VALUX サービス

認証局運用規程

2013 年 11 月 1 日

NTT データ

Version 3.2

1. はじめに

VALUX サービス認証局運用規程（以下、「本 CPS」という）は、VALUX サービス認証局（以下、「本認証局」という）の運用内容に関する規程である。

本認証局は、NTT データがシステム全体の維持管理業務および発行局、登録局の運用業務を実施し、またその業務の責任を負う。

1.1 概要

VALUX サービスは、インターネット上にコンテンツ提供のためのセキュアなネットワークを提供するために、証明書の発行・更新を実現する認証局業務や証明書の有効性検証や利用者の契約管理を提供する。

VALUX サービスの利用者が VALUX サービスを利用するにあたって、セキュリティを確保する観点から強固なユーザ認証を実施する必要がある。

本認証局は、VALUX サービスの利用者に対して、VALUX サービスへのアクセスの際に使用するユーザ認証用の証明書（以下、「VALUX クライアント証明書」という）を発行する。

VALUX サービスの利用者は、VALUX サービスを利用する際に VALUX クライアント証明書を使用して、SSL クライアント認証を実施する。

なお、この文書は、RFC 3647 に準拠している。

1.2 文書名と識別

この文書の名称は、「VALUX サービス 認証局運用規程」（以下、「本 CPS」）とする。

また、本 CPS に割り当てられるオブジェクト識別子については規定しない。

1.3 PKI の関係者

本 CPS の適用範囲は、本認証局により実施される証明書の発行業務、失効業務、および付帯するその他の業務に適用される。

本認証局は、発行局、登録局、およびリポジトリによって構成される。本認証局は、NTT データがシステム全体の維持管理および発行局、登録局の運用業務を実施する。

1.3.1 発行局

発行局は、本認証局における VALUX クライアント証明書の発行業務を行う。発行局は、本認証局の秘密鍵（以下、「認証局秘密鍵」という」）の生成、管理、廃棄、VALUX クライアント証明書の発行処理を行う。

発行局は証明書発行対象者による VALUX クライアント証明書の発行要求および登録局による VALUX クライアント証明書の発行の許可に基づき、VALUX クライアント証明書の発行処理を実施する。

NTT データは、発行局のシステムの維持管理業務および運用業務を外部に委託し、またそれらの業務の責任を負う。

1.3.2 登録局

登録局は、VALUX クライアント証明書の発行の可否を判断する。判断の結果、VALUX クライアント証明書の発行を実施することとなった場合、登録局は VALUX クライアント証明書の発行を許可する。

また、登録局は、VALUX クライアント証明書の失効の可否を判断する。判断の結果、VALUX クライアント証明書の失効を実施することとなった場合、登録局は VALUX クライアント証明書の失効を実施する。

NTT データは、登録局のシステムの維持管理業務を実施し、またその業務の責任を負う。一方、登録局の運用業務は NTT データが実施し、またその業務の責任を負う。

NTT データは、VALUX サービスの利用者に対して提示される VALUX サービスの利用者向けの利用規約（以下、「VALUX サービス利用規約」という）の内容を規定する。

1.3.3 証明書発行対象者

証明書発行対象者は、VALUX サービスの利用者であり、登録局に対して VALUX クライアント証明書の発行申請を行い、かつ発行が認められた者である。VALUX サービスの利用者は、NTT データが定める VALUX サービス利用規約に同意し、遵守しなければならない。

1.3.4 証明書検証者

VALUX クライアント証明書の検証者は、VALUX サービスのサービス提供者である NTT データである。NTT データは、VALUX クライアント証明書の検証を行い、VALUX サービスへのアクセスを許可するかどうかを判断する。

1.3.5 リポジトリ

本認証局は、ANSER(VALUX)サーバ、全銀ファイル伝送(VALUX)サーバおよびNTTデータに対して、発行したVALUXクライアント証明書の状態に関する情報を提供する。

本認証局から発行したVALUXクライアント証明書は、リポジトリを用いて外部に対して公開しない。また、VALUXクライアント証明書の失効情報はVALUXサービスでのみ使用するため、リポジトリを用いて外部に対して公開しない。

1.3.6 申込者

申込者は、VALUXサービスの申込、および、証明書申込内容を登録局に申請する者である。

1.4 証明書の用途

1.4.1 適切な証明書の用途

VALUXクライアント証明書は、VALUXサービスの利用者がVALUXサービスへアクセスする際のユーザ認証の用途にのみ使用される。

また、ルートCA証明書は、VALUXサービスの利用者がVALUXサービスへアクセスする際に、VALUXサービスのサーバがVALUXクライアント証明書の検証を行う際に使用される。

1.4.2 禁止される証明書の用途

VALUXクライアント証明書は、本CPSの「１．４．１適切な証明書の用途」で規定した用途以外の用途に使用してはならない。

1.5 ポリシ運用管理

1.5.1 文書を管理する組織

本CPSは、以下の組織が管理する。本CPS中、「NTTデータ」と記された箇所は以下の組織体を指す。

株式会社エヌ・ティ・ティ・データ　パブリック＆フィナンシャルカンパニー
第二金融事業本部　ｅービジネスビジネスユニット　法人ｅービジネス統括部
東京都港区三田4-19-15 NTTDATA三田ビル　03-5765-0517

1.5.2 問合せ先

本 CPS に関する問合せ先は、以下のとおりである。

VALUX カスタマーセンタ

電話　0570-041800

1.5.3 CPS に対する適合性を判断する者

NTT データは、「VALUX サービス CPS 管理要領」に既定の手続に従って適合性を判断する。

1.5.4 CPS の承認の手順

NTT データは、「VALUX サービス CPS 管理要領」に既定の手続に従って本 CPS を承認する。

1．6 用語の定義と略語

本利用規約で使用される用語および略語の定義を以下に示す。

項番	略語	正式名称	意味
1	CPS	Certification Practice Statement	認証局で証明書の発行などの運用を行うときの手順を規定した文書
2	認証局		利用者を識別・認証し、証明書等を発行する機関
3	発行局		登録局で識別された利用者の証明書等を発行する部門 NTT データは、クライアント証明書の発行に関する発行局の業務を、シマンテック マネージド PKI サービスの契約を通じて、日本ベリサイン株式会社に委託する
4	登録局		利用者を識別・認証し、発行局に証明書等の発行要求を行う部門
5	証明書		利用者が使用する公開鍵を証明する電子データ
6	公開鍵		公開鍵暗号で生成される２つの暗号鍵のうち、公開してもよい暗号鍵
7	秘密鍵		公開鍵暗号で生成される２つの暗号鍵のうち、生成した当人のみが所有する暗号鍵
8	SSL	Secure Socket Layer	Netscape 社が開発した通信の暗号化や通信相手を識別する技術
9	RFC 3647		CPS の記載項目について規定している規約
10	オブジェクト識別子		電子データがどのような意味を持つのかを識別するために付与する数字
11	PKI	Public Key Infrastructure	認証局が発行した証明書を用いて認証を行うシステムの基盤
12	リポジトリ		証明書や CRL を格納し、公開するためのサーバ
13	ユーザ認証		SSL クライアント認証のことであり、証明書等を用いてサーバに接続したユーザの認証を行うこと
14	ルート CA		認証局の信頼の元となる上位の認証局
15	自己署名証明書		ルート CA の認証局自身の証明書
16	CRL	Certificate Revocation List	失効した証明書の一覧が記載されている電子データ
17	ITU X.500 識別名		国際電気通信連合が定めたディレクトリサービスの国際標準
18	DN	Distinguished Name	証明書に記載している識別するための名称

項番	略語	正式名称	意味
19	電子署名		秘密鍵で暗号化された電子データ １人のみ所有している暗号鍵で暗号化することで、電子データが誰によって作成された物かを保証することができる
20	危殆化		情報が漏洩、紛失、類推などによって信頼性が失われた状態
21	FIPS 140-1 レベル 3		米国の NIST によって定められた暗号モジュールのセキュリティ要件 レベル 3 は、ハードウェアから電子データ（暗号鍵など）を取り出せないような要件が定められている
22	CA	Certificate Authority	認証局のこと

2. 公開とリポジトリの責任

2.1 リポジトリ

本認証局では、リポジトリを用いて VALUX クライアント証明書および VALUX クライアント証明書の失効情報を外部に対して公開しない。このため本項目を規定しない。

2.2 認証情報の公開

本認証局は、自己署名証明書、VALUX クライアント証明書および CRL を公開しない。

また、本認証局に関する重大な情報は、NTT データより VALUX サービスの利用者ならびに外部に対して開示は行わない。VALUX サービスの利用者ならびに外部に対しての情報公開は、NTT データが自身の判断により実施する。

2.3 公開の頻度

本認証局は、自己署名証明書、VALUX クライアント証明書および CRL を公開しない。

2.4 リポジトリへのアクセス制御

本認証局では失効情報を外部に公開しない。このため本項目を規定しない。

2.5 発行局の業務に関する義務

発行局は署名鍵が危殆化しないよう、善良なる管理者の注意をもって管理する。

また、発行局は登録局の発行指示に基づき加入者証明書の発行、失効を行う。

3. 識別と認証

3.1 命名

3.1.1 名前の型

VALUX クライアント証明書の発行者名(Issuer Name)および所有者名(subject Name)は、ITU X.500 識別名の形式に従い設定する。

以下に、VALUX クライアント証明書で使用する名前の型を示す。ただし、各 DN の値は例である。

VALUX クライアント証明書の Issuer
CN = Payment Solutions Sector CA-2048 または Payment Solutions Sector CA-SHA2
O = NTT DATA CORPORATION

VALUX クライアント証明書の subject
T = (**任意**)
CN = AAAAAAAAAAAA BBBBBBBB YYYYMMDDhhmmssSSSCC
OU = Payment Solutions Sector CA-2048 または Payment Solutions Sector CA-SHA2
O = NTT DATA CORPORATION
C = JP

ただし、2012 年 9 月 30 日までに発行される証明書の情報は以下のとおり。
VALUX クライアント証明書の issuer：
ou = Root CA
ou = Payment Solutions Sector CA
o = NTT DATA CORPORATION
c = JP

VALUX クライアント証明書の subject
t = (任意)
cn = AAAAAAAAAAAA BBBBBBBB YYYYMMDDhhmmssSSSCC
ou = Payment Solutions Sector CA
o = NTT DATA CORPORATION
c = JP

3.1.2 名前の意味に関する要件

VALUX クライアント証明書には、本 CPS の「３．１．１名前の型」で表した意味を持つ。

3.1.3 証明書発行対象者の匿名性、仮名性

VALUX クライアント証明書では、NTT データが認証した VALUX サービスの利用者を一意に識別する値として VALUX クライアント証明書の subject における CN を使用する。これにより、証明書発行対象者の識別を行う。

3.1.4 名前形式を解釈するための規則

名前形式の解釈は、ITU X.500 識別名の規定に従う。

3.1.5 名前の一意性

VALUX クライアント証明書に記載する subject は、本認証局によって、VALUX クライアント証明書ごとに一意に付与される。

3.1.6 認識、識別および商標の役割

VALUX クライアント証明書には、発行者名または所有者名に、NTT データまたは NTT データが保有している商標が含まれることがある。

3.2 初回の本人確認

3.2.1 秘密鍵の所有を証明する方法

VALUX クライアント証明書の発行において、鍵ペアの生成は VALUX サービスの利用者により行われる。当該 VALUX サービスの利用者は生成した鍵ペアを用いて VALUX クライアント証明書の発行要求を作成する。

3.2.2 組織の実在性の認証

VALUX クライアント証明書の発行における、VALUX サービスの利用者が所属する組織の実在性の確認は、NTT データが独自に規定する方式に基づき行う。

3.2.3 個人の実在性の認証

VALUX クライアント証明書の発行における、VALUX サービスの利用者の実在性の確認は、NTT データが独自に規定する方式に基づき行う。かつ、申請者が組織に所属している場合、本 CPS の「3.2.2　組織の実在性の認証」に示した方法で、VALUX サービスの利用者が実在性を確認した組織に所属していることもあわせて確認する。

3.2.4 検証されない証明書発行対象者の情報

本認証局は、証明書発行対象者の VALUX サービスの利用適格性以外の情報の検証を行わない。

3.2.5 権限の検証

本認証局は、VALUX クライアント証明書の発行可否を判断する際に、証明書発行対象者の VALUX サービスの利用適格性を検証する。その他の権限、資格等の検証は実施しない。

3.2.6 相互運用の基準

本認証局では、他の認証局との相互運用を行わない。このため相互運用の基準を規定しない。

3.3 証明書の更新または再発行の識別と認証

3.3.1 証明書の更新の識別と認証

VALUX クライアント証明書の更新時の本人確認は、旧 VALUX クライアント証明書を用いたユーザ認証を用いて行う。

3.3.2 失効後の証明書の再発行の識別と認証

VALUX クライアント証明書の失効後の再発行時の本人確認は、本 CPS の「３．２初回の本人確認」で規定した内容と同一の方法をもって行う。

3.4 失効要求の識別と認証

本認証局は、VALUX クライアント証明書の失効時の本人確認を、NTT データが独自に規定する方式に基づき行う。かつ、申請者が組織に所属している場合、本 CPS の「３．２．２組織の実在性の認証」に示した方法で、VALUX サービスの利用者が実在性を確認した組織に所属していることもあわせて確認する。

4. 証明書ライフサイクルの運用要件

4.1 VALUX 利用申請

4.1.1 VALUX サービス利用申込を実施できる者

VALUX サービスの利用申込を実施できる者は、VALUX サービスを希望する者とする。

4.1.2 利用申込の処理と責任

VALUX サービスの申込者は、VALUX サービスの使用申込を正確な内容で作成し、登録局に対して送付する。

4.2 証明書の発行申込

4.2.1 証明書の発行申込を実施できる者

VALUX クライアント証明書の発行申込を実施できる者は、VALUX サービスの申込が完了した申込者である。

4.2.2 使用申請の処理と責任

申込者は、VALUX クライアント証明書の発行申込を正確な内容で作成し、登録局に対して送付する。

4.3 証明書の発行申請

4.3.1 証明書の発行申請を実施できる者

VALUX クライアント証明書の発行申請をできる者は、識別コードを所有する利用者である。

4.3.2 発行申請の処理と責任

VALUX サービスの利用者は、VALUX サービスの利用申請を正確な内容で作成し、登録局に対して提出する。

また、VALUX クライアント証明書の発行許可が出た場合、VALUX サービスの利用者は VALUX クライアント証明書の発行要求を VALUX クライアントを用い、インターネットを経由して登録局に送信する。

4.4 証明書の発行申請の処理

4.4.1 識別および認証の作業の実行

NTT データは、VALUX クライアント証明書の発行申請が届いた場合、速やかに証明書発行のための審査を実施する。

4.4.2 証明書の発行申請の承認または拒絶

申込者により払い出された識別コードにより、認証した場合は、登録局のシステムは当該 VALUX クライアント証明書の発行を可能とする状態にする。

4.4.3 証明書の発行申請を処理する期間

NTT データは、VALUX クライアント証明書の発行申請の審査および VALUX クライアント証明書の発行処理を、商業上合理的な期間でできるだけ速やかに実施する。

4.5 証明書の発行

4.5.1 証明書の発行における発行局の動作

発行局では、登録局から送信された VALUX クライアント証明書の発行要求を受領した後、VALUX クライアント証明書を発行する。

4.5.2 発行局による証明書発行のエンドユーザへの通知

発行局は、新しい鍵ペアによる認証用証明書をインターネットを経由して VALUX クライアントに送信する。

4．6 証明書の受領

4．6．1 証明書の受領が成立するための行為

VALUX サービスの利用者は、VALUX クライアントを用いた証明書発行申請が正常に完了したことを確認することをもって証明書の受領が成立したとみなす。

4．6．2 発行局による証明書の公開

本認証局では発行した VALUX クライアント証明書を外部に公開しない。このため本項目を規定しない。

4．6．3 発行局による、証明書の発行の関係者への通知

本認証局では発行した VALUX クライアント証明書を外部に公開しない。このため本項目を規定しない。

4．7 鍵ペアと証明書の用途

4．7．1 証明書発行対象者の秘密鍵と証明書の用途

VALUX サービスの利用者は、VALUX クライアント証明書および秘密鍵を VALUX サービスのユーザ認証にのみ使用することができる。それ以外の用途に VALUX クライアント証明書および秘密鍵を使用することはできない。

4．7．2 検証者の公開鍵と証明書の用途

VALUX クライアント証明書の検証者は、VALUX サービスのサービス提供者である NTT データである。それ以外の者が VALUX クライアント証明書の検証を行い、検証結果に依拠した場合、本認証局はそのいかなる結果に対しても責任を持たない。

4．8 証明書の更新

本認証局では、旧 VALUX クライアント証明書と同じ鍵ペアを使用した VALUX クライアント証明書の更新を行わない。このため本項目を規定しない。

4.8.1 証明書の更新を行う場合

規定しない。

4.8.2 証明書の更新を要求できる者

規定しない。

4.8.3 証明書の更新の要求の処理

規定しない。

4.8.4 更新された証明書の発行の証明書発行対象者への通知

規定しない。

4.8.5 更新された証明書の受領が成立するための要件

規定しない。

4.8.6 発行局による更新された証明書の公開

規定しない。

4.8.7 発行局による、更新された証明書の発行の関係者への通知

規定しない。

4.9 証明書の鍵ペアの再生成

4.9.1 証明書の鍵ペアの再生成を行う場合

VALUX クライアント証明書の有効期間が短くなり、かつ引き続き VALUX サービスの利用を継続する場合、鍵ペアを再生成した VALUX クライアント証明書の更新を行う。なお、本行為のことを、利用者に対しては「証明書の更新」と呼称する。

４．９．２ 新しい公開鍵の証明を要求できる者

鍵ペアを再生成したVALUXクライアント証明書の更新は、VALUXサービスの利用者が実施できる。

４．９．３ 証明書の鍵ペアの再生成の要求の処理

VALUXサービスの利用者は、旧VALUXクライアント証明書を用いたユーザ認証を登録局に対して行う。

登録局ではユーザ認証を実施する。ユーザ認証が正常に実施された場合、VALUXサービスの利用者はVALUXクライアント証明書の発行要求をVALUXクライアントを用い、インターネットを経由して登録局に送信する。

４．９．４ 新しい鍵ペアによる証明書の発行の証明書発行対象者への通知

発行局は、新しい鍵ペアによる認証用証明書をインターネットを経由してVALUXクライアントに送信する。

４．９．５ 新しい鍵ペアによる証明書の受領が成立するための要件

VALUXサービスの利用者は、VALUXクライアントを用いた証明書発行申請が正常に完了したことを確認することをもって証明書の受領が成立したとみなす。

４．９．６ 発行局による新しい鍵ペアによる証明書の公開

本認証局では発行したVALUXクライアント証明書を外部に公開しない。このため本項目を規定しない。

４．９．７ 発行局による、新しい鍵ペアによる証明書の関係者への通知

本認証局では発行したVALUXクライアント証明書を外部に公開しない。このため本項目を規定しない。

4. 10 証明書の変更

本認証局では、VALUX クライアント証明書の設定値の内容を変更するために、VALUX クライアント証明書を発行することはない。このため本項目を規定しない。

4. 10. 1 証明書の変更を行う場合

規定しない。

4. 10. 2 証明書の変更を要求できる者

規定しない。

4. 10. 3 証明書の変更の要求の処理

規定しない。

4. 10. 4 変更後の新しい証明書の証明書発行対象者への通知

規定しない。

4. 10. 5 変更後の証明書の受領が成立するための要件

規定しない。

4. 10. 6 発行局による変更後の証明書の公開

規定しない。

4. 10. 7 発行局による、変更後の証明書の関係者への通知

規定しない。

4.11 証明書の失効と効力の一時停止

4.11.1 失効を行う場合

VALUX クライアント証明書は、以下の事由がある場合には失効される。

・当該 VALUX サービスの利用者が VALUX サービスの使用を終了するとき
・本認証局の運用を終了するとき
・当該 VALUX クライアント証明書の内容に不備があるとき
・当該 VALUX クライアント証明書の秘密鍵が危殆化したとき
・認証局秘密鍵が危殆化したとき
・その他、当該 VALUX クライアント証明書を失効するに足る理由があるとき

4.11.2 失効を要求できる者

VALUX クライアント証明書の失効の申請は、利用者および本認証局の双方が実施できる。

4.11.3 失効の要求の処理

VALUX サービスの利用者が当該 VALUX クライアント証明書の失効を申請する場合、申込者を経由して失効申請書類を本認証局に対して提出する。

緊急時は、NTT データが別途定めた方式に基づき、失効申請者の本人確認を実施した上で、失効申請を行う。

登録局では当該 VALUX クライアント証明書の失効申請内容を審査し、失効を認めた場合は失効の処理を行う。

4.11.4 失効要求の猶予期間

VALUX サービスの利用者が VALUX サービスの利用を終了する場合、または当該 VALUX クライアント証明書の内容に不備があるとき、VALUX サービスの利用者は当該 VALUX クライアント証明書の失効申請を速やかに提出する。

一方、当該 VALUX クライアント証明書の秘密鍵が危殆化した場合、VALUX サービスの利用者は即座に当該 VALUX クライアント証明書の失効申請を提出する。

4.11.5 認証局が失効要求を処理しなければならない期間

VALUX サービスの利用者が VALUX サービスの利用を終了する場合、または当該 VALUX クライアント証明書の内容に不備があるとき、VALUX サービスの利用者は当該 VALUX クライアント証明書

の失効申請を速やかに提出する。

一方、当該 VALUX クライアント証明書の秘密鍵が危殆化した場合、VALUX サービスの利用者は即座に当該 VALUX クライアント証明書の失効申請を提出する。

4.11.6 関係者に対する失効の確認の要件

本認証局では、失効情報を VALUX サービスの内部でのみ使用する。このため本項目を規定しない。

4.11.7 CRL の発行周期

本認証局では、失効情報を VALUX サービスの内部でのみ使用する。このため本項目を規定しない。

4.11.8 CRL の発行から公開までの時間

本認証局では、失効情報を VALUX サービスの内部でのみ使用する。このため本項目を規定しない。

4.11.9 オンラインでの失効または状態の確認の可能性

本認証局では、失効情報を VALUX サービスの内部でのみ使用する。このため本項目を規定しない。

4.11.10 オンラインでの失効の確認の要件

本認証局では、失効情報を VALUX サービスの内部でのみ使用する。このため本項目を規定しない。

4.11.11 その他の利用が可能な失効通知の形式

本認証局では、失効情報を VALUX サービスの内部でのみ使用する。このため本項目を規定しない。

4.11.12 鍵の危殆化の場合の特殊な要件

VALUX クライアント証明書の秘密鍵の危殆化または認証局秘密鍵の危殆化が発生した場合、本認証局は即座に失効要求を処理する。

4.11.13 効力の一時停止を行う場合

VALUX サービス利用規約に違反する事実が確認された場合、VALUX の判断により、証明書の効力の一時停止を行う場合がある。

4.11.14 効力の一時停止を要求できる者

VALUX サービス利用規約に違反する事実が確認された場合、VALUX の判断により、証明書の効力の一時停止を行う場合がある。

4.11.15 効力の一時停止の要求の処理

VALUX サービス利用規約に違反する事実が確認された場合、VALUX の判断により、証明書の効力の一時停止を行う場合がある。

4.11.16 効力の一時停止の期間の上限

VALUX サービス利用規約に違反する事実が確認された場合、VALUX の判断により、証明書の効力の一時停止を行う場合がある。

4.12 証明書の状態を確認するためのサービス

4.12.1 運用上の特徴

本認証局では、VALUX サービスのサーバおよび NTT データに対して証明書の状態を確認するためのサービスを内部でのみ使用する。このため本項目を規定しない。

4.12.2 サービスの利用可能性

本認証局では、VALUX サービスのサーバおよび NTT データに対して証明書の状態を確認するためのサービスを内部でのみ使用する。このため本項目を規定しない。

4.12.3 オプション機能

本認証局では、VALUX サービスのサーバおよび NTT データに対して証明書の状態を確認するためのサービスを内部でのみ使用する。このため本項目を規定しない。

4．13 登録の終了

VALUX サービスの利用者が VALUX サービスの利用を終了する場合、VALUX サービスの利用者は本 CPS の「４．１１証明書の失効と効力の一時停止」の規定に従い、当該 VALUX クライアント証明書の失効を行うものとする。

4．14 鍵の預託と復旧

4．14．1 秘密鍵の預託と復旧に関する規定

本認証局では、秘密鍵の預託を行わない。このため本項目を規定しない。

4．14．2 セッション鍵のカプセル化と復旧に関する規定

本認証局では、秘密鍵の預託を行わない。このため本項目を規定しない。

5. 設備、運用、操作に関する管理

5.1 物理的管理

5.1.1 登録局に関する記述

本登録局は、財団法人　金融情報システムセンタが制定した「金融機関等コンピュータシステムの安全対策基準・解説書　第6版追補」に準拠した施設のセキュリティを確保している。

5.1.1.1 施設の場所と建物の構造

本登録局施設を収容する建築構造物（建物および部屋）は、耐震耐火設計、自動火災報知器と消火装置の設置、水害防止等の措置が予め十分講じられている等、地震、火災、水害等を想定した災害対策がなされた施設である。登録局施設へは、建物に入館後、複数のセキュリティレベルで区画された場所を通った後に入室できるものとする。

5.1.1.2 物理的アクセス

本登録局の施設は、不正侵入による被害を防ぐための設備を用意し、適切な物理的アクセスのみが許可されるようにする。

5.1.1.3 電源設備および空調設備

本登録局の施設は、電源設備および空調設備において、一次および予備の設備を備えている。

5.1.1.4 水害対策

本登録局の施設は、水害による被害を防止するための設備を備えている。

5.1.1.5 火災対策

本登録局の施設は、火災による被害を防止するための設備を備えている。

5.1.1.6 媒体管理

本登録局のシステムのバックアップデータを保管する媒体は、本登録局の施設または外部の安全な施設で保管される。

5．1．1．7 廃棄物処理

本登録局より排出される廃棄物は、秘密情報が完全に消去されるための回復不可能な方法で破壊または処分を行う。

5．1．1．8 外部バックアップ

本登録局については規定しない。

5．1．2 発行局に関する記述

5．1．2．1 施設の場所と建物の構造

本発行局施設を収容する建築構造物（建物および部屋）は、耐震耐火設計、自動火災報知器と消火装置の設置、防火区画内設置、隔壁による区画、水害防止等の措置が予め十分講じられている等、地震、火災、水害等を想定した災害対策がなされた施設である。発行局施設へは、建物に入館後、複数のセキュリティレベルで区画された場所を通った後に入室できるものとする。

発行局施設の所在および仕様は、関係者以外には公表されない。建物の内外には発行局施設の所在については表示されない。災害対策設備に関しても発行局施設と同等の管理を行う。

5．1．2．2 物理的アクセス

本発行局施設については、次により厳重に管理されるものとする。

(1) 発行局施設は厳重に施錠管理され、その入室は入室者の身体的特徴の識別手段を用いた施錠設備による本人認証を行ってはじめて可能となるよう予め防護措置が講じられている。発行局施設に入室権限を有しない者は、付添なしで入室することはできない。

(2) セキュリティおよび監査要件ガイドに従い、発行局施設の一部には、複数人によってのみ入退室可能な領域を設置している。

(3) 入室のための装置操作に不正常な時間を要した場合においては、警報が発せられるよう予め設定されるものとする。

(4) 発行局施設への入退室者および在室者の状況については、遠隔監視装置、モーションセンサーおよび映像記録装置によって自動的かつ継続的に監視記録され、その記録については、正確に点検され、定められた期間、安全に保存される。

5．1．2．3 電源設備および空調設備

本発行局施設は停電に備えたUPS・自家発電機の設置、配置された設備に応じた空調機器の設置等、サービスの継続に必要な適切な措置が講じられている。

5．1．2．4 水害対策

本発行局施設は水害防止等の措置が予め講じられている。

5．1．2．5 火災対策

本発行局施設は、火災予防と火災被害への対応に関して合理的な対策を講じている。本発行局施設の火災予防対策は、国内の火災予防規則に則って設計されている。

5．1．2．6 媒体管理

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

5．1．2．7 廃棄物処理

本発行局より排出される重要な文書などは廃棄時に回復不可能な方法により処理される。重要な情報を含む媒体は廃棄前に再読み出しが不可能なようにフォーマットする。また、暗号モジュールデバイスは廃棄前に物理的に破壊されるか、デバイスの機能を用い初期化する。

5．1．2．8 外部バックアップ

本発行局については「５．７．３．２災害後の業務の継続の能力」のとおり。

5．2 手続的管理

5．2．1 登録局に関する記述

5．2．1．1 信頼を受けた役割

登録局設備において信頼される人物となるためには、人事担当者との面接および広く認識されている身分証明書（パスポート、運転免許証等）の調査により、身元についての確認作業を行う。

信頼される人物には、認証局の運用業務に関わるすべての従業員、独立請負業者およびコンサルタントが含まれる。

以上に加えて、クライアント証明書発行要求と承認を管理する管理者および責任者については、発行局運営者側からも次のいずれかの情報を照合することで、存在確認を行う。

・存在確認のためのサービス(主要な信用機関またはその他の信用できる情報提供サービス)

・証明書を承認する登録局の従業員または顧客リストなどの業務上の記録またはデータベースに含まれる情報

5．2．1．2 作業を実施する際に必要な人数

本登録局は、システム全体の維持管理業務および認証局の運用業務において個人情報を取り扱うような重要な作業を行う場合は、複数の信頼される人物により行われ、相互牽制および相互確認を実施する。

これらの内部統制手続は、物理的または論理的に登録局施設にアクセスするために最低 2 名の信頼される人物が必要となり、満足しない場合は検知して是正できるよう設計されている。

5．2．1．3 それぞれの役割の識別と認証

本登録局は、システム全体の維持管理業務および認証局の運用業務において、施設への入館時やシステムの利用時等の際に、適切な方法を用いて各役職の本人性確認を実施する。

5．2．1．4 任務の分離が必要な役割

本登録局は、システム全体の維持管理業務および認証局の運用業務において、相互牽制が行なくなる組み合わせでの役職の兼任を認めない。

5．2．2 発行局に関する記述

5．2．2．1 信頼を受けた役割

発行局施設において信頼される人物となるためには、人事担当者との面接および広く認識されている身分証明書（パスポート、運転免許証等）の調査により、身元についての確認作業を行う。

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

・証明書申請中の情報の検証
・証明書申請、失効要求、更新要求または申込情報の承認、拒絶その他の処理
・証明書の発行または失効
・利用者の情報または要求の取り扱い

信頼される人物には、以下の者が含まれるが、これに限定されない。

・カスタマ・サービス要員
・キーマネージャ
・セキュリティ要員
・システム管理者
・技術要員のうち指定された者
・認証事業の基盤の信頼性を管理するために指名された経営陣

5．2．2．2 作業を実施する際に必要な人数

発行局施設では、業務内容に基づく職務分掌を確実にするための方針と厳格な管理手続を維持している。発行局用暗号ハードウェアおよび関連する鍵関係資料等の最も機密を要する業務へのアクセスおよび管理は、複数の信頼される人物により行われる。

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

5．2．2．3 それぞれの役割の識別と認証

「５．２．２．１信頼を受けた役割」のとおり。

5．3 要員管理

外部委託している発行局施設の運用員に関する要件は本 CPS で規定しないが、本 CPS で規定される発行業務運用要件に照らして十分な要件を満たしていることを事前に確認している。本項では登録局における人事統制を示す。

5．3．1 資格、経験、および身分証明に関する要件

本登録局は、本登録局の運用を行うために十分な資格を持ち、十分な教育を受けた者のみが本登録局の運用を行うものとする。

5．3．2 経歴確認の手順

本登録局は、適切な方法を用いて運用を行う要員の経歴を確認するものとする。

5．3．3 トレーニングに関する要件

本登録局は、運用を行う要員に対して本登録局の運用に必要な知識を習得させるためのトレーニングを行う。

5．3．4 再トレーニングに関する周期と要件

本登録局は、適切な周期および要件に基づいて、運用を行う要員に対してトレーニングを行う。

5．3．5 仕事のローテーションの周期と順序

規定しない。

5．3．6 権限外の行為に対する制裁

本登録局は、運用を行う要員が権限外の行為を行った場合、懲戒を行うことがある。

5．3．7 請負事業者に関する要件

本登録局は、本登録局の運用を行うにあたって外部の請負事業者に業務の一部を委託することがある。このとき、本登録局のセキュリティが保たれるように、本登録局は必要な対策を行う。

5.3.8 作業者に対する資料の提供

本登録局では、運用を行う要員に対して本登録局の運用に必要な知識を習得させるための資料を提供する。

5.4 監査ログの記録手順

5.4.1 登録局に関する記述

5.4.1.1 記録されるイベントの種類

本登録局は、手動または自動により、次の重要なイベントについて監査ログとして記録する。

・次の事項を含む、セキュリティに関するイベント

・NTT データの要員および NTT データが外部委託した要員によってなされた本登録局のシステムに対する行為。

・取り扱いに慎重を要するファイルまたは記録に関する読み込み、書き込み削除その他変更行為。

・登録局の設備への入退室

本登録局は、本登録局で発生した運用面、セキュリティ面、システム面等の各種情報を監査ログに記載する。

5.4.1.2 ログを取得する周期

監査ログは、記録すべき処理、操作または事象が発生した都度記録される。

5.4.1.3 監査ログの保存期間

監査ログは、1 年間保存する。

5.4.1.4 監査ログの保護

監査ログは、漏洩、改ざん、亡失等を防止する処置を行い、保護を行う。

5．4．1．5 監査ログのバックアップの手順

本登録局は、バックアップが必要な監査ログが存在する場合は、監査ログのバックアップを行う。

5．4．1．6 監査ログ収集システム(内部および外部)

本登録局を構成するシステムの自動処理により、監査ログを取得する。

5．4．1．7 イベントを発生させた者に対する通知

規定しない。

5．4．1．8 脆弱性の評価

本登録局は、週に1回監査ログを検査し、脆弱性の有無を確認する。

5．4．2 発行局に関する記述

5．4．2．1 記録されるイベントの種類

本発行局施設において、次の重要なイベントについて記録する。

(1) 以下の事項を含む、証明書のライフサイクル管理イベント

・証明書申請、更新、失効

・要求の処理

・証明書の生成

(2) 以下の事項を含む、セキュリティに関連するイベント

・発行局施設への来訪者の入退室

・発行局施設システムへのアクセスの試み

・セキュリティ上取り扱いに慎重を要するファイルまたは記録に関する読み込み、書き込みまたは削除

なお、各記録は以下の情報を含む。

・記録の種別

・記録の日時

・記録者の身元（特定できる場合）

5．4．2．2 ログを取得する周期

重要なイベントが発生した場合、発行局施設内の監査ログの確認は随時実施する。

5．4．2．3 監査ログの保存期間

発行局施設において、監査ログは少なくとも２ヶ月間保存される。
証明書のライフサイクルに関する監査ログは少なくとも５年間保存される。

5．4．2．4 監査ログの保護

監査ログは、漏洩、改ざん、亡失等を防止する処置を行い、保護を行う。

5．4．2．5 監査ログのバックアップの手順

バックアップが必要な監査ログは所定のバックアップ手順に従いバックアップを行う。

5．4．2．6 監査ログ収集システム(内部および外部)

発行局施設における監査ログは、発行局施設内のシステムによる自動処理および発行局施設の要員による手作業を組み合わせて、監査ログを収集する。

5．4．2．7 イベントを発生させた者に対する通知

発行局施設における監査ログの監査において調査の必要性がある事象が検出された場合、当該事象の発生者に対し通知なく調査を行う。

5．4．2．8 脆弱性の評価

規定しない。

5．5 記録の保管

5．5．1 登録局に関する記述

5．5．1．1 保管する記録の種類

本登録局は次の記録を保管する。
・「５．４．１．１記録されるイベントの種類」で規定したログ。
・VALUX サービスの申込に関する書類。

5.5.1.2 記録の保存期間

本登録局は「5．5．1．1保管する記録の種類」で規定した記録を次の期間保存する。

・「5．4．1．1記録されるイベントの種類」で規定したログ　1年間
・VALUX サービスの申込に関する書類　7年間

5.5.1.3 記録の保護

本登録局は記録に対して、漏洩、改ざん、亡失等を防止する処置を行い、保護を行う。

5.5.1.4 記録のバックアップ手順

本登録局は、バックアップが必要な記録が存在する場合は、記録データのバックアップを行う。

5.5.1.5 記録のタイムスタンプに関する要件

本登録局は、日付の記載が必要な記録が存在する場合は、日付の記載を行う。

5.5.1.6 記録の収集システム(内部または外部)

本登録局は、通常の運用業務において記録の保管を行う。

5.5.1.7 記録の取得および検証の手順

規定しない。

5.5.2 発行局に関する記述

5.5.2.1 保管する記録の種類

本発行局は、次の記録を保管する。
・「5．4．2．1記録されるイベントの種類」で規定したログ。
・利用者証明書。

5.5.2.2 記録の保存期間

「５．４．２．３監査ログの保存期間」のとおり。

5.5.2.3 記録の保護

「５．４．２．４監査ログの保護」のとおり。

5.5.2.4 記録のバックアップ手順

「５．４．２．５監査ログのバックアップの手順」のとおり。

5.5.2.5 記録のタイムスタンプに関する要件

発行局で管理される記録は、日時の情報を含む。これらは暗号化されていない。

5.5.2.6 記録の収集システム(内部または外部)

「５．４．２．６監査ログ収集システム（内部および外部)」のとおり。

5.5.2.7 記録の取得および検証の手順

「５．４．２．４監査ログの保護」のとおり。

5.6 発行局の鍵の切り替え

証明書の更新時における鍵対の扱いについては2通り方式が想定される。

方式1:証明書の更新に合わせ鍵対を置き換える鍵更新方式(Rekey)

方式2:同じ鍵対に対し有効期間を延長した証明書を発行する延長方式(Renewal)

本発行局証明書は方式2により証明書の延長(Renewal)を行う。

延長(Renewal)が行われた場合、延長(Renewal)証明書の DN、および、有効期間の開始日時(Validity:not before)は延長(Renewal)前の証明書と同じ値である。自己署名証明書、下位発行局証明書の延長(Renewal)は認証設備運用者により、複数人の信頼できる人間のもと、制御された手順によって行われる。

発行局証明書の更新はRenewal方式を採用しているため､発行局鍵更新については規定しない。

5．7 鍵の危殆化と災害における復旧

5．7．1 インシデントおよび危殆化の場合の取り扱い手順

本認証局でインシデントおよび危殆化が発生した場合、関係者は速やかに本認証局に通知を行うものとする。

5．7．2 登録局に関する記述

5．7．2．1 コンピュータのリソース、ソフトウェア、またはデータの破壊

本登録局のハードウェア、ソフトウェア、またはデータが破壊された場合は、本登録局は速やかに復旧作業を行う。

5．7．2．2 証明書発行対象者の秘密鍵の危殆化の場合の手順

VALUX クライアント証明書の秘密鍵が危殆化した場合、即座に当該 VALUX クライアント証明書を失効するものとする。

5．7．2．3 災害後の業務の継続の能力

本登録局は、災害の発生により主に使用している登録局施設が損傷を受けた場合、バックアップを使用して運用を再開する。

5．7．3 発行局に関する記述

5．7．3．1 コンピュータのリソース、ソフトウェア、またはデータの破壊

発行局施設におけるハードウェアは二重化されており、ハードウェアの破壊が発生した場合、待機系のハードウェアにより業務を継続する。

発行局施設におけるソフトウェアまたはデータの破壊が発生した場合、発行局施設運用者はバックアップされたソフトウェアまたはデータにより復旧を行う。

5．7．3．2 災害後の業務の継続の能力

発行局施設は日本国内において十分に遠隔な地域に災害対策用の設備を設けている。災害発生時には鍵の危殆化の恐れがない場合、本災害対策用設備により運用を継続する。

5.8 発行局または登録局の終了

本認証局の運用を終了する場合、VALUX サービスの利用者には商業上合理的な期間をあけて事前に通知を行う。

6. 技術的セキュリティに関する管理

6.1 鍵ペアの生成とインストール

6.1.1 鍵ペアの生成

本発行局鍵ペアの生成は、発行局施設内で、権限を持つ複数名の要員がそろい、一人の操作だけではできない方法により暗号モジュール内で生成する。

また、VALUX クライアント証明書の鍵ペアは、VALUX サービスの利用者のアプリケーションソフトおよび関連プログラムによって生成する。

6.1.2 証明書発行対象者への秘密鍵の受け渡し

VALUX クライアント証明書の鍵ペアは、VALUX サービスの利用者自身によって生成される。このため、VALUX サービスの利用者に対して VALUX クライアント証明書の秘密鍵を引き渡す運用は行われない。

6.1.3 証明書発行者への公開鍵の受け渡し

VALUXクライアント証明書の発行要求には当該VALUXサービスの利用者の公開鍵が含まれている。VALUX サービスの利用者は、当該 VALUX クライアント証明書の発行要求を作成し、登録局経由で発行局に提出することで、発行局に対して当該 VALUX サービスの利用者の公開鍵を引き渡す。

6.1.4 発行局の公開鍵の関係者への受け渡し

認証局は必要と認めた者に対してのみ、本認証局の CA 公開鍵を配布する。

6.1.5 鍵のサイズ

本認証局で使用する鍵のサイズは、以下のとおりとする。

・本認証局のルート CA 証明書：2048 ビットの RSA 暗号鍵
・VALUX クライアント証明書：2048 ビットの RSA 暗号鍵(2012 年 9 月 30 日までに発行されるクライアント証明書は 1024 ビット)

6．1．6 公開鍵のパラメータ生成と品質チェック

規定しない。

6．1．7 鍵の用途

本認証局の公開鍵の使用目的は、以下のとおりとする。

・本認証局のルート CA 証明書：証明書への電子署名、失効情報への電子署名
・VALUX クライアント証明書：電子署名、クライアントの認証

6．1．8 鍵を生成するハードウェア／ソフトウェア

認証局秘密鍵を生成するハードウェア／ソフトウェアについては「６．２．１暗号モジュールの標準と管理」のとおり。

6．1．9 認証局秘密鍵使用目的

認証局秘密鍵は、以下の目的以外に使用されることはない。

(1) VALUX クライアント証明書に対する署名
(2) 発行局証明書に対する自己署名、および、下位発行局が存在する場合には下位発行局証明書に対する署名
(3) CRL に対する署名

6．2 秘密鍵の保護と暗号モジュールの工学的管理

本認証局は、認証局秘密鍵を適切に保護するための技術面、設備面、運用面での対策を実施し、認証局秘密鍵を保護する。

6．2．1 暗号モジュールの標準と管理

認証局秘密鍵は、発行局施設内において暗号モジュール内で保護されている。暗号モジュールに、FIPS 140-1 レベル 3 の要件を満たしたハードウェアセキュリティモジュール(HSM)を利用している。

6.2.2 複数人による秘密鍵の管理

本発行局は、機密を要する発行局施設の暗号運用について複数の信頼できる個人が関与することを要求する技術的・手続的な仕組みを実施している。本発行局は、認証局秘密鍵を利用するために「シークレット・シェアリング」という手法を用いる。この手法では、必要な起動データを、「シークレット・シェア」と呼ばれる別々のパーツに分割し、「シェアホルダー」と呼ばれる訓練を受けた信頼できる個人が保有する。特定のハードウェア暗号モジュールに保管されている認証局秘密鍵を起動させるためには、当該モジュールに関して生成・分配されたシークレット・シェア総数のうち、一定数のシークレット・シェアが必要となる。

6.2.3 秘密鍵の預託

VALUX クライアント証明書の秘密鍵の預託は行わない。
認証局秘密鍵の預託については規定しない。

6.2.4 秘密鍵のバックアップ

認証局秘密鍵のバックアップは、鍵が格納されている暗号モジュールと同型の暗号モジュール間のクローニング（複製）機能によりバックアップを行う。バックアップは、複数人の管理の下、発行局施設内において行われる。バックアップ用の暗号モジュールは発行局施設内の安全な場所に保管される。

また、VALUX クライアント証明書の秘密鍵については、VALUX サービスの利用者がバックアップを取得することを許可しない。

6.2.5 秘密鍵の記録

認証局秘密鍵のアーカイブは行わない。

6.2.6 暗号化モジュールへの秘密鍵の格納

認証局秘密鍵は暗号モジュール内で生成されるため、規定しない。

6.2.7 秘密鍵を活性化する方法

「６．２．２複数人による秘密鍵の管理」のとおり。

6.2.8 秘密鍵を不活性化する方法

認証局秘密鍵はシステムの停止、もしくは、暗号モジュールをトークンリーダから抜き取ることにより不活性化する。

6.2.9 秘密鍵を消去する方法

本認証局は、必要に応じて複数人の操作により認証局秘密鍵を完全に消去し、破棄を行う。

6.2.10 暗号モジュールの評価

本 CPS の「６．２．１暗号モジュールの標準と管理」にて規定する。

6.3 鍵ペア管理の他の観点

6.3.1 公開鍵の保管

本認証局は、CA 証明書および VALUX クライアント証明書のバックアップを取得する。
ルート CA 証明書は発行局のサービス期間中アーカイブされる。

6.3.2 証明書の有効期間および鍵ペアの使用期間

本認証局で使用する鍵ペアの有効期間、すなわち証明書の有効期間は、以下のとおりとする。
・本認証局のルート CA 証明書：5 年
・VALUX クライアント証明書:最大 約 1 年(387 日)

6.4 活性化データ

6.4.1 活性化データの生成とインストール

認証局秘密鍵は、「６．２．２複数人による秘密鍵の管理」および「６．２．９秘密鍵を消去する方法」に規定したシェア情報によって活性化される。シェア情報は「６．１．１鍵ペアの生成」で規定された秘密鍵の生成時に権限者へ渡される。

6.4.2 活性化データの保護

認証局秘密鍵を活性化するためデータは、適切な方法によって保護される。

認証局秘密鍵の活性化情報は複数人に分割されて管理されている。また、各活性化情報は権限者の責任で拳銃に管理される。

6.4.3 活性化データの他の観点

規定しない。

6.5 コンピュータセキュリティの管理

6.5.1 登録局に関する記述

6.5.1.1 規定されたコンピュータセキュリティの技術的要件

本登録局は、アクセス制御機構、操作者の識別の本人認証等、適切なセキュリティ要件を満たしたコンピュータシステムを使用する。

6.5.1.2 コンピュータセキュリティの評価

本登録局については規定しない。

6.5.2 発行局に関する記述

6.5.2.1 規定されたコンピュータセキュリティの技術的要件

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

6.5.2.2 コンピュータセキュリティの評価

本発行局施設のうち、専ら証明書の作成に係る装置は「ISO/IEC 15408-3:1999, Information technology - Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements」の EAL４レベル相当のシステムを利用している。

6．6 ライフサイクルの技術的管理

6．6．1 登録局に関する記述

6．6．1．1 システム開発における管理

本登録局設備で使用するアプリケーションは、開発時において、品質管理および変更管理基準を定めた実施要領に従い、開発され実装される。

6．6．1．2 セキュリティの管理

本登録局施設では、システムの状況を管理し、監視するための仕組みおよび方策を有している。登録局施設におけるすべてのソフトウェア・パッケージおよびソフトウェアのアップデートについて、ハッシュを生成する。当該ハッシュは、当該ソフトウェアの完全性を手動で証明するために用いられるものであり、インストレーション時に、システムの完全性を確認する。

6．6．1．3 ライフサイクルのセキュリティ管理

規定しない。

6．6．2 発行局に関する記述

6．6．2．1 システム開発における管理

本発行局施設において、アプリケーションは、システム開発および変更管理基準に従い、開発され実装される。

6．6．2．2 セキュリティの管理

本発行局施設では、システムの状況を管理し、監視するための仕組みおよび方策を有している。発行局施設におけるすべてのソフトウェア・パッケージおよびソフトウェアのアップデートについて、ハッシュを生成する。当該ハッシュは、当該ソフトウェアの完全性を手動で証明するために用いられるものである。インストレーション時およびその後定期的に、システムの完全性を確認する。

6．6．2．3 ライフサイクルのセキュリティ管理

規定しない。

6．7 ネットワークセキュリティ管理

6．7．1 登録局に関する記述

本登録局施設では、権限のない者によるアクセスおよび他の不正な活動を防止するため、ファイアウォールとアクセス制御リスト等により、セキュリティの確保されたネットワークを用いて、そのすべての業務を実施している。

6．7．2 発行局に関する記述

本発行局施設では、権限のない者によるアクセスおよび他の不正な活動を防止するため、セキュリティおよび監査要件ガイドに従い、セキュリティの確保されたネットワークを用いて、そのすべての業務を実施している。秘密情報の通信は、暗号化およびデジタル署名を用いて行う。

6．8 タイムスタンプ

本認証局ではタイムスタンプを使用しない。このため本項目を規定しない。

6．9 暗号モジュールの技術統制

本発行局で使用するモジュールは、「６．２．１暗号モジュールの標準と管理」に定める要件に合致している。

7. 証明書、CRL、および OCSP のプロファイル

7.1 証明書のプロファイル

本認証局が発行する、CA 証明書および VALUX クライアント証明書のプロファイルは以下のとおりである。

・CA 証明書（CA 証明書の設定値を一覧表の形式で表示する）

領域名	クリティカルフラグ	値(例)	説明
version (バージョン番号)	—	3	証明書のバージョンが X.509 のバージョン 3 であることを示す。INTEGER 型。
serial Number (シリアル番号)	—	24 (例)	証明書のシリアル番号を示す。INTEGER 型。
signature algorithm ID (署名アルゴリズム)	—		認証局が発行する証明書に署名する際に使用した署名アルゴリズム。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5 または 1.2.840.113549.1.1.11	sha1WithRSAEncryption または sha256WithRSAEncryption を表す OID の値を示す。
Issuer Name (発行者名)	—	O=NTT DATA CORPORATION CN=Payment Solutions Sector CA-2048 または Payment Solutions Sector CA-SHA2	VALUX サービス認証局の識別名 (DN) を示す。英語表記、PrintableString 型を使用。
validity period (証明書有効期間)	—		証明書の有効期間を示す。
notBefore (発行日)		051219000000Z(例)	証明書の有効期間開始日を示す。UTCTime 型。
notAfter (終了日)		1012182359595Z(例)	証明書の有効期間終了日を示す。UTCTime 型。
subject Name (主体者名)	—	O=NTT DATA CORPORATION CN=Payment Solutions Sector CA-2048 または Payment Solutions Sector CA-SHA2	VALUX サービス認証局の識別名 (DN) を示す。英語表記、PrintableString 型を使用。
subject public Key info (主体者公開鍵情報)	—		証明書の公開鍵アルゴリズムを示す。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、rsaEncryption を表す OID の値を示す。
parameter (パラメータ)		NULL	RSA の場合、本項目には値が設定されない。
public Key (公開鍵)		※公開鍵の値	証明書の公開鍵の値を示す。BIT STRING 型。
Extensions (証明書拡張領域)			
Netscape Cert Type (Netscape Cert Type)	FALSE	“00000110” (2 進数表記)	証明書の利用制限を設定する。(Netscape 社独自拡張)
SSLClient		0	SSL クライアント。

領域名	クリティカルフラグ	値(例)	説明
SSLServer		0	SSL サーバ。
S/MIME		0	S/MIME クライアント。
Object Signing		0	オブジェクトサイン。
Reserved		0	予約済。
SSL CA		1	SSL 認証局。
S/MIME CA		1	S/MIME 認証局。
Object Signing CA		0	オブジェクトサイン認証局。
basicConstraints (基本制約)	FALSE		
CA		TRUE	CA 証明書であることを表す。Internet Explorer では「subject Type=CA」と表示される。
pathLenConstraint		0	
keyUsage (鍵用途)	TRUE	“00000110” (2 進数表記)	鍵の使用目的を設定する。
digitalSignature		0	署名検証ができる。
nonRepudiation		0	否認防止用の署名検証ができる。
keyEncipherment		0	共通鍵等の鍵を暗号化できる。
dataEncipherment		0	データを直接暗号化できる。
keyAgreement		0	鍵は鍵交換ができる。
keyCertSign		1	証明書署名の検証ができる。
cRLSign		1	CRL 署名の検証ができる。
encipherOnly		0	交換した鍵でデータを暗号化できる。(keyAgreement がセットされている場合のみ指定可)
decipherOnly		0	交換した鍵でデータを複合化できる。(keyAgreement がセットされている場合のみ指定可)
SubjectAltName (サブジェクト代替名称)	FALSE		サブジェクトの代替名称が設定される。
CN		TestPriv2-48(例)	
Issuer’s signature (発行者署名)			
			証明書に付与した署名の値を示す。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5 または 1.2.840.113549.1.1.11	sha1WithRSAEncryption または sha256WithRSAEncryption を表す OID の値を示す。
ENCRYPTED (署名値)		※署名値	証明書に付与した署名の値を示す。

・VALUX クライアント証明書 (VALUX クライアント証明書の設定値を一覧表の形式で表示する)

領域名	クリティカルフラグ	値(例)	説明
version (バージョン番号)	—	3	証明書のバージョンが X.509 のバージョン 3 であることを示す。INTEGER 型。

領域名	クリティカルフラグ	値(例)	説明
serial Number (シリアル番号)	—	A52C (例)	証明書のシリアル番号を示す。INTEGER 型。
signature algorithm ID (署名アルゴリズム)	—		認証局が発行する証明書に署名する際に使用した署名アルゴリズム。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5 または 1.2.840.113549.1.1.11	sha1WithRSAEncryption または sha256WithRSAEncryption を表す OID の値を示す。
Issuer Name (発行者名)	—	O=NTT DATA CORPORATION CN=Payment Solutions Sector CA-2048 または Payment Solutions Sector CA-SHA2	VALUX サービス認証局の識別名 (DN) を示す。英語表記、PrintableString 型を使用。
validity period (証明書有効期間)	—		証明書の有効期間を示す。
notBefore (発行日)		060123090000Z(例)	証明書の有効期間開始日を示す。UTCTime 型。
notAfter (終了日)		070123085959Z(例)	証明書の有効期間終了日を示す。UTCTime 型。
subject Name (主体者名)	—	T = manager(例) CN = 000000000001 00000001 2006091412345677701 OU = Payment Solutions Sector CA-2048 または Payment Solutions Sector CA-SHA2 TEST O = NTT DATA CORPORATION C = JP	※VALUX サービスの利用者の識別名 (DN) を示す。英語表記、PrintableString 型を使用。
subject public Key info (主体者公開鍵情報)	—		証明書の公開鍵アルゴリズムを示す。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、rsaEncryption を表す OID の値を示す。
parameter (パラメータ)		NULL	RSA の場合、本項目には値が設定されない。
public Key (公開鍵)		※公開鍵の値	証明書の公開鍵の値を示す。BIT STRING 型。
Extensions (証明書拡張領域)			
Basic Constraints (基本的制約)	FALSE		証明書サブジェクトが CA かどうか、およびその CA 中の証明書パスがどのくらい深いかを示す。
cA		TRUE	証明書サブジェクトが CA かどうかを示す
pathLenConstraint		0	CA 中の証明書パスがどのくらい深いかを示す。
CRLDistributionPoints (CRL 配布ポイント)	FALSE		CRL 情報がどのように得られるかを示す。
dist-point		(例) fullName http://pilotonsitecrl.verisign.co.jp/NTTDATACORPORATIONPaymentSolutionsSectorCA2048TEST/LatestCRL.crl	CRL 情報がどのように得られるかを示す。

領域名	クリティカルフラグ	値(例)	説明
keyUsage (鍵用途)	FALSE	“10100000” (2 進数表記)	鍵の使用目的を設定する。
digitalSignature		1	署名検証ができる。
nonRepudiation		0	否認防止用の署名検証ができる。
keyEncipherment		1	共通鍵等の鍵を暗号化できる。
dataEncipherment		0	データを直接暗号化できる。
keyAgreement		0	鍵は鍵交換ができる。
keyCertSign		0	証明書署名の検証ができる。
cRLSign		0	CRL 署名の検証ができる。
encipherOnly		0	交換した鍵でデータを暗号化できる。（keyAgreement がセットされている場合のみ指定可)
decipherOnly		0	交換した鍵でデータを複合化できる。（keyAgreement がセットされている場合のみ指定可)
Netscape Cert Type (Netscape Cert Type)	FALSE	“10000000” (2 進数表記)	証明書の利用制限を設定する。(Netscape 社独自拡張)
SSLClient		1	SSL クライアント。
SSLServer		0	SSL サーバ。
S/MIME		0	S/MIME クライアント。
Object Signing		0	オブジェクトサイン。
Reserved		0	予約済。
SSL CA		1	SSL 認証局。
S/MIME CA		1	S/MIME 認証局。
Object Signing CA		0	オブジェクトサイン認証局。
2.16.840.1.113733.1.6.9	FALSE		
		01 01 ff(16 進数表記)	
Issuer’s signature (発行者署名)			
			証明書に付与した署名の値を示す。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5 または 1.2.840.113549.1.1.11	sha1WithRSAEncryption または sha256WithRSAEncryption を表す OID の値を示す。
ENCRYPTED (署名値)		※署名値	証明書に付与した署名の値を示す。

ただし、2012 年 9 月 30 日までに発行される証明書については以下のプロファイルとなる。

・CA 証明書（CA 証明書の設定値を一覧表の形式で表示する）

領域名	クリティカルフラグ	値(例)	説明
version (バージョン番号)	—	2	証明書のバージョンが X.509 のバージョン 3 であることを示す。INTEGER 型。
serial Number (シリアル番号)	—	24 (例)	証明書のシリアル番号を示す。INTEGER 型。
signature algorithm ID (署名アルゴリズム)	—		認証局が発行する証明書に署名する際に使用した署名アルゴリズム。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha1withRSAEncryption を表す OID の値を示す。
issuer name (発行者名)	—	ou = Root CA ou = Payment Solutions Sector CA o = NTT DATA CORPORATION c = JP	VALUX サービス認証局の識別名 (DN) を示す。英語表記、PrintableString 型を使用。
validity period (証明書有効期間)	—		証明書の有効期間を示す。
notBefore (発行日)		051219000000Z(例)	証明書の有効期間開始日を示す。UTCTime 型。
notAfter (終了日)		101218235959Z(例)	証明書の有効期間終了日を示す。UTCTime 型。
subject name (主体者名)	—	ou = Root CA ou = Payment Solutions Sector CA o = NTT DATA CORPORATION c = JP	VALUX サービス認証局の識別名 (DN) を示す。英語表記、PrintableString 型を使用。
subject public key info (主体者公開鍵情報)	—		証明書の公開鍵アルゴリズムを示す。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、rsaEncryption を表す OID の値を示す。
parameter (パラメータ)		NULL	RSA の場合、本項目には値が設定されない。
public key (公開鍵)		※公開鍵の値	証明書の公開鍵の値を示す。BIT STRING 型。
Extensions (証明書拡張領域)			
authorityKeyIdentifier (機関鍵識別子)	FALSE		ルート CA 証明書の署名の検証に使用する証明書を識別するための情報を表す。
keyIdentifier		※ルート CA 証明書の公開鍵の SHA-1 によるハッシュ値	ルート CA 証明書の公開鍵の SHA-1 によるハッシュ値を示す。
authorityCertIssuer		ou = Root CA ou = Payment Solutions Sector CA o = NTT DATA CORPORATION c = JP	VALUX サービス認証局の識別名 (DN) を示す。英語表記、PrintableString 型を使用。
authorityCertSerialNumber		24 (例)	ルート CA 証明書の証明書のシリアル番号を示す。INTEGER 型。

領域名	クリティカルフラグ	値(例)	説明
subjectKeyIdentifier (所有者鍵識別子)	FALSE		ルート CA 証明書の公開鍵を識別するための情報を表す。
keyIdentifier		※ルート CA 証明書の公開鍵の SHA-1 によるハッシュ値	ルート CA 証明書の公開鍵の SHA-1 によるハッシュ値を示す。
basicConstraints (基本制約)	FALSE		
cA		True	CA 証明書であることを表す。Internet Explorer では「Subject Type=CA」と表示される。
pathLenConstraint		0	
keyUsage (鍵用途)	TRUE	“00000110” (2 進数表記)	鍵の使用目的を設定する。
digitalSignature		0	署名検証ができる。
nonRepudiation		0	否認防止用の署名検証ができる。
keyEncipherment		0	共通鍵等の鍵を暗号化できる。
dataEncipherment		0	データを直接暗号化できる。
keyAgreement		0	鍵は鍵交換ができる。
keyCertSign		1	証明書署名の検証ができる。
cRLSign		1	CRL 署名の検証ができる。
encipherOnly		0	交換した鍵でデータを暗号化できる。(keyAgreement がセットされている場合のみ指定可)
decipherOnly		0	交換した鍵でデータを複合化できる。(keyAgreement がセットされている場合のみ指定可)
issuer’ s signature (発行者署名)			
			証明書に付与した署名の値を示す。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha1WithRSAEncryption を表す OID の値を示す。
ENCRYPTED (署名値)		※署名値	証明書に付与した署名の値を示す。

・VALUX クライアント証明書 (VALUX クライアント証明書の設定値を一覧表の形式で表示する)

領域名	クリティカルフラグ	値(例)	説明
version (バージョン番号)	—	2	証明書のバージョンが X.509 のバージョン 3 であることを示す。INTEGER 型。
serial Number (シリアル番号)	—	A52C (例)	証明書のシリアル番号を示す。INTEGER 型。
signature algorithm ID (署名アルゴリズム)	—		認証局が発行する証明書に署名する際に使用した署名アルゴリズム。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	SHA1withRSAEncryption を表す OID の値を示す。
issuer name (発行者名)	—	ou = Root CA ou = Payment Solutions Sector CA o = NTT DATA CORPORATION c = JP	VALUX サービス認証局の識別名 (DN) を示す。英語表記、PrintableString 型を使用。

領域名	クリティカルフラグ	値(例)	説明
validity period (証明書有効期間)			証明書の有効期間を示す。
notBefore (発行日)	—	060123090000Z(例)	証明書の有効期間開始日を示す。UTCTime 型。
notAfter (終了日)		070123085959Z(例)	証明書の有効期間終了日を示す。UTCTime 型。
subject name (主体者名)	—	t = manager cn = 000000000001 00000001 2006091412345677701 ou = Payment Solutions Sector CA o = NTT DATA CORPORATION c = JP	※VALUX サービスの利用者の識別名(DN)を示す。英語表記、PrintableString 型を使用。
subject public key info (主体者公開鍵情報)			証明書の公開鍵アルゴリズムを示す。
algorithm identifier (アルゴリズム識別子)	—	1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、rsaEncryption を表す OID の値を示す。
parameter (パラメータ)		NULL	RSA の場合、本項目には値が設定されない。
public key (公開鍵)		※公開鍵の値	証明書の公開鍵の値を示す。BIT STRING 型。
Extensions (証明書拡張領域)			
authorityKeyIdentifier (機関鍵識別子)	FALSE		ユーザ認証用証明書の署名の検証に使用する、ルート CA 証明書を識別するための情報を表す。
keyIdentifier		※ルート CA 証明書の公開鍵の SHA-1 によるハッシュ値	ルート CA 証明書の公開鍵の SHA-1 によるハッシュ値を示す。
authorityCertIssuer		ou = Root CA ou = Payment Solutions Sector CA o = NTT DATA CORPORATION c = JP	VALUX サービス認証局の識別名(DN)を示す。英語表記、PrintableString 型を使用。
authorityCertSerialNumber		24 (例)	ルート CA 証明書の証明書のシリアル番号を示す。INTEGER 型。
subjectKeyIdentifier (所有者鍵識別子)	FALSE		ユーザ認証用証明書の公開鍵を識別するための情報を表す。
keyIdentifier		※ユーザ認証用証明書の公開鍵の SHA-1 によるハッシュ値	ユーザ認証用証明書の公開鍵の SHA-1 によるハッシュ値を示す。
keyUsage (鍵用途)	TRUE	“10000000”(2 進数表記)	鍵の使用目的を設定する。
digitalSignature		1	署名検証ができる。
nonRepudiation		0	否認防止用の署名検証ができる。
keyEncipherment		0	共通鍵等の鍵を暗号化できる。
dataEncipherment		0	データを直接暗号化できる。
keyAgreement		0	鍵は鍵交換ができる。
keyCertSign		0	証明書署名の検証ができる。
cRLSign		0	CRL 署名の検証ができる。
encipherOnly		0	交換した鍵でデータを暗号化できる。(keyAgreement がセットされている場合のみ指定可)

領域名	クリティカルフラグ	値(例)	説明
decipherOnly		0	交換した鍵でデータを複合化できる。（keyAgreement がセットされている場合のみ指定可）
extendedKeyUsage (拡張鍵用途)	FALSE		鍵の使用目的を設定する。
clientAuth		1.3.6.1.5.5.7.3.2	クライアント認証を表すOIDの値を示す。
issuer' s signature (発行者署名)			
			証明書に付与した署名の値を示す。
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha1WithRSAEncryption を表す OID の値を示す。
ENCRYPTED (署名値)		※署名値	証明書に付与した署名の値を示す。

7．2 CRL のプロファイル

本認証局では、失効情報を公開しない。従ってCRLのプロファイルを記載しない。

7．3 OCSP のプロファイル

本認証局では、失効情報を公開しない。従ってOCSPのプロファイルを記載しない。

8. 準拠性監査と他の評価

8.1 登録局に関する記述

8.1.1 監査を行う周期または場合

本登録局は、システム全体の維持管理業務および発行局の運用業務を対象に、定期的に監査を実施する。また、必要に応じて不定期に監査を実施することがある。

8.1.2 監査人の身元および資格

監査人は、外部の監査法人の担当者により実施される。

8.1.3 監査人と被監査組織との関係

監査人は、本認証局の運用作業に関係しない者を任命する。

8.1.4 監査を受ける事項

監査では、本登録局が本 CPS および本 CPS に基づいた運用マニュアルを遵守した運用を行い、認証局として適切な運用を行っているかどうかを監査する。

8.1.5 不備に対する対応

本登録局は、監査で指摘された指摘事項を受けて、運用面およびシステム面での対策を実施する。

8.1.6 監査結果の公開

本登録局は、外部に対して監査結果を公開しない。ただし、公的機関などから法律に基づく開示要求があった場合は、その指示に従いこれを開示する。

8.2 発行局に関する記述

8.2.1 監査を行う周期または場合

外部委託される発行局施設は準拠性監査を随時実施する。

8.2.2 監査人の身元および資格

本発行局施設の監査人はPKIに関する十分な知識を持った者が任命される。

8.2.3 監査人と被監査組織との関係

本発行局施設の監査人は運用部門とは独立した部門の者が任命される。

8.2.4 監査を受ける事項

規定しない。

8.2.5 不備に対する対応

監査結果での指摘事項を踏まえ、新技術の動向を考慮して業務、および、設備の改善を行い、必要である場合はCPSを改訂し、その結果の評価を行う。

8.2.6 監査結果の公開

本発行局施設の監査結果は公開されない。ただし、公的機関から法律に基づく開示要求があった場合や、公表が妥当であると発行局運用者が判断した場合、監査結果を開示する。

9. その他の業務事項および法的事項

9.1 料金

9.1.1 証明書の発行または更新の料金

本認証局の利用に関する料金は、VALUX サービス利用規約によるものとする。

9.1.2 証明書へのアクセスの料金

規定しない。

9.1.3 失効または状態の情報へのアクセス料金

規定しない。

9.1.4 その他のサービスの料金

その他のサービスに関する料金は、VALUX サービス利用規約によるものとする。

9.1.5 返金方針

本認証局の利用に関する料金の返金は、VALUX サービス利用規約によるものとする。

9.2 財政的責任

9.2.1 保険の範囲

規定しない。

9.2.2 その他の資産

規定しない。

9.2.3 証明書発行対象者に対する保険または保証の範囲

規定しない。

9.3 業務情報の機密保持

9.3.1 登録局に関する記述

9.3.1.1 機密情報の範囲

本登録局は、本 CPS の「９．３．１．２機密情報に含まれない情報」で規定した情報を除いたすべての情報を機密情報として取り扱う。

機密情報は、本 CPS において規定された開示手続を行わない場合は、原則として一切開示しない。

9.3.1.2 機密情報に含まれない情報

本登録局は、以下の情報を機密情報として取り扱わない。

・VALUX クライアント証明書に記載する情報
・その他、本認証局の運用を行う上で外部に対する公開が必要な情報

9.3.1.3 機密情報の保護の責任

本登録局は、機密情報を外部に漏洩させないための責任を持つ。

ただし、以下の場合に本登録局は機密情報を開示することがある。
・捜査機関、裁判所等、法律上権限を有している者からの情報開示要求があった場合
・訴訟等の法的手続で必要な場合

9.3.2 発行局に関する記述

9.3.2.1 機密情報の範囲

本発行局施設が保有する以下の情報は機密情報とする。

(1) 証明書申請記録。

(2) 処理記録（すべての記録および監査証跡記録の双方を含む)。

(3) 偶発事故に対する災害復旧計画。

(4) 発行局施設のハードウェアおよびソフトウェアの運用ならびに証明書サービスおよび申請サービスの管理を制御するセキュリティの手段。

(5) 監査人によって作成された監査記録。

9.3.2.2 機密情報に含まれない情報

本発行局は以下の情報を機密扱いとしない。

(1) 証明書、証明書失効および他のステータス情報。

9.3.2.3 機密情報の保護の責任

本発行局施設で取り扱う秘密情報に対して、裁判手続、行政手続またはその他の法的手続に対応するために法執行機関から開示の要求があった場合、法執行機関に対し秘密情報を開示することができるものとする。また、本発行局施設で取り扱う個人情報については、個人情報保護に関する法令に従う。

9.4 個人情報保護

VALUX サービス認証局は、財団法人　金融情報システムセンタが制定した「金融機関等コンピュータシステムの安全対策基準・解説書　第6版追補」に準拠した、個人情報保護の対策を実施している。

9.4.1 プライバシープラン

本認証局は、別途定めるプライバシーポリシに準じて、個人情報を適切に扱うものとする。

9.4.2 個人情報として扱われる情報

本認証局は、別途定めるプライバシーポリシで規定する個人情報を、個人情報として扱う。

9.4.3 個人情報とはみなされない情報

本認証局は、本 CPS の「９．４．２個人情報として扱われる情報」以外の情報を、個人情報として扱わない。

9.4.4 個人情報保護の責任

本認証局は、別途定めるプライバシーポリシに準じて、個人情報の漏洩等を発生させないための責任を持つ。

9.4.5 個人情報の利用のための通知と同意

本認証局は、VALUX サービスの利用申請等の際に、VALUX サービスの利用者に対して個人情報の利用のための通知を行い、かつ VALUX サービスの利用者から同意を得る。

9.4.6 司法または行政上の手続による開示

本認証局は、以下の場合に個人情報を開示することがある。

・捜査機関、裁判所等、法律上権限を有している者からの情報開示要求があった場合
・訴訟等の法的手続で必要な場合

9.4.7 その他の情報を開示する場合

本認証局は、VALUX サービスの利用者からの利用者自身の個人情報の開示請求または本 CPS の「９．４．６司法または行政上の手続による開示」で規定する理由以外の理由で、個人情報の開示を行わない。

9.5 知的財産権

NTT データは、以下の文書に関する知的財産権を保有する。
・本 CPS

9．6 表明および保証

9．6．1 発行局の表明および保証

NTT データは、本 CPS を遵守した発行局のシステムの維持管理および運用を外部委託し、VALUX クライアント証明書の発行を適切に行う。

9．6．2 登録局の表明および保証

NTT データは、本 CPS を遵守した登録局のシステムの維持管理を適切に行う。

また、NTT データは、本 CPS を遵守した登録局の運用を実施し、VALUX クライアント証明書の発行申請および失効申請の審査、ならびに審査結果に基づいた、発行許可の発行局への送信および失効の発行局への送信を適切に行う。

9．6．3 証明書発行申請者の表明および保証

VALUX サービスの利用者は、本 CPS を遵守した VALUX クライアント証明書の発行申請、使用、失効申請、ならびに秘密鍵の管理を実施する。

9．6．4 証明書の検証者の表明および保証

VALUX クライアント証明書の検証者である NTT データは、本 CPS を遵守した VALUX クライアント証明書の検証を実施する。

9．6．5 その他関係者の表明および保証

規定しない。

9．7 保証の免責事項

NTT データによる保証の免責事項については、VALUX サービス利用規約によるものとする。

9．8 責任の制限

VALUX サービスの利用者に対する責任の制限は VALUX サービス利用規約によるものとする。

9．9 損害賠償の免責事項

VALUX サービスの利用者に対する損害賠償の免責事項は、VALUX サービス利用規約によるものとする。

9．10 期間と終了

9．10．1 期間

本 CPS は、VALUX サービスの利用者が VALUX サービスのサービス利用の契約を締結した場合、有効となる。

9．10．2 終了

本 CPS は、VALUX サービスの利用者が VALUX サービスのサービス利用の契約を終了した場合、有効性は終了する。

9．10．3 終了の効力および存続条項

規定しない。

9．11 個別の通知および関係者との連絡

本 CPS に関する問合せを行う場合は、本 CPS の「１．５．２問合せ先」に記載した問合せ先に対して行うものとする。

9．12 修正

9．12．1 修正の手続

NTT データは、「VALUX サービス CPS 管理要領」に規定した手続に従って本 CPS を変更する。

9.12.2 通知の手段および期間

NTT データは、本 CPS を変更した場合、速やかに変更後の CPS を公表する。これをもって、証明書利用者への通知とする。

9.12.3 OID を変更しなければならない場合

規定しない。

9.13 紛争解決条項

本認証局に関して紛争が発生した場合、紛争解決の手続は、VALUX サービス利用規約によるものとする。

9.14 準拠法

本 CPS の解釈および有効性等は、日本国の法令により判断される。

9.15 適用法の遵守

規定しない。

9.16 雑則

9.16.1 完全なる合意

規定しない。

9.16.2 権利の譲渡

規定しない。

9.16.3 分離可能性

規定しない。

9.16.4 強制執行(訴訟費用および権利の放棄)

強制執行については、VALUX サービス利用規約によるものとする。

9.16.5 不可抗力

不可抗力については、VALUX サービス利用規約によるものとする。

9.17 その他

規定しない。