ＩＹＡＳコミュニケーションフィールディングス
認証局運用規定（ＣＰＳ）

2017年6月21日　第1版
2017年6月26日　第2版
2017年7月15日　第3版
2019年6月23日　第4版

1.　はじめに

1.1.　概　要

1.1.1.　認証局開局宣言

ＩＹＡＳコミュニケーションフィールディングス（以下、「当組織」）は、2017年7月15日午前9時（日本時間）より、自己専用の認証局自己署名証明書（以下「ルート証明書」）をトラストアンカー（信頼の起点）としたＰＫＩシステムを構築し、認証局（以下「ＣＡ」）の運用を開始する。ＣＡは、登録局（ＲＡ）を兼務する。

本ＣＰＳは、当組織がX.509準拠の電子証明書（以下、「証明書」）を発行するためのＣＡ業務に関する運用方針を定めるものであり、当組織が行う証明書発行及び運用は、本ＣＰＳに従って行うことを宣言する。

1.1.2.　構成

本ＣＰＳの構成は、ＩＥＴＦ　ＰＫＩＸによるＲＦＣ２５２７「Certificate Policy and Certification Practices Statement Framework」に準拠し、各項の日本語訳は独立行政法人情報処理推進機構公開の訳文を使用している。

1.1.3.　オブジェクト識別子の使用権原

当組織は、オブジェクト識別子の構成要素値の指定に関する規程（平成２年郵政省告示第７３０号）第８条の規定に基づき、日本国政府（主管庁：総務省）より、2017年7月6日にオブジェクト識別子構成要素値の指定を受けている。日本国政府がITUより指定を受けているオブジェクト識別子を含めた一意なプレフィックス（以下「ＯＩＤプレフィックス」）は、「0.2.440.200326」で、当組織は、レベル５以降を適法かつ独占的に指定する権原を有している。

1.1.4.　オブジェクト識別子

当組織は、ＣＡ業務に「0.2.440.200326.1」のＯＩＤプレフィックスを指定する。
本ＣＰＳのオブジェクト識別子（以下「ＯＩＤ」）は、「0.2.440.200326.1.1.99」である。
その他ＣＡにより使用されるＯＩＤは、本ＣＰＳにおいて規定するものとする。

1.1.5.　上位及び下位認証局との関係

当組織のＣＡ証明書は、上位認証局よりクロス署名を受けることがあり、また、中間証明機関へ中間認証局証明書を発行し、当組織が承認した範囲内において認証業務を委任することがある。中間証明機関は、本ＣＰＳ又は当組織が承認した別のＣＰＳに従って認証業務を実施する。

1.2.　識　別

当組織が発行する証明書には、「７．１．証明書プロフィール」に規定の情報を記録することにより当組織が発行する証明書であることを識別することができるようにする。

1.3.　コミュニティと適用可能性

当組織のＣＡは、下記の対象へ証明書を発行することができる。証明書を発行された対象をサブジェクト（以下「証明書所有者」）とする。

(1)　当組織の構成員
(2)　当組織の管理下にあるシステム（サーバーや端末等の証明書認証を実施する装置類）
(3)　当組織外の個人又は組織等で、当組織の管理下にあるシステムへのアクセスを必要とする場合
(4)　当組織が証明書の発行を委任した下位認証局（以下、「中間証明機関」）

1.4.　連絡先の詳細（認証局管理責任者）

本組織の認証局の管理責任者は代表／湯浅　徹　１名とする。
連絡先は、RFC822 Name = t.yuasa@iyas.yuasa.org　とする。

2.　一般的な規定

2.1.　義務

2.1.1.　ＣＡの義務

(1)　当組織は、本ＣＰＳに従って認証業務を適正かつ公正にＣＡ業務を実施する義務を負う。
(2)　証明書要求者への証明書発行の承認又は否認もしくは留保を通知する。
(3)　利用を中止した証明書（退会者、サーバーの廃止）や、秘密鍵が紛失・盗難された場合は、失効リストに当該証明書情報を記載し、所定のＵＲＩに発行する。
(4)　構成員による証明書の取り扱いなどの指導及び監督を行い、組織外へ発行された証明書については、その取扱いについて十分留意するように要請する。

2.1.2.　証明書所有者の義務

ＣＡより証明書の発行を希望する者は、所定の申請を提出することにより証明書要求者となり、ＣＡにより要求を承認され、証明書の発行を受けた時点をもって証明書所有者なり、以下の義務を負う。

(1)　証明書要求者がＣＡへ申請する事項は、真実を間違いなく申請し、証明書所有者となったのちも申請事項に変更が発生した場合は速やかに申請すること。
(2)　秘密鍵を盗用等されないよう、最善の注意をもって適切に管理すること。
(3)　証明書が承認している用途以外に使用しないこと。
(4)　秘密鍵の危殆化（漏洩、盗難、紛失等）又はその可能性が発生した場合、直ちにＣＡに失効要求をすること。

2.1.3.　証明書利用者の義務

ＣＡが発行する証明書の送信を受けた者を証明書利用者とし、以下の義務を負う。

(1)　送信を受けた証明書が、目的の用途に使用を承認されているか確認すること。
(2)　送信を受けた証明書が、正規の方式にて有効なデジタル署名が行われていることを確認すること。
(3)　送信を受けた証明書が、失効されていないかを失効リストと照合し確認すること。
(4)　本ＣＰＳの規定を承認すること。

2.2.　責任

ＣＡが発行する証明書は、通信の相手方確認手段の一つ及び通信の暗号化の鍵として発行されるものである。
技術的要因に　より、証明書に通常使用される暗号理論などの技術に瑕疵や危殆化が発生し、その信頼性が損なわれる可能性や、人的要因による証明書所有者の故意又は過失により秘密鍵や証明書が悪用される可能性も発生し得る。
証明書利用者は、これらに限らず、想定される事故等を十分考慮して、証明書の信用や使用を受け入れるかの最終判断責任は、証明書利用者がその責を負うものとする。
当組織では、証明書のみを信頼して実施された行為について、何らかの損害（財産損害など）が発生してもその責は負わない。

2.3.　財務的な責任

「２．２．責任」と同様とする。

2.4.　解釈と執行

本ＣＰＳの内容は、日本国の法令および規則に基づき解釈、履行する。

2.5.　料金

規定しない。

2.6.　公開とリポジトリ

当組織は、ＣＰＳ、ＣＡ証明書、失効リスト、運営情報を当組織ＷＥＢサイトにて公開する。公開に際してのアクセス制限は行なわない。失効リストは、失効した証明書がない場合でも失効リストに定めた期限までに定期更新し、また、失効を行った場合は随時公開する。

2.7.　準拠性監査

規定しない。

2.8.　守秘性のポリシ（守秘義務）

ＣＡは、認証業務に際して取得した個人・組織を特定できる情報（申請事項や添付書類等）及びＣＡ秘密鍵及び発行ログファイルを機密情報と定義し、これを守秘する。個人・組織を特定できる情報であっても証明書に記載した事項（氏名・電子メールアドレスなど、証明書の用途により適宜記載）は機密情報の対象外とする。また、失効リストの発行において、失効リストに記載される内容も同様とする。

権限のある法執行機関から法律に基づく開示請求が書面によりあった場合には、ＣＡ秘密鍵を除き、機密情報を開示する。

2.9.　知的財産権

規定しない。

3.　識別と本人認証

3.1.　初期登録

証明書を発行する場合は、偽りその他不正な手段により、不正な証明書が発行及び取得されることの無いよう、証明書の用途に応じた適切な本人認証を行う。

3.1.1　Class 1 証明書

クラス１証明書は、Domain Validation(DV)相当で、証明書所有者の Fully Qualified Domain Name（完全修飾ドメイン名）又は、RFC822 Name（電子メールアドレス）の占有のみを確認して発行される証明書である。

(1)　証明書ポリシフィールドに記載される OID は、「0.2.440.200326.1.1.11」を記録する。
(2)　証明書の要求には、FQDN 又は RFC822 Name の所有をＣＡの指定する方法にて証明することを必要とする。
(3)　証明書のサブジェクトには、C=JP 及び FQDN 又は RFC822 Name のみが記載される。
(4)　証明書は、下記の簡易な用途に厳格な本人認証を必要としない場合に使用されることを想定する。
　1　Email protection
　2　TLS Web client authentication
　3　TLS Web server authentication

3.1.2　Class 2 証明書

クラス２証明書は、Personal Validation(PV)相当で、証明書所有者個人の存在を確認して発行される証明書である。

(1)　証明書ポリシフィールドに記載される OID は、「0.2.440.200326.1.1.12」を記録する。
(2)　証明書の要求には、個人の存在を証明する書類の提示を必要とする。
(3)　証明書のサブジェクトには、用途に応じて適切な情報が記載される。
(4)　発行される証明書の用途は、申請により必要と認められた用途に限る。

3.1.3　Class 3 証明書

クラス３証明書は、Organization Validation(OV)相当で、証明書所有者組織等の存在を確認して発行される証明書である。

(1)　証明書ポリシフィールドに記載される OID は、「0.2.440.200326.1.1.13」を記録する。
(2)　証明書の要求には、組織等の存在を証明する書類の提示を必要とする。
(3)　証明書のサブジェクトには、用途に応じて適切な情報が記載される。
(4)　発行される証明書の用途は、申請により必要と認められた用途に限る。

3.2.　鍵の更新

証明書は、有効期限の６０日前から有効期限日まで更新手続きを行うことができ、この期間内の更新による証明書更新は「３．１．初期登録」による本人認証を必要としない。ただし、証明書記載事項に変更が生じる場合や「３．４．失効要求」に該当する事項が発生している場合は、この限りではない。

3.3.　失効後の鍵更新

証明書が有効期限切れにより失効した場合、「３．１．初期登録」による本人認証を再度必要とする。

3.4.　失効要求

証明書所有者は、次の場合は失効を「１．４．認証局管理責任者」へ要求しなければならない。

(1)　秘密鍵の危殆化が発生又はその恐れがある場合（端末の紛失、不正アクセス、ウィルス感染等）
(2)　証明書が不要となった場合

失効を要求した後は、以降当該証明書と秘密鍵の鍵ペアを用いて通信等を行ってはならない。ただし、電子メール保護用の証明書で既に送受信を行った電子メールを確認するための暗号解除にのみ用いる場合はこの限りではない。

4.　運用要件

4.1.　証明書アプリケーション（申請）

証明書要求者は、本ＣＰＳを承認し、ＣＡが指定する申請事項及び書類を偽りなく提示することを必要とする。

4.2.　証明書発行

ＣＡは、証明書要求者からのアプリケーションを１０日以内に審査し承認する場合、証明書を発行する。

4.3.　証明書受け入れ

規定しない。

4.4.　証明書留保と失効

ＣＡは、証明書の利用中止、秘密鍵の漏洩や紛失などこれらに限定されないその他理由により証明書を失効する権利を留保する。また、ＣＡは申請が行われた証明書を必ず発行するものではなく、これを否認又は留保する権利を有する。

ＣＡは、発行を失効した証明書は失効リストに記載し、所定のＵＲＩへ公開する。

4.5.　セキュリティ監査手続き

規定しない。

4.6.　レコードのアーカイブ化（記録の保管）

ＣＡは、発行した証明書リスト、失効した証明書リスト、ＣＡ情報（以下「証明書発行システム」）を保管する。各情報はインターネットから直接アクセスできない方法（ネットワークへ接続しないコンピュータや取り外し可能媒体等）にて保管する。

4.7.　鍵再発行

規定しない。

4.8.　改ざんや災害からの復旧

証明書発行システムに不整合が発生した場合やＣＡ秘密鍵などの危殆が懸念される場合には、ルート証明書を含むすべての証明書を失効させる。

予期せぬ証明書発行システムの破損、バックアップの不備、その他の当組織の業務システムが災害により利用不能となり、認証業務や失効リストの発行が不可能な場合には、その時点において最大限の努力で実現可能な適切な方法により運営情報を公表する。

4.9.　ＣＡ期限

当組織の解散やその他事情により、認証業務を終了することがある。

5.　物理的、手続き的および要員的なセキュリティ統制

5.1.　物理的セキュリティ統制

(1)　ＣＡ事務局は、第三者が通常容易に立ち入ることのできない場所に設置する。

(2)　証明書発行システムは、インターネットから直接アクセスできない方法にて保管し、施錠可能な保管庫等に保管する。

(3)　ＣＡ及び証明書発行システムに関する全ての書類（紙面、デジタルデータを問わない）は、バックアップを耐火耐水金庫に保管して保護する。

5.2.　手続き的統制

証明書発行システムは、「１．４．認証局管理責任者」が行い、作業終了後は、直ちに「５．１．物理的セキュリティ統制」に従った状態で保管する。

5.3.　要員的セキュリティ統制

「５．２．手続き的統制」と同様とする。

6.　技術的セキュリティ制御

6.1.　鍵生成とインストール

6.1.1.　ＣＡ鍵の要件

(1)　鍵ペア生成は、「５．２．手続き的統制」に従い、ソフトウェアシステムを用いて認証局管理責任者が行う。
(2)　公開鍵は、当組織ＷＥＢサイトに発行して提供する他、発行した証明書とともに送信する。
(3)　鍵サイズはRSA4096bit 以上とする。

6.1.2.　証明書所有者鍵の要件

(1)　秘密鍵生成は、原則として証明書要求者が行う。ただし、その操作が困難である場合、認証局管理責任者が証明書発行システムを用いて作成を行うことができる。この場合、(2)により配布しその到達が確認された後は直ちに秘密鍵を削除する。
(2)　ＣＡが署名した公開鍵（又は鍵ペア）は、適切な方法により証明書所有者に配布する。
(3)　鍵サイズはRSA2048bit 以上とする。

6.2.　秘密鍵保護

6.2.1.　ＣＡ秘密鍵

(1)　秘密鍵は、ソフトウェアにより生成管理されるため、ハードウェア保護は存在しない。
(2)　秘密鍵は、本ＣＰＳの規定により取り外し可能媒体に記録し、施錠可能な保管庫に保管する。
(3)　秘密鍵は、本ＣＰＳの規定により耐火耐水金庫にバックアップを保管する。

6.2.2.　証明書所有者秘密鍵

(1)　秘密鍵は、証明書要求者が適切に管理を行う。

6.3.　鍵ペア管理の他の側面

規定しない。

6.4.　活性化データ

規定しない。

6.5.　コンピュータセキュリティ統制

証明書発行システムを操作する端末は、セキュリティソフト等によりウィルスおよびマルウェアから保護されている端末を使用する。

6.6.　ライフサイクルセキュリティ統制

ライフサイクルセキュリティは、証明書発行システムソフトウェアに依存する。ソフトウェアは、可能な限り最新のバージョンを利用する。

6.7.　ネットワークセキュリティ統制

「６．５．コンピュータセキュリティ統制」と同様とする。

6.8.　暗号モジュールのエンジニアリング統制

「６．６．ライフサイクルセキュリティ統制」と同様とする。

7.　証明書と CRL プロフィール

7.1.　証明書プロフィール

7.1.1.　基本プロフィール

基本プロフィールは、証明書プロフィールの基本的な記録事項を定めたものであり、本ＣＰＳに別の定めがある区分の証明書場合は、別の定めを優先する。

(1)　発行者フィールドに、当組織の英文名称「IYAS Communication Fieldings」を含む発行者名を記録する。

(2)　証明書ポリシフィールドに、「３．１．初期登録」で規定する証明書クラスをＯＩＤ及び、本ＣＰＳを公開する当組織ＷＥＢサイトＵＲＩを記録する。
ＣＰＳのＵＲＩは、「http://iyas.yuasa.org/pki/」とする。

(3)　機関情報アクセス（AIA）フィールドに、ＣＡ証明書を公開する当組織のＷＥＢサイトＵＲＩを記録する。
ＡＩＡのＵＲＩは、「http://iyas.yuasa.org/pki/(証明書ファイル名).crt」とする。

(4)　失効情報アクセス（CRL）フィールドに、失効リストを公開する当組織のＷＥＢサイトＵＲＩを記録する。
ＣＲＬのＵＲＩは、「http://iyas.yuasa.org/pki/(CRL ファイル名).crl」とする。

(5)　キー使用法フィールド及び拡張キー使用法フィールドに、別表１に従いＣＡが承認するキーの使用法を記録する。

(6)　他、証明書の用途に応じ、３．１．（初期登録）で規定する事項のほか、適宜追加情報を記録する。

(7)　基本制限（Basic Constraints）及び、キー使用法（Key Usage）フィールドにクリティカルを指定する。
クリティカルフラグを有するフィールドは、ＣＡが当該証明書について特に重要な制限を規定するものであり、当該フィールドの制限を適切に処理できない証明書利用者（ソフトウェア等）においては、ＣＡが証明書の使用を拒否することを明示するものである。

7.1.2.　ルートＣＡ証明書プロフィール　第１世代（2017 年発行）

ルート証明書は、ＣＡのトラストアンカーである。

(1)　フィンガープリント（拇印）は、「sha1：77 f1 43 f3 c0 fa 49 22 e9 e2 09 18 81 ed c1 d2 6a e4 e4 18」である。

(2)　記録事項は、別表２による。

7.2.　CRL プロフィール

(1)　CRL の有効期間は、２か月以内とする。

8.　仕様管理

(1)　本ＣＰＳは、2017 年 07 月 15 日において第３版の最新版であり、適宜改定されることがある。最新版は当組織ＷＥＢサイト（http://iyas.yuasa.org/pki/）に公開する。

(2)　証明書発行システムは、汎用ソフトウェアであり当組織において仕様管理は行わない。仕様は、証明書発行システムソフトトウェアの仕様変更に依存する。

以上（本文）

別表１　キー使用法フィールド及び拡張キー使用法フィールドの指定方法

（1）　キー使用法

指定	許可される事項
Digital signature	公開鍵をデジタル署名機構で使用して、Non-repudiation、Certificate signing、CRL signing 以外のセキュリティサービスをサポートすることを許可する。 Digital signature は、多くの場合、エンティティ認証やデータ送信元認証で整合性を保つために使用される。
Non-repudiation	公開鍵を使用して、Non-repudiation サービスを提供するために使用する Digital signature を検証することを許可する。 Non-repudiation を指定すると、署名エンティティが何らかのアクション（Certificate signing と CRL signing を除く）を間違って拒否しないように保護できる。
Key encipherment	キーを暗号化するプロトコルと証明書の併用することを許可する。 一例である S/MIME エンベロープでは、証明書の公開鍵を使用して高速（対称）キーが暗号化される。SSL プロトコルでも、キー暗号化が実行される。
Data encipherment	暗号化キーではなく公開鍵を使用してユーザーデータを暗号化することを許可する。
Key agreement	公開鍵の送信者と受信者が、暗号化を使用しないで公開鍵を抽出することを許可する このキーを使用すると、送信者と受信者の間でやり取りするメッセージを暗号化できます。これは通常、Diffie-Hellman 暗号化方式と併用される。
Certificate signing	対象者の公開鍵を使用して、証明書の署名の検証を許可する。 CA 証明書でのみ指定を許可する。
CRL signing	対象者の公開鍵を使用して、失効情報（CRL など）について署名を検証を許可する。
Encipher only	Key agreement と同時に指定し、Key agreement を実行しながら、公開鍵をデータの暗号化のみに使用することを許可する。
Decipher only	Key agreement も同時に指定し、Key agreement を実行しながら、公開鍵をデータの暗号化解除のみに使用することを許可する。

（2）　拡張キー使用法（用途）と、対応するキー使用法の指定方法

指定する拡張キー使用法	対応して指定するキー使用法
TLS Web server authentication	Digital signature、**Key encipherment**、Key agreement
TLS Web client authentication	**Digital signature**、Key agreement
Sign (downloadable) executable code	**Digital signature**
Email protection	**Digital signature**、Non-repudiation、**Key encipherment**、Key agreement
IPSEC End System (host or router)	Digital signature、Key encipherment、Key agreement
IPSEC Tunnel	Digital signature、Key encipherment、Key agreement
IPSEC User	Digital signature、Key encipherment、Key agreement
Timestamping	Digital signature、Non-repudiation

・**太字**は、指定が必須のキー使用法。

別表２　ルート証明書（第１世代）　記録事項

```
        Serial Number: 0 (0x0)

        Validity
            Not Before: Jul 15 00:00:00 2017 GMT
            Not After : Jul 14 23:59:59 2047 GMT

        Subject:
            countryName               = JP
            stateOrProvinceName       = Aichi
            organizationName          = IYAS Communication Fieldings
            organizationalUnitName    = 0.2.440.200326
            commonName                = IYAS Communication Fieldings Root Certification Authority 2017

        X509v3 extensions:
            X509v3 Basic Constraints: critical   (基本制限：クリティカル)
                CA:TRUE

            X509v3 Key Usage: critical   (キー使用法：クリティカル)
                Certificate Sign, CRL Sign

            X509v3 Subject Key Identifier:   (サブジェクトキー識別子)
                8C:10:B6:4F:59:A3:00:F3:31:70:FE:0D:37:02:6B:3A:CA:E3:EB:A8

            X509v3 Authority Key Identifier:   (機関キー識別子)
                keyid:8C:10:B6:4F:59:A3:00:F3:31:70:FE:0D:37:02:6B:3A:CA:E3:EB:A8

            X509v3 CRL Distribution Points:   (ＣＲＬ配布ポイント)
                Full Name:
                  URI:http://iyas.yuasa.org/pki/IYAS_RSA_RootCA.crl

            Authority Information Access:   (機関情報アクセス)
                CA Issuers - URI:http://iyas.yuasa.org/pki/IYAS_RSA_RootCA.crt

            X509v3 Certificate Policies:   (証明書ポリシ)
                Policy: X509v3 Any Policy
                Policy: 0.2.440.200326.1.1.1
                  CPS: http://iyas.yuasa.org/pki/
```

以上