認証局運用規定(CPS)

目次

1. はじめに

この文書は、EU-Create（以下、当方と記す）が自分で電子証明書（以下、証明書と記す）を発行するためのプライベート認証局の運用規定を定めたものです。当方の証明書の発行・運用は、この文書の記述にそって実行されています。

なお、この文書の記述は表紙に記載された日付において最新版であり、適宜改定されることがありますので、最新版をご覧になる方は当方ホームページ（http://www.eu-create.net/）よりダウンロードしてくださるようお願い致します。

1.1. 概要

当方は、以下の三種類の証明書を発行します。

(1) ルート証明書：当方が発行する証明書の基本（ルート）となる証明書です。
お客様やお取り引き企業様のパソコンにインストールして頂く証明書でもあるため、当方より直接お受け取りになるか、当方ホームページよりダウンロードをお願い致します。

(2) 個人証明書：当方々員が社員証として使用する証明書で、お客様やお取り引き企業様に当方々員であることを証明した「電子署名メール」を送る際などに使用します。

また、当方が発行する失効リストは、以下の一種類です。

(3) 失効リスト：証明書の紛失などにより、無効となった証明書の一覧です。

1.2. 識別

当方が発行する証明書は、以下の情報にて当方の証明書であることを識別することができます。

(1) 発行者：証明書の発行者フィールドに、当方の名称と住所が記載されています。

(2) 拇印：証明書の拇印（指紋）フィールドに、証明書固有の情報が記載されています。

1.3. 範囲

当方が発行する証明書は、以下の範囲内にてのみ有効です。

(1) ルート証明書：当方の発行する個人証明書の電子署名（または電子メールの暗号化）のみに使用します。

(2) 個人証明書：当方であることを証明した電子署名（または電子メールの暗号化）メールは Thunderbird より送信されます。

1.4. 連絡先

当方が発行する証明書に関する連絡は、下記の通りとなります。

認証局・電子証明書 発行担当
氏　　名：内堀 英一
メールアドレス：info@eu-create.net

2. 一般規定

2.1. 義務

当方は認証局を運営するにあたり、以下の義務を負っています。

(1) 紛失・盗難時に、失効リストを発行します。

(2) 証明書の日常での取り扱いを行います。

なお、お客様やお取り引き企業様においては、失効リストによる証明書の有効性確認をお願い致します。

2.2. 責務

証明書に使用される暗号理論などの技術において隠れた瑕疵があったとき、当方ではその一切の責務を負わないこととしています。

2.3. 責任

当方が発行する証明書において、その運用責任は以下の通りと致します。

(1) 当方が発行したルート証明書を、お客様やお取り引き企業様がお使いのパソコンにインストールされていなければ、当方は証明書に帰責する一切の責任を負いません。

(2) 第三者がその証明書を取得し、悪意を持って使用し損害が発生した場合、その時までに当方が失効リストを作成し公開していなければ当方がその責任を負うこととします。

(3) 上記の場合において、当方が失効リストを作成し公開しても、お客様やお取り引き企業様がお使いのパソコンに失効リストを反映されていなければ、当方はその責任を負いません。

(4) お客様やお取り引き企業様がお使いのパソコンに失効リストを反映されていてなお、何らかの損害が発生した場合、それは証明書によるものと認められませんので、別途規定により協議致します。

2.4. 解釈と実行

この文書の内容は、日本国の法令および規則に基づき解釈され、実行されます。

2.5. 料金

当方が発行する証明書は、当方が行う業務の一環であり、料金は発生致しません。

2.6. 公開とリポジトリ

この文書および当方が発行する証明書・失効リストの情報は、当方ホームページにて公開しています。なお、公開に際してのアクセス制限などは行っておりません。

失効リストの公開は、毎月１日（１日が土日祝日の場合は翌営業日）に行うほか、緊急に際しては随時公開し、その旨をホームページにて通知致します。

2.7. 準拠性監査

当方は証明書の発行・運営を、この文書に準拠して実施していることを定期的に監査しています。

監査は当方の責任者もしくはそれに準ずる者が行い、この文書に準拠していなければその是正を行います。

2.8. 機密保持

当方が運営する認証局においては、当方の個人を特定するための情報および秘密鍵を機密情報と定義しますが、名前およびメールアドレスなどの証明書に記載する内容は機密情報の対象外と致します。また、失効リストの発行において、失効理由などの失効リストに記載される内容も同様とします。

なお、警察その他の法的機関より書面による開示請求があった場合には、機密情報を開示することがあります。

2.9. 知的財産権

当方が運営する認証局および発行する証明書の知的財産権の規定は行っていません。

3. 識別と認証

3.1. 初期登録

当方の証明書は当方に対して発行するため、証明書発行に際しては特別に識別・認証を行うことはありません。

なお、個人証明書に記載される住所は所属部署の住所、氏名は証明書発行時点のものとします。

3.2. 鍵の更新

証明書および鍵の更新手順については、特に規定しません。

3.3. 失効後の鍵更新

「３．２．鍵の更新」と同様とします。

3.4. 失効要求

「３．２．鍵の更新」と同様とします。

4. 運用要件

4.1. 証明書適用

当方が発行する証明書は当方々員に対するものですので、適用要件を特に規定はしません。

4.2. 証明書発行

「４．１．証明書適用」と同様とします。

4.3. 証明書受け入れ

「４．１．証明書適用」と同様とします。

4.4. 証明書失効

当方では、以下の場合に証明書の失効を行い、失効リストにその理由を記載します。

(1) 当方が証明書を漏洩・紛失の場合に、「エンドエンティティのキーが危害を受けた」を理由として失効リストを作成します。

(2) Web サービスを終了または中止した場合に、「利用中止」を理由として失効リストを作成します。

(3) その他の場合に、理由なしで失効リストを作成します。

4.5. セキュリティ監査手続き

当方では証明書の発行に際して、すべての事象をログに記録し保管しています。ログにはコンピュータ名、アカウント、日時、事象の内容などを暗号化して保存し、改ざんが発見された場合にはすべての証明書が失効されます。

4.6. 記録の保管

当方では、発行した証明書と認証局情報、ログを定期的にバックアップし、保管しています。認証局情報およびログは暗号化し、改ざんが発見された場合にはすべての証明書が失効されます。

4.7. 鍵の切り替え

ルート証明書の鍵の切り替えは、以前の鍵の有効期間が終了する一ヶ月前より新たなルート証明書をホームページからダウンロード可能とし、その旨を掲載致します。

4.8. 鍵の危殆と災害回復

管理データーベースおよびログなどに不整合が発生し秘密鍵などの危殆が懸念される場合には、ルート証明書を含むすべての証明書を失効させ、新たなルート証明書により運用を再開致します。

なお、予期せぬパソコンの破損、バックアップの不備、その他の災害により失効リストの発行そのものができない場合には、ホームページにてその旨を通知いたしますので、お客様やお取り引き企業様ご自身にてルート証明書のアンインストールを実施願います。

4.9. 認証局の終了

当方の倒産・整理など止むを得ない事情により、認証業務を終了することがあります。

5. 物理的手続き、個人のセキュリティ制御

5.1. 物理セキュリティ制御

証明書を発行するシステムは、証明書の発行業務が必要となった時にのみセキュリティ対策を施したパソコンに接続して実施致します。

5.2. 手順制御

証明書を発行するシステムは、当方の社印と同じ扱いとし、それを捺印する権限のある管理職に許可を得て、その管理下で実行します。

証明書の発行後はすみやかにパソコンから切り放し、管理職の手により保管を行います。

5.3. 個人のセキュリティ制御

証明書を発行された者は、当方が承認した保管方法にて証明書を管理し、外には持ち出さないこととしています。

6. 技術的セキュリティ制御

6.1. 鍵生成とインストール

鍵の生成および証明書の発行までの一連の操作は担当者が一括して行い、証明書とパスワードは別々の媒体に記録して直接手渡します。

6.2. 秘密鍵保護

当方の秘密鍵はソフトウェアにて生成されるため、ハードウェア保護規定はありません。

6.3. 鍵生成管理に関する他の局面

証明書の発行システムと鍵ペア・証明書は、オフライン上の媒体に活性化された状態で格納されています。

6.4. 活性化データ

「６．３．鍵生成管理に関する他の局面」と同様とします。

6.5. コンピュータセキュリティ制御

証明書を作成するパソコンは、市販のセキュリティソフトによりウィルスおよびマルウェアから保護されており、証明書の発行時にはオフライン化によりハッキングと盗聴を防ぎます。

6.6. ライフサイクルセキュリティ制御

ライフサイクルセキュリティは、“電子証明書作成ソフトウェア「k9pca」”に依存します。

6.7. ネットワークセキュリティ制御

「６．５．コンピュータセキュリティ制御」と同様とします。

6.8. 暗号モジュールのエンジニアリング制御

「６．６．ライフサイクルセキュリティ制御」と同様とします。

7. 証明書と CRL プロフィール

7.1. 証明書プロフィール

当方が発行する証明書は、以下のフォーマット形式です。

(1) バージョン：V3

(2) 証明書拡張とその重要度：「証明書ポリシー」「CRL 配布ポイント」「機関情報アクセス」があり、いずれも非重要（non-criticality）です。

(3) 署名アルゴリズム：RSA および SHA-1 を使用しています。

(4) 名前形式：「Printable string」または「UTF-8 string」になっています。

(5) 名前制限：200 文字以内に制限されています。

7.2. CRL プロフィール

当方が発行する失効リストは、以下のフォーマット形式です。

(1) バージョン：V2

(2) 証明書拡張とその重要度：「理由コード」「無効日」「機関識別子」があり、いずれも非重要（non-criticality）です。

(3) 署名アルゴリズム：RSA および SHA-1 を使用しています。

8. 仕様書の管理

すべての仕様変更は、“電子証明書作成ソフトウェア「k9pca」”に依存します。

発効日：2019 年 1 月 20 日 第 1.00 版
発行者：EU-Create
問合せ：info@eu-create.net