COMODO 認証局運用規程

Comodo Group
Version 3.0
22 September 2006
New Court, Regents Place, Regent Road,
Manchester M5 4HB United Kingdom,
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
www.comodogroup.com

目次

Comodo 認証局運用規程（以下、本 CPS という）で使用する頭字語の正式名称及び和訳を以下に示す。

CA	Certificate Authority（認証局）
CPS	Certification Practice Statement（認証局運用規程）
CRL	Certificate Revocation List（証明書失効リスト）
CSR	Certificate Signing Request（証明書署名リスクエスト）
EPKI	Enterprise Public Key Infrastructure Manager（EPKI は製品名）
FTP	File Transfer Protocol（ファイル・トランスファー・プロトコル）
HTTP	Hypertext Transfer Protocol（ハイパーテキスト・トランスファー・プロトコル）
ITU	International Telecommunication Union(国際電気通信連合)
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector（国際電気通信連ー電気通信セクタ）
PKI	Public Key Infrastructure(公開鍵基盤)
PKIX	Public Key Infrastructure X.509(和訳対応無し。（PKIX は、インターネットに関連する技術の標準化を行っている団体である IETF（Internet Engineering Task Force）のワーキンググループの 1 つである。本書での PKIX とは、同ワーキンググループが X.509 に基づいて定めた PKI を利用するうえでの各種標準をいう。））
PKCS	Public Key Cryptography Standard(公開鍵暗号規格)
RA	Registration Authority(登録局)
SSL	Secure Sockets Layer(セキュア・ソケット・レイヤー)
TLS	Transport Layer Securrity（トランスポート・レイヤー・セキュリティ）
URL	Uniform Resource Locator（和訳対応無し）
X.509	X.509（和訳対応無し（X.509 は、ITU-T が定めた公開鍵証明書に関する仕様である。）

本 CPS で使用する用語の定義を以下に示す。

申請者	証明書の申請を行う個人または企業である。
加入者	証明書の発行を受ける個人または企業である。
信頼者	加入者の証明書を信頼する個人または企業である。
加入者利用規約	証明書を申請する前に、申請者が読み、承諾する必要のある契約である。加入者利用規約は証明書の種類ごとに存在し、オンライン申請時に確認できるほか、www.comodogroup.com/repository で参照可能である。
信頼者利用規約	証明書の検証・利用、あるいは Comodo のリポジトリへのアクセス・利用の前に信頼者が読み、承諾する必要のある契約である。www.comodogroup.com/repository で参照可能である。
証明書ポリシー	Comodo が定める証明書の使途に関する規程

概要

本書は Comodo 認証局の CPS であり、Comodo が証明書サービスを提供する上での法的・商的・技術的な遵守事項を定めるものである。これらの中には、電子証明書の発行承認、発行、使用、及び管理に関わる事項が含まれるが、この限りでない。また、Comodo が定める証明書ポリシーを遵守した PKIX を確保するための事項についても定められている。

さらに本書は、証明書ライフサイクルにおいて加入者が関係する各プロセスを定義し、Comodo のリポジトリの運用についても記述するとともに、Comodo PKI において証明書を利用する関係各位の役務と責任を明らかにする手段でもある。

1.1. Comodo について

Comodo は、本 CPS に基づいて、有限・株式会社や個人等に対し高品質で極めて信頼性の高い電子証明書を発行する CA である。Comodo が CA として担う役務は、Comodo PKI で証明書を使用するユーザーに対し、申請の受理、電子証明書の発行、失効、及び更新に加え、CRL の運用、発行、及び公開を含む、公開鍵の運用に関連する機能を果たすことである。PKI サービスを提供するにあたり、Comodo は European Directive99/9 に則った Qualified Certificate や、電子署名に関連する法律、及びその他の関連する法令や規制を含むハイレベルな国際基準に関し、あらゆる面において準拠するものである。

Comodo は、PKI を構成するメンバーとして、RA の機能を第三者に合意のもとで委託することがある。全世界にわたり存在する Comodo RA のネットワークは、Comodo のポリシーと各種規程、及び CA インフラストラクチャを共有して、Comodo 電子証明書、または、自社もしくは自身のプライベートブランドの電子証明書の発行を行う。

1.2. Comodo CPS について

Comodo CPS は、Comodo の運用、及び Comodo 独自の信頼階層の下で発行される証明書の発行、失効及び更新の条件を公式に表明する規程書である。本 CPS は、CA のタスクに準じ、技術、組織管理、運用、及び法的要件に大別されて記述されている。

本 CPS、本 CPS において参照される契約（規約）及び証明書ポリシーは、Comodo Certificate Policy Authority によって維持される。Certificate Policy Authority の連絡先を以下に示す。

Certificate Policy Authority
3 rd Floor,Office Village,Exchange Quay,Trafford Road
Solidford,Manchester,M5 3EQ,United Kingdom
Tel: +44 (0) 161 874 7070, Fax: +44 (0) 161 877 1767

Attention: Legal Practices

Email: legal@comodogroup.com

本 CPS 及び本 CPS において参照される規約及び証明書ポリシーは、Web サイト www.comodogroup.com/repository から入手することもできる。

1.3. Comodo CPS の適合性、改訂及び公開について

Certificate Policy Authority は、本 CPS で説明される証明書ポリシーの適合性を判断する責任を有する。また、Certificate Policy Authority は、改訂版の公開に先立ち、本 CPS の改訂案の適合性を判断する責任も有する。

本 CPS のユーザーに重大な影響を与えるものと CA の Policy Authority が判断した改訂案が、Certificate Policy Authority によって承認されると、正式な改訂版となる前の 30 日間は Comodo リポジトリ（www.comodogroup.com/repository）に公開され、改訂箇所が公表される。この時、改訂版であることが識別できるようにするため、バージョン番号を付番する。

加入者や、CA が発行する証明書や CRL を利用する信頼者に対し、改訂案の与える影響が極めて軽微もしくは皆無であると CA の Policy Authority が判断した場合、改訂はユーザーへの事前通知なく、また、CPS のバージョンを変更せずに行うことができる。

また、Comodo は、事前に Certificate Policy Authority の承認を得ずに Comodo CPS が改訂されたり、公開されたりしないことを合理的に保証するために、CPS の適切な管理を行うものとする。

1.4. その他の規程及び規約

本 CPS は、Comodo の証明書サービスの提供に関連する一連の文書の一つにすぎない。本節に含まれる文書の一覧は、本 CPS が都度言及することのあるその他の文書を示しているが、全てを網羅しているわけではない。下表において、これら文書の名称、参照場所、機密レベルを示す。

ドキュメント名	機密レベル	参照場所
Comodo Certification Practice Statement（本書）	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Digital Certificate Terms and Conditions		
Relying Party Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Instant SSL Pro Certificate Subscriber Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Premium SSL Certificate Subscriber Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Premium SSL Certificate Subscriber Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Premium SSL Wildcard Certificate Subscriber Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Intranet Certificate Subscriber Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Trial SSL Certificate Subscriber Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Secure Email Certificate Subscriber Agreement	公開	Comodo リポジトリ内：www.comodogroup.com/repository
Enterprise Public Key Infrastructure Manager Agreement	非公開	パートナーへ適宜提出
Web ホストリセラー Agreement	非公開	パートナーへ適宜提出
Reseller Agreement	非公開	パートナーへ適宜提出
Powered SSL Partner Agreement	非公開	パートナーへ適宜提出
Enterprise Public Key Infrastructure Manager Guide	非公開	パートナーへ適宜提出
Web ホストリセラー Guide	非公開	パートナーへ適宜提出
Reseller Guide Powered SSL	非公開	パートナーへ適宜提出
Partner Guide	非公開	パートナーへ適宜提出
Web ホストリセラー Validation Guidelines	非公開	パートナーへ適宜提出

1.5. Comodo の義務

本 CPS が定める Comodo の法的義務については、第 5 章「発行に関する法的義務」を参照すること。

1.6. 規格への準拠性

本 CPS の規程は、AICPA/CICA Web Trust Program for Certification Authorities、ANS X9.79:2001 PKI Practies and Policy Framework といった規格の他、CA の運用上一般的に遵守すべき業界標準に対し、これらの要件を満たすか、もしくは上回るよう策定されている。

AICPA/CICA Web Trust Program for Certification Authorities への準拠性監査については、独立した外部の監査機関によって毎年行われる。この年次監査の対象となる項目を以下に示すが、これらに限られるものではない。

- ビジネス実務の規程
- サービス・インテグリティ
- CA 設置環境の管理

1.7. 電子証明書ポリシーの概要

電子証明書は、本人確認が済んだ加入者と公開鍵を、暗号的に結びつける形式化されたデータである。電子証明書の使用により、電子的なトランザクションに参加する者は、トランザクションに参加している他者に対し、自身の本人性を証明することができる。電子証明書は、通常の商環境で使用される身分証明書のデジタル版である。

本 CPS に詳述の通り、Comodo は多様な証明書を提供している。各証明書は、使途やポリシーが異なっている。

申請者	証明書の種類	入手方法	審査レベル[*1]	推奨される用途
個人または企業	Secure Server Certificate: InstantSSL	-Comodo Web サイト -リセラーネットワーク -Web ホストネットワーク -Powered SSL ネットワーク -EPKI マネージャー	申請の際に使用された企業名の使用権に加え、申請されたドメイン名の使用権の確認について、第三者機関の DB、ビジネス文書の両方もしきはいずれかにより行う。最初に IdAuthority の DB を使用するが、十分な情報が得られない場合は、審査員が個別に確認を行う。	Secure Server Certificate をインストールしたサーバと、クライアント/顧客/Web サイトの利用者の間での SSL/TLS セッション。このプロトコルは、クライアントに対しサーバの認証を提供し、SSL/TLS セッションでやり取りされるデータの機密性を確保する。
個人または企業	Secure Server Certificate: InstantSSL Pro	-Comodo Web サイト	申請の際に使用された企業名の使用権に加え、申請されたドメイン名の使用権の確	Secure Server Certificate をインストールしたサーバと、クライアント/顧客/Web サイトの利用者の間での SSL/TLS セッション。こ

[1] 審査レベル：審査は、Comodo または Comodo の登録局（Web ホストリセラーまたは Powered SSL パートナーを通じて証明書を申し込んだ場合）が、厳格なガイドラインに基いて行う。本 CPS の第 1.9 節において登録局の定義と、その役割と責任について概説する。

		-リセラーネットワーク -Web ホストネットワーク -Powered SSL　ネットワーク -EPKI マネージャー	認について、第三者機関のDB、ビジネス文書の両方もしきはいずれかにより行う。最初に IdAuthority　の DB を使用するが、十分な情報が得られない場合は、審査員が個別に確認を行う。	のプロトコルは、クライアントに対しサーバの認証を提供し、SSL/TLS セッションでやり取りされるデータの機密性を確保する。
個人または企業	Secure Server Certificate: Premium SSL	-Comodo Web サイト -リセラーネットワーク -Web ホストネットワーク -Powered SSL　ネットワーク -EPKI マネージャー	申請の際に使用された企業名の使用権に加え、申請されたドメイン名の使用権の確認について、第三者機関のDB、ビジネス文書の両方もしきはいずれかにより行う。最初に IdAuthority　の DB を使用するが、十分な情報が得られない場合は、審査員が個別に確認を行う。	Secure Server Certificate をインストールしたサーバと、クライアント/顧客/Web サイトの利用者の間での SSL/TLS セッション。このプロトコルは、クライアントに対しサーバの認証を提供し、SSL/TLS セッションでやり取りされるデータの機密性を確保する。
個人または企業	Secure Server Certificate: Premium SSL Wildcard	-Comodo Web サイト -リセラーネットワーク -Web ホストネットワーク -Powered SSL　ネットワーク -EPKI マネージャー	申請の際に使用された企業名の使用権に加え、申請されたドメイン名の使用権の確認について、第三者機関のDB、ビジネス文書の両方もしきはいずれかにより行う。最初に IdAuthority　の DB を使用するが、十分な情報が得られない場合は、審査員が個別に確認を行う。	Secure Server Certificate をインストールしたサーバと、クライアント/顧客/Web サイトの利用者の間での SSL/TLS セッション。このプロトコルは、クライアントに対しサーバの認証を提供し、SSL/TLS セッションでやり取りされるデータの機密性を確保する。
個人または企業	Secure Server Certificate: Intranet SSL	-Comodo Web サイト -リセラーネットワーク -Web ホストネットワーク -Powered SSL　ネットワーク -EPKI マネージャー	申請項目の一部である Common Name にプライベート IP アドレスのみが含まれていることを自動的に確認する。	Secure Server Certificate をインストールした内部ネットワーク向けのサーバと、内部ネットワーク内のクライアントマシンとの間での SSL/TLS セッション。このプロトコルは、クライアントに対しサーバの認証を提供し、SSL/TLS セッションでやり取りされるデータの機密性を確保する。
個人または企業	Secure Server Certificate: TrialSSL	-Comodo Web サイト -リセラーネットワーク -Web ホストネットワーク -Powered SSL　ネットワーク -EPKI マネージャー	申請の際に使用された企業名の使用権に加え、申請されたドメイン名の使用権の確認について、第三者機関のDB、ビジネス文書の両方もしくはいずれかにより行う。最初に IdAuthority　の DB を使用するが、十分な情報が得られない場合は、審査員が個別に確認を行う。	Secure Server Certificate をインストールしたサーバと、クライアント/顧客/Web サイトの利用者の間での SSL/TLS セッション。このプロトコルは、クライアントに対しサーバの認証を提供し、SSL/TLS セッションでやり取りされるデータの機密性を確保する。
非営利目的で使用する個人	Secure Email Certificate:	-Comodo Web サイト -リセラーネットワーク	Comodo PKI 内に確かに存在し、唯一であることを保証するため、メールアドレスの検索を行う。電子メールアドレス所有者の確認は、自動	証明書の所有者は電子メールへの電子的な署名や、暗号化を行うことができる。証明書の信頼者は電子署名が施された電子メールの検証を行うことができる。また、証明書所有者の本人確認を別途実施する必要

	Free Version		的、取得プロセスの一環として行われる。	がなければ、Web ベースのアクセスコントロールとして利用することもできる。
営利目的で使用する企業の者	Secure Email Certificate: Corporate Version	-EPKI マネージャー	EPKI アカウントの開設に際し、申請者は、申請した企業名の使用権を有することを、第三者機関の DB、ビジネス文書の両方もしくはいずれかにより証明しなければならない。また、EPKI マネージャーアカウント内に確かに存在し、唯一であることを保証するため、メールアドレスの検索を行う。EPKI マネージャーアカウントの運営管理を行う企業は、企業用セキュア電子メール証明書の発行に先立って行われる確認の際に、使用するドメイン名を申請する義務がある。	証明書の所有者は電子メールへの電子的な署名により、企業の代表者であることの証明や、暗号化を行うことができる。証明書の信頼者は電子署名が施された電子メールの検証を行うことができる。また、証明書所有者の本人確認を別途実施する必要がなければ、Web ベースのアクセスコントロールとして利用することもできる。

電子証明書の使用方法は、使用するアプリケーションごとに異なるため、加入者は Comodo の証明書を申し込む前に、使用上必要な条件を十分に調査・検討する必要がある。

1.8. Comodo PKI の階層

Comodo PKI の信頼階層を以下に記す。

1.8.1. Entrust 証明書

Entrust.net Secure Server Certification Authority (シリアルナンバー = 37 4a d2 43、有効期限 = 2019 年 5 月 25 日)

↳ Entrust Comodo 中間 CA (シリアルナンバー ならびに有効期限 は後記)

↳ End Entity SSL/End Entity Secure Email (シリアルナンバー = x、有効期限 = 発効日より 1、2、または 3 年)

1.8.2. GTE 証明書

GTE CyberTrust Root (シリアルナンバー = 01A5, 有効期限 = 2018 年 8 月 14 日)

↳ Comodo Class3 Security Services CA (シリアルナンバー = 0200 029B、有効期限 = 2006 年 2 月 23 日)

↳ End Entity SSL/End Entity Secure Email (シリアルナンバー = x、有効期限 = 発効日より 1、2、または 3 年)

注:日本コモドが発行する証明書は、Comodo Class3 Security Services CA に代わり、以下を使用する。

Comodo Japan CA (シリアルナンバー = 0400 0382、有効期限 = 2012 年 8 月 27 日)

1.8.3. UTN/Addtrust 証明書

1.8.3.1. IE 互換ブラウザ上における見え方

UTN=USERFirst-Hardware（シリアルナンバー = 44 be 0c 85 50 00 24 b4 11 d3 36 2a fe 65 0a fd , 有効期限 = 2019 年 7 月 10 日）

↳ End Entity SSL/End Entity Secure Email（シリアルナンバー = x、有効期限 = 発効日より 1、2、または 3 年）

1.8.3.2. Netscape 互換ブラウザ上における見え方

クロスチェーンしており、NetScape 互換ブラウザ上では、以下のように見える

AddTrust External CA Root（シリアルナンバー = 01、有効期限 = 2020 年 5 月 30 日）

↳ UTN=USERFirst-Hardware（シリアルナンバー = 44 be 0c 85 50 00 24 b4 11 d3 36 2a fe 65 0a fd , 有効期限 = 2019 年 7 月 10 日）

↳ End Entity SSL/End Entity Secure Email（シリアルナンバー = x、有効期限 = 発効日より 1、2、または 3 年）

1.9. Comodo 認証局（CA）

Comodo は CA として、Comodo PKI において証明書サービスを提供する。このために Comodo CA は以下を行う。

- CPS（またはそれ以外の CA 業務の規程）への準拠。なお、改訂により CPS が変更される場合は、Comodo のリポジトリ（www.comodogroup.com/repository/）で公開される改訂版に準拠するものとする。
- 本 CPS に規定の発行時間に基づく適時な証明書の発行と公開。
- 証明書の失効申請を許可されている担当者から申請された証明書失効申請の受理後、本 CPS に記載の失効手順に従って、Comodo PKI で使用するために発行された証明書を失効する。
- 適用される証明書ポリシー及び本 CPS に記載の条項に基づく定期的な CRL の発行。
- 本 CPS に記載の手順に基づいた証明書の配付。
- 本 CPS に記載された手順に基づく適時な CRL の更新。
- 電子メールによる Comodo が発行した証明書の有効期限の加入者への通知（本 CPS に開示された期間）

1.10. Comodo 登録局（RA）

Comodo PKI における電子証明書のライフサイクルを完全に管理するため、Comodo は必要なセキュア・インフラストラクチャを確立している。また、RA のネットワークを介し、Comodo の加入者が、CA サービスを使用することも可能としている。以下に Comodo RA の役割を示す。

- 証明書申請の受理、審査、発行もしくは拒否。
- Comodo の審査ガイドラインに則して行う、申請者が提供した情報の正確性と信頼性の確認。

- 申請者の審査に要する正式で公的な文書、あるいは他の文書を使用
- Comodo の審査ガイドライン文書に則して行う、再発行または更新時に加入者が提供した情報の正確性と信頼性の確認。

Comodo　RA は、Comodo の定める規程と手順に従い、Comodo より承認と認可を受けた地理的またはパートナーシップの範囲内で実務を行う。

Comodo は、Web ホストリセラー、Enterprise Public Key Infrastructure（EPKI）、及び Powered SSL プログラムに対する RA の使用を認める。各プログラムへの加盟が承認されると、Web ホストリセラーの加入者、EPKI Manager の加入者、またはパワード SSL の加入者は、Comodo の代わりに、RA として機能することが許可される。RA がプログラムに参加した暁には、RA は Comodo から発行された審査ガイドラインの範囲内に限定して運用を行う。これらの RA を介して発行された証明書は、RA が介在したことを信頼者に明示すために証明書プロファイルが変更されて発行される。

1.10.1. リセラー・パートナー

Comodo はリセラー・パートナー・ネットワークを展開し、認定されたパートナーのプロダクト・ポートフォリオに Comodo の電子証明書を統合することを認める。リセラー・パートナーは、申請受付、発行、更新、及び失効を含む証明書ライフサイクルの全過程を管理下におき、PKI を管理する Comodo に対し、電子証明書の顧客を照会させる責任を有する。リセラー・プログラムの性質上、リセラーは、リセラーのアカウントを通じて申請された保留中の顧客の申請について、Comodo がその証明書の審査に着手する前に承認する必要がある。全てのリセラー・パートナーは、企業のステータスを証明するもの（必要文書の例については第 4.3.2 項を参照）を Comodo に提示する必要がある他、Comodo リセラー・パートナー契約を締結する必要がある。

1.10.2. Web ホスト・リセラー・パートナー

Web ホスト・リセラー・パートナー・プログラムは、ホスティング・サービスを提供する企業が、同サービスを利用する顧客に代わり、証明書のライフサイクルを管理できるプログラムである。パートナーは、顧客に代わり Secure Server Certificate を申請できる。

「Management Area」と呼ばれる「フロントエンド」を介することで、Web　ホスト・リセラー・パートナーは、Secure Server Certificate の発行を含む RA 機能へアクセスすることができる。Web ホスト・リセラー・パートナーは、契約の一部として Comodo が提供する審査ガイドラインに記載の審査プロセスを厳守するものとする。Web ホスト・リセラー・パートナーは、審査ガイドラインに基づいて審査を行う義務を有し、また、証明書の発行に先立ち、オンライン上での手続きを通じて、十分な審査を行うことに合意する（「I have sufficiently validated this application」チェックボックスを証明書の申請時にチェックする）。

全ての Web ホスト・リセラー・パートナー は、企業のステータスを証明するもの（必要文書の例については第 4.3.2 項を参照）を Comodo に提示する必要がある他、Comodo Web ホスト・リセラー・パートナー契約を締結する必要がある。

1.10.3. EPKI マネージャー・アカウント保持者

Comodo EPKI マネージャーは、フル・アウトソースの企業向け PKI サービスで、承認された EPKI マネージャーのアカウント保持者が、企業のサーバ、イントラネット、エクストラネット、パートナー、従業員、及びハードウェアに使用する証明書の申請受付、発行、更新及び失効を含む、証明書ライフサイクルの全過程を管理する権限を与える。

「Management Area」と呼ばれる「フロントエンド」を介することで、EPKI マネージャーのアカウント保持者は、Secure Server Certificate 及び Corporate Secure Email Certificate の発行を含む RA 機能へアクセスすることができる。

EPKI マネージャーのアカウント保持者が証明書を発行する対象は、ドメイン名（サーバ）、イントラネット、エクストラネット、パートナー、従業員、及びハードウェアを含む正当な企業リソースに限定される。

1.10.4. Powered SSL パートナー

Comodo は、Comodo が定める規程やポリシーを遵守することを条件に、企業が個人や企業に対し独自のブランド名を付加して Secure Server Certifivate を発行できる Powered SSL サービスを展開する。同サービスは、様ざまな企業から構成され、国際的ネットワークを形成している。Comodo は、Powered SSL 証明書の審査、発行、更新、及び失効を含むがそれらに限定されないバックエンドにおける証明書ライフサイクルのあらゆる局面を管理する。但し、発行される証明書のプロファイルは、信頼者（最終的に証明書を利用する顧客）が Powered SSL を利用した企業の証明書であることを認識できるようにするために変更される。

「Management Area」として呼ばれる「フロントエンド」を介して、Powered SSL パートナーは、Web ホスト・リセラー・パートナーが使用する RA 機能へのアクセスや、リセラー・パートナーが使用する標準的なアカウント管理機能へのアクセスができる。Web ホスト・リセラーと同様に、Powered SSL パートナーは、契約の一部として Comodo が提示する審査ガイドラインに記載の審査プロセスを厳守するものとする。Powered SSL パートナーは、審査ガイドラインに基づいて審査を行う義務を有し、また、証明書の発行に先立ち、オンライン上での手続きを通じて、十分な審査を行うことに合意する（「I have sufficiently validated this application」チェックボックスを証明書の申請時にチェックする）。また、Powered SSL パートナーは、RA の役割を Comodo に委託することもできる。

全ての Powered SSL Partners は、企業のステータスを証明するもの（必要文書の例については第 4.3.2 項を参照）を Comodo に提示する必要がある他、Powered SSL パートナー契約を締結する必要がある。

1.11. 加入者

Comodo サービスの加入者は、Comodo がサポートするトランザクション及び通信と関連する PKI を使用する個人または企業である。加入者とは証明書の中で本人確認がされた主体であり、加入者の証明書に掲載されている公開鍵に対応する秘密鍵を所有する主体である。本人確認の審査と証明書の発行が行われるまで、加入者は Comodo のサービスの申請者と定義される。

1.12. 信頼者

信頼者は、Comodo の証明書に関連する PKI サービスを利用し、加入者の証明書と、加入者の証明書に実装されている公開鍵を参照することで検証できる電子署名の両方あるいはいずれかを合理的に信頼する。

信頼者が受理した証明書の有効性を検証するため、信頼者は証明書に記載されている情報を信頼する前に、証明書失効リスト（CRL）を参照し、Comodo が当該証明書を失効していないことを確認する必要がある。CRL の公開場所は証明書内に記載されている。

2. テクノロジー

本章は Comodo インフラストラクチャ及び PKI サービスの技術的な側面ついて取り扱う。

2.1. Comodo CA インフラストラクチャ

Comodo CA インフラストラクチャは、信頼できるシステムを使用して証明書サービスを提供している。信頼できるシステムとは、セキュリティリスクに対し許容できる柔軟性を有する他、合理的なレベルの可用性、信頼性、及び的確なオペレーションを提供し、かつセキュリティポリシーを実践できるコンピュータ・ハードウェア、ソフトウェア、及びプロシージャのことである。

2.1.1. Comodo Root CA 署名鍵のプロテクション及びリカバリ

Comodo は、鍵の生成、保存、及び使用のために FIPS140-1 レベル 4 認定の IBM 4578 暗号プロセッサー装置を使用することで、CA Root 署名鍵のプロテクションを確実なものとしている。CA Root 鍵ペアは、RSA アルゴリズムを用いて IBM 4578 装置内で生成された 2048 ビットの鍵ペアである。

鍵ナンバー	CA ナンバー	名称	用途	有効期間	鍵長
2	2	Class 1 Public Primary CA	Class1 中間 CA 署名用自己署名ルート CA	20 年	2048
.3	3	Class 2 Public Primary CA	Class2 中間 CA 署名用自己署名ルート	20 年	2048

			CA（現在商用利用はされていない）		
4	4	Class 3 Public Primary CA	Class3 中間 CA 署名用自己署名ルート CA	20 年	2048
5	5	Class 4 Public Primary CA	Class4 中間 CA 署名用自己署名ルート CA（現在商用利用はされていない）	20 年	2048
6	6	Comodo Class 1TTB 中間 CA	IDAuthority Website Certificate 用中間 CA	10 年	2048
7	7	Comodo Class 3 TTB/Verification Engine Intermediate CA	IdAuthority Premium、Card Payment 及び Verification Engine Certificate 用中間 CA	10 年	2048
8	8	Comodo Classs 1 Individual Subscriber CA （本人確認省略）	Class1 電子メール用中間 CA	10 年	2048
9	9	Comodo Class 3 Secure Server CA	SSL 証明書用中間 CA（現在商用利用はされていない）	10 年	2048
10	10	Comodo Class 3 Software Developer CA	コード署名証明書用中間 CA（現在商用利用はされていない）	10 年	2048
11	11	“Global Signed” Class 3 Security Services CA	SSL 証明書用中間 CA	2014 年 1 月 28 日まで有効	2048
16	11	“Baltimore Signed” Class 3 Security Services CA (2018)	コード署名証明書用中間 CA	2018 年まで有効	2048
17	11	“Baltimore Signed” Class 3 Security Services CA (2006)	SSL 証明書、Class1&3 電子メール証明書用中間 CA	2006 年 2 月 23 日まで有効	2048
18	12	Comodo Certified Delivery Plug-in CA	「Certified Delivery Plug-in」証明書用中間 CA（現在商用利用はされていない）	10 年	2048
19	13	Comodo Certified Delivery Manager CA	「Certified Delivery Manager」証明書用中間 CA（現在商用利用はされていない）	10 年	2048
20	14	Comodo Certified Delivery Authority CA	「Certified Delivery Authority」証明書用中間 CA（現在商用利用はされていない）	10 年	2048

CA ルート・キーの復旧のため、ルート CA の署名鍵は暗号化され、安全な環境に保存される。復号鍵は m 個のリムーバル・メディアに分割され、複号鍵の再構成には、n/m 個の復号鍵が必要になる。物理的に安全な場所に分配された当該リムーバル・メディアから物理的に復号鍵を回収するには、カストディアン（保管人）として認定された Comodo の役員 2 人以上の立会いが必要である。

CA のルート署名鍵を、別の暗号化ハードウェア・セキュリティ・モジュールにバックアップする場合、当該鍵は暗号化されたフォーマットでのみ、デバイス間での移動が可能である。

Entrust ensures は、AICPA/CICA Web Trust プログラム準拠の基盤及び CPS に従って、同社の CA ルート署名鍵ペアの保護を保証する。Entrusst の Web Trust への準拠は、同社の公式な Web サイトから入手可能である（www.entrust.com）

Baltimore Technologies, plc は、AICPA/CICA Web Trust プログラム準拠の基盤及び CPS に従って、同社の CA ルート署名鍵ペアの保護を保証する。Baltimore の Web Trust への準拠は、同社の公式な Web サイトから入手可能である（www.betrusted.com）。

同様に、Comodo は、AICPA/CICA Web Trust プログラム準拠の基盤及び CPS に従って、UTN ならびに Addtrust の

CA ルート署名鍵ペアの保護を保証する。Comodo の Web Trust への準拠は、同社の公式な Web サイトから入手可能である（www.comodogroup.com）。

2.1.2. Comodo CA ルート署名鍵生成プロセス

Comodo の秘密鍵は、信頼性の高いシステム（FIPS PUB140-1 level4 認定の IBM4758）で安全に生成され、保護されているのみならず、当該秘密鍵の危殆化や、不正利用を防ぐために必要な予防策を講じている。

Comodo CA ルート鍵は、「Root Key Generation Ceremony Reference」に詳細が示されているあるガイドラインにしたがって生成されたものである。Root Key Generation Ceremony で完了した作業や、関与した Comodo の担当者は、監査のため記録される。その後行われる Root Key Generation Ceremony も同様に、前述のリファレンス・ガイドの記載に従って行われる。

2.1.3. Comodo CA 署名鍵のアーカイブ

有効期限が切れた Comodo CA ルート署名鍵ペアは、最低 7 年間アーカイブに保管される。当該鍵は、本 CPS の第 2.1.1 節に詳細を示すとおり、有効期限が切れる前に、安全な保存場所により、安全な暗号ハードウェア・モジュールにアーカイブされる。

2.1.4. CA ルート署名鍵の切り替えで採用されている手順

Comodo のルート署名秘密鍵は、2018 年 8 月 14 日の 00:59:00 まで有効である。秘密鍵の期限切れが近づくと、新規 CA 署名鍵ペアが手配され、その後発行されるすべての証明書及び CRL は、その新しい署名用秘密鍵を使用して署名される。新旧 2 つの鍵は同時に有効使用することができる。新規の CA 秘密鍵に対応する証明書は、本 CPS の第 2.1.5 節に詳細を示す送付方法で加入者と信頼者に提供される。

2.1.5. Comodo CA ルート公開鍵の加入者への送付

Comodo はすべての CA ルート証明書を、インターネット上のリポジトリで公開している（www.Comodogoup.com^repository）。GTE CyberTrust ルート証明書は、現在 IE5.0 以上、Netscape 4.x 以上、及び Opera 5.0 以上に対応し、前述の各ブラウザを通じて信頼者に提供される。
加入者証明書の発行及び送付後、Comodo は完全な証明書チェーン（本 CPS の第 1.7 節参照のこと）を加入者に提供している。

2.1.6. 物理的な CA の運用

Comodo 施設の安全警備された部分へのアクセスは、物理的なアクセス・コントロールを実施することにより制限されており、適宜権限を与えられた個人（以降信頼される者）のみがアクセスを許されている。カード・アクセス・システムを配置し、施設内全域の制御、監視、及びアクセス記録を行っている。安全な施設内にある Comodo CA の物理的なマシンへのアクセスは、施錠されたキャビネットと論理アクセス制御を併用して保護されている。

Comodo は施設を以下の危険から確実に守るため、十分な取り組みを行ってきた。

- 火気・煙害によるダメージ（各地の規制に準拠した防火対策）
- 洪水及び水害

Comodo の安全な施設には、第一電源と第二電源が備えられ、継続的かつ途絶えることのない電源が確保されている。また暖房・/空気調整システムの使用により、過熱を防ぎ、適正な湿度レベルが維持される。

Comodo は上記資材の不履行、損失、損害あるいは資産の危殆化、及び事業活動の中断を察知し、回避するため、不断の努力を行う。

2.2. 電子証明書の管理

Comodo 証明書の管理は、以下を含むが、それに限定されない機能のことを言う。

- 証明書申請者の身元の実在性確認
- 証明書発行の認証
- 証明書の発行
- 証明書の失効
- 証明書の失効手順を伴うプロセスによる対応する秘密鍵の取り消し
- 証明書の一覧
- 証明書の配布
- 証明書の公開
- 証明書の保存
- 特定用途に基づく証明書の回収

Comodo は、直接または認定された RA を通じて、Comodo PKI 内における証明書管理を包括的に行う。Comodo は加入者鍵ペアの生成、発行、取り消し、または破棄に関する機能については関与しない。

2.3. Comodo ディレクトリ、レポジトリ、及び証明書失効リスト

Comodo は証明書失効リスト（CRL）を使用して失効した証明書を管理し、失効した証明書のディレクトリを一般に公開

する。Comodo が発行するすべての CRL は、RFC3280 に概要を示すX.509v2 対応の CRL である。ユーザーと信頼者は、証明書の情報を信頼する前には必ず、発行証明書及び失効証明書のディレクトリを調べて確認することが求められる。Comodo は日々 CRL を更新し、新しい CRL は毎日 6:05 に公開される。状況によっては、更に頻繁に更新・公開することもある。エンド・エンティティ証明書用の CRL は、下記の URL からアクセスできる。

http://crl.comodo.net/Class3SecurityServices_3.crl

http://crl.comodoca.com/Class3SecurityServices3.crl

失効された中間以上の証明書については、下記の CRL で公開される。

http://crl.comodoca.com/Class3SecurityServices_3.crl

http://crl.comodoca.com/Class3SecureServices3.crl

Comodo の PKI サービスに関する法律上の通知を掲載するリポジトリは、本 CPS、契約書、及び本 CPS で参照される通知と同様にその他のサービスに不可欠とみなされる情報も含めて公開される。Comodo の法律に関するリポジトリは、www.comodogroup.com/repository からアクセスできる。

2.4. Comodo 証明書の種類

Comodo は現在、個人あるいは事業用通信の安全性に対するユーザーのニーズを満たすために使用される電子証明書と関連製品を提供している。 その対象範囲は、セキュアな e メール、オンライン取引の保護、ネットワーク上、あるコミュニティ内の法的、物理的なもの本人確認などが含まれる。

Comodo は、同社が発行する証明書の種類を含め、適正であると判断した場合は、同社の製品一覧を更新したり、拡張する場合がある。Comodo 製品の一覧の公開や更新は、いかなる第三者も権利を主張できるのものではない。Comodo の階層に新規証明書製品が含まれると、2 日以内に本 CPS の改訂版が Comodo の正式な Web サイトに公開される。

発行された証明書は Comodo のディレクトリで公開される。一時停止あるいは失効した証明書は適宜 CRL で参照され、Comodo のディレクトリに公開される。Comodo は加入者の秘密鍵の預託は行わない。

2.4.1. Comodo Secure Server 証明書

Comodo は、一般サーバーの実存性確認を十分な認証を行って保証したり、企業顧客及び企業のビジネス・パートナーが安全に通信できるよう、Secure Socket Layer(SSL)ウェブ・サーバーと組み合わせて使用する Secure Server 証明書を提供している。Comodo の提供する Secure Server 証明書には、Instant SSL、InstantSSL Pro、PremiumSSL、PremiumSSL Wildcard、Intranet SSL、及び Trial SSL 証明書の 6 種類があり、これらの証明書の価格体系については、関連する Comodo の公式 Web サイトで確認できる。

a) InstantSSL 証明書

InstantSSL 証明書は、エントリー・レベル版の Secure Server 証明書である。当該証明書は、さほど取引金額の多くない電子商取引や、あまり重要ではないデータをやり取りする Web サイト、及び内部ネットワークでの利用を想定した証明書である。

本 CPS の第 4.2.2 節(「審査規程」)に従い、Instant SSL 証明書は、証明書の発行時間を短縮するため、証明書申請の審査に Comodo の IdAuthority を利用する。IdAuthority は、一般に公開されているデータの組み合わせを情報源とした 5 百万件を超える一意な法的主体の記録を収容している。可能であれば、当該ディレクトリを証明書の申請者の本人確認に使用する。当該ディレクトリでは証明書の申請者の審査が十分に行えない場合は、申請者の提出した情報を元にコールバックを行うなど、更なる審査プロセスを行うこともある。

検証時間の短縮と、Comodo が意図する InstantSSL 証明書の使用方法の性質上、証明書の保証額は減額される。InstantSSL 証明書の最高保証額は＄50 とする。

InstantSSL 証明書の加入者料金は、Comodo の公式 Web サイトで確認できる。

b) InstantSSL Pro 証明書
InstantSSLPro 証明書は、中級レベルの Secure Server 証明書である。当該証明書は、Web サイトで電子商取引を行ったり、データのやり取りを行ったり、また内部ネットワークにおける利用を想定した証明書である。

本 CPS の第 4.2.3 節(「検証規定」)に従い、Instant SSL Pro 証明書もまた、証明書申請処理の一環として Comodo の IdAuthority を利用する場合がある。InstantSSL Pro 証明書のすべての申請において、申請者の提出した情報は、コールバックをはじめとする審査の対象となる。

InstantSSL Pro 証明書の最高保証額は＄2,500 とする。

InstantSSLPro 証明書の加入者料金は、Comodo の公式 Web サイトで確認できる。

c) PremiumSSL
PremiumSSL 証明書は、Comodo のプロフェッショナルレベルの Secure Server 証明書である。Web サイトで、高額な電子商取引を行ったり、重要なデータのやり取りを行ったり、また内部ネットワークにおける利用を想定した証明書である。

本 CPS の第 4.2.3 節(「検証規程」)に従い、PremiumSSL 証明書もまた、証明書申請処理の一環として Comodo の IdAuthority を利用する場合がある。PremiumSSL 証明書のすべての申請において、申請者の提出した情報は、コールバックをはじめとする審査の対象となる。

PremimuSSL 証明書の最高保証額は＄10,000 とする。

PremiumSSL 証明書の加入者料金は、Comodo の公式 Web サイトで確認できる。

d) PremiumSSL　Wildcard

PremiumSSL Wildcard 証明書は、Comodo のプロフェッショナルレベルの Secure Server 証明書で、一枚の PremiumSSL 証明書で複数のサブドメインを保護する際に使用される。Web サイトで、高価値の電子商取引を行ったり、重要なデータのやり取りを行ったり、また内部ネットワークにおける利用を想定した証明書である。

本 CPS の第 4.2.3 節（「検証規程」）に従い、PremiumSSL Wildcard 証明書もまた、申請処理の一環として Comodo の IdAuthority を利用する場合がある。PremiumSSL　Wildcard 証明書のすべての申請において、申請者の提出した情報は、コールバックをはじめとする審査の対象となる。

PremimuSSL Wildcard 証明書の最高保証額は＄10,000 とする。

PremiumSSL Wildcard 証明書の加入者料金は、Comodo の公式 Web サイトで確認できる。

e) Intranet　SSL

Intranet SSL 証明書は、内部ネットワークでの使用に特化した Secure　Server 証明書である。当該証明書の使用は、プライベート IP アドレス、または完全なサーバー名のみに限定されている。

Intranet SSL 証明書は商業目的では使用されないので、信頼者は Comodo や信頼に値する第三者に対し、証明書の誤発行による保証は求めない。

本 CPS の第 4.2.4 節（「検証規程」）に従い、Intranet SSL 証明書は、非公開のネットワーク内での使用に特化しているので、当該証明書の発行に際して、Comodo は審査を行わない。したがって Intranet SSL 証明書は保証の対象ではない。

Intranet SSL 証明書の加入者料金は、Comodo の公式 Web サイトで確認できる。

f) Trial SSL

Trial SSL 証明書は Secure Server 証明書で、SSL ソリューションの本格運用に先立ち、テスト環境で SSL を使用する顧客の支援を目的とした証明書である。–

Trial SSL 証明書は外部環境で使用される場合があり、最終的に信頼者により信頼される情報を含むものである。したがって、すべての Trial SSL 証明書は、本 CPS の第 4.2.2 説に従い、発行前に審査される。

Trial SSL 証明書はテスト専用で、保証は何も伴わない。

Trial SSL 証明書は無料で提供される。

2.4.2. Comodo Secure Email 証明書

Comodo は、加入者が信頼者用に電子署名を行ったり、あるいは信頼者が加入者に電子メールを暗号化できるよう、S/MIME 準拠の電子メールアプリケーションと併せて使用する Secure Email 証明書を提供している。当該証明書の価格体系については、関連する Comodo の公式 Web サイトで確認できる。Comodo は、標準価格に影響する可能性のあるプロモーション価格で当該証明書を販売する権利を有する。

a) Free Secure Email 証明書
Free Secure Email 証明書は自然人にのみ発行され、特定企業を代表する個人が使用してはならない。
本 CPS の第 4.2.5 節(「審査規定」)に従い、電子メールの所有者審査基準の実行を通じ、Comodo は当該加入者が Secure Email 証明書に明記されている電子メールアドレスを所有しているか、あるいはそのアドレスに直接アクセスできるかについて保証する。しかし、加入者の本人確認は行われないので、加入者が本人であるかどうかは保証されない。
Free Secure Email 証明書は無料である。

b) Corporate Secure Email 証明書
Corporate Secure Email 証明書は自然人にのみ発行され、証明書に記載のある企業を代表する個人によって使用されることがある。

Comodo EPKI Manager アカウントの保有者は、Corporate Secure Email 証明書を使用することができる。EPKI Manager アカウントは、Comodo 証明書(SSL 及び Secure Email)の申請に使用され、アカウントの保有者である企業の企業情報(社名、所在地、国)が含まれている。

EPKI Manager 認定管理者は、EPKI Manager のオンライン・アカウントにログインし、従業員または認定された企業の代表者についてのみ、Corporate Secure Email 証明書を申請する。

本 CPS の第 4.2.6 節(「審査規定」)に従い、Comodo は Corporate Secure Email 証明書で規定されたドメイン名を該当する企業が使用する権利を審査する。当該企業は Corporate Secure Email 証明書の発行前に、申請に名を連ねている個人の正当性を保証する必要がある。
Corporate Secure Email 証明書については、最高保証額を＄10,000 とする。
Corporate Secure Email 証明書の加入者料金は Comodo の公式 Web サイトで確認できる。

2.5. エクステンションとネーミング規程

2.5.1. 電子証明書エクステンション

Comodo PKI 内で使用される電子証明書は、X.509 version 3 に基づいて作成されている。X.509v3 を使用することにより、CA は特定の証明書エクステンションを基本的な証明書構造に追加できる。Comodo は 1995 年 ISO/IEC9594-8 の Amendment 1 により、X.509v3 の意図する目的に合わせて、多くの証明書エクステンションを使用している。X.509v3 は国際電気通信連合が定めた電子証明書に関する規格である。

2.5.2. エクステンション及びエンハンスドネーミングの参照組み込み

エンハンスドネーミングは、X.509v3 証明書内の拡張された組織フィールドの使用法である。組織単位フィールドに含まれる情報は、Comodo が使用する可能性のある Certificate Policy エクステンションにも含まれる。

2.6. 加入者秘密鍵生成プロセス

証明書リクエストで使用される秘密鍵の生成に関しては、加入者がすべての責任を負うものである。Comodo は鍵生成、エスクロー、リカバリあるいはバックアップサービスの提供は行わない。

証明書の申請にあたり、申請する証明書の種類に合った適切な RSA 鍵ペアの生成についても、加入者がすべての責任を有する。申請の際、加入者は公開鍵とその他の個人情報・企業情報を、証明書署名リクエスト（CSR）として提出するよう求められる。

一般的に、Secure Server 証明書のリクエストは、加入者の Web サーバー・ソフトウェアが対応する鍵生成システムを用いて生成される。一般的に、Secure Email 証明書のリクエストは、汎用ブラウザに備わっている FIPS140-1 Level1 暗号サービス・プロバイダ・モジュール・ソフトウェアを使用して生成される。

2.7. 加入者秘密鍵の保護とバックアップ

加入者の秘密鍵の保護は、加入者の自己責任で行う。Comodo は当該鍵の生成、保護、または配布については何ら関与しない。

加入者はパスワードあるいは同等の認証手続きを使用して、加入者の秘密鍵に対する不正なアクセスや不正使用を防止する必要がある。

2.8. 加入者の公開鍵の Comodo への配送

Secure Server 証明書リクエストは、加入者の Web サーバー・ソフトウェアを使用して生成され、当該リクエストは

PKCS＃10 証明書署名要求（CSR）として Comodo に提出される。提出は Comodo の Web サイトあるいは Comodo の認定 RA を介して電子的に行われる。

Secure Email 証明書要求は、加入者のブラウザに備わっている暗号化サービス・プロバイダ・ソフトウェアを使用して生成され、PKCS#10 証明書署名申請（CSR)として提出される。提出は Comodo の Web サイトあるいは Comodo の認定 RA を介して電子的に行われる。

2.9. 発行された加入者証明書の加入者への配送

関連する加入者への加入者証明書の配送は、以下の通り証明書の製品種類によって異なる。

2.9.1. Secure Server Certificate: InstantSSL タイプ

Comodo が運用する IdAuthority データベースに、十分な審査情報が収容されている場合は、InstantSSL の自動審査が実行される。自動審査の場合、InstantSSL 証明書は、申請時に使用されたドメイン名で許可された担当者に属し、一般的に使用される総称的な電子メールアドレス（例：webmaster@..., admin@..., postmaster@...）宛てに配送される。証明書配送場所の確認は、申請プロセスで提示された管理者の連絡先に送られる。

2.9.2. Secure Server Certificate：InstantSSL Pro、PremiumSSL、PremiumSSL Wildcard、Intranet SSL、及び Trial SSL

InstantSSL Pro、PremiumSSL、PremiumSSL Wildcard、Intranet SSL、及び Trial SSL 証明書は、電子メールにより、申請プロセスで提示された管理者の電子メールアドレスを介して加入者へ配送される。

2.9.3. Secure Email Certificate：無料版

無料版の Secure Email Certificate が発行されると、申請時に提示された加入者の電子メールアドレス宛に、証明書の取得リンクが送付される。加入者は、最初に証明書申請を行ったのと同じコンピュータを使用して取得リンクにアクセスしなければならない。加入者の暗号化サービス・プロバイダ・ソフトウェアは、加入者が申請時に提出した公開鍵に対応する秘密鍵を、所有していることを確認する。証明書取得が成功すると、発行された証明書は加入者のコンピュータに自動的にインストールされる。

2.10. 発行された加入者証明書の Web ホストリセラー Partner への配送

加入者本人の代わりに Web ホストリセラー Partner を通じて申請された加入者の Secure Server Certificate が発行されると、Web ホストリセラー Partner のアカウントの管理者の連絡先に電子メールが送信される。「自動申請」インターフェースを使用した Web ホストリセラー Partners は、発行された証明書を Web ホストリセラーの指定 URL から取得するための追加オプションが得られる。

2.11. 発行された加入者証明書の EPKI Manager アカウント所有者への配送

EPKI Manager を通じて申請された加入者用 Secure Server Certificate が発行されると、Web ホストリセラー Partner アカウントの管理者の連絡先へ電子メールが配送される。

発行された Corporate Secure Email Certificate は、本 CPS の第 2.9.3 節に従って送付される。

2.12. Comodo 証明書プロファイル

証明書プロファイルに含まれるフィールドを以下に示す。

2.12.1. Key Usage エクステンション・フィールド

Comodo 証明書は汎用的で、地理的領域や業種の制限に捉われず使用される。Comodo 証明書を使用し、信頼するには、信頼者は X.509v3 に準拠したソフトウェアを使用する必要がある。Comodo 証明書には、X.509v3 準拠のソフトウェア使用する場合に、証明書の用途を指定し、機能を技術的に制限するための Key Usage エクステンション・フィールドが含まれている。Key Usage エクステンション・フィールドの信頼性は、ソフトウェアの X.509v3 規格の実装に依存するもので、Comodo の関知するものではない。
X.509v3 規格により特定される可能な鍵の用途を以下に示す。

a）電子署名：下記の b)、f)、または g)により示される以外の目的を有する電子署名の検証。つまりエンティティとデータ発生源の同一性証明と認証。
b）非否認性：署名を行うエンティティが不当に行為を否定することに対する防御策として非否認サービスを提供する際に使用される電子署名の検証（下記 f）、または g）に示される証明書、または CRL への署名を除く）
c）鍵の暗号化：鍵の暗号化またはその他のセキュリティ情報（鍵の移動など）の暗号化
d）データの暗号化：ユーザー・データの暗号化。但し、上記 c）による鍵やセキュリティ情報は除く
e）鍵の一致：公開鍵に一致する鍵として使用
f）鍵証明書署名： 証明書上の CA の署名の検証（CA 証明書でのみ使用）
g）CRL への署名：CRL 上の CA の署名の検証
h）暗号化専用：公開鍵一致鍵は、鍵の一致で使用される場合、データの暗号化にのみ使用
i）復号化専用：公開鍵一致鍵は、鍵の一致で使用される場合、データの復号化にのみ使用

2.12.2. Extension Critically フィールド

Extension Critically フィールドは、Key Usage フィールドに対する 2 つの異なる使用法を示す。エクステンションに

Critical と表示されている場合は、証明書の鍵は明記された用途にのみ適用される。この場合に当該鍵を他の用途に使用することは、発行者のポリシー違反とみなされる。エクステンションに Critical と表示されていない場合、Key Usage フィールドは、アプリケーションによる特定用途に合った鍵の検索を支援するために存在する。

2.12.3. Basic Constraints エクステンション

Basic Constraints エクステンションは、証明書の名義人が CA として機能するのか、単なるエンド・エンティティ証明書なのかを明示する。Basic Constraints フィールドの信頼性は、ソフトウェアの X.509v3 規格の実装に依存するもので、Comodo の関知するものではない。

2.12.4. 証明書ポリシー

証明書ポリシー（CP）は、発行状況において、発行者により規定された電子証明書の用途を表す記述である。ポリシー識別子は、特定の領域内にのみ通用する番号で、この番号を使用すると、証明書ポリシーを含むポリシーを明確に識別できる。
Comodo 証明書のプロファイルを下表に示す。

Comodo Secure Server Certificate – InstantSSL, InstantSS+ Pro, PremiumSSL, PremiumSSL Wildcard		
Signature Algorithm	Sha1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	© 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.c omodogroup.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1year / 2 year / 3 year	

Subject	CN	Common Name
	OU	InstantSSL/ InstantSSL Pro / PremiumSSL / PoweredSSL Product Name*
	OU	Hosted by [Web ホストリセラー Subscriber name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]
	O	Organization
	OU	Organization Unit
	L	Locality
	S	State
	C	Country
Authority Key Identifier	KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1	
Key Usage (Non Critical)	Digital Signature, Key Encipherment (A0)	
Netscape Certificate Type	SSL Server Authentication (40)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1, 1]Policy QualifierInfo: Policy Qualifier Id=CPS Qualifier: http://www.c omodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.c omodo.net/Class3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.c omodoca.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@crl.c omodo.net [1]CRL Distribution Point	

	Distribution Point Name: Full Name: URL=http://crl.Comodo.net/Class3SecurityServices 3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.Comodoca.com/Class3SecurityServices 3.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= Class3SecurityServices 3@crl.Comodo.net
Subject Alternate Name	DNS Name
Netscape SSL Server Name	
Thumbprint Algorithm	SHA1
Thumbprint	

Comodo Secure Server Certificate – IntranetSSL		
Signature Algorithm	Sha1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	© 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1year / 2 year / 3 year	
Subject	CN	Common Name
	OU	IntranetSSL[2]
	OU	Hosted by [Web ホストリセラー Subscriber name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]
	O	Organization
	OU	Organization Unit
	L	Locality
	S	State
	C	Country
Authority Key Identifier	KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1	
Key Usage (Non Critical)	Digital Signature, Key Encipherment (A0)	
Netscape Certificate Type	SSL Server Authentication (40)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1, 1]Policy QualifierInfo: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.Comodo.net/Class3SecurityServices.crl	

	[2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.comodoca.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@crl.comodo.net [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.comodo.net/Class3SecurityServices 3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices 3.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= Class3SecurityServices 3@crl.comodo.net
Subject Alternate Name	DNS Name
Netscape SSL Server Name	
Thumbprint Algorithm	SHA1
Thumbprint	

2

[2] [2] PoweredSSL サービスの加入者は、所有している製品名を InstantSSL Certificate、InstantSSL Pro Certificate、PremiumSSL Certificate、PremiumSSL Wildcard Certificate、IntranetSSL Certificate、Trial SSL Certificate の商標に付け替える。

Comodo Secure Server Certificate – Trial SSL		
Signature Algorithm	Sha1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	© 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1year / 2 year / 3 year	
Subject	CN	Common Name
	OU	TrialSSL[3]
	OU	TEST USE ONLY – NO WARRANTY ATTACHED
	OU	Hosted by [Web ホストリセラー Subscriber name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]
	O	Organization
	OU	Organization Unit
	L	Locality
	S	State
	C	Country
Authority Key Identifier	KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1	
Key Usage (Non Critical)	Digital Signature, Key Encipherment (A0)	
Netscape Certificate Type	SSL Server Authentication (40)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1, 1]Policy QualifierInfo: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.Comodo.net/Class3SecurityServices.crl	

	[2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.Comodoca.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@crl.Comodo.net [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.Comodo.net/Class3SecurityServices 3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.Comodoca.com/Class3SecurityServices 3.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= Class3SecurityServices 3@crl.Comodo.net
Subject Alternate Name	DNS Name
Netscape SSL Server Name	
Thumbprint Algorithm	SHA1
Thumbprint	

Comodo Secure Server Certificate –Secure Email Certificate (Free Version)		
Signature Algorithm	Sha1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	© 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network

	O	Comodo CA Limited
	C	GB
Validity	1year	
Subject	E	Email address
	CN	Common Name（name of subscriber）
	OU	OU=© 2001 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network-PERSONA NOT VALIDATED
Authority Key Identifier	KeyID=F652 2217 1513 0803 59BF 1895 9F48 B4B9 E9FE F866	
Key Usage (Non Critical)	Secure Email(1.3.6.1.5.5.7.3.4) Unknown Key Usage(1.3.6.1.4.1.6449.1.3.5.2[)4]	
Netscape Certificate Type	Smime(20)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1, 1]Policy QualifierInfo: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.Comodo.net/Class3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.Comodoca.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Po[3]int Name: Full Name: RFC822 Name=Class3SecurityServices@crl.Comodo.net	
Subject Alternate Name	RFC822Name=email address	
Thumbprint	SHA1	

[3] [4] Comodo Certificate Delivery Service の受理施設に使用。Certified Delivery Service は本 CPS では取り扱っていない。

Algorithm	
Thumbprint	

Comodo Secure Server Certificate –Secure Email Certificate (Corporate Version)		
Signature Algorithm	Sha1	
Issuer	CN[4]	Comodo Class 3 Security Services CA
	OU	© 2002 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network
	O	Comodo CA Limited
	C	GB
Validity	1year	
Subject	E	Email address
	CN	Common Name（name of subscriber）
	OU	OU=© 2001 Comodo CA Limited
	OU	Terms and Conditions of use: http://www.comodogroup.com/repository
	OU	Comodo Trust Network-PERSONA NOT VALIDATED
Authority Key Identifier	KeyID=F652 2217 1513 0803 59BF 1895 9F48 B4B9 E9FE F866	
Key Usage (Non Critical)	Secure Email(1.3.6.1.5.5.7.3.4) Client Authentication(1.3.6.1.5.5.7.3.2) Smart Card Logon(1.3.6.1.4.1.311.20.2.2) Unknown Key Usage(1.3.6.1.4.1.6449.1.3.5.2)[5]	
Netscape Certificate Type	SSL Client Authentication, SMIME(A0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1, 1]Policy QualifierInfo: Policy Qualifier Id=CPS Qualifier: http://www.comodogroup.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name:	

[45] Comodo Certificate Delivery Service の受理施設に使用。Certified Delivery Service は本 CPS では取り扱っていない。

	Full Name: URL=http://crl.Comodo.net/Class3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.Comodoca.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@crl.Comodo.net
Subject Alternate Name	RFC822Name=email address
Thumbprint Algorithm	SHA1
Thumbprint	

2.13 Comodo 証明書失効リストプロファイル[5]

Comodo 証明書失効リストのプロファイルは下表の通りである。

Version	[Version 1]	
Issuer Name	countryName=[Root Certificate Country Name], organizationName=[Root Certificate Organization], commonName=[Root Certificate Common Name] [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 2 hours]	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

[55] Comodo Certificate Delivery Service の受理施設に使用。Certified Delivery Service は本 CPS では取り扱っていない。

3. 組織

Comodo は英国内での営業活動に加え、他に研究開発及びサーバーの運用を行うサイトを擁している。すべてのサイトは、CA 関連施設への不正な論理的あるいは物理的アクセスを検知し、阻止し、防止するために策定されたセキュリティ・ポリシーに基づいて運営されている。本節では、信頼性が高く、安全な CA の運用を提供するために実施されているセキュリティ・ポリシー、物理的及び論理的アクセス・コントロール機構、サービ・レベル、及び社員ポリシーの概要を示す。

3.1. 本 CPS への準拠

Comodo がサービスを提供する際は、本 CPS、ならびに関連する契約を通じて責任の生じるその他の義務に従う。

3.2. CA 運用の終了

CA 運用終了の理由がいかなるものであっても、Comodo は時宜を得た通知を行い、引継ぎ機関へ責任を委譲し、記録を維持するとともに救済措置を提供する。CA の活動を停止する前に、可能であれば Comodo は以下の手段を講じる。

- CA としての活動終了を予告し、90 日間有効な証明書を加入者に提供する
- 90 日間の通知期間が満了した時点で失効されていない証明書あるいは有効期限切れになっていないすべての証明書を、加入者の同意を得ず失効させる
- 影響を受ける個々の加入者に対し、失効の通知を速やかに行う
- 本 CPS に従って、記録を保存するために正当な手配を行う
- 証明書の再発行を行うための一連の許可を得て、すべての必要な規則に準拠する一方、少なくとも Comodo と同等の安全な運用を行う CA の引継ぎを行う後継者に対し、業務の引継契約を提供する権利を留保する

本項の用件は契約によって異なる場合がある。 しかし、その変更点は契約当事者間のみに影響を与える範囲に限定される。

3.3. 記録形式

Comodo は本 CPS の第 3.4 節に詳細を示す期間にわたり、電子的あるいは紙ベースの形式で記録を保持する。Comodo は証明書申請の確認のため、適切な文書の提出を加入者に要求することがある。

Comodo RA(登録局)は、Reseller　Partner 契約、Web ホストリセラー Partner 契約、EPIK マネージャアカウント保持者契約、Powered SSL　Partner 契約に示された適切な文書の提出が求められ、審査後、正式な Comodo CA(認証局)として認定される。

Comodo RA(登録局)として、RA は証明書申請の確認のため、適切な文書の提出を加入者に要求することがある。その場合、RA は Comodo が採用し、本 CPS に記載されている記録保持及び記録保護の規程に従って当該記録を保持する義務がある。

3.4. 記録保持期間

Comodo は電子証明書の記録とその関連文書を、少なくとも 7 年間は保持する。記録保持期間は有効期限が切れた日付あるいは失効日より開始される。証明書のコピーはその状態によらず、たとえ有効期限切れでも失効されていても、保存される。当該記録は電子的または紙ベースの形式、あるいは Comodo が適正とみなしたその他の任意の形式で維持される。
記録は安全な、別の離れた場所で保管され、記録の不正な改変や差し替え、または破棄ができない形式で維持される。

3.5. コア機能のログ

監査の目的のため、Comodo ではコア機能の下記のイベントに関する電子的あるいは手書きのログの整備を行う。すべてのログはリムーバブル・メディアにバックアップされ、当該メディアは安全な、別の離れた場所に保管される。前述したメディアは、データ・センターを訪れた Comodo の従業員によってのみ消去される。データ・センター以外では、開発サイト内の鍵のかかったオフィス内か、あるいは安全な保管施設内の別の場所で保管される。
監査ログはリムーバブル・メディアのすべての動きを収録している。ログはシステム管理者によって毎週アーカイブに保管され、イベント・ジャーナルは CA 管理者によって毎週見直される。現在のログも、アーカイブされた過去のログのいずれも、不正な改正や差し替え、または破棄ができない形式で維持される。リムーバブル・メディアが耐用年数に達すると、第三者の安全なデータ破棄施設ですべての情報を消去し、破棄された証明書はアーカイブに残される。
すべてのログは以下の要素を含む。

- エントリの日付と時刻
- エントリのシリアル・ナンバーまたはシーケンス・ナンバー
- エントリの方法
- エントリのソース
- ログ・エントリを行った個人・法人の身元保証

3.5.1. CA 及び証明書ライフサイクル管理

- CA ルート署名鍵の機能(鍵の生成、バックアップ、回復及び破棄を含む)
- 加入者証明書のライフサイクル管理(受理された証明書申請と拒否された証明書申請、証明書の発行、証明書の再発行、証明書の更新を含む)
- 加入者証明書の失効要求(失効理由を含む)

- 既存の証明書を無効にする恐れのある加入者との関係の変更
- 証明書失効リストの更新、生成及び発行
- 鍵及び鍵を格納したデバイスやメディアの保護・管理
- 秘密鍵の危殆化

3.5.2. セキュリティ関連イベント

- システム運用停止時間、ソフトウェアのクラッシュ及びハードウェアの故障
- Comodo の社員によって実行される CA システム業務（ソフトウェアの更新、ハードウェアの置き換え及びアップグレードを含む）
- 暗号化ハードウェア・セキュリティ・モジュールのイベント（HSM の使用、インストール解除、保守サービスまたは修理及び HSM の廃止、など）
- 成功、失敗を問わず、Comodo PKI へのアクセス試行
- 安全な CA 施設への訪問者の入退記録

3.5.3. 証明書申請情報

- 申請検証プロセスの一部として、申請者によって提示された文書及びその他の関連情報
- 提示された文書の物理的あるいは電子的な保存場所

3.5.4. ログの保持期間

Comodo は、ログの記録を 7 年間、あるいは適用法の規定に準拠する期間維持する。

3.6. 事業継続計画及び災害復旧

サービスの完全性を維持するため、Comodo は適切な事業継続計画及び災害復旧計画の手順の策定、文書化、及び定期的テストを行う。当該計画は必要に応じて、少なくとも年に 1 度は改訂、更新される。

- Comodo は完全に冗長化された CA システムを運用する。バックアップ CA は主となる CA が万一運用を停止しても、即座に使用できるよう待機される。Comodo の重要なコンピュータ機器は、商業的なデータ・センターが運営する共同施設内に設置され、すべての主要なコンピュータ機器は当該施設内で二重化されている。入力電源及び接続用の給電線も二重化されている。二重化された機器は CA 業務をいつでも引き継げるように準備されており、システムの最長停止時間は 1 時間以内で指定できる（重大なシステム故障の場合）。
- 重要な CA ソフトウェアのバックアップは毎週実施され、別の離れた場所で保存される。

- 重要な営業情報のバックアップは毎日行われ、別の離れた場所で保存される。
- Comodo は、英国内の 2 ヶ所のサイトに分けて運用を行っている。West Yorkshire 州 Bradford で第 1 運用サイトを、また第 2 運用サイトを Kent 州の Tonbridge で運用している。両サイトはともに、証明書の申請、発行、失効、及び更新を含むがこれらに限定されない証明書のライフサイクルを管理する施設を提供する。

完全に冗長化された CA システムに加え、第 1 運用サイトで完全なシステムの崩壊が発生した場合に備え、Comodo はバックアップ CA と第 2 サイトを始動させる準備を怠らない。この災害復旧計画は、CA の運用が中断されるのを最小限に抑えるための Comodo の不断の努力の表明である。

3.7. 失効データの入手

Comodo は証明書失効リスト（CRL）を公開することで、Comodo が発行した電子証明書を使用した電子署名を、信頼者が検証できるようにしている。各 CRL には有効期限内に失効したすべての発行済み証明書のエントリが含まれており、24 時間有効となっている。Comodo は現行の CRL の有効期限が切れる前の 6:05 に新しい CRL を発行し、各 CRL には発行するごとに 1 づつ増える連続した番号が割り当てられる。特殊な状況下においては、Comodo は現行 CRL の有効期限が切れる前に新しい CRL を発行する可能性がある。有効期限が切れたすべての CRL は、本 CPS の第 3.4 節に記載される通りアーカイブされ、7 年間あるいは必要に応じて、それ以上の期間保存される。Comodo は OCSP（Online Certificate Status Protocol） のサポートは行わない。

3.8. 重要情報の公開

Comodo は発行された電子証明書のすべての失効データ、本 CPS、証明書の契約条件、信頼者契約及びすべての加入者契約の控えを、Comodo の公式なリポジトリで公開する（www.comodogroup.com/repository）。Comodo リポジトリは、Comodo 証明書ポリシー認証局によって維持されており、すべての更新、改変及び法的特別措置は、本 CPS に明記された記録手順に従って記録される。

3.9. 機密情報

Comodo は、法律あるいは Comodo のプライバシー・ポリシー（本 CPS の第 3.11 節を参照）により機密情報とみなされる個人データの保護に関する適用規則を遵守する。

3.9.1. 機密とみなされる情報の種類

Comodo では以下の情報を機密情報とみなして管理し、当該記録が信頼されない者に漏洩しないよう適正な管理を

堅持する。

- 加入者契約
- 証明書申請の受理・拒否によらず、証明書申請記録及び証明書申請の審査のため提出された補足文書
- トランザクションの記録及び財務監査記録
- 外部または内部監査履歴記録及び報告書（Comodo の自由裁量で公開される Web Trust 監査報告は除く）
- 事業継続計画及び災害復旧計画
- Comodo の基盤、証明書管理及び登録サービスとデータ運用に関する内部履歴及び記録

3.9.2. 機密とみなされない情報の種類

加入者は、Comodo CA が発行したすべての証明書の失効データは、24 時間ごとに定期的に Comodo リポジトリに公開される公の情報であることを認識する。関連の加入者契約に「公開」と記されていて、証明書申請の一部として提出された加入者の申請データは、本 CPS の第 2.12.4 節に従い、発行される電子証明書内で公開される。

3.9.3. 機密情報へのアクセス

信頼される立場にある従業員は全員、あらゆる情報を厳正な機密情報として取り扱う。RA や LRA に携わる担当者は特に、個人データの保護に関する英国法の要件に従わなければならない。

3.9.4. 機密情報の開示

Comodo は、法律によって命ぜられない限り、信用性の確認なく、許可された関係者による正当な特定の要求も、いかなる機密情報の公開要求に応じない。

- Comodo が情報を機密に保持する義務を有する相手である関係者
- 前述の情報を要求する関係者
- 裁判所命令（発令された場合）

3.10. 従業員管理と規程

本 CPS に従い、従業員が信頼に値し、有能であると同時に、従業員の業務遂行が満足できるものであることを正当に保証する就業規定及び管理規程を定めます。

信頼される役割

信頼される役割は Comodo のアカウント管理システムへのアクセスに関連し、個人ごとに職務上の許可が与えられる。許可は管理チームの上級メンバーによって決定され、許可証は署名され、アーカイブに記録される。

信頼される従業員は、システムにアクセスする権利を得る前に、本人確認を行い、システムに自身であることを証明する必要がある。本人確認はユーザー名と併せ、パスワードと電子証明書の両方が必要である。

従業員管理

信頼される従業員は全員、Comodo のシステムへアクセスする権利を得る前に、身元の確認が行われる。当該確認には、信用履歴、照会用職務履歴、及び役員失格者の Companies House cross –reference を含むが、これらに限定されるものではない。従業員の教育は、各自が所属するチームの先輩社員が関わるメンターリングを通じて行われる。

3.11. プライバシー・ポリシー

Comodo では、本 CPS に準拠したプライバシー・ポリシーを実践している。Comodo のプライバシー・ポリシーは Comodo リポジトリ（www.comodogroup.com/repository）で公開されている。

3.12. 情報の公開

Comodo 証明書サービス及び Comodo リポジトリは、以下に挙げる複数の通信手段を通じてアクセスできる。

- Web：www.comodogroup.com
- 電子メール：legal@comodogroup.com
- 郵送：Comodo CA Ltd

Attention: Legal Practices, Campus House, 10 Hey Street, Bradford, UK

Tel: +44(0)1274.730505

Fax: +44(0)1274.730909

- 電子メール：legal@comodogroup.com

4. 運用業務及び手続き

本節は、証明書申請の受理に必要な情報を含めた、証明書申請プロセスについて解説する。

4.1. 証明書申請要件

すべての証明書申請は、以下の登録プロセスを含む手続きを完了する必要がある。

- RSA 鍵ペアを生成し、有効な PKCS#10 証明書署名リクエスト（CSR）を提出することで、その鍵ペアの片方に当たる秘密鍵の所有権を Comodo に提示する
- 当該鍵ペアの片方に当たる秘密鍵の完全性を確保すべくあらゆる努力を行う
- 証明書の申請を Comodo に提出する。申請には本 CPS に詳細を示す申請情報、鍵ペアの片方に当たる公開鍵、及び関連する加入者契約への同意を含む
- 登録プロセスの間に Comodo から要求される公式文書を提出し、本人確認の証明を提供する

証明書の申請は Comodo あるいは認定 ComodoRA に提出する。下表に証明書申請処理に関わる関係者の詳細を示す。実際の処理担当に関係なく、すべての証明書は Comodo が発行する。

証明書の種類	登録対象	処理担当	発行局
Secure Server Certificate（本 CPS の第 2.4.1 節による全種類）	エンド・エンティティ加入者	Comodo	Comodo
Secure Server Certificate（本 CPS の第 2.4.1 節による種類）	Web ホストリセラー（エンド・エンティティ加入者の代理人として）	Web ホストリセラー	Comodo
Secure Email Certificate（本 CPS の第 2.4.2 節による無料版）	エンド・エンティティ加入者	Comodo	Comodo
Secure Email Certificate（本 CPS の第 2.4.2 節による企業版）	エンド・エンティティ加入者	EPKI マネージャアカウン保有者	Comodo

4.1.1. Web ホストリセラーパートナーによる証明書申請

Web ホストリセラーパートナーは、本 CPS に記載の規程とポリシーに基づき、RA の役割を担う。RA は Web ホストリセラープログラムに従い、申請者に代わって証明書の申請を行う。

前述の状況においては、本 CPS の第 4.1 節に詳細を示す通り、証明書の申請者に代わり、すべての機能の責任を RA が負うこととなる。当該責任は Web ホストリセラー契約及びガイドラインに詳細が示されており、それが遵守される。

4.1.2. EPIK マネージャアカウント保持者による証明書申請

EPKI マネージャアカウント保持者は、本 CPS に記載の規程とポリシーに基づき、RA の役割を担う。RA は指定されたサーバーが使用する Secure Server Certificate、あるいは指定された従業員、パートナー、または EPKI Manager Account を所有する法人組織に属しているか、または法律的に使用されていることを Comodo が検証したドメイン名の下のエクストラネット・ユーザーが使用する Secure Emai Certificate を申請する。

4.1.3. 申請方法

一般的には、申請者は、Comodo または認定 RA がそれぞれの公式な Web サイトで提供しているオンラインフォームに情報を入力して提出する。状況によっては、申請を電子メールで送信することもあるが、このプロセスは Comodo または当該 RA の自由裁量で判断される。

EPIK マネージャアカウント保持者の証明書申請は、EPKI Manager 管理コンソール（Comodo がホストとなりサポートを提供する Web ベースのコンソール）から行われる。

4.2. 申請の審査

証明書を発行する前に、Comodo は証明書申請に記載された加入者情報が正しく、本人のものであることを審査を行う。当該管理は製品の種類により異なる。

4.2.1. Secure Server Certificate の申請：2 段階の審査プロセス

Comodo は Secure Server Certificate の発行に先立ち、2 段階の審査を行う。

本プロセスにおける、加入者（本 CPS の第 4.3 節による）が提供した申請情報の調査は、自動的あるいは人為的に Comodo が関与する。本プロセスでは以下を審査を行う。

1. 申請者が、申請に使用したドメイン名を利用する権利を有しているかどうか
    - インターネットまたは認定されたグローバル・ドメイン名登録を通じ、一般的に入手できるドメイン名の所有者の記録を調査して検証する
    - ドメイン名の登録記録に関する管理者の連絡先を通じて、Comodo の審査担当者から連絡を取るか、自動電子メール・チャレンジを行って、検証の裏づけを取る
    - 通常はドメイン名の管理者のみが使用できる一般的な電子メール（例：webmaster@...、postmaster@... 、

admin@...）の使用を通じて、検証の裏づけを取る

2. 申請者が法的な責任を果たせる法人組織または個人かどうか
   - 法人の場合は、事業許可証、基本定款、販売許可証、またはその他の関連文書などの公式な企業文書の提示を求めて検証する。法人以外の申請者は、銀行の明細、パスポートのコピー、運転免許証のコピー、またはその他の関連文書などにより検証する・

上記の申請内容は、自動化されたプロセス、担当者による補助文書の確認、及び第三者の公式データベースへの信用照会を通じて再調査される。

4.2.2. InstantSSL 及び Trial SSL

Comodo は IdAuthority と呼ばれる本人確認保証データベースを Web サイト上で運用している。本データベースには既知のドメイン名について、予め検証された本人確認情報の記録が収録されており、自動化されたアルゴリズムを使用して、グローバル・ドメイン名登録からのドメイン名所有権の記録と、政府及び第三者企業の公式な情報資源から得た企業の所有権を証明する記録とを結び付ける。

申請に使用されたドメイン名に関して、十分な事前検証された記録が IdAuthority から得られた場合は、Comodo は IdAuthority に収録されているデータを使用して、審査プロセスの短縮を図ることがある。申請データが IdAuthority に収録されている記録と一致する場合は、人為的な審査は省略される。申請データが IdAuthority の記録と一致しない場合は、本 CPS の第 4.2.1 節に概要を示す 2 段階のプロセスに従って、Comodo の審査担当者が申請の審査を行う。

4.2.3. InstantSSL Pro、PremiumSSL、PremiumSSL Wildcard タイプ

InstantSSL Pro、PremiumSSL、及び PremiumSSL Wildcard 証明書は、本 CPS の第 4.2.1 節に概要を示す 2 段階のプロセスに従って、Comodo の審査担当者が審査を行う。

Comodo は審査プロセスの迅速化のために、IdAuthority に格納されているデータを使用することがある。申請データが IdAuthority に収録されている記録と一致する場合は、人為的な審査は省略される。申請データが IdAuthority の記録と一致しない場合は、本 CPS の第 4.2.1 節に概要を示す 2 段階のプロセスに従って、Comodo の審査担当者が審査の検証を行う。

4.2.4. Intranet SSL タイプ

イントラネット証明書の申請は、不完全な適格ドメイン名★non-Fully Qualified Domain Names★と非公開★Non—public★のIPアドレスによって規定される内部ネットワーク上のサーバーに対してのみよってのみ受領される。申請プロセス中、Comodoは提出された一般名★Common name★（サーバー名）が完全な適格ドメイン名★Fully Qualified Domain Names★でも、一般に公開されているIPアドレスのいずれでもないことを検証する。無事検証が済んで発行されるイントラネット証明書は、インターネット上で公的に使用することはできない。

Comodoはイントラネット証明書が公的証明書として使用されないことを検証する。イントラネット証明書は非公開ネットワークの内部に使用が制限されているので、証明書に関連して企業の実存性を確認する検証は必要ないか、あるいは検証されない。

4.2.5. Secure Email Certificate：無料版

Secure Email Certificateの無料版は、証明書の名義人が検証されない。Comodoは、提出された電子メールのアドレスを使用する権利を申請者が有しているかどうかだけを検証する。これはComodoがホストとして提供するオンラインの証明書取得施設へのComodo独自のログイン情報を電子メールで配送することにより実現する。ログイン情報は、Secure Email Certofocateの無料版申請の際に提出されたアドレス宛に電子メールで送信される。

オンラインの証明書取得施設にログイン後、Secure Email Certificateの無料版をインストールする前に、Comodoは、自動化された暗号化チャレンジを通じて、証明書の申請者が申請プロセスの際に提出した公開鍵に関連する秘密鍵を所有しているかどうかの検証を行う。自動チャレンジが成功した場合、Comodoは加入者に電子証明書を発行する。

4.2.6. Secure Email 証明書：法人版

Secure Email Certificateの法人版は、EPKI Managerからのみ入手が可能で、認定されたドメイン名内の電子メールアドレスについてのみ発行される。EPIKマネージャアカウント保持者は、まずドメイン名をComodoに提出する。ドメイン名は、本CPSの第4.2.1節に従って、適切なドメイン名の所有権、またはドメイン名の使用権を有しているかどうか検証が行われる。提出したドメイン名の検証が無事終了すると、EPIKマネージャアカウント保持者はドメイン名内で電子メールアドレスを使用することができる。

Secure Email証明書の法人版は、EPKI Managerが指定した管理者によって申請される。管理者はSecure Email Certificateのエンド・エンティティ情報を本人に代わって提出する。その後、Comodoがホストとして提供するオンラインの証明書生成及び取得施設にログインするのに必要な情報が含まれた電子メールがエンド・エンティティに配送される。

オンラインの証明生成及び取得施設にログインすると、エンド・エンティティのブラウザは公開鍵と秘密鍵の鍵ペアを生成する。公開鍵はComodoに提出され、Comodoはその公開鍵を含むSecure Email Certificateの法人版を発行

する。その後、自動化された暗号チャレンジを行い、証明書の申請者が自動申請プロセスの際に送信した公開鍵に関連する秘密鍵を所有しているかどうかを検証する。自動チャレンジが成功した場合、Comodo は加入者に電子証明書を発行する。

4.3. 証明書申請の検証情報

Comodo 証明書の申請者は、申請者の本人確認を行うための適切な文書により、検証の裏づけがなされる。
Comodo の要件、電子署名の用途の営業内容に応じ、または法律の規定により、個人の申請情報に関連する条件をまれに変更することがある。

4.3.1. 法人組織申請者の申請情報

以下は Comodo が発行する法人組織用証明書の重要な情報要素である。以下の項目中「公開」と表記されている項目は、発行される証明書内に表示され、パブリック・ドメイン内に存在する。「公開」の表記がない項目については、本 CPS に概要を示した機密情報及びデータ保護とともに、機密情報として扱われる。

- 法人組織の正式名称（公開）
- 所属部署名（公開）
- 所在地（番地、郵便番号、国）（公開）
- VAT 番号（該当する場合のみ）
- 企業番号/DUNS 番号（該当する場合のみ）
- サーバー・ソフトウェアの ID
- 支払い情報
- 管理者の連絡先（氏名、電子メールアドレス、及び電話番号）
- 支払い請求担当者及び担当部署の代表者
- 完全な適格ドメイン名、ネットワーク・サーバー名、パブリックまたはプライベート IP（公開）
- 公開鍵（公開）
- 名称使用権の証明書類
- 法人組織の存在証明及び格付け情報の証明書類
- 署名済みの加入者契約書（オンライン以外の方法で申し込まれた場合）

4.3.2. 法人組織申請者の補助文書

法人組織の申請には、以下のいずれかあるいはすべての文書が必要である。

- 会社約款
- 事業免許

- 遵守証明書
- 会社設立証明書
- 納税証明書
- 法人組織設立許可
- 政府組織の認定された代表者からの正式な書状
- 学部長あるいは学長からの正式な書状（教育機関の場合）

Comodo の自由裁量により、これら以外の公式な法人組織からの文書を伴った申請を認める場合がある。

4.3.3. 個人申請者の申請情報

以下は、Comodo が個人に証明書を発行する際に重要な情報の要素である。

- 個人の正式氏名（公開）
- 所属部署名（公開）
- 所在地（番地、郵便番号、国）（公開）
- VAT 番号（当該当する場合のみ）
- サーバー・ソフトウェアの ID
- 支払い情報
- 管理者の連絡先（氏名、電子メールアドレス、及び電話番号）
- 支払い請求担当者及び担当部署の代表者
- サーバ名（FQDN）、ネットワーク・サーバー名、パブリックまたはプライベート IP（公開）
- 公開鍵（公開）
- 名称使用権の証明書類
- 法人組織の存在証明及び格付け情報の証明書類
- 署名済みの加入者契約書（オンライン以外の方法で申し込まれた場合）

4.3.4. 個人申請者の補助文書

個人の申請には、本人確認ができる要素を含む以下の文書が必要である。

- パスポート
- 運転免許証
- 銀行口座計算書

Comodo の自由裁量により、これら以外の公式な法人組織からの文書を伴った申請を認める場合がある。

4.4. 証明書申請の検証要件

電子証明書の申請書を受理した時点で提出された情報に基づき、Comodo は以下の情報の確認を行う。

- 証明書の申請者が証明書要求の名義人と同一人物であること
- 証明書の申請者が証明書に含まれる公開鍵に対応する秘密鍵を所持していること
- 証明書に表示される情報が正しいこと（検証対象ではない加入者情報は覗く）
- 証明書を申請した代理人が、証明書申請者の公開鍵を証明書に記載する正当な認可を得ていること

Comodo 証明書の種類を問わず、加入者は、提出した情報の正確性を監視し、証明書の有効性に何らかの影響を及ぼすいかなる変更についても、Comodo に通知する継続的な義務を有する。加入者契約で規定された当該義務の不履行は、加入者へ通知することなく、加入者の電子証明書の失効に帰される。加えて、加入者は契約に基づき、未払いの支払うべき請求金額を全額支払う。

4.4.1. 企業法人情報の第三者確認

Comodo は、電子証明書を申し込んだ企業法人の情報確認に、第三者サービスを利用することがある。Comodo は第三者法人組織、その他の第三者のデータベース、及び政府機関からの確認を仰ぐものである。

Comodo は、申請した企業の登記を確認し、重役会のメンバー、及び企業を代表する役員会を明記する同業者信用照会の謄本を含めた管理を行う。

Comodo は、法人組織あるいは個人の申請者の実在性や本人確認をするために、いかなる通信手段をも自由に用いる。Comodo は、なんら制限を受けることなく、自由裁量の拒否権を留保する。

4.4.2. シリアル番号の割り当て

Comodo は、Comodo 証明書に表示される証明書のシリアル番号を割り当てている。割り当てられるシリアル番号は唯一無二の番号である。

4.5. 提出されたデータの確認時機

Comodo は証明書申請情報の確認に十分な努力を行い、正当な期間内に電子証明書を発行する。

Comodo は、必要な本人確認に必要な検証情報を受理してから 2 日以内に、本 CPS に基づきすべての証明書を発行することを保証する。

4.6. 証明書申請の承認と拒否

証明書申請に必要なすべての検証が無事に完了すると、Comodo は電子証明書の申請を承認する。

証明書申請の検証結果が条件に満たない場合、Comodo は証明書の申請を拒否する。Comodo は、独自の評価により、証明書を当該関係者に発行することで、評判の良い、信頼される Comodo の社名が汚されたり、矮小化されたり、あるいは企業価値を低減されたりする可能性がある場合、申請者への証明書の発行申請を拒否する権利を留保する。また、前述の状況においては、証明書申請を拒否した結果生じるいかなる損失や費用に対する義務、あるいは責任からも免除される。

申請が拒否された申請者は、その後再申請することができる。

4.7. 証明書の発行と加入者の同意

証明書申請が承認されると、Comodo は証明書を発行する。電子証明書は加入者がそれを受領した瞬間から有効とみなされる（本 CPS の第 4.9 節参照）。電子証明書の発行は、Comodo が証明書の申請を認めたことを意味する。

4.8. 証明書の有効期限

証明書は Comodo が発行し、加入者が受理した時点から有効となる。一般的には、証明書の有効期限は 1 年、2 年または 3 年のいずれかであるが、Comodo はこれらの標準的な有効期限以外の有効期間を提示する権利を留保する。

4.9. 加入者による証明書の受領

発行された証明書は電子メールで配送されるか、あるいはオンラインの取得方法を通じて、加入者のコンピュータ・ハードウェアセキュリティ・モジュールにインストールされる。加入者は以下により証明書を受領したとみなされる。

- 加入者が証明書を使用したとき
- 証明書の発行から 30 日を過ぎたとき

4.10. 電子署名の実在性確認

電子署名実在性確認は、以下を判断するために行われる。

- 電子署名が署名者の証明書に記載された公開鍵に対応する秘密鍵によって作成されたこと
- 当該電子署名に関連する署名されたデータが、電子署名が作成されてから変更されていないこと

4.11. 電子署名の信頼性

検証した電子署名を信頼するかどうかの最終的な判断は、信頼者の一存によるものである。電子署名の信頼性は、以下の場合に限り発生する。

- 電子署名が有効な証明書の運用期間内に作成されていて、検証された証明書を参照すると、実在性確認ができる場合
- 信頼者が、関連する証明書失効リストを確認して証明書の失効状態を確認し、当該証明書が失効していないことを確認した場合
- 信頼者が、電子証明書が特定の目的のために加入者に発行されていることを理解し、電子証明書に関連する秘密鍵が、当該 CPS に示唆された方法に従ってのみ使用され、証明書プロファイルでは Object Identifiers と名付けられることを理解した場合

信頼性は、本 CP に基づいて信頼者のために設けられた条項の下、及び信頼者契約の範囲内で正当であると認められる。環境の信頼性が、本 CPS の条項に基づき Comodo が供与する保証を超えている場合は、信頼者は追加保証を求めなければならない。

保証は上記の手順がすべて実行された場合にのみ有効である。

4.12. 証明書の一時停止

Comodo は証明書の一時停止は行わない。

4.13. 証明書の失効

証明書の失効は、証明書に明記の有効期限に至る前に、証明書の有効期間を恒久的に終了することである。Comodo は以下の場合に証明書を失効する。

- 当該証明書に関連する秘密鍵の損失、盗難、改変、不正な暴露、または危殆化
- 加入者あるいは Comodo による本 CPS 規定の必須義務不履行
- 本 CPS の規定の義務が、加入者あるいは Comodo によって遅延されたか、自然災害、コンピュータまたは通信障害、人間が正当に制御できる範囲を超えたその他の原因によって履行されなかったか、あるいは他者の情報が、著しく脅威にさらされたか危殆化された場合
- 証明書に含まれている加入者に関する情報の改変

4.13.1. 失効要求

加入者または RA のように適切に認可された関係者は、証明書の失効要求をすることができる。証明書の失効に先立ち、Comodo は以下の事項について失効要求の審査を行う。

- 証明書を申請した法人組織あるいは個人によって要求されていること
- RA を使用して証明書申請を代行させた法人組織あるいは個人の場合、申請と同じ RA によって失効が要求されていること

Comodo は、以下の手順により失効要求の認証を行う。

- 失効要求は、証明書申請に関連する管理者の連絡先によって受領される必要がある。Comodo は必要に応じて、法人組織の連絡先や、支払い請求担当者による失効リクエストを求めることもある
- 失効要求の受領後、Comodo は既知の管理者のオンライン以外の連絡先情報、つまり電話またはファックスのいずれかによる確認を求める
- 続いて、Comodo の審査担当者は証明書の失効と審査担当者の本人確認情報の記録を命じ、失効理由については、本 CPS に規定されている記録手順に従って維持される。

4.13.2. 失効の効果

証明書の失効により、当該証明書の運用期間は即座に終了したとみなされる。失効した証明書のシリアル番号は、証明書失効リスト（CRL）に掲載され、証明書の本来の有効期限が過ぎるまで CRL 上に残される。更新された CRL は Comodo のウェブサイトに 24 時間ごとに公開されるが、特殊な状況によっては、より頻繁に CRL 公開する可能性がある。

4.14. 更新

申請時に選択したオプションによって、Comodo 証明書の有効期限は、発行日より 1 年（365 日）、2 年（730 日）、あるいは 3 年（1,095 日）のいずれかとなり、証明書の関連フィールドに詳細が示される。

更新料は Comodo の公式 Web サイトで確認するか、証明書の有効期限が近付いている加入者に送信される文書に詳細を示す。

更新申請要件及び手順は、新規顧客の申請検証及び発行要件に準じる。

4.15 有効期限の事前通知

Comodo は、電子証明書の有効期限が近付いていることを、加入者に電子メールで通知をする正当な努力を行う。通知は通常、証明書の有効期限が切れる前の 60 日以内に行われる。

5. 発行に関する法的義務

本節は Comodo の電子証明書に関する法律上の事実の表示、保証、及び制限について解説する。

5.1. Comodo の事実の表示

Comodo は、すべての加入者及び信頼者に対し、以下に列記する当社の公共サービスに関する事実の表示を確認する。Comodo は、適正であると判断した場合や、法律によって義務付けられた場合は、以下の事実の表示を変更する権利を留保する。

5.2. 電子証明書に組み込まれる参照情報

Comodo が発行するすべての電子証明書は、以下の参照情報が組み込まれる。

- 電子証明書の利用規定
- 本 CPS の参照場所を含む、発行済み Comodo 証明書に明記されるすべての証明書ポリシー
- X.509v3 標準の必須要素
- X.509v3 標準の必須要素ではなく、X.509v3 標準をカスタマイズしたもの
- 証明書内で完全には表記されていないエクステンションと、拡張ネーミングの内容
- 証明書にフィールドが表示されているその他の情報

5.3. 補償制限及び保証拒否

Comodo 証明書には、補償制限、トランザクションの上限額、有効期間、証明書の用途、及び適用の可能性のある保証拒否を記述したショートステートメントが含まれている。加入者は証明書の契約を交わす前に、Comodo の契約条件に合意する必要がある。情報の通信に、Comodo は以下を利用することがある。

- 法人組織の属性
- 証明書ポリシーへの Comodo の標準的なクウォリファイヤー
- 所有権登録済みのエクステンションまたは他ベンダーの登録済エクステンション

5.4. 証明書失効データの公開

Comodo は CRL（証明書失効リスト）を表示どおりに公開する権利を留保する。

5.5. 提出情報の正確性を監視する義務

あらゆる場合において、且つすべての Comodo 証明書に関し、加入者は提出した情報の正確性を絶えず監視し、いかなる変更も Comodo に通知する義務を有する。

5.6. 情報の公開

公開された重要情報は、本 CPS に規定の方法に基づき、随時更新される。当該更新は、改訂された情報上に適切なバージョン番号と公開日を表示して示される。

5.7. Comodo 実装の改造

加入者、信頼者、及びその他の関係者は、本 CPS において明示的に許可されている場合、または事前に Comodo の書面による許可を受けている場合を除き、鍵生成プロセス、公式 Web サイト、及び Comodo リポジトリを含む Comodo PKI サービスの技術的な実装を改造したり、リバース・エンジニアリング処理を施してはならない。加入者による本項の不履行は、当該加入者に通知することなく電子証明書の失効に帰され、加入者は本契約書に基づく未払いの支払うべき請求金額を全額支払うものである。信頼者による本項の不履行は、信頼者との契約終了に帰され、Comodo が提供する Comodo リポジトリ及び電子証明書またはサービスの使用あるいはアクセスの許可が取り下げられる。

5.8. 標準

Comodo は、ユーザー・ソフトウェアが X.509v3 に準拠し、その他の適用される標準規格が本 CPS に規定の要件を実現しているものと仮定する。Comodo は当該ユーザー・ソフトウェアが、Comodo の求める制御機能をサポートし、実現できるものであることを保証することはできないが、ユーザーは適切な助言を求める必要がある。

5.9. Comodo パートナーシップの制限

Comodo ネットワークのパートナーは、Comodo 製品及びサービスに関連する信用を脅かしたり、疑いを招じさせたり、低下させる恐れのあるいかなる行動も慎まなければならない。Comodo のパートナーは、特に、他のルート認証局とのパートナーシップ締結や、ルート認証局からの手順の採用は控えるものとする。本項の不履行は、信頼者との契約終了、及び Comodo が提供する Comodo リポジトリ及び電子証明やサービスの使用あるいはアクセスの許可の取り下げに帰される。

5.10. Comodo パートナーに対する Comodo の責任制限

Comodo のネットワークには Comodo の規程及び手順に基づき運用される RA を含むので、Comodo の自社ルートの元に発行されるすべての証明書の真正性を、Comodo の保険契約の限度額を超えない範囲で保証する。

5.11. 暗号化方式の選択

関係者は、PKI は言うまでもなく、各自の安全要件のソリューションと同様に、各自のパラメータ、手順、及びテクニックを含むセキュリティ・ソフトウェア、ハードウェア、及び暗号化・電子証明書アルゴリズムの選択に各自が責任をもって判断を下し、適切なトレーニングを実施する責任を有する。

5.12. 実在性確認のされていない電子署名の信頼性

電子証明書を信頼する関係者は、Comodo が公開している関連の CRL で当該電子証明書の有効性をチェックして、常に電子証明書の実在確認を行う必要がある。信頼者は、実在性が未確認な電子証明を加入者の有効な署名として選定することはできないことに留意する。

実在性確認を行っていない電子署名を信頼することは、信頼者がすべてのリスクを負うものであって、Comodo は何ら責任を問われるものではない。

Comodo は、本 CPS 及び Comodo 公開リポジトリ（www.comodogroup.com/repository）で公開されているその他の文書を通じ、または本 CPS の「文書管理」の節に記載された問い合わせ先のアドレスを通じた例外的な方法で連絡を取ることによって、電子署名の利用方法と審査に関する適切な情報を本 CPS を用いて信頼者に通知するものである。

5.13. 拒否された証明書の申請

拒否された証明書を申請する際に提出された公開鍵に関連する秘密鍵は、署名が拒否された証明書に基づいて信頼を形成する場合、いかなるときも電子署名の作成に使用してはならない。当該秘密鍵はまた、他の証明書の申請に再提出してはならない。

5.14. 証明書発行の拒否

Comodo は適正であると判断した場合、いかなる関係者に対しても証明書の発行を拒否する権利を留保する。当該拒否に際して発生するいかなる損失や支出についても、Comodo はなんら義務や責任を問われるものではない。

5.15. 加入者の義務

本 CPS に別段の記載がない限り、加入者は以下の責任を果たすものとする。

- 適切な知識を確保し、PKI のトレーニングを内部で行うことにより、秘密鍵の危殆化の内部リスクを最低限に

抑制する

- Comodo または Comodo RA に提出した証明書要求と関連して使用される秘密鍵と公開鍵の鍵ペアを自身で生成する
- Comodo または Comodo RA に提出した公開鍵が、使用される秘密鍵と対応していることを保証する
- Comodo または Comodo RA に提出した公開鍵が、正しい鍵であることを保証する
- Comodo または Comodo RA とのコミュニケーションに正しく正確な情報を提供する
- 証明書が有効な間のいかなる段階においても、初めに送信した情報に変更があった場合は、Comodo または Comodo RA へ報告する
- Comodo または Comodo RA に要求する証明書と関連して使用する新規の安全な鍵ペアを生成する
- Comodo リポジトリ（www.comodogroup.com/repository）で公開されている本 Comodo CPS のすべての契約条件及び関連ポリシーについて、熟読し、理解し、合意する
- Comodo 証明書を改ざんしない
- 本 CPS で示されている使用法及び規程に従い、合法的かつ正当に認められた目的のために Comodo 証明書を使用する
- 証明書の情報が紛らわしかったり、古かったり、無効な場合は、Comodo 証明書の使用を中止する
- 有効期限が切れていたり、元々インストールされていたアプリケーションやデバイスから消去された Comodo 証明書の使用を中止する
- エンド・エンティティの電子証明書やサブ CA の電子証明書の発行に、Comodo が発行した証明書に含まれている公開鍵に対応する加入者の秘密鍵を使用しない
- Comodo 証明書に公開される公開鍵に対応する秘密鍵の危殆化、損失、露呈、改変、またはそれ以外に、秘密鍵を不正に使用されないよう正当な努力を行う
- Comodo 証明書の真正性に著しい影響を及ぼす事件が発生した場合は、証明書の失効を要求する
- パートナーやエージェントが秘密鍵の生成、保管、エスクロー・サービスまたは秘密鍵の破棄を行う際の行動と怠慢

5.16. 受領の加入者による表明

証明書の受領に伴い、加入者は受領時から追加通知までの間に、Comodo 及び信頼者に対し以下に挙げる事実の表明を行う。

- 証明書に含まれている公開鍵に対応する秘密鍵を使用して作成した電子署名が加入者の電子署名で、証明書を受領していること。また、証明書は電子署名が作成された時点で、適切に運用されていること
- 加入者の秘密鍵に、許可されていない人間がアクセスした履歴がないこと
- 証明書に含まれる情報に関して、加入者が Comodo に提出したすべての報告が正確で真実に基づいていること
- 証明書に含まれているすべての情報が、加入者の知りうる限り、あるいは加入者が当該情報の通知を受けるまでは正確かつ真正な情報であり、同時に、当該情報に重大な誤りがあった場合は、速やかに Comodo に通知すること

- 証明書を、正式に認められた合法的な目的に限り、本 CPS に従って使用すること
- Comodo 証明書を、電子証明書の法人組織フィールドに明記されているエンティティと関連している場合にのみ使用すること(該当の場合のみ)
- 加入者は自身の秘密鍵の管理を怠らず、信頼できるシステムを使用し、秘密鍵の損失、露呈、改変、または不正な使用を防ぐべく正当な予防策を講じること
- 加入者は CA ではなく、エンドユーザー加入者であって、加入者と Comodo の間で、別途書面による合意がない限り、証明書(またはその他の認定された公開鍵のフォーマット)または CRL に、CA あるいはそれ以外の何者としても、証明書に記載されている公開鍵に対応する秘密鍵を署名目的に使用しないこと
- 加入者は本 CPS の契約条件、及び Comodo の他の契約及びポリシー規程に合意すること
- 関係者は、その居住国、または販売領域における知的所有権の保護、ウィルス、コンピュータシステムへのアクセスなどの関連法を含む適用法に準拠すること
- 加入者は適用される可能性のある二重利用製品の輸出法及び輸出規制に準拠すること

5.17. 加入者による損失補償

証明書を受領することにより、加入者は、Comodo ならびにその代理人及び契約当事者をいかなる行為または怠慢の責任からも補償し、Comodo 及び前述の関係者に損害を与えないものとする。当該行為または怠慢の結果として、証明書の使用や公開が原因となり、以下の状況により生じる責任、損失や損害、及び適正な弁護士費用を含む訴訟費用やあらゆる種類の経費が発生する

- 加入者または代理人によって提供されたデータに虚偽または不当表示がある場合
- 加入者が重大な事実を隠蔽し、不当表示あるいは怠慢が、過失または CA、Comodo、あるいは証明書の受領者または証明書の信頼者を欺く目的でなされた場合
- 秘密鍵を含む加入者の機密データ保護の不履行、または加入者の機密データの危殆化、損失、露呈、改変あるいは不正使用を防ぐために必要な正当な予防策の不行使
- 関係者は、その居住国、または販売領域における知的所有権の保護、ウィルス、コンピュータシステムへのアクセスなどの関連法を含む適用法に準拠すること

5.18. Comodo 登録局の義務

Comodo RA は本 CPS に詳細を示すポリシー及び規程と同様に、関連する Web ホストリセラー契約、Powered SSL 契約及び EPKI マネージャアカウント契約に基づいて運用される。RA は契約により以下を義務付けられる。

- 本 CPS に従った Comodo 証明書の申請の受理
- Comodo の審査手順及び本 CPS に規定されたすべての実在性確認の実行
- Comodo の失効手順及び本 CPS に従った Comodo 証明書のすべての失効要求の受理、実在性確認及び Comodo への取次ぎ
- 関連法及び規制に基づく行為

5.19. 信頼者の義務

Comodo 証明書を信頼する関係者は、Comodo 証明書を十分に信用するために、以下を実行する必要があることを了承するものである。

- 電子証明書と PKI の使用に関する十分な知識を得るための適切な努力を行い、不正な証明書、失効した証明書、有効期限が切れた証明書あるいは拒否された証明書によって作成された電子署名を信頼するリスクを最低限に抑える
- 電子証明書の使用制限を学び、Comodo の電子証明書を使用して行えるトランザクションの最高額を信頼者契約を通じて確認する
- Comodo CPS 及び信頼者契約の契約事項を熟読し、合意する
- 関連の CRL ならびに、Comodo リポジトリで入手できる中間 CA 及び CRL とルート CA の CRL を参照して、Comodo 証明書の実在性確認を行う
- Comodo 証明書が有効で、失効されていたり、有効期限が切れていない場合にのみ証明書を信頼する
- 本節及び本 CPS で関連する他の節に掲載されている状況下で正当と思われる場合に限り Comodo 証明書を信頼する

5.20. 情報の合法性

本 CPS に基づいて発行される証明書で使用するために加入者が提示した情報の合法性は、当該内容が使用されたり表示されるすべての裁判管轄において、加入者がすべての責任を負うものである。

5.21. 信頼者に対する加入者の責任

本 CPS に明記された他の加入者義務に制限を設けることなく、加入者は証明書のいかなる不実の表示についても、証明書の表示を正当に信頼し、当該電子証明書の 1 つ以上の電子署名の実在性確認を行った第三者に対する責任を有する。

5.22. 代理人の監視義務

加入者は代理人が Comodo に提供するデータを管理するとともに、その責任を負うものである。代理人によるいかなる不当表示及び怠慢についても、加入者は発行者に速やかに報告する義務がある。本項の義務は継続される。

5.23. 代理人の使用

加入者の代理人の要求によって発行された証明書の場合、代理人及び加入者の両者が連帯で、それぞれ Comodo、及びその代理人と契約当事者への補償を行う。

5.24. Comodo リポジトリ及び Web サイトの利用条件

Comodo リポジトリ（www.comodogroup.com/repository）及び公式 Web サイトにアクセスする関係者（加入者と信頼者を含む）は、本 CPS の条項及び Comodo が提示するその他の利用条件に合意する。

関係者が Comodo の発行した証明書を使用することにより、本 CPS の利用条件を受諾したとみなされる。

Comodo リポジトリ及び Web サイトの利用条件への準拠の不履行は、Comodo と当該関係者間の関係の終了を伴う場合がある。

5.25. 情報の正確性

Comodo は自らが信頼される立場にあることを自負し、あらゆる適正な努力を行い、弊社のリポジトリにアクセスする関係者が、正確で、更新された、正しい情報を受理できるよう保証する。Comodo はしかしながら、本 CPS 及び Comodo の保険契約に規定されている制限を超えるいかなる義務についても、認めることはできない。

Comodo リポジトリ及び Web サイトの利用条件の不履行は、Comodo と当該関係者間の関係の終了を伴う場合がある。

5.26. Comodo の義務

本 CPS の関連する節において規定された範囲で、Comodo は以下を行うことを約束する。

- 本 CPS 及び社内または公開されたポリシーと手順に準拠する
- 適用法と規制に準拠する
- PKI サービスを運用するための Comodo リポジトリ及び Web サイトの設立及び運営を含むがそれに限られない、基盤と認証サービスを提供する
- 自社の基盤に関して、鍵生成メカニズム、鍵の保護、及び秘密共有手順を含む信頼の仕組みを提供する
- 自社の秘密鍵が危殆化した場合は、速やかに通知する
- 幅広く一般的に使用されるよう、多様な種類の証明書の申請手順を提供し検証を行う
- 本 CPS に従って電子証明書を発行し、ここに提示される自社の義務を全うする
- Comodo のネットワーク内で運用している RA からの要求を受理したら、本 Comodo CPS に従い速やかに

Comodo 証明書を発行する手配を行う

- Comodo のネットワーク内で運用している RA からの要求を受理したら、本 Comodo CPS に従い速やかに Comodo 証明書を失効する手配を行う
- 本 CPS に従い、認証された証明書を発行する
- 本 CPS に規定の通り、加入者及び信頼者にサポートを提供する
- 本 CPS に従い証明書を失効する
- 本 CPS に従い、証明書の有効期限完了手続き及び更新を行う
- 本 CPS と適用されるポリシーのコピーを、要求した関係者に提供する
- 欧州指令 99/93 の用件に European Directive 従って発行された適格証明書に公開される情報の正確性を保証する
- European Directive 99/93 に規定の適格証明書の要件に従って発行された証明書の発行時刻に、署名者が秘密鍵を所有していたことを保証する

Comodo は本 CPS に基づき、いかなる追加義務も有さないことを、加入者は承認するものである。

5.27. 特定目的適合性

Comodo は、ここに含まれていて、法律上除外できないものを除き、特定目的適合性の保証及び提供された実在性の確認されていない情報の正確性の保証を含む、いかなる種類の保証や義務も否認する。

5.28. その他の保証

European Directive 99/93 の要件に従って発行された適格証明書に関連して明記されている場合を除き、Comodo は以下の保証は行わない。

- 本 CPS の下記の関連製品の説明、または Comodo の保険契約において明記されているものを除き、証明書に含まれている情報の実在性が確認されていないか、あるいは Comodo の代理によりコンパイルされているか、公開されているか、または配布されている情報の正確性、確実性、完全性または適合性
- Comodo Personal Certificate の Class1、無料版、トライアル版またはデモ用証明書に含まれる情報の正確性、確実性、完全性あるいは適合性
- 本 CPS の下記の関連製品の説明に明記されている場合を除き、証明書に含まれる情報の事実の表示に関する責任は問われない
- いかなるソフトウェア、またはハードウェアの品質、機能または性能に対する保証
- Comodo は証明書の失効に対する責任を有するが、自社の制御の範囲を超えた理由により証明書の失効を実行できない場合は、責任を問われない
- Comodo が特に明記していない限り、第三者（代理人を含む）によって発行された証明書のディレクトリの有

効性、完全性あるいは可用性

5.29. 実存性確認をしていない加入者の情報

本 CPS の製品に関する節に基づく制限保証にも拘らず、European Directive99/93 の要件に従って発行された適格証明書と関連して別途明記のない限り、実存性確認がなされていない加入者情報が、Comodo、または Comodo のディレクトリ、あるいは証明書への掲載を意図して提出された場合は、Comodo は責任を問われない。

5.30. 損害要素の一部除外

詐欺または故意の過失を除き、以下の場合,いかなる場合も、Comodo はなんら責任を負うものではない。

- 間接的、偶発的あるいは必然的な損害
- 利益の損失
- データの損失
- その他、証明書あるいは電子署名の使用法、配送、ライセンス、機能または機能しないことに由来して、または関連して生じるその他の間接的、偶発的あるいは懲罰による損害
- 本 CPS の枠内で提供されている以外のトランザクションまたはサービス
- 信頼に由来する原因以外の、証明書に掲載された情報、証明書の実在性が確認された情報に関するその他の損害
- 実在性を確認した情報の欠陥が、申請者の詐欺行為あるいは故意の過失を原因として発生した場合のすべての義務。本 CPS に準拠して発行または使用されなかった証明書の利用から生じるすべての義務
- 有効ではない証明書の使用法から生じるすべての義務
- 証明書または本 CPS に明記された使用法、価値、及びトランザクションの制限を超えた証明書の利用から生じるすべての義務
- 加入者が使用するハードウェア及びソフトウェアを含む各種製品の安全性、可用性、真正性から生じるすべての義務
- 加入者の秘密鍵の危殆化から生じるすべての義務

Comodo は死亡や個人の傷害についての義務は制限や除外をしない。

5.31. 証明書の保険プラン

故意の違反行為の範囲を除き、証明書のクラス及び、または種類に適した方法を用いて検証された証明書の加入者に属する無効な情報を含む証明書を発行したことに対して、Comodo が認める累積最高保証額を以下に列記する。

5.31.1. InstantSSL 証明書

InstantSSL 証明書の申請者、加入者、及び信頼者それぞれに対する累積最高保証額は、$ 50.00（五拾 USドル）未満である。

5.31.2. InstantSSL　Pro 証明書

InstantSSL　Pro 証明書の申請者、加入者、及び信頼者それぞれのに対する累積最高保証額は、$ 2,500（二千五百 USドル）未満である。

5.31.3. PremiumSSL 証明書

PremiumSSL 証明書の申請者、加入者、及び信頼者それぞれに対する累積最高保証額は、$ 10,000.00（壱万 USドル）未満である。

5.31.4. InstantSSL Wildcard 証明書

InstantSSL 証明書の申請者、加入者、及び信頼者それぞれに対する累積最高保証額は、$ 10,000.00（五拾 USドル）未満である。

5.31.5. IntranetSSL 証明書

申請者、加入者、及び信頼者への債務はない。

5.31.6. Trial SSL 証明書

申請者、加入者、及び信頼者への債務はない。

5.32. 証明書利用額の制限

Comodo 証明書は、証明書に関連し、本 CPS の第 5.31 節に詳細を示す保証のレベルを超えない金額（US＄）の価値を有するデータ転送及びトランザクションに関連してのみ使用される。

5.33. 損害と損失の制限

いかなる場合（詐欺または故意の違法行為を除く）においても、証明書に関連するすべての電子署名及びトランザクションの加入者、申請者、受理者、または信頼者を制限することなく含むすべての関係者に対する Comodo の債務総額は、本CPSの第 5.3.1 節に詳細を示す Comodo の保険プランに明記されている証明書の負債額の上限を超えることはない。

5.34. 規則の抵触

本 CPS が他の規則、ガイドライン、または契約に抵触する場合は、他の契約が以下のいずれかの場合を除き、本 CPS（2003 年 4 月 16 日付）が優先され、加入者及びその他の関係者は本 CPS を守る義務を負うものとする。

- 本 CPS の現行バージョンを初めて一般公開した日より前の日付の場合
- 当該契約が明示的に本 CPS に優先し、そのため当該契約がそれに関連する関係者を法律が認める範囲で支配する場合

5.35. 知的所有権

Comodo またはそのパートナーあるいは提携者は、本 CPS を含む Comodo に由来するデータベース、Web サイト、Comodo 電子証明書及びその他すべての発表物に関連するすべての知的所有権を有する。

5.36. 権利の侵害及びその他の損害要素

Comodo の加入者は、Comodo に提出するとき、及びドメイン名と識別名★Distinguished name★、及びその他のすべての証明書申請情報を使用するときは、商標権、サービス・マーク、商号、法人名称、またはその他の知的所有権に関し、いかなる裁判管轄におけるいかなる第三者の権利も、妨害や当該権利を侵害しないことを表明し、保証するとともに、ドメイン名及び識別名を、無制限に、契約の婉曲的な妨害や、将来有望な事業の有利性、不等な競争、他社の評判の侵害、及び個人を錯乱または誤解させるようなことを含むいかなる不法な目的においても使用を意図しないものである。

5.37. 所有権

証明書は Comodo の所有物である。Comodo は当該証明書が完全に再作成され配布されるという条件の下、非独占的な、ロイヤルティ支払い義務のない証明書の再作成及び配布許可を与える。Comodo は証明書を随時失効する権利を留保する。

秘密鍵と公開鍵は、合法的にそれらを生成し、保持する加入者の所有物である。

Comodo の秘密鍵のすべての秘密の分配(配布された要素)は、Comodo の所有権の範疇にとどまる。

5.38. 準拠法

本 CPS は英国の法律に準拠し、同法に従って解釈される。同法律は、居住地や Comodo 電子証明書あるいはその他の製品やサービスを使用する場所に関わらず、本 CPS の均一な解釈を確保するために選択される。英国法は、Comodo が提供者であり、供給者であり、受益者であり、またはその他の役割を果たす Comodo 製品及びサービスに関連して、本 CPS が適用されるか、または黙示的または明示的に引用されるすべての Comodo の商業的関係あるいは契約上の関係に適用される。

5.39. 裁判管轄

Comodo のパートナー、加入者及び信頼者を含む各関係者は、本 CPS または Comodo の PKI サービスの条項から発生するか、あるいは関連して発生するいかなる控訴、法的措置、あるいは訴訟についても、審問及び判決の専属管轄権が英国及びウェールズ裁判所にあることを絶対的に合意するものである。

5.40. 紛争解決

裁判あるいはいかなる種類の裁判外紛争処理(簡易裁判、調停、拘束力のある専門家の勧告、共同監査及び一般専門家の勧告を含む)を含むいかなる紛争解決の仕組みに訴える前に、関係者は紛争解決を目指す目的で、Comodo に紛争の通知をすることに合意する。

5.41. 後継者及び譲受人

本 CPS は、後継者、指定遺言執行者、相続人、代表者、管理者に義務を負わせ、明示されたか、黙示されたか、明白であるかによらず、関係者を指定するものである。本 CPS に詳細を示す権利と義務は、当該譲渡が本 CPS 条項の

運用の終了または停止に反することなく行われた場合、または、当該譲渡が、譲渡する関係者が、当該契約の締結時に他の関係者に負っている他のいかなる債務または義務の更改に影響しない場合は、関係者、法律の運用（合併あるいは投票権のある株式の支配株式の譲渡の結果も含む）、あるいは別の方法によって譲渡される。

5.42. 契約条項の分離

本 CPS の条項あるいは当該条項が適用される事項（及び無効または強制できない条項の他関係者や状況への適用）が、いかなる理由によっても、またいかなる範囲に及んでも、無効であるかあるいは強制できないと判明した場合は、本 CPS の残りの条項は関係者の本来の意味に影響する方法で解釈される。

本 CPS において責任制限、保証またはその他の義務からの免責事項または制限、あるいは損失の除外を提供するすべての条項は、他のすべての条項から分離可能とみなされ、独立しているとみなされ、そのように施行される。

5.43. 解釈

本 CPS は適正な条件かつ、意図された製品またはサービスの用途の下、ビジネス習慣、商業的な正当な適用範囲内で解釈される。 本 CPS の解釈において、関係者は Comodo のサービスと製品及び国際的な登録ネットワークについて、商習慣上の良識を持って、その国際的な適用範囲や利用方法を考慮しなければならない。

本 CPS の表題、副題、及びその他の説明文は、参照の便宜を図るためだけのものであり、本 CPS のいかなる条項の解釈、構成、または実行にも使用されてはならない。

本 CPS の付録と定義は、本 CPS の真正性と法的拘束力効果のために存在する。

5.44. 権利放棄の無効

本 CPS は包括的に試行され、いかなる人物による本 CPS のいかなる条項の不履行も、将来の当該条項の施行またはその他の条項の施行の権利の放棄とはみなされない。

5.45. 通知

Comodo は、本 CPS に関連する通知を、電子的に署名したメッセージまたは書状の形式で受領する。Comodo から有効な電子的に署名された受領通知書を受理したら、通知の送り主は両者間の通信が有効であるとみなす。送り主は、前述の通知書を 5 日以内に受理するか、あるいは書状の通知を、郵便料金前払いの受取証明郵便または書留郵便

で、配達証明返送が必要な書面として、配送サービスを介し、下記の住所あてに送付する義務がある。

Certification Policy Authority
Black Barn Offices
Cornwells Farm, Sheephurst Lane
Marden, Tonbridge
Kent, TN12 9NS, United Kingdom
Attention: Legal Practices
Email: legal@comodogroup.com

本 CPS、関連契約並びに本書で参照されている証明書ポリシーは、Web サイト（www.comodogroup,com/repository）でも確認することができる。

5.46. 料金

Comodo は、発行、更新及び再発行を含む、Comodo の提供する証明書サービスの一部に対する料金を加入者に請求する（本 CPS の第 5.47 節に記載の「Comodo 再発行ポリシー」に基づく）。当該料金は Comodo の公式 Web サイトにおいて公開されている（www.comodogroup.com 及び www.instantssl.com）。

Comodo は、証明書の失効、または Comodo が発行した証明書の検証状態を、証明書失効リストを通じて確認する信頼者に対しては、料金の請求は行わない。

Comodo は当該料金を変更する権利を留保する。Reseller、Web ホストリセラー、EPIK マネージャアカウント保持者 s、及び Powered SSL Partners を含む Comodo のパートナーは、関連のパートナー契約に詳細を示すとおり、価格改正に適切な忠告を与えることができる。

5.47. 再発行ポリシー

Comodo は、30 日間の再発行ポリシーを提供する。加入者は 30 日（証明書を発行した初日から起算）以内に証明書の再発行を要求することができ、その際は、再発行費用は一切発生しない。公開鍵以外の詳細に改変が必要な場合は、Cpmodo は本 CPS に詳細を示す検証プロセスに従って、当該申請を再検証する権利を留保する。再発行要求が検証プロセスをパスできなかった場合は、Comodo は再発行申請を拒否する権利を留保する。前述の状況では、最初の証明書が失効され、Comodo 全額返金を要求することができる。前述の状況においては、最初の証明書は失効され、代金は申請者に払い戻される。

Comodo は、30 日間の再発行ポリシー期間が切れた後は、証明書の再発行の義務は有しない。

5.48. 払い戻しポリシー

Comodo は、30 日間の払い戻しポリシーを提供する。加入者は 30 日間（証明書を発行した初日から起算）以内に、証明書の全額返金を要求することができる。前述の状況においては、最初の証明書は失効され、代金は申請者に払い戻される。

6. 一般発行手順

6.1. 概要

Comodo は、安全性の高いオンライン・トランザクション及び電子メールを実現するため、SSL 及び S/MIME 技術を利用したさまざまな種類の証明書を提供している。証明書の発行に先立ち、Comdoo は本 CPS に従って申請の検証を行う。検証に際して、Comodo は申請内容の確認に必要な関連する公式文書を申請者に求めることがある。

Comodo 証明書は法人組織あるいは個人に対して発行される。

Comodo 証明書の有効期限は証明書の種類によって異なるが、通常は 1 年、2 年、あるいは 3 年間有効となる。Comodo は、これらの設定された期間以外の有効期限を持つ証明書を、自由裁量で発行する権利を留保する。

6.2. 個人及び法人組織に発行される証明書

証明書要求は以下の方法によって行われる。

オンライン：Web（https）から
証明書の申請者は、Comodo が提供する手順に従い、安全なオンライン・リンクを介して申請を提出する。Comodo は、申請者の本人確認及び実在確認に必要な申請の補助文書として、追加の文書を要求することがある。申請者は Comodo に要求された追加文書を提出する。申請者の実存性が確認できると、Comodo は証明書を発行して申請者に通知を送信する。申請者は証明書をそれぞれのデバイスにダウンロードして、インストールする。申請者は、いかなる不正確な情報や欠損についても、証明書の受理後速やかに Comodo に通知し、また、証明書に含む情報の内容を予め通知する義務がある。

Comodo は自由裁量で申請を電子メールで受理することがある。

6.3. 内容

Comodo 証明書に公開される一般的な情報に含まれる内容を以下に示すが、以下の要素の情報に限定されるものではない。

6.3.1. Secure Server Certificate

- 申請者の完全に適格なドメイン名

- 申請者の法人組織名
- 申請者の国コード
- 所属部署名、番地、市、県
- 証明書発行認証局（Comodo）
- 申請者の公開鍵
- Comodo の電子署名
- アルゴリズムの種類
- 電子証明書の有効期限
- 電子証明書のシリアル番号

6.3.2. Secure Email Certificate

- 申請者の電子メールアドレス
- 申請者名
- 申請者の国コード
- 法人組織名、所属部署名、番地、市、県
- 申請者の公開鍵
- 発行認証局（Comodo）
- Comodo の電子署名
- アルゴリズムの種類
- 電子証明書の有効期限
- 電子証明書のシリアル番号

6.4. 提出されたデータの確認時期

Comodo は、証明書の申請情報を確認し、合理的な時間内に電子証明書を発行する正当な努力を行う。発行までの時間は、加入者が必要な情報及び、または文書を速やかに提出するか否かによって決まる。必要な情報及び、または文書の受領後、Comodo は提出された申請者のデータを確認し、審査プロセスを完了し、2 営業日以内に証明書申請の発行あるいは拒否を実行する。

時により、Comodo の制御できる範囲外のイベントの発生により、発行プロセスが遅れることがあるが、Comodo は発行時間を守るよう全力を尽くすとともに、発行時間に影響を及ぼすと思われるすべての因子を申請者に理解してもらえるよう正当な努力を行う。

6.5. 発行手順

以下に、Secure Server Certificate を発行する際の目安となる手順を示す。

a) 申請者は Comodo のウェブサイトからオンライン・リクエストを入力し、所定の情報を提出する【提出する情報】証明書署名要求(CSR)、電子メールアドレス、一般名、法人組織情報、国コード、実存性確認方法及び支払い請求書情報
b) 申請者はオンライン加入者契約を受領する
c) 申請者は所定の情報を Comodo に提出する
d) 申請者は証明書の料金を支払う
e) Comodo は提出された情報を、第三者データベースや政府機関の記録と照合する
f) 申請情報の検証後、Comodo は申請者に証明書を発行するか、あるいは申請を拒否する発行を拒否する場合、Comodo は申請者に検証結果を伝える
g) 更新は本 CPS 及び Comodo の公式なウェブサイトに概略を示す手順に従って行われる。
h) 失効は本 CPS に概略を示す手順に従って行われる

文書管理

本書は Comodo　CPS のバージョン 2.1 で、2003 年 4 月 16 日に作成され、Comodo 証明書ポリシー局によって監修された。

Comodo CA Limited
New Court,
Regents Place,
Regent Road,
Manchester
M5 4HB
United Kingdom

URL: http://www.comodogroup.com
E-mail: legal@comodogroup.com
Tel:　+44 (0) 161 874 7070
Fax:　+44(0)1618771767