H12－認証・公証WG－２

電子認証サービス約款作成ガイドライン

平成13年3月

電子商取引推進協議会

認証・公証WG

はじめに

背景

次々に新しい形態のＥＣが現れ、また、従来ＥＣには余り関係がないと思われていた業界においてもＥＣが普及・伸張している現在の情況には、数年前では予想のつかないものがある。この一方で、インターネットにおいては全体としての管理者がいないため、不正アクセスや成りすましによる被害も多く報告されている。こうした状況下で認証の重要性が増加するのは述べるまでも無い事であるが、ＥＣにおける電子認証関連のシステムは普及の途上にあり、これを利用する企業や個人の間の取決め事については、まだまだ不充分な業界が多いと考えられる。

このような状況を踏まえ、より多くの業界において電子認証が普及し、安全性と利便性が向上する事を目指して、電子認証システムを利用する利用者間の事前取決め事項をどのように考え作成するべきか、その指針として頂く事を目的に、「電子認証サービス約款作成ガイドライン」を策定した。これはこれから電子認証システムを導入する企業や、導入したがその運用経験から約款等を補完したいと考えている企業において、ご利用頂ければと考えている。

対象とする取引モデル

電子商取引における取引モデルの形態としては、クローズドモデルとオープンモデルがある。前者の場合においては、企業グループ内で行うＢtoＢと、取引仲介の場を通じて複数の企業が対等な立場で行うＢtoＢがある。後者においてはＢtoＣ及び個人間ＥＣであるＣtoＣがある。以下に示す「電子認証サービス約款作成ガイドライン」では、最初に普及すると考えられるクローズドモデルを対象とし、そこにおいて電子商取引を行う企業間の電子認証サービス利用における事前取決め事項をどのように考え作成するか、その指針を示した。

ガイドラインの構成

当ガイドラインの構成としては、第１章で約款の全体構成を記している。約款は、前半で証明書の申請手続きから有効期間が満了するまでの一連の流れを記述し、後半でユーザや認証局の義務をまとめて記述することとした。また、第２章として、約款の各条項を記述する場合の考え方を記している。なお、条文の内容は適用する業務に依存する事から、このガイドラインでは、各々の条項を記述する場合の考え方を記した後に、あくまで（例）として条文を枠で囲んで付している。

企業間電子商取引における電子認証システムに係る、企業間の事前取決め事項検討において、本ガイドラインがその一助になれば幸いと思っております。また、各界各方面から忌憚の無いご意見を頂きたいと考えております。ご意見等ございます方は下記連絡先までお寄せ頂くようお願い申し上げます。

連絡先

電子商取引推進協議会（ＥＣＯＭ）
認証・公証ＷＧ
〒 135-8073
東京都江東区青海 2-45　タイム 24 ビル 10 階
TEL. 03-5500-3600
FAX. 03-5500-3660
Ｅ-mail： info@ecom.or.jp
http://www.ecom.or.jp/

目 次

1　電子認証サービス約款の全体構成

ここでは、約款の全体構成として、記すべき章立てを示す。

第 1条　目的
1. 1 目的
1. 2 認証局運用規定
第 2条　公開鍵証明書
2. 1 証明書の種類
2. 2 証明書のフォーマット
第 3条　申請手続き
3. 1 オンライン／オフライン申請の条件
3. 2 オンライン申請
3. 3 オフライン申請
第 4条　証明書発行
4. 1 証明書発行
4. 2 証明書の受領と承諾
第 5条　証明書失効
5. 1 証明書の失効事由と認証局の失効の権利
5. 2 失効に対する認証局の義務
5. 3 ユーザによる失効要請の権利
5. 4 ユーザによる失効要請の義務
5. 5 認証局による証明書失効公開の義務
5. 6 失効時のユーザの義務
第 6条　有効期間・満了・再発行
6. 1 証明書有効期間
6. 2 再発行
第 7条　ユーザの義務・権利
7. 1 正確な証明書申請内容の提示
7. 2 証明書の内容確認とその後の記載事項管理
7. 3 利用目的の制限
7. 4 秘密鍵の管理
7. 5 依存する当事者としてのユーザの義務
7. 6 ユーザによる認証局に対する補償

2　約款の各条項を記述する場合の考え方

ここでは、電子認証サービス約款の各条項を記述する場合の考え方を記す。またその後に、例としてあげられるものに付いてはこれを付す。

A.『第１条　目的』の考え方

a)『１．１　目的』の考え方

本約款が、ある企業等が運営する認証局が提供しユーザが受ける認証サービスに関する条件を決めるものである旨を記述する。

（例）認証局 が提供し、ユーザが受ける認証サービス（証明書申請、証明書発行及び証明書失効に関するサービスを含むが、これらに限定されない）に関する条件を定めるものである。

b)『１．２　認証局運用規定』の考え方

約款の下により詳しい内容を定めた認証局運用規定がある旨の記述を行う。一般的に認証局 は、証明書発行業務の運営方針をＣＰＳ（Certification Practice Statement：認証局運用規定）と呼ばれる規定で記載している。認証局 ／ユーザ間契約の一部でもあるＣＰＳ では、証明書申請～失効の手続きや、物理的・手続き的・人事的管理、認証局 の義務等、より詳細な規定が記されている。

（例）　認証局 は、_____において、その認証局運用規定（以下「認証局運用規定」という）を公表している。証明書申請を提出し、かつ電子署名サービス契約を締結することにより、ユーザは認証局運用規定の条件に同意したものとみなされる。

B.『第２条　公開鍵証明書』の考え方

a)『２．１　証明書の種類』の考え方

何の為に誰から誰へ証明書を発行するかを記述する。証明書の内容あるいは詳細は認証局運用規定に記載する旨の記述を行う。

（例１）　認証局はユーザの代表取締役（又はこれに相当する代表者）及び担当者に対して証明書を発行する。

（例２）

（１）本認証局が発行する証明書とは、調達手続きを行うにあたって、本認証局が利用者からの依頼によって発行する電子データであり、利用者が利用者本人である事を証明するものである。

（２）証明書は、第＿＿条第＿＿項に示す条件を満たした申請者に対して発行され、第＿＿条第＿＿項に示す条項に抵触しない限りにおいて、第＿＿条第＿＿項に示す期間、効力を発揮する。

（３）証明書の証明内容については、認証局運用規定に定める通りとする。

b)『２．２　証明書のフォーマット』の考え方

Ｘ．５０９ｖ．３の形式に一致しているといった記述又は、認証局運用規定に記載する旨を記述する。また、各フィールドの設定者と設定値の詳細は認証局運用規定に記載する旨の記述を行う。

（例１）　認証局 は、Ｘ．５０９ ｖ．３ の形式に実質的に一致した証明書を発行する。証明書は、基本部と標準拡張部によって構成される。証明書の形式の詳細（証明書に記載される拡張部及び情報を含む）は、認証局運用規定に記載する。

C.『第３条　申請手続き』の考え方

a)『３．１　オンライン／オフライン申請の条件』の考え方

認証局に対するユーザの証明書発行の申請には、認証局が定める手続きに従い、認証局が指定するソフトウェアを使用してオンラインで申請を提出する方法と、ユーザの本人性を証明する一定の文書をはじめ、認証局が要請する情報を郵送、海外宅配便または認証局まで持参することによって、オフラインで提出する方法とが考えられる。オンライン申請では、対面でのユーザの本人性確認ができないため、認証局が認める機関の証明書に基づく申請書への電子署名をもってユーザの本人性を確認する。

他機関発行の証明書を入手できているか否か、できている場合はオンライン申請が可能であること、できていない場合は郵送など具体的輸送手段を示して記述を行う。

（例）　ユーザが日本法人である場合で、＿＿＿＿証明書を取得しているときには、当該 ユーザは、認証局運用規定に定める手続に従い、認証局 が指定するソフトウェアを使用して、申請を提出することができる。しかし、ユーザが日本法人であるが、証明書をまだ取得できないとき、またはユーザが日本法人でない場合には、ユーザは、郵送、クーリエ便または認証局まで持参することによって申請を行うことができる。

b)『３．２　オンライン申請』の考え方

i. ユーザの義務

オンラインで申請書を提出するときの、必要情報・入力方法については、認証局運用規定に記述するか、本項に詳細に記述するかを検討して記述する。ユーザの義務として、ユーザが申請に際し提示する情報には、他機関の証明書の秘密鍵により電子署名して送付し、正確性を保証することや、署名に用いた秘密鍵の非危殆化の保証を行うことを記述する。

（例）

（１）ユーザは認証局運用規定に従い申請画面で要求されている申請情報を入力する。

（２）ユーザは申請情報が正確であることを確認し、その上で＿＿＿証明書で証明される公開鍵に対応する秘密鍵により、当該申請書に電子署名するものとする。

（３）ユーザは上記（２）の電子署名を付すことにより、当該電子署名が付された申請書に記載されている申請情報の正確性（被発行者となる担当者の氏名及びその役職を含むがこれに限られない）、及び＿＿＿証明書により証明される公開鍵に対応する秘密鍵が危殆化していない事を認証局 に対して保証するものとする。

ii. 証明書発行申請の認証局による審査

認証局は申請画面にて要求する情報がすべて入力されているかの審査を行うこと、認証局は入力された情報について必要に応じて申請者本人に問い合わせができること、また、入力された情報の審査については認証局運用規定に定めることの記述を行う。認証局は審査を通過しなかったユーザに対し、その旨及び不通過の理由を認証局運用規定に定める方法により通知することを記述する。

iii. 認証局による本人性の確認

認証局が認める機関の証明書に基づく署名が付された申請を受領したとき、認証局は当該証明書の検証を行い、電子署名が有効であることで本人性を確認する。

c)『３．３　オフライン申請』の考え方

i. ユーザの義務

ユーザが、認証局が認める他機関の証明書を取得できていないとき、ユーザは認証局が要請する情報をすべて記入した申請書と、ユーザの本人性を証明するための一定の文書を提出しなければならない。本人性を証明する文書は、申請された証明書の被発行者がユーザの代表者であるか担当者であるか、またユーザが存立している国の法制度・入手できる公文書によって異なる。必要とする情報・文書については、認証局運用規定に記述するか、本項に詳細に記述するかを検討して記述する。

（例）
（1）ユーザが日本法人である場合、以下の文書の提出が必要となる。.
（a）申請日に先立つ３ヶ月以内に発行された代表取締役の印鑑証明書
さらに、被発行者が担当者である場合、以下の文書の提出が必要となる。
（b）申請日に先立つ３ヶ月以内に発行された 担当者の住民票の謄本
（c）当該担当者がユーザの従業員または役員であることを証する内容の在職(または雇用)証明書で、ユーザの代表取締役が作成するもの
（d）(担当者が代理人である場合)ユーザの代表取締役が作成する委任状又は代理契約
（2）ユーザが外国法人である場合、以下の文書の提出が必要となる。
（a）商業登記簿謄本またはそれに相当する文書で、ユーザの組織の適法性及び法人の存在を証する上で、認証局 が十分であるとみなす文書(基本定款及び営業許可書を含むが、これらに限定されない)
（b）ユーザを代理して証明書の申請を行う代表者のサイン証明で、公証人が作成するもの
（c）認証局への証明書申請と電子署名サービス契約の締結を承諾する取締役会の決議証明書
さらに、被発行者が担当者である場合、以下の文書の提出が必要となる。
（d）担当者のパスポートの写し
（e）当該担当者がかかる法人の従業員または役員であることを証する内容の在職(または雇用)証明書で、ユーザの代表者が作成するもの
（f）(担当者が代理人である場合)ユーザの代表者が作成する委任状又は代理契約。

ii. 証明書発行申請の認証局による審査

認証局は申請書に必要な情報が記入されているかの審査を行うこと、また、認証局は提出された申請書に記載された情報について､必要に応じて問い合わせができることを記述する。提出情報・文書の審査については認証局運用規定に定めることの記述を行う。認証局は審査を通過しなかったユーザに対し、その旨及び不通過の理由を認証局運用規定に定める方法により通知することを記述する。

iii. 認証局による本人性の確認

証明書申請書に記述されたユーザ名と申請者が同一であるかの検証を行うことを記述する。確認方法は認証局運用規定に定めることを記述する。

D.『第４条　証明書発行』の考え方

a)『４．１　証明書発行』の考え方

認証局の発行する証明書の発行対象、発行期限、証明書の有効期限、効力発生時期及び認証局が証明書発行時点で表明する事項について記述する。証明書の発行方法、ユーザへの送付方法などの手続きについては認証局運用規定に定めることを記述する。

（例）

（１）認証局は__章__条記載の審査を通過した申請者に対し証明書を発行する。

（２）（ａ）オンライン申請の場合認証局は、申請書に付された_____証明書による電子署名の有効性を確認した時点をもって申請を許可し、ユーザに対し証明書を発行する。

（ｂ）オフライン申請の場合認証局は、認証局運用規定に定める必要な確認手続きが完了した時点において申請を許可するものとし、証明書を発行する。

（３）認証局は認証局運用規定に定める方法にてユーザに証明書を送付する。

（４）認証局が申請を拒否する場合認証局はユーザに対し、速やかにこれを通知するものとする。

（５）証明書の有効期間は１年とする。証明書にその後の日付が記載されていない限り、証明書の有効期間は発行時に開始される。これはユーザが証明書を承諾していないために証明書がまだ有効でない場合も同様である。証明書はユーザが承諾した時点をもって有効となる。

（６）証明書の発行時点において、認証局は本約款及び認証局運用規定の要件を遵守していること、証明書中の情報が信頼できるものであることを表明する。

（７）認証局は証明書を発行した後、リポジトリに登録することによって証明書を公表する。

b)『４．２　証明書の受領と承諾』の考え方

認証局から発行された証明書のユーザによる受領、証明書の内容の確認と承諾の手続き、ユーザが証明書承諾時に表明・保証する事項について記述する。ユーザは証明書の受領後内容を確認し、その内容に誤りがあれば直ちに認証局に連絡すること、証明書発行後、認証局運用規定に定める期間を経て連絡が無い場合は、ユーザが証明書の内容をすべて承諾したものとみなし、証明書の内容につき認証局の責任は問えず、証明書が有効となることなどを記述する。証明書の受領の方法、受領後の報告期限、誤りがある場合の連絡方法、誤りが無い場合の報告要否、ユーザが証明書を承諾したとみなされるまでの期間など、詳細を認証局運用規定に定める場合はその旨記述する。

（例）
（１）ユーザは認証局の認証局運用規定に定める方法にて証明書を受領する。
（２）ユーザは証明書の発行から、認証局運用規定に定める期間以内にその内容を確認し、内容に誤りがある場合は直ちに認証局に連絡しなければならない。ユーザからの連絡が無かった場合は、ユーザが証明書の内容をすべて承諾したものとみなし、証明書の内容について認証局の責任は問えない。
（３）ユーザによる証明書の承諾をもって、証明書は効力を生じるものとする。
（４）ユーザは、認証局に対して提示し証明書に表記された情報はすべて正確であることを表明、保証する。

E.『第５条　証明書失効』の考え方

a)『５．１　証明書の失効事由と認証局の失効の権利』の考え方

証明書が失効となる事由を示し、該当する事由が発生した時は、認証局は証明書を失効させる権限を有していることを記述する。失効の手続きの詳細は認証局運用規定に定めることを記述する。

（例）
認証局は以下に示す事由が発生した時は、認証局運用規定に定める手続きに従って証明書を失効させる権限を有す。
（ａ）ユーザが本約款または認証局運用規定に基づく義務の不履行があった場合
（ｂ）ユーザから証明書の失効の要請があった場合
（ｃ）認証局の秘密鍵が危殆化された場合、又はその危険性があると認証局が認めた場合
（ｄ）ユーザの秘密鍵が危殆化された場合、又はその危険性があると認証局が認めた場合
（ｅ）証明書が不正使用された場合、又はその危険性があると認証局が認めた場合
（ｆ）証明書記載の情報に虚偽があり、又は情報が変更されたことを認証局が確認した場合
（ｇ）証明書の規格変更がなされた場合
（ｈ）ユーザが解散し、又は存続しなくなったことを認証局が確認した場合
（ｉ）その他、認証局が必要と判断した場合

b)『５．２　失効に対する認証局の義務』の考え方

認証局は証明書の失効をユーザに通知すること、またユーザの、証明書失効に対する意義申立を受付けることを記述する。ユーザへの通知及びユーザの意義申立手続きの詳細は認証局運用規定に定めることを記述する。

（例）
（１）認証局は証明書を失効させた時は、認証局運用規定に従って速やかにユーザに通知する。
（２）ユーザは、認証局が証明書を失効させた場合には、認証局運用規定に定める期間内に意義申立てをすることができる。
（３）認証局は、ユーザの意義申立てがあった場合、認証局運用規定に定める手続きに従って対応する。

c)『５．３　ユーザによる失効要請の権利』の考え方

ユーザの、認証局に対する証明書失効要請に関わる権利について記述する。ユーザは、認証局への証明書失効要請後は、証明書の使用を停止しなければならないことを記述する。失効要請の手続きの詳細は認証局運用規定に定めることを記述する。

（例）　ユーザは、認証局運用規定に定める手続きに従い、事由の如何を問わず証明書の失効を、認証局に対しいつでも要請することができる。ユーザは、認証局に対する失効要請後は、証明書の使用を停止しなければならない。

d)『５．４　ユーザによる失効要請の義務』の考え方

ユーザが、認証局に対し証明書の失効要請を行わなければならない場合について、記述する。

また、ユーザが認証局に証明書失効要請を行わねばならなかったにもかかわらず、実施しなかった場合に発生した事態に対し、認証局は責任を負わないことを記述する。失効要請の手続きの詳細は認証局運用規定に定めることを記述する。

（例）
（１）ユーザは以下の場合には、直ちに認証局運用規定に定める手続きに従って、認証局に証明書の失効を要請しなければならない。
（ａ）証明書に記載されるユーザの秘密鍵が危殆化された場合
（ｂ）被発行者がユーザの代表者または担当者ではなくなった場合
（ｃ）証明書の内容に変更があった場合
（２）上記状況において、ユーザが証明書の失効の要請を行わなかった場合、その結果発生したいかなる事態に対しても、認証局は責任を負わない。

e)『５．５　認証局による証明書失効公開の義務』の考え方

証明書が失効された場合、認証局はその失効情報を公開しなければならない。失効情報の公開手段は、認証局リポジトリに証明書失効リスト（ＣＲＬ）を公表する方法、またはオンライン証明書ステータスプロトコル（ＯＣＳＰ）により証明書の有効・失効情報を提供する方法のいずれかによることを記述する。失効情報の提供の詳細を認証局運用規定に定める場合はその旨記述する。

（例）　認証局が証明書の失効を行った場合には、証明書失効リスト（ＣＲＬ）に登録し、その事実を公開する。

f)『５．６　失効時のユーザの義務』の考え方

証明書が失効したときにユーザが実施しなければならない事項について記述する。

（例）　証明書が失効したときには、ユーザは、証明書がインストールされているユーザのサーバから、速やかに該当証明書を除去し、その後の使用を停止しなければならない。

F.『第６条　有効期間・満了・再発行』の考え方

a)『６．１　証明書有効期間』の考え方

証明書の有効期間、有効期間の開始日時あるいは開始すると見なされる条件について記述する。公開鍵と秘密鍵の使用期間については認証局運用規定に記述することとするか否か検討する。

（例１）ユーザ証明書の有効期間は、１　年とする。証明書にその後の日付が記載されていない限り、有効期間は発行時に開始される。これは、ユーザが証明書を承諾していないために当該証明書がまだ有効でない場合であっても同様である。各証明書は、認証局 が発行し、ユーザが承諾した時点で有効とみなされる。

（例２）証明書の有効期間は、証明書の発行から利用者の参加資格の資格満了日までとする。

b)『６．２　再発行』の考え方

再発行に至る事由別の記述を行う。

i. ユーザ事由による場合

証明書有効期間満了時の、再発行に向け認証局に再申請するなどのユーザのとるべき行動を記述する。この場合、鍵ペアについての対応（旧鍵ペアの対処、鍵ペアの更新）も記述する。ユーザの証明書失効届時、認証局の判断による証明書失効時、紛失時の再発行に向けた対応についても同様に記述する。また、再発行に伴う費用をどのような場合に誰が負担するか、検討を行い記述する。

（例１）利用者が紛失などの理由によって証明書の再発行を希望する場合には、再発行を受け付けるものとする。再発行は、通常の発行の手順に準じて、認証局が定めた方法で行うものとする。

（例２）　期間満了時において、ユーザは、直ちに証明書の使用を中止し、自己のサーバから当該証明書を削除するものとする。ユーザが満了日後にも証明書の使用の継続を希望する場合、ユーザは新規に鍵ペアを作成し、認証局運用規定に定める手続に従って、認証局 に新規の証明書申請を提出しなければならない。これにより認証局は、認証局運用規定に定める検証手続の後に、ユーザに対し、新規の証明書を発行する。上記の手続は、失効後の新規証明書の再発行にも適用される。

ii. 認証局事由による場合

認証局秘密鍵が危殆化した場合、それ以外で認証局の権限により証明書を失効させる場合において、再発行に向けた認証局のとるべき行動について記述する。前者については、認証局は証明書の失効を行った後、認証局は再発行を行う旨を記述し、後者については再発行が必要な場合を検討し、その場合において再発行を行う旨を記述する。また、再発行に伴う費用をどのような場合に誰が負担するか、検討を行い記述する。

（例）　本認証局は、証明書の安全が脅かされるような事態が発生していると判断した場合に、利用者の事前の承諾を得なくても、必要に応じて証明書の規格を変更する権利を有する。 当規格変更の際には、既取得済の証明書は全て失効し、本認証局の費用負担により証明書を再発行する。

iii. その他事由による場合

不可抗力等により証明書の再発行を行うべき場合の対応について記述する。例えば自然災害により認証局が事業遂行できなくなってしまった場合、あるいはユーザが消滅し事業を遂行できなくなってしまった場合など、想定される事態を検討し、その場合の対応を記述するか、認証局運用規定に記載する旨記述する。

G. 『第７条　ユーザの義務・権利』の考え方

a)『７．１　正確な証明書申請内容の提示』の考え方

証明書を取得する際に認証局に提示する申請内容は正確でなければならないことを記述する。オンライン／オフラインの２つの申請手続きがある場合、それぞれに対してその提示に関する考え方を記述する。

オンライン申請手続きの場合、認証局としては、申請者であるユーザ（法人）に関する認証とともに、被発行者である担当者に関する認証が必要となる。前者の点に関しては、ユーザが申請書に対して行う電子署名により検証される。ただし、その証明書に関連する秘密鍵が危殆化するなど、証明書に失効すべき事由が存在するにもかかわらず失効されていないときには、かかる信頼の前提が成立しない。よって申請時においてかかる失効事由がないことをユーザに保証させる必要がある。また後者の点に関しては、認証局としての独自の検証を行うことも考えられるが、証明書が個人として使用されるものではなく法人としてユーザの電子署名の検証に使用されることを考慮すると、ユーザが電子署名することにより、当該担当者の氏名および役職の正確性を保証するという運用であっても問題はないと考えることもできる。

オフライン申請手続きの場合、認証局としては、ユーザおよび担当者に関する認証は、証明書申請書の記述、およびそれらの本人性を証明するための所定の文書を提出させることで検証される。

（例）

（１）　オンライン申請

____証明書を取得している場合には、認証局運用規定に定める手順に従い、認証局が指定するソフトウェアを使用して申請を提出することができる。____証明書で証明されている公開鍵に対する秘密鍵により当該申請書に電子署名を付すことで、当該電子署名が付された証明書に記載されている申請情報の正確性（被発行者となる担当者の氏名およびその役職を含むがこれに限られない）、および____証明書により証明される公開鍵に対する秘密鍵が危殆化していないことを認証局に対して保証するものとする。

（２）　オフライン申請

____証明書を取得していない場合には、書面による申請を行うことができる。ユーザは、証明書申請書の全事項を記入し、かつ記入された申請内容はユーザの現状を正確に表してものでなければならない。それに加え、ユーザ自身又は担当者の本人性を証明するために認証局運用規定に定める一定の文書を提示しなければならない。

b)『７．２　証明書の内容確認とその後の記載事項管理』の考え方

認証局から発行された証明書の内容確認、およびその記載事項に誤りがあった場合の報告義務について記述する。また上記確認により証明書は承認されたものとし、以後証明書の内容について認証局の責任を問えないことも記述する。

（例）
（１）ユーザは、証明書の到達から２週間以内にその内容を確認し、その内容に誤りがあれば直ちに連絡しなければならない。
（２）その後も証明書の使用前に確認を行い、記載事項がユーザの現状に合わなくなった場合は、すみやかに失効申請を行わなければならない。
（３）ユーザからの連絡が無かった場合には、ユーザが証明書の内容を全て承認したものと扱い、証明書の内容について認証局の責任を問えないものとする。

c)『７．３　利用目的の制限』の考え方

証明書の利用目的と使用方法の制限について記述する。なお、具体的な利用目的や使用方法の制限については、本約款または認証局運用規定に記述する。

（例）
（１）約款に記述する場合の記述例

ユーザは、証明書に関して以下の使用制限を遵守する義務を有し、さらに、担当者に同様に以下の使用制限を遵守させるものとする。
（ａ）ユーザおよび担当者は、____取引に関連して行われるデータ及びメッセージの送信のみを目的として、又はこれに関連してのみ、証明書を使用するものとし、その他についてこれを使用することは禁止する。
（ｂ）ユーザおよび担当者は、証明書に記載されている公開鍵に対する秘密鍵を、証明書への署名のために使用してはならない。
（ｃ）ユーザおよび担当者は、証明書の内容を変更してはならない。

（２）認証局運用規定に記述する場合の記述例

証明書は、認証局運用規定にもとづいて発行されている。従ってユーザはその範囲外の用途に証明書を提示、使用してはならない。

d)『７．４　秘密鍵の管理』の考え方

証明書に記載されている公開鍵に対応する秘密鍵の管理責任、および秘密鍵を喪失、もしくは危殆化された場合の失効申請について記述する。

（例）

ユーザは、証明書を受領した時点より、ユーザ証明書および証明書に記載された公開鍵に対する秘密鍵の管理義務を負う。

ユーザは、証明書に記載された公開鍵に対する秘密鍵の紛失、不正使用、盗用について一切の責任を負う。そのため、秘密鍵使用の際に求められる PIN などの情報をユーザ本人以外に知られないよう十分に管理しなければならない。

ユーザは、以下に定める事由が発生したときは、直ちにその旨を認証局に報告し、当該秘密鍵または証明書の利用を止めなければならない。

（１） 秘密鍵の紛失、破損、詐取、横領、不正使用等を知った場合

（２） 証明書の記載事項が事実と異なることを発見した場合

（３） 証明書の記載事項に変動が生じた場合

e)『７．５　依存する当事者としてのユーザの義務』の考え方

証明書に依存する当事者間取引においては、証明書の有効性確認の手段を用いて、かかる他のユーザの証明書を検証しなければならず、かかる検証により、当該証明書が有効である場合にのみ依拠する旨を記述する。

（例）

依存者は、取引相手である証明書の有効性についてチェックしなければならない。

（１）　証明書の利用制限

証明書は認証局運用規定にもとづいて運用されており、依存者はこれらを理解し、承認した上で証明書を利用しなければならない。通信相手から提示された証明書は、それ自身に記載されたり引用されたりしている使用目的の範囲内で使用しなければならない。

（２）　証明書の有効性確認義務

証明書を利用する際には以下を含む有効性確認を行わなければならない。

（ａ）証明書パス上の全証明書について、

・証明書が改ざんされていないこと

・有効期限内であること

・失効していないこと

・上記（１）の証明書使用目的が正しいこと

（ｂ）ユーザ証明書の署名を検証すること

（ｃ）提示された証明書記載項目が、証明書の記載の規定に合致していること

（３）　認証局ルート証明書の組み込み

認証局ルート証明書が組み込まれていないアプリケーションを使用する場合には、認証局ルート証明書を信頼できるルート証明書として組み込むことができる。組み込みの際には、Ｗｅｂサイトに公開されている認証局ルート証明書のハッシュ値と比較検証しなければならない。

f) 『７．６　ユーザによる認証局に対する補償』の考え方

証明書の使用、又は認証局が提供するサービスから生じるあらゆる債務、損失、費用、経費、損害および申立において、ユーザが認証局を補償する事項について記述する。

（例）

ユーザは、証明書の使用又は証明書に関して認証局が提供するサービスから生じるあらゆる債務、損失、費用、経費、損害および申立（合理的な弁護士費用を含む）で、かつ以下の事項によって生じるものにつき、認証局を補償し、これに被害を蒙らせないようにする。

（１）証明書の使用又は申請についてユーザが不正表示、不作為又は虚偽の事実を述べること

（２）証明書の内容について、ユーザ又は担当者が修正を行うこと

（３）ユーザ又は担当者が本契約、認証局運用規定および適用法に許可される以外に証明書を使用すること

（４）ユーザが、証明書の公開鍵に対応する秘密鍵の喪失、開示、危殆化又は許可のない使用を防ぐための必要な予防策をとらないこと

（５）ユーザが、証明書の失効の要請またはリポジトリからの証明書の非登録化を要請しないこと

（６）オンライン申請したユーザが、認証局が認める他機関の証明書の失効原因があるにもかかわらず失効要請をしないこと

（７）ユーザに本契約および認証局運用規定上のその他の違反があること。

H.『第８条　認証局の義務・権利』の考え方

a)『８．１　損害賠償責任と賠償額の制限』の考え方

電子認証サービスの遂行中の過失等により、利用者に損害を与えた場合の損害賠償及び責任制限について規定する。また賠償額に限度を設ける場合は、それが、１利用者あたりなのか、１事故（１つの原因または事由に起因して発生した事故）あたりなのか、１証明書あたりなのか、あるいは一定の期間を定めてその期間内の賠償額の総額なのかについて規定する。

限度額は一定金額を定める場合や利用者からのサービス料金を基準とした一定倍率とする場合がありうる。なお、期間あたりの賠償額の総額に制限を設けた場合は、賠償額の総額が上限を超えた場合の支払における優先順位を規定する。

また、損害賠償の範囲を“通常損害”、“通常損害または予見可能な特別損害”“予見可能な相当因果関係のある損害”と限定する場合の他、“逸失利益などの間接損害、懲罰的賠償については賠償しない”と規定する場合などがありうる。

（例）

（１）本認証局の業務が遂行または業務の結果に起因して、ユーザに損害が生じた場合、本認証局が賠償する損害の範囲は予見可能な相当因果関係のある損害のみとし、また賠償額は、当該ユーザが支払ったサービス料金を限度とする。

（２）前項の規定にかかわらず、本認証局が支払う賠償額の総額は、１会計年度（本認証局の１会計年度のことをいう。）あたり、＿＿＿＿を限度とする。また、１会計年度中の賠償額の総額が、＿＿＿＿を超える場合、本認証局は、原則的に、最終的な紛争解決が行われたものから順次賠償金を支払っていくものとする。ただし、利用者が紛争解決に協力しているにもかかわらず賠償額の認定に時間がかかるなど、最終的な紛争解決が遅延することがやむをえないときに、部分的に確定した賠償額を支払う場合または管轄裁判所から別途命令があった場合はこの限りではない。

b)『８．２　免責事項』の考え方

認証局が業務を適正に遂行していた場合、事故の原因が認証局の責によらない場合または不可抗力的な事故の場合などにおいては、認証局は責任を負わない旨を規定する。よって例に挙げたような場合は責任を負わない旨を規定することが考えられる。ただし、免責条項を設けた場合でも、認証局としては事故の発生を未然に防ぐ措置を講じる必要があることはいうまでもない。また、事故防止措置に著しい不備があった場合には免責条項の有効性が否定されるおそれがあることに注意が必要である。

（例）

前条の規定に拘わらず下記の場合においては、本認証局はユーザに対して賠償義務を負わないこととする。ただし、本認証局に故意または重過失があった場合を除く。

（１）本認証局が業務を適正に遂行していた場合

（２）ユーザの故意、過失または違法行為に起因して損害が発生した場合

（３）ユーザの認証局運用規定違反に起因して損害が発生した場合

（４）次に掲げる本認証局の支配を超えた事由に起因して損害が発生した場合

（ａ）地震、噴火、津波、台風などの自然災害に起因して損害が発生した場合

（ｂ）戦争、暴動、変乱、争乱、労働争議に起因して損害が発生した場合

（ｃ）放射性物質、爆発性物質、環境汚染物質に起因して損害が発生した場合

（ｄ）その他の本認証局の支配を超えた事由に起因して損害が発生した場合

（５）次に掲げるやむを得ない事由によりサービス中断または終了に起因し損害が発生した場合。なおこの場合、本認証局は予告なくサービスの中断または終了ができるものとする。

（ａ）火災・停電・不正アクセス等の事故によりサービス中断がやむを得ない場合。

（ｂ）保守・運用上の点検整備またはセキュリティ管理上中断がやむを得ない場合。ただし、定期的な点検整備による中断については＿＿日前までに、認証局運用規定に基づいた方法でユーザに通知することとする。

（ｃ）ユーザの債務不履行により当該ユーザにサービス提供を中断または終了する場合。

（ｄ）システム構成機器の重大な故障やその他システムに関する重大な障害が発生し、サービスを継続する事により被害が拡大するおそれがある場合のサービスの中断または終了。

（ｅ）本認証局の秘密鍵情報の漏洩、偽造または変造など本認証サービスのシステム全体等に重大な障害をあたえる可能性がある事由が発生した場合のサービスの中断または終了。

（その他、アプリケーションに応じて、想定されるやむを得ない場合を記載する。）

c)『８．３　記録の保存』の考え方

認証局が保存すべき記録について、その内容、保存方法、保存期間について検討し記述する。

（例１）　本認証局は、証明書発行機関として必要となる詳細な記録を、改ざん防止できる適切な方法を講じて、保存するものとする。保存期間については、以下の通りとする。

（１）鍵の生成・保管・失効などに関するすべての鍵管理の記録	７年間
（２）証明書・ＣＲＬの発行及び失効に関する記録	７年間
（３）証明書発行機能要員の管理記録	３年間
（４）証明書発行機能施設への入退室及び設備・装置の操作の記録	３年間
（５）証明書発行システムへのアクセス及び不正アクセスの記録	３年間
（６）監査情報の点検記録及び監査調書へのアクセス記録	３年間
（７）証明書申請の際に申請者から受領した申請書及び添付書類一切	３年間

（例２）本認証局は、次の（１）から（５）までに掲げる記録に関しては、当該記録に係る証明の有効期間終了後、１０年間保存するものとする。

また（６）及び（７）に掲げる記録に関しては、当該記録発生期間に対する監査及び認定の更新時の実地の調査が終了するまで保存するものとする。

ユーザから提出された申込書、証明取消依頼書、ユーザの真偽の確認資料及びユーザ署名鍵の受領証等のうち、ユーザ等の自署又は押印があるものは原本で保存し、これら以外のものの保存は、電磁的記録に係る記録媒体により行うことができるものとし、この場合、当該記録を必要に応じ電子計算機その他の機器を用いて直ちに表示できることとする。また本認証局は帳簿書類が滅失し、または毀損する事を防止するために必要な措置を講じるものとする。

（１）利用申込関連記録
（２）証明取消関連記録
（３）認証業務規定関連記録
（４）組織管理関連記録
（５）認証業務署名鍵関連記録
（６）セキュリティ関連記録
（７）帳簿書類へのアクセス及び廃棄記録

（それぞれの具体的中身はアプリケーションや認証局運用規定に応じて記載する。）

（「電子署名及び認証業務に関する法律の施行に関する意見募集」（2000 年 11 月 20 日　郵政省・通産省・法務省）における別紙「電子署名及び認証業務に関する法律に基づく関係政省令等に盛り込む事項について」より部分的に引用）

d)『８．４　秘密情報の管理』の考え方

認証局は、秘密にすべき情報及び秘密と見なされない情報をそれぞれ明らかにし、その扱い方法について定めておく必要がある。

（例）　本認証局はユーザの書面による事前の承諾なくして、本契約に関連して知り得たユーザ固有の秘密情報を第三者に開示・漏洩しないものとする。

前記の規定にかかわらず、次の各号に定める情報については、秘密情報とはみなされないものとする。

（１）証明書、ＣＲＬその他のリポジトリに含まれるべき情報

（２）ユーザから認証局に開示された時点で、本認証局がすでに保有している情報または公知の情報

（３）ユーザから認証局に開示された後本認証局の責によらずして公知となった情報

（４）第三者から秘密保持義務を負うことなく適法に入手した情報

（５）本認証局が開示された情報によらずして独自に開発した情報

（６）認証局が第三者に対して、秘密保持義務を課すことなく開示した情報

e)『８．５　公的機関等への情報の開示』の考え方

公的機関からの監査や捜査があった場合には、その対応を検討し記述する。

（例）　本認証局は、捜査機関、裁判所、監督官庁その他の公的機関等（以下、公的機関等という。）から捜査、監査、検査または照会（以下、捜査等という。）があった場合については、当該捜査等について公的機関等が正当な権利及び目的を有している場合に限り、当該公的機関等に対して、利用者の秘密情報を、秘密情報である旨を示した上で開示できることとする。

f)『８．６　約款変更権限』

原則的には、一方的な約款変更は認められるものではないが、アプリケーションによっては、そのアプリケーションが認証局の支配の範囲外で変更され、その対応として、約款を変更せざるを得ない場合も想定される。その場合、ユーザの承諾が特に無い場合でも正当な理由がある場合には認証局は約款の変更ができる権限がある旨を記述する。また、この改定が有効な時はいつからか（通知し

た時、等）を記述する。ただし、約款の変更内容がユーザに対して不利になる場合には約款の有効性が否定されるおそれもあるため､約款変更はユーザに不利にならないものでかつ全体としての利益につながるものに限定される。

（例）
（１）本認証局は、利用者の事前の承諾を得なくとも、＿＿＿＿＿等正当な理由がある場合には、本約款を改定できるものとし、利用者はあらかじめこれを承諾するものとする。
（２）本認証局は、前項の規定に基づき本約款の改定を行う場合、利用者に対して、認証局運用規定に定める方法により、その改定内容および有効となる時期を、公知または通知するものとする。

g)『８．７　知的財産権』の考え方

認証局がユーザに貸与しているソフト・ハードウェア等の知的財産権について規定する。アプリケーションによっては、ユーザが認証局運用規定等を参考にして､自らの運用規定に引用するなどのケースも考えられる場合にはその点についても記述する。

（例）本認証局がユーザに対して貸与するソフトウェア、ハードウェア及びその他文書等（認証局運用規定、マニュアルを含む。）の知的財産権は本認証局に帰属する。ただし、ユーザが、本認証局の了承を得た上で、自らのセキュリティポリシーを作成する際に、当該文書等を参考または引用することができる。

h)　約款に記述するべきか否か検討すべき項目

以下の項目は認証局運用規定で定めるべきか、当約款に記述するべきか検討し、認証局運用規定において定めると判断したときは、認証局運用規定を参照する、または認証局運用規定において定める旨を、当約款に記述すること。

i.　ユーザの秘密鍵の回復に関する事項
ii.　セキュリティ監査手続き：運用ログの記録と監査
iii.　有効期限満了後の証明書及びＣＲＬの扱い：保存するのか否か
iv.　物理的・手続き的・人事的セキュリティ管理
v.　技術的セキュリティ管理：鍵ペア生成・組込み管理、秘密鍵の保護、活性化データ、コンピュータセキュリティ管理、システム開発管理、システムセキュリティ管理、ネットワークセキュリティ管理・暗号化モジュール管理

l. 『第９条 雑則』の考え方

a)『９．１ 通知』の考え方

本電子認証サービスに関する通知をはじめ、要求や要請は、どのように伝達されるかを記述する。また、その通知等はいついかなる条件の時から効力を発生するのかも併せて記述する。

（例）本電子認証サービスに関するあらゆる通知、要求又は要請は、書面によって、又はデジタル署名の付されたメッセージによって、なされるものとする。書面による通信は、受領日をもって有効とするが、当該通知にその後の日付が記載される場合はこの限りでない。また書面による通信は、以下の住所に宛てたクーリエ便又は配達証明郵便もしくは書留郵便によって送付された場合のみ、有効とする。

b)『９．２ 譲渡の禁止』の考え方

本電子認証サービスの当事者は、相手側の同意なくして一方的に契約の譲渡、売却、移転を禁止することを記述して、お互いの知らぬ間に相手が変わり不利益になる危険を回避するためのものである。

（例）いずれの当事者も、相手方当事者の事前の書面による同意を得ることなく、本契約を譲渡、売却又は移転（合併、吸収合併、新設合併又は組織変更による移転を含む）することはできない。書面による同意を取得することなく企図された本電子認証サービスの契約譲渡は無効とし、効力を有しないものとする。

c)『９．３ 輸出規制の遵守』の考え方

ソフトウェアの輸出又は技術情報の提供は、輸出規制に関する法律や規則等の対象になる。従って、本サービスにおいても輸出規制に関する法律の対象になることを記述して注意を促す必要がある。

（例）本電子認証サービスに関連して用いられる一定のソフトウェアの輸出及び技術情報の提供は、日本又は他の国の輸出規制に関する法律、規則、又は命令等による規制の対象になる。本電子認証サービスのユーザは、日本又は適用ある各国の輸出法規を遵守し、直接的にも間接的にも、必要となる輸出許可又はその他の政府承認を取得することなく、いかなるソフトウェア又は技術情報の全部又は一部をも第三国に輸出、再輸出、または提供してはならないものとする。

d)『９．４ 準拠法』の考え方

本電子認証サービスの諸契約に関する準拠法を定めない場合、日本以外の法で解釈される場合も考えられるため、日本法に準拠する旨を記述する。

（例）本電子認証サービス約款は日本国内法及び規制に基づき解釈されるものとする。

e)『９．５ 管轄裁判所』の考え方

紛争が起きた場合で裁判所にその解決を求める際は、認証局の最寄りの裁判所を管轄裁判所とする様に予め定めておくものである。定めがない場合は、認証局から遠い場所の裁判所となることがある。

（例）本電子認証サービス約款に関するあらゆる紛争を法廷にて解決を図る場合は、＿＿＿＿地方裁判所を管轄裁判所とする。

f)『９．６ 契約の終了』の考え方

どの様な場合に本電子認証サービスの契約が終了となるのか、また、その際の手続き・料金の取り扱い等を記述する。

（例）

（１）解約の申出

認証局は、ユーザから書面により認証局との契約の解除の申出があった場合には、これに応じなければならない。この場合、認証局はユーザに対し、予め定めた算定基準に従って利用料を払い戻さなければならない。

（２）解除権

ユーザについて以下に定める自由が発生した時、認証局は何ら催告をすることなくユーザとの契約を解除することが出来る。

（ａ）支払い停止の状態に陥るか、破産、会社整理、特別生産、会社更正、民事再生の申立があったとき。

（ｂ）廃業、法人の解散（吸収合併を含む）があったとき。

（ｃ）ユーザが、当サービス約款に違反したとき。

g)『９．７　料金』に関する考え方

料金に関しては改定する事を想定して本電子認証サービス約款に記述せずに、別途定める旨の記述をする。

（例）本電子認証サービスの料金に関する定めは＿＿＿＿に記述する。

J. 『第１０条　定義』の考え方

約款で使用されている主な用語についての記述を行う。具体的には、認証システム関連の用語と共に、必要に応じ、契約関連で使用される用語を列挙する。

（例１）

証明書失効リスト(ＣＲＬ)：

認証機関がデジタル署名を付する失効した証明書について、定期的に発行するリストをいう。

危殆化：

秘密鍵や関連機密情報等が、盗難や漏洩、第三者による解読等によってその機密性を失ったか、あるいはその可能性があること。

オンライン証明書ステータスプロトコル（ＯＣＳＰ）：

リアルタイムでオンラインにより証明書の有効性状況を確認するためのＩＥＴＦの標準である。

認証局運用規定（ＣＰＳ）：

証明書ポリシーに基づいて、認証の実施における手続き、遵守事項などを文書化したもの。利用者等の認証局の外部者に開示されるもの。

有効期間：

認証機関が証明書を発行する日時(又は証明書に記載される場合には、その後の日時)に開始され、これが満了又は早期に失効する日時に終了する期間をいう。

秘密鍵：

公開鍵暗号システムにおける鍵ペアの内の一つで、他人には知られないように秘密にしておき、デジタル署名を作成するために使用される鍵をいう。

公開鍵：

公開鍵暗号システムにおける鍵ペアの内の一つで、それに対応する秘密鍵を持つ署名者から公開され、デジタル署名を検証するために使用される鍵をいう。

依拠する当事者：

証明書及び当該証明書に記載する公開鍵により検証可能なデジタル署名に依拠する者をいう。

リポジトリ：

証明書や失効リスト等を保管し、証明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。

証明書失効：

証明書の有効期間内に、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証明書を無効にする行為。

被発行者：

ユーザ証明書の名義人又はこれに特定される者をいう。

担当者：

ユーザから、その為にそれを代理して取引システムに基づき取引を行うことを授権されたユーザの代表取締役を除く役員、従業員、契約者、又は代理人をいう。

ユーザ証明書：

その被発行者がユーザの代表取締役であるか担当者であるかに関わらず、電子署名サービス契約に基づいて認証局 がユーザに対して発行する証明書をいう。

認証局 リポジトリ：

認証局 が維持し、運営するリポジトリをいう。

（例２）

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)を使用する非対称暗号方式(asymmetric cryptographic algorithm)の一つであり、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システム。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つ。
2. **公開鍵（Public Key）**
   公開鍵暗号システムにおける鍵ペアの内の一つで、それに対応する秘密鍵を持つ署名者から公開され、デジタル署名を検証するために使用される鍵をいう。
3. **秘密鍵（Private Key）**
   公開鍵暗号システムにおける鍵ペアの内の一つで、他人には知られないように秘密にしておき、デジタル署名を作成するために使用される鍵をいう。
4. **鍵ペア（Key Pair）**
   公開鍵暗号システムにおける公開鍵及びそれに対応する秘密鍵。
5. **共通鍵（Secret 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対称暗号方式(symmetric cryptographic algorithm)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、装置等を対象として、証明書を生成するプロセス。
8. **本人確認（Identification & Authentication）**
   個人、法人、装置等の認証対象者に関する情報が真正であることを審査する行為。
9. **証明書（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、発行認証局名などが含む一連の情報に、認証局のデジタル署名を付加したもの。従って、厳密には公開鍵証明書であるが、本書では曖昧さがない限り単に証明書という。
10. **証明書の発行（Certificate Issuance）**
    証明書を生成し、証明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. **証明書の失効（Certificate Revocation）**
    証明書の有効期間内に、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証明書を無効にする行為。

12. 証明書の一時失効（Certificate Suspension）
証明書の有効期間中に一時的に証明書を失効させる行為。
13. 失効リスト（Certificate Revocation List＝ＣＲＬ）
失効した証明書のリスト。通常認証局によるデジタル署名が付される。
14. 認証局（Certification Authority＝ＣＡ）
証明書の発行、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。
15. 登録局（Registration Authority＝ＲＡ）
証明書の発行や失効のプロセスにおいて、本人確認などの一部機能を認証局の承認を受けて行う個人または法人。登録局は、証明書や失効リストの生成は行わない。
16. リポジトリ（Repository）
証明書や失効リスト等を保管し、証明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。
17. 証明書加入者（Certificate Subscriber）
認証局から証明書の発行を受けた者。本書では特に区別が必要な場合を除いて、単に「加入者」という。
18. リライングパーティー（Relying Party）
取引等において証明書を利用する場合、証明書を受け取って、それを信頼して行動する者。加入者ばかりでなく非加入者も含まれる。本書では特に区別が必要な場合を除いて、単に「信頼者」という。
19. 証明書利用者（Certificate User）
証明書加入者及び証明書信頼者などの証明書を利用する者。本書では特に区別が必要な場合を除いて、単に「利用者」という。
20. 証明書ポリシー（Certificate Policy）
認証局のサービス・運用等に関する方針や規定、基準。
21. 認証局運用規定（Certification Practice Statement＝ＣＰＳ）
証明書ポリシーに基づいて、認証の実施における手続き、遵守事項などを文書化したもの。利用者等の認証局の外部者に開示されるもの。
22. 事務取扱要領（Operation Manuals）
認証局運用規定に基づいて、認証局内部における実務を詳細に規定したもの。
23. 危殆化（Compromise）
秘密鍵や関連機密情報等が、盗難や漏洩、第三者による解読等によってその機密性を失ったか、あるいはその可能性があること。

24. 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。

25. 電子署名（Electronic Signature）
間違い無く本人である事を証明する電子的なデータ。デジタル署名と同義で使われる事が多いが、広義ではアナログ署名を電子データにしたものも含む。

26. 暗号モジュール（Cryptographic Module）
暗号鍵等の生成、保管、利用などにおいて、セキュリティを確保する目的で使用されるソフトウェア、ファームウエア、ハードウェアあるいはそれらを組み合わせた装置。

3　参考文献

今回検討を進めるにあたって参考にした文献を以下に示す。（ＵＲＬは2001年3月現在）

1. TEDI 電子署名サービス契約（解説付き）
   http://www.fujitsu.co.jp/hypertext/solution/edi/japan/pdf/CA-japanease_anno.pdf
2. SecureSign®　パブリックサービス標準規程（V1.0）（2000 年３月３１日）（日本認証サービス株式会社）　http://www2.jcsinc.co.jp/repository1/sscpsv1.0-ja.pdf
3. 認証サービス利用約款Ｂ案（公共調達）
4. DC CARD－インターネットショッピング－証明書約款（株式会社ﾃﾞｨｰｼｰｶｰﾄﾞ）
   http://www.dccard.co.jp/ec/ec_set_i.shtml
5. “電子調達マーケットプレイス”利用規約（ＮＴＴコミュニケーションズ株式会社）
   http://www.marketcrosssite.net/agreement/index.html
6. TWX‐21　一般参加登録企業規約（株式会社日立製作所）
   http://mcharge.twx-21.hitachi.ne.jp/MiMC/MCMijk31.htm
7. ASKUL　B2B　MART　利用規約（アスクル株式会社）
   http://auction.askul.co.jp/demomall/guide/b2b_kiyaku.html

4 メンバーリスト

事務局

菅　　知之　　電子商取引推進協議会　主席研究員

紙田　政典　　電子商取引推進協議会　主席研究員

米倉　早織　　電子商取引推進協議会　主席研究員

ＴＦ３メンバー（編集メンバー）

No.	氏名	会社名
1	宮崎　裕二	ＮＴＴコムウェア株式会社
2	後藤　啓一	株式会社ＮＴＴデータ
3	長嶋　　潔	東京海上火災保険株式会社
4	須賀　英興	三菱電機株式会社

SWG２メンバー（上記以外）

No.	氏名	会社名
1	中嶋　伸之	RSA セキュリティ株式会社
2	金子　　実	株式会社イトーキ
3	熊木　克巳	株式会社エヌジェーケー
4	河田　悦生	NTT ドコモ株式会社
5	関野　公彦	NTT ドコモ株式会社
6	関　　信雄	NTT コムウェア株式会社
7	武藤　　裕	NTT コミュニケーションズ株式会社
8	島田　　晃	株式会社 NTT データ
9	高村　昌興	株式会社 NTT データ
10	小熊　慶一郎	株式会社 NTT データ
11	酒田　　健	川鉄情報システム株式会社
12	保倉　　豊	グローバルフレンドシップ株式会社
13	高崎　政嗣	グローバルフォーカス株式会社
14	三原　裕ニ	住友金属工業株式会社(鋼材倶楽部)
15	宮下　　毅	コンピュータ･アソシエイツ株式会社
16	大西　雅春	佐川急便株式会社
17	宮本　直樹	三洋電機ソフトウェア株式会社
18	安江　　洋	株式会社三和銀行
19	時見　正隆	株式会社シー・アイ・シー
20	新谷　　敦	株式会社セントラルファイナンス
21	渡辺　秀明	ソニー株式会社
22	小林　由幸	株式会社第一勧業銀行
23	松山　博顕	株式会社第一勧業銀行
24	城野　剛伸	中部電力株式会社

25	北川　雅之	株式会社ディーシーカード
26	星野　　理	株式会社帝国データバンク
27	石井　幹夫	株式会社東海銀行
28	中原　　康	株式会社東芝
29	中川　宣彦	東電ソフトウェア株式会社
30	長谷　容子	日本アイ・ビー・エム株式会社
31	松本　　恵	日本アビオニクス株式会社
32	西岡　誠治	財団法人日本建設情報総合センター
33	織　晃一郎	社団法人日本航空宇宙工業会
34	小野　千秋	株式会社日本システムディベロップメント
35	塚本　哲史	株式会社日本システムディベロップメント
36	石井　範康	日本信販株式会社
37	村田　祐一	日本電信電話株式会社
38	春田　克治	日本認証サービス株式会社
39	荒木　義晴	日本ベリサイン株式会社
40	谷野　柾雄	日本ベリサイン株式会社
41	古寺　　薫	日本ユニシス株式会社
42	久米本　文哉	株式会社日立情報システムズ
43	千葉　寛之	株式会社日立製作所
44	飯塚　光二	富士重工業株式会社
45	小笠原　文夫	株式会社富士総合研究所
46	小村　　元	富士通株式会社
47	石丸　誠孝	富士通株式会社
48	大竹　範明	富士電機情報サービス株式会社
49	村山　英樹	株式会社三菱総合研究所
50	高田　修一	ﾏｲｸﾛｿﾌﾄ　ﾌﾟﾛﾀﾞｸﾄ　ﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ　ﾘﾐﾃｯﾄﾞ
51	田中　　稔	三菱電機株式会社
52	加藤　素樹	安田火災海上保険株式会社

平成１３年３月発行
発行：電子商取引推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5500-3600
E-mail　info@ecom.or.jp