<table>
<tr><th>掲載箇所</th><th>改定後</th><th>改定前</th><th>差分</th></tr>
<tr><td>表紙</td><td>2023 年 12 月</td><td>2019 年 1 月</td><td>変更</td></tr>
<tr><td>表紙</td><td>Version 4.0</td><td>Version 3.0</td><td>変更</td></tr>
<tr><td>改版履歴</td><td>
<table>
<tr><th colspan="3">改版履歴</th></tr>
<tr><th>版数</th><th>日付</th><th>内容</th></tr>
<tr><td>1.0</td><td>2005.03.28</td><td>初版発行</td></tr>
<tr><td>1.1</td><td>2006.04.17</td><td>1.5.2. 連絡先　住所表示の変更</td></tr>
<tr><td>1.2</td><td>2010.11.15</td><td>1.5.2. 連絡先　住所表示の変更</td></tr>
<tr><td>1.3</td><td>2012.03.13</td><td>受領書廃止に伴う関連項目の変更</td></tr>
<tr><td>1.4</td><td>2013.03.01</td><td>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</td></tr>
<tr><td>1.5</td><td>2013.04.01</td><td>1.5.1.及び 1.5.2.　組織変更に伴う部署名の変更</td></tr>
<tr><td>1.6</td><td>2014.10.01</td><td>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</td></tr>
<tr><td>1.7</td><td>2015.08.03</td><td>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</td></tr>
</table>
</td><td>
<table>
<tr><th colspan="3">改版履歴</th></tr>
<tr><th>版数</th><th>日付</th><th>内容</th></tr>
<tr><td>1.0</td><td>2005.03.28</td><td>初版発行</td></tr>
<tr><td>1.1</td><td>2006.04.17</td><td>1.5.2. 連絡先　住所表示の変更</td></tr>
<tr><td>1.2</td><td>2010.11.15</td><td>1.5.2. 連絡先　住所表示の変更</td></tr>
<tr><td>1.3</td><td>2012.03.13</td><td>受領書廃止に伴う関連項目の変更</td></tr>
<tr><td>1.4</td><td>2013.03.01</td><td>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</td></tr>
<tr><td>1.5</td><td>2013.04.01</td><td>1.5.1.及び 1.5.2.　組織変更に伴う部署名の変更</td></tr>
<tr><td>1.6</td><td>2014.10.01</td><td>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</td></tr>
<tr><td>1.7</td><td>2015.08.03</td><td>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</td></tr>
</table>
</td><td>追加</td></tr>
</table>

掲載箇所	改定後			改定前			差分
	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	1.8	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	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	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	

<table>
<tr><th>掲載箇所</th><th>改定後</th><th>改定前</th><th>差分</th></tr>
<tr><td></td><td>
<table>
<tr><td>3.0</td><td>2019.1.21</td><td>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</td></tr>
<tr><td>4.0</td><td>2023.12.12</td><td>7.1. 証明書のプロファイルの変更
7.2. CRL のプロファイルの変更</td></tr>
</table>
</td><td>
<table>
<tr><td>3.0</td><td>2019.1.21</td><td>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</td></tr>
</table>
</td><td></td></tr>
<tr><td>4.5.1. 秘密鍵および証明書の利用</td><td>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-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。</td><td>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。</td><td>削除</td></tr>
<tr><td>7.1-1 証明書のプロファイルー基本領域</td><td>
<table>
<tr><th>フィールド（説明）</th><th>当行CA証明書</th><th>利用者証明書</th><th>備考（証明書の記載内容）</th></tr>
<tr><td>version（証明書形式のバージョン）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>serialNumber（証明書ごとに割り当てられるユニークな番号）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>signature</td><td>○</td><td>○</td><td>当行はアルゴリズムとして sha256withRSAEncryption (1 2 840 113549 1 1 11) を使用します。</td></tr>
</table>
</td><td>
<table>
<tr><th>フィールド（説明）</th><th>当行CA証明書</th><th>利用者証明書</th><th>備考（証明書の記載内容）</th></tr>
<tr><td>version（証明書形式のバージョン）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>serialNumber（証明書ごとに割り当てられるユニークな番号）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>signature（CA が証明書に署名する際に使用する</td><td>○</td><td>○</td><td>当行は、アルゴリズムとして sha1withRSAEncryption (1 2 840 113549 1 1 5)又は</td></tr>
</table>
</td><td>削除</td></tr>
</table>

<table>
<tr><th>掲載箇所</th><th>改定後</th><th>改定前</th><th>差分</th></tr>
<tr><td></td><td>
<table>
<tr><td>（CA が証明書に署名する際に使用する署名アルゴリズム）</td><td></td><td></td><td></td></tr>
<tr><td>validity
（証明書の有効期間（開始および終了））</td><td>○</td><td>○</td><td>当行が発行する証明書は、UTCTime で記載します。</td></tr>
<tr><td>issuer
（証明書の発行者名）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>subject
（証明書に対応する秘密鍵の所有者名）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>subjectPublicKeyInfo
（秘密鍵に対応している公開鍵情報）</td><td>○</td><td>○</td><td>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。</td></tr>
</table>
</td><td>
<table>
<tr><td>署名アルゴリズム）</td><td></td><td></td><td>sha256withRSAEncryption (1 2 840 113549 1 1 11) を使用します。</td></tr>
<tr><td>validity
（証明書の有効期間（開始および終了））</td><td>○</td><td>○</td><td>当行が発行する証明書は、UTCTime で記載します。</td></tr>
<tr><td>issuer
（証明書の発行者名）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>subject
（証明書に対応する秘密鍵の所有者名）</td><td>○</td><td>○</td><td>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。</td></tr>
<tr><td>subjectPublicKeyInfo
（秘密鍵に対応している公開鍵情報）</td><td>○</td><td>○</td><td>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。</td></tr>
</table>
</td><td></td></tr>
<tr><td>7.2-1 CRL プロファイルー証明書リスト領域</td><td>
<table>
<tr><th>フィールド（説明）</th><th>CRL</th><th>備考（CRL の記載内容）</th></tr>
<tr><td>version
（CRL 形式のバージョン）</td><td>○</td><td>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。</td></tr>
<tr><td>signature
（CA が CRL に署名する際に使用する署名アルゴリズム）</td><td>○</td><td>当行はアルゴリズムとして sha256withRSAEncryption (1 2 840 113549 1 1 11) を使用します。</td></tr>
</table>
</td><td>
<table>
<tr><th>フィールド（説明）</th><th>CRL</th><th>備考（CRL の記載内容）</th></tr>
<tr><td>version
（CRL 形式のバージョン）</td><td>○</td><td>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。</td></tr>
<tr><td>signature
（CA が CRL に署名する際に使用する署名アルゴリズム）</td><td>○</td><td>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。</td></tr>
</table>
</td><td>削除</td></tr>
</table>

<table>
<tr><th>掲載箇所</th><th>改定後</th><th>改定前</th><th>差分</th></tr>
<tr>
<td></td>
<td>
<table>
<tr><td>issuer
（CRL の発行者名）</td><td>○</td><td>当行が発行する CRL には、当行の CA の名前を記載します。</td></tr>
<tr><td>thisUpdate
（CA により CRL が発行された日時）</td><td>○</td><td>当行が発行する CRL は、UTCTime で記載します。</td></tr>
<tr><td>nextUpdate
（CRL が次回発行される日時）</td><td>○</td><td>当行が発行する CRL は、UTCTime で記載します。</td></tr>
<tr><td>RevokedCertificates
（失効された証明書の情報）</td><td>○</td><td>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。</td></tr>
</table>
</td>
<td>
<table>
<tr><td></td><td></td><td></td></tr>
<tr><td>issuer
（CRL の発行者名）</td><td>○</td><td>当行が発行する CRL には、当行の CA の名前を記載します。</td></tr>
<tr><td>thisUpdate
（CA により CRL が発行された日時）</td><td>○</td><td>当行が発行する CRL は、UTCTime で記載します。</td></tr>
<tr><td>nextUpdate
（CRL が次回発行される日時）</td><td>○</td><td>当行が発行する CRL は、UTCTime で記載します。</td></tr>
<tr><td>RevokedCertificates
（失効された証明書の情報）</td><td>○</td><td>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。</td></tr>
</table>
</td>
<td></td>
</tr>
</table>