認証に関わる諸外国の法制度
調査報告

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

オープンな環境をベースとする電子商取引が進展するにつれ、その特徴の１つである国境を越えたグローバルな取引形態の実現が予測されている。グローバルな電子商取引の実現に際して、それ以前に実施されている地域限定もしくは単一アプリケーション向けの認証ドメインが国際的に連携を取ったり、グローバル・ドメインを形成する等の所謂国際相互認証が必要になる。

国際相互認証を実施するためには、各国の認証局が採用している認証ポリシー、認証書フォーマット、暗号アルゴリズム等の技術的な整合性を図る事が重要であるが、それ以前に考慮すべき事項として各国の電子商取引に関連する制度、特に法制度の相違による影響を明らかにする事が挙げられる。

受発注電文にデジタル署名を付して電文の完全性、発信者の身元の正当性を保証しても、その有効性の解釈に違いがあったり、取引当事者の真正性を保証する認証書を発行する認証局の有効性に対する理解が異なったり、暗号の利用に対する制限の有無があったりしては、安心してグローバルな電子商取引を行なう事が出来ない。

本報告書は、こうしたグローバルな電子商取引を推進するために理解しておく事が必要と思われる各国の法制度の内、認証に関わるものを調査した結果であり以下の内容で構成されている。

- デジタル署名法
- 認証局認可制度
- 暗号規制

本報告書は、巻末にある参考文献に基づいて調査した結果であり必ずしも全ての国の状況を網羅しているものではない。又、電子商取引に関連する技術、ビジネス環境等が必ずしも安定しているとは言えない現在、それに関わる法制度への各国の取り組み姿勢にはかなりの違いがあるが、弾みがつく事により急激に変化する可能性もある事も留意願いたい。

本書は、平成８年度に「海外認証局活動調査報告」を作成後、継続して活動してきた下記グループによってまとめられたものです。
関係各位から忌憚のないご意見、ご要望を期待していますので、下記までお寄せ下さい。

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/国際相互認証検討サブワーキンググループ
(WG08/SWG3)
〒135-8073 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

目次

1 デジタル署名法

現在幾つかの国においてデジタル署名に関する法制度整備の動きがある。その多くは、電子的な認証を法制度において手当てすることにより、電子的情報処理による効率的な情報交換を目的としている。そのような法制度の対象は、一般的な電子的認証、手書き電子署名を含む広義の電子署名、そして公開鍵暗号システムによる狭義の電子署名までその分布には広がりがある。

本章は特に暗号鍵による電子的署名、狭義には X.509 認証のしくみ（PKI）において今後必要であると考えられる認証局の国際的相互認証を実現するにあたり、法制度上どのような問題が考えられるかとの視点に立って調査したものである。調査対象は、主として X.509 認証のしくみを含む法制度、電子商取引やビジネス上で利用されるであろう国際的な電子的情報交換に関係すると思われる法制度に限定している。

PKI ベースで認証書を発行する機関は、当 WG では認証局と表現しているが、広義の電子署名を包含する法制度では意味合いが多少違ってくる。しかしながら、この章ではいわゆる信頼できる第三者機関として、手書き電子署名等を含む一般的な認証サービスを提供する実体も含めて認証局と表現している。

1.1 調査国並びに調査項目

(1) **法律の状態・分類**
法文の分類であり、Act、Bill、Draft、Proposed、Regulation 等に分類している。Draft や Proposed の場合法的には未だ拘束力を持っていないが調査対象としている。

(2) **法規の適用範囲**
全てに適用されるのか公的機関だけなのか等という内容。

(3) **署名の定義と範囲（技術特性）**
公開鍵インフラ（PKI）をベースとしているのか、単にデジタル署名であるのか、あるいは広く電子署名としているのかを区別する。認証局の相互認証という点からは公開鍵インフラをベースとした法制度と関係が大きい。電子的な認証は新しい技術分野であり、言葉の使いかたも各法制度によって違っている。言葉は各法制度の中で慎重に定義されているが、electronic signature, digital signature, の意味するところは微妙に違っている。一般に、digital signature（デジタル署名）は暗号による署名を、electronic signature（電子的署名もしくは電子署名）は暗号による署名と電子的処理による手書き署名を意味することが多い。

(4) **認証局の責任**
認証局に責任があった場合、相互認証において発生する責任分担をどうするかの問題がある。ここでは認証書の発行の後、利用者が何らかの損失を被ったような場合、その損失に対する責任等を法制度で規定している場合、そのような内容を説明している。

(5) **デジタル署名有効性・証拠力**
一般にデジタル署名法はデジタル署名に法的効力を認める目的で策定されている。従来、紙に手書きで書かれた書名の法的規定があった。通常は電子的記録に対して手書き署名と同様の効果をデジタル署名にも認める内容であることが多い。

(6) **義務・要件**
認証局には一般にいろいろな意味において信頼性が求められている。この点において法制度のなかで規定している場合がある。例えば、資本金、監査条件、信用力、ユーザに対する責任通知義務、発行数等が規定される。

(7) **認証局の相互認証**
認証局の相互認証について規定している法制度は少ない。これは相互認証そのものが、効力を有する法制度の範囲の外側との関係であるあることに一因がある。通常は国際間の相互運用の重要性、国家間の相互提携の必要性や可能性を追求するべきだとの点に触れている。

(8) **料金の考え方**
法で料金を規定している場合、相互認証では相互の料金体系が大きく異なっていると問題となること予想される。

1.2 米国

米国は州法としてデジタル署名法、電子署名法の制定が進んでいる。この背景には American Bar Association **のデジタル署名ガイドラインの策定、各州政府が業務の電子化に対して積極的に取り組んできたことがあげられる。その先鋒となったのはユタ州デジタル署名であり、現在多くの州で発効、あるいは策定が進行している。現在、連邦政府としての明示的な電子署名法はない。**
電子署名法の多くは認証書発行機関等に関する規定であるが、これとは別に電子的署名を規制の中で認める規制緩和の動きがある。食品・薬品局（Food and Drag Administration**）では数年の検討の結果、電子記録・電子認証に関する規制を策定し、**1997 **年** 8 **月に発効した。その中で一定要件のもとで暗号による電子署名や広くバイオメトリックスによる認証手段を認めている。従来、紙媒体と手書き署名により諸手続きが規制されていたところを電子的に処理するため要件を与えている。統一商法典（**Uniform Commercial Code**）の** 2B **編では電子的な署名の法的効力について議論されているものの、認証書発行機関等に関する議論がないためここでは含まれていない。この章では認証書発行機関の相互認証の観点から関係するものに限定し、それ以外の法制度は除かれている。**

1.2.1 米国連邦政府関係

1.2.1.1 電子金融サービス法（Electronic Financial Services Efficiency Act of 1997）

米国の資本市場、決済システムの健全な発展のために従来の紙ベースのしくみに代わる電子的認証を認めることを目的としている。

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Act (1997 House Bill 2937)

(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て

(3) **署名の定義と範囲（技術特性）（**PKI/**デジタル署名/電子署名）**
電子署名

(4) **認証局の責任**
規定はないが、認証局はこの法律が定める全米認証局協会（NACA: National Association of Certification Authority**）のメンバーになり、その中で構成される電子認証標準化審議会（**Electronic Authentications Standards Review Committee**）が責任について定めるとしている。**

(5) **デジタル署名有効性・証拠力**

規定なし

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
規定なし（NACA により評価されることになる）

(7) **認証局の相互認証**
規定なし

(8) **料金の考えかた**
規定なし

1.2.2 米国州法

1.2.2.1 ユタ州デジタル署名法(Utah Digital Signature Act)

ユタ州は世界的に見てもデジタル署名法を最初に制定したことで有名である。この法律は民間の認証局の許認可制を定めており、これにより Digital Signature Trust 社が認可を取得した。（初期は 1997 年 11 月 13 日から 6 ヶ月間）

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
一般

(3) **署名の定義と範囲 （技術特性）（**PKI/**デジタル署名/電子署名）**
PKI

(4) **認証局の責任**
認証書に記載の勧告信頼限度額

(5) **電子情報の証拠力**
無免許認証局の発効した認証書の法的効力もある

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
- 運用すべき信頼システムの要件が定義されている
- 監査の条件（１回/年、監査人の要件、監査免除の条件）
- 禁止事項
- 認証局の義務（開示情報、発行・運用業務）
- 鍵預託の要件

(7) **認証局の相互認証**
規定なし

(8) **料金の考えかた**
失効手続に関する料金の問題点と指針が与えられている

1.2.2.2 ユタ州デジタル署名実施法(Digital Signature Administrative Rules)

ユタ州デジタル署名法の実施に際しての規則として制定された。

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Rule

(2) **法規の適用範囲（指定なし/公的機関/全て）**
ユタ州デジタル署名法に準ずる

(3) **署名の定義と範囲 （技術特性）（**PKI/**デジタル署名/電子署名）**
ユタ州デジタル署名法に準ずる

(4) **認証局の責任**
ユタ州デジタル署名法に準ずる

(5) **電子情報の証拠力**
ユタ州デジタル署名法に準ずる
(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
- **当局への登録料金（年間**$500.00）
- **保証金として**$75,000.00 **を納める**
- **開示情報項目（住所、**URL **等）**
- **十分な資本、**$5,000.00 **以上、があることの提示**
- **認証書の項目**
- CPS **の形式**
- **保管記録の条件**
- **認証業務停止時の義務**
- **リポジトリの要件**
- **監査人の要件**
- **規則の見直しについて**

(7) **認証局の相互認証**
規定なし
(8) **料金の考えかた**
認証局と当局との料金が与えられている

1.2.2.3 カリフォルニア電子署名法(California Government Code 16.5,1995)

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation）
Code 16.5(1995), 1995 California AssemblyBill1577
(2) **法規の適用範囲（指定なし/公的機関/全て）**
公的機関
(3) **署名の定義と範囲（技術特性）（**PKI/**ディジタル署名/電子署名）**
電子署名
(4) **認証局の責任**
規定なし
(5) **デジタル署名有効性・証拠力**
電子署名は５つの要件のもとで従来の手書き署名と同じように有効である
- **利用者に固有であること**
- **照合可能であること**
- **利用者のみにより管理されている**
- **データに結合しており、データの変更に対して無効になる**
- **州長官が採用する規制に適合している**

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
規定なし
(7) **認証局の相互認証**
規定なし
(8) **料金の考えかた**
規定なし

1.2.2.4 カリフォルニア電子署名規制法(California Digital Signature Regulations)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Regulation、Code 16.5 のに対する規制

(2) **法規の適用範囲（指定なし/公的機関/全て）**
公的機関

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI

(4) **認証局の責任**
規定なし

(5) **デジタル署名有効性・証拠力**
Code16.5 に準ずる

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
州当局の信用審査を受ける

(7) **認証局の相互認証**
規定なし

(8) **料金の考えかた**
規定なし

1.2.2.5 フロリダ州電子署名法(Electronic Signature Act of 1996)

認証局の認可や要件については今後検討される。

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
電子署名とデジタル署名とを定義

(4) **認証局の責任**
規定なし

(5) **デジタル署名有効性・証拠力**
手書き署名と同様

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
規定なし、州当局自身は可

(7) **認証局の相互認証**
規定なし

(8) **料金の考えかた**
規定なし

1.2.2.6 フロリダ州電子署名法(1997 Florida House Bill 1413)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Bill 1413

(2) **法規の適用範囲（指定なし/公的機関全て）**
公証業務、公的技術文書

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI

(4) **認証局の責任**
規定なし

(5) **デジタル署名有効性・証拠力**
手書き署名と同様
(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
鍵失効の手続き
(7) **認証局の相互認証**
規定なし
(8) **料金の考えかた**
規定なし

1.2.2.7 イリノイ州電子商取引安全法(Illinois Electronic Commerce Security Act)

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Act
(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て
(3) **署名の定義と範囲（技術特性）（**PKI/**デジタル署名/電子署名）**
PKI を含む電子署名
(4) **認証局の責任**
規定なし
(5) **デジタル署名有効性・証拠力**
通常の署名と同じ
(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
- 信頼性
- 情報公開（CPS，鍵失効等）

(7) **認証局の相互認証**
規定なし
(8) **料金の考えかた**
規定なし

1.2.2.8 ミネソタ州電子認証法(Minnesota Electronic Authentication Act)

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Act
(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て
(3) **署名の定義と範囲（技術特性）（**PKI/**デジタル署名/電子署名）**
PKI
(4) **認証局の責任**
ユタ州法に類似（制限つき）
(5) **デジタル署名有効性・証拠力**
一定要件のもとで有効
(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
認可条件を規定
(7) **認証局の相互認証**
規定なし
(8) **料金の考えかた**
規定なし

1.2.2.9 ミシシッピ州デジタル署名法(Digital Signature Act of 1997)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI

(4) **認証局の責任**
不明

(5) **デジタル署名有効性・証拠力**
認可された発行機関の認証書により有効

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
州の長官は認証書を発行することができ、さらに私的機関を以下の条件で認可する
- 暗号技術に精通している
- 十分な資本
- 州内に事務所がある

(7) **認証局の相互認証**
不明

(8) **料金の考えかた**
不明

1.2.2.10 ニューハンプシャー州法(1997 New Hampshire S．B．207)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Bill 290

(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI

(4) **認証局の責任**
不明

(5) **デジタル署名有効性・証拠力**
手書きと同様

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
州の長官は認証書を発行することができる

(7) **認証局の相互認証**
不明

(8) **料金の考えかた**
不明

1.2.2.11 ニューメキシコ州電子ドキュメント認証法(Electronic Authentication of Documents Act)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
指定なし

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）

デジタル署名

(4) **認証局の責任**
電子文書局が認証局になり、公開鍵の保持、管理を行なう

(5) **デジタル署名有効性・証拠力**
記述なし（この法律で管理される公開鍵の場合は有効と理解される）

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
電子文書局は公開鍵を公開、管理する

(7) **認証局の相互認証**
記述なし

(8) **料金の考えかた**
記述なし

1.2.2.12 ニューヨーク州デジタル署名法(Digital Signature Act)

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て

(3) **署名の定義と範囲（技術特性）（**PKI/**デジタル署名/電子署名）**
PKI

(4) **認証局の責任**
有限責任

(5) **デジタル署名有効性・証拠力**
記述なし

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
ユタ州法に類似

(7) **認証局の相互認証**
記述なし

(8) **料金の考えかた**
記述なし

1.2.2.13 オレゴン州署名法(1997 Oregon House Bill 3046)

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Bill 3046

(2) **法規の適用範囲（指定なし/公的機関/全て）**
不明

(3) **署名の定義と範囲（技術特性）（**PKI/**デジタル署名/電子署名）**
PKI を含む電子署名

(4) **認証局の責任**
●消費者/ビジネスサービス局が認証書を発行する
●消費者/およびビジネスサービス局は発行機関を登録する権限をもつ

(5) **デジタル署名有効性・証拠力**
通常署名と同等に有効

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
不明

(7) **認証局の相互認証**
不明
(8) **料金の考えかた**
不明

1.2.2.14 テキサス州署名規制法(1997 Texas H.B. 984)

カリフォルニア州電子署名法に類似している。

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Draft Rule
(2) **法規の適用範囲（指定なし/公的機関/全て）**
不明
(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI と動的電子署名
(4) **認証局の責任**
規定なし
(5) **デジタル署名有効性・証拠力**
通常署名と同等に有効
(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
監査、信用力等の審査を州当局が行なう
(7) **認証局の相互認証**
記述なし
(8) **料金の考えかた**
記述なし

1.2.2.15 バーモント州署名法(1997 Vermont House Bill 60)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
1997 Vermont H.B. 60
(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て
(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI
(4) **認証局の責任**
上限を定めその範囲に限定
(5) **デジタル署名有効性・証拠力**
通常署名と同等に有効
(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
ユタ州法に類似（州当局が認証書を発行する場合と、発行機関を認可する場合がある）
(7) **認証局の相互認証**（4624 条,(e)項）
- 他州の相当の規則が同等と認められる場合にはお互いの州政府同士で相互に認め合う
- 相互に認証している場合には法的効果も同様とする

(8) **料金の考えかた**
記述なし

1.2.2.16 ワシントン州電子認証法(Washington Electronic Authentication Act)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI

(4) **認証局の責任**
上限を定めその範囲に限定

(5) **デジタル署名有効性・証拠力**
通常署名と同等に有効

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
ユタ州法に類似（州当局が認証書を発行する場合と、発行機関を認可する場合がある）

(7) **認証局の相互認証**（新しい WAC 434-200-245 項）
認証局同士の相互認証に関するものではない
- 他州の相当の規則が同等と認められる場合にはそこでの認可を審査する
- 他州から審査を受けるには 2 万 5 千ドルの保証金を納める
- 相互に認証している場合には法的効果も同様とする

(8) **料金の考えかた**（WAC 434-200-130 項）
- 発行機関としての認可には 5 万ドルの保証金が適当としている
- 認証業務従事者の刑罰に関する適確審査の費用は 25 ドル、資格試験は 50 ドル

1.3 ドイツ国デジタル署名法(German Digital Signature Law/Ordinance)

1997 年 6 月 13 日に議会を通過し、同年 8 月 1 日に発効したマルチメディア法の第 3 条がデジタル署名法であり、同法には実施規則がある。このデジタル署名法は安全な PKI を実現する目的で策定されている。

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
指定なし

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名/手書きの電子署名）
PKI

(4) **認証局の責任**
特に規定されていない

(5) **電子情報の証拠力**
デジタル署名の法的有効性についてはふれていない

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
- セキュリティ計画書の提出、確保すべきセキュリティレベル
- ドキュメントの保存期間
- 利用者の情報保護
- 利用者に対するセキュリティに関する情報提供

(7) **認証局の相互認証**

国際的な協定のもとに海外の認証書も有効である

(8) **料金の考えかた**
当局の審査の料金は示されているが発行機関の料金は示されていない

1.4 英国

２章 認証局認可制度を参照のこと。

1.5 フランス

３章 暗号規制を参照のこと。

1.6 イタリア

デジタル署名法が 1997 年 3 月 15 日に発効している。規制法についてはドラフトの段階にある。

1.6.1 イタリアデジタル署名法

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
不明

(3) **署名の定義と範囲（技術特性）（**PKI/**デジタル署名/電子署名）**
デジタル署名

(4) **認証局の責任**
一般に、鍵ペア管理の過失により損失を与えた場合には補償しなければならない

(5) **デジタル署名有効性・証拠力**
通常の署名同様に有効

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
不明

(7) **認証局の相互認証**
不明

(8) **料金の考えかた**
不明

1.6.2 イタリアデジタル署名規制法

(1) **法律の状態・分類（**Act/Bill/Draft/Proposed/Regulation**）**
Draft Regulation

(2) **法規の適用範囲（指定なし/公的機関/全て）**
不明

(3) **署名の定義と範囲（技術特性）（**PKI/**デジタル署名/電子署名）**
デジタル署名

(4) **認証局の責任**
不明（デジタル署名法に準拠）

(5) **デジタル署名有効性・証拠力**
不明（デジタル署名法に準拠）

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
公的、私的でも公開鍵を 10 年間以上保管する

(7) **認証局の相互認証**

不明

(8) **料金の考えかた**
不明

1.7 アルゼンチン

行政省の電子署名小委員会により法案が策定されている。法案では、行政における非対称暗号システムによるデジタル署名の利用が規定されている。

1.8 マレーシアデジタル署名法(Digital Signature Bill 1997)

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
Act

(2) **法規の適用範囲（指定なし/公的機関/全て）**
全て

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名）
PKI

(4) **認証局の責任**
種類に応じて上限を定める

(5) **デジタル署名有効性・証拠力**
認可を受けた発行機関の認証書であれば有効である

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**
全ての認証書発行機関は認可が必要（内部利用は除く）、一般的要件として、
- 信頼されるシステム
- 要求による情報公開
- 利用者への認証書発行の必要条件
- 発行された認証書の公開
- 間違って発行された認証書の失効手続き
- 要求による鍵失効の手続き

(7) **認証局の相互認証**（Recognition of other licenses）
認証局の相互認証に関する直接の記述はないが、関連する内容として、
- 当局は海外で認可された機関が規定の要求を満たせば認可する
- 海外の認証局の責任には上限がある

(8) **料金の考えかた**
記述なし

1.9 UN/UNCITRAL の電子署名一般規則（Draft Uniform Rules on Electronic Signatures）

現在、電子署名、認証局、関連の法的事項についての検討計画が策定中である（文書番号A/CN.9/437、A/CN.9/WG.IV/WP.73）

(1) **法律の状態・分類**（Act/Bill/Draft/Proposed/Regulation）
ドラフト

(2) **法規の適用範囲（指定なし/公的機関/全て）**
国際統一規則

(3) **署名の定義と範囲（技術特性）**（PKI/デジタル署名/電子署名） Article 1

電子署名をひろい意味での電子的署名とし、その中でも個人に対応した特性をもつものとしてセキュア電子署名の要件を与えている。このドラフトでは特に PKI ベースのデジタル署名について検討されている。

(4) **認証局の責任**

1. Article 11. 契約上の責任

①認証局と利用者間の責任は契約により決められる。

②認証局は契約により、認証書の記載事項、もしくは技術的不可避な事項について責任を回避する。しかし契約の主旨に則り契約内容があまりにも不公平であれば、責任回避もしくはその有限性については別となる。

③認証局の意図的な行為あるいは不注意によって発生した損失の場合、認証局の責任は有限ではない。

2. Article 12. 認証書の利用者に対する認証局の責任

相互契約がない場合、認証書を発行する認証局は、以下の事象に対してその利用に次の責任を負う。

①認証書の記載内容の誤り

②失効要求に対する手続きの不履行

③以下の事項の無視：

ａ認証局により公表される認証実施規定、CPS の内容

ｂ適用される法律

但し、以下の除外規定が設けられている。

①認証局もしくはその代理機関が問題発生防止に対してあらゆる措置をとったことを示すことができる場合、あるいは認証局もしくはその代理機関がそのような措置をとることが不可能であったことを示すことができれば、認証局は責任を回避することができる。

②認証局は認証書においてその利用目的を限定することができる。認証局はそのような目的以外に使われた場合の損害について責任を負わないでよい。

③認証局は認証書において認証書が有効であるトランザクションの金額を制限することができる。認証局はそのような金額を超える損害に対しては責任を負わないでよい。

(5) **デジタル署名有効性・証拠力** Article 5

1. (a)認証書の有効期間のもの、(b)個人に対応していることが、(i)認可された認証局発行である、（ii）もしくは基準に基いた認証局が発行した認証書である、ことにより確かである。
2. あるいは認証書が利用者と正しく対応していることが状況からもっともらしい。

等の条件による。

(6) **義務・要件（資本金、監査、信用力、ユーザに対する責任通知義務、発行数等）**

パラグラフ 48 では認可認証局について以下の項目を検討したいとしている。

- 独立性
- リスク損失に耐えられる経済的基盤
- 暗号技術などへの精通していること
- 継続性
- ソフトウェア、ハードウェアの承認
- 監査証跡の保持、外部からの監査

- **非常事態対応計画**
- **信頼できる人選**
- **認証局自身の秘密鍵の保護管理対策**
- **内部セキュリティ**
- **利用者への通知を含む業務停止に対する対策**
- **保証とその表示**
- **責任の範囲**
- **保険**
- **他認証局との相互運用性**
- **（鍵紛失もしくは不正利用時の）鍵失効の手続き**
- **認証局のサービスのうち認証機能の独立性**

(7) **認証局の相互認証**

1. Article 17. **この規則によりサービスを提供する国外認証局**

①変則 A(1)**： 国外の機関は、もし国内で認証局となろうとする機関が従うのと同一の基準に準拠し、同一の手続きに従うのであれば、国内で認証局となることができる、あるいは国内に存在することなしに国外からサービスを提供することができる。**

②変則 B**：国外の認証局を認可することに関する規則を策定する権限を国から与えられている機関は国外認証局を認可する権限を有し、その認可規則を策定する。**

2. Article 18. **国内認証局による国外認証局の保証**

実施国の法律のもとに運用されている認証局により認知されており、その認証局が自身の認証書と同じ水準で認証書の項目についての正しさと有効性を保証するのであれば、国外認証局から発行された認証書はこの規則で対象とする認証書と同じ意味でデジタル署名に利用することができる。

3. Article 19. **国外認証書の認知**

①国外認証局の運用実施が少なくともこの規則のもとでの認証局に要求されている信頼性の水準と同じであれば、国外認証局で発行された認証書は実施国の法律のもとで運用されている認証局発行の認証書と法的に同等であるとみなされる。

②他国の法律が要求している信頼性の水準が、実施国の法律に準拠している記録あるいは署名のそれと少なくとも同じであれば、デジタル署名あるいはその他の電子署名に関する他国の法律に準拠している署名および記録は、この規則に準拠する署名および記録と法的に同等であると理解される。[そのような認識は国家間もしくは多国国家間の公開された合意により得られるであろう。]

③国外認証局の認証書があらゆる状況に照らして信頼できるものであり、発行された目的のために妥当なものであれば、国外認証局で発行された認証書を参照して照合されるデジタル署名は、法廷や当事者にとって効力を有するものである。

④前項に拘わらず、政府機関は政府機関に提出されるメッセージもしくは署名に関して、特定の認証局、認証局の水準、あるいは認証書のクラスが使われなければならないことを指定することができる。

(8) **料金の考えかた**

規定なし

2 認証局の認可制度

認証局が発行する認証書が、電子商取引において本人の身元を確認出来る重要な証明である事を認識し、国もしくは州政府が認証局の義務・責任、運用のための要件等を定め、認可制を制定しているもしくはそうしようとしている所がある。その様な国もしくは州は、他の国から送られてきた認証書が、その国の政府が認可した認証局が発行したものでないと受け入れない場合がある。これも国際相互認証の実現を阻害する要因になる。多くの国もしくは州の場合、認証局の認可制はデジタル署名法にリンクして制定されるきらいがあるが、英国のように独自に認可制を設け様とする動きもある事や、米国の州でデジタル署名は規定しているが認証局の認可制は規定していない州もある。

2.1 米国

Utah 州、Washington 州では各々認証局の許可制度を法制化。
Minnesota 州は法制準備中。Florida 州、Mississippi 州、その他の州が検討中。

2.1.1 Utah 州（www.commerce.state.ut.us）

(1) **対象：デジタル署名**
(2) **技術：公開鍵**
(3) **許可取得する認証局は政府機関が民間か？：両方可能**
(4) **認証局の許可登録先：**Utah Department of Commerce
(5) **認証局の許可取得要件：**
    ① 詐欺・偽証などの前科ある従業員がいないこと
    ② 民間の場合、適当な保証の差し入れ（＊75,000 ドル）
    ③ 信頼のおけるコンピュータシステムで運用すること
    ④ 充分な資本金を有すること
    ⑤ ユタ州に自社または正規代理人の事務所を保有すること
    ⑥ その他の州の規則に従うこと
    ⑦ 規定の登録料（＊500 ドル）の支払い

    注）（＊　　）内の数字は現時点で適用されているもの。
(6) **認証局の責任：**
    ① 認証局運用規定（CPS）の公開
    ② 認証局の認証行為に不備がある場合且つ認証書に記載の推奨上限金額範囲内且つ直接損害の範囲での賠償責任
(7) **認証局の相互認証：なし**

2.1.2 Washington 州

(1) **対象：デジタル署名**
(2) **技術：公開鍵**
(3) **認証局は政府か民間か：**the Secretary of the Washington State **自身、又は許可を受けた民間または政府**
(4) **認証局の許可登録先：**the Secretary of the Washington State
(5) **認証局の許可取得要件：**
    ① 規定の登録料の支払い
    ② 民間の場合、適当な保証の差し入れ
    ③ 充分な資本金を有すること
    ④ 信頼のおけるコンピュータシステムで運用できること且つ監査報告書の提

出
⑤ 申請認証局の運用従業員が、詐欺・偽証などの前科がないことなど、要件を満足することを示す書類の提出
⑥ 書面の認証局運用規程（CPS）を有すること

(6) **認証局の責任：**
① 認証に係る記録の保管（失効後 10 年間）、その他の記録 5 年間保管
② Washington 州から取得の許可証の開示
③ 認証局運用規定（CPS）の the Secretary of Washington State への提出
④ Trustworthy System による運用

(7) **認証局の相互認証：**

厳密な意味での相互認証規定ではないが、Wahsington 州法は州外の政府により許可を得た認証局が次の条件を満たす時、Washington 州政府は同州と同様の認証局許可をこの州外認証局に与えるとしている。

① 州外認証局が the Secretary of Washington State に自社の許可証の写しを提示、且つ
② その州外政府の認証局許可要件が Washington 州と類似であること、且つ
③ PKI ベースであること

2.1.3 Minnesota 州

(1) **対象：デジタル署名**
(2) **技術：公開鍵**
(3) **許可取得する認証局は政府機関か民間か？：両方可能**
(4) **認証局の許可登録先：**the Minnesota secretary of state
(5) **認証局の許可取得要件：**
① 運営要員に過去 15 年間重罪又は詐欺・偽証罪の前科がないこと
② 運営要員が充分な知識・能力を有すること
③ 民間の場合、適当な保証の差し入れ
④ 信頼のおけるコンピュータシステムで運用すること
⑤ 充分な資本金を有すること
⑥ ミネソタ州に自社または正規代理人の事務所を保有すること
⑦ その他の州の規則に従うこと
⑧ 登録料の支払い

(6) **認証局の責任：**
① 充分知識を有する公認会計士による最低年一回の監査実施。州政府はこの監査結果を公開
② 認証局運用規定（CPS）の公開

2.1.4 Florida 州（案）

(1) **対象：電子署名**
(2) **技術：公開鍵**
(3) **許可取得する認証局は政府機関か民間か？：両方可能**
(4) **認証局の許可登録先：**the secretary of state
(5) **認証局の許可取得要件**
① 10 万ドルのボンド提出（但し、地方公共団体は除く）
② 州内に存在、又は、代理店を設置
③ 年間ライセンス料 500 ドル

④ 認証局自身の情報開示
⑤ システムが trustworthy であること
⑥ 充分な資本金を備えていること
⑦ 記録保存
⑧ 事業の廃業－90 日前通知
⑨ 監査を受けること

2.1.5 Mississippi 州

(1) **対象：電子署名**
(2) **技術：公開鍵**
(3) **許可取得する認証局は政府機関か民間か？：両方可能**
(4) **認証局の許可登録先：**the secretary of state
(5) **認証局の許可取得要件**
① 充分な知識を保有
② 充分な資本金を保有
③ ミシシッピ州に事務所または正規代理店を保有

2.2 ドイツ

(1) **対象：電子署名**
(2) **技術：公開鍵**
(3) **許可取得する認証局は政府機関か民間か？：両方可能**
(4) **認証局の許可登録先：当局**
(5) **認証局の許可取得要件**
① 充分な信頼を有する
② 充分な知識・能力・経験を有する
③ セキュリティ規定を保有する
④ 廃業の場合、有効な認証書にかかる記録を当局又は移管先認証局に提出する
⑤ 認証データを充分保護する
(6) **外国（ドイツ外）で発行された認証書**
EU 参加国または Agreement on the European Economic Area の参加国で承認された公開鍵で且つ本法制と同等のセキュリティレベルの電子署名は本法制での電子署名と同じ効果を有するものとする。

2.3 英国

信頼される第三機関（Trusted Third Parties）の規制および認可に関する制度化への提案が貿易産業省から 1997 年 3 月に発表されている。その中で、電子商取引において暗号使用の重要性を説きながらも、犯罪やテロリスト活動の隠れ蓑にならないよう暗号情報への合法的なアクセスのしくみが必要であるとしている。このために鍵預託もしくは鍵回復（key escrow/recovery）システムを要件としている。さらに、国際間での暗号サービスの利用について議論されている。

(1) **法規の適用範囲（指定なし／公的機関／全て）：**
国民に暗号サービスを提供する組織（公的機関と民間機関の TTP、地方、国、国際的なレベルまで）
(2) **法律の状態・分類（**Act / Bill / Draft / Proposed / Regulation**）：**Proposed

(3) **署名の定義と範囲（技術特性）（**PKI / **デジタル署名／電子署名／手書きの署名）：**
暗号サービス（PKI）

(4) **認証局の責任：**
① **十分な利用者に対する責任**
② **鍵が開示された場合、それによって被った利用者の損失を保証する。雇用人の責任も負う**
③ **責任範囲は** TTP **と利用者で取り決めることができる**

(5) **電子情報の証拠力：**
別途検討する

(6) **義務・要件（資金、監査、信用力、ユーザに対する責任通知義務、発行数等）：**
① **鍵への合法的アクセスができる鍵管理のしくみ**
- **令状の提出から** 1 **時間以内に中央のリポジトリに復号鍵を提出する、あるいはそれができる能力**
- **合法的な令状だけを認識できる能力の提示**
- **合法的アクセス要求の監査可能記録の保持**
- **合法的アクセスの安全性を妨げること、アクセス対象を明らかにしないこと**

② **信頼性の確保、技術力、財務基盤の安定性、運用の機密等の合法的な行使**
③ **データリカバリー（キーリカバリー、エスクロー）のサービス**
④ **契約ベースで秘密鍵を利用者に開示する（例えば、会社の社員が退職した場合等）**

(7) **認可の条件：**
① **情報セキュリティ関係者、管理者の信頼性**
② **情報セキュリティの管理**
③ **鍵管理と保管の情報セキュリティ装置（**ITSEC **への準拠性）**
④ **標準化とその手続きへの対応（**ISO-9000）
⑤ **ビジネスプランと長期的な経営方針の評価**
⑥ TTP **機能の独立性（他のビジネス機能からの独立性）**
⑦ **他の許可** TTP **とのインターフェース**
⑧ **組織と所有権の明確化**

(8) **認証局の相互認証：**
TTP **は相互契約を交わすことによりネットワークを形成し、その利用者は相互に安全な通信をすることができる。**
国際的な相互運用をする TTP **の要件を以下の様に与えている。**
① **国内外ともに利用できる** TTP **があり、どの** TTP **を使うかは利用者の任意である**
② **電子メールを含む全ての通信に適用する**
③ **司法の令状のもとで合法的アクセスを提供する**
④ **令状のもとでは利用者にわからないようにかつほぼリアルタイムでのアクセスを提供すること**
⑤ **送信者の悪用は受信者に通知される**
⑥ **国外の** TTP **を利用することを要求しない**
⑦ **海外の認可れれていない** TTP **とは法的な義務が発生しない範囲で相互認証する**

(9) **料金の考え方：**
①認可については、初期審査と毎年の更新費用を支払う
②TTP とその利用者については言及していない

2.4 マレーシア

(1) **対象：電子署名**
(2) **技術：公開鍵**
(3) **許可取得する認証局は政府機関か民間か：規定なし**
(4) **認証局の許可取得先**
① a Controller of Certification Authorities
② The Minister が a Controller を指名
③ a Controller は許可供与先の認証局の情報を開示
(5) **認証局の許可取得要件**
① 信頼の置けるシステムの使用
② 認証局運用規程（CPS）の開示
(6) **認証局の義務**
① 最低年一度監査を受け、本法律規定条件を満たしていることを確認する
② 許可を受けた認証局はその許可条件に明示された業務以外を行ってはいけない
③ 許可証の表示
④ 信頼のおけるシステムの使用
⑤ 発行済み認証書の公開
(7) **認証局の賠償責任範囲**
① 認証局は偽造された認証書の使用による損害は免責
② 認証局は認証書に推奨利用額を明示することができ、この額が明示された認証書で損害が発生した場合、認証局の賠償責任額はこの推奨額を上回ることはない
③ 認証局は精神的損害、又は罰則的な賠償については免責
(8) **認証局の相互認証**
the Controller は外国政府より許可された認証局を、その許可条件が本許可条件を満たす場合、認めることがある。

2.5 ＥＵ

現時点では規定はないが、デジタル署名、TTP、などを検討している。

3 暗号規制

国際相互認証において、認証に使用する暗号技術が、その認証局が属する国の法制度により異なる規制を受けた場合、認証書の発行等に使用する暗号技術の互換性が保たれず、国際間の相互認証に大きな支障をきたし、ネットワーク取引のグローバルな進展を妨げる可能性が大きい。従って、認証局同士の国際的な相互認証においては、各国の暗号政策に配慮しつつも、認証に係る暗号技術の規制に関して国際的な整合性を確保していく検討が不可欠である。
本章は、各国の「暗号製品（ソフト・機器）の使用及び輸出入に関する規制の現状」を調査した結果をまとめたものである。

3.1 米国の現状

米国においては、これまで国家安全保障及び外交政策上の観点から、国家の重要な政策として暗号製品の輸出規制が行なわれている。

(1) **法的根拠**
輸出管理法（Export Administration Act Of 1979）の輸出管理規制（Export Administration Regulations）に基づく

(2) **規制の内容**

① **使用に関する規制**
規制なし

② **輸出に関する規制**
1996 年 12 月 30 日、商務省（Department of Commerce）による輸出管理規制の一部改正により暗号製品の輸出規制が緩和され、1997 年 1 月 1 日から施行されている。具体的な規制内容は以下の通りである。

- 鍵長 40 ビット未満の一般市場向け暗号化ソフト
  暗号製品規制の対象外。商務省・輸出管理局（Bureau of Export Administration）の 7 日間の審査後、一般市場向け製品として扱われる。
- キーリカバリー可能な暗号化ソフトと機器
  暗号製品規制の対象外。商務省輸出管理局の審査後、許可（規制）対象外の「キーリカバリー可能暗号ソフトおよび機器（Recoverable Software and Equipment）」として扱われる。
- 優良企業のサポートと製品・サービスの販売計画のある鍵長 56 ビット以下の DES（Data Encryption Standard）または、同等の強度を持つ非キーリカバリー暗号化ソフトおよび機器
  暗号製品と販売計画を商務省輸出管理局が審査後、6 ヶ月有効な輸出または再輸出許可が発行される。
- 対金融機関向け暗号製品
  基本情報、決済情報のみを送信する対金融機関向け取引に限定した暗号製品であれば、DES56 ビット、RSA1024 ビットまで輸出許可が発行される。
  （例：マイクロソフト、ネットスケープ、ベリフォン、IBM 等の SET 製品）
- その他の暗号製品

A. 暗号許可契約を有するもの
現在、国際武器通商規則（International Traffic in Arms Regulations）の下で許可されている配布と管理に関する協定が継続適用される。

B. 暗号許可契約の無いもの
ケースバイケースで個別許可となる。
C. 暗号技術の申請
暗号技術の輸出および再輸出の申請は、ケースバイケースで個別許可となる。

③ 輸入に関する規制
規制なし

3.2 イギリスの現状

EU 諸国においては、欧州連合議会規制（EU Council Regulation：ECR）等の取り決めに沿った規制がなされており、EU 域外への輸出に限り規制されているところが多い。
イギリスにおいては、情報セキュリティ社会への企業や産業界の参加を促進する目的で、EU 諸国と共同で許可を受けた TTP による有益な暗号製品に適用する輸出規制を簡素化する方向にあり、1997 年 3 月 21 日、貿易産業省（Department of Trade and Industry）は TTP（Trusted Third Party）に関する提言を発表している。

(1) 法的根拠
輸出入および関税法（Import , Export and Customers Powers Act）に基づく

(2) 規制の内容
① 使用に関する規制
規制なし
② 輸出に関する規制
EU 域外へ向けた暗号製品の輸出のみ規制されている。輸出には貿易産業省による許可が必要となる。
③ 輸入に関する規制
規制なし

3.3 ドイツの現状

ドイツにおいても、ECR に沿って EU 域外への輸出に限り規制されている。また、1997 年 7 月に「デジタル署名法（Gesetz zur Digitalen Signatur）」が成立しているが、暗号に関する法制度については未整備となっている。

(1) 法的根拠
Sechsunddreissigste Verurdnung zur Anderung der Aussenwirtschaftsverordnung に基づく

(2) 規制の内容
① 使用に関する規制
規制なし
② 輸出に関する規制
EU 域外へ向けた暗号製品の輸出のみ規制されている。輸出には連邦輸出局（The Federal office of Export）の許可が必要となる。
③ 輸入に関する規制
規制なし

3.4 フランスの現状

フランスにおいては、独自の暗号政策があり輸出入規制のほか、国内における暗号機器の使用も規制されている。

(1) **法的根拠**
電気通信法に基づく
(2) **規制の内容**
① 使用に関する規制
情報の秘匿を目的とする暗号機器を使用する場合には、その秘密鍵を政府によって承認された機関（秘密鍵管理機関）に寄託することを義務付けている。
② 輸出に関する規制
EU **諸国内外を問わず秘匿機能を有する暗号機器を輸出する場合は、政府の承認を受けなければならない。秘匿機能を持たない暗号機器の輸出は、申告するだけでよい。**
③ 輸入に関する規制
EU **域外から暗号機器を輸入する場合は、政府の承認を受けなければならない。秘匿機能を持たない暗号機器の輸入は、申告するだけでよい。**

3.5 その他諸国の現状

その他の諸国においては、暗号規制に関する法制度が未整備、または情報量が少ない事などから「暗号製品（ソフト・機器）の使用及び輸出入に関する規制の現状」に関して全ての情報が得られなかった。
調査した国々の多くは、暗号に関して何らかの制限が設けられているが、その対応方針、制限内容などにばらつきが見られた。
(1) **カナダ**
輸出規制リストに掲載されている暗号製品が規制対象となり、鍵長 56 **ビット以下の暗号製品は** 1 **年間の輸出許可がおりる。**
(2) **スイス**
OECD **諸国以外の国への輸出は許可が必要。また、電気通信免許規制では、電気通信における暗号製品の使用に許可を要する。**
(3) **オーストリア**
企業通信法で、国内企業・組織の無線送信における暗号化を禁止している。
(4) **デンマーク**
1996 **年の防衛政策によれば、暗号製品の使用に関しては特に制限なし。**
(5) **フィンランド**
輸入に関しては規制なし。輸出に関しては許可取得が義務づけられている。
(6) **スウェーデン**
輸出は規制あり。輸入は規制なし。
(7) **ベルギー**
暗号技術の使用には許可が必要。また、ベネルクス外への暗号製品の輸出には許可が必要となる。
(8) **オランダ**
公共分野、一般大衆向け製品については規制なし。その他の目的の暗号製品は、期限付きの許可取得が必要となる。
(9) **ポーランド**
暗号製品の輸出には許可が必要。輸入に関しては輸入認証書などが必要となる。
(10) **ロシア**
暗号製品の輸入は許可が必要で、輸入に関しても厳しい規制がある。また、暗号製

品の使用も禁止されており、国家の公的組織においても、暗号技術の使用に許可が必要となる。
さらに、国内規制により、暗号製品の開発から製造、運用、操作は、政府情報通信連邦機関の許可なしでは禁止されている。

(11) **イスラエル**
輸出入の規制がある。強力な暗号技術の使用には軍の許可が必要となる。

(12) **パキスタン**
電子メールの暗号化が禁止されている。

(13) **サウジアラビア**
暗号技術の使用が禁止されている。

(14) **オーストラリア**
暗号製品の輸出に関する規制あり。暗号製品の国外持ち出しについても許可が必要となる。

(15) **ニュージーランド**
暗号技術の輸出規制あり。

(16) **中国**
音声暗号化装置の輸出入を禁止している。

(17) **韓国**
暗号化装置の輸入は銀行であっても禁止されている。

(18) **フィリピン**
電子メールの暗号技術使用については規制なし。

(19) **インド**
暗号製品の輸入には許可が必要となる。

3.6 OECD 暗号政策ガイドライン

OECD の暗号政策に関するガイドラインは、1997 年 3 月 27 日に正式に発表され、以下の 8 項目について方針を定めている。

(1) **信頼性のある暗号方式の利用**
(2) **一般利用者の選択権利**
(3) **自由な暗号方式の開発**
(4) **暗号方式の標準化**
(5) **プライバシー、個人情報の保護**
(6) **公権力の行使**
(7) **暗号利用、暗号サービスの責任**
(8) **暗号政策の国際協調**

国際相互認証に関連するのは、8 項目の「暗号政策の国際協調」に関する項目である。ここには次の 4 項目が述べられている。

① 関連国内法において暗号の国際利用を許す
② 国際的な暗号鍵への合法的アクセスは、各国間での協調・合意により達成される
③ 政府は暗号政策によって、自由な暗号の利用を妨げてはならない。
④ グローバルな電子商取引の障壁になるような暗号政策を実施してはならない、国際的な暗号利用の障害を作ってはならない

この方針は国際的な暗号の利用を促進するために、各国が協調すべきであることを述べた

ものであり、実質的には国際相互認証、各国間相互認証についての指針と理解することができる。

4 参考文献

4.1 デジタル署名関連

- American Bar Association **デジタル署名ガイドライン**
  http://www.abanet.org/scitech/ec/isc/dsgfree.html
- Food and Drag Administration
  http://www.fda.gov/cder/esig/part11.htm
- **統一商法典**（Uniform Commercial Code）**の** 2B **編**
  http://www.law.upenn.edu/library/ulc/ulc.htm
- **電子金融サービス法**（Electronic Financial Services Efficiency Act of 1997）
  http://www.house.gov/banking/hr2937ss.htm
- **ユタ州デジタル署名法**(Utah Digital Signature Act)
  http://www.commerce.state.ut.us/web/commerce/digsig/dsmain.htm
- **ユタ州デジタル署名実施法**(Digital Signature Administrative Rules)
  http://www.commerce.state.ut.us/web/commerce/digsig/rule.htm
- **カリフォルニア電子署名法**(California Government Code 16.5,1995)
  http://www.gcwf.com/articles¥digsig.htm
- **カリフォルニア電子署名規制法**(California Digital Signature Regulations)
  http://www.ss.ca.gov/digsig/finalregs.htm
- **フロリダ州電子署名法**(Electronic Signature Act of 1996)
  http://www.scri.fsu.edu/fla-leg/bills/senate-1996/sb0942.html
- **フロリダ州電子署名法**(1997 Florida House Bill 1413)
  http://www.scri.fsu.edu/fla-leg/bills/house-1997/hb1413e2.html
- **イリノイ州電子商取引安全法**(Illinois Electronic Commerce Security Act)
  http://www.mbc.com/ceccmsg.html
- **ミネソタ州電子認証法**(Minnesota Electronic Authentication Act)
  http://www.revisor.leg.state.mn.us/cgi-bin/bldbill.pl?bill=S0173.1&session=ls80
- **ニューメキシコ州電子ドキュメント認証法**(Electronic Authentication of Documents Act)
  http://www.nm.org/legislature/Jan_96/house/0516/hb0516.txt
- **ニューヨーク州デジタル署名法**(Digital Signature Act)
  http://assembly.state.ny.us/cgi-bin/showbill?billnum=S02238
  http://assembly.state.ny.us/cgi-bin/showbill?billnum=A06183
- **テキサス州署名規制法**(1997 Texas H.B. 984)
  http://www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?TYPE=B&LEG=75&SESS=R&CHAMBER=H&BILLTYPE=B&BILLSUFFIX=00984&VERSION=5"1997 Texas H.B. 984
- **バーモント州署名法**(1997 Vermont House Bill 60)
  http://www.leg.state.vt.us/database/status/summary.cfm?Bill=H%2E0060&Session=1998
- **ワシントン州電子認証法**(Washington Electronic Authentication Act)
  http://www.wa.gov/sec/corps/digsig.htm

- **ドイツ国デジタル署名法**(German Digital Signature Law/Ordinance)
  http://ourworld.compuserve.com/homepages/ckuner/digsig4.htm
- **アルゼンチン**
  http://www.sfp.gov.ar/firma.html
- **マレーシアデジタル署名法**(Digital Signature Bill 1997)
  http://www.cert.org.my/bill.html
- UN/UNCITRAL **の電子署名一般規則**（Draft Uniform Rules on Electronic Signatures）
  A/CN.9/437: http://www.un.or.at/uncitral/sessions/unc/unc-30/acn9-437.htm
  および A/CN.9/WG.IV/WP.73

4.2 認証局の認可制度関連

- McBride Baker & Coles
  http://www.mbc.com
- German Federal Ministry of Education,Science,Research and Technology
  http://www.iid.de1
- Ministry for science & Technology
  http://dtiinfol.dti.gov.uk
- http://www.cert.org.my

4.3 暗号規制関連

- **全般**

・Crypto Law Survey
  http://cwis.kub.nl/~frw/people/koops/cls2.htm
・The Cryptography Project
  http://guru.cosc.georgetown.edu/~denning/crypto

- **アメリカ**

・Administration Statement on Commercial Encryption Policy(July 12, 1996)
  http://www.epic.org/crypto/key_escrow/wh_cke_796.html
・Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List
  http://www.bxa.doc.gov/encreg.htm
・Order on Administration of Export Controls on Encryption Products
  http://www.law.miami.edu/~froomkin/nov96-regs.htm
・Draft Encryption Export Rule, December 9, 1996
  http://www.jya.com/commerce.htm
・Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List
  http://jya.com/bxa123096.txt
・PART 774--THE COMMERCE CONTROL LIST Category 5--Telecommunications and Information Security

http://jya.com/774-ccl05.htm

● **イギリス**

・UK Government Policy on Encryption
http://www.ncl.ac.uk/~nlawwww/1997/issue1/akdeniz1.html

・GOVERNMENT SETS OUT PROPOSALS FOR ENCRYPTION ON PUBLIC TELECOMMUNICATIONS NETWORKS (DTI 06/96)
http://www.coi.gov.uk/coi/depts/GTI/coi9303b.ok

・UK paper on Licensing Trusted Third Parties for the Provision of Encryption Services - March 1997
http://dtiinfo1.dti.gov.uk/pubs/#sec4

・U.K. Paper on Regulatory Intent Concerning Use of Encryption on Public Networks June 10, 1996
http://dtiinfo1.dti.gov.uk/cii/encrypt/

● **フランス**

・France's Proposed Statutory Trusted Third Party Rules for Encryption
http://www.steptoe.com/france.htm

● **オーストラリア**

・AUSTRALIAN CONTROLS ON THE EXPORT OF DEFENCE AND STRATEGIC GOODS(Department of Defence / November 1996)
http://iic.spirit.net.au/imat/publications/excontrl/excohome.htm

・The Walsh Report (Australian crypto policy)
http://www.efa.org.au/Issues/Crypto/walsh.html

● EU/EC

・Pan-European Confidentiality Services Pilot with Key Recovery
http://www.seven77.demon.co.uk/krisis/

・Towards A European Framework for Digital Signatures And Encryption(*4)
http://www.ispo.cec.be/eif/policy/97503.html

● **国際機関等**

・ICC General Usage for International Digitally Ensured Commerce
http://www.iccwbo.org/guidec2.htm

・ THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES
http://jya.com/wa/watoc.htm#General

・OECD：Recommendation of the Council concerning Guidelines for Cryptography Policy(27 March,1997.)
http://www.oecd.org/dsti/sti/it/secur/index.htm

- SET 関連

・ RSA Encryption Incorporared into Hewlett-Packerd's New International Cryptografy Framework
http://www.rsa.com/pressbox/html/961118.html

・Hewlett-Packerd/Press Release,November 18,1996
http://www.hp.com/csopress/96nov18d.html

・RSA S/PAY：“誰よりも早く市場に出せる”利点と地球規模の販売
http://www.rsa-japan.co.jp/products/set/set_time2mkt.htm

5 検討メンバー一覧

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・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 専務付 シニアリーダ

メンバー

渥美 懋	日本アイ・ビー・エム株式会社 ＮＣ事業推進 ｅ－ＢＺｅｒ
奥田 哲也	三菱商事株式会社 マルチメディア事業推進部 主任
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 ＳＩ推進部ＳＩ技術グループ 主任
生井 均	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	マスターカード・インターナショナル・ジャパンインク ディレクター