの構成が提案されている。

(1) はじめに
(2) 公開とリポジトリの責任
(3) 識別と認証
(4) 証明書のライフサイクルに対する運用上の要件
(5) 設備上、運営上、運用上の管理
(6) 技術的セキュリティ管理
(7) 証明書、CRL、及びOCSPのプロファイル
(8) 準拠性監査とその他の評価
(9) 他の業務上の問題、及び法的問題

CP（Certificate Policy）とはCPSの上位に位置づけられる規程である。CPはPKIが利用されるある一定の領域において、そこに参画する認証局に対して一定のセキュリティ基準を課すことを目的として作成される。CPには、PKIが利用される領域において、各認証局が守るべき最低限の事項が規定されるが、各認証局が定めるCPSには各認証局の認証業務の実践内容が規定される。

ただし、PKIが利用される領域が小規模であり、当該領域で証明書を発行する認証局が一つ、もしくは少数存在しない場合は、CPとCPSは同一となる場合もある（図 1参照）。

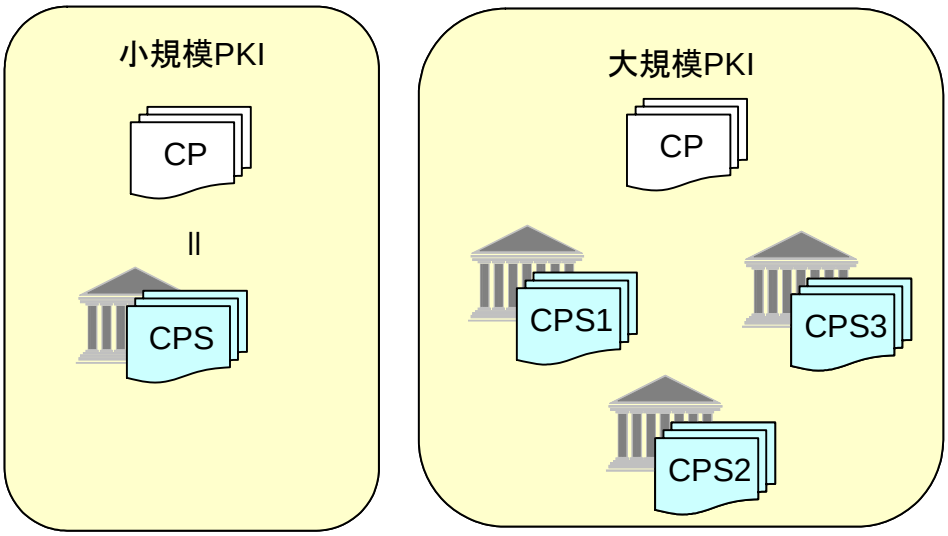

図 1　CP と CPS の関係

表 1にCP及びCPSで記載される内容の違いをまとめる。

表 1　CP と CPS で記載内容の違い

No.	内容	CP（Certificate Policy）	CPS（Certification Practice Statement）
1	適用範囲と参加者の定義	構築される PKI の全体像を示し、適用される範囲の最大範囲と制限を規定し、参加する可能性のある参加者の範囲が示される。	証明書が実際に利用できる範囲と、利用者と依拠当事者等を具体的に定める。
2	認証要件と具体的運用	PKI 内において共通に守るべき、最低限の認証要件が示される。 例 : この PKI グループの利用者は外部情報によってその存在確認が行われなければならない。	CP に規定された認証要件を満たすための具体的な方式と運用ルールを定める。 例：この認証局から証明書を受領する法人は、TDB コードによる法人の実在性確認を受けなければならない。
3	適用される技術情報と運営される PKI システムのセキュリティ	PKI において共通に準拠すべき技術要件が示される。 例 : この PKI グループに参加する認証局の公開鍵は RSA を利用した 1024 ビット以上でなければならない。	CP に規定された技術要件の具体的な実施方法を規定する。 例：この認証局の公開鍵は 2048 ビットの RSA によるものを採用する。

一般に PKI の世界では、多くの認証局が同一の PKI の利用領域の中で証明書を発行する場合は、認証局が最低限満たすべき基準として CP またはそれに準ずるガイドラインが作成される。各認証局は当該 CP またはそれ準拠するガイドラインを満たす自らの CPS を定めて公開し、それに準拠して業務を行うことで関係者に対して一定水準の信頼性を与えている

1.2.2. 準拠性監査

監査とは、ある対象について、何らかの基準に照らして証拠の収集を行い、その証拠に基づいて評価を行い、評価結果をその対象の特定の関係者に対して伝えることをいう。

PKI の世界においても認証局が CP/CPS に準拠して業務を行っていることを確実にする

ために準拠性監査が行われる場合がある。先に述べた RFC3647 等の CP/CPS のフレームワークにおいても監査に関する項目が設けられている。認証局の準拠性監査では、外部の法人等に依頼して行う外部監査や、または認証局の内部の者が行う内部監査が行われる。

2. 総合セキュリティ基盤における認証局の認定制度

本章では、認証局の認定機関に求められる要件について検討を行う。

2.1. 前提条件

本章において、認証局の認定機関に求められる要件について検討を行う際には、本報告書の第一部において検討を行った内容に従い、流通業界共通認証局の信頼モデルとしてマルチトラスト方式を採用することを前提条件とする。

2.2. 認証局の認定制度の定義

本節では認証局の認定制度の定義を行う。

「認証局の認定制度の目的」

総合セキュリティ基盤のおいて証明書を発行するための認証局が一定以上のセキュリティ要件を満たしていることを確実にするため。

「認証局の認定制度の構成要素及びその関係」

認定制度の構成要素及びその関係を表 2にまとめる。

表 2 構成要素及びその関係

No.	名称	説明
1	認定機関	流通業界の総意の基づいて設立される機関。総合セキュリティ基盤において証明書を発行することを希望する認証事業者を一定の条件を課した上で、「流通業界共通認証局」として「認定」する。認定の際には「流通業界共通認証局証明書ポリシー」と「その他の基準」に基づいて認定の判断を行う。
2	流通業界共通認証局	認定機関から認定を受けた上で、総合セキュリティ基盤の中で証明書を発行する認証局。
3	流通業界共通認証局証明書ポリシー	認証業務を実施するにあたり、流通業界共通認証局が守るべき事項を定めた証明書ポリシー。RFC3647 に従って記述が行われている。本報告書別冊を参考のこと。
4	誓約書	認証事業者が、証明書ポリシーに準拠して業務を行っていることを認定機関に確約する誓約書。
5	その他の基準	認定の際に認定機関が、流通業界共通認証局　証明書ポリシーの他に課す基準。認定取得に関わる欠格条項（個人には認定を付与しない等）等から構成される。

No.	名称	説明
6	利用者	流通業界共通認証局から証明書の発行を受けて証明書の利用を行うもの。
7	依拠当事者	認定を受けた流通業界共通認証局を信頼し、利用者から提示された証明書に依拠するもの。
8	認定	認定機関が、総合セキュリティ基盤において証明書の発行を希望する認証事業者を、証明書を発行する認証局として認める行為。認定には有効期間が設定される。また、認定を受ける事業者は必ず、誓約書を提出しなければらない。
9	認定の効果	認定を取得することにより、流通業界共通認証局は依拠当事者に信頼できる認証局としての認知を受けることが出来る。
10	初回認定	認定を取得していない認証事業者が認定を取得すること。
11	更新認定	認定を取得している流通業界共通認証局が、認定の有効期間が満了することに伴い、継続して認定を取得すること。

図 2に認証局の認定制度の概略図を示す。

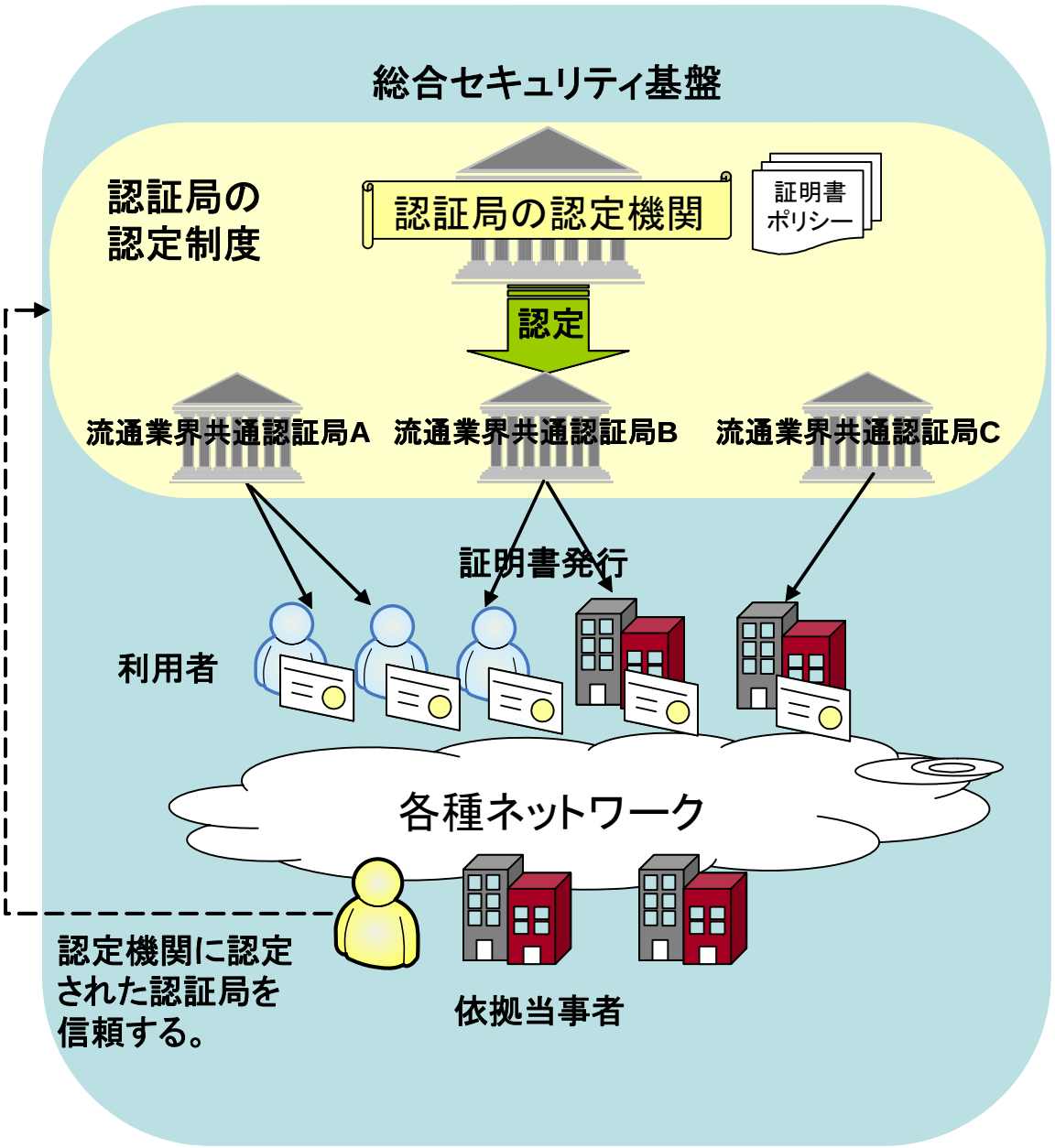

図 2　認証局の認定制度の概略

2.3. 認定機関の構成

本節では認定機関における体制の案を示す。

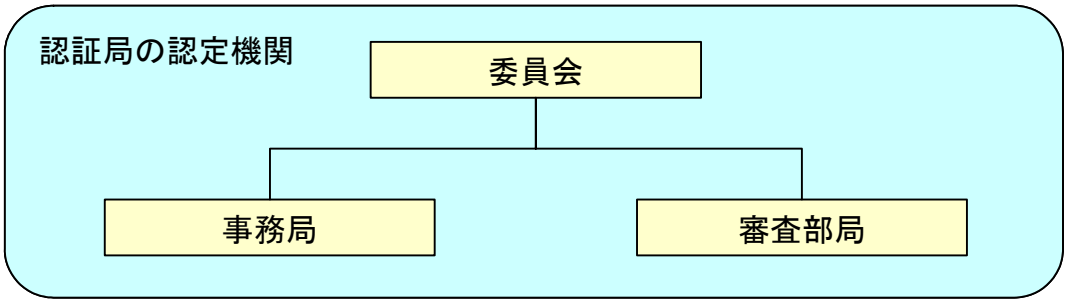

図 3　認定機関の体制

表 3　各構成要素の実施業務

No.	構成要素	役割
1	委員会	構成員の合議により下記の意思決定を行う。 • 認定付与に関する判断 • CP の改訂に関する判断 • その他基準の改訂に関する判断 • 緊急を要する外的要因発生時の対応　等 構成員の対象については別途定める。
2	事務局	認定機関の事務作業を実施。また、窓口業務や認定機関の情報公開に関する業務を行う。 • 事務処理一般 • 証明書ポリシーの公開 • 各流通業界共通認証局の認証局証明書の公開 • 認定取得・認定解除に関する情報の公開　等 事務局の対象については別途定める。
3	審査部局	認証局の認定に関わる審査業務の実務を担い、報告書を作成した上で、委員会に提出する。 審査部局については外部の法人等に委託することも考えられる。

2.4. 認定機関の業務

本節では認定機関が実施することが必要とされる業務を整理する。

表 4 認定機関の業務

No.	大分類	小分類	担当	業務内容
1	認定業務	初回認定	審査部局が証明書ポリシーへの準拠性を確認し、委員会が最終的な認定付与の判断を行う。	認定の取得を希望する認証事業者が証明書ポリシーに準拠していることを確認し、またその他の基準を満たしていることを確認した上で認定を付与する。 2.5節において詳細の業務は検討する。
2		更新認定	審査部局が証明書ポリシーへの準拠性を確認し、委員会が最終的な認定付与の判断を行う。	流通業界共通認証局が継続して、証明書ポリシーに準拠していることを確認し、またその他の基準を満たしていることを確認した上で認定を付与する。 2.6節において詳細の業務は検討する。
3		臨時審査	審査部局が、実務処理を行い、対応等については委員会が判断する。	何らかの問題が発生した場合に、流通業界共通認証局に対して臨時の審査を行う。
4	基準管理	証明書ポリシーの管理	委員会が主担当となり、連絡等の事務作業は事務局が実施する。	総合セキュリティ基盤を取り巻く環境の変化に応じて、証明書ポリシーの改訂を行う。 委員会において 1 年に 1 回は証明書ポリシーの改訂の必要性についての検討を行う。 ただし、セキュリティ上緊急を要する外的要因等が発生した場合は、委員会の構成員の発議によって臨時に委員会の召集を行い改訂の必要性の検討を行う場合がある。 なお、証明書ポリシーの改訂の必要性が認められた場合、実際の改訂業務については外部の専門業者に支援等を要請することもあると想定する。

No.	大分類	小分類	担当	業務内容
5		その他の基準の管理	委員会	証明書ポリシー以外に、認定の取得を希望する認証事業者に課す基準を管理する。
6	その他の業務	情報の公開	事務局	以下の情報を公開する（SSL を利用するものとする)。 • 証明書ポリシー • 全ての流通業界共通認証局の認証局証明書（なお、流通業界共通認証局においても自身の認証局証明書は公開しなければならない。） • 新規に認定を取得した流通業界共通認証局に関する情報 • 認定を解除された流通業界共通認証局に関する情報
7		事務処理	事務局	認定機関の運用に関する事務処理一般を行う。 事務処理には更新認定の際に、流通業界共通認証局の運用状況（証明書発行数）の確認等も含まれる。

2.5. 認定を希望する認証事業者の初回認定に関する要件

本節では認定機関が、初回認定を行う際に必要となる業務について検討を行う。

2.5.1. 準拠性の確認方法

本項では審査部局が認定を希望する認証事業者が証明書ポリシーに準拠していることの確認を行うための手法の整理を行う。なお、これらの手法はそれぞれ組み合わせることが出来るため、次節においてこれらの手法を組み合わせた監査方法の整理を行う。

表 5 準拠性の確認方法

No.	方式	概要
1	実地審査	審査部局が、認定を希望する認証事業者に出向き、認定を希望する認証事業者が証明書ポリシーを満たしていることの確認を直接行う監査手法。認証事業者の要員に対してヒアリングを行ったり、認証事業者の設備を目視で確認することなどを実施する。

No.	方式	概要
2	書類審査	審査部局が、認定を希望する認証事業者には赴かず、書面のやり取りによって認定を希望する認証事業者が証明書ポリシーを満たしていることの確認を行う監査手法。認定を希望する認証事業者は、審査部局に求められる書類を全て準備し、これを審査部局に提出する。当該書類の準備のためには内部監査を行うことが必要となる。審査部局では当該書類の内容を入念に確認することで、審査を行う。認証事業者の運用内容について疑義が持たれるような場合は、審査部局は書面による証跡の提出を認証事業者に求めることができる。
3	チェックリスト確認	審査部局は、認定を希望する認証事業者に対して証明書ポリシーへの準拠性に関するチェックリスト等を送付する。認定を希望する認証事業者は当該チェックリストに、内部監査等の結果等に基いて記入を行い、回答を行う。チェックリストにより認証事業者の証明書ポリシーの誤解釈や、対応の漏れ等を防ぐことができる。

2.5.2. 監査手法の整理

本項では適切な証明書ポリシーへの準拠性に関する監査手法の検討を行う。2.5.1項で整理した確認方法の適切な組合せを考えると以下の方式が考えられる。

表 6　監査手法のタイプ

No.	方式名	実地審査	書類審査	チェックリスト確認	特徴
1	タイプ1	○	○	○/×	• 準拠性の保証度は最も高い。 • 審査部局に高度な専門知識が要求される。 • 認定を希望する認証事業者のポリシー等により実地審査を行える対象が制限される場合がある。 • コスト面では負荷が非常に負荷が高く、利用者等への影響が懸念される。

No.	方式名	実地審査	書類審査	チェックリスト確認	特徴
2	タイプ２	×	○	○/×	• 準拠性の保証度合いはタイプ１に比べて弱い。 • 審査部局に高度な専門知識が要求される。 • コスト面の負荷はタイプ１に比べて軽いが、コスト不可は高く、利用者等への影響が懸念される。
3	タイプ３	×	△ （一部実施する。）	○	• 準拠性の保証度合いはタイプ１とタイプ２に比べて低い。ただし、書類審査を一部取り入れることで保証度合いを高くすることができる。 • 審査部局に高度な専門知識は要求されない。 • コスト面の負荷は軽い。

2.5.3. 最適な方式の検討

本項では2.5.2項で整理を行った方式のうち最も適切だと考えられる方式の検討を行う。

実現可能性の観点から考えると、タイプ１の方式は、実地審査を行うために、実現性可能性はかなり低くなる。これは、認証事業者にとっては設備やシステムセキュリティの確保の手段は重要な企業秘密に相当するため、実地審査を認証事業者が受け入れられない可能性があるためである。このため、流通業界共通認証局としての認定の窓口を広めるという立場から考えるとタイプ１を選択するのは望ましくない。

セキュリティの観点から考えると、タイプ 3 の方式は、チェックリストのみの確認によるため準拠性の確認は若干弱い。ただし、一部書面審査を取り入れることでセキュリティはそれなりに高くすることが可能である。また、認定の条件には証明書ポリシーへの準拠性の誓約書の提出が条件になるため、その他の基準等によって実績等が少ない認証事業者の参入を制限すれば、誓約書によってタイプ 3 の方式のセキュリティの弱さを補完することが可能である。

コストの観点から考えると、タイプ 2 の方式は入念な書類審査を行うためにコスト面での負荷が高い。当該コストは認定を希望する認証事業者が負担することが妥当だと考えられる。このため、当該コストは最終的には利用者の証明書取得コストに跳ね返ると考えら

れる。一方タイプ３の方式はコスト面での負荷が非常に軽いと考えられる。

このため、コスト等の負荷の問題点を考慮し、認定の方式としてはタイプ３を採用することが最適であると考えられる。

2.6. 流通業界共通認証局の認定の更新に関わる要件

本節では既に流通業界共通認証局として認定されている認証局の認定の更新に関する要件について検討を行う。

一般に各種の認定制度では、認定対象に対して認定の有効期間が設定される。当該有効期間の満了後にも継続して認定を取得したい場合、認定対象は認定機関に対して認定期間の延長を申請することが必要である。このような手続きを更新申請と呼ぶ。更新申請の際は認定機関のポリシーに応じて、認定対象に再度認定を付与して問題がないかの確認が行われる。更新申請の際の確認では、初回認定と同様の確認手続きが行われる場合や、初回認定よりも簡易な確認手続きが行われる場合がある。また、認定期間が比較的長い場合は、認定期間の途中で、維持審査と呼ばれる、認定対象に対する審査が行われることがある。維持審査では初回認定よりも簡易な審査手続きが採用されるケースが一般的である。

認証局の認定制度においても認定期間、更新認定、維持審査に関する要件を定めなければならない。認証局の認定制度においては、初回認定の要件が最低限必要となる確認レベルで設定されているために、認定期間については較的短くする必要があると考えられる。このため、認定期間については 1 年程度とし、維持審査は行わず 1 年後に更新認定を行うのが妥当だと考えられる。また、更新認定時の審査内容は初回認定と同様とするのが妥当だと考えられる。

3. 認証局の認定制度の今後の課題

本章では、認証局の認定制度について考えられる今後の課題について整理を行う。

3.1. 認定時に流通業界共通認証局が過去に発行していた証明書の扱いについて

認定制度においては、既存の認証局が認定を取得するケースが考えられる。その認定の際に確認される内容はあくまで、現在において当該認証局が認定基準を満たして業務を行っているということである。つまり、過去において当該認証局が認定基準に満たしていたかの確認は行われない。このため、既存の認証局が認定を取得する前に発行していた証明書（有効期間内にある）を総合セキュリティ基盤におけるに利用を認めるかは検討を要する。対応としては、既存の認証局が認定を取得する際に都度判断を行うか、または明確に基準を設ける等が考えられる。