山口フィナンシャルグループ認証局証明書ポリシー
（Certificate Policy）
Version1.22

2022 年 1 月 13 日

株式会社山口フィナンシャルグループ

改版履歴		
版数	日付	内容
1.00	2009/03/19	初版
1.10	2010/04/03	「インターネットバンキングシステムで提供する証明書交付」の開始に関する改訂
1.20	2017/11/30	「有効期間 1 年以内」の文言削除
1.21	2020/06/21	7.1 証明書のプロファイル　表 7.1-1 証明書プロファイルに Extended Key Usage（拡張鍵用途）を追加
1.22	2022/01/13	CA（SHA-256）提供開始に関する改訂

目次

1. はじめに

1.1 概要

山口フィナンシャルグループ認証局証明書ポリシー（以下、「本 CP」という）は、株式会社山口フィナンシャルグループ（以下、「山口フィナンシャルグループ」という）が認証局（以下、「CA」という）として発行する電子証明書の用途、利用者手続、発行手続等、電子証明書に関するポリシーを定めるものである。

山口フィナンシャルグループは CA として、本 CP に基づき、証明書利用者が利用する端末に対して電子証明書を発行する。証明書利用者は、当該端末に本 CA が発行する電子証明書を組み込むことで、山口フィナンシャルグループ企業のインターネットバンキングシステムにアクセスし、関連するサービスを受けることができる。

また、本 CA のシステム運用基準、設備基準等を認証運用規程（以下、「CPS」という）として別途定め、CPS に基づき本 CA の運用を行う。

CA（SHA-1）は、Security Communication RootCA1 により、片方向相互認証証明書の発行を受けており、各 CA が定める運用基準に従い運用される。

CA（SHA-256）は、自己署名証明書を発行しており、本 CP および本 CP が参照する CPS が定める運用基準に従い運用される。

本 CP は、IETF が認証局運用のフレームワークとして提唱する RFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

1.2 文書名と識別

本 CP の正式名称は、「山口フィナンシャルグループ認証局証明書ポリシー」という。本 CA では、発行する証明書の種類及び発行基準に応じて一意となるオブジェクト識別子（以下、OID という）が割り当てられ、各証明書内に示される。本 CA が本 CP に基づき発行する証明書及び対応する OID、並びに本 CP が参照する CPS の OID は以下のとおりとする。

CP/CPS	OID
山口フィナンシャルグループ認証局証明書ポリシー	1.2.392.200091.110.201.1
セコム電子認証基盤認証運用規程	1.2.392.200091.100.401.1

1.3 PKI の関係者

1.3.1 認証局

CA（Certification Authority : 認証局）とは、IA（Issuing Authority : 発行局）及び RA（Registration Authority : 登録局）によって構成される。IA は、証明書の発行、取消、CRL（Certificate Revocation List : 証明書失効リスト）の開示等を行い、RA は、証明書の発行、取消を申請する申請者の実在性確認、本人性確認の審査及び証明書を発行、失効するための登録業務等を行う。

1.3.2 登録局

「1.3.1.認証局」に含む。

1.3.3 証明書利用者

証明書利用者とは、CA から証明書の発行を受け、山口フィナンシャルグループ企業が提供するインターネットバンキングサービスへのアクセスのために当該証明書を利用する者をいう。

1.3.4 検証者

検証者とは、インターネットバンキングサービスへのアクセスのために利用される証明書について、その証明書が間違いなく証明書利用者によって行われているということを検証する山口フィナンシャルグループ企業をいう。

1.4 証明書の用途

1.4.1 適切な証明書の用途

証明書利用者は、CA が発行する証明書をインターネットバンキングサービスへのアクセスのためのみに用いるものとする。

1.4.2 禁止される証明書の用途

CA が発行する証明書の用途は「1.4.1 適切な証明書の用途」のとおりであり、証明書をそれ以外の目的に利用することはできないものとする。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CP の維持、管理は、山口フィナンシャルグループ企業が行う。

1.5.2 連絡先

本 CP に関する連絡先は次のとおりである。

窓口 ： セコムトラストシステムズ株式会社

電子メールアドレス ： ca-support@secom.co.jp

1.5.3 ポリシー適合性を決定する者

本 CP の内容について、ポリシー承認機関が適合性を決定する。

1.5.4 承認手続

本 CP は、ポリシー承認機関の承認によって発効される。

1.6 定義と略語

「あ」～「ん」

アーカイブ

法的又はその他の事由により、履歴の保存を目的に取得する情報のことをいう。

エスクロー

第三者に預けること（寄託）をいう。

鍵ペア

公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいう。

監査ログ

認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。

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をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

私有鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。

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。

電子証明書

ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。

リポジトリ

CA 証明書及び CRL 等を格納し公表するデータベースのことをいう。

「A」～「Z」

CA（Certification Authority）：認証局
証明書の発行・更新・失効、CA 私有鍵の生成・保護及び証明書利用者の登録等を行う主体のことをいう。

CP（Certificate Policy）
CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のことをいう。

CPS（Certification Practices Statement）：認証運用規定
CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいう。

CRL（Certificate Revocation List）：証明書失効リスト
証明書の有効期間中に、証明書記載内容の変更、私有鍵の紛失等の事由により失効された証明書情報が記載されたリストのことをいう。

FIPS140-2
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。

HSM（Hardware Security Module）
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をいう。

IA（Issuing Authority）：発行局
CA の業務のうち、証明書の発行・更新・失効、CA 秘密鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。

OID（Object Identifier）：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、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。

PKI（Public Key Infrastructure）：公開鍵基盤
電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。

RA（登録局）（Registration Authority）：登録機関
CA の業務のうち、申込情報の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等を行う主体のことをいう。

RFC3647（Request For Comments 3647）
インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、CP/CPS のフレームワークを規定した文書のことをいう。

RSA
公開鍵暗号方式として普及している最も標準的な暗号技術のひとつ。

SHA-1（Secure Hash Algorithm 1）
電子署名に使われるハッシュ関数（要約関数）のひとつ。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。SHA-1 は 160 ビットのハッシュ値を生成する。
データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

SHA-2（Secure Hash Algorithm 2）
電子署名に使われるハッシュ関数（要約関数）のひとつ。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。SHA-2 には SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256 の種類があり、それぞれ 224 ビット、256 ビット、384 ビット、512 ビット、224 ビット、256 ビットのハッシュ値を生成する。
データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

2. 公開とリポジトリの責任

2.1 リポジトリ

本 CA は、リポジトリを 24 時間 365 日利用できるように維持管理を行う。ただし、利用可能な時間内においてもシステム保守等により利用できない場合がある。

2.2 証明情報の公開

本 CA は、証明書失効リスト（以下「CRL」という）、本 CP および CPS をリポジトリ上に公開し、証明書利用者および検証者がオンラインによって閲覧できるようにする。

2.3 公開の時期又は頻度

本 CP 及び CPS は、改訂の都度、リポジトリ上に公開する。

本 CA は、24 時間ごとに新たな CRL を発行し、リポジトリ上に公開する。また、証明書の失効が行われた場合、即時に新たな CRL を発行し、リポジトリ上に公開する。また、証明書の有効期間を過ぎたものは CRL から削除される。

2.4 リポジトリへのアクセス管理

本 CA は、リポジトリでの公開情報に関して、特段のアクセスコントロールは行わない。証明書利用者は、本 CA の CRL を、リポジトリを通じて入手することが可能。リポジトリへのアクセスは、一般的な Web インターフェースを通じて可能とする。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本 CA が発行する証明書に記載される発行者及び証明書利用者の名前は、X.500 シリーズの識別名規定に従って設定する。

3.1.2 名前が意味を持つことの必要性

本 CA が発行する証明書利用者の証明書に記載される名前には、証明書利用者個人・組織等の名前、又はインターネットバンキングサービス内において識別可能な発行対象者に関連した名前を用いる。

3.1.3 加入者の匿名性又は仮名性

証明書利用者の名前に関する要件は、3.1.1 及び 3.1.2 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

様々な名前の形式を解釈する規則は、X.500 シリーズの識別名規定に従う。

3.1.5 名前の一意性

本 CA が発行する証明書に記載される識別名(DN)(distinguished name) の属性は、通常発行対象となる証明書利用者に対して一意なものとする。

3.1.6 認識、認証及び商標の役割

規定しない。

3.2 初回の本人確認

3.2.1 私有鍵の所持を証明する方法

私有鍵を所有していることの証明として、本 CA が証明書利用者の私有鍵を生成する場合は、本 CA において利用者の鍵ペアを生成する事により、公開鍵と私有鍵との対応を結びつける事が出来る。証明書利用者が自身の私有鍵を生成する場合、本 CA は証明書利用者からオンラインによって受け付けた証明書発行要求（Certificate Signing Request：以下、「CSR」という）の署名の検証を行い、当該 CSR が、公開鍵に対応する私有鍵で署名されていることを確認する。

3.2.2 組織の認証

本 CA は、インターネットバンキングサービス契約先であることを確認する。

3.2.3 個人の認証

本 CA は、山口フィナンシャルグループ企業が提供するインターネットバンキングサービスで定められた契約及び管理責任者届出に関する手続き内容から、当該証明書利用者がインターネットバンキングサービス契約先の一員であることを確認する。なお、証明書利用者は、インターネットバンキングサービス契約締結の際、契約先は管理責任者を設け、証明書利用者は契約先の管理責任者が承認した者とする。

3.2.4 検証されない加入者の情報

規定しない。

3.2.5 権限の正当性確認

本 CA は、証明書に関する申請を行う者が、その申請を行うための正当な権限を有していることを本 CP「3.2.2.組織の認証」及び「3.2.3.個人の認証」によって確認する。

3.2.6 相互運用の基準

CA（SHA-1）は、Security Communication RootCA1 より、片方向相互認証証明書を発行されている。

CA（SHA-256）は、相互認証証明書をもたない。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 通常の鍵更新時における本人性確認と認証

鍵更新時における証明書利用者の本人性確認及び認証は、「3.2 初回の本人性確認」と同様とする。

3.3.2 証明書失効後の鍵更新時における本人性確認と認証

証明書失効後の鍵更新時における証明書利用者の本人性確認及び認証は、「3.2 初回の本人性確認」と同様とする。

3.4 失効申請時の本人性確認と認証

証明書の失効を申請する場合、証明書利用者は本 CA に対して失効に関する申請を提出するものとする。

本 CA は、失効に関する申請情報により、証明書利用者、失効理由等を確認する。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書申請を提出することができる者

証明書の発行申請を行うことができる者は、山口フィナンシャルグループ企業とのインターネットバンキング契約における管理責任者とする。

4.1.2 登録手続及び責任

証明書の発行申請を行う者は、本 CA に対する申請内容が正確な情報であることを保

証するものとする。申請の方法は、インターネットバンキングサービス契約における管理責任者のみアクセス可能な証明書申請画面より行う。

本 CA は、管理責任者が証明書の発行申請を行ったことを確認し、問題が無ければ申請情報に従った証明書の発行登録を行う。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本 CA は、本 CP「3.2. 初回の本人確認」に記載の情報をもって、申請情報の審査を行う。

4.2.2 証明書申請の承認又は却下

本 CA は、審査の結果、承認を行った申請について証明書の発行登録を行う。

不備がある申請については、申請を却下し、申請を行った者に対し申請の再提出を依頼する。

4.2.3 証明書申請の処理時間検証者

本 CA は、承認を行った申請について、適時証明書の発行登録を行う。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本 CA は、受け付けた申請に対し、証明書の発行が完了した後、発行した証明書をオンラインで申請者又は証明書利用者に配布する。証明書利用者は証明書発行用 Web サイトから証明書をダウンロードする。

4.3.2 証明書利用者への証明書発行通知

本 CA は証明書発行サイトの URL を通知、または証明書を配布することによって証明書の発行通知とする。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

証明書利用者は、証明書のダウンロードを行った時点で受領したものする。

4.4.2 認証局による証明書の公開

本 CA は、証明書利用者の証明書の公開は行わない。

4.4.3 他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知は行わない。

4.5 鍵ペア及び証明書の用途

4.5.1 証明書利用者の私有鍵及び証明書の用途

証明書利用者の私有鍵及び証明書の用途は、インターネットバンキングサービスへのアクセスに限られる。証明書利用者は、その他の用途に私有鍵及び証明書を使用せず、自身の責任のもと私有鍵を保護するものとする。

証明書利用者は、本 CA が発行する秘密鍵および証明書を利用するにあたって、以下の義務を負うものとする。

・秘密鍵を紛失から防止し、第三者に対する開示又は危殆化を防止すること。
・証明書に格納されたデータや情報を修正し、変更しまたは改変しないこと。
・秘密鍵の危殆化またはそのおそれが生じた場合、直ちに本 CA に失効の申込を行うこと。
・証明書に記載されているデータまたは情報に変更がある場合、本 CA に対し、直ちに変更に関する申請を行うこと。
・証明書に対応する秘密鍵を利用する前に、証明書の記載内容に誤りがないということを確認すること。
・証明書を利用する場合における電子署名方式は、ハッシュアルゴリズムとして SHA-1 または SHA-256 を用いた RSA 方式であって、鍵長は SHA-1 の場合 1024 ビット以上、SHA-256 の場合 2048 ビット以上とすること。なお、使用するハッシュアルゴリズムに脆弱性が発見された場合、本 CA はより暗号強度が高いハッシュアルゴリズムを適用するなど、対応を行う。

4.5.2 信頼者の公開鍵及び証明書の用途

検証者は、証明書を信頼し利用するにあたって、次の義務を負うものとする。

・検証者の責任において、証明書を信頼することを決定する前に、証明書利用者を適切に評価し、合理的な判断を行うこと。
・証明書の利用目的が、自己の利用目的に合致していることを承諾していること。
・CA 公開鍵を用いて証明書に行われた電子署名を検証することにより、当該証明書の発行者を確認すること。
・フィンガープリントを確認し、CA 証明書であることを確認すること。
・証明書の有効期限が満了していないことを確認すること。

・証明書が失効又は一時停止されていないことを CRL によって確認すること。
・本 CP に定める諸規則を遵守すること。

4.6 証明書の更新

私有鍵の更新を行わない証明書更新は行わない。

4.6.1 証明書の更新事由

規定しない。

4.6.2 証明書の更新を申請することができる者

規定しない。

4.6.3 証明書の更新申請の処理

規定しない。

4.6.4 加入者に対する新しい証明書発行通知

規定しない。

4.6.5 更新された証明書の受領確認の行為

規定しない。

4.6.6 認証局による更新された証明書の公開

規定しない。

4.6.7 他のエンティティに対する認証局の証明書発行通知

規定しない。

4.7 鍵更新を伴う証明書の更新

4.7.1 更新事由

証明書の更新は、証明書の有効期限の到来に伴い行う。

4.7.2 新しい証明書の申請を行うことができる者

「4.1.1.証明書申請を提出することができる者」と同様とする。

4.7.3 更新申請の処理

「4.3.1.証明書発行時の処理手続」と同様とする。

4.7.4 証明書利用者に対する新しい証明書の通知

「4.3.2.加入者への証明書発行通知」と同様とする。

4.7.5 鍵更新された証明書の受領確認手続き

「4.4.1.証明書の受領確認手続」と同様とする。

4.7.6 認証局による鍵更新済みの証明書の公開

本 CA は、証明書利用者の証明書の公開は行わない。

4.7.7 他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知は行わない。

4.8 証明書の変更

4.8.1 証明書の変更事由

証明書の変更は、証明書の記載内容に変更が発生した場合に行う。

4.8.2 証明書の変更を申請することができる者

「4.1.1.証明書申請を提出することができる者」と同様とする。

4.8.3 変更申請の処理

「4.3.1.証明書発行時の処理手続」と同様とする。

4.8.4 証明書利用者に対する新しい証明書発行通知

「4.3.2.加入者への証明書発行通知」と同様とする。

4.8.5 変更された証明書の受領確認の行為

「4.4.1.証明書の受領確認手続」と同様とする。

4.8.6 認証局による変更された証明書の公開

本 CA は、利用者証明書の公開は行わない。

4.8.7 他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知は行わない。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

本 CA は、次の事由が発生した場合、失効申請者からの申請に基づき証明書の失効を行う。

- 証明書記載情報に変更があった場合
- 私有鍵の盗難、紛失、漏洩、不正利用等により私有鍵が危殆化した又は危殆化のおそれがある場合
- 証明書の内容、利用目的が正しくない場合
- 証明書の利用を中止する場合
- 証明書の一時停止を行った場合

また、本 CA は、次の事由が発生した場合に、本 CA の判断により証明書利用者の証明書を失効することができる。

- 証明書利用者が本 CP/CPS、関連する契約又は法律に基づく義務を履行していない場合
- 当社が本 CA を終了する場合
- 本 CA の私有鍵が危殆化した又は危殆化のおそれがあると判断した場合
- 本 CA が失効を必要とすると判断するその他の状況が認められた場合

4.9.2 証明書失効を申請することができる者

証明書の失効の申請を行うことができる者は、山口フィナンシャルグループ企業とのインターネットバンキングサービス契約における管理責任者とする。なお、本 CP/CPS「4.9.1. 証明書失効事由」に該当すると本 CA が判断した場合、本 CA が失効申請者となり得る。

4.9.3 失効申請手続

失効時の処理手順は、次のとおりとする。

・失効申請者は、本 CP/CPS「3.4. 失効申請時の本人性確認と認証」に定める情報を、郵送又は電子メールにより本 CA へ届け出るものとする。

・本 CA は、所定の手続によって受け付けた情報が有効な失効の申請であることを確認し、証明書の失効処理を行う。

4.9.4 失効申請の猶予期間

私有鍵が危殆化した場合を除く取消申請は、取消を希望する 3 営業日前までに本 CA に行うこととする。ただし、私有鍵が危殆化した又はそのおそれがある場合は、当該問題を発見後、速やかに取消申請を行うこととする。

4.9.5 認証局が失効申請を処理しなければならない期間

本 CA は、有効な失効の申請を受け付けてから速やかに証明書の失効処理を行い、CRL へ当該証明書情報を反映させる。

4.9.6 失効調査の要求

本 CA が発行する証明書には、CRL の格納先である URL が記載される。CRL へのアクセスは、一般的な Web インターフェースを用いて可能としている。なお、CRL には、有効期限の切れた証明書情報は含まない。

4.9.7 証明書失効リストの発行頻度

CRL は、失効処理の有無に関わらず、24 時間ごとに更新を行う。証明書の失効処理が行われた場合には、その時点で CRL の更新を行う。

4.9.8 証明書失効リストの発行最大遅延時間

本 CA は、発行した CRL を即時にリポジトリに反映させる。

4.9.9 オンラインでの失効/ステイタス確認の適用性

規定しない。

4.9.10 オンラインでの失効/ステイタス確認を行うための要件

規定しない。

4.9.11 利用可能な失効情報の他の形式

本 CA は、CRL 以外による失効情報の公開は行わない。

4.9.12 鍵の危殆化に対する特別要件

規定しない。

4.9.13 証明書の一時停止事由

一時停止は実施しない。

4.9.14 証明書の一時停止を申請することができる者

規定しない。

4.9.15 証明書の一時停止申請手続

規定しない。

4.9.16 一時停止を継続することができる期間

規定しない。

4.10 証明書のステイタス確認サービス

規定しない。

4.10.1 運用上の特徴

規定しない。

4.10.2 サービスの利用可能性

規定しない。

4.10.3 オプショナルな仕様

規定しない。

4.11 加入（登録）の終了

インターネットバンキングサービスへのアクセスの終了に伴って証明書の利用を終了する場合、証明書利用者又は証明書利用者の属する組織の管理責任者は、本 CA に対し証明書の失効の申請を行わなければならない。本 CA は、有効な申請を受け付けた後、証明書の失効を行う。

4.12 キーエスクローと鍵回復

4.12.1 キーエスクローと鍵回復ポリシー及び実施

本 CA は、証明書利用者の秘密鍵のエスクローは行わない。

4.12.2 セッションキーのカプセル化と鍵回復のポリシー及び実施

本 CA は、証明書利用者の秘密鍵のエスクローは行わない。

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
本項については、CPS に規定する。

5.1.2 物理的アクセス
本項については、CPS に規定する。

5.1.3 電源及び空調
本項については、CPS に規定する。

5.1.4 水害対策
本項については、CPS に規定する。

5.1.5 火災防止及び火災保護対策
本項については、CPS に規定する。

5.1.6 媒体保管
本項については、CPS に規定する。

5.1.7 廃棄処理
本項については、CPS に規定する。

5.1.8 オフサイトバックアップ
本項については、CPS に規定する。

5.2 手続的管理

5.2.1 信頼すべき役割
本項については、CPS に規定する。

5.2.2 職務ごとに必要とされる人数
本項については、CPS に規定する。

5.2.3 個々の役割に対する本人性確認と認証

本項については、CPS に規定する。

5.2.4 職務分割が必要となる役割

本項については、CPS に規定する。

5.3 人事的管理

5.3.1 資格、経験及び身分証明の要件

本項については、CPS に規定する。

5.3.2 背景調査

本項については、CPS に規定する。

5.3.3 教育要件

本項については、CPS に規定する。

5.3.4 再教育の頻度及び要件

本項については、CPS に規定する。

5.3.5 仕事のローテーションの頻度及び順序

本項については、CPS に規定する。

5.3.6 認められていない行動に対する制裁

本項については、CPS に規定する。

5.3.7 独立した契約者の要件

本項については、CPS に規定する。

5.3.8 要員へ提供される資料

本項については、CPS に規定する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

本項については、CPS に規定する。

5.4.2 監査ログを処理する頻度

本項については、CPS に規定する。

5.4.3 監査ログを保持する期間

本項については、CPS に規定する。

5.4.4 監査ログの保護

本項については、CPS に規定する。

5.4.5 監査ログのバックアップ手続

本項については、CPS に規定する。

5.4.6 監査ログの収集システム

本項については、CPS に規定する。

5.4.7 イベントを起こした者への通知

本項については、CPS に規定する。

5.4.8 脆弱性評価

本項については、CPS に規定する。

5.5 記録の保管

5.5.1 アーカイブの種類

本項については、CPS に規定する。

5.5.2 アーカイブ保存期間

本項については、CPS に規定する。

5.5.3 アーカイブの保護

本項については、CPS に規定する。

5.5.4 アーカイブのバックアップ手続

本項については、CPS に規定する。

5.5.5 記録にタイムスタンプを付与する要件

本項については、CPS に規定する。

5.5.6 アーカイブ収集システム

本項については、CPS に規定する。

5.5.7 アーカイブの検証手続

本項については、CPS に規定する。

5.6 鍵の切り替え

本 CA の私有鍵は、私有鍵に対応する証明書の有効期間が証明書利用者の証明書の最大有効期間よりも短くなる前に新たな私有鍵の生成及び証明書の発行を行う。新しい私有鍵が生成された後は、新しい私有鍵を使って証明書及び CRL の発行を行う。

5.7 危殆化及び災害からの復旧

本 CA は、本 CA の私有鍵が危殆化した場合又は事故・災害等により本 CA の運用の停止を伴う事象が発生した場合は、速やかに業務復旧に向けた対応を行うとともに、証明書利用者、その他関係者に対し、必要情報を連絡する。

5.7.1 事故及び危殆化時の手続

本項については、CPS に規定する。

5.7.2 ハードウェア、ソフトウェア又はデータが破損した場合の手続

本項については、CPS に規定する。

5.7.3 エンティティの私有鍵が危殆化した場合の手続

本項については、CPS に規定する。

5.7.4 災害後の事業継続性

本項については、CPS に規定する。

5.8 認証局又は登録局の終了

山口フィナンシャルグループは、本 CA を終了する場合、終了する少なくとも 90 日前までに証明書利用者及び関係者に対して終了の事実を通知または公表し、所定の終了手続を行う。ただし、緊急やむをえない場合、この期間を短縮できるものとする。

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

認証基盤システムでは、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）上で CA の鍵ペアを生成する。鍵ペアの生成作業は、複数名の権限者による操作によって行う。

証明書利用者の鍵ペアは、証明書利用者の端末又は本 CA の設備によって生成するものとする。

6.1.2 証明書利用者に対する私有鍵の交付

本 CA が証明書利用者の私有鍵を生成する場合は、鍵ペア及びそれを使用するための PIN を 2 系統によって配付を行う。

6.1.3 認証局への公開鍵の交付

本 CA への証明書利用者公開鍵の送付は、オンラインによって行われる。この時の通信は TLS/SSL により暗号化され、通信経路を保護する。

6.1.4 検証者への CA 公開鍵の交付

検証者は、本 CA のリポジトリにアクセスすることにより、CA 公開鍵を入手することができる。

6.1.5 鍵サイズ

証明書利用者の鍵ペアの電子署名方式は、ハッシュアルゴリズムとして SHA-1 または SHA-256 を用いた RSA 方式であり、鍵長は SHA-1 の場合 1024 ビット以上、SHA-256 の場合 2048 ビット以上とする。なお、使用するハッシュアルゴリズムに脆弱性が発見された場合、本 CA はより暗号強度が高いハッシュアルゴリズムを適用するなど、対応を行う。

6.1.6 公開鍵のパラメータの生成及び品質検査

規定しない。

6.1.7 鍵の用途

証明書利用者証明書の keyUsage には、digitalSignature、keyEncipherment のビットを設定する。

6.2 私有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

本項については、CPS に規定する。

6.2.2 私有鍵の複数人管理

本項については、CPS に規定する。

6.2.3 私有鍵のエスクロー

本項については、CPS に規定する。

6.2.4 私有鍵のバックアップ

本項については、CPS に規定する。

6.2.5 私有鍵のアーカイブ

本項については、CPS に規定する。

6.2.6 私有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

本項については、CPS に規定する。

6.2.7 暗号モジュールへの私有鍵の格納

本項については、CPS に規定する。

6.2.8 私有鍵の活性化方法

本項については、CPS に規定する。

6.2.9 私有鍵の非活性化方法

本項については、CPS に規定する。

6.2.10 私有鍵の破棄方法

本項については、CPS に規定する。

6.2.11 暗号モジュールの評価

本項については、CPS に規定する。

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
本項については、CPS に規定する。

6.3.2 私有鍵及び公開鍵の有効期間
本項については、CPS に規定する。

6.4 活性化データ

6.4.1 活性化データの生成及び設定
本項については、CPS に規定する。

6.4.2 活性化データの保護
本項については、CPS に規定する。

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
本項については、CPS に規定する。

6.5.2 コンピュータセキュリティ評価
本項については、CPS に規定する。

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
本項については、CPS に規定する。

6.6.2 セキュリティ運用管理
本項については、CPS に規定する。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPS に規定する。

6.7 ネットワークセキュリティ管理

本項については、CPS に規定する。

6.8 タイムスタンプ

本項については、CPS に規定する。

7. 証明書及び証明書失効リストのプロファイル

7.1 証明書のプロファイル

CA（SHA-1）が発行する証明書のプロファイルは、次表のとおりである。

表 7.1-1 CA（SHA-1）証明書プロファイル

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） 2345678901	–
Signature Algorithm（署名アルゴリズム）		SHA-1 with RSAEncryption	–
Issuer（発行者）	Country（国）	c=JP	–
	Organization（組織）	o=Yamaguchi Financial Group Inc.	
	Common Name(主体者名)	cn=Yamaguchi Financial Group CA	
Validity（有効期限）	NotBefore（有効性開始日時）	例） 2009/01/01 12:00:00 GMT	–
	NotAfter（有効性終了日時）	例） 2010/01/01 12:00:00 GMT	
Subject（主体者）	Country（国）	c=JP ＊固定	–
	Organization（組織）	o= Yamaguchi Financial Group Inc. ＊固定	
	Organizational Unit（組織単位）	例）ou= The Yamaguchi Bank Ltd. ＊ 山口フィナンシャルグループ会社名	
	Common Name（主体者名）	例）cn=契約社番号 + 利用者 ID	
	Serial Number（シリアル番号）	例）serialNumber=012345	
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
Subject Alt Name(主体者別名)		Rfc822Name=主体者のメールアドレス	
Certificate Policies（証明書ポリシー）		Policy: 1.2.392.200091.110.201.1 CPS: https://repo1.secomtrust.net/sppca/ymfg/	n
Extended Key Usage(拡張鍵用途)		clientAuth（クライアント認証）	n

CRL Distribution Points（CRL 配布ポイント）	http://repo1.secomtrust.net/sppca/ymfg/fullcrl.crl	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

CA（SHA-256）が発行する証明書のプロファイルは、次表のとおりである。

表 7.1-2 CA（SHA-256）証明書プロファイル

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） 2345678901	–
Signature Algorithm（署名アルゴリズム）		SHA-256 with RSAEncryption	–
Issuer （発行者）	Country（国）	c=JP	–
	Organization（組織）	o=Yamaguchi Financial Group Inc.	
	Common Name(主体者名)	cn=Yamaguchi Financial Group CA G2	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2022/01/01 12:00:00 GMT	–
	NotAfter （有効性終了日時）	例） 2042/01/01 12:00:00 GMT	
Subject （主体者）	Country（国）	c=JP ＊固定	–
	Organization（組織）	o= Yamaguchi Financial Group Inc. ＊固定	
	Organizational Unit（組織単位）	例）ou= The Yamaguchi Bank Ltd. ＊ 山口フィナンシャルグループ会社名	
	Common Name（主体者名）	例）cn=契約社番号 + 利用者 ID	
	Serial Number（シリアル番号）	例）serialNumber=012345	
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
Subject Alt Name(主体者別名)		Rfc822Name=主体者のメールアドレス	

Certificate Policies（証明書ポリシー）	Policy: 1.2.392.200091.110.201.1 CPS: https://repo1.secomtrust.net/sppca/ymfg/	n
Extended Key Usage(拡張鍵用途)	clientAuth (クライアント認証)	n
CRL Distribution Points（CRL 配布ポイント）	http://repo1.secomtrust.net/sppca/ymfg/fullcrlg2.crl	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

7.2 CRL のプロファイル

CA（SHA-1）が発行する CRL のプロファイルは、次表のとおりである。

表 7.2-1 CA（SHA-1）CRL プロファイル

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-1 with RSAEncryption	–
Issuer （発行者）	Country（国）	c=JP	–
	Organization（組織）	o=Yamaguchi Financial Group Inc.	
	Common Name(主体者名)	cn=Yamaguchi Financial Group CA	
This Update(更新日時)		例） 2009/01/01 00:00:00 GMT	–
Next Update(次回更新予定日時)		例） 2010/01/05 00:00:00 GMT ＊ CRL 記載更新間隔 96 時間、実更新間隔 24 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） 2010/01/01 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

CA（SHA-256）が発行する CRL のプロファイルは、次表のとおりである。

表 7.2-1 CA（SHA-256）CRL プロファイル

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	－
	Organization（組織）	o=Yamaguchi Financial Group Inc.	
	Common Name(主体者名)	cn=Yamaguchi Financial Group CA G2	
This Update（更新日時）		例） 2022/01/01 00:00:00 GMT	－
Next Update（次回更新予定日時）		例） 2022/01/05 00:00:00 GMT ＊ CRL 記載更新間隔 96 時間、実更新間隔 24 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） 2022/01/01 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

山口フィナンシャルグループは、本 CA の運用が本 CP 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 監査人の身元／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 監査人と被監査部門の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。監査の実施にあたり、被監査部門は監査に協力するものとする。

8.4 監査で扱われる事項

監査は、本 CA の運用の本 CP に対する準拠性を中心として行う。

8.5 不備の結果としてとられる処置

本 CA は、監査報告書で指摘された事項に関し、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、監査人から本 CA に対して報告される。

本 CA は、法律に基づく開示要求があった場合、山口フィナンシャルグループとの契約に基づき関係組織からの開示要求があった場合、及びポリシー承認機関が承認した場合を除き、監査結果を外部へ開示することはない。

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 企業情報の機密性

9.3.1 機密情報の範囲

山口フィナンシャルグループが保持する個人情報及び組織情報は証明書。CRL、本 CP 及び CPS の一部として明示的に公開されたものを除き、機密保持対象として扱う。

9.3.2 機密情報の範囲外の情報

証明書及び CRL に含まれている情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持対象外とする。

- 山口フィナンシャルグループの過失によらず知られた、あるいは知られるようになった情報

・ 山口フィナンシャルグループ以外の出所から、機密保持の制限無しに山口フィナンシャルグループに知られた、あるいは知られるようになった情報
・ 山口フィナンシャルグループによって独自に開発された情報
・ 開示に関して証明書利用者によって承認されている情報

9.3.3 機密情報を保護する責任

山口フィナンシャルグループは、法の定めによる場合、機密情報を開示することがある。その際、その情報を知り得た者は、契約あるいは法的な制約によりその情報を第三者に開示させない。

9.4 個人情報の保護

山口フィナンシャルグループの個人情報保護方針については、山口フィナンシャルグループのホームページにて公表する。

9.5 知的財産権

本 CP は著作権を含み、山口フィナンシャルグループの権利に属するものとする。

9.6 表明保証

9.6.1 認証局の表明保証

9.6.1.1 IA の表明保証

本 CA は、認証業務を遂行するにあたり次の義務を負うものとする。
・CA 私有鍵のセキュアな生成・管理
・RA からの申請に基づいた証明書の正確な発行・失効管理
・IA のシステム稼動の監視・運用
・CRL の発行・公表
・リポジトリの維持管理

9.6.1.2 RA の表明保証

本 CA は、RA の業務を遂行するにあたり次の義務を負うものとする。
・登録端末のセキュアな環境への設置・運用
・証明書発行・失効申請における IA への正確な情報伝達
・証明書失効申請における IA への運用時間中の速やかな情報伝達

9.6.2 証明書利用者の表明保証

証明書利用者は、本 CP に定める諸事項を遵守することについて保証するものとする。また、証明書利用者は、本 CP に遵守しない場合、すべての責任を有するものとする。

9.6.3 検証者の表明保証

検証者は、本 CP に定める諸事項を遵守することについて保証するものとする。また、信頼者は、本 CP に遵守しない場合、すべての責任を有するものとする。

9.6.4 他の関係者の表明保証

規定しない。

9.7 無保証

本 CA は、本 CP「9.6.1 認証局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、また、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わないものとする。

9.8 責任の制限

本 CP「9.6.1 認証局の表明保証」の内容に関し、次の場合、本 CA は責任を負わないものとする。

・本 CA に起因しない不法行為、不正使用又は過失等により発生する一切の損害
・証明書利用者が自己の義務の履行を怠ったために生じた損害
・証明書利用者のシステムに起因して発生した一切の損害
・本 CA、証明書利用者のハードウェア、ソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
・証明書利用者が契約に基づく契約料金を支払っていない間に生じた損害
・本 CA の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
・本 CA の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
・証明書の使用に関して発生する取引上の債務等、一切の損害
・現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
・天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本 CA の業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書を申請、受領、信頼した時点で、証明書利用者には、本 CA 及び関連する組織等に対する損害賠償責任及び保護責任が発生するものとする。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行等の各種責任が含まれる。

9.10 有効期間と終了

9.10.1 有効期間

本 CP は、ポリシー承認機関の承認により有効となる。

9.10.2 終了

本 CP は、本 CA の終了と同時に無効となる。

9.10.3 終了の効果と効果継続

本 CA 自体を終了する場合であっても、その性質上存続されるべき条項は終了の事由を問わず証明書利用者及び本 CA 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 CA は、証明書利用者に対する必要な通知を、電子メール又は書面等によって行う。

9.12 改訂

9.12.1 改訂手続

本 CP は、本 CA の判断によって適宜改訂され、ポリシー承認機関の承認によって発効するものとする。

9.12.2 通知方法及び期間

本 CP を変更した場合、速やかに変更した本 CP を公表することにより、証明書利用者に対しての告知とする。証明書利用者からの本 CP の変更内容に関する質問は、「1.5.2 連絡先」に記載の連絡先にて受け付けるものとする。

証明書利用者からの質問が無い場合、変更された本 CP は証明書利用者に同意されたものとみなす。

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

証明書の利用に関し、本 CA に対して訴訟、仲裁を含む解決手段に訴えようとする場合、本 CA に対して事前にその旨を通知するものとする。なお、仲裁及び裁判地は山口県内における紛争処理機関を専属的管轄とする。

9.14 準拠法

本 CA、証明書利用者の所在地にかかわらず、本 CP の解釈、有効性及び証明書の利用にかかわる紛争については、日本国の法律が適用されるものとする。

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。