
ビジネス mopera GPS ロケーション認証局 認証業務運用規程

第 1.6 版

株式会社 N T T ドコモ

2016 年 11 月 22 日

改訂履歴

項番	改訂日	改版	改訂内容	改訂理由
1	2012/05/10	1. 1	3. 1. 1. 名称タイプの追加	第二世代証明書対応
2	2012/05/10	1. 1	3. 1. 4. 3. 1. 9. 3. 2. 4. 1. 1. 6. 1. 5. 第二世代証明書対応に伴う文章修正	
3	2012/05/10	1. 1	3. 3. 3. 4. 4. 1. 3. 発行処理に伴う手続きの変更	
4	2012/05/10	1. 1	7. 1. 電子証明書プロファイルの追加	第二世代証明書対応
5	2013/11/1	1. 2	3. 1. 1. 第一世代証明書削除対応に伴う文章修正 6. 1. 5. 第一世代証明書削除対応に伴う文章修正 7. 1. 電子証明書プロファイルの変更 7. 2. 電子証明書プロファイルの変更	
6	2014/4/1	1. 3	7. 1. 電子証明書プロファイルの変更 7. 2. 電子証明書プロファイルの変更	
7	2015/4/1	1. 4	3. 1. 8 押印に関する表記を削除 4. 1. 1 押印に関する表記を削除	
8	2016/6/8	1. 5	3. 2 有効期間変更 証明書送付方法変更 7. 1. 3 有効期間変更	
9	2016/6/21	1. 5	4. 2 証明書発行に必要な情報の送付方法を変更	
10	2016/11/16	1. 6	4. 2 証明書発行に必要な情報の送付方法を変更 7. 1 電子証明書プロファイルの内容を現行化 7. 2 CRL プロファイルの現行化	

商標に関する表示

本文書で使用している社名、製品名等は、各社の登録商標または商標です。

目次

1.	はじめに.....	- 8 -
1.1	概要	- 8 -
1.2	識別	- 8 -
1.3	運営体制と適用範囲	- 8 -
1.3.1	認証局	- 9 -
1.3.2	RA (Registration Authority)	- 10 -
1.3.3	IA (Issuing Authority)	- 10 -
1.3.4	証明書利用者	- 10 -
1.3.5	依拠当事者	- 10 -
1.3.6	適用範囲.....	- 10 -
1.4	問い合わせ先.....	- 11 -
2.	一般規定	- 12 -
2.1	義務	- 12 -
2.1.1	認証局の業務に関する義務	- 12 -
2.1.2	証明書利用者の義務	- 12 -
2.1.3	依拠当事者の義務	- 13 -
2.2	責任	- 14 -
2.2.1	認証局の責任	- 14 -
2.2.2	証明書利用者の責任	- 14 -
2.2.3	依拠当事者の責任	- 14 -
2.3	財務上の責任.....	- 14 -
2.4	解釈、及び、執行.....	- 14 -
2.4.1	準拠法	- 15 -
2.4.2	分割、継続、併合、及び、通知	- 15 -
2.4.3	紛争解決の手続き.....	- 15 -
2.5	料金	- 15 -
2.6	公表とリポジトリ.....	- 15 -
2.6.1	サービスに関する情報の公表.....	- 15 -
2.6.2	公表の頻度	- 16 -
2.6.3	アクセス制御	- 16 -
2.6.4	リポジトリ.....	- 16 -
2.7	準拠性監査	- 16 -
2.7.1	準拠性監査の頻度	- 16 -
2.7.2	監査人の識別／認定	- 16 -

2.7.3	監査人と被監査人の関係	- 16 -
2.7.4	準拠性監査のトピックス	- 16 -
2.7.5	監査指摘事項への対応	- 17 -
2.7.6	監査結果	- 17 -
2.8	機密保持	- 17 -
2.8.1	機密扱いとする情報	- 17 -
2.8.2	機密扱いとしない情報	- 17 -
2.8.3	電子証明書の失効情報の公表	- 18 -
2.8.4	法執行機関への情報公開	- 18 -
2.8.5	民事手続き上の情報公開	- 18 -
2.8.6	証明書利用者の要求に基づく公開	- 18 -
2.8.7	その他の公開条件	- 18 -
2.9	知的財産権	- 18 -
3.	識別と認証	- 19 -
3.1	初期登録	- 19 -
3.1.1	名称のタイプ	- 19 -
3.1.2	名称の意味	- 20 -
3.1.3	名称の変換ルール	- 20 -
3.1.4	名称のユニーク性	- 20 -
3.1.5	名称に関する紛争解決手段	- 20 -
3.1.6	認定、認証、商標の扱い	- 20 -
3.1.7	秘密鍵の所有を証明する方法	- 21 -
3.1.8	組織の確認	- 21 -
3.1.9	個人の確認	- 21 -
3.2	電子証明書の更新	- 22 -
3.3	電子証明書失効後の再発行	- 22 -
3.4	失効要求	- 22 -
4.	運用要件	- 24 -
4.1	電子証明書の申請	- 24 -
4.1.1	新規申請	- 24 -
4.1.2	更新申請	- 25 -
4.1.3	再発行申請	- 25 -
4.2	電子証明書の発行	- 25 -
4.3	電子証明書の受領	- 26 -
4.4	電子証明書の失効、及び、一時停止	- 26 -
4.4.1	失効条件	- 26 -

4.4.2	失効要求者	- 26 -
4.4.3	失効手続き	- 27 -
4.4.4	失効要求の猶予期間	- 27 -
4.4.5	一時停止条件	- 27 -
4.4.6	一時停止要求者	- 27 -
4.4.7	一時停止手続き	- 27 -
4.4.8	一時停止期間の制限	- 27 -
4.4.9	CRL 発行頻度	- 27 -
4.4.10	CRL の確認要件	- 28 -
4.4.11	オンラインステータスチェック	- 28 -
4.4.12	オンライン失効チェック要件	- 28 -
4.4.13	その他の利用可能な失効情報確認手段	- 28 -
4.4.14	その他の利用可能な失効情報確認手段における要件	- 28 -
4.4.15	危殆化時の特別対応	- 28 -
4.5	セキュリティ監査の手順	- 28 -
4.5.1	記録される情報のタイプ	- 28 -
4.5.2	ログが処理、検査される頻度	- 29 -
4.5.3	ログの保管期間	- 29 -
4.5.4	監査ログの保護	- 29 -
4.5.5	監査ログのバックアップ手順	- 29 -
4.5.6	監査ログの収集システム	- 29 -
4.5.7	監査結果の通知	- 29 -
4.5.8	脆弱性評価	- 29 -
4.6	記録のアーカイブ	- 29 -
4.6.1	アーカイブデータの種類	- 30 -
4.6.2	アーカイブデータの保管期間	- 30 -
4.6.3	アーカイブデータの保護	- 30 -
4.6.4	アーカイブデータのバックアップ手順	- 30 -
4.6.5	記録へのタイムスタンプ要件	- 30 -
4.6.6	アーカイブデータの収集システム	- 30 -
4.6.7	アーカイブデータの入手、検証手続き	- 31 -
4.7	鍵更新	- 31 -
4.8	危殆化と災害復旧	- 31 -
4.8.1	ハードウェア、ソフトウェアまたはデータの破壊	- 31 -
4.8.2	電子証明書の失効と再発行	- 31 -
4.8.3	利用者秘密鍵の危殆化	- 31 -

4.8.4	災害等発生時の設備の確保	- 31 -
4.8.5	危殆化、災害からの復旧	- 31 -
4.9	サービスの終了	- 32 -
5.	物理面、手続面及び人事面のセキュリティ統制	- 33 -
5.1	物理的統制	- 33 -
5.1.1	施設の位置と建物構造	- 33 -
5.1.2	物理的アクセス	- 33 -
5.1.3	電源設備と空調設備	- 33 -
5.1.4	水害対策	- 34 -
5.1.5	火災対策	- 34 -
5.1.6	媒体管理	- 34 -
5.1.7	廃棄物処理	- 34 -
5.1.8	オフサイトバックアップ	- 34 -
5.2	手続統制	- 34 -
5.2.1	信頼される役割	- 34 -
5.2.2	役割ごとの職務者数	- 35 -
5.3	人事統制	- 36 -
6.	技術的セキュリティ統制	- 37 -
6.1	鍵ペア生成とインストール	- 37 -
6.1.1	鍵ペア生成	- 37 -
6.1.2	秘密鍵の配布方法	- 37 -
6.1.3	公開鍵の提出方法	- 37 -
6.1.4	認証局公開鍵の提供方法	- 37 -
6.1.5	鍵長	- 37 -
6.1.6	公開鍵パラメータの生成	- 38 -
6.1.7	パラメータ精度の検査	- 38 -
6.1.8	鍵を生成するハードウェア／ソフトウェア	- 38 -
6.1.9	鍵使用目的	- 38 -
6.2	秘密鍵の保護	- 38 -
6.2.1	暗号モジュールに関する標準	- 38 -
6.2.2	秘密鍵の複数人制御	- 38 -
6.2.3	秘密鍵の預託	- 39 -
6.2.4	秘密鍵のバックアップ	- 39 -
6.2.5	秘密鍵のアーカイブ	- 39 -
6.2.6	暗号モジュールへの秘密鍵の格納	- 39 -
6.2.7	秘密鍵の活性化方法	- 39 -

6.2.8	秘密鍵の非活性化方法.....	- 39 -
6.2.9	秘密鍵の破棄方法.....	- 39 -
6.3	鍵ペア管理に関するその他の項目.....	- 39 -
6.3.1	公開鍵のアーカイブ.....	- 40 -
6.3.2	鍵ペアの利用期間.....	- 40 -
6.4	活性化データ.....	- 40 -
6.4.1	活性化データの生成とインストール.....	- 40 -
6.4.2	活性化データの保護.....	- 40 -
6.4.3	活性化データに関するその他の項目.....	- 40 -
6.5	コンピュータセキュリティ統制.....	- 40 -
6.5.1	コンピュータセキュリティ機能要件.....	- 40 -
6.5.2	コンピュータセキュリティ評価.....	- 40 -
6.6	システムのライフサイクルにおけるセキュリティ統制.....	- 41 -
6.6.1	システム開発統制.....	- 41 -
6.6.2	セキュリティマネージメント統制.....	- 41 -
6.6.3	セキュリティ評価の基準.....	- 41 -
6.7	ネットワークセキュリティ統制.....	- 41 -
6.8	暗号モジュールの技術統制.....	- 41 -
7.	電子証明書と CRL のプロファイル.....	- 42 -
7.1	電子証明書のプロファイル.....	- 42 -
7.1.1	ビジネス mopera GPS ロケーションルート認証局.....	- 42 -
7.2	ビジネス mopera GPS ロケーション中間認証局.....	- 43 -
7.2.1	証明書利用者(GPS サービス提供者).....	- 44 -
7.2.2	証明書利用者(ドコモ装置管理者).....	- 45 -
7.2.3	Critical にセットされた拡張子に対するポリシー.....	- 45 -
7.3	ARL/CRL プロファイル.....	- 46 -
7.3.1	ARL(Authority Revocation List).....	- 46 -
7.3.2	CRL(Certificate Revocation List).....	- 47 -
8.	CPS の管理.....	- 48 -
8.1	CPS の変更.....	- 48 -
8.2	公表と通知に関する方針.....	- 48 -
8.3	CPS の承認手順.....	- 48 -

1. はじめに

1.1 概要

本書は株式会社 NTT ドコモ（以下「ドコモ」という）が提供するビジネス mopera GPS ロケーション認証局（以下「本認証局」という）の認証業務運用規程（Certification Practice Statement、以下「本 CPS」という）です。本 CPS は本認証局が電子証明書の発行、管理、失効及び更新を含む一連のサービスを提供する際に採用する手続を記載したものです。これらのサービスをビジネス mopera GPS ロケーション認証局電子証明書発行サービス（以下「本サービス」という）と呼びます。本サービスは、ドコモが提供するビジネス mopera GPS ロケーションサービスにおいて、位置情報の提供機能及び現在位置通知を受ける機能をインターネット上で安全に実現するための仕組みを提供します。

本サービスの関係者には、ドコモ及びビジネス mopera GPS ロケーションサービスを利用する事業者（以下「GPS サービス提供者」という）が存在します。

本 CPS は、IETF(Internet Engineering Task Force) の PKIX(Public Key Infrastructure working group)が提唱する「電子証明書ポリシーと認証実践の枠組み(Certificate Policy and Certification Practices Framework)」(RFC2527)に従い記述されています。

1.2 識別

本認証局では、本 CPS によって規定される本サービスについて、オブジェクト識別子 (OID) を割り当てません。

1.3 運営体制と適用範囲

図 1-1に本サービスの参加者（以下「参加者」という）を示します。参加者は認証局、証明書利用者及び依頼当事者から構成されます。また、本認証局の構成は図 1-2のとおりです。

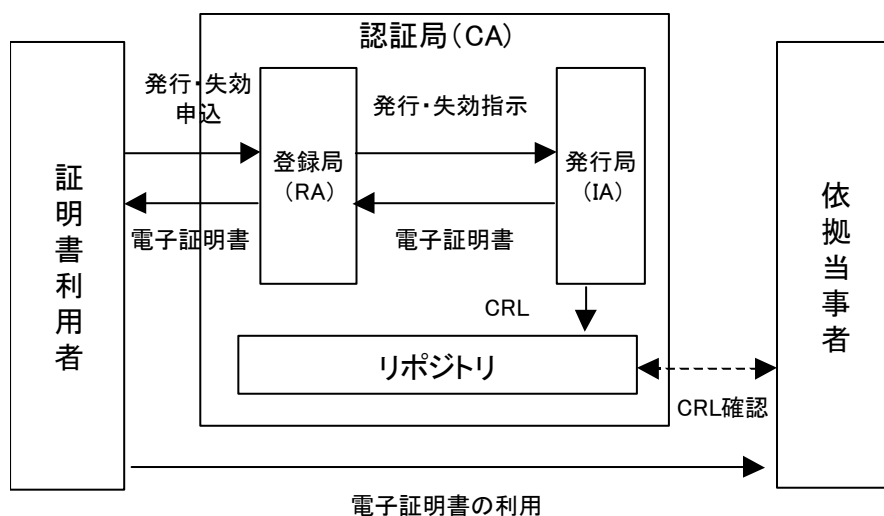


図 1-1 サービスの参加者

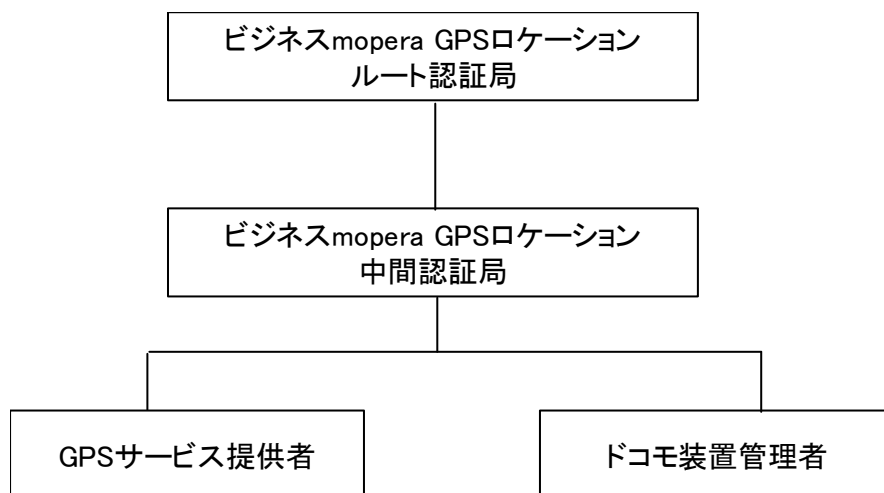


図 1-2 認証局の階層構造

1.3.1 認証局

本 CPS では、本認証局を登録局（以下「RA」という）、発行局（以下「IA」という）及びリポジトリを含む総称として取り扱います。RA の定義は1.3.2項を、IA の定義は1.3.3項を参照してください。リポジトリは電子証明書の失効情報リスト（以下「CRL」という）を一部の依頼当事者に提供する機関です。

1.3.2 RA (Registration Authority)

RA は証明書利用者の識別と電子証明書の申請の審査及び承認、電子証明書の失効申請の審査及び承認、電子証明書の発行、失効、再発行の指示を IA に対して行う機関です。本 CPS では RA 業務を実施するのに利用する設備を RA 設備、RA 業務が実施される部屋を RA 業務室と呼びます。

1.3.3 IA (Issuing Authority)

IA は電子証明書を発行する機関です。本サービスにおいて、IA は本認証局の認証局秘密鍵の管理を行い、電子証明書の発行処理及び失効処理を行います。また、CRL の作成を行い、リポジトリに提供します。本 CPS では IA 業務を実施するのに利用する設備を IA 設備、IA 業務が実施される部屋を IA 設備室と呼びます。また、RA 設備と IA 設備をあわせて認証局設備と呼びます。

1.3.4 証明書利用者

証明書利用者は、電子証明書を本認証局から取得し、電子証明書に記載された（電子証明書で証明された）公開鍵と対になる秘密鍵を管理します。証明書利用者はビジネス mopera GPS ロケーションサービスにおいて、本サービスを利用し、インターネットを経由して位置情報の受領を行うための通信を安全に行います。

本サービスにおける証明書利用者は、GPS サービス提供者及びドコモが準備する装置（以下「ドコモ装置」という）の管理者（以下「ドコモ装置管理者」という）です。

1.3.5 依拠当事者

依拠当事者は本認証局が発行した電子証明書に記載された公開鍵を使用して証明書利用者の認証やデータの暗号化を行います。

本サービスにおける依拠当事者は、GPS サービス提供者及びドコモ装置管理者です。

1.3.6 適用範囲

本認証局は、GPS サービス提供者が自己の電子証明書を利用する、または GPS サービス提供者の電子証明書が利用される範囲を以下のように指定します。GPS サービス提供者は、指定された範囲以外では電子証明書を利用してはなりません。

- GPS サービス提供者の装置（クライアント）からドコモ装置（サーバ）に、インターネットを経由して接続する際の、SSL クライアント認証のための電子証明書としての利用
- ドコモ装置（クライアント）から GPS サービス提供者の装置（サーバ）に、インターネットを経由して接続する際の、SSL サーバ認証のための電子証明書としての利用
- GPS サービス提供者が GPS サービスパスワード変更サイトに、インターネットを経由し

て接続する際の、SSL クライアント認証のための電子証明書としての利用

本認証局は、ドコモ装置管理者に対しても電子証明書を発行します。本 CPS ではドコモ装置管理者用の電子証明書の利用範囲は規定しません。

また、本認証局が発行する電子証明書は、いかなる状況においても以下のような利用目的のために利用してはなりません。

- 犯罪行為または公序良俗若しくは法律に反する行為
- 暗号技術を危殆化させるような試み
- その他ドコモまたは第三者に対して損害を与える行為

1.4 問い合わせ先

本サービスに関する問い合わせ窓口は、『ビジネス mopera GPS ロケーションサービスガイドブック』をご参照ください。

2. 一般規定

2.1 義務

本節では本サービスにおける各参加者の義務について規定します。

2.1.1 認証局の業務に関する義務

本認証局は、証明書利用者及び依拠当事者に対し、以下の義務を負います。

- ① 本認証局は、本 CPS に基づき運用を行います。
- ② 本認証局は、証明書利用者の電子証明書の発行申請を本 CPS に定められた手続に従って適正に審査し、電子証明書の発行を行います。
- ③ 本認証局は、証明書利用者の電子証明書の失効申請を本 CPS に定められた手続に従って適正に審査し、電子証明書の失効を行います。
- ④ 本認証局は、一部の依拠当事者が電子証明書の有効性を検証できるように CRL を定期的に更新します。
- ⑤ 本認証局は、認証局自身の秘密鍵が危殆化することがないように、十分な認証局秘密鍵の管理を行います。
- ⑥ 本認証局は、2.8節で規定された内容に従って情報の管理を適切に行います。
- ⑦ 本認証局は、証明書利用者が守るべき事項を定め、証明者利用者が当該事項を遵守するために、商業的に合理的な施策を実施します。
- ⑧ 本認証局は、業務の一部を外部に委託することができます。本認証局が外部委託を行った場合は、当該業務委託先を適正に管理します。

2.1.2 証明書利用者の義務

本 CPS では、証明書利用者としての、GPS サービス提供者の義務を以下のとおり規定します。

GPS サービス提供者はビジネス mopera GPS ロケーションサービスの利用に先立ち、『ビジネス mopera GPS ロケーションサービスご利用規約』に同意する必要があります。

(1) 利用者秘密鍵の保護

GPS サービス提供者は秘密鍵が他人に使用されないように十分な管理を行わなければなりません。GPS サービス提供者は秘密鍵が記録された装置を他人に貸与してはならず、また、秘密鍵の複製等が行われないように安全に管理する義務があります。

(2) 虚偽申請の禁止

GPS サービス提供者はビジネス mopera GPS ロケーションサービスの利用申請にあたり、虚偽の申告や虚偽の申請を行ってはなりません。

(3) 電子証明書受領時の確認

GPS サービス提供者は、本資料 4.3 節に従い、電子証明書の受領時に電子証明書内に記載

されているグローバル IP アドレスに関する情報に誤りがないことを確認しなければなりません。

(4) 失効申請の義務

GPS サービス提供者は秘密鍵が危殆化した場合、秘密鍵が危殆化した恐れのある場合、秘密鍵の使用を中止する場合、または、申請情報（IP アドレス等）に変更が生じた場合に遅滞なくドコモに対し失効申請を含む適切な申請を行う必要があります。

(5) 電子証明書の利用範囲

電子証明書はその利用範囲を記載した本 CPS に基づいて発行されています。GPS サービス提供者は本 CPS に定める利用以外に、電子証明書を使用してはなりません。また、GPS サービス提供者は有効期限が切れた電子証明書を使用してはなりません。

(6) 本 CPS の承認

本 CPS は本認証局の運営に関わる基本方針を示しています。GPS サービス提供者は本認証局が本 CPS に基づいて運用されていることを理解し、承認しなければなりません。

なお、本 CPS では証明書利用者としてのドコモ装置管理者の義務を規定しません。

2.1.3 依拠当事者の義務

本 CPS では、依拠当事者としての、GPS サービス提供者の義務を以下のとおり規定します。

GPS サービス提供者はビジネス mopera GPS ロケーションサービスの利用に先立ち、『ビジネス mopera GPS ロケーションサービスご利用規約』に同意する必要があります。GPS サービス提供者はドコモ装置管理者の電子証明書に依拠する際に、以下のとおり、ドコモ装置管理者の電子証明書の妥当性を検証しなくてはなりません。

(1) 電子証明書の真正の確認

GPS サービス提供者は、ビジネス mopera GPS ロケーションサービスの利用に先立ち、電子証明書の信頼の起点とするビジネス mopera GPS ロケーションルート認証局及びビジネス mopera GPS ロケーション中間認証局の電子証明書をドコモから確実に入手しなければなりません。GPS サービス提供者は、ドコモ装置管理者の電子証明書に依拠する前に、認証局電子証明書を用いてドコモ装置管理者用の電子証明書に認証局秘密鍵による電子署名が正しく行われており、当該電子証明書が本認証局から発行されたものであること、並びに当該電子証明書が改ざんされていないことを確認しなければなりません。

(2) 電子証明書の有効期間の確認

GPS サービス提供者は、ドコモ装置管理者の電子証明書に依拠する際に、電子証明書が検証時点において有効期間内であることを確認しなければなりません。

なお、本 CPS では依拠当事者としてのドコモ装置管理者の義務を規定しません。

2.2 責任

本節では各参加者の責任を規定します。

2.2.1 認証局の責任

(1) 認証局の責務

本認証局は、本 CPS に従い、証明書利用者の真偽の確認を適切に行い、本認証局が発行及び失効する電子証明書に関わる情報の信頼性を確保します。また、証明書利用者の真偽確認のために提供された個人の情報を適切に保護します。本認証局は、本 CPS 上で規定する本認証局の義務、責任以外の事項に関しては、故意・重過失の場合を除き、責任を負いません。

(2) 損害賠償上の責任の制限

本 CPS では規定しません。『専用回線等接続サービス契約約款』をご参照ください。

2.2.2 証明書利用者の責任

GPS サービス提供者は、証明書利用者としての本 CPS 及び『ビジネス mopera GPS ロケーションサービスご利用規約』、『専用回線等接続サービス契約約款』で規定された義務を遵守しないことにより発生したドコモ、依拠当事者、他の証明書利用者、及び第三者の損害に対し責任を負うものとします。

なお、本 CPS では証明書利用者としてのドコモ装置管理者の責任については規定しません。

2.2.3 依拠当事者の責任

GPS サービス提供者は、依拠当事者としての本 CPS 及び『ビジネス mopera GPS ロケーションサービスご利用規約』、『専用回線等接続サービス契約約款』で規定された義務を遵守しないことにより発生したドコモ、証明書利用者、他の依拠当事者、及び第三者の損害に対し責任を負うものとします。

なお、本 CPS では依拠当事者としてのドコモ装置管理者の責任については規定しません。

2.3 財務上の責任

本サービスは、業務を実施するにあたり十分な財政的基盤を持つドコモによって運営されています。当社の財務情報は、<http://www.nttdocomo.co.jp> より入手が可能です。

2.4 解釈、及び、執行

本節では本サービスにおける本 CPS の解釈の仕方、及び本 CPS に関連した係争の解決の仕方について規定します。

2.4.1 準拠法

本 CPS は、日本国法に基づき解釈されます。この準拠法の選択は、本サービスの利用者の住所地または電子証明書の使用地の場所を問わず、全関係者において統一的な手続及び解釈を確保するためのものです。

2.4.2 分割、継続、併合、及び、通知

本 CPS の一部分の規定が、いかなる程度でも無効または執行不可能であるとされた場合であっても、本 CPS のその他の規定の有効性には影響を及ぼさず、ドコモ及び GPS サービス提供者の意思に最も合理的に合致するよう解釈されるものとします。

本認証局が廃止され、または本サービスが終了した場合においても、機密として取り扱う情報に関する規定の効力はドコモの社内規程に規定された期間は存続するものとします。

本サービスの権利義務に直接影響する本 CPS、及び、その他の契約、合意の規定は、本 CPS に別段の定めをしている場合を除き、書面によらず口頭で修正、放棄、追加、変更、削除または終了させることはできないものとします。

GPS サービス提供者が、本 CPS、及び、その他の契約、合意に対して何らかの通知、請求、依頼をする場合の連絡は、『ビジネス mopera GPS ロケーションサービスガイドブック』で定められた問い合わせ先に対し行われるものとします。また、ドコモが重要な通知を行う場合には書面を通じて行うこととします。

2.4.3 紛争解決の手続き

本 CPS 及び関連する諸規程または電子証明書に関して生じた紛争についての第一審の専属管轄裁判所は東京地方裁判所とします。本 CPS、『ビジネス mopera GPS ロケーションサービスご利用規約』、及び、『専用回線等接続サービス契約約款』に定められていない事項やこれらの文書の解釈に関して疑義が生じた場合、各当事者は、その課題を解決するために訴訟に先立ち誠意をもって協議するものとします。

2.5 料金

本認証局のサービスに関する利用料金については『ビジネス mopera GPS ロケーションサービスガイドブック』をご参照ください。

2.6 公表とリポジット

本節では本サービスにおける情報の公表の方法について規定します。

2.6.1 サービスに関する情報の公表

ビジネス mopera GPS ロケーションサービスの保守メンテナンスの情報の公表については『専用回線等接続サービス契約約款』にて記載されています。本サービスの保守メンテナンス等

の情報については、必要に応じて公表または開示します。

2.6.2 公表の頻度

本サービスに関する情報の通知は随時行います。

2.6.3 アクセス制御

規定しません。

2.6.4 リポジットリ

本認証局では失効された電子証明書が利用されないように CRL の管理及び発行を行います。ただし、CRL については GPS サービス提供者への提供は行わないものとします。

2.7 準拠性監査

本節では本認証局に対する監査について規定します。

2.7.1 準拠性監査の頻度

RA では年に一回以上の準拠性監査を実施します。IA では監査を随時実施します。

2.7.2 監査人の識別／認定

RA の監査人は、RA 業務の準拠性監査を行うための十分な知識を持ったものが任命されます。IA の監査人は、PKI に関する十分な知識を持ったものが任命されます。

2.7.3 監査人と被監査人の関係

RA の監査人は、ドコモ社内の内部監査人が任命されます。IA の監査人は、IA の運用部門と独立した部門の者が任命されます。

2.7.4 準拠性監査のトピックス

RA 業務の準拠性監査は、本 CPS に準拠して運用されていることを確認するために行われます。RA 業務の準拠性監査の主な監査項目は次のとおりです。

- 電子証明書の発行及び失効に係る RA の運用業務
- ソフトウェア、ハードウェア及びネットワーク
- 機密として扱う情報の管理
- 物理的環境及び設備

IA の監査については本 CPS では規定しません。

2.7.5 監査指摘事項への対応

本認証局では監査結果での指摘事項を踏まえ、セキュリティ対策技術の最新の動向を考慮して、業務及び設備の改善や必要に応じ本 CPS を改訂し、その結果の評価を行います。また、必要に応じて当該評価結果に基づき対応措置の見直しを行いません。

2.7.6 監査結果

本認証局は監査結果の外部への開示を行いません。ただし2.8.4項で規定した公的機関から法律に基づく開示要求があった場合や、公表が妥当であると本認証局が判断した場合、監査結果を開示します。

2.8 機密保持

本節では本サービスにおける機密保持の仕組みを規定します。

2.8.1 機密扱いとする情報

本サービスにおいて、認証局は、以下の情報を機密として取り扱います。

- ① 認証局秘密鍵及び秘密鍵の管理情報
- ② 電子証明書の申請に関わる記録
- ③ 本認証局の構築、運用に関する記録、及び、トランザクションの記録
- ④ 本 CPS 運用に関する内部規定及びマニュアル
- ⑤ 準拠性監査の結果
- ⑥ 証明書利用者の情報（3.1.9 項に定める連絡担当者に関する情報を含む）
- ⑦ その他本 CPS で明示的に機密に扱うと定義した情報

なお、2.8.2項において機密として扱わないと定義されたものに関しては機密として取り扱いません。

2.8.2 機密扱いとしない情報

本サービスにおいて、認証局は、以下の情報を機密として取り扱いません。

- ① 電子証明書及び電子証明書に含まれる情報
- ② CRL 及び CRL に含まれる情報
- ③ ドコモが公開した規程文書等に含まれる情報
- ④ その他リポジトリ上に公開される情報

なお、2.8.1項において明示的に機密として取り扱うと定義された情報以外の情報は機密として取り扱いません。

2.8.3 電子証明書の失効情報の公表

本認証局では電子証明書の失効情報を機密として取り扱いませぬ。本認証局は、失効情報をドコモ装置管理者やその他の者に公開します。

2.8.4 法執行機関への情報公開

本サービスで取り扱う情報に対し、法的根拠に基づいて情報を開示するように要求があった場合は、本認証局は法の定めに従い法執行機関へ情報を開示します。

2.8.5 民事手続き上の情報公開

本認証局は訴訟、調停等の裁判手続または行政手続、その他の法的手続の過程において、機密保持対象である情報を開示することができるものとします。

2.8.6 証明書利用者の要求に基づく公開

GPS サービス提供者が当該電子証明書にかかわる情報の開示を希望する場合は、『ビジネス mopera GPS ロケーションサービスガイドブック』をご参照ください。

2.8.7 その他の公開条件

ドコモは、本認証業務の一部を外部に委託する場合、当該業務を実施するために必要な情報を外部委託先に開示する場合があります。ドコモが外部委託を行うにあたり、2.8.1項に規定された機密として取り扱う情報の開示を実施する場合には、ドコモは当該情報が適切に保護されるように、適切な外部委託契約を締結する等を管理します。

2.9 知的財産権

別段の合意がなされない限り、以下の情報資料及びデータに関する著作権その他の知的財産権は本認証局に帰属し、その他の者には帰属しないものとします。本サービスは本 CPS に同意した証明書利用者または依頼当事者にのみ認証局電子証明書の複製を許可します。

- 本認証局から発行された電子証明書（ただし、証明書利用者の公開鍵情報を除く）
- 本認証局から発行された認証局電子証明書
- 本認証局秘密鍵
- 本認証局により作成された失効情報（CRL を含む）
- 本 CPS
- その他ドコモが公表する情報

3. 識別と認証

3.1 初期登録

本節では本サービスにおいて、電子証明書を、GPS サービス提供者に対して初めて発行する際の手続きを規定します。

3.1.1 名称のタイプ

本認証局が発行する電子証明書及び認証局電子証明書の発行者名及び利用者名は、X.500 識別名 (DN:Distinguished Name) の形式に従って設定します。

ビジネス mopera GPS ロケーションルート認証局、ビジネス mopera GPS ロケーション中間認証局、及び、証明書利用者の識別名は以下のとおりです。

属性	値	説明
c (国名)	"JP"	日本
o (組織名)	"NTT DoCoMo, Inc."	ドコモの英文名
ou (組織単位名)	"Business mopera GPS Location Root CA - G2"	ビジネス mopera GPS ロケーションルート認証局の英文名

表 3-1 ビジネス mopera GPS ロケーションルート認証局の識別名

属性	値	説明
c (国名)	"JP"	日本
o (組織名)	"NTT DoCoMo, Inc."	ドコモの英文名
ou (組織単位名)	"Business mopera GPS Location CA - G2"	ビジネス mopera GPS ロケーション中間認証局の英文名

表 3-2 ビジネス mopera GPS ロケーション中間認証局の識別名

属性	値	説明
c (国名)	"JP"	日本
o (組織名)	"NTT DoCoMo, Inc."	ドコモの英文名
ou (組織単位名)	GPS サービス提供者の場合は "Business mopera GPS Location CA Client - G2" ドコモ装置管理者の場合は "Business mopera GPS Location CA Gateway - G2"	GPS サービス提供者の場合は前者、ドコモ装置管理者の場合は後者とする。
cn (共通名)	<IP アドレス> または <ホスト名 (FQDN)>	GPS サービス提供者の場合は前者とする。

表 3-3 証明書利用者の識別名

3.1.2 名称の意味

本サービスにおける、ルート認証局及び中間認証局の識別名については3.1.1項のとおりに定めます。証明書利用者の識別名については証明書利用者が申請したグローバル IP アドレスを元に3.1.1項のとおりに定めます。

3.1.3 名称の変換ルール

規定しません。

3.1.4 名称のユニーク性

本認証局が発行する電子証明書の証明書利用者の識別名には3.1.1項に示すとおり、証明書利用者が申請したグローバル IP アドレスが含まれます。また、本認証局では同一のグローバル IP アドレスを含む複数の電子証明書の発行は行いません（第一世代と第二世代の移行時および証明書更新時のぞく）。

ビジネス mopera GPS ロケーションサービスにおいて、GPS サービス提供者がドコモとの接続回線としてインターネットを利用する場合に利用できるグローバル IP アドレスは、ビジネス mopera GPS ロケーションサービス契約ごとに一つに制限されます。また、GPS サービス提供者が複数のビジネス mopera GPS ロケーションサービス契約を利用する場合は、ドコモと個々に契約を結ぶ必要があります。GPS サービス提供者はこれらの個々の契約を結ぶにあたり、契約ごとに異なったグローバル IP アドレスを用意しなければなりません。このため、原則的に証明書利用者の識別名が重複することは想定されません。

なお、ドコモでは GPS サービス提供者が申請したグローバル IP アドレスが、その時点で本サービスにて利用されている他のグローバル IP アドレスと重複していないことの確認を行います。ただし、ドコモでは申請されたグローバル IP アドレスが、当該 GPS サービス提供者が真に利用権を有しているかどうかの確認は行いません。

3.1.5 名称に関する紛争解決手段

本サービスが発行する電子証明書の証明書利用者の識別名は、3.1.1項のとおり取り決められています。このため、名称に関する紛争の発生は、通常想定されませんが、万が一、名称に関する紛争が発生した場合、ドコモ及び GPS サービス提供者間において、その課題を解決するために訴訟に先立ち誠意をもって協議するものとします。

本認証局は、誠意ある協議により紛争が解決されない場合には、当該電子証明書の失効を行う権利を有します。

3.1.6 認定、認証、商標の扱い

3.1.5 項のとおりとします。

3.1.7 秘密鍵の所有を証明する方法

GPS サービス提供者の秘密鍵と公開鍵の鍵ペアは、GPS サービス提供者自身が管理する装置上で生成します。本サービスは、GPS サービス提供者が生成した公開鍵を、GPS サービス提供者から PKCS#10（利用者公開鍵、及び当該公開鍵に係る情報に対し利用者秘密鍵で電子署名した情報を含む）等の特定の形式で受け取ります。本サービスは、GPS サービス提供者から受け取ったデータの電子署名の検証を行うことで、GPS サービス提供者が間違いなく秘密鍵を所有していることの確認を行うことができます。

3.1.8 組織の確認

GPS サービス提供者はビジネス mopera GPS ロケーションサービスの申し込みの際に、以下の書類をドコモの営業担当者（以下「ドコモ営業担当者」という）に提出しなければなりません。

（１）契約申込書

法人名、連絡担当者名、連絡担当者の所属、連絡担当者の連絡先住所、連絡担当者のメールアドレス、グローバル IP アドレス等の情報の記載が必要です。

（２）登記簿謄本または印鑑証明書

発行後 3 ヶ月以内のものに限ります。ただし、ドコモが提示の必要がないと認める場合はこの限りではありません。

ドコモでは受領した書類をドコモの内部の規定に従って審査し、GPS サービス提供者の確認を行います。また、上記書類の提出の際に GPS サービス提供者の連絡担当者は3.1.9項で示す確認を受けなければなりません。

3.1.9 個人の確認

GPS サービス提供者の連絡担当者はビジネス mopera GPS ロケーションサービスの利用申請の際に以下の書類をドコモ営業担当者に提示し、個人の認証を受けなければなりません。ただし、ドコモが提示の必要がないと認める場合はこの限りではありません。

（１）社員証

GPS サービス提供者の社員であることが確認可能なもの。

（２）本人確認書類

以下のいずれかのもの。

- 運転免許証
- 日本国パスポート
- 住民基本台帳カード（「顔写真」「生年月日」「住所」が記載されているもの）
- 身体障害者手帳または療育手帳または精神障害者保健福祉手帳

- 健康保険証と、住民票または公共料金領収書
- 外国人登録証明書
- 米軍 ID カードと、外国パスポートまたは在日米軍個人車両操縦許可証または公的機関（政府・軍司令部等）が発行した書類

なお、本サービスを利用している過程において、GPS サービス提供者の連絡担当者に変更になった場合、新規の連絡担当者は変更届を提出するとともに、ドコモの営業担当者に対して、上記の本人確認書類と社員証を提示する必要があります。また、GPS サービス提供者は連絡担当者のメールアドレスまたは連絡先住所が変更された場合にもドコモに対し変更届けを提出する必要があります。

3.2 電子証明書の更新

GPS サービス提供者の電子証明書の有効期間は 3 年です。GPS サービス提供者は電子証明書の有効期間の満了前に電子証明書の更新を行う必要があります。ドコモは、電子証明書の有効期間が満了する 30 日前までに GPS サービス提供者の連絡担当者のメールアドレスに対して電子証明書の更新に関する連絡をメールにて行います。その後、ドコモは電子証明書の発行に必要な情報（パスワード等）をドコモの営業担当者から GPS サービス提供者の連絡担当者に送付します。連絡担当者は本節及び4.2節で定められた手続きに従って、電子証明書の更新を行わなければなりません。

3.3 電子証明書失効後の再発行

何らかの事由により、GPS サービス提供者が利用中の電子証明書の失効を行い、電子証明書の再発行を行う場合は以下の規定に従い実施されます。

GPS サービス提供者は、以下の書類をドコモに提出する必要があります。

（1）証明書再発行申請書

法人名、連絡担当者名、連絡担当者の所属、連絡担当者の連絡先住所、再発行の理由、サービス変更希望日等の情報の記載が必要です。

ドコモでは受領した書類をドコモの内部の規定に従って審査し、電子証明書の再発行及び失効を行います。

3.4 失効要求

GPS サービス提供者がビジネス mopera GPS ロケーションサービスの利用を停止する場合や、利用する回線を専用線に切り替える時は以下の証明書失効申請書をドコモ営業担当者に提出する必要があります。

(1) 証明書失効申請書

法人名、連絡担当者名、連絡担当者の所属、連絡担当者の連絡先住所等の記載が必要です。

ドコモでは受領した書類をドコモが定める規定に従って審査し、電子証明書の失効を行います。

4. 運用要件

4.1 電子証明書の申請

本節では GPS サービス提供者が利用する電子証明書の新規申請、更新申請、再発行申請の手順等の詳細について規定します。

4.1.1 新規申請

(注:2015 年 9 月末をもってビジネス mopera GPS ロケーションサービスの新規受付は終了いたしました)

ビジネス mopera GPS ロケーションサービスの利用に際し、GPS サービス提供者が回線種別としてインターネットを希望する場合は、以下の手順により電子証明書の取得を行う必要があります。

GPS サービス提供者はビジネス mopera GPS ロケーションサービスの利用に際し以下の書類をドコモに提出しなければなりません。

(1) 契約申込書

法人名、連絡担当者名、連絡担当者の所属、連絡担当者の連絡先住所、連絡担当者のメールアドレス、グローバル IP アドレス等の情報の記載が必要です。

(2) 登記簿謄本または印鑑証明書

発行後 3 ヶ月以内のものに限ります。ただし、ドコモが提示の必要がないと認める場合はこの限りではありません。

また、GPS サービス提供者の連絡担当者は以下の書類をドコモ営業担当者に提示しなければなりません。ただし、ドコモが提示の必要が無いと認める場合はこの限りではありません。

(1) 社員証

GPS サービス提供者の社員であることが確認可能なもの。

(2) 本人確認書類

以下のいずれかのもの。

- 運転免許証
- 日本国パスポート
- 住民基本台帳カード（「顔写真」「生年月日」「住所」が記載されているもの）
- 身体障害者手帳または療育手帳または精神障害者保健福祉手帳
- 健康保険証と、住民票または公共料金領収書
- 外国人登録証明書

- 米軍 ID カードと、外国パスポートまたは在日米軍個人車両操縦許可証または公的機関（政府・軍司令部等）が発行した書類

ドコモでは登記簿謄本または印鑑証明書で組織の確認を行い、社員証、本人確認書類で個人の確認を行います。その後の電子証明書の発行の手順は4.2節に従います。

4.1.2 更新申請

GPS サービス提供者は電子証明書の有効期間が満了する前に、電子証明書の更新を行わなければなりません。電子証明書の更新時に、GPS サービス提供者は自発的に申請処理を行う必要はありません。ドコモは登録されている連絡担当者に対し有効期間の満了の 30 日前までにメールにて電子証明書の更新に関する連絡を行います。その後の電子証明書の更新の手順は4.2節に従います。

4.1.3 再発行申請

GPS サービス提供者が利用中の電子証明書を失効させ、電子証明書の再発行を受ける場合は、以下の書類をドコモに提出する必要があります。

（1）証明書再発行申請書

法人名、連絡担当者名、連絡担当者の所属、連絡担当者の連絡先住所、再発行の理由等の情報の記載が必要です。

ドコモでは再発行申込書の記載内容の確認を行います。その後の証明書再発行の手順は4.2節に従います。

4.2 電子証明書の発行

電子証明書の発行、更新、再発行が認められた場合は、以下の手順により、電子証明書が GPS サービス提供者に発行されます。

- ① ドコモにて当該 GPS サービス提供者用の証明書発行 ID 及び証明書取得のためのパスワードの生成を行います。
- ② ドコモは登録されている連絡担当者のメールアドレス宛に、電子証明書の更新に関する連絡をメールにて行います。その後、ドコモは電子証明書の発行に必要な情報（Web サイト URL、パスワード等）をドコモの営業担当者から GPS サービス提供者の連絡担当者に送付します。
- ③ GPS サービス提供者はドコモが指定した Web サイトにドコモが指定する Web ブラウザでアクセスします。
- ④ GPS サービス提供者はドコモが指定する Web ブラウザにより自身の鍵ペアの生成を

行い、パスワード等を入力します。

- ⑤ 本認証局は電子証明書を発行します。
- ⑥ GPS サービス提供者は発行された電子証明書のダウンロードを行います。

本 CPS ではドコモ装置管理者の電子証明書の発行方法を規定しません。

4.3 電子証明書の受領

GPS サービス提供者は発行された電子証明書内に記載されているグローバル IP アドレスに誤りが無いことを確認しなければなりません。万が一、記載されているグローバル IP アドレスに誤りがあった場合、GPS サービス提供者は遅滞なくドコモに対して連絡を行わなければなりません。本認証局では GPS サービス提供者が電子証明書のダウンロードを行った段階で電子証明書の受領が完了したと判断します。

本 CPS ではドコモ装置管理者の電子証明書の受領方法を規定しません。

4.4 電子証明書の失効、及び、一時停止

本節では電子証明書の失効及び一時停止について規定します。

4.4.1 失効条件

以下の事項に該当する場合、本認証局は、GPS サービス提供者の電子証明書を失効するものとします。

- GPS サービス提供者が、自身の秘密鍵が危殆化しているまたは危殆化の恐れがあると判断した場合。
- GPS サービス提供者が、自身の秘密鍵を紛失した場合。
- GPS サービス提供者が使用しているグローバル IP アドレスに、変更があった場合。
- GPS サービス提供者が、ビジネス mopera GPS ロケーションサービスの利用を停止する場合。
- GPS サービス提供者が、利用回線を専用線に変更する場合。
- その他、本認証局が電子証明書の失効が必要と判断した場合。

なお、ドコモ装置管理者の電子証明書の失効条件については本 CPS では規定しません。

4.4.2 失効要求者

本サービスでは、以下の参加者が電子証明書の失効要求を行う場合があります。

- 証明書利用者（GPS サービス提供者、ドコモ装置管理者）
- 本認証局

4.4.3 失効手続き

GPS サービス提供者がビジネス mopera GPS ロケーションサービスの利用を停止する場合や、利用する回線を専用線に切り替える時は失効申込書をドコモ営業担当者に提出する必要があります。ドコモでは受領した失効申込書を内部の規定に従って審査し、審査終了後に決められた手続きに従い、電子証明書の失効を行います。

GPS サービス提供者が、電子証明書の再発行のために電子証明書の失効を希望する場合は、連絡担当者は4.1節及び4.2節で定められた手続きに基づき、電子証明書の再発行を受けなければなりません。ドコモは、GPS サービス提供者から再発行の申請を受けた場合、当該申請において GPS サービス提供者が指定したサービス変更希望日に、再発行の対象となる古い電子証明書の失効処理を行います。ただし、電子証明書の再発行申請の理由が、GPS サービス提供者が所有する秘密鍵の危殆化または危殆化した恐れがある場合のときは、本認証局では再発行申込書の審査終了後、遅滞なく当該電子証明書の失効処理を行います。

また、GPS サービス提供者は失効手続きの際に4.4.4項の失効猶予期間を遵守する必要があります。

4.4.4 失効要求の猶予期間

証明書利用者は4.4.1項の失効条件に該当することに気づいてから、遅滞なく失効申請または再発行申請をする必要があります。また、本認証局は失効要求の受付処理が完了後、電子証明書の失効処理を行います。

4.4.5 一時停止条件

規定しません。

4.4.6 一時停止要求者

規定しません。

4.4.7 一時停止手続き

規定しません。

4.4.8 一時停止期間の制限

規定しません。

4.4.9 CRL 発行頻度

本認証局は1日に1度、CRLの更新を行います。

4.4.10 CRL の確認要件

規定しません。

4.4.11 オンラインステータスチェック

規定しません。

4.4.12 オンライン失効チェック要件

規定しません。

4.4.13 その他の利用可能な失効情報確認手段

規定しません。

4.4.14 その他の利用可能な失効情報確認手段における要件

規定しません。

4.4.15 危殆化時の特別対応

本認証局では、GPS サービス提供者より、秘密鍵の危殆化または危殆化した恐れがあるために証明書再発行の申請を受けた場合は、4.4.3項に示すとおりにより再発行申込書の審査終了後、即座に当該電子証明書の失効を行います。

4.5 セキュリティ監査の手順

本節ではセキュリティ監査手順について規定します。

4.5.1 記録される情報のタイプ

本認証局設備では、次の重要なイベントについて記録します。

(1) 電子証明書のライフサイクル管理イベント（以下の事項を含む）

- 電子証明書申請、更新、失効
- 要求の処理
- 電子証明書及び CRL の生成並びに発行

(2) セキュリティに関するイベント

- IA 設備が設置された施設への来訪者の入退室記録
- IA 設備が提供するシステムへのアクセスの試み
- セキュリティ上取り扱いに慎重を要するファイルもしくは記録に関する読み込み、書き込みまたは削除

なお、各記録は以下の情報を含みます。

- 記録の種別
- 記録の日時
- 記録者の身元（特定できる場合）

4.5.2 ログが処理、検査される頻度

本認証局設備内における監査ログの検査は、本システムを安全に運営するために適切と考えられる頻度で実施されます。また、本認証局設備内ではそのために必要な監査ログを記録します。

4.5.3 ログの保管期間

IA 設備において、監査ログは少なくとも 2 ヶ月間保管されます。証明書ライフサイクルに関するログは少なくとも 5 年間保管されます。

4.5.4 監査ログの保護

本認証局設備の監査ログは、漏洩、改ざん、危殆化等が発生しないように安全に保管管理されます。

4.5.5 監査ログのバックアップ手順

本認証局設備においてバックアップが必要な監査ログは所定のバックアップ手順に従いバックアップを行います。

4.5.6 監査ログの収集システム

本認証局設備ではシステムによる自動処理及びオペレータによる手作業を組み合わせ、監査ログを収集します。

4.5.7 監査結果の通知

本認証局設備の監査ログの監査において調査の必要性がある事象が検出された場合、当該事象の発生者に対し通知なく調査を行います。

4.5.8 脆弱性評価

規定しません。

4.6 記録のアーカイブ

本節では本サービスに関わる記録の保管方法について規定します。

4.6.1 アーカイブデータの種類

RA では以下のアーカイブデータを保管します。

- 発行及び再発行申請に関するアーカイブデータ
 - ① サービス申込に関する書類（契約申込書、印鑑証明書等）とその記録
- 失効に関するアーカイブデータ
 - ① 失効に関する書類（失効申請書）
- 組織管理に関するアーカイブデータ
 - ① 本 CPS とその変更に関する記録
 - ② 業務手順を記述した書類とその変更に関する記録
 - ③ 業務に従事する者の責任及び権限並びに指揮命令系統を記述した書類とその変更に関する記録
 - ④ 認証業務の一部を外部に委託する場合の委託契約に関わる書類
 - ⑤ その他組織管理に関する書類一式

IA では以下のアーカイブデータを保管します。

- 4.5.1項で規定されている監査ログ、及び電子証明書

4.6.2 アーカイブデータの保管期間

RA のアーカイブデータについてはドコモの社内規程に規定された期間の間、保存します。IA のアーカイブデータについては4.5.3項に規定されているとおり保存します。

4.6.3 アーカイブデータの保護

RA のアーカイブデータについてはドコモの社内規程に従い保護します。IA のアーカイブデータについては4.5.4項に規定されているとおりに保護します。

4.6.4 アーカイブデータのバックアップ手順

RA 設備については規定しません。IA 設備については4.5.5項に規定されているとおりにバックアップを行います。

4.6.5 記録へのタイムスタンプ要件

RA 設備については規定しません。IA 設備で管理される記録は、日時の情報を含みます。これらの記録は RFC3161 で規定されているようなタイムスタンプ技術による処理は行われていません。

4.6.6 アーカイブデータの収集システム

本認証局ではシステムによる自動処理及びオペレータによる手作業を組み合わせ、アーカイ

ブデータを収集します。

4.6.7 アーカイブデータの入手、検証手続き

RA 設備については規定しません。IA 設備については4.5.4項に規定されたとおりに保護を行います。

4.7 鍵更新

規定しません。

4.8 危殆化と災害復旧

本節では災害や鍵の危殆化が発生した時の本認証局の対応を規定します。

4.8.1 ハードウェア、ソフトウェアまたはデータの破壊

RA 設備におけるハードウェアの破壊が生じた場合は、代替機により業務の継続を行います。

IA 設備におけるハードウェアは二重化されており、ハードウェアの破壊が発生した場合、待機系のハードウェアにより業務を継続します。

本認証局設備におけるソフトウェアまたはデータの破壊が発生した場合、認証局の運用者はバックアップされたソフトウェアまたはデータにより復旧を行います。

4.8.2 電子証明書の失効と再発行

災害時において、GPS サービス提供者が装置の被災等により所有する秘密鍵を紛失した場合は、本認証局に証明書再発行申請書を提出する必要があります。本認証局は、電子証明書の再発行を行い、その後、再発行前の電子証明書の失効を行います。

4.8.3 利用者秘密鍵の危殆化

災害時において GPS サービス提供者は、所有する秘密鍵が危殆化した恐れがある場合は、遅滞なく再発行申込書を提出する必要があります。証明書再発行申請書を受けた本認証局では当該 GPS サービス提供者の電子証明書の失効を行います。また本認証局は、電子証明書の再発行を行います。

4.8.4 災害等発生時の設備の確保

IA 設備は日本国内においても十分に遠隔な地域に災害対策用の設備を設けています。災害発生時には鍵の危殆化の恐れがない場合、本災害対策用設備により運用を継続します。

4.8.5 危殆化、災害からの復旧

IA 設備が天災事変等の被災、認証設備の故障等により、運用を停止した場合、鍵の危殆化の

恐れがない場合、所定の手続きに従って復旧を行います。

4.9 サービスの終了

本認証局が本サービスを終了する場合は、その終了に先立ち、終了プランを作成します。本認証局は、当該終了プランの作成において、以下の事項の検討を行い、検討結果に基づいて本サービスを終了するものとします。

- GPS サービス提供者に対し、本認証局の終了を通知するための方法
- 上記通知の実施時期
- 本認証局が保管しているデータの、本 CPS4.6節で必要とされる期間中の取り扱い
- 機密として取り扱う情報の措置
- リポジトリの運用について

5. 物理面、手続面及び人事面のセキュリティ統制

5.1 物理的統制

本節では本認証局が設置される設備の物理的な管理統制について規定します。

5.1.1 施設の位置と建物構造

本認証局設備を収容するすべての建築構造物（建物及び部屋）は、耐震耐火設計、自動火災報知器と消火装置の設置、防火区画内設置、隔壁による区画、水害防止等の措置が予め十分講じられている等、地震、火災、水害等を想定した災害対策がなされた施設です。

なお、IA 設備室の所在及び仕様は、関係者以外には公表されません。建物の内外には IA 設備室の所在については表示されません。

5.1.2 物理的アクセス

RA では、RA 業務室への入退室の管理を厳格に行います。RA 業務室には IC カード等を用いた認証が行われてから入室が可能となるように防護装置が講じられています。RA 業務室に入室権限を有しない者は、入室権限を有する者の付添なしで入室することはできません。

IA 設備室への入退室等については、次により厳重に管理されるものとします。

- IA 設備室は厳重に施錠管理され、その入室は入室者の身体的特徴の識別手段を用いた施錠設備による本人認証を行って初めて可能となるよう予め防護装置が講じられています。IA 設備室に入室権限を有しない者は、入室権限を有する者の付添なしで入室することはできません。
- 別途定められたセキュリティ及び監査要件ガイドに従い、IA 設備室の一部には、複数人によってのみ入退室管理可能な領域を設置しています。
- 入室のための装置操作に非正常な時間を要した場合においては、警報が発せられるように予め設定されるものとします。
- IA 設備室へ入退室者及び在室者の状況については、遠隔監視装置、モーションセンサー及び映像記録装置によって自動的かつ継続的に監視記録され、その記録については、正常に点検され、定められた時間、安全に保管されます。

5.1.3 電源設備と空調設備

RA については規定しません。IA が収容されるすべての施設は停電に備えた UPS・自家発電機の設置、配置され設備に応じた空調機器の設置等、サービスの継続に必要な適切な措置が講じられています。

5.1.4 水害対策

RA については規定しません。IA が収容されるすべての施設は水害防止等の措置が予め講じられています。

5.1.5 火災対策

RA については規定しません。IA が収容されるすべての施設は火災予防と火災被害に関して合理的な対策を講じています。設備の火災予防対策は、国内の火災予防規則に則って設計されています。

5.1.6 媒体管理

本認証局におけるアーカイブ、及び、バックアップデータは本認証局設備内、または、安全なオフサイト設備に保管されています。これらの設備は不適切なアクセスがないように適切な物理的論理的アクセスコントロールが実施されており、また、事故的な災害から媒体を保護するように設計されています。

5.1.7 廃棄物処理

本認証局における重要な文書等は廃棄時に回復不可能な方法により処理されます。重要な情報を含む媒体は廃棄前に再読み出しが不可能なようにフォーマットします。また、暗号モジュールデバイスは廃棄前に物理的に破壊されるか、デバイスの機能を用いて初期化します。

5.1.8 オフサイトバックアップ

RA については規定しません。IA については4.8節で規定したとおりです。

5.2 手続統制

本節では本認証局で行われる手続きの管理方法について規定します。

5.2.1 信頼される役割

RA には以下の構成員が存在します。

- 認証局代表者（本認証局の代表者。）
- 認証局管理者（本認証局の管理者。RA 全般の管理及び IA の監督を行う。）
- RA 業務責任者（RA 業務の責任者。RA 設備の管理、RA 業務担当者の管理を行う。）
- RA 業務担当者（RA 端末の操作、申請書類の確認等を行う。）
- RA 認証業務担当者（ドコモ営業担当者等。GPS サービス提供者の真偽を確認する。）

上記の構成員を選定するにあたり、ドコモではドコモ内部の人事規定に従い、本人の確認を行います。ドコモが、一部の RA 業務を外部に委託する場合は、ドコモは当該要員についてドコモ

と同等の管理統制が行われることを契約等によって管理します。RA では上記の構成員を信頼する人物として取り扱います。

RA での信頼される人物は以下の作業を実施します。

- GPS サービス提供者が提示した書類の確認
- 提出された各種申請書を検証し、承認または拒絶の実施
- 各種アーカイブデータの管理・保管
- RA 設備の管理
- 認証局に関する通知の作成
- 証明書利用者への各種情報の送付
- IA の監督

本認証局では IA 業務は外部委託を行います。IA において信頼される人物となるためには、外部委託先の人事担当者との面接及び広く認識されている身分証明書(パスポート、運転免許証等)により本人の確認をおこないます。

信頼される人物には、以下の事項に重大な影響を及ぼすような、認証または暗号作業に関わる全ての従業員、独立請負業者及びコンサルタントが含まれます。

- 電子証明書申請中の情報の検証
- 電子証明書申請、失効要求、更新要求または申込情報の承認、拒絶その他の処理
- 電子証明書の発行または失効（リボジトリの制限された部分へのアクセスを含む）
- 利用者の情報または要求の取り扱い

IA において信頼される人物には、以下の者が含まれますが、これに限定されません。

- カスタマ・サービス要員
- キーマネジャー（秘密鍵の管理を行う要員）
- セキュリティ要員
- システム管理者
- 技術要員のうち指定された者
- 認証事業の基盤の信頼性を管理するために指定された経営陣

5.2.2 役割ごとの職務者数

RA では、従業者による不正及び過失による事故を防ぐための管理手続きを維持しています。RA 業務を実施するにあたり、GPS サービス提供者から提出された書類の確認は複数人によるチェックを必ず行います。

IA では、業務内容に基づく職務分掌を確実にするための方針と管理手続きを維持しています。認証局用暗号ハードウェア及び関連する鍵関連資料等の最も機密を要する業務へのアクセス及

び管理は、複数の信頼される人物により行われます。

これらの内部統制手続きは、物理的または論理的にデバイスにアクセスするために最低 2 名の信頼される人物が確実に必要になるように設計されています。認証局用暗号ハードウェアへのアクセスは、その受け入れから最終の論理的・物理的破壊の検査までのライフサイクルを通じて、複数の信頼される人物により実施されています。モジュールがサービスに提供されると、当該モジュールに関する一切の操作は、物理的及び論理的にも複数人及び複数の権限により管理されます。モジュールへの物理的なアクセスができる者は、シークレット・シェアを保有しておらず、シークレット・シェアを保有する者は、モジュールへの物理的なアクセスできません。

5.3 人事統制

本サービスの要員の適格性の審査、教育、配置転換等については、ドコモの人事規程に基づいて運用します。また、すべての要員には、運営を行うために必要な知識及び技術を習得するための教育訓練を行います。

ただし、外部委託を行う場合、その要員に関する要件は本 CPS では規定しませんが、本 CPS で規定される認証業務運用要件に照らして十分な要件を満たしていることを事前に確認します。

6. 技術的セキュリティ統制

6.1 鍵ペア生成とインストール

本節では本認証局及び証明書利用者の鍵ペア生成及び装置へのインストール方法を規定します。

6.1.1 鍵ペア生成

認証局鍵ペアの生成は、認証設備室内で、権限を持つ複数名の要員がそろい、一人の操作だけではできない方法により暗号モジュール内で生成します。また、GPS サービス提供者は自己の責任によって鍵ペアの生成を行います。本 CPS ではドコモ装置管理者の鍵ペアの生成方法を規定しません。

6.1.2 秘密鍵の配布方法

GPS サービス提供者が利用する秘密鍵は GPS サービス提供者自身によって生成されます。このため本 CPS では秘密鍵の配布方法について規定しません。

6.1.3 公開鍵の提出方法

GPS サービス提供者の公開鍵は、Web ブラウザにより PKCS#10 のファイルフォーマットにて本認証局に配送されます。

6.1.4 認証局公開鍵の提供方法

ビジネス mopera GPS ロケーションルート認証局の公開鍵が記載されている認証局電子証明書はビジネス mopera GPS ロケーションサービス申込み時にドコモより、GPS サービス提供者に CD-R 等にて提供されます。またビジネス mopera GPS ロケーション中間認証局の認証局電子証明書（公開鍵を含む）は証明書発行時に PKCS # 12 の形式にてダウンロードすることが可能です。

6.1.5 鍵長

本サービスで用いられる鍵ペアに関する技術的仕様は以下のとおりです。

- (1) ビジネス mopera GPS ロケーションルート認証局の鍵ペア：
rsaEncryption(1.2.840.113549.1.1.1) 2048bit（第二世代）
- (2) ビジネス mopera GPS ロケーション中間認証局の鍵ペア：
rsaEncryption(1.2.840.113549.1.1.1) 2048bit（第二世代）
- (3) 証明書利用者の鍵ペア：
rsaEncryption(1.2.840.113549.1.1.1) 2048bit（第二世代）

6.1.6 公開鍵パラメータの生成

規定しません。

6.1.7 パラメータ精度の検査

規定しません。

6.1.8 鍵を生成するハードウェア／ソフトウェア

認証局の秘密鍵を生成するハードウェア／ソフトウェアについては、6.2.1項を参照してください。GPS サービス提供者の秘密鍵は Web ブラウザにより、GPS サービス提供者の装置上で生成されます。

6.1.9 鍵使用目的

本認証局は、認証局秘密鍵を、以下の目的以外に使用することはありません。

- ① 証明書利用者の電子証明書に対する署名
- ② 認証局電子証明書に対する自己署名、及び、下位認証局が存在する場合には下位認証局電子証明書に対する署名
- ③ CRL、ARL に対する署名

GPS サービス提供者の秘密鍵は、以下の目的以外に使用されることはありません。

- ① SSL 通信におけるサーバ認証
- ② SSL 通信におけるクライアント認証

なお、ドコモ装置管理者の秘密鍵の利用方法については規定しません。

6.2 秘密鍵の保護

本節では認証局秘密鍵の保護について規定します。証明書利用者の秘密鍵の保護については本節では規定しませんが、証明書利用者は自身の秘密鍵を自身の責任において保護する必要があります。

6.2.1 暗号モジュールに関する標準

認証局秘密鍵は IA 設備内において暗号モジュール内で保護されています。暗号モジュールには FIPS 140-1 level 3 相当のハードウェアセキュリティモジュール (HSM) を利用しています。

6.2.2 秘密鍵の複数人制御

本認証局は、機密を要する IA 設備の暗号運用について複数の信頼できる個人が関与すること

を要求する技術的・手続的な仕組みを実施しています。本認証局は、認証局の秘密鍵を利用するために「シークレット・シェアリング」という手法を用いています。この手法では、必要な起動データを、「シークレット・シェア」と呼ばれる別々のパーツに分割し、「シェアホルダー」と呼ばれる訓練を受けた信頼できる個人が保有します。特定のハードウェア暗号モジュールに保管されている認証局の秘密鍵を起動させるためには、当該モジュールに関して生成・分配されたシークレット・シェアの総数のうち、一定数のシークレット・シェアが必要となります。

6.2.3 秘密鍵の預託

本サービスでは秘密鍵の預託（エスクロー）は行いません。

6.2.4 秘密鍵のバックアップ

認証局秘密鍵は、鍵が格納されている暗号モジュールと同型の暗号モジュール間のクローニング（複製）機能によりバックアップが行われます。バックアップは、複数人の管理の下、認証設備室内において行われます。バックアップ用の暗号モジュールは認証局設備内の安全な場所に保管されます。

6.2.5 秘密鍵のアーカイブ

本認証局は認証局秘密鍵のアーカイブを行いません。

6.2.6 暗号モジュールへの秘密鍵の格納

認証局秘密鍵は暗号モジュール内で生成されるため、本 CPS では規定しません。

6.2.7 秘密鍵の活性化方法

6.2.2項を参照してください。

6.2.8 秘密鍵の非活性化方法

認証局秘密鍵はシステムの停止、または、暗号モジュールをトークンリーダーから抜き取ることにより非活性化します。

6.2.9 秘密鍵の破棄方法

規定しません。

6.3 鍵ペア管理に関するその他の項目

本節では鍵ペア管理のその他の項目について規定します。

6.3.1 公開鍵のアーカイブ

証明書利用者の電子証明書、認証局電子証明書は認証局のサービス期間中アーカイブされます。

6.3.2 鍵ペアの利用期間

規定しません。

6.4 活性化データ

本節では秘密鍵を活性化するためデータについて規定します。

6.4.1 活性化データの生成とインストール

証明書利用者の秘密鍵は適切に保護（活性化のためにパスワードを設定する等）されなければなりません。

認証局秘密鍵は6.2.2項、及び、6.2.7項に規定したシークレット・シェアによって活性化されます。シークレット・シェアは6.1.1項で規定された秘密鍵の生成時に権限者へ渡されます。

6.4.2 活性化データの保護

認証局秘密鍵の活性化情報は複数人に分割されて管理されています。また、各活性化情報は権限者の責任で厳重に管理されます。証明書利用者の秘密鍵の活性化データについては本 CPS では規定しません。

6.4.3 活性化データに関するその他の項目

規定しません。

6.5 コンピュータセキュリティ統制

本節では IA 設備のコンピュータセキュリティ統制について規定します。RA 設備については規定しません。

6.5.1 コンピュータセキュリティ機能要件

IA 設備に用いられるシステムはアクセス制御機能、監査ログ記録機能を持つ信頼性の高いシステムにより構築されます。

6.5.2 コンピュータセキュリティ評価

IA 設備のうち専ら電子証明書の作成に関わる装置は ISO/IEC15408-3:1999, Information technology-Security techniques--Evaluation criteria for IT Security--Part 3: Security assurance requirements の EAL レベル相当のシステムを利用しています。

6.6 システムのライフサイクルにおけるセキュリティ統制

本節ではシステムのライフサイクルにおけるセキュリティ統制について規定します。

6.6.1 システム開発統制

本認証局設備のシステム開発、修正または変更に当たっては、所定の手続に基づき、信頼できる組織及び環境下において作業を実施します。

6.6.2 セキュリティマネージメント統制

本認証局設備におけるソフトウェアの設定、及び、ソフトウェアは所定の手順によってその完全性、バージョン、及び、設定が管理されています。

6.6.3 セキュリティ評価の基準

規定しません。

6.7 ネットワークセキュリティ統制

RA は RA 設備内のネットワークを適切に管理します。また、RA 設備と IA 設備の間で行われる通信については、IA 機器による RA 業務担当者の認証、通信の内容の暗号化、改ざん検知を行うセキュリティ機能を有したアプリケーションが使用されます。

IA では、権限のない者によるアクセス及び他の不正な活動を防止するため、別途定められたセキュリティ及び監査要件ガイドに従い、セキュリティの確保されたネットワークを用いて、その全ての業務を実施しています。秘密とすべき情報の通信は、暗号化等を用いて行います。

6.8 暗号モジュールの技術統制

本認証局で使用する暗号モジュールは、6.2.1項に定める要件に合致しています。

7. 電子証明書と CRL のプロファイル

7.1 電子証明書のプロファイル

本節では電子証明書のプロファイルについて規定します。

7.1.1 ビジネス mopera GPS ロケーションルート認証局

第二世代(G2)ルート認証局の電子証明書プロファイルを規定します。

【基本領域】

領域名	設定値(例)	補足説明
version (X.509 のバージョン)	2	X.509 バージョンが3であることを示す。
serialNumber (発行番号)	...	ユニークな値。
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す。
issuer (発行者名)	c="JP" o="NTT DoCoMo, Inc." ou="Business mopera GPS Location Root CA - G2"	PrintableString 型で記載。
validity (有効期間)		21 年有効。
notBefore (開始日)	YYMMDDHHMMSS(年月日時分秒)	UTC 時刻型(UTCTime)で記載。
notAfter (終了日)	YYMMDDHHMMSS(年月日時分秒)	UTC 時刻型(UTCTime)で記載。
subject (主体者名)	c="JP" o="NTT DoCoMo, Inc." ou="Business mopera GPS Location Root CA - G2"	PrintableString 型で記載。 issuer と同じ値。
subjectPublicKeyInfo (主体者の公開鍵)		
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	rsaEncryption を示す。
subjectPublicKey (公開鍵)	...	主体者の公開鍵。2048 ビット長。

【拡張領域】

領域名	Critical フラグ	設定値(例)	補足説明
basicConstraints (基本制約)	TRUE		
cA		TRUE	認証局であることを示す。
pathLenConstraint		1	
subjectKeyIdentifier (主体者鍵識別子)	FALSE	...	主体者の公開鍵の SHA-1 ハッシュ値。
keyUsage (鍵使用法)	TRUE	keyCertSign, cRLSign	

7.2 ビジネス mopera GPS ロケーション中間認証局

第二世代(G2)中間認証局の電子証明書プロファイルを規定します。

【基本領域】

領域名	設定値(例)	補足説明
version (X.509 のバージョン)	2	X.509 バージョンが3であることを示す。
serialNumber (発行番号)	...	ユニークな値。
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す。
issuer (発行者名)	c="JP" o="NTT DoCoMo, Inc." ou="BusinessmoperaGPSLocation Root CA - G2"	PrintableString 型で記載。
validity (有効期間)		21 年有効。
notBefore (開始日)	YYMMDDHHMMSS(年月日時分秒)	UTC 時刻型(UTCTime)で記載。
notAfter (終了日)	YYMMDDHHMMSS(年月日時分秒)	UTC 時刻型(UTCTime)で記載。
subject (主体者名)	c="JP" o="NTT DoCoMo, Inc." ou="BusinessmoperaGPSLocation CA - G2"	PrintableString 型で記載。
subjectPublicKeyInfo (主体者の公開鍵)		
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	rsaEncryption を示す。
subjectPublicKey (公開鍵)	...	主体者の公開鍵。2048 ビット長。

【拡張領域】

領域名	Critical フラグ	設定値(例)	補足説明
basicConstraints (基本制約)	TRUE		
cA		TRUE	認証局であることを示す。
pathLenConstraint		0	
subjectKeyIdentifier (主体者鍵識別子)	FALSE	...	主体者の公開鍵の SHA-1 ハッシュ値。
authorityKeyIdentifier (認証局鍵識別子)	FALSE		
keyIdentifier		...	ルート認証局の公開鍵の SHA-1 ハッシュ値。
keyUsage (鍵使用法)	TRUE	keyCertSign, cRLSign	
subjectAltName (主体者別名)	FALSE	...	PrintableString 型で記載。
cRLDistributionPoints (CRL配布点)	FALSE		
distributionPoint		"http://onsitecrl.s ymauth.jp/ARL/NTTDo CoMoIncBusinessmope raGPSLocationRootCA G2/LatestARL.crl"	URI にて記載。
Netscape Cert Type (ネットスケープ証明書型)	FALSE	SSL CA, S/MIME CA	

7.2.1 証明書利用者(GPS サービス提供者)

第二世代(G2)証明書利用者の電子証明書プロファイルを規定します。

【基本領域】

領域名	設定値(例)	補足説明
version (X.509 のバージョン)	2	X.509 バージョンが3であることを示す。
serialNumber (発行番号)	...	ユニークな値。
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す。
issuer (発行者名)	c="JP" o="NTT DoCoMo, Inc." ou="BusinessmoperaGPS Location CA - G2"	PrintableString 型で記載。
validity (有効期間)		原則3年有効(1095 日間)。
notBefore (開始日)	YYMMDDHHMMSS (年月日時分秒)	UTC 時刻型(UTCTime)で記載。
notAfter (終了日)	YYMMDDHHMMSS (年月日時分秒)	UTC 時刻型(UTCTime)で記載。
subject (主体者名)	c="JP" o="NTT DoCoMo, Inc." ou="BusinessmoperaGPS Location CA Client - G2" cn=<IP アドレス>	PrintableString 型で記載。
subjectPublicKeyInfo (主体者の公開鍵)		
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	rsaEncryption を示す。
subjectPublicKey (公開鍵)	...	主体者の公開鍵。2048 ビット長。

【拡張領域】

領域名	Critical フラグ	設定値(例)	補足説明
basicConstraints (基本制約)	FALSE		
cA		FALSE	認証局でないことを示す。
keyUsage (鍵使用法)	FALSE	digitalSignature, keyEncipherment	
cRLDistributionPoints (CRL配布点)	FALSE		
distributionPoint		"http://onsitecrl.s ymauth.jp/NTTDoCoMo IncBusinessmoperaGP SLocationCAClientG2 /LatestCRL.crl"	URI にて記載。

7.2.2 証明書利用者(ドコモ装置管理者)

第二世代(G2)証明書利用者の電子証明書プロファイルを規定します。

【基本領域】

領域名	設定値(例)	補足説明
version (X.509 のバージョン)	2	X.509 バージョンが3であることを示す。
serialNumber (発行番号)	...	ユニークな値。
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す。
issuer (発行者名)	c="JP" o="NTT DoCoMo, Inc." ou="BusinessmoperaGPS Location CA - G2"	PrintableString 型で記載。
validity (有効期間)		原則3年有効(1095 日間)。
notBefore (開始日)	YYMMDDHHMMSS (年月日時分秒)	UTC 時刻型(UTCTime)で記載。
notAfter (終了日)	YYMMDDHHMMSS (年月日時分秒)	UTC 時刻型(UTCTime)で記載。
subject (主体者名)	c="JP" o="NTT DoCoMo, Inc." ou="BusinessmoperaGPS Location CA Gateway - G2" cn="61.195.223.182"	PrintableString 型で記載。
subjectPublicKeyInfo (主体者の公開鍵)		
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	rsaEncryption を示す。
subjectPublicKey (公開鍵)	...	主体者の公開鍵。2048 ビット長。

【拡張領域】

領域名	Critical フラグ	設定値(例)	補足説明
basicConstraints (基本制約)	FALSE		
cA		FALSE	認証局でないことを示す。
keyUsage (鍵使用法)	FALSE	digitalSignature, keyEncipherment	
cRLDistributionPoints (CRL配布点)	FALSE		
distributionPoint		"http://onsitecrl.s ymauth.jp/NTTDoCoMo IncBusinessmoperaGP SLocationCAGatewayG 2/LatestCRL.crl"	URI にて記載。

7.2.3 Critical にセットされた拡張子に対するポリシー

規定しません。

7.3 ARL/CRL プロファイル

本節では失効情報（ARL、CRL）のプロファイルを規定します。

7.3.1 ARL (Authority Revocation List)

認証局失効リスト（ARL）のプロファイルを規定します。

【基本領域】

領域名	設定値(例)	補足説明
version (X.509 バージョン番号)	1	X509 バージョンが 2 であることを示す。
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	sha256WithRSAEncryption を示す。
issuer (発行者名)	c="JP" o="NTT DoCoMo, Inc." cn="Business mopera GPS Location Root CA - G2"	PrintableString 型で記載。
thisUpdate (今回の更新日時)	YYMMDDHHMMSS (年月日時分秒)	UTC 時刻型で記載。
nextUpdate (次の更新期限)	YYMMDDHHMMSS (年月日時分秒)	ルート認証局と同じ期間 UTC 時刻型で記載。
revokedCertificates (失効した電子証明書のリスト)		
userCertificate (失効した電子証明書)	...	失効した電子証明書の発行番号 (serialNumber)。
revocationDate (失効日時)	YYMMDDHHMMSS (年月日時分秒)	失効処理が行われた日時。 UTC 時刻型で記載。

【拡張領域 (crlExtensions / 失効リスト拡張領域)】

領域名	Critical フラグ	設定値(例)	補足説明
authorityKeyIdentifier (認証局鍵識別子)	FALSE		
keyIdentifier		...	ルート認証局の公開鍵の SHA-1 ハッシュ値
crlNumber (CRL 番号)	FALSE	...	CRL の通し番号

【拡張領域 (crlEntryExtensions / 失効リストエントリ拡張領域)】

領域名	Critical フラグ	設定値(例)	補足説明
reasonCode (失効理由)	FALSE	...	失効理由

7.3.2 CRL (Certificate Revocation List)

証明書失効リスト (CRL) のプロファイルを規定します。

【基本領域】

領域名	設定値(例)	補足説明
version (X.509 バージョン番号)	1	X.509 バージョンが2であることを示す。
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	sha256WithRSAEncryption を示す。
issuer (発行者名)	c="JP" o="NTT DoCoMo, Inc." ou="Business mopera GPS Location CA - G2"	PrintableString 型で記載。
thisUpdate (今回の更新日時)	YYMMDDHHMMSS (年月日時分秒)	24 時間で更新。 UTC 時刻型で記載。
nextUpdate (次の更新期限)	YYMMDDHHMMSS (年月日時分秒)	thisUpdate + 96 時間。 UTC 時刻型で記載。
revokedCertificates (失効した電子証明書のリスト)		
userCertificate (失効した電子証明書)	...	失効した電子証明書の発行番号 (serialNumber)。
revocationDate (失効日時)	YYMMDDHHMMSS (年月日時分秒)	失効処理が行われた日時。 UTC 時刻型で記載。

【拡張領域 (crlExtensions / 失効リスト拡張領域)】

領域名	Critical フラグ	設定値(例)	補足説明
crlNumber (CRL 番号)	FALSE	...	CRL の通し番号

【拡張領域 (crlEntryExtensions / 失効リストエントリ拡張領域)】

領域名	Critical フラグ	設定値(例)	補足説明
reasonCode (失効理由)	FALSE	...	失効理由

8. CPS の管理

8.1 CPS の変更

ドコモは、GPS サービス提供者の事前の承諾なしに随時、本 CPS を変更することができます。
ドコモは、本 CPS を変更した場合、本 CPS の修正版または変更部分を GPS サービス提供者に通知または提供します。

GPS サービス提供者は、ドコモより通知または提供された変更後の本 CPS に従わなければならないものとします。

8.2 公表と通知に関する方針

GPS サービス提供者は本サービスを利用するにあたって、事前に本 CPS を受領することができます。また、GPS サービス提供者は本サービスの利用中に、本 CPS の最新版を受領することができます。

ドコモは本サービスを実施するにあたり、必要な社内規程を定め、これに従い業務を実施します。ただし、これらの規定について原則として公開しません。

8.3 CPS の承認手順

本 CPS の変更にかかる承認手順は8.1節を参照してください。