

日本銀行外為法手続きオンラインシステム用認証局

Certification Practice Statement

——Symantec Trust Network Certification Practice Statement の付属書——

バージョン 3.2
2015 年 7 月 6 日

日本銀行

商標に関する表示

シマンテック (Symantec)、 ノートン (Norton)、およびチェックマークロゴ (the Checkmark Logo) は米国シマンテック・コーポレーション (Symantec Corporation) またはその関連会社の米国またはその他の国における登録商標、または、商標です。

1. はじめに

「日本銀行外為法手続きオンラインシステム用認証局（以下「オンラインシステム用認証局」という）CPS（Certification Practice Statement）」（以下「本 CPS」という）は、日本銀行が証明書の発行、更新、取消しおよび管理を含む一連のサービス（以下「証明書発行等サービス」という）を提供する際に準拠する Symantec Corporation（注 1）の CPS に対する付属書である。

オンラインシステム用認証局では、Symantec Corporation の CPS に規定されている内容のうち以下に関する事項が適用される。本 CPS では、以下の事項のうち日本銀行が個別に適用範囲を限定する内容を記載している。

（注 1） 「Symantec Corporation」は「米国シマンテック・コーポレーション」およびその完全子会社（株式会社シマンテックを含む）を意味する。株式会社シマンテックについては、以下「シマンテック」という。

- Class 1 の個人向け証明書を発行するマネージド PKI サービス（注 2）
- Symantec Trust Network（「STN」とも表記する）
- Symantec Trust Network Certificate Policies（「STN CP」、「CP」とも表記する）
- 認証機関（第一次認証機関、シマンテック認証機関、エンタープライズ・カスタマの認証機関、インフラストラクチャ認証機関、管理認証機関を含む）
- 利用規約（シマンテックが制定した「クライアント ID 利用規約」を指す）
- 依拠当事者規約
- エンタープライズ・カスタマ（「カスタマ」とも表記する）
- 依拠当事者
- 利用者（「エンド・エンティティ」、「エンドユーザ」とも表記する）
- 認証機関証明書
- 管理者証明書
- 利用者証明書
- リポジトリ
- CRL
- リキーによる利用者証明書の更新
- 暗号モジュール

（注 2） 但し、キーマネージメントサービス、利用者の秘密鍵のバックアップおよび預託、自動承認、自動承認モジュールおよび自動承認サーバ、OCSP（「オンライン証明書ステータス・プロトコールサービス」とも表記する）は適用対象外。

また、仮に、本 CPS と Symantec Corporation の CPS の記述に矛盾が存在した場合、

Symantec Corporation の CPS の記述が優先されるものとする。Symantec Corporation の CPS はシマンテックのホームページ (<https://www.symauth.com/cps>) で公開している。

なお、日本銀行が発行する証明書に関する利用者向けの利用規約は、以下の 2 種類の利用規約を同時に使用する。

- シマンテックが制定した、「クライアント ID 利用規約」(シマンテックのホームページ (<http://www.symantec.com/about/profile/policies/repository.jsp>) で公開している)
- 日本銀行が制定した「日本銀行外為法手続きオンラインシステム用認証局が発行する証明書に関する利用規約」(以下「オンラインシステム用認証局の利用規約」という。日本銀行のホームページ (<http://www.boj.or.jp/>) および日本銀行外為法手続きオンラインシステム (以下「オンラインシステム」という) の情報提供ページで公開している)

「クライアント ID 利用規約」は、シマンテックとオンラインシステムの利用者 (以下「システム利用者」という) の間で締結される利用規約となる。「オンラインシステム用認証局の利用規約」は、日本銀行とシステム利用者の間で締結される利用規約となる。

Symantec Corporation の CPS および Symantec Corporation の CPS に関連する文書において、「他の利用規約」と表記されている利用規約は、オンラインシステム用認証局の利用規約を指す。

1.1 概要

日本銀行は、シマンテックの PKI サービスであるマネージド PKI のエンタープライズ・カスタマであり、オンラインシステム用認証局として認証機関の機能を果たし、システム利用者に対して証明書発行等サービスを提供する。日本銀行は、オンラインシステムでの以下の用途に使用されるクラス 1 証明書を発行する。

- システム利用者がオンラインシステムにアクセスする際のユーザ認証 (以下「クライアント認証」という) に使用する証明書 (以下「クライアント証明書」という)
- オンラインシステムとシステム利用者の間で送受信するデータの暗号に使用する証明書 (以下「暗号用証明書」という)

日本銀行は、上記以外の用途に使用する証明書を発行しない。

オンラインシステムの管理者による暗号用証明書の運用およびオンラインシステムの維持管理用に日本銀行が使用する証明書に関しては、Symantec Corporation の CPS に準ずるため、本 CPS の本項以降の記述の対象外とする。

1.3.1 認証機関

日本銀行が提供する証明書発行等サービスにおける認証機関は、以下のとおりである。

- 第一次認証機関：米国シマンテック・コーポレーション
- 第一次認証機関によって CA 証明書を発行された認証機関：シマンテック
- シマンテックによって CA 証明書を発行された認証機関：日本銀行

なお、日本銀行はオンラインシステム用認証局の運用業務の一部を、シマンテックに委託している。

それぞれの認証機関と CA 証明書の対応関係は以下のとおり。

- 米国シマンテック・コーポレーション：ルート CA 証明書
- シマンテック：中間 CA 証明書（シマンテック）
- 日本銀行：中間 CA 証明書（日本銀行）

1.3.3 エンド・エンティティ

日本銀行は、クライアント証明書をオンラインシステムのシステム利用者によりのみ発行する。

1.3.4 依拠当事者

オンラインシステム用認証局での依拠当事者は、日本銀行である。

1.4.1.1 個人に発行される証明書

システム利用者は、クライアント認証のためにのみ、日本銀行が発行したクライアント証明書を使用する。

1.4.2 禁止される証明書の用途

システム利用者は、日本銀行が発行したクライアント証明書を、本 CPS の 1.4.1.1 で規定した用途以外に使用してはならない。

1.5.1 本文書の管理部署

本 CPS についての管理部署は、日本銀行のホームページ (<http://www.boj.or.jp/>) およびオンラインシステムの情報提供ページに掲載する。

1.5.2 連絡先

本 CPS についての照会先は、日本銀行のホームページ (<http://www.boj.or.jp/>) およびオンラインシステムの情報提供ページに掲載する。

1.6 定義

別表参照。

2. 公表及びリポジトリに関する責任

2.2 証明書情報の公表

日本銀行は、本 CPS およびオンラインシステム用認証局の利用規約を、日本銀行のホームページ (<http://www.boj.or.jp/>) およびオンラインシステムの情報提供ページにて公表する。

2.3 公表の頻度

日本銀行は、本 CPS またはオンラインシステム用認証局の利用規約を変更した場合には、本 CPS2.2 に従い、最新版を公表する。

3. 確認と認証

3.1.1 識別名の種類

日本銀行が提供する証明書発行等サービスでは、中間 CA 証明書（日本銀行）の識別名を以下のとおり規定する。

CN = Gaitame CA - G3

OU = Class 1 Managed PKI Individual Subscriber CA

OU = Symantec Trust Network

O = Bank Of Japan

C = JP

3.2.3 個人の実在性確認

日本銀行は、クライアント証明書の発行において、Symantec Corporation の CPS で規定された事項に追加して、次の事項のすべてを確認する。

- システム利用者が提出した、オンラインシステムの利用申込書の内容が正確であること
- システム利用者がオンラインシステムの正当な利用権限を有していること

3.2.5 権限の確認

日本銀行は、クライアント証明書の発行において、Symantec Corporation の CPS で規定された事項に追加して、システム利用者がオンラインシステムの正当な利用権限を有していることを確認する。

3.3.1 定期的なリキーに関する確認と認証

日本銀行は、発行したクライアント証明書の更新において、以下のいずれかの方法で本人確認を実施する。

- 発行済みの有効なクライアント証明書を用いた電子署名による確認
- Symantec Corporation の CPS3.2.3 および本 CPS3.2.3 に定める方法

3.3.2 証明書失効後のリキーに関する確認と認証

システム利用者は、取消し後のリキーを行うことはできない。取消されたクライアント証明書のシステム利用者は、Symantec Corporation の CPS3.2.3 および本 CPS3.2.3 に従って、再度発行申請を行う。

3.4 失効申請に関する確認と認証

日本銀行は、発行したクライアント証明書の取消しにおいて、別途定める方法を用いて本人確認を実施する。

4. 証明書のライフサイクルに対する運用要件

4.1.1 証明書申請を行うことができる者

オンラインシステムの利用者になることを希望する者（以下「申請者」という）は、クライアント証明書の発行申請を行うことができる。

4.1.2.1 エンドユーザ証明書の利用者

申請者は、クライアント証明書の発行申請において、Symantec Corporation の CPS の規定に追加して以下の申請手続きを実施する。

- 申請者は、Web を用いたクライアント証明書の発行申請の前に、オンラインシステムの利用申込書を日本銀行に提出し、審査を受けること

審査において申請を承認された申請者に対して、日本銀行はクライアント証明書の発行申請に必要な情報の一部をオフラインで安全に配付する。

4.2.1 本人性確認と認証機能の実施

日本銀行は、本 CPS3.2.3 および 3.2.5 に規定される方法で申請者の全情報の確認および認証を行う。

4.2.2 証明書申請の承認もしくは拒絶

日本銀行は、本 CPS3.2.3 および 3.2.5 に規定される方法で確認および認証が問題なく完

了した場合、クライアント証明書の発行申請を承認する。

4.2.3 証明書申請の処理時間

日本銀行は、申請から妥当な時間内に証明書申請の手続きを開始する。オンラインシステム用認証局の利用規約、本 CPS に別段の定めがない限り、申請処理を完了するまでの時間に関する規定は定めない。そのクライアント証明書申請は、拒絶されるまで有効である。

4.3.2 認証機関の利用者に対する証明書発行通知

日本銀行は、クライアント証明書の発行申請を承認された申請者に対して、クライアント証明書の発行申請に必要な情報の一部をオフラインで安全に配付する。

4.4.1 証明書の受領となる行為

日本銀行が提供する証明書発行等サービスでは、申請者による Web を用いたクライアント証明書の発行申請の後に、当該申請者のクライアント証明書の生成を行う。クライアント証明書が生成され次第、申請者はクライアント証明書をダウンロードして受領する。

4.5.1 利用者の秘密鍵及び証明書の使用

クライアント証明書における公開鍵に対応した秘密鍵の使用は、システム利用者が、オンラインシステム用認証局の利用規約に同意し、クライアント証明書を受領した場合にのみ許可される。そのクライアント証明書は、オンラインシステム用認証局の利用規約および本 CPS の条件に従って合法的に使用されなければならない。

4.8.1 証明書が変更される場合

システム利用者は、既存のクライアント証明書の情報に変更があった場合、クライアント証明書の変更のための再発行申請を行う。

4.8.2 証明書の変更を申請することができる者

システム利用者は、既存のクライアント証明書の情報に変更があった場合、クライアント証明書の変更のための再発行申請を行う。

4.8.3 証明書の変更申請の手続

日本銀行は、本 CPS3.2.3 および本 CPS3.2.5 に規定される方法でクライアント証明書の変更のための再発行申請の確認と認証を行う。

4.8.4 利用者に対する新しい証明書発行通知

日本銀行は、クライアント証明書の変更のための再発行申請を承認された申請者に対し

て、クライアント証明書の再発行申請に必要な情報の一部をオフラインで安全に配付する。

4.8.5 変更された証明書の受領確認の行為

システム利用者は、Web を用いたクライアント証明書の発行申請の後に、当該システム利用者のクライアント証明書の生成を行う。クライアント証明書が生成され次第、システム利用者は変更されたクライアント証明書をダウンロードして受領する。

4.9.1 失効が行われる場合

日本銀行は、Symantec Corporation の CPS で規定されたクライアント証明書の取消し事由に次の事由を追加する。

- システム利用者がオンラインシステムの利用を取止めるとき

また、システム利用者は、Symantec Corporation の CPS4.9.3.1 および本 CPS4.9.3.1 に従い、その秘密鍵の危殆化を知りまたはその疑いがある場合には、直ちにその旨を日本銀行に速やかに通知することとする。

4.9.3.1 エンドユーザ利用者の証明書の失効申請手続

クライアント証明書の取消しを要求しようとするシステム利用者は、別途定める方法を用いて日本銀行にクライアント証明書の取消しを申請する。

4.9.5 認証機関が失効申請を処理しなければならない期間

日本銀行は、遅延なく失効申請を処理する。

4.11 利用の終了

オンラインシステムの利用を終了するシステム利用者は、別途定める方法を用いて日本銀行にクライアント証明書の取消しを申請する。

5. 設備、管理及び運用統制

5.2.1 信頼される役割

日本銀行は、証明書発行等サービスを適切に提供するための体制を整備して、同サービスを提供する。

5.2.2 職務ごとに必要とされる人数

日本銀行は、複数人の関与によって証明書発行等サービスを提供する。

5.2.3 それぞれの任務に必要な身元の確認

日本銀行は、証明書発行等サービスの運用を行う日本銀行の要員の身元確認を実施する。

5.2.4 職務の分離を必要とする役割

日本銀行は、複数の役割によって証明書発行等サービスを提供する。

5.3 人事的管理

日本銀行は、証明書発行等サービスの運用を行う日本銀行の要員に対して、同サービスの運用に必要な知識および技術を習得するための教育訓練を行う。

6. 技術的セキュリティ・コントロール

6.1.2 秘密鍵の受渡

日本銀行が適用する証明書発行等サービスでは、システム利用者の秘密鍵は該当システム利用者自身により生成される。このため、秘密鍵のシステム利用者への受渡は生じない。

6.1.5 鍵のサイズ

日本銀行が提供する証明書発行等サービスでは、使用する鍵ペアのサイズを証明書の種類ごとに以下のとおり規定する。

- ルート CA 証明書：2048 ビット
- 中間 CA 証明書（シマンテック）：2048 ビット
- 中間 CA 証明書（日本銀行）：2048 ビット
- クライアント証明書：2048 ビット

6.3.2 証明書の運用期間及びキー・ペアの使用期間

日本銀行が発行するクライアント証明書の有効期間は 3 年とする。

7. 証明書、CRL 及び OCSP のプロファイル

7.1 クライアント証明書の設定値

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)	—	19A5 F607 4C42 F1CD 33C1 64A9 EF35 C6CF (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)	—		日本銀行が、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)		1.2.840.113549.1.1.11	sha256WithRSAEncryption を表す OID の値を示す。
Issuer name (発行者名)	—	CN = Gaitame CA - G3 OU = Class 1 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = Bank Of Japan C = JP	中間 CA 証明書 (日本銀行) 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)		YYMMDDHHMMSSZ 130511000000Z (例)	証明書の有効期間開始日を示す。UTCTime 型。
notAfter (終了日)		YYMMDDHHMMSSZ 160510235900Z (例)	証明書の有効期間終了日を示す。UTCTime 型。
subject name (主体者名)	—	※日本銀行が作成した命名規則 (非公表) に基づき、システム利用者を識別できる識別名を設定する。	システム利用者の識別名 (DN) を示す。英語表記、CA 名称は T61STRING、メールアドレスは IA5STRING、その他は PrintableString 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)		BIT STRING	証明書の公開鍵の値を示す。BIT STRING 型。
Extensions (証明書拡張領域)			
basicConstraints (基本制約)	FALSE		CA 証明書であるかどうか、および CA 証明書の階層の制限を示す。
cA		False	CA 証明書ではなく、エンド・エンティティ証明書であることを表す。Internet Explorer では「Subject Type=End Entity」と表示される。

領域名	クリティカルフラグ	値(例)	説明
keyUsage (鍵用途)	FALSE		鍵の使用目的を設定する。
digitalSignature		1	署名に使用することを表す。
KeyEncypherment		1	共通鍵の暗号化に使用することを表す。
certificatePolicies (証明書ポリシー)	FALSE		
policyIdentifier			
certPolicyId		2.16.840.1.113733.1.7.23.1	証明書ポリシーを表す OID の値を示す。
policyQualifiers			ポリシー修飾子 (CP/CPS へのポインタまたはユーザ通知情報) を示す。
policyQualifierId		id-qt-cps	
qualifier		https://www.symauth.com/rpa	
policyQualifierId		id-qt-unotice	
qualifier		Use for Bank of Japan Gaitamehou Tetsuzuki Online System only. Terms of use at http://www.boj.or.jp/ (Please find Web pages related to reports prescribed by foreign exchange and foreign trade laws.)	
cRLDistributionPoints (CRL 配布点)	FALSE	URL= http://onsitecrl.symauth.jp/BankOfJapanGaitameCA/G3/LatestCRL.crl	CRL の配布点を、URI と fullName を使用して示す。
Subject Key Identifier (サブジェクトキーの識別子)	FALSE	bb12 1e07 f205 15c2 915a e500 4c3c 91cd 605b 11fe (例)	クライアント証明書の RSA 鍵ペアを識別する情報を設定する。
Authority Key Identifier (発行者の公開鍵識別子)	FALSE	KeyID = 8238 300f a427 44e8 daac c17f 5e77 aa75 de1a e97d	中間 CA 証明書 (日本銀行) の RSA 鍵ペアを識別する情報を設定する。
Extensions (証明書拡張領域) の記載はここまで			
issuer's signature (発行者署名)	—		日本銀行が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)		1.2.840.113549.1.1.11	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。

9. 業務及び法律に関するその他の事項

9.1.1 証明書発行または更新の手数料

日本銀行は、システム利用者に対し、証明書発行等サービスに関し、手数料を請求しない。

9.6.1 認証機関の表明と保証

日本銀行はシステム利用者に対し、次の事項を保証する。

- クライアント証明書に記載される事実には、日本銀行が知り、またはそこから生じる重要な不実の記載は存在しないこと
- クライアント証明書中の情報には、日本銀行が、クライアント証明書の発行申請の取扱において合理的注意を用いることを怠ったことにより生じた誤りが存在しないこと
- システム利用者よりクライアント証明書の取消し申請があった場合には、取消し申請の審査、および取消し手続きに相当な注意を払い、取消対象のクライアント証明書を取消すること
- クライアント証明書が本 CPS に定める全ての重要な要件に合致していること

9.6.3 利用者の表明と保証

システム利用者は、クライアント証明書の秘密鍵が危殆化した場合（または危殆化する恐れがある場合）、またはその秘密鍵を保護するデータもしくはクライアント証明書中の情報が不正確であるか変更されたという事態が生じた場合には、クライアント証明書の取消し請求を日本銀行に速やかに行う。

また、システム利用者は、日本銀行に対し、クライアント証明書が、正当で合法的な目的のためにのみ、かつ、本 CPS を遵守した態様によってのみ、使用されることを保証する。

9.7 保証の否認

適用される法律上許される範囲内において、オンラインシステム用認証局の利用規約は、日本銀行のその他一切の保証を否定する。

9.8 責任の制限

日本銀行は、クライアント証明書の取得、使用等によって生じた損害に対する賠償責任を、一切負わない。

9.10.1 有効期間

本 CPS は、日本銀行のホームページおよびオンラインシステムの情報提供ページに掲載されたときに有効になる。本 CPS の変更も、日本銀行のホームページおよびオンラインシ

システムの情報提供ページに掲載されたときに有効になる。

9.10.2 終了

本 CPS は、新たな CPS が効力を発するまで、有効とする。

9.10.3 終了の効果と効力の残存

本 CPS が終了した場合においても、システム利用者は発行したクライアント証明書の残存有効期間中は、本 CPS の条項に拘束されるものとする。

9.12.1 改訂手続き

日本銀行は、システム利用者の事前の了解を得ることなく、必要に応じて適宜本 CPS の内容を、Symantec Corporation の CPS に対して矛盾のないように変更することができる。

9.12.2 通知方法と期間

日本銀行は、本 CPS の変更内容を日本銀行のホームページ (<http://www.boj.or.jp/>)およびオンラインシステムの情報提供ページにて公表する。

9.13 紛争の解決

本 CPS のいずれかの事項にかかわる紛争を解決する場合、法的措置を講じる前に、システム利用者は、日本銀行その他の紛争にかかわる当事者に通知して、当事者間で紛争の解決を求めることとする。当事者間で紛争が解決できなかった場合、当該紛争の解決については東京地方裁判所を第一審の専属管轄裁判所とする。

別表：定義

用語	定義
日本銀行外為法手続きオンラインシステム（オンラインシステム）	外国為替および外国貿易法において日本銀行が事務委任を受けて受理する報告手続きに係るものを処理するシステムおよび電子報告手続きを支援するための各種情報等を提供するシステム。
日本銀行外為法手続きオンラインシステム用認証局（オンラインシステム用認証局）	日本銀行外為法手続きオンラインシステム用認証局は、日本銀行外為法手続きオンラインシステムにおけるクライアント証明書の発行、更新、取消しおよび管理を含む一連のサービスを提供する機関である。なお、日本銀行は、日本銀行外為法手続きオンラインシステム用認証局の運用業務の一部を、シマンテックに委託している。
情報提供ページ	日本銀行外為法手続きオンラインシステムのうち、電子報告手続きを支援するための各種情報等を提供するページ。