金融庁クライアント証明書認証局
CP/CPS

平成 30 年 8 月 17 日

金融庁総合政策局秘書課情報化統括室

1. はじめに

本 CP/CPS は、金融庁業務支援統合システム（以下「統合システム」という。）のセキュリティ強化のため、金融庁が運営するクライアント証明書認証局（以下「金融庁 CA」という。）の認証業務に関する運営方針を定める。

現在、行政機関の認証局として、政府認証基盤のブリッジ認証局及び政府共用認証局が存在するが、認証用途のクライアント証明書は発行されておらず、また、署名用途のクライアント証明書の発行対象も行政機関内の官職等に限られていることから、政府認証基盤は利用することが出来ない。従って、金融庁専用の認証局を構築し、認証業務を行うものである。

なお、本 CP/CPS の構成は、IETF PKIX による RFC3647「Certificate Policy and Certification Practices Statement Framework」に準拠している。

1.1 概要

金融庁 CA は、不正な端末による統合システムへのアクセスを防ぎ、正当な環境下で統合システムが利用されていることを確認するために、インターネット経由で統合システムに接続する金融機関等の利用者（以下「証明書利用者」という。）に対して、認証用のクライアント証明書を発行する。

金融庁 CA は、CP（証明書ポリシ）及び CPS（認証実施規程）をそれぞれ独立したものとせず、本 CP/CPS を金融庁 CA の認証業務に関する運営方針として位置付ける。

1.2 文書名と識別

金融庁 CA の証明書ポリシは、登録された一意のオブジェクト識別子(OID)によって発行されたクライアント証明書に示される。

・ 金融庁 CA の証明書ポリシ OID：1.2.392.200091.110.207.1

1.3 PKI の関係者

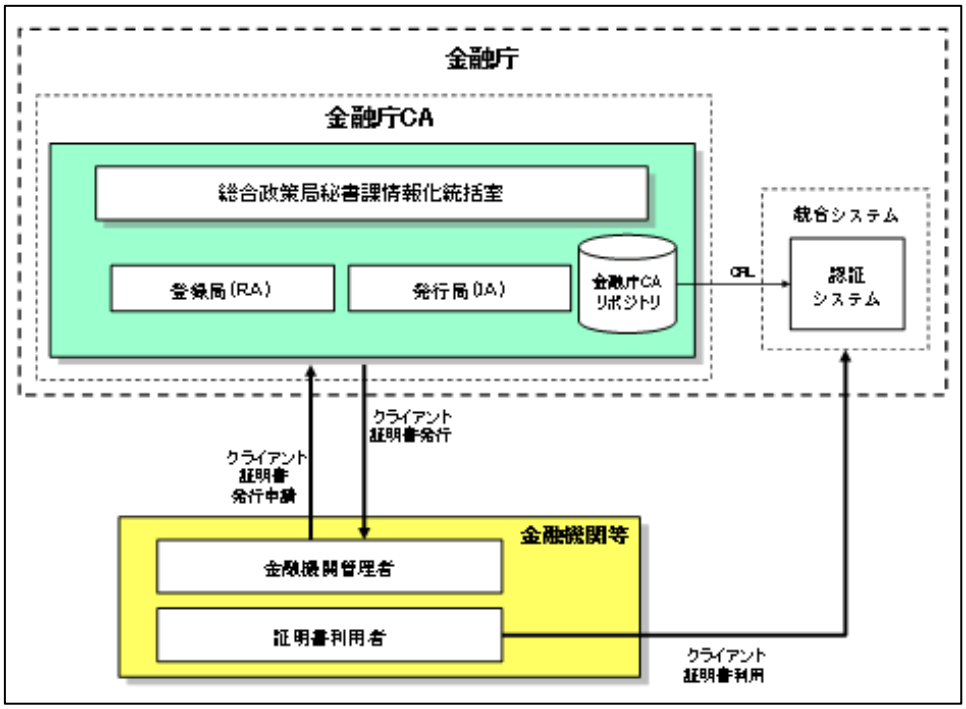

図 1-1 組織体制図

1.3.1 総合政策局秘書課情報化統括室

金融庁 CA の運営に関する意思決定は、総合政策局秘書課情報化統括室が行う。

総合政策局秘書課情報化統括室の機能は、次のとおりとする。

- 金融庁 CA の CP/CPS に関する決定
- 金融庁 CA 秘密鍵危殆化時の対応に関する決定
- 災害発生等による緊急時対応に関する決定

1.3.2 発行局（IA）及び登録局（RA）

クライアント証明書発行申請の受付及び審査並びにクライアント証明書等の発行、更新、失効等の運営業務は、承認者及び審査担当者が行う。

また、システムオペレーション、システムの維持管理等の運用業務は、サービス運用管理者、CA 管理者、RA 担当者及びログ検査者が行う。

それぞれの業務については、「5.2 手続的管理」において定める。

1.3.3 金融機関管理者

金融機関管理者とは、金融庁 CA に対してクライアント証明書の発行、失効に関する申請、発行されたクライアント証明書の管理、及び金融庁 CA との間における連絡窓口となる業務

担当者のことをいう。

1.3.4 証明書利用者

証明書利用者とは、金融庁 CA が発行するクライアント証明書を管理し、本 CP/CPS に従いクライアント証明書を利用するものであり、統合システムにアクセスする金融機関等の利用者のことをいう。

1.3.5 証明書検証者

証明書検証者とは、クライアント証明書の失効情報を公表する失効リスト（以下「CRL」という。）によりクライアント証明書の有効性を確認するものである。

1.3.6 その他関係者

規定しない。

1.4 証明書の用途

クライアント証明書は、統合システムにアクセスする証明書利用者が利用する端末を認証するために使用する。証明書利用者は、物理的、論理的にセキュリティが確保された金融機関等が業務を行うための端末のみにクライアント証明書をインストールし、利用しなければならない。また、金融庁 CA が発行するクライアント証明書を統合システムへのアクセス以外に利用してはならない。

クライアント証明書の有効期間は、証明書を有効とする日から起算して 3 年とする。

1.5 ポリシ管理

1.5.1 文書を管理する組織

本 CP/CPS の変更、更新等に関する事務は、総合政策局秘書課情報化統括室が行う。

1.5.2 連絡先

本 CP/CPS に関する照会は、総合政策局秘書課情報化統括室を窓口とする。

窓口の連絡先は、以下の URL に掲示する。

URL: http://www.fsa.go.jp/

1.5.3 ポリシを決定する者

金融庁 CA の CP/CPS を決定する者は、総合政策局秘書課情報化統括室とする。

1.5.4 承認手続

金融庁 CA の CP/CPS は、総合政策局秘書課情報化統括室の決定をもって有効なものとする。

1.6 定義と略語

＜アルファベット＞

・ CA（Certification Authority：認証局）

IA 及び RA により構成され、証明書の発行・更新・失効、CA 等秘密鍵の生成・保護及び証明書利用者の登録を行う機関。単に CA と言う場合は証明書発行業務及び登録業務を含む。

・ CP/CPS（Certificate Policy：証明書ポリシ/Certification Practices Statement：認証実施規程）

CP ：CA が証明書を発行する際の運用方針を定めた文書。

CPS：CA の信頼性、安全性を対外的に示すために、CA の運用、証明書ポリシ、鍵の生成・管理、責任等に関して定めた文書。証明書ポリシが何を運用方針にするのかを示すのに対して、認証実施規程は運用方針をどのように適用させるのかを示す。

・ CRL(Certificate Revocation List：証明書失効リスト)

証明書の有効期間中に、秘密鍵の危殆化等の事由により失効されたクライアント証明書のリスト。このリストには、失効した証明書を発行した CA の署名が付与される。

・ FIPS 140-2(Federal Information Processing Standard)

米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のことをいう。最低レベル 1 から最高レベル 4 まで定義されている。

レベル 1：FIPS で定義している最低限のセキュリティレベル。一般的な PC に適用されているような暗号モジュールに適用されているレベル。

レベル 2：暗号モジュールに、不正アクセスされた場合に、侵入の痕跡を残せるような仕組みを備えているレベル。

レベル 3：暗号モジュールに、不正アクセスされた場合に、侵入の痕跡を残せるような仕組みを備えている。レベル 2 に比べ、痕跡をより厳密に追跡できるような仕組みを備えているレベル。特殊なハードウェア装置を使い、侵入があった場合にはデータを消去するような仕組みをもつ。

レベル 4：FIPS で定義している最高のセキュリティレベル。温度の変化や電流の変化等

の環境の変動も検知できるような仕組みを導入しているレベル。

・ HSM（Hardware Security Module：ハードウェアセキュリティモジュール）
私有鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用する耐タンパー機能を備えた暗号装置のこと。

・ IA（Issuing Authority：発行局）
CA の業務のうち、証明書発行業務を行う機関。

・ IETF（Internet Engineering Task Force）
インターネットの技術的活動部会。インターネットにおけるプロトコルの技術開発、標準化を主な目的としている。作成された仕様は RFC（Request For Comments）と呼ばれる。

・ ITU (International Telecommunication Union)
国際連合(UN)の専門機関の１つである国際電気通信連合。電気通信の改善、合理的利用を目的としている。

・ ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)
国際電気通信連合の電気通信標準化部門。

・ OID（Object Identification：オブジェクト識別子）
ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関（ISO、ITU）に登録された、世界中のネットワーク間で一意となる値のこと。PKI で使うアルゴリズム、証明書内に格納する名前（subject）のタイプ（Country 名等の属性）等は、オブジェクト識別子として登録されているものが使用される。

・ PKI（Public Key Infrastructure：認証基盤）
公開鍵の正当性を保証する公開鍵証明書を利用するための基盤。

・ PKIX(Public-Key Infrastructure (X.509))
IETF セキュリティ分野の１つの作業部会。証明書及び CRL のプロファイル、CP と CPS のフレームワーク等の制定を目的としている。

・ RA（Registration Authority：登録局）
CA の業務のうち、登録業務を行う機関。主な業務は、証明書発行に必要な情報の登録、

IA に対する証明書発行要求等である。

・ RFC3647（Request For Comments3647）

RFC とは、インターネットに関する標準文書の総称。その１つである RFC3647 は、CP 又は CPS を作成するためのフレームワーク及びガイドラインを提供している。

・ RSA

公開鍵暗号方式で利用する暗号アルゴリズムの１つ。十分に大きな２つの異なる素数を掛け合わせた整数の素因数分解が困難であることに安全性の根拠をおく。

・ SSL（Secure Socket Layer）

サーバとクライアント間の通信の暗号化と認証を行い、安全にデータをやりとりするプロトコル。

・ X.500 識別名(DN: Distinguished Name)

X.500 とは、名前及びアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的に ITU が開発したディレクトリ標準。X.500 識別名は、X.509 の発行者名及び主体者名に使用される。

・ X.509

ITU－T が定めた証明書及び CRL のフォーマット。X.509 v3(Version 3)では、任意の情報を保有するための拡張領域が追加された。金融庁 CA では、証明書は X.509 v3、CRL は X.509 v2 を使用する。

＜五十音順＞

・ アーカイブ

証明書の発行履歴、失効履歴等を長期間保管すること。

・ アクセス制御

コンピュータ等、情報の供給源への不正アクセスを防止するための制御機能。アクセス者を識別し、本人であることを確認したうえで、予め設定してある権限（読出し、書込み等）の操作を可能にする。

・ アルゴリズム

計算や問題を解決するための手順、方式。

・ 暗号モジュール

暗号化、復号、デジタル署名、認証技術、乱数生成などの暗号化機能を実装したハードウェア、ファームウェア、ソフトウェア及びその組み合わせ製品。

・ 改ざん

データの内容を書き換えられること。

・ 鍵のサイズ（鍵長）

暗号の強度を決定する要素の１つ。鍵の長さをビット数で表したものが鍵のサイズであり、鍵のサイズが大きいほど暗号の強度は増す。

・ 鍵ペア

公開鍵暗号方式における公開鍵と秘密鍵のペア。一方の鍵から他方の鍵を導き出せない性質を持つため、一方（秘密鍵）を秘密にすることで、他方（公開鍵）を公開することができる。本 CP/CPS においては、金融庁 CA の鍵ペアを「金融庁 CA 鍵ペア」といい、証明書利用者の鍵ペアを「証明書利用者鍵ペア」という。

・ 活性化

システム、装置等を使用可能な状態にすること。

・ 活性化データ

システム、装置等を活性化するために必要となるデータ（パスワード等）。

・ 危殆化

信頼性が喪失された可能性のある事態の発生をいう。CA の場合、CA 秘密鍵が危殆化することによって、発行したすべての証明書の信頼性が失われる。

・ 公開鍵

公開鍵暗号方式において用いられる鍵ペアの一方。秘密鍵に対応する、公開されている鍵。本 CP/CPS においては、金融庁 CA 秘密鍵に対応する公開鍵を「金融庁 CA 公開鍵」といい、証明書利用者秘密鍵に対応する公開鍵を「証明書利用者公開鍵」という。

・ 公開鍵暗号方式

メッセージを暗号化した鍵と異なる鍵を用いて復号する暗号方式。代表的なものに RSA 暗号方式がある。

・ コンピュータセキュリティ

コンピュータシステムを中心とした情報処理活動に関する資産を、それを取り巻く脅威から保護し、情報の機密性、完全性及び可用性を満たすための対策。

・ 失効リスト

「CRL」参照。

・ 主体者名

証明書を所有し、証明書に格納されている公開鍵に対応する秘密鍵を所有している証明書利用者を識別する名前。

・ 証明書（公開鍵証明書）

ある公開鍵を、記載されたものが保有することを証明する電子的文書。CA が記載内容を確認のうえ、CA の署名を付与することで、その公開鍵の正当性を保証する。

金融庁 CA が発行する証明書は次の通りである。

金融庁 CA 証明書	:	金融庁 CA の公開鍵に対して、金融庁 CA の秘密鍵を用いて署名を付すことで発行される電子証明書
クライアント証明書	:	証明書利用者の公開鍵に対して、金融庁 CA の秘密鍵を用いて署名を付すことで発行される電子証明書。

・ 証明書発行要求（CSR：Certificate Signing Request）

証明書を発行する際の元となるデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。

・ 署名（デジタル署名）

公開鍵暗号方式の秘密鍵を利用した、メッセージの完全性を保証する仕組み。メッセージの送信者が保有する秘密鍵でメッセージのハッシュ値を暗号化し、メッセージに付与すること。メッセージ受信者側は、署名者の公開鍵を用いて、送信者の本人確認及びメッセージの改ざん検知を行う。

・ タイムスタンプ

電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。

・ 発行者名

証明書を発行し署名を施した CA を識別する名前。

・ 非活性化

システム、装置等を使用不可能な状態にすること。

・ 秘密鍵

公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、本人のみが保有する鍵。本 CP/CPS においては、金融庁 CA が保有する秘密鍵を「金融庁 CA 秘密鍵」といい、証明書利用者が所持する秘密鍵を「証明書利用者秘密鍵 」という。

・ 秘密鍵の預託

本人しか持ち得ない秘密鍵を第三者に預けること。

・ フィンガープリント

任意のメッセージに対するハッシュ値。ハッシュ関数の性質で一意に決まることからフィンガープリント（指紋）と呼ばれる。

・ プロファイル

証明書及び CRL に含まれるデータの内容を定義したもの。RFC5280 により証明書及び CRL のプロファイルについて定義されている。

・ リポジトリ

証明書及び CRL 等を格納し公表するデータベース。

・ ログ

コンピュータ上で行った操作及び処理を記録したファイル。

2. 公表とリポジトリの責任

2.1 リポジトリ

金融庁 CA に関する情報は、リポジトリ及び Web で公表する。

2.2 証明情報の公表

(1) リポジトリ上での公表

次の情報をリポジトリに登録し、公表する。

- 金融庁 CA 証明書
- CRL

(2) Web での公表

次の情報を Web に登録し、公表する。

- 金融庁 CA 証明書のフィンガープリント
- 金融庁 CA 秘密鍵危殆化に関する情報
- 本 CP/CPS
- 証明書利用者向けのマニュアル

2.3 公表の時期又は頻度

公表する情報の更新頻度は次のとおりとする。

- 金融庁 CA 証明書（フィンガープリントを含む）及び CRL は、発行及び更新の都度
- 本 CP/CPS 及び証明書利用者向けのマニュアルは、変更の都度
- 金融庁 CA 秘密鍵危殆化に関する情報は、事象発生時

2.4 リポジトリ及び Web へのアクセス管理

リポジトリ及び Web 上で公表する情報については、特段のアクセス制御は行わない。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

金融庁 CA が発行するクライアント証明書の発行者名及び主体者名は、X.500 識別名（DN:Distinguished Name）の形式に従って設定する。

3.1.2 名前が意味を持つことの必要性

クライアント証明書において使用する名前は、金融庁 CA が定める一意の値とする。

3.1.3 証明書利用者の匿名性又は仮名性

「3.1.2.名前が意味を持つことの必要性」のとおりとする。

3.1.4 様々な名前形式を解釈するための規則

様々な名前形式を解釈するための規則は、X.500 シリーズの識別名規定に従う。

3.1.5 名前の一意性

金融庁 CA の発行するクライアント証明書の主体者名は、証明書利用者ごとに一意に割り当てる。

3.1.6 認識、認証及び商標の役割

規定しない。

3.2 初回の識別と認証

3.2.1 証明書利用者秘密鍵の所持を証明する方法

クライアント証明書の申請手続において、金融庁 CA は証明書発行要求の署名の検証を行い、含まれている証明書利用者公開鍵に対応する証明書利用者秘密鍵で署名されていることを確認する。

3.2.2 組織の認証

クライアント証明書の申請手続において、金融庁 CA は、証明書利用者の属する組織の実在性を確認する。

3.2.3 個人の認証

クライアント証明書の申請手続において、金融庁 CA は金融機関管理者の実在性を確認する。なお、証明書利用者の確認は行わない。

3.2.4 検証されない証明書利用者の情報

金融庁 CA は、証明書利用者の情報は所持しないため、該当しない。

3.2.5 権限の正当性確認

金融機関管理者の権限の正当性確認は、「3.2.3 個人の認証」において定める手続に基づいて行う。

3.2.6 相互運用の基準

該当しない。

3.3 更新申請時の識別と認証

3.3.1 通常の更新時における識別と認証

クライアント証明書の有効期間が満了する際は、金融庁 CA より金融機関管理者に対して更新通知を行う。金融庁が統合システムの利用を許可している限り、更新時に特段の認証は行わない。

3.3.2 失効後の再発行時における識別と認証

クライアント証明書失効後の再発行時における識別と認証は、「3.2 初回の識別と認証」において定める手続に基づいて行う。

3.4 失効申請時の識別と認証

クライアント証明書の失効時における識別と認証は、「3.2.2 組織の認証」及び「3.2.3 個人の認証」において定める手続に基づいて行う。

4. クライアント証明書のライフサイクルに対する運用上の要件

4.1 クライアント証明書申請

4.1.1 証明書申請者

金融庁 CA に対するクライアント証明書の発行申請は、金融機関管理者が行うことが出来る。

4.1.2 登録手続及び責任

クライアント証明書の発行申請は、所定の申請書を金融庁 CA に提出することによって行う。

クライアント証明書の申請手続きにおいて、金融機関管理者は、金融庁 CA に対して正確な情報を申請するものとする。

4.2 クライアント証明書申請手続

金融庁 CA は、「3.2.2 組織の認証」及び「3.2.3 個人の認証」において定める手続を実施し、申請内容が適切であることを確認した上で、クライアント証明書の発行申請の登録を行う。

4.3 クライアント証明書の発行

金融庁 CA は、クライアント証明書の発行申請の登録後、クライアント証明書を取得する Web サイトの URL 及びパスワードを金融機関管理者に対して通知する。

金融機関管理者は、当該 URL 及びパスワードを証明書利用者に配付し、証明書利用者が端末にクライアント証明書をインストールする。

金融機関管理者は、金融機関等が業務を行うための正当な端末のみにクライアント証明書がインストールされるよう、クライアント証明書及び端末を適切に管理しなければならない。

4.4 クライアント証明書の受領

クライアント証明書のインストール後、証明書利用者は、遅滞なくクライアント証明書の内容を確認しなければならない。クライアント証明書の内容に問題がある場合、証明書利用者は金融機関管理者に報告し、金融機関管理者が金融庁 CA に申し出るものとする。

金融庁 CA、は、金融機関管理者からの申し出に基づき、クライアント証明書の再発行が必要と認められる場合は、再発行を行う。

4.5 証明書利用者鍵ペア及びクライアント証明書の使用

4.5.1 証明書利用者秘密鍵及びクライアント証明書の使用

証明書利用者は、証明書利用者秘密鍵及びクライアント証明書を利用するにあたり、次の義務を負う。

- クライアント証明書は、本 CP/CPS に従って利用する。
- クライアント証明書及び対応する証明書利用者秘密鍵を安全に管理する。
- 物理的、論理的にセキュリティが確保された金融機関等が業務を行うための端末のみにクライアント証明書をインストールする。
- 証明書利用者秘密鍵が危殆化した場合は、直ちに金融機関管理者に報告する。

4.5.2 証明書検証者による証明書利用者公開鍵及びクライアント証明書の使用

証明書検証者は、証明書利用者公開鍵及びクライアント証明書を信頼し利用するにあたり、次の義務を負う。

- クライアント証明書の利用目的を確認する。
- クライアント証明書が改ざんされていないことを確認する。
- クライアント証明書の有効性（有効期間及び失効の有無）について検証する。

4.6 証明書利用者秘密鍵更新を伴わないクライアント証明書の更新

証明書利用者秘密鍵の更新を伴わないクライアント証明書の更新は行わないため、該当しない。

4.7 証明書利用者秘密鍵更新を伴うクライアント証明書の更新

クライアント証明書の有効期限が近づいた場合等、クライアント証明書の更新を行う場合は、対応する証明書利用者秘密鍵を新たに生成することとし、その手続は「4.3 証明書の発行」と同様の手続とする。

4.8 クライアント証明書の変更

クライアント証明書の情報に変更が生じる場合は、「4.2 クライアント証明書申請手続」及び「4.3 クライアント証明書の発行」と同様の手続により、クライアント証明書を発行するものとする。また、「4.9.3 失効申請手続」に基づき、発行済みのクライアント証明書に対する失効申請を行わなければならない。

4.9 クライアント証明書の失効と一時停止

4.9.1 クライアント証明書失効事由

金融庁 CA は、次の失効事由が発生した場合、クライアント証明書を失効する。

- 証明書利用者秘密鍵の紛失等、危殆化時
- クライアント証明書記載事項の変更
- 金融庁 CA 秘密鍵の紛失等、危殆化時
- クライアント証明書の利用停止
- 金融機関管理者又は証明書利用者による本 CP/CPS に定める義務違反があった場合
- その他、金融庁 CA が必要と判断した場合

4.9.2 失効の申請者

金融庁 CA に対するクライアント証明書の失効申請は、金融機関管理者が行うことが出来る。

4.9.3 失効申請手続

金融機関管理者は、所定の申請書を用いて金融庁 CA に対しクライアント証明書の失効申請を行う。

金融庁 CA は、「3.4 失効申請時の識別と認証」において定める手続を実施し、申請内容が適切であることを確認した上で、クライアント証明書の失効申請の登録を行い、CRL をリポジトリに登録する。

金融庁 CA は、クライアント証明書の失効完了を確認した後、金融機関管理者に失効した旨を通知する。

4.9.4 失効申請を行わなければならない期間

失効の申請は、失効すべき事象が発生してから速やかに行わなければならない。

4.9.5 金融庁 CA が失効申請を処理しなければならない期間

金融庁 CA は、失効申請の受領後、速やかに失効処理を行う。

なお、発行したクライアント証明書の失効申請の受領後は、その失効処理の取消しは行わない。失効したクライアント証明書を再発行する場合は、あらためて発行手続を行う。

4.9.6 失効調査の要求

証明書検証者は、CRL によってクライアント証明書の有効性を確認しなければならない。金融庁 CA は、この確認が行えるようリポジトリで CRL を公表する。

4.9.7 CRL の発行頻度

金融庁 CA は、有効期間 96 時間の CRL を発行し 24 時間ごとに更新する。なお、クライ

アント証明書の失効処理を行った場合は、その時点で CRL を更新する。

4.9.8 CRL の発行最大遅延時間

金融庁 CA は、発行した CRL を速やかにリポジトリに反映させる。

4.9.9 オンラインでの失効/ステータス確認の可用性

金融庁 CA が提供する失効情報は CRL のみであるため、該当しない。

4.9.10 オンラインでの失効/ステータス確認を行うための要件

金融庁 CA が提供する失効情報は CRL のみであるため、該当しない。

4.9.11 利用可能な失効情報の他の形式

金融庁 CA が提供する失効情報は CRL のみであるため、該当しない。

4.9.12 鍵の危殆化に対する特別要件

証明書利用者秘密鍵が危殆化した場合、金融機関管理者は、直ちに金融庁 CA に報告しなければならない。金融庁 CA は、金融機関管理者からの失効申請に基づき、速やかにクライアント証明書の失効処理を行う。

4.9.13 クライアント証明書の一時停止事由

金融庁 CA は、クライアント証明書の一時停止を行わない。

4.9.14 クライアント証明書の一時停止の申請者

金融庁 CA は、クライアント証明書の一時停止を行わないため、該当しない。

4.9.15 クライアント証明書の一時停止申請手続

金融庁 CA は、クライアント証明書の一時停止を行わないため、該当しない。

4.9.16 一時停止を継続できる期間

金融庁 CA は、クライアント証明書の一時停止を行わないため、該当しない。

4.10 クライアント証明書のステータス確認サービス

金融庁 CA は、CRL 以外によるクライアント証明書のステータス確認手段は提供しない。

4.11 登録の終了

証明書利用者は金融庁 CA が発行するクライアント証明書の利用を終了する場合、金融機

関管理者を介して金融庁 CA に対し、クライアント証明書の失効申請を行わなければならない。

4.12 証明書利用者秘密鍵の預託と回復

金融庁 CA は、証明書利用者秘密鍵の預託は行わない。

5. 設備上、運営上、運用上の管理

5.1 物理的管理

5.1.1 立地場所及び構造

金融庁 CA システムは、セキュアなデータセンター内に設置する。データセンターは、水害、地震、その他の災害の被害を容易に受けない場所に建設されており、かつ建物の構造上も、これら災害防止のための対策を講じている。

5.1.2 物理的アクセス

金融庁 CA システムを設置する施設は、金融庁 CA を構成するシステム及び実施する業務の重要度に応じ、複数のセキュリティレベルで入退室制御を行う。入退室時における認証は、入退室者が特定できる IC カード認証、生体認証、又はその両方の組み合わせによる認証により行う。

また、監視カメラ、各種センサーを設置し、金融庁 CA システムへのアクセスを監視する。

5.1.3 電源及び空調

データセンターでは、瞬断及び長時間の停電時においても金融庁 CA システムの運用を可能とするために、無停電電源装置及び自家発電装置による電源対策を施している。

また、金融庁 CA システムは、空気調和機により最適な温度、湿度を一定に保つことが可能な環境下に設置する。

5.1.4 水害対策

水害対策として、金融庁 CA システムを建物の二階以上に設置する。また、防水対策として、金融庁 CA システムを設置する室には漏水検知器を設置する。

5.1.5 地震対策

金融庁 CA システムを設置する建物は耐震構造とし、機器･什器の転倒及び落下を防止する対策を講ずる。

5.1.6 火災防止及び火災保護対策

金融庁 CA システムを設置する室は、防火壁によって区画された防火区画とし、火災報知機及び消火設備を設置する。

5.1.7 媒体保管

金融庁 CA は、アーカイブデータ、バックアップデータを含む認証業務を行う上で必要な

情報を、適切な入退管理が行われた室内の保管庫に保存するとともに、毀損、滅失防止のための措置を施す。

5.1.8 廃棄処理

金融庁 CA は、機密情報を含む書類及び電子媒体の廃棄を、情報の初期化、裁断等により行う。

5.1.9 オフサイトバックアップ

金融庁 CA は、金融庁 CA システムの運用のために必要なデータ、機器等を、遠隔地に保管する。データ、機器等の移送経路やこれらを保管する施設については、十分なセキュリティ対策を講ずる。

5.2 手続的管理

5.2.1 信頼すべき役割

(1) 運営責任者

運営責任者は、金融庁 CA の運営に関する責任者であり、次の業務を行う。

運営責任者の役割は、総合政策局秘書課情報化統括室長が担う。

- 認証業務の統括
- CA 秘密鍵の危殆化発生時、災害発生時等緊急時における対応の統括
- クライアント証明書発行、失効申請の承認
- その他金融庁 CA の運営に関する統括

(2) 承認者

承認者は、クライアント証明書発行、失効申請の審査結果の承認、クライアント証明書の発行、失効指示を行う。

(3) 審査担当者

審査担当者は、申請等の受付、審査業務を行う。また、金融機関管理者との連絡調整業務及び申請書類等の管理を行う。

(4) サービス運用管理者

サービス運用管理者は、金融庁 CA の運用に関する責任者であり、次の業務を行う。

- CA 管理者、RA 担当者、ログ検査者への作業指示
- CA 秘密鍵に関する作業立会い
- システム運用の全般管理

(5) CA 管理者

CA 管理者は、金融庁 CA システムに関する次の業務を行う。なお、金融庁 CA システムに関する操作は複数人の CA 管理者が行う。

・ CA サーバ、リポジトリサーバ等、金融庁 CA システムの維持管理
・ CA 秘密鍵の活性化、非活性化等の操作

(6) RA 担当者

RA 担当者は、金融庁 CA に対し、クライアント証明書の発行、更新及び失効に係る申請の登録を行う。

(7) ログ検査者

ログ検査者は、入退室ログ、システムログ等の検査を行う。

5.2.2 職務ごとに必要とされる人数

CA 秘密鍵の生成及び自己署名証明書の発行等の重要な業務については、複数名の要員で行う。

5.2.3 個々の役割に対する識別と認証

金融庁 CA システムへのアクセスに関し、物理的又は論理的な方法によってアクセス権限者の識別と認証、及び認可された権限の操作であることを確認する。

5.2.4 職務分割が必要となる役割

本 CPS「5.2.1.信頼すべき役割」に記載する役割は、原則として異なる要員がその役割を担う。なお、サービス運用管理者については、ログ検査者との兼務を可能とする。

5.3 人事的管理

本 CPS「5.2.1.信頼すべき役割」に記載する役割を担う者は、PKI の概要とシステムの操作方法等を理解している者を配置する。

また、金融庁 CA の運用の一部を外部組織に委託する場合、業務委託先との契約によって、業務委託先のもとで運用業務が適切に行われていることを確認する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

次の内容を監査ログとして記録する。

(1) 金融庁 CA システムに関するログ
・ 金融庁 CA の秘密鍵の操作
・ 金融庁 CA システムの起動･停止
・ データベースの操作
・ 権限設定の履歴
・ クライアント証明書の発行、失効の処理履歴
・ CRL の発行の処理履歴

(2) 入退室・ネットワークに関するログ
・ 金融庁 CA システムを設置する室への入退室に関する記録
・ 金融庁 CA システムへの不正アクセスに関する記録

監査ログは、以下の項目を含む。
・ 日付
・ 時刻
・ イベントを発生させた主体
・ イベントの内容

5.4.2 監査ログを処理する頻度

ログ検査者は、監査ログを定期的に確認する。

5.4.3 監査ログの保管期間

監査ログは、アーカイブとして最低 10 年保存する。入退室、ネットワークに関するログについては最低 1 年間保存する。

5.4.4 監査ログの保護

監査ログには、認可された者のみが監査ログにアクセスすることができるよう、論理的、物理的に適切なアクセスコントロールを採用する。

5.4.5 監査ログのバックアップ手続

監査ログは定期的に記録媒体にバックアップとして取得し、それらの媒体を安全な場所に保管する。

5.4.6 監査ログの収集システム

監査ログの収集システムは、金融庁 CA システムの機能に含まれており、本 CPS「5.4.1 記録されるイベントの種類」に記載するログを含むセキュリティに関する重要なイベントを

記録する。

5.4.7 イベントを起こした者への通知

事象を発生させた者、システム又はアプリケーションに対して通知することなく、監査ログの検査を行う。

5.4.8 脆弱性評価

監査ログの検査結果をもとに、運用面及びシステム動作面におけるセキュリティ上の脆弱性を評価するとともに、必要に応じて最新の実装可能なセキュリティテクノロジの導入等、セキュリティ対策の見直しを行う。

5.5 記録の保管

5.5.1 アーカイブの種類

次の情報をアーカイブとして保存する。

- 金融庁 CA 証明書及び金融庁 CA 公開鍵
- クライアント証明書及び証明書利用者公開鍵
- CRL
- 金融庁 CA 証明書、クライアント証明書及び CRL の発行履歴
- 起動停止ログ
- 操作ログ

5.5.2 アーカイブ保管期間

アーカイブデータは、最低 10 年間保存する。

5.5.3 アーカイブの保護

アーカイブは、許可された者以外がアクセスできないようアクセスが制限された施設において保管する。

5.5.4 アーカイブのバックアップ手続

証明書発行、失効又は CRL の発行等、金融庁 CA システムに関する重要なデータに変更がある場合は、適時、アーカイブのバックアップを取得する。

5.5.5 記録にタイムスタンプを付与する要件

金融庁 CA システムの時刻同期を行い、金融庁 CA システム内で記録される重要な情報に対しタイムスタンプを付与する。

5.5.6 アーカイブ収集システム

アーカイブの収集システムは、金融庁 CA システムの機能に含まれている。

5.5.7 アーカイブの検証手続

定期的にアーカイブデータが記録された媒体の可読性確認を行う。また必要に応じ、アーカイブの完全性及び機密性の維持を目的として、新しい媒体への複製を行う。

5.6 鍵の切り替え

金融庁 CA 秘密鍵は、金融庁 CA 秘密鍵に対応する金融庁 CA 証明書の有効期間がクライアント証明書の最大有効期間よりも短くなる前に新たな金融庁 CA 秘密鍵の生成及び金融庁 CA 証明書の発行を行う。

5.7 危殆化及び災害からの復旧

5.7.1 事故及び危殆化時の手続

事故及び危殆化が発生した場合に速やかに金融庁 CA システム及び関連する業務を復旧できるよう、以下を含む事故及び危殆化に対する対応手続を策定する。

- CA 秘密鍵の危殆化
- ハードウェア、ソフトウェア、データ等の破損、故障
- 水害、地震等の災害

5.7.2 ハードウェア、ソフトウェア又はデータが破壊された場合の手続

金融庁 CA システムのハードウェア、ソフトウェア又はデータが破損した場合、バックアップ用として保管しているハードウェア、ソフトウェア又はデータを使用して、速やかに金融庁 CA システムの復旧作業を行う。

5.7.3 金融庁 CA 秘密鍵及び証明書利用者秘密鍵が危殆化した場合の手続

金融庁 CA 秘密鍵が危殆化した場合、及び災害等により金融庁 CA システムの運用が中断、停止につながるような状況が発生した場合には、予め定められた計画、手順に従い、安全に運用を再開させる。

証明書利用者秘密鍵が危殆化した場合は、「4.9 証明書の失効と一時停止」において定める手続に基づき、クライアント証明書の失効手続を行う。

5.7.4 災害後の事業継続性

不測の事態が発生した場合に備え、メインサイトから数百キロ以上離れた場所にバック

アップサイトを設置する。また、バックアップサイトへの切替時に速やかに復旧作業を実施できるよう、予め金融庁 CA システムの代替機の確保、復旧に備えたバックアップデータの確保、復旧手続の策定等を行う。

5.8 認証業務の終了

金融庁 CA が認証業務を終了する場合は、事前に金融機関等にその旨を通知する。金融庁 CA によって発行された全てのクライアント証明書は、金融庁 CA の終了以前に失効を行う。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成及びインストール

6.1.1 鍵ペアの生成

金融庁 CA は、FIPS140-2 レベル 3 準拠のハードウェアセキュリティモジュール（Hardware Security Module：以下、「HSM」という）を用いて金融庁 CA 鍵ペアの生成を行う。金融庁 CA 鍵ペアの生成作業は、複数名の CA 管理者による操作によって行う。

証明書利用者は、証明書利用者の環境において証明書利用者鍵ペアを生成する。

6.1.2 証明書利用者に対する証明書利用者秘密鍵の配付

金融庁 CA は、証明書利用者に対して証明書利用者秘密鍵の配付は行わない。

6.1.3 金融庁 CA への証明書利用者公開鍵の配付

金融庁 CA に対する証明書利用者公開鍵の配付は、オンラインによって行うことができる。この時の通信経路は SSL により暗号化を行う。

6.1.4 証明書検証者への金融庁 CA 公開鍵の配付

証明書検証者は、金融庁 CA のリポジトリにアクセスすることによって、金融庁 CA 公開鍵及び金融庁 CA 証明書を入手することができる。

6.1.5 鍵のサイズ

金融庁 CA 鍵ペアは、RSA 方式で鍵長 2048 ビットとする。

証明書利用者鍵ペアは、RSA 方式で鍵長 2048 ビットとする。

6.1.6 公開鍵パラメータの生成及び品質検査

金融庁 CA 公開鍵のパラメータの生成、及びパラメータの強度の検証は、鍵ペア生成に使用される暗号装置に実装された機能を用いて行われる。

証明書利用者公開鍵のパラメータの生成及び品質検査については証明書利用者の端末によって行われる。

6.1.7 鍵の用途

金融庁 CA 証明書の KeyUsage には、クライアント証明書及び CRL を発行するために keyCertSign 及び cRLSign のビットを設定する。

クライアント証明書の KeyUsage には、認証用途でクライアント証明書を利用するために digitalSignature 及び keyEncipherment のビットを設定する。

6.2 秘密鍵の保護及び暗号モジュール技術の管理

6.2.1 暗号モジュールの標準及び管理

金融庁 CA は、金融庁 CA 秘密鍵の生成、保管、署名操作を行う際、FIPS140-2 レベル 3 準拠の HSM を用いて行う。

証明書利用者秘密鍵については証明書利用者の端末によって行われるため規定しない。

6.2.2 秘密鍵の複数人管理

金融庁 CA は、金融庁 CA 秘密鍵の活性化、非活性化、バックアップ等の操作を行う際、安全な環境において複数人の CA 管理者によって行う。

証明書利用者は、証明書利用者秘密鍵の活性化、非活性化等の操作を行う際、証明書利用者の管理の下で安全に行うものとする。

6.2.3 秘密鍵の預託

金融庁 CA は、金融庁 CA 秘密鍵の預託は行わない。

証明書利用者は、証明書利用者秘密鍵の預託を行ってはならない。

6.2.4 秘密鍵のバックアップ

金融庁 CA は、金融庁 CA 秘密鍵のバックアップを行う際、セキュアな室において複数名の CA 管理者によってバックアップを作成し、暗号化した状態で保管する。

証明書利用者は、証明書利用者秘密鍵について、そのバックアップを含む一切の複製を作成してはならない。

6.2.5 秘密鍵のアーカイブ

金融庁 CA は、金融庁 CA 秘密鍵のアーカイブは行わない。

証明書利用者は、証明書利用者秘密鍵について、そのバックアップを含む一切の複製を作成してはならない。

6.2.6 秘密鍵の暗号モジュールへの又は暗号モジュールからの転送

金融庁 CA は、金融庁 CA 秘密鍵の HSM への転送又は HSM からの転送を行う際、セキュアな室において、秘密鍵を暗号化した状態で行う。

証明書利用者は、証明書利用者秘密鍵について、物理的、論理的にセキュリティが確保された金融機関等が業務を行うための端末のみに格納するものとする。

6.2.7 暗号モジュールへの秘密鍵の格納

金融庁 CA は、金融庁 CA 秘密鍵を暗号化した状態で HSM 内に格納する。

証明書利用者は、証明書利用者秘密鍵について、物理的、論理的にセキュリティが確保された金融機関等が業務を行うための端末のみに格納するものとする。

6.2.8 秘密鍵の活性化方法

金融庁 CA は、金融庁 CA 秘密鍵の活性化を行う際、セキュアな室において複数名の CA 管理者によって行う。

証明書利用者は、証明書利用者秘密鍵について、証明書利用者のみが証明書利用者秘密鍵にアクセスできるよう、金融機関管理者により、端末の管理を適切に行わなければならない。

6.2.9 秘密鍵の非活性化方法

金融庁 CA は、金融庁 CA 秘密鍵の非活性化を行う際、セキュアな室において複数名の CA 管理者によって行う。

証明書利用者は、証明書利用者秘密鍵について、証明書利用者のみが証明書利用者秘密鍵にアクセスできるよう、金融機関管理者により、端末の管理を適切に行わなければならない。

6.2.10 秘密鍵の破棄方法

金融庁 CA は、金融庁 CA 秘密鍵を破棄する際、複数名の CA 管理者によって完全に初期化又は物理的に破壊することによって行う。バックアップについても同様の手続によって行う。

証明書利用者は、証明書利用者秘密鍵を破棄する際、端末内の情報を初期化又は端末自体を物理的に破壊することによって行うことができる。

6.2.11 暗号モジュールの評価

金融庁 CA で使用する HSM の品質基準については、本 CP/CPS「6.2.1.暗号モジュールの標準及び管理」のとおりである。

証明書利用者秘密鍵については証明書利用者の端末によって行われるため規定しない。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ

金融庁 CA 公開鍵及び証明書利用者公開鍵のアーカイブは、本 CP/CPS「5.5.1 アーカイブの種類」に含まれる。

6.3.2 秘密鍵及び公開鍵の有効期間

金融庁 CA 秘密鍵及び公開鍵の有効期間は 20 年とする。

証明書利用者秘密鍵及び公開鍵の有効期間は 3 年とする。

6.4 活性化データ

6.4.1 活性化データの生成及び設定

金融庁 CA は、金融庁 CA 秘密鍵を操作するために必要な活性化データについて、複数名の CA 管理者によって生成し、電子媒体に格納する。

6.4.2 活性化データの保護

金融庁 CA は、金融庁 CA 秘密鍵の活性化に必要なデータが格納された電子媒体について、セキュアな室において保管管理を行う。

6.4.3 活性化データの他の考慮点

規定しない。

6.5 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

金融庁 CA は、金融庁 CA システムに導入するハードウェア、ソフトウェアについて、その品質、安定性、安全性等を十分に検討した上で導入を決定する。

6.5.2 コンピュータセキュリティ評価

金融庁 CA は、金融庁 CA システムにおいて使用する全てのソフトウェア、ハードウェアに対して事前にシステムテストを行い、システムの信頼性の確保に努める。また、システムのセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、脆弱性が発見された場合には、速やかに必要な対処を行う。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

金融庁 CA は、金融庁 CA システムの構築及びメンテナンスについて、安全な環境下で行う。システムの変更を行う場合は、十分に安全性の評価、確認を行う。

6.6.2 セキュリティ運用管理

金融庁 CA システムを維持管理するため、不正侵入対策、ウイルス対策等のセキュリティ対策ソフトウェアの更新等を適時行い、セキュリティを確保する。

6.6.3 ライフサイクルセキュリティ管理

金融庁 CA システムの開発、運用、保守が適切に行われていることを、監査等を通じて適時評価し、必要に応じ改善を行う。

6.7 ネットワークセキュリティ管理

金融庁 CA システムに対する不正アクセス対策として、ファイアウォール、不正侵入検知システム等を設置する。

6.8 タイムスタンプ

タイムスタンプに関する要件は、本 CP/CPS「5.5.5 記録にタイムスタンプを付与する要件」と同様とする。

7. 証明書、証明書失効リストのプロファイル

7.1 金融庁 CA 証明書

表 7-1 金融庁 CA 証明書

フィールド（基本領域）		内容	critical
Version（X.509証明書バージョン）		Version 3	–
Serial Number（証明書シリアル番号）		例）0a1b2c3d4e5f6789	
Signature Algorithm（署名アルゴリズム）		SHA-256 with RSAEncryption	
Issuer（発行者）	Country（国）	C= JP	
	stateOrProvinceName（都道府県）	ST= なし	
	localityName（市区町村）	L= なし	
	Organization（組織）	O= Japanese Government	
	Organizational Unit（組織単位）	OU= Financial Services Agency	
	Common Name（一般名）	CN= Financial Services Agency Certification Authority	
Validity（有効期限）	NotBefore（有効性開始日時）	例）2008/01/01 00:00:00 GMT	
	NotAfter（有効性終了日時）	例）2028/01/01 00:00:00 GMT ＊20年の有効期間	
Subject（主体者）	Country（国）	C= JP	
	stateOrProvinceName（都道府県）	ST= なし	
	localityName（市区町村）	L= なし	
	Organization（組織）	O= Japanese Government	
	Organizational Unit（組織単位）	OU= Financial Services Agency	
	Common Name（一般名）	CN= Financial Services Agency Certification Authority	
Subject PublicKey Info（主体者公開鍵情報）		主体者のRSA公開鍵（2048bit）	

フィールド（拡張領域）	内容	citical
Basic Constraints（基本的制約）	TRUE（CAである）	Y
Key Usage（鍵用途）	keyCertSign（証明書への署名） cRLSign（CRLへの署名）	Y
Subject Key Identifier（主体者鍵識別子）	主体者の公開鍵識別子 （主体者公開鍵の160bit SHA-1ハッシュ値）	N

7.2 クライアント証明書

表 7-2 クライアント証明書

証明書フィールド（基本領域）		内容	critical
X.509 Version（X.509証明書バージョン）		Version 3	–
Serial Number（証明書シリアル番号）		例） 0a1b2c3d	
Signature Algorithm（署名アルゴリズム）		SHA-256 with RSAEncryption	
Issuer（発行者）	Country（国）	C= JP	
	stateOrProvinceName（都道府県）	ST= なし	
	localityName（市区町村）	L= なし	
	Organization（組織）	O= Japanese Government	
	Organizational Unit（組織単位）	OU= Financial Services Agency	
	Common Name（一般名）	CN= Financial Services Agency Certification Authority	
Validity（有効期限）	NotBefore（有効性開始日時）	例） 2013/01/01 12:00:00 GMT	
	NotAfter（有効性終了日時）	例） 2016/01/01 12:00:00 GMT ＊有効期間3年	
Subject（主体者）	Country（国）	C= JP	
	stateOrProvinceName（都道府県）	ST= なし	
	localityName（市区町村）	L= なし	
	Organization（組織）	O= Financial Services Agency Business Support Integration System	
	Organizational Unit（組織単位）	OU= ”証明書利用者の所属する組織の金融機関基本コード”	
	Common Name（一般名）	CN= ”金融機関基本コード”-”金融機関毎の連番”	
	Serial Number（シリアル番号）	SN= なし	
Subject PublicKey Info（主体者公開鍵情報）		主体者の公開鍵データ	

証明書フィールド（x.509 v3拡張領域）	内容	critical
Key Usage（鍵用途）	digitalSignature（ディジタル署名） keyEncipherment（鍵暗号化）	Y
Extended Key Usage（拡張鍵用途）	TLS WWW client authentication（クライアント認証）	N
Subject Alt Name（主体者別名）	なし	N
CRL Distribution Points（CRL配布ポイント）	http://repo1.secomtrust.net/sppca/fsa/fullcrl.crl	N
Certificate Policies（証明書ポリシ）	Policy: 1.2.392.200091.110.207.1 CPS: https://repo1.secomtrust.net/sppca/fsa/	N
Authority Key Identifier（発行者鍵識別子）	発行者の公開鍵識別子 （発行者公開鍵の160bit SHA-1ハッシュ値）	N
Subject Key Identifier（主体者鍵識別子）	主体者の公開鍵識別子 （主体者公開鍵の160bit SHA-1ハッシュ値）	N

7.3 CRL

表 7-3 CRL

フィールド（基本領域）		内容	critical
Version（X.509CRLバージョン）		Version 2	–
Signature Algorithm（署名アルゴリズム）		SHA-256 with RSAEncryption	
Issuer （発行者）	Country （国）	C= JP	
	stateOrProvinceName （都道府県）	ST= なし	
	localityName （市区町村）	L= なし	
	Organization （組織）	O= Japanese Government	
	Organizational Unit （組織単位）	OU= Financial Services Agency	
	Common Name （一般名）	CN= Financial Services Agency Certification Authority	
This Update（更新日時）		例） 2013/09/01 00:00:00 GMT	
Next Update（次回更新予定日時）		例） 2013/09/05 00:00:00 GMT ＊ 実更新間隔24時間、有効期間96時間	
Revoked Certificates （失効証明書）	Serial Number （失効証明書シリアル番号）	例） 1234567890	
	Revocation Date （失効日時）	例） 20013/09/01 12:00:00 GMT	
	Reason Code （失効理由）	unspecified(未定義) Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) cessation of operation(運用停止)	
フィールド（拡張領域）		内容	critical
CRL Number （CRL番号）		例） 1 （CRLの発行順序を示す整数値）	N
Authority Key Identifier （発行者鍵識別子）		発行者の公開鍵識別子 （公開鍵のSHA-1ハッシュ値）	N

8. 準拠性監査と他の評価

8.1 監査の頻度

金融庁は、金融庁 CA の運用が本 CP/CPS に準拠して行われているかについて、適時、監査を行う。

8.2 監査者の身元／資格

準拠性監査は、十分な監査経験を有する監査人が行うものとする。

8.3 監査者と被監査者の関係

監査人は、被監査部門の業務から独立した立場にあるものとする。

8.4 監査で扱われる事項

監査は、本 CP/CPS に対する準拠性を中心とする。

8.5 不備の結果としてとられる処置

金融庁 CA は、監査報告書で指摘された事項に関しては、速やかに必要な是正措置を行う。

8.6 監査結果の開示

監査結果は、監査人から金融庁 CA に対して監査報告書として提出される。

監査報告書の外部への公開は、原則として行わない。

9. 他の業務上及び法的事項

9.1 料金

規定しない。

9.2 財務的責任

規定しない。

9.3 情報の機密性

9.3.1 機密情報の範囲

漏えいすることによって金融庁又は金融庁 CA の認証業務の信頼性が損なわれる恐れのある情報を機密扱いとする。

9.3.2 機密情報の範囲外の情報

金融庁が保有する情報のうち、クライアント証明書、CRL、本 CP/CPS 等、公表する情報として明示的に示すものは機密扱いとしない。

9.3.3 機密情報を保護する責任

機密情報は、「行政機関の保有する個人情報の保護に関する法律」及び「金融庁情報セキュリティポリシ」等に従い、当該情報を含む書類及び記憶媒体の管理責任者を定め、安全に管理する。

9.4 個人情報の保護

「行政機関の保有する個人情報の保護に関する法律」及び「金融庁情報セキュリティポリシ」等に従い、適切に保護する。

9.5 知的財産権

金融庁 CA 鍵ペア、クライアント証明書、CRL、金融庁 CA 証明書、本 CP/CPS 及び金融機関等に対して提供するマニュアルの知的財産権は、金融庁に帰属するものとする。

ただし、証明書利用者鍵ペアの知的財産権は、その限りではない。

9.6 表明保証

9.6.1 金融庁 CA の表明保証

金融庁 CA は、認証業務に関して次の内容を表明し、保証する。

・ 本 CP/CPS に基づき金融庁 CA 秘密鍵のセキュアな生成・管理を行うこと
・ 金融機関管理者からの申請に基づいたクライアント証明書の正確な発行、失効及び管理を行うこと
・ システムの運用、稼動監視を適切に行うこと
・ CRL の発行、公表を行うこと
・ リポジトリの維持管理を行うこと
・ 登録端末のセキュアな環境への設置・運用を行うこと

9.6.2 金融機関管理者及び証明書利用者の表明保証

金融機関管理者及び証明書利用者は、「1.4 証明書の用途」、「4.5.1 証明書利用者の秘密鍵及び証明書の使用」に定める内容及び以下に定める内容を遵守することについて表明し、保証する。

・ 物理的、論理的にセキュリティが確保された金融機関等が業務を行うための端末のみにクライアント証明書をインストールすること
・ クライアント証明書は、統合システムへのアクセスのみに使用すること
・ 金融庁 CA に対し、クライアント証明書を発行、失効するための正確な情報を申請すること
・ クライアント証明書を受領する時点で、クライアント証明書の情報が正しいことを確認すること
・ クライアント証明書の記載事項が変更となる場合、利用を停止する場合及び証明書利用者秘密鍵の紛失等が発生した場合は、速やかに金融庁 CA に申請すること

9.6.3 証明書検証者の表明保証

証明書検証者は、「4.5.2 証明書検証者の公開鍵及び証明書の使用」に定める内容を遵守することについて表明し、保証する。

9.6.4 他の関係者の表明保証

規定しない。

9.7 無保証

規定しない。

9.8 責任の制限

規定しない。

9.9 補償

規定しない。

9.10 有効期間と終了

9.10.1 有効期間

本 CP/CPS は、総合政策局秘書課情報化統括室の承認により有効となる。本 CP/CPS「9.10.2 終了」に規定する終了以前に本 CP/CPS が無効となることはない。

9.10.2 終了

本 CP/CPS は、「9.10.3 終了の効果と効果継続」に規定する内容を除き、金融庁が金融庁 CA を終了した時点で無効となる。

9.10.3 終了の効果と効果継続

証明書利用者がクライアント証明書の利用を終了する場合、又は金融庁 CA の業務を終了する場合であっても、「9.3 情報の機密性」、「9.4 個人情報の保護」、「9.5 知的財産権」及び「9.14 準拠法」の条項は終了の事由を問わず金融機関管理者、証明書利用者、証明書検証者及び金融庁に適用されるものとする。

9.11 関係者間の個別通知と連絡

本 CP/CPS 上必要とされ、又は許容される金融庁 CA に対する通知、請求、要求、依頼その他の連絡は総合政策局秘書課情報化統括室を窓口とする。連絡先は「1.5.2 連絡先」に規定する。

9.12 改訂

9.12.1 改訂手続

総合政策局秘書課情報化統括室は、本 CP/CPS を必要に応じて変更する。

9.12.2 通知方法及び期間

総合政策局秘書課情報化統括室は、本 CP/CPS を変更した場合、速やかに変更した CP/CPS を公表する。これをもって金融機関管理者、証明書利用者及び証明書検証者への通知とする。

9.12.3 オブジェクト識別子が変更されなければならない場合

規定しない。

9.13 紛争解決手続

規定しない。

9.14 準拠法

本 CP/CPS に基づく認証業務から生ずる紛争については、日本国の法令を適用する。

9.15 適用法の遵守

規定しない。

9.16 雑則

規定しない。

9.17 その他の条項

規定しない。