三井住友銀行の ValueDoorIC カード認証サービス

証明書ポリシー／認証局運用規定

2019 年 1 月

Version 3.0

改版履歴		
版数	日付	内容
1.0	2005.03.28	初版発行
1.1	2006.04.17	1.5.2. 連絡先　住所表示の変更
1.2	2010.11.15	1.5.2. 連絡先　住所表示の変更
1.3	2012.03.13	受領書廃止に伴う関連項目の変更
1.4	2013.03.01	ＩＣカード管理責任者を ValueDoor 管理専用ＩＤ保有者へ表記の変更
1.5	2013.04.01	1.5.1.及び 1.5.2.　組織変更に伴う部署名の変更
1.6	2014.10.01	1.1.概要の変更 3.2.2.提出書類の変更 3.2.3.申込み手続きの変更 3.2.5.確認手続きの変更 3.3.1. 4.5.1. 6.1.4. 6.3.2.鍵長及び有効期間の変更 5.2.1 業務責任者の職務内容の変更
1.7	2015.08.03	1.5.2. 連絡先の変更 3.1.2. 名前の意味に関する要件の変更 9.1. 料金の変更
1.8	2015.08.18	目次 1.3.3. 契約者の変更 3.2.2. 契約者の認証の変更 3.2.3. 証明書利用者の認証の変更 3.2.5. 権限の正当性確認の変更 3.3.1. 通常の秘密鍵更新に伴う証明書申込時の識別と認証の変更 3.3.2. 証明書失効後の秘密鍵更新に伴う証明書申込時の識別と認証の変更 6.3.2. 鍵ペアの有効期間の変更

1.9	2017.05.22	目次 1.5.1. CP/CPS を管理する組織の変更 1.5.2. 連絡先の変更 3.1.2. 名前の意味に関する要件の変更 4.5.1. 秘密鍵および証明書の利用の変更 6.1.4. 鍵長の変更 7.1-2 証明書プロファイル　拡張領域の変更 9.7. 補償の変更
2.0	2017.08.21	4.8.1 証明書失効事由の変更 4.9. PIN コードのロック解除手続を追記
3.0	2019.1.21	3.3.1. 通常の秘密鍵更新に伴う証明書申込時の識別と認証 6.3.2. 鍵ペアの有効期間 7.1-1 証明書のプロファイルー基本領域 7.1-2 証明書プロファイルー拡張領域 7.2-1 CRL プロファイルー証明書リスト領域 10. 用語

目次

1. はじめに

1.1. 概要

この三井住友銀行の ValueDoor IC カード認証サービス証明書ポリシー/認証局運用規定（以下「この CP/CPS」といいます）は、株式会社三井住友銀行（以下「当行」といいます）の ValueDoor IC カード認証サービス（以下「本サービス」といいます）を規定するものです。この CP/CPS は、当行の ValueDoor IC カード認証サービス利用規定（以下「サービス利用規定」といいます）に基づいて、当行が契約者（以下「契約者」といいます）により指名された証明書利用者に発行する電子証明書（以下「証明書」といいます）に関する当行のポリシーおよびこのポリシーを運用するための方針、諸手続を定めます。この CP/CPS の変更は、当行の判断によって時宜公表され、その公表をもって発効するものとします。したがって、契約者は、証明書を使用する場合または証明書を信頼して利用する場合において、この CP/CPS の最新の内容を確認することが必要です。この CP/CPS およびサービス利用規定は、当行の Web サイトから入手することができます。

この CP/CPS は、インターネット X.509 公開鍵基盤証明書ポリシーおよび認証運用フレームワークである IETF PKIX RFC3647 に準拠しています。

1.2. 文書の名前と識別

この CP/CPS の正式名称は「三井住友銀行の ValueDoor IC カード認証サービス証明書ポリシー/認証局運用規定」といいます。

1.3. PKI の関係者

1.3.1. CA

CA は、当行または当行以外の企業等が個別サービスごとの規定に基づき提供するサービス（以下「所定のサービス」といいます）の情報交換を安全に行うことを目的に、RA からの発行要求を受け入れ、証明書を発行します。

1.3.2. RA

RA は、契約者からの証明書の発行申込等を受け付け、申込内容の審査を行い、問題がない場合、申込情報をもとに CA に対して証明書発行要求等を行います。

1.3.3. 契約者

契約者とは、本サービスのサービス利用規定に基づいて、当行所定の手続を行うことにより本サービスを利用する法人、法人格なき団体、政府機関、個人事業者等を含む個人消

費者以外の団体および個人をいいます。

1.3.4. ValueDoor 管理専用ＩＤ保有者

当行所定の手続により、契約者が ValueDoor 管理専用 ID 保有者として指定した契約者の役員または従業員で当行が承認した個人をいい、IC カードおよび証明書のすべてについて、当行所定の手続を行う個人をいいます。

1.3.5. 証明書利用者

当行所定の手続により、契約者が IC カードの利用者として指名した契約者の役員または従業員で当行が承認した個人をいい、自己の使用する IC カードまたは証明書について、当行所定の手続を行う権限を契約者から付与された個人をいいます。

1.3.6. 信頼者

信頼者とは、証明書利用者の証明書の有効性を確認し信頼する法人、法人格なき団体、政府機関、個人事業者等を含む個人消費者以外の団体および個人をいいます。

1.3.7. その他の関係者

（1） ポリシー承認機関

当行は、本サービスに関する事項についての意思決定する機関をポリシー承認機関と呼称します。ポリシー承認機関は、当行所定の手続により定められ、本サービスにかかわるこの CP/CPS、関連するポリシーおよび規定を策定し承認する最終的な権限を有します。

1.4. 証明書の利用方法

1.4.1. 適切な証明書の利用

証明書は、所定のサービスの情報交換を、電子署名または暗号化により安全に行うことを目的に用いられるものとします。

1.4.2. 禁止される証明書の利用

証明書利用者は、この CP/CPS「1.4.1. 適切な証明書の利用」およびサービス利用規定に定めのある用法に従って、証明書を利用するものとし、証明書をそれ以外の目的に利用することはできないものとします。

1.5. ポリシー管理

1.5.1. CP/CPS を管理する組織

この CP/CPS の維持、管理は、株式会社三井住友銀行決済商品開発部が行います。

1.5.2. 連絡先

この CP/CPS に関する連絡先は、次のとおりです。

株式会社三井住友銀行 決済商品開発部

1.5.3. CP/CPS のポリシー適合性を決定する者

この CP/CPS の内容に関しては、ポリシー承認機関が適合性を決定します。

1.5.4. CP/CPS 承認手続

この CP/CPS の承認は、当行所定の手続によりポリシー承認機関が行います。

2. 公表とリポジトリの責任

2.1. リポジトリ

当行は、当行のリポジトリを X.500 ディレクトリにて提供します。リポジトリへのアクセスは、一般的な Web インターフェースを通じて可能とします。

2.2. 証明書情報の公表

当行は、次の内容をリポジトリに格納し、証明書利用者および信頼者がオンラインによって閲覧できるようにします。

a. この CP/CPS に基づく証明書失効リスト（以下「CRL」といいます）
b. 当行 CA の自己署名証明書
c. 当行 CA の自己署名証明書の値を SHA-1 で変換した値（フィンガープリント）
d. この CP/CPS の最新版

2.3. 公表の時期および頻度

当行が公表する情報について、公表の時期および頻度は次のとおりとします。

a. CRL は、発行の都度公表します。
b. 当行 CA の自己署名証明書は、発行および更新の都度公表します。
c. この CP/CPS の最新版は、改訂の都度公表します。

2.4. リポジトリへのアクセスコントロール

当行は、この CP/CPS「2.2. 証明書情報の公表」に記載の情報を、リポジトリ上で証明書利用者および信頼者に公表します。ただし、利用可能な時間内においても利用できない場合があります。

3. 識別と認証

3.1. 名前

3.1.1. 名前の種類

すべての識別名は、X.500 識別名（DN :Distinguished Name）の基準を採用します。

3.1.2. 名前の意味に関する要件

当行は、識別名の構成要素である主体者名（CN: CommonName、以下「主体者名」といいます）に反映させる名前として、個人の姓名等や本サービス内で証明書利用者ごとに割り当てられる ID を用いるものとします。個人の姓名等の記録にはローマ字表記を用い、ID の記録には数字を用います。

3.1.3. 利用者の匿名性または仮名性

当行が発行する証明書の主体者名について匿名や仮名は認められません。

3.1.4. 証明書に記載される名前の形式を解釈するためのルール

証明書に記載される名前を解釈するルールは、X.500 の基準に準拠適合するものとします。

3.1.5. 名前の一意性

証明書に記される主体者名は、あいまいさや混乱を避けるために、本サービスにて発行される証明書の中で、明瞭かつ一意なものとします。証明書利用者に対しては属性 CommonName と SerialNumber の組み合わせで名前を一意に識別します。名前を一意にするうえで必要がある場合、数字や文字が付加されることもあります。

3.1.6. 認識、認証および商標の役割

商標の取り扱いは、関連する契約書および適用する法律の定めに従うものとします。

3.2. 初回の識別と認証

3.2.1. 秘密鍵の所有を証明する方法

当行が証明書利用者の鍵ペアを生成し配布するので、公開鍵と秘密鍵の対応および証明書利用者との結びつきは明らかです。

3.2.2.契約者の認証

本サービスを利用する場合、契約者は、当行が合理的に必要と認める文書の提出等、当行所定の手続きを行うものとします。

当行は申込書類その他により下記の事項を確認します。

a. 契約者の住所（所在地）
b. 契約者の氏名（名称）
c. 契約者の申込に関する真正性

3.2.3. 証明書利用者の認証

証明書を発行する場合、契約者は、証明書利用者に関し、当行が合理的に必要と認める文書の提出等、当行所定の手続きを行うものとします。

3.2.4. 検証されない利用者の情報

規定しない。

3.2.5. 権限の正当性確認

当行は、契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者が、本サービスの申込を行うための正当な権限を有しているかを、この CP/CPS「3.2.2. 契約者の認証」および「3.2.3. 証明書利用者の認証」に従い確認します。

3.2.6. 相互運用の基準

規定しない。

3.3. 鍵更新申込時の識別と認証

3.3.1. 通常の秘密鍵更新に伴う証明書申込時の識別と認証

証明書利用者の秘密鍵および証明書の有効期間は、生成の日から当行が定める所定の期間とします。証明書利用者は、原則、当行所定の手続により秘密鍵および証明書の更新（すなわち、新しい証明書の発行）の申込を行うものとします。また、この CP/CPS「3.2.3. 証明書利用者の認証」に記載された方法により、秘密鍵および証明書の更新を申込むことができます。

3.3.2. 証明書失効後の秘密鍵更新に伴う証明書申込時の識別と認証

秘密鍵および証明書の更新の申込のあったときに証明書が失効している場合、または有効期限切れの場合、当行は、この CP/CPS「3.2.3. 証明書利用者の認証」と同一の手続をとるものとします。

3.4. 失効申込時の識別と認証

証明書の失効の申込は、契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者が、当行所定の申込書を、当行の本店/支店の店頭での手交、または当行の営業担当者への手交により、行うことができます。

当行は、当行所定の手続により失効の申込を受け付けた場合、下記の事項を確認し、失効手続を開始するものとします。

a. 当行所定の申込書に押捺された印鑑が契約者届出印と一致していることの確認（印鑑照合）
b. 失効対象となる証明書内の情報が、発行時の情報と一致していることの確認

4. 証明書のライフサイクルに対する運用要件

4.1. 証明書の申込

4.1.1. 証明書の発行の申込を行うことができる者

当行に対する証明書の発行の申込は、契約者が行うことができます。契約者、ValueDoor 管理専用ＩＤ保有者および証明書利用者は、証明書の発行の申込を行う前に、この CP/CPS およびサービス利用規定を承諾するものとします。

4.1.2. 登録手続および責任

当行より所定のサービスで利用する証明書の発行を受けようとする契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者は、この CP/CPS「3.2. 初回の識別と認証」に定める書類を、当行の本店/支店の店頭での手交、または当行の営業担当者への手交により提出するものとします。当行所定の申込書は、当行の本店/支店の店頭での手交、当行からの郵送、または当行の営業担当者からの手交により入手することができます。

なお、指定した方式以外の申込については受け付けません。

4.2. 証明書の発行の申込手続

4.2.1. 識別と認証の手続

当行は、提出された証明書発行の申込について、この CP/CPS「3.2. 初回の識別と認証」に基づく確認を行います。当行は、証明書発行の申込を行った契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者について、当行所定の要件に定める資格を有するかどうかを、当行の裁量に基づいて判断を行うものとします。

4.2.2. 証明書の申込の受理または却下

当行は、申込に対して、証明書を発行するか否かの判断を実施し、契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者に対し、IC カードの発送によって審査結果の通知を行います。

申込に不備がある場合には、IC カードの発送は行わず、書類の再提出を依頼します。

4.3. 証明書発行

4.3.1. 証明書の発行時の処理手続

当行は、当行所定の手続により秘密鍵の生成および証明書の発行を行い、それらを IC カ

ードに格納します。また、必要な PIN コード設定用暗証番号の生成を行います。

4.3.2. 証明書発行通知

当行は、この CP/CPS「4.3.1. 証明書の発行時の処理手続」に定める手続を実施後、ValueDoor 管理専用ＩＤ保有者に対し証明書が格納された IC カードを郵送または手交により提供するものとします。ValueDoor 管理専用ＩＤ保有者は、証明書が格納された IC カードを証明書利用者に渡すことについての責任を有します。

なお、必要な PIN コード設定用暗証番号は、証明書利用者に対し手交または郵送により配付されるものとします。

4.4. 証明書の受領確認

4.4.1. 証明書の受領確認手続

契約者は、証明書利用者が自身の証明書が格納された IC カードを受領したことおよび証明書の内容に誤りがないということの確認を行うものとします。また、証明書利用者は、自身の証明書が格納された IC カードを受領し、証明書の内容に誤りがないということの確認を行うものとします。証明書の内容に誤りがある場合には、当行に対して、証明書に対応する秘密鍵を利用する前にその誤りの修正を求めなければなりません。証明書利用者が対応する秘密鍵を利用した場合には、当行は契約者および証明書利用者が証明書の内容を承認したものとみなし、その承認につき撤回できないものとします。

4.4.2. 証明書の公表

当行は、リポジトリで利用者証明書の公表を行いません。

4.4.3. 第三者に対する証明書発行通知

当行は契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者に対し証明書発行時の通知を行い、原則として第三者に対しては、発行時の通知は行いません。

なお、信頼者から証明書発行等に関する照会があり、当行が合理的であると判断した場合、当行は、当行所定の手続により、これに応じることがあります。

4.5. 鍵ペアと証明書の利用

4.5.1. 秘密鍵および証明書の利用

当行が発行する秘密鍵および証明書は、署名や暗号化を利用し、所定のサービスの情報交換を安全に行うことを目的に用いられるものであって、その他の目的に利用することは認められません。

契約者、ValueDoor 管理専用ＩＤ保有者および証明書利用者は、当行が発行する秘密鍵および証明書を利用するにあたって、以下の義務を負います。

a. いかなるときにおいても、既に発行されまたは生成された秘密鍵を紛失から防止し、正当に証明書利用者として任命されたもの以外の第三者に対する開示または危殆化を防止すること。
b. 証明書に格納されたデータや情報を修正し、変更しまたは改変しないこと。
c. この CP/CPS、サービス利用規定および関連文書の規定に従い、証明書への無権限アクセスまたは使用を防止すること。
d. 秘密鍵の無権限使用防止目的のために使用される英数字の PIN コードを秘密鍵と同一の場所に格納せず、また、無権限アクセスまたは使用防止目的のために十分な保護がなされていない記録媒体に格納しないこと。
e. 秘密鍵の危殆化またはそのおそれが生じた場合、直ちに当行に通知し、かつ、その具体的事情および詳細を知らせること。
f. 証明書に記載されているデータまたは情報に変更がある場合、当行に対し、直ちに具体的事情および詳細を知らせること。この場合において、契約者は、その証明書が失効することに同意し、この CP/CPS およびサービス利用規定に記載の発行手続が新しい代替の証明書の発行に適用されることに同意するものとします。
g. この CP/CPS およびサービス利用規定に規定され記述され、合意された手続を読み、遵守すること。
h. 証明書に対応する秘密鍵を利用する前に、証明書の記載内容に誤りがないということを確認すること。
i. 証明書を利用する場合における電子署名方式は、ハッシュアルゴリズムとして SHA-1 または SHA-2 を用いた RSA 方式であって、鍵長は 2048 ビット以上とすること。

4.5.2. 信頼者による証明書の利用

信頼者は、証明書を信頼し利用するにあたって、次の義務を負うものとします。

a. 信頼者の責任において、証明書を信頼することを決定する前に契約者および証明書利用者を適切に評価し、合理的な判断を行うこと。
b. 証明書の利用目的が、自己の利用目的に合致していることを承諾していること。
c. 当行の CA 公開鍵を用いて証明書に行われた電子署名を検証することにより、当該証明書の発行者を確認すること。
d. フィンガープリントを確認し、当行の CA 証明書であることを確認すること。
e. 証明書の有効期限が満了していないことを確認すること。
f. 証明書が失効または一時停止されていないことを CRL によって確認すること。
g. この CP/CPS およびその他当行が定める諸規定を遵守すること。

4.6. 証明書の更新

4.6.1. 証明書の更新事由

当行は、次の場合に証明書の更新を行います。

a. 証明書の有効期間が満了する場合

b. 当該証明書が失効または一時停止となっていない場合

c. 契約者および証明書利用者の情報に変更が無い場合

4.6.2. 証明書の更新申込を行うことができる者

新しい証明書の更新申込を行うことができる者は、契約者とします。ただし、当行は、当行所定の手続により証明書の更新を行うことができるものとします。

4.6.3. 証明書更新時の処理手続

当行は、この CP/CPS「4.6.1. 証明書の更新事由」の判断に基づき、当行所定の手続により証明書の更新を行います。

4.6.4. 新しい証明書の発行通知

この CP/CPS「4.3.2. 証明書発行通知」と同様とします。

4.6.5. 更新に伴い発行された証明書の受領確認手続

この CP/CPS「4.4.1. 証明書の受領確認手続」と同様とします。

4.6.6. 更新済みの証明書の公表

この CP/CPS「4.4.2. 証明書の公表」と同様とします。

4.6.7. 第三者に対する証明書発行通知

この CP/CPS「4.4.3. 第三者に対する証明書発行通知」と同様とします。

4.7. 証明書の変更

4.7.1. 証明書の変更の事由

当行は、証明書の記載事項に変更が生じた場合、契約者からの申込に基づき、証明書の変更手続を行うものとします。

4.7.2. 証明書の変更の申込を行うことができる者

証明書の変更の申込を行うことができる者は、契約者とします。

4.7.3. 証明書の変更時の処理手続

当行は、証明書の変更処理をこの CP/CPS「4.2. 証明書の発行の申込手続」および「4.8.3. 失効時の処理手続」に基づき行うものとします。

4.7.4. 利用者に対する新しい証明書の発行通知

この CP/CPS「4.3.2. 証明書発行通知」と同様とします。

4.7.5. 変更された証明書の受領確認手続

この CP/CPS「4.4.1. 証明書の受領確認手続」と同様とします。

4.7.6. 変更された証明書の公表

この CP/CPS「4.4.2. 証明書の公表」と同様とします。

4.7.7. 第三者に対する証明書発行通知

この CP/CPS「4.4.3. 第三者に対する証明書発行通知」と同様とします。

4.8. 証明書の失効および一時停止

4.8.1. 証明書失効事由

当行は、次の場合に証明書の失効手続を行うものとします。

a. この CP/CPS「3.4. 失効申込時の識別と認証」に基づく当行所定の手続により、証明書の失効の申込を受け付けた場合
b. この CP/CPS「4.7.1. 証明書の変更の事由」に基づく当行所定の手続により、証明書の変更の申込を受け付けた場合
c. 当行が、この CP/CPS「4.4.1. 証明書の受領確認手続」に基づく契約者および証明書利用者から所定の期日を過ぎたにも関わらず証明書未受領である旨の連絡を受けた場合
d. IC カードを盗難、遺失した場合
e. 秘密鍵の開示、変更、漏洩等、危殆化もしくは危殆化のおそれがある場合
f. PIN コードの漏洩または PIN コード設定用暗証番号の紛失、失念もしくは漏洩した場合
g. 当行が、証明書に含まれる重要情報またはデータが虚偽であること、または虚偽であると信じることが相当であることを発見した場合
h. 当行が、証明書に含まれる重要な情報が不正確または不適当となったことを発見した場合
i. 一時停止状態で証明書の有効期間が満了した場合

j. この CP/CPS「4.10. 本サービスを解約する場合」に基づき本サービスを解約する場合
k. 契約者に関して、正当な権限を有する第三者により正当かつ適切な当該証明書に関する失効の申込（例えば、裁判所の命令を含みかつそれに限定されないものとします）を当行が受領した場合
l. 契約者に関して、支払いの停止もしくは破産、民事再生手続開始、会社更生手続開始もしくは特別清算開始、その他今後施行される倒産処理法に基づく倒産手続開始の申立があった場合、契約者の財産について仮差押、保全差押、差押または競売手続開始があった場合
m. 上記の他、契約者の信用状態に重大な変化が生じたと当行が判断した場合
n. 契約者に関して、監督官庁より営業停止の処分を受け、または営業免許もしくは営業登録の取消または一時停止の処分を受けた場合
o. 契約者が解散その他営業活動を休止した場合
p. 契約者が手形交換所またはこれに準ずる電子債権記録機関の取引停止処分を受けた場合
q. その他、当行が、契約者に関して本サービスの継続を困難と認めるとする事実が発生した場合

4.8.2. 証明書の失効の申込を行うことができる者

証明書の失効の申込を行うことができる者は、契約者とします。また、当行は、この CP/CPS「4.8.1. 証明書失効事由」に該当すると判断した場合、証明書の失効を行うことができるものとします。

4.8.3. 失効時の処理手続

失効時の処理手順は、次のとおりとします。

a. 当行は、失効の申込を受け付け、この CP/CPS「3.4. 失効申込時の識別と認証」に従い、申込を行った者の本人確認を行います。
b. 当行は、証明書が現時点で有効なものであることを確認します。失効の処理は、原則として受付順に行います。
c. 当行は、当行所定の手続により、証明書の失効を行います。
d. 当行は、失効した証明書の情報を追加した新しい CRL を発行するとともに、リポジトリ上に反映させます。

4.8.4. 信頼者による失効確認要求

信頼者は、証明書を信頼し利用する前に、CRL でその証明書の有効性を確認するものとします。

なお、CRL で確認できる情報は、当行において失効処理を行った証明書の情報のみです。

当行は、信頼者からの有効期間の満了した証明書の有効性確認についての問合せに対しては応じません。

4.8.5. 証明書失効リストの発行頻度

当行は、証明書の失効、一時停止および一時停止解除処理を行った場合、CRL を即時に発行します。これらがない場合も、CRL を 24 時間ごとに発行します。

4.8.6. 証明書の一時停止事由

当行は、次の事由に該当する場合に証明書の一時停止を行います。

a. 契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者が証明書の一時停止の申込をした場合
b. 当行が、この CP/CPS「4.4.1. 証明書の受領確認手続」に基づく契約者および証明書利用者から所定の期日を過ぎたにも関わらず証明書未受領である旨の連絡を受けた場合
c. 当行が証明書に対応する秘密鍵に危殆化のおそれがあると判断した場合
d. 当行が、利用者がこの CP/CPS、サービス利用規定等に従わないと判断した場合
e. その他、当行の本サービスの信用性を低下するおそれがある場合
f. 法令、規則等により、証明書の一時停止が正当と認められる場合

4.8.7. 証明書の一時停止の申込を行うことができる者

証明書の一時停止の申込を行うことができる者は、契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者とします。また、当行は、この CP/CPS「4.8.6. 証明書の一時停止事由」に該当すると判断した場合、証明書の一時停止を行うことができるものとします。

4.8.8. 通常の証明書の一時停止時の処理手続

通常の一時停止の場合、契約者は、当行所定の申込書により一時停止の申込を行うものとします。

通常の一時停止の処理手続は次のとおりとします。

a. 当行は、一時停止の申込を受け付け、この CP/CPS「3.4. 失効申込時の識別と認証」と同様の本人確認を行います。
b. 当行は、証明書が現時点で有効なものであることを確認します。一時停止の申込の処理は、原則として受付順に行います。
c. 当行は、当行所定の手続により、証明書の一時停止を行います。
d. 当行は、一時停止処理をした証明書の情報を追加した新しい CRL を発行するとともに、リポジトリ上に反映させます。

4.8.9. 緊急を要する証明書の一時停止時の処理手続

緊急を要する一時停止の場合、ValueDoor 管理専用ＩＤ保有者または証明書利用者は、当行所定の手続により電話等で一時停止の申込を行うものとします。ただし、後日、契約者は当行所定の申込書を提出するものとします。

緊急時の一時停止の処理手続は、次のとおりとします。

a. 当行は、緊急の一時停止の申込を受け付け、申込を行った ValueDoor 管理専用ＩＤ保有者または証明書利用者の本人確認を行います。
b. 電話による申込時の本人確認は、企業名、本人の氏名等、当行所定の事項を確認します。
c. 当行は、証明書が現時点で有効なものであることを確認します。緊急の一時停止の申込の処理は、原則として受付順に行います。
d. 当行は、当行所定の手続により、証明書の一時停止を行います。
e. 当行は、一時停止処理をした証明書の情報を追加した新しい CRL を発行するとともに、リポジトリ上に反映させます。

4.8.10. 証明書の一時停止解除事由

当行は、契約者が自らの責任に基づく合理的な判断によって一時停止の必要性がないと判断し、当行に一時停止解除の申込を行った場合に、一時停止解除を行います。

4.8.11. 証明書の一時停止解除の申込みを行うことができる者

証明書の一時停止解除の申込を行うことができる者は、契約者とします。また、当行は、当行の裁量により証明書の一時停止解除を行うことができるものとします。

4.8.12. 証明書の一時停止解除時の処理手続

契約者は、当行所定の申込書により一時停止解除の申込を行うものとします。

一時停止解除時の処理手順は、次のとおりとします。

a. 当行は、証明書が現時点で一時停止中であることを確認します。一時停止解除の処理は、原則として受付順に行います。
b. 当行は、当行所定の手続により、証明書の一時停止解除を行います。
c. 当行は、一時停止解除を行った証明書の情報を削除した新しい CRL を発行するとともに、リポジトリ上に反映させます。
d. 当行は一時停止解除手続が完了した後、申込を行った者に対して処理結果を通知します。

4.8.13. 一時停止を継続することができる期間

一時停止を継続できる期間は、当該証明書の有効期間内とします。当該証明書の有効期間を満了した場合、当行は証明書の失効を行います。

4.9. PIN コードのロック解除手続

IC カードの PIN コードを既定回数誤って入力した場合や PIN コードの失念等で、IC カードを利用することができなくなった場合、当行所定の手続により、PIN コードを再設定し IC カードを利用可能とすることができます(PIN コードロック解除といいます)。なお、PIN コードロック解除操作において、既定回数操作を誤ると、IC カードは完全に利用することができなくなります。その場合、契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者は、この CP/CPS「3.4. 失効申込時の識別と認証」に定める手続により、証明書の失効の申込を行うものとします。

4.10. 本サービスを解約する場合

契約者の都合により本サービスを解約する場合、契約者は証明書の失効の申込を行わなければなりません。解約の効力は、当行所定の手続により（証明書の失効処理を含みます）当行が解約処理を行った時点から発生するものとします。

また、当行は、この CP/CPS「5.7. 認証業務の終了」に定める場合に、当行所定の手続により証明書の失効処理および解約処理ができるものとします。

4.11. キーエスクローと鍵回復

当行は証明書利用者の秘密鍵のエスクローを行いません。

5. 物理的、手続上、人事上のセキュリティ管理

5.1. 物理的管理

5.1.1. 立地および建物構造

当行 CA は、火災、水害、地震等による災害の被害を受けるおそれの少ない場所に位置し、災害対策を講じます。また、当行 CA は、サービスに利用する機器類（以下「CA システム」といいます）を災害および不正侵入から防護された安全なエリアの内部に設置します。

5.1.2. 物理的アクセス

当行 CA は、セキュリティレベルを分けて入退室管理を行います。各室への入室権限は、これらのセキュリティレベルに基づき、各室内で行われる業務あるいは操作に応じて、サービス運用管理者が付与します。

CA システムが設置される室は、セキュリティレベルに応じた認証方式を行うことによりアクセス制御を施し、さらに各室への入室には、サービス運用管理者の承認を必要とします。機器保守、設備保守等で入室権限が無い者の入室が必要な場合は、サービス運用管理者が承認し、権限者の立会いを必要とします。

CA サーバの設置された室への入室は、2 名の権限者の認証を必要とします。

施設内の様子は監視カメラ、各種センサー、入退室制御を行う装置により常時監視されます。

5.1.3. 電源管理および空調管理

当行 CA は、CA システムの運用のために十分な容量の電源を確保し、CVCF を設置するとともに、商用電源が供給されない事態に備え非常用自家発電機を装備しています。

また、空調設備を用意し、機器類の動作環境および要員の作業環境を適切に維持します。

5.1.4. 水害対策

当行の CA が設置される建物には漏水検知器を設置し、天井および床には防水対策を講じます。

5.1.5. 火災防止

当行の CA が設置される建物は耐火構造とします。CA システムを設置する室は防火区画とし、消火設備を備えます。

5.1.6. 地震対策

当行の CA が設置される建物は耐震構造とし、機器・什器の転倒、落下防止策を講じます。

5.1.7. 媒体管理

アーカイブデータ、バックアップデータは、権限者以外が入室できないよう入退室制御された室内の保管庫に安全を確保して保管します。保管場所と遠隔地保管場所の間の媒体搬送は、移送中の安全を確保して行います。

5.1.8. 廃棄処理

本サービスに関連する重要な文書類、機器類、磁気媒体、HSM 等を廃棄する場合の規則は次のとおりとします。

a. 文書類は裁断し廃棄します。
b. 機器類は記録領域を初期化するか、電磁的に破壊するかまたは物理的に破壊し廃棄します。
c. 磁気媒体は初期化するか、電磁的に破壊するかまたは物理的に破壊し廃棄します。
d. HSM は内容を完全に初期化するかまたは物理的に破壊し廃棄します。

廃棄物の処理作業は、複数名で行うものとします。

5.1.9. オフサイトバックアップ

当行は、障害、自然災害等による CA システムの重要データの喪失に備え、また、業務継続性を確保することを目的に、CA システムに関する重要なデータを定期的に当行 CA の施設と同程度の物理的セキュリティを備えた遠隔地保管場所へ保管します。

5.2. 手続上の管理

5.2.1. 信頼される役割

当行は、セキュリティ確保のため、当行所定の手続により本サービスの業務に従事する者の職務権限を分離し、業務を行う者が単独で不正を行うことができないよう管理を行います。

本サービスに従事する担当者の職務は以下のとおりです。

（1） 業務責任者

業務責任者は、登録担当者が審査した証明書に関する各作業申請を承認し、登録担当者に作業を指示することをはじめ、本サービスに関する業務全般を統括し、管理します。

（2） 受付担当者

受付担当者は、当行所定の手続により契約者、ValueDoor 管理専用ＩＤ保有者または証明書利用者から申込を受け付け、本人確認および審査結果の通知等を行います。

（3） 登録担当者

登録担当者は、受け付けた申込に関してこの CP/CPS に基づいて審査を行い、業務責任者の承認を得た後、証明書の発行、更新、失効、一時停止、一時停止解除処理の登録作業を行います。

（4） サービス運用管理者

サービス運用管理者は、業務責任者による証明書発行承認に基づき、RA 担当者に IC カードの発行作業指示を行います。また、CA 管理者、RA 担当者およびログ検査者の業務全般を統括し、管理を行います。

（5） CA 管理者

CA 管理者は、サービス運用管理者の作業指示に基づき、CA システムの運用管理を行います。また、サービス障害時の障害復旧対応を行います。

（6） RA 担当者

RA 担当者は、サービス運用管理者の作業指示に基づき、業務責任者により承認され発行された証明書を、IC カードへ格納する作業を行います。

（7） ログ検査者

ログ検査者は、証明書発行処理、一時停止処理、失効処理等が正しく行われたかを各種の監査ログを用いて検査を行います。

5.2.2. 必要とされる人数

この CP/CPS「5.2.1. 信頼される役割」の職務は、原則として、それぞれ別の異なった要員が行います。当行は、CA 秘密鍵を用いた操作等の重要操作については複数人によって行います。

5.2.3. CA システムに対する識別と認証

証明書の発行等の処理を行うに当たっては、この CP/CPS「5.1.2. 物理的アクセス」の他に、CA システムによって操作者の識別と認証を行います。

5.3. 人事上のセキュリティ管理

当行は、本サービスの運用のセキュリティを確立するため、当行所定の手続によって適切な人事管理を行います。

5.3.1. 教育要件

当行は、本サービスの業務に従事する者に対し、職務ごとに適切な教育を必要に応じて行うものとします。

5.3.2. 業務委託先に対する要件

当行は、本サービスの運用業務のすべてあるいは一部を外部機関に委託する場合、当該業務委託先との契約によって、当該業務委託先のもとで本サービスに従事する者の人事管理が適切に行われていることを確認します。

5.3.3. 要員へ提供される資料

当行は、本サービスに従事する者に対して、本サービスに関し業務上必要な文書のみの閲覧を許可します。

5.4. セキュリティ監査の手順

5.4.1. 記録されるイベントの種類

CA システム上で起こるセキュリティに関するすべての重要な事象は、その事象の種類および発生時刻とともに自動的に監査ログファイルに記録されます。この中には、以下の事象を含みます。

a. CA 秘密鍵の操作
b. システムの起動･停止
c. データベースの操作
d. 権限設定の変更履歴
e. 証明書の発行
f. 証明書の失効
g. CRL の発行
h. 監査ログの検証
i. RA からの操作ログ
j. 入退室時の認証の記録
k. 不正侵入検知機等の警報ログ

5.4.2. 監査ログの処理頻度

監査ログの検査は、ログ検査者が毎営業日行います。

5.4.3. 監査ログの保存期間

CA システム上で生成される監査ログは、当行所定の期間、CA システム上に保管されます。監査ログは、 この CP/CPS「5.5.2. アーカイブの保存期間」に従い、保管用記録として、保存されます。

5.4.4. 監査ログの保護

CA システム上の監査ログは、盗聴防止措置、改ざん検知措置を施しています。監査ログは、予め定められた者だけが、調査し、確認することができます。

5.4.5. 監査ログのバックアップ

監査ログは、CA システム上のデータと同様の手続で、バックアップ用の媒体に保管されます。

5.4.6. 監査ログの収集システム

監査ログの収集は、当行が利用するシステムまたはソフトウェアにより自動的に行われます。

5.4.7. ぜい弱性評価

当行は、監査ログの検査結果をもとに、必要に応じて運用面およびシステム動作面でのセキュリティ上のぜい弱性の評価を行い、見直しを行います。

5.5. 記録の保管

5.5.1. アーカイブの種類

当行は、次の情報をアーカイブとして作成し、保管します。

a. 発行したすべての証明書
b. 証明書の発行、秘密鍵の生成、失効、一時停止等に関する情報（申込書類、審査記録等を含みます）
c. CA の鍵ペアおよびその作成に関する情報
d. CRL およびその作成に関する記録
e. 本サービスの業務に関する基準および手順を記載した書類およびその変更に関する情報
f. 当行の業務の一部を他に委託する場合においては、委託契約に関する書類

g. 監査の実施結果に関する記録

5.5.2. アーカイブの保存期間

アーカイブの保存期間は、7 年間または法律で規定された保存期間のどちらか長い期間とします。

5.5.3. アーカイブの保護

当行は、適切なアクセスコントロールまたは改ざん防止措置等によりアーカイブの保護を行います。

5.5.4. アーカイブのバックアップ手順

アーカイブは、当行所定の手続によりバックアップを行います。

5.6. 危殆化および災害からの復旧

5.6.1. 災害および危殆化の対応手続

災害および危殆化等により本サービスの中断、停止につながるような問題が発生した場合、当行は、当行所定の手続により本サービスの提供を停止し、被害状況および原因の調査を行います。この場合、当行は、当行所定の手続により契約者および信頼者に通知または公表します。

5.6.2. システム障害またはデータが破損した場合の手続

システム障害またはデータの破損が発生したもしくは破損されたおそれがある場合、当行は当行所定の手続により本サービスの提供を停止し、被害状況および原因の調査を行います。この場合、当行は、当行所定の手続により契約者および信頼者に通知または公表します。

5.6.3. CA 秘密鍵が危殆化した場合の手続

CA 秘密鍵が危殆化したまたは危殆化のおそれがある場合、当行は、当行所定の手続により本サービスの提供を停止し、被害状況および原因の調査を行います。また、発行した全ての証明書を失効することがあります。この場合、当行は、当行所定の手続により契約者および信頼者に通知または公表します。

5.6.4. 復旧

災害等によって中断した本サービスの再開が可能であると当行が判断した場合、当行所定の手続により可能な限り速やかにシステム復旧を行い、本サービスの提供を再開します。

正常復旧を確認した後、当行は、当行所定の手続により契約者および信頼者に通知または公表します。

5.7. 認証業務の終了

当行は、当行の判断により本サービスを終了することができるものとします。この場合、当行は本サービスを終了する少なくとも 90 日前までに契約者および信頼者に対して通知または公表します。ただし、緊急やむをえない場合、当行は、この期間を短縮できるものとします。

6. 技術的セキュリティ管理

6.1. 鍵ペアの生成と格納

6.1.1. 鍵ペア生成

当行の CA 鍵ペアは、FIPS140-2 レベル 3 準拠の HSM によって生成します。CA 鍵ペアの生成手続は、CA サーバの設置された室において複数名の CA 管理者によって行われるものとします。

6.1.2. 利用者への秘密鍵の送付

当行は、当行所定の手続により証明書利用者の秘密鍵を CA サーバの設置された室において生成します。秘密鍵の IC カードへの格納は複数名の権限者によって行われ、格納後、当該秘密鍵は CA システム上からは削除されます。IC カードは、この CP/CPS「4.3.2. 証明書発行通知」に定める手続によって配付するものとします。

6.1.3. 当行の CA 公開鍵の送付

当行の CA 公開鍵は、証明書利用者の秘密鍵および証明書とともに IC カードに格納し、当行所定の手続により証明書利用者に配布するとともに、リポジトリ上に当行の CA 公開鍵を公表します。

6.1.4. 鍵長

当行の CA 秘密鍵の鍵長は RSA の 2048 ビットとし、証明書利用者の秘密鍵の鍵長は、RSA の 2048 ビット以上とします。

6.1.5. 当行の CA 秘密鍵の利用目的

当行の CA 秘密鍵は、以下の目的のために利用されます。

a. 証明書利用者の証明書への電子署名
b. 当行の CA 証明書への電子署名
c. CRL への電子署名
d. CA システムに対する証明書への電子署名
e. CA システムを操作する者に対する証明書への電子署名

6.2. 秘密鍵の保護

6.2.1. 暗号モジュール

当行の利用する暗号モジュールの基準は、FIPS140-2 レベル 3 の認定を取得した HSM を利用します。

6.2.2. 当行の CA 秘密鍵の複数人管理

当行の CA 秘密鍵の起動、停止、バックアップ等の操作は、CA サーバの設置された室において複数名の CA 管理者によって行われます。

6.2.3. 当行の CA 秘密鍵のエスクロー

当行は CA 秘密鍵および証明書利用者の秘密鍵のエスクローを行いません。

6.2.4. 秘密鍵のバックアップ

当行の CA 秘密鍵のバックアップは、当行所定の手続により、CA サーバの設置された室において複数名の CA 管理者によって生成されます。当行の CA 秘密鍵のバックアップは、暗号化された状態で、CA サーバの設置された室に保管します。

当行は、証明書利用者の秘密鍵のバックアップは行いません。

6.2.5. 秘密鍵のアーカイブ

当行は、当行の CA 秘密鍵および証明書利用者の秘密鍵のアーカイブは行いません。

6.2.6. 秘密鍵の暗号モジュールへの格納

当行の CA 秘密鍵は、当行所定の手続により暗号化した状態で格納されるものとします。

証明書利用者の秘密鍵は、当行所定の手続により安全な環境で生成し、IC カード内に格納されます。

6.2.7. 秘密鍵の起動方法

当行の CA 秘密鍵の起動方法は、複数名の CA 管理者が HSM を操作するために必要な管理用 IC カードを用いて行います。

証明書利用者の IC カード内の秘密鍵を起動させるためには、対応する PIN コードを利用するものとします。証明書利用者は、秘密鍵を利用する度ごとにその PIN コードを入力するものとします。

6.2.8. 秘密鍵の停止

当行の CA 秘密鍵の起動を停止する場合は、複数名の CA 管理者が HSM を操作するために必要な管理用 IC カードを用いて行います。

6.2.9. 秘密鍵の破棄方法

当行の CA 秘密鍵を廃棄しなければならない状況の場合は、当行所定の手続により、CA サーバの設置された室において複数名の CA 管理者によって完全に初期化または物理的に破壊し、廃棄されるものとします。バックアップについても同様の手続によるものとします。

証明書の有効期間の満了した、またはこの CP/CPS「4.8.1. 証明書失効事由」により失効された証明書利用者の IC カードは、契約者の責任のもと廃棄するものとします。

6.2.10. 暗号モジュールの技術管理

当行が利用する暗号モジュールの品質基準については、この CP/CPS「6.2.1. 暗号モジュール」のとおりとします。

6.3. 鍵ペア管理のその他の側面

6.3.1. 公開鍵のアーカイブ

当行の CA 公開鍵および証明書利用者の公開鍵は、証明書のアーカイブに含まれ、この CP/CPS「5.5.2. アーカイブの保存期間」において規定された期間保存します。

6.3.2. 鍵ペアの有効期間

当行は、CA 秘密鍵の有効期間 20 年に対して、14 年ごとに更新を行い、連続性を確保します。ただし、暗号のセキュリティが容認できないほどぜい弱になった場合は、当行の判断により、CA 鍵ペアの更新を行うことができるものとします。

更新前の CA 秘密鍵および証明書は、その 20 年の有効期間を満了するまでの間、有効となります。CA 秘密鍵および証明書の更新は、当行所定の手続により安全に行われます。

当行は、常に最新の CA 秘密鍵を用いて証明書の発行を行います。

証明書利用者の秘密鍵および証明書の有効期間は、当行が定める所定の期間とします。

6.4. 起動データ

6.4.1. 起動データの生成と格納

当行の CA 秘密鍵を操作するために必要な起動データは、複数名の CA 管理者によって生成され、管理用 IC カードに格納されます。

証明書利用者に配付する、IC カードについての PIN コード設定用暗証番号は、安全な環境において IC カードに対して生成されます。

6.4.2. 起動データの保護

当行で使用する HSM の起動は管理用 IC カードで行います。管理用 IC カードは、当行所定の手続により HSM と同等の環境において保管管理します。

6.5. コンピュータのセキュリティ管理

当行のコンピュータセキュリティ管理は、当行所定の手続により行われます。CA システムは、物理的に安全な環境に設置され、アクセスコントロール、複数人の立会いによる操作、監査ログの検査等、運用面においても適切なセキュリティ管理を行います。

6.6. セキュリティ技術のライフサイクル管理

当行は、CA システムの構築およびメンテナンスを安全な設備の中で行います。CA システムの変更を行う場合は、当行所定の手続により安全性を評価、確認するものとします。当行が CA システムに導入するコンピュータセキュリティ技術の管理においては、適切なサイクルで最新のセキュリティ技術を導入するために定期的にセキュリティチェックを行います。

6.7. ネットワークセキュリティ管理

CA システムへのアクセスは、許可された者だけがアクセスできるように制限されており、外部からのアクセスは認証局のソフトウェアの特性を使用して、真正性が確認され、暗号化されたセッションだけが、アクセスを許可されます。

7. 証明書および CRL のプロファイル

7.1. 証明書のプロファイル

当行が発行する証明書は、X.509 バージョン 3 形式に準拠し、作成します。当行が発行する証明書のプロファイルは、次のとおりです。

○ ＝ 使用する

× ＝ 使用しない

7.1-1 証明書のプロファイルー基本領域

フィールド （説明）	当行 CA 証明書	利用者 証明書	備考（証明書の記載内容）
version （証明書形式のバージョン）	○	○	当行が発行する証明書には、バージョン 3 を示す値を記載します。
serialNumber （証明書ごとに割り当てられるユニークな番号）	○	○	当行が発行する証明書には、一意に定める整数を記載します。
signature （CA が証明書に署名する際に使用する署名アルゴリズム）	○	○	当行は、アルゴリズムとして sha1withRSAEncryption (1 2 840 113549 1 1 5)又は sha256withRSAEncryption (1 2 840 113549 1 1 11）を使用します。
validity （証明書の有効期間（開始および終了））	○	○	当行が発行する証明書は、UTCTime で記載します。
issuer （証明書の発行者名）	○	○	当行が発行する証明書には、当行の CA の名前を記載します。
subject （証明書に対応する秘密鍵の所有者名）	○	○	当行が発行する証明書には、証明書の所有者名を記載します。
subjectPublicKeyInfo （秘密鍵に対応している公開鍵情報）	○	○	当行は、アルゴリズムとして rsaEncryption（1 2 840 113549 1 1 1）を使用します。

7.1-2 証明書プロファイルー拡張領域

フィールド （説明）	当行 CA 証明書	利用者 証明書	備考（証明書の記載内容）
authorityKeyIdentifier （証明書の発行者の公開鍵の識別子）	○	○	当行の CA 公開鍵の Sha-1 ハッシュ値を記載します。
subjectKeyIdentifier （証明書の所有者の公開鍵の識別子）	○	○	当該証明書の公開鍵の Sha-1 ハッシュ値を記載します。
keyUsage （公開鍵の使用目的）	○	○	証明書利用者の証明書は、digitalSignature、nonRepudiation 、 keyEncipherment 、dataEncipherment、keyAgreement を記載します。当行の CA 証明書は、keyCertSign、cRLSign を記載します。
certificatePolicies （証明書のポリシー）	×	○	当行が発行する証明書には、当行の証明書ポリシーを一意に識別するためのオブジェクト識別子、およびこの CP/CPS の公開場所を示す URI を記載します。
basicConstraints （証明書の発行対象が CA であるかどうか）	○	×	当行の CA 証明書には、CA であることを示す情報を記載します。
cRLDistributionPoints （CRL の配布場所）	○	○	当行が発行する証明書には、CRL の公開場所を示す URI を記載します。

7.2. CRL のプロファイル

当行が発行する CRL は、X.509 バージョン 2 形式に準拠し、作成します。当行が発行する CRL のプロファイルは、次のとおりです。

○ ＝ 使用する

× ＝ 使用しない

7.2-1 CRL プロファイルー証明書リスト領域

フィールド （説明）	CRL	備考 （CRL の記載内容）
version （CRL 形式のバージョン）	○	当行が発行する CRL には、バージョン 2 を示す値を記載します。
signature （CA が CRL に署名する際に使用する署名アルゴリズム）	○	当行は、アルゴリズムとして sha1withRSAEncryption (1 2 840 113549 1 1 5)又は sha256withRSAEncryption (1 2 840 113549 1 1 11) を使用します。
issuer （CRL の発行者名）	○	当行が発行する CRL には、当行の CA の名前を記載します。
thisUpdate （CA により CRL が発行された日時）	○	当行が発行する CRL は、UTCTime で記載します。
nextUpdate （CRL が次回発行される日時）	○	当行が発行する CRL は、UTCTime で記載します。
RevokedCertificates （失効された証明書の情報）	○	当行が発行する CRL には、失効した証明書のシリアル番号および失効日時を記載します。

7.2-2 CRL プロファイルーCRL エントリ拡張

フィールド （説明）	CRL	備考 （CRL の記載内容）
reasonCode （失効理由）	○	当行が発行する CRL には、失効理由を示す情報を記載します。

7.2-3 CRL プロファイルーCRL 拡張

フィールド （説明）	CRL	備考　（CRL の記載内容）
authorityKeyIdentifier （証明書の発行者の公開鍵の識別子）	○	当行の CA 公開鍵の Sha-1 ハッシュ値を記載します。
cRLNumber （発行ごとに増加する CRL の番号）	○	当行が発行する CRL は、発行の都度、このフィールドに記載される番号が増加します。

8. 準拠性監査

8.1. 監査の頻度

当行は、本サービスの運用がこの CP/CPS に準拠して行われていることを、適時、監査を行います。

8.2. 監査人の適格性

監査は、十分な監査経験を有する監査人が行います。

8.3. 監査人と当行の被監査部門との関係

監査人は、監査に関する事項を除き、当行の被監査部門の業務から独立した立場にあるものとします。監査の実施にあたり、当行の被監査部門は監査に協力するものとします。

8.4. 監査対象

監査対象は、本サービスの運用がこの CP/CPS に準拠して行われていること、並びに外部からの不正アクセスおよび内部における不正行為に対するコントロールが適切に行われていること等とします。

8.5. 監査指摘事項への対応

重要または緊急を要する監査指摘事項に対しては、速やかに是正を行います。その場合、是正されるまでの間、当行は本サービスの提供を停止することがあります。

8.6. 監査結果

監査結果は、監査人からポリシー承認機関に報告されます。この監査結果は、この CP/CPS「5.5.2. アーカイブの保存期間」に定める期間、保存します。

9. 他の業務上および法的問題

9.1. 料金

規定しない。

9.2. 機密保持

9.2.1. 機密情報

契約者および当行は、本サービスに関して知り得た一切の情報および資料（以下「情報等」といいます）について機密を保持し、次に定める者以外の第三者に対し開示または漏洩してはならないものとします。ただし、証明書に含まれる情報は、登録手続の一部として提供されたとしても、機密情報とはみなされないものとします。

a. 自己の役員または従業員のうち、本サービスまたはその利用に関連する業務を直接担当する者
b. 相手方が事前に文書で承諾した者

また、当行は、親会社、弁護士、公認会計士等の専門家および業務委託先、その他当行が本サービスを実施するために必要な第三者に対し、当行と同一の機密保持義務を課すことにより（ただし、これらの者が法令上機密保持義務を負う場合は、重ねて義務を課す必要はないものとします)、情報等を開示することができるものとします。

9.2.2. 機密情報に関する例外

次の事項にあたる情報等については、この CP/CPS「9.2.1. 機密情報」の適用はないものとします。

a. 情報等の取得時期を問わず、公知の事実に関するものである場合
b. 情報等を取得した際、既に自ら正当に所有していたものである場合
c. 情報等を取得した後、正当な権限を有する第三者から同様の内容の情報等を正当に取得したものである場合
d. 情報等の開示につき、適正な法律・法令等、行政または司法による義務が課せられたものであるとき

9.3. 個人情報の保護

9.3.1. 個人情報として扱われる情報

本サービスでは、申込書その他書類に記載される契約者、ValueDoor 管理専用ＩＤ保有

者および証明書利用者の情報として、氏名、メールアドレス等を個人情報として取り扱います。

9.3.2. 個人情報保護

当行は、個人情報を保護するため、個人情報の取扱に関するわが国の法令、並びに当行所定の手続により適切に収集、利用、管理を行います。

9.3.3. 個人情報の開示

法令、規則、行政庁の命令等により本サービスに関わる個人情報の開示が義務付けられる場合（当局検査を含みます）、当行は契約者の承諾なくして当該法令、規則、命令等の定める手続に基づいて個人情報を開示することがあります。当行が個人情報を開示したことにより生じた損害について、当行は責任を負いません。

9.4. 著作権

この CP/CPS の著作権は、当行に帰属します。

9.5. 保証

9.5.1. 当行の保証

当行は、この CP/CPS を遵守して、証明書の発行、失効、一時停止、一時停止解除、失効情報の公表等を行うことを保証します。

9.5.2. 契約者、ValueDoor 管理専用ＩＤ保有者および証明書利用者の表明保証

契約者、ValueDoor 管理専用ＩＤ保有者および証明書利用者は、この CP/CPS に定める事項を遵守することについて保証するものとします。また、契約者は、契約者自身、ValueDoor 管理専用ＩＤ保有者または証明書利用者がこの CP/CPS に遵守しない場合、すべての責任を有するものとします。

9.5.3. 信頼者の表明保証

信頼者は、この CP/CPS に定める事項を遵守することについて保証するものとします。また、信頼者は、この CP/CPS に遵守しない場合、すべての責任を有するものとします。

9.6. 免責

この CP/CPS「9.5.1. 当行の保証」の内容に関し、次の場合、当行は責任を負わないものとします。ただし、当行に故意または重大な過失がある場合はこの限りではありません。

a. 当行に起因しない不法行為、不正使用並びに過失等により発生する一切の損害

b. 契約者、ValueDoor 管理専用ＩＤ保有者、証明書利用者または信頼者が自己の義務の履行を怠ったために生じた損害
c. 契約者、ValueDoor 管理専用ＩＤ保有者、証明書利用者または信頼者のシステムに起因して発生した一切の損害
d. 契約者、ValueDoor 管理専用ＩＤ保有者、証明書利用者または信頼者の端末のソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
e. 契約者が契約に基づく契約料金を支払っていない間に生じた損害
f. 当行の責に帰することのできない事由で証明書および CRL に公開された情報に起因する損害
g. 当行の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
h. 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
i. 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本サービスの業務停止に起因する一切の損害

また、当行は、契約者と第三者間（これには信頼者を含みます）における契約その他取引関係については一切関与せず、いかなる責任も負わないものとします。

9.7. 補償

本サービスに関連して契約者の責任によらず契約者に損害が発生した場合、当行は契約者の本サービスの利用状況やセキュリティ対策状況を具体的に伺った上で、個別に補償の実施可否を検討することとします。

9.8. 改訂手続

この CP/CPS は、当行の判断によって適宜改訂され、ポリシー承認機関の承認後、公表することをもって発効するものとします。契約者、ValueDoor 管理専用ＩＤ保有者および証明書利用者は、公表された内容に同意しない場合には、公表から 1 週間以上の当行が相当と認める期間内にその旨を当行に通知するものとします。当行がこの変更に同意しない旨の通知を受領しない場合には、変更に同意があったものとみなします。

また、変更に同意しない旨の通知があった場合には、当行は事前に通知することなく本サービスの解約および証明書の失効を行うことができるものとします。

9.9. 紛争解決手段

契約者は、本サービスにおける紛争について、当行の本店または取引店の所在地を管轄する裁判所を専属的合意管轄裁判所とします。

9.10. 準拠法

この CP/CPS の効力、履行および解釈に関しては、すべて日本法が適用されるものとします。

9.11. 雑則

9.11.1. 譲渡等の禁止

契約者は、この CP/CPS に基づく権利または義務の全部または一部を、当行の書面による承諾を得ないで、第三者に譲渡、貸与、質権設定その他担保に供することはできないものとします。

9.11.2. 一部無効

この CP/CPS の一部の条項が無効であったとしても、当該文書に記述された他の条項は有効であるものとします。

9.11.3. 契約終了後の有効条項

本サービスの契約が終了した場合であっても、この CP/CPS「9. 他の業務上および法的問題」の効力は、有効に存続するものとします。

9.11.4. 通知

本サービスでは、契約者、ValueDoor 管理専用ＩＤ保有者、証明書利用者および信頼者に対する必要な通知をホームページ上、リポジトリ上、電子メール、電話または書面の郵送等によって行います。

10. 用語

A～Z

CA（Certification Authority）：認証局

証明書の発行・更新・失効、CA 秘密鍵の生成・保護および加入者の登録等を行う機関をいいます。

CP（Certificate Policy）：証明書ポリシー

CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書をいいます。

CPS（Certification Practices Statement）：認証局運用規定

CA を運用する上での諸手続、セキュリティ基準等を定める CA の運用を規定する文書をいいます。

CVCF（Constant-Voltage Constant-Frequency）

電圧・周波数を安定化した電源をいいます。

IC カード

IC チップ（半導体集積回路）が内蔵されたキャッシュカード大のプラスチックカードをいいます。

この CP/CPS で用いられる「IC カード」には、USB トークン等その他の電子媒体を含みます。

FIPS 140-2

米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準をいいます。最低レベル 1 から最高レベル 4 まであります。

HSM（Hardware Security Module）

秘密鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用するハードウェアをいいます。不正アクセスに備えるためのデータを保護する機能を有します。

PIN コード

証明書に対応する秘密鍵を使用するために必要な、証明書利用者が任意に設定する半角の英数字による符号をいいます。

RA（Registration Authority）：登録機関

CA の業務のうち、登録業務を行う機関をいいます。主な業務は、申込情報の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等です。

RFC3647（Request For Comments 3647）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、CP/CPS のフレームワークを規定したドキュメントをいいます。

RSA（Rivest Shaman Adleman）

公開鍵暗号方式の標準として普及している暗号技術のひとつです。
鍵の長さ（強度）はビットで示します。

Serial Number

証明書を一意に区別するために割り振られる情報をいいます。

SHA-1（Secure Hash Algorithm 1）

電子署名などに使われるハッシュ関数（要約関数）のひとつです。ハッシュ関数とは、与えられた原文から固定長の疑似乱数を生成する演算手法です。
データの送信側と受信側でハッシュ値比較することで、通信途中で原文が改ざんされていないかを検出することができます。

SHA-256（Secure Hash Algorithm 256）

電子署名に使われるハッシュ関数（要約関数）のひとつで、SHA-2 ファミリーのバリエーションの 1 つです。ビット長は 256 ビット。データの送信側と受信側でハッシュ値比較することで、通信途中で原文が改ざんされていないかを検出することができます。

URI（Uniform Resource Identifier）

インターネット上に存在する情報の所在を示す記述方式をいいます。

UTC（Coordinated Universal Time）

全世界で時刻を記録する際に用いられる公式時刻をいいます。

X.500

名前やアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的に ITU-T が定めたディレクトリ標準です。X.500 識別名は、X.509 の発行者名および主体者名に使用されます。

X.509

ITU-T （ International Telecommunication Union – Telecommunication Standardization Sector）が定めた証明書の標準仕様をいいます。多くの場合、証明書には X.509 バージョン 3 という形式が、CRL には X.509 バージョン 2 という形式が用いられます。

あ～ん

アーカイブ

法的またはその他の事由により、履歴の保存を目的に取得する情報をいいます。

暗号アルゴリズム

暗号化するための処理手順をいいます。

暗号化

通信の内容が当事者以外には解読できないように、文字や記号を一定の約束で他の記号に置き換えることをいいます。

オブジェクト識別子

ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字をいいます。

鍵ペア

公開鍵暗号方式において、秘密鍵と公開鍵から構成される鍵の対をいいます。

起動データ

HSM や IC カード等を使用する際に必要なパスワード等のデータをいいます。

公開鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、秘密鍵に対応し、通信相手の相手方に公開される鍵をいいます。

識別子

当行の CA 公開鍵や証明書利用者の公開鍵等を見分けるために付けられる数字等の情報をいいます。

識別名：DN（Distinguished Name）

CA が発行する証明書において、一意な名称となる属性の集まりをいいます。

自己署名証明書

自 CA の公開鍵に対して、自 CA の秘密鍵で電子署名した証明書をいいます。自 CA の公開鍵の正当性を保証します。

主体者名：CN（Common Name）

CA が発行する証明書において、証明書の所有者の名前が記載される DN の一部をいいます。

証明書失効リスト：CRL（Certificate Revocation List）

証明書の有効期間中に、証明書記載内容の変更、秘密鍵の紛失等の事由により失効された証明書のリストをいいます。

相互運用

2 つの異なる CA がお互いを認証することをいいます。

ディレクトリ

階層構造のファイル管理方式であり、ある 1 つの階層をディレクトリといいます。

電子証明書

ある公開鍵を、記載された者が保有することを証明する電子データをいいます。CA が電子署名を施すことで、その正当性が保証されます。

電子署名

秘密鍵を利用して、送受信するデータの信頼性を保証する仕組みをいいます。「なりすま

し」や「改ざん」が行われていないことを証明できます。また、送信者の「否認防止」ができます。

バックアップ

システム障害やデータの破損等により使用することができなくなったデータ等を復旧させることを目的に使用するデータ等をいいます。
オフサイトバックアップとは、CA が設置される施設とは別の遠隔地にデータ等を保管することをいいます。

ハッシュ値

ハッシュ関数から生成される値をいいます。

秘密鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵をいいます。

秘密鍵のエスクロー

秘密鍵の紛失対策等として、秘密鍵を第三者に預けることをいいます。

リポジトリ（Repository）

CA の証明書および CRL 等を格納し公表するデータベースをいいます。