H８－WG０８－２

海外認証局活動調査報告

平成９年３月

電子商取引実証推進協議会

認証局検討ＷＧ

はじめに

インターネットのような分散したネットワーク環境において、利用者が安全かつ安心して取引や情報交換を行なえるようにするためには、取引（情報交換）に参加している当事者が真正な個人（あるいは法人）であることが証明されていなければならない。
この取引当事者が真正な個人（あるいは法人）であることを確認し、証明書（認証書）を発行する機関が認証局である。

しかしながら、認証局は誰もが運営できるわけではなく、認証局に課せられる主要な要件として、信頼性、公平性（中立性）、守秘性、相互運用性などがあり、かつこれら要件に加え組織的、経済的にも確固たる基盤を備えていなければならない。

このような種々の要件を備えた認証局を設立するための基盤整備を図り、国内外を含めた多種多様の認証局との相互運用性を確立するために、ＥＣＯＭ内に認証局検討ＷＧが設置されている。

本ＷＧでは企業・消費者が安心して継続的に利用できる認証局の運営を目指すとともに、最小限の認証により認証局間の相互運用が行なえる環境の構築を目的として、この目的達成のため、認証局の役割、目的等について検討を行い、認証局システムの安全対策、システムおよび財務監査、プライバシー保護等に関するガイドラインを作成し、且つ今後多種多様な認証局が設立運営されてくることに備え、認証局間の相互運用性、接続性を確保するための技術的、制度的課題について検討を行なっている。

これらの内容を検討するにあたって、認証局検討ＷＧを３つのサブＷＧに分け、それぞれ以下に示す内容について検討を行なっている。

①運用制度検討サブＷＧ

認証の信用力、継続性、安全性を保証するための広義の認証局運用ガイドラインを策定し、実証実験プロジェクトへの適用評価を行ない、実現性を高める。

②相互認証検討サブＷＧ

多種多様の認証局間での相互認証を行なうため、公開されている相互認証技術の検討・調査を行い、相互認証基本仕様を提案するとともに、それをベースにした、日本のビジネスにおける仕組み、ルールを前提とした相互認証ガイドラインの策定を行なう。

③国際相互認証検討サブＷＧ

国際的な相互認証を行なうため、各国における認証局の動向調査を行ない、法的、制度的課

題等を洗い出し、国際認証条件の整備を図る。

本報告書は、運用制度検討サブWGおよび相互認証検討サブWGが検討経過で取りまとめて既に出版済みの「認証局運用ガイドライン」並びに「相互認証技術解説および基本仕様案」に引き続き、国際相互認証検討サブWGの中間成果を報告するものであり、両報告書と併せて読まれることをお薦めする。

「認証局運用ガイドライン（α版）」（認証局検討報告書として出版済）

本ガイドラインは、公開鍵基盤における認証局の運営について、その拠り所となる指針を提示しているものであり、公開鍵基盤を構成する暗号サービス、認証書管理サービス、その他関連するサービスなど認証局が提供し得るサービスに基づき、これらに関わる認証局に課される業務要件やマネジメント要件などについて提示している。

なお、本ガイドラインはホームページにおいて平成９年１月にＥＣＯＭ会員限定で公開し、翌２月に一般に公開している。

「相互認証技術解説および基本仕様案」（認証局検討報告書として出版済）

本書は、公開鍵基盤に基づいた認証局の相互認証技術の調査、検討結果をまとめたものである。既に公開されている技術の紹介と解説、加えて米国において実際に検討されている事例を解説し、これらの技術の検討結果を基に、独自に検討を行い相互認証の推奨技術として紹介している。

「海外認証局活動調査報告」（今回出版）

各国における認証局活動についての調査報告である。

本報告は各国の認証局活動、法律と制度、国際相互認証の動向および相互認証技術の海外動向の３つの観点から調査を行なったものであり、国際間取引における相互認証のための基盤ルール、仕組の検討を行なうための基礎資料とするものである。

目次

1.海外の認証局の動向

ＥＣＯＭ　ＷＧ８　ＳＷＧ３の９６年度活動の一環として現在活動中の海外認証局の動向を調査した。

1.1.ＧＴＥ

1.1.1.会社概要

１５年にわたり、アメリカ政府の音声、データ通信用に、公開鍵方式による認証局サービスを提供している。マスターカード社の Secure Electronic Transactions（ＳＥＴ）における認証局として同社と協力している。１９９７年４月にＢＵＧ、野村総研、ＮＴＴ移動通信網等とともに、日本における認証局サービス会社、サイバートラスト社を設立した。

所在地：GTE CyberTrust Business Office

77 'A' Street Needham, MA 02194-2892 USA

Tel: 1/800-487-8788　Fax:1/617-455-4005　URL:http://www.cybertrust.gte.com/

1.1.2.サービス内容

基本サービス：ＳＥＴ、Secure Sockets Layer（ＳＳＬ）に対する認証局サービス

カスタムサービス：企業などに対して、その企業の独自使用に準拠した認証局サービスを提供。

1.1.3.特徴

ＳＥＴ、Ｘ．５０９、ＰＫＣＳ＃１，＃７，＃１０、ＡＳＮ．１ ＩＳＯ／ＩＥＣ、ＤＥＲ ＩＳＯ／ＩＥＣなどの標準に準拠。また、ルートＣＡサービス、Registration Authority、などのサービスも提供している。

1.1.4.セキュリティ

ＣＡセンターに入室するには ID カードによるセキュリティガードされた２つのドアを通る。

この２つのドアの間には受付があり、入室者は氏名と会社名、入室日を要求される。

センター内には CA サーバ関連システムを設置した５つの部屋があり、各部屋は２人一組での指紋

によるバイオチェックとダイヤルロック式の鍵の組合せによるセキュリティガードが施されている。

また、各部屋には外部からの侵入者を検知するシステム（モーションディテクター）が設置されている。

CA の秘密鍵は SPYRUS 社のセキュア PCMCIA カードが保管され、専用の個室にバックアップのカードを保管する金庫が設置されている。

1.2.SUN Certificate Authorities

1.2.1.会社概要

Sun Microsystems がハード(Sun Screen SPF-100 など)を、Trident Data Systems がソフトを担当してセキュリティシステムを開発し、そのユーザー向けに Sun がＣＡとして活動する。例えば、Small Office Home Office 等を狙った製品と思われる。

所在地：Sun Microsystems, Inc., 2550 Garcia Ave.,

Mtn. View, Ca 94043-1100 USA

Tel: 1/415-336-0018　URL:http://www.sun.com/security/product/ca.html

1.2.2.サービス内容

・Certificate の発行。

・Certificate の更新。

・Certificate Revocation，同リストの公開。

1.2.3.特徴

SunCA certificate(1024 ビットキー)、SunCAglobal certificate（512 ビットキー）の、２種類の認証書を発行する。

1.3.VeriSign, Inc.

1.3.1.会社概要

１９９５年４月に米国ＲＳＡ社の子会社として設立された。マイクロソフト、ネットスケープ、ビザ・インターナショナル、ＡＯＬ、ＩBMなどと提携している。１９９６年２月に、ＮＴＴデータ通信などとともに、日本ベリサイン社を設立。

所在地：VeriSign, Inc.

2593 Coast Avenue, Mountain View, CA 94043 USA

1.3.2.サービス内容

Ｘ．５０９に準拠したＣＡサービス。

個人認証書：個人向け。ブラウザ（Netscape Navigator 等）や電子メール等に用いる。

サーバー認証書：ｗｅｂサーバー（ＩＢM，オラクル等）向け。

認証書のレベルとして４段階あり（最高クラスは現在は不可)、料金、発行手順、必要書類が異なる。

認証書の記載内容は、

・ユーザー（名前、住所、所属等）

・公開鍵

・有効期限

・シリアル番号

・ＣＡのディジタル署名、ＩＤ情報

ＣＡとしての具体的活動として、

・認証書の発行

・認証書の更新（有効期間：１年間）

・認証書の失効，同リストの公開

・認証書の検索

・タイムスタンプサービス

等を行う。鍵の生成は行わない。

1.3.3.特徴

認証局活動のガイドラインとして、Certification Practice Statement を発行。

1.3.4.セキュリティ

・データセンター

データセンターの廊下に面した部分はガラス張りで内部が見えるようになっているが、室内の一部はパーテションで仕切られており外部からは見えない。

室内は、クラス２の認証を自動発行するシステムが設置されており無人稼動。ハードはＳｕｎ社のマルチプロセッサ（ＤＢサーバ、ＣＡサーバ）とＢＢＮ社の鍵管理ユニットが３台設置されており、認証発行の処理能力を高めている。

センターのドアは、指紋と電子キー（シークレットシェアという）で解錠。このキーを　保持しているのは、従業員８５名中１５名のみ。

ドアが解錠されると、天井に設置してある赤外線感知警報装置が停止し、入室可能となる。

退室は、室内の読み取り装置に電子キーを読み込ませ退室する。退室後警報装置が作動。

室内には無線電話があり、電源が遮断された場合などの緊急時に、この無線電話で外部に連絡するようになっている。

・ＣＡカスタマーサービスセンター

データセンターと同様のセキュリティで運用。

クラス３の認証を発行。４台のワークステーションがあり、各々のオペレータ（ボンデッドオペレータという）がおり、受付処理を行う。勤務体系は２交代制で２４時間運用。

ボンデッドオペレータとは、信用の高い人間を指し、VeriSign ではこのオペレータに公証人の資格をとらせる予定。

申請書類は３０年間保管。期間は American Bar Association（ABA）のガイドラインと同じ。

1.4.ＣＯＳＴ－ＣＡ

1.4.1.会社概要

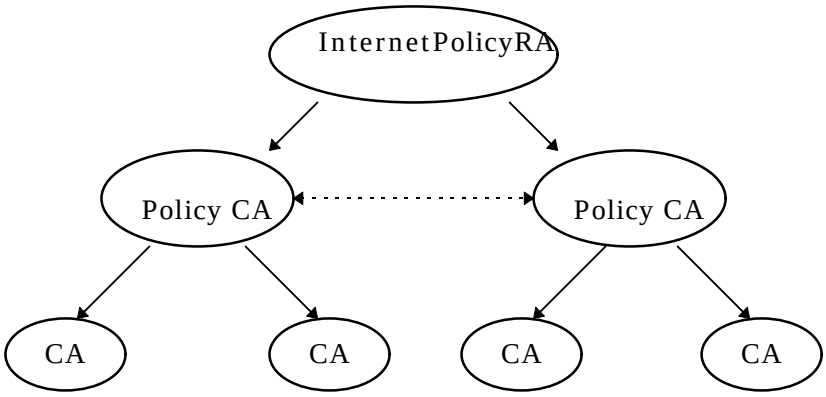
ストックホルムを拠点とした、ヨーロッパが中心のＣＡ。現在は電子メールとWWWを用いることを前提としている。３段階の認証書を発行し、それぞれ電子メール（Low Level)、ビジネス文書配布など（Medium Level)、ＥＣや金融（High Level）に活用することを想定している。

所在地：COST Computer Security Technologies

Finlandsgatan 60 164 74 Kista, SWEDEN

URL: http://www.cost.se/

1.4.2.サービス内容



図－１　ＣＯＳＴ－ＣＡの構成

ＣＡの上下関係は図に示す通りである。ＣＡを Policy CA が認証する。Policy CA 間では、直接相互に認証するか（X.509)、より上位に Internet Policy CA を設けるか（Internet PEM)、いずれかの方策を採る。

ＣＡの機能は以下の通りである。将来的には公証機能を追加する予定。

・ＣＡやユーザーの身元確認と登録

・個人識別情報の保管と配布

・認証と認証書管理（発行、保管、配布、認証、失効）

1.4.3.特徴

ＣＯＳＴでは３段階の認証書を発行する際に、技術、運営手続き、監査方法、システム管理などに関する１０の評価項目を定め、判断基準とする（表－１参照)。

1.4.4.ＣＯＳＴ－ＣＡの現況

現在、ＣＯＳＴ－ＣＡはアメリカ資本の ENTEGRITY Solutions が吸収し、上記のサービス提供は行なっていない。

表－１　ＣＯＳＴ－ＣＡ認証書発行評価基準

評価基準	Low Level Assurance	Medium Level Assurance	High Level Assurance
ＣＡ及びユーザへのＲＤＮ割り当て手順	CA：PCA に標準文書で申請 ﾕｰｻﾞ：各 CA で割り当て匿名も可能	CA：公式登録文書を提出し、 PCA が審査　ﾕｰｻﾞ：各 CA の内部手続きで処理　身分証明要	上位 CA が承認文書を作成
ＣＡ及びユーザのＤＮｓに関する規則	○CA,ﾕｰｻﾞのｿﾌﾄｳｪｱをｶｽﾀﾑ化 ○PCA が DNs 重複を削除 ○必要なら RDN を修正	Low Level での手続きと同一	Medium Level での手続きに加え、DNs 重複解決は IPCA と協力して行う
認証書署名要請の確認	○全ての要請を受理する ○承認基準設定 ○オンライン署名	○ Low Level と同じ承認基準設定 ○オフライン署名	Medium Level での手続きに加え、要請者の認証手続きをｵﾌﾗｲﾝで行う
認証書署名手順と秘密事項（秘密鍵)の保護	PCA,CA,ﾕｰｻﾞ:認証書署名はソフトウェアで行う 秘密事項保護はパスワード	PCA,CA：ｽﾏｰﾄｶｰﾄﾞで認証書署名と秘密事項保護 ﾕｰｻﾞ：認証書署名はｿﾌﾄｳｪｱ 秘密事項保護はﾊﾟｽﾜｰﾄﾞ	PCA,CA,ﾕｰｻﾞ:認証書署名、秘密事項保管ともｽﾏｰﾄｶｰﾄﾞで行う
認証書取り消しとＣＲＬ	○CRL を毎月更新 ○CRL を PCA に送付 ○他 CA,ﾕｰｻﾞも請求可能	○CRL は Low Level 準拠 ○“ホットリスト”発行 ○現状報告請求にも対応	○認証書有効性確認請求に対応 ○ディジタル署名確認作業
ＣＡデータベースとソフトウェアの保護	○ﾃﾞｰﾀﾍﾞｰｽ真正性定期確認 ○ﾛｰｶﾙﾊﾞｯｸｱｯﾌﾟによる復旧 ○正常状態確認状態に復旧	○ｿﾌﾄｳｪｱ真正性とﾃﾞｰﾀﾍﾞｰｽ保護定期確認　ｽﾏｰﾄｶｰﾄﾞにﾊﾟﾗﾒｰﾀ保管　PCA がﾊﾞｯｸｱｯﾌﾟ保管	Medium Level での手続きに加え、トラブル時のシステム一貫性を保証
ＣＡ監査	システム管理者がログファイルをチェック	外部監査向け文書を CA 登録時に PCA が作成	国際安全基準（ITSEC)準拠評価
システム管理者とユーザ向けガイドライン	マニュアル類（インストール手順、使用手順）	○ルールと手順の文書作成 ○システム管理確認テストをｿﾌﾄｳｪｱに組み込む	Medium Level での手続きと同一
ＣＡ公証機能	なし	○CA がディジタル署名認定	○ディジタル署名認定 ○ＣＡによる再署名 ○タイムスタンプ
ＣＯＳＴ－ＰＣＡ機能動作保証	最善を尽くす｡保証なし。停止による損失への補償無し	停止時間２時間以下保証 停止による損失への補償無し	連続動作保証

2. 相互認証の動向

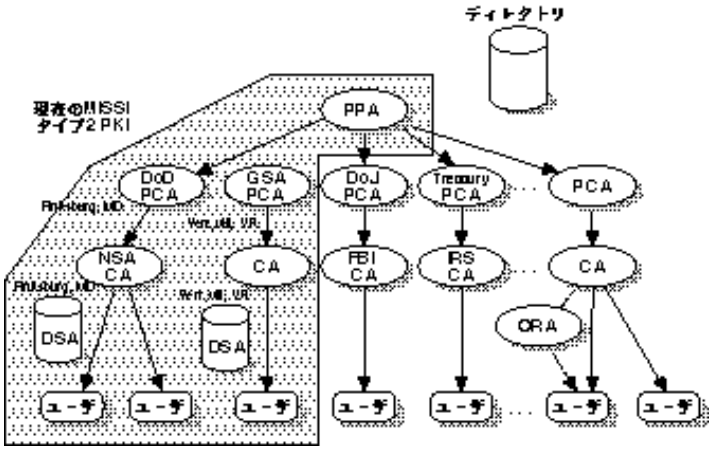
2.1.米国連邦政府における相互運用の検討

2.1.1.目的

米国連邦政府内の職員が使用している F-PKI と、他の PKI（主として民間で広く使われている RSA）を使用している外部の組織および市民との間に交わされる、要注意であるが機密扱いではない通信についての**相互運用**を目標にしており、F-PKI が他の PKI と相互運用が可能となるような F-PKI 自身またはそのユーザへの変更点を定義することを目的としている。

注）F-PKI は米国連邦政府内の PKI ということで、一般の民間の PKI とは違う点を考慮しておかなければいけない。またこれは EC 上での相互運用を行う相手が、それぞれ同じ PKI を使用していたような場合、安易に相互運用を行えるような誤解が生まれる可能性もあるが、たとえ同じ PKI を使用していたような場合でも、ビジネスレベルでの相互運用はこの中で定義されている範囲を超えて討議される内容も含まれると思われる。

2.1.2. F-PKI の構成およびその構成要素



図－２　連邦ＰＫＩのアーキテクチャ

(1) PPA（方針承認機関：第１水準ノード）

PPA は F-PKI のツリー構造のルートとなる機関で、PCA のセキュリティ方針を承認する機関

(2) PCA（方針作成機関：第２水準ノード）

PCA は PCA 自身とその下位機関の認証書を発行する際のセキュリティ方針を作成する

(3) CA（証明機関：第３水準ノード）

CA は上位方針作成機関（PCA）が定義したセキュリティ方針に基づき、ユーザに対して認証書を発行する

(4) ORA（組織登録機関）

ORA はユーザの身元および組織への所属を確認する機関

(5) DSA（ディレクトリ・システム・エージェント）

認証書および認証書失効リスト（CRL）の格納と取り出しを行う機関

(6) ユーザ

ここで言うユーザとは、F-PKI の中のツリーの末端の“葉”の１つにあたるもので、通常は１個人を扱う

(7) CMA（証明書管理機関）

第１～３水準までのノードである方針承認機関、方針作成機関、証明機関のいずれかまたはすべてをさす

(8)DoD（米国国防省）

(9)GSA（共通役務庁）

2.1.3.相互運用のための一般的な条件

2.1.3.1.相互運用の一般的な前提条件

一般に、異なった PKI 間の各ユーザの対話には、以下のことが必要になる。

(1)各証明書管理機関（F-PKI でいう CMA）間に信用のチェインがなければならない

(2)ユーザは相互のディレクトリにアクセスして（直接、紹介、ディレクトリ間のチェインにより）、認証書のチェインおよび認証書失効リストを所得できなければならない

(3)ユーザは相互に相手のアプリケーション・プロトコルを処理できなければならない

2.1.3.2.安全な通信の条件

また、F-PKI とその他の PKI との間では、当然安全な通信が行われなければならない。当事者間での安全な通信とは、以下のようなセキュリティ・サービスの呼び出す能力を（お互いが）持つこ

とである。

(1) 送信者の確認（送信者か確実に実在し、かつ本人からの送信なのか）

(2) メッセージの正当性（送信者からの情報に改ざん等が行われていないか）

(3) 秘密保持

(4) 送信者の否認防止（送信者が“送信した”のに“送信しなかった”と言えないように）

(5) 受領の証拠（確実に相手に届いたことを証明）

2.1.3.3.相互運用性の制約事項

F-PKI とその他の PKI との間には、以下のような相違点があっても上記のような安全な通信が行えなければならない。

(1) 署名アルゴリズムの違い

２人のユーザが、それぞれのパブリックキー暗号化方式アルゴリズムによる、

- 異なったハッシング（安全ハッシュ基準（SHS)、メッセージ・ダイジェスト５（MD-5）等）を使用し、
- 異なったデジタル署名方式（リベスト、シャーマ（Shamir)、アデルマン（RSA）等）でデジタル署名を行う場合。

(2) キー配送アルゴリズムの違い

２人のユーザが、それぞれのパブリックキー暗号化方式に基づく、

- 異なったキー配送アルゴリズム（ディフィー－ヘルマン、RSA、キー交換アルゴリズム（KEA）等）を使用する場合。

(3) データ暗号化アルゴリズムの違い

２人のユーザが、それぞれ、

- 異なったデータ暗号化アルゴリズム（データ暗号基準（DES)、国際データ暗号アルゴリズム（IDEA）等）を使用する場合。

(4) データフォーマットの違い

２人のユーザが、それぞれ、

- 異なった認証書の基準やバージョンの違う（フォーマット：X.509 v1、X509V3 等）認証書を使用する場合。

(5) PKI の構造の違い

２人のユーザが、それぞれ、

● 異なったアーキテクチャの PKI 構造（厳格なツリー構造、多数の親を持つツリー構造、同僚認証を行うグラフ方式等）を使用する場合

(6) 認証書および認証書失効リストの普及（配布）方法の違い

２人のユーザが、それぞれ、

● 異なった認証書および認証書失効リストの普及（配布）方法（X.500 に基づくもの、信用ディレクトリ所有方式を使用する場合

(7) 認証書（発行／運用？）方針の違い

２人のユーザが、それぞれ、

● 異なった認証書（発行／運用？）方針に基づいて認証を受けている場合

(8) ネーミングの違い

２人のユーザが、それぞれ、

● 異なったネーミング規約による名前づけをされている場合

この項目を“相互運用性の制約事項”と呼び、次降の項目でそれぞれに対するアプローチを検討している。

注） **F-PKI のユーザは，連邦政府情報処理基準（FIPS）186 に指定されているデジタル署名基準（DSS）を使わなければならない。**DSS には，FIPS 186 および FIPS 180-1 にそれぞれ定義されているデジタル署名アルゴリズムと安全ハッシュアルゴリズム（SHA）の両方が含まれる。上記の暗号方式は連邦政府の強制的な基準であり，連邦 PKI の唯一の運用担当構成要素であるマルチレベル情報システム・セキュリティ・イニシアティブ（MISSI）によって現在使われている。

2.1.4.相互運用性の制限事項に対するF-PKI のアプローチ

2.1.4.1.署名アルゴリズムが違う場合（DSS と RSA）の解決案

(1) エンド・システム両暗号システムによる署名を確認できるようにする（DSS ユーザは自己のワークステーションに RSA の確認機能を追加し，RSA のユーザは DSS 確認機能を追加する）

(2) RSA を使用する領域に登録しているユーザと通信する必要のある DSS ユーザのみに対して，RSA と DSS 両方の証明書を発行する

(3)信用ゲートウェーを使用する

(4)全面的に DSS を使用する

(5)全面的に RSA を使用する

2.1.4.2.キー配送のアルゴリズムが違う場合（ DH と RSA）の解決案

(1)1 つのアルゴリズムによる証明書--この方法では, ユーザは RSA かディフィーヘルマンかどちらか 1 つのアルゴリズムよるキー配送証明書を持つ。

(2)複数のアルゴリズムによる証明書--この方法では，連邦政府のユーザは自分が選んだアルゴリズムによる証明書を持つことができる。通常，アルゴリズムは連邦政府のユーザが通信を希望する領域に基づいて決まる。

(3)信用ゲートウェイを使う

(4)全面的にディフィーヘルマンを使用する

(5)全面的に RSA を使用する

2.1.4.3.データ暗号化アルゴリズムが違う場合（SKIPJACK と DES）の解決案

(1)全面的に SKIPJACK を使用する

(2)全面的に DES を使用する

2.1.4.4.データのフォーマットに対するアプローチ

(1)基準となるフォーマットが決定した時点でそれを採用する

(2)ISO，CCITT, および ANSI の各基準の調和をサポートする

2.1.4.5.証明書のフォーマットに対するアプローチ

(1)X.509v3 を使用する

(2)X.509v3 基準で推奨され他（MISSI）が使用しているような基本的な制約事項のフィールド内の主体の種類のサブフィールドを使用する

(3)F-PKI は方針承認機関のレベルでのみ，他の領域からの証明書管理機関を認証する

2.1.4.6. 証明書失効リストのフォーマットに対するアプローチ

(1)X.509v2 の証明書失効リストを使用する

(2)F-PKI が使用する X.509v2 の証明書失効リストの拡張部分を定義する

2.1.4.7.データの配布に対するアプローチ

(1)標準 X.500 の属性に基づいて証明書および証明書失効リストを登録する

(2)上位証明書管理機関は，下位証明書管理機関の証明書を「証明機関証明書」という属性で保管する

(3)上位および下位の各機関は,「相互証明書ペア」という属性で相互に発行された証明書を保管する

2.1.4.8.方針に対するアプローチ

(1)階層的分類法による証明書の方針を作成する

＜証明書の方針の階層的分類法＞

証明書の方針は３つの方針があり、証明書発行機関のための方針は必須であると考えられる。

証明書発行機関のための方針（必須）

- コミュニティ（エンドエンティティの定義）
- 同一性証明方針
- 同一性確認方針
- キー管理方針
  - 暗号解読時間（MIPS 年）
  - パラメータ生成システムのレベル（FIPS 140-1 のレベル）
  - 用途定義
  - 生成方法定義
  - エスクロー、バックアップ、アーカイブ定義
  - エントリ定義
  - 格納方法定義
  - 活動化方針定義
  - 非活動化方針定義
  - キー再発行方法定義
  - キー破棄方法定義

・失効定義

● セキュリティ方針

・物理的管理方法定義

・証明書発行機関オペレーション人物定義

・技術管理方法定義

・監査方針定義

・アーカイブ結果管理方針定義

● 責任方針

(2)主体証明機関のための方針（推奨）

(3)主体エンド実体のための方針（推奨）

2.1.4.9.ネーミングに対するアプローチ

(1)証明書および証明書失効リストに X.500 の識別名を使用する

(2)通常、証明書発行機関は上位機関のネーミング制約に従う

2.1.5.相互認証の具体的プロセス

ここでは、ある証明書管理機関が別な証明書管理機関と相互認証するために使用するプロセスを示す。以下に示す交換や合意の 1 つまたはそれ以上を行うために，2 つの証明書管理機関の適切な代表者が直接面談することを想定する。

● それぞれのパブリック・キーを交換する。

● 責任についての合意を確立する。

● 信用性毀損の通知についての合意を確立する。

● キーの再発行を含む，信用性毀損からの回復手順についての合意を確立する。

● 少なくとも，互いの運用状況を定期的に監査することについての合意を確立する。

● 名前スペース，すなわち互いに相手からの証明書を尊重するための名前スペースについての合意を確立する。

● 方針のマッピングを確立する，すなわち一方の領域のどの方針を，相手の領域の方針と同等のものとして承認するかについて，またその逆について，合意する。

● ディレクトリのチェイン作成の規則およびディレクトリへのアクセスのための認証プロトコル

を確立する。

- **合意を文書化署名し、お互いにその控えを持ち合う。**

2.2.NetDox 社における相互認証について

2.2.1.NetDox 社とは

NetDox 社は、米国で Accounting、auditing、Tax などの業務や企業の経営コンサルタントを行っている Deloitte & Touche Consulting Group LLC（以下 D&T）の一部から派生した子会社として 1997 年 1 月 30 日に設立された。NetDox 社は現在のところ D&T のビルの一部にある。

2.2.2.サービス概要

NetDox 社で提供するサービスは、送受信者それぞれが使用する専用アプリケーションと NetDox 社が用意する Hub をつなぐことにより、各種ドキュメント（Text、spreadseet、audio file、EDI Document、etc）を用いた（e-mail ベースの）送受信に対して以下のサービスを提供する。

a.送信者と受信者の確認

b.送信者と受信者の確認のためのパブリック、プライベート認証局発行の（認証書の）相互認証

c.認証局の公開鍵の管理

d.メッセージの（NetDox 社以外の第三者による）公証

e.ログ／記録

f.暗号化されたメッセージの（改ざんされていないことの）確認

g.配送の確認

h.付加価値サービス（Financially による保証（保険）、D&T の持っている Audit 情報の付加等）

ここで、このサービスを受ける送受信者は、それぞれに Internet 上の e-mail address、認証局発行の認証書が必ず必要になる。しかし、送受信者がそれぞれ所有している認証書の認証局発行機関は同一でなくても良いとなっており、この形態が信用ゲートウェイによる相互認証にあたると思われる。

2.2.3.技術的概要

送受信者は、双方があらかじめ NetDox 社に登録（サービス提供）を受けていることが前提で、NetDox 社の Hub（信用ゲートウェイ）を必ず経由することによりサービスが実現されている。異

なるドキュメントのフォーマットは、e-mail ベース（ファイルのアタッチ）で作成され、NetDox 社の提供するクライアントアプリケーションを使って所定のフォーマットに変換し、NetDox 社の Hub に送られ、受信者に送られる。受け取った受信者は NetDox 社のクライアントアプリケーションによって元のドキュメントに変換される。

a.送信者と受信者の確認

送信者と受信者の確認は、e-mail address と認証書によって確認される。

b.送信者と受信者の確認のためのパブリック、プライベート認証局発行の（認証書の）相互認証。

これは、 パブリックな証明書に関しては、あらかじめ NetDox 社が指定（登録）した認証局のみが使用できる。プライベート認証局については、その認証局のルート鍵を NetDox 社に登録し、かつ所定の監査を受けなければいけない。

c.認証局の公開鍵の管理

パブリック認証局の公開鍵を、 NetDox 社で保管する。

d.メッセージの（NetDox 社以外の第三者による）公証

US. Surety 社のシステム、サービスを利用している。

e.ログ／記録

Hub 内にあるログ／記録を、必要があれば公開する。

f.暗号化されたメッセージの（改ざんされていないことの）確認

ハッシュ値の計算／確認により改ざんされていないことの確認を行っている。

g.配送の確認

NetDox 社のクライアントアプリケーションの機能により、送信情報が受信者に到着すると、その旨の“ レシピ ”が送信者に返送される。

肝心の相互認証の部分については、あまり詳しい情報が得られず、また、パブリック認証局に対しての相互認証証明書の発行等の説明はなかった。なお、現在のシステムは各アプリケーションを含めベータ版とのことであった。（http://www.netdox.com/ppt/ppframe.htm を参照）

2.2.4.価格形態および保障額

現在のところ、まだ完全にサービスを提供は提供されていないため、サービスの価格形態については完全には決まっていないようだが、初回登録料とトランザクションごとの課金という形態を考えている。

また、このサービスを受けているときの事故が起きた場合には、保険的なものが用意されており、NetDox 社の過失による事故の場合には保証金を支給するようになっている。

2.2.5.NetDox 社の相互認証

NetDox 社で提供するサービスは、それぞれ違う Public CA や Private CA 発行の証明書を持った人たちの相互認証を行い、その人たちの間での情報のやり取りを安全に行い、かつ第三者による公証的機能によって、公式な記録の残るやり取りのためのサービスである。また、第三者による公証的機能については、米国 Surety 社の“Digital Notary”の技術およびサービスを使用している。

2.2.6.関連 URL

NetDox：http://www.netdox.com/

D&T ： http://www.dtcg.com/

Surety： http://www.surety.com/

2.3.JapanNet プロジェクトにおける相互認証

2.3.1.概要

2.3.1.1.世界最初の国際相互認証実験

CommerceNet の９７年３月の発表によれば JapanNet と CommerceNet は世界で最初の国際相互認証実験を共同で実施する。

JapanNet と CommerceNet は各々独立した認証局を日本と米国に設立する。JapanNet は日本国内の電子商取引参加者各自に認証書を発行、CommerceNet は米国の電子商取引参加者に認証書を発行する。認証書の発行を受けた日本の電子商取引関係者と米国の電子商取引関係者は互いに商取引関連書類をデジタル署名と暗号の仕組みを利用して電子的に両社間で交換する。

この国際相互認証は「電子商取引での認証の利用が一つの認証局のピラミッドの中で利用する」ことから先ず始まり、必ず進む次のステップとなる。

CommerceNet と JapanNet は協力して国際相互認証に基づく「電子商取引契約モデル」、「認証ポリシー」、「認証局運用規定書」、などを順次作成する予定。尚、本ﾌﾟﾛｼﾞｪｸﾄに係るプレスリリースの一部を原文のまま抜粋すると次の通りとなる。

＝抜粋スタート＝

JapanNet and CommerceNet are collaborating to conduct the world's first cross certification pilot involving two Certification Authorities (CAs) in two different countries.

Mitsubishi Corporation and a US Trading Partner will use the certificates issued by their respective CAs to support the generation and validation of digitally signed and encrypted business documents.

JapanNet and CommerceNet will each provide independent CA services for their clients, Mitsubishi and a US Trading Partner, respectively. In order for the trading partners to communicate securely they will need to be able to validate each others' certificate. The JapanNet and CommerceNet CAs will cross certify each other and as a result will be able to validate certificates issued by both CAs. Other pilots have used certificates issued by a common root CA, which avoids the need for cross certification.

This is a logical next step for all certificate-based security services. The commercial focus to date has been on closed communities, where all the certificates originate from a common root. There is a need to explore the issues associated with the use of a single certificate in multiple communities.

During the pilot JapanNet and CommerceNet will participate in the development of an electronic commerce trade agreement, a certification authority policy for cross certification, and a certification practice statement for cross certification. This pilot will start in May, 1997, and continue through the first quarter of 1998.

JapanNet (http://www.japannet.or.jp) is a consortium of companies initiated by Mitsubishi Corporation and supported by MITI.

CommerceNet (http://www.commerce.net), in cooperation with its global partners, is a premier industry association for promoting and building global electronic commerce solutions on the Internet.

＝＝＝抜粋終了＝＝＝

2.3.1.2.開発課題

JapanNet と CommerceNet は共同して下記項目の書式・契約書・など電子商取引実行可能な標準化を検討する。

(1) 国際相互認証をベースにした認証ポリシー

(2) インターネット利用の海外契約

(3) 両社間での電子商取実施で引包括契約

(4) その他

2.3.2.電子商取引手順

2.3.2.1.ビジネスの概要

三菱商事（MC）は米国のビジネスパートナーと日常的に輸入取引を行っている。現在はファックス・電話・郵便などを利用しているが、今後はこれをインターネットでの電子商取引に移行する。これには JapanNet と CommerceNet の各々からの認証書発行とこの２つの認証局の相互認証をベースとする。

2.3.2.2.電子商取引化されるビジネスプロセス

(1) MC and TP conclude InterNetting Agreement to cover the whole business arrangement.

(2) MC sets its CA policy.

(3) MC appoints JapanNet as its CA.

(4) JapanNet issues certificates to employees of MC.

(5) TP sets its CA policy.

(6) TP appoints US CA as its CA.

(7) US CA issues certificates to employees of TP.

(8) MC generates a purchase order, digi-signs it, and sends it to TP via internet.

(9) TP receives purchase order, validate a certificate of that digital signature with US-CA.

(10) MC does the sam with JapanNet CA.

システム概要図は次ページ。

3.認証局関連法制度及び標準化動向

3.1.米国

米国は州法としてのデジタル署名法の制定が進んでいる。また、ABA(米国法律協会)、NIST、ANSI等で標準化の動きがある。

3.1.1.ABA のディジタル署名ガイドライン

ABA には幾つかの分科会があり、インターネット、商取引に関する検討グループは Section of Sci. & Tech., Electronic Commerce and Information Technology Division が担当している。ここで検討された"DIGITAL SIGNATURE GUIDELINES" (1996 年 8 月出版) はディジタル署名法のひとつのリファレンスとされており、後述の最初のディジタル署名法であるユタ州法とともにひろく知られている。 これは認証局のあり方に関するガイドラインであり、そのなかで認証局の運用基準、責任等について記述されている。 URL : <http://www/gvnfo.state.ut.us/ccjj/digsig/dsut-gl.htm>。

ABA 関連事項：ABA の URL: <http://www.abanet.org/>。 Section of Sci. & Tech., Electronic Commerce and Information Technology Division の URL は <http://www.intermarket.com/ecl/>。このサイトはよく変わるので頻繁にアクセスするようにとしている。この中に４つの委員会がある。

1.CyberNotaryCommittee<http://www.intermarket.com/ecl/notary.html>

"The CyberNotary:Public key registation and certification of international legal transactions" by Theodore Sedgwick Barassi, Esq. 約 7 頁。<http:www.intermarket.com/ecl/cybrnote.html>

この中で、国際電子商取引のための準公的な電子公証, CyberNotary も提案している。

2.Information Security Committee

3.Electronic Commerce Payment Committee

4.Judicial EDI Committee

3.1.2. 米国各州のデジタル署名／電子署名に関する法律

幾つかの州で制定の準備が進行しており、一部の州では既に実施されている。いずれの州法にも認証局間の相互認証に関する明確な記述は見当たらない。州によって内容に分布がある。例えば、ディジタル署名の定義においては、署名の特性のみを記述した広義の電子署名(フロリダ、マサチューセッツ) から、公開鍵システム上のデジタル署名（ユタ州、カリフォルニア州等）まである。1997年２月現在、法律が実施されているのは約１５州、制定の作業にあるのは１１州以上にのぼっている。代表的なものとして以下がある。

ユタ州 Utah Digital Signature Legislation(1995 年２月より実施)

<http://www.gvnfo.state.ut.us/ccjj/digsig/dsut-act.htm>

ワシントン州 Washington Electronic Authentication Act

<http://access.wa.net/sb6423”_info/6423.html>

ジョージア州 DRAFT :Georgia Digital Signature Act

<http://www.efa.org/digsig/lawdraft.htm>

<http://emory.edu/BUSINESS/digital”_signature”_draft.html>

オレゴン州 Oregon Digital Signature Act

<gopher://gopher.leg.state.or.us:70/00/measure.dir/Senate_Measures/sb900_dir/sb0992g.a>

カリフォルニア州 California Digital Signature Act

<gopher://sen.ca.gov>

より BILL Number AB 1577 **検索あるいは**

<http://www.sen.ca.gov/htbin/ca-html?GOPHER”_ROOT2:[BILL.CURRENT.AB1577]CURRVER.TXT;1/bill/AB1577> **など。**

フロリダ州 Florida Digital Signature Act

<http://www.scri.fsu.edu/fla-leg/bills/senate-1996/sb0942.html>

<http://www.complaw.com/pgp/digsiglegis.html>

ニューメキシコ州 ELECTRONIC AUTHENTICATION。

<httb://www.webcom.com/software/issues/nmdsregs.html>

バージニア州 VIRGINIA DIGITAL SIGNATURE ACT

<httb://leg1.state.va.us/961/ful/HB822.htm>

ワイオミング州 Electronic filing system.

<httb://legisweb.state.wy.us/96session/enroll/senate/sf0012.htm>

その他 アリゾナ、コネチカット、デラウェア、ハワイ、アイダホ、イリノイ、アイオワ、カンサス、ケンタッキー、ルイジアナ、ミシガン、ミネソタ、ニュージャージ、ニューヨーク、ノースダコタ、オクラホマ、ロードアイランド、ウェストバージニア等で制定の動きがある。

3.1.3.米国各州法の比較

別添の表 2-1,2,3,4 は米国各州の、電子署名法、ディジタル署名法の比較表であり、米国マサチューセッツ州の情報技術部門（Information Technology Division）が調査・公表している、インターネット上の情報から抜粋したものである。以下に比較点について説明する。

[Scope]　法律の適用範囲を州政府機関に限定するのか､それとも民間機関なども対象としているのかということ。

[技術的中立性(Technology Neutrality)] 前提としている技術をどこまで規定しているか。 “digital signature” は、 公開鍵システムによるディジタル署名を前提としていることを、”neutral” は特定の技術を前提とせず単に電子的な方法による署名と表現されていることを、表している。広義の電子署名は、電子ペンを用いて書くことにより得られる電子署名を含む。これに対して、暗号系、特に、非対称暗号系を用いて数学的アルゴリズムによる演算によって得られるディジタル署名は、電子署名の一手法であり、多くの場合、電子署名と混同されている。 技術を特定すれば、いわゆる公開鍵インフラを共通に利用することが期待される。これに対して、中立的な規定、広義の定義にとどまれば、将来的な技術進歩の変化に対応できると期待されている。

ECOM WG8 で策定された認証局ガイドラインは狭義の電子署名、即ちディジタル署名に関する認証局に関するものであり、そのスコープについての見解はガイドラインの冒頭に説明されている。広義の認証局は、電子署名に限定されず、バイオメトリックスなどにより本人を認証する機関と解釈するのが正確であろう。

[Signing/Writing] 従来の紙を用いる慣習での署名とか、書くという表現は、紙を用いた場合の定義に基づいている。紙のかわりに電子情報が利用されるようになると、従来用いていた署名もしくは書くという言葉の定義あるいは、解釈を再度する必要がある。このような記述があるかどうか。

[責任(Liability)]　認証局発行の証明書利用に関する責任の範囲の記述。

[許認可(License)]　認証局運用に対して、当局の許認可制に関する記述。

[証拠に関する記述(Evidentiary Rules)]　法廷における証拠物件としての電子情報に関する記述。

3.1.4.関連 URL

インターネット上の最新情報として以下の WWW サイトがある。(1997 年３月時点)
<http://www.webcom.com/software/issues/1digsig.html> 米国および国際のデジタル署名法、暗号、デジタル署名の背景情報等が案内されている。

<http://www.magnet.state.ma.us/itd/legal/>

3.1.5.NIST (National Institute of Standards and Technology)

連邦公開鍵インフラ、Federal Public Key Infrastructure では、異なる公開鍵技術基準間での相互運用に関する考察が行われている。FIPS (Federal Information Processing Standards) では公開鍵インフラの整備のために各種の活動が行なわれている。最近、認証ポリシー及び認証局実施基準作成のフレームワークのドラフト策定を行なっている。 <http://csrc.nist.gov/pki/welcome.html/>

3.1.6.ANSI/IISP

American National Standard Institute の Information Infrastructure Standard Panel。公開ドキュメント<http://www.ansi.org/iisp/need32.html>には、今後、”Authentication of content” の標準が必要であるとしている。その中で、幾つかの公開鍵認証管理のインフラが共存し、この標準が政府、科学データ、ビジネス情報、医療、娯楽、標準化の開発、そして電子出版物を用いた国家安全保障管理等に必要であるとしている。

A standard to describe a means by which the origin of content can be reliably determined is needed. It should provide a means of stamping or certifying content as having a particular origin (e.g., by identifying an individual or provider organization) and for applications and human interfaces to display that information. The standard should permit a variety of supporting services (e.g., one or more public key certificate management infrastructures) to be used in implementing the authentication service. The standard should specify programming interfaces for associating and validating content origin information. This standard is needed in government, scientific data, business information, medicine, entertainment, standards development, and national security management electronic publishing applications.

3.1.7.合衆国政府の暗号政策Clipper III

EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET の公開ドキュメント Draft paper, “Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure”, <http://www.epic.org/crypto/key_escrow/white_paper.html>の中で、KMI (Key Management Infrastructure) の必要性、CA が法律に準拠して運用されるべきことが述べられている。国際間での合意に関する記述、国際間での相互認証に関する記述がある。

3.2.ドイツディジタル署名法

同署名法ではセキュリティの基準についての条件付きで、欧州経済圏で発行されたディジタル署名にも適応されるとしている。秘密鍵の行使の際に、バイオメトリックス技術等を使い本人確認をすることが望ましい等の勧告が含まれている。ドラフトとその英文訳が以下にある。
<http://outworld.compuserve.com/homepages/ckuner/>

3.3.カナダ、 チリ

カナダ、チリで制定の動きがある。国際商工会議所 ICC の関連委員会で Authentication and Certification Practices” ではカナダ、チリ等を含めた各国の関係法制度が参照されている。

3.4.英国（Licensing of Trusted Third Parties for The Provision of Encryption Services ）

暗号技術を基にした信頼できる第 3 者機関の認可制度が提案されている。TTP に対して鍵預託(Key escrow) が行われるべき事が含まれている。本人の他に、公権が必要に応じてこのしくみを利用することが含まれる。<http://dtiinfo1.dti.gov.uk>

3.5.国際的標準の動き

3.5.1.ISO/IEC

情報技術におけるセキュリティに関するの小委員会、SC27 がある。現在、WG 1 において、認証局を含む信頼出来る第三者機関(TTP)の運用ガイドラインが検討されている。

3.5.2. UNCITRAL

電子商取引に関するモデル法がある。認証局に関するものは現時点ではまだ公表されていない。

<http://www.un.or.at/uncitral/>

3.5.3.OECD

<http://www.oecd.org/publications/catalog/> OECD 出版物のタイトルには認証局そのものはない。またこれに関する報告はまだのよう。関連のものとして”Guidelines for the security of information systems” <http://www.oecd.org/dsti/iccp/legal/secur-en.html>。暗号政策に関するものは、”Ad-hoc Meeting on Exports on Cryptography Policy”,Dec.18,1995,

<http://www.us.net/”steptoe/276908.htm>。

1997 年 3 月下旬に暗号政策に関するガイドライン策定の正式発表があった。

<http：//www.oecd.org/dsti/iccp/crypto-e.htm>。このガイドラインには以下の 8 つの基本原則がうたわれている。

1. 情報システム、通信システム利用における信頼性を出すために、暗号方式は信用のおけるものでくてはならない。
2. 一般利用者は、適用される法律に従い、暗号方式方式を選択する権利を有しなければならない。
3. 暗号方式は必要性、個人の責任と要求度、ビジネス、そして政府からの要求に応じて開発されなければならない。
4. 暗号方式の技術標準、基準、そして交換規約は国家および国際レベルで開発され、また公表されるべきである。
5. 通信の秘密と個人情報の保護を含む、個人のプライバシーという基本的権利は、国家の暗号政策と暗号方式の実施において考慮されなければならない。
6. 国家の暗号政策は、暗号化されたデータの平文、あるいはその暗号鍵に合法的にアクセスする

ことを許すであろう。

7. 契約もしくは法律のもとで確立しようとも、個人と、暗号サービスの提供、あるいは、暗号鍵を管理もしくはアクアセスする主体との間の責任は明確に宣言されてけければならない。
8. 国家間においては暗号政策の協調に関して協力すべきである。この努力のひとつとして、貿易に対する不公平な障害を撤廃し、あるいは、暗号政策の名のもとに生成してはならない。

3.5.4.ICC(International Bureau of Chambers of Commerce)

プロジェクト E-100 を設立して、電子取引に関する活動を行なっている。前出 ICC Document No.E100-26/1 “Uniform International Authentication and Certification Practices” では関連国際法、各国の関係法制度、米国各州の電子署名法が 参照されている。この中で、認証局の相互運用に関する記述は見当たらない。 また、現時点で日本からこのプロジェクトに対する寄与はないようである。

3.5.5.IBCC (International Bureau of Chambers of Commerce)

IBCC-Net は国際的な EC のテストベッド。<http://www1.usa1.com/ibnet/ediobjct.html>。 日本からは中小企業国際情報ネットワーク<http://www.gin.ipa.go.jp/> が参加している。各国連絡先は<http://www.cordis.lu/esprit/src/smecoord.htm>。

日本国内は MITI/Masaaki Kobashi 氏 e-mail:kmaa9627@miti.go.jp, と MPT/Jun Okayama 氏 e-mail:j-okayama@mpt.go.jp。IBCC-Net の目的の中で、Thema2 に Privacy and Security (including confidenciality, authentication, certification, etc,) とある。IBCC は ICC の下部組織であるので、電子商取引に関する活動は E-100 と重なっているものと思われる。

4.付録　検討メンバーリスト

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・サブリーダー

中村 吉人　リーダー　　三菱商事株式会社 マルチメディア事業推進部 次長

田吹 隆明　サブリーダー　株式会社キャディックス 第二営業部 課長

メンバー

渥美 懋　　日本アイ・ビー・エム株式会社 ＮＣ事業推進 シニアマネージャー

倉部 啓　　ビザ・インターナショナル　メンバー・リレーションズ

佐藤 順一　日本信販株式会社 マルチメディア推進室 チーフマネージャー

杉森 眞二　株式会社ジャストシステム 技術本部 開発企画部

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

中村 彰宏　株式会社日本総合研究所 事業企画部 副主任研究員

吉川 義幸　ﾏｽﾀｰｶｰﾄﾞ・ｲﾝﾀｰﾅｼｮﾅﾙ・ｼﾞｬﾊﾟﾝ・ｲﾝｸ日本支社 ディレクター

平成９年３月発行

発行：電子商取引実証推進協議会

東京都江東区青海２－４５

タイム２４ビル１０階

Tel　　03-55310061㈹

E-Mail　info@ecom.or.jp