（通信プロトコル・セキュリティの検討）

相互セキュリティ基盤に関する検討・認証局構築

認証局構築　調査報告書（1）

第一部　流通システムにおけるPKIを利用した

総合セキュリティ基盤の考え方

平成18年度　経済産業省委託事業

流通システム標準化事業

目次

1. はじめに 5

1.1. 本報告書の目的 5
1.2. 本書の位置付け 5
1.3. 用語定義 6

2. インターネットを利用した電子商取引のセキュリティ上の課題 8

2.1. インターネットを利用した電子商取引に関連するセキュリティインシデント 8
2.2. インターネットを利用した電子商取引に関連するセキュリティ上の脅威 9
2.2.1. 情報漏えい 11
2.2.2. 成りすまし 12
2.2.3. 改ざん 12
2.2.4. 事後否認 13
2.2.5. その他の脅威 13

3. PKIを用いたセキュリティの確保 14

3.1. 暗号化 14
3.2. 電子署名 18
3.3. 認証 19
3.4. 脅威と対応策との関係 20
3.5. PKIと証明書 21
3.6. 各種セキュリティプロトコル 22
3.6.1. SSL/TLS 22
3.6.2. S/MIME 23
3.6.3. AS2 24
3.6.4. ebMS 25
3.6.5. SOAP-RPC 26

4. 総合セキュリティ基盤 27

4.1. 総合セキュリティ基盤の目的及び定義 27
4.2. 総合セキュリティ基盤の構成 28
4.3. 総合セキュリティ基盤の利用者 29
4.4. 総合セキュリティ基盤における証明書発行時の利用者の認証方法 30
4.4.1. 証明書発行時の利用者の認証に必要な事項の整理 30
4.4.2. 総合セキュリティ基盤の証明書発行時における利用者の認証方法 30
4.5. 総合セキュリティ基盤で利用される証明書の利用用途 33

4.6. 総合セキュリティ基盤で利用される利用者の証明書の形式 35
4.7. 総合セキュリティ基盤を構成する認証局に関する要件 46

5. 総合セキュリティ基盤を構成する認証局の信頼モデル 47

5.1. PKIにおける認証局の階層モデル 47
5.1.1. 無階層構造 48
5.1.2. 多階層構造 49
5.1.3. ツリー構造 51
5.2. 複数の流通業界共通認証局が存在する場合の証明書の相互利用性の確保 52
5.2.1. 複数の流通業界共通認証局が存在する場合の問題点 52
5.2.2. マルチトラスト方式 54
5.2.3. マルチトラスト改良型方式 56
5.2.4. 相互認証方式 58
5.2.5. ブリッジ接続方式 60
5.2.6. スーパールート方式 62
5.2.7. 各方式の評価の整理 64
5.3. 総合セキュリティ基盤で採用する信頼モデルを検討する上で考慮すべき事項 65
5.4. 総合セキュリティ基盤において採用すべき信頼モデル 65

6. 既存認証局の利用可能性 68

6.1. 商用サービスによるSSLサーバ向けパブリック認証局 68
6.1.1. 商用サービスによるSSLサーバ向けパブリック認証局の特徴 68
6.1.2. 商用サービスによるSSLサーバ向けパブリック認証局の利用可能性 68
6.2. 商用サービスによる法人向けパブリック認証局 69
6.2.1. 商用サービスによる法人向けパブリック認証局の特徴 69
6.2.2. 商用サービスによる法人向けパブリック認証局の利用可能性 69
6.3. 商用サービスによる個人向け向けパブリック認証局 69
6.3.1. 商用サービスによる個人向けパブリック認証局の特徴 69
6.3.2. 商用サービスによる個人向けパブリック認証局の利用可能性 70
6.4. 流通業界における既存認証局 70
6.4.1. 流通業界における既存認証局の特徴 70
6.4.2. 流通業界における既存認証局の利用可能性 71
6.5. 電子署名法による認定認証局 71
6.5.1. 電子署名法による認定認証局の特徴 71
6.5.2. 電子署名法による認定認証局の利用可能性 71
6.6. 商業登記に基づく電子認証制度 72
6.6.1. 商業登記に基づく電子認証制度の特徴 72

6.6.2. 商業登記に基づく電子認証制度の利用可能性 72
6.7. 公的個人認証サービス 72
6.7.1. 公的個人認証サービスの特徴 72
6.7.2. 公的個人認証サービスの利用可能性 73
6.8. その他 73
7. 総合セキュリティ基盤において今後予想される課題 74
7.1. 今後において想定される総合セキュリティ基盤に関わる環境の変化 74
7.2. 環境変化に対する対応策 74

1. はじめに

1.1. 本報告書の目的

経済産業省が執り行う「平成 18 年度流通システム標準化事業」（以下、「標準化事業」）においては GDS および EDI のシステム基盤の共通化に関する検討が行われている。この共通化に関する検討では将来の EPC での利用についても考慮が行われている。

本年度においては、標準化事業に参画する企業に対して GDS 及び EDI 用途に使用する証明書を発行するための認証局（以下、「標準化事業認証局」）が二つ構築された。標準化事業認証局によって発行された証明書及びそれらを利用したアプリケーションについては、標準化事業において、入念な検証が行われている。当該検証作業には異なる標準化事業認証局間で発行された証明書の相互利用に関する検証なども含まれている。

現在運用されている標準化事業認証局は、十分なセキュリティの確保や将来の拡張性等に関する考慮が行われて構築されている。ただし、標準化事業内での利用を前提としているために、標準化事業終了後に、そのままの運用にて商用として業務を継続しようとした場合、幾つかの問題が発生することが想定される。また、現状では標準化事業の一部として標準化事業認証局の運用が行われているが、今後においては商用の認証局や流通業界において独自の認証局を構築している企業が商用サービスとして GDS、EDI 及び EPC の分野において証明書の販売を行うことを希望することが想定される。

本報告書（「相互セキュリティ基盤に関する検討・認証局構築」）の目的は、流通業界において合理的な価格で信頼性が確保された証明書が継続して供給される枠組みのガイドラインを示すことである。これらのガイドラインには認証局が満たすべき技術仕様や運用に関する要件、認証局に認定を与える機関などの要件が含まれている。

1.2. 本書の位置付け

本報告書は第一部、第二部、証明書ポリシーから構成されており、本書は本報告書の第一部に相当する。本書の名称は「第一部　流通システムにおける PKI を利用した総合セキュリティ基盤の考え方」である。

本書では、インターネット上の脅威及び、それに対する PKI を利用した対策について整理を行った後に、本報告書において「総合セキュリティ基盤」と呼ぶ GDS、EDI 及び EPC において安全な通信を行うために必要となる基盤に関するガイドラインについて示す。なお、総合セキュリティ基盤の中で中核的な役割を果たす認証局の認定機関については、本報告書の第二部である「第二部　PKI を用いた総合セキュリティ基盤構築に向けた対応」において要件等がまとめられる。また、認定機関が認定の際に利用する認証局のガイドラインは「流通業界共通認証局　証明書ポリシー」においてまとめられる。

1.3. 用語定義

用語集

No.	用語	意味
1	ASP	アプリケーションサービスプロバイダ。アプリケーションレベルのサービスを提供する事業者等。
2	CP	Certificate Policy（証明書ポリシー）。 認証局が証明書を発行する際の運用方針を定めた文書。
3	CPS	Certification Practice Statement（認証業務運用規程）。認証局の信頼性、安全性を対外的に示すために、認証局の運用、証明書ポリシー、鍵の生成・管理、責任等に関して定めた文書。
4	CRL	Certification Practice Statement（認証業務運用規程）。認証局の信頼性、安全性を対外的に示すために、認証局の運用、証明書ポリシー、鍵の生成・管理、責任等に関して定めた文書。
5	EPC	Electronic Product Code（電子製品コード）。
6	EPC グローバル	EPC グローバルは RFID 関連の標準ネットワーク「The EPCglobal Network」を普及させるための非営利団体
7	FIPS 140-1	米国 NIST(National Institute of Standards and Technology）が策定した米国連邦情報処理標準。暗号モジュールが満たすべきセキュリティ要件等について定めている。
8	FQDN	Fully Qualified Domain Name（完全に条件付けられたホスト名）。インターネット上でホストを唯一に識別するために設定される。
9	GDS	Global Data Synchronization（商品情報同期化）。
10	GDSN	Global Data Synchronization Network（商品情報同期化ネットワーク）。
11	IC カード	情報を記録し、計算することができる集積回路を組み込んだカードのこと。
12	SDP	Source Data Pool（提供者側データプール）。GDNS における商品情報の提供者側データプール。
13	TDB コード	株式会社帝国データバンクが定める企業の識別コード。
14	TSR コード	株式会社東京商工リサーチが定める企業の識別コード。
15	RDP	Recipient Data Pool （利用者側データプール）。GDNS における商品情報の利用者側データプール

No.	用語	意味
16	PKCS#10	PKCSとは旧米国RSA Data Security社（現在、米国EMC社）による公開鍵暗号方式を実現するための技術標準。その１つであるPKCS #10は、証明書発行要求メッセージの構文に関する規格。IETFにおいてRFC2986として規定されている。
17	PKI	Public Key Infrastructure（公開鍵基盤）。公開鍵暗号方式を基盤としたセキュリティ技術基盤、環境の総称。
18	XML	Extensible Markup Language（拡張可能なマーク付け言語）。データを記述するマークアップ言語を定義するためのメタ言語。
19	依拠当事者	証明書の有効性を確認し、当該証明書に依拠して電子署名の検証を行う者、または当該証明書に依拠して暗号文の作成を行う者。
20	クロスサイトスクリプティング	動的にWebページを生成するアプリケーションの脆弱性を利用し、悪意のスクリプトを実行させる攻撃手法。
21	データプール	GDSN において商品情報を登録するデータベース。
22	登録局	認証局が証明書を発行する際の利用者の審査（認証）を行う組織。
23	認証局	利用者に関する情報を確認した上で証明書を発行する組織。認証局は、その役割を細分化するために発行局と登録局に分けることがある。
24	認証局秘密鍵	認証局が所有する秘密鍵。証明書または CRL の作成に利用される。
25	発行局	認証局の秘密鍵の適正な管理に責任を負う組織。
26	リポジトリ	認証局の情報公開を行う組織。Web サーバもしくは LDAP サーバを利用して情報公開をすることが多い。
27	利用者	認証局が証明書を発行する対象者。利用者は、認証局が発行した証明書の公開鍵に対応する秘密鍵を所持している。

2. インターネットを利用した電子商取引のセキュリティ上の課題

2.1. インターネットを利用した電子商取引に関連するセキュリティインシデント

1990 年代にインターネットを利用した商取引が開始されてから、2007 年現在まで BtoB または BtoC の形態を問わず市場規模は拡大の一途をたどっている。経済産業省による「平成 17 年度電子商取引に関する市場調査　報告書」によればインターネット等を利用した電子商取引の市場規模は 2005 年において BtoB では 140 兆円、BtoC は 3.5 兆円であると推定されている。また、これらの市場規模の数値は今後も継続して増加することが見込まれている。

電子商取引の市場規模が拡大する一方、インターネットまたは情報技術に関わる犯罪・事故（電子商取引に関わらないものも含む）は増加の一途をたどっている。警察庁による「平成 18 年のサイバー犯罪の検挙及び相談状況について」によれば平成 18 年度中の情報技術をした犯罪の検挙件数は 4,425 件で前年度より 40%程度増加しており、過去 5 年間で約 3.3 倍程度になっている。なお、これらの数字は検挙に至った件数であるために、現実に起きた犯罪についてはこれらの件数よりも遥かに多いことが推定される。

以下に、近年話題になっている代表的なインターネットを利用したセキュリティインシデントについて解説を行う。

(1) フィッシング詐欺

フィッシング詐欺とは、悪意の第三者がオンラインバンキングを提供している金融機関や会員制のインターネットオークション事業者を装い、「パスワードの有効期限が満了したので新規のパスワードを設定してください」等の内容と本物のウェブサイトを装った偽のウェブサイトへの URL を貼ったメールを送付し、偽のウェブサイトで ID 及びパスワードやクレジットカード番号を入力させて、当該情報を不正に詐取する詐欺手法である。

フィッシング詐欺は、日本においては 2004 年頃に初めて詐欺の被害が確認されており、不正に取得された ID 及びパスワードが利用され、不正な現金の送金等の実害が発生している。現在においても、フィッシング詐欺を目的としていると考えられる迷惑メールはインターネット上に大量に流れている。

初期のフィッシング詐欺では偽装対象は金融機関が対象となることが多かったが、最近では、比較的に利用者がセキュリティ関する注意を払わない会員性のインターネットオークションなどが対象とされることも多い。不正に入手したインターネットオークションのアカウントについては、落札値を不正に吊り上げる等の行為に利用されていることが指摘されている。

EDI 等の分野においてもフィッシング詐欺同様のサーバ等の成りすましが発生する可能性があるために、何らかの対策が必要であると考えられる。

(2) DoS 攻撃によるサービスの停止

DoS（Denial of Service)攻撃とは、サーバなどのネットワークを構成する機器に対して、大量のアクセスを行い、サーバが提供するサービスを停止またはそれと同様の状態にする攻撃手法のことである。DoS 攻撃には DDoS 攻撃と呼ばれる複数台のコンピュータを用いて攻撃する手法も存在する。DDoS 攻撃では、攻撃者が管理するコンピュータだけではなく、コンピュータウィルスに感染したコンピュータも利用されることがある。海外では、インターネット上でサービスを提供する事業者に対して、クラッカーによる DoS 攻撃を利用したゆすり行為が行われていることが報告されている。

近年においては、異常トラフィックを自動的に検出して、そらの通信を遮断する侵入検知システム等も利用されているが、遮断すべき対象に正式な利用者までもが含まれる可能性は否定できないために、現在において DoS 攻撃を完全に防御する方法は存在しない。ただし、一般にクライアントに対するサーバ側の認証機能や制限機能が提供されている場合はサーバの DoS 攻撃への耐性が高くなる傾向にある。このため、GDS及びEDIで利用されるサーバについても同様の機能を組み込む必要性があると考えられる。

(3) SQLインジェクションによるサービスの停止・個人情報漏洩

SQL インジェクションとは、Web アプリケーション等のセキュリティ上の問題点を利用し､アプリケーション内部で SQL 文として解釈されうる入力値を送信することで、データベースを不正に操作する等を行う攻撃手法のことである。

SQL インジェクションにより、インターネットにおいて情報を提供しているサイトが不正に改ざんされてサービスの停止に陥ったり、オンラインショッピングから個人情報が流出する事件が発生している。

(4) その他

インターネットを利用した犯罪ではないが、P2P（Peer to Peer)ソフトを媒介として公共組織・企業等が所有する機密情報がインターネット上に流出する事故が多発している。これらの事故は、社員等が組織のセキュリティポリシーなどに反して機密情報を自宅に持ち帰って個人所有の PC で作業し、さらに当該 PC がコンピュータウィルスに感染したことによって発生している。このような、P2P ソフトによる情報漏えいのセキュリティインシデントは認知されているケースでも年間で数百件に達しており、認知されていないケースはその何倍にも登ると想定されている。

2.2. インターネットを利用した電子商取引に関連するセキュリティ上の脅威

前節ではインターネットに関連した代表的なセキュリティインシデントについて解説したが、本節ではインターネット上の脅威について一般的な概念の整理を行う。

現在のインターネットなどで使われる TCP/IP と呼ばれる通信プロトコルは､米国内の研究機関や大学などの限られたネットワーク環境での利用を想定して策定されていた。

悪意のある者が参加する可能性のある環境での利用を想定して作成されていないために、

TCP/IP のプロトコル自体にはセキュリティに関する配慮等は十分に成されていない。TCP/IP のプロトコルはその後、インターネットへの接続が ISP 等の民間企業にも開放されるようなってからも、インターネット上で主要なプロトコルとして利用されている。

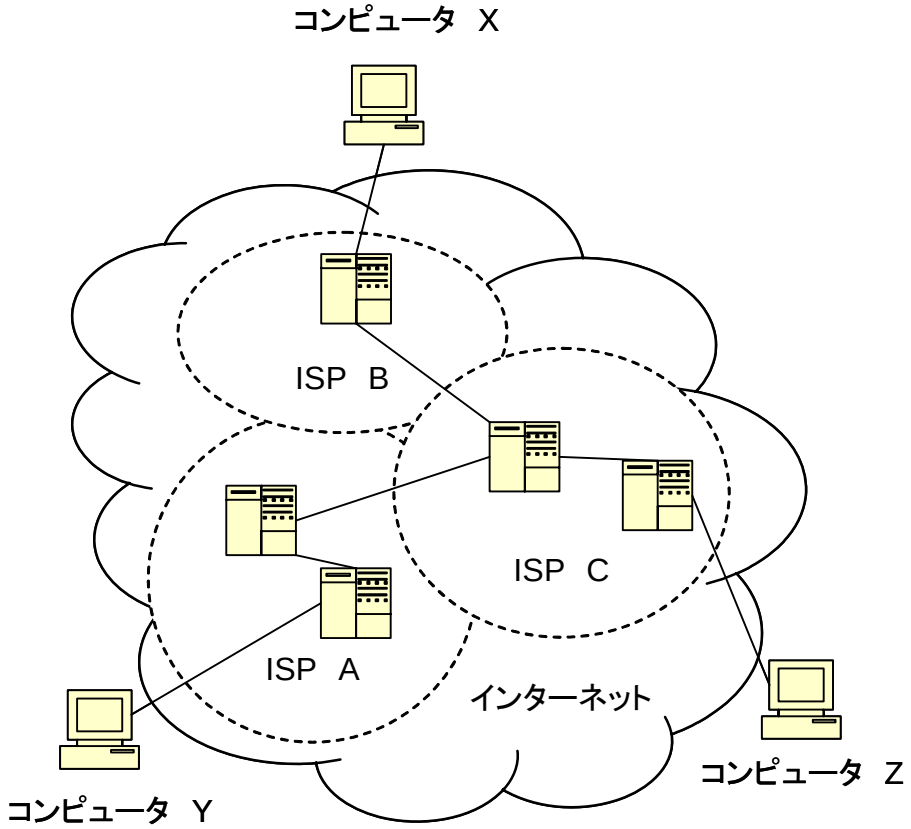

図 1 インターネットの構造

また、インターネットは各種のコンピュータネットワークを相互に接続した形態をとっているためにインターネット内の通信においては、送信者及び受信者と全く関わりのないネットワークを通過する場合がある（図 1 参照）。

このため、インターネットにはその性質上、セキュリティに関する問題点があり、インターネットを利用した電子商取引には幾つかの脅威が存在する。

これらのインターネットを利用した電子商取引の脅威の代表的なものは「情報漏えい」、「改ざん」、「成りすまし」、「事後否認」と分類されている。本節の以降の部分ではこれらの脅威及びその他の脅威について説明を行う（表 1 参照）。

表 1　インターネットを利用した電子商取引の脅威の概要

No.	脅威の種類	概要
1	情報漏えい	インターネット上の通信等において情報が漏洩すること。
2	成りすまし	インターネット上の通信において送信者または受信者が成りすましされること。
3	改ざん	インターネット上の通信等において情報が改ざんされること。
4	事後否認	インターネット上で通信された内容を送信者が、事後になって送信していないと否認すること。
5	その他	上記に含まれていない脅威。 電子商取引で利用されているシステムに存在する脆弱性等に攻撃が行われ、システムの停止、システムからの個人情報の漏洩が起こること。

2.2.1. **情報漏えい**

インターネットによる通信は、葉書による情報伝達に類似している点がある。葉書にはあて先や差出人の住所氏名だけでなく、本来伝えたい情報も保護されない状態で通常の場合は記載されている。葉書は、その配送過程において仕分け担当者や配達員によってあて先等の情報が逐次チェックされて、受信先に送られる。その際には、悪意のあるなしに関わらず、本来伝えたい情報までものが葉書を手にする者の目に触れる可能性がある。

インターネット上の通信も上記と同様の問題点を抱えている。インターネットにおいて現状使用されている通信プロトコルでは、通信されるデータはパケットと呼ばれる少量のデータに分割されて送信される(図 2 参照)。それぞれのパケットには宛先に関する情報や、適当な単位に分割された本来伝えたい情報が含まれている。これらのパケットはインターネットを通過する際に様々なNW機器やサーバ等を経由して送信者から受信者まで送信される。NW機器やサーバ等を経由する際にはパケット内のあて先等に関する情報は、NW機器やサーバ等にチェックされて、次の受信先に転送される。このため、悪意のあるNW機器等の管理者等がNW機器の設定を変更して、パケットのデータ部分の情報もチェックし、コピーを取得するなどの設定を行えば容易に情報の取得を行うことが可能である。

このように悪意のある第三者によって、インターネットを流れる情報が不正に詐取される場合や、システムの脆弱性を攻撃されることによって情報が不正に詐取される脅威のことを「情報漏えい」と呼ぶ。

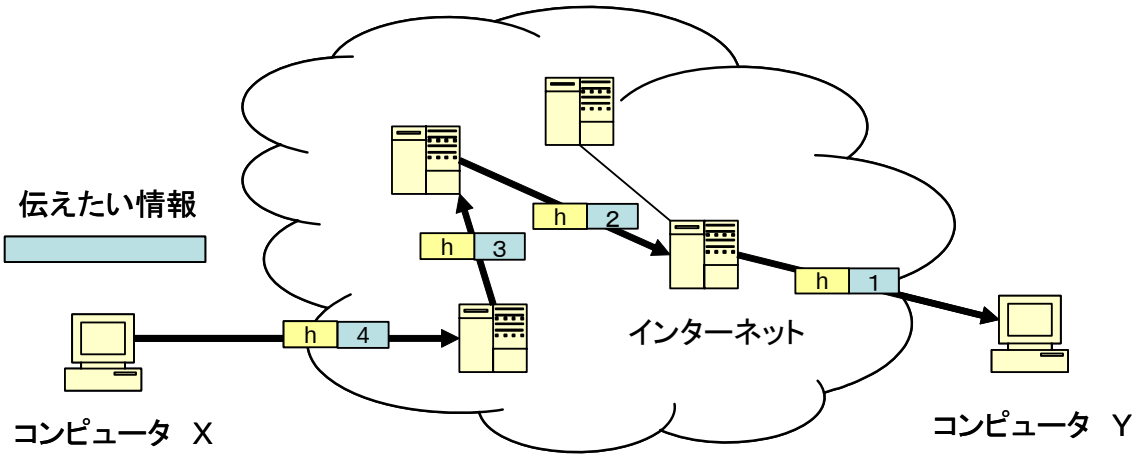

図 2　インターネット上の通信

2.2.2. 成りすまし

インターネットにおいて、現在使用されている通信プロトコルでは、送信者及び受信者間の強固な認証機能は提供されていない。

インターネットにおいては、特に BtoC などの取引を中心に直接会った事がない者同士が取引を行うことが多く、相手を正しく識別するのは非常な困難を伴う。

一般にインターネット上での通信においては受信先の指定は IP アドレスを直接しているするのではなく、URL などの送信元にとって認識がしやすい記述方式によって指定される。URL と IP アドレスのマッピングは通常は DNS に問い合わせることで行うことが一般的である。ただし、DNS に格納される情報については、悪意の第三者が一時的に書き換える等を行うことが可能である場合があり、これを利用して悪意の第三者が正しい受信先に成りすますことは可能である。また、別の手法としては悪意の第三者が受信先が所有するドメインと類似のドメイン名を取得し、送信元の不注意さを利用して受信先に成りすますことが行われる。この手法はフィッシングなどの攻撃に利用されている。

このような方法によって、悪意のある第三者が別の者に成りすます脅威のことを「成りすまし」と呼ぶ。

2.2.3. 改ざん

先に記載したとおりインターネット上の通信は、送信内容が保護されていない状態で、送信元および受信先が管理に携わっていないネットワーク上を通過することがある。このため、通信系路上に悪意のある第三者がアクセス可能な場合、悪意のある第三者は送信元

が送付した電子データを自身にとって都合が良い内容に改ざんし、受信先に対して改ざんした情報を送付することが可能である。

また、受信先が悪意を持っている場合は、送信元から受け取った情報を改ざんし、自身の都合のよい内容へ変更することが可能である。これは、インターネット上で受発注情報を電子データで送受するような場合は、受注元が受注数の水増し等を行えることを意味する。

なお、改ざんは悪意のある者によってのみよって引き起こされる場合だけでなく、ウィルスチェッカ等の善意のアプリケーションによって起こる場合もあることが指摘されている。

このように、情報が不正に書き換えられる脅威のことを「改ざん」と呼ぶ。

2.2.4. 事後否認

電子データは改ざんすることが容易であり、情報を削除すると痕跡が残らないという性質を有している。この性質はインターネット上で受発注情報を電子データで送受する際には大きな問題点となりうる。インターネット上で受発注情報を電子データをやりとりする場合、発注元は以下の不正を働くことができる。

- 発注元が、両者での合意が成立した後になって発注情報の変更や、発注自体を取り消すことを意図して、本来発注した情報について送付した事実を否認する。

このような場合では、改ざんの脅威のところで述べたように受注元も不正を働くことが出来るので、発注元と受注元で係争が発生したとしても第三者にとってはどちらの主張が正しいのか判別することができない。

上記のケースのように、インターネット上において電子データの交換時に、送信元が過去に送信した電子データについて送信した事実を否認するような脅威のことを「事後否認」と呼ぶ。

2.2.5. その他の脅威

インターネットを利用した電子商取引には、上記以外においても様々な脅威がある。例としては DoS 攻撃によるサービスの停止や、電子商取引で利用しているアプリケーションの脆弱性を突いてのサービスの停止、個人情報の不正詐取などである。近年話題となっているアプリケーションの脆弱性を突く攻撃方法としては、クロスサイトスクリプティング、SQL インジェクションなどがある。

3. PKI を用いたセキュリティの確保

本章では、2 章で整理を行ったインターネットを利用した電子商取引において発生する脅威に対してセキュリティを確保するための手段について記述する。

3.1. 暗号化

暗号化とは、ある情報を正当な読み取り権限を有しない第三者には理解が出来ないような状態に変換する技術である。通信の際に悪意の第三者の盗聴を防ぐ目的や、秘匿性を保ちながら情報を保管する目的等において暗号化が利用される。

暗号に関する基礎用語を 表 2 にまとめる。

表 2 暗号の基礎用語

No.	用語	意味
1	平文	暗号の対象となるデータ。
2	暗号文	暗号化された平文。
3	暗号化	平文を暗号文に変換すること。
4	復号	正規の手続きによって暗号文を平文に変換すること。
5	解読	正規の手続きによらず暗号文を平文に変換すること、またはそれを試みること。
6	鍵	暗号化時または復号化時に使用する特別なデータ。
7	暗号プロトコル	暗号技術を利用したプロトコル。

現代において利用されている暗号は二つの方式に分類することが可能である（図 3 参照）。

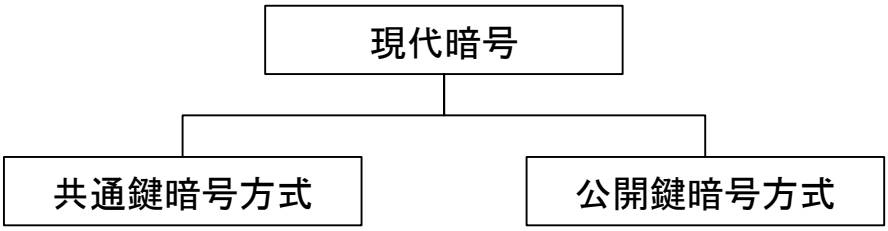

図 3 現代暗号の分類

共通鍵暗号方式はデータの暗号化を行う際と、暗号されたデータを元に戻す復号化の際に同一の鍵を利用する暗号方式である。別名として対称鍵暗号方式、慣用暗号方式または秘密鍵暗号方式と呼ばれる。

一方、公開鍵暗号方式は、1970 年代頃に発明された暗号で、別名として非対称鍵暗号方式とも呼ばれる。公開鍵暗号は暗号化を行う際と、復号化の際に異なる鍵を利用する。公開鍵暗号で暗号化に利用される鍵は公開鍵と呼ばれ、この鍵は秘密とされずに公開される。

復号化に利用される鍵は秘密鍵と呼ばれ、この鍵は復号化の権限を持つ者が安全に管理して利用する。

共通鍵暗号と公開鍵暗号は対照的な特徴を有しており、それを表 3 にまとめる。

表 3　共通鍵暗号と公開鍵暗号の比較

No.	比較項目	共通鍵暗号	公開鍵暗号
1	計算速度	実装が公開鍵暗号に比べて容易であり、計算速度は比較的早い。	一般に同じ強度の安全性を持つ共通鍵暗号に比べて 100 倍程度以上の計算時間を要する。
2	鍵配布の容易性	送信者と受信者が鍵を共有する必要がある。	送信者と受信者が鍵を共有する必要はない。
3	利用用途	• 暗号化	• 暗号化 • 電子署名 • 認証
4	その他の観点	長期にわたって利用されてきた暗号方式である。	歴史が比較的新しい暗号方式である。また、素因数分解問題、離散対数問題等を安全性の根拠に置いているため、当該問題を効率的に解決する方法が発見された場合は解読が行われる可能性がある。

共通鍵暗号方式と公開鍵暗号方式については、計算速度の観点では共通鍵暗号方式に優位性があり、鍵の配布に関しては公開鍵暗号方式の方に優位性がある。一般に、各種のプロトコルにおいては、データ（平文）の暗号化は一時的な鍵（セッション鍵）を利用して共通鍵暗号方式を用いて行い、共通鍵暗号方針で利用したセッション鍵を公開鍵暗号方式で暗号化して相手側に伝えるなどの、各暗号方式のメリットを補完的に利用した方法が利用されている。

表 4 に代表的な共通鍵暗号方式をまとめる。

表 4 代表的な共通鍵暗号方式

No.	名称	説明
1	DES	DES（Data Encryption Standard)は 1977 年に米国において現在の NIST（米国標準技術局）によって採用された共通鍵暗号の規格。暗号化の際のブロック長は 64 ビットで、実質的な鍵長は 56 ビットである。現在では、鍵長が短いなどの理由により利用が推奨されていない。
2	Triple DES	Triple DES とは一度の暗号化の際に DES を 3 回適用して、DES よりも安全な暗号化を行う暗号方式である。 3 回の処理に全ての異なる鍵を使う方式（3key Triple DES)と 1 回目と 3 回目の処理に同一の鍵を利用する方式（2key Triple DES)が存在する。ただし、現在ではセキュリティの観点から利用されている方式はほぼ 3key Triple DES である。 3key Triple DES の鍵長は 168 ビットであるが、総当り攻撃等は 168 ビット全ての鍵空間を計算するより効率的に行えることが知られている。3key Triple DES は NIST によって SP800-67 に規定されている。
3	AES	NIST によって DES の後継規格として公募が行われ、2001 年に採用された暗号。ベルギー人の研究者 Joan Daemen と Vincent Rijmen によって開発された。ブロック長は 128 ビット固定で、鍵は 128 ビット、192 ビット、256 ビットから選択することが可能。ソフトウェアによる実装にもハードウェアによる実装においても高速で動作するなどの特徴がある。 今後、様々な局面での利用が見込まれている。

また、表 5 に代表的な公開鍵暗号方式をまとめる。

表 5 代表的な公開鍵暗号方式

No.	名称	説明
1	RSA 暗号	RSA 暗号とは Ron Rivest、Adi Shamir、Len Adleman により 1977 年に開発された初の公開鍵暗号である。大きな合成数の素因数分解が非常に困難であることを安全性の根拠においている。 RSA 暗号は初めて実用化された公開鍵暗号であるために、セキュリティに関する検証は非常に行われているが、致命的な問題は指摘されていない。現在最も利用されている公開鍵暗号でもある。 RSA 暗号は秘密鍵と公開鍵を入れ替えても暗号化を行うことができる。この特徴は電子署名などに利用されている。
2	Elgamal 暗号	Elgamal が開発した公開鍵暗号。離散対数問題を安全性の根拠に置いている。これに関する暗号として、楕円曲線上の点の集合において Elgamal 暗号を適用する楕円暗号なども存在する。

なお、経済産業省と総務省は、平成 15 年に電子政府における調達のための推奨すべき暗号リスト（電子政府推奨暗号リスト）を作成し、これを公開した。電子政府推奨暗号リストには、各府省が情報システムの構築にあたって可能な限り利用を推進すべき暗号が示されている。電子政府推奨暗号リストで推奨されている暗号技術には公開鍵暗号、共通鍵暗号、ハッシュ関数等が含まれている。

3.2. 電子署名

電子署名とは、作成者の証明及び偽造・改ざん防止を目的として電子データに付与される付加的な電子データのことである。電子署名は、RSA 暗号が開発された後に、併せて提案された技術である。

電子署名では、電子署名を作成する者が署名鍵、検証鍵と鍵のペアを生成し、検証鍵を外部に公開する（図 4 参照)。電子署名を作成する際には電子署名対象データに対して署名鍵を利用して署名用アルゴリズムを適用して電子署名を作成する。一方、電子署名を検証する側であは、電子署名対象データと電子署名の組に対して、検証鍵を利用して検証用のアルゴリズムを適用して電子署名の検証を行う。電子署名が検証鍵に対応する署名鍵を所有する者によって行われていた場合、電子署名の検証は成功する。

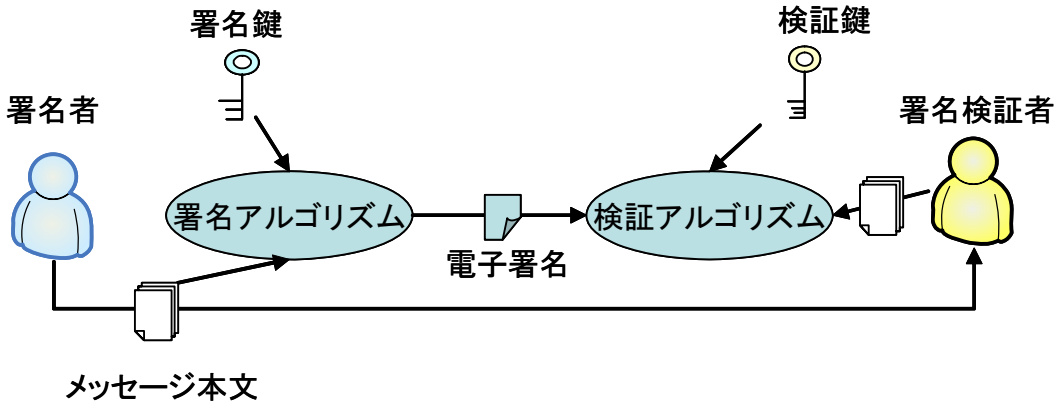

図 4　電子署名

表 6 に代表的な電子署名方式をまとめる。

表 6 代表的な電子署名方式

No.	名称	説明
1	RSA 署名	RSA 署名とは、RSA 暗号を利用した電子署名方式である。 RSA 暗号と同様に大きな合成数の素因数分解が非常に困難であることを安全性の根拠においている。 RSA 署名は、RSA 暗号が秘密鍵と公開鍵を入れ替えても暗号化を行うことができる特徴を利用している。 RSA 署名を行う場合は秘密鍵が署名鍵の機能を果たし、公開鍵が検証鍵の機能を果たすことができる。 RSA 署名は RSA 暗号同様に最も利用されている電子署名方式である。
2	DSA	DSA（Digtal Signature Algorithm)とは、NIST が制定した電子署名方式。離散対数問題を安全性の根拠においている。 楕円曲線上の点の集合において DSA を適用する楕円 DSA なども存在する。

なお、電子署名は、一般に公開鍵暗号の技術を応用しているために、大量のデータに対して単純に電子署名を行おうとすると非常に膨大な計算時間がかかるという問題点がある。このため通常は、（一方向性）ハッシュ関数と呼ばれる関数を対象データに適用して、電子署名の対象データを短くする工夫が行われる。

3.3. 認証

認証とは、何かしらの情報を元に、対象の本人性を確認する行為のことである。認証の方法には大きく分けて以下の三つの方法がある。

(1) 本人が知っていることを確認する
(2) 本人が持っている物を確認する
(3) 本人の生体的な特徴を確認する

これらの方法は単一で利用されることもあれば、複数の方法を組み合わせて利用されることもある。

一般にインターネットの世界における認証は(1)の本人が知っていることを確認することだけにより行われることが多い。本人が知っていることを確認することを用いた最も簡単な方式としては、パスワードの確認が挙げられる。パスワードを確認することは現在最も利用されている認証方法であるが、以下のような問題があることが指摘されている。

- 利用者がパスワードをメモに書きとめる等のずさんな管理を行う場合がある。

- 利用者が弱いパスワードを設定する場合がある。
- 利用者が同じパスワードを使いまわす場合がある。
- 管理者側でも利用者のパスワードを管理しなければならない等。

このため、パスワードを利用した認証の方式はセキュリティ的に弱いと考えられている。

本人が知っていることを確認する方法のもう一つの方法に電子署名の技術を応用した認証方式がある。この方式では、本人が自身の署名鍵を持っていることを確認することで相手の認証を行う。一般に、電子署名を利用した認証においては、認証を行う側が予め認証される側の検証鍵を入手しておく。認証の際には認証される側に乱数等を送付し、認証される側は当該乱数に対して電子署名を作成して、認証を行う側に送付する。認証を行う側は当該電子署名を検証することで、相手が署名鍵を持っていることを確認して認証を行う。

ただし、この方式は署名鍵は本人が記憶して保管されるのではなく、IC カードに格納されて管理されることや、PC 上で OS の機能により強固に守られて管理されることが一般的なので、本人が持っているものを利用した認証方式として扱われることもある。

この方法は、パスワードを利用した方式とは違い、秘密にしておくべき情報は本人のみが管理すればよい。このため、その点においてセキュリティ的に高いと考えられており幾つかのプロトコルで利用されている。

3.4. 脅威と対応策との関係

本節では 2.2 節で整理したインターネット上の脅威と 3.1 節から 3.3 節で説明を行ったセキュリティ確保のための対応策の関係についてまとめる。ただし、2.2.5 項において整理した、その他の脅威については暗号化、電子署名、認証を利用しても対応することが出来ない場合があるために、ここでは対応策を記載しない。

各脅威とそのための対応策を 表 7 にまとめる。

表 7　脅威と対応策の関係

No.	脅威の種類	対応策
1	情報漏えい	暗号化
2	改ざん	電子署名
3	成りすまし	認証
4	事後否認	電子署名

ただし、これらの公開鍵暗号方式を利用した対応策は通信相手等の公開鍵を確実に確認できることが前提になる。相手の公開鍵を確認するための手段は 3.5 節において説明を行う。

3.5. PKI と証明書

PKI（public key infrastruture)とは、公開鍵暗号、証明書及び認証局などを用いて、盗聴、改ざん、成りすまし、事後否認といった各種脅威を取り除くためのインフラストラクチャである（図 5 参照)。

証明書とは組織・個人・機器等（エンドエンティティ）を対象として、エンドエンティティが所有している公開鍵を証明する電子データである。

認証局とは、エンドエンティティを識別・認証しさらにエンドエンティティの公開鍵を確認した上で、エンドエンティティに証明書を発行する機関である。証明書には発行した認証局の電子署名が付与されている。証明書の正しさを検証する者（依拠当事者）は、信頼できる方法で直接または間接的に認証局の公開鍵が記載された認証局証明書を入手し、証明書に記載されている認証局による電子署名を確認することで、当該証明書の正しさの判断を行う。

なお、認証局は内部で階層構造を持つことができるため、依拠当事者は内部に存在する各認証局の証明書を階層構造に従って検証するなどの手続きが必要になる。証明書の検証の仕組み等については 5 章において概略の説明を行う。

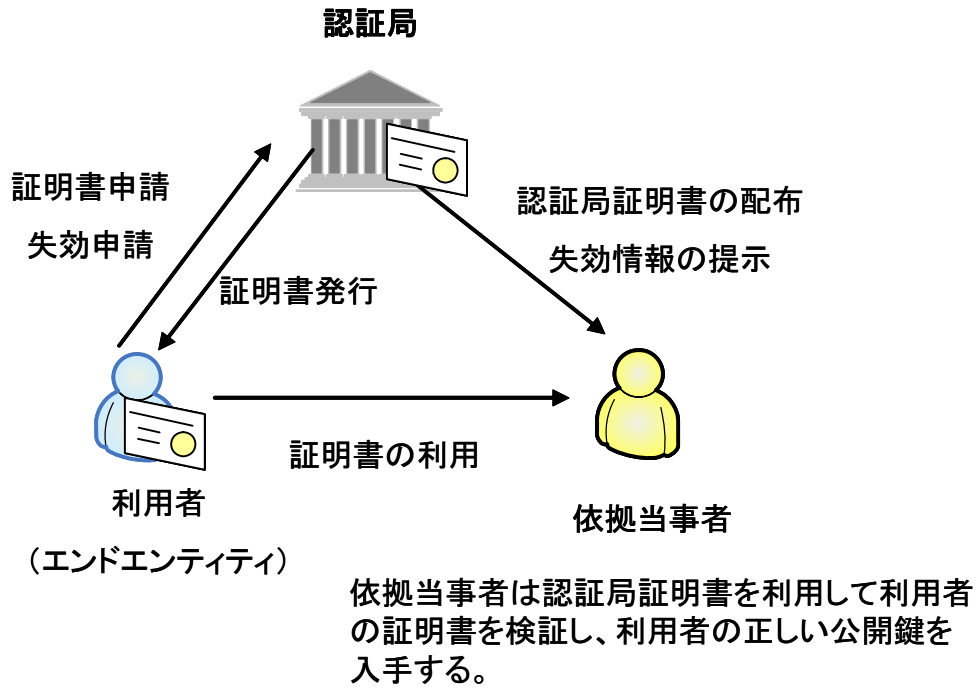

図 5　PKI の概要図

3.6. 各種セキュリティプロトコル

本節では、流通システムにおいて適用される PKI を利用した各種セキュリティプロトコルについて説明を行う。

3.6.1. SSL/TLS

SSL（Secure Sockets Layer)とは旧米国 Netscape Communications 社によって開発されえた通信プロトコルである。SSL は OSI の 7 層ネットワークモデルのトランスポート層に位置し、暗号化や認証の機能を提供する。SSL の主な適用範囲は WEB サーバと WEB ブラウザ間の通信であるが、それ以外の用途においても利用されている。SSL の最新バージョンは 3.0 である。TLS（Transport Layer Security）とは SSL3.0 の後継規格として IETF に RFC2246 として定められた標準規格である。

SSL/TLS にはサーバ認証だけを行うモードと、サーバ及びクライアント双方が認証対象となるモードがある。サーバ側には必ず証明書が必要であり、クライアントが認証対象となる場合はクライアントにも証明書が必要となる。

SSL/TLSが提供する機能を 表 8 にまとめる

表 8 SSL/TLS の機能

No.		SSL/TLS が提供する機能
1	情報漏えい防止	サーバとクライアント間の通信路は共通鍵暗号及び公開鍵暗号を利用して暗号化されるので、通信経路上の情報漏えいは防止できる。
2	成りすまし防止	サーバ側については、法人の実在性確認、当該法人が FQDN を管理していることがことの確認が一般的に行われる。 クライアント認証が利用された場合は、クライアントの認証も行われる。
3	改ざん防止	ハッシュ関数等を利用してチェック用のデータを生成することで、通信経路上においてサーバとクライアント以外の者が改ざんすること防止している。
4	事後否認防止	実現されない。

3.6.2. S/MIME

S/MIME(Secure/Multipurpose Internet Mail Extensions）とは IETF によって定められた電子メールの暗号化及び電子署名の付与を行うための仕様である。最新のバージョンは 3.1 であり、これらの仕様は RFC 3850～3853 で定義されている。

S/MIME は暗号化メールを送信する際は、相手の証明書を入手している必要があり、電子書名付きメールを送信するときは自身が証明書を取得していなければならない。暗号化と電子署名の機能は独立しており、各機能は同時に利用することも片方だけ利用することも可能である。

S/MIMEが提供する機能を 表 9 にまとめる。

表 9　S/MIME の機能

No.		S/MIME が提供する機能
1	情報漏えい防止	暗号化を利用することにより、メール本文は共通鍵暗号及び公開鍵暗号を利用して暗号化される。このため、メールの送信過程での情報漏えいを防止することが出来る。
2	成りすまし防止	電子署名を利用することにより、メールの送信元が確認できるために送信元の成りすましを防止することが出来る。
3	改ざん防止	電子署名を利用することにより、メールへの改ざんが検知できるため、改ざんを防止することが出来る。
4	事後否認防止	電子署名を利用することにより、受信者は送信者の電子署名が付与されたメールを受け取ることができる。このため、送信者がメール送信後に当該メールの内容について否認することは非常に困難である。

3.6.3. AS2

AS2 とは(Applicability Statement2）とは IETF によって定められたサーバ間でメッセージの交換を行うための仕様である。これらの仕様は RFC4130 で定められている。

AS2 はデータ発生の都度メッセージを送付するので、常時稼働可能なサーバでの運用を前提とし、グローバル IP アドレスが必要などの制約がある。AS２は米国ウォルマート社が採用しており、海外での利用が広がっている。また GDS の分野では標準の通信プロトコルとして利用されている。

AS2 ではセキュリティの機能として通信プロトコルの部分では SSL を利用し、メッセージ認証及び事後否認の機能については S/MIME を利用している。

AS2 が提供する機能を 表 10 にまとめる。

表 10　AS2 の機能

No.		AS2 が提供する機能
1	情報漏えい防止	サーバ間の通信は通信路は共通鍵暗号及び公開鍵暗号を利用して暗号化されるので、通信経路上の情報漏えいは防止できる。
2	成りすまし防止	双方のサーバについて、SSL と同様に法人の実在性確認、当該法人が FQDN を管理していることがことの確認が一般的に行われる。
3	改ざん防止	通信メッセージに電子署名を付与した場合は、当該メッセージの改ざんが防止される。また、通信データについても SSL と同様の改ざん防止機能が適用される。
4	事後否認防止	S/MIME の電子署名を利用する設定を行った場合は、通信メッセージの事後否認防止が実現される。

3.6.4. ebMS

ebMS とは、次世代 EDI の国際標準である ebXML の通信プロトコル部分の規格である。

ebMS は AS2 と同様にデータ発生の都度メッセージを送付するので、常時稼働可能なサーバでの運用を前提とし、グローバル IP アドレスが必要などの制約がある。ebMS では通信プロトコルの部分では SSL を利用しており、メッセージ認証及び事後否認の機能については XML 署名を利用している。

ebMSが提供する機能を 表 11 にまとめる。

表 11　ebMS の機能

No.		ebMS が提供する機能
1	情報漏えい防止	サーバ間の通信は通信路は共通鍵暗号及び公開鍵暗号を利用して暗号化されるので、通信経路上の情報漏えいは防止できる。
2	成りすまし防止	双方のサーバについて、SSL と同様に法人の実在性確認、当該法人が FQDN を管理していることがことの確認が一般的に行われる。
3	改ざん防止	通信メッセージに電子署名を付与した場合は、当該メッセージの改ざんが防止される。また、通信データについても SSL と同様の改ざん防止機能が適用される。
4	事後否認防止	通信プロトコル自体では保証されないが、メッセージレベルでの XML 署名を利用することで実現することができる。

3.6.5. SOAP-RPC

SOAP-RPC とは XML を利用して遠隔サーバの処理を呼び出すための仕様である。SOAP-RPC は、クライアント/サーバ型の構成のため、ebMS 等とは異なり、片側が常時稼働できないような環境でも利用することができる。このため、SOAP-RPC は中小企業などにおいての利用が見込まれている。SOAP-RPC では通信プロトコルにおいて SSL を利用しており、メッセージ認証及び事後否認の機能については XML 署名を利用している。

SOPA-RPCが提供する機能を 表 12 にまとめる。

表 12　SOAP-RPC の機能

No.		SOAP-RPC が提供する機能
1	情報漏えい	サーバとクライアントの通信は共通鍵暗号及び公開鍵暗号を利用して暗号化されるので、通信経路上の情報漏えいは防止できる。
2	成りすまし防止	サーバ側については、法人の実在性確認、当該法人が FQDN を管理していることがことの確認が一般的に行われる。 クライアント認証が利用された場合は、クライアントの認証も行われる。
3	改ざん防止	通信メッセージに電子署名を付与した場合は、当該メッセージの改ざんが防止される。また、通信データについても SSL と同様の改ざん防止機能が適用される。
4	事後否認防止	通信プロトコル自体では保証されないが、メッセージレベルでの XML 署名を利用することで実現することができる。

4. 総合セキュリティ基盤

前章までにおいて、インターネット上において電子商取引を実施する際の脅威及び PKI を利用した脅威の対応策の整理を行った。本章では流通業界において PKI を利用して安価に GDN、EDI、及び EPC の通信を行うための「総合セキュリティ基盤」について説明する。

4.1. 総合セキュリティ基盤の目的及び定義

本報告書では総合セキュリティ基盤の目的及び定義を以下の通りとする。

「総合セキュリティ基盤の目的」

インターネットのネットワーク上において、GDS、EDI、EPC に関する通信を安全かつ安価に行うため。

「総合セキュリティ基盤の定義」

総合セキュリティ基盤とは、上記目的を達成するための枠組み全体とする。総合セキュリティ基盤においては以下のことを実現する。

- GDS、EDI、EPC の分野において行われるインターネット上の通信の情報漏えいを防止する。
- GDS、EDI、EPC の分野においてサーバの成りすまし、クライアントの成りすましを防止する。
- GDS、EDI、EPC の分野において、やり取りが行われる情報の改ざんを防止する。
- GDS、EDI、EPC の分野において、やり取りが行われる重要な情報については送信者の事後否認を防止する。

4.2. 総合セキュリティ基盤の構成

総合セキュリティ基盤の概要図を 図 6 に示す。

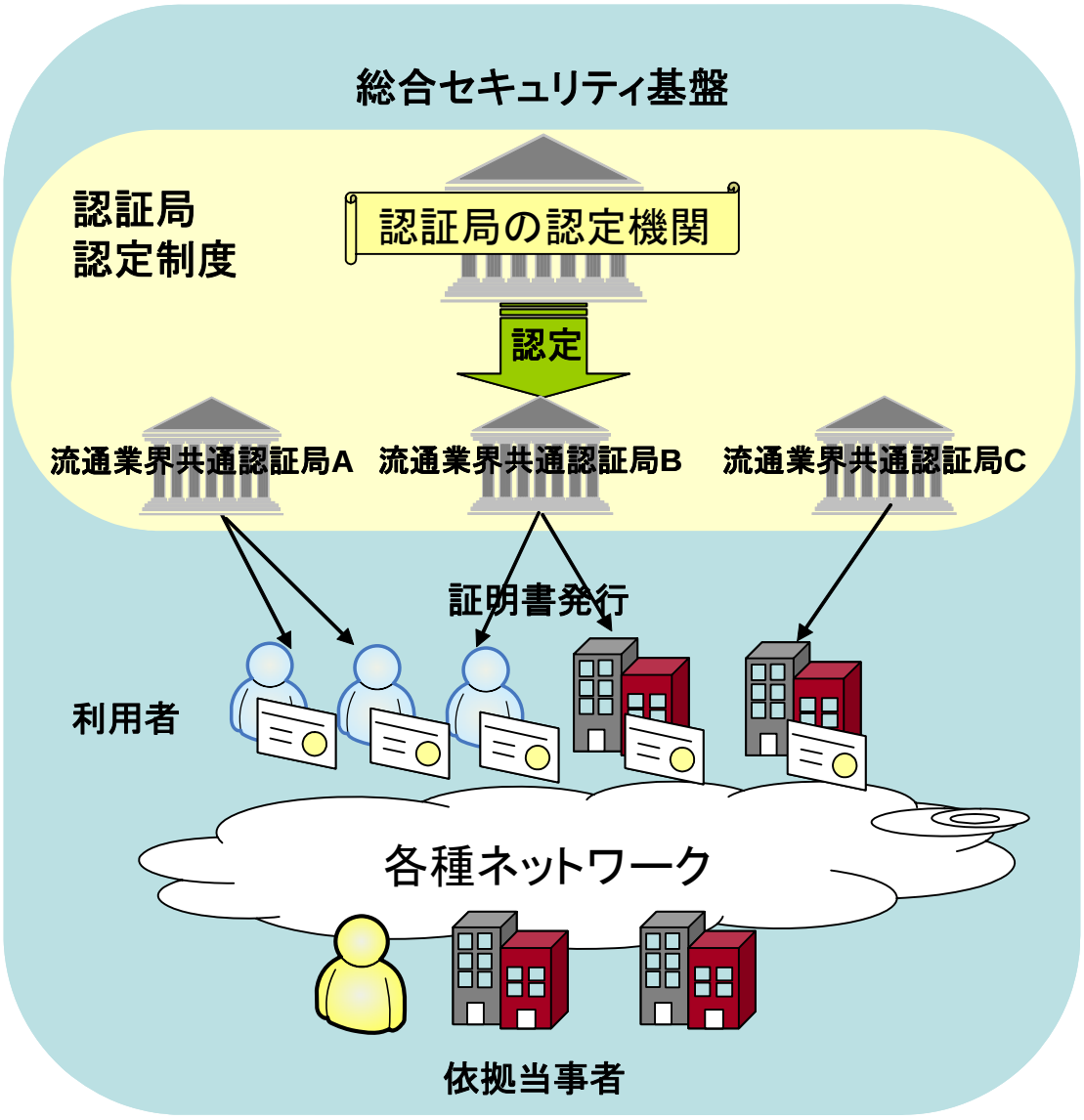

図 6 総合セキュリティ基盤の概要図

総合セキュリティ基盤の各構成要素の役割を 表 13 にまとめる。

表 13　総合セキュリティ基盤の構成要素の役割

No.	構成要素	役割
1	認定機関	総合セキュリティ基盤内において証明書の発行を希望する認証事業者が、一定水準のセキュリティ要件を満たしていることを確認し、これを「流通業界共通認証局」として認定する機関。また、ある流通業界共通認証局より証明書を入手した利用者が、総合セキュリティ基盤内のどのシステムにおいても当該証明書を利用できるようにするための処置を行う。認定機関の要件等については本報告書の第二部にて整理を行う。
2	流通業界共通認証局	認定機関より認定を受けて、総合セキュリティ基盤内で証明書を発行する認証事業者。利用者の認証を行い、証明書の発行を行う。流通業界共通認証局は内部で 3 階層以上の階層構造を採用することができる。
3	利用者	流通業界共通認証局から証明書の発行を受け、証明書を利用するものを指す。電子署名の作成や、暗号文の受領の際に証明書を利用する。利用者の対象範囲は 4.3 節で整理を行う。利用者の例としてはDPサーバ、EDI用サーバ等。
4	依拠当事者	利用者の証明書を検証し、依拠する者。依拠当事者による証明書への依拠は電子署名の検証や暗号文の作成を行う際に実施される。総合セキュリティ基盤においては依拠当事者の大部分は利用者でもある可能性が高い。依拠当事者の例としては DP サーバ、EDI 用サーバ、EDI 用クライアント等。

4.3.　総合セキュリティ基盤の利用者

本節では総合セキュリティ基盤における利用者の対象について整理する。総合セキュリティ基盤における利用者とは以下のものとする。

(1) 法人（法人登記を行って個人で事業を営んでいる者も含む。以下同様）
(2) 法人の従業者（役員、社員、契約社員等）
(3) 法人が所有するシステムまたはサーバ
(4) 個人事業主（法人登記を行わず、個人で事業を営んでいる者。以下同様）
(5) 個人事業主が所有するシステムまたはサーバ

ただし、上記に記載されている法人または個人事業主とは、流通業界において事業を行

っているか、流通業界において事業を行っている法人または個人事業主と取引関係にあるものに制限される。

4.4. 総合セキュリティ基盤における証明書発行時の利用者の認証方法

本節では総合セキュリティ基盤における証明書発行時の利用者の認証方法について検討を行う。

4.4.1. 証明書発行時の利用者の認証に必要な事項の整理

PKI の世界では組織や個人が証明書を必要とする場合、自身または代理のものを申請者として認証局に対して証明書の申請を行う。申請を受けた認証局は証明書の発行の前に当該申請について審査を実施する。この審査の際に確認される内容は以下の内容が含まれる。

(1) 証明書発行対象の実在性の確認

申請された証明書発行対象が確かに実在することを確認すること。法人の場合は、商業登記簿謄本の確認、または信頼できる民間の調査機関が所有するデータベースの情報等を確認することで当該法人が実在することの確認が行われることがある。個人の場合は、住民票、印鑑登録証明書、運転免許証の確認等により個人が実在することの確認が行われる。

(2) 証明書発行対象の本人性の確認

証明書発行対象が、実在性を確認した者と同一であることを確認すること。法人の場合は、申請書への法人代表印の押印及び印鑑証明書の提出による方法や、認証局が管理する外部情報を利用した企業代表電話等への電話照会等による確認が行われることがある。個人の場合は、申請書への実印への押印及び印鑑登録証明書の提出による確認が行われる。

(3) 証明書発行の意思の確認

証明書発行対象が証明書を取得することを希望していることの確認。通常は本人性の確認の際に提出した申請書により当該意思の確認が行われたと考える。

4.4.2. 総合セキュリティ基盤の証明書発行時における利用者の認証方法

実証実験の結果及び流通業界において最低限必要と考えられるセキュリティ要件を考慮し、総合セキュリティ基盤の証明書発行時において必要と考えられる利用者ごとの認証方法を 表 14 にまとめる。

表 14　利用者の認証方法

No.	利用者の種類	申請者	認証方法
1	法人	法人	認証局に対して申請者は、法人代表印による押印がなされた申請書（法人に関する情報を含む）と印鑑証明書と商業登記簿謄本を提出する。認証局は、商業登記簿謄本により法人の実在性の確認を行い、法人代表印の押印によって本人性の確認を行い、申請書によって意思の確認を行う。 または、認証局に対して申請者は、信頼できる民間調査会社から取得したコード等が記載された申請書を提出する。認証局は、当該コードを利用して法人の実在性の確認を行い、当該コードより企業代表電話番号を入手して電話確認を行うことで当該企業の本人性の確認を行い、申請書によって意思の確認を行う。
2	法人の従業者	法人	認証局に対して申請者は、法人代表印による押印がなされた申請書（法人の従業者に関する情報を含む）と印鑑証明書と商業登記簿謄本を提出する。認証局は、商業登記簿謄本により法人の実在性の確認を行い、法人代表印の押印によって法人の従業者の実在性及び本人性を認める。また、申請書によって法人の従業者の意思の確認を行う。 または、認証局に対して申請者は、信頼できる民間調査会社から取得したコード等が記載された申請書（法人の従業者に関する情報を含む）を提出する。認証局は、当該コードを利用して法人の実在性の確認を行い、当該コードより企業代表電話番号を入手して、法人の従業者に電話確認を行うことで本人性の確認を行い、申請書によって意思の確認を行う。

No.	利用者の種類	申請者	認証方法
3	法人が所有するサーバまたはシステム	法人	認証局に対して申請者は、法人代表印による押印がなされた申請書（サーバまたはシステムに関する情報を含む）と印鑑登録証明書と商業登記簿謄本を提出する。認証局は、商業登記簿謄本により法人の実在性の確認を行い、法人代表印の押印によって法人がサーバまたはシステムを所有していることを確認する。また、申請書によって法人の意思の確認を行う。 または、認証局に対して申請者は、信頼できる民間調査会社から取得したコード等が記載された申請書（サーバまたはシステムに関する情報を含む）を提出する。認証局は、当該コードを利用して法人の実在性の確認を行い、当該コードより企業代表電話番号を入手して、サーバまたはシステムの管理者に電話確認を行うことで法人がサーバまたはシステムを所有していることを確認する。また、申請書によって法人の意思の確認を行う。 さらに FQDN については whois 検索またはその他確実な方法により当該法人が当該 FQDN を利用する権利を有していることの確認を行う。
4	個人事業主	個人事業主	認証局に対して、申請者は実印による押印がなされた申請書（個人事業主に関する情報を含む）と印鑑登録証明書を行う。 認証局では、印鑑登録証明書により個人事業主の実在性確認を行い、実印の押印によって本人性の確認を行い、申請書によって意思の確認を行う。

No.	利用者の種類	申請者	認証方法
5	個人事業主が所有するサーバまたはシステム	個人事業主	認証局に対して、申請者は実印による押印がなされた申請書（サーバまたはシステムに関する情報を含む）と印鑑登録証明書を行う。 認証局では、印鑑登録証明書により個人事業主の実在性確認を行い、実印の押印によって個人事業主がサーバシステムを所有していることの確認を行う。申請書によって意思の確認を行う。 さらに FQDN については whois 検索またはその他確実な方法により当該個人事業主が当該 FQDN を利用する権利を有していることの確認を行う。

4.5. 総合セキュリティ基盤で利用される証明書の利用用途

各利用者が所有する証明書の利用用途は、実証実験の結果及び今後の拡張性を考慮して表 15 の通りとする。

表 15 証明書の利用用途

No.	証明書の種類	利用用途
1	法人	GDS・EDI 用途の電子署名・暗号化 GDS・EDI 用途の SSL クライアント認証
2	法人内の従業者	GDS・EDI 用途の電子署名・暗号化 GDS・EDI 用途の SSL クライアント認証
3	法人が所有するサーバまたはシステム	GDS・EDI 用途のサーバ認証・暗号化
4	個人事業主	GDS・EDI 用途の電子署名・暗号化 GDS・EDI 用途の SSL クライアント認証
5	個人事業主が所有するサーバまたはシステム	GDS・EDI 用途のサーバ認証・暗号化

なお、各証明書が利用される個別の暗号プロトコルについては規定しない。

また、EPC で使用される証明書については証明書のプロファイルの仕様は標準（「EPCglobal Certficate Profile Ratified Specification 1.0」2006 月 3 月 8 日 EPCglobal Inc.）として定められているものの、具体的な証明書を利用した通信プロトコルの仕様が本

報告書作成時において定められていないために、利用用途を規定しない。

また、EDI等の用途においてはASP事業者が、法人・個人事業主の代行者となって他の法人等と通信を行う場合が想定される（図 7 参照）。

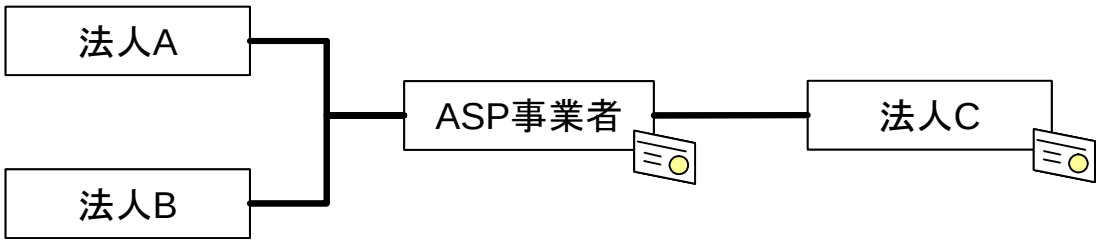

図 7　ASP 事業者を介した通信

このような場合、利用者の証明書の取得の仕方によっては下記の考慮すべき事項が存在する。

法人 A 及び法人 B がそれぞれ証明書を取得せず、ASP 事業者が自身のシステムを証明する証明書を取得しているような場合、法人 C が AS2 等の通信プロトコルを利用して認証することが出来るのは ASP 事業者までである。このため、法人 A と法人 C 間との通信については通信プロトコルレベルでは双方の認証は実施されない。このため、以下の方法による対応が必要と考えられる。

(1) 法人 A が AS2 等の通信プロトコルで使う証明書を取得し、ASP 事業者に当該証明書の利用を許可する。
(2) 法人 A がメッセージ署名のための証明書を取得し、取引上重要な情報の交換を行う際には、当該証明書によるメッセージ署名を行う。
(3) 法人 A は証明書を取得せずに、ASP 事業者及び法人 C との三者間の取り決めにより、当該認証レベルでの運用を認める。

4.6. 総合セキュリティ基盤で利用される利用者の証明書の形式

本節では総合セキュリティ基盤で利用される利用者の証明書の形式について整理を行う。なお、別冊の 7 章も参照のこと。

表 16　法人の証明書

― 基本領域 ―

No.	フィールド	設定
1	version	バージョン 3 を利用
2	serialNumber	各流通業界認証局が設定
3	signature	sha1WithRSAEncryption を利用
4	validity	3 年 2 ヶ月以内
5	issuer	証明書を発行した認証局の名称
6	subject	必須項目 C="jp" O="法人の英語名称" CN="法人の英語名称" 上記以外は任意
7	subjectPublicKeyInfo	rsaEncryption を利用 鍵長は 1,024 ビット以上
8	issuerUniqueID	使用してはならない
9	subjectUniqueID	使用してはならない

― 拡張領域 ―

No.	フィールド	設定	クリティカル	設定
10	authorityKeyIdentifier	△	FALSE	各流通業界認証局が設定
11	subjectKeyIdentifier	△	FALSE	各流通業界認証局が設定
12	keyUsage	◎	TRUE または FALSE	digitalSignature,keyEncipherment,dataEncipherment を設定
13	extendedKeyUsage	△	FALSE	各流通業界認証局が設定
14	privateKeyUsagePeriod	×	-	-
15	certificatePolicies	△	FALSE	各流通業界認証局が設定
16	policyMapping	×	-	-
17	subjectAltName	△	FALSE	各流通業界認証局が設定
18	issuerAltName	△	FALSE	各流通業界認証局が設定
19	basicConstraints	△	FALSE	各流通業界認証局が設定

No.	フィールド	設定	クリティカル	設定
20	nameConstraints	×	-	-
21	policyConstraints	×	-	-
22	cRLDistributionPoints	◎	FALSE	CRL を配布する URI を記載する

― プライベート拡張領域 ―

No.	フィールド	設定	クリティカル	
23	subjectDirectoryAtributes	×	-	-
24	authorityInfoAccess	△	FALSE	各流通業界共通認証局が設定

(◎は必須、○は推奨、△は任意、×は不可を表す。)

表 17　法人の従業者の証明書

― 基本領域 ―

No.	フィールド	設定
1	version	バージョン 3 を利用
2	serialNumber	各流通業界認証局が設定
3	signature	sha1WithRSAEncryption を利用
4	validity	3 年 2 ヶ月以内
5	issuer	証明書を発行した認証局の名称
6	subject	必須項目 C="jp" O="法人の英語名称" CN="従業者の名称のヘボン式ローマ字表記" 推奨項目 OU="従業者が所属する部署の英語名称" 上記以外は任意
7	subjectPublicKeyInfo	rsaEncryption を利用 鍵長は 1,024 ビット以上
8	issuerUniqueID	使用してはならない
9	subjectUniqueID	使用してはならない

― 拡張領域 ―

No.	フィールド	設定	クリティカル	設定
10	authorityKeyIdentifier	△	FALSE	各流通業界認証局が設定
11	subjectKeyIdentifier	△	FALSE	各流通業界認証局が設定
12	keyUsage	◎	TRUE または FALSE	digitalSignature,keyEncipherment,dataEncipherment を設定
13	extendedKeyUsage	△	FALSE	各流通業界認証局が設定
14	privateKeyUsagePeriod	×	-	-
15	certificatePolicies	△	FALSE	各流通業界認証局が設定
16	policyMapping	×	-	-

No.	フィールド	設定	クリティカル	設定
17	subjectAltName	△	FALSE	各流通業界認証局が設定
18	issuerAltName	△	FALSE	各流通業界認証局が設定
19	basicConstraints	△	FALSE	各流通業界認証局が設定
20	nameConstraints	×	-	-
21	policyConstraints	×	-	-
22	cRLDistributionPoints	◎	FALSE	CRL を配布する URI を記載する

— プライベート拡張領域 —

No.	フィールド	設定	クリティカル	
23	subjectDirectoryAtributes	×	-	-
24	authorityInfoAccess	△	FALSE	各流通業界共通認証局が設定

(◎は必須、○は推奨、△は任意、×は不可を表す。)

表 18　法人が所有するサーバまたはシステムの証明書

― 基本領域 ―

No.	フィールド	設定
1	version	バージョン 3 を利用
2	serialNumber	各流通業界認証局が設定
3	signature	sha1WithRSAEncryption を利用
4	validity	3 年 2 ヶ月以内
5	issuer	証明書を発行した認証局の名称
6	subject	必須項目 C="jp" O="法人の英語名称" CN="サーバまたはシステムの FQDN 名またはシステム名称" 推奨項目 OU="サーバまたはシステムを管理する部署の英語名称" 上記以外は任意
7	subjectPublicKeyInfo	rsaEncryption を利用 鍵長は 1,024 ビット以上
8	issuerUniqueID	使用してはならない
9	subjectUniqueID	使用してはならない

― 拡張領域 ―

No.	フィールド	設定	クリティカル	設定
10	authorityKeyIdentifier	△	FALSE	各流通業界認証局が設定
11	subjectKeyIdentifier	△	FALSE	各流通業界認証局が設定
12	keyUsage	◎	TRUE または FALSE	digitalSignature,keyEncipherment,dataEncipherment を設定
13	extendedKeyUsage	△	FALSE	各流通業界認証局が設定
14	privateKeyUsagePeriod	×	-	-

No.	フィールド	設定	クリティカル	設定
15	certificatePolicies	△	FALSE	各流通業界認証局が設定
16	policyMapping	×	-	-
17	subjectAltName	△	FALSE	各流通業界認証局が設定
18	issuerAltName	△	FALSE	各流通業界認証局が設定
19	basicConstraints	△	FALSE	各流通業界認証局が設定
20	nameConstraints	×	-	-
21	policyConstraints	×	-	-
22	cRLDistributionPoints	◎	FALSE	CRL を配布する URI を記載する

― プライベート拡張領域 ―

No.	フィールド	設定	クリティカル	
23	subjectDirectoryAtributes	×	-	-
24	authorityInfoAccess	△	FALSE	各流通業界共通認証局が設定

(◎は必須、○は推奨、△は任意、×は不可を表す。)

表 19　個人事業主の証明書

― 基本領域 ―

No.	フィールド	設定
1	version	バージョン 3 を利用
2	serialNumber	各流通業界認証局が設定
3	signature	sha1WithRSAEncryption を利用
4	validity	3 年 2 ヶ月以内
5	issuer	証明書を発行した認証局の名称
6	subject	必須項目 C="jp" O="Natural Person" CN="個人事業主の名称のヘボン式ローマ字表記" 上記以外は任意
7	subjectPublicKeyInfo	rsaEncryption を利用 鍵長は 1,024 ビット以上
8	issuerUniqueID	使用してはならない
9	subjectUniqueID	使用してはならない

― 拡張領域 ―

No.	フィールド	設定	クリティカル	設定
10	authorityKeyIdentifier	△	FALSE	各流通業界認証局が設定
11	subjectKeyIdentifier	△	FALSE	各流通業界認証局が設定
12	keyUsage	◎	TRUE または FALSE	digitalSignature,keyEncipherment,dataEncipherment を設定
13	extendedKeyUsage	△	FALSE	各流通業界認証局が設定
14	privateKeyUsagePeriod	×	-	-
15	certificatePolicies	△	FALSE	各流通業界認証局が設定
16	policyMapping	×	-	-
17	subjectAltName	△	FALSE	各流通業界認証局が設定
18	issuerAltName	△	FALSE	各流通業界認証局が設定
19	basicConstraints	△	FALSE	各流通業界認証局が設定

No.	フィールド	設定	クリティカル	設定
20	nameConstraints	×	-	-
21	policyConstraints	×	-	-
22	cRLDistributionPoints	◎	FALSE	CRL を配布する URI を記載する

― プライベート拡張領域 ―

No.	フィールド	設定	クリティカル	
23	subjectDirectoryAtributes	×	-	-
24	authorityInfoAccess	△	FALSE	各流通業界共通認証局が設定

(◎は必須、○は推奨、△は任意、×は不可を表す。)

表 20　個人事業主が所有するサーバまたはシステムの証明書

― 基本領域 ―

No.	フィールド	設定
1	version	バージョン 3 を利用
2	serialNumber	各流通業界認証局が設定
3	signature	sha1WithRSAEncryption を利用
4	validity	3 年 2 ヶ月以内
5	issuer	証明書を発行した認証局の名称
6	subject	必須項目 C="jp" O="法人の英語名称" CN="サーバまたはシステムの FQDN 名またはシステム名称" 推奨項目 OU="サーバまたはシステムを管理する部署の英語名称" 上記以外は任意
7	subjectPublicKeyInfo	rsaEncryption を利用 鍵長は 1,024 ビット以上
8	issuerUniqueID	使用してはならない
9	subjectUniqueID	使用してはならない

― 拡張領域 ―

No.	フィールド	設定	クリティカル	設定
10	authorityKeyIdentifier	△	FALSE	各流通業界認証局が設定
11	subjectKeyIdentifier	△	FALSE	各流通業界認証局が設定
12	keyUsage	◎	TRUE または FALSE	digitalSignature,keyEncipherment,dataEncipherment を設定
13	extendedKeyUsage	△	FALSE	各流通業界認証局が設定
14	privateKeyUsagePeriod	×	-	-

No.	フィールド	設定	クリティカル	設定
15	certificatePolicies	△	FALSE	各流通業界認証局が設定
16	policyMapping	×	-	-
17	subjectAltName	△	FALSE	各流通業界認証局が設定
18	issuerAltName	△	FALSE	各流通業界認証局が設定
19	basicConstraints	△	FALSE	各流通業界認証局が設定
20	nameConstraints	×	-	-
21	policyConstraints	×	-	-
22	cRLDistributionPoints	◎	FALSE	CRL を配布する URI を記載する

― プライベート拡張領域 ―

No.	フィールド	設定	クリティカル	
23	subjectDirectoryAtributes	×	-	-
24	authorityInfoAccess	△	FALSE	各流通業界共通認証局が設定

(◎は必須、○は推奨、△は任意、×は不可を表す。)

4.7. 総合セキュリティ基盤を構成する認証局に関する要件

PKI の世界においては、第二部において解説が行われる通り、同様の証明書を発行する複数の認証局が存在する可能性がある場合、各認証局が一定のセキュリティ要件を満たすことを維持するために証明書ポリシーが作成される。

総合セキュリティ基盤において、流通業界共通認証局に適用される証明書ポリシーについては「流通業界共通認証局　証明書ポリシー」として別冊にまとめる。

5. 総合セキュリティ基盤を構成する認証局の信頼モデル

本章では総合セキュリティ基盤において採用すべき流通業界共通認証局間の信頼モデルについて検討を行う。5.2.1 項にて説明が行われるとおりに複数の流通業界共通認証局が存在する場合は、証明書の相互利用性に関する問題が発生する。当該問題を解決するには適切な認証局間の信頼モデルを選定する必要がある。本章では、5.1 節において前提知識となる認証局の階層モデルの説明を行い、以降の節において採用すべき信頼モデルの検討を行う。

5.1. PKI における認証局の階層モデル

本節では PKI における認証局の階層モデルに関する説明を行う。

5.1.1. 無階層構造

無階層構造とは認証事業者AがA認証局を一つだけ構築し、A認証局が利用者の証明書を直接発行する方式のことである（図 8 参照)。

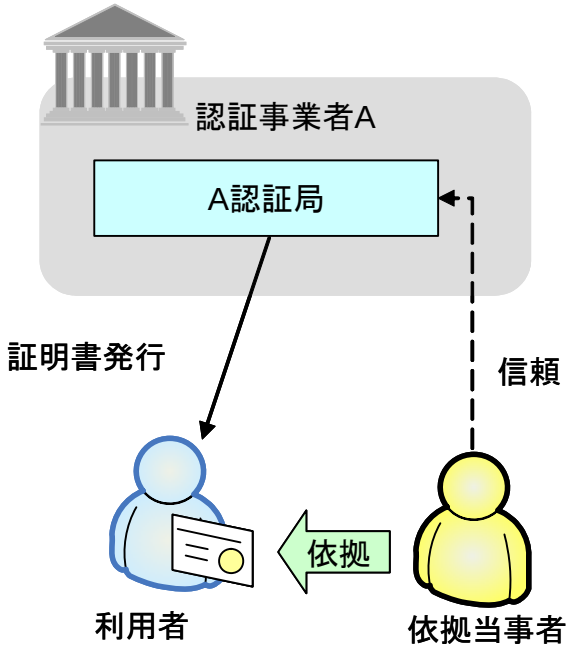

図 8　無階層構造

本構造では、依拠当事者は認証事業者 A の A 認証局を信頼する。信頼することの具体的な手続きとして、依拠当事者は A 認証局の認証局証明書を何らかの安全な方法で入手しなければならない。依拠当事者は、利用者の証明書に依拠する際に、利用者の証明書に付与されている電子署名を、A 認証局の認証局証明書に記載されている公開鍵を利用して検証する。当該検証が成功した場合、依拠当事者は、利用者の証明書は認証事業者 A によって発行されているものと判断する。

本構造は、拡張性に制限がある等の理由により、利用されるケースは限定的である。

5.1.2. 多階層構造

多階層構造では、認証事業者AがAルート認証局を含め、幾つかの中間認証局を構築する。Aルート認証局はA中間認証局１に対して証明書を発行する。A中間認証局１もさらにA中間認証局２に対して証明書を発行し、一番下位のA中間認証局Nが利用者の証明書を発行する（図 9 参照）。

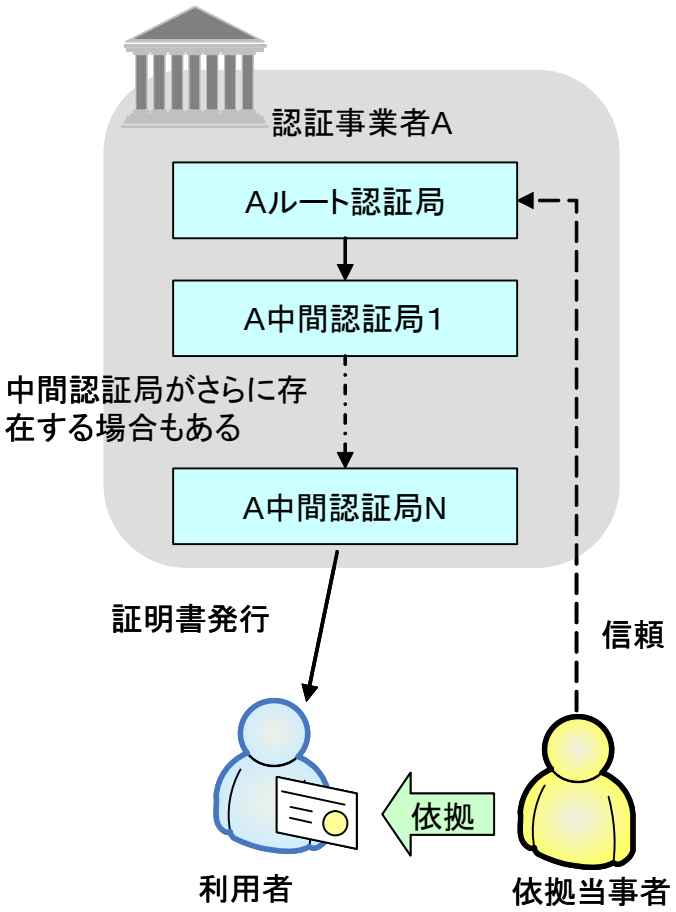

図 9　多階層構造

本構造では、依拠当事者は認証事業者 A の A ルート認証局を信頼し、A ルート認証局の認証局証明書を何らかの安全な方法で入手する。

また、依拠当事者は利用者の証明書に依拠する際には、A 中間認証局 1 から A 中間認証局 N の認証局証明書を入手していなければならない。各中間認証局の認証局証明書は、利用者が利用するアプリケーション等によって、利用者の証明書と一緒に依拠当事者に提示されることが多いが、そうでない場合は何らかの方法で各中間認証局の認証局証明書を入手することが必要となる。ただし、各中間認証局の認証局証明書は A ルート認証局の認証局証明書を信頼の拠点として、改ざんされていないことを検知することが可能である。このため、各中間認証局の認証局証明書は、A ルート認証局の認証局証明書に比べて容易に入

手することが可能である。

依拠当事者は利用者の証明書に依拠する際に、以下の手続きにより利用者の証明書に付与されている電子署名の検証を行う。

まず、A ルート認証局の認証局証明書に記載された公開鍵を利用して A 中間認証局 1 の認証局証明書の検証を行う。次に、A 中間認証局 1 の認証局証明書に記載された公開鍵を利用して A 中間認証局 2 の認証局証明書の検証を行う。このような手続きを中間認証局の数だけ繰り返し、最終的には A 中間認証局 N の公開鍵を利用して利用者の証明書に付与されている電子署名の検証を行う。当該検証が成功した場合、依拠当事者は利用者の証明書は認証事業者 A によって発行されているものと判断する。

5.1.3. ツリー構造

ツリー構造は、多階層構造の応用であり、証明書の利用用途やユーザグループごとに証明書を発行する認証局を構築する場合に利用される。

ツリー構造では、認証事業者AがAルート認証局を含め、幾つかの中間認証局を構築する（図 10 参照）。Aルート認証局はA中間認証局X1 及びA中間認証局Y1 に対して証明書を発行する。さらに、A中間認証局Y1 では多階層構造と同様にA中間認証局Y2 に対して証明書を発行する。

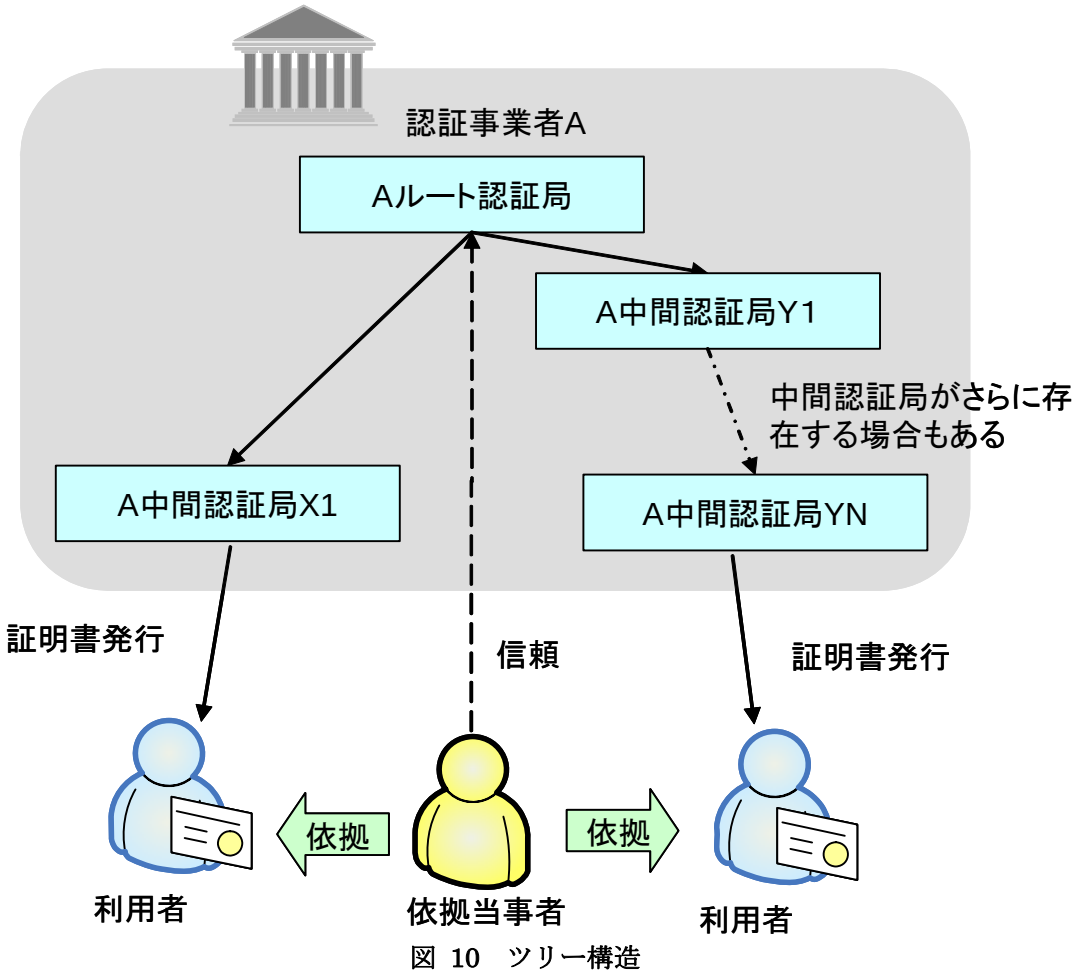

図 10　ツリー構造

本構造では、依拠当事者は認証事業者 A の A ルート認証局を信頼し、A ルート認証局の認証局証明書を何らかの安全な方法で入手する。

また、依拠当事者は利用者の証明書に依拠する際には、利用者の証明書から A ルート認証局までの各中間認証局の認証局証明書を入手していなければならない。これは多階層構造と同じである。また、依拠当事者は多階層構造と同じ方法にて利用者の証明書の検証を行う。

5.2.　複数の流通業界共通認証局が存在する場合の証明書の相互利用性の確保

本節では複数の流通業界共通認証局が存在する場合の問題点を指摘し、流通業界共通認証局間での証明書の相互利用性の確保を実現するための５つの方式を説明し、各方式の特徴の整理を行う。

5.2.1.　複数の流通業界共通認証局が存在する場合の問題点

5.1 節では認証事業者が唯一つ事業者のみ場合についての認証局の階層モデルの説明を行った。認証事業者が唯一つ事業者しか存在しない場合は前述のように、当該事業者のルート認証局証明書を依拠当事者が安全に入手していれば、全ての利用者の証明書の検証を行うことが可能である（中間認証局証明書の入手等について別途対応が必要)。

ただし、認証事業者が複数存在するようなケースでは問題が発生する（図 11 参照)。

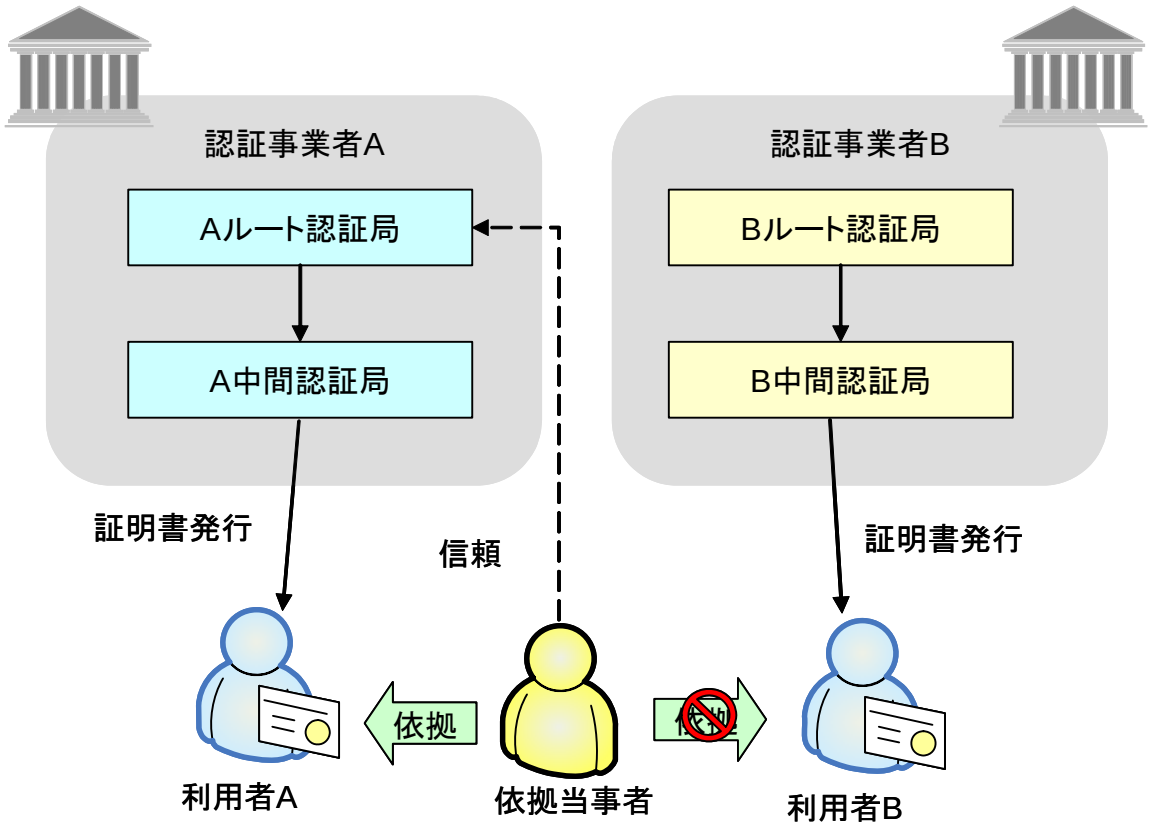

図 11　複数の認証事業者が存在する場合の問題点

認証事業者が複数存在する場合には、認証事業者 A の依拠当事者は、A ルート認証局証明書を安全な手段で入手しておくことで、認証事業者 A の利用者 A の証明書は信頼することが出来る。ただし、当該依拠当事者は、認証事業者 B の利用者 B の証明書については、B ルート認証局の認証局証明書を入手していないので信頼することは出来ない。

上記の問題は総合セキュリティ基盤において、流通業界共通認証局として認定された認

証事業者が複数以上存在する場合にも発生する。総合セキュリティ基盤では、複数の認証事業者が流通業界共通認証局として認定されることが想定されるため、この問題点についての対策が必要となる。本章の以降の部分では、当該問題を解決するための考えられる対策の整理と、最適な対応策の選定を行う。

5.2.2. マルチトラスト方式

マルチトラスト方式とは依拠当事者が、すべての流通業界共通認証局のルート認証局を信頼する方法である（図 12 参照）。

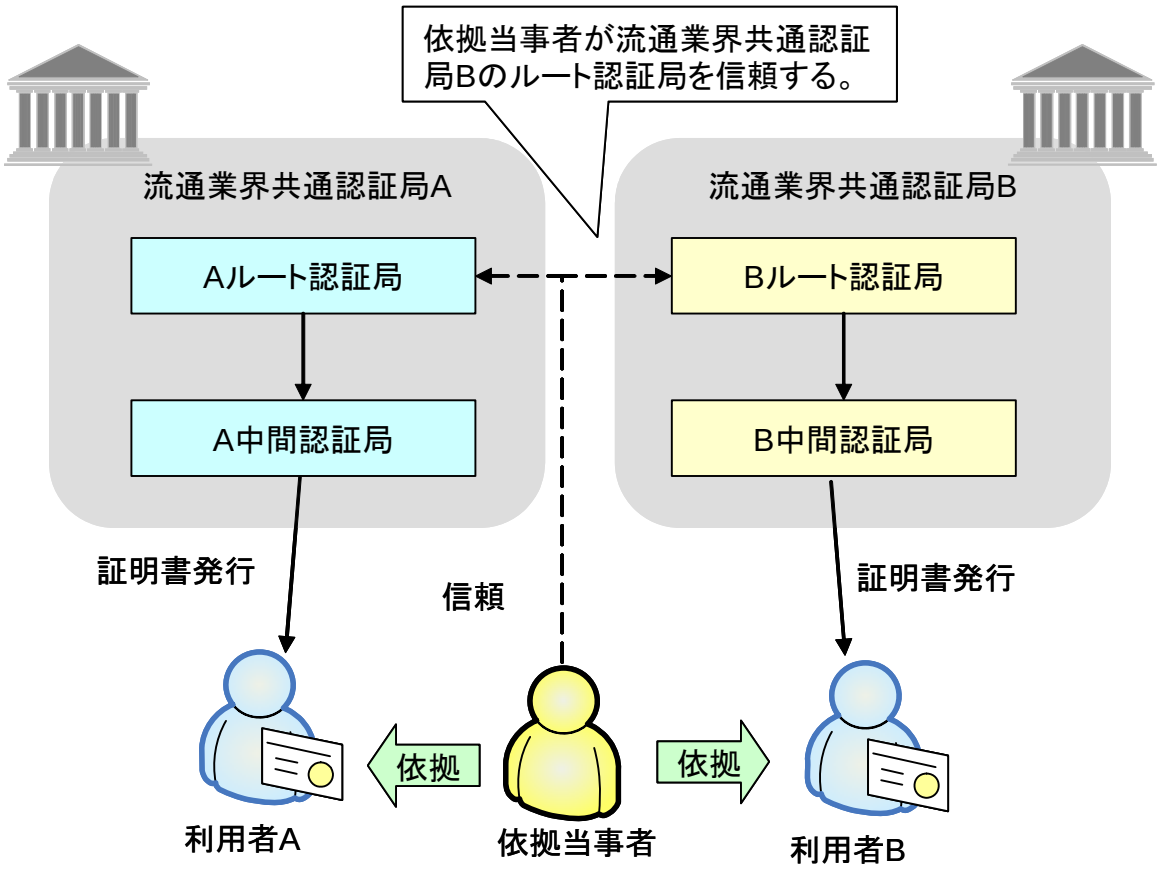

図 12　マルチトラスト方式

マルチトラスト方式では依拠当事者がすべての流通業界共通認証局のルート認証局を個別に入手し、インストール等の手続きを行う必要がある。

マルチトラスト方式を適用した場合の、各関係者の通常時の管理負荷、及び新規に流通業界共通認証局が認定された際の各関係者への影響を 表 21 にまとめる。

表 21　マルチトラスト方式の特徴

No.	評価項目	管理負荷、及び認定時の影響	評価
1	利用者	• 証明書の相互利用性の確保のための作業は特に必要ない。（証明書のコストの観点は除く）	◎
2	依拠当事者	• 総合セキュリティ基盤に参画する段階で既に認定を取得している流通業界共通認証局の認証局証明書を安全に入手する必要がある。 • 以下の証明書を何らかの手段により入手する必要がある ✓ 全ての流通業界共通認証局の中間認証局証明書 • 新規に認定を取得した流通業界共通認証局が現れた場合、当該認証局証明書を安全に入手する必要がある。	×/〇
3	認定機関	• 認定の他に、特に大きな作業及び管理負荷は発生しない。	◎
4	新規に認定を取得した流通業界共通認証局	• 自身のルート認証局の認証局証明書を依拠当事者全てが安全に入手できるための仕組みを提供する必要がある。	〇
5	既に認定を取得している流通業界共通認証局	• 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。	◎
6	その他の観点（アプリケーションへの影響等）	• 利用者の証明書の検証方法は極めてシンプルである。 • 既存アプリケーションの流用可能性が高い。	◎

（No.2 については流通業界共通認証局の全体数及び増加数が少ない場合は、作業負荷が軽いと想定されるために、評価を「×/〇」とした）

5.2.3. マルチトラスト改良型方式

マルチトラスト方式の応用として改良型を採用することも考えられる（図 13 参照）。

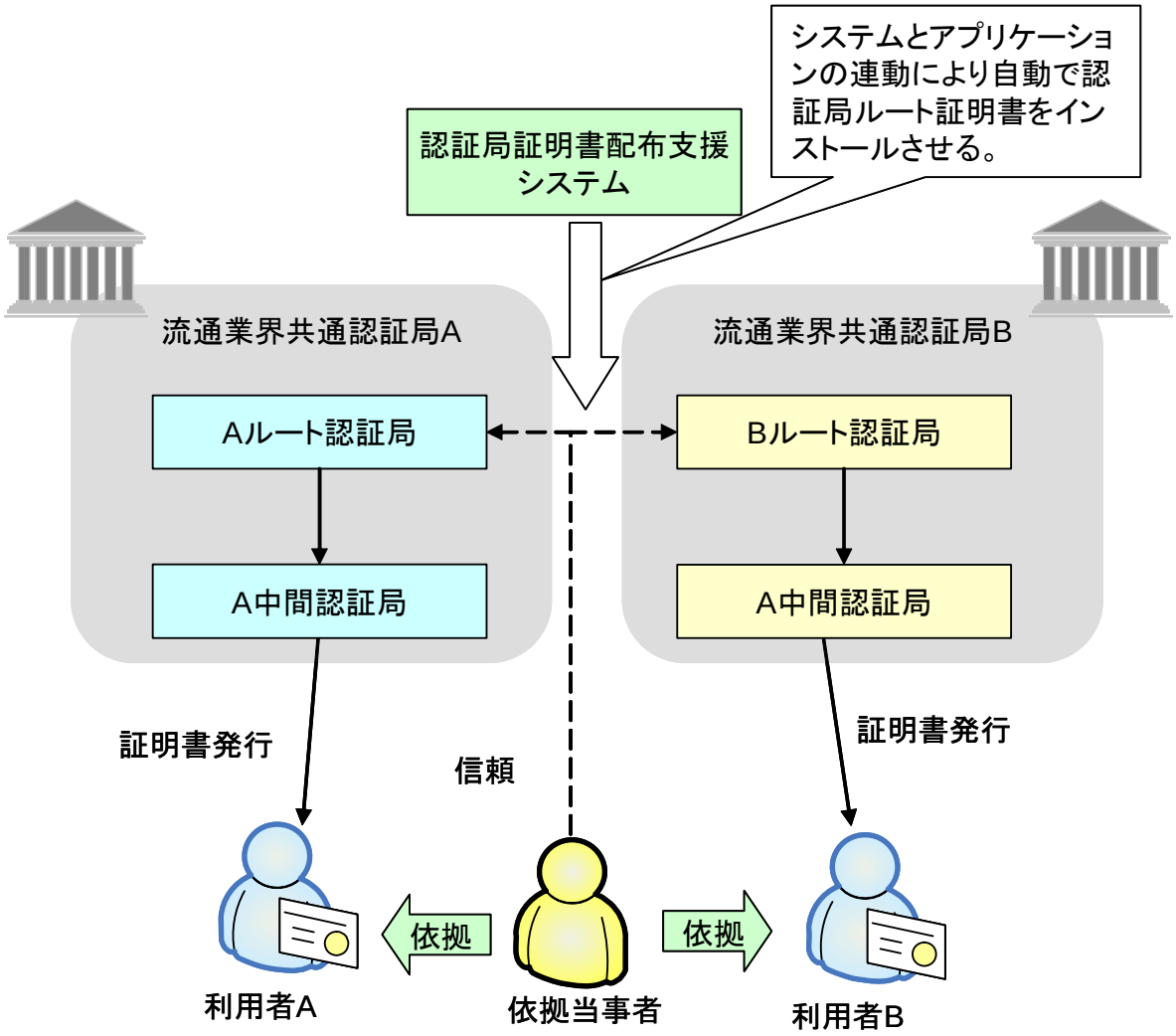

図 13　マルチトラスト改良型方式

マルチトラスト改良型方式では、依拠当事者に証明書を配布するための認証局証明書配布支援システムを構築する。当該システムではすべての流通業界共通認証局証明書を、安全な方法にて入手し、安全な方法で公開を行う。また、依拠当事者側の環境には新規に作成を行った認証局証明書取得アプリケーションを導入する。当該アプリケーションは定期的に認証局証明書配布支援システムへ問い合わせを行い、新規に認定を受けた流通業界共通認証局の認証局証明書が存在する場合、自動的に依拠当事者の環境に当該認証局証明書をインストールする。

マルチトラスト改良型方式を適用した場合の、各関係者の通常時の管理負荷、及び新規に流通業界共通認証局が認定された際の各関係者への影響を 表 22 にまとめる

表 22　マルチトラスト改良型方式の特徴

No.	評価項目	管理負荷、及び認定時の影響	評価
1	利用者	• 証明書の相互利用性の確保のための作業は特に必要ない。（証明書のコストの観点は除く）	◎
2	依拠当事者	• 認証局証明書取得アプリケーションをインストールする必要がある。 • 認証局証明書取得アプリケーションをインストールできない可能性がある。 • 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。 • 中間認証局証明書等の取得も自動化される。	△
3	認定機関	• 総合セキュリティ基盤を円滑に運営するために、認証局証明書配布支援システムを構築・運用するのは認定機関が適切であると判断される。このため、通常時の運用負荷が極めて高い • 認証局証明書取得アプリケーションを開発・保守するのは認定機関が適切であると判断される。このため、通常時の運用負荷が極めて高い。	×
4	新規に認定を取得した流通業界共通認証局	• 自身のルート認証局の認証局証明書を認証局証明書配布支援システムに安全に配布しなければならない。	○
5	既に認定を取得している流通業界共通認証局	• 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。	◎
6	その他の観点（アプリケーションへの影響等）	• 利用者の証明書の検証方法は極めてシンプルである。 • 既存アプリケーションの流用可能性が高い。	◎

5.2.4. 相互認証方式

相互認証方式とは各流通業界共通認証局のルート認証局同士がお互いに認める方式である（図 14 参照）。

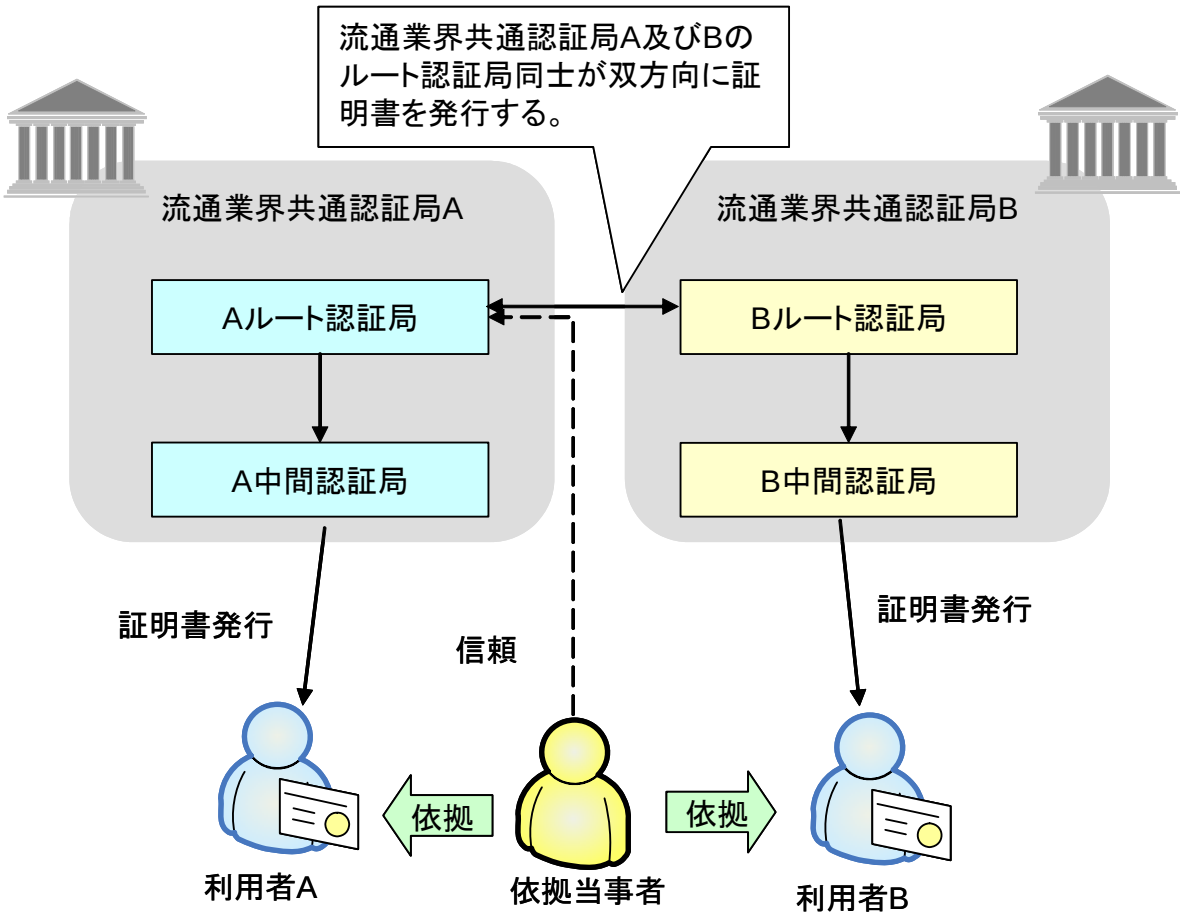

図 14　相互認証方式

相互認証方式では、依拠当事者は自身が既に信頼している流通業界共通認証局のルート証明書を基点とし、相互証明書を利用して他の流通業界共通認証局のルート認証局の公開鍵を検証する経路をたどり、他の流通業界共通認証局の利用者の証明書の検証を行う。

相互認証方式を適用した場合の、各関係者の通常時の管理負荷、及び新規に流通業界共通認証局が認定された際の各関係者への影響を 表 23 にまとめる。

表 23　相互認証方式の特徴

No.	評価項目	管理負荷、及び認定時の影響	評価
1	利用者	• 証明書の相互利用性の確保のための作業は特に必要ない。（証明書のコストの観点は除く）	◎
2	依拠当事者	• 初めに自身が信頼する流通業界共通認証局のルート証明書を安全に入手する必要がある。 • 以下の証明書を何らかの手段により入手する必要がある ✓ 全ての流通業界共通認証局の中間認証局証明書 ✓ 相互認証証明書（流通業界共通認証局の数だけ） • 相互認証証明書を経由した検証を行う必要がある。 • 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。	△
3	認定機関	• 総合セキュリティ基盤を円滑に運営するために、新規に認証を受けた流通業界認証局が現れた場合は、相互認証証明書を発行のために、既存の流通業界共通認証局との仲介を行う必要がある。	○
4	新規に認定を取得した流通業界共通認証局	• 新規に認定を取得した際に、既存の全ての流通業界共通認証局と相互認証証明書を発行する必要がある。	×/△
5	既に認定を取得している流通業界共通認証局	• 新規に認定を取得した流通業界共通認証局が現れ場合、相互認証証明書を発行する必要がある。	×/△
6	その他の観点（アプリケーションへの影響等）	• 既存アプリケーションが流用できない可能性がある。 • 認証事業者の技術仕様によっては、相互認証証明書を発行できない場合や、過度にコストが必要となる場合がある。	△

（No.4 及び No.5 については流通業界共通認証局の全体数及び増加数が少ない場合は、作業負荷がさほど重くないと想定されるために、評価を「×/△」とした）

5.2.5. ブリッジ接続方式

ブリッジ接続方式とは流通業界共通認証局間を仲介するブリッジ認証局を構築する方式である。ブリッジ認証局は全ての流通業界共通認証局のルート認証局と双方向に証明書を発行しあう（図 15 参照）。

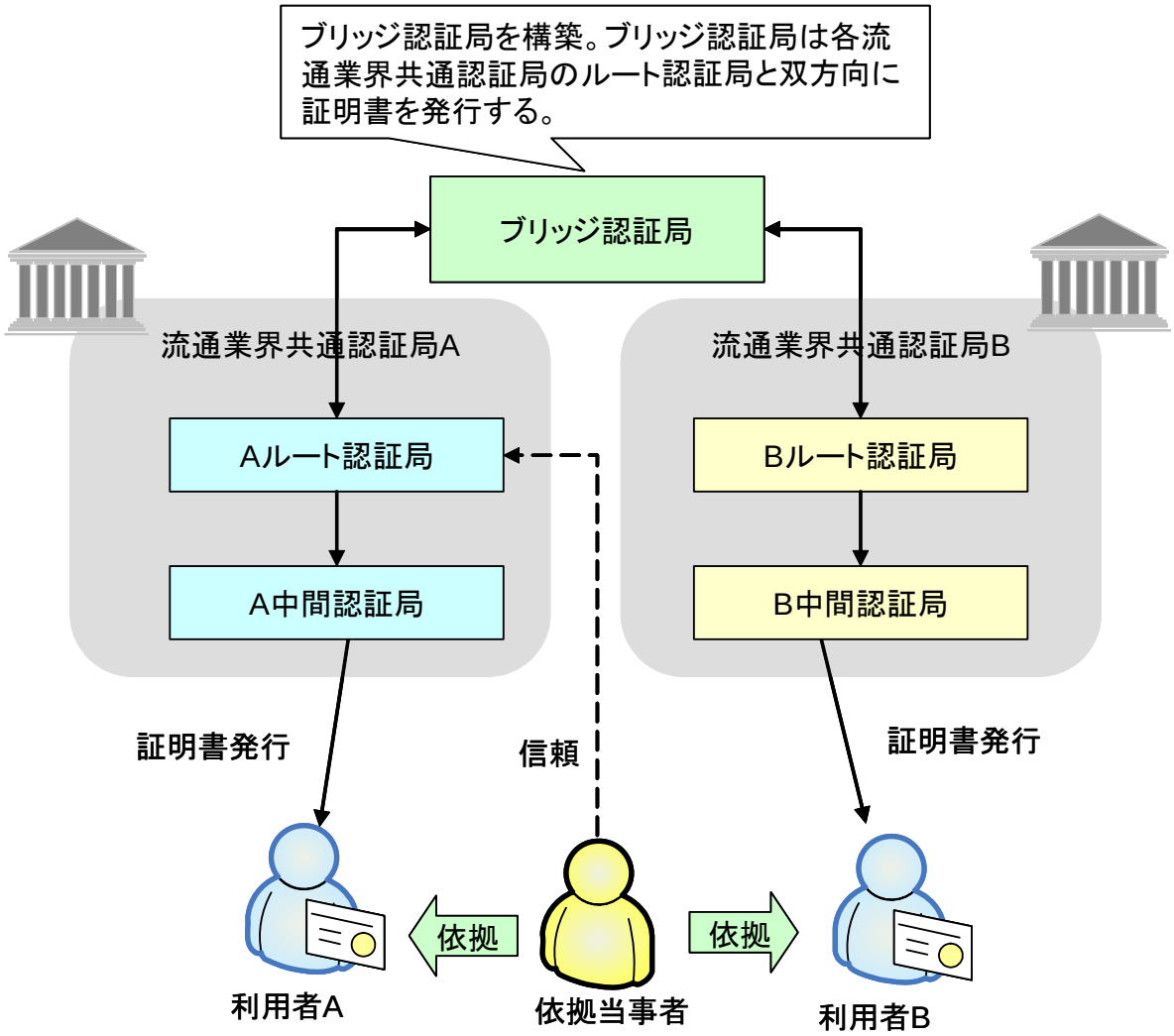

図 15　ブリッジ接続方式

ブリッジ接続方式では、依拠当事者は自身が既に信頼している流通業界共通認証局のルート証明書を基点とし、ブリッジ認証局及び他の流通業界共通認証局のルート認証局を経由して、他の流通業界共通認証局の利用者の証明書の検証を行う。

ブリッジ接続方式を適用した場合の、各関係者の通常時の管理負荷、及び新規に流通業界共通認証局が認定された際の各関係者への影響を 表 24 にまとめる。

表 24　ブリッジ接続方式の特徴

No.	評価項目	管理負荷、及び認定時の影響	評価
1	利用者	• 証明書の相互利用性の確保のための作業は特に必要ない。（証明書のコストの観点は除く）	◎
2	依拠当事者	• 初めに自身が信頼する流通業界共通認証局のルート証明書を安全に入手する必要がある。 • 相互証明証明書を 2 枚経由した検証を行わなければならない。 • 以下の証明書を何らかの手段により入手する必要がある ✓ 全ての流通業界共通認証局の中間認証局証明書 ✓ 相互認証証明書（全ての流通業界共通認証局数＋１） • 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。	△
3	認定機関	• 総合セキュリティ基盤を円滑に運営するために、ブリッジ認証局を構築・運用するのは認定機関が適切であると判断される。このため、通常時の運用負荷が極めて高い • 新規に認定を取得した流通業界共通認証局が現れた場合は相互認証証明書を発行する必要がある。	×
4	新規に認定を取得した流通業界共通認証局	• 新規に認定を取得した際に、ブリッジ認証局に相互認証証明書を発行する必要がある。	△
5	既に認定を取得している流通業界共通認証局	• 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。	◎
6	その他の観点（アプリケーションへの影響等）	• 既存アプリケーションが流用できない可能性がある。 • 認証事業者の技術仕様によっては、相互認証証明書を発行できない場合や、過度にコストが必要となる場合がある。	△

5.2.6. スーパールート方式

スーパールート方式とは各流通業界認証局の上位に認証局（スーパールート認証局）を構築する方式である。スーパールート認証局はすべての流通業界共通認証局のルート認証局に対して証明書を発行する（図 16 参照）。

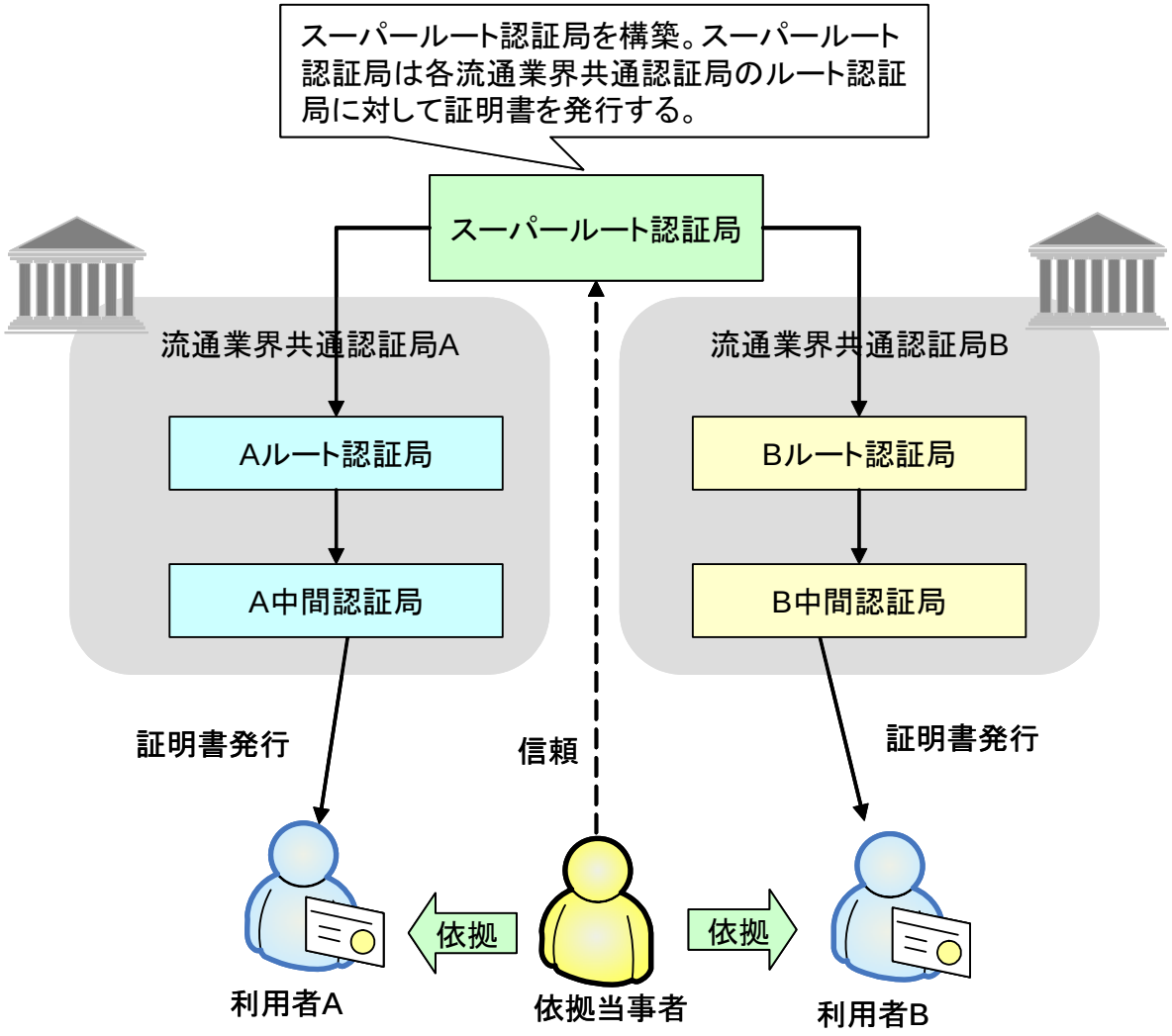

図 16　スーパールート方式

スーパールート方式では、依拠当事者はスーパールート認証局の認証局証明書を安全に入手し、これを信頼の起点とする。

依拠当事者はスーパールート認証局より、各流通業界共通認証局のルート認証局を経由して各利用者の証明書の検証を行う。

スーパールート方式を適用した場合の、各関係者の通常時の管理負荷、及び新規に流通業界共通認証局が認定された際の各関係者への影響を 表 25 にまとめる。

表 25　スーパールート方式の特徴

No.	評価項目	管理負荷、及び認定時の影響	評価
1	利用者	• 証明書の相互利用性の確保のための作業は特に必要ない。（証明書のコストの観点は除く）	◎
2	依拠当事者	• 初めにスーパールート認証局の認証局証明書を安全に入手する必要がある。 • 以下の証明書を何らかの手段により入手する必要がある ✓ 全ての流通業界共通認証局の中間認証局証明書 ✓ スーパールート認証局が発行した認証局証明書（全ての流通業界共通認証局数） • 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。	○
3	認定機関	• 総合セキュリティ基盤を円滑に運営するために、スーパールート認証局を構築・運用するのは認定機関が適切であると判断される。このため、通常時の運用負荷が極めて高い。 • 新規に認定を取得した流通業界共通認証局が現れた場合は認証局認証証明書を発行する必要がある。	×
4	新規に認定を取得した流通業界共通認証局	• 新規に認定を取得した際に、スーパルート認証局からの認証局証明書の発行を受ける必要がある。	△
5	既に認定を取得している流通業界共通認証局	• 新規に認定を取得した流通業界共通認証局が現れても特に作業は必要ない。	◎
6	その他の観点（アプリケーションへの影響等）	• 相互認証方式、ブリッジ接続方式に繰れべれば既存のアプリケーションの流用可能性は高い。	○

5.2.7. 各方式の評価の整理

各方式の評価を表 26 にまとめる。

表 26　各方式の評価の整理

No.	評価項目	マルチトラスト方式	マルチトラスト改良方式	相互認証方式	ブリッジ接続方式	スーパールート方式
1	利用者	◎	◎	◎	◎	◎
2	依拠当事者	×/○	△	△	△	○
3	認定機関	◎	×	○	×	×
4	新規に認定を取得した流通業界共通認証局	○	○	×/△	△	△
5	既に認定を取得している流通業界共通認証局	◎	◎	×/△	◎	◎
6	その他の観点（アプリケーションへの影響等）	◎	◎	△	△	○

5.3. 総合セキュリティ基盤で採用する信頼モデルを検討する上で考慮すべき事項

本節では、総合セキュリティ基盤で採用する信頼モデルを検討する上で考慮すべき事項について整理する。

(1) 既存の認証局の流用可能性への考慮

現在、流通業界においては、一部の大規模小売店や商社等が認証局を構築し、PKI の利用が行われている。これらの利用目的の多くは、旧来は専用線を利用していた取引先企業と EDI 通信をインターネットを介して行うことを目的としたものである。このため、一部の流通業界の企業では認証局の運用ノウハウが蓄積されており、また当該企業の取引先等では PKI の利用のノウハウが蓄積されていると想定される。今後、総合セキュリティ基盤において、流通業界共通認証局として認定を取得することを希望する企業を広く外部から求める場合、既に流通業界において認証局を構築している企業は認定を希望する企業として名乗りを上げる場合があると考えられる。

ただし、これらの既存の認証局は独自の技術仕様に基づいて運用を行っている可能性が高いと想定される。このため、当該企業に対する認定の窓口を広げることを考慮した場合は、信頼モデルについても技術的要件が低い方式を採用することが望ましいと考えられる。

(2) 想定される流通業界共通認証局の数

現在、商用のサービスとして証明書が販売されている最も主要な分野はパブリック SSL サーバ用証明書である。

当該分野において証明書を販売している認証事業者の数は比較的少なく、日本国内の場合、大手 5 社で市場の 90 パーセント以上を占めている。

このため、総合セキュリティ基盤においても流通業界共通認証局として認められる認証事業者の数はさほど多くないと予想される。

また、認証局を認定する制度として、総合セキュリティ基盤と類似のものに電子署名法による認証業務の認定制度が存在する（ただし、目的や規模が総合セキュリティ基盤と全く異なるのであくまでも参考情報である）。

当該認定制度において 2006 年 12 月 26 日現在、認定を受けている認証業務は 18 業務である。認定認証業務の証明書発行対象が、ほぼ国民全体であるという市場規模等の違いを考慮すると、流通業界共通認証局として認定を希望する企業の数は 18 よりもかなり少ない数であることが予想される。

5.4. 総合セキュリティ基盤において採用すべき信頼モデル

本節では、5.2 節及び 5.3 節の内容を踏まえ、総合セキュリティ基盤において採用すべき信頼モデルの検討を行う。

採用すべき信頼モデルの選択においては以下の事項への考慮が必要だと考えられる。

(1) 利用者が流通業界共通認証局より証明書を取得する際のコストが高くなる信頼モデルを採用するのは望ましくない。当該取得コストは認定機関または流通業界共通認証局の負荷が高い信頼性モデルであるほど、高くなることが想定される。
(2) 総合セキュリティ基盤の利用促進を考慮すると、依拠当事者に過大の負荷がかかる信頼モデルを採用するのは望ましくない。
(3) 依拠当事者が所有する既存のアプリケーションの流用に大きな制限がかかる信頼モデルを採用するのは望ましくない。
(4) 認定機関に過度の業務負荷を要求するような信頼モデルを採用するのは望ましくない。
(5) 流通業界共通認証局に過度の業務負荷を要求するような信頼モデルを採用するのは望ましくない。
(6) 流通業界で利用されている既存の認証局に関する受け入れ窓口を狭めるような技術要件の高い信頼モデルを採用するのは望ましくない。

また、検討においては以下の事項を前提条件とする必要がある。

「当面の間、総合セキュリティ基盤において流通業界共通認証局として認定される認証事業者の数は比較的少ないと想定される」

上記前提事項を踏まえ、各考慮事項について各方式の評価を 表 27 にまとめる。

表 27　各方式の評価

No.	考慮事項	マルチトラスト方式	マルチトラスト改良方式	相互認証方式	ブリッジ接続方式	スーパールート方式
1	（1）	○	×	○	×	×
2	（2）	○	×	○	○	○
3	（3）	○	○	×	×	○
4	（4）	○	×	○	×	×
5	（5）	○	○	×	○	○
6	（6）	○	○	×	×	○

表 27 で示すとおりに、認定される流通業界共通認証局が少ない場合は、マルチトラスト方式のみが、各考慮事項を問題なく満たすことが可能であり最もすぐれた方式と考えることができる。また、他の方式については、スーパールート方式がマルチトラスト方式に次いですぐれた方式であると考えることができる。

このため本報告書では、総合セキュリティ基盤において流通業界共通認証局が発行した

証明書の相互利用性の確保の手段としては、信頼モデルにマルチトラスト方式を採用することを推奨する。

6. 既存認証局の利用可能性

本章では、既に構築されている認証局の総合セキュリティ基盤での利用可能性について検討を行う。

6.1. 商用サービスによる SSL サーバ向けパブリック認証局

6.1.1. 商用サービスによる SSL サーバ向けパブリック認証局の特徴

商用サービスによるSSLサーバ向けパブリック認証局の特徴を 表 28 にまとめる。

表 28 商用サービスによる SSL サーバ向けパブリック認証局の特徴

No.	観点	概要
1	認証局の運営主体	商用サービスを提供する各認証事業者。
2	証明書の発行対象	多くの場合、法人が管理する SSL サーバ。一部法人登記を行っていない個人事業主に対して証明書を発行する認証事業者も存在する。
3	証明書の利用用途	SSLサーバ認証(主に 表 15 のNo.3 とNo.5 に相当する)。
4	証明書の特徴	法人が管理する SSL サーバの証明書においては、法人に関する情報及びサーバの FQDN 等が記載される。個人が管理する SSL サーバの証明書においては、個人に関する情報及びサーバの FQDN 等が記載される。
5	証明書の価格	1 年あたりの価格は数万～十数万。
6	その他の観点	-

6.1.2. 商用サービスによる SSL サーバ向けパブリック認証局の利用可能性

法人向けに発行されているパブリックの SSL サーバ証明書に関しては、多くの認証事業者も一定水準のセキュリティを確保していると想定される。このため、法人が所有するサーバまたはシステムの証明書として総合セキュリティ基盤において利用できる可能性は高いと想定される。よって、本報告書に定める基準等を課した上で、認定機関が流通業界共通認証局として認定を付与することに関しては問題がないと考えられる。

なお、利用者が流通業界共通認証局としての認定を取得していない認証事業者の SSL サーバ証明書を利用したとしても、パブリックサービスであるために多くの局面で利用可能であると考えられる。ただし、そのような利用についてはあくまでも利用者と依拠当事者の判断に基づいて行われるべきものである。

なお、個人事業主向けに発行されているパブリックの SSL サーバ証明書に関しては、一部において、個人事業者の書面等による認証が行われていない存在する。そのような証明書については総合セキュリティ基盤の利用はふさわしくないと想定される。また、個人事業主の書面等による認証が行われている証明書については、個人が所有するサーバまたは

システムの証明書として総合セキュリティ基盤において利用できる可能性は高いと想定される。このため、所定の手続き及び基準を課した上で、当該証明書を発行している認証局を、認定機関が流通業界共通認証局として認定を付与することに関しては問題がないと考えられる。

なお、法人向け証明書と同様に、個人事業主が流通業界共通認証局としての認定を取得していない認証事業者の SSL サーバ証明書を利用したとしても、パブリックサービスであるために多くの局面で利用可能であると考えられる。ただし、そのような利用についてはあくまでも利用者と依拠当事者の判断に基づいて行われるべきものである。

6.2. 商用サービスによる法人向けパブリック認証局

6.2.1. 商用サービスによる法人向けパブリック認証局の特徴

商用サービスによる法人向けパブリック認証局の特徴を 表 28 にまとめる。

表 29 商用サービスによる法人向けパブリック認証局の特徴

No.	観点	概要
1	認証局の運営主体	商用サービスを提供する各認証事業者。
2	証明書の発行対象	法人。
3	証明書の利用用途	S/MIME 等における電子署名・暗号化が主な用途（主に表 15 のNo.1 に相当する）。
4	証明書の特徴	法人の名称等が記載される。
5	証明書の価格	1 年あたりの価格は数万～十数万。
6	その他の観点	-

6.2.2. 商用サービスによる法人向けパブリック認証局の利用可能性

法人向け証明書に関しては、多くの認証事業者も一定水準のセキュリティを確保していると想定される。このため、法人の証明書として総合セキュリティ基盤において利用できる可能性は高いと想定される。よって、本報告書に定める基準等を課した上で、認定機関が流通業界共通認証局として認定を付与することに関しては問題がないと考えられる。

なお、利用者が流通業界共通認証局としての認定を取得していない認証事業者の法人向け証明書を利用したとしても、パブリックサービスであるために多くの局面で利用可能であると考えられる。ただし、そのような利用についてはあくまでも利用者と依拠当事者の判断に基づいて行われるべきものである。

6.3. 商用サービスによる個人向け向けパブリック認証局

6.3.1. 商用サービスによる個人向けパブリック認証局の特徴

商用サービスによる個人向けパブリック認証局の特徴を 表 30 にまとめる。

表 30　商用サービスによる個人向けパブリック認証局の特徴

No.	観点	概要
1	認証局の運営主体	商用サービスを提供する各認証事業者。
2	証明書の発行対象	組織内個人を対象としている認証事業者が多い。
3	証明書の利用用途	S/MIME等における電子署名及び暗号化が主な用途。(主に 表 15 のNo.2 またはNo.4 に相当する)。
4	証明書の特徴	個人の名称及び所属組織等が記載されている。
5	証明書の価格	1 年当たり数千～数万円。
6	その他の観点	-

6.3.2. 商用サービスによる個人向けパブリック認証局の利用可能性

個人向けパブリック証明書に関しては、多くの認証事業者も一定水準のセキュリティを確保していると想定される。このため、法人の従業者の証明書または個人事業主の証明書として総合セキュリティ基盤において利用できる可能性は高いと想定される。よって、本報告書に定める基準等を課した上で、認定機関が流通業界共通認証局として認定を付与することに関しては問題がないと考えられる。

なお、利用者が流通業界共通認証局としての認定を取得していない認証事業者の個人向け証明書を利用したとしても、パブリックサービスであるために多くの局面で利用可能であると考えられる。ただし、そのような利用についてはあくまでも利用者と依拠当事者の判断に基づいて行われるべきものである。

6.4.　流通業界における既存認証局

6.4.1. 流通業界における既存認証局の特徴

流通業界においてに既に利用されている既存認証局の特徴を 表 31 にまとめる。

表 31　流通業界における既存認証局の特徴

No.	観点	概要
1	認証局の運営主体	大規模小売、大規模メーカー、商社等が独自に構築を行っている。
2	証明書の発行対象	認証局の目的によるが、多くの場合、認証局の運営主体の取引先や子会社等である。
3	証明書の利用用途	認証局の目的によるが、多く場合、従来専用線で行っていた通信をインターネットを介して行うために利用されている。

No.	観点	概要
4	証明書の特徴	認証局の目的によるが、多くの場合、法人に関する情報が記載されていると想定される。
5	証明書の価格	認証局によって異なる。無償または、認証局が設定した価格により販売されていることが想定される。
6	その他の観点	失効情報は公開されていない可能性がある。

6.4.2. 流通業界における既存認証局の利用可能性

各認証局の運用によるので一概に既存の認証局が利用可能であるか判断することは出来ない。ただし、本報告書に定める基準等を満たす認証局であれば、利用者のコスト削減の観点により、認定機関が認定を付与し、流通業界共通認証局と認めることは問題がないと想定される。

6.5. 電子署名法による認定認証局

6.5.1. 電子署名法による認定認証局の特徴

電子署名法による認定認証局の特徴を 表 32 にまとめる。

表 32　電子署名法による認定認証局の特徴

No.	観点	概要
1	認証局の運営主体	電子署名法に基づき認定を取得した認定認証事業者
2	証明書の発行対象	個人が対象となるが、組織内個人等も認められる。
3	証明書の利用用途	各認定認証局による。用途は原則として電子署名であるが、暗号化も制限されていいない。
4	証明書の特徴	各認証局による。個人の名称の他、主に所属組織、メールアドレスが記載される。(主に表 15のNo.2またはNo.4に相当する)。
5	証明書の価格	各認証局による。おおよそ１年あたりの価格は数万程度。
6	その他の観点	-

6.5.2. 電子署名法による認定認証局の利用可能性

電子署名法による認定認証局の関しては、どの認証事業者も一定水準のセキュリティを確保していると想定される。このため、本報告書に定める基準等を課した上で、認定機関が流通業界共通認証局として認定を付与することに関しては問題がないと考えられる。ただし、認証事業者が流通業界共通認証局の認定を希望する可能性は、証明書の価格等を考慮すると低いと想定される。

6.6. 商業登記に基づく電子認証制度

6.6.1. 商業登記に基づく電子認証制度の特徴

商業登記に基づく電子認証制度の特徴を 表 33 にまとめる。

表 33 商業登記に基づく電子認証制度の特徴

No.	観点	概要
1	認証局の運営主体	法務省。利用者からの申請の処理等は法人の登記を管轄する全国の登記所が行う。
2	証明書の発行対象	法人代表者（一部制限あり）。
3	証明書の利用用途	法人代表者による電子署名の作成。 利用用途としては、行政に対する電子申請だけでなく、民間での利用も認められている。（主に 表 15 のNo.2 に相当する）。
4	証明書の特徴	商号・名称、本店・主たる事務所、代表者の資格・氏名を記載している。
5	証明書の価格	12 ヶ月の場合は 7,900 円
6	その他の観点	-

6.6.2. 商業登記に基づく電子認証制度の利用可能性

商業登記に基づく認証制度は一定水準のセキュリティを確保していると想定される。このため、本報告書に定める基準等を課した上で、認定機関が流通業界共通認証局として認定を付与することに関しては問題がないと考えられる。ただし、制度の性質上、当該認証局が認定を取得することはないと想定される。

6.7. 公的個人認証サービス

6.7.1. 公的個人認証サービスの特徴

公的個人認証サービスの特徴を 表 34 にまとめる。

表 34 公的個人認証サービスの特徴

No.	観点	概要
1	認証局の運営主体	各都道府県。ただし、利用者からの申請の処理等は各市町村が行う。
2	証明書の発行対象	国民（住民基本台帳に登録されているもの）
3	証明書の利用用途	国民が行政に対する電子申請を行う際に必要となる電子署名の作成等。
4	証明書の特徴	氏名、生年月日、性別、住所が記載されている。

No.	観点	概要
5	証明書の価格	3 年の有効期間の証明書が 500 円。
6	その他の観点	失効情報の利用は、行政に対する電子申請等の利用目的以外では認められていない。

6.7.2. 公的個人認証サービスの利用可能性

行政機関への電子申請等以外の利用用途では失効情報の利用が制限されているために、総合セキュリティ基盤内において、利用することは困難である。

なお、当該サービスは国民全てが格安の価格にて電子証明書を取得することを可能にすることを目的としている。このため、流通業界共通認証局への利用者の申請の際等に利用できれば利用者のメリットになるが、上記と同様の理由により、当該用途に利用することは困難である。

6.8. その他

上記以外の日本における代表的な PKI の基盤として、政府認証基盤（GPKI:Government Public Key Infrastructure)と呼ばれるものが存在する。GPK I は府省への申請・届出などをインターネット等を経由して行えるように日本政府が構築した認証基盤である。ただし、GPKI は府省へ所属する者に対して証明書を発行する基盤である。このため、GPKI を総合セキュリティ基盤において利用することは困難である。

7. 総合セキュリティ基盤において今後予想される課題

本章では総合セキュリティ基盤において今後予想される課題について検討行う。

7.1. 今後において想定される総合セキュリティ基盤に関わる環境の変化

先の述べたように、総合セキュリティ基盤において、認定機関による認証局の認定が行われてから当面の間は流通業界共通認証局として認定を希望する事業者は少ないと考えられる。しかし、EDI の分野に関して中小企業の参画が非常に進んだ場合などは、流通業界共通認証局の証明書の需要が大幅に増えることが想定される。そのような場合、証明書の需要増大に触発され、新規に流通業界共通認証局として認定を取得する認証事業者が大幅に増えることが起こりえないとは言えない。

そのような状況に陥った場合は、依拠当事者の負荷が非常に高くなるので何らかの対応策を適用する必要があると考えられる。

7.2. 環境変化に対する対応策

考えられる対応策としては、総合セキュリティ基盤において採用する信頼モデル、5 章で検討において次善の策であったスーパールート方式に移行することである。スーパールート方式は、マルチトラスト方式とは異なり、流通業界共通認証局の増加等によっても依拠当事者側の負荷は特に高くはならないという性質を持つ。このため、上記のような環境変化が起こった場合は最善の信頼モデルあると考えられる。ただし、通常の場合では既に運用が行われている認証局の上位に新規で認証局が構築されることは行われないので、スーパールート方式への移行にはかなりの技術検証等が必要と想定される。

以下に、マルチトラスト方式からスーパールート方式に移行する際に必要と考えられる作業の概略を示す。

(1) スーパールート認証局を運営する機関の選定
(2) スーパールート認証局が採用する技術仕様の決定
(3) スーパールート認証局の CPS の作成
(4) 「流通業界共通認証局　証明書ポリシー」の改訂
(5) スーパールート認証局の構築
(6) スーパールート認証局の機能検証・運用試験
(7) スーパールート認証局を利用した流通業界共通認証局間の相互接続性の検証
(8) 移行時期等に関する関係者間の調整
(9) 依拠当事者へのスーパールート認証局証明書の適用支援　等