サイバートラスト デバイス ID 認証局運用規程

(Certification Practice Statement)

Version 2.1

サイバートラスト株式会社

2015 年 7 月 21 日

改訂履歴

Version	日付	改訂事由
1.0	2009 年 6 月 29 日	・ 初版
1.1	2009 年 8 月 17 日	・ 誤字訂正
1.2	2009 年 12 月 1 日	・ 証明書中の組織単位名（Organization Unit）の 64 バイト制限を考慮した指定文字列の変更（短縮） 具体的には、組織単位名を「Cybertrust DeviceiD RA operated by <<お客様会社名称＋会社識別子>>」から「RA operated by <<お客様会社名称＋会社識別子>>」に変更
1.3	2010 年 5 月 12 日	・ ネットワーク機器専用サーバ証明書に関わる記載を追加
1.4	2010 年 12 月 1 日	・ 証明書発行対象に関わる記載を以下のとおり統一 ・加入者管理組織が認めるデバイス ・加入者が利用または管理するネットワーク機器 ・ 登録局オペレータ責任者の選任基準に関わる記載を修正 ・ 監査結果に対する登録局の是正措置対応に関わる記載を修正 ・ 誤字訂正
1.5	2011 年 4 月 28 日	・ 構成プロファイル署名用証明書に係わる記載を追加 ・ 一部表記を統一・修正
1.6	2013 年 3 月 28 日	・ 本認証局における構成プロファイル署名用証明書の発行停止に伴い、同証明書に関わる記載を削除 ・ ネットワーク機器専用サーバ証明書の申請フローの変更を反映 ・ CRL 中の invalidityDate に関する仕様変更を反映
1.7	2013 年 4 月 26 日	・ OCSP サーバの提供開始を反映 ・ CRL の有効期間等に関わる記載を追記・修正
1.8	2013 年 10 月 22 日	・ 第 2 世代認証局に関わる記載を追記・修正 ・ CRL の発行・公開、および OCSP 提供に関わる記載を追記・修正 ・ 誤字訂正
1.9	2014 年 4 月 21 日	・ 第 2 世代認証局 Cybertrust DeviceiD Public CA G2is の記載を追記 ・ 認証局の鍵更新期間、証明書の有効期間を改定 ・ デバイス ID 事務局からデバイス ID サポートデスクへ名称等変更 ・ 誤字等を訂正
2.0	2015 年 5 月 14 日	・ 第 2 世代認証局 Cybertrust DeviceiD Public CA G2sp の記載を追記 ・ CRL 中の invalidityDate に関する仕様変更を反映 ・ 誤字等を訂正
2.1	2015 年 7 月 21 日	・ 第 3 世代認証局 Cybertrust DeviceiD Public CA G3k に関わる記載を追記・修正 ・ デバイス ID 証明書に Authority Information Access を追加（第 3 世代認証局のみ） ・ 誤字等を訂正

目次

1. はじめに

1.1 概要

サイバートラスト株式会社（以下、「サイバートラスト」という。）は、デバイス証明書管理サービスであるサイバートラスト デバイス ID（以下、「本サービス」という。）を提供する。

本サービス利用者は、本サービスにより、デバイスの認証に特化したデバイス ID 証明書の登録局を運営し、デバイス ID 証明書の発行・失効を含む証明書管理を行わせることができる。デバイス ID 証明書は、ネットワーク・アクセス認証におけるスタンダード規格である SSL、IPsec、IEEE802.1x 等での強固な認証に用いることができる証明書であり、本サービス利用者は、デバイス ID 証明書による統合的なネットワーク・アクセス・コントロールによって、ネットワークの安全性の確保、および情報資産の安全な活用の実現を図ることが可能である。

また、本サービス利用者は、ネットワーク機器またはサーバ機器（以下、「ネットワーク機器」という。）専用のサーバ証明書（以下、「ネットワーク機器専用サーバ証明書」という。）の発行を受け、利用することができる。ネットワーク機器専用サーバ証明書は、デバイス ID 証明書を主に iPhone や Windows OS 標準搭載のサプリカントと組み合わせて利用する場合の対向となるネットワーク機器等に必須となるサーバ証明書である。

デバイス ID 証明書およびネットワーク機器専用サーバ証明書は、サイバートラストが管理する下記の認証局より発行される。以下、特段の規定がない限り、「本認証局」という場合、Cybertrust DeviceiD Public CA G1、Cybertrust DeviceiD Public CA G2、Cybertrust DeviceiD Public CA G2s、Cybertrust DeviceiD Public CA G2k、Cybertrust DeviceiD Public CA G2is 、Cybertrust DeviceiD Public CA G2sp 、および Cybertrust DeviceiD Public CA G3k を含むものとする。

認証局名称	Cybertrust DeviceiD Public CA G1
有効期間	2009 年 6 月 23 日 ～ 2019 年 7 月 23 日
鍵長	2048 bit
署名方式	SHA1withRSA

認証局名称	Cybertrust DeviceiD Public CA G2
有効期間	2013 年 10 月 16 日 ～ 2028 年 11 月 16 日
鍵長	2048 bit
署名方式	SHA1withRSA

認証局名称	Cybertrust DeviceiD Public CA G2s
有効期間	2013 年 10 月 16 日 ～ 2028 年 11 月 16 日
鍵長	2048 bit
署名方式	SHA1withRSA

認証局名称	Cybertrust DeviceiD Public CA G2k

有効期間	2013 年 10 月 17 日 ～ 2028 年 11 月 17 日
鍵長	2048 bit
署名方式	SHA1withRSA

認証局名称	Cybertrust DeviceiD Public CA G2is
有効期間	2014 年 3 月 20 日 ～ 2029 年 4 月 20 日
鍵長	2048 bit
署名方式	SHA1withRSA

認証局名称	Cybertrust DeviceiD Public CA G2sp
有効期間	2014 年 12 月 5 日 ～ 2030 年 1 月 5 日
鍵長	2048 bit
署名方式	SHA1withRSA

認証局名称	Cybertrust DeviceiD Public CA G3k
有効期間	2015 年 4 月 20 日 ～ 2030 年 5 月 20 日
鍵長	2048 bit
署名方式	SHA256withRSA

本認証局は、デバイス ID 証明書およびネットワーク機器専用サーバ証明書を発行する。

なお、特段の規定がない限り、本認証局から発行される各証明書を総称して「証明書」という。

本認証局は、証明書を発行するために、以下のガイドラインおよび法令等に準拠する。

① サイバートラスト デバイス ID 認証局運用規程(Certification Practice Statement)

② その他日本国内に設置される本認証局の業務上関連する日本国法

「サイバートラスト デバイス ID 認証局運用規程（Certification Practice Statement）」（以下、「本 CPS」という。）は、本認証局が証明書を発行するための要件を規定する。要件には、本認証局の義務、加入者の義務、信頼当事者の義務を含む。

また、各種要件を本 CPS に明記する上で、本認証局は、IETF PKIX ワーキンググループが定める RFC3647「Certificate Policy and Certification Practices Framework」を採用する。RFC3647 は、CPS または CP のフレームワークを定めた国際的ガイドラインである。RFC3647 のフレームワークに準じて設けた本 CPS の各規定において、本認証局に適用されない事項については、「規定しない」と記載する。

なお、本認証局は、加入者の証明書毎の証明書ポリシー（以下、「CP」という。）を個別に定めず、本 CPS が各 CP を包含するものとする。

1.2 文書名と識別

本 CPS の正式名称は、「サイバートラスト デバイス ID 認証局運用規程 (Certification Practice Statement)」とする。

1.3 PKI の関係者

本 CPS に記述される PKI の関係者を以下に定める。各関係者は、本 CPS が定める義務を遵守しなければならない。

1.3.1 認証局

本 CPS「1.1 概要」に定める本認証局をいう。本認証局は、発行局および登録局から構成される。本認証局は本 CPS「5.2.1 信頼される役割および人物」に定める認証局責任者が総括し、本 CPS を承認する。また、本 CPS の改定のほか、登録局の登録･抹消や登録局オペレータ等の登録･抹消、本 CPS 等に関する照会受け付け等本認証局としての実務に対応するデバイス ID サポートデスクを内包する。

1.3.2 登録局

登録局は、次に掲げるものから成る。

1.3.2.1 デバイス ID 証明書登録局

デバイス ID 証明書の証明書管理に関わる登録局であり、加入者管理組織（本 CPS「1.3.4 加入者管理組織」に記載）によって運営される。デバイス ID 証明書登録局は、加入者管理組織の依頼を受け、加入者管理組織によって加入者に配付されるデバイス ID 証明書を発行し、または失効するため、発行局に対し、同処理を指示する。

1.3.2.2 ネットワーク機器専用サーバ証明書登録局

ネットワーク機器専用サーバ証明書の証明書管理に関わる登録局であり、サイバートラストによって運営される。ネットワーク機器専用サーバ証明書登録局は、加入者である加入者管理組織から、ネットワーク機器専用サーバ証明書の発行または失効の申請を受け、申請内容確認後、発行局に対し、これらの処理を指示する。なお、加入者が申請等を行うネットワーク機器専用サーバ証明書登録局の窓口については、デバイス ID サポートデスクが対応する。

1.3.3 発行局

発行局はサイバートラストが運営し、登録局の指示に基づき、証明書の発行または失効を行う。また、本 CPS に基づき、本認証局の秘密鍵を管理する。

1.3.4 加入者管理組織

加入者管理組織は、デバイス ID 証明書の管理を行うため、本 CPS および本 CPS「2.2 公開する情報」に定める関連諸規程に同意の上、加入者管理組織が申込責任者として選任した加入者管理組織に属する個人（以下、「本サービス申込責任者」という）をして本サービス申込書をデバイス ID サポートデスクに対し申請し、受理･登録された組織であり、デバイス ID 証明書登録局を運営する。加入者管理組織は、自らが運営するデバイス ID 証明書登録局に対し、デバイス ID 証明書の発行等を依頼し、発行されたデバイス ID 証明書を自らが管理する加入者に配付する。

また、加入者管理組織は、ネットワーク機器専用サーバ証明書登録局に対し、自らが利用または管理するネットワーク機器に対するネットワーク機器専用サーバ証明書の発行、または失効を依頼することができる。

加入者管理組織は、証明書の利用に際しては、自らが管理する加入者および信頼当事者をして、本 CPS および関連諸規程に同意させ、これらを遵守させる。

1.3.5 加入者

1.3.5.1 デバイス ID 証明書の加入者

デバイス ID 証明書における加入者とは、加入者管理組織の管理の下にある個人であって、加入者管理組織が認めるデバイスに加入者管理組織が配付するデバイス ID 証明書を導入したうえで当該デバイスを利用･管理する個人をいう。なお、加入者は、デバイス ID 証明書の利用の停止の必要が生じた場合には、加入者管理組織の指示または定めに従うものとする。

1.3.5.2 ネットワーク機器専用サーバ証明書の加入者

ネットワーク機器専用サーバ証明書については、加入者管理組織が加入者となる。加入者は、本認証局から発行されたネットワーク機器専用サーバ証明書を自らが利用または管理するネットワーク機器に導入する。なお、加入者は、ネットワーク機器専用サーバ証明書の利用の停止の必要が生じた場合には、ネットワーク機器専用サーバ証明書登録局に連絡する等、本 CPS および関連諸規程に従わなければならない。

1.3.6 信頼当事者

信頼当事者は、加入者管理組織の指示または定める事項に従い、本認証局および加入者の証明書の有効性について検証を行い、それらの証明書を信頼するよう設定された、ネットワーク･アクセス認証を実現するためのデバイスまたはネットワーク機器を利用または管理する組織または個人である。

1.3.7 その他の関係者

規定しない。

1.4 証明書の用途

1.4.1 証明書の種類

本認証局は、以下の証明書を発行する。

1.4.1.1 自己署名証明書

自己署名証明書は、本認証局自身の証明書であり、本認証局の公開鍵に対して本認証局の秘密鍵で電子署名をしている。本認証局の秘密鍵は、加入者に配付されるデバイス ID 証明書、ネットワーク機器専用サーバ証明書、OCSP サーバ証明書および証明書失効リスト（以下、「CRL」という。）への電子署名の用途に使用される。

1.4.1.2 デバイス ID 証明書

デバイス ID 証明書は、加入者管理組織が認めるデバイスを認証し、また、それらと信頼当事者のネットワーク機器間における SSL、IPsec、IEEE802.1x 等でのネットワーク･アクセス認証を実現する。本認証局は、本認証局の判断および管理の下、動作確認等を目的としたデバイス ID 証明書の発行･失効を行えるものとする。

1.4.1.3 ネットワーク機器専用サーバ証明書

ネットワーク機器専用サーバ証明書は、ネットワーク機器専用サーバ証明書の加入者のネットワーク機器を認証し、また、それらと信頼当事者のデバイス間における IPsec または IEEE802.1x でのネットワーク･アクセス認証を実現する。本認証局は、本認証局の判断および管理の下、動作確認等を目的としたネットワーク機器専用サーバ証明書の発行･失効を行えるものとする。

1.4.1.4 OCSP サーバ証明書

OCSP（Online Certificate Status Protocol）サーバ証明書は、本認証局が提供するオンライン失効情報への電子署名の用途に使用される。

1.4.2 適切な証明書の用途

証明書の用途は次のとおり定める。

1.4.2.1 デバイス ID 証明書の用途

① 証明書を導入したデバイスの認証

② その他本認証局が認める用途

1.4.2.2 ネットワーク機器専用サーバ証明書の用途

① デバイス ID 証明書を用いた IPsec または IEEE802.1x でのネットワーク･アクセス認証における、対向となるネットワーク機器の認証

② その他本認証局が認める用途

1.4.3 禁止される証明書の用途

本認証局は、本 CPS「1.4.2 適切な証明書の用途」に定める用途以外での利用を禁止する。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CPS は、本認証局により管理される。

1.5.2 連絡窓口

本認証局は、サイバートラストが提供するサービスおよび本 CPS 等に関する照会を以下の連絡先で受け付ける。

連絡先
サイバートラスト株式会社　デバイス ID サポートデスク 受付日:　月曜日～金曜日（祝祭日、年末年始 12 月 30 日～1 月 4 日を除く） 受付時間: 9:00～12:00　13:00～17:00 お問合せ: did_support@cybertrust.ne.jp 住　所:　〒107-6030　東京都港区赤坂 1 丁目 12 番 32 号　アーク森ビル 30 階

1.5.3 CPS の適合性を決定する者

規定しない。

1.5.4 適合性の承認手続き

規定しない。

1.6 定義と略語

本 CPS の Appendix A に規定する。

2. 公開とリポジトリの責任

2.1 リポジトリを管理する組織

本認証局のリポジトリは、サイバートラストが管理する。

2.2 公開する情報

本認証局は、次のとおりリポジトリで公開する。

以下の情報を https://www.cybertrust.ne.jp/deviceid/repository.html に公開する。

- 本 CPS
- その他本サービスに関わる利用約款等（リポジトリにより公開される本サービスに関わる利用約款等で、サイバートラスト デバイス ID 利用約款を含むが、これらに限られない。以下、「関連諸規程」という。）
- 自己署名証明書（但し、混同を避けるため、リポジトリには、Cybertrust DeviceiD Public CA G1 および G2 認証局の自己署名証明書のみを公開し、他の認証局の自己署名証明書については、デバイス ID サポートデスクが必要に応じ個別に提供することとする。）

本認証局が発行する CRL については、以下の各 URL で公開する。

- http://mpkicrl.managedpki.ne.jp/mpki/CybertrustDeviceiDPublicCAG1/cdp.crl
- http://crl.deviceid.ne.jp/deviceid/g2.crl
- http://crl.deviceid.ne.jp/deviceid/g2s.crl
- http://crl.deviceid.ne.jp/deviceid/g2k.crl
- http://crl.deviceid.ne.jp/deviceid/g2is.crl
- http://crl.deviceid.ne.jp/deviceid/g2sp.crl
- http://crl.deviceid.ne.jp/deviceid/g3k.crl

本認証局が提供するオンライン失効情報(OCSP)については、以下の URL で提供する。

- http://ocsp.deviceid.ne.jp/deviceid

2.3 公開の時期と頻度

本認証局が公開する情報について、公開の時期と頻度は以下のとおりである。ただし、リポジトリのメンテナンス等が生じる場合は、この限りでないものとするが、CRL および OCSP は 24 時間公開もしくは提供される。

① 本 CPS、関連諸規程については、改訂の都度、公開される。

② CRL は、本 CPS「4.9.7 CRL 発行周期」で規定された周期で更新を行い、公開される。

③ OCSP は、本 CPS「4.9.9 オンラインでの失効情報の確認」で規定された周期で更新を行い、提供される。

④ 自己署名証明書については、少なくとも有効期間中は公開される。

2.4 リポジトリに対するアクセスコントロール

本認証局は、リポジトリに対する特段のアクセスコントロールは講じない。

3. 識別および認証

3.1 名前の決定

3.1.1 名称のタイプ

加入者は、証明書の中の X.500 識別名 Distinguished Name（以下、「DN」という。）により識別される。

3.1.2 名称の意味に関する要件

証明書の DN 等に含まれる名称は、次項の意味を持つ。

3.1.2.1 デバイス ID 証明書の場合

DN 項目	意味
コモンネーム（Common Name）	デバイス ID 証明書登録局が定めるデバイスの識別情報（MAC アドレス等を含むが、それらに限られない）
組織名（Organization）	<加入者管理組織の名称＋会社識別子>（注）
組織単位名（Organization Unit）	RA operated by <加入者管理組織の名称＋会社識別子>（注）
	デバイス ID 証明書登録局が定める部署名等 ※（任意項目、最大2つまで）
国名（Country）	事業所住所（国）

注 組織名（Organization）については、デバイス ID 証明書を発行したデバイス ID 証明書登録局を運営する加入者管理組織を区分する名称が＜加入者管理組織の名称＋会社識別子＞ として記載される。
また、組織単位名（Organization Unit）の1つについても同様に、"RA operated by "に続き、同名称：＜加入者管理組織の名称＋会社識別子＞が記載される。
具体的に＜加入者管理組織の名称＋会社識別子＞としては、加入者管理組織による本サービス利用開始にあたってのデバイス ID サポートデスクによるデバイス ID 証明書登録局の本認証局への登録に際し、本認証局デバイス ID サポートデスクが一意に定めた同組織の英語名称（ただし、Co.,Ltd.等の記載を除く）、およびデバイス ID 証明書登録局を一意に定めた会社識別子（4桁の 16 進数値）が用いられる。

3.1.2.2 ネットワーク機器専用サーバ証明書の場合

DN 項目	意味
コモンネーム（Common Name）	加入者管理組織が利用または管理するネットワーク機器の FQDN
組織名（Organization）	<加入者管理組織の名称＋会社識別子>（注）
組織単位名（Organization Unit）	加入者管理組織の部署名等　※（任意項目、最大2つまで）
都道府県名（State or Province）	加入者管理組織の事業所住所（都道府県）　※（任意項目）
市町村名（Locality）	加入者管理組織の事業所住所（市町村）　※（任意項目）
国名（Country）	加入者管理組織の事業所住所（国）

証明書拡張領域の項目	意味
別名（SubjectAltName）	加入者管理組織が利用または管理するネットワーク機器の FQDN ※（任意項目、複数可）

注.　組織名（Organization）については、ネットワーク機器専用サーバ証明書の発行を受ける加入者管理組織を区分する名称が＜加入者管理組織の名称＋会社識別子＞　として記載される。具体的には、本 CPS「3.1.2.1 デバイス ID 証明書の場合」の注と同じ値が用いられる。

3.1.3　加入者の匿名・仮名についての要件

規定しない。

3.1.4　様々な名称形式を解釈するためのルール

本認証局が発行する証明書の DN の形式を解釈するためのルールは、X.500 に準ずる。

3.1.5　名称の一意性

3.1.5.1　デバイス ID 証明書の場合

本認証局は、デバイス ID 証明書に記載される組織名（Organization）によりデバイス ID 証明書登録局を一意に識別する。デバイス ID 証明書登録局は、当該登録局を運営する加入者管理組織が認めるデバイスを DN により一意に識別するよう、デバイス ID 証明書を発行・管理しなければならない。

3.1.5.2　ネットワーク機器専用サーバ証明書の場合

本認証局は、ネットワーク機器専用サーバ証明書に記載される DN および SubjectAltName によりネットワーク機器を一意に識別する。

3.1.6　商標等の認識、認証および役割

本認証局は、登録局の登録および証明書の発行に際し、著作権、営業秘密、商標権、実用新案権、特許権その他の知的財産権（特許その他の知的財産を受ける権利を含むがこれらに限られない。以下単に「知的財産権」という。）については、確認しない。

3.2　初回の本人性確認

3.2.1　秘密鍵の所有を確認する方法

3.2.1.1　デバイス ID 証明書の場合

本認証局は、加入者管理組織の依頼に基づき、デバイス ID 証明書の加入者に配付される秘密鍵を生成し、本 CPS「6.1.2 加入者秘密鍵の配付」の定めに従い配付を行う。同配付をもって、加入者が秘密鍵を保有したものとみなす。

3.2.1.2 ネットワーク機器専用サーバ証明書の場合

加入者管理組織からの申請情報の一部である証明書発行要求（以下、「CSR」という。）には、公開鍵および公開鍵に対応する秘密鍵による電子署名が含まれる。本認証局は、CSR に含まれる公開鍵を使用して電子署名を検証することで、当該 CSR が加入者の秘密鍵で署名されていることを確認し、これにより加入者が秘密鍵を所有していると判断する。

3.2.2 加入者の確認

3.2.2.1 デバイス ID 証明書の場合

本認証局は、デバイス ID 証明書登録局が、当該登録局を運営する加入者管理組織から、当該組織が認めるデバイスに関わる情報と併せ、当該デバイスを管理し、デバイス ID 証明書を配付すべき加入者のリストを受け取ることをもって、加入者の確認とする。

3.2.2.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書については、加入者である加入者管理組織が、本 CPS「1.3.4 加入者管理組織」に定める本サービス申込責任者をして、ネットワーク機器専用サーバ証明書の申請を行わせるものとする。
本認証局は、加入者管理組織の本サービス申込責任者からネットワーク機器専用サーバ証明書の発行申請が行われていること、かつ、その申請内容に不備が無いことをもって、加入者の確認とする。

3.2.3 確認しない加入者情報

3.2.3.1 デバイス ID 証明書の場合

本認証局は、デバイス ID 証明書の加入者のコモンネーム（CN）および組織単位名（OU）については、デバイス ID 証明書登録局に対し、その値の真正性または正確性の確認を求めない。

3.2.3.2 ネットワーク機器専用サーバ証明書の場合

本認証局は、ネットワーク機器専用サーバ証明書の加入者のコモンネーム（CN）、別名（SubjectAltName）、組織単位名（OU）、都道府県名（S）および市町村名（L）については、加入者によるそれらの値の真正性および正確性の表明を確認するのみとし、値の直接の確認は行わない。

3.2.4 権限の正当性確認

本認証局は、登録局による「3.2.2 加入者の確認」に定める確認をもって、当該加入者が証明書の発行をうける権限を有することの確認とする。

3.2.5 相互運用性基準

規定しない。

3.3 鍵（証明書）更新申請時の本人性確認と認証

3.3.1 鍵（証明書）定期更新時の本人性確認と認証

本 CPS「3.2 初回の本人性確認」を準用する。

3.3.2 失効後の鍵（証明書）再発行時の本人性確認と認証

本 CPS「3.2 初回の本人性確認」を準用する。

3.4 失効申請時の確認と認証

3.4.1 失効申請時の確認と認証

3.4.1.1 デバイス ID 証明書の場合

本認証局は、デバイス ID 証明書登録局が、当該登録局を運営する加入者管理組織から失効が必要となるデバイス ID 証明書のリストを受け取ることをもって、失効申請時の確認とする。

3.4.1.2 ネットワーク機器専用サーバ証明書の場合

本認証局は、ネットワーク機器専用サーバ証明書登録局に対するネットワーク機器専用サーバ証明書の失効申請が、加入者管理組織の本サービス申込責任者から行われ、かつ、その申請内容に不備が無いことをもって、失効申請時の確認とする。

4. 証明書のライフサイクル運用的要件

4.1 証明書申請

4.1.1 証明書の申請が認められる者

4.1.1.1 デバイス ID 証明書の場合

デバイス ID 証明書登録局を運営する加入者管理組織。

4.1.1.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書の加入者である加入者管理組織。

4.1.2 申請方法および責任

4.1.2.1 デバイス ID 証明書の場合

本 CPS「3.2 初回の本人性確認」に記載のとおり、加入者管理組織が、デバイス ID 証明書の加入者のリストをもって申請を行うものとする。

4.1.2.2 ネットワーク機器専用サーバ証明書の場合

本 CPS「3.2 初回の本人性確認」に記載のとおり、ネットワーク機器専用サーバ証明書の加入者である加入者管理組織は、加入者管理組織の本サービス申込責任者をして、ネットワーク機器専用サーバ証明書登録局の窓口であるデバイス ID サポートデスクに対し、申請を行うものとする。当該申請は、本サービス申込責任者がサイバートラスト所定の Web サイトから行うものとする。申請に際して加入者は、申請情報の真正性および正確性の表明を行わなければならない。なお、ネットワーク機器専用サーバ証明書の CSR については、ネットワーク機器専用サーバ証明書登録局が当該申請を受領後、加入者管理組織の登録局オペレータが、別途サイバートラスト所定の Web サイトへ申請するものとする。

4.2 証明書申請の処理

4.2.1 本人性確認と認証業務の実行

本 CPS「3.2 初回の本人性確認」を準用する。

4.2.2 証明書申請の承認または拒否

本 CPS「3.2 初回の本人性確認」を準用する。

4.2.3 証明書申請の処理に要する時間

規定しない。

4.3 証明書の発行

4.3.1 認証局における証明書発行処理

4.3.1.1 デバイス ID 証明書の発行処理

デバイス ID 証明書登録局は、加入者管理組織の依頼に基づき、発行局に対してデバイス ID 証明書の発行を指示する。発行局は、デバイス ID 証明書を発行すると同時に、発行の通知については本 CPS「4.3.2 加入者に対する証明書の発行通知」に従い対応する。
なお、デバイス ID 証明書および秘密鍵の加入者への配付については、本認証局は以下の 2 種類の方法のいずれかを用いる。

① 加入者への鍵･証明書の個別配付
デバイス ID 証明書の加入者は、発行通知に記載される、デバイス ID 証明書および秘密鍵を受領するために必要な手続きに従い、インターネットを経由して直接デバイス ID 証明書および秘密鍵をダウンロードする。

② 加入者管理組織を経由した鍵･証明書の加入者への配付
デバイス ID 証明書の加入者は、加入者管理組織を経由して、デバイス ID 証明書および秘密鍵のデータを配付される。なお、加入者管理組織は、デバイス ID 証明書登録局からメディア等を用いて当該データを直接受け渡される。

4.3.1.2 ネットワーク機器専用サーバ証明書の発行処理

ネットワーク機器専用サーバ証明書登録局は、ネットワーク機器専用サーバ証明書の加入者からの依頼に基づき、発行局に対しネットワーク機器専用サーバ証明書の発行を指示する。発行局は、ネットワーク機器専用サーバ証明書を発行すると同時に、本 CPS「4.3.2 加入者に対する証明書の発行通知」に定める通知をネットワーク機器専用サーバ証明書の加入者に対し行う。

4.3.2 加入者に対する証明書の発行通知

4.3.2.1 デバイス ID 証明書の発行通知

本認証局は、デバイス ID 証明書の発行の通知については、その配付方法により、以下のとおり定める。

① 加入者への鍵･証明書の個別配付時
デバイス ID 証明書の加入者がデバイス ID 証明書および秘密鍵をダウンロードするために必要な手続きの情報を添えて、デバイス ID 証明書登録局が発行局に指示した当該加入者の電子メールアドレスに対し通知する。

② 加入者管理組織を経由した鍵･証明書の加入者への配付時
デバイス ID 証明書および秘密鍵を直接、加入者管理組織へ受け渡すことをもって通知とする。この場合、本認証局は、デバイス ID 証明書の加入者への個別の通知を行わない。

4.3.2.2 ネットワーク機器専用サーバ証明書の発行通知

本認証局は、ネットワーク機器専用サーバ証明書の発行後、発行の旨を加入者に対して通知する。通知は、加入者管理組織の登録局オペレータがネットワーク機器専用サーバ証明書の CSR を申請した際に指定した電子メールアドレスに対し行われる。

4.4 証明書の受領

4.4.1 証明書受領確認手続き

4.4.1.1 デバイス ID 証明書の場合

本認証局は、デバイス ID 証明書の受領確認手続きについては、証明書等の配付方法により、以下のとおり定める。

① 加入者への鍵･証明書の個別配付時

デバイス ID 証明書の加入者は、本 CPS「4.3.2 加入者に対する証明書の発行通知」の規定に基づく本認証局から送信された電子メールに記録された通知内容に従い、自らの認証の上、デバイス ID 証明書および当該証明書に関わる秘密鍵をダウンロードする。本認証局は、加入者がサイバートラスト所定の Web サイトよりデバイス ID 証明書および秘密鍵をダウンロードしたことをもって、当該証明書に関わる加入者が自らのデバイス ID 証明書を受領したものとみなす。

② 加入者管理組織を経由した鍵･証明書の加入者への配付

本認証局は、デバイス ID 証明書および秘密鍵を直接、加入者管理組織に引渡したことをもって、デバイス ID 証明書の受領確認とする。加入者管理組織は、受領したデバイス ID 証明書および秘密鍵を正しく加入者に配付しなければならない。

4.4.1.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書の加入者は、本 CPS「4.3.2 加入者に対する証明書の発行通知」の規定に基づく本認証局から送信された電子メールに記録された通知内容に従い、ネットワーク機器専用サーバ証明書をダウンロードする。本認証局は、ネットワーク機器専用サーバ証明書の加入者が、サイバートラスト所定の Web サイトよりネットワーク機器専用サーバ証明書をダウンロードしたことをもって、当該加入者がネットワーク機器専用サーバ証明書を受領したものとみなす。

4.4.2 認証局による証明書の公開

本認証局は、加入者の証明書を公開しない。

4.4.3 認証局による他の関係者に対する証明書発行の通知

本認証局は、本 CPS「4.3.2 加入者に対する証明書の発行通知」の規定に基づくもの以外の証明書の発行通知を行わない。

4.5 鍵ペアと証明書の利用

4.5.1 加入者による秘密鍵と証明書の利用

4.5.1.1 デバイス ID 証明書

デバイス ID 証明書の加入者は、本 CPS「1.4.2.1 デバイス ID 証明書の用途」に定める用途に限り秘密鍵およびデバイス ID 証明書が利用されるよう、加入者管理組織が認めるデバイスに対し、秘密鍵および証明書を導入するものとする。また、秘密鍵および証明書は、導入が認められたデバイスにおいてのみ利用できるものとし、他のデバイスにおいて利用できるようにしてはならない。なお、秘密鍵と証明書の利用に関するその他の加入者の義務は、本 CPS「9.6.3 加入者の表明保証」に定められ、デバイス ID 証明書の加入者は、加入者管理組織の指示または定めに従い、これらを遵守しなければならない。

4.5.1.2 ネットワーク機器専用サーバ証明書

ネットワーク機器専用サーバ証明書の加入者は、本 CPS「1.4.2.2 ネットワーク機器専用サーバ証明書の用途」に定める用途に限りネットワーク機器専用サーバ証明書が利用されるよう、コモンネーム（CN）もしくは別名(SubjectAltName)が該当するネットワーク機器に、当該証明書を導入するものとする。当該証明書は、当該ネットワーク機器においてのみ利用されるものとし、加入者は、他のネットワーク機器において利用できるようにしてはならない。なお、ネットワーク機器専用サーバ証明書の利用に関するその他の加入者の義務は、本 CPS「9.6.3 加入者の表明保証」に定められ、ネットワーク機器専用サーバ証明書の加入者は、これらを遵守しなければならない。

4.5.2 信頼当事者による加入者の公開鍵と証明書の利用

信頼当事者は、加入者管理組織の指示または定めに従い本認証局および加入者の証明書の有効性について検証が行われ、それらの証明書が信頼されるようデバイスもしくはネットワーク機器を設定･管理するものとする。

なお、信頼当事者による加入者の公開鍵と証明書の利用に関するその他の義務は、本 CPS「9.6.5 信頼当事者の表明保証」に定められ、信頼当事者は、加入者管理組織の指示または定めに従い、これらを遵守しなければならない。

4.6 鍵更新を伴わない証明書の更新

本認証局は、鍵ペアの更新を伴わない証明書の更新は認めない。

4.6.1 鍵更新を伴わない証明書の更新に関する要件

規定しない。

4.6.2 更新申請が認められる者

規定しない。

4.6.3 更新申請の手続き

規定しない。

4.6.4 更新された証明書の発行に関する通知

規定しない。

4.6.5 更新された証明書の受領手続き

規定しない。

4.6.6 更新された証明書の公開

規定しない。

4.6.7 認証局による他の関係者に対する証明書の発行通知

規定しない。

4.7 鍵更新を伴う証明書の更新

4.7.1 鍵更新を伴う証明書の更新に関する要件

4.7.1.1 デバイス ID 証明書の場合

デバイス ID 証明書登録局は、当該登録局を運営する加入者管理組織によりデバイス ID 証明書の更新を認められた加入者に対し、デバイス ID 証明書の更新発行を行う。ただし、本認証局はデバイス ID 証明書の更新に際しては、新たな鍵ペアを生成するものとする。

4.7.1.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書の更新に際して、ネットワーク機器専用サーバ証明書の加入者は、新たな鍵ペアを生成しなければならない。

4.7.2 更新申請が認められる者

本 CPS「4.1.1 証明書の申請が認められる者」を準用する。

4.7.3 鍵更新申請の手続き

本 CPS「4.2 証明書申請の処理」を準用する。

4.7.4 鍵更新された証明書の発行に関する通知

本 CPS「4.3.2 加入者に対する証明書の発行通知」を準用する。

4.7.5 鍵更新された証明書の受領手続き

本 CPS「4.4.1 証明書受領確認手続き」を準用する。

4.7.6 鍵更新された証明書の公開

本 CPS「4.4.2 認証局による証明書の公開」を準用する。

4.7.7 他の関係者に対する鍵更新された証明書の発行通知

本 CPS「4.4.3 認証局による他の関係者に対する証明書発行の通知」を準用する。

4.8 証明書の変更

4.8.1 証明書の変更に関する要件

4.8.1.1 デバイス ID 証明書の場合

デバイスID証明書登録局は、既に発行されたデバイス ID 証明書の変更の申請を受け付けないものとする。デバイス ID 証明書の加入者は、証明書情報の変更の必要が生じた場合、その利用または管理を認めた組織に連絡する等、加入者管理組織の指示または定めに従うものとする。

4.8.1.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書登録局は、既に発行されたネットワーク機器専用サーバ証明書の変更の申請を受け付けないものとする。ネットワーク機器専用サーバ証明書の加入者は、証明書情報の変更の必要が生じた場合、ネットワーク機器専用サーバ証明書の失効申請および新規申請を個別に行うものとする。

4.8.2 証明書変更申請が認められる者

規定しない。

4.8.3 証明書変更の手続き

規定しない。

4.8.4 変更された証明書の発行に関する通知

規定しない。

4.8.5 変更された証明書の受領手続き

規定しない。

4.8.6 変更された証明書の公開

規定しない。

4.8.7 他の関係者に対する変更された証明書の発行通知

規定しない。

4.9 証明書の失効および一時停止

4.9.1 失効に関する要件

4.9.1.1 登録局による失効事由

登録局は、自らが発行局に申請し、発行した証明書について、以下のいずれかの事由が生じた場合、それが判明した時点で、当該証明書を失効するものとする。

① 加入者の秘密鍵が、危殆化または危殆化の可能性があることを合理的な証拠に基づき知り得た場合

② 証明書の内容が事実と異なることを合理的な証拠に基づき知り得た場合

③ 証明書が不正に使用されていることを合理的な証拠に基づき知り得た場合

④ 加入者以外の者へ証明書が不正に発行されていることを合理的な証拠に基づき知り得た場合

⑤ 本 CPS または関連諸規程に違反した証明書の発行を行っていたことを合理的な証拠に基づき知り得た場合

4.9.1.2 本認証局デバイス ID サポートデスクによる失効事由

本認証局デバイス ID サポートデスクは、以下のいずれかの事由が生じた場合、それが判明した時点で、発行局に対し、関連する証明書の失効を指示できるものとする。ただし、⑥については、別途本認証局が業務終了前に事前に通知した日の失効を指示することができる。

① 加入者管理組織による本サービスの利用が解除された場合

② 登録局または当該登録局を運営する加入者管理組織が本 CPS または関連諸規程に違反し、本認証局デバイス ID サポートデスクがその違反の是正を求める通知を発送した後、7 日間を経過した後においても、違反が是正されなかった場合

③ 登録局の指示によらない、または指示とは異なる証明書が発行されていたことを合理的な証拠に基づき知り得た場合

④ 本認証局の秘密鍵が危殆化または危殆化の可能性があることを知り得た場合

⑤ 本認証局が、本 CPS に準拠せずに証明書を発行した場合

⑥ 本認証局が認証業務を終了する場合

4.9.1.3 加入者管理組織による失効事由

加入者管理組織は、加入者管理組織が管理する加入者に配付したデバイス ID 証明書、および加入者管理組織が発行を受けたネットワーク機器専用サーバ証明書について、その失効の必要を認めた場合（以下のいずれかの事由を含むが、これらに限られない）、直ちに当該証明書の失効を該当する登録局に依頼するものとする。

① 証明書を導入したデバイスもしくはネットワーク機器の利用を中止する場合

② デバイスもしくはネットワーク機器における証明書の利用を中止する場合

③ デバイスもしくはネットワーク機器の秘密鍵が、危殆化または危殆化の可能性があることを合理的な証拠に基づき知り得た場合

④ 証明書の内容が事実と異なることを合理的な証拠に基づき知り得た場合

⑤ 証明書が不正に使用されていることを合理的な証拠に基づき知り得た場合

⑥ 加入者以外の者へ証明書が不正に発行されていることを合理的な証拠に基づき知り得た場合

⑦ 本 CPS または関連諸規程に違反した証明書の発行または利用を行っていたことを合理的な証拠に基づき知り得た場合

4.9.1.4 加入者による失効事由

① デバイス ID 証明書の場合

デバイス ID 証明書の加入者は、デバイス ID 証明書の失効の必要を認めた場合（以下のいずれかの事由を含むが、それらに限られない）、利用または管理を認めた組織に連絡する等、加入者管理組織の指示または定めに従うものとする。

a デバイス ID 証明書を導入したデバイスの利用を中止する場合

b デバイスにおけるデバイス ID 証明書の利用を中止する場合

c デバイスに導入した秘密鍵が、危殆化または危殆化の可能性があることを合理的な証拠に基づき知り得た場合

d デバイス ID 証明書の内容が事実と異なることを合理的な証拠に基づき知り得た場合

e デバイス ID 証明書が不正に使用されていることを合理的な証拠に基づき知り得た場合

f 本 CPS または関連諸規程に違反したデバイス ID 証明書の利用を行っていたことを合理的な証拠に基づき知り得た場合

② ネットワーク機器専用サーバ証明書

ネットワーク機器専用サーバ証明書の加入者による失効事由については、本 CPS「4.9.1.3 加入者管理組織による失効事由」の定めに従う。

4.9.2 失効申請が認められる者

失効申請が認められる者は、次のとおりである。
なお、本 CPS「4.1.9.2 本認証局デバイス ID サポートデスクによる失効事由」に記載の通り、デバイス ID サポートデスクが必要と認める場合、発行局に対し、失効を指示することができる。

4.9.2.1 デバイス ID 証明書の場合

・ 加入者管理組織

4.9.2.2 ネットワーク機器専用サーバ証明書の場合

・ 加入者管理組織

4.9.3 失効申請の手続き

登録局は、証明書毎に認められた申請者からの失効申請をもって失効を行う。
また、本 CPS「4.1.9.2 本認証局デバイス ID サポートデスクによる失効事由」に記載のとおり、デバイス ID サポートデスクが必要と認める場合、発行局に指示し、失効を行うことができる。

4.9.4 失効申請までの猶予期間

失効申請を行う者は、失効の必要を認めた場合、速やかに失効の申請を行うものとする。

4.9.5 認証局における失効処理にかかる時間

発行局は、失効の指示を受けた後、遅滞無く当該証明書を失効する。

4.9.6 信頼当事者による失効の確認方法

信頼当事者は、本認証局が発行する CRL または OCSP により、証明書の失効を確認する。

4.9.7 CRL 発行周期

本認証局は、失効を行う都度 CRL を発行する。失効が行われない場合でも、少なくとも 24 時間に 1 度、CRL を発行する。

4.9.8 CRL 発行までの最大遅延時間

本認証局の CRL の有効期間は 168 時間である。本認証局は、遅くとも発行から 1 時間以内に最新の CRL をリポジトリに公開する。但し認証局の判断により、当該有効期間・遅延時間を超えて CRL を発行・公開する場合がある。

4.9.9 オンラインでの失効情報の確認

本認証局は、CRL に加え OCSP により失効情報を提供する。本認証局の OCSP レスポンスの有効期間は 168 時間である。本認証局は、リポジトリに公開された最新の CRL に基づき OCSP レスポンスを更新する。但し認証局の判断により、当該有効期間・周期を超える場合がある。

4.9.10 オンラインでの証明書ステータスの確認

規定しない。

4.9.11 その他の利用可能な失効情報の提供手段

規定しない。

4.9.12 鍵の危殆化に関する特別要件

規定しない。

4.9.13 証明書の一時停止に関する要件

本認証局は、証明書の一時停止を許可する。
発行局は、登録局からの証明書の一時停止の指示を受け、CRL に当該証明書情報を登録し、また一時停止の解除の指示を受け、CRL に登録された当該証明書の情報を CRL より削除する。

4.9.14 一時停止の申請が認められる者

本 CPS「4.9.2 失効申請が認められる者」を準用する。

4.9.15 一時停止の申請手続き

本 CPS「4.9.3 失効申請の手続き」を準用する。

4.9.16 一時停止の期間

規定しない。

4.10 証明書のステータス確認サービス

本認証局は、CRL および OCSP 以外で証明書のステータスを確認できるサービスを提供しない。

4.10.1 運用上の特徴

規定しない。

4.10.2 サービスレベル

規定しない。

4.10.3 その他の要件

規定しない。

4.11 加入（登録）の終了

本認証局では、本 CPS「3.2.2 加入者の確認」に記載された確認が行われた者が、加入者として登録され、当該加入者に発行された証明書の有効期間満了をもって、登録の終了となる。証明書が有効である間については、本 CPS「4.9.1 失効に関する要件」に基づく証明書の失効をもって、登録の終了となる。

4.12 鍵の第三者預託および鍵回復

4.12.1 鍵の預託および鍵回復のポリシーならびに手順

規定しない。

4.12.2 セッションキーのカプセル化・復旧のポリシーの手順

規定しない。

5. 運営、運用、物理的管理

5.1 物理的管理

5.1.1 立地場所および構造

本認証局のシステム（サイバートラストが管理する本サービスを提供するためのシステムをいい、登録局が認証業務に用いる端末等は含まれない。以下、「本認証局システム」という。）は、地震、火災、水害、およびその他の災害による影響を容易に受けない施設（サイバートラストが管理する施設を指し、以下、「本施設」という。）内に設置される。また、本施設には、建築構造上、耐震、耐火および水害その他の災害防止ならびに不正侵入防止の措置が講じられる。なお、本施設が設置される建築物の外部および建築物内には、本認証局の所在に関わる情報を表示しない。

5.1.2 物理的アクセス

本施設は、業務の重要度に応じたセキュリティ・レベルが設けられ、相応の入退室管理が行われる。入退室時の認証には、セキュリティ・レベルに応じ、入退室用カードまたは生体認証その他の実装可能な技術的手段を用いるほか、特に重要な各室への入室に際しては、入室権限を有する複数名が揃わなければ開扉されない措置を講ずる。

本施設は、監視システムにより、24 時間 365 日の監視が行われる。

5.1.3 電源・空調設備

本施設では、本認証局システムおよび関連機器類の運用のために必要かつ十分な容量の電源を確保する。また、瞬断ならびに停電対策として、無停電電源装置および自家発電機を設置する。さらに、認証業務を行う各室には空調設備を設置し、特に重要な室内は 2 重化する。

5.1.4 水害対策

本施設内の特に重要な各室には漏水検知機を設置し、天井および床には防水対策を講じる。

5.1.5 火災対策

本施設は、耐火構造の建物である。また、特に重要な各室は防火区画内に設置され、火災報知機および自動ガス式消火設備を備える。

5.1.6 地震対策

本施設は、耐震構造の建物である。また、本認証局システムに関わる機器および什器には転倒および落下を防止する対策を講じる。

5.1.7 媒体保管場所

本施設では、本認証局システムのバックアップデータが含まれる媒体、関連する書類等については、職務上利用することが許可された者のみが入室できる室内に保管する。

5.1.8 廃棄物処理

本施設では、機密情報を含む書類はシュレッダーにより裁断の上、廃棄する。電子媒体については、物理的破壊、初期化、消磁等の措置によって記録されたデータを完全に抹消の上、廃棄する。

5.1.9 遠隔地保管

規定しない。

5.2 手続的管理

5.2.1 信頼される役割および人物

本認証局は、認証局を運営するために必要な人員（以下、「認証局員」という。）およびその役割を以下のとおり定める。

5.2.1.1 認証局責任者

認証局責任者は、サイバートラストから選任され、本認証局を総括する。

5.2.1.2 発行局責任者

発行局責任者は、サイバートラストから選任され、本認証局の発行局業務を管理する。

5.2.1.3 発行局システムアドミニストレータ

発行局システムアドミニストレータは、発行局責任者の管理の下、本認証局システムの維持･管理を行う。

5.2.1.4 発行局オペレータ

発行局オペレータは、発行局責任者および発行局システムアドミニストレータの業務を補佐する。ただし、本認証局システムを操作する権限は付与されない。

5.2.1.5 登録局オペレータ責任者（RA オペレータ責任者）

① デバイス ID 証明書の場合

デバイス ID 証明書の登録局オペレータ責任者（RA オペレータ責任者）は、加入者管理組織の従業員または役員から加入者管理組織により選任され、本認証局デバイス ID サポートデスクに登録受理された者をいい、本認証局のデバイス ID 証明書の登録業務を管理する。

② ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書の登録局オペレータ責任者（RA オペレータ責任者）は、サイバートラストにより選任された者をいい、本認証局のネットワーク機器専用サーバ証明書の登録業務を管理する。

5.2.1.6 登録局オペレータ（RA オペレータ）

① デバイス ID 証明書の場合

デバイス ID 証明書の登録局オペレータ（RA オペレータ）は、加入者管理組織により選任され、本認証局デバイス ID サポートデスクに登録受理された者をいい、デバイス ID 証明書の登録局オペレータ責任者の管理の下、加入者管理組織が認めた加入者のデバイス ID 証明書を発行または失効するために、発行局に対して発行または失効の処理を指示する。

② ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書の登録局オペレータ（RA オペレータ）は、サイバートラストにより選任された者をいい、ネットワーク機器専用サーバ証明書の登録局オペレータ責任者の管理の下、ネットワーク機器専用サーバ証明書を発行または失効するために、発行局に対して発行または失効の処理を指示する。

5.2.2 役割ごとに必要とされる人数

本認証局は、発行局システムアドミニストレータについては 2 名以上配置する。

5.2.3 各役割における本人性確認と認証

本認証局は、各役割に応じ、本施設内の各室の入室権限および本認証局システムへのアクセス権限を定める。各室の入室時またはシステムへのアクセス時においては、入退室カード、生体認証、証明書、ID およびパスワード等の単体または組合せ等の必要な措置がとられ、本人性および権限の確認ならびに認証が行われる。

5.2.4 職務の分離が必要とされる役割

本認証局は、デバイス ID 証明書登録局と発行局の業務の兼務を認めない。また、認証局責任者が他の役割を兼務することも認めない。

登録局においては、登録局オペレータ責任者と登録局オペレータの兼務を認めない。

5.3 人事的管理

5.3.1 経歴、資格、経験等に関する要求事項

認証局員（ただし、デバイスID証明書の登録局オペレータ責任者および登録局オペレータは除く。以後、同様とする。）は、サイバートラストが別途定める採用基準に基づき採用、選任され、配置される。

デバイスID証明書の登録局オペレータ責任者および登録局オペレータの選任、配置については、当該責任者およびオペレータを選任した加入者管理組織の基準、規程等による。

5.3.2 身元調査手続き

規定しない。

5.3.3 教育および訓練

本認証局は、認証局員として配置されるサイバートラストのすべての従業員に対し、必要な教育および訓練を実施する。

デバイスID証明書の登録局オペレータ責任者および登録局オペレータへの教育および訓練については、 デバイスID証明書の登録局オペレータ責任者および登録オペレータを選任した加入者管理組織が必要と認めた場合、別途サイバートラストと合意の上、サイバートラストが教育および訓練を行う場合がある。

5.3.4 再教育･訓練の周期と要件

本認証局は、認証局員に対する再教育および訓練を適宜実施する。少なくとも以下の事態が生じた場合は、教育･訓練を実施する。

① 本 CPS、および関連諸規程の変更時で、認証局責任者、発行局責任者、またはネットワーク機器専用サーバ証明書の登録局責任者が必要と判断した場合

② 本認証局システムの変更をする場合であって、認証局責任者、発行局責任者、またはネットワーク機器専用サーバ証明書の登録局責任者が必要と判断した場合

③ その他、認証局責任者、発行局責任者、またはネットワーク機器専用サーバ証明書の登録局責任者が必要と判断した場合

なお、デバイス ID 証明書の登録局オペレータ責任者および登録局オペレータへの再教育･訓練については、選任者が変更となった場合等、加入者管理組織が必要と認めた場合、別途サイバートラストと合意の上、サイバートラストが再教育･訓練を行う場合がある。

5.3.5 職務ローテーションの周期と順序

本認証局は、必要に応じ認証局員の配置転換を行う。

デバイス ID 証明書の登録局オペレータ責任者および登録局オペレータについては規定しない。

5.3.6 許可されていない行動に対する罰則

サイバートラストは、認証局員として配置されるサイバートラストの従業員が本 CPS および関連諸規程に反する行動をした場合、速やかに原因ならびに影響範囲等の調査を行った上で、サイバートラストの就業規則および社内規程に準じ、処罰を課す。

本認証局デバイス ID サポートデスクは、デバイス ID 証明書の登録局オペレータ責任者または登録局オペレータが本 CPS および関連諸規程に反する行動をしたことを知り得た場合、デバイス ID サポートデスクは当該登録局に対し、その違反の是正を求める通知を発送する。発送後、7 日間を経過した後においても、違反が是正されなかった場合、デバイス ID 証明書登録局としての登録を解除する等、必要な対応を行う。

5.3.7 契約社員等に対する契約要件

サイバートラストは、業務委託先の社員、契約社員または派遣社員等（以下、「契約社員等」という。）を認証局員として配置する場合、担当業務の内容、契約社員等に課す守秘義務および罰則等を明確に定めた契約を結ぶとともに、契約社員等に対し、本 CPS およびサイバートラストの社内規程の遵守を要求する。契約社員等が本 CPS およびサイバートラストの社内規程に反する行動をした場合、処罰については、当該契約に基づき行う。

加入者管理組織は、同組織が管理責任を負う契約社員等をデバイス ID 証明書の登録局オペレータとして配置する場合、担当業務の内容、契約社員等に課す守秘義務および罰則等を明確に定めた契約を結ぶとともに、契約社員等に対し、本 CPS および関連諸規程の遵守を要求し、同意を得るものとする。

5.3.8 認証局員が参照できる文書

本認証局は、各認証局員に対し、役割に応じた必要な文書のみが参照できる措置を講ずる。

5.4 監査ログの手続き

5.4.1 記録されるイベントの種類

本認証局は、本 CPS の準拠性およびセキュリティの妥当性を評価するため、監査ログとして以下の記録を収集する。なお、記録には日時、記録の主体、イベントの内容を記録する。

① 本認証局システム上の記録（登録局による発行・失効の申請の記録を含む）
② 本認証局システムに関わるネットワークセキュリティに関する記録
③ 本施設の入退室に関する記録
④ 本施設の維持管理に関する記録

5.4.2 監査ログを処理する頻度

本認証局は、本 CPS「5.4.1 記録されるイベントの種類」に規定された監査ログに関し、必要に応じ月次または随時確認する。

5.4.3 監査ログの保管期間

5.4.1「記録されるイベントの種類」①については、発行された証明書の有効期間満了後の少なくとも1年間は保管する。

他の記録については、少なくとも 3 年間は保管する。

本認証局は、監査ログが不要となったとき、本 CPS「5.1.8 廃棄物処理」の規定に基づき廃棄する。

5.4.4 監査ログの保護

本認証局は、許可された者のみが閲覧可能となるよう、監査ログへのアクセスコントロールを施す。保管庫への物理的なアクセスコントロール、電子媒体であればフォルダ等への論理的なアクセスコントロールを施す。

5.4.5 監査ログのバックアップ手続き

本認証局は、発行局のシステム上のログについては、バックアップを取得する。紙媒体については、原本のみを保管する。

5.4.6 監査ログの収集システム

発行局のシステムは、実装された機能により監査ログを自動的に収集する。

5.4.7 当事者への通知

本認証局は、イベントを発生させた当事者に通知することなく、監査ログを収集、検査する。

5.4.8 脆弱性評価

本認証局は、本認証局システムに対し、外部の専門家による脆弱性に関する評価を受け、当該脆弱性を是正するために必要な対応を行う。また、監査ログの検査により脆弱性が発見された場合についても、同様に必要な対応を行う。

5.5 記録の保管

5.5.1 保管対象となる記録

本認証局は、本 CPS「5.4.1記録されるイベントの種類」で規定された監査ログのほか、以下の情報を保管する。

① 自己署名証明書
② 加入者の証明書
③ CRL
④ 内部監査報告書
⑤ 加入者管理組織より受理した本サービス申請等の書類
⑥ 本 CPS および関連諸規程

5.5.2 記録の保管期間

本認証局は、本 CPS「5.5.1 保管対象となる記録」に規定される記録について、関連する証明書の有効期間を超えて少なくとも1年間保管する。

本認証局は、記録が不要となったとき、本 CPS「5.1.8 廃棄物処理」の規定に基づき廃棄する。

5.5.3 記録の保護

本 CPS「5.4.4 監査ログの保護」と同様の手続きにより行う。

5.5.4 記録のバックアップ手続き

本 CPS「5.4.5 監査ログのバックアップ手続き」と同様の手続きにより行う。

5.5.5 タイムスタンプ

本認証局は、本 CPS「5.5.1 保管対象となる記録」に関し、帳票類については起票日または処理した日付を記録する。また、日付のみでは記録としての立証性に欠ける場合は、時刻も記録する。本認証局および加入者の証明書については、発行された日時を記録する。また、本認証局システムには、発行する証明書および監査ログに対して正確な日付･時刻を記録するために必要な措置を講じる。

5.5.6 記録収集システム

本認証局は、本 CPS「5.5.1 保管対象となる記録」に関し、証明書については、本認証局システムの機能により自動的に収集する。その他の紙媒体については、認証局員が収集する。

5.5.7 記録の取得と検証手続き

本認証局は、本 CPS「5.5.1 保管対象となる記録」に関し、記録の取得および閲覧が認められる者として、認証局員、監査人および認証局責任者が認めた者に限定する。また、記録の可読性に関わる検証は、必要に応じ、実施する。

5.6 認証局の鍵更新

本認証局は、少なくとも 10 年毎に、認証局の鍵ペアを更新する。

更新された本認証局の公開鍵が含まれる証明書は、サイバートラストの Web サイトに公開する。

5.7 危殆化および災害からの復旧

5.7.1 危殆化および災害からの復旧手続き

サイバートラストは、発行局の責による場合を除き、本認証局の秘密鍵の危殆化による本サービスの停止を不可抗力事項として取り扱い、本サービス再開に要する時間について保証しない。

本認証局デバイス ID サポートデスクは、本認証局の秘密鍵が危殆化した場合、加入者管理組織に当該事実を通知する他、本認証局のリポジトリにおいても、その旨公開する。加入者管理組織は、本認証局デバイス ID サポートデスクよりかかる通知を受領した後は直ちに当該事実を自らが管理する加入者および信頼当事者へ通知するものとする。

本認証局は、以上に掲げる措置を実施するとともに、以下を実行して本サービスの再開に努める。

① 危殆化した秘密鍵を用いた認証業務の停止
② すべての証明書の失効
③ 危殆化の原因調査
④ 是正処置案の策定ならびに認証局責任者による評価･承認
⑤ 是正処置の実行
⑥ 業務再開の妥当性の評価
⑦ 新たな鍵ペアの生成および証明書の発行
⑧ 認証業務の再開（加入者および信頼当事者への通知を含む）
⑨ 証明書の再発行

また、本認証局が被災した場合には、本 CPS「5.7.4 災害時等の事業継続性」の規定に基づき本サービスの再開に努める。

5.7.2 システム資源の障害時の手続き

本認証局は、ハードウェア、ソフトウェア、またはデータが破壊された場合には、バックアップ用のハードウェア、ソフトウェア、またはデータを用いて復旧作業を行い、認証業務を継続する。

5.7.3 加入者秘密鍵の危殆化時の手続き

5.7.3.1 デバイス ID 証明書の場合

デバイス ID 証明書の加入者は、加入者管理組織によって配付された秘密鍵の危殆化または危殆化が疑われる事態が生じた場合、本 CPS「4.9.1 証明書の失効の要件」に記載されたとおり、当該事態の発生を加入者管理組織に連絡する等、加入者管理組織の指示または定めに従うものとする。

5.7.3.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書の加入者は、ネットワーク機器において利用される秘密鍵の危殆化または危殆化が疑われる事態が生じた場合、当該ネットワーク機器において該当する証明書の利用を停止し、本 CPS「4.9.1 証明書の失効の要件」に記載されたとおり、ネットワーク機器専用サーバ証明書登録局に失効の申請を行わなければならない。

5.7.4 災害時等の事業継続性

サイバートラストは、災害による本サービスの停止を不可抗力事項として取り扱い、本サービス再開に要する時間について保証しない。

本認証局デバイス ID サポートデスクは、災害により本サービスが停止した場合、加入者管理組織に当該事実を通知する他、サイバートラストの Web サイトにおいても、その旨公開する。加入者管理組織は、本認証局デバイス ID サポートデスクよりかかる通知を受領した後は直ちに当該事実を関連する加入者および信頼当事者へ通知するものとする。

本認証局を管理するサイバートラストは、以上に掲げる措置を実施するとともに、被災状況の調査を行い、調査結果に基づき、復旧方針を定めるものとし、発行局、登録局、本認証局デバイス ID サポートデスクは当該復旧方針に従い復旧作業を実施する。

5.8 認証局の業務の終了

本認証局は、本認証局の業務を終了する場合、加入者管理組織に事前に通知するほか、サイバートラストの Web サイトにおいても、その旨公開する。

本認証局が保有する証明書発行･失効申請に関わる情報については、廃棄するものとし、この旨は業務終了時にサイバートラストの Web サイト上で告知される。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成および導入

6.1.1 鍵ペアの生成

本認証局および OCSP サーバで使用する鍵ペアは、認証局責任者の指示を受け、発行局責任者の管理の下、複数の発行局システムアドミニストレータにより生成される。本認証局の鍵ペア生成の際には、FIPS 140 レベル 4 の規格を満たした秘密鍵暗号モジュール（以下、「HSM」という。）が用いられる。OCSP サーバで使用する鍵ペア生成の際には、FIPS 140 レベル 1 の規格を満たしたソフトウェアが用いられる。

6.1.2 加入者秘密鍵の配付

6.1.2.1 デバイス ID 証明書の場合

本認証局は、デバイス ID 証明書については、加入者管理組織の依頼に基づきデバイス ID 証明書に関わる秘密鍵を生成し、その機密性および完全性を確保する措置を講じたうえで、加入者へ配付する。

6.1.2.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書については、本認証局は、その秘密鍵を配送しない。秘密鍵は、加入者自らが生成する。

6.1.3 認証局への加入者公開鍵の配送

6.1.3.1 デバイス ID 証明書の場合

本認証局は、デバイス ID 証明書については、加入者からの公開鍵の配送を受け付けない。

6.1.3.2 ネットワーク機器専用サーバ証明書の場合

ネットワーク機器専用サーバ証明書については、ネットワーク機器専用サーバ証明書の発行申請情報の一部である CSR に含められ、加入者より配送される。

6.1.4 信頼当事者への認証局公開鍵の配送

本認証局は、信頼当事者に対する本認証局の公開鍵の配送を行わない。本認証局の公開鍵が含まれる自己署名証明書は、本認証局のリポジトリで公開される。

6.1.5 鍵長

本認証局が発行する証明書の署名方式および鍵長は下表のとおりとする。

証明書	署名方式	鍵長
自己署名証明書	SHA1 with RSA または SHA256 with RSA	2048 bit
デバイス ID 証明書	SHA1 with RSA または SHA256 with RSA	2048 bit（注）
ネットワーク機器専用サーバ証明書	SHA1 with RSA または SHA256 with RSA	1024 bit 以上
OCSP サーバ証明書	SHA1 with RSA または SHA256 with RSA	2048 bit

注. デバイスが 2048bit 鍵長に対応不能な場合に限り、1024bit を許容する。

6.1.6 公開鍵パラメータ生成および検査

規定しない。

6.1.7 鍵用途

本認証局が発行する証明書の鍵用途は下表のとおりとする。

証明書	鍵用途（Key Usage）
自己署名証明書	Certificate Signing, CRL Signing
デバイス ID 証明書	Digital Signature, Key Encipherment
ネットワーク機器専用サーバ証明書	Digital Signature, Key Encipherment
OCSP サーバ証明書	Digital Signature

6.2 秘密鍵の保護およ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および管理

本認証局の鍵ペアを管理するための暗号モジュールは、FIPS 140 レベル 4 の規格を満たした HSM とする。HSM は、発行局が管理する。

OCSP サーバで使用する鍵ペアは、FIPS 140 レベル 1 の規格を満たしたソフトウェアにより管理する。OCSP サーバは、発行局が管理する。

6.2.2 秘密鍵の複数人管理

本認証局および OCSP サーバで使用する秘密鍵の管理は、常時複数の発行局システムアドミニストレータが行う。

6.2.3 秘密鍵の預託

本認証局は、本認証局および OCSP サーバで使用する秘密鍵の預託を行わない。また、加入者の秘密鍵の預託も行わない。

6.2.4 秘密鍵のバックアップ

本認証局の秘密鍵のバックアップは、発行局システムアドミニストレータが行う。HSM からバックアップされた秘密鍵は、暗号化された上で複数に分割され、各々が施錠可能な保管庫に安全に保管される。HSM の故障等により秘密鍵の復元が必要となる場合、発行局システムアドミニストレータが、当該バックアップを用いて復元する。

OCSP サーバで使用する秘密鍵については、暗号化された状態で、システムのバックアップとして、発行局システムアドミニストレータによりバックアップされ、保管される。

6.2.5 秘密鍵のアーカイブ

本認証局は、本認証局および OCSP サーバで使用する秘密鍵のアーカイブを行わない。

6.2.6 秘密鍵の移送

本認証局は、本認証局および OCSP サーバで使用する秘密鍵のコピーを本施設外へ移送しない。

6.2.7 暗号モジュール内での秘密鍵保存

本認証局の秘密鍵は、HSM 内で生成され、暗号化された上で保存される。

6.2.8 秘密鍵の活性化

本認証局および OCSP サーバで使用する秘密鍵は、発行局責任者の承認の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータにより活性化される。また、活性化作業は記録される。

6.2.9 秘密鍵の非活性化

本認証局および OCSP サーバで使用する秘密鍵は、発行局責任者の承認の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータにより非活性化される。また、非活性化作業は記録される。

6.2.10 秘密鍵破壊の方法

本認証局および OCSP サーバで使用する秘密鍵は、認証局責任者の指示を受け、発行局責任者の管理の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータにより破壊される。同時に、本 CPS「6.2.4 秘密鍵のバックアップ」に規定されたバックアップされた秘密鍵についても、同様の手順に基づき破壊される。また、破壊作業は記録される。

6.2.11 暗号モジュールの評価

本認証局は、本 CPS「6.2.1 暗号モジュールの標準と管理」に定める標準を満たした HSM を使用する。

6.3 鍵ペアのその他の管理

6.3.1 公開鍵の保存

公開鍵の保存は、それが含まれる証明書を保存することで行う。

6.3.2 鍵ペアの有効期間

本認証局が発行する証明書の有効期間は下表のとおりとする。

証明書	有効期間
自己署名証明書	181 ヶ月以内とする。
デバイス ID 証明書	61 ヶ月以内とする。
ネットワーク機器専用サーバ証明書	62 ヶ月以内とする。
OCSP サーバ証明書	25 ヶ月以内とする。

6.4 活性化データ

6.4.1 活性化データの作成および設定

本認証局で使用する活性化データは、容易に推測されないよう配慮の上作成され、設定される。

6.4.2 活性化データの保護および管理

本認証局内で使用される活性化データは、本 CPS「5.1.2 物理的アクセス」の規定に基づき入退室管理が施された室内において、施錠可能な保管庫に保管される。

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

本認証局システムは、セキュリティ対策として以下を実施する。

① 操作者の権限の認証
② 操作者の識別と認証
③ 重要なシステム操作に対する操作ログの取得
④ 適切なパスワード設定および定期的な変更
⑤ バックアップ・リカバリ

6.5.2 コンピュータセキュリティの評価

本認証局は、本認証局が本施設内に導入するハードウェア、ソフトウェアに対して、事前に導入評価を実施する。また、使用する本認証局システムにおけるセキュリティ上の脆弱性に関する情報収集および評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対応を行う。

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

本認証局システムの構築および変更は、サイバートラスト内部で任命された開発責任者の管理の下、別途定められた規定に基づき行う。開発責任者が必要と判断する場合は、テスト環境において必要かつ十分な検証を行い、セキュリティ上問題がないことを確認する。

6.6.2 セキュリティ運用管理

本認証局システムは、十分なセキュリティを確保するために必要な設定が行われる。また、セキュリティ・レベルに則した入退室管理やアクセス権限管理、システムのウィルス対策等を実施するとともに、セキュリティ上の脆弱性についての情報収集および評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対応を行う。

6.6.3 ライフサイクルセキュリティ管理

本認証局は、本認証局システムの開発、運用、変更、廃棄の各工程において責任者を定め、作業計画または手順を策定・評価し、必要に応じ試験を行う。また、各作業は記録される。

6.7 ネットワークセキュリティ管理

本認証局システムとインターネット等の外部システムとは、ファイアウォール等を介し接続され、また、侵入検知システムによる監視が行われる。

6.8 タイムスタンプ

本 CPS「5.5.5 タイムスタンプ」を準用する。

7. 証明書および CRL のプロファイル

7.1 証明書のプロファイル

7.1.1 バージョン番号

自己署名証明書、デバイス ID 証明書、ネットワーク機器専用サーバ証明書および OCSP サーバ証明書については、Appendix B に定める。

7.1.2 証明書拡張領域

自己署名証明書、デバイス ID 証明書、ネットワーク機器専用サーバ証明書および OCSP サーバ証明書については、Appendix B に定める。

7.1.3 アルゴリズムオブジェクト識別子

自己署名証明書、デバイス ID 証明書、ネットワーク機器専用サーバ証明書および OCSP サーバ証明書については、Appendix B に定める。

7.1.4 名前の形式

自己署名証明書、デバイス ID 証明書、ネットワーク機器専用サーバ証明書および OCSP サーバ証明書については、Appendix B に定める。

7.1.5 名称の制約

規定しない。

7.1.6 証明書ポリシーオブジェクト識別子

本認証局が発行する証明書の証明書ポリシーオブジェクト識別子は下表のとおりとする。

証明書	証明書ポリシーオブジェクト識別子
デバイス ID 証明書	1.2.392.00200081.1.11.1
ネットワーク機器専用サーバ証明書	1.2.392.00200081.1.11.2

7.1.7 ポリシー制約拡張の使用

規定しない。

7.1.8 ポリシー修飾子の構文および意味

自己署名証明書、デバイス ID 証明書およびネットワーク機器専用サーバ証明書については、Appendix B に定める。

7.1.9 証明書ポリシー拡張についての処理方法

規定しない。

7.2 CRL のプロファイル

7.2.1 バージョン番号

本認証局が発行する CRL については、Appendix B に定める。

7.2.2 CRL、CRL エントリ拡張

本認証局が発行する CRL については、Appendix B に定める。

7.3 OCSP のプロファイル

7.3.1 バージョン番号

OCSP サーバ証明書については、Appendix B に定める。

7.3.2 OCSP 拡張

OCSP サーバ証明書については、Appendix B に定める。

8. 準拠性監査およびその他の評価

8.1 監査の頻度および要件

本認証局は、認証業務に疑義を生じた場合、発行局および登録局の全部または一部について、本 CPS「8.2 監査人の要件」で定める監査人による監査を実施することができる。

登録局はサイバートラストが行うかかる監査に協力しなければならない。

8.2 監査人の要件

本認証局の監査は、必要な知識と経験を有するものが行う。

8.3 監査人と被監査者の関係

監査人は、原則として本認証局の業務から独立し、中立性を保つ者とする。

8.4 監査の範囲

本認証局の認証業務が、本 CPS に準拠して実施されていることの監査を範囲とする。

8.5 指摘事項の対応

監査により発見された指摘事項は、認証局責任者へ報告される。

発行局またはネットワーク機器専用サーバ証明書登録局に対する是正措置が必要と判断された場合、発行局責任者の管理の下、是正措置を実施する。

デバイス ID 証明書登録局に対する是正措置が必要と判断された場合、本認証局デバイス ID サポートデスクは当該登録局に対し、当該是正措置の実施を求める通知を発送し、当該登録局はこれに対応しなければならない。

8.6 監査結果の開示

本認証局は、監査結果を加入者および信頼当事者には開示しない。

本認証局は、本認証局が認めた対象にのみ監査結果を開示する。

9. その他の業務上および法的な事項

9.1 料金

サイバートラストと加入者管理組織との間で締結されるサイバートラスト デバイス ID 利用約款に従うものとする。

9.2 財務的責任

サイバートラストは、本 CPS に定める内容を遵守のうえ本認証局を運営するために、十分な財務的基盤を維持するものとする。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

本認証局は、発行局、登録局およびデバイス ID サポートデスクが保有する情報のうち以下の情報を機密として取り扱う（以下、「機密情報」という。）。

① 加入者管理組織からの依頼情報

② 本 CPS「9.4.2 個人情報として扱われる情報」に定める情報

③ 本認証局のセキュリティに関する情報

9.3.2 機密情報の範囲外の情報

本認証局は、発行局、登録局およびデバイス ID サポートデスクが保有する情報のうち、以下の情報については機密情報の範囲外とする。

① 本 CPS「2.2 公開する情報」において公開するものとして定める情報

② 発行された証明書

③ 本認証局の過失によらず公知となった情報

④ 本認証局以外のものから機密保持の制限なしに開示され公知となった情報

⑤ 加入者管理組織から事前に開示または第三者への提供の承諾を得た情報

なお、上記によらず、加入者管理組織自らが管理するデバイス ID 証明書の加入者および信頼当事者の情報については、加入者管理組織が、その自己の責任において管理し、かつ取り扱うものとし、本認証局はその管理責任を負わず、機密情報としては取り扱わない。

9.3.3 機密情報の保護責任

本認証局は、機密情報の漏洩を防止する対策を実施する。また、本認証局の運営の用に供する以外には使用しない。ただし、機密情報に関して、裁判上、行政上その他の法的手続きの過程において機密情報の開示要求があった場合、買収、合併等に関連して財務アドバイザー、潜在的買収・合併当事者等サイバートラストとの間で守秘義務契約を締結した者および／または弁護士、公認会計士、税理士等の法により守秘義務を負う者に開示する場合、または加入者から事前の承諾を得た場合、サイバートラストは、当該機密情報を開示要求者に対して開示することができるものとする。この場合、開示を受ける当該開示要求者は当該当該情報をいかなる方法によっても第三者に開示し、または漏洩させてはならない。

なお、個人情報の保護の取扱いは、本 CPS「9.4 個人情報の保護」に定める。

9.4 個人情報の保護

9.4.1 プライバシー・ポリシー

本認証局は、発行局、登録局およびデバイス ID サポートデスクが保有する情報のうち、9.4.2「個人情報として扱われる情報」に該当する情報については、本 CPS に定める事項以外の事項に関しては個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）に基づいて取り扱う。

なお、サイバートラストは、本認証局の業務のうちサイバートラストが担当する業務については、サイバートラストが管理する Web サイト（https://www.cybertrust.ne.jp/corporate/privacy_policy.html）で公開するプライバシー・ポリシーも遵守する。

9.4.2 個人情報として扱われる情報

本認証局は、デバイス ID 証明書登録局から発行局へのデバイス ID 証明書の発行または失効の指示等に含まれる、生存する個人の情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。) を個人情報として扱う。

9.4.3 個人情報とみなされない情報

本認証局は、本 CPS「9.4.2 個人情報として扱われる情報」に定める情報以外は、個人情報とみなさない。

9.4.4 個人情報の保護責任

本認証局が保有する個人情報の保護責任は、本 CPS「9.4.1 プライバシー・ポリシー」に定めるとおりとする。

9.4.5 個人情報の使用に関する個人への通知および承認

本認証局は、本サービスの利用申請の受理をもって、本認証局が本 CPS で予定している証明書発行・失効業務の履行、本認証局の監査の実施、その他本サービスの提供に必要となる業務のために個人情報を使用することについて、当該申請を行った組織より承諾を得たものとみなす。なお、本認証局は、当該個人情報について、本サービスの提供および認証業務の実施以外の目的で使用しない。ただし、本 CPS「9.4.6 司法手続または行政手続に基づく公開」に定める場合を除くものとする。

9.4.6 司法手続または行政手続に基づく公開

本認証局で取扱う個人情報に関して、法令の定めに基づき裁判上、行政上その他の法的手続きの過程において情報の開示要求があった場合、本認証局は、当該個人情報を開示することができるものとする。

9.4.7 他の情報公開の場合

本認証局は、業務の一部を外部に委託する場合、機密情報を委託先に対して開示することがある。この場合、当該委託に関する契約において、当該委託先に対して機密情報の守秘義務および個人情報保護義務を課す規定を置くものとする。

9.5 知的財産権

特段の合意がなされない限り、以下の情報に関するすべての知的財産権は、サイバートラストまたは本認証局のサービスに関するサイバートラストの仕入先またはライセンサーに帰属するものとする。

① 本認証局が発行した証明書、証明書の失効情報
② 本 CPS および関連文書
③ 本認証局の公開鍵および秘密鍵
④ 本認証局から貸与されたソフトウェア、ハードウェア

9.6 表明保証

以下に発行局、登録局、加入者管理組織、加入者および信頼当事者の表明保証を規定する。なお、本 CPS「9.6 表明保証」で明示的に規定された発行局、登録局、加入者管理組織、加入者および信頼当事者の表明保証を除き、各当事者はいかなる明示的または黙示的な表明保証をも行わないことを相互に確認する。

9.6.1 発行局の表明保証

サイバートラストは、本認証局を構成する発行局として発行局の業務の遂行にあたり、以下の義務を負うことを表明し保証する。

① 認証局秘密鍵の安全な管理を行うこと
② 登録局からの指示に基づき正確に証明書の発行および失効を行うこと
③ CRL の発行および公開、ならびに OCSP サーバをもって失効情報の提供を行うこと
④ システムの監視および運用を行うこと
⑤ リポジトリの維持・管理を行うこと

9.6.2 登録局の表明保証

デバイス ID 証明書登録局を運営する加入者管理組織ならびに、ネットワーク機器専用サーバ証明書登録局を運営するサイバートラストは、本認証局を構成する登録局として、登録局の業務の遂行にあたり、以下の義務を負うことを表明し保証するものとする。

① 本 CPS および関連諸規程を遵守すること
② 発行局への証明書発行および失効の正確な指示を行うこと
③ 証明書の発行を加入者に正しく通知し、または発行された証明書を正しく配付すること

④ 本項に規定された登録局の義務、債務の不履行により発生した事態に対し、責任を負うこと

9.6.3 加入者管理組織の表明保証

加入者管理組織は、以下の義務を負うことを表明し保証する。

① 本 CPS および関連諸規程を遵守すること

② 自らが管理する加入者および信頼当事者をして、本 CPS および関連諸規程を遵守させること

③ 登録局を運営すること

④ 証明書の発行または失効の正確な依頼を登録局に対して行うこと

⑤ 本項に規定された加入者管理組織の義務の不履行により発生した事態に対し、責任を負うこと

⑥ 本 CPS「4.9.1.3 加入者管理組織による失効事由」を遵守すること

9.6.4 加入者の表明保証

加入者は、以下の義務を負うことを表明し保証する。

① 本 CPS および関連諸規程を遵守すること

② 証明書用途（本 CPS「1.4.2 適切な証明書の用途」）を遵守すること

③ 加入者管理組織が認めるデバイスおよび自らが利用または管理するネットワーク機器・サービスにのみ証明書を導入すること

④ 証明書をデバイスもしくはネットワーク機器・サービスに導入する際に、証明書に含まれる情報が正当であることを確認すること

⑤ 秘密鍵およびパスワードの機密性ならびに完全性を確保するための厳重な管理を行うこと

⑥ 本 CPS「4.9.1.3 加入者による失効事由」を遵守すること

⑦ 有効期間が満了した証明書および失効された証明書を使用しないこと

9.6.5 信頼当事者の表明保証

信頼当事者は、以下の義務を負うことを表明し保証する。

① 加入者管理組織の指示または定めに従い、正しく認められたデバイスもしくはネットワーク機器において証明書を検証し信頼する設定を行うほか、本 CPS および関連諸規程を遵守すること

② 証明書が本 CPS「1.4.2 適切な証明書の用途」に定める用途で利用されていることの確認を行うこと

③ 本認証局が発行した証明書の有効期間と記載項目の確認を行うこと

④ 証明書に行われた電子署名の検証と発行者の確認を行うこと

⑤ CRL または OCSP による失効登録の有無の確認を行うこと

⑥ 本項に規定された義務の不履行により発生した事態に対し、責任を負うこと

9.6.6 他の関係者の表明保証

本認証局 デバイス ID サポートデスクは、以下の義務を負うことを表明し、保証する。

① 本 CPS および関連諸規程を遵守すること

② 問合せの受付（本 CPS「1.5.2 連絡窓口」）を行うこと

③ デバイス ID 証明書登録局の登録･抹消を行うこと

④ デバイス ID 証明書登録局オペレータ責任者および登録局オペレータの登録等を管理すること

⑤ デバイス ID 証明書登録局または加入者管理組織に対し是正の必要を認めた場合、通知を行うこと

⑥ ネットワーク機器専用サーバ証明書登録局における窓口業務を行うこと

⑦ 本認証局の秘密鍵が危殆化した場合、当該事実について加入者管理組織に通知し、また本認証局のリポジトリに公開すること

9.7 不保証

本認証局は、本 CPS「9.6.1 発行局の表明保証」、本 CPS「9.6.2 登録局の表明保証」および「9.6.5 他の関係者の表明保証」に定める保証に関連して発生する直接損害以外の損害については、本 CPS に基づく債務不履行に関していかなる責任も負わない。

また、当該保証に関連して直接損害が発生した場合でも、当該損害は、サイバートラストと加入者管理組織との間で締結されるサイバートラスト デバイス ID 利用約款に従い処理されることとし、本認証局は、加入者および信頼当事者に対していかなる責任も負わない。

9.8 責任の制限

本認証局は、本 CPS「9.6.1 発行局の表明保証」、本 CPS「9.6.2 登録局の表明保証」および「9.6.5 他の関係者の表明保証」の内容に関し、以下の場合に一切の責任を負わないものとする。

① 発行局、登録局および本認証局デバイス ID サポートデスクが、本 CPS および法規制を遵守したにも関わらず発生するいかなる損害

② 本認証局に起因しない、不法行為、不正使用または過失等により発生するいかなる損害

③ 加入者管理組織が、本 CPS「9.6 表明保証」の規定に基づき負う義務の履行を怠ったために生じた損害

④ 加入者または信頼当事者が、本 CPS「9.6 表明保証」の規定に基づきそれぞれが負う義務の履行を怠ったために生じた損害

⑤ 本認証局が発行した証明書に関わる鍵ペアが本認証局以外の第三者の行為により漏洩、または解読等され、生じた損害

⑥ 証明書が加入者管理組織、加入者、信頼当事者または第三者の著作権、営業秘密またはその他の知的財産権を侵害したことによって生じる損害

⑦ 暗号アルゴリズム解読技術の向上等、技術の進歩に伴う暗号強度の弱体化、その他の脆弱性等に起因する損害

本認証局が加入者管理組織に対して負担する賠償額については、サイバートラストと加入者管理組織との間で締結されるサイバートラスト デバイス ID 利用約款に従うものとする。
なお、本 CPS「9.14 準拠法」に定める準拠法により認められる範囲において、本 CPS および関連諸規程に基づく債務不履行、違反について生じる損害のうち、データ消失、得べかりし利益を含む間接損害、派生的損害、懲罰的損害に対し、本認証局は責任を負わない。

9.9 補償

加入者管理組織は、当該組織が管理する加入者または信頼当事者が、故意または過失によらず為した以下に掲げるいずれかの行為に起因して生じた本認証局に対する第三者からの請求、訴訟の提起その他の法的措置に対し、本認証局が被った損害を賠償し、かつ本認証局に損害を生じることがないようにする責任が生じるものとする。

① 証明書の不正使用、改ざん、利用時の不実の表明

② 本 CPS または関連諸規程への違反

③ 加入者による秘密鍵の保全の怠慢

また、本認証局は、加入者管理組織、加入者または信頼当事者の代理人、受託者、またはその他代表者ではない。

9.10 文書の有効期間と終了

9.10.1 文書の有効期間

本 CPS は、認証局責任者が承認することにより有効となる。また、本 CPS「9.10.2 終了」に定める時点の前に本 CPS が無効となることはない。

9.10.2 終了

本 CPS は、本 CPS「9.10.3 終了の影響と存続条項」に定める規定を除き、本認証局が業務を終了した時点で無効となる。

9.10.3 終了の影響と存続条項

本 CPS 9.3、9.4、9.5、9.6、9.7、9.8、9.9、9.10.2、9.10.3、9.13、9.14、9.15、9.16の規定については本 CPS の終了後も、存続するものとする。

9.11 関係者間の個別通知と連絡

本認証局から加入者に対し、発行通知等、個別の通知を行う場合は、電子メールを送信したときをもって通知がなされたものとみなす。
加入者からの通知については、当該加入者に対して証明書の発行を指示した登録局が、その通知を受け付けるものとし、本認証局およびデバイス ID サポートデスクは、特に明示した場合を除き、デバイス ID 証明書およびネットワーク機器専用サーバ証明書の加入者からの直接の通知を受け付けないこととする。
なお、本サービスの利用申請･解除等に関する通知については、サイバートラストと加入者管理組織との間で締結されるサイバートラスト デバイス ID 利用約款に従うこととし、本 CPS では規定しない。

9.12 改訂

9.12.1 改訂手続き

本認証局は、認証局責任者の指示に基づき、適宜、本 CPS の改訂を行うことができる。認証局員の評価、または弁護士等外部の専門家または有識者の評価を得た後、認証局責任者が改訂の承認を行う。

9.12.2 通知方法と期間

本認証局は、本 CPS の改訂を認証局責任者が承認した後、改訂後および改訂前の CPS を一定期間 Web サイトに公開し、各当事者がその変更内容について確認できる措置を講ずる。本認証局から当該改訂の撤回の通知が公表されない限り、当該改訂は認証局責任者が別途定める時点をもって発効するものとする。発効後 15 日以内に、加入者管理組織が登録局をして証明書の失効を指示しない場合、有効な証明書に関わる各当事者は改訂後の本 CPS につき同意したものとみなされる。

9.12.3 オブジェクト識別子の変更

規定しない。

9.13 紛争解決手続き

本 CPS または本認証局が発行する証明書に関連して生じたすべての訴訟については、東京地方裁判所を第一審の専属的合意管轄裁判所とする。また、本 CPS に定めのない事項または本 CPS に疑義が生じた場合は、当事者が誠意をもって協議するものとする。

9.14 準拠法

本 CPS の解釈およびに本 CPS に基づく認証業務にかかわる紛争については、日本国の法律が適用される。

9.15 適用法の遵守

規定しない。

9.16 雑則

9.16.1 完全合意条項

本 CPS における合意事項は、特段の定めをしている場合を除き、本 CPS が改訂または終了されない限り、他のすべての合意事項より優先される。

9.16.2 権利譲渡条項

本認証局は、登録局業務について、第三者への譲渡を認めない。
なお、サイバートラストによる本サービスの第三者への譲渡については、サイバートラストと加入者管理組織との間で締結されるサイバートラスト デバイス ID 利用約款に従うこととする。

9.16.3 分離条項

本 CPS の一部の条項が、何らかの事由により無効となった場合においても、その他の条項は有効であるものとする。

9.16.4 強制執行条項

規定しない。

9.16.5 不可抗力条項

天災地変、裁判所の命令、労働争議、その他本認証局の責に帰さない事由により、本 CPS 上の義務の履行が一部または全部を遅延した場合には、本認証局は当該遅延期間について本 CPS 上の義務の履行を免れ、加入者または証明書の全部または一部を信頼し、または利用した第三者に対し、何らの責任をも負担しない。

Appendix A:用語の定義

用語	定義
アーカイブ	本書でのアーカイブとは、使用期限が過ぎたものを所定の期間保管することをいう。
暗号モジュール	秘密鍵の生成、保管、使用等において、セキュリティを確保する目的で使用されるソフトウェア、ハードウェア、またはそれらを組み合わせた装置である。
一時停止	証明書の有効期間中、証明書の有効性を一時的に無効とする措置である。
鍵ペア	公開鍵暗号方式における公開鍵および秘密鍵である。2 つの鍵は、一方の鍵から他方の鍵を導き出せない性質を持つ。
鍵長	鍵の長さをビット数で表したもので、暗号強度を決定する一要素である。
活性化	システムや装置等を使用可能な状態にすることである。活性化には活性化データを必要とし、具体的には PIN やパスフレーズ等が含まれる。
危殆化	秘密鍵および秘密鍵に付帯する情報の機密性または完全性が失われる状態である。
公開鍵	公開鍵暗号方式における鍵ペアの 1 つで、通信相手等の他人に知らせて使用される鍵である。
構成プロファイル	iPhone, iPad 等 iOS を搭載するデバイス用の XML ファイルで、当該デバイスに係わるデバイス・セキュリティ・ポリシー、VPN 構成情報、Wi-Fi 設定、APN 設定、Exchange アカウント設定、メール設定、およびデバイス ID 証明書等の証明書が含まれる。
コモンネーム	Common Name (CN)。Distinguished Name における Attribute Type。個体名を表す。本認証局が発行するデバイス ID 証明書では、デバイスの識別情報（MAC アドレス等）が記載される。
サイバートラスト デバイス ID 利用約款	本サービスの利用に際し、加入者管理組織とサイバートラストとの間で締結される契約である。本 CPS は、利用約款の一部を構成する。
失効	証明書が有効期間中であっても、証明書を無効とする措置である。
自己署名証明書	Self-signed Certificate。認証局が、自身を証明するために発行する証明書。証明書に記載される証明書発行者と被発行者とが同一になっている。
証明書	X.509 公開鍵証明書をいう。本 CPS では特段の指定がない限り、デバイス ID 証明書およびネットワーク機器専用サーバ証明書を総称して指す。
証明書失効リスト	英語では Certificate Revocation List であり、本 CPS では CRL という。CRL は、失効された証明書のリストである。本認証局は、加入者

	および信頼当事者が証明書の有効性を確認するために、CRL を公開する。
組織単位名	Organization Unit Name (OU)。Distinguished Name における Attribute Type。一般に部署名を表し、複数指定が可能である。本認証局が発行するデバイス ID 証明書では、OU の1つに、加入者管理組織を一意に区分する名称が記載される。また、他に最大2つまで OU を指定可能であり、部署名等が記載される場合がある。
組織名	Organization Name (O)。Distinguished Name における Attribute Type。一般に組織名を表す。本認証局が発行するデバイス ID 証明書では、加入者管理組織を一意に区分する名称が記載される。
デバイス	PC,スマートフォン、業務専用端末等のネットワーク上の機器ないし端末をいう。
電子署名	間違いなく本人であることを証明する電子的なデータ。本 CPS では、デジタル署名(digital signature)の意味で用いる。具体的には、署名対象データのハッシュ値に対して、秘密鍵で暗号化したものをいう。電子署名の検証は、電子署名を公開鍵で復号化した値と元のデータのハッシュ値とを照合することで可能となる。
認証業務	証明書のライフサイクル管理を行う上での一連の業務をいう。発行・失効の申請受付業務、審査業務、発行・失効・棄却業務、問合対応業務、請求業務、本認証局システムの維持管理業務を含むが、これらに限定されない。
秘密鍵	公開鍵暗号方式における鍵ペアの 1 つで、他人には知られないように秘密にしておく鍵である。
ポリシー	認証局を運用していく際の方針、もしくは、証明書がどのように使用されるかの指針を指す言葉として用いられる。前者は認証局運用規定「CPS」として、後者は証明書ポリシー「CP」として規定されるが、特に CP を区分せず、包含した形で CPS が策定される場合もある。本 CPS は CP を包含している。
預託	本 CPS での預託とは、秘密鍵または公開鍵を第三者に登録保管することである。
リポジトリ	本 CPS や CRL 等、公開情報を掲載する Web サイトやシステムである。
CP	Certificate Policy。証明書ポリシー。証明書の利用目的、適用範囲等の指針を定めた文書をいう。
CPS	Certification Practice Statement。認証局運用規程。認証局の責任や義務、運用方針や運用手順等を規定した文書をいう。
CRL	Certificate Revocation List。証明書失効リストを参照。
Distinguished Name	ITU-T が策定した X.500 勧告において定められた識別名である。コモンネーム、組織名、組織単位名、国名等の属性情報で構成される。

FIPS 140 レベル 4	FIPS（Federal Information Processing Standards Publication 140)は、暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格。同規格では、セキュリティ要件によりレベルを 1（最低）～4（最高）に分類している。
IETF PKIX ワーキンググループ	Internet Engineering Task Force（IETF）は、インターネットで利用される技術を標準化する組織であり、同組織の PKIX ワーキンググループが RFC3647 を定めた。
ITU-T	国際電気通信連合の電気通信標準化部門である。
OCSP	OCSP Online Certificate Status Protocol の略であり、証明書の失効情報をするための通信プロトコルである。本認証局では、信頼当事者が証明書の有効性を確認するために、CRL の公開に加え OCSP サーバを運用する。
ネットワーク機器	ネットワーク機器またはサーバ機器等のネットワーク上の機器で、特に、デバイス ID 証明書の利用において、iPhone や Windows OS 標準搭載のサプリカントと組み合わせて利用する場合の機器を指す。
MAC アドレス	各Ethernetネットワーク･インタフェースに固有のID番号。物理的なインタフェース毎に全世界で一意に割り当てられており、これを元にカード間のデータの送受信が行われる。一意性を利用して、デバイスを特定することに用いることができる。
PKI	Public Key Infrastructure。公開鍵暗号を用いたアーキテクチャー･運用･手続き等を包括的に指す。
RSA	Rivest、Shamir、Adelman の 3 人が開発した公開鍵暗号方式である。
SHA1/SHA2	電子署名等に使用されるハッシュ関数である。ハッシュ関数は、データを数学的な操作により一定の長さに縮小させるものであり、異なる 2 つの入力値から同じ出力値を算出することを困難とする特性を持つ。また、出力値から入力値を逆算することは不可能である。
X.500	ITU-T により規格化されたネットワーク上での分散ディレクトリサービスの国際標準である。
X.509	ITU-T により規格化された証明書の国際標準である。

Appendix B:証明書等のプロファイル

自己署名証明書

(標準領域)

Version		値
Version	証明書フォーマットのバージョン番号 型:INTEGER 値:2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	証明書のシリアル番号 型:INTEGER 値:ユニークな整数	 *シリアル番号
Signature		**値**
AlgorithmIdentifier	証明書への署名に使用された署名アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)	
Algorithm	署名アルゴリズムのオブジェクト ID 型:OID 値:右記いずれかの値	 CA G1: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2k: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	署名アルゴリズムの引数 型:NULL 値:	 NULL
Issuer		**値**
CountryName	証明書発行者の国名	
Type	国名のオブジェクト ID 型:OID 値:2 5 4 6	 2.5.4.6
Value	国名の値 型:PrintableString 値:JP	 JP
OrganizationName	証明書発行者の組織名	
Type	組織名のオブジェクト ID 型:OID 値:2 5 4 10	 2.5.4.10
Value	組織名の値 型:PrintableString 値:Cybertrust Japan Co.,Ltd.	 Cybertrust Japan Co.,Ltd.
CommonName	証明書発行者の固有名称	
Type	固有名称のオブジェクト ID 型:OID 値:2 5 4 3	 2.5.4.3
Value	固有名称の値 型:PrintableString 値:右記のいずれかの認証局名	 Cybertrust DeviceiD Public CA G1 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k

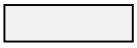
		Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G3k
Validity		**値**
Validity	証明書の有効期間	認証局により以下の値をとる CA G1: 10 年+1 ヶ月 CA G2: 15 年+1 ヶ月 CA G2s: 15 年+1 ヶ月 CA G2k: 15 年+1 ヶ月 CA G2is: 15 年+1 ヶ月 CA G2sp: 15 年+1 ヶ月 CA G3k: 15 年+1 ヶ月
notBefore	開始日時 型：UTCTime or GeneralizedTime 値：年（2 桁 or4 桁）月日時分秒 Z	認証局により以下の値をとる CA G1: 090623072354Z CA G2: 131016025113Z CA G2s: 131016110203Z CA G2k: 131017021450Z CA G2is: 140320051900Z CA G2sp: 141205021856Z CA G3k: 150420054150Z
notAfter	終了日時 型：UTCTime or GeneralizedTime 値：年（2 桁 or4 桁）月日時分秒 Z	認証局により以下の値をとる CA G1: 190723072354Z CA G2: 281116025113Z CA G2s: 281116110203Z CA G2k: 281117021450Z CA G2is: 290420051900Z CA G2sp: 300105021856Z CA G3k: 300520054150Z
Subject		**値**
CountryName	証明書発行者の国名	
Type	国名のオブジェクト ID 型：OID 値：2 5 4 6	2.5.4.6
Value	国名の値 型：PrintableString 値：JP	JP *固定
OrganizationName	証明書発行者の組織名	
Type	組織名のオブジェクト ID 型：OID 値：2 5 4 10	2.5.4.10
Value	組織名の値 型：PrintableString 値：Cybertrust Japan Co.,Ltd.	Cybertrust Japan Co.,Ltd.
CommonName	証明書発行者の固有名称	
Type	固有名称のオブジェクト ID 型：OID 値：2 5 4 3	2.5.4.3
Value	固有名称の値 型：PrintableString 値：右記のいずれかの認証局名。但し、Issuer 名と同一値	Cybertrust DeviceiD Public CA G1 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G3k
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子認証書発行者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY) 型：OID 値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
Parameters	署名アルゴリズムの引数	

subjectPublicKey	型：NULL 値： 公開鍵値 型：BIT STRING 値：公開鍵値	NULL ＊2048bit 長の公開鍵

(拡張領域)

basicConstraints (extnId :== 2 5 29 19, critical :== TRUE)		**値**
BasicConstraints cA	基本的制限 CA かどうかを示すフラグ 型：Boolean 値：True（CA である）	 TRUE
subjectKeyIdentifier (extnId :== 2 5 29 14, critical :== FALSE)		**値**
SubjectKeyIdentifier keyIdentifier	証明書発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値：発行者の subjectPublicKey の Hash 値	 認証局により以下の値をとる CA G1: 89:3C:E3:F0:D7:ED:87:47:25:CF: 89:F9:C5:99:4E:6A:F2:3F:73:94 CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC
keyUsage （extnId :== 2 5 29 15, critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BIT STRING 値：00000110 (CertificateSigning,CRLSigning)	 00000110

デバイス ID 証明書



網掛け部分は加入者管理組織の申請により設定できる箇所

（標準領域）

Version		**値**
Version	証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier Algorithm	証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：右記いずれかの値	 CA G1: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2k: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	署名アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**値**
CountryName Type Value	証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP	 2.5.4.6 JP
OrganizationName Type Value	証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10 組織名の値 型：PrintableString 値：Cybertrust Japan Co.,Ltd.	 2.5.4.10 Cybertrust Japan Co.,Ltd.
CommonName Type Value	証明書発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3 固有名称の値 型：PrintableString 値：デバイス ID 証明書を発行する右記のいずれかの認証局名	 2.5.4.3 Cybertrust DeviceiD Public CA G1 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp

		Cybertrust DeviceiD Public CA G3k
Validity		**値**
Validity	証明書の有効期間	（5 年＋猶予期間（1 ヵ月））以内
notBefore	開始日時	
	型：UTCTime or GeneralizedTime	＊有効開始日時
	値：年（2 桁 or4 桁）月日時分秒 Z	例 0904010000000Z
notAfter	終了日時	
	型：UTCTime or GeneralizedTime	＊有効終了日時
	値：年（2 桁 or4 桁）月日時分秒 Z	例 1405010000000Z
Subject		**値**
CountryName	証明書被発行者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP　*固定
OrganizationName	証明書被発行者の組織名	
Type	組織名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString or UTF8String	＊文字値により変更される
	値：<<お客様会社名称＋会社識別子>>	＊会社識別子は、本認証局デバイス ID サポートデスクによる採番となる
OrganizationalUnitName(1)	証明書被発行者の部署名	
Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString or UTF8String	＊文字値により変更される
	値：RA operated by <<お客様会社名称＋会社識別子>>	会社識別子は、本認証局デバイス ID サポートデスクによる採番となる
OrganizationalUnitName(2, 3)	証明書被発行者の部署名	＊必要な場合のみ（最大 2 つまで）
Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString or UTF8String	＊文字値により変更される
	値：<<部署名等>>	
CommonName	証明書被発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString or UTF8String	＊文字値により変更される
	値：<<デバイスの識別情報>>	MAC アドレス等
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	証明書被発行者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL
	値：	
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	＊鍵長は、2048bit（但し、1024bit が許容される場合あり）

(拡張領域)

authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**値**
AuthorityKeyIdentifier keyIdentifier	証明書発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値：認証局の subjectPublicKey の Hash 値	認証局により以下の値をとる CA G1: 89:3C:E3:F0:D7:ED:87:47:25:CF: 89:F9:C5:99:4E:6A:F2:3F:73:94 CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC
authorityCertIssuer	発行者名 型：GeneralNames 値：認証局の subject の値	認証局により以下の値をとる CA G1: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Public CA G1 CA G2: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Public CA G2 CA G2s: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Public CA G2s CA G2k: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Public CA G2k CA G2is: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Public CA G2is CA G2sp: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Public CA G2sp CA G3k: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Public CA G3k
authorityCertSerialNumber	発行者証明書シリアル番号 型：INTEGER 値：認証局証明書の serialNumber 値	＊発行者証明書のシリアル番号（認証局により異なる）
subjectKeyIdentifier (extnId :== 2 5 29 14, critical :== FALSE)		**値**
SubjectKeyIdentifier keyIdentifier	証明書被発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値：被発行者の subjectPublicKey の Hash 値	＊被発行者の subjectPublicKey の Hash 値
keyUsage （extnId :== 2 5 29 15, critical :== FALSE）		**値**
KeyUsage	鍵の使用目的 型：BIT STRING 値：101000000 (digitalSignature,keyEncipherment)	101000000
cRLDistributionPoints (extnId :== 2 5 29 31, critical :== FALSE)		**値**
cRLDistributionPoints	CRL 配付ポイント	

DistributionPoint fullName	CRL 配付ポイント CRL を配付する URI 型：OCTET STRING 値：http URI	 認証局により以下の値をとる CA G1: http://mpkicrl.managedpki.ne.jp/mpki/CybertrustDeviceiDPublicCAG1/cdp.crl CA G2: http://crl.deviceid.ne.jp/deviceid/g2.crl CA G2s: http://crl.deviceid.ne.jp/deviceid/g2s.crl CA G2k: http://crl.deviceid.ne.jp/deviceid/g2k.crl CA G2is: http://crl.deviceid.ne.jp/deviceid/g2is.crl CA G2sp: http://crl.deviceid.ne.jp/deviceid/g2sp.crl CA G3k: http://crl.deviceid.ne.jp/deviceid/g3k.crl
subjectAltName (extnId :== 2 5 29 17，critical :== FALSE)		**値**
subjectAltName dNSName	証明書被発行者の別名 フルコンピュータ名 型：IA5String 値：フルコンピュータ名	（ActiveDirectory を利用する場合のオプション） ＊フルコンピュータ名
extKeyUsage (extnId :== 2 5 29 37，critical :== FALSE)		**値**
extKeyUsage KeyPurposeId clientAuth	鍵の使用目的（拡張） 使用目的 ID クライアント認証利用 型：OID 値：1 3 6 1 5 5 7 3 2	 1.3.6.1.5.5.7.3.2 (clientAuth)
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1，critical :== FALSE)		**値**
Authority Information Access Access Method Alternative Name	認証局情報アクセス アクセス法 型：OID 値：1 3 6 1 5 5 7 48 1 別名	＊下記認証局に限る：CA G3k 1.3.6.1.5.5.7.48.1 (OCSP)
	型：OCTET STRING 値：OCSP の URL	 http://ocsp.deviceid.ne.jp/deviceid

ネットワーク機器専用サーバ証明書

(標準領域)

Version		値
Version	証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier Algorithm	証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：右記いずれかの値	 CA G1: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	署名アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**値**
CountryName Type Value	証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP	 2.5.4.6 JP
OrganizationName Type Value	証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10 組織名の値 型：PrintableString 値：Cybertrust Japan Co.,Ltd.	 2.5.4.10 Cybertrust Japan Co.,Ltd.
CommonName Type Value	証明書発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3 固有名称の値 型：PrintableString 値：ネットワーク機器専用サーバ証明書を発行する右記のいずれかの認証局名	 2.5.4.3 Cybertrust DeviceiD Public CA G1 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G3k
Validity		**値**
Validity notBefore notAfter	証明書の有効期間 開始日時 型：UTCTime or GeneralizedTime 値：年（2 桁 or4 桁）月日時分秒 Z 終了日時	（5 年＋猶予期間（2 ヵ月））以内 ＊有効開始日時 例 090401000000Z

	型：UTCTime or GeneralizedTime 値：年（2 桁 or4 桁）月日時分秒 Z	＊有効終了日時 例 140601000000Z
Subject		**値**
CountryName Type Value StateOrProvinceName Type Value LocalityName Type Value OrganizationName Type Value OrganizationalUnitName(1,2) Type Value CommonName Type Value 	証明書被発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 証明書被発行者の都道府県名 都道府県名のオブジェクト ID 型：OID 値：2 5 4 8 都道府県名の値 型：PrintableString 値：<<都道府県名 >> 証明書被発行者の市町村名 市町村名のオブジェクト ID 型：OID 値：2 5 4 7 市町村名の値 型：PrintableString 値：<<市町村名>> 証明書被発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10 組織名の値 型：PrintableString or UTF8String 値：<<お客様会社名称＋会社識別子 >> 証明書被発行者の部署名 部署名のオブジェクト ID 型：OID 値：2 5 4 11 部署名の値 型：PrintableString or UTF8String 値：<<部署名等>> 証明書被発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3 固有名称の値 型：PrintableString 値：<<固有名称>>	 2.5.4.6 JP　*固定 ＊必要な場合のみ 2.5.4.8 ＊必要な場合のみ 2.5.4.7 2.5.4.10 ＊文字値により変更される ＊会社識別子は、本認証局デバイス ID サポートデスクによる採番となる ＊必要な場合のみ（最大 2 つまで） 2.5.4.11 ＊文字値により変更される ネットワーク機器の FQDN 2.5.4.3 ネットワーク機器の FQDN
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo AlgorithmIdentifier Algorithm parameters subjectPublicKey 	証明書被発行者の公開鍵情報 暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数） 暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY) 型：OID 値：1 2 840 113549 1 1 1 署名アルゴリズムの引数 型：NULL 値： 公開鍵値 型：BIT STRING 値：公開鍵値	 1.2.840.113549.1.1.1 NULL ＊鍵長は、1024bit 以上

(拡張領域)

authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**値**
AuthorityKeyIdentifier	証明書発行者の公開鍵に関する情報	

keyIdentifier	公開鍵の識別子 型：OCTET STRING 値：認証局の subjectPublicKey の Hash 値	認証局により以下の値をとる CA G1: 89:3C:E3:F0:D7:ED:87:47:25:CF: 89:F9:C5:99:4E:6A:F2:3F:73:94 CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC
subjectKeyIdentifier (extnId :== 2 5 29 14，critical :== FALSE)		**値**
SubjectKeyIdentifier keyIdentifier	証明書被発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値：被発行者の subjectPublicKey の Hash 値	＊被発行者の subjectPublicKey の Hash 値
keyUsage （extnId :== 2 5 29 15，critical :== FALSE）		**値**
KeyUsage	鍵の使用目的 型：BIT STRING 値：101000000 (digitalSignature,keyEncipherment)	101000000
cRLDistributionPoints (extnId :== 2 5 29 31，critical :== FALSE)		**値**
cRLDistributionPoints DistributionPoint fullName	CRL 配付ポイント CRL 配付ポイント CRL を配付する URI 型：OCTET STRING 値：http URI	認証局により以下の値をとる CA G1: http://mpkicrl.managedpki.ne.jp/ mpki/CybertrustDeviceiDPublicCAG1/c dp.crl CA G2: http://crl.deviceid.ne.jp/deviceid/g2.crl CA G2s: http://crl.deviceid.ne.jp/deviceid/g2s.crl CA G2k: http://crl.deviceid.ne.jp/deviceid/g2k.crl CA G2is: http://crl.deviceid.ne.jp/deviceid/g2is.crl CA G2sp: http://crl.deviceid.ne.jp/deviceid/g2sp.crl CA G3k: http://crl.deviceid.ne.jp/deviceid/g3k.crl
subjectAltName (extnId :== 2 5 29 17，critical :== FALSE)		**値**
subjectAltName dNSName	証明書被発行者の別名 フルコンピュータ名 型：IA5String 値：フルコンピュータ名	（ActiveDirectory を利用する場合のオプション） ＊フルコンピュータ名

OCSP サーバ証明書

(標準領域)

Version		値
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
Serialnumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号（ユニークな整数）
Signature		**値**
AlgorithmIdentifier algorithm	電子証明書への署名に使用された暗号アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 暗号アルゴリズムのオブジェクト ID 型：OID 値：右記いずれかの値	 CA G1: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2k: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA)
parameters	暗号アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**値**
CountryName Type	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6	 2.5.4.6
Value	国名の値 型：PrintableString 値：JP	 JP
OrganizationName Type	電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10	 2.5.4.10
Value	組織名の値 型：PrintableString 値：Cybertrust Japan Co., Ltd.	 Cybertrust Japan Co., Ltd.
CommonName Type	電子証明書発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3	 2.5.4.3
Value	固有名称の値 型：PrintableString 値：OCSP サーバ証明書を発行する右記のいずれかの認証局名	 Cybertrust DeviceiD Public CA G1 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G3k
Validity		**値**
Validity	電子証明書の有効期間	

notBefore	開始日時 型：UTCTime 値：yymmddhhmmssZ	＊有効開始日時
notAfter	終了日時 型：UTCTime 値：yymmddhhmmssZ	＊有効終了日時
Subject		**値**
CountryName	電子証明書所有者の国名	
type	国名のオブジェクト ID 型：OID 値：2 5 4 6	2.5.4.6
value	国名の値 型：PrintableString 値：JP	JP
OrganizationName	電子証明書所有者の組織名	
type	組織名のオブジェクト ID 型：OID 値：2 5 4 10	2.5.4.10
value	組織名の値 型：PrintableString 値：Cybertrust Japan Co., Ltd.	Cybertrust Japan Co., Ltd.
CommonName	電子証明書所有者の固有名称	
type	固有名称のオブジェクト ID 型：OID 値：2 5 4 3	2.5.4.3
value	固有名称の値 型：PrintableString 値：OCSP サーバを識別する右記いずれかのサーバ名	Cybertrust DeviceiD Public CA G1 OCSP Responder Cybertrust DeviceiD Public CA G2 OCSP Responder Cybertrust DeviceiD Public CA G2s OCSP Responder Cybertrust DeviceiD Public CA G2k OCSP Responder Cybertrust DeviceiD Public CA G2is OCSP Responder Cybertrust DeviceiD Public CA G2sp OCSP Responder Cybertrust DeviceiD Public CA G3k OCSP Responder
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子証明書所有者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY) 型：OID 値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	暗号アルゴリズムの引数 型：NULL 値：	NULL
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値	＊2048bit 長の公開鍵

(拡張領域)

basicConstraints (extnId :== 2 5 29 19, critical :== FALSE)		**値**
BasicConstraints	基本的制限	
cA	CA かどうかを示すフラグ 型：Boolean 値：	FALSE

authorityKeyIdentifier (extnId :== 2 5 29 35，critical :== FALSE）		**値**
AuthorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値：発行者の subjectPublicKey の Hash 値	認証局により以下の値をとる CA G1: 89:3C:E3:F0:D7:ED:87:47:25:CF: 89:F9:C5:99:4E:6A:F2:3F:73:94 CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC
subjectKeyIdentifier (extnId :== 2 5 2 14，critical :== FALSE）		**値**
SubjectKeyIdentifier keyIdentifier	電子証明書所有者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値：所有者の subjectPublicKey の Hash 値	＊所有者の subjectPublicKey の Hash 値
keyUsage （extnId :== 2 5 29 15，critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BIT STRING 値：100000000 (digitalSignature)	100000000
extendedKeyUsage (extnId :== 2.5.29.37，critical :== FALSE）		**値**
extendedKeyUsage	拡張鍵用途 型：OID 値：1.3.6.1.5.5.7.3.9	1.3.6.1.5.5.7.3.9（OCSPSigning）
OCSP No Check (extnId :== 1.3.6.1.5.5.7.48.1.5 ，critical :== FALSE）		**値**
OCSP No Check OCSP No Check	署名者証明書の失効確認 失効確認を実施しない	NULL

CRL

(標準領域)

Version		値
Version	フォーマットのバージョン番号 型：INTEGER 値：1	 1 (Ver.2)
Signature		**値**
AlgorithmIdentifier Algorithm	証明書失効リストへの署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：右記いずれかの値	 CA G1: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2k 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp 1.2.840.113549.1.1.5(SHA1withRSA) CA G3k 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	署名アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**値**
CountryName Type Value OrganizationName Type Value CommonName Type Value	証明書失効リスト発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 証明書失効リスト発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10 組織名の値 型：PrintableString 値：Cybertrust Japan Co.,Ltd. 証明書失効リスト発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3 固有名称の値 型：PrintableString 値：CRL を発行する右記のいずれかの認証局名	 2.5.4.6 JP 2.5.4.10 Cybertrust Japan Co.,Ltd. 2.5.4.3 Cybertrust DeviceiD Public CA G1 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G3k
thisUpdate		**値**
thisUpdate	有効開始日 型：UTCTime or GeneralizedTime 値：年（2 桁 or4 桁）月日時分秒 Z	 ＊有効開始日時 例 090401000000Z
nextUpdate		**値**
nextUpdate	次回更新予定日時 型：UTCTime or GeneralizedTime 値：年（2 桁 or4 桁）月日時分秒 Z	 ＊更新予定日時 例 090408000000Z

(拡張領域)

authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		値
AuthorityKeyIdentifier	証明書失効リスト発行者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子 型：OCTET STRING 値：認証局の subjectPublicKey の Hash 値	認証局により以下の値をとる CA G1: 89:3C:E3:F0:D7:ED:87:47:25:CF: 89:F9:C5:99:4E:6A:F2:3F:73:94 CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC
cRLNumber (extnId :== 2 5 29 20, critical :== FALSE)		**値**
cRLNumber	CRL の番号 型：INTEGER 値：ユニークな整数	＊CRL の番号

(エントリ領域)

revokedCertificates		値
CertificateSerialNumber	証明書失効リストのシリアル番号 型：INTEGER 値：ユニークな整数	＊シリアル番号
revocationDate	失効日時 型：UTCTime or GeneralizedTime	

(エントリ拡張領域)

invalidityDate (extnId :== 2 5 29 24, critical :== FALSE)		値
invalidityDate	無効化日時 型：GeneralizedTime 値：yyyymmddhhmmssZ	＊該当証明書の失効処理日時
cRLReason (extnId :== 2 5 29 21, critical :== FALSE)		**値**
cRLReason	失効理由コード 型：Enumerated 値：失効理由コード	(1) keyCompromise (2) cACompromise (3) affiliationChanged (4) superseded (5) cessationOfOperation ＊unspecified は、cRLReason として記載しない。

以上