相互認証ガイドライン

(アルファ版)

平成 10 年 3 月

電子商取引実証推進協議会(ECOM)
認証局検討ワーキンググループ

はじめに

電子商取引において、取引の安全性を確保する上でデジタルな認証は重要な役割を果たす。
また、電子商取引の発展に伴い、各種ビジネスプロセスにデジタル認証が使用されることが想定される。
このような状況で電子商取引参加者の利便性を考えると、相互認証は重要な技術課題と考えられる。
本書は、このような相互認証における以下の内容を記述している。

- 相互認証の運用モデル
  相互認証を行うにはいくつかの方式があるが、本書で対象とする相互認証のモデルについて記述している。
  本書で対象とする相互認証モデルは、相互認証を行う認証局が「相互認証書」を共有することにより実現する方式とした。
- 相互認証を行う認証局の運用要件
  上記相互認証書による相互認証を行うにあたり、認証局が遵守すべき運用要件について、本ワーキンググループ発行の「認証局運用ガイドライン」に記述されている要件に加え、相互認証のために必要な要件を記述している。
- 相互認証の技術要件
  相互認証書による相互認証を行うための以下の技術要件を記述している。
  ・相互認証書および CRL 形式
  ・相互認証インタフェース
  ・CRL 運用

本ガイドラインは、平成８年度に「相互認証技術解説および基本仕様案」を作成後、継続して活動してきた下記グループによって相互認証を行う認証局の運用要件までを含め、ガイドラインとしてまとめられたものです。
関係各位からの忌憚のないご意見、ご要望を期待していますので、下記までお寄せください。

電子商取引実証推進協議会（ECOM）
認証局検討ワーキンググループ／相互認証検討サブワーキンググループ（WG08/SWG2）
〒135-8076　東京都江東区青海 2-45 タイム 24 ビル 10 階
TEL(03)5531-0065　FAX(03)5531-0068
E-Mail:yonekura@ecom.or.jp（米倉）
http://www.ecom.or.jp

1 目的

電子商取引の発展には、取引情報を第三者から守るための機密性、真正性の保持が重要であり、且つ取引相手が本人であることを証明する認証技術が極めて重要な鍵となる。
発展段階にある現在の電子商取引での認証は、クレジットや銀行決済等のアプリケーション毎に閉じた世界で機能している。
今後、ますます発展すると思われる電子商取引では、多種多様の認証局が設立、運営され、エンドエンティティはサービスやアプリケーション毎に複数の認証書を所持しなければならなくなることが想定される。
本書はこのように認証書を利用するエンドエンティティがサービスやアプリケーション毎に認証書を取得することなく、同一もしくは異なる認証ドメインの認証書を相互に運用させることにより、様々なサービスを享受できるようにするためのものである。

1.1 「相互認証ガイドライン」の構成

ガイドラインを構成する運用要件、技術要件等の各項目を説明する。

(1) **検討の前提**
いくつかの相互認証の形態を考察するとともに、ガイドラインが対象とする形態を述べる。加えて相互認証における契約の条件等について記述する。

① **相互認証の概要**
いくつかの相互認証の形態を説明するとともに、ガイドラインが対象とする相互認証の形態を記述する。

② **相互認証書の形式と配布方法**
相互認証書に関し、その配布手順等について記述する。

③ **相互認証の契約**
相互認証を行なう認証局間における契約条件に加え、国際間において契約を行う場合に留意することを記述する。

④ **相互認証の制限**
相互認証書の利用について、自己の認証ドメインの安全性を保持するために制限を定めることを記述するとともに、セキュリティレベルの低下を防ぐため、相手先認証局のレベルに合せた相互認証書を配布することを推奨している。

⑤ **認証書**／CRL **フォーマット**
本ガイドラインの検討にあたり、参考とする認証書および CRL フォーマットについて記述する。

⑥ **認証書管理プロトコル**
相互認証を行う場合の異なるフォーマットの認証書を利用して認証書管理プロトコルが実行される点を記述する。

⑦ **認証局におけるポリシーの扱い**
認証書発行に関しポリシーを定める必要性の記述に加え、相互認証を行う相互の認証ドメインの管理者が事前合意することの必要性を記述する。

(2) **運用要件**
相互認証を実行するために必要なマネジメント、運用、責務の要件に関し、ポリシー、準備事項や手続きなどを規定する。

① **相互認証のマネジメント要件**
相互認証を行なう認証局の審査・配布基準について相互契約することを記述する他、エンドエンティティに対して技術情報等を公開することの必要性を記述する。

② **相互認証の信用レベル**

相互認証を行う場合の認証局間の信用レベルの整合性並びにその公開について記述する。

③ **責務**

相互認証を行う認証局の責任と保証の必要性を記述する。

④ **監査**

相互認証契約においてチェックアンドバランスを図るため、監査機構を採用することを記述する。

⑤ **相互認証の運用**

相互認証書の配布手続き、配布方法の他、相互認証における更新や失効の手続きを記述する。

(3) **技術要件**

運用要件で規定した要件に対し、これを実装する際の技術要件を規定する。

① **認証書および** CRL **形式**

相互認証時に配布される認証書および CRL の形式について X.509 で規定されるフィールドの拡張部に関し、相互認証で定義するものについて規定する。

② **相互認証インタフェース**

本ガイドラインでは、特定の認証書管理プロトコル等を想定しない汎用性のある相互認証を対象としている。このため、これを実現するためのインタフェースについて記述する。

③ CRL **運用**

認証局認証書の CRL 管理に依存する相互認証書の失効について、相互認証を行なう認証局が行なうべき失効のための共通要件について規定する。

(4) **付録**

今回のガイドライン作成にあたり、参考とした資料および取りまとめのベースとしたものは以下の通りである。

なお、特定のプロトコルについては、参考例として記載しているものである。

① **付録Ａ　参考資料**

本ガイドライン作成のために参考とした文献並びに URL を掲載している。

② **付録Ｂ**　SET **における有効期限の考え方**

認証書の有効期限に関し、ひとつのモデルとして SET における有効期限設定の考え方を例示した。

③ **付録Ｃ　相互認証の形態**

本ガイドラインが対象としている相互認証形態の他に、諸外国において検討あるいは実装されている相互認証のモデルを掲載している。

④ **付録Ｄ　第 3 者機関を仲介する方式**

相互認証の当事者となる認証局とは独立した第三者的立場としてのレポジトリおよび中継ハブの機能、役割について記述したものである。

⑤ **付録Ｅ**　SET **相互認証技術**

クレジットカード決済の標準プロトコルである SET において、相互認証を行った場合を想定しての技術解説である。

⑥ **付録Ｆ　相互認証技術解説**

相互認証技術の基本となる方式並びに IETF 等で公開された認証技術の解説を紹介するとともに、これと対比して相互認証技術を解説している。

⑦ **付録Ｇ　メンバー一覧**

本ガイドライン作成に協力いただいた、メンバーを掲載している。

1.2 用語の定義

本ガイドライン中で使用している用語について規定する。

１．公開鍵暗号システム（Public Key Cryptosystem）
関連した２つの鍵（公開鍵と秘密鍵）を使用する暗号システムであり、一方の鍵（公開鍵）で暗号化したデータは他方の鍵（秘密鍵）でのみ復号化できるようになっている。２つの鍵は、公開鍵が与えられても、秘密鍵を導き出す事が計算上不可能な特性を持っている。

２．公開鍵（Public Key）
公開鍵暗号システムにおける鍵ペアのうちの一つで、通信相手等の他人に知らせて利用してもらうための鍵。

３．秘密鍵（Private Key）
公開鍵暗号システムにおける鍵ペアのうちの一つで、他人に知られないようにしておく鍵。

４．鍵ペア（Key Pair）
公開鍵暗号システムにおける公開鍵およびそれに対応する秘密鍵。

５．共通鍵（Symmetric Key）
発信者と受信者が同一の暗号鍵を使用してデータの暗号化と復号化を行う共通鍵暗号システムにおける鍵。

６．公開鍵基盤（Public Key Infrastructure）
公開鍵暗号システムを用いて情報システムやコミュニケーションシステムのセキュリティを確保するための一連の技術およびサービス。

７．認証（Certification）
個人、法人、システム等に対して認証書を生成するプロセス。

８．認証書（Certificate）
認証対象者の識別情報と公開鍵とが対応していることを証明するデジタル文書。認証対象者の識別情報、その公開鍵、鍵の利用目的・範囲、発行認証局名などを含む一連の情報に、認証局のデジタル署名を付加したもの。

９．デジタル署名（Digital Signature）
署名対象データのハッシュ値（データを数学的な操作によって一定の長さに縮小させたもの。ハッシュ値から元のデータは再現不可能）に対して、秘密鍵で暗号化したもの。デジタル署名の検証は、デジタル署名を公開鍵で復号化した値と元のデータのハッシュ値とを照合することで可能。デジタル署名は、当該秘密鍵の保有者のみが生成できることから文字による署名と同等の効果が推定される。

１０．認証書の発行（Certificate Issuance）
認証書を生成し、認証書に登録された申請者に対し、その内容を通知する行為。

１１．認証書の失効（Certificate Revocation）
認証書の有効期限内に、秘密鍵が危瀕した場合、あるいは氏名等の重要な属性情報に変更が生じた場合に認証書そのものを無効にする行為。

１２．認証書の一時失効（Certificate Suspension）
認証書の有効期限中に一時的に認証書を失効させる行為。

１３．失効リスト（Certificate Revocation List＝CRL）
失効した認証書が登録されたリスト。通常認証局によるデジタル署名が付される。

１４．認証書の検証（Certificate Verification）
認証局、エンドエンティティにおいて認証書の正当性を確認すること。
具体的にはデジタル署名により内容が改竄されていないこと、正当な認証局から発行されていること、有効期限内であること等を確認する。

１５．認証局（Certification Authority）
認証書の発行、開示、失効、もしくは一時失効等のサービスを行なう信頼された個人または法人。

１６．認証ドメイン（Domain）
認証局および認証局から発行される認証書を使用するエンドエンティティから構成される EC 業務を実現するシステム全体を示す。SET により実現されるクレジットカード決済システム、企業間の取引を実現するシステムがそれぞれのドメインとなる。

１７．相互認証（Cross Certification）
２つの認証局が相互にお互いの公開鍵を認証するプロセス。相互認証により、異なる認証局が発行した認証書の相互流通が可能になり、加入者の認証書利用領域が拡大する。

１８．相互認証書（Cross Certificate）
認証局が相互に認証するための認証書。２つの認証局が、相手の認証局に発行した認証局認証書を少なくとも一つ含む形式で定義している。

１９．認証局認証書（CA Certificate）
認証局に対して発行する認証書。

２０．認証書の配布（Distribution）
認証書を用いるシステムでは、各エンティティは自身の認証書だけでなく、通信相手のユーザ認証書、自身および通信相手の認証局認証書、相互認証を行う場合の相互認証書等を必要とする。各エンティティに対してこれらの認証書を利用可能とすることをいう。

２１．認証書管理プロトコル（Certificate Management Protocol）
認証書を各エンティティ間（認証局⇔認証局、認証局⇔エンドエンティティ、エンドエンティティ⇔エンドエンティティ）で転送するためのプロトコル。

２２．ビジネスプロトコル（Business Protocol）
エンドエンティティ間で実装する業務を実現するために規定したプロトコル。具体的には VISA、Mastercard の規定するクレジット決済用の SET、クレジット/銀行決済用の SECE や、企業間取引を実現するプロトコルを意味する。一般に認証書管理プロトコルを含んでビジネスプロトコルが実装されている。

２３．認証実施規定（Certification Practice Statement＝CPS）
認証書の発行において、認証局が採用する一連の規定を盛り込んだ声明文。

２４．エンティティ（Entity）
認証の対象となる実在する個人および法人。認証局、登録局、エンドエンティティが含まれる。

２５．エンドエンティティ（End Entity）
認証書に署名する以外の目的で秘密鍵を使用する認証書取得者。

２６．危瀕（Compromise）
秘密鍵、機密情報等が不正に漏洩、公開されたかその可能性がある状況に瀕している事。

２７．ポリシー（Policy）
認証局がサービスを提供する上で、認証書利用者等に開示する方針や規定、基準。

２８．リポジトリ（Repository）
認証書や失効リスト等を保管し、認証書利用者等に対してこれらの開示や配布もしくは検索等のサービスを提供するシステム。

2 検討の前提

本章では、本書で規定する相互認証の運用および技術要件の前提となる相互認証の形態、相互認証書の考え方等の基本条件を規定する。

2.1 相互認証の概要

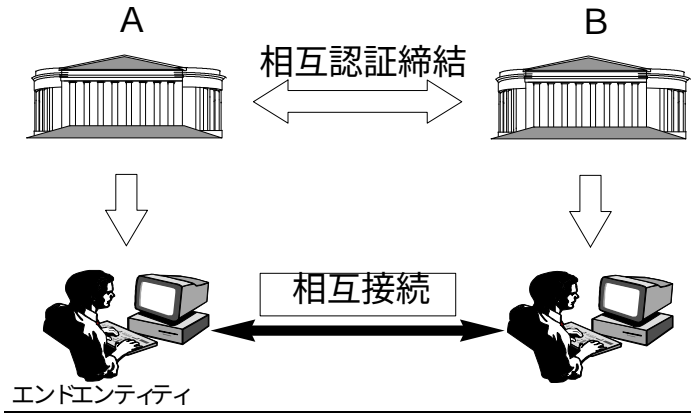
相互認証を実現する方式にはいくつかの方式がある。
本項ではそのうち代表的な方式を解説し、本書で対象とする方式について記述する。

2.1.1 相互認証形態

本書は、同一もしくは異なる認証ドメイン間で相互に目的を達せられるものは、相互認証を前提とする。

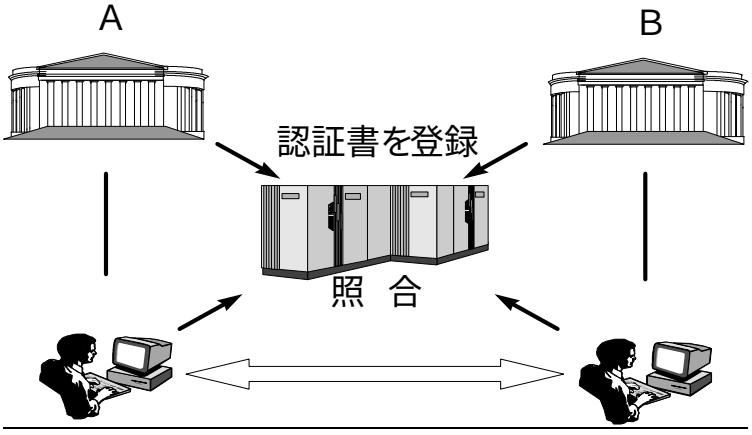
2.1.1.1 相互認証書を配布する方式

この方式は、相互認証を希望する認証局間にて、両局管轄の認証ドメインにおけるポリシー・認証審査レベル等の調整を行い、管轄下のエンティティに対し認証局が相互認証書を作成・配布し、この相互認証書を用いて両認証ドメイン間の相互認証を可能とする方式。



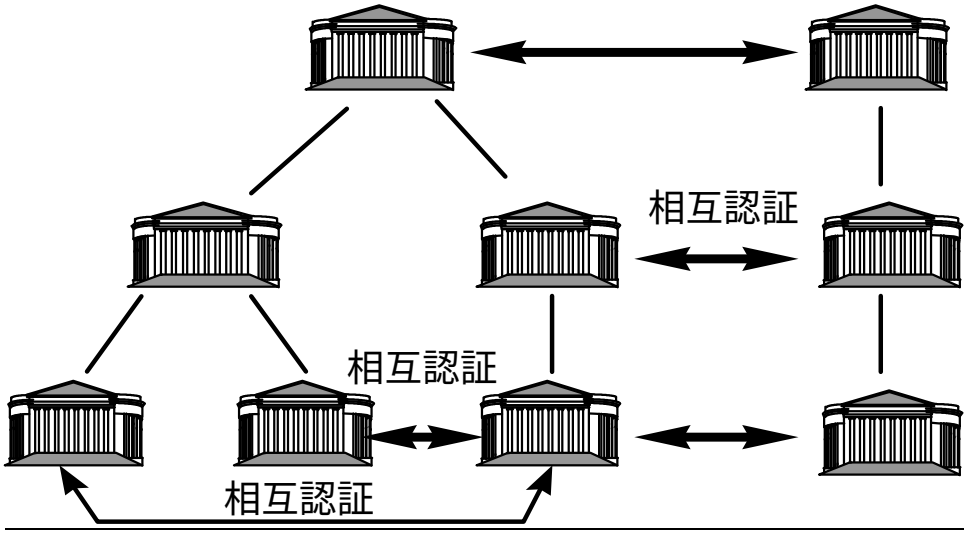
2.1.1.2 第三者機関を使用する方式

この方式は、相互認証を締結した両認証局が信頼のおける第三者機関を設定し、各認証局のエンドエンティティ間において取引を行う際、この第三者機関を使用して相手エンティティの認証を確立する方式。



2.1.2 本書対象の相互認証

本書では認証局もしくはルート認証局がお互いの信用レベル・ポリシーに整合性を持たせ、相互認証書を自局エンティティに対して配布する形態の相互認証契約を対象としており、第三者機関を使用する方式に関しては参考として記載し、本編では詳細を規定しない。



2.1.3 相互認証する認証局の数

２者間のエンドエンティティモデルで考える。３者間以上のモデルは、２者間モデルの拡張であり、２者間モデルを２つ組み合わせて動作させるモデルとして扱うこととする。

2.2 相互認証書の形式と配布方法

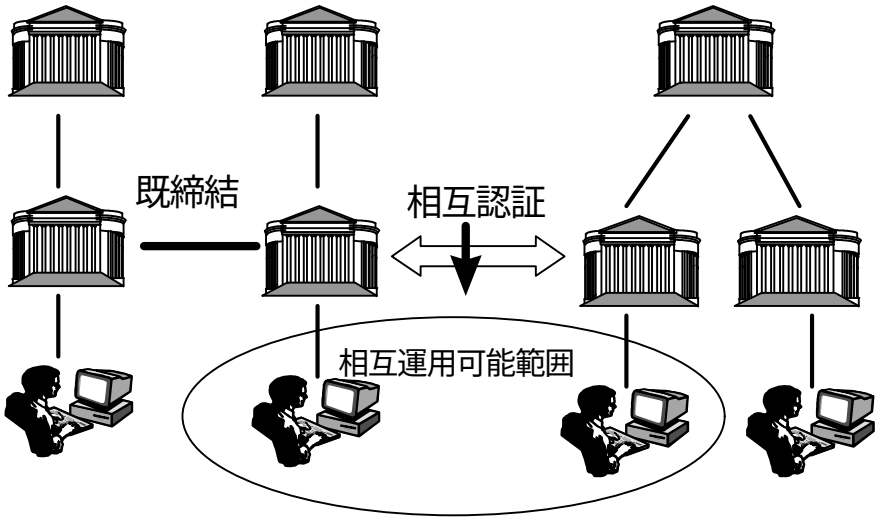
本書における相互認証の範囲においては、相互認証書と認証局認証書とは分けて考える。
また、レポジトリ等を置かない本書相互認証の範囲では、認証局がエンドエンティティに対してユーザ認証書を配布するタイミングで相互認証書を配布することを前提とする。

2.3 相互認証の契約

本項では相互認証にあたり、相互認証を行う認証局間の契約内容について考慮すべき点および国際間で行う場合の留意点について記述する。

2.3.1 契約の条件

認証局間における相互認証契約は、各々の階層における個々の認証局が持つ役割を遂行する上で各階層を超えて締結することはせずに、同一の階層内の認証局間にて締結することが望ましい。
例えば、階層型認証経路を形成する二つの認証ドメイン間で相互認証を行う場合、ルート認証局と認証局が相互認証の契約を行うことは、ポリシー、ビジネスプロトコル、認証審査レベル等の整合性を図る上で望ましくなく、階層を形成する中で同一の役割を持つ認証局間で契約の締結を行う必要性がある。
また、相互認証に関する認証局間での契約は、相互認証を行う毎に締結することが望ましい。
仮に締結先の認証局がすでに他の認証局と相互認証契約を締結していた場合でも、自局との相互認証契約によって包括的に相手認証局の既締結認証局との相互認証契約は行えない。



2.3.2 国際間の相互認証

国際間における相互認証は、認証局の認可制、デジタル署名法、暗号規制等の制度に基づく各国の電子商取引に関する政策の相違や個々の国々が持つ独特の取引形態（商習慣）などの相違を考慮する事が必要である。

2.4 相互認証の制限

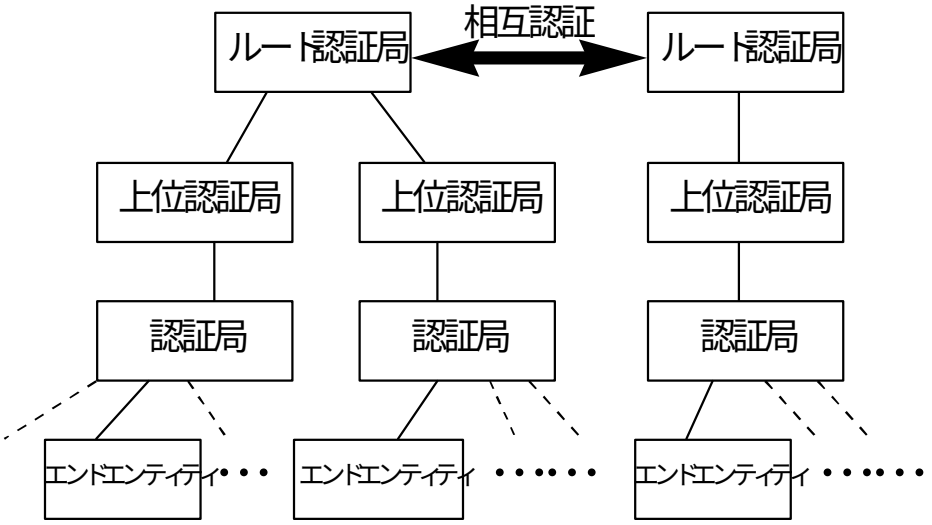
相互認証を行う個々の認証局は、自局認証ドメインの保全のため相互認証の制限を行えるようにする必要がある。

2.4.1 相互認証書利用の制限

認証局間においては、相互認証を行うことで自局が所属する認証ドメインに信用レベル、セキュリティレベル、ポリシー等の低下を招く可能性がある場合、相手先認証ドメインとの相互認証を拒否、若しくは取引内容に両者合意のもと何らかの制限を持たせ、自局が所属する認証ドメインの保全を図る必要がある。

2.4.2 下位認証局への制限

認証局もしくはルート認証局が相互認証を締結する際、各認証局もしくはルート認証局の下位階層に属する下位認証局、エンドエンティティを包括して相互認証させることが望ましい。
但し、相手先の下位認証局の信用レベル、設備レベルによっては、各々の認証局のレベルに合わせ、取引内容に制限を持たせた相互認証書を配布するなど、自局の信用レベル、セキュリティレベルの低下等を防ぐことが望ましい。



2.5 認証書/CRL フォーマット

認証書は X.509V3 ベースとし、相互認証書を使用することで相互認証を実現する。また認証書の失効には X.509CRL フォーマット V2 を使用する。

2.6 認証書管理プロトコル

認証書として X.509V3 フォーマットを前提とするが、各ビジネスプロトコル毎に認証書のフォーマットが設計されるため、相互認証を行う場合に異なるフォーマットの認証書を用いて認証書管理プロトコルが実行される点について考慮する必要がある。

2.6.1 同一ビジネスプロトコルでの相互認証

同一のビジネスプロトコルが異なる認証ドメインで運用されている状態において、異なる認証ドメインに属するエンティティの相互認証を可能とするケースである。

使用する認証書は、適用するビジネスプロトコルの要件を満足するように設計されており認証書の相互認証を可能とすることで、相互運用が可能となるケースである。

2.6.2 異なるビジネスプロトコルでの相互認証

異なるビジネスプロトコルが異なる認証ドメインで運用されている状態において、異なる認証ドメインに属するエンティティの相互認証を可能とするケースである。例えば、クレジット決済用認証書をメールで使用する場合である。

使用する認証書は、それぞれのビジネスプロトコルの要件を満足するように設計されているため、相互認証時には本来の目的と異なるビジネスプロトコルで認証書が利用される。このため、両ビジネスプロトコルが参照している認証書のフィールドについて次の要件を満足する必要がある。

- 両ビジネスプロトコルが参照する認証書のフィールドが一致している。フィールドの使用有無の一致だけでなく、設定値の意味も含めて一致している必要がある。
- 両ビジネスプロトコルが参照する認証書のフィールドの使用有無は一致しない場合、一方のビジネスプロトコルは必要とするフィールドを参照できなくなる。参照できなかった場合の動作について相互認証を行う前に両認証ドメインの管理者が合意する必要がある。
- 両ビジネスプロトコルが参照する認証書のフィールドの使用有無が一致しているが設定値の意味が異なる場合、一方のビジネスプロトコルは必要とするフィールドを参照し、自認証ドメインで発行された認証書と同じ解釈をして動作してしまうことが考えられる。そのような場合、解釈が本来の意味と異なる場合の動作について相互認証を行う前に両認証ドメインの管理者が合意することが必要である。

2.7 認証書におけるポリシーの扱い

認証局の運用に当たっては、各認証局の発行する認証書の利用についてポリシー(「信用レベル」「権限レベル」という表現を用いる事もある)を定める必要がある。相互認証を行う場合の認証書管理プロトコルの前提について、２．６項で述べたが、特に、ポリシーを含めた認証書を利用している場合について考え方を明確にする必要がある。
ビジネスプロトコルにおいて認証書を正しく検証できた場合に通信相手を認証（特定）することができる。ただし、認証書の検証は相手を特定しているだけであり、相手にどこまでの権限を与えるか（ポリシー）は別の問題と考える必要がある。
例えば、認証書の利用目的として、電子メール用、電子商取引用といった区別をする場合には、単に認証書の検証によりビジネスプロトコルを実行してはならず、ポリシーが一致（妥当）であることを確認しなければならない。
認証書にはポリシーを表現するためのフィールドが存在するが、標準的な規定はされていないため、本書では相互認証する相互の認証ドメインが、認証書に含まれるポリシー記述フィールドを解釈可能であることを前提とする。一方の認証ドメインのみがポリシー記述フィールドを使用する場合には相互認証を行う前に両認証ドメインの管理者が合意することが必要である。

2.8 暗号アルゴリズム

本書においては、使用する暗号については規定しないものとする。
本書は認証書の相互認証に限定するものであり、暗号の相互接続性に関しては各認証ドメインにおいて解決すべき問題としたい。
例えば、RSA・楕円曲線暗号等については意識せずに、公開鍵の認証書の相互認証にのみ着目し、各認証ドメインが相互に使用できる暗号を実装することが前提。

3　運用要件

3.1 マネジメント要件

認証局が同一もしくは異なる認証ドメインの認証局と相互認証を行うにあたり、考慮すべきマネジメント要件について記述する。

3.1.1 審査・発行

各々の認証局は、配布する認証書の審査規準・発行規準を相互で合意のもとでのみ相互認証を可能とする。また、その合意は基本的に相互が持つ個々のポリシーから見てエンドエンティティに対しサービス低下とならないことが望ましい。

その合意は書面による行為が好ましく､相互認証の対象となる認証書を明確にしておく必要がある。

同一の発行認証局から信用レベルの異なる認証書が発行された場合は、包括的に全体として合意を交わすのではなく、各々の信用レベルに従い相互認証の合意を交わすことが必要である。

3.1.2 公開・通知

相互認証を行う認証局は、認証局個々の認証局運営ポリシーの公開とは別に、相互認証を実現する相手認証局、相互認証する認証書の名称、相互認証の制限事項およびエンドエンティティ間で相互認証を可能とする技術的方法等の内容をエンドエンティティにわかりやすく誤解を与えないように公開する必要がある。

公開内容に対してエンドエンティティは、ウェッブ等の一般的な広告手段にて随時確認できることが望ましい。この情報は常にアップデートして最新の情報を公開することが望ましい。

3.2 相互認証の信用レベル

相互認証の対象とする認証ドメインの信用レベルについて、その整合性および公開について記述する。

3.2.1 信用レベルの整合性

認証書には、その認証書を発行する審査のレベルにより信用レベルに相違がある。

例えば、住民票による在住確認レベルの認証書と信用状況確認による認証書では、その認証書の信用レベルに相違があり、その認証書の利用可能範囲にも相違があると考えられる。

そこで、相互認証にあたり、個々の認証局が発行する複数の認証書レベルの内どれを相互認証の対象とするかを、相互認証契約時に確認する必要がある。

相互認証の信用レベルの合意にあたっては､できる限り､同一信用レベルでの相互認証が望ましい。また、それが不可能なときには、低い信用レベルの利用範囲に限定することが望ましい。

以下に一例として、信用レベルと相互認証の望ましい形を例示する。

各信用レベルの概要

審査レベル	審査内容の概要
低レベル	被認証者の名前／E メールアドレス等の存在
中レベル	個人・法人等を証明する書類の提示と、その書類の第三者機関への確認
高レベル	上記に加え、本人との直接接触を含む複数の手段での本人確認

信用レベルと相互認証の関連

	低レベル	中レベル	高レベル
低レベル	○	△	△
中レベル	△	○	△
高レベル	△	△	○

○：望ましい形態であり、それぞれのレベル機能範囲がサービス可能となる。

△：異なる信用レベル間の相互認証であり、機能範囲が低い信用レベルに合わせることが望ましい。

3.2.2 信用レベルの公開

上記 3.2.1 で述べた相互認証の信用レベルは、個々の認証局が発行する認証書の顧客であるエンドエンティティにとって特に重要な情報である。
そこで、相互認証対象の認証書種類および相互認証での信用レベルは、明確にかつエンドエンティティが誤解しないような方法で公開することが望ましい。
また、すでに相互認証の対象となる認証書を入手しているエンドエンティティに対する相互認証書の配布基準を明示することが望ましい。

3.3 責務

相互認証を行う認証局は、「認証局運用ガイドライン」に記述された認証局の責任と保証に加え、相互認証に関する責任と保証を相互認証当事者認証局間で規定しておく必要がある。
内容は、「認証局運用ガイドライン」にある、実施規定違反・不法侵入・暗号解読等による、エンドエンティティ等の情報漏洩・認証書不正使用等について責任と保証を規定することが望ましい。

3.4 監査

相互認証を実現している相手の認証局に対して、その契約あるいは覚書内容に疑義が無いことを確認するため相互に監査する機構を採用することが必要がある。
監査タイミングは相互認証書の有効期限等の技術的要因による定期的な監査を基本としながら、お互いの事前合意のもと不定期の監査も取り込むことが望ましい。
尚、監査をより有効にするため、第三者機関による外部監査を、相互認証をおこなう認証局間の事前承認を前提に利用することが望ましい。

3.5 相互認証の運用

相互認証を行う認証局が、相互認証可能な認証書を配布するにあたり、遵守すべき認証局運用上の内容について記述する。

3.5.1 相互認証書配布手続き

相互認証書は、２つの認証局が個々に配布するエンドエンティティ向け認証書を、相互に利用可能とするために、２つの認証局が共有する認証書であり、本項では相互認証書の配布手続きについて記述する。

3.5.1.1 相互認証書配布の承認

相互認証書配布にあたっては、以下の内容について、認証局間で確認し何らかの契約行為を行うと同時に、広く利用者であるエンドエンティティに公開する必要がある。本契約行為を両認証局が承認することにより、相互認証書の配布を行う必要がある。

(1) **運用上の内容**

- 相互認証書の配布
- 相互認証書の有効期限
- 相互認証書の更新

- 相互認証書の失効手続き
- 認証局の責任範囲と免責条件
- その他

(2) **技術上の内容**

- 認証書形式
- 相互認証書の配布
- エンドエンティティ認証書の検証方式

3.5.1.2 相互認証書の配布方法

相互認証書を、認証局が入手する方法であり、以下の内容を規定することが望ましい。

(1) **相互認証書を入手するにあたって提示する内容**
基本的には、相互認証の技術的内容に左右されるが、本提示内容に相互認証書取得者を特定可能な情報が含まれることが必要である。

(2) **相互認証書を入手する手段**
認証局が相互認証書を取得する手段であり、オンライン・オフラインの区別及びそれぞれの具体的内容（例えばオフラインであれば、相互認証書の格納媒体・受け渡し場所・受領者・資格等）を規定することが望ましい。

(3) **相互認証用公開鍵の生成**
相互認証書に使用する公開鍵は､個々の認証局認証書公開鍵とは別にすることも可能であり、その場合、生成場所・生成機器及び生成立ち会い者（基本的に相互認証に関わる認証局の責任者を含むことが望ましい）等を規定することが必要である。

3.5.1.3 相互認証書の有効期限

相互認証書は、２つの認証局の相互認証を保証する重要な認証書である。
その為、相互認証書は可能な限り短期に更新することが望ましい。
但し、エンドエンティティの利便性を損なわないよう、エンドエンティティ認証書の有効期限を配慮し、相互認証書の有効期限を設定すべきである。
付録 B に、SET における認証書有効期限の考え方を参考として掲載する。

3.5.1.4 相互認証書の更新

配布された相互認証書を何らかの事由により再度配布する手続きであり、基本的に 3.5.1.2「相互認証書の配布方法」で記述した内容を含むことが望ましい。
また、相互認証書更新に至る事由を明確にすることが必要であり、その事由は、有効期限満了および 3.5.1.5「相互認証書の失効手続き」で記述する事由に限定する必要がある。

(1) **再配布相互認証書を入手するに当たって提示する内容**
基本的には、相互認証の技術的内容に左右されるが、本提示内容に再配布相互認証書取得者を特定可能な情報が含まれる必要がある。

(2) **再配布相互認証書を入手する手段**
認証局が再配布相互認証書を取得する手段であり、オンライン・オフラインの区別及びそれぞれの具体的内容（例えばオフラインであれば、相互認証書の格納媒体・受け渡し場所・資格・等）を規定することが望ましい。

(3) **再配布相互認証用公開鍵の生成**
再配布相互認証書に使用する公開鍵の生成方法の規定であり、生成場所・生成機器及び生成立ち会い者（基本的に相互認証に関わる認証局の責任者を含むことが望ましい）等を規定することが望ましい。

3.5.1.5 相互認証書の失効手続き

本項では、相互認証を目的に配布される相互認証書の失効について述べる。
失効の一種に一時失効があり、これはある期間だけ失効させるもので、その期間が終わると失効が

解除され、一時失効の手続きは通常の失効と同様であると考えられる。
相互認証書の失効とは、何らかの事由により相互認証に使用する相互認証書を利用不能とすることをいい、認証局間の相互認証契約の解消を意味するものではない。
尚、個々の認証局の相互認証書以外の認証書の失効は、個々の認証局のルールに依存する。
相互認証書の失効手続きには、以下の内容を明確にすることが望ましい。

(1) **失効基準**

相互認証書の失効の事由は、基本的に当該相互認証書の公開鍵暗号方式における秘密鍵の紛失、盗難、漏洩、非公式な開示等にすることが望ましい。
また、相互認証書の失効は、相互認証を利用するエンドエンティティに大きな影響を与える為、相互認証開始に当たり事前にその基準を公開する必要がある。

① 失効手続き

- 失効決定までの手続き

  上記の失効事由が存在することを確認し失効決定までの手続きであり、なにをもって確認し、どのような手続きで決定するかを具体的に規定することが望ましい。また、決定にあたっては相互認証に関わっている認証局当事者が、関与する必要がある。

  相互認証書の重要性を考慮し、確実かつ迅速に行えるルールが望ましい。

② 失効を行う手続き

上記失効決定に基づき、具体的に失効を行う手続きであり、失効リストの形式、失効リストの作成、失効リストの配布、及びエンドエンティティにおける失効リスト参照の技術的方法を規定する必要がある。

失効リストの作成及び失効リストの配布規定については、相互認証書の重要性を考慮し、失効リストの作成者・作成方法・確認方法及び全てのエンドエンティティがその失効を確認できることを前提とした配布方法を具体的にしておくことが望ましい。

③ 失効を公開する手続き

前項の失効リストのエンドエンティティへの配布とは別に、失効を利用者に公開する手続きである。公開は失効決定から遅延なく行い、且つできる限り一般的手段が望ましく、且つエンドンティティに公開の手段をあらかじめ通知しておくことが望ましい。

3.5.2 相互認証の解消

相互認証は、複数の認証局が関係するので相互認証解消の可能性が考えられる。そこで、エンドエンティティの利便性を考慮し、相互認証開始に当たり、相互認証解消の条件・手続き・解消後の相互認証の扱い等について事前に取り決めると同時に利用者に公開する必要がある。

4 技術要件

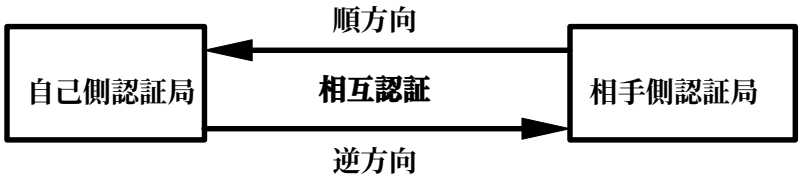
本章では、相互認証を実装する場合の技術的観点から、相互認証書形式、相互認証インタフェース及び CRL 運用について規定する。

4.1 認証書およびＣＲＬ形式

ディレクトリに保持される認証書の形式は X.509 で次の３つの属性に分類されている。

（１） ユーザ認証書**UserCertificate**
（２） 認証局認証書**CACertificate**
（３） 相互認証書　**CrossCertificatePair**

本章で規定する相互認証書は X.509 で定義する相互認証書（Cross-Certificate-Pairs）の属性を前提とし、順方向と逆方向の相互認証を定義している。
順方向とは相手側の認証局から自己側の認証局に対する認証を行い、逆方向とは自己側から相手側に対する相互認証をいう。順方向／逆方向の相互認証書は少なくともいずれか一方のみ存在すればよく、どの方向の相互認証を行うかは各認証局のポリシーによる。



4.1.1 認証書形式

認証書には大きく分けて X.509 認証書フォーマットの基本部（V1）と拡張部（V3）があり、相互認証書では基本部及び V3 拡張部を用い実現を行う。また、V3 拡張部の各フィールドに関して定義する必要のあるもの（実装規約）について規定する。

4.1.2 認証書標準形式

X.509（V3）で定義されている認証書の形式を相互認証書に適用する各フィールドの実装条件について規定する。

相互認証実装規約（基本部及びＶ２拡張部）

○：使用する、　　×：使用しない

区分	フィールド	相互認証 実装規約
基本部	バージョン番号（version）	○(V3)
	シリアル番号（serial Number）	○
	署名情報（signature） ・AlgorithmIdentifier	○
	発行者名（issuer）	○
	有効期間（validity） ・notBefore　・notAfter	○
	所有者名（subject）	○
	所有者公開鍵情報 （subject Public Key Info） ・AlgorithmIdentifier	○
V2 拡張部	発行者特定識別子 (Issuer Unique Identifier)	×
	所有者特定識別子 (subject Unique Identifier)	×

一般認証書と比較し、特に相互認証書において必要なフィールドは以下の通り。

●バージョン番号(version)
相互認証実装規約では Version ３(version=２)を使用する。

●シリアル番号(serial Number)
相互認証の認証経路を検証するために使用する（詳細は 4.2.3.1 章を参照）。

●発行者名（issuer)
相互認証を行う認証局名はユニーク性が必要であるため、発行者名にて行うことを推奨する。
また、相互認証の認証経路を検証するためにも使用する（詳細は 4.2.3.1 章を参照）。

4.1.3 相互認証拡張部分

相互認証実装規約として、認証書の検証を確実に行うために必要なフィールド以外については、使用任意とする。ポリシー等を反映させるフィールド等については、相互認証した場合に各認証ドメインのポリシーを反映するために使用することが将来的な目標であるが、現状各フィールドの使用方法等が曖昧な部分が多いため、使用任意とし運用管理者の合意によりポリシーの整合性を実現することが望ましい。

相互認証実装規約（V3 拡張部）

○：使用する、 △ :使用任意　 C=: クリティカリティ、Y=認識、N=無視

区分	フィールド	クリティカル	相互認証実装規約	
鍵及びポリシー情報	認証局鍵識別(Authority KeyIdentifier)	無視	○(C=Y)	
	---鍵識別情報(KeyIdentifier)		○	×
	---認証書発行者名(authorityCertIssuer)		×	○
	---シリアル番号(authorityCertSerialNumber)		×	○
	所有者鍵識別(Subject Key Identifier)	無視	△	
	鍵種別(Key Usage)	任意	△(C=Y)	
	秘密鍵使用期間(Private Key Usage Period)	任意	△(C=N)	
	認証局ポリシー(Certificate Policies)	任意	△(C=Y)	
	---ポリシー識別(policyIdentifier)		△	
	---ポリシー権限(policyQualifiers)		△	
	ポリシー関連付け(Policy Mappings)	無視	△(C=Y)	
認証書所有者属性	所有者別名(Subject Alternative Name)	任意	△(C=N)	
発行者属性	発行者別名(Issuer Alternative Name)	任意	△(C=N)	
	所有者ディレクトリィ属性 (SubjectDirectoryAttributes)	無視	△(C=N)	
認証経路の制限	基本制限(Basic Constraints)	任意	△(C=Y)	
	---認証局(cA)		△	
	---認証経路制限(pathLenConstraint)		△	
	名前制限(Name Constraints)	任意	△(C=Y)	
	---許容サブツリー(permittedSubtree)		△	
	---除外サブツリー(excludeSubtree)		△	
	ポリシー制限(Policy Constraints)	任意	△(C=Y)	
	---ポリシーセット(policySet)		△	
	---明示的ポリシー要求(requireExplicitPolicy)		△	
	---ポリシー関連付禁止(inhibitPolicyMapping)		△	
ＣＲＬ識別	ＣＲＬ配布元(CRL Distribution Points)	任意	△(C=N)	
	---配布元(distributionPoint)		△	
	---理由(reasons)		△	
	---ＣＲＬ発行者(cRLIssuer)		△	

一般認証書と比較し、特に相互認証において必要なフィールドは以下の通り。

●認証局鍵識別(AuthorityKeyIdentifier)
鍵識別情報(KeyIdentifier)または認証書発行者名(authorityCertIssuer)、シリアル番号(authorityCertSerialNumber)を相互認証として認証経路の検証として使用する。
●認証局ポリシー(CertificatePolicies)
各認証局として相互認証ポリシーとして使用することを推奨するが、本書としては必須としない。
●ポリシー関連付け(PolicyMappings)
発行元認証局の相互認証ポリシーが同等であるか記述し、認証経路などで検証することを推奨するが、本書としては必須としない。

4.1.4 CRL 形式

相互認証書の CRL 形式フィールドは以下の通りであり、相互認証書を意識して記述する必要のあるフィールドは特にない。

Version	フィールド	相互認証 実装規約
V1	署名方式(**signature.algorithmIdentifier**)	○
	ＣＲＬ発行局名(**issuer**)	○
	ＣＲＬ発行日時(**thisUpdate**)	○
	発行予定日時(**nextUpdate**)	○
V2	バージョン番号(**version**)	○
	認証確認用識別子(**authorityKeyIdentifier**)	○
	発行通し番号(**cRLNumber**)	○
	配布局と性質(**issuingDistributionPoint**)	○
	デルタＣＲＬ識別(**deltaCRLIndicator**)	○
V1	認証番号(**certificateSerialNumber**)	○
	失効申請受理番号(**revocationDate**)	○
V2	失効理由(**reasonCode**)	○
	一時利用中止対処方法(**holdInstructionCode**)	○
	危害日時(**invalidityDate**)	○
	認証発行局名(**certificateIssuer**)	○

4.2 相互認証インタフェース

本書においては、特定の認証書管理プロトコル、ビジネスプロトコルを想定せず、汎用的な相互認証を実現するためのガイドラインとする。
この目的のために、相互認証インタフェースを次のレベルで記述する。

①相互認証を実現するためにエンティティ間で転送が必要となる情報を示す。特定のプロトコルに依存しないように、認証の本質的な技術要素として記述する。
②①で転送する情報の処理の考え方を記述する。

規定するインタフェースは、次の２つとする。

●認証インタフェース（認証局・エンドエンティティの認証書取得）の実装
●CRL 配布インタフェース

4.2.1 認証インタフェースの規定

4.2.1.1 相互認証書の管理

相互認証を実現するために、認証局認証書、ユーザ認証書に加えて相互認証書を使用する。相互認証書を各エンティティに配布することが必要となるが、このためには２つの方式が可能である。

- 認証局にレポジトリ機能を実装する方式
  各エンティティが相互認証書を利用する場合に認証局のレポジトリ機能にアクセスして相互認証書を取得する方式である。レポジトリ機能としては、LDAP 等の標準的なインタフェースを想定し、本書では特定のレポジトリ機能を想定しない。
- 認証書管理プロトコルで実装する方式
  認証書管理プロトコルに、相互認証書をユーザ認証書発行のメッセージに添付して、認証局－エンドエンティティ間で転送する方式である。
  このためには、メッセージフォーマットを規定する必要がある。
  考え方として、認証局－エンドエンティティ間のメッセージは改竄、なりすましを防止するために認証局による署名データ形式をとる。相互認証書を添付する場合には、ユーザ認証書と共に相互認証書をリスト形式で配布することとする。

4.2.2 認証局における実装

4.2.2.1 認証局にレポジトリ機能を実装する方式

- 認証局は、発行した相互認証書,CRL を管理し、レポジトリとして相互認証書をアクセスするサービスを実装する必要がある。対象としては、相互認証書、CRL とする。
- 認証局は、発行した相互認証書をレポジトリ管理し、他認証局、エンドエンティティからのアクセスに対して相互認証書を配布する必要がある。
- 認証局は、発行した相互認証書の有効期限が切れた場合にレポジトリから削除しレポジトリ対象外とする必要がある。
- 認証局は、相互認証書を無効化する必要が発生した場合に、相互認証書をレポジトリから削除しレポジトリ対象外とすると共に、CRL を作成しレポジトリに登録し、認証局、エンドエンティティからのアクセスに対して CRL を配布する必要がある。

4.2.2.2 認証書管理プロトコルで実装する方式

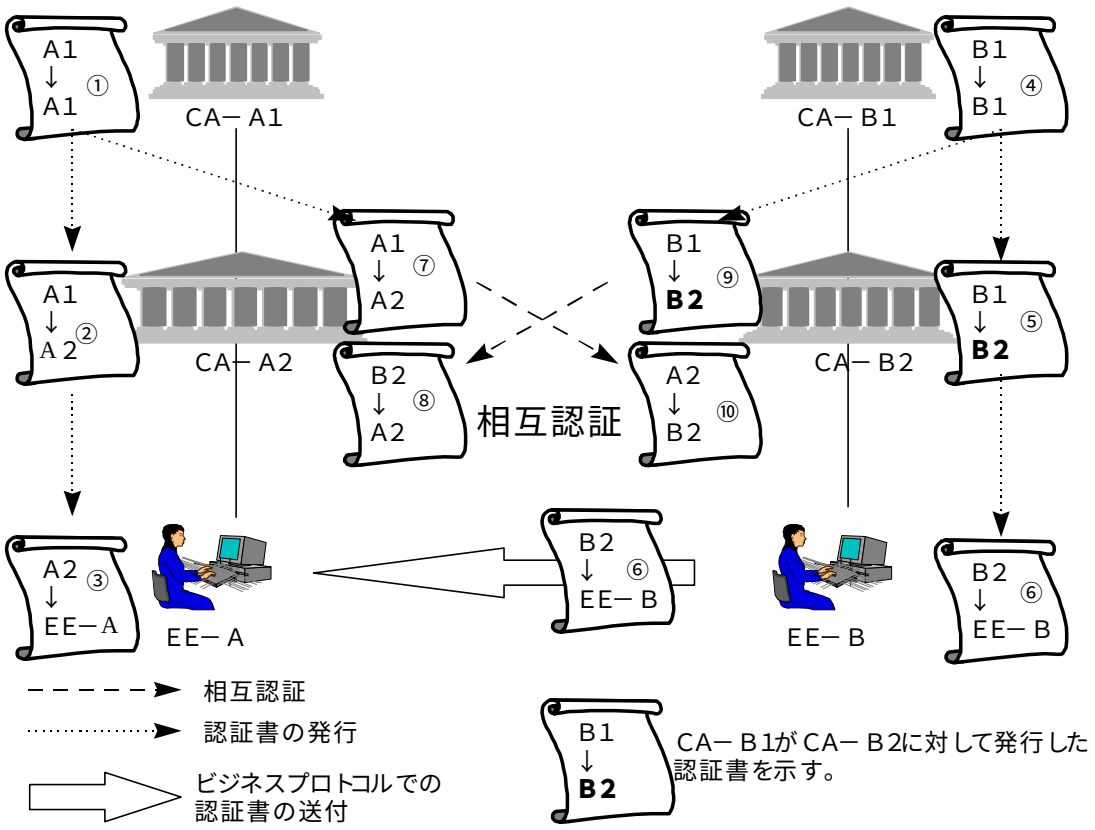
- 認証局がエンドエンティティに対して、認証書を発行するメッセージに相互認証書を添付する機能を実装する必要がある。
- 相互認証書の CRL を発行する機能を実装する必要がある。
- 相互認証書の管理機能を実装する必要がある。１つの認証局は相互認証する複数の認証局との相互認証書を管理しなければならない。エンドエンティティに対してユーザ認証書を発行する時点で、認証局が保持する全ての相互認証書をメッセージに添付してエンドエンティティに配布しなければならない。相互認証書のデータ量が大きくなること防ぐために、指紋(fingerprint)による転送データ量の削減等の改善は、各認証プロトコルの実装において可能とする。

4.2.3 エンドエンティティにおける実装

4.2.3.1 認証書の検証機能の考え方

エンドエンティティは、ビジネスプロトコル実行時に相手エンティティの認証書を検証する必要がある。認証書の検証は相互認証のない場合にも実行するが、相互認証を行う場合には相互認証書を含めた検証が必要となる。
次頁の図は相互認証を行う形態での認証書の検証の考え方を示している。
エンドエンティティ A とエンドエンティティ B が接続する場合、エンドエンティティ A における認証書の検証を例とする。（この例では相互認証を行う CA は相互認証書に署名するために、下位エンティティに署名するための鍵ペアと別の鍵ペアを使用するケースを想定している。）

エンドエンティティ A はエンドエンティティ B から送付された認証書⑥を検証する。認証書⑥→⑤→④と認証書チェインを検証するが④(ルート CA-B1)まで検証しても自己認証ドメインの①(ルート CA-A1)と一致しないため、次の相互認証による検証を行う。
具体的にはエンドエンティティ A の保持する相互認証書から CA-B1、CA-B2 に対して発行した認証書を検索し、認証書⑩を求める。
次に認証書⑩の検証を行う。認証書⑩→⑦→①とチェインを検証し自己認証ドメインのルート CA-A1 へのチェインが確認されることにより検証を完了する。



認証書の検証機能の考え方

4.2.3.2 認証書の検証機能の実装

前項に述べた認証書の考え方に従った実装方式について記述する。ただし、相互認証書の検証方式についてはここで示す方式以外も可能であり、実装例として記述する。

- エンドエンティティは、まず相互認証のない自身の認証ドメイン内の相手との認証書検証手順を実行する。認証経路に従ってルート認証局まで検証した結果、失敗した場合には、以下に示す相互認証の検証を行う必要がある。
- エンドエンティティは、相手エンドエンティティのユーザ認証書および認証経路に従ったルート認証局までの認証局認証書の発行者名を全て取り出す。
- 取り出した発行者名の少なくとも一つが、エンドエンティティの所持する相互認証書の所有者名と一致する場合には、その相互認証の認証経路の検証を行う。
  相互認証書の認証経路の検証は、最低次の項目の検証を行うことが必要である。

- 相互認証書の発行者名(issuer)がエンドエンティティの認証経路上に存在する認証局認証書の所有者名(subject)と一致すること。[相互認証書を発行した認証局の一致]
- 相互認証書の認証局鍵識別(Authority Key Identifier)の鍵識別情報(KeyIdentifier)がエンドエンティティの認証経路上に存在する認証局認証書の所有者鍵識別(SubjectKeyIdentifier)と一致する。または、相互認証書の認証局鍵識別(Authority Key Identifier)の認証書発行者名(AurhorityCertIssuer)およびシリアル番号(authorityCertSerialNumber)が、エンドエンティティの認証経路上に存在する認証局認証書の発行者名(issuer)およびシリアル番号(serialNumber)とそれぞれ一致すること。[相互認証書を発行した認証局認証書の一致]

上記の検証を完了した場合にポリシーの確認を行う。

- ポリシーの確認は、認証書のポリシー記述フィールドを使用しているドメインのエンドエンティティのみが行う。認証書に対するポリシーの反映方法は、次のようなフィールドを使用することが一般的である。
- certificatePolicies
- policyMapping

ただし標準的な規定はされていないため、本書では相互認証する相互の認証ドメインが認証書に含まれるポリシー記述フィールドを解釈可能であることを前提とする。一方の認証ドメインのみがポリシー記述フィールドを使用する場合には、相互認証を行う前に両認証ドメインの管理者が合意することが必要である。

4.2.3.3 相互認証書の管理機能

- 認証局にレポジトリ機能を実装する方式では、認証局認証書、ユーザ認証書の検証処理において相互認証書の検証が必要となった時点で、認証局にアクセスして相互認証書を取得する機能を実装する必要がある。
- 認証書管理プロトコルで実装する方式では、認証局－エンドエンティティ間メッセージに格納された相互認証書を認識する機能を実装する必要がある。

4.2.3.4 相互認証書の保管・管理機能

認証局から取得したまたは、認証書管理プロトコルに添付された相互認証書を保管・管理する機能を実装する必要がある。

4.2.3.5 相互認証書無効化機能

- 無効化された相互認証書を削除する機能を実装する必要がある。
- 相互認証書の CRL を処理する機能を実装する必要がある。

4.3 CRL 運用

4.3.1 検討要件

認証局およびエンドエンティティの認証書を無効にする場合の運用を規定する必要がある。相互認証のない世界では、それぞれのビジネスモデルの一部として規定されるべきものである。相互認証があるとそれぞれサービスが異なるため、必要となる共通的要件を規定する。

例えば、緊急性に対する要件がビジネスモデル毎に異なる。CRL 作成・配布に要する時間が 0 でないため、CRL 配布が完了するまでサービスを停止し、配布完了後にサービスを再開する運用がある。この場合、CRL を作成する認証ドメインはサービス停止が可能であるが、相互認証している認証ドメインは CRL 発行ドメインからの通知を受けるまで停止ができない。また停止が不可能な運用者もあり、相互接続時に解決すべき要件となる。

4.3.2 CRL 配布インタフェースの実装

相互認証書の失効は、相互認証書に含まれる認証局認証書の失効により実現するため、相互認証書の CRL は存在せず、認証局認証書の CRL 管理に依存する。

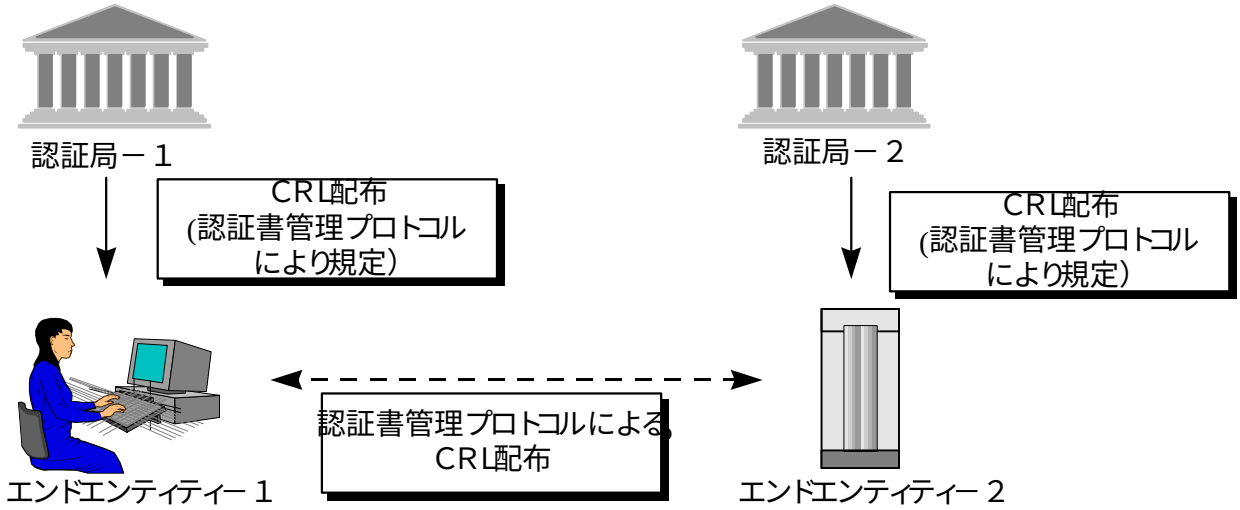
各認証局、エンドエンティティが相互認証書の有効性を確認するためには、認証局認証書の CRL を参照する必要がある。
各認証ドメインの採用しているプロトコルまたは運用による CRL 配布は、同一認証ドメイン内のエンティティに対する配布を規定しているのみであり、相互認証している異なる認証ドメインに対しての CRL 配布についての規定が必要である。

4.3.2.1 認証局がレポジトリ機能を実装する場合

認証局がレポジトリ機能を実装する場合には、CRL を認証局から配布することが可能である。この場合、CRL が随時更新される可能性があるため、各エンティティは CRL を最新の状態に保つ必要がある。各エンティティは、そのポリシーに従う頻度で認証局から CRL を取得する。

4.3.2.2 認証局がレポジトリ機能を実装しない場合

認証局がディレクトリサービス機能を実装しない場合には、認証書管理プロトコルにより CRL を配布する方式を必要とする。（下図参照）
CRL 配布を実施しない設計となっている認証書管理プロトコルを使用して相互認証を行うことは、相手認証ドメインのエンティティに対して信用度レベルを低下させる可能性があり、相互接続を行うべきではない。または事前に両認証ドメインの管理者が合意しておく必要がある。



認証書管理プロトコルによるCRL 配布

5 付録

5.1 付録A：参考資料

(1)電子商取引実証推進協議会、「認証局運用ガイドライン（アルファ版）」1997.3

(2)電子商取引に関する検討課題について(電子商取引環境整備研究会中間報告), 通商産業省, 1996.4
"http://www.ecom.or.jp/miti/press960423.html"

(3)暗号認証技術を利用した鍵管理システムの調査研究, 認証実用化実験協議会(ICAT), 1996.3.14
[ICAT ホームページ: "http://www.icat.or.jp/"]

(4)情報システム安全対策基準解説書、(社)情報サービス産業協会、1996．10

(5)コンピュータ不正アクセス対策基準解説書、（財）日本情報処理開発協会、1996．11

(6)ISO/IEC 9594-8：1995| ITU-T Recommendation X.509(1993E), Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1993.11
[案内："http://www.itu.ch/itudoc/itu-t/rec/x/x500up/x509_27505.html"]

(7)D. Solo,Russ Housley,Warwick Ford,T.Polk, Internet Public Key Infrastructure X.509 Certificate and CRL Profile
"http://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki-part1-06.txt"

(8)Internet X.509 Public Key Infrastructure Operational Protocols,1998.1
“http://www.internic.net/internet-drafts/draft-ietf-pkix-ipki2opp-06.txt”

(9)S.Farrell, C Adams , Internet Public Key Infrastructure Certificate Management Protocols, 11.19.1997
"http://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki3cmp-06.txt"

(10)Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework,1997.9.30
“http://www.internic.net/internet-drafts/draft-ietf-pkix-ipki-part4-02.txt”

(11)Federal Public Key Infrastructure Technical Specifications Part A: Requirements, NIST, 1996.1.31
"http://csrc.ncsl.nist.gov/pki/require5.ps"

(12)Federal Public Key Infrastructure Technical Specifications Part B: Technical Security Policy, NIST, 1996.1.24
"http://csrc.ncsl.nist.gov/pki/tspolicy.ps"

(13)Burr, Federal Public Key Infrastructure Technical Specifications Part C: Concept of Operations, NIST, 1996.2.12
"http://csrc.ncsl.nist.gov/pki/conops.ps"

(14)Federal Public Key Infrastructure Technical Specifications Part D: Interoperability Profile, NIST, 1995.9.27
"http://csrc.ncsl.nist.gov/pki/cross.ps"

(15)Santosh Chokhani and Warwick Ford, The Certificate Policy and Certification Practice Statement Framework(Draft), NIST, 1996.11.3
"http://csrc.ncsl.nist.gov/pki/docs/fmk03nov.doc"

(16)Minimum Interoperability Specifications for PKI Components (MISPC),NIST, 1997.6.5
“http://csrc.ncsl.nist.gov/pki/mispcv1.doc”

(17)VeriSign Certification Practice Statement, VeriSign, Inc., 1996.8.7
"http://www.verisign.com/repository/CPS/"
(18)Netdox secured assured notarized insured
“http://www.netdox.com/Nocorporate.html”
(19)White Paper: Secure LDAP: Making better use of digital certificates
“http://www.xcert.com/support/papers/SecureLDAP.html”
(20)Commerce Net
“http://www.commerce.net/index.html”
(21)Secure Electronic Transaction(SET)Specification Book2:Programmer's Guide Draft for testing(96/6)

5.2 付録Ｂ：ＳＥＴにおける有効期限の考え方

SET では、秘密鍵及び認証書の有効期限に関し、以下のように推奨している。

秘密鍵の最長有効期限

エンティティ	メッセージ署名	鍵交換	認証書署名	ＣＲＬ署名
カード会員	３年	－	－	－
加盟店	１年	１年	－	－
ペイメントゲートウエイ	１年	１年	－	－
ＣＣＡ	１年	１年	１年	－
ＭＣＡ	１年	１年	１年	－
ＰＣＡ	１年	１年	１年	１年
(ＧＣＡ)	１年	１年	１年	１年
ＢＣＡ	１年	１年	１年	１年
ＲＣＡ	１年	１年	１年	１年

認証書の最長有効期限

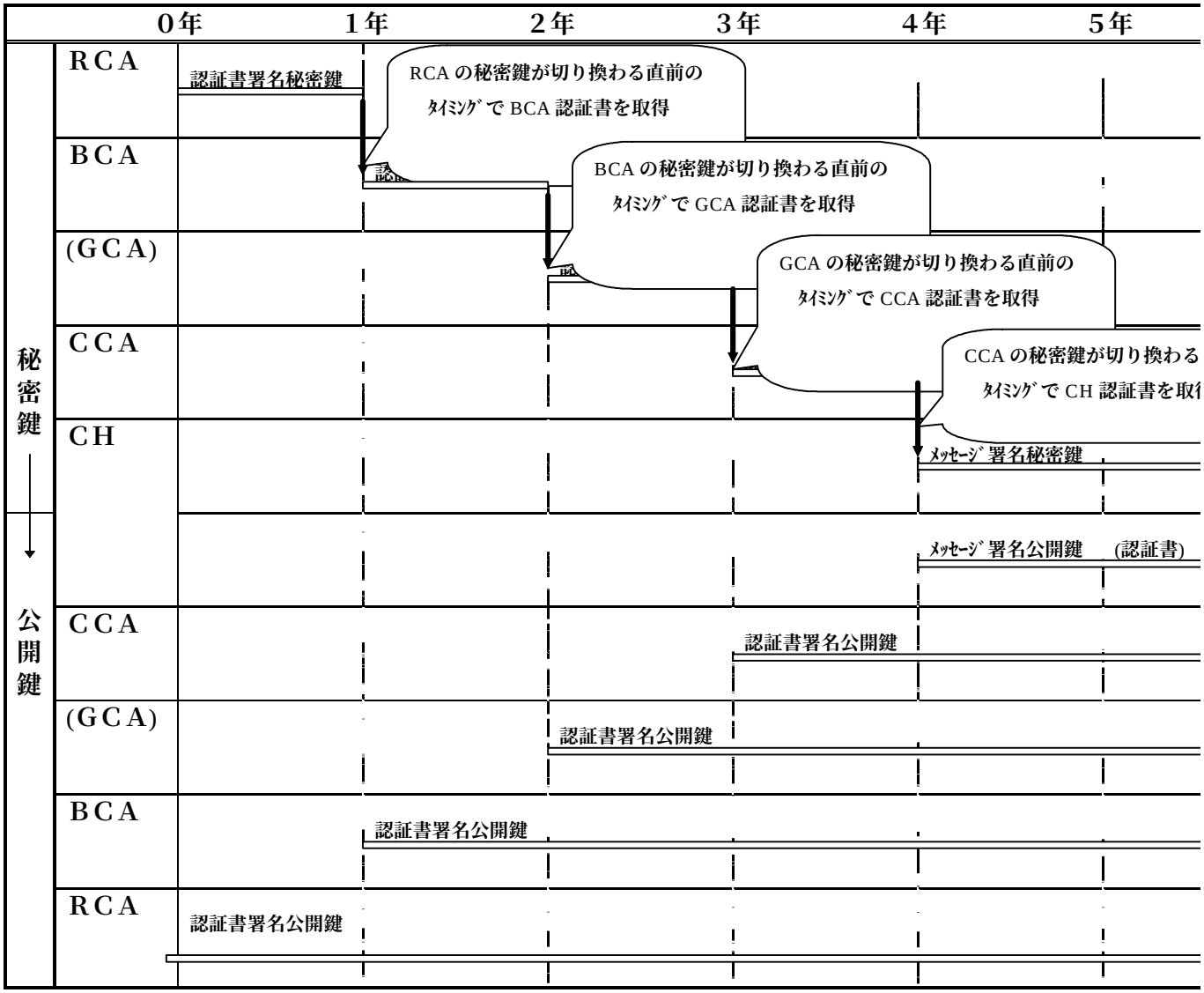
エンティティ	メッセージ署名	鍵交換	証明書署名	ＣＲＬ署名
カード会員	３年	－	－	－
加盟店	１年	１年	－	－
ペイメントゲートウエイ	１年	１年	－	－
ＣＣＡ	１年	１年	４年	－
ＭＣＡ	１年	１年	２年	－
ＰＣＡ	１年	１年	２年	２年
(ＧＣＡ)	－	－	５年	２年
ＢＣＡ	－	－	６年	２年
ＲＣＡ	－	－	７年	２年

SET 制約事項

秘密鍵有効期限 ≦ 認証書有効期限

→秘密鍵無効後も認証書の公開鍵を使った署名の検証は許される。

有効期限の関連（例:カード会員）



VISA/Master が委託した RCA の認証書署名公開鍵の有効期限が 7 年であることから、CH 認証書有効期限は最大 3 年となる

5.3 付録Ｃ：相互認証の形態

海外における相互認証の代表的なものには以下のような形態がある。

	FPKI (NIST)	信用機関 (NetDox)	Cross Authentication (XCert)	金融機関相互認証 (Commerce Net)
構成要素	CA 相互認証書	中継システム（ハブ） [E-Mail ベース送受信] （CA）	PA／DA（CA相当） [SSL＋LDAP]	CDS CI（＝S／MIME） CA
相互認証手順	① すべての認証局間相互認証書を事前に発行 ② ユーザ間でユーザ認証書と相互認証書を交換	① ﾕｰｻﾞはCAから認証書を事前発行 ② NetDox 社は各 CA を事前確認 ③ ﾕｰｻﾞA,B は NetDox 社に登録 ④ ﾕｰｻﾞA は中継局（ﾊﾌﾞ）へ送信 ⑤ NetDoxﾊｯｼｭを付加しﾕｰｻﾞBへ転送 ⑥ ﾕｰｻﾞBはﾊｯｼｭを確認 ⑦ ﾕｰｻﾞAへﾕｰｻﾞBの受信通知送付	① 前相互認証 ② ｸﾗｲｱﾝﾄからｻｰﾊﾞへｱｸｾｽ要求 ③ ｻｰﾊﾞからPAへｸﾗｲｱﾝﾄ確認要求 ④ PA<->DA間でSSL+LDAPでｸﾗｲｱﾝﾄ認証ﾃﾞｰﾀ転送 ⑤ ｻｰﾊﾞでｸﾗｲｱﾝﾄ認証ﾃﾞｰﾀ確認 ⑥ ｻｰﾊﾞからｸﾗｲｱﾝﾄへ結果を送信	① Cust は YCA から認証書を事前発行 ② 最寄りの金融機関 XCA へｱｸｾｽ ③ Cust の Y 発行認証書をｵﾝﾗｲﾝ確認 ④ YCA は XCA へ確認結果を応答 ⑤ XCA は Cust へ結果を返信
モデル構成図				

5.4 付録D：第3者機関を仲介する方式

5.4.1 第3者機関としてのレポジトリと中継ハブの役割

レポジトリとは、複数の認証局の認証書情報を第３者的に保管・管理し、それらの認証局に属するエンドエンティティに対しその情報を提供するエンティティであり、中継ハブは第3者的に管理している情報を使用し認証を行う主体となるエンティティである。

第3者機関として存在することのメリットは、認証書やCRL(Certificate Revocation List)の配布が複数の認証局をまたがって１カ所で行うことができることにある。特にCRLに関しては、認証を受ける側が自分にとって不利な情報を相手に渡すことになるため第3者機関の存在は重要である。

5.4.2 第3者機関としてのレポジトリと中継ハブの認証

第3者機関としてのレポジトリや中継ハブは、認証書の情報を提供する認証局から認証され認証書を発行してもらわなければならない。

5.4.2.1 レポジトリの認証

レポジトリはそれぞれの認証局と外部から完全に独立した接続が確保できない場合は、認証書情報の格納時に情報の提供者であるそれぞれの認証局もしくはその配下のレポジトリを認証し、認証書情報のなりすましや改竄を防がなければならない。

レポジトリはエンドエンティティへの認証書情報提供時に認証されなければならない。レポジトリは、エンドエンティティより認証を受け、情報の提供時にはなりすましや改竄を防がなければならない。また、レポジトリへの参照情報が傍受される事を防ぐ必要がある場合には、暗号化しなければならない。レポジトリは複数の認証局より認証書の発行を受けるため、情報を参照するエンティティに対し適切な認証書を提示しなければならない。

レポジトリはエンドエンティティが参照できる情報を制限する場合には、エンドエンティティを認証しなければならない。

5.4.2.2 中継ハブの認証

レポジトリの場合の時と同様に中継ハブは、認証書情報の格納時に認証書情報の提供者である認証局を認証し、なりすましや改竄を防がなければならない。

中継ハブは、発信元エンドエンティティから中継すべきデータを受け取る際に、エンドエンティティを認証しなければならない。

中継ハブは送信先エンドエンティティへ送信する中継データを認証しなければならない。中継ハブが発する中継情報は、相互認証時にエンドエンティティが属する認証局から発行された認証書を使用して、エンドエンティティより認証を受け、なりすましや情報の改竄を防がなければならない。

5.4.3 第3者機関としてのレポジトリと中継ハブへの情報転送インターフェイス

第3者機関はX.500ディレクトリもしくはそれを簡略化したものであり、認証局の認証書及びCRL(Certificate Revocation List)情報がオンラインで転送される場合のインターフェイスは、それに関連して規定された通信プロトコルおよびデータフォーマットを使用する。通信路の安全性が確保できない場合には、情報を暗号化し署名を付加した通信を行わなければならない。

5.4.4 第3者機関としてのレポジトリと中継ハブへの情報転送運用

認証局は第3者機関に対し、認証書及びCRLの更新情報を、相互認証締結時に規定した期間内に転送しなければならない。第3者機関は認証局から転送された更新情報を、相互認証締結時に規定した期間内に提供しなければならない。

5.4.5 ユニーク性の保証

第3者機関に複数の認証局の情報が格納されている場合、それぞれの認証局のDistinguished Nameは、ユニークに識別可能でなければならない。

5.4.6 性能に関する技術要件

第3者機関は、安定した運用ができる十分な処理能力を持ち、多重化されていなければならない。

また、第 3 者機関が各認証局と取り交わす認証書は、そのサービスに見合う十分な長さの鍵長を持っていなければならない。
第 3 者機関として 2 つのモデルを提示したが、そのモデルごとに性能上のボトルネックとなる処理について、性能を維持するための技術要件を示す。

5.4.6.1 レポジトリの場合

認証書は頻繁に更新されるものではないため、同一の認証書の検証のために毎回レポジトリに問い合わせを行うことはレポジトリの負荷を不必要に高める原因となる。このため、レポジトリに問い合わせを行うアプリケーションは、認証書をある一定期間キャッシュして使用する事が望ましい。しかしながら、CRL のキャッシュは認証書の安全性を損なう可能性があるため、キャッシュを行わないか、キャッシュを行うのであれば認証書が提供するサービスに見合う必要最低限の期間にすべきである。

5.4.6.2 中継ハブ相当の場合

中継ハブは認証処理からデータへの署名といった処理を全て行うため、システム全体の性能を低下させるボトルネックとなりやすいエンティティである。システムの稼働率を維持するためにも、安定した運転が保証されなければならない。
このため中継ハブは、その負荷の分散、システム停止の危険を回避するための多重化、定期的なシステムのバックアップが運用時の必要条件となる。

5.5 付録Ｅ：SET 相互認証技術[1]

Secure Electronic Transaction（SET）は米国のビザとマスターカードとが共同で開発したカード決済プロトコルで、認証プロトコルと支払プロトコルの２つを定義している。
また、SET では多くの仕様がオプションの扱いになっており、これらのオプションの実装が異なる製品間ではその相互接続も難しいと想定される。(例えばカード所有者が認証書を持つかどうかがオプションになっている。)
SET の相互認証を検討する前に、これらのオプションの実装を事前に相互に確認される事を推奨する。
SET の認証プロトコルでは各ブランドごとに閉じた階層型の認証局構成を前提としている。最上位のルート認証書を何らかの方法ですべてのエンドシステムに事前に組み込むことを前提とし、支払プロトコルにおいて相手の認証書を最初に検証する。相手認証書の検証は、認証局の認証書およびその上位のすべての認証書をルート認証書まで検証する。各カードブランドごとに閉じた認証システムを構成し、異なるカードブランド間の相互接続は対象としていない。このため SET には相互認証という考え方はなく、相互認証に関しては何も規定されていない。
ここでは、まず SET で相互認証を行うとした場合を想定した技術的な検討課題を整理し、次にこの検討課題を解決することができるとして、SET における相互認証の構成及び相互認証書の形式を定義する。さらに、SET における相互認証書の交換手順と支払プロトコルにおける相互認証書による認証手順について考察する。

5.5.1 SET 相互認証の課題

カード決済の現実世界を考えると、消費者側のカード所有者（CH）はある特定のカードブランドに加盟している。単一または複数のブランドに加盟できるが、カード決済の時には、どのカードブランドのカードで決済するかをカード所有者が決定しなければならない。一方、商店側の販売店（M）は通常複数のカードブランドと契約している。
販売店の規模にもよるが、理想的には主要なカードブランドのすべてに加盟する。
この現実世界でも、異なるカードブランド間の決済は想定されていないが、日本ではインターナショナル兼用のカードブランドの幾つかは、インターナショナルブランドが同じ場合には、日本のブランドが異なっている場合でも決済が可能である。

（1）ブランドの一致性に関する課題

SET の支払プロトコルでは最初の初期手順でカードブランド ID をカード所有者（CH）が販売店（M）に対して通知する。販売店（M）ではこのカードブランド ID に加盟しているかどうかを検証する。もし販売店（M）がカード所有者のカードブランドに加盟していない場合には支払い取引き不成立になると考えられる。もし加盟している場合には認証経路は両者で一致するため相互認証は使用しない。

（2）認証書の組織名

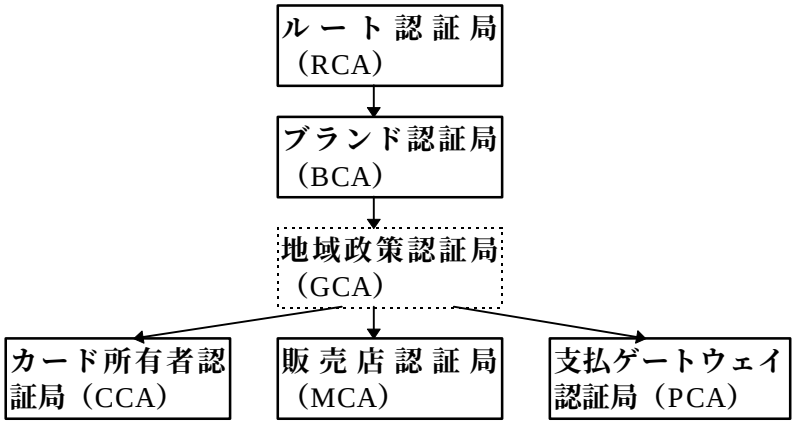
ブランドごとに閉じている現状の認証モデルを前提とする SET では、ブランドと認証書とが対応している。SET ではエンドシステム認証書の所有者名における X.500 識別名（DN）の組織名（O=）としてブランド ID を使用する。エンドシステム認証書の認証書発行者名（認証局）の組織名は認証局の組織名を使用する。認証書の検証においても相手組織名を事前に検証している可能性がある。

（3）SET 認証局の構成

SET の認証局はブランド全体を管轄するブランド認証局（BCA）とその上位に位置するルート認証

[1] 本項は、SETバージョン1.0が規定される前のドラフト版「SET Specification Book2:Programmer’s Guide Draft for Testing(96/6)」をベースに検討したものである。

局（RCA）から構成される。ブランドＣＡの下位に中間の認証局（オプション）である地域政策的CA（GCA）があり、その下位にエンドシステムを認証する３種類の CA がある。カード所有者認証書を発行する CCA、販売店認証書を発行する MCA、アクワイアラ支払ゲートウェイ認証書を発行する PCA から構成される。

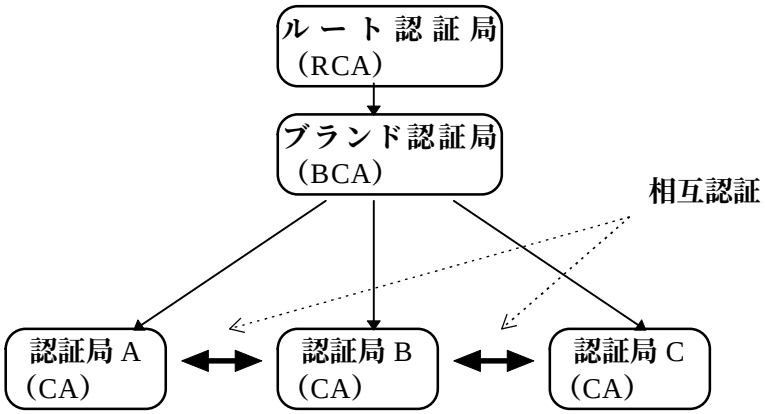


SET 認証局の構成

5.5.2 SET 相互認証の構成

SET 相互認証を行うとした場合の認証局システム構成について提案する。

SET ではブランド ID の一致がカード支払プロトコルの前提になっている。このため、異なるブランド間の相互認証を実現することが不可能と考えられる。SET で相互認証が可能なのは、同一ブランド内での支払取引で最短経路による相互認証のケースに限定される。このシステム構成例はつぎの通りである。



SET 相互認証システム構成例

5.5.3 SET 相互認証書の形式

X.509V3 で定義される部分の相互認証書の形式は、後述の相互認証書の実装規約で規定している内容と同じである。ここでは SET の仕様として独自に拡張された、SET 個別拡張部の相互認証書での形式についてまとめる。

認証書 SET 個別拡張部の構成

SET 個別拡張部	適用	クリティカル	拡張詳細情報	属性
ハッシュルート鍵 Hashed Root Key	ルート認証書	認識 (YES)	ダイジェストアルゴリズム ルート鍵の指紋	ＯＩＤ OctetString
認証書のタイプ Certificate Type	すべての認証書	認識 (YES)	認証書の種類 (認証局は複数指定可能)	BIT STRING
販売店データ Merchant Data	販売店認証書	無視 (NO)	販売店識別子 販売店アクワイアラＢＩＮ 販売店の名前 販売店の所在都市名 販売店の所在都道府県名 販売店郵便コード 販売店所在国名 販売店承認フラグ	CharacterString CharacterString CharacterString CharacterString CharacterString CharacterString CharacterString BIT STRING
カード所有者認証要否 Cardholder Certificate Required	支払GW認証書	無視 (NO)	カード所有者認証フラグ (認証書を持たないカード所有者のサポート可否)	Boolean
トンネリング Tunneling	支払GW認証局	無視 (NO)	トンネリングサポート トンネリングアルゴリズム	Boolean ＯＩＤ
ＳＥＴの格付け SET Qualifier	ルートを除くすべての認証書	認識 (YES)	ポリシー宣言掲示ＵＲＬ ポリシー宣言 Email ハッシュアルゴリズム ポリシー ポリシーダイジェスト 認証書発行ポリシー	IA5 String IA5 String ＯＩＤ OctetString IA5 String

(1) ハッシュルート鍵

ルート鍵のハッシュ（指紋）はルート認証書でのみ適用される。SET 相互認証では異なるルート認証局間の相互認証は有り得ない。実装規約では対象外とする。

```
hashedRootKey EXTENSION ::= { -- Only in root certificates
        SYNTAX          HashedRootKeySyntax
        IDENTIFIED BY   { id-set-hashedRootKey } }

HashedRootKeySyntax ::= RootKeyThumb

RootKeyThumb ::= SEQUENCE
        digestAlgorithm     DAlgorithmIdentifier -- (sha1)--、
        rootKeyThumbprint           Digest }
```

(2) 認証書のタイプ

認証書のタイプはすべての認証書で適用される。相互認証書においてもこの情報を適用する。

```
certificateType EXTENSION ::=
        SYNTAX                  CertificateTypeSyntax
        IDENTIFIED BY    { id-set-certificateType } }

CertificateTypeSyntax ::= BIT STRING
        card (0)、
        mer (1)、
        pgwy (2)、
        cca (3)、
        mca (4)、
        pca (5)、
        gca (6)、
        bca(7)、
        rca (8)、
        acq (9) }
```

(3) 販売店データ

この情報は販売店の認証書でのみ適用される。CA の相互認証では対象外である。

```
merchantData EXTENSION ::=
        SYNTAX          MerchantDataSyntax
        IDENTIFIED BY   { id-set-merchantData }}

MerchantDataSyntax ::= SEQUENCE
        merID           MerchantID、
        merAcquirerBIN  BIN、
        merName                 DirectoryString { 25 }、
        merCity         DirectoryString { 13 }、
        merStateProvince DirectoryString { 3 }、
        merPostalCode   DirectoryString { 14 }、
        merCountry      DirectoryString { 3 }、
        merAuthFlag     BOOLEAN DEFAULT FALSE }
```

(4) カード所有者認証要否･トンネリング

これらの情報は支払 GW でみ適用される。 CA の相互認証では対象外である。

```
cardCertRequired EXTENSION ::=
        SYNTAX                  BOOLEAN
        IDENTIFIED BY   { id-set-cardCertRequired }}

tunneling EXTENSION ::=
        SYNTAX                  TunnelingSyntax
        IDENTIFIED BY   { id-set-tunneling } }

TunnelingSyntax ::= SEQUENCE
        tunneling               BOOLEAN DEFAULT FALSE、
        tunnelAlgIDs    TunnelAlg }

TunnelAlg ::= SEQUENCE OF OBJECT IDENTIFIER
```

(5) SET の格付け

認証局のポリシーに関連する付加情報である。相互認証書においてもこの情報を適用する。

```
setQualifier EXTENSION ::=
        SYNTAX                  SETQualifierSyntax
        IDENTIFIED BY   { id-set-setQualifier } }

SETQualifierSyntax ::= SEQUENCE
        policyDigest    OCTET STRING (SIZE(16..20))、
        digestAlgorithm DAlgorithmIdentifier、
        terseStatement  IA5String (SIZE(1..150))、
        policyURL       IA5String、
        policyEmail     IA5String }
```

相互認証書 SET 個別拡張部の実装規約

SET 個別拡張部	適用	クリティカル	拡張詳細情報	相互認証実装規約
認証書のタイプ Certificate Type	すべての認証書	認識 (YES)	認証書の種類 (認証局は複数指定可能)	○
ＳＥＴの格付け SET Qualifier	ルートを除くすべての認証書	認識 (YES)	ポリシー宣言掲示ＵＲＬ	○
			ポリシー宣言 Email	○
			ハッシュアルゴリズムポリシー	○
			ポリシーダイジェスト	○
			認証書発行ポリシー	○

5.5.4 SET 相互認証書交換手順

SET ではエンドシステムと認証局間の認証書発行手順を規定しているが、認証局間の認証書の発行手順については対象外としている。相互認証における相互認証書の交換は認証局間で行われるため、以下に示す規定は SET の仕様には直接の影響をもたらすものではない。しかし、認証局の実装を容易にするため、仮想的に一方の認証局がエンドシステムのプロトコル相当の処理を実行する方式を前提とする。

SET の認証プロトコルでは、非同期型（メール等）と同期型（WWW 等）の２種類の手順が定義されている。いずれの形態も適用可能である。

(1) 非同期型相互認証プロトコル

双方の認証局が非同期に認証要求を発行し、それに対して双方が非同期に認証応答を返する。
事前準備に関しては本資料の対象外である。双方ともセキュアなメールを使用することを推奨する。

非同期型相互認証手順

(2) 同期型相互認証プロトコル

一方の認証局が相互認証手順を開始する。エンドシステムの場合と同様に認証開始手順を起動してから認証要求を開始する。

同期型相互認証手順

5.5.5 相互認証書による支払認証手順

カードホルダーと販売店、支払ゲートウェイ間で実行される SET の支払手順において、相手認証書の確認を行う。SET では支払開始手順で要求側（カードホルダー）が販売店に対して自認証書のセット（認証局の認証書を含む）を渡す。販売店はこの認証書のセットを使って認証ルートを検証する。この検証結果が可であれば、 販売店は同様に自認証書のセット（認証局の認証書を含む）をカードホルダーに渡す。カードホルダーもこの認証書のセットを使って認証ルートを検証する。
この認証書のセットの中に、相互認証書を含む場合の認証ルートの検証方法についてまとめる。
SET での認証ルート検証は通常ルート認証書まで確認するが、相互認証による検証は次の手順で行う。

【販売店が行うカードホルダーの検証】

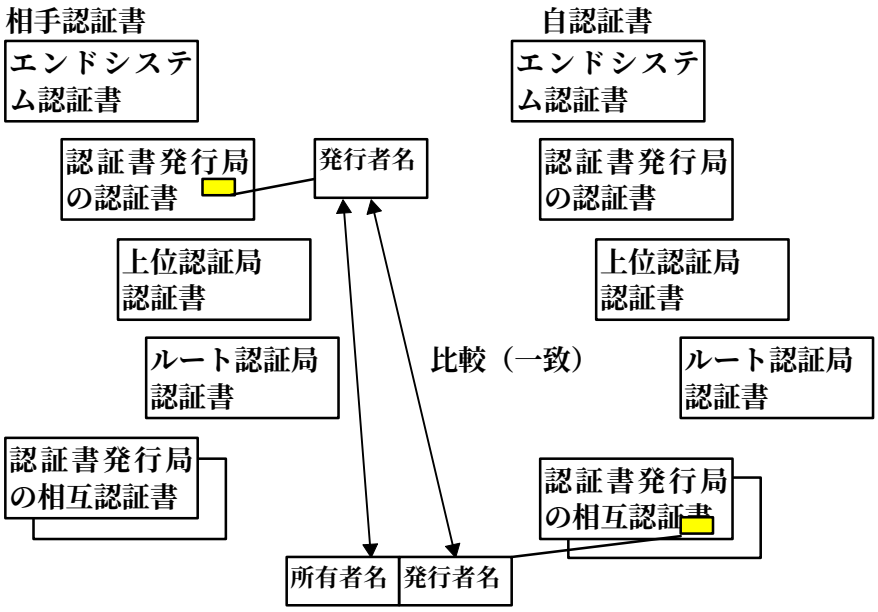
① 相手認証書のセットの中から、最初にカードホルダーの認証書を検証する。
② 次にカードホルダー認証書を発行した認証局の発行者名と、販売店自身が保有する認証局相互認証書の発行者名とを比較する。一致する相互認証書を検索する。
③ ②で一致する相互認証書が存在する場合、次に認証局相互認証書の所有者名がカードホルダー認証書の発行者名と一致するものがあるかどうかを検索する。

以上の手順のすべてで可となった場合には、カードホルダーの認証は完了したとみなす。
この手順は後述する、最短経路相互認証手順に相当する。

【カードホルダーが行う販売店の検証】

① 相手認証書のセットの中から、最初に販売店の認証書を検証する。
② 次に販売店認証書を発行した認証局の発行者名と、 カードホルダー自身が保有する認証局相互認証書の発行者名とを比較する。一致する相互認証書を検索する。
③ ②で一致する相互認証書が存在する場合、次に認証局相互認証書の所有者名が販売店認証書の発行者名と一致するものがあるかどうかを検索する。

以上の手順のすべてで可となった場合には、 販売店の認証は完了したとみなす。
この手順は後述する、最短経路相互認証手順に相当する。



支払手順における相手認証書検証方法

5.6 付録Ｆ：相互認証技術解説

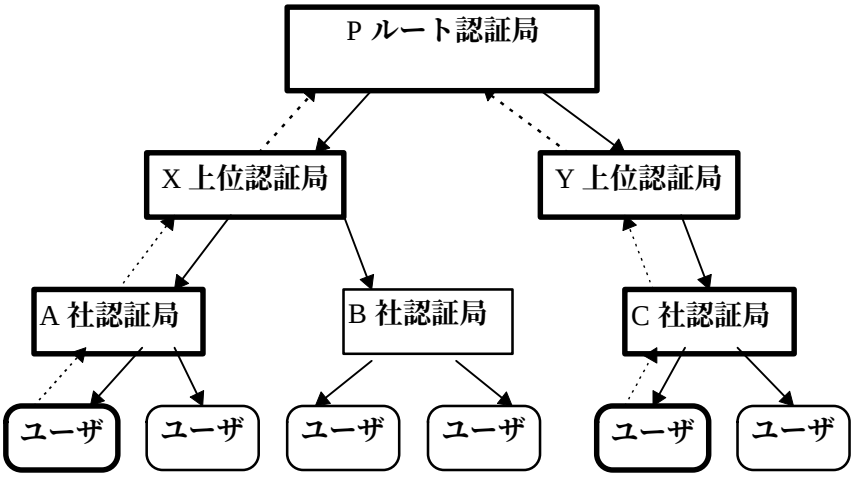
相互認証技術の基本となる方式を解説する。まず、IETF 等で最初に RSA 社が公開した階層型認証技術を紹介し、これと対比して相互認証技術を解説する。

5.6.1 階層型認証技術

認証書を発行する認証局（CA）の信頼性を保証するために、階層型の認証局モデルでは上位の認証局が下位の認証局を認証するという方式になっている。最上位の認証局をルート認証局といい、このルート認証局のルート認証書は自らがルート認証用の署名鍵で署名した自己署名認証書である。ルート認証書の署名鍵自体の認証書は存在しない。このため、ルート認証局は信頼できる第三者機関（TTP）として社会的かつ技術的な信頼性が必要とされる。

相手公開鍵の認証(Authentication)を行うための手段として認証書(Certificate)が提供される。この認証は認証経路(Certificate Path)に従って、最上位のルート認証書まで確認される。

階層型モデルでは、最上位のルート認証局はシステムで唯一の認証局である。相手認証書の検証はルート認証書まで正しく確認されれば認証経路の確認が完了する。



階層型モデルの認証経路

5.6.2 相互認証技術

階層型モデルにおけるシステムとしてつぎの２つが前提となっている。

① 最上位の認証局であるルート認証局はシステムで唯一。
② 認証経路は最上位のルート認証書まで確認。

システムによってはこの前提を実現することが困難なことがある。

① ルート認証局が同様のサービスを提供するシステムの中で唯一ではなく、複数存在する場合。
② 認証局の階層が多段になり、認証経路の確認に伴う性能上の問題が無視できない場合。
③ サーバシステムがクライアントの認証を行う場合で、処理すべき認証書の数が性能上無視できない場合など。（最短経路が必要とされるシステム）

相互認証における認証経路の確認は単体で実現されるシステムではなく、階層型の認証経路の確認と相互認証による認証経路の確認とが混在する形態が現実的である。この形態を前提とした相互認証による認証経路の確認方法はつぎの通りである。

【方式１】相互認証経路優先方式

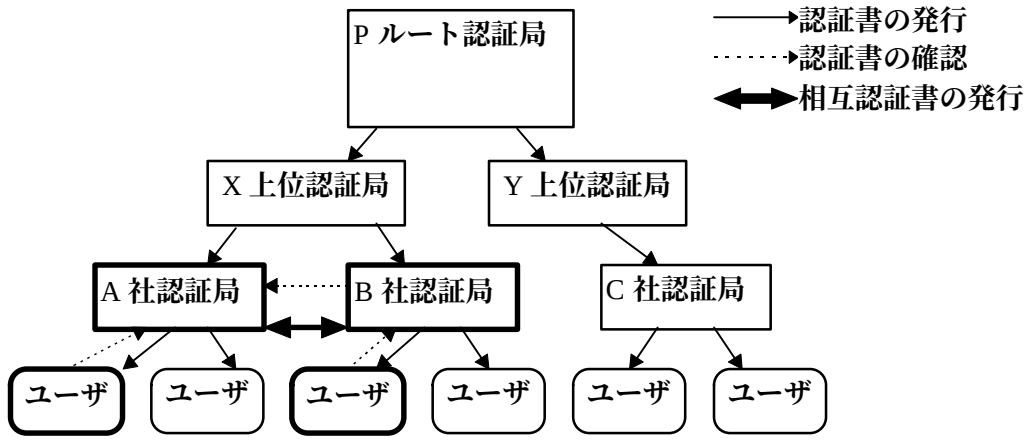
この方式は最短経路が必要とされるシステムに向いている。相手公開鍵の認証書を発行した認証局の認証書をすべて検証することなく、自公開鍵の認証書を発行した認証局の相互認証書の発行者が相手公開鍵の認証局認証書の発行者に含まれる場合には、認証経路の確認が完了とみなす。

【方式２】階層型認証経路優先方式

この方式は最短経路の確認が必要とされるシステムには向いていないが、ルート認証局がシステムで唯一でない場合の認証経路の解決手段として適用される。
まず、階層型の認証経路に従ってルート認証書までを確認するが、ルート認証書が自システムのルート認証書と異なる場合、認証局の相互認証書を検証する。相互認証経路によりその上位認証局が階層型のルートに結合している場合には、認証経路の確認が完了したとみなす。

(1) 相互認証経路優先方式

この方式では認証局の相互認証書が事前にユーザに配布されている事を前提としている。
何等かの手段によって相手の公開鍵認証書を入手した時、相手認証書の発行者名を確認する。事前入手した相互認証書の所有者名を検査して発行者名と一致する所有者名があるかを確認する。一致する場合には、その時点で認証経路の確認を完了する。
簡便な方法といえるが、相互の信頼性を前提としているので、信頼性がそこなわれないような事前検討が必要である。



最短経路による相互認証経路

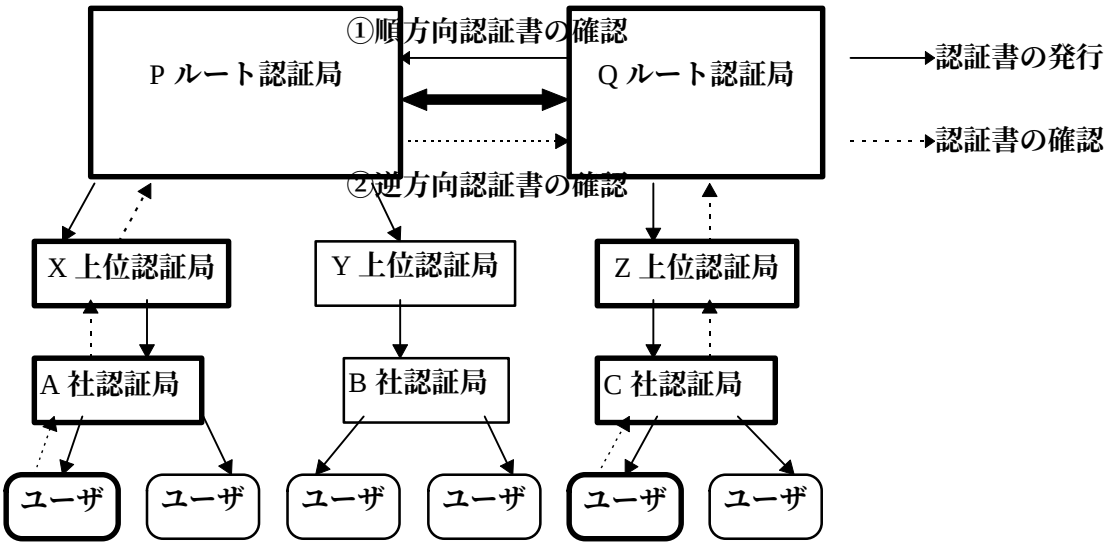
(2) 階層型認証経路優先方式

この方式は、異なるルート認証局を持つ場合のシステムに適用される。
まず、階層型の認証経路に従ってルート認証局まで検証する。この時にルート認証書が自分のルート認証書と異なる場合には、ルート認証書の相互認証書を検証する。このルート相互認証書は何等かの手段によって入手できるものとする。ルート相互認証書の確認手段としてつぎの３通りがある。

① 順方向相互認証書による確認
この方式は相手のルート認証書に付随する順方向ルート相互認証書を検証する。順方向ルート相互認証書の発行者名が自ルート認証局名と一致する場合には、認証経路の確認を完了する。

② 逆方向相互認証書による確認
この方式は自ルート認証書に付随する逆方向ルート相互認証書を検証する。逆方向ルート相互認証書の所有者名が相手ルート認証局名と一致する場合は、認証経路の確認を完了する。

③ 両方相互認証書による確認
この方式は①及び②の確認を両方とも行ってから認証経路の確認を完了する方式である。より厳密な相互認証を期待する場合に適用される。



異なるルート認証局経由の相互認証経路

5.6.3 相互認証書の形式

ディレクトリィに保持される認証書の形式は、ISO で規定されている国際標準である X.509 認証書を基本とする。

X.509 ではつぎの３つの属性に分類されている。

（１） ユーザ認証書　**UserCertificate**

（２） 認証局認証書　**CACertificate**

（３） 相互認証書　**CrossCertificatePair**

ここで解説する相互認証書は X.509 で定義する相互認証書（Cross-Certificate-Pairs）の属性を前提としている。[2]　順方向の相互認証と逆方向の相互認証とが定義されている。順方向とは相手側の認証局から自側の認証局に対する相互認証をいう。逆方向とは自側から相手側に対する相互認証をいう。

```
crossCertificatePair      ATTRIBUTE ::=     {
      WITH SYNTAX         CertificatePair
      ID                  id-at-crossCertificatePair }

CertificatePair           ::=     SEQUENCE {
      forward     [0]     Certificate OPTIONAL、
      reverse     [1]     Certificate OPTIONAL
                          -- at least one of the pair shall be present -- }
```

この両方向の相互認証書は少なくともいずれか一方のみ存在すればよいのであるが、どの方向の相互認証を行うかは各認証局のポリシーによる。

認証局が他の認証局を相互認証する範囲は認証局相互に別途協議される。

各認証局の「認証実施規定(CPS)」と認証ポリシーを双方が事前審査する。各認証局はそのユーザによる認証経路確認に対する適当な制限を決定する。双方の合意により、各認証局は相互認証書を交換し、対になる認証書を作成する。各相互認証書をユーザが入手するための方法については各認証局のポリシーによる。

5.6.4 相互認証書の基本構成

(1) 他の認証書と同様に相互認証書においても X.509 V3 認証書を基本構成とする。
基本構成上の必要最小限の実装規約については後述する。

認証書の基本構成

基本部	**バージョン番号** Version	version3 = 2
	シリアル番号 Serial Number	認証局ごとの認証書番号
	発行者署名アルゴリズム Signature Algorithm	別表１を参照
	発行者名 Issuer Distinguished Name	X.500 識別名(別表２参照)
	有効期間 Varidity Period	開始年月日と終了年月日
	所有者名 Subject Distinguished Name	X.500 識別名(別表２参照)
	所有者公開鍵 Subject Public Key Info.	アルゴリズム識別と公開鍵
V2 拡張部	**発行者特定識別子** Issuer Unique Identifier	これらの識別子を使用しない事を推奨する。(有効期間を越えて再使用するための識別子である。)
	所有者特定識別子 Subject Unique Identifier	
V3 拡張部	----別表３に示す----	
発行者署名		

[2] Refer to ISO/IEC 9594-8 Clause8 Obtaining a user's public key

(2) X.509 で定義する認証書の定義はつぎの通りである。[3]
V3 拡張部の表記については、NIST の資料[4] を参照している。

```
Certificate             ::=     SIGNED { SEQUENCE {
        version                 [0]     Version DEFAULT v1、
        serialNumber                    CertificateSerialNumber、
        signature                       AlgorithmIdentifier、
        issuer                  Name、
        validity                        Validity、
        subject                         Name、
        subjectPublicKeyInfo            SubjectPublicKeyInfo、
        issuerUniqueIdentifier  [1]     IMPLICIT UniqueIdentifier OPTIONAL、
                                        -- if present、 version must be v2
        subjectUniqueIdentifier [2]     IMPLICIT UniqueIdentifier OPTIONAL
                                        ---if present、 version must be v1 or v2--
        extensions              [3]     Extensions Optional
                                        --if present、 version must be v3--}  }

Version                 ::=     INTEGER { v1(0)、 v2(1) }

CertificateSerialNumber ::=     INTEGER

AlgorithmIdentifier             ::=     SEQUENCE {
        algorithm               ALGORITHM.&id ({SupportedAlgorithms})、
        parameters              ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm})
OPTIONAL }
--      Definition of the following information object set is deferred、 perhaps to standardized
--      profiles or to protocol implementation conformance statements. The set is required to
--      specify a table constraint on the parameterscomponent of AlgorithmIdentifier.
--      SupportedAlgorithms     ALGORITHM::=    { ... | ... }

Validity                ::=     SEQUENCE {
        notBefore       UTCTime、
        notAfter        UTCTime }

SubjectPublicKeyInfo    ::=     SEQUENCE {
        algorithm               AlgorithmIdentifier、
        subjectPublicKey        BIT STRING }

Extensions              ::=     SEQUENCE OF Extension

Extension               ::=     SEQUENCE {
        extnId                  EXTENSION.&id ({ExtensionSet})、
        critical                BOOLEAN DEFAULT FALSE、
        extnValue               OCTET STRING
                                -- contains a DER encoding of a value of type &ExtnType for the
                                -- extension object identified by extnId --
```

[3] Refer to ISO/IEC 9594-8:1993 (E)、 Amendment 1 to ISO/IEC 9594-8:1995 (E).

[4] NIST Minimum Interoperability Specification for PKI Components:1996-12-2

別表１ 署名アルゴリズム

区分	署名とハッシュの組み合わせ	出典	適用例
RSA	RSA with MD2	PKCS #1	IETF PKIX[1], SSL[2]
	RSA with MD5		SSL[2]
	RSA with SHA-1	FIPS 180-1	SET[3], NIST MISPC[4]
DSA	DSA with SHA-1	FIPS 186	IETF PKIX[1], NIST MISPC[4]

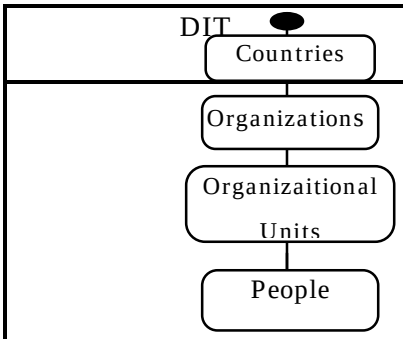
md2WithRSAEncryption OBJECT IDENTIFIER ::= {
iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1)
pkcs-1(1) 2 }

md5WithRSAEncryption OBJECT IDENTIFIER ::= {
iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1)
pkcs-1(1) 4 }

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
iso(1) identified-organization(3) oiw(14) secsig(3)
algorithm(2) 29 }

dsaWithSHA-1 OBJECT IDENTIFIER ::= {
iso(1) identified-organization(3) oiw(14) secsig(3)
algorithm(2) 27 }

別表２ X.500 識別名[5]



RDN	認証局名への適用例		
	USA Federal	SSL	SET
root			
C＝	US	US	ISO3166 国名コード
O＝	U.S.Federal Govt.	Verisign	認証組織名
OU＝	DoD NSA		
CN＝	MISSI	Verisign Class1root	ユニークな CA の ID

DIT: Directory Information Tree 、 RDN: Relative Distinguished Name

X.520 で定義する名前の属性はつぎの通りである。

commonName ATTRIBUTE WITH ATTRIBUTE-SYNTAX
caseIgnoreStringSyntax(SIZE(1..ub-common-name)
::= { attributeType 3}
countryName ATTRIBUTE WITH ATTRIBUTE-SYNTAX
PrintableString(SIZE(2)) - IS 3166 codes only
MATCHES FOR EQUALITY SINGLE VALUE
::= {attributeType 6}
organizationName ATTRIBUTE WITH ATTRIBUTE-SYNTAX
caseIgnoreStringSyntax(SIZE(1..ub-organization-name)
::= {attributeType 10}

[5] Refer to X.501 Determination of distinguished name.

5.6.5 相互認証書の拡張構成

V3 拡張部は拡張情報識別子とクリティカル識別子及び拡張情報の３つから各情報ごとに構成されている。クリティカル識別子の定義は X.509 V3 での標準定義を示している。
クリティカル識別子はその情報を受信する側がその情報を認識すべき(YES)か無視(NO)してよいかを示している。その扱いを規定しないものは任意(YES/NO)としている。
本参考資料での実装規約については、本文で述べた通りである。

別表３ 認証書 V3 拡張部の構成

区分	V3 拡張部	クリティカル	拡張詳細情報	属性
(1)	**認証局鍵識別** Autority Key Identifier	無視 (NO)	鍵識別情報	[0]OCTET STRING
			認証書発行者名	[1]General Names
			認証書シリアル番号	[2]Serial Number
	所有者鍵識別 Subject Key Identifier	無視 (NO)	鍵識別情報	OCTET STRING
	鍵種別 Key Usage	任意	鍵種別情報	BIT STRING
	秘密鍵使用期間 Private Key Usage Period	任意	使用開始/終了日	Generalized Time
	認証局ポリシー Certificate Policies	任意	ポリシー識別子	OBJECT IDENTIFIER
			ポリシー権限情報	OBJECT IDENTIFIER
	ポリシー関連付け Policy Mappings	無視	認証局ポリシー識別子	OBJECT IDENTIFIER
(2)	**所有者別名** Subject Alternative Name	任意	一般名	General Names
	発行者別名 Issuer Alternative Name	任意	一般名	General Names
	所有者ディレクトリィ属性 Subject Directory Attribute	無視	ディレクトリィ属性	Attribute
(3)	**基本制限** Basic Constraints	任意	認証局	BOOLEAN
			認証経路長制限	INTEGER
	名前制限 Name Constraints	任意	許容サブツリー	General Names
			除外サブツリー	BaseDistance
	ポリシー制限 Policy Constraints	任意	ポリシーセット	OBJECT IDENTIFIER
			明示的ポリシー要求	INTEGER
			ポリシー関連付け禁止	INTEGER
(4)	**ＣＲＬ配布元** CRL Distribution Points	任意	配布元	Name
			理由	Flags
			ＣＲＬ発行者	General Names

一般名は X.509V3 で定義されておりつぎの通りである。

```
GeneralName ::= CHOICE {
        otherName                       [0]     INSTANCE OF OTHER-NAME、
        rfc822Name                      [1]     IA5String、
        dNSName                         [2]     IA5String、
        x400Address                     [3]     ORAddress、
        directoryName           [4]     Name、
        ediPartyName            [5]     EDIPartyName、
        uniformResourceIdentifier [6]   IA5String、
        iPAddress                       [7]     OCTET STRING、
        registeredID                    [8]     OBJECT IDENTIFIER }
```

(1) 鍵及びポリシー情報 (key and policy informationy information)

つぎの６種類のパラメタが拡張定義されている。

ａ） **認証局鍵識別** (*Authoority key identifier)*
ｂ） **所有者鍵識別** (*Subjeubjecct key identifier*)
ｃ） **鍵種別** (*Key usage*)
ｄ） **秘密鍵使用期間** (*Private key usage period*)
ｅ） **認証局ポリシー** (*Certificate policies*)
ｆ） **ポリシー関連付け** (*Policy mappings*)

ａ） **認証局鍵識別**

認証局の鍵更新が一定期間あるいは特別の状況において発生する。認証書の署名を確認するために使用する公開鍵の識別子である。

```
authorityKeyIdentifier EXTENSION ::= {
        SYNTAX          AuthorityKeyIdentifier
        IDENTIFIED BY   { id-ce 35 } }

AuthorityKeyIdentifier ::= SEQUENCE {
        keyIdentifier                   [0] KeyIdentifier           OPTIONAL、
        authorityCertIssuer             [1] GeneralNames            OPTIONAL、
        authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }
        ( WITH COMPONENTS     {...、 authorityCertIssuer PRESENT、
                                     authorityCertSerialNumber PRESENT} |
        WITH COMPONENTS       {...、 authorityCertIssuer ABSENT、
                                     authorityCertSerialNumber ABSENT} )
KeyIdentifier ::= OCTET STRING
```

ｂ） **所有者鍵識別**

通常、認証書の所有者は目的別に複数の認証書とそれぞれに対応する公開鍵を所有している。認証書の所有ユーザが目的別の公開鍵と認証書を識別するための所有者の公開鍵の識別子である。

```
subjectKeyIdentifier EXTENSION ::= {
        SYNTAX                  SubjectKeyIdentifier
IDENTIFIED BY       { id-ce 14 } }

SubjectKeyIdentifier ::= KeyIdentifier
```

ｃ） **鍵種別**

所有者の鍵更新も一定期間あるいは特別の状況において発生する。同一の鍵所有者の異なる公開鍵を識別するための所有者公開鍵の鍵種別である。

```
keyUsage EXTENSION ::= {
        SYNTAX          KeyUsage
        IDENTIFIED BY { id-ce 15 } }

KeyUsage ::= BIT STRING {

        digitalSignature                (0)、
        nonRepudiation          (1)、
        keyEncipherment         (2)、
        dataEncipherment        (3)、
        keyAgreement            (4)、
```

```
        keyCertSign             (5)、
        cRLSign                 (6) }
```

d） 秘密鍵使用期間

認証された公開鍵と対応する秘密鍵は公開鍵の有効期限とは異なる期間使用される。このために秘密鍵の使用期間を認証書に表示可能とする要求がある。

```
privateKeyUsagePeriod EXTENSION ::= {
        SYNTAX          PrivateKeyUsagePeriod
        IDENTIFIED BY { id-ce 16 } }

PrivateKeyUsagePeriod ::= SEQUENCE {
        notBefore       [0]     GeneralizedTime OPTIONAL、
        notAfter        [1]     GeneralizedTime OPTIONAL }
        ( WITH COMPONENTS           {...、 notBefore PRESENT} |
        WITH COMPONENTS  {...、 notAfter PRESENT} )
```

e） 認証局ポリシー

認証書は複数の認証ポリシーが適用される環境で使われるかもしれないので、認証局のポリシーを認証書で提供する事がある。

```
certificatePolicies EXTENSION ::= {
        SYNTAX          CertificatePoliciesSyntax
        IDENTIFIED BY { id-ce 32 } }

CertificatePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
        policyIdentifier    CertPolicyId、
        policyQualifiers    SEQUENCE SIZE (1..MAX) OF
                PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
        policyQualifierId       CERT-POLICY-QUALIFIER.&id
                                        ({SupportedPolicyQualifiers})、
        qualifier               CERT-POLICY-QUALIFIER.&Qualifier
                                ({SupportedPolicyQualifiers}{@policyQualifierId})
                                OPTIONAL }

SupportedPolicyQualifiers CERT-POLICY-QUALIFIER ::= { ... }

CERT-POLICY-QUALIFIER ::= CLASS {
        &id             OBJECT IDENTIFIER UNIQUE、
        &Qualifier      OPTIONAL }
WITH SYNTAX {
        POLICY-QUALIFIER-ID         &id
        [QUALIFIER-TYPE    &Qualifier] }
```

f） ポリシー関連付け

ある組織から他の組織に対して相互認証を行う時、両者の組織のポリシーの幾つかは同一のポリシーであると想定されている。このようなポリシーの対応付けをポリシー関連付けという。

```
policyMappings EXTENSION ::= {
        SYNTAX          PolicyMappingsSyntax
```

```
        IDENTIFIED BY { id-ce 33 } }

PolicyMappingsSyntax ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
        issuerDomainPolicy          CertPolicyId、
        subjectDomainPolicy     CertPolicyId }
```

(2) 認証書所有者属性及び認証書発行者属性

(certificate subject and certificate issuer attributes)

つぎの３種類のパラメタが拡張定義されている。

ａ） **所有者別名** (*Subject alternative name)*
ｂ） **発行者別名** (*Issuer alternative name*)
ｃ） **所有者ディレクトリィ属性** (*Subject directory attributes*)

ａ） **所有者別名及び発行者別名**

認証書は様々な形式を持つアプリケーションによって使用できなければならない。インターネットの電子メール名、インターネットドメイン名、X.400 発信/受信者アドレス、及び EDI 組織名などが含まれる。このため認証書において複数の名称形式を表現できることが必要である。

```
subjectAltName EXTENSION ::= {
        SYNTAX          GeneralNames
        IDENTIFIED BY { id-ce 17 } }

issuerAltName EXTENSION ::= {
        SYNTAX          GeneralNames
        IDENTIFIED BY { id-ce 18 } }

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
        otherName                       [0]     INSTANCE OF OTHER-NAME、
        rfc822Name                      [1]     IA5String、
        dNSName                         [2]     IA5String、
        x400Address                     [3]     ORAddress、
        directoryName           [4]     Name、
        ediPartyName            [5]     EDIPartyName、
        uniformResourceIdentifier       [6]     IA5String、
        iPAddress                       [7]     OCTET STRING、
        registeredID                    [8]     OBJECT IDENTIFIER }

OTHER-NAME ::= TYPE-IDENTIFIER

EDIPartyName ::= SEQUENCE {
        nameAssigner                    [0]     DirectoryString {ub-name} OPTIONAL、
        partyName                       [1]     DirectoryString {ub-name} }
```

(b) **所有者ディレクトリィ属性**

認証書ユーザはある所有者に関して、その所有者が実際に意図したその人物であるという事を確認するためにある識別情報を安全に知る必要があると思われる。(郵便の住所、企業内の所属、写真イメージなど) その様な情報はディレクトリィ属性として表現するのが便利であると思われるが、それらの属性は識別名の一部としては不要である。
このような識別名を越える付加的なディレクトリィ属性を運ぶための情報が認証書に必要である。

```
subjectDirectoryAttributes EXTENSION ::= {
        SYNTAX          AttributesSyntax
        IDENTIFIED BY { id-ce 9 } }

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute
```

(3) 認証経路の制限 (certification pathtion path constraints)

X.509 における認証経路の制限はつぎのような考え方に基づいている。

- たとえば信頼性の低い CA が不適当な名前を持つ認証書を発行したためにシステムの信用がそこなわれていないかを認証書のユーザがチェックできるようにするために、CA が認証経路上の制限を規定することがある。
- 複数の認証ポリシーが容認されている環境で認証経路を指定することがある。CA は他のドメインの CA を信用するかどうかを規定する。複数のポリシードメイン間の連携をサポートする場合に使用する。
- 単一の組織の場合には階層モデルの認証経路でシステムが閉じているが、 複数の組織が相互接続された環境では認証経路の柔軟性が必要になる。
- 認証ポリシーの異なる CA との相互接続を拒否する場合のためにポリシーマッピングの使用を禁止することがある。

つぎの３種類のパラメタが拡張定義されている。

ａ）**基本制限**(*Basic constraints*)
ｂ）**名前制限**(*Name constraints*)
ｃ）**ポリシー制限**(*Policy constraints*)

ａ）基本制限

認証書の所有者が CA の場合に存在し、認証経路の長さ制限を規定する。

```
basicConstraints EXTENSION ::= {
        SYNTAX          BasicConstraintsSyntax
        IDENTIFIED BY { id-ce 19 } }

BasicConstraintsSyntax ::= SEQUENCE {
        cA                      BOOLEAN DEFAULT FALSE、
        pathLenConstraint       INTEGER (0..MAX) OPTIONAL }
```

ｂ）名前制限

CA の認証書においてのみ使用される。認証書所有者の名前の長さを規定する。

```
nameConstraints EXTENSION ::= {
        SYNTAX          NameConstraintsSyntax
        IDENTIFIED BY { id-ce 30 } }

NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees       [0]     GeneralSubtrees OPTIONAL、
        excludedSubtrees        [1]     GeneralSubtrees OPTIONAL }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
        base                    GeneralName、
        minimum                 [0]     BaseDistance DEFAULT 0、
        maximum                 [1]     BaseDistance OPTIONAL }
```

```
BaseDistance ::= INTEGER (0..MAX)
```

c）ポリシー制限

明示的な認証ポリシーの表示及びポリシーマッピングの禁止の表示を規定する。

```
policyConstraints EXTENSION ::= {
        SYNTAX          PolicyConstraintsSyntax
        IDENTIFIED BY { id-ce 34 } }

PolicyConstraintsSyntax ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
        policySet                       [0] CertPolicySet OPTIONAL、
        requireExplicitPolicy   [1] SkipCerts OPTIONAL、
        inhibitPolicyMapping            [2] SkipCerts OPTIONAL }

SkipCerts ::= INTEGER (0..MAX)

CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId
```

(4) ＣＲＬ配布元 (CRL distribution points)

X.509 における CRL の配布元に関する考え方はつぎの通りである。
リボケーションリストは数が多くなり扱いにくくなる可能性がある。このため
部分的な CRL を提供できる必要がある。
このような CRL は大規模サーバシステムでは CRL の更新により、前回の CRL と現在
の最新の CRL との差分情報として提供される。
このような差分 CRL の配布元の指定に適用される。

```
cRLDistributionPoints EXTENSION ::= {
        SYNTAX          CRLDistPointsSyntax
        IDENTIFIED BY       { id-ce 31 } }

CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
        distributionPoint       [0]     DistributionPointName OPTIONAL、
        reasons         [1]     ReasonFlags OPTIONAL、
        cRLIssuer               [2]     GeneralNames OPTIONAL }

DistributionPointName ::= CHOICE {
        fullName                        [0]   GeneralNames、

        nameRelativeToCRLIssuer     [1]   RelativeDistinguishedName }

ReasonFlags ::= BIT STRING {
        unused                  (0)、
        keyCompromise           (1)、
        cACompromise            (2)、
        affiliationChanged      (3)、
        superseded              (4)、
        cessationOfOperation    (5)、
        certificateHold         (6) }
```

5.7 付録Ｇ：メンバー一覧

ECOM

米倉 昭利	主査	電子商取引実証推進協議会	主席研究員
長　博連	副主査	電子商取引実証推進協議会	主席研究員
角間 和博	副主査	電子商取引実証推進協議会	主席研究員

リーダー

鍛冶 俊彦	富士通株式会社 第二システム事業部 ＥＣソリューション推進室 担当課長

メンバー

池田 伸次	株式会社シー・アイ・シー 首都圏支店 営業二課
越湖 正道	株式会社日本ダイナースクラブ 業務部 マルチメディア推進室 室長
大谷 彰宏	三菱電機株式会社 情報システム製作所 Ｃ／Ｓネットワークシステム部 主事
北井 富士夫	株式会社東芝 府中工場 電算機ソフトウェア部
鈴木 雅人	日本ベリサイン株式会社 エンジニアリンググループ エンジニア
竹永 三郎	サイバー・コマース・シティー・コンソーシアム　主席研究員
久留 吉伸	株式会社ジャストシステム 技術本部開発部 福岡研究所 サブリーダー
松谷 英夫	財団法人情報処理相互運用技術協会 技術部 第二技術課長
松永 和男	株式会社日立製作所 ソフトウェア開発本部 第４ＯＳ設計部 主任技師