別紙２

プラットフォームサービスに関する研究会

最終報告書

2020 年２月

目次

はじめに

本研究会は、IoT（Internet of Things:モノのインターネット)、ビッグデータ、AI（Artificial Intelligence：人工知能）などの新たな技術の普及に伴い、情報通信が我が国の経済・社会活動、国民生活の基盤として重要な役割を果たすようになりつつある中で、これまでのネットワーク構造やサービスを前提とした電気通信分野における競争ルールや基盤整備、消費者保護の在り方についての見直しが急務になっていることを踏まえて、2018 年８月に情報通信審議会に諮問した「電気通信分野における競争ルール等の包括的検証」の一環として、同年 10 月に立ち上げられたものである。

近年、情報通信技術（ICT）の進展が、従来の産業・ビジネスのバリューチェーンの各要素の分離（モジュール化)、ひいては市場のレイヤ構造化をもたらし、これにより、多様なサービスを提供するサプライヤー及びそれらのサービスを享受するユーザの双方が利用する基盤としての機能を有するプラットフォームレイヤがビジネスの拡大に重要な役割を果たすようになり、同機能を提供する事業者（以下「プラットフォーム事業者」という。）が市場プレゼンスを増大させるようになっている。

プラットフォームサービスは今日、利用者に多くの便益をもたらしており、また、イノベーションの基盤としての役割を担うようになっている一方で、その普及・拡大による多様な環境変化に伴い、様々な課題や懸念も生じつつある。

本研究会では、2019 年４月に、それまでの議論を踏まえ、プラットフォームサービスの拡大に伴う政策対応上の主要論点と基本的方向性に係る提言を中間報告書として公表したところである。また、同中間報告書において、引き続き研究会において、政策対応上解決すべき課題を洗い出し、具体的な整理について最終報告書として取りまとめることが適当としたところである。

同中間報告書の公表以降、利用者情報の適切な取扱いの確保の在り方及びフェイクニュースや偽情報への対応の在り方については、本研究会において、また、トラストサービスの在り方については、同年１月に本研究会の下に設置したトラストサービス検討ワーキンググループにおいて、それぞれ有識者、国内外のプラットフォーム事業者その他の関係者から累次にわたるヒアリングを実施し、主要課題の検討及び論点の整理のための議論を重ねてきたところである。

本最終報告書は、これまでの検討結果を踏まえ、それぞれのテーマについて、具体的な方策の在り方や今後の検討の具体的な方向性を示すものである。

第１章　利用者情報の適切な取扱いの確保について

利用者情報の適切な取扱いの確保に係る方策の在り方については、中間報告書において、政策対応上の主要論点と基本的方向性が示されるとともに、今後の検討の進め方として、次の事項を中心に、政策対応上解決すべき課題を洗い出し、具体的な整理について最終報告書として取りまとめることが適当であるとされたところである。

「①　利用者情報の適切な取扱いの確保に係る政策対応に関し、国外プラットフォーム事業者が我が国の利用者を対象として通信サービスを提供する場合における、電気通信事業法に定める通信の秘密の保護規定の適用、及び、その履行確保に係る共同規制的なアプローチを含めた適切な方策の実現のための法整備等に向けた整理

②　電気通信サービス・機能とプラットフォームサービス・機能の一体化や連携・融合の進展を踏まえ、通信の秘密・プライバシーの保護の観点からの規律（ガイドライン等）の適用範囲・対象の見直し・明確化に向けた整理」

本研究会では、中間報告書の取りまとめ以降、情報通信審議会電気通信事業政策部会の下に設置された「電気通信事業分野における競争ルール等の包括的検証に関する特別委員会グローバル課題検討ワーキンググループ」との合同によるヒアリングも実施した上で、主要課題の検討及び論点の整理のための議論を重ねてきたところであり、これらの議論を踏まえて、以下、各論点について、整理に当たっての基本的視点及び具体的な方策の在り方、又は、今後の検討の具体的な方向性を示したものである。

第１節　国外事業者に対する通信の秘密の保護規定の適用及び法執行における履行確保の方策の在り方

１．整理に当たっての基本的視点

国外に拠点を有するプラットフォーム事業者がインターネットを介し国境を越えてビジネスを拡大し、今後とも多様なサービスの展開が見込まれる中、我が国の利用者が安心してこれらのサービスを利用できるようにするためには、我が国の利用者を対象とするサービスであればサービスの提供主体が国内事業者であるか国外事業者であるかにかかわらず通信の秘密の保護規定について等しく適用することが必要と考えられる。

また、国外事業者に通信の秘密に係る規律を及ぼす場合、我が国の利用者の保護が十分に図られるようにするためには、これら事業者による当該規律に従った適切な取扱いの確保が図られることが重要である。したがって、その履行を確保するための担保措置を設けることが必要と考えられる。具体的には、国内における電気通信サービス及び電気通信事業者に対する規律とのイコールフッティングの確保も念頭において、現行の電気通信事業法における国内事業者に対する担保措置と同様の行政規律を及ぼすことが適当と考えられる。

もっとも、電気通信事業法における通信の秘密の保護規定に係る行政規律を外国にある者に対して執行しようとする場合、当該外国の主権に抵触し得ることとなるため、法執行（執行管轄権）の観点で課題が生じること、また、国外事業者に対する刑事罰についても同様の課題があることから、検討に当たってはこれらの点に留意する必要がある。

次に、通信の秘密の保護規定及び同規定に係る行政規律の執行や運用に当たっては、個々の電気通信事業者によって提供するサービスの形態、取り扱う通信の秘密に係る情報の種類や規模、利用形態が異なることから、各事業者において、それぞれの状況に応じた適切な対応が図られるようにすることが必要である。

なお、各事業者による自律的な対応に資するための指針として、総務省では従来から「電気通信事業における個人情報保護に関するガイドライン」及び同解説を策定・公表するとともに、環境の変化に応じて、その都度、適時適切かつ柔軟に当該ガイドラインを改定してきたところである。

多様かつ急速に環境が変化する情報通信分野において、通信の秘密に係る規律の円滑な履行確保を実現するには、各電気通信事業者による通信の秘密に係る情報の適切な取扱いを確保するための具体的な取組・対応を促すとともに、その取組が十分に機能しなかった場合には行政当局が関与する（行政処分を課す）ことが適当と考えられる。

今後、こうしたアプローチを効果的に機能させ、国内事業者のみならず、国外事業者も含めて、各事業者において適切に通信の秘密の保護に係る取組・対応が図られるようにするとともに、事業者に対する萎縮効果を防止する観点から、行政当局がどのような場合に事業者の取組・対応が不十分であると判断す

るのか（行政処分の発動の基準等）についての透明性及び予見可能性を高めることも重要と考えられる。

また、各電気通信事業者と行政当局との間の対話・意思疎通の充実も、透明性及び予見可能性の向上のために有効と考えられる。

２．具体的な方策の在り方

（１）電気通信事業法に定める通信の秘密の保護に係る規律を国外事業者に及ぼすための措置

今日国外のプラットフォーム事業者のプレゼンスが増大し、多くの利用者がこれらの事業者が提供するプラットフォームサービスを利用している状況や国外のプラットフォーム事業者による利用者情報の大量流出事案が相次いでいる状況に鑑みると、国外のプラットフォーム事業者による利用者情報の適切な取扱いの確保がなされなければ、利用者が安心してサービスを利用することができなくなり、ひいてはプラットフォームサービスに対する利用者の信頼の確保が図られず、プラットフォームを通じた多様なサービスの普及による電気通信の健全な発展と国民の利便の確保に支障が生じ得ると考えられる。

したがって、我が国の利用者を対象にサービスを提供する場合には、提供主体が国内か国外かにかかわらず等しく通信の秘密の保護に係る規律を及ぼすことにより、我が国の利用者の利用者情報の適切な取扱いが確保されるようにすることが適当である。また、国内外の事業者間の公平性を確保し、イコールフッティングを図る観点からも、国内事業者か国外事業者かにかかわらず、通信の秘密の保護に係る規律が等しく及ぶようにすることが適当である。

具体的には、国外事業者が、我が国の利用者を対象としてウェブメールやインスタント・メッセンジャーなど電気通信役務に相当する役務を提供する場合、電気通信事業法に定める通信の秘密の保護に係る規律が及ぶよう所要の措置を講ずることが適当である。

（２）国外事業者に対する通信の秘密の保護に係る行政処分

上記（１）のとおり、国外事業者に通信の秘密の保護に係る行政規律が及ぶよう所要の措置を講じた場合、その履行を確保するための担保措置として、国内事業者に対する規律と同様に、これら事業者に対する通信の秘密の保護に係る行政処分の執行を確保することが必要である。

具体的には、国外事業者の業務の方法に関し通信の秘密の確保に支障があると認めるときには、総務大臣はこれら事業者に対する行政処分（業務改善命令）を発することができる（第 29 条第１項第１号参照）ようにすることが適当である。

（３）国内代表者等の指定等

上記（２）のとおり、電気通信事業法における通信の秘密の保護規定に係る業務改善命令を外国にある者に対して発しようとする場合、当該外国の主権に抵触し得ることとなるため、法執行（執行管轄権）の観点で課題が生じ得る。

そこで、執行管轄権の課題を考慮の上、国外事業者に対する業務改善命令に係る文書の送達先を国内とすることにより当該事業者に対して通信の秘密の保護に係る業務改善命令の効果を確実に及ぼすため、国内における代表者又は代理人（以下「国内代表者等」という。）を介して、国内での当該業務改善命令を確実に執行することとするほか、法執行の実効性強化のための所要の措置を講ずることが適当である[1]。

具体的には、国外事業者による通信の秘密の漏えい等が発生した場合や通信の秘密の不適切な取扱いが疑われるような場合に、総務省においてその実態を把握し、必要に応じて、再発の防止や是正のための適切な措置を講じるよう求めるなど、上記（２）の業務改善命令を国外事業者に確実に執行する観点から、国外事業者に対して電気通信事業の参入規律（登録又は届出）を及ぼし、その際に国内代表者等を指定しなければならないこととすることが適当である。また、通信の秘密の漏えいその他総務省令で定める重大な事故が発生した場合、総務大臣に報告することとする（第 28 条参照）とともに、法の執行に必要な限度で、報告徴収等ができることとする（第 166 条参照）ことが適当である。

[1] 本研究会においては、我が国の利用者を対象としてサービスを提供する国外事業者に対する規律の在り方については、電気通信事業法に限らない課題であることにも留意する必要がある旨の指摘もあった。

（４）刑事罰に代替する措置の検討

電気通信事業法においては、例えば、通信の秘密の保護に係る業務改善命令に違反した場合の刑罰規定（第 186 条第３号）など、電気通信事業者が業務改善命令に違反した場合の刑罰規定及び両罰規定（第 190 条）を設け、行政規律の実効性の確保を刑罰面から担保している。また、電気通信事業者の取扱中に係る通信の秘密を侵した者を処罰する規定（第 179 条）及び両罰規定により、通信の秘密を保護するための規定の実効性についても刑罰面から担保しているが、国外事業者に対してこれらの刑事罰を実効的に適用することは、執行管轄権の観点等から困難があり、慎重な検討を要すると考えられる。

しかしながら、国外事業者に対する刑事罰の適用の困難性により通信の秘密の保護の担保が不十分となることは法執行の実効性の観点から適当ではない。そこで、刑事罰に代替する担保措置として、利用者利益の保護の観点も踏まえた法令違反行為に関する公表など一定の措置を講ずることが適当である。

（５）通信の秘密の保護に係る業務改善命令の発動に係る基準（執行に関する指針）の策定等

情報通信分野においては、新たな技術の進展や急速な市場構造の変化等により、今後とも通信の秘密に係る情報を含む利用者情報を活用したサービスが、電気通信事業者によって次々に提供されることが想定される。各電気通信事業者がこれらのサービスの提供に当たって取り扱うこととなる通信の秘密に係る情報については、個々の事業者によって提供するサービスの形態、取り扱う通信の秘密に係る情報の種類や規模、利用形態が異なることから、各事業者において、それぞれの状況に応じて自律的に適切な対応が図られることが必要である。

電気通信事業者による適切な対応が図られることを担保するためには、当該事業者の業務の方法に関し通信の秘密に係る情報の取扱いが不適切であるなど、自律的な対応が十分に機能せず、通信の秘密の確保に支障があると認められる場合には、行政当局が上記（２）の業務改善命令を機動的に発動することにより、利用者が安心して電気通信サービスを利用できるよ

うにすることが重要である。

しかしながら、市場環境のグローバル化や新たな技術の進展により電気通信事業者が提供するサービスの多様化や複雑化等が進みつつある中で、どのような場合に行政当局の関与を受けることになるかがわからない等の萎縮効果につながるとの懸念もあり得る。したがって、こうした萎縮効果を防止する観点から、また、通信の秘密の確保に係る行政当局の考え方を明らかにすることにより、利用者が安心して電気通信サービスを利用できるようにする観点から、業務改善命令の発動に当たっての透明性及び予見可能性を高めるための措置を講ずることが適当である。

具体的には、電気通信事業法第 29 条第 1 項第 1 号において「電気通信事業者の業務の方法に関し通信の秘密の確保に支障がある」と認められるときは、業務改善命令を発することができると規定されているところ、どのような場合に、各事業者の取組が十分機能していないとして、行政当局が業務改善命令を発動するのか等についての一定の基準や事例を法執行に係る指針として策定・公表[2]することが適当である。

なお、同指針において定める電気通信事業者による対応として不十分なケース（業務改善命令が発動され得るケース）としては、例えば、通信の秘密に係る情報を含む利用者情報の取扱い等の方針（ポリシー等）が利用者にわかりやすく示されていないなど透明性の確保が十分に図られていない場合や、通信の秘密に係る情報の管理態勢・通信の秘密に係る情報の取扱いに関する利用者からの苦情処理態勢（救済施策を含む。）が十分に整っていない場合などが該当し得ると考えられ、これらの点を含めて業務改善命令の発動に係る基準を示すことが適当である。

（６）電気通信事業者と行政当局との継続的な対話等を通じた透明性・予見可能性の向上

次の観点から、電気通信事業者と行政当局との間で対話を継続することが適当である。すなわち、各電気通信事業者にとっては、上記法執行に係る指針などを踏まえた法律の解釈や運用について理解を深められる。他方、行政当局にとっては、各電気通信事業者による通信の秘密に係る情報の取

[2] 本研究会においては、法執行に係る指針の策定・公表に当たっては、国際的な調和に留意しつつ、外国語版の策定などの対応も求められる旨の指摘があった。

扱いの実態を正確に把握するとともに、新たな技術やサービスの動向を理解することによって、より柔軟かつ機動的な法執行を実現することに資する。

また、行政当局においては、電気通信事業者との対話を通じて、市場環境の変化に伴うサービスの一層の多様化等を踏まえ、法執行に係る指針等を必要に応じ見直し、その指針を広く電気通信事業者に周知することなどを通じ、行政の透明性・予見可能性を向上させるとともに、各事業者における通信の秘密に係る情報の適切な取扱いの確保や情報管理態勢・苦情相談態勢などの一層の充実が図られるよう、各事業者に対して継続的に促していくことが望ましい。

第２節　市場環境の変化を踏まえた規律の適用範囲・対象の見直し

１．整理に当たっての基本的視点

電気通信サービスは、５Ｇの普及に伴い、今後さらにAIやIoTなどの最新技術を駆使したものに変遷・進化していくとともに、電気通信事業者とプラットフォーム事業者との協業や連携・融合が進み、市場環境も一変していくことが想定される。

こうした変化に伴い、多様な電気通信サービスを通じて取得・活用される通信の秘密に係る情報を含む利用者情報についても、例えば、より多くの種類の情報が、より頻繁に、かつ、より多くの事業者間で共有・活用されるようになるなど、その取扱いが質・量ともに深化・拡大していくことが想定される。

通信の秘密に係る情報の取扱いに当たっては、法令行為や正当業務行為、緊急避難等に該当する場合を除いて、利用者の同意を取得することが必要とされており、また、当該同意は、従来原則として利用者の「個別具体的かつ明確な同意」でなければならないとされているところ、ネット環境の進化に伴って多様なサービスが展開される中、累次の同意取得が繰り返され、かえって利用者の理解が不十分となる、いわゆる「同意疲れ」が課題となりつつある。

また、スマートフォンやタブレットなどの通信端末の位置情報や、ウェブ上の行動履歴、特に、利用者の端末から発せられ、または、利用者の端末に蓄積される端末IDやクッキーなどの端末を識別する情報等（以下「端末情報」とい

う。）については、プロファイリングや行動ターゲティングなど多様なサービスやビジネスにおいて活用されることが考えられる一方、通信の秘密やプライバシー保護との関係でその取扱いの在り方が課題となりつつある。

２．今後の検討の具体的な方向性

（１）いわゆる「同意疲れ」への対応

いわゆる「同意疲れ」は、より多くの利用者情報が利用者から取得されるようになり、また、その活用の方法が複雑かつ多岐にわたるようになり、さらに、その結果同意取得時の説明も複雑で分かりにくくなるといった事情が相まって生じているものと考えられることから、こうした事情を踏まえて、有効な同意の取得やその際の説明の在り方について、さらに検討を深めることが必要である。

（２）端末情報の取扱い

インターネットを取り巻く環境が進化すればするほど、今後、通信の秘密に係る情報に該当するか否かにかかわらず、端末情報をはじめ多様な利用者情報の取得・活用ニーズが一段と高まっていくことが想定される中、利用者の利便性と通信の秘密やプライバシー保護とのバランスを適切に確保することが一層重要になっていくものと考えられる。

このため、端末情報の適切な取扱いを確保することにより、利用者が自らの端末を用いて安心して電気通信サービスやプラットフォームサービスを利用できるようにすることは、利用者の保護及びこれらサービスの利活用の促進の観点から重要な課題であり、端末情報の適切な取扱いの確保のための具体的な規律の在り方については、欧州の e プライバシー規則（案）の議論等も参考にしつつ、今後引き続き検討を深めることが必要である。

その際、必要に応じ、これまで総務省において策定してきた指針等（電気通信事業における個人情報保護に関するガイドライン、位置情報プライバシーレポート、スマートフォン・プライバシー・イニシアティブ等）の改廃・統合を含めて対応することが適当であるほか、今後のさらなる AI の活用や IoT 化の進展に伴い、電気通信分野における市場構造やデータ流通環境が大きく変化することが想定される中で、通信の秘密に係る基本理念を維持しつつ、新しい時代

に相応しい通信の秘密・プライバシーの保護に係る規律の在り方を念頭に置いて、具体的な検討を進めていくことが適当である。

第２章　フェイクニュースや偽情報への対応

インターネット上のフェイクニュースや偽情報（以下「偽情報」という[3]。）への対応については、中間報告書において、以下の記述の点に関して今後さらに政策対応上解決すべき課題を洗い出し、具体的な整理について最終報告書として取りまとめることが適当であるとされたところである。

「③　フェイクニュースや偽情報に係る政策対応に関し、民間部門における自主的な取組を基本として、ファクトチェックの仕組みやプラットフォーム事業者とファクトチェック機関との連携などの自浄メカニズム等について、プラットフォーム事業者の役割の在り方にも留意して検討を深めるなど、具体的な施策の方向性の検討に向けた整理」

本研究会では、中間報告書の取りまとめ以降、海外の取組状況について幅広く把握するとともに、ファクトチェック推進団体、有識者、ネットメディア、国内外のプラットフォーム事業者から累次にわたってヒアリングを実施した上で、主要課題の検討及び論点の整理のための議論を重ねてきたところであり、以下、これらの議論を踏まえて、政府及び関係者が実施すべき取組・対応の方向性を示すものである。

第１節　フェイクニュースや偽情報への対策の必要性及び目的

近年、欧米諸国を中心に、インターネット上での偽情報の流通の問題が顕在化しており、これらの国々では、偽情報への対策が進みつつある。

偽情報に関しては、インターネット上に限った問題ではなく、真偽が不明で信頼性の低い情報（例えばデマや流言飛語など）が人々の間の口コミ等で拡散される事例はこれまでも存在したが、ソーシャルネットワーキングサービス（以下「SNS」という。）等のプラットフォームサービスには次のような固有の特性があり、そのことがインターネット上において偽情報を顕在化させる一因になっていると考え

[3] 後述するとおり、「フェイクニュース」について国際的に定まった定義はなく、対象範囲についても統一的な考え方はないことに留意が必要である。本報告書の検討対象としては、インターネット上に流通する情報に限定するものの、「フェイクニュース」の多義的な側面を捉えて検討を深める観点から、政治・選挙に係る情報に限らず、災害、健康・医療情報に係る情報なども広く含めて対象とするほか、「偽情報（disinformation）」（＝何らかの意図性を持った虚偽の情報）及び「誤情報（misinformation）」（＝単なる誤った情報）を含め、また、ニュースの形式を持たない情報や、部分的に不正確、根拠が不明、ミスリードな情報も含めるなど、対象範囲を限定せずに検討するものとし、諸外国政府の政策文書等では「fake news（フェイクニュース）」ではなく「disinformation（偽情報）」が用いられることが多い点も踏まえ、これらの検討対象を単に「偽情報」と表記するものとする。

られる。

① SNS では一般の利用者でも容易に情報発信（書込み）や拡散が可能であり、偽情報も容易に拡散されやすいこと

② 多くの利用者がプラットフォームサービスを通じて情報を収集･閲覧していることから、情報が広範囲に、かつ、迅速に伝播されるなど、影響力が大きいこと[4]

③ 偽情報は、SNS 上において正しい情報よりもより早く、より広く拡散する特性があること[5]や、SNS 上の「ボットアカウント[6]」が拡散を深刻化させていること[7]

④ 自分と似た興味・関心・意見を持つ利用者が集まるコミュニティが自然と形成され、自分と似た意見ばかりに触れてしまうようになる（＝「エコーチェンバー」）、パーソナライズされた自分の好み以外の情報が自動的にはじかれてしまう（＝「フィルターバブル」）などの技術的な特性があること[8]

⑤ 各利用者の利用者情報の集約・分析によって、個々の利用者の興味や関心に応じた情報配信（例：ターゲティング広告）が可能であるなど、効果的・効率的な利用者へのアプローチが可能であること

プラットフォーム上において多くの不確かな情報や悪意のある情報が容易に流通・拡散することは、利用者が多様な情報をもとに物事を正確に理解して適切な判断を下すことを困難にし、結果として、利用者が安心・信頼してプラットフォームサービスを利用することができなくなる、また、利用者の知る権利が阻害されるのみならず、利用者に直接的な損害を与え得るなど、利用者にとって様々な不利益が生じるおそれがある。

---

[4] 2018 年度における主なソーシャルメディア系サービス・アプリ等の利用率は、LINE：82.3%、Twitter：37.3%、Facebook：32.8%、Instagram：35.5%、TikTok：10.3%、YouTube：75.7%。
また、2018 年度におけるテキスト系ニュースサービスの利用率は、紙の新聞：50.7%、新聞社の有料ニュースサイト：2.5%、新聞社の無料ニュースサイト：12.4%、ポータルサイトによるニュース配信：66.3%、ソーシャルメディアによるニュース配信：38.7%、キュレーションサービス：16.0%。
（総務省情報通信政策研究所　「平成 30 年度　情報通信メディアの利用時間と情報行動に関する調査」2019 年９月）

[5] Vosoughi 助教授らが Twitter 上の情報を利用して行った研究によると、「事実は 1000 人以上にツイートされるのは稀だが、誤情報はもっと多くの人にツイートされた」「最初の投稿がリツイートされるまでの速さは誤情報のほうが 20 倍速く、1500 人に届くまでにかかる時間も事実より６倍も速い」などの調査結果が示された。
（science 2018 年３月）
https://science.sciencemag.org/content/359/6380/1146

[6] 人間ではなく機械により自動的に投稿を行うアカウント。

[7] Stella らの研究によると、2017 年のカタルーニャ地方独立の住民選挙に関して、Twitter 上でボットアカウントからハブユーザ（影響力の高いアカウント、インフルエンサー）を狙って情報を拡散している例が見られた。
（PNAS 2018 年 12 月）
https://www.pnas.org/content/115/49/12435

[8] 読売新聞社による全国世論調査によると、インターネットなどを利用するとき、「自分と近い意見や考え方」に接する方が多い人：59%、「自分と異なる意見や考え方」に接する方が多い人：22%（読売新聞　2019 年 10 月 14 日朝刊２面）

このほか、選挙の候補者等に関する不正確な情報が流布されることなどによって有権者の理性的な判断が妨げられることで投票結果が歪められたり、政治的分断が深まるおそれや、外国政府が誤った情報を流布することで国家安全保障が揺るがされたりするおそれなども考えられる。

後述のとおり、米国や欧州においては実際に偽情報が選挙時において大きな社会問題になっていることから、我が国においても近い将来同様の問題が生じ得ることを念頭に、今後の対策を検討すべきであると考えられる。この点、特に SNS を始めとするプラットフォームサービスは、経済活動や国民生活などの社会基盤になりつつあり、情報流通の基盤にもなっていることから、また、上記のプラットフォームサービスの特性が偽情報の生成・拡散を容易にし、偽情報を顕在化させる一因となっていると考えられることから、特にこうしたプラットフォーム上の偽情報への適切な対応が求められる。

なお、検討に当たっては、先行する欧米等の事例を参考にするほか、我が国においてどのような偽情報の流通が問題になり得るのか、我が国における現状を踏まえた上で、とるべき取組・対応について検討することが適当である[9]。

上記の点を踏まえ、次節以降では、まず諸外国及び我が国における偽情報の現状等を確認し、次に諸外国において先行して行われている対応の状況を参照し、さらに我が国におけるこれまでの偽情報への対応の状況を踏まえて、今後我が国においてとるべき取組・対応及びその方向性を示すこととする。

第２節　フェイクニュースや偽情報の現状等

１.「フェイクニュース」の定義及び分類

我が国では一般的に「フェイクニュース」という言葉が報道等で利用されることが多いが、「フェイクニュース」について国際的に定まった定義はなく、また、諸外国の政府の政策文書等では「disinformation（偽情報）」や「misinformation（誤情報）」という表現が用いられることが多い。

例えば、後述の欧州委員会の政策文書（Tackling online disinformation：

[9] 偽情報の類型・性質は多様であり、例えば、安全保障に関わる情報への対応と単なる誤情報への対応では、求められる対策の在り方も異なり得る。この点、本研究会においては、国家安全保障の確保や選挙の安全ではなく、インターネット空間の信頼性を高め、我が国の利用者が安心・信頼してプラットフォームサービスや電気通信サービスを利用できるようにすることを主な目的として検討を行うものであることに留意が必要である。

a European Approach）では、「disinformation」について「検証可能な、虚偽又は誤解を招く情報で、経済的利益を得るため又は公共を欺くことを目的として生成、表示、拡散され、それによって公共への損害が生じ得るもの」と定義している[10]。

また、「フェイクニュース」や偽情報を流通させる目的や当該情報に含まれる誤りの程度（分量・誤りの部分など）によって利用者に与える影響も異なり得るところであり、海外の一部においてはこうした点についての分類を試みる取組があるものの（次頁の取組事例を参照。）、国際的に確立した分類の考え方があるわけではない[11]。

このほか、例えば、

・インターネット上の情報に限られるのか、あるいは、それ以外のメディアにおける情報も含む概念であるのか
・ニュースの形式に限定されるのか、あるいは、それ以外の単なる情報も含むのか
・政治的・経済的・個人的な利益を得ることを目的とするなど、何らかの意図をもった情報に限るのか、あるいは、単なる誤った情報を含むのか
・明確に虚偽である情報に限られるのか、あるいは、部分的に不正確、根拠が不明、ミスリードであるといったケースも該当するのか

といった点についてはそれぞれの場合でまちまちに用いられているのが現状であるなど、「フェイクニュース」の対象範囲についても、統一的な考え方はないことに留意が必要である。

[10] このほか、例えば、英国議会下院デジタル・文化・メディア・スポーツ（DCMS）特別委員会の報告書では、「disinformation」について「害を及ぼす目的又は政治的、個人的若しくは金銭的な利益のために、人々を欺き誤解を生じさせることを意図した虚偽の情報及び/又は操作された情報を意図的に作成・共有すること」と定義しており、「misinformation」については「意図せずに誤った情報を共有すること」と定義している。また、英英辞典の「Cambridge Dictionary」では、「fake news」について「インターネットやそのほかのメディア上で拡散される、一見ニュースのようなストーリー。政治的な影響を与えることを目的とするか、あるいはジョークとして作られる。」と説明されており、「disinformation」については「人々を欺く目的で拡散される誤った情報。」と定義されている。

[11] フェイクニュースとして情報を流通させる目的や情報の誤りの質的・量的な違いを分類しようとする取組も、一部の政府機関や非営利団体において行われている。例えば、アメリカの非営利団体「First Draft」では７つに、英国議会下院 DCMS 特別委員会の中間報告書では６つに、欧州の非営利団体 EAVI の授業用教材では 10 に、フェイクニュースを分類しているなどの取組例がある。

《参考１》「フェイクニュース」の分類の取組事例：「フェイクニュースという言葉を使わず考えてみよう ― 10 種類の情報区分」(Beyond 'fake news' - 10 types of misleading news)[12]

そこで、本報告書の検討対象としては、インターネット上に流通する情報に限定するものの、「フェイクニュース」の多義的な側面を捉えて検討を深める観点から、政治・選挙に係る情報に限らず、災害、健康・医療情報に係る情報なども広く含めて対象とするほか、「偽情報（disinformation）」（＝何らかの意図性を持った虚偽の情報）及び「誤情報（misinformation）」（＝単なる誤った情報）を含め、また、ニュースの形式を取らない情報や部分的に不正確・根拠が不明・ミスリードな情報も含めるなど、対象範囲を限定せずに検討するものとする。

[12] 日本ジャーナリスト教育センター（JCEJ）が EAVI の許可を得て邦訳・公開している日本語版。
http://jcej.hatenablog.com/entry/2019/03/27/104845
http://jcej.info/lib/BeyondFakeNewsPosterJP_v1.pdf

２．フェイクニュースや偽情報の具体的事例

諸外国においては、以下の主な具体的事例のとおり、偽情報の流通が問題になったことがある。

・米国では、2016 年 12 月に実施された大統領選挙の際、民主党クリントン候補（当時）の評価を貶める目的で、共和党トランプ候補（当時）を支持する陣営や外国から偽情報が発信・拡散され、大統領選挙の結果に影響があったと言われている。具体例には、「ローマ教皇がドナルド・トランプ支持を表明する声明がバチカン（ローマ教皇庁）から発表された」旨の情報（後日、ローマ教皇が同記事情報を否定）が SNS 上で拡散されるなどの事例がある[13]。

・英国では、2016 年６月に実施された EU からの離脱を問う国民投票に対して、偽情報が影響を与えたといわれている[14]。

・フランスでは、2017 年５月に実施された大統領選挙において、マクロン候補（当時）が租税回避地にペーパーカンパニーや銀行口座を保有している旨の偽情報の拡散が問題となった。

・ドイツでは、2016 年に連続発生した移民によるテロ事件に関して、事件と無関係の難民とメルケル首相との写真が利用され、同首相がテロリストと関係があったかのような偽情報の拡散が問題となった。

一方、我が国においては、米国や欧州ほど大きな問題には至っていない、というのが関係者間の認識である。特に、米国や欧州では選挙時における他国からの偽情報が大きな脅威になっているところ、我が国では現時点ではそのような大きな問題は生じていない。

しかしながら、過去に我が国でも偽情報が問題となった事例は存在する。代表的な事例としては、①災害時[15]、②選挙時[16]、③キュレーションサイト等の問題[17]、という３つの大きな分類が挙げられるが、米国や欧州とは問題となる場面・情報の性質などが異なる点が特徴的である。

---

[13] https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook

[14] https://www.bbc.com/japanese/features-and-analysis-36628343

[15] 例えば、2016 年４月に発生した熊本地震の直後に「動物園からライオンが放たれた」という偽情報が SNS で拡散され、発信者が偽計業務妨害で逮捕された事例などがある。

[16] 例えば、2018 年の沖縄県知事選の際には、「沖縄県知事選挙 2018.com」というサイトが登場し、立候補者の一人である玉城氏（現知事）を批判する真偽・出所不明の情報や動画が掲載された事例などがある。

[17] 例えば、2016 年、株式会社 DeNA が運営するキュレーションサイト、「WELQ」において、専門家による監修がなされていない信頼性の低い医療情報に関する記事が公開されていた事例などがある。

第３節　諸外国におけるフェイクニュースや偽情報への対応状況

１．米国

米国では、合衆国憲法修正第１条により表現の自由を手厚く保障してきた伝統もあり、偽情報への法的規制には基本的に慎重な姿勢がとられており、プラットフォーム事業者による自主的な取組が進められている。なお、インターネット上に流通する情報に関するプラットフォーム事業者の責任については、通信品位法第 230 条の規定があり、同条によって、プラットフォーム事業者は第三者により発信された情報を編集・削除した場合に免責されるが、同規定が自主規制のインセンティブとして機能してきたとも言われている[18]。

米国における偽情報への対応としては、2016 年の大統領選挙時における問題を契機として、連邦議会において、以下のとおり、プラットフォーム事業者の取組に対する公聴会が行われてきた。

・2017 年 10～11 月、上院司法委員会犯罪・テロに関する小委員会及び上下院情報常任特別委員会において、ロシアによる米国大統領選挙介入について公聴会が開催され、Facebook・Google・Twitter が証言を行い、３社から、外国勢力・テロリスト・犯罪者による SNS の悪用を防ぐための方針を新たに制定している等の説明がなされた。
・2018 年４月、上院商業委員会・同司法委員会の合同公聴会及び下院エネルギー商業委員会において、偽情報や利用者データの不正利用などの問題に関して公聴会が開催され、Facebook（ザッカーバーグ CEO）が証言を行った。同社は、データ利用についての透明性義務、利用者によるデータの管理といった面での規制にはオープンな姿勢を示す一方、行き過ぎた規制には懸念を示した。
・2018 年９月、上院情報委員会において、米国選挙に対する外国からの干渉に関する公聴会が開催され、Twitter（ドーシーCEO）及び Facebook（サンドバーグ COO）が証人として出席し、外国勢力の選挙干渉工作や偽情報の流布に対する対策を説明した。

これらの公聴会等の動きも踏まえて、第４節で後述するとおり、米国では基

[18] なお、2019 年６月に通信品位法第 230 条の改正案（Ending Support for Internet Censorship Act：一定規模以上のプラットフォーム事業者が免責を受けるためには、他者の発信した情報を政治的に偏向した仕方で調整していないことについて政府機関（FTC）の認証を受けることを求める内容）が提出され、同年 10 月には同条の改正に関して下院通信小委員会と同消費者保護小委員会の合同公聴会が開かれるなどの議論が行われているが、表現の自由が抑制されるおそれがあるなどとして、利用者団体や業界団体から批判が寄せられている。

本的にはプラットフォーム事業者による自主的な対応が進められている。

また、2019 年５月、連邦下院議会議長（ペローシ氏）の演説を合成・改変したディープフェイク動画[19]が SNS で拡散し、プラットフォーム事業者により削除等の対応方針が分かれるという事態が生じた[20]。これらの問題を受けて、ディープフェイク動画がもたらす危険についての理解を深めることを目的とし、ディープフェイク技術の使用状況について年次報告を作成することを政府に義務づける法案「Deepfake Report Act」が同年 10 月に上院で可決され、現在下院で審議中となっている[21]。

２．欧州連合（EU）

欧州委員会では、ロシアによる偽情報のキャンペーンを契機として、偽情報に関する検討が行われてきた。これまでの基本的な方向性としては、民間主体との対話を重視し、行動規範の策定によりプラットフォーム事業者等の関係者に自主的な対応を求める方向で様々な取組が進められてきている。

まず、2018 年４月に、欧州委員会は、政策への助言を行うために設置されたハイレベル専門家グループから 2018 年３月に同委員会へ提出された報告書を受けて、対処すべき問題と政策方針の提示を行う政策文書（The Communication "Tackling online disinformation: a European approach"）を作成・公表した[22]。同政策文書では、偽情報対策へのアプローチとして、①透明性の向上、②情報の多様性促進、③情報の信頼性向上、④包括的解決策の形成、という４つの指針を掲げるとともに、具体的な対応策として、特に、プラットフォーム事業者、広告事業者、広告主等を含むステークホルダーが集まり、偽情報への対応のための「行動規範（Code of Practice on Disinformation)」を策定することを求めた。「行動規範」は、スポンサードコンテンツ（特に政治広告）の透明性を確保すること、偽アカウントを特定し閉鎖すること、ファクトチェック機関等が継続的に監視できるようにすること等を目的とすべきであるとされた。

その他の具体的な対応策としては、①より高い透明性、信頼性、説明能力を

[19] AI 技術や機械学習の技術を悪用して作り出された偽の映像
[20] https://www.nytimes.com/2019/05/24/us/politics/pelosi-doctored-video.html
[21] https://thehill.com/policy/cybersecurity/467462-senate-passes-legislation-to-combat-deepfake-videos
[22] https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach
なお、当該施策に関しては、欧州委員会の中で、通信ネットワーク・コンテンツ・技術総局（DG CONNECT)が主に担当している。

持つオンライン・エコシステム、②安全かつ強靭な選挙プロセス、③教育とメディアリテラシーの育成、④民主的社会の重要な要素としてのクオリティジャーナリズムへの支援、⑤戦略的なコミュニケーションを通じた、内外のフェイクニュースの脅威への対策が掲げられた。

《参考２》欧州委員会の政策文書において示された具体的な対応策[23]

実施項目		主な取組項目
1. より高い透明性、信頼性、説明能力を持つオンライン・エコシステム	1.1. オンラインプラットフォームによる、迅速かつ効果的な、偽情報からのユーザーの保護	利害関係者（オンラインプラットフォーム、広告主、広告事業者等）との協力の枠組の策定、行動規範の策定とその実施状況・効果の測定、EU規則の適用可能性の検討　等
	1.2. 偽情報に対するファクトチェック、集合知、モニタリング能力の強化	欧州におけるファクトチェッカーの独立ネットワークの形成支援、ファクトチェッカー及び学術研究者を支援するオンラインプラットフォーム（データの収集・分析ツール等）の提供　等
	1.3. オンラインの説明責任の強化	eIDAS協力ネットワークによるオンラインの認証の推進　等
	1.4. 新技術の活用	新技術利用・各種ツールの開発に対するHorizen2020プログラムの最大限の活用、追加的支援策の検討、等
2. 安全かつ強靭な選挙プロセス		民主主義に関する対話イベントの開催、サイバー攻撃及び偽情報による選挙プロセスへのリスクの管理に関する加盟国との対話、NISとの連携　等
3. 教育とメディアリテラシーの育成		ファクトチェッカーや市民団体による教材提供の支援、EU関係機関やその取組との連携、デジタル人材教育との連携　等
4. 民主的社会の重要な要素としてのクォリティジャーナリズムへの支援		クォリティジャーナリズムに対する各加盟国の援助策の情報整理・データベース化、クォリティジャーナリズム活動の募集、ジャーナリスト育成や商品・サービスのイノベーションに対する支援、技術開発やプラットフォーム整備プロジェクトへの追加的支援、メディア向けツールキットの提供　等
5. 戦略的なコミュニケーションを通じた、内外の偽情報の脅威への対策		欧州対外行動庁（EEAS）との連携、EC及びEEASのもつ知見のEUの他機関への展開、外国政府による偽情報・ハイブリッド妨害に対抗するための対応や仕組を発展させるための選択肢検討、戦略コミュニケーション能力等に関する報告　等

2018 年９月には、前述の政策文書を受けて、欧州委員会により、５分類 15 項目からなる「行動規範」が策定・公表され、同年９月から 10 月にかけて、Facebook、Google、Twitter、Mozilla の４事業者と、プラットフォーム事業者関連又は広告事業者関連の８団体が同行動規範に同意する署名を行い、行動規範を実施するためのロードマップを策定・公表した。また、2019 年５月には、Microsoft も行動規範への同意署名及びロードマップの策定・公表を行った。

[23] 第８回事務局資料より引用

《参考３》偽情報に関する行動規範（Code of Practice on Disinformation）[24]

分類	項目
広告配置の監視	1. 不正確・虚偽の広告や収益化のインセンティブを防ぐためのポリシー・プロセスを設ける
政治的広告及び論点広告	2. すべての広告は、編集されたコンテンツと明確に区別されることができなければならない
	3. 政治的広告に関する開示を可能にする
	4. 論点に関する広告を開示する方法を工夫する
サービスの完全性	5. 自動化されたbotの特定と誤用に対する明確なポリシーを策定する
	6. 自動化されたシステムの使用を認めない場合におけポリシーを策定し、公表する
消費者のエンパワー	7. 虚偽の可能性のある情報に接した際、十分な情報に基づいて決定することを支援する製品、技術等に投資する
	8. 検索、フィードなどの自動的に順位付けする配信システムにおいて、信頼すべき情報の優先順位を高める技術的手段に投資する
	9. 公共の利益に関する話題について、多様な視点を得やすくするためのツールや機能に投資する
	10. メディアリテラシーの向上に関する取組を支援するため、市民団体、政府、教育機関等とパートナーを組む
	11. 消費者が特定の広告が表示されている理由を理解することを助けるツールを、市場が取り込むことを促進する
研究コミュニティのエンパワー	12. 偽情報の追跡及びその影響の理解に関する、誠意ある独立した取組を支援する
	13. 自社プラットフォームにおける偽情報及び政治広告に関する誠意ある研究を禁止又は抑制しない
	14. 偽情報及び政治広告に関する研究を促進する
	15. 学術機関、ファクトチェック・コミュニティ、関係事業者による議論を促進するイベントを毎年開催する

2019 年５月に欧州議会選挙が予定されていたことから、欧州委員会は、同年１月から５月にかけて、Facebook、Google、Twitter の３社に対して行動規範に関する取組状況の提出を求め、それらに対する評価及びレポートの公表を毎月実施した。さらに、同年６月、欧州委員会は、欧州議会議員選挙が終了したことを受けて、３社の対策の成果及び欧州議会選挙の教訓に関するレポートを公表した。レポートでは、「３社の取組は欧州議会選挙における偽情報対応に貢献したが、偽情報が完全になくなったわけではなく、今後も取り組むべきことが多く残されている」「Facebook、Google、Twitter に関して、行動規範を通じて、虚偽情報への取組に改善が見られたとして、継続努力を期待」といった評価がなされた[25]。

以上のように、欧州では、欧州委員会の策定した行動規範を通じてプラットフォーム事業者等の自主的な取組が進められるとともに、プラットフォーム事業者以外の多様な関係者が連携し、偽情報への取組・対応が行われている。

なお、欧州における取組・対応の中では、プラットフォーム事業者の透明性の確保という観点が重視されているところ、例えば、「デジタル単一市場における著作権指令（DSM 著作権指令）」（2019 年６月発効、「オンライン仲介サービスのビジネスユーザにとっての公正性・透明性の促進に関する規則（オンライン・プラットフォーム規則）」（2019 年７月発効）等においても、プラットフォーム

[24] 第８回事務局資料より引用

[25] 欧州委員会が 2019 年 11 月に公表した声明によると、同委員会においては 2020 年初頭に「行動規範」に基づく対応状況の包括的な評価を行う予定であるとし、行動規範による自主的取組が不十分だと評価された場合には規制的措置を提案する可能性についても示唆している。

事業者の透明性確保や苦情処理、モニタリングに関する規定が盛り込まれている。

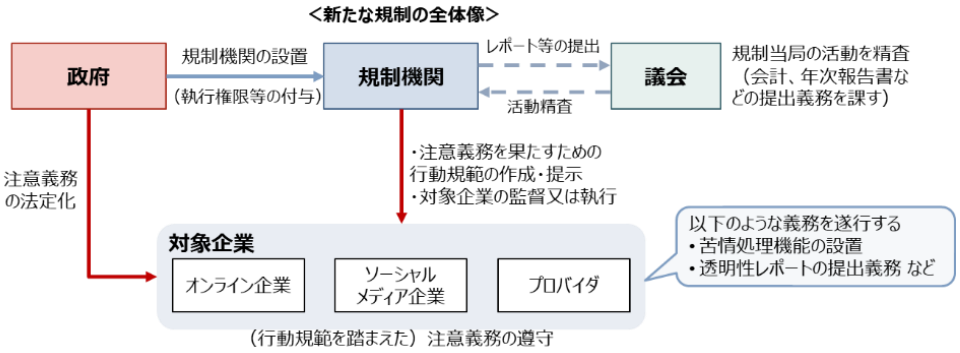
３．英国

英国では、2016 年６月の EU 離脱に関する国民投票を契機として、デジタル・文化・メディア・スポーツ省（DCMS）を中心に、偽情報への対策を含むインターネット上の安全性確保を目的とした調査や取組を行っている[26]。

2019 年４月、英国における安全なインターネット環境の確保のための将来の政府の対策を示すことを目的として、DCMS と内務省が共同で作成した「オンラインセーフティ白書（Online Harms White Paper）」案が公表された。白書案については、同年７月までのパブリックコメントを経て、今後、最終取りまとめが予定されている。

白書案では、偽情報を含む幅広い有害情報を対象とし、①法定の注意義務の創設、②独立した規制機関の設置、③行動規範の策定などにより、自主規制を超えた新しい規制の枠組みを作ることが提案されている。

《参考４》白書案で示された新たな規制の全体像[27]



４．フランス

フランスでは、2018 年 11 月に、選挙時における偽情報への対策を目的とし

[26] このほか、英国議会（超党派議員で構成される「下院デジタル・文化・メディア・スポーツ特別委員会」）における、フェイクニュースが民主主義に与える影響に関する調査報告（2019 年２月）や、ジャーナリストのケアンクロス氏による、英国における質の高いジャーナリズムの持続可能性についてのレビュー及び政策提言を取りまとめた報告（2019 年２月、通称「ケアンクロス・レビュー」）などの動きもある。

[27] 第 11 回事務局資料より引用

て、「情報操作との戦いに関する法律」[28]が議会で成立した。同法の対象となる情報（「選挙時における偽情報」）の定義は、「予定される投票の誠実性を損なうような、不正確若しくは誤解を招く主張又は非難が、オンライン公衆通信サービスを通じて、意図的に、人為的に又は自動的に、大量に伝播された場合」とされている。

同法では、選挙期間内（投票日前３ヶ月）に、上記の情報が拡散されている場合、候補者等から申立を受けた裁判官は、プラットフォーム事業者に対して送信防止措置を命じることができ、裁判官は申立から 48 時間以内に停止に関する判断を行わなければならないとされている。

また、プラットフォーム事業者は、①アルゴリズムの透明性確保、②スポンサードコンテンツであること及びその資金源・発信主体の情報公開、③偽情報を大量に拡散する偽アカウント対策、④拡散メカニズムの情報提供、⑤メディア・情報教育、などの協力義務を負い、これらの実施方法を公表することとされている。

なお、同法に対しては、成立後、上院議員の有志等が同法は違憲であるとして憲法評議会に提訴した結果、一部の規定について限定解釈付きで合憲との判断が示された[29]。このほか、「民主主義を危険にさらし、報道の検閲につながる」「実務的に、情報内容が虚偽であるか否かを裁判官が 48 時間以内に判断することは不可能」といった反対意見や批判もみられた。

５．ドイツ

ドイツでは、2017 年６月、難民の増加に伴う SNS 上のヘイトスピーチや偽情報等の増加への対策として、「ネットワーク執行法（NetzDG)」が成立、同年 10 月に施行した。同法により、ドイツ国内の登録利用者数が 200 万人以上のプラットフォーム事業者は、苦情処理に関する報告義務や、申告のあった違法コンテンツへの対応義務を負う。

また、同法では、プラットフォーム事業者は、違法コンテンツの申告のため

[28] LOI organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information（情報の操作に対する戦いに関する 2018 年 12 月 22 日の基本法）及び LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information（情報の操作に対する戦いに関する 2018 年 12 月 22 日の法律）の２つの法で構成される。

[29] オンライン・プラットフォーム上の送信防止は、「虚偽だと客観的に証明されるもの」のみに適用されうる。また、オンライン・プラットフォーム上の送信防止や放送停止は、その情報の不正確又は誤解を招く性質や投票の誠実性を毀損するリスクが明白である場合にのみ正当化される。

の窓口を設けた上で、利用者から申告があった場合は、直ちに違法性を審査し、原則として、①明らかに違法なコンテンツについては申告を受けてから 24 時間以内、②それ以外の違法コンテンツについては申告を受けてから７日以内に、当該コンテンツを削除する義務を負うとされている。このほか、適切な対応を行わなかった場合、最大 500 万ユーロの過料（法人・団体には最大 5,000 万ユーロの過料）が課せられる。

対象となる違法コンテンツは、ドイツ刑法の特定の犯罪に該当するものとされており、違憲組織のシンボル使用、国家を危険にさらす重大な暴力行為の準備、民衆扇動、人種憎悪挑発などに加え、悪評の流布、中傷といったものまで、幅広い犯罪が対象となっている。

なお、同法に対しては、①削除するのかどうかの判断が SNS 事業者にとって困難である、②削除しないことのリスクがプラットフォーム事業者にとって高い、といった理由により、プラットフォーム事業者による過剰な削除が起きることによって表現の自由が阻害されることへの懸念が議論されている。

６．マレーシア

マレーシアでは、2018 年４月、前政権（ナジブ政権）下において「フェイクニュース対策法（The Anti-Fake News Act)」が制定された。

同法に対しては、「フェイクニュース」や「悪意」の定義が曖昧なため、恣意的運用が強く懸念されていたところ、政権交代後、現政権（マハティール政権）は、同法の執行を停止するとともに、2018 年８月に廃止法案を議会へ提出し、2019 年 10 月に廃止法案が下院議会において再可決された。今後、国王の同意を得ることにより、同法は廃止される見通しとなっている。

７．シンガポール

シンガポールでは、2019 年５月に「オンラインの偽情報・情報操作防止法案（New Protection from Online Falsehoods and Manipulation Bill)」が可決、同年 10 月に施行された。

同法では、「シンガポールの安全保障、安寧な社会環境や他国との友好関係に脅威を与える偽情報」が対象とされており、政府が虚偽と判断した場合には、プラットフォーム事業者に対して当該コンテンツの削除等を命じることができ

る。

さらに、政府は誤ったオンラインニュースサイトの収入の流れを遮断することを命令できるとされており、企業が当該プラットフォームで広告を出すことについても禁止している[30]。

８．台湾

台湾では、2018 年９月に、関西国際空港が台風で閉鎖された際、空港に足止めされた台湾の旅行者への対応を巡って偽情報が拡散し、当局への批判が集中したことをきっかけに外交官が自殺するという事件が起こった。これを契機として、2019 年５月に、偽情報の拡散に歯止めをかけることを目的として、厳しい罰則を設けた災害防止救助法の改正案が可決された。同法では、災害に関する噂や虚偽の情報を広め公共又は他人に損害を与えた場合、最大 10 年の懲役（死亡させた場合は７年以上の懲役又は無期懲役）等を課すこととされている。なお、同月には食品安全衛生管理法と感染症予防管理法（傳染病防治法）の改正案、また、６月には農産品市場交易法と食品管理法の改正案が続けて可決され、これらの中にも偽情報の拡散の防止のための規定が盛り込まれた。

第４節　諸外国における関係者の取組状況

１．諸外国におけるプラットフォーム事業者の取組

（１）プラットフォーム事業者による主な取組

国外のプラットフォーム事業者は、上記第３節における記載のとおり、偽情報が大きな問題となり先行して議論が行われていた欧米における政府等の検討も踏まえ、様々な取組を実施している。ここでは、主にFacebook、Google、Twitterの取組について取り上げるが、Facebook と Twitter は主にオープン SNS を運営している一方で、Google は検索サービス、動画投稿サービス（YouTube）、ニュースプラットフォームサービス（Google ニュース）とサービスの種類が様々である点に留意が必要である。

Facebook は、偽情報への対応に関する基本的スタンスとして、削除、抑制、

[30] 2019 年 11 月、シンガポール政府は、野党の国会議員による SNS への投稿が偽情報を含むとして同法に基づく初めての訂正命令を出した。

情報提供という対策を実施しており、①ポリシーに違反するコンテンツやアカウントの削除[31]、②偽情報や不正なコンテンツの拡散の抑制、③信頼できる第三者ファクトチェッカーからのチェック結果の活用等の追加コンテキストの情報提供という３本柱の対策を行っている[32][33]。

2019 年 10 月には、2020 年の米国大統領選挙を前に、外国勢力の介入への対応として大量の偽アカウントを削除したと発表した。その他、虚偽情報の流布や投票妨害を防止するための対策（外部のファクトチェック機関が虚偽と判断したコンテンツについて虚偽である旨の表示を強化、米国市民に投票の棄権を呼びかける有料広告を禁止するポリシーの策定等）を導入し、メディアリテラシーを高めるための取組に 200 万ドルの投資を行うと発表した[34]。

Google は 2019 年２月に自社サービス（Google サーチ、Google ニュース、YouTube 及び広告システム）における偽情報対策に関するホワイトペーパーを公開した[35]。ホワイトペーパーでは、①検索ランク等のアルゴリズムの改善などにより情報の質を確保する[36]、②身元を偽ったりスパム行為を行ったりする利用者など悪意のある主体に対抗措置をとる[37]、③検索サービスやニュースサイトにおいてファクトチェックの情報を見つけやすくするなど利用者により多くの文脈を提供する、といった方針を対策の３つの柱としている。

Twitter は、偽情報への対応として、主に①スパム等のコンテンツやアカウントに関するポリシー策定及び削除[38]、②信頼性の高い情報の提供などを行っている[39]。

---

[31] 削除等の結果は透明性レポートによって公開されている。最新のものは、コミュニティ規定施行レポート第４版。
https://about.fb.com/ja/news/2019/11/community-standards-enforcement-report-nov-2019/

[32] https://about.fb.com/ja/news/2019/05/remove-reduce-inform-new-steps-remove/

[33] https://about.fb.com/news/2018/05/hard-questions-false-news/

[34] https://about.fb.com/news/2019/10/update-on-election-integrity-efforts/

[35] https://www.blog.google/around-the-globe/google-europe/fighting-disinformation-across-our-products/

[36] 検索等のアルゴリズムに関して、関連性が高い情報だけでなく専門家の情報など権威性の高い情報を優先して表示している。また、人の目で検索結果の品質評価を行う仕組みがあり、品質評価者に配布されるガイドラインでは、信頼性の低いウェブページの基準等が明記されている。
https://static.googleusercontent.com/media/guidelines.raterhub.com/ja//searchqualityevaluatorguidelines.pdf

[37] 例えば YouTube におけるスパムアカウント等の削除結果が透明性レポートによって公開されている。2019 年 7 月～9 月の間にコミュニティガイドライン違反のために YouTube から削除された動画件数は 8,765,893 件であり、そのうち「スパム、誤解を招く表現、詐欺」として削除された動画の割合は 54.4%である。
https://transparencyreport.google.com/youtube-policy/removals?hl=ja

[38] 透明性レポートによると、2019 年上半期のスパム対応件数は 9700 万件。
https://transparency.twitter.com/ja/platform-manipulation.html

[39] 利用者がワクチンに関するキーワードを検索した場合に検索結果のトップに厚生労働省の予防接種情報を案内するなど、信頼性の高い情報を提供する取組を行っている。

その他、前述の欧州委員会が策定した行動規範に対して主要なプラットフォーム事業者が提示した、主なベストプラクティスは以下のとおりである。

《参考５》行動規範に対してプラットフォーム事業者が提示したベストプラクティス[40]

	Facebook	Google	Mozilla	Twitter
広告に関する方針	● 虚偽ニュースに関するFacebookポリシー(アカウント・コンテンツ削除等) ● Facebook広告ポリシー(禁止コンテンツの例等)	● 虚偽・詐称に関するGoogleポリシー(虚偽・詐称広告の禁止) ● 悪い広告に関するGoogle年次報告書		● Twitter広告ポリシー(Twitterにおける広告主の責任を明確化) ● Twitter広告品質ポリシー(広告の透明性と条件を規定)
政治的広告に関する方針	● 広告・ページ透明性表示サービス(ユーザへのより詳細な情報提示) ● Facebook政治広告ポリシー(政治広告が認められる条件の提示) ● 「なぜ私はこの広告を見ているか」サービス(広告表示理由の説明)	● 消費者向けGoogle広告設定機能(表示される広告をユーザが設定する機能の提供) ● 政治広告に関するGoogleポリシー(消費者のターゲティングの禁止)		● Twitter広告透明性センター(広告に関する詳細情報を提供するダッシュボード) ● 「Twitter広告のしくみ」(特定の広告が表示されるしくみの解説、表示される広告の設定機能) ● Twitter政治運動ポリシー
サービスの完全性に関する方針	● 虚偽・詐称に関するFacebookポリシー(虚偽・詐称の禁止) ● Facebookスパムポリシー(スパム広告の禁止) ● Facebook透明性レポート(偽アカウント削除の実績公表)	● 正式コンテンツに関するGoogleの取組(検索アルゴリズム改善) ● ニュースコンテンツに関するGoogleポリシー(ニュースコンテンツに対する透明性・説明性の要求) ● Webマスター向けガイドライン(詐欺的・情報操作的にならないためのガイドライン)		● 自動化及び虚偽・詐称に関するTwitter規則 ● Twitter詐称ポリシー(詐称アカウントの永久停止等) ● Twitterスパムポリシー(スパムの定義と禁止)
消費者のエンパワーのための方針・行動	● ファクトチェックを行う第三者機関とのパートナーシップ情報の周知 ● 消費者に対する、虚偽ニュースの判定方法・拡散防止方法の情報提供 ● 信頼された情報源からの情報を優先する戦略 ● ニュースフィード透明性サイト・ブログ(ニュースフィードのしくみ・アルゴリズム変更の情報) ● 虚偽ニュース通報ツール	● Googleファクトチェックツール【開発者向け】(Googleの検索結果やニュースに含まれるコンテンツについてのファクトチェックツール) ● 消費者向けGoogle広告設定機能(表示される広告をユーザが設定する機能)の提供	● 情報・信頼性イニシアチブ ● Firefox 'Facebookコンテナ'拡張(サイト間追跡を困難にするツールの提供) ● Mozilla's lightweight Firefox Focus(プライバシーにフォーカスしたモバイルデバイス用ブラウザ) ● The Coral Project(ジャーナリストが偽情報を特定するための多様な方法を提供) ● Mozilla Fellowship Program ● Mozilla's Reality Redrawn	● ユーザー個人設定及びデータ設定(ユーザーデータ使用の個人設定) ● Twitter広告のレポート(ユーザーが広告について報告・通知する方法) ● Twitter透明性レポート(透明性やプライバシーに関する対応状況の隔年レポート) ● 「Twitter for Good」(メディア・デジタルリテラシー、オンライン安全教育、表現の自由に関する協力状況)
研究コミュニティのエンパワーのための方針・行動	● Facebook選挙研究協議会の運営 ● 社会科学研究(民主主義や選挙へのソーシャルメディアの効果)へのデータ提供	● Datacommons.orgプロジェクト(ファクトチェックデータの共有)	● Mozilla Fellowship Program(技術者と政策担当者が共同で対策を検討する場) ● Mozilla's Reality Redrawn(偽情報の影響を複合現実感で可視化)	● 「Do more With data」イニシアチブ(ユーザデータの活用事例) ● Twitter健康測定提案(共同研究提案) ● Twitter開発者ポリシー(共同研究・開発に関する規定)

上記のベストプラクティス以外の主要な取組としては、ICT リテラシー向上の取組[41]、デジタルジャーナリズム支援[42]、研究活動などへの支援などが行われ

---

https://blog.twitter.com/ja_jp/topics/company/2019/vaccines.html

[40] 第８回事務局資料より引用

[41] 例えば、Google は、若者のデジタルリテラシー向上や、フェイクか事実かをオンラインで分類する方法を若者に教えることを目的として、プロジェクト「MediaWise」を立ち上げた。https://www.blog.google/outreach-initiatives/google-news-initiative/mediawise-media-literacy/

また、2017 年６月には、「Be Internet Awesome」というウェブサイトを立ち上げ、インターネットに関する知識をゲーム感覚で身につけられるように開発された無料のサービスなどが公開されている。
https://beinternetawesome.withgoogle.com/en_us

Facebook は、2018 年８月に、無料レッスンプラン「デジタルリテラシーライブラリ」をアメリカ国内向けに提供開始し、同年 12 月には同レッスンプランの日本語版の提供を開始した。
https://ja.newsroom.fb.com/news/2018/12/digitalliteracylibrary/

Twitter は、UNESCO とパートナーシップを結び、2019 年 10 月に教育者向けの新しいハンドブック「Twitter を活用した教育と学習」を英語や日本語を含む９カ国語で提供開始した。当該取組と同時に、合成もしくは悪意を持って操作された画像や映像メディアに対応するためのポリシー策定に関するパブリックコメントを開始した。
https://blog.twitter.com/ja_jp/topics/company/2019/twitter-launches-new-media-literacy-handbook-for-schools.html

[42] 例えば、Google は、2018 年３月、報道機関と連携して、質の高いジャーナリズムの強化、持続可能な成長を促進するためにビジネスモデルの確立、技術革新を通じた報道機関の支援を目的として、「Google ニュース イニシアティブ」を発表した 。
https://blog.google/topics/google-news-initiative/announcing-google-news-initiative/

アリゾナ州立大学 Walter Cronkite School of Journalism は、Facebook の協力を得て、2017 年 10 月に研究拠点「News Co/lab」を設立し、利用者が偽情報に騙されないためのノウハウの普及を目的とし、メディアによるニュースの透明性確保に関するベストプラクティス集が作成されている。

ている。

（２）ファクトチェック機関との連携

プラットフォーム事業者は、偽情報への対応として、外部のファクトチェック機関との連携を進めることにより、プラットフォームサービス上の情報の質を高める取組を行っている。

例えば、Facebook は、2016 年 12 月から、各国のファクトチェック機関によるファクトチェックと連携した仕組みを導入した[43]。
ファクトチェック機関がコンテンツを虚偽であると評価すると、ニュースフィードにおける該当記事の表示順位が下がり、繰り返しフェイクニュースを配信するページやウェブサイトには、配信数の抑制などの制限が課され、収益化や広告に関する機能が利用できなくなる[44]。

Google は、2016 年 10 月に、ファクトチェック機関との連携により、ファクトチェック結果が検索結果画面や Google ニュースの画面に表示されるという取組を開始し、2017 年４月には日本でも同機能が導入された。ファクトチェッカーに対してファクトチェック結果を表示させるためのツールの提供[45]も行っている。
また､Google は 2017 年 10 月に米国のファクトチェック機関｢Poynter IFCN｣とのパートナーシップを締結したことを公表した[4647]。

---

https://newscollab.org/best-practices/
また、2018 年４月には SNS が民主主義や選挙に与える影響について研究を行うためのイニシアティブを立ち上げると宣言し、2018 年７月に７つの非営利団体が立ち上げた「Social Science One」への協力を開始した（Facebook は利用者のデータ提供のみを行っている)。
https://socialscience.one/blog/social-science-one-public-launch

[43] 2019 年３月現在、55 のパートナーを有している（日本には存在しない。）
https://www.facebook.com/help/publisher/182222309230722

[44] その他、Facebook は、ファクトチェック機関ごとに、その業績と効果を示す統計を記載した報告書を四半期ごとに送付している。第三者ファクトチェック機関の具体的な評価指針は公開されている。その他、ファクトチェック機関に対して、安全性に関する研修を提供している。

[45] https://toolbox.google.com/factcheck/markuptool

[46] https://www.blog.google/outreach-initiatives/google-news-initiative/building-trust-online-partnering-international-fact-checking-network/

[47] パートナーシップにより、①グローバルなファクトチェックワークショップの開催、コーチングの提供、新しいファクトチェック機関への奨励金支給などの様々な取組により信頼できるファクトチェック機関の数を増やすこと、②IFCN が策定したファクトチェック機関に関する行動規範を 10 の言語に翻訳し、ファクトチェックをより多くの地域に拡大すること、③ファクトチェックツールを無料で IFCN コミュニティに提供し、技術トレーニングやエンジニアのサポートを提供することが目的とされている。

（３）政治広告への対応

ターゲティング技術を活用した政治広告に関連した偽情報は特に選挙結果へ大きな影響を与える可能性がある[48]ことから、米国のプラットフォーム事業者は、広告の透明性を高めるなど、政治広告への自主的な対応を進めている。

Facebook では、政治広告の広告主に対して身元証明を求めること、政治広告であることの表記や広告主の表記を行うこと、政治広告に関する情報を検索可能な「広告ライブラリ」を公開するなどの取組を順次進めている[49]。

他方で、2019 年９月に、政治広告については外部のファクトチェック機関からのファクトチェック対象外とするポリシーを発表した[50]。

Google は、選挙広告に関する透明性レポートを公開し、広告主や広告費、ターゲティングに関する情報など、政治広告に関する詳細な情報の提供を行ってきた[51]。

これに加えて、2019 年 11 月に、政治広告に係るポリシーを見直し、政治広告のターゲティングに公共の有権者登録情報や支持政党などのデータを提供することを中止すると発表した[52]。また、ディープフェイクや著しい偽情報を発信する政治広告も禁止するほか、政治広告の透明性を高める情報開示の範囲を拡大するとした。

Twitter は、政治広告に関する透明性の確保方策として、「広告の透明センター」[53]を開設し、広告主や広告費、ターゲティングに関する情報など、政治広告に関する詳細な情報の提供を行ってきたが、2019 年 11 月に、偽情報を含む広告が有権者の投票行動に悪影響が及ぶことを防ぐため、Twitter 上の政治広告を全世界で禁止するポリシー変更を行った[54]。

---

[48] 2016 年米国大統領選挙の際に、Facebook から流出した利用者の個人情報を用いて、英国の Cambridge Analytica 社が米国の有権者に向けたターゲティング広告を提供し投票行動を誘導した疑惑が大きな問題となった。

[49] https://www.facebook.com/business/help/167836590566506?id=288762101909005
https://www.facebook.com/ads/library/

[50] https://about.fb.com/news/2019/09/elections-and-political-speech/

[51] https://transparencyreport.google.com/political-ads/home

[52] なお、政治広告においては個人の趣味や行動パターンを把握して広告を出す詳細なマイクロターゲティングは以前より禁止されており、引き続き許容されないが、他方、年齢・性別・住所（郵便番号レベル）などに基づく一般レベルのターゲティングについては引き続き許容されると発表された。
https://www.blog.google/technology/ads/update-our-political-ads-policy/

[53] https://ads.twitter.com/transparency

[54] https://business.twitter.com/ja/help/ads-policies/prohibited-content-policies/political-content.html

２．諸外国におけるファクトチェックの取組

欧米を中心とした諸外国においては、偽情報に対抗するために、情報の真偽を検証するファクトチェックという活動が行われている。欧米では非営利の団体が主体となってファクチェックを行っているケースが多く、米国デューク大学の「Reporters’ Lab」によると、2019 年 11 月時点で、ファクトチェック機関は全世界で 70 カ国以上に 225 団体存在しているとのことである[55][56]。

ファクトチェック機関は、財団や個人からの寄付等により運営されている場合が多く、上記の大規模なファクトチェック機関はプラットフォーム事業者と連携して活動を行っている。また、ファクトチェック活動のみならず、ニュースメディアやプラットフォーム事業者に対して偽情報への対策に関する助言を行ったり、利用者に対して ICT リテラシー向上のための活動を行っているファクトチェック機関も存在する。

第５節　我が国における関係者の取組状況

１．我が国におけるプラットフォーム事業者の取組

我が国においては現時点で偽情報が大きな問題にはなっていないものの、各プラットフォーム事業者においては、それぞれのサービスの性質に応じた形で、偽情報への対策にもなり得る取組・対応がとられている。

（１）Yahoo!JAPAN の取組

Yahoo!JAPAN における偽情報が問題となり得る主なサービスとしては、①ニュースプラットフォームサービスである「Yahoo!ニュース」、②個人が自由に書込み可能な「Yahoo!知恵袋」、③検索サービスが存在する。

---

[55] https://reporterslab.org/fact-checking/
https://reporterslab.org/how-we-identify-fact-checkers/

[56] 代表的なファクトチェック機関としては、米国の Poynter IFCN、PolitiFact、Snopes、英国の Full Fact などが挙げられる。フランスには、2017 年のフランス大統領選挙の際に立ち上げられた CrossCheck というファクトチェック機関が存在していたが、現在は活動を終了している。特に Poynter IFCN は、60 以上の世界の主要なファクトチェック機関を支援し、それらの成果を研究する団体であり、偽情報対策に取り組む団体の先駆的な存在として、ファクトチェック機関に対する専門的な教育も行っている。

Yahoo!ニュースにおいては、コンテンツの提供元となる媒体社及び個人の書き手は、Yahoo!JAPAN と契約したパートナーとなっており、根拠のない偽情報が入りにくい仕組みがとられている。具体的には、媒体選別や契約時に情報提供元に関する信頼性・専門性等が調査される[57]とともに、個別の記事の入稿後には、媒体社や Yahoo!JAPAN 自身の判断又は外部からの指摘に基づいて記事の取り下げや修正が検討される場合があり、その後一定の要件を満たす場合[58]には契約の解消が行われる。さらに、誤った情報の拡散が生じた場合等は、その旨利用者に向けて、ページ上で説明を行っている。

Yahoo!知恵袋に関しては、サービス利用にあたっての遵守事項として、法令に違反する行為、権利侵害行為、社会規範・公序良俗に反する行為等について禁止する旨を定めているほか、Yahoo!JAPAN では投稿内容の信憑性や正確性を保証していないが、利用者自身の責任と判断で利用することを求める注意喚起がなされている。

検索サービスに関しては、「検索結果とプライバシーに関する有識者会議」を設置し、検索サービスの社会的役割や対応方針について説明を行っている[59]。また、癌や反ワクチンなど、医療に関する情報については、通常の検索結果とは別の枠に専門機関による情報を表示させる取組を行っている。

（２）LINE の取組

LINE における偽情報が問題となり得る主なサービスとしては、①クローズド SNS である LINE、②ニュースプラットフォームサービスである LINE NEWS、③広告配信サービスである LINE 公式アカウントが存在する。

LINE NEWS では、情報提供元のメディアと提携を行い、メディアのニュースを配信している。提携にあたっては事前に媒体の編集方針・記事内容などの審査をおこなっている。また大きなトラヒックが見込まれる記事配信に当たっては、LINE 側の編集者により手動でニュースを選別し、記事内容の確認を行った上で掲載を行い、誤報があった場合には訂正フローなどのガイドラインを整備している。

編集部が手動で選別していない記事については、独立した校正・校閲の専門チームを組織し、必要に応じて１次ソースの確認や、事実誤認・ミスリードの

[57] 記事内容は情報提供元の責任とされている。
[58] 記事を更新しない場合、記事の質が一定レベルに届かないと判断された場合など。
[59] https://publicpolicy.yahoo.co.jp/2015/03/3016.html

排除に努めるための取組が行われている。

広告配信主体としてのLINE公式アカウントサービスでは、アカウント開設に当たって開設基準[60]を定めている。また、ディスプレイ広告に関しても広告表現に関して、注意・制限事項[61]を定めており、不当表示などに関して禁止行為を定めている。これらは利用者への表示前に確認をされるが、特に公式アカウントでは開設後にもレギュレーション違反がされていないか確認を行っている。

その他、防災・減災に関する偽情報への対策として、LINEでは、内閣府の戦略的イノベーション創造プログラム（SIP）を活用し、災害発生時にLINE公式アカウントと組み合わせて迅速かつ適切な情報収集や情報提供を可能とするAI防災チャットボットの研究開発に取り組んでいる[62]。この中で、偽情報への対策として、国立研究開発法人情報通信研究機構（NICT）が開発したSNS上の災害関連情報をリアルタイムに集約・分析・整理する「DISAANA」や「D-SUMM」といった技術も活用して取組が進められている[63]。

２．我が国におけるファクトチェックの取組

我が国におけるファクトチェックの取組に関しては、2012年４月にメディアの誤報を検証するサイト「GoHoo」[64]が設立され、2017年６月には、ファクトチェック活動を推進する団体であるファクトチェック・イニシアティブ（FactCheck Initiative Japan（FIJ））が設立されるなど、徐々に取組が進められている[65]。

FIJにおける主な取組としては、AI技術を活用したファクトチェック活動の支援が挙げられる。自然言語処理技術を応用して、SNS上の情報からファクトチェックの端緒となる「疑義言説」の候補を自動的に捕捉収集し絞り込むシステムを開発し、メディアに提供を行っている[66]。

---

[60] 現時点で政党はアカウントを開設することはできないこととされている。
[61] ディスプレイ広告では、政党からの広告を受け付けていない。
[62] 国立研究開発法人防災科学技術研究所、ウェザーニューズ及びNICTと連携している。
[63] 具体的には、Twitter等のSNS又はLINEの防災チャットボットに投稿された情報について、それと矛盾する情報が見つかった場合には、双方の情報を併記して提示することで利用者がフェイクニュースの可能性を判断するための材料を提供するなど、正確な情報収集・情報提供を目指した取組が進められている。
[64] 2019年８月に事業を終了。
http://wanj.or.jp/%e8%a7%a3%e6%95%a3%e3%81%ab%e3%81%a4%e3%81%84%e3%81%a6/
[65] 主な活動としては、2017年に行われた衆議院議員総選挙の際に、バズフィードジャパン・GoHoo・Japan In-depth・ニュースのタネの４メディアが参加し、FIJのもとでファクトチェックプロジェクトが行われた。
[66] http://archive.fij.info/project/technology

３．我が国におけるネットメディアの取組

2019 年４月に、インターネット上で発信されるメディアの情報の信頼性を高め、偽情報へ対抗することを目的として、インターネットメディア協会（JIMA）が設立された。

JIMA には、ニュースメディアやコンテンツメディアなど、さまざまなレイヤの主要メディアが参加している。

JIMA では、倫理綱領の策定、発信者としての信頼向上のための取組の共有、各媒体の自主的なガイドライン策定などをサポートするための知見共有、読者のリテラシー教育など啓発活動への取組などを実施することとされている。

第６節　我が国におけるフェイクニュースや偽情報への対応の在り方

１．自主的スキームの尊重

偽情報への対応の在り方の基本的な方向性としては、法律による規制、自主的取組とその実効性を支える法的規律を組み合わせた共同規制的な枠組みの構築、業界に対して行動規範の策定を求める等による自主的な対応、個社ごとの自主的な対応など、様々なレベルの対応が考えられる。

この点、第３節における記載のとおり、選挙への影響等により早くから問題が顕在化していた米国や欧州においては、プラットフォーム事業者による自主的な対応を中心に取組が進められてきたところである。一方、一部の国々、具体的には、ドイツ・フランス・シンガポール等の国々では、偽情報の削除義務等を定めた法律が制定されているが、表現の自由への萎縮効果への懸念や、偽情報の該当性判断の困難性による実効性の欠如及び恣意的運用への懸念など、多くの課題や批判の声もある。

したがって、我が国における偽情報への対応の在り方の基本的な方向性としては、まずはプラットフォーム事業者を始めとする民間部門における関係者による自主的な取組を基本とした対策を進めていくことが適当である。

政府は、これらの民間による自主的な取組を尊重し、その取組状況を注視し

ていくことが適当である。特に、プラットフォーム事業者による情報の削除等の対応など、個別のコンテンツの内容判断に関わるものについては、表現の自由の確保などの観点から、政府の介入は極めて慎重であるべきである。

他方で、仮に民間による自主的スキームが達成されない場合、あるいは、将来的に偽情報の拡散等の問題に対して効果がないと認められる場合には、透明性・アカウンタビリティの確保方策に関して、プラットフォーム事業者に対する行動規範の策定や対応状況の報告・公表など、行政からの一定の関与も視野に入れて検討を行うことが適当である。

２. 我が国における実態の把握

偽情報への対応の在り方の具体的な検討に際しては、まずは我が国においてどのような情報の流通が問題になっているのか、また、今後問題になり得るのかを明らかにする必要がある。この点、我が国において対処すべき偽情報の類型や性質、偽情報の流通状況、偽情報により引き起こされる可能性のある問題などについて、行政及び研究者等が協力して、その実態を正確かつ客観的に把握した上で取組を進めていくことが必要である。

偽情報の実態の把握に当たっては、偽情報自体に着目した調査のみならず、プラットフォームサービスにおける偽情報の生成、拡散の各場面において、どのような主体にどのような問題が生じているのかについて把握することが必要であると考えられる。具体的には、我が国において、どのような主体がどのような目的で偽情報の一次的な発信を行っているのか、また、どのような利用者がそれらの偽情報の影響を受けて拡散等を行っているのかといった内容について実態の把握を行うことが必要である。

また、行政や研究者等がプラットフォーム上に流通する偽情報の調査を実施するに当たっては、プラットフォーム事業者しか持ち得ない情報が利用できれば、より詳細かつ正確な調査を行うことが可能になると考えられる。

このため、プラットフォーム事業者は、利用者のプライバシーに配慮しつつ行政や研究者等が調査を行う際に必要な情報を提供するなど、我が国における偽情報の流通状況の実態の把握に関して協力を行うことが期待される。

加えて、プラットフォーム事業者は、将来的に偽アカウントの急増などの事態が生じ得ることに備え、自らのサービスの提供に当たっては、常に偽情報の発生・拡散状況を把握できるようにしておくことが望ましい。

３.多様なステークホルダーによる協力関係の構築

偽情報の問題の背景には、プラットフォームサービスの特性のみならず、社会的・政治的背景（災害、選挙、国際関係など）、利用者（ICT リテラシーなど）、メディア環境（発信側の信頼性など）、といった複数の要素が多元的に働いていると考えられる。これらを踏まえ、偽情報への対応に当たっては、多面的な解決策を検討していくことが必要である。

多面的に対応を進めていく際には、プラットフォーム事業者のみならず、産学官民の多様なステークホルダーによる協力関係の構築を図り、対話の枠組みを設けることが重要と考えられる。

具体的には、国内外の主要なプラットフォーム事業者・政府・有識者・利用者等の関係者で構成するフォーラムを設置し、偽情報の実態や各ステークホルダーの取組の進捗状況を共有しつつ継続的な議論を行っていくことが適当である。

フォーラムにおいては、例えば、プラットフォーム事業者を始めとする関係者の取組や我が国における偽情報の最新の状況などが共有され、国民（利用者）やメディア等に対してプラットフォーム事業者を始めとする各関係者の取組の効果や課題などが明らかになることで社会全体としてのモニタリング機能が果たされ、それらの反応を踏まえて各関係者によって更なる取組が進められていく、というサイクルが回っていくことが期待される。

なお、フォーラムの在り方に関しては、上記で例示した関係者以外にも、例えば、ファクトチェック機関やネットメディアなど、プラットフォームサービス事業者と利害関係や緊張関係にある主体がどのように関わるべきか、あるいは、政府がどのような形でフォーラムの運営や議論の方向性に関わるかといった点を含めて、並行して検討を行っていくことが適当であると考えられる。

例えば、政府は、多様なステークホルダー間の協力関係の構築を支援するコーディネーターとしての役割を果たすことも考えられる。

その他、フォーラムの開催以外にも、後述のファクトチェック機能の強化を目的としたプラットフォーム事業者とファクトチェック機関との連携や、効果的・実践的な ICT リテラシー向上の推進を目的としたプラットフォーム事業者と ICT リテラシー向上推進団体との連携など、個別の対策に関連する関係者間

の協力関係の構築が重要であり、政府はそれらの協力関係の構築に向けて支援することが適当である。

４. プラットフォーム事業者による適切な対応及び透明性･アカウンタビリティの確保

第１節で記載したとおり、プラットフォームサービスは、経済活動や国民生活などの社会基盤となりつつあり、特に情報流通の基盤を形成している。他方で、プラットフォームサービスに固有の特性がインターネット上の偽情報の顕在化の一因になっていると考えられ、それにより利用者が多様な情報をもとに物事を正確に理解して適切な判断を下すことが困難になり、結果として、利用者にとって様々な不利益が生じるおそれがある。

したがって、インターネット空間の信頼性を高め、我が国の利用者が安心・信頼してプラットフォームサービスを利用できるようにする観点からは、様々な関係者の中でも、特にプラットフォーム事業者が偽情報に対する取組・対応を主体的に進めることが期待される。

（１）プラットフォーム事業者による偽情報の削除等の適切な対応

偽情報への対応として、偽情報の生成・拡散を直接的に防ぐ観点から、問題となる様々な種類の情報やアカウント（ボットアカウント）の削除等を行うことが考えられるが、これらの対応については、各プラットフォームサービスの性質や考え方に応じたポリシーに沿って、プラットフォーム事業者自身が自律的に判断して対処することが期待される。

この点、これらの個別のコンテンツの内容判断に関わる対応については、表現の自由の確保の重要性に鑑み、過剰な削除などの問題が生じないようにする観点から、政府の介入は極めて慎重であるべきである。

（２）プラットフォーム事業者による透明性・アカウンタビリティの確保

利用者が安心・信頼してプラットフォームサービスを利用することができるよう、上記（１）で記載したプラットフォーム事業者による自律的な情報の削除等の対応に加えて、それらの取組が適切に行われていることが利用者や社会全体に対して明らかにされることが望ましい。また、利用者の表現の自由を確保する観点から、プラットフォーム事業者によって過剰な削除や不当なアカウント停止等の行き過ぎた対応が行われていないかという点についても明らかに

されることが望ましい。

以上の観点から、プラットフォームサービスの提供に当たって、いわばプラットフォーム事業者によるガバナンスが適切に機能しているか否かについて、利用者や社会全体が把握することができるようにすることが重要であることから、プラットフォーム事業者は、自らの取組の透明性やアカウンタビリティを確保する方策についても、上記の削除等の対応と同時に積極的に取り組むことが適当である。

プラットフォーム事業者による透明性やアカウンタビリティの具体的な確保方策としては、例えば、

① どのような種類・性質の情報又はアカウントに対して、どのような対応を行うのか、自らが提供するサービスの全体的な考え方や具体的な対応に関するポリシーをあらかじめ明確に定めて公開すること
② 自らが実際に行った取組の結果を公開すること
③ 取組の効果について分析を行い公開すること
④ 取組の効果や偽情報の流通状況について外部の研究者等が調査分析を行う際に必要な情報を提供すること
⑤ 削除やアカウント停止等の対応に関して利用者からの苦情や問合せ等がある場合に備え、苦情受付態勢及び苦情処理プロセスを適切に定め、利用者に対してわかりやすく公開し、適切に運用を行うこと

などの取組を実施することが望ましい。

なお、このうちプラットフォーム事業者自らが実際に行った取組の結果の公開に関しては、削除等の個別の対応全てに関して逐一公開することはプラットフォーム事業者の負担の面でも、また、利用者にとってのわかりやすさの面でも現実的ではないと考えられる。この点、各プラットフォーム事業者においては、一部のプラットフォーム事業者が実施している透明性レポートの作成の取組なども参考にしつつ、一定期間内に実施した取組を定期的に取りまとめて公表するなど、自らが実施した取組全体についてのアカウンタビリティを果たすとともに、個別の対応について利用者から苦情や問合せがあった場合には、苦情処理プロセスの中で適切に個々の利用者に対してもアカウンタビリティを果たすことが望ましい。

上記の①～⑤を始めとした透明性やアカウンタビリティの確保方策について、グローバルにサービスを提供している国外のプラットフォーム事業者において

は、米国や欧州の英語圏のみで実施しており、必ずしも我が国では実施されていない場合や、日本で実施されているとしても日本の利用者向けにわかりやすく日本語で説明されていない場合がある、という指摘がなされている。

したがって、国外のプラットフォーム事業者においては、第４節における記載のとおり、既に米国や欧州において多くの取組を実施しているところ、これらの取組について、欧米と我が国との間の偽情報の現状、社会状況、法制度等の違いに留意しつつ、可能な限り我が国でも実施されることが望ましい。

さらに、問題となる情報の分類及び具体的な対応に関するポリシーの策定、透明性レポート等の作成・公開、苦情受付態勢の整備などに関しては、我が国の利用者に対して、わかりやすく、我が国における個別事情に応じた対応が行われることが期待される。具体的には、

① 日本語で我が国の利用者にもわかりやすい形でポリシーや透明性レポートなどの情報を公開すること
② 透明性レポートを公開する際には、グローバルな対応件数の総数だけではなく、我が国の国内における対応件数についても併せて公開すること
③ 日本語を正しく理解できるスタッフを十分確保した上で、日本語で手続可能な適切な苦情受付態勢および苦情処理プロセスを整備するとともに、裁判手続を含めた国内での迅速な救済メカニズムを確保すること
④ 偽情報も含め、日本特有のプラットフォーム上の情報流通の問題にも適切に対応できるポリシーを策定すること

などの取組を実施することが望ましい。

なお、プラットフォーム上では大量の情報が流通することから、プラットフォーム事業者は、機械学習を含むAIによるアルゴリズムを活用して情報の流通をコントロールすることが一般的になっている。この点、機械学習を含むAI技術により情報の削除等の対応を行う場合には、AIにより誤った判定がなされ、本来は削除されるべきでない情報まで過剰に削除されてしまう可能性や、アルゴリズムにより不当に表示順位が低くなってしまうなどの可能性がある点が課題と考えられる。

したがって、プラットフォーム事業者は、機械学習を含むAIによるアルゴリズムの活用により情報の流通をコントロールしたり削除等の対応を行う場合には、どのような考え方に基づいて問題となる情報に対処するのかを明らかにする観点から、アルゴリズムに関する透明性を確保したり、アカウンタビリティ

を果たすことが重要である。その際、「人間中心の AI 社会原則」[67]、「国際的な議論のための AI 開発ガイドライン案」[68]や「AI 利活用ガイドライン」[69]などを参考にすることが期待される[70]。

また、AI 技術により削除等の対応を行った結果として利用者から苦情や問合せがあった場合には、適切なアカウンタビリティを確保する観点から、苦情処理プロセスの中で人による確認や対応を行うことが望ましい。

以上のとおり、プラットフォーム事業者が自主的に取組を実施し、それらの取組に関する透明性及びアカウンタビリティの確保を図るとともに、プラットフォーム事業者自身による対応状況等の公開・説明やフォーラムの開催等を通じて、国民（利用者）やメディア等に対して取組の効果や課題などが明らかになることで社会全体としてのモニタリング機能が果たされ、それらの反応を踏まえてプラットフォーム事業者による更なる取組が進められていく、というサイクルが回っていくことが期待される。

また、政府は、こうしたプラットフォーム事業者による透明性やアカウンタビリティの確保方策の状況について、フォーラム等の場を通じて随時適切に把握することが適当であり、仮にこれらの自主的スキームが達成されない場合、あるいは将来的に偽情報の拡散等の問題に対して効果がないと認められる場合には、透明性・アカウンタビリティの確保方策に関して、プラットフォーム事業者に対する行動規範の策定や対応状況の報告・公表など、行政からの一定の関与も視野に入れて検討を行うことが適当である[71]。

---

[67] 「人間中心の AI 社会原則会議」においてとりまとめられ、統合イノベーション戦略推進会議において 2019 年３月に決定・公表。

[68] 総務省情報通信政策研究所で開催する「AI ネットワーク社会推進会議」において、2017 年７月に取りまとめ・公表。

[69] 脚注 68 と同様に、同会議において、2019 年８月に取りまとめ・公表。

[70] 例えば、「AI 利活用ガイドライン」においては、透明性の原則に関して、「AI サービスプロバイダ及びビジネス利用者は、AI システム又は AI サービスの入出力等の検証可能性及び判断結果の説明可能性に留意する」としており、具体的には、「説明可能性の確保」について、「AI サービスプロバイダ及びビジネス利用者は、個人の権利・利益に重大な影響を及ぼす可能性のある分野において AI を利用する場合など、AI を利活用する際の社会的文脈を踏まえ、利用者の納得感や安心感の獲得、また、そのための AI の動作に対する証拠の提示等を目的として、AI の判断結果の説明可能性を確保することが期待される」としている。なお、説明可能性の確保はプライバシーの原則（プライバシーの確保）等とトレードオフの関係になる面もあり、両者のバランスを考慮することも必要である。また、アカウンタビリティの原則に関して、「利用者は、ステークホルダに対しアカウンタビリティを果たすよう努める」としており、具体的には、「アカウンタビリティを果たす努力」について、「消費者的利用者、AI の利活用により影響を受ける第三者等に対し、利用する AI の性質及び目的等に照らして、それぞれが有する知識や能力の多寡に応じ、AI システムの特性について情報提供と説明を行うことや、多様なステークホルダとの対話を行うこと等により、相応のアカウンタビリティを果たすよう努めることが期待される」としている。

[71] 欧州委員会のフェイクニュース対策に関する行動規範や、オンライン・プラットフォーム規則における透明性確保及び苦情処理スキーム、又は英国で検討中の共同規制的枠組案が参考となると考えられる。

５.利用者情報を活用した情報配信への対応

プラットフォーム事業者は、利用者情報の集約・分析を行い、各利用者の行動データに基づいて、個々の利用者ごとの興味や関心に応じて、効果的・効率的な情報配信を始めとするマーケティングを行うこと（いわゆる「行動ターゲティング」）が可能である。

行動ターゲティングに関しては、2016 年の米国大統領選挙の際に、プラットフォーム事業者から流出した利用者情報を用いて政治利用目的のターゲティング広告が行われたことが大きな問題となったことを契機として、欧米を中心として政治広告におけるターゲティング技術活用の是非に関する議論が行われている。

行動ターゲティングの技術は、効率的な広告配信を可能にするほか、利用者の好みに応じて利用者にとって有益なニュースや情報を選別し配信するなど、利用者の利便性に資するために用いることができるものである一方で、政治広告における悪用事例のように、利用者の脆弱性につけ込み偽情報を拡散する使い方も可能である[72]。

この点、行動ターゲティングの仕組みに起因する問題は、プラットフォーム事業者のほか広告主や広告事業者等も含めた幅広い関係者にまたがる課題であり、また、偽情報への対応という観点にとどまらない課題でもあることから、より広い観点から慎重な検討を要すると考えられる。

したがって、利用者情報を活用した情報配信への対応については、一般的な行動ターゲティングにおける利用者情報の取扱いの問題と、政治広告など偽情報の生成・拡散のために悪用され、大きな問題を引き起こす可能性がある行動ターゲティングの問題との間に違いがあることを認識した上で、引き続き対応策を検討していくことが必要である。

プラットフォーム事業者においては、利用者情報を活用した情報配信を行う場合には、まずは自ら透明性及びアカウンタビリティの確保を図りつつ適切に活用・実施することが望ましい。また、広告主や広告事業者といった関係者とも連携しつつ適切に透明性及びアカウンタビリティの確保に取り組んでいくこ

[72] Cambridge Analytica 事件においても、ターゲティング技術により偽情報が配信されていたという疑惑が問題視された。

とが望ましい。

利用者情報を活用した情報配信への対応に関する透明性及びアカウンタビリティの確保方策の具体例としては、第４節における記載のとおり既に諸外国において行われている取組を参考にしつつ、例えば、情報配信に関するアルゴリズムの透明性、ターゲティング広告に関するポリシーや資金源等の公開などが考えられる。

ただし、仮にこれらの自主的スキームが達成されない場合、あるいは将来的に偽情報の拡散等の問題に対して効果がないと認められる場合には、政府は、透明性・アカウンタビリティの確保方策に関して、プラットフォーム事業者に対する行動規範の策定や対応状況の報告・公表の求めなど、行政からの一定の関与も視野に入れて検討を行うことが適当である。

６. ファクトチェックの推進

偽情報への対応として、諸外国ではファクトチェックの取組が盛んであり、多様な民間主体による多元的なファクトチェックの実践により、表現や言論に関する自律的な取組を通じて一般利用者が発信・拡散した真偽不明の情報や、情報源・出所が不明なニュースなどの偽情報の自然淘汰を目指すことは、我が国においても有用であると考えられる。

この点、我が国においても、ファクトチェックを支援するための団体が設立されるなど、ファクトチェックの取組が徐々に広がってきているものの、持続可能なファクトチェックの事業モデルが存在せず、ファクトチェックの担い手が不足していることや、社会的認知度や理解度が不足しているという課題が存在している。したがって、これらの課題を踏まえ、ファクトチェックの活性化のための環境整備を推進していくことが適当である。

ファクトチェックの活性化のための環境整備や、ファクトチェック活動への支援を実施する際には、ファクトチェック機関には政府やプラットフォーム事業者からの一定の独立性・第三者性が求められることから、その活動コストを、どの主体が[73]どのようなファクトチェック機関の活動に対して負担するのが望ましいのか、また、資金提供者とファクトチェック活動の独立性確保の仕組みなどについて議論を継続することが適当である。

[73] 例えば、財団や個人からの寄付や、助成プログラムの活用などが考えられる。

また、ファクトチェック機関への支援方策の検討に当たっては、海外における事例を参考にしつつ、また、ファクトチェック機関の独立性・第三者性を確保しつつ、ファクトチェック機関とプラットフォーム事業者の連携を進めていくことも望ましい。

具体的には、例えば、プラットフォーム上の情報へのファクトチェック結果の紐付け、ファクトチェックを容易にするツールの開発及び提供、ファクトチェックを実施する人材の育成などの取組がプラットフォーム事業者との協力・連携のもとで進められることが望ましい。

この際、政府は、ファクトチェック機関とプラットフォーム事業者の間の協力・連携関係が維持・向上するよう、適切な役割を果たしていくことが適当である。

このほか、ファクトチェック結果が効果的に利用者に伝達されるためには、信頼性の高い情報源を参照するといった ICT リテラシーが重要になることから、ファクトチェックの取組と ICT リテラシー向上の取組との連携方策についても検討を深めることが望ましい。

なお、効率的なファクトチェック作業を行うためには、大量の情報の中からファクトチェックの対象となる疑義情報をある程度自動的に選別するために機械学習を含む AI の活用が有用であり、実際に我が国におけるファクトチェックにおいても、自然言語処理に関する機械学習技術が活用されている。

したがって、ファクトチェック活動において、後述のファクトチェックに資する AI 技術等に関する研究開発の成果が活用されることが期待される。

7.ICT リテラシー向上の推進

近年、多くの利用者が、他人とのコミュニケーションやニュース等の情報源としてプラットフォームサービスを活用しているが、プラットフォーム上の情報は、新聞や放送といった伝統的なメディアと異なり、一般利用者（悪意のある者を含む。）により発信・拡散される情報などが多く含まれており、偽情報を含む、信頼性の低い情報に接する機会も飛躍的に増加している[74] [75]。

---

[74] 読売新聞社による全国世論調査によると、インターネットなどに流れている偽の情報を信じてしまったことが「ある」44%、「ない」41%（ネット利用者に限った場合、「ある」54%）。（読売新聞　2019 年 10 月 14 日朝刊２面）

[75] MMD 研究所及び株式会社テスティーが共同で行ったスマートフォンを所有する 12-18 歳を対象に実施した調査によると、フェイクニュースを「見たことがある」43.0%、「見たことがない」57.0%。フェイクニュースを見たことがあると回答した者のうち、フェイクニュースに「騙されたことがある」26.3%、「騙されたことはない」73.7%。https://mmdlabo.jp/investigation/detail_1782.html

偽情報は、SNS 等のプラットフォーム上で、一般利用者が発信した真偽不明の情報を信じて拡散してしまったり、あるいは、情報源・出所が不明なニュースをそのまま拡散してしまったりすることにより、短期間で多くの人々に拡散し、影響や被害が広がってしまうという特徴がある。

したがって、偽情報の拡散を防ぐためには、利用者が情報を適切に読み取るための ICT リテラシーを身につけることが必要である。具体的には、偽情報を容易に信じて拡散等しないようにする判断能力や、信頼性のある情報源を確認する能力などが求められる[76]。

また、偽情報の拡散には、エコーチェンバーやフィルターバブルなどの現代のメディア環境に関する特性や、人間の認知に関する特性が寄与している。そのため、利用者に求められる ICT リテラシーとしては、上記の基本的なインターネット上の情報の利活用に必要な読み書きに関する能力に加え、現代の情報メディア環境に関する知識も重要と考えられる。すなわち、プラットフォーム事業者のサービスに関する具体的な仕組みや、エコーチェンバーやフィルターバブルといった現代の情報メディア環境の特性、その環境の中で偽情報が拡散する仕組みなどを学ぶことで、偽情報に対抗する ICT リテラシーを身につけることが重要になっていくと考えられる。

さらに、偽情報に関しては、利用者は被害者になるだけではなく、意図せず拡散に寄与してしまい加害者になってしまう可能性があるという点や、情報の発信には一定の責任が伴うことなどについても、ICT リテラシー教育の内容に含まれることが望ましい。

この点、放送分野においては、放送番組におけるニュースや広告等をどのように読み解くのか、あるいは、放送番組がどのように制作されているのかといった、映像メディアを主体的に読み解く能力や映像メディア発信者として求められる能力について、放送分野に関わるメディアリテラシーの在り方に関する

[76] MMD 研究所及び株式会社テスティーの同調査によると、フェイクニュースに騙された経験があると回答した者のうち、フェイクニュースの拡散経験として「RT やいいね!による拡散経験あり」27.0%、「SNS では拡散しなかったが友人や家族に話した経験あり」34.0%。
フェイクニュースを見破る自信について、「自信がある」14.4%、「やや自信がある」32.5%、「やや自信がない」38.5%、「自信がない」14.5%。
https://mmdlabo.jp/investigation/detail_1782.html

蓄積が一定程度存在する[77]。

したがって、偽情報に対抗する ICT リテラシーの向上に関しては、このような放送分野にも関連する ICT リテラシーを含め、現代の情報メディア環境全般に対応した ICT リテラシー向上の取組の在り方を意識することが必要である。

政府や ICT リテラシー向上の取組に関わる関係者は、既存の ICT リテラシー向上施策において、上記の点を踏まえ、偽情報の問題に対応した教材やカリキュラムにアップデートしていくことが適当である。

また、今後も情報メディア環境は進展し続けることから、これまで ICT リテラシー向上の取組の対象として重要視されてきた青少年だけではなく、成人であっても継続的に学び続けることが重要であり、幅広い利用者に対する ICT リテラシー向上の推進が必要であると考えられる。

加えて、前述２．における記載のとおり、どのような利用者が偽情報の影響を受けて拡散等を行っているのかといった点について実態の把握を行うことが適当であるところ、それらの結果も踏まえながら、どのような対象者にどのような内容の ICT リテラシー向上の取組を実施することが効果的であるかについて検討を行っていくことが必要である。

なお、ICT リテラシー向上の推進は、これまでも行政や民間団体、通信事業者等によりそれぞれ実施されてきたが、ICT リテラシー向上の取組の目的（例えば、インターネットを安全に利用するためなのか、あるいは、ICT メディアを有効に利活用するためなのか）や対象（例えば、携帯電話やスマートフォンといった機器の使い方なのか、あるいは、インターネットやプラットフォームサービスの使い方なのか）は多様であるため、これらを有機的に結びつけることでより効果的な ICT リテラシー向上のための取組が可能になると考えられる。

したがって、総務省は、ICT リテラシー向上の推進に当たって、行政や民間団体、通信事業者等による既存の施策について、どのような主体・場所（学校等の教育現場、それ以外など）において、どのような観点から ICT リテラシー向上の取組が実施されているかを整理し、様々な主体の連携を促進することが適当である。

---

[77] 放送分野におけるメディアリテラシー
http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/hoso/kyouzai.html
ここでは、メディアリテラシーとは、「①メディアを主体的に読み解く能力、②メディアにアクセスし、活用する能力、③メディアを通じコミュニケーションする能力。特に、情報の読み手との相互作用的（インタラクティブ） コミュニケーション能力、３つを構成要素とする、複合的な能力のこと」とされている。

さらに、プラットフォームサービスの様々な特性が偽情報の問題を深刻化させている側面があると考えられることや、国外のプラットフォーム事業者はすでに諸外国において ICT リテラシー向上の推進を支援している実績があることも踏まえて、我が国においても、行政や民間団体のみならず、プラットフォーム事業者と協働した ICT リテラシー向上の取組を推進していくことが適当である。

その際、プラットフォーム事業者は、先行する海外事例において現代のメディア環境の特性に応じた偽情報対策としての ICT リテラシー向上の取組に関して一定の知見を有していると考えられることから、我が国においても利用者が十分かつ信頼できる情報をもとに正確な判断を行うことを可能にする、いわゆる消費者へのエンパワーメント[78]に資する積極的な ICT リテラシー向上への貢献が期待される。

８.研究開発の推進

前述４．における記載のとおり、プラットフォーム事業者においては、偽情報への対応に関して、大量の情報の投稿やアカウントの削除等を行ったり、情報の表示順位等を重み付けする等のコントロールを行ったりする場合には、機械学習を含む AI によるアルゴリズムを活用することが考えられる。

今後、プラットフォーム上で流通する情報の量は増え続けていくことが予想され、人の目によるチェックだけではプラットフォーム事業者による監視及び削除等の対応にかかるコストが非常に重くなるとともに、対応に漏れが生じてしまうことも想定されるため、プラットフォーム事業者は、今後も機械学習を含む AI を活用した技術について研究開発を推進していくことが望ましい。

また、前述６．における記載のとおり、ファクトチェックの効果的・効率的な実施等の観点からも、政府においては、プラットフォーム上に流通する大量の情報から疑義情報を選別することに資する AI を活用した技術等[79]の研究開発を引き続き推進するとともに、研究活動を行う研究者等を支援していくことが望ましい。

さらに、ディープフェイクなど、近年新たな技術による偽情報の形態が出現しており、今後さらに人の目だけでは見抜くことが困難な情報の流通が課題に

[78] 具体的には、プラットフォームサービス上で信頼すべき情報の優先順位を高めるための取組や、ICT リテラシー向上推進団体、政府、教育機関等と連携した取組等が考えられる。

[79] 例えば、第５節における記載のとおり、NICT では、SNS 上の災害関連情報をリアルタイムに集約・分析・整理する「DISAANA」や「D-SUMM」を開発し、試験公開中。

なっていくと想定されることから、こうした新たな技術を悪用した偽情報に対抗する技術に関する研究を推進していくことがより一層重要になると考えられる。

なお、前述４．における記載のとおり、プラットフォーム事業者は、AI の技術やアルゴリズムの活用により情報の流通をコントロールしたり削除等の対応を行う場合には、どのような考え方に基づいて問題となる情報に対処するのかを明らかにする観点から、アルゴリズムに関する透明性やアカウンタビリティを確保することが望ましい。

AI やアルゴリズムの透明性やアカウンタビリティの確保方策に関しては、「国際的な議論のための AI 開発ガイドライン案」や「AI 利活用ガイドライン」、「人間中心の AI 社会原則」などを参考にすることが期待される。

加えて、AI 技術により削除等の対応を行った結果として利用者から苦情や問合せがあった場合には、適切なアカウンタビリティを確保する観点から、苦情処理プロセスの中で人による確認や対応を行うことが望ましい。

９.情報発信者側における信頼性確保方策の検討

SNS 等のプラットフォーム上には、新聞や放送などの伝統的なメディアにより発信される情報のほか、新たなネットメディアにより発信される情報も流通する場となっている。さらに、コミュニケーションの場として一般利用者が発信する情報が流通することにより、不確かな情報や悪意のある情報なども混在しており、こうした不確かな情報などがプラットフォーム上に蔓延すれば、利用者が多様な情報をもとに物事を正確に理解し、適切な判断を下すことを困難にし、結果として、利用者に様々な不利益が生じるおそれがある。

この点、プラットフォーム上における偽情報の問題に対抗するためには、信頼性の高い情報の流通を増やし、利用者が容易にそれらを参照できるようになっていることが必要である。

そのためには、インターネット上におけるメディア全体の情報の信頼性を確保するための方策が求められるところ、伝統的なメディアにおける情報の信頼性の確保のための取組やノウハウも参考とし、これをネットメディアにも広げていくという考え方も取り入れつつ、現代のメディア環境に対応した情報の信頼性の確保の在り方について検討を深めていくことが適当である。

また、SNS 等のプラットフォームサービスとは別に、一定のメディアによる情

報に限定して掲載するニュース配信プラットフォームサービスがある。これらのニュース配信プラットフォームサービスにおけるプラットフォーム事業者の対応の在り方については、SNS 等のプラットフォームサービスにおいて一般利用者によって発信・拡散された情報が引き起こす偽情報の問題に対するプラットフォーム事業者の対応の在り方とは異なるものであり、また、ニュースや情報に関する選別・編集については各サイト開設者の責任において実施されるべきであることに留意が必要であるところ、各ニュース配信プラットフォーム事業者においては、提供するニュース配信プラットフォームサービスの性質に応じて、配信に関する透明性やアカウンタビリティの確保方策を適切に実施することが望ましい。

インターネット上におけるメディア全体の情報の信頼性をどのように確保していくかについては、例えば、前述３．で言及したフォーラムの場を活用する可能性も含めて、伝統的なメディア・ネットメディア・プラットフォーム事業者等の関係者間で今後検討をさらに深めていくことが望ましい。

その際、プラットフォーム事業者とメディアの協力関係の構築や、海外事例を参考とした信頼性確保のための施策の在り方等についても関係者間で検討することが望ましい。

そのほか、信頼できる質の高い情報をどのようにインターネット上に増やしていくのかについて検討する際には、ファクトチェック活動との連携も含め、信頼性の高い情報のデジタルアーカイブの推進と拡大という観点も意識することが適当である。

さらに、信頼できる質の高い情報に対するセキュリティを確保する観点から、情報源のトレーサビリティを確保するための仕組みや、なりすましを防ぐ認証の仕組み、データの改ざんを防止するタイムスタンプ等の仕組み等に関して、後述の第３章において検討を行ったトラストサービスの活用や連携も視野に入れながら、偽情報への対応に資する取組を検討していくことが適当である。

１０．国際的な対話の深化

偽情報への対応に関しては、第４節における記載のとおり、欧米等で先行した議論や取組が行われてきていることから、我が国において偽情報への対応を検討していくに当たって、国際的な対応状況を注視しつつ、また、対応方針について国際的な調和（ハーモナイゼーション）を図りつつ進めていくことが重

要であり、そのために、国際的な対話を深化させていくことが適当である。

具体的には、欧州委員会における行動規範策定を中心とした民間の自主的取組、フランス・ドイツ・一部のアジアの国々等における法的規制など、様々な方法論が試行されている中で、それぞれの国・地域における文化的背景の違いを認識しながら、表現の自由などの重要な価値観を共有し、インターネット上のルールメイキングに関して国際社会においてコンセンサスが得られるよう、政府は、例えば、二国間対話やOECDなどの国際機関での議論を通じて、国際的な対話を深めていくことが適当である。

第３章　トラストサービスの在り方

トラストサービスの在り方については、本年１月より、本研究会の下に設置した「トラストサービス検討ワーキンググループ」において主に検討を進めてきたところである。

同ワーキンググループでは、本年８月の中間とりまとめでは、特にタイムスタンプ、e シール及びリモート署名について制度の在り方について、検討を深めることとされた。

その後、ユーザ企業へのヒアリング、トラストサービスの利用動向に関する経団連デジタルエコノミー推進委員会加盟企業へのアンケート、先進的な取組を進めるEU 等の海外動向調査等を踏まえながら、具体的なニーズと課題が顕在化しているタイムスタンプ、e シール及びリモート署名について、制度の具体的な在り方について議論を重ね、本年 11 月にトラストサービスに関する論点と取組の方向性を取りまとめた。

本研究会においては、同ワーキンググループから報告を受けて、議論を行ったところであり、検討の具体的内容を別紙として盛り込むこととしたものである。

おわりに

本最終報告書は、中間報告書での指摘を踏まえて、同中間報告書の公表以降に取り組んできた主要課題の検討及び論点の整理のための議論を踏まえて、具体的な方策の在り方や今後の検討の具体的な方向性を示したものである。

各章において示した提言事項については、プラットフォームサービスの普及・拡大に伴う急速な環境変化に迅速かつ適切に対応する観点から、政府をはじめ関係者において、可能なものから順次取組を進めていくことが適当である。特に制度整備に係る事項については、総務省において速やかに対応を行うことが適当である。また、プラットフォーム事業者においても、利用者からの期待を踏まえて、その影響力の大きさに相応した役割を適切に果たすことが期待される。

今後さらなるICTの進展とともにグローバル化・ボーダレス化の拡大が見込まれる中、プラットフォームサービスがさらに電気通信分野においてプレゼンスを高めていくことが予想されるとともに、プラットフォームサービス・ビジネスの急速な進展と多様化に伴い、これまで想定されなかった新たな検討課題を惹起させることも考えられる。

総務省においては、今後ともプラットフォームサービスを巡る市場動向が電気通信分野に及ぼす影響や環境変化、さらには国際動向を注視するとともに、必要に応じて、政策対応の在り方について不断の見直しを行い、利用者が安心・信頼してプラットフォームサービス及び電気通信サービスを利用できるよう努めていくことが適当である。

別紙

プラットフォームサービスに関する研究会
トラストサービス検討ワーキンググループ
最終取りまとめ

プラットフォームサービスに関する研究会

トラストサービス検討ワーキンググループ

目　次

はじめに

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）、Society5.0。

このような Society5.0 として実現される社会においては、ICT 機器の爆発的な普及や、AI の能力の飛躍的な増大とその活用に伴うビッグデータの分析・利活用の進展、すべての人とモノが繋る IoT（Internet of Things)等の社会実装が進み、社会のあらゆる場面でデジタル革命が浸透することで、今までにない、新たな価値が生み出されることが期待される。

Society5.0 の中核となるデータ駆動型社会（Data-driven society）では、良質、最新、正確かつ豊富なリアルデータが価値の源泉となり、経済社会活動を支える最も重要な糧となることが見込まれる。これは、とりもなおさず、経済社会を支える中核的な要素としてのデータの重要性が飛躍的に増大することを意味する。

このような様々な可能性を秘めるデータ駆動型社会においては、そのバックボーンとなるデータの真正性やデータ流通基盤の信頼性を確保することが極めて大切となる。そのためには、インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み（トラストサービス）の実現に向けて、包括的な検討を加えることが必要となってくる。

また、海外に目を転じてみれば、EU では、デジタル・シングル・マーケットを創設するために、その基盤を支えるために包括的なトラストサービスの法制化が進められており、このような国際的な動向も見据えながら、我が国におけるトラストサービスの在り方を検討することが必要である。

このような状況を背景に、本ワーキンググループが「プラットフォームサービスに関する研究会」の下に設置された。本ワーキンググループは、我が国におけるトラストサービスの現状と課題を整理し、課題を解決するための方策について検討を行い、今般、これまでの事業者ヒアリングや構成員の意見等を踏まえ、取り組むべき事項の全体像を最終取りまとめとして整理した。

第１章　　トラストサービスをめぐる状況

１．１　概説

（１）トラストサービスの意義

Society5.0 の実現に向けて、サイバー空間と実空間の一体化が進展し、社会全体のデジタル化が進む中、その有効性を担保する基盤として、送信元のなりすましやデータの改ざん等を防止する仕組みであるトラストサービスが必要となる。トラストサービスの重要性が高まる背景として、次の二つが挙げられる。

① 実空間からサイバー空間へ

情報通信技術が急速に進展し、少子高齢化などの社会課題の迅速かつ柔軟な解決や持続的な経済成長を実現するためには、社会全体のデジタル化を急速に進め、より効率的な社会を実現することが必要不可欠である。

現在、実空間において対面や紙を通じて行っているやりとりが、今後ますますサイバー空間における電子的なやりとりに置き換わり、地方・民間を含めた「社会全体のデジタル化」が進展するための基盤として、電子データの信頼性を確保することが重要である。

② 組織やモノからの情報発信の増大

Society5.0 においては、センサーをはじめとする様々なモノがネットワークにつながり、これまで人を介在して行われていたデータのやりとりが、モノとモノとの間で自動的に行われるといったこれまでにない形態でデータが流通することとなる。

そのため、正当でないモノがネットワークにつながることや、誤ったデータや改ざんされたデータが紛れ込まないよう、データの真正性を確保した上でデータを流通させる必要が生じるため、ヒトだけではなく、組織やモノの正当性、また、それらから発信されるデータの完全性を確認できる仕組みの構築が必要となる。

本ワーキンググループにおいては、後述の EU の eIDAS 規則で規定されているトラストサービスや、近年の IoT 技術の進展への対応等を踏まえて、上記の観点において優先的に検討すべきと判断したトラストサービスのうち以下のものを取り上げ、その課題や取組みの方向性についての検討を行った。各種トラストサービスのイメージは図 1 のとおりである。

（ア） 電子データを作成した本人として、ヒトの正当性を確認できる仕組み
　　→電子署名（個人名の電子証明書）
（イ） 電子データがある時刻に存在し、その時刻以降に当該データが改ざんされていない

ことを証明する仕組み
→タイムスタンプ

（ウ） 電子データを発行した組織として、組織の正当性を確認できる仕組み
→e シール[1]（組織名の電子証明書）

（エ） ウェブサイトが正当な企業等により開設されたものであるか確認する仕組み
→ウェブサイト認証

（オ） IoT 時代における各種センサーから送信されるデータのなりすまし防止等のため、モノの正当性を確認できる仕組み
→モノの正当性の認証

（カ） 送信・受信の正当性や送受信されるデータの完全性の確保を実現する仕組み
→e デリバリー

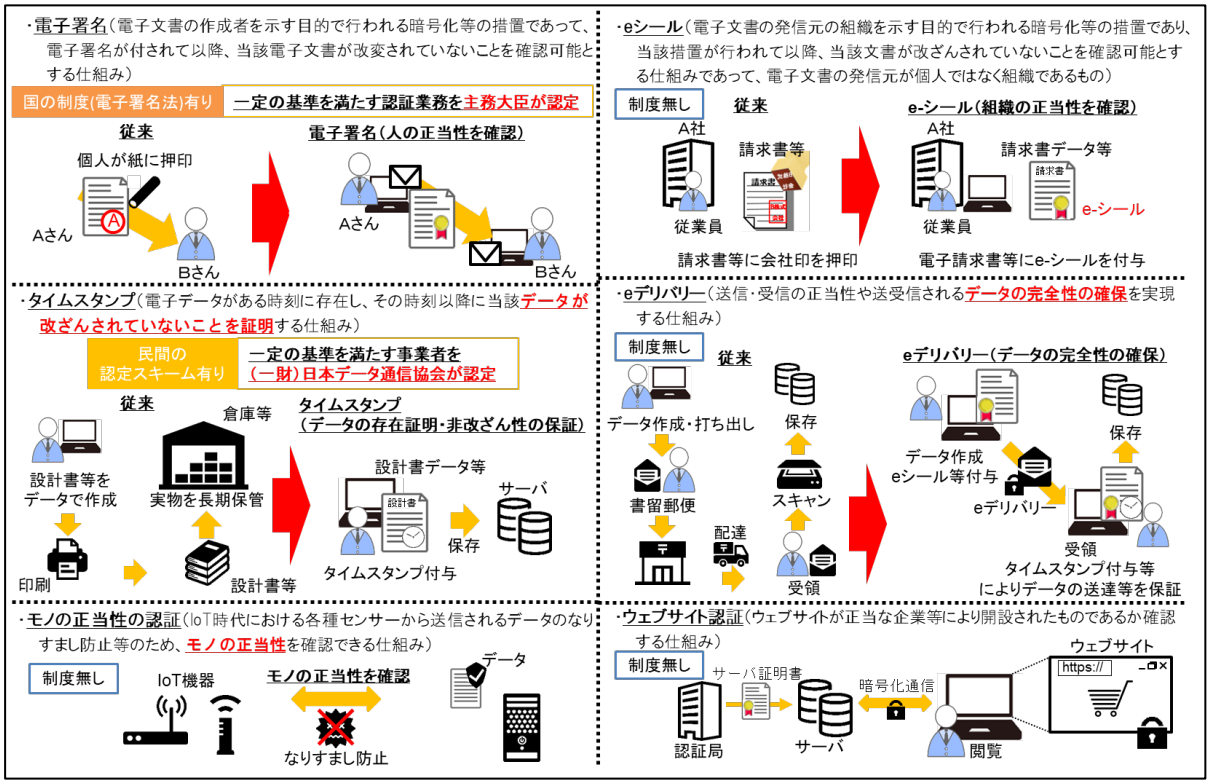


図 1 各種トラストサービスのイメージ

（2）各種トラストサービスの現況

① 電子署名

電子署名とは、電子文書の作成者を示す目的で行われる暗号化等の措置であって、電

[1] 我が国において、電子文書の発信元の組織を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降、当該文書が改ざんされていないことを確認可能とする仕組みであって、電子文書の発信元が個人ではなく組織であるものを「e シール」と呼ぶことが一般的かは定かではないが、本取りまとめにおいては便宜上、EU における呼称である「e シール」を用いることとする。

子署名が付されて以降当該電子文書が改変されていないことを確認可能とする仕組みである。公開鍵暗号方式を用いた電子署名が一般的に利用されている。

また、電子文書の送信者が電子署名を行った者であることを受信者が確認できるよう、その確認に用いられる事項（公開鍵暗号方式においては公開鍵）が当該送信者のものであることを第三者が証明する認証業務が提供されている。公開鍵暗号方式においては、認証事業者から送信者に対して電子証明書が発行され、例えば送信者は当該電子証明書を電子署名付きの電子文書とあわせて受信者に送付し、受信者は当該電子証明書を発行した認証事業者にその有効性を確認することで、送信者がなりすまされていないかを確認する等の利用方法がある。

これら電子署名及び認証業務については、「電子署名及び認証業務に関する法律」（平成 12 年法律第 102 号。以下「電子署名法」という。）に規定されている。電子署名法は、本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る）が電子文書に付されている場合には当該電子文書が真正に成立したものと推定する法的効果が働く旨を規定するとともに、一定の基準を満たす認証業務を主務大臣が認定する制度を設けている。

当該制度に基づき認定を受けた電子署名発行事業者により発行された電子証明書について、平成 30 年度の有効枚数は年間約 35 万件程度となっている（図 2）。

また、電子署名法においては、署名鍵が IC カード等の「物件」に格納され、利用者が手元で管理することを想定している。一方、サービス提供事業者のサーバに利用者の署名鍵を設置・保管し、利用者がサーバにリモートでログインした上で自らの署名鍵で当該事業者のサーバ上で電子署名を行うリモート署名については、一定のネットワーク環境があれば、端末を選ばずに電子署名ができるようになるという利便性向上に加え、IC カードの紛失等のリスクが無くなる等のメリットから、電子契約等の場面で利用拡大が期待されるものの、現状の電子署名法令上どのように位置付けられているか必ずしも明らかではない状況である。

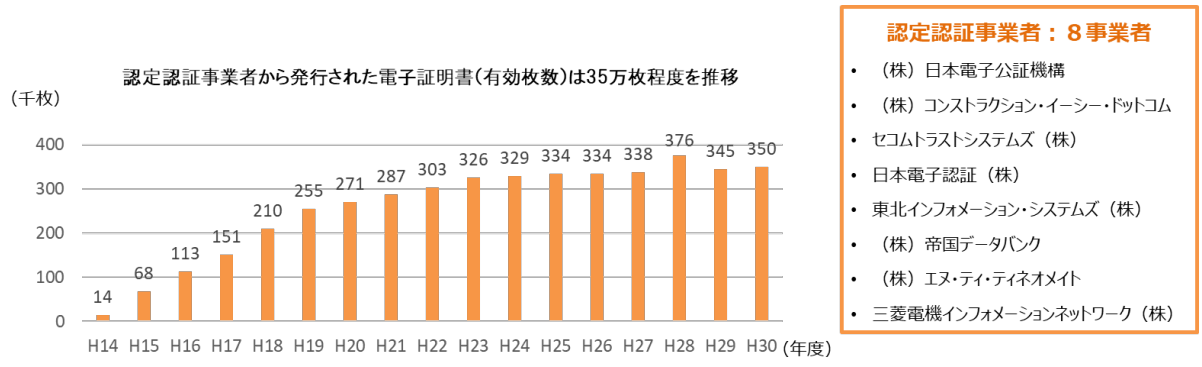


図 2 電子署名法に基づく認定認証事業者から発行された電子証明書（有効枚数）

② タイムスタンプ

タイムスタンプとは、電子文書に正確な時刻情報を加えて暗号化等の措置を講ずることで、タイムスタンプが付された時刻に当該電子文書が存在していたこと及びその時刻以降、

当該文書が改ざんされていないことを確認可能とする仕組みである。

現在は、タイムスタンプ発行業務[2]や当該業務を行う事業者に対して時刻の配信及び監査を行う時刻配信業務に求められる要件を定めた「タイムビジネスに係る指針」（平成 16 年総務省公表）に基づき、（一財）日本データ通信協会によってこれらの業務のうち一定の基準を満たすものの認定（タイムビジネス信頼・安心認定制度）が行われている（図 3）。認定においては、技術、運用、設備等の審査基準を満たし、厳正に業務が実施されているかについて、その適合性が評価の対象となっている。

タイムスタンプは、特定の時点から改ざんされることなく存在していることの証明が求められる知的財産保護のための証拠保全を目的とした技術文書等での利用が期待されているほか、国税関係書類等一部の分野において利用が進んでいる。

具体的には、国税関係書類をスキャナ保存する場合に、「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律（以下「電子帳簿保存法」という）施行規則」（平成 10 年大蔵省令第 43 号）において、タイムスタンプの使用が位置づけられていることから、国税関係書類の保存におけるタイムスタンプの利用が進んでいる[3]。このほか、建築や医療などの特定分野においては、関係文書の電子的な保存に係るガイドラインにタイムスタンプの使用が記載されている例があるものの、他の分野では特段のガイドラインがない等、規定の有無やその水準が分野により異なる状況であることから、各業界におけるタイムスタンプの利用の程度にも差が生じている。

また、電子署名に用いられる電子証明書の有効期間は一般的に5年以下である[4]一方、タイムスタンプの有効期間は一般的に 10 年であり、また、タイムスタンプは有効期間が到来する前に再度付すことでより長期間にわたりその効力を持続させることが可能であるため、電子文書を長期的に保存する場合は、電子署名とタイムスタンプを組み合わせた「長期署名」を利用することが有効である。

---

[2] 「タイムビジネスに係る指針」においては「時刻認証業務」と呼称されている。

[3] 電子帳簿保存法上の「電子で保存」には、①紙で受領した請求書等をスキャンしたデータを保存する場合と②電子的に受領した請求書等を電子データのまま保存する場合の二類系が存在しており、①の場合はタイムスタンプを付すことが義務づけられているものの、②の場合はタイムスタンプの付与又は改ざん防止等の内規の作成及び運用のいずれかが保存の要件となっている。現在、②の場合において、クラウドサービス等の利用者がデータを変更することのできないシステムを用いることを保存の一要件（選択肢）として追加することなどが検討されている。

[4] 電子署名法に基づく認定認証事業者が発行する電子証明書の有効期間は、認定基準において最長5年とされている（電子署名及び認証業務に関する法律施行規則（平成 13 年総務省・法務省・経済産業省令第2号）第6条第4号）。

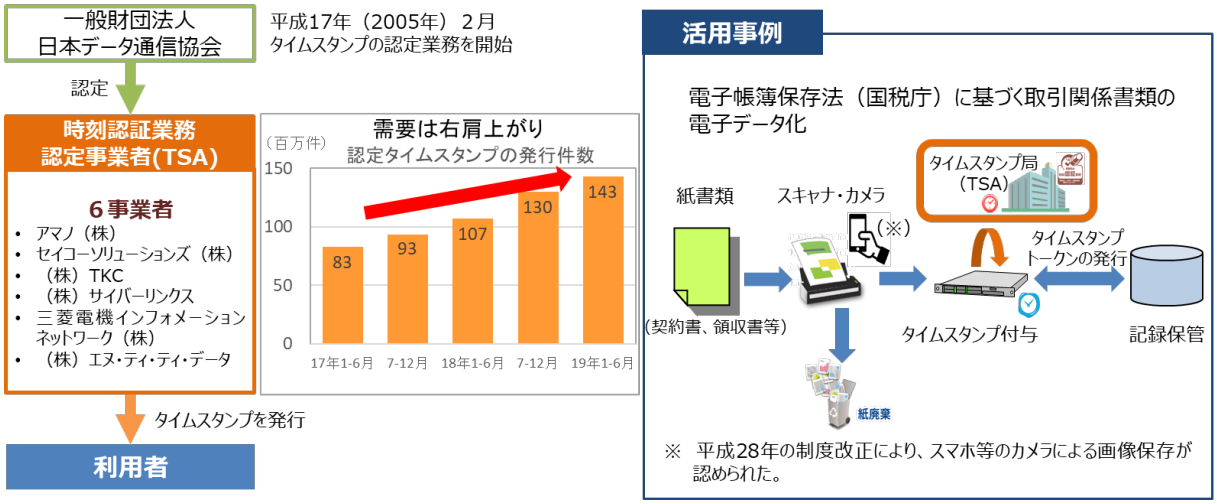


図 3　我が国におけるタイムスタンプの利用の現状

③　e シール

e シールとは、電子文書の発信元の組織を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書が改ざんされていないことを確認可能とする仕組みであって、電子文書の発信元が個人ではなく組織である場合のものである。公開鍵暗号方式を用いる場合には、個人名ではなく組織名の電子証明書が発行されると想定される。e シールを利用することで、受信者は電子文書が確かに送信元の組織から送られたものであることを確認可能となる。なお、EU においては、eIDAS 規則[5]の中で、個人名の電子証明書に基づく電子署名等と同様に e シールについても、適格な発行事業者を EU 各国が認定する制度が存在しており、一定の要件を満たす e シールについては所定の法令上の効果が与えられている。

我が国においては、e シールに関する公的な仕組みは現状存在していないものの、一部の企業において、組織名の電子証明書として e シールの導入が進んでいる。e シールは、電子証明書の発行に当たって e シールを使うことになる個々人の本人確認が不要であることや、担当者の異動に伴う電子証明書の再取得が不要であること、同時に大量に付すことが可能であること等の利点があり、請求書・領収書等に付し、それらの電子的な処理を可能とすることで、支払請求業務等の大幅な効率化に資することが期待されている。

また、我が国では、軽減税率の実施に伴い、2023 年 10 月に「適格請求書等保存方式」（インボイス制度）の導入が予定されており、仕入税額の控除に当たっては、税務署に登録された適格請求書発行事業者が発行した適格請求書等を保存することが要件とされる。書面の適格請求書等については授受や保管のためのコストがかかるほか、発行者が適格請求書発行事業者に該当するか否かを事後的に確認する場合にはそのための事務作業が生じる。

[5] 各トラストサービスの事業者について一定の要件を満たすものを公的に認定する仕組み等を規定した規則（eIDAS 規則：electronic identification and authentication services regulation）

これに対し、適格請求書（インボイス[6]）が電子化（電子インボイス）されれば、授受や保管のためのコストが軽減できるとともに、突合、検索、計算等の自動処理が可能となる。

このように電子インボイス及びｅシールを最大限活用することにより、大幅なコスト削減、効率的で正確な税務処理や納税手続等の実現が期待される。

④ ウェブサイト認証

ウェブサイト認証とは、利用者がウェブサイトを閲覧する際、ウェブブラウザでサーバ証明書を確認することにより、そのウェブサイトが正当な企業等により開設されたものであるかどうかを確認することができる仕組みである。ウェブブラウザに用いられるサーバ証明書は、当該ウェブサイトの真正性を確認する認証事業者により、個人ブログ等に用いられるドメイン認証型証明書、企業サイト等に用いられる実在認証型証明書、オンラインショッピング等金銭のやり取りが発生するサイトに用いられるEV SSL 証明書が発行されている。このようなサーバ証明書をウェブブラウザ上で検証することで、当該ウェブサイトが改ざん、なりすましをされていないことが確認できる。なお、ウェブサイトの真正性が検証された場合、ブラウザ上にその旨の表記がなされることで利用者が確認することが可能となる。

ウェブサイト認証のための電子証明書を発行する認証事業者に求められる基準について、認証事業者[7]と米国のウェブブラウザベンダ等からなる団体であるCA／ブラウザフォーラムにおいて議論が行われており、以下の要件等がガイドラインとして定められ、デファクトスタンダード化されている。

- ポリシーの変更等への迅速な対応
- 認証事業者の運用体制等の透明性の確保
- なりすまし防止等のための証明書発行における確認事項の厳格性の確保

当該要件を満たすと認められなくなると、必ずしも直ちにセキュリティ上問題がない場合であっても、ウェブブラウザ上、安全ではないサイトと表示されるおそれがある。

⑤ モノの正当性の認証

IoT 機器は幾何級数的に増加しており、民間の調査会社によると、2017 年時点の世界中の IoT 機器は約 275 億個、2020 年には約 400 億個まで増加すると予測されている。2017 年時点ではスマートフォンなどの通信機器が多くを占めていたが、今後は自動車・輸送機器分野、医療分野、産業分野で IoT 機器が急速に普及することが見込まれている。

Society5.0 時代においては、モノから発信されるデータが利便性の向上や経済活動の生産性を向上させるための基盤となることが想定されるが、それらのデータが適切なIoT 機器

---

[6] 消費税法（昭和 63 年法律第 108 号）改正（2016 年4月）により消費税の軽減税率制度が 2019 年 10 月から開始されたところ、複数税率（標準税率 10%、軽減税率8%）の下で適正な課税を確保する仕組み（仕入税額控除の方式）として、2023 年 10 月から適格請求書等保存方式（いわゆるインボイス制度）が実施される。

適格請求書とは「売手が買手に対し正確な適用税率や消費税額等を伝えるための手段」であり、一定の事項（適格請求書発行事業者の氏名・登録番号、取引年月日、消費税率、消費税額等、軽減税率の対象品目である旨等）が記載された書類のこと。

[7] 日本からは GMO グローバルサイン㈱、セコムトラストシステムズ㈱が参加。

等のモノから発されている正当なデータであるかを確認した上で利活用することが求められる。

⑥ e デリバリー

eデリバリーとは、あらかじめ登録された送受信者の識別とデータの送受信日時の正確性、送受信データの完全性を保証するものであり、各種トラストサービスを組み合わせることで可能となる「電子的な書留」に相当するトラストサービスである。

例えばドイツでは、ドイツテレコムなどによって「De-Mail」サービスが提供されており 、B2C では保険契約事項に関する連絡や株主総会に関する連絡等、B2G では不動産事業者の認可申請や商業登記申請等、C2G では住宅給付申請や税額の査定申請等で使用されている。

こうしたサービスにおいては、受信者・送信者個人が特定されるので、フィッシング詐欺やマルウェア配布を防止することにもつながると考えられるが、e デリバリーは、厳格にヒトや組織の確認がされた送受信者双方が登録して成立するサービスであり、我が国においいても一部の企業で導入が進んでいる。

1．2 トラストサービスの利用動向

現状のトラストサービスの利用に関する企業のニーズや、利用に当たっての懸念事項、制度化に関する要望について把握するため、経団連デジタルエコノミー推進委員会加盟企業に対してアンケートを実施した（当該委員会加盟企業 184 社のうち 39 社から回答が得られた）。

当該アンケートにおいては、各企業の電子化の状況や電子化に当たってのトラストサービスの利用状況について調査したほか、「Ⅰ)文書・データを電子的に組織外部と送受信する時」又は「Ⅱ)文書・データを電子的に保存する時」の場面について、①電子署名（個人名の電子証明書）（リモート署名を含むものとする。以下、本章において同じ。）、②タイムスタンプ、③e シール（組織名の電子証明書）[8]のそれぞれに関する利用の有無や使用に当たっての課題等の調査を実施しており、得られた結果は以下のとおりである。

（1） 総論（電子化の状況及びその際のトラストサービスの利用状況について）

回答のあった 39 社のうち、約9割の 36 社が電子的手段を用いてデータ等の送受信や保存を行っており、書類の電子化自体は徐々に進展していると考えられる。その一方、電子化を行っている企業 36 社のうちトラストサービス（電子署名・タイムスタンプ・e シール）の利用は約5割の 17 社にとどまっていたことから、今後更なるトラストサービス普及拡大の余地があると考えられる。

[8] 当該アンケートでは、組織名の電子証明書と記載して調査を実施。

（２） 各トラストサービスの利用状況

① 電子署名（個人名の電子証明書）

電子署名（個人名の電子証明書）を「Ⅰ）文書・データを電子的に組織外部と送受信する時」に使用しているのは 39 社中９社、「Ⅱ）文書・データを電子的に保存する時」に使用しているのは 39 社中7社であり、使用している企業の多くが、建設業法や印紙税法等の法令・民間ガイドライン等の基準を満たすために使用していることがわかった。

そのことから、各種制度において電子署名の利用が義務づけられている又は推奨されていることで電子署名が法令上の要件を満たしていることが明確になるため、利用者が一定の信頼感を持って電子署名を使用でき、利活用が進展していることが考察された。

② タイムスタンプ

タイムスタンプをⅠ）文書・データを電子的に組織外部と送受信する時」に使用しているのは 39 社中９社、「Ⅱ）文書・データを電子的に保存する時」に使用しているのは 39 社中 11 社であり、タイムスタンプを使用している社の多くが、電子文書の長期保存を利用の目的としているため、使用している企業の多くがタイムスタンプサービスの永続性に関する不安を抱いていることがわかった。また、知財保護の目的から、特許関連文書にタイムスタンプを付与し当該文書を保存するケースにおいては、訴訟時にタイムスタンプの有効性が認められるか、又は当該タイムスタンプが国際的な通用性を有しているかについての不安を感じていることがわかった。

その他、既存のタイムスタンプサービスによる電子文書の保存が、法令・民間ガイドライン等を満たすものであるかに懸念を抱いていることがわかった。

その上で、これらの課題を解決するためタイムスタンプの公的な制度への位置付けを求める声があった。

③ ｅシール（組織名の電子証明書）

ｅシールを「Ⅰ）文書・データを電子的に組織外部と送受信する時」に使用しているのは 39 社中7社、「Ⅱ）文書・データを電子的に保存する時」に使用しているのは 39 社中7社であり、異動手続きが不要、本人確認が不要、大量に付与できる等の利便性が認識され、一部で導入されている。

更に、2023 年に導入される適格請求書（インボイス制度）への対応に当たっては、現状ｅシールを使用していない 29 社のうち 26 社の約9割の企業が使用してみたい旨の回答をしていたことから、ｅシールのニーズは潜在的にはあるものと考えられる。

他方、使用している社の課題として、ｅ シールには適格な事業者を認定する制度がなく、公的な位置付けがないという声があがっていることから、今後のサービス拡大に当たっては、何らかの公的な枠組みを設けることで、更なる利用促進につながっていくのではないかと考えられる。

１．３　我が国におけるデジタル化に関する政策

我が国における文書の電子化についての政策的な推進については、「e-文書法」（「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年法律第 149 号）」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律（平成 16 年法律第 150 号）」2法の総称）の制定によって、民間に保存が義務付けられている書類のうち、電子的な保存が認められていないものについても電子保存が可能となり、飛躍的に進展した。

そして、国税関係書類については、「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」（平成 10 年法律第 25 号。以下「電子帳簿保存法等」という。）によって、法令の規定により民間事業者等が行う書面の保存等の手続について、原則全て電子的に行うことが可能となった。

また、急速な少子化・人口減少等の我が国が抱える諸課題に対処すべく、データ流通の拡大による社会全体の生産性の向上を目的とし、2016 年に「官民データ活用推進基本法」（平成 28 年法律第 103 号）が制定され、同法において、①行政手続をオンラインにより行うことを原則とするよう国が必要な措置を講ずること、②民間事業者が行う契約の申込みその他の手続をオンラインにより行うことを促進するよう国が必要な措置を講ずることが定められた。

さらに、同法の規定を受け、本年、デジタル3原則（デジタルファースト、ワンスオンリー及びコネクテッド・ワンストップ）を基本原則として、「情報通信技術を活用した行政の推進等に関する法律」（平成 14 年法律第 151 号。以下「デジタル手続法」という。）が改正され、国の行政手続についてオンライン化の実施を原則とすること、行政機関間の情報連携等によって行政手続における添付書類の省略を推進すること等が規定された。

2019 年１月に開催された「世界経済フォーラム年次総会（ダボス会議）」では、安倍首相が「成長のエンジンはガソリンによってではなくデジタル・データで回っている」、「新しい経済にとって Data Free Flow With Trust（DFFT）が最重要課題」と述べている。また、2019 年６月に開催された「G20 茨城つくば貿易・デジタル経済大臣会合」では、DFFT のコンセプトに G20 全体で合意がなされ、「自由な開かれたデータ流通」と「データの安心・安全」を両輪とする DFFT のコンセプトについての重要性が議論され、データの信頼性確保の重要性が認識された。

１．４　トラストサービスの活用・普及による経済効果

e-文書法の制定時においては、（一社）日本経済団体連合会の「税務書類の電子保存に関する報告書 [9]」（2004 年3月）にて、税務書類の紙による保存コストは経済界全体で年間 3,000 億円であると試算が示された。

このような効果に加えて、トラストサービスにおいては、契約に係る手続の一連の業務の効率化や、請求・支払い業務の電子での一括処理等、さまざまな場面での活用や効果が考えられる。

そこで、トラストサービスの活用・普及によって、実際にユーザ側での効果としてどの程度の業務効率化が期待できるかに着目 [10]し、一定の前提を置いたうえで、試算を行った。また、トラストサービス及び関連サービス市場の今後の成長の見通しについても試算も行った（業務効率化及びトラストサービス市場の成長試算は、いずれも㈱三菱総合研究所による試算）。

（１） 業務効率化の試算

トラストサービスの導入により、主に間接業務（総務人事系、経理系の業種共通業務）の効率化が期待でき、生産性の向上、他業務への振分け、長時間労働の削減、人員不足の解消等に寄与すると考えられる。

例えば、富士通㈱が行った支払請求事務に関する電子化実証実験 [11]では、e シールなどのトラストサービスの利用によって、請求企業については請求書の印刷・封入・発送処理が不要になることや手作業で行っていた入金消込処理を自動化して効率化できることで、毎月発生する請求業務に係る時間が 98%程度削減されることが示され、また、支払企業については、手作業で行っていた請求書受領後の書類の照合や請求データの入力処理が機械処理できるようになり効率化されることで、支払業務に係る時間が 50～80%程度削減されることが示された。

㈱三菱総合研究所が行った本試算では、e シールなどのトラストサービスを導入することによって、これまで人手で実施していた業務をデジタルで機械的に効率よく処理することが可能となり、

- 例えば、経理系業務の場合、請求書・領収書等の業務文書の物理的なやり取り（書類の郵送や手渡し）が省略可能となったり、請求書・領収書等の記載内容の入力及びその入力内容の確認業務等が不要となったりする等の効果が期待され、

[9] https://www.keidanren.or.jp/japanese/policy/2004/018report.pdf

[10] 文書の処理のデジタル化による効果として、既存の業務のデジタル化に加え、新たな付加価値も期待できるが、後者の定量化は困難なため、ここでは既存プロセスのデジタル化を試算の対象とした。

[11] 本ワーキンググループ（第 10 回）の富士通㈱による発表資料（http://www.soumu.go.jp/main_content/000644760.pdf）より

➢ 大企業1社あたり、10.2 万時間／月かかっている業務が、5.1 万時間／月へ
➢ 小企業1社あたり、502 時間／月かかっている業務が、151 時間／月へ
大幅に削減されることが示された。

- 間接業務（総務人事系、経理系の業種共通業務）全体でも、社内外の紙の文書のやり取りや保存がデジタルに置き換わり RPA（Robotic Process Automation）等を活用して自動処理可能になることや、個人名の電子証明書が e シール（組織名の電子証明書）に置き換わりその管理業務が効率化されること等の効果が期待され、
  ➢ 大企業 1 社あたり、22.6 万時間／月が 15.4 万時間／月へ
  ➢ 小企業 1 社あたり、1,116 時間／月が 608 時間／月へ
  削減されることが示された。

直接業務（業種固有業務）では、業種により異なるものの文書情報の取扱業務の多い業種（特に金融・保険、不動産・物品賃貸、卸売・小売り、運輸・郵便、宿泊・飲食、各種サービス等）ほど高い効果が期待されることが示された。

（２）トラストサービス市場の成長試算

トラストサービス及び関連サービス市場の成長試算に当たっては、ベースケース[12]と成長ケース[13]の両方を考慮して 2030 年頃の市場規模を試算した。なお、現状のトラストサービス及び関連サービスの市場については、電子署名及びタイムスタンプの発行枚数や事業者へのヒアリング、企業数、想定普及率等を踏まえて推計している。

試算の結果、2018 年における我が国のトラストサービス（電子署名、タイムスタンプ、e シール）の市場規模は、50 億円、関連サービスの市場規模は 44 億円で、合計 94 億円と推計され、ベースケースでは、2030 年頃に 271 億円（トラストサービス：146 億円、関連サービス：125 億円）にとどまる一方、成長ケースでは、1,035 億円（トラストサービス：556 億円、関連サービス：479 億円）に達すると推計された（図 4）。

なお、関連サービス市場の推計については、電子契約サービスを中心に、トラストサービスと関係の深いサービス（例：請求・支払関係業務、経費精算等）を対象として推計したが、この他にも、トラストサービスの導入に伴う新たなシステムの構築等に関連する IT システムの導入やアプリケーション等の整備等に関する投資が増加するといった効果も見込まれる。

また、企業内外との文書のやりとりがデジタルに置き換わり、デジタル・トランスフォーメイション（DX）が一層進展し、これまでの紙ベースの業務が効率化され、生産性が向上するこ

[12] 電子署名は微増を継続、タイムスタンプは現状のトレンド+αで推移（対前年比 30%増程で推移）、e シールは微増ないしやや成長、関連サービスは成熟化する想定。
[13] 各トラストサービスについて制度化等の環境が整うことを前提に、電子署名はリモート署名の増加によって約8倍に成長、タイムスタンプは知財保護等の需要により約 50 倍に急成長、e シールは制度化及びインボイス対応等の需要により約 20 倍に急成長し、関連サービスはトラストサービスの成長の影響を受けて約 10 倍に拡大する想定。

とで、更なる波及的な経済効果も期待される。

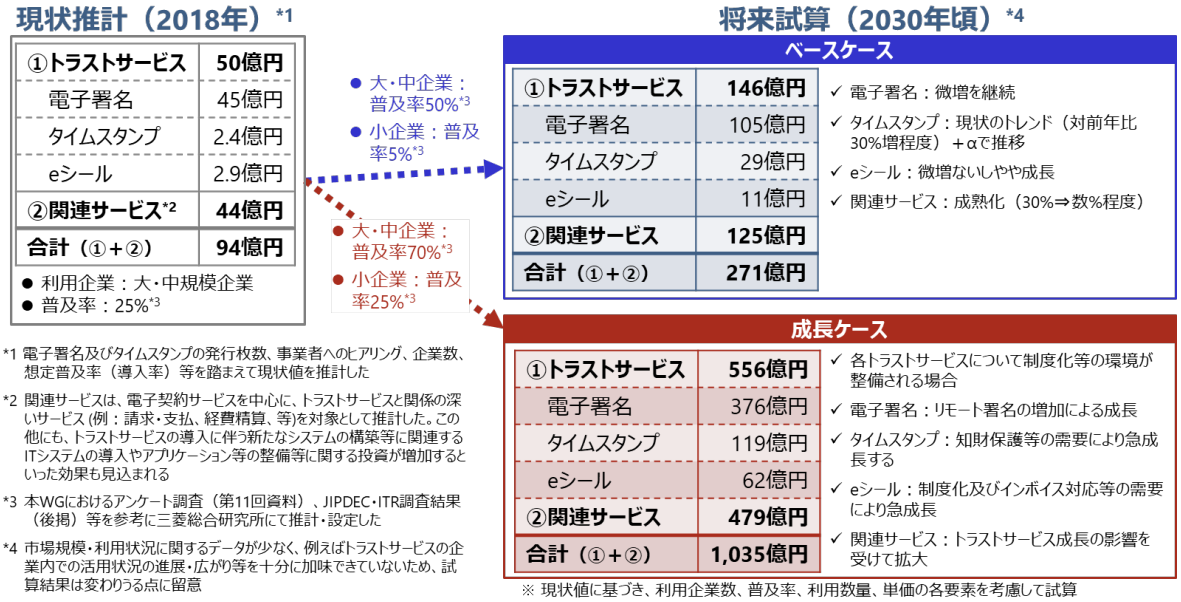


図 4 トラストサービス及び関連サービスの市場の現状推計と将来試算

1．5 諸外国におけるトラストサービスの動向

諸外国におけるトラストサービスの動向について、調査を行った[14]。

（1）EU

① eIDAS 規則

EU は、域内市場を統一し電子商取引を促進するために、いわゆる電子署名指令[15]を策定し、主に適格電子署名を中心に域内全域に広めるために、各国が国内措置をとってきた。しかし、適格電子署名は法令上利用が義務づけられた場面にしか広がりを見せず、その普及が課題となってきた。こうした状況を改善するため、EU では、デジタル・シングル・マーケットを目指し、上記の電子署名指令を廃止して、2014 年に、電子署名以外のタイムスタンプや e シールを含む、各種認証手段の共通規則を定める eIDAS（electronic Identification and Authentication Services）規則を制定した（同規則は、2016 年7月に発効）。

eIDAS 規則では、一定の要件を満たすトラストサービスの提供者を適格トラストサービスプロバイダー（Qualified Trusted Service Provider: QTSP）として認定する仕組みを規定し、EU 各国は認定した事業者をトラストリストとして公開している。2019 年 11 月時点で、欧州

[14] 業務委託先である㈱三菱総合研究所を通じて、欧州、米国、中国の調査を行った。
[15] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[16]では、178 の適格サービスプロバイダー（QTSP）がトラストサービスを提供している。QTSP の構成は図 5 のとおりである。

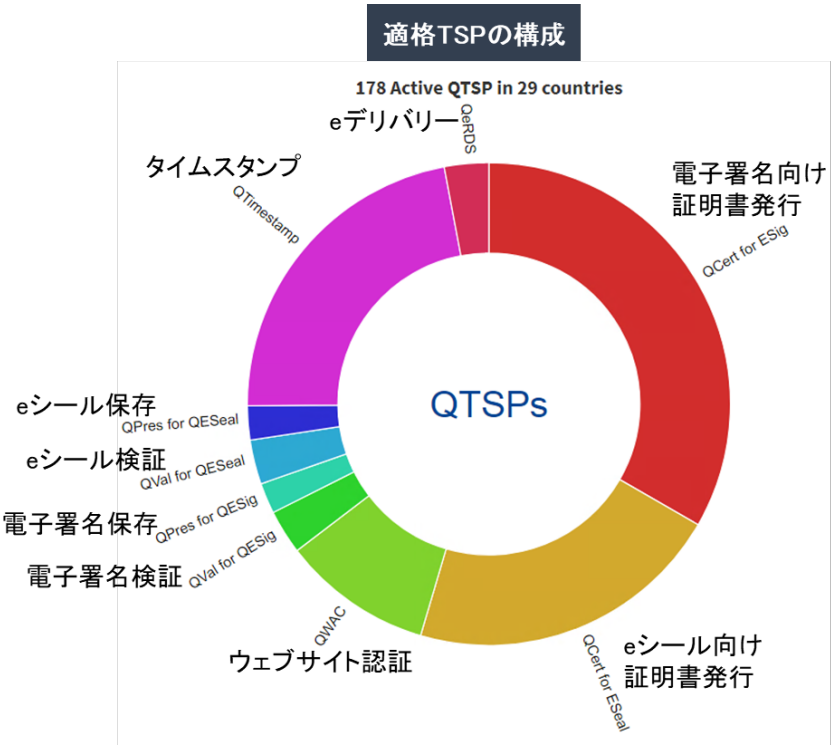


図 5 適格 TSP の構成

eIDAS 規則には、図 6 のとおり法的枠組みが規定されている。

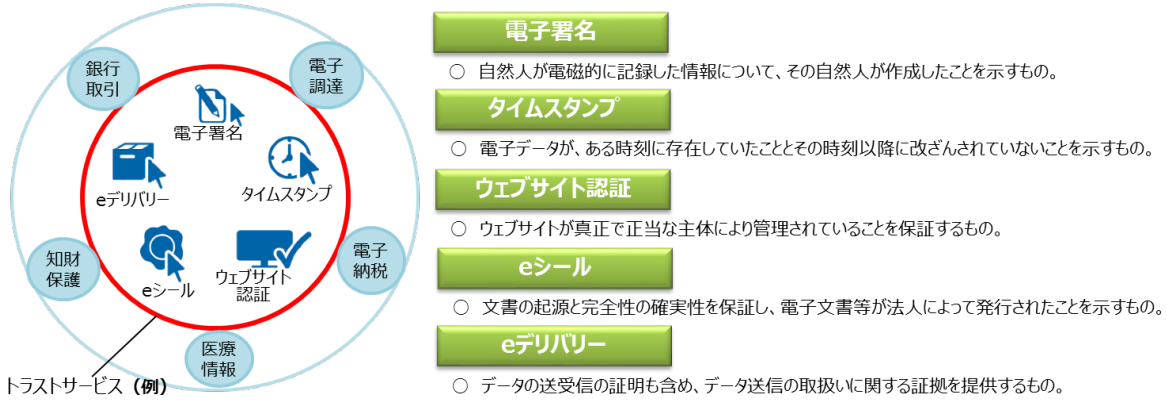


図 6 EU におけるトラストサービスのイメージ [17]

[16] EU 加盟国 28 カ国にアイスランド、リヒテンシュタイン、ノルウェーを加えた 31 カ国で構成される EEA(European Economic Area: 欧州経済領域)

[17] ENISA（European Network and Information Security Agency:欧州ネットワーク情報セキュリティ庁）公表資料をもとに総務省作成。
https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust

② EU のトラストサービスの動向

（ア） EU 全体

欧州については、㈱三菱総合研究所を通じ、フランス、ドイツ、イギリスにおけるトラストサービスの利用動向に関して調査を行った。

EU 全体でみると、トラストサービスプロバイダーは、eIDAS 規則発効以降増えており、金融、不動産、会計等の分野を中心に、本人確認（KYC）や契約手続きなどの場面で、電子署名などのトラストサービスの利用が進んでいる。

欧州委員会は、トラストサービスの利用が有効と期待されている分野・領域として、以下を例示している。

- ◆ 単一デジタルゲートウェイ（域内の各種行政手続きのオンライン窓口の一本化）
- ◆ KYC[18]（オンラインによる顧客確認）
- ◆ 偽情報・フェイクニュース対策
- ◆ GDPR[19]対応（属性、資格などの確認結果をやり取りする際のデータ最小化）

また、トラストサービスの利用を促すため、以下の各種制度・法律において、トラストサービスの利用が認められている。

- ◆ マネーロンダリング対策指令（5MLD（5th Money Laundering Directive））
- ◆ 改正決済サービス指令（PSD2（Payment Service Directive Ⅱ））
- ◆ 会社法指令（企業におけるデジタルツール・プロセスの利用に向けて改正）
- ◆ AVMS 指令 [20]（マイノリティ保護、年齢認証、保護者同意）

その一方で、フランスのトラストサービスプロバイダー（Yousign、CDC ARKHINEO など）やフランスやドイツの政府機関（フランス：ANSSI（国家サイバーセキュリティ庁）、ドイツ：連邦ネットワーク庁（BNetzA））へのインタビューによれば、トラストサービスの更なる普及に向けた課題として、トラストサービス及びその利用のメリット等に対する利用者の認知度が低いこと、トラストサービスの提供コストが比較的高いこと、従来の慣習等を変更してトラストサービスを導入する心理的障害が存在すること等を指摘する声がある。

今後、欧州委員会は、eIDAS 規則第 49 条に基づき、2020 年7月1日までに eIDAS 規則のレビュー及び議会への報告を行うこととなっている。各国レベルでは、トラストサービスの普及・促進は、直接的には事業者の活動や市場に委ねる傾向にあるが、今後、個別の業法等でトラストサービスの利用が推奨されることで、普及が促進される可能性がある。

---

[18] KYC とは Know your customer の略であり、顧客本人の確認における書類手続の総称を指す。

[19] General Data Protection Regulation（一般データ保護規則）の略で、EU における個人データの保護について規定している。

[20] Audiovisual Media Service Directive（視聴覚メディア・サービス指令）の略で、EU における視聴覚コンテンツやサービス（例：放送やオンライン配信等）に関する規定を定めている。

このように、EU はトラストサービスの制度的枠組みの整備で先行していることから、我が国としても、今後の国際的なデータ流通の進展に合わせて、日 EU ICT 政策対話・戦略ワークショップ等の場を通じて、EU との相互運用を検討することが求められる[21]。

（イ） フランス、ドイツ、イギリス

各国におけるトラストサービスの普及状況を見てみると、国により事情が異なっている。

i. フランス

フランス国内には、適格 TSP が総数で 23 社ある（表 1）。

表 1 フランス国内の TSP 内訳（2019 年 10 月9日時点）

総数	**23 社（QTSP:23 社）**
電子署名	15 社（QTSP:15 社）
e シール	8社（QTSP:8社）
タイムスタンプ	9社（QTSP:9社）
e デリバリー	6社（QTSP:6社）
Web 認証	3社（QTSP:3社）

銀行・保険などの金融業界、不動産業界などで、主に KYC（オンラインでの顧客確認）や契約・行政手続（公共調達・入札等）等の場面において、電子署名やタイムスタンプ等の利用が他国と比べて進んでいる。

セキュリティやトレーサビリティの確保、コンプライアンス対応へのニーズが高まっていることから、今後は、トラストサービスの利用が増加すると考えられており、不動産、弁護士・会計士事務所など多くの書類を扱う分野での利用が期待されている。

また、フランスでは、公証人が日常的に書留を送っており、物理的な書留と比べ、受信者の受領証明が担保できる（送達とその記録が確実に行える等）観点から、e デリバリーの利用が拡大傾向にある。e デリバリーは公証人以外にも、契約書等の文書を送付するため、不動産等の分野でも、その利用が広がっているとの調査がある。

他方、フランスのトラストサービスプロバイダー（Yousign、CDC ARKHINEO、AR24、Clearbus）やフランスの政府機関（ANSSI（国家サイバーセキュリティ庁）へのインタビューによれば、利用者側におけるトラストサービスやそのメリットに対する認知度がまだ低いこと、導入等に伴う既存の業務フローや慣習を変更することに対する心理的なハードルが存在すること、個人宛の e デリバリーでは、事前に受領者の合意を得る必要があり（B2B では不要）、それが利用促進の妨げとなっていること、などが課題として挙げられる。

ii. ドイツ

ドイツ国内には、総数 12 社の TSP、うち 11 社が適格 TSP である（表 2）。

[21] 直近では、2019 年 10 月に、欧州委員会の通信ネットワーク・コンテンツ・技術総局(DG CONNECT)、駐日欧州連合代表部と総務省にてテレビ会議を行った。

表 2 ドイツ国内の TSP 内訳（2019 年 10 月９日時点）

総数	12 社（QTSP:11 社）
電子署名	8社（QTSP:7社）
e シール	3社（QTSP:2社）
タイムスタンプ	6社（QTSP:5社）
e デリバリー	2社（QTSP:2社）
Web 認証	2社（QTSP:2社）

従来の国内基準が eIDAS 規則よりも厳しかったところ、eIDAS 規則によって EU レベルの基準が明確になったため、今後は、金融、年金などの社会保障分野、特許などの知的財産権関連、税務、産業廃棄物関連などでの利用が期待されている。また、住民票の取得や外国人の滞在許可など市民のオンライン行政手続も有望分野とみられている。

他方、課題として、政府（ドイツ連邦ネットワーク庁：BNetzA）関係者より、

- 需要がまだ貧弱であること（トラストサービスを利用できる場面が限られ、利用しようとする者が少ない）
- 供給が限定的であること（実際にトラストサービスを提供している事業者が少ない）
- トラストサービスの提供コストが比較的高いこと
- eIDAS 規則で定めているセキュリティ基準（暗号アルゴリズム）の幅が広く、相互運用性のためにどのアルゴリズムをサポートするべきかについて、実装上の困難があること

等が指摘されており、トラストサービスの利用状況はいまだ発展途上段階であり、トラストサービス普及に伴う実質的な効果が出てくるのはこれからとみられている。

ドイツ政府としては、今後の普及・促進に向け、市場モニタリングの実施や、トラストサービスの相互運用性等の観点から、セキュリティ基準を満たす適格な暗号アルゴリズムのリストの提供を検討している。

iii. イギリス

イギリス国内には、総数 11 社の TSP があるが、適格 TSP は0社となっており、（表 3）、フランスやドイツよりも、トラストサービスの利用が進んでいない。

表 3 イギリス国内の TSP 内訳（2019 年 10 月9日時点）

総数		11 社（QTSP:0 社 [22]）
	電子署名	8社 （電子署名と e シールの区分は確認できず）
	e シール	
	タイムスタンプ	2社
	e デリバリー	確認できず
	Web 認証	4社

トラストサービスプロバイダー（Experian）やデジタル・文化・メディア・スポーツ省（DCMS）、民間の事業者団体である tScheme から、課題として、

- ◆ トラストサービスの需要が他国と比較すると小さい
- ◆ トラストサービスの提供コストが比較的高く、それに伴う便益も低く見られる傾向にある（トラストサービスのメリットと理解の促進がまだ必要）
- ◆ 法律などで強制しないと、国内での利用は急速には進まない

といったことが指摘されている。

現状、政府機関による市場モニタリングは実施しておらず、トラストサービスプロバイダー（TSP）リストについては、民間の事業者団体である tScheme が認定し、整備している。なお、民間認定ではあるが、国内のトラストリストとして、一定の信頼性があるものとして認められている [23]。

（2） 米国

トラストサービスについて、米国では、電子署名法が連邦法及び州法として制定されているが、タイムスタンプや e シールに関する包括的な法律は確認されていない。他方、例えば、ヘルスケアなどの個別分野では、タイムスタンプの使用を求めている場合があるとされている。

電子署名の技術基準等は NIST（アメリカ国立標準技術研究所）が作成しているが、連邦政府による電子署名サービス提供者の認定・認証等が行われていることは確認されていな

[22] 国内独自の認定制度 Verify があるため、適格 TSP（QTSP）の認定が進んでいない。

[23] なお、eIDAS の適格 TSP 認定は、認定機関である UK Accreditation Service(UKAS)から認定された後で、情報コミッショナーオフィス（ICO）の審査を受けることとされている。仏、独は政府が認定している。

い。民間企業である Microsoft や Google 等のブラウザベンダ [24]や、Adobe[25]が独自のトラストリストを作成しており、また州政府による電子署名サービス提供者に対する認可 [26]などが行われている。

米国の電子署名市場は 2 億 3070 万ドル（約 251 億円)とされ [27]、電子署名の主な利用分野としては、会計・法律、金融・保険、不動産、政府（調達プロセス等）、教育（学生管理、研究助成等）、テレコム・メディア、ヘルスケア（医療記録などの管理）[28]が挙げられる。

（3） 中国

中国では、トラストサービスに関する法制度として「中華人民共和国電子署名法」（以下「電子署名法」という。）が施行されており、その中で、タイムスタンプの法的効力についても規定されているが、e シールを含む包括的な法律は確認されていない。同法第 17 条で定められた、人員、事業資産、国家標準への準拠、その他の要件に基づき、政府が電子署名事業者の審査・管理を行い、署名の有効性について、確認・保証することになっている。

「電子署名法」は 2005 年に施行され、電子署名行為の法的効力を認め [29]、政府による認可や電子署名事業者の法的責任等も規定している。2019 年には、不動産の権利などの譲渡も対象に含めるよう、電子署名の利用範囲を拡大する改正がなされ、電子署名の市場規模は拡大し、サービスプラットフォーマーも増加傾向にある（図 7）。

---

24 主要なブラウザベンダは、WebTrust for CA（電子証明書発行機関としての適格性について、米国公認会計士協会及びカナダ勅許会計士協会によって共同開発された電子商取引認証局監査プログラム）により認定された認証局を信頼されたルート認証機関としてブラウザ内のリストに格納している。

25 電子文書が法的要件に準拠した信頼できるものであることを確認するためには、文書に付された電子署名を検証することが必要となる。電子署名を行った者のデジタル証明書を予め認定し、Adobe Approved Trust List (AATL)としてリスト化することで、文書の信頼性確認をスムーズに行えるようにしている。このリストには、eIDAS で認定された信頼あるプロバイダーのリストや Web Trust の認証局リストなど、機械可読なリストも含まれている。

26 カリフォルニア州政府は、カリフォルニア州の公的機関との間での電子署名の証明書発行が認可された認証局のリストを公開している。

27 P&S Intelligence 社”U.S. Digital Signature Market”による。

28 HIPAA（医療保険の携行性と責任に関する法律）によって、保険情報などの授受・管理において、電子署名やタイムスタンプの利用を要求している。

29 次の場面を除いて有効とされる：①婚姻、養子、継承人など対人関係に関連すること、②水道、ガス、熱の停止など公共サービスに関すること、③法律、行政法規の定めた電子署名が適さない文書、④土地、敷地、またはその他の不動産の権利または利益の譲渡を伴うもの。

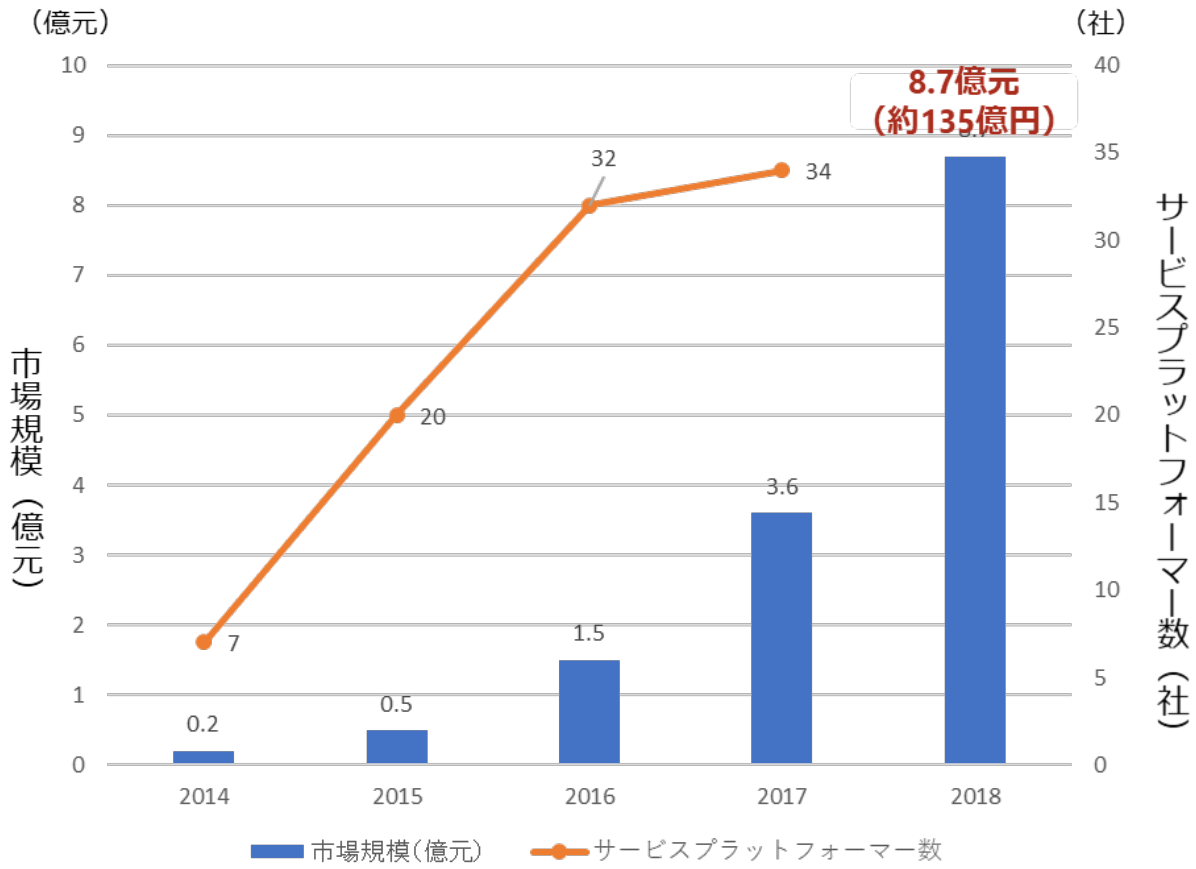


図 7　電子署名の市場規模とサービスプラットフォーマー数の推移 [30]

電子認証サービスの提供事業者は、電子署名法第 18 条に基づき、国務院情報産業主管部門（工業信息化部）の認可を取得すれば、電子認証サービス [31]を提供することが可能である。タイムスタンプサービスを提供する事業者としては、中国国家授時センター（NTSC）と北京聯合信任技術サービス有限公司との合弁により聯合信任タイムスタンプサービスセンター（TSA）がある。

[30] 市場規模及びサービスプラットフォーマー数は「2019-2025 年中国第三方电子签名行业市场需求预测及投资未来发展趋势报告」（2019-2025 中国サードパーティ電子署名業界の市場規模予測及び将来の投資動向レポート）に基づき作成。

[31] タイムスタンプ及びその提供事業者について、中国の法律には明白な規定がなく、「電子署名法」第 18 条に規定された「電子認証サービスの提供者」とは、電子署名及びタイムスタンプの法的効力を証明する第三者のプロバイダーであり、電子署名を認証する際、その署名とともにタイムスタンプが付随してなされることがある、との海外調査がある。また、タイムスタンプ事業者は、電子認証サービスの提供者に含まれるのではないか、という指摘がシンクタンクよりなされている。

第2章　　論点と取組の方向性

2．1　総論

（1）本取りまとめにおける主な検討事項

第1章で見たとおり、トラストサービスは、その普及により Society5.0 時代における社会全体のデジタル化を推進することが期待されるため、我が国においてもその普及を推進することが重要であるが、現時点で広く普及しているとは言い難い状況である。

第1章で紹介した国内企業のアンケート調査結果や諸外国の動向を踏まえると、トラストサービスの普及促進のためには、公的な枠組みによってその信頼性を確保することや利用者が安心して利用できる環境を整備することが有効と考えられることから、我が国においても、そのような措置を含め、トラストサービスの普及促進のために国として措置を講ずることが重要である。

本ワーキンググループは、トラストサービスの普及に向け、トラストサービス全般の在り方を検討事項とするものであるが、各サービスの普及促進のために必要な措置の具体的な在り方を検討するに当たっては、各サービスの発展段階に応じた検討が必要となることから、原則として個別のサービスごとに検討し、必要に応じて各サービスに横断的な要素を検討することが適当であると考えられる。そこで本取りまとめにおいては、一定のサービス提供の実態又は具体的なニーズの見込みがあり、利用者がより安心して利用できる環境の構築に向けた課題が顕在化しているタイムスタンプ、e シール及びリモート署名に関する制度の在り方について主に検討する。

詳細は2．2各論において述べるが、タイムスタンプ及び e シールについては、ユーザ企業側の意向を確認するためのヒアリングやアンケート調査の結果も踏まえ、次の論点を中心に整理を行う。

(a) 信頼性の基点としてタイムスタンプ発行事業者や e シールの認証局の信頼性をどう確保するか。
(b) タイムスタンプや e シールの利用が電子文書の送受信・保存について規定している法令との関係において、有効な手段として認められるか。

EUにおいてeIDAS規則の導入のみでは大きな変化は見られなかったことに鑑みても、信頼性確保の取組だけでなく、業法等の個別の法令との関係でトラストサービスの利用が有効と認められることがその普及に有効と考えられることから、(a)及び(b)を両輪として検討することが重要である。

また、リモート署名については、日本トラストテクノロジー協議会（JT2A）におけるガイドラインの検討が行われているところであり、まずはこのような民間団体の取組を尊重し、JT2A のガイドラインの検討状況を踏まえ、現行の電子署名法及び認証業務の認定制度

を前提に、リモート署名を電子署名法制度上どのように位置づけることができるか、その前提として、関係者によるどのような取組が必要かという論点を中心に整理を行う。

（２）トラストサービスの信頼性確保に関する基本的な考え方

上記（１）において論点(a)として掲げたトラストサービスの信頼性確保に関して、各サービスに共通する基本的な考え方は以下のとおりである。

電子的なやり取りにおける信頼性を確保する仕組みであるトラストサービスを利用することにより、利用者が安心して電子契約やデータの利活用を行えるようにするためには、トラストサービスそれ自体が信頼の置けるサービスであること及び利用者がそのようなサービスを適切に選択可能とすることが必要である。

そのためには、トラストサービスにおける信頼の基点となるサービス・事業者が、信頼の置けるものであることを利用者が容易に判別できるようにすることが重要である。具体的には、当事者間の自己申告のみに基づき利用者が信頼性を判断することは容易でないため、信頼の置けるサービス・事業者に求められる客観的な基準が策定・公表されるとともに、あるサービス・事業者の当該基準への適合性を第三者が審査・評価・認定し、その結果を利用者に情報提供する仕組みが重要である。

基準や認定の仕組みの整備・運用を行う主体については、各サービスの利用者のニーズやユースケース、技術開発やサービス展開の動向等を踏まえ、サービスの円滑な提供を確保しつつ、利用者が信頼を置けるサービスとするために必要かつ十分なものとすることが求められ、特に国際的な通用性が重要と考えられるサービス（例：タイムスタンプ）については、国の関与により信頼性を担保することがより重要と考えられる。

我が国のトラストサービスの信頼性を確保するための方策の検討は、各サービスの状況を踏まえつつ、これらの基本的な考え方を念頭に置いて行うことが適当である。

（３）検討の視点

① トラストサービスの信頼性確保に関する検討の視点

上記（２）の基本的な考え方を踏まえると、トラストサービスの信頼性確保のための仕組みの検討に当たって留意すべき点として以下の４点が挙げられる。

（ア） トラストサービス提供事業者への評価・認定体制の構築

信頼の置けるサービス・事業者を利用者が容易に判別できるよう、信頼の置けるサービス・事業者に求められる客観的な基準が策定・公表されるとともに、あるサービス・事業者の当該基準への適合性を第三者が評価・認定する体制を構築することが重要である。

（イ） 一定の要件を満たすトラストサービスの機械可読な形での公表

信頼の置けるサービス・事業者を利用者が容易に判別できるよう、第三者による審査・評価・認定の結果を、例えば認定事業者の一覧表といった形で国等の公的機関が公表することで、利用者に情報提供する仕組みが重要である。その際、利便性の観点からは、EU におけるトラストリスト[32]のように、各サービスの認定サービス・事業者を横断的に一覧でき、かつ、データを自動処理できる機械可読な形で公表することが有用である。

（ウ） トラストサービスに関する技術基準の整備・維持

トラストサービスの信頼性確保のためには、用いられている技術が最新の動向を踏まえた適切な水準に維持されることが重要である。そのため、信頼性確保の仕組みの構築に当たっては、技術基準を整備・維持する体制を官民の協力の下で整備することが重要である。

（エ） 国際的な通用性

特に海外における通用性が重要と考えられるサービス（例：タイムスタンプ）については、EU の eIDAS 規則等の海外の制度との相互運用等、国際的な通用性の確保を図ることが重要である。このため、国の関与により信頼性を担保し、国際連携・調整を進めていくことが求められる。

② その他の検討の視点

アンケート調査において、トラストサービスの導入に当たってコストや手間が課題との意見が多かったことを踏まえると、トラストサービスの導入コストの削減及び利便性の向上など、以下の取組が求められると考えられる。

（ア） トラストサービス提供事業者やその利用者にとって過度なコスト負担や不便を強いることのない制度、仕組みの構築

（イ） トラストサービス提供事業者のサービス提供の効率化等による価格低廉化

（ウ） 業界全体による利用者目線での創意工夫

具体的には、例えば利用者の手間を軽減するための取組や各サービスをまとめる形での横断的なサービスの提供、利用者が提供事業者によらずトラストサービスを横断的に利用するための共通 API の導入等が考えられる。

その他、トラストサービスの実現に当たっては、機密性、完全性とともに、利用者が簡便に利用できるような可用性を含めた情報セキュリティの三要素を確保する必要があることや、プライバシー・バイ・デザインにも配慮する必要がある。

[32] Trusted List。eIDAS に基づく適格トラストサービス提供事業者の一覧表。eIDAS において、自動処理に適した形で作成、維持及び公表することとされている。

2.2 各論

以下、各トラストサービスごとに論点と取組の方向性を検討する。

（1）タイムスタンプ

① 現状・課題

国税関係書類の保存など一部の分野においてはタイムスタンプの利用が進み、文書の電子的な保存が進んでいる一方、例えば建築士の設計図書は電子的に作成するが保存のためだけに紙で印刷している等、タイムスタンプが利用されず、保存の段階まで電子化が貫徹されていない例が見られる。

このため、国税関係書類以外の分野でタイムスタンプの普及が進んでいない原因を分析した上で、タイムスタンプの利用を社会全体に広げるための制度の在り方について、検討を行った。

② 論点

タイムスタンプの制度の在り方に関する論点としては、以下の2つが挙げられる（図 8）。

論点(a) 信頼性の基点として信頼性をどう担保するか。

論点(b) タイムスタンプの利用が電子文書の送受信・保存について規定している法令との関係において有効な手段として認められるか。

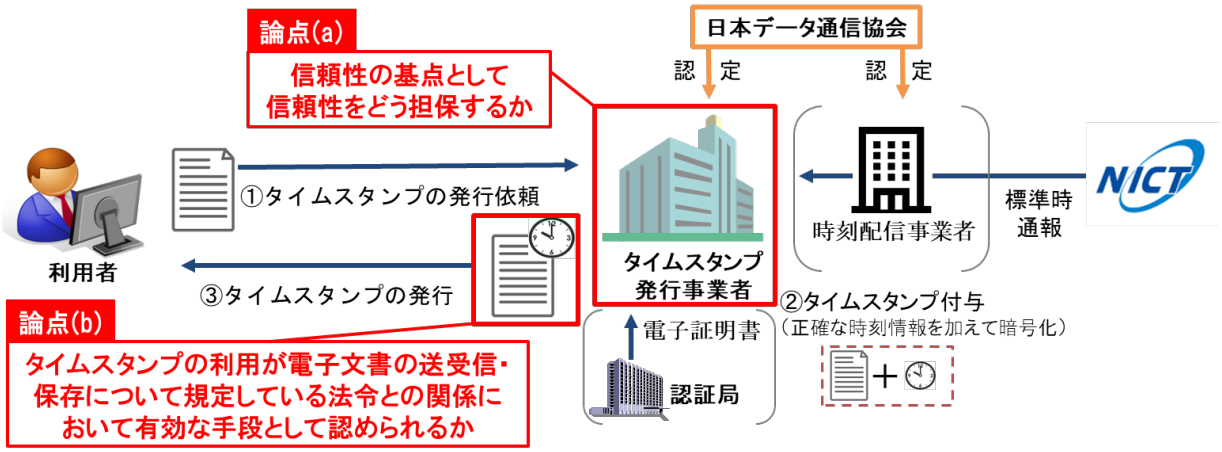


図 8 タイムスタンプの制度の在り方に関する論点

③ 取組の方向性（論点(a)関係）

タイムスタンプの利用者等に対して更なるヒアリング及びアンケート調査を実施したところ、タイムスタンプの利用に関する課題として寄せられた主な意見は以下のとおりである。

（ヒアリングで寄せられた主な意見）

- 民間の認定制度のタイムスタンプでは、その永続性に不安がある。国としての認定制度があればその不安が解消され、長期保存におけるデータの電子化の進展が期待される。タイムスタンプは電子取引の基盤となるインフラであり、その信頼性を国が担保しないと、長期間安心して利用することができない。
- タイムスタンプに関する制度が国の制度ではないため、制度への認知度が高くなく導入の必要性の検討に苦労している。
- 民間の認定制度のタイムスタンプでは、その証拠性に不安がある。国としての認定制度があれば、特に海外事業者とのやりとりにおける契約の迅速化が期待される。

（アンケートで寄せられた主な意見）

- 送受信の場面でタイムスタンプを使用している9社のうち4社、保存の場面でタイムスタンプを使用している 11 社のうち5社、送受信の場面でタイムスタンプの導入検討後、断念した5社のうち4社及び保存の場面でタイムスタンプの導入検討後、断念した7社のうち4社が「サービスが将来にわたっても提供されるか不安」であることを課題と感じている。
- 保存の場面でタイムスタンプの導入検討後、断念した7社のうち3社が「法制度が存在しない、法令上の保存義務を満たすものであるかが不安」であることを課題と感じている。

これらを踏まえると、利用者が安心してタイムスタンプを利用可能とし、電子文書の信頼性を高め、電子化を進めるためには、電子署名に係る認証業務のように国が何らか関与することでその信頼性に裏付けを与えることが重要である。

第三者による認定の仕組みを備えた国の関与としては以下の手法が考えられるところ、それぞれについて表 4 のようなメリット・課題が想定される。

表 4　タイムスタンプにおける国による認定と国による基準の提示のメリットと課題

	①　国による認定	②　国による基準の提示
概要	国による優良事業者の認定制度を創設	国が信頼の置けるサービス・事業者に求められる技術上・運用上の基準を提示（認定は民間による枠組み）
例	＜個別法に基づくもの＞ ・認定認証業務 ・認定電子委任状取扱業務 ＜個別法に基づかないもの＞ ・大気環境配慮型 SS（サービスステーション）認定 ・第四次産業革命スキル習得講座認定 ・健康増進施設認定	・情報銀行（一般社団法人日本 IT 団体連盟） ・タイムスタンプ（一般財団法人日本データ通信協会） ※総務省がタイムスタンプに求められる大まかな要件を定めた「指針」を提示。
メリット	・国の関与が明確 ・認定事業者を騙る事業者を処罰可能（個別法に基づく場合）	技術革新に応じた制度の柔軟な改善が可能
課題	個別法で措置する場合には、紙媒体において相当する概念がない中でタイムスタンプに特別な法的位置づけを与えることの整合性	・国による関与の度合いは①に比べて弱い ・国際的な相互運用性の観点から十分といえるか ・認定制度の永続性に不安がある

タイムスタンプについては、技術やサービス内容が確立されており、日本データ通信協会による認定制度も14年間運用されてきたが、国による信頼性の裏付けがないことや国際的な通用性への懸念が更なる普及を妨げている要因の一つであると考えられ、より信頼性の高い措置を講ずる必要があると考えられる。

したがって、タイムスタンプの更なる普及に向け、その信頼性を一層担保することが適当であり、具体的には、国が信頼の置けるサービス・事業者を認定する仕組みを設けることが適当である。

このような仕組みを設けることは、上記2．1（3）①の留意点のうち「（ア） トラストサービス提供事業者への評価・認定体制の構築」及び「（エ） 国際的な通用性」に照らして妥当と考えられる。

なお、一定の基準を満たすサービス・事業者を国が認定する仕組みを構築する際に新たな立法によらず実施している例も複数あることから、そのような仕組みにより対応することが可能と考えられる。

また、今後、以下の事項について検討することが必要である。

- 上記2．1（3）①の留意点のうち「（イ） 一定の要件を満たすトラストサービスの機械可読な形での公表」に照らし、国による認定を受けたサービス・事業者を機械可読な形で公表する手法
- 上記2．1（3）①の留意点のうち「（ウ） トラストサービスに関する技術基準の整備・維持」に照らし、認定の仕組みの運用開始後における技術基準のメンテナンスを行う体制
- タイムスタンプ発行事業者に対して時刻情報の配信及び時刻精度の計測等の監査を行う時刻配信事業者の扱い
- タイムスタンプ発行事業者やその利用する認証局が廃止される際の対応

- 審査・評価実務を国に代わって実施する機関の在り方

④ 取組の方向性（論点(b)関係）

ヒアリング及びアンケート調査においては、タイムスタンプのような仕組みを用いて電子的な保存を行うに当たっての課題として、一定の文書の保存に関する法令上の要件との関係が挙げられた。

（ヒアリングで寄せられた主な意見）

- 様々な電子署名（認定認証、特定認証、電子サイン等）とタイムスタンプのどのような組み合わせにより、適法性が担保されるかの指針を明示してほしい。
- 仮にタイムスタンプに対する正当性に疑義が生じた場合に、保存義務等の法令を遵守していると主張できるのか。

（アンケートで寄せられた主な意見）

- 送受信の場面でタイムスタンプの導入検討後、断念した5社のうち4社が「法令上認められる送付時の要件を満たすものか不明確」であることを課題と感じている。
- 保存の場面でタイムスタンプの導入検討後、断念した7社のうち3社が「法制度が存在しない、法令上の保存義務を満たすものであるかが不安」であることを課題と感じている（再掲）。
- タイムスタンプを用いた保存に関して，他国との相互認証が課題である。

この点、電子帳簿保存法施行規則において日本データ通信協会の認定を受けた事業者が発行するタイムスタンプの使用が明示的に規定された国税分野においてタイムスタンプの利用が進んでいることを踏まえ、電子文書の送受信・保存について規定している法令を所管する省庁において、有効な手段として認められるタイムスタンプの要件をそれぞれの省令・告示等で具体的に規定するよう、所管省庁に働きかけることが有効である。

（2） e シール

① 現状・課題

ヒアリングやアンケート調査によれば、企業における文書の電子化については進展が見られるが、e シールについては広く利用されているとは言いがたい状況であり、また、電子化が行われていても紙で発行した文書をスキャナ等により電子化しただけという例も見られるところである。

（ヒアリングで述べられた現状）

- 現状の支払業務フローは、取引先（請求企業）からの請求書は紙又は PDF データで受領（社印の押印あり）、受領した請求書の内容を購買システムに手入力、証拠書類としての請求書原本は紙で保管。打鍵ミスや書類紛失等のリスクが内在。
- 取引先（支払企業・団体）への請求書は紙で提出（社印を押印）。全体の1／3が手渡し。同時に請求書データ（CSV ファイル）の提供を要請される例が増加しているが、請求書原本の提出は免除されない。

（アンケートで述べられた現状）

- 文書・データ等の送受信や保存の場面で、何らかの電子化を行っている社は 39 社中 36 社。
- e シールを使用している社は、送受信・保存いずれの場面でも 39 社中 7 社。

今後、Society 5.0 時代においてデータの利活用が一層活発化することや適格請求書等保存方式（インボイス制度）の導入により、大量の文書やデータを人手を介さずに自動的に処理することで業務を効率化するニーズが高まることが見込まれる。この点、アンケート調査においても、e シールを使用していない 29 社のうち、「適格請求書対応でコスト等が見合えば使用したい」と回答した社が 26 社に上った。

その際には、データの自動処理の前提として、データを信頼してやり取りできるよう、データの送信元がなりすまされていないか、データの内容が改ざんされていないかを確認可能とする仕組みが必要となる。e シールはこのような機能を有する仕組みであり、e シールの普及により、文書の電子化やデータの自動処理による生産性の大幅な向上が期待される。

このような状況を踏まえ、ユーザ企業側のニーズやユースケースを明確化した上で、どのような枠組みで e シールに係るサービスが提供されれば、利用者が安心して利用できるかについて、制度化も視野に入れて検討を行った。

② 論点

e シールの制度の在り方に関する論点としては、以下の2つが挙げられる（図 9）。

論点(a) 信頼性の基点として認証局が信頼の置けるものであるか。

論点(b) e シールの利用が電子文書の送受信・保存について規定している法令との関係で有効な手段として認められるか。

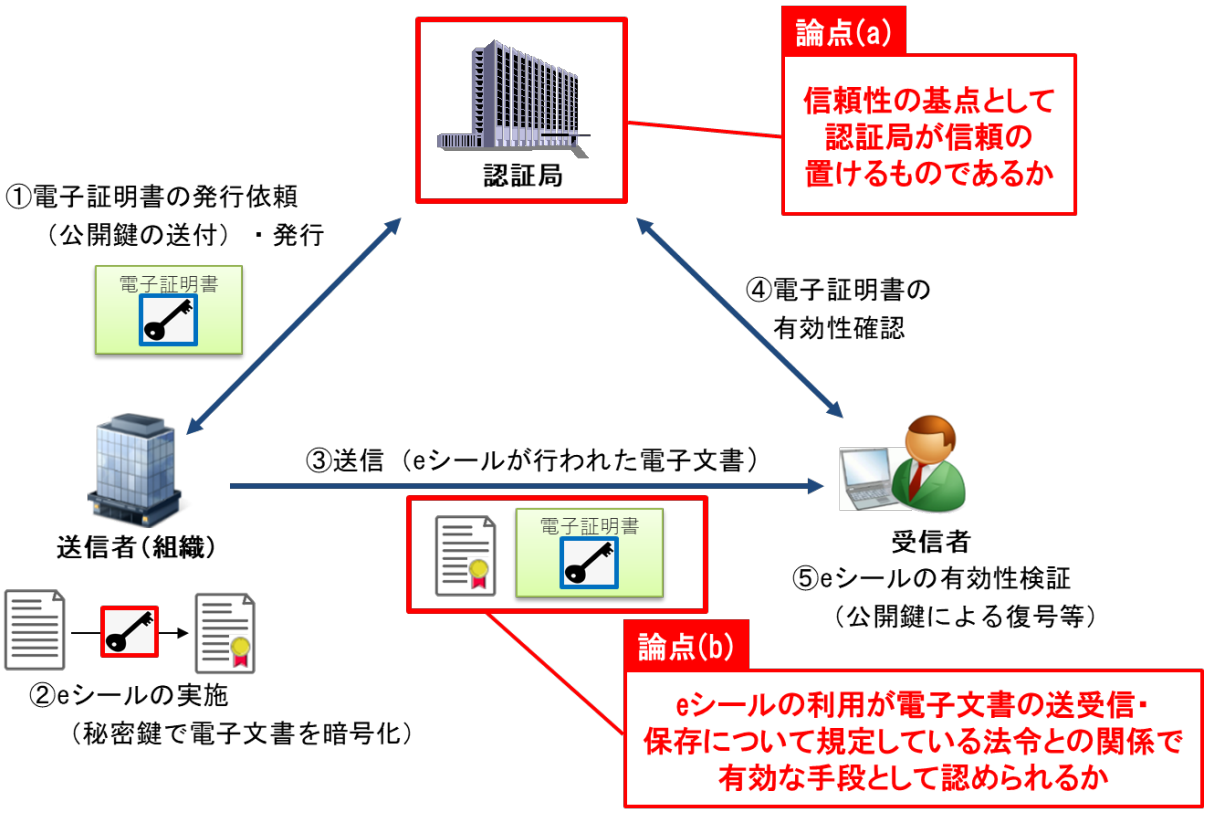


図 9　e シールの制度の在り方に関する論点

③　取組の方向性（論点(a)関係）

e シールの利用者等に対する更なるヒアリング及びアンケート調査を実施したところ、e シールの利用に関する課題として寄せられた主な意見は以下のとおりである。

（ヒアリングで寄せられた主な意見）

- 制度上の位置づけが存在しない場合、また民間の基準・認定制度しか存在しない場合は運用上の懸念があり普及しないため、今後普及が必要なトラストサービスについては公的な枠組みが必要。
- 適格請求書発行事業者の登録番号を属性とした e シールが制度化され、認定を受けた事業者の e シールを利用できることになれば、懸念を持つことなく、電子インボイスの真正性確保に e シールを用いることができるため、電子インボイスの利用が促進される。

（アンケートで寄せられた主な意見）

- e シールを使用している7社のうち3社が「法制度が存在しない」ことを課題と感じている（送受信・保存いずれの場面でも同様）。

これを踏まえると、e シールの導入・普及により、業務の効率化や生産性の向上が見込まれるところ、利用者が安心して e シールを利用可能とし、これを進めるためには、その信頼性に裏付けを与えることが重要である。

信頼性に裏付けを与えるためには、信頼の置けるサービス・事業者かどうかの判別を

利用者に委ねるのではなく、第三者が認定して利用者に情報提供する仕組みが必須である。

第三者による認定の仕組みを備えた国の関与としては以下の手法が考えられるところ、それぞれについて表 5 のようなメリット・課題が想定される。

表 5 e シールにおける国による認定と国による基準の提示のメリットと課題

	① 国による認定	② 国による基準の提示
概要	国による優良事業者の認定制度を創設	国が信頼の置けるサービス・事業者に求められる技術上・運用上の基準を提示（認定は民間による枠組み）
例	＜個別法に基づくもの＞ ・認定認証業務 ・認定電子委任状取扱業務 ＜個別法に基づかないもの＞ ・大気環境配慮型 SS（サービスステーション）認定 ・第四次産業革命スキル習得講座認定 ・健康増進施設認定	・情報銀行（一般社団法人日本 IT 団体連盟） ・タイムスタンプ（一般財団法人日本データ通信協会） ※総務省がタイムスタンプに求められる大まかな要件を定めた「指針」を提示。
メリット	・国の関与が明確 ・認定事業者を騙る事業者を処罰可能（個別法に基づく場合）	技術革新に応じた制度の柔軟な改善が可能
課題	・個別法で措置する場合には、紙媒体において相当する概念である社印・角印に法的位置づけがない中で e シールについて法的に位置づけることの整合性 ・サービスの内容が確立され広く提供されていない中で国の制度に位置づけることによる今後の技術開発・サービス展開への影響	・国による関与の度合いは①に比べて弱い ・国際的な相互運用性の観点から十分といえるか ・認定制度の永続性に不安がある

e シールについては、新しいサービスであることから、その導入が進むためには、利用者が安心して利用できるよう、信頼の置けるサービス・事業者に求められる技術上・運用上の基準の提示や、それを満たすサービス・事業者について利用者に情報提供する仕組みが重要である。

他方、現時点では e シールはサービス内容や提供するための技術などが確立されておらず、広く提供されていない状況であり、そのような中で国による認定制度に位置づけることで、今後の技術開発やサービス展開に影響を与える可能性が懸念される。

そのため、まずは、一定程度国が関与しつつも、基本的には民間の自主的な仕組みにより、e シールを提供するサービスの立上げやその導入が促進されるよう、信頼の置けるサービス・事業者を認定する民間の仕組みの創設に向け、信頼の置けるサービス・事業者に求められる技術上・運用上の基準や認定の仕組みに関する検討を進めることが適当である。

その上で、基準や認定の仕組みの運用状況、e シールの普及状況、国際的な相互運用の必要性等を踏まえ、基準や認定の仕組みの見直しや国のより強い関与の必要性を検討することが適当である。

このような仕組みを設けることは、上記2．1（3）①の留意点のうち「（ア） トラストサー

ビス提供事業者への評価・認定体制の構築」及び「(エ) 国際的な通用性」に照らして妥当と考えられる。

④ 取組の方向性(論点(b)関係)

また、e シールのような仕組みを用いて電子化を図るに当たっての課題として、一定の文書の発行や保存等に関する法令上の要件との関係が挙げられている。

(ヒアリングで寄せられた主な意見)

- 国において、基準に適合した e シールを利用した場合の法的効果(電子化に当たっての要件を定める法令への適合など)を制度化することにより、阻害要因の解消につなげていただきたい。
- 請求書以外でも長期間の保存・保管が必要な領収書などの国税関係書類、法人取引における各種書類においてもeシールの活用が期待される。法令への適合性が明確化されるよう制度化に期待。

(アンケートで寄せられた主な意見)

- 保存の場面で e シールを使用している7社のうち3社が「法令上認められる保存義務の要件を満たすものか不明確」であることを課題と感じている。
- 送受信の場面で e シールの導入検討後、断念した5社のうち4社が「法令上認められる送付時の要件を満たすものか不明確」であることを課題と感じている。

この点、電子文書の送受信・保存について規定している法令を所管する省庁において、有効な手段として認められる e シールの要件をそれぞれの省令・告示等で具体的に規定するよう、e シールのサービスの提供状況や認定の仕組みの検討状況を踏まえつつ、所管省庁に働きかけることが有効である。

⑤ その他

今後、e シールに関する上記の取組を進めるに当たっては、以下の検討事項等に留意することが適当である。

- e シールについては、電子署名やタイムスタンプと異なり、サービスの内容が確立されておらず、広く提供されていない状況であるところ、国の関与について検討するに当たり、例えば e シールの対象となる「組織」の範囲をどう考えるか等、その外延を定めるために引き続き検討が必要な課題が存在する。
- 制度設計に際しては、今後、以下の事項について検討することが必要である。
  - 上記2．1(3)①の留意点のうち「(イ) 一定の要件を満たすトラストサービスの機械可読な形での公表」に照らし、認定を受けたサービス・事業者を機械可読な形で公表する手法
  - 上記2．1(3)①の留意点のうち「(ウ) トラストサービスに関する技術基準の整備・維持」に照らし、認定の仕組みの運用開始後における技術基準のメンテナンスを行う体制

- その際、e シールとタイムスタンプを組み合わせた長期署名類似のサービスが想定され、そのようなサービスの信頼性を確保するという観点にも配慮が必要である。
- また、e シールは使い方も含めてまだ浸透していないサービスであり、想定される用途やユースケースを整理して利用者に周知することが必要である。

（3）リモート署名

① 現状・課題

電子契約サービス等において、リモート署名の利用拡大が期待されるところ、リモート署名は利便性を向上させる一方で、どのような要件を満たせば「本人による電子署名」（電子署名法第3条）だと法的に評価できるのか、制度的な整理が明確ではない。

「本人による電子署名」だと法的に評価できるためには、少なくとも、その電子署名が本人の意思に基づいて生成されたことの保証が必要である。このため、リモート環境へのアクセス方法等について、本人以外には本人の電子署名を生成できないといえるだけの技術的要件を明確化する必要がある。この点については、経済産業省の平成 27 年度及び平成 28 年度電子署名法研究会においても検討が行われ、そこでの議論を踏まえ、現在、日本トラストテクノロジー協議会（JT2A）により、EU 及び米国におけるリモート署名関連の標準を参照しながら、リモート署名の技術的要件に関するガイドラインの策定に向けた作業が行われているところである。

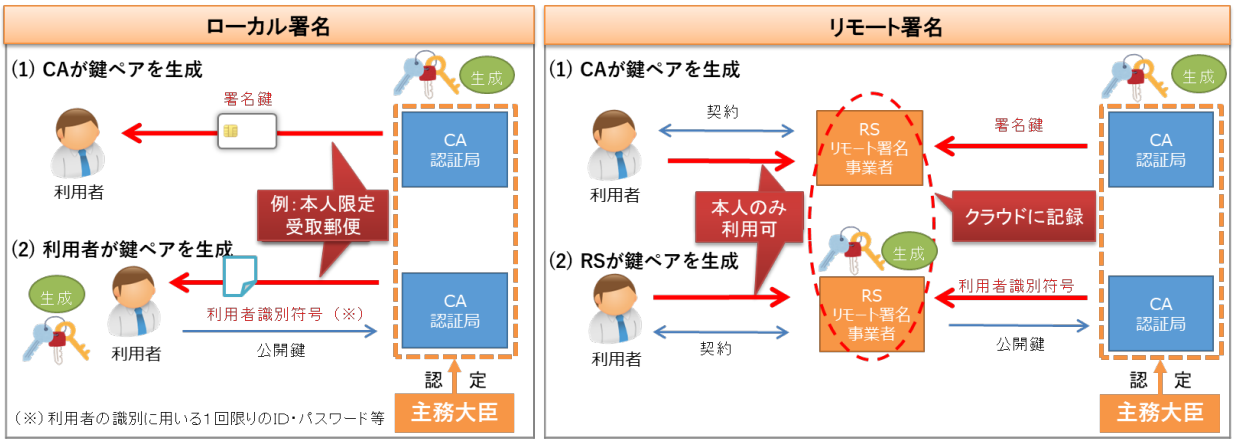
＜検討中の JT2A「リモート署名ガイドライン（案）」の主な内容＞[33]
- リモート署名事業者に求められるセキュリティ要件を①一般的セキュリティ要件、②署名活性化モジュールのセキュリティ要件及び③署名値生成モジュールのセキュリティ要件に分類。
- いずれの要件についても、リモート署名事業者が共通で対策すべき内容のほか、一部（署名鍵の活性化、インポート及び生成）については最低限・推奨・附帯という3段階の措置を定義。
- 「推奨」レベルでは、署名鍵の生成及び保管は HSM（Hardware Security Module。耐タンパ性を有する頑強なモジュール。）に限定。
- 「推奨」レベルでは、署名鍵の活性化には複数要素認証を必須化。
- また、建物内の各エリアにおける入退室管理等の物理的セキュリティの要件を規定。

このような、電子署名法研究会での議論を踏まえて JT2A において検討が進められている経緯を踏まえ、JT2A によるガイドラインの策定を前提に、リモート署名の電子署名法上の扱いについて検討を行った。

[33] 詳細は参考3を参照。

② 論点

リモート署名においては、現状行われている電子署名のやり方（ローカル署名（署名鍵を IC カード等に格納して利用者の手元で管理する方式の電子署名））と比べて、以下の図 10 のとおり、認証局との間の署名鍵又は公開鍵の受渡しを利用者に代わってリモート署名事業者が行うという違いがある。



署名鍵や利用者識別符号を「**安全かつ確実に利用者に渡すことができる方法**」により交付

リモート署名においては、署名鍵や利用者識別符号を利用者が委託する事業者（RS）のサーバに記録することにより行われる。

図 10 リモート署名のイメージ

このような違いを踏まえ、リモート署名の制度の在り方に関しては、認証業務を電子署名に関する信頼性の基点としている現行の電子署名法及び認証業務の認定制度を前提に、リモート署名を電子署名法制度上どのように位置づけることができるか、また、その前提として、今後、関係者によるどのような取組が必要かが論点として挙げられる。

③ 取組の方向性

まず、JT2A におけるガイドラインの現在の検討状況を踏まえると、JT2A においては、ガイドラインの策定・公表に向けた検討作業を継続する場合には、特に以下の事項に留意することが適当である。

- 利用者やリモート署名サービスを提供する事業者（以下、リモート署名事業者という。）にとってもわかりやすいものとなるよう、ガイドラインが前提とするリモート署名の仕組みやガイドラインの対象範囲、専門用語についての解説を充実させること
- 事業者がガイドラインに適合するかどうかの評価を外部から行いやすくなるよう、具体的な要求事項を単なる規格や標準のような形よりも詳細かつわかりやすく提示すること

また、信頼の置けるリモート署名サービスの普及に向け、ガイドラインに適合するリモート署名事業者を利用者が容易に判別可能となるよう、ガイドラインが民間において策定されることを踏まえ、当該事業者のガイドラインへの適合性評価を適切な第三者が行う

民間の自主的な仕組みを設けることが有用である。

その上で、利用者が本人による電子署名として利用可能な信頼できるサービスを利用できるようにし、利用者によるリモート署名の円滑な利用を図るため、JT2A のガイドラインの策定・公表や自主的な適合性評価の仕組みの整備を受け、リモート署名の電子署名法上の位置づけについて、主務省[34]において以下の取組を進めながら検討することが適当である。

- JT2A により策定されるリモート署名に関する技術的なガイドライン等の内容の精査
- 当該ガイドライン及び適合性評価の仕組みの運用状況のモニタリング
- 当該ガイドライン及び適合性評価の仕組みやそれらの運用状況を踏まえ、リモート署名の電子署名法第3条の規定による真正成立の推定効の適用の可否及び同法第6条に規定する認証業務の認定基準との関係の整理に関する検討

（４）その他のトラストサービス

① ウェブサイト認証

(ア) 課題

CA／ブラウザフォーラムはルート証明書の発行・管理を行う認証局に求められる要件等に関するガイドラインを策定しており、ブラウザベンダは認証事業者に対して、セキュリティ確保の観点に基づいた運用体制や証明書発行に係る技術的な要件等を要求しており、認証事業者は一方的に求められるそれらの要求に随時対応しなければならず、利用者にとっても短期間で証明書を切り替える必要があるなど、各種コストを要している。

また、法人名の日本語表記は海外の人には読めない、登記簿には英字表記は存在しないなど、日本独自の仕様が CA／ブラウザフォーラムに認められないことがある。そのため、日本の事情を十分に説明し、理解を求めていくことが必要である。

(イ) 取組の方向性

ウェブサイト認証については、CA／ブラウザフォーラムが定める基準に基づき、世界各国で普及しているが、CA／ブラウザフォーラムが定める要件への対応について、政府や関連団体等が連携し、日本固有の事情に応じた必要な対策をトラストサービス推進フォーラム（TSF）などにおいて検討・整理・集約した上で、CA／ブラウザフォーラムの運営に積極的に参画している EU の活動を参考にしつつ、CA／ブラウザフォーラムのガバナンスに戦略的に関与していくことが必要である。

② IoT 機器等のモノの正当性を確認できる仕組み等

(ア) 課題

データを発する IoT 機器等のモノの正当性を確認する仕組みについては、センサー等の小さな IoT 機器（チップ）に PKI の仕組みを導入することには機能的な制約があるほか、PKI

[34] 総務省、法務省及び経済産業省。

の仕組みを IoT 機器に導入するに当たってのコストも踏まえ、費用対効果の観点からも対象とする機器についての検討が必要である。

また、モノの認証については、ヒトや組織の認証と違い、様々な単位（機器ごとか、製造ロットごとか等）で行うことが考えられ、それぞれの利用実態に応じて柔軟に対応できる仕組みとすることが求められる。

さらに、IoT 機器の廃棄に関して、データの出所を後で追跡や検証する際には、漏洩した鍵で不正に署名されたものでないことを確認できることが必要となるため、廃棄の際の鍵の扱いなどについても検討が必要である。

（イ） 取組の方向性

ヒトを起点として発信されるデータだけではなく、Society5.0 時代においては、モノから発信されるデータが利便性の向上や経済活動の生産性を向上させるための基盤となることから、モノの認証の実現は、そのデータの正当性を確保する上で極めて重要である。

我が国では、IoT 機器の認証の実現に向けて、IoT 機器内の各チップに分散して固定鍵及び秘密鍵を配付することや、チップのみでなく IC ボード全体のモニタリングを実施する事等によって、IoT 機器の真正性を確認する仕組みの検討が民間において進められている。

特に、重要 IoT 機器については、デバイスの製造段階からソフトウェアの更新、廃棄までの一連のライフサイクルにおいて「安全」を確認できることが重要であり、PKI 等による認証の仕組みを導入することが考えられるが、モノの認証の具体化に当たっては、e シールとの違いも考慮しながら、コストや機能上の制約等の課題を踏まえ、どのような分野への適用が適当かを整理する必要がある。また、現在（一社）セキュア IoT プラットフォーム協議会において、総務省の戦略的情報通信研究開発推進事業（SCOPE）における研究開発や、実証実験が行われている。

当面は、上記のような民間で進められているサービス開発や実証実験の動向を踏まえながら、制度の在り方について、検討を引き続き進めていくことが適当である。

③ データの送達等を保証する仕組み（e デリバリー）

（ア） 課題

e デリバリーは、厳格にヒトや組織の確認がされた送受信者双方が登録して成立するサービスであるが、現時点において、そのようなサービスを利用する送受信者それぞれにおいて当該サービスに係る制度化についてのニーズは顕在化していない。

（イ） 取組の方向性

e デリバリーは、電子署名、e シール、タイムスタンプの仕組みを組み合わせたものであることから、当該サービスの普及に当たっては、今後の我が国における各トラストサービス

の進展を踏まえつつ、ユーザ企業側のニーズやユースケース等を注視し、引き続き、検討を進めていくことが必要である。

以上に挙げたトラストサービス以外にも、技術革新の早い ICT 分野の発展に伴って、民間の創意工夫により、新たなサービスが登場し新しい利用の場面が生まれることが期待される。そのため、市場の動きや諸外国の動向も踏まえながら、今後とも、トラストサービスの在り方について検討を進めていくことが必要である。

おわりに

データが価値の源泉となり、極めて重要な価値を持つデータ駆動型社会では、データの信頼性の確保、それを支えるデータの流通基盤の整備が鍵を握る。データの流通基盤の信頼性の確保においては、トラストサービスが中核的な役割を担うことが期待され、トラストサービスの制度化の進展は、様々な電子文書や電子取引の利活用を促し、社会全体のデジタル化、ひいては新たな付加価値の創出に貢献する大きな可能性を秘めている。

これまで見てきたように、本ワーキンググループでは、我が国におけるトラストサービスの在り方について、制度化に向けて詳細な検討を行ってきた。

今後は、このような重要性を持つトラストサービスが実際に社会でより活用されるよう、総務省及び関係省庁において、制度の要件や基準等の策定について具体的な対応が進むことが期待される。また、タイムスタンプ、ｅ シール、リモート署名及びその他のトラストサービスのいずれについても、今後の技術進歩やサービス展開の動向、本取りまとめを踏まえて講じられる措置の内容やその運用状況、国際的な議論の状況等を踏まえ、その信頼性を確保するための仕組みの在り方について、随時見直しを図ることが重要である。

本取りまとめをもとに、トラストサービスの重要性が、トラストサービスプロバイダーやシステムベンダーだけでなく、トラストサービスを利用するユーザ企業や個人にも理解され、トラストサービスの普及が進み、また、信頼してデータを自由に活用できる社会的基盤が構築され、グローバルに展開されることを期待してやまない。

「トラストサービス検討ワーキンググループ」開催要綱

1　目的

近年のIoTの爆発的な普及等に伴い、サイバー空間と実空間の一体化が加速的に進展しており、実空間での様々な活動がサイバー空間に置き換わる中で、その有効性を担保するためには、サイバー空間の安全性や信頼性の確保がますます重要な課題となっている。

Society5.0の基盤として、誰からの／何からのデータであるかを確認する仕組みや、データの完全性を確保する仕組みとしてのトラストサービスが不可欠であると考えられる。

このため、「プラットフォームサービスに関する研究会」の下に本ワーキンググループを設置し、我が国におけるトラストサービスに関する課題を整理し、その在り方について、検討を行う。

2　名称

本ワーキンググループは、「トラストサービス検討ワーキンググループ」と称する。

3　検討事項

（1）我が国のトラストサービスに係る現状と課題
（2）上記（1）の課題を解決するための方策
（3）その他

4　構成及び運営

（1）本ワーキンググループの主査は、プラットフォームサービスに関する研究会の座長が指名する。
（2）本ワーキンググループの構成員は、「トラストサービス検討ワーキンググループ」構成員名簿のとおりとする。
（3）主査は、本ワーキンググループを招集し、主宰する。
（4）主査は、必要があると認めるときは、主査代理を指名することができる。
（5）主査代理は、主査を補佐し、主査不在のときは主査に代わって本ワーキンググループを招集し、主宰する。
（6）本ワーキンググループの構成員は、やむを得ない事情により出席できない場合において、代理の者を指名し、出席させることができる。
（7）主査は、必要に応じ、オブザーバーを招聘することができる。
（8）主査は、必要に応じ、外部の関係者の出席を求め、意見を聞くことができる。
（9）その他、本ワーキンググループの運営に必要な事項は、主査が定める。

5　議事・資料等の扱い

（1）本ワーキンググループは、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする。
（2）本ワーキンググループで使用した資料は、原則として、総務省のウェブサイトに掲載し、公開する。ただし、公開することにより、当事者又は第三者の利益を害するおそれがある場合若しくは主査が必要と認める場合については、非公開とする。
（3）本ワーキンググループの議事要旨は、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする。

6　その他

本ワーキンググループの事務局は、サイバーセキュリティ統括官室が行う。

「トラストサービス検討ワーキンググループ」構成員名簿

（敬称略、五十音順）

【構成員】

新　井　　聡　株式会社エヌ・ティ・ティ ネオメイト IT ビジネス本部
プラットフォームサービス推進部　電子認証サービス担当　主査

小笠原　弘貴　株式会社エヌ・ティ・ティ・データ　セキュリティ技術部
サイバーセキュリティ統括部　ソリューション担当　課長

小　川　　博　久　日本トラストテクノロジー協議会　運営委員長

楠　　俊　樹　株式会社三井住友銀行　事務統括部　上席推進役

繁　戸　　和　幸　株式会社安井建築設計事務所
執行役員　ICT・環境領域統括　ICT 室長

柴　田　　孝　一　セイコーソリューションズ株式会社
DX ソリューション統括部　部長

渋　谷　　秀　人　富士通株式会社 金融ビジネス本部 金融デジタル営業統括部
イノベーション戦略部　シニアエキスパート（第9回から）

袖　山　喜久造　SKJ 総合税理士事務所　所長

谷　　幹　也　日本電気株式会社　セキュリティ研究所　所長

（主査）手　塚　　悟　慶應義塾大学　環境情報学部　教授

西　山　　晃　セコムトラストシステムズ株式会社
プロフェッショナルサポート1部　担当部長

中　村　　信　次　株式会社日立製作所　公共イノベーションビジネス推進本部
公共戦略企画部　部長（第6回から）

（古　屋　　晶　彦　株式会社日立製作所　公共システム事業部
公共ソリューション推進第二部　担当部長（第5回まで））

宮　内　　宏　宮内・水町 IT 法律事務所　弁護士

宮　崎　　一　哉　トラストサービス推進フォーラム　副会長

【オブザーバー】

山　内　　徹　一般財団法人日本情報経済社会推進協会　常務理事

「プラットフォームサービスに関する研究会　トラストサービス検討ワーキンググループ」
開催状況

	開催日程	内　容
第1回	平成 31 年 1月 31 日（木）	○ 開催要綱について（事務局） ○ トラストサービスに関する主な検討事項について（事務局） ○ 構成員からのプレゼンテーション ・ 我が国のトラストサービスの在り方（柴田構成員） ・ データ主導社会のトラストサービス（古屋構成員） ○ 意見交換
第2回	平成 31 年 2月 15 日（金）	○ 構成員、関係者ヒアリング ・ リモート署名の検討状況（小川構成員） ・ PDF 文書を対象にした電子署名/タイムスタンプ技術の実装例（アドビシステムズ株式会社　今西氏） ○ 意見交換
第3回	平成 31 年 2月 28 日（木）	○ 構成員、関係者ヒアリング ・ 我が国のタイムスタンプサービスについて（柴田構成員） ・ トラストサービスに関する取り組み（三菱電機インフォメーションネットワーク株式会社　工藤氏） ○ 意見交換
第4回	平成 31 年 3月 19 日（火）	○ 構成員、関係者ヒアリング ・ 日本における e シールのユースケースと課題（西山構成員） ・ e シール及び e デリバリーについて（株式会社コスモス・コーポレイション　濱口氏） ○ 意見交換

第5回	平成 31 年 4月 15 日（月）	○ 関係者ヒアリング ・ ウェブサイト認証(SSL サーバ証明書)の現状と課題（GMO グローバルサイン株式会社　稲葉氏） ・ web サーバ証明書に関連する課題（セコム株式会社 IS 研究所　伊藤氏） ・ モノの本物性を確認するために（セキュア IoT プラットフォーム協議会　松本氏） ○ 意見交換
第6回	令和元年 5月 13 日（火）	○ 関係者ヒアリング ・ リモート署名について（株式会社コスモス・コーポレイション　濱口氏） ○ 議題整理 ・ これまでのヒアリング等で示された課題（事務局） ○ 意見交換
第7回	令和元年 5月 31 日（金）	○ 構成員、関係者ヒアリング ・ EU 調査報告（宮崎構成員） ・「電子インボイスとトラストサービスについて」（袖山構成員） ・ 第2回日欧インターネットトラストシンポジウムの結果概要について（日本情報経済社会推進協会　山内氏） ○ 中間取りまとめ骨子（案）（事務局） ○ 意見交換
第8回	令和元年 6月 24 日（月）	○ 中間取りまとめ（案）について（事務局） ○ 意見交換

第9回	令和元年 8月8日（木）	○ 構成員、関係者ヒアリング ・ 製薬業界における、測定機器データ等の電子化、長期保存・施設間移行の現状と課題（JIIMA R&Dデータ保存研究会 上原氏） ・ 丹青社における電子化の取り組み（株式会社丹青社 谷川氏） ・ リモート署名の検討（小川構成員） ○ 意見募集の結果等について（事務局） ○ 意見交換
第 10 回	令和元年 9月 12 日（木）	○ 構成員、関係者ヒアリング ・ 電子契約活用の広がりと課題について（日鉄ソリューションズ株式会社 後藤氏） ・ 請求書の電子化への取組みについて（渋谷構成員） ・ インボイス制度に向けた流通・DIY業界におけるシステム対応状況について（日本ドゥ・イット・ユアセルフ協会 上月氏） ○ 米国事情報告（手塚主査） ○ 意見交換
第 11 回	令和元年 10 月 11 日（金）	○ トラストサービスの利用動向に関するアンケート調査の結果（事務局） ○ トラストサービス全体に係る議論（宮内主査代理） ○ 意見交換
第 12 回	令和元年 10 月 18 日（金）	○ トラストサービスの制度化に向けた論点について（事務局） ○ 意見交換
第 13 回	令和元年 10 月 28 日（月）	○ トラストサービスの制度化に向けた論点について（事務局） ○ リモート署名ガイドライン（案）について（小川構成員） ○ トラストサービスに関する海外調査について（株式会社三菱総合研究所 安江氏） ○ 意見交換

第 14 回	令和元年 11 月8日(金)	○ 関係者ヒアリング ・ モノの認証について(セキュア IoT プラットフォーム協議会　豊島氏) ○ リモート署名の制度化に向けた論点について(事務局) ○ トラストサービス検討ワーキンググループ最終報告書骨子(案)について(事務局) ○ トラストサービスの活用・普及による経済効果について(株式会社三菱総合研究所　安江氏) ○ 意見交換
第 15 回	令和元年 11 月 28 日(木)	○ トラストサービス検討ワーキンググループ最終取りまとめ(案)について(事務局) ○ 意見交換

参考１

トラストサービスの利用動向に関する アンケート調査の結果

アンケートの概要

アンケートの目的

対面や紙を通じて行われているやりとりが今後ますます電子的なやりとりに置き換わり、「社会全体のデジタル化」が進展することが想定される中で、その基盤として電子データの信頼性（データの作成者の真正性やデータの非改ざん性）を確保するための技術的・制度的仕組みとして「トラストサービス」の在り方について、検討を行っているところ、トラストサービスの利用に関する企業のニーズや、利用に当たっての懸念事項、制度化に関する要望について把握するため。

アンケート対象企業および回答数

一般社団法人 日本経済団体連合会　デジタルエコノミー推進委員会加盟企業**184社中39社**から回答（2019年９月実施）

調査事項

Ⅰ）文書・データ（以下①～③の文書やデータ）を電子的に組織外部と送受信する時（以下、送受信）

Ⅱ）文書・データ（以下①～⑤の文書やデータ）を電子的に保存する時（以下、保存）

のそれぞれの場面におけるトラストサービス利用の有無や使用にあたっての課題等に関する調査

Ⅰ）文書・データを電子的に組織外部と送受信する時

①社外との取引に関する文書のうち、文書の作成者の真正性・非改ざん性を厳格に担保する必要のある書類（例：紙媒体の場合に代表者印を必要とする書類（契約書等））

②社外との取引に関する文書のうち、文書の作成者の真正性・非改ざん性を一定程度担保する必要のある書類（例：紙媒体の場合に社印（角印）を必要とする書類（請求書、注文書等））

③製品・サービス等の貴社の商材に関する文書・データで貴社の知的財産として保護する必要があるもの

Ⅱ）文書・データを電子的に保存する時

①社外との取引に関する文書のうち、文書の作成者の真正性・非改ざん性を厳格に担保する必要のある書類（例：紙媒体の場合に代表者印を必要とする書類（契約書等））

②社外との取引に関する文書のうち、文書の作成者の真正性・非改ざん性を一定程度担保する必要のある書類（例：紙媒体の場合に社印（角印）を必要とする書類（請求書、注文書等））

③社内の意思決定や内部管理に関する文書（主に社内でのみ使用することが想定されるもの）のうち、法令または社内規定による一定期間の保存義務があるもの

④製品・サービス等の貴社の商材に関する文書・データで、所管法令・業界ガイドライン等で一定期間の保存義務があるもの

⑤製品・サービス等の貴社の商材に関する文書・データで、貴社の知的財産として保護する必要があるもの

総論

電子化の状況	文書・データ等の送受信や保存の場面で、何らかの電子化を行っている社は36/39社

・約9割の社が、電子的手段を用いてデータ等の送受信や保存を行っており、書類の電子化自体は徐々に広まっている。

トラストサービス利用の状況	何らかの電子化を行っている社のうち、 トラストサービス（電子署名、タイムスタンプ）を使用している社は17/36社 ・送受信の場面で電子化を行っている社のうち、トラストサービスを使用している社：15（※1）/32社 ・保存の場面で電子化を行っている社のうち、トラストサービスを使用している社：14（※2）/35社 ※保存の場面において、7社が電子署名とタイムスタンプを併用し、長期署名としている

・送受信、保存いずれかの場面で、何らかのトラストサービスを使用している社は約４割程度であり、まだまだ普及が進んでいない。

送受信	電子署名（個人名）	電子署名（組織名）	タイムスタンプ	トラストサービスを使用している社（文書ごと）
Ⅰ－①	7社	3社	6社	9社
Ⅰ－②	4社	4社	4社	7社
Ⅰ－③	1社	3社	2社	5社
トラストサービスを使用している社（トラストサービスごと）	9社	7社	9社	15社（※1）

※送受信・保存のそれぞれの場面における、使用しているトラストサービスは複数回答可のため、列及び行の合計数は、必ずしもサービスごと、あるいは文書ごとのトラストサービスを使用している社の総数には一致しない

保存	電子署名（個人名）	電子署名（組織名）	タイムスタンプ	トラストサービスを使用している社（文書ごと）
Ⅱ－①	4社	2社	4社	6社
Ⅱ－②	2社	4社	5社	8社
Ⅱ－③	1社	1社	3社	3社
Ⅱ－④	0社	0社	1社	1社
Ⅱ－⑤	0社	2社	4社	4社
トラストサービスを使用している社（トラストサービスごと）	7社	7社	11社	14社（※2）

Ⅰ）文書・データを電子的に組織外部と送受信する時

①文書の作成者の真正性・非改ざん性を厳格に担保する必要のある書類（契約書等）

②文書の作成者の真正性・非改ざん性を一定程度担保する必要のある書類（請求書等）

③知的財産として保護する必要があるもの

Ⅱ）文書・データを電子的に保存する時

①文書の作成者の真正性・非改ざん性を厳格に担保する必要のある書類（契約書等）

②文書の作成者の真正性・非改ざん性を一定程度担保する必要のある書類（請求書等）

③社内の意思決定や内部管理に関する文書で一定期間の保存義務があるもの

④製品・サービス等の貴社の商材に関する文書・データで所管法令・業界ガイドライン等で一定期間の保存義務があるもの

⑤知的財産として保護する必要があるもの

電子署名（個人名の電子証明書）について

		送受信	保存
結果	傾向	・39社中9社が送受信の場面において電子署名（個人名の電子証明書）を使用 ・9社中6社の使用目的が、社外との取引を電子的に行う際の条件を定める法令・業界ガイドライン等の基準を満たすため（建設業法、印紙税法、電子帳簿保存法等） ・9社中5社が使用していて何かしらの課題を感じている	・39社中7社が保存の場面において電子署名（個人名の電子証明書）を使用 ・7社中6社の使用目的が、社外との取引を電子的に行う際の条件を定める法令・業界ガイドライン等の基準を満たすため（建設業法、印紙税法、電子帳簿保存法等） ・7社中4社が使用していて何かしらの課題を感じている
	企業の声	＜使用していて課題を感じている社（5社）の課題＞ ・利用にあたり、手間やコストがかかる（4/5社） ・サービスが将来にわたっても提供されるか不安（3/5社） ・法令上認められる送付時の要件を満たすものか不明確（2/5社）	＜使用していて課題を感じている社（4社）の課題＞ ・利用にあたり、手間やコストがかかる（3/4社） ・サービスが将来にわたっても提供されるか不安（2/4社） ・電子文書を長期的にきちんと保存できるか技術的に不安（2/4社）
		＜導入検討後、断念した社（5社）の課題＞ ・利用にあたり、手間やコストがかかる（5/5社） ・法令上認められる送付時の要件を満たすものか不明確（4/5社） ・サービスが将来にわたっても提供されるか不安（3/5社）	＜導入検討後、断念した社（6社）の課題＞ ・利用にあたり、手間やコストがかかる（4/6社） ・サービスが将来にわたっても提供されるか不安（3/6社）
サマリー		・電子署名（個人名の電子証明書）を使用している社の大多数が法令・業界ガイドライン等の基準を満たすために使用 ・使用している社および導入検討後に断念した社の多くが、使用にあたっての手間やコスト、事業者の永続性、法令上の要件を満たすかどうかを課題としてあげている	

電子署名（組織名の電子証明書）について

		送受信	保存
結果	傾向	・39社中7社が送受信の場面において電子署名（組織名の電子証明書）を使用 ・7社中4社の使用目的が、ガイドライン等の基準はないが、社内・社外に対して文書の真正性・非改ざん性を証明するため ・7社中4社が使用していて何かしらの課題を感じている	・39社中7社が保存の場面において電子署名（組織名の電子証明書）を使用 ・7社中4社の使用目的が、法令・業界ガイドライン等の基準を満たすため（建設業法、電子帳簿保存法、医薬品GCP等） ・7社中4社が使用していて何かしらの課題を感じている
	企業の声	＜使用していて課題を感じている社（4社）の課題＞ ・法的効果を規定する法制度が存在しない（3/4社） ・事業者の認定制度がない、事業者のサービス永続性に不安、真正性が国際的に認められるか不安（2/4社） ＜使用している社（7社）が感じているメリット＞ ・利用者の本人確認が不要（3/7社）、異動に伴う手続きが不要（3/7社）、大量に付せるので便利（3/7社）	＜使用していて課題を感じている社（4社）の課題＞ ・法的効果を規定する法制度が存在しない（3/4社） ・法令上認められる保存義務の要件を満たすものか不明確（3/4社） ＜使用している社（7社）が感じているメリット＞ ・利用者の本人確認が不要（3/7社）、異動に伴う手続きが不要（3/7社）、大量に付せるので便利（2/7社）
		＜導入検討後、断念した社（5社）の課題＞ ・利用にあたり、手間やコストがかかる（5/5社） ・法令上認められる送付時の要件を満たすものか不明確（4/5社） ・サービスが将来にわたっても提供されるか不安（3/5社）	＜導入検討後、断念した社（6社）の課題＞ ・利用にあたり、手間やコストがかかる（4/6社） ・サービスが将来にわたっても提供されるか不安（4/6社）
		＜Ⅰ-②の文書で電子署名（組織名）を使用していない社（29社）の声＞ ・適格請求書対応でコスト等が見合えば使用したい（26/29社）	
サマリー		・使用している社の課題として、法的効果を規定する法制度がないことを懸念している企業が多い ・利便性（本人確認不要、異動手続き不要、大量に付せる）の高さに魅力を感じている企業が多い ・導入検討後、断念した社の多くが、使用にあたっての手間やコストを課題としているが、使用している社でコストや手間を課題としてあげている社はほとんどいない ・ Ⅰ-②の文書で電子署名（個人名および組織名）を使用していない社の約9割が、適格請求書の対応で電子署名（組織名）を使ってみたいという声をあげている	

タイムスタンプについて

		送受信	保存
結果	傾向	・39社中9社が送受信の場面においてタイムスタンプを使用 ・9社中5社の使用目的が、電子データがある時点で存在し、以降改ざんされていないことを証明するため ・9社中3社の使用目的が、紙で送付する場合に比べコスト削減、業務効率化に資するため ・9社中7社が使用していて何かしらの課題を感じている	・39社中11社が保存の場面においてタイムスタンプを使用 ・11社中5社の使用目的が、電子データがある時点で存在し、以降改ざんされていないことを証明するため ・11社中3社の使用目的が、紙で送付する場合に比べコスト削減、業務効率化に資するため ・11社中3社の使用目的が、法令・業界ガイドライン等の基準を満たすため ・11社中8社が使用していて何かしらの課題を感じている
	企業の声	＜使用していて課題を感じている社（7社）の課題＞ ・サービスが将来にわたっても提供されるか不安（4/7社） ・利用にあたり、手間やコストがかかる（2/7社）	＜使用していて課題を感じている社（8社）の課題＞ ・サービスが将来にわたっても提供されるか不安（5/8社） ・真正性が国際的にも認められるものであるか不安（3/8社） ・利用にあたり、手間やコストがかかる（2/8社）
		＜導入検討後、断念した社（5社）の課題＞ ・法令上認められる送付時の要件を満たすものか不明確（4/5社） ・利用にあたり、手間やコストがかかる（4/5社） ・サービスが将来にわたっても提供されるか不安（3/5社）	＜導入検討後、断念した社（7社）の課題＞ ・サービスが将来にわたっても提供されるか不安（4/7社） ・利用にあたり、手間やコストがかかる（3/7社） ・法的効果を規定する法制度が存在しない、法令上の保存義務を満たすものであるかが不安（3/7社）
サマリー		・電子署名に比べてタイムスタンプの方が、使用にあたっての課題を感じている社（送受信：7/9社、保存：8/11社）の割合が大きく、最も多くあがった課題は、サービスの永続性である ・保存の場面においては、真正性が国際的に認められるかが不安という声が強い ・使用している社および導入検討後、断念した社の課題として、使用にあたっての手間やコストがあげられる ・導入検討後、断念した社は、サービスの永続性や法制度がないことや、法令上の保存義務を満たすかどうかの不安を課題としてあげている	

まとめ

電子署名（個人名の電子証明書）

・使用している企業の大多数が法令・業界ガイドライン等の基準を満たすために使用していることから、各業界の制度に電子署名の利用が位置付けられていることで、利用者が一定の信頼感をもって電子署名を使用することができ、利活用が進んでいることと考察される。

電子署名（組織名の電子証明書）

・先進的な企業においては、一部で導入が進んでおり、その利便性（本人確認不要、異動手続き不要、大量に付せる）を感じている。

・使用している社の課題として、法的効果を規定する法制度がないという声があがっていることから、今後のサービス拡大にあたっては、なんらかの公的な枠組みを設けることで、更なる利用促進につながっていくのではないか。

・今後、2023年に導入される適格請求書の対応では、ほとんどの企業が電子署名（組織名の電子証明書）を使用してみたいと回答していることから、電子署名（組織名の電子証明書）のニーズは潜在的にはあるものと考えられる。

タイムスタンプ

・タイムスタンプにおいては、長期保存での利用を目的としているため、サービスの永続性に不安を抱える企業が多い。

・保存の場面においては、国際的にも通用するか（他国との相互認証）を課題にあげる企業が多い。

・サービスの永続性の課題や国際的にも通用するかという課題を払拭するために、公的な制度に基づくタイムスタンプが求められているのではないか。

その他

・各トラストサービスを使用している社および導入検討後に断念した社の多くは、手間やコストを課題にあげていることから、更なる普及の拡大や、より利用しやすくなるビジネス上の工夫によって、これらの課題が解決していくのではないか。

参考２

トラストサービスの活用・普及による経済効果等

株式会社三菱総合研究所
デジタル・イノベーション本部

※ 本資料は、総務省からの（令和元年度「トラストサービスに関する調査の請負）を受託し、三菱総合研究所が作成したものです。

トラストサービスの経済効果の考え方

- トラストサービスの経済効果としては、ユーザ側での効果（直接コストの削減、業務効率化、文書処理のデジタル化による新たな付加価値）、提供者側での効果（トラストサービス市場及び関連市場の成長）が考えられる

ユーザ側での効果

文書処理のデジタル化による新たな付加価値

✓ デジタル文書処理システム/サービスを前提とした業務プロセス改革（例：文書検索等の効率化、業務プロセス改革、コンプライアンス・内部統制強化、等）

文書情報の取扱（作成・送受信・確認・処理・保存等）の直接コストの削減

✓ 紙代、郵送費、印紙代、保管のためのオフィス賃料・倉庫代、等の削減・効率化

✓ 文書を作成、送付、受領、処理（例：文書内容の確認、入力）、保管するための業務の効率化（→業務効率化による生産性向上、他業務へのリソース配分、長時間労働・人手不足解消、等）

上記に関する業務の効率化

提供者側での効果

トラストサービス市場（及び関連市場）の成長

✓ 左記を実現するために提供・利用されるトラストサービスや関連ソリューション（例：電子契約サービス、請求書発行/支払処理サービス、文書保存システム、クラウドサービス、等）の市場規模

トラストサービスの経済効果　（1）コスト削減・業務効率化の例

- トラストサービス・関連サービスの利用によりもたらされる効果として、税務関係書類の電子化による経済効果、契約や請求・支払業務の電子化によるコスト削減効果等が試算・例示されている

【コスト削減・業務効率化の計量・試算の代表的な例】

対象分野	効果等	出典等
税務書類の電子保存	● 税務書類の紙による保存コストは経済界全体で3,000億円/年（注：電子保存に移行するための費用は別途推計している（紙での保存コストよりも小さい）） ● 「倉庫代などの保管コスト、書類等の発生場所から倉庫までの運搬コスト、書類等の廃棄コスト、税務調査の便宜等のために保管されている書類の一覧等を印刷するコスト、これら取扱いのための人件費」が含まれている	日本経済団体連合会「税務書類の電子保存に関する報告書」（2004年）
電子契約	● 書面による契約から電子契約に移行すると、1部あたり300円（410円⇒110円）のコスト削減が可能になり、また印紙税が不要となる（※他に業務時間効率化も期待できる）	日鉄ソリューションズ　パンフレット「CONTRACTHUB@absonne」
	● 作業時間（80h/月、4h/日）、印紙税額（約1,000万円）の削減効果（セブン-イレブン・ジャパンの事例）	トラストサービス推進フォーラム「トラストサービスのユースケース」（2019年10月23日）
	● 注文書・注文請書・契約書等の電子化により発注契約から契約までの業務効率が2倍に向上（リクルートテクノロジーズの事例）	日鉄ソリューションズ　第10回本WG資料
請求・支払	● 請求：請求書発行～入金消込の工数が2,600h/月⇒50h/月へ98%削減 ● 支払：書類の照合～請求データの入力の工数が50%～80%削減	富士通　第10回本WG資料
その他	● 流通・DIY業界で適格請求書（インボイス）に対応する場合、対象となる伝票は約1千万件/月⇒3～4千万件/月に増加すると見込まれ、eシールを活用したシステム対応が必須	日本ドゥ・イット・ユアセルフ協会　第10回本WG資料
	● 出張経費：ソリューションを利用することで、企業は年間約30千ドル/社、従業員1人当たり600ドル、の経費を節約（豪、加、日、英、米での420社調査）	コンカー（SAP Concur）　Webサイト

トラストサービスの経済効果　（2）業務の効率化（潜在規模）の試算

- トラストサービスにより例えば下記の業務の効率化が期待でき、生産性向上、他業務への振分け、長時間労働・人員不足解消等に寄与すると考えられる

※ 文書処理デジタル化による新たな付加価値の定量化は困難なため、下記では既存プロセスのデジタル化を対象に試算している

間接業務	総務人事系	雇用契約、事業所の不動産契約等の効率化、等
	経理系	契約、見積・提案・納品・請求・支払等の各文書、税務関連文書、社内精算（旅費交通費、物品購入等）、等
	その他	社内文書記録・保存、等（※知財関連もここに含む）
直接業務	建築	建築に関する各種申請、各種点検
	金融・保険	住宅ローン契約、各種保険手続
	不動産	賃貸契約、重要事項説明書交付
	卸売・小売、飲食	店舗関連の各種手続（例：賃借契約、雇用契約） ※とくにチェーン店、フランチャイズ店等
	医療・介護	各種記録（診療、介護等）の他機関への提供
	サービス	店舗関連の各種手続（例：賃借契約、雇用契約）
	運輸・郵便	荷受・配送伝票等
	専門サービス	各種文書送付※例えば弁護士、会計士、税理士等
	電気・ガス・熱供給・水道	各種施設・設備等の法定点検

*1 上記は効率化が考えられる主な業務（必ずしも網羅的ではない）

✓ 例えば経理系業務の場合

- 大企業1社あたり、**10.2万時間/月⇒5.1万時間/月**への効率化余地が期待できる
- 小企業1社あたり、**502時間/月⇒151時間/月**への効率化余地が期待できる

✓ 間接業務全体では

- 大企業1社あたり、22.6万時間/月⇒15.4万時間/月への効率化余地が期待できる
- 小企業1社あたり、1,116時間/月⇒608時間/月への効率化余地が期待できる

✓ 直接業務では、業種により異なるが、以下の業種でとくに高い効果が期待される：

- 金融・保険、不動産・物品賃貸、卸売・小売、運輸・郵便、宿泊・飲食、各種サービス（文書情報の取扱業務の多い業種ほど、高い効果が期待される）

✓ 全業務(間接業務+直接業務)では

- 大企業1社あたり、66.8万時間/月⇒53.4万時間/月への効率化余地が期待できる
- 小企業1社あたり、5,526時間/月⇒4,440時間/月への効率化余地が期待できる

*2 業務時間配分及び効率化率を設定して行ったものであり（設定の考え方は後掲）、設定条件により試算結果は変動しうる

トラストサービスの経済効果　（3）トラストサービス市場の成長試算

- トラストサービス（電子署名、タイムスタンプ、eシール）の市場規模は2018年に約50億円と推計され、2030年頃には146億円（ベースケース）、556億円（成長ケース）に達すると試算された

現状推計（2018年）*1

①トラストサービス	**50億円**
電子署名	45億円
タイムスタンプ	2.4億円
eシール	2.9億円
②関連サービス*2	**44億円**
合計（①＋②）	**94億円**

- 利用企業：大・中規模企業
- 普及率：25%*3

将来試算（2030年頃）*4

ベースケース

- 大・中企業：普及率50%*3
- 小企業：普及率5%*3

①トラストサービス	**146億円**
電子署名	105億円
タイムスタンプ	29億円
eシール	11億円
②関連サービス	**125億円**
合計（①＋②）	**271億円**

- ✓ 電子署名：微増を継続
- ✓ タイムスタンプ：現状のトレンド（対前年比30%増程度）＋αで推移
- ✓ eシール：微増ないしやや成長
- ✓ 関連サービス：成熟化（30%⇒数%程度）

成長ケース

- 大・中企業：普及率70%*3
- 小企業：普及率25%*3

①トラストサービス	**556億円**
電子署名	376億円
タイムスタンプ	119億円
eシール	62億円
②関連サービス	**479億円**
合計（①＋②）	**1,035億円**

- ✓ 各トラストサービスについて制度化等の環境が整備される場合
- ✓ 電子署名：リモート署名の増加による成長
- ✓ タイムスタンプ：知財保護等の需要により急成長する
- ✓ eシール：制度化及びインボイス対応等の需要により急成長
- ✓ 関連サービス：トラストサービス成長の影響を受けて拡大

※ 現状値に基づき、利用企業数、普及率、利用数量、単価の各要素を考慮して試算

*1 電子署名及びタイムスタンプの発行枚数、事業者へのヒアリング、企業数、想定普及率（導入率）等を踏まえて現状値を推計した

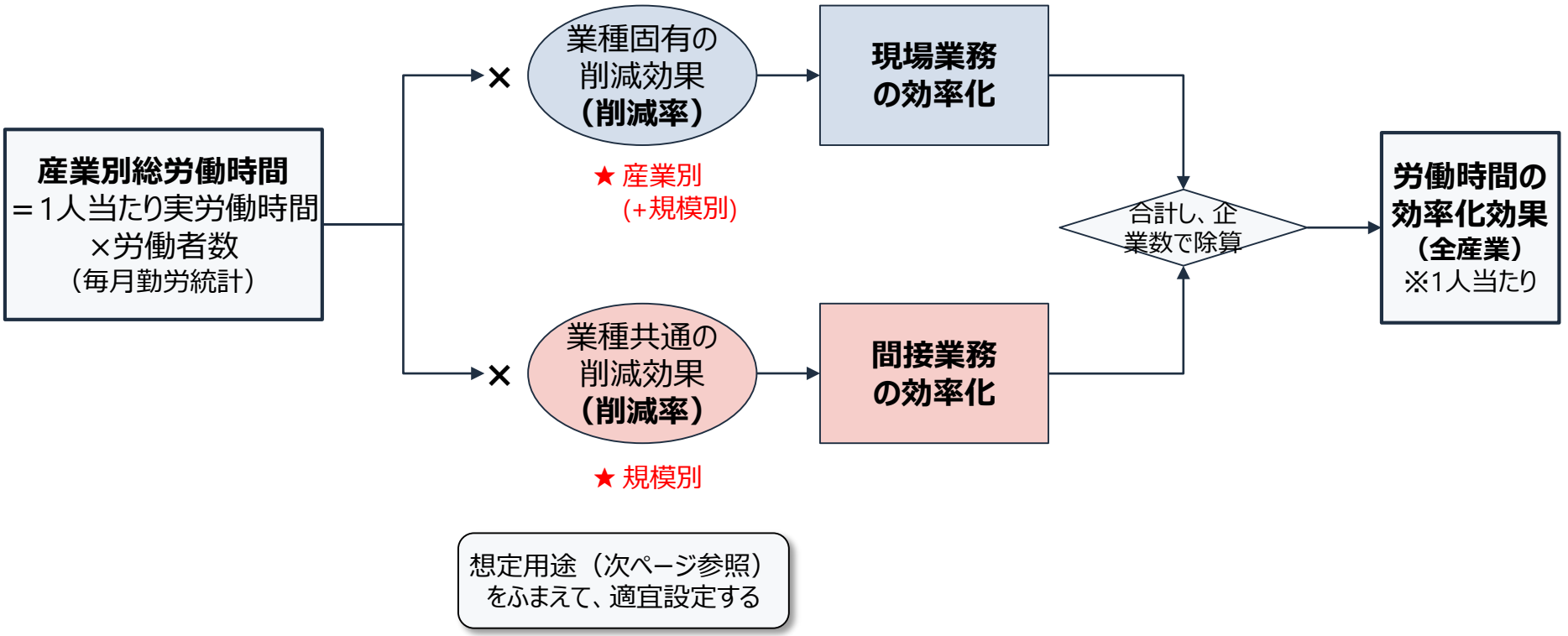
*2 関連サービスは、電子契約サービスを中心に、トラストサービスと関係の深いサービス（例：請求・支払、経費精算、等）を対象として推計した。この他にも、トラストサービスの導入に伴う新たなシステムの構築等に関連するITシステムの導入やアプリケーション等の整備等に関する投資が増加するといった効果も見込まれる

*3 本WGにおけるアンケート調査（第11回資料）、JIPDEC・ITR調査結果（後掲）等を参考に三菱総合研究所にて推計・設定した

*4 市場規模・利用状況に関するデータが少なく、例えばトラストサービスの企業内での活用状況の進展・広がり等を十分に加味できていないため、試算結果は変わりうる点に留意

参考）トラストサービスによる業務効率化　（1）試算の考え方

- トラストサービスによる業務効率化を、業務時間に着目して以下のように試算した



※ 産業別総労働時間データは「賃金構造基本統計調査」（労働政策研究・研修機構）を用いる
（なお、2015年時点のデータが最新）

参考）トラストサービスによる業務効率化　（2）試算条件の検討

- 業務効率化の試算条件は、粗い推定だが以下のように設定した

	業種共通業務の効率化	業種固有業務の効率化
対象業務	間接業務	直接業務（※業種に固有の現場業務）
時間配分	各業種の総労働時間の1/5～1/3 （企業規模10～99人→1/5、100～999人→1/4、1,000人以上→1/3）	各業種の総労働時間の4/5～2/3 （企業規模10～99人→4/5、100～999人→3/4、1,000人以上→2/3）
業務時間効率化の要因及び程度	● 総務人事系（上記時間の45%）：10%【雇用契約、事業所の不動産契約等の効率化、等】 ● 経理系（上記時間の45%）：50～80%【契約、見積・提案・納品・請求・支払等の各文書、税務、等】 ● その他（上記時間の10%）：50%【社内文書記録・保存、等】※知財関連もここに含む	● 医療・介護：10%【各種記録（診療、介護等）の他機関への提供、等】 ● 建築：10%【各種申請業務、法定点検、等】 ● 流通・飲食：20%【店舗関連の各種手続（例：賃借契約、雇用契約）、等） ● サービス：20%【店舗関連の各種手続（例：賃借契約、雇用契約）、等） ● 不動産：30%【賃貸契約、等】 ● 運輸：20%【配送伝票、等】 ● 電気・ガス・熱供給・水道：10%【各種法定点検】 ● 金融：30%【住宅ローン、各種保険手続、等】 ● 専門サービス：20%【各種文書送付】 ● 全般：ベースとして1～3%

※　時間配分及び効率化の程度については、試算のために設定した

参考）トラストサービス市場の推計・試算の参考データ

- 市場の現状推計・成長試算に際し、事業者等へのヒアリングの他、以下のデータも参考とした

項目	概要	出典等
電子契約サービス	**電子契約の利用状況（2019年）** 「複数部門で利用」／「現在利用」＋「利用を検討」 ・ 全体（N=686）：22.0%／67.4% ・ 5,000人以上（N=139）：35.3%／82.0% ・ 1,000～4,999人（N=156）：22.4%／73.8% ・ 300～999人（N=168）：23.3%／68.5% ・ 50～299人（N=223）：12.6%／53.0%	JIPDEC・ITR「企業IT利活用動向調査2019」 https://www.jipdec.or.jp/library/itreport/2019itreport_spring.html
	市場規模予測 ・ 2018年度の市場規模：39億円 ・ 2023年度の市場規模：83億円 ・ CAGR (2018→2023)：16.3% ※ 市場成長の見方は調査会社により異なり、より高成長を予測するものある	矢野経済研究所「リーガルテックウォッチ2019」 https://www.yano.co.jp/press-release/show/press_id/2224
クラウドサービス	**企業におけるクラウドサービスの利用動向** 「一部でもクラウドサービスを利用している企業」 ・ 2013年：33.1%　2014年：38.7%　2015年：44.6% 2016年：46.9%　2017年：56.9%	総務省「情報通信白書 平成30年版」（通信利用動向調査） http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd252140.html
	国内クラウドサービス市場規模 ・ 2018年度：1兆9,422億円（パブリッククラウド6,165億円(+34.1%)、プライベートクラウド1兆3,257億円(+18.1%)） ・ 2023年度：4兆4,754億円（パブリッククラウド1兆6,490億円、プライベートクラウド2兆8,264億円） ・ CAGR (2018→2023)：パブリッククラウド21.7%、プライベートクラウド16.3%	MM総研「2019年国内クラウドサービス需要動向調査」 https://www.m2ri.jp/news/detail.html?id=354

参考３

リモート署名ガイドライン(案)

パートⅠ.一般的セキュリティ対策

日本トラストテクノロジー協議会（JT2A）

2019 年 12 月 18 日時点版

目　　次

1 目的・背景

最近の国際的なデジタルエコノミー推進の中で、事業者環境に署名鍵を預けて契約を締結するリモートで署名するサービスが存在している。本ガイドラインはリモート署名の概要を解説するとともに、リモート署名にて作成された電子署名文書の信頼性を確保するため提供事業者や事業関係者及び利用者が留意すべき基準をとりまとめた。

日本政府の情報化施策によって、2016 年からマイナンバーカードの利活用が進み、2017 年にマイナポータルにおいて官民が連携し、各種の申請や手続きが電子化、また、2019 年 1 月に電子委任状法が施行され、国民にとっても電子証明書及び電子署名がより身近に利用できる環境が整った。

これらの環境を利用したサービスのなかでも、特に電子的な契約では、利用者の IT 環境の変化や電子的に契約を行う上での署名鍵の管理の負担軽減のために、事業者環境に署名鍵を預けて契約を締結するリモート署名サービス（利用者の署名鍵を預かり、自社のサーバ等で保管し、利用者の指示に基づき、保管している利用者の署名鍵と自社が管理する署名用アプリケーションを用いて署名し、その結果を利用者に返すサービス）も存在している。

わが国では認定認証事業を行う法人が認証局とは別のサービスとして 2009 年 11 月にリモート署名を採用した Web 型の署名サービスを開始したのが最初の利用事例であった。その後、2016 年 2 月に大手金融機関によりリモート署名を採用した融資契約の電子化サービスが開始された。現在では多くの民間事業者が提供する電子契約サービスの中でリモート署名が採用されているがその方法は様々である。これらの電子契約については、利便性が高く、安全なサービスが求められるが、その安全性や信頼性の指標が定まっていない。

一方、経済産業省では 2015 年度、2016 年度の電子署名法研究会においてリモート署名の関連動向やその在り方の検討を行い、その実施のために必要となる事項が整理された。

JT2A ではこの検討を受けて提供事業者や利用者がリモート署名の理解を深め、一定の指標として参照可能なリモート署名のガイドラインを作成することとした。

また、最近の国際的なデジタルエコノミー推進の動きの中で、2018 年 7 月「日 EU 経済連携協定（EPA)」の中で電子商取引において電子署名、電子認証に関する基本ルールが規定され、2019 年 1 月の世界経済フォーラム年次総会（「ダボス会議」）にて国際間で「信頼ある自由なデータ流通（DFFT : データ・フリー・フロー・ウィズ・トラスト)」の確立が最重要課題であるべきことがわが国から提唱されている。

そのため、本ガイドラインでは、リモート署名を用いた電子商取引の EU などとの国際相互連携も踏まえつつそのあるべき内容の検討結果をまとめた。

本書にてリモート署名の概要を解説するとともに、リモート署名にて作成された電子署名文書の信頼性を確保するため提供事業者や事業関係者及び利用者が留意すべき基準をとりまとめたので、今後のデジタルトランスフォーメーションの推進に向けて参考にされたい。

日本トラストテクノロジー協議会　一同

2 用語

略語	正式名称
CA 認証局（CA）	Certification Authority、署名鍵に紐づく電子証明書を発行する機関。例えば、認定認証局など。一般に認証局は、発行局（IA）、登録局（RA）、電子証明書の失効情報等を公開するリポジトリなどで構成される。
CM	Cryptographic Module、暗号モジュールの略称であり、欧州においては EN 419 221-5:2016 を用いた評価を行っている。
CSP 認証クレデンシャル発行機関（CSP）	Credential Service Provider、認証クレデンシャルを発行する機関。（例えば、JPKI 利用者証明用証明書やマイナンバーカード内の利用者証明用電子証明書、認証局が発行する利用者証明用電子証明書等がある。また、オンラインサービスの利用申請を受付け、利用者に対して ID/パスワードを発行するオンラインサービス提供者などを含む。サービス提供形態によっては認証局とは異なる事業体もあり得る）
CSR	Certificate Signing Request、電子証明書を発行する際の元となるデータ。CSR には電子証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して電子証明書を発行する。データ形式として、PKCS#10 などがある。
DTBS	Data to be Signed、署名対象データ。（指令 1999/93/EC[3]で定義されている）また、単体及び複数のセットで構成する場合には、DTBS/R(s)とする。
HSM	Hardware Security Module、ハードウェアの暗号モジュールであり、ハードウェア内で鍵を保管し、暗号化機能や署名機能を有する装置。
PIN	Personal Identification Number、本人確認のために用いる本人のみが知る番号などの情報。
PKCS#12	Personal Information Exchange Syntax Standard 12、秘密鍵と電子証明書を安全に交換するための方法を定義した仕様。
RA 登録局（RA）	Registration Authority、署名者の本人確認を行い、IA へ電子証明書の発行を依頼する機関。本書では、署名用の電子証明書の登録局を意味する。
RP リライングパーティ（RP）	Relying Party、署名の受領者（署名受領者）。
SAD	Signer's Activation Data、署名鍵を活性化するデータであり、IC カードでは PIN 等である。（指令 1999/93/EC[3]で定義されている）
SAM	Signature Activation Module
SAP	Signature Application、SCM を用いて電子署名を生成するアプリケーション。（日本国内のリモート署名を検討するために新たに定義したアプリケーションである）
SCA	Signature Creation Application、電子署名を生成するアプリケーション。
SCD	Signature Creation Data、署名鍵。（指令 1999/93/EC[3]で定義されている）
SCDev	Signature Creation Device、SCD を実行するための設定済みソフトウェアまたはハードウェア。（指令 1999/93/EC[3]で定義されている）
SCDid	Signature Creation Device Identifier、署名鍵の識別子。（指令 1999/93/EC[3]で定義されている）
SCM	Signature Creation Module、電子署名を生成するモジュール。（日本国内のリモート署名を検討するために新たに定義したモジュールである）
SCM-C	SCM 内に格納している署名鍵を活性化するクレデンシャル。
SCM-CV	SCM 内に格納している署名鍵を活性化するクレデンシャルを検証する情報。
SCP	SASC Policy
SIC	Signer Interaction Component

Signer' s SCD	Signer's Signature Creation Data、署名者の署名鍵。（指令 1999/93/EC[3]で定義されている）
SSA	Server Signing Application、SCA へのリモートアクセスを提供するアプリケーション。（指令 1999/93/EC[3]で定義されている）
SSCD	Secure Signature Creation Device、欧州指令の附属書 III で規定されている要求事項を満たす署名生成装置。（指令 1999/93/EC[3]で定義されている）
SSM	Software Security Module、ソフトウェアの暗号モジュールであり、暗号化機能や署名機能を有するソフトウェア。
SVD	Signature Verification Data の略称
TSP	Trust Service Providers の略称
VA 検証局（VA）	Verification Authority、電子証明書の有効性の確認を行う機関。または、失効リストを管理する機関。本書では、電子署名の有効性を確認する機関を意味する。
リモート署名サーバ	リモート署名事業者が管理するサーバであり、利用者の署名鍵を保管し、リモート署名を実施する。
リモート署名事業者（RSSP）	Remote Signature Service Provider、利用者の署名鍵を設置・保管するサーバとそのサーバ上で利用者の指示に基づき、電子署名を行う機能を提供する者
検証鍵	署名検証に用いる鍵（公開鍵）。電子署名法では「利用者署名検証符号」と称される。
署名鍵	署名に用いる鍵（秘密鍵・私有鍵）。署名サーバ内で HSM 等により安全に管理される。署名を行う際に署名鍵に設定された PIN などにより活性化される。電子署名法では「利用者署名符号」と称される。
署名鍵 ID	署名鍵の識別子。
電子証明書	利用者の公開鍵が本人に帰属していることを証明するために認証局が発行する電子的な証明書。公開鍵証明書ともいう。
認証クレデンシャル（RS-C）	署名者が署名サーバを利用する際の認証に用いるための情報。（例えば、JPKI 利用者証明用証明書、ID/パスワード、ワンタイムパスワードなど）リモート署名（RSSP）の利用者認証に用いるクレデンシャルについては RS-C と表記する。
認証クレデンシャル検証情報（RS-CV）	リモート署名（RSSP）の利用者認証に用いるクレデンシャルを検証する情報。
発行局（IA）	Issuing Authority、電子証明書発行や失効等を行う機関。本書では、署名用の電子証明書を発行する機関を意味する。
利用者	リモート署名サービスを利用して署名を行う者（署名者）。
利用者 ID	利用者の識別子。

3 ガイドラインの構成と想定読者

3.1 本ガイドラインの構成

本ガイドラインの各分冊の章構成を以下に示す。パートⅠはリモート署名の概要及び一般的なセキュリティ対策を記載し、パートⅡは署名活性化モジュール、パートⅢは署名値生成モジュールについて記載している。

分冊	章	事業者	利用者
パートⅠ	1章　目的・背景	○	○
	2章　用語	○	○
	3章　ガイドラインの構成と想定読者	○	○
	4章　リモート署名の概要	○	○
	5章　セキュリティ検討事項	○	
	6章　セキュリティ対策事項	○	
	7章　参照情報	○	○
	附録	○	○
パートⅡ	1章　署名活性化モジュールの概要	○	
	2章　セキュリティ検討事項	○	
	3章　セキュリティ機能要件	○	
	4章　参照情報	○	
	附録	○	
パートⅢ	1章　署名値生成モジュールの概要	○	
	2章　セキュリティ検討事項	○	
	3章　セキュリティ機能要件	○	
	4章　参照情報	○	
	附録	○	

本ガイドラインは、リモート署名サービスを提供及び関連する事業者、及び利用者を想定読者とする。

・リモート署名の利用者　・・・　電子契約などを利用する契約の当事者　など
・リモート署名の事業者　・・・　電子契約事業者（設計開発事業者、管理運用事業者）など

リモート署名の事業者は、本ガイドラインのすべての章を参考に対策を行う必要がある。リモート署名の利用者は、自らの署名鍵を安全に管理し、利用するためにパートⅠの 1 章から 4 章及び必要に応じて 7 章、附録を参考にリモート署名事業者が提供するサービスを選定する必要がある。以降に、リモート署名サービスを選定するための重要項目を示す。

3.2 重要項目

リモート署名の重要事項は、鍵生成（署名鍵の生成）、鍵設置（署名鍵保管場所への格納）、鍵認可（署名鍵の活性化）の 3 つである。鍵生成及び鍵設置については、署名者の署名鍵を安全に設置し、管理するために、利用する署名鍵は、正しく生成されること、または正しくインポートされることが求められる。また、鍵認可については、署名者の署名鍵を安全に管理し、署名者のみの利用意図に応じて安全に利用でき（署名者だけが署名鍵を活性化でき署名者以外は署名鍵を利用できないことが求められる。本ガイドラインでは、正しい署名鍵を安全に管理するために最低限必要な対策、推奨する対策、及び欧州等との相互運用性等を考慮した対策として附帯を定めた。以下に最低限、推奨、附帯で求める対策を示す。

表 3-1　重要項目（鍵生成、鍵設置、鍵認可）のレベル

項目	最低限	推奨	附帯
鍵生成	• HSM※1 を利用せずに署名鍵の生成が可能	• HSM でのみ署名鍵の生成が可能	• 欧州の署名生成デバイスの評価・認証取得品※2 である HSM でのみ署名鍵の生成が可能
鍵設置	• 署名鍵のインポート可能	• 認定認証事業者など信頼できる CA(認証局)からのみ署名鍵のインポートが可能	• 外部からのインポート不可。HSM 内で生成した署名鍵のみを利用する
鍵認可	• 鍵認可は単要素認証 • 利用者認証で鍵認可を行ってもよい（＊１）	• 鍵認可は複数要素認証 • 利用者認証と別に鍵認可を行わなければならない（＊２）	• 推奨に追加して、評価・認証取得※3 し、耐タンパ領域に実装した署名鍵活性化モジュールでの鍵認可が必要（＊３）

※1：Hardware Security Module の略称。耐タンパ性を有する頑強なモジュールであり、CMVP の認証取得製品。CM で用いる。
※2：署名生成デバイス（SCDev）の欧州規格。
※3：署名活性化を行うモジュール（SAM）の欧州規格（耐タンパな環境での設置が必須）。

リモート署名で想定する利用シーンの例としては署名対象となる電子的な契約書ファイル等を作成、保管する電子契約サービス等がある。この時、電子契約サービスで利用者認証を行い、その後、リモートで署名を行う際に、署名鍵を活性化（鍵認可）を行うこととなる。その際、リモート署名の対象となる情報の重要度やリスクに応じて、鍵認可の対策が異なる。表 3-1 の鍵認可の対策及び考え方について以下に示す。

（＊１）: SCA への利用者認証①により、RSSP への利用者認証②を兼ねてもよいし、RSSP への利用者認証を別途行う場合（利用者認証③）も考えられる。また、鍵認可は直接（鍵認可①または鍵認可④）行ってもよいが、SCA（鍵認可②）あるいは SSA（鍵認可③）が代行しても良い。

（＊２）: 鍵認可は必ず利用者認証とは別に行わなければならない（鍵認可①または鍵認可④）。

（＊３）: 鍵認可は必ず SAM 経由で行わなければならない（鍵認可④）。

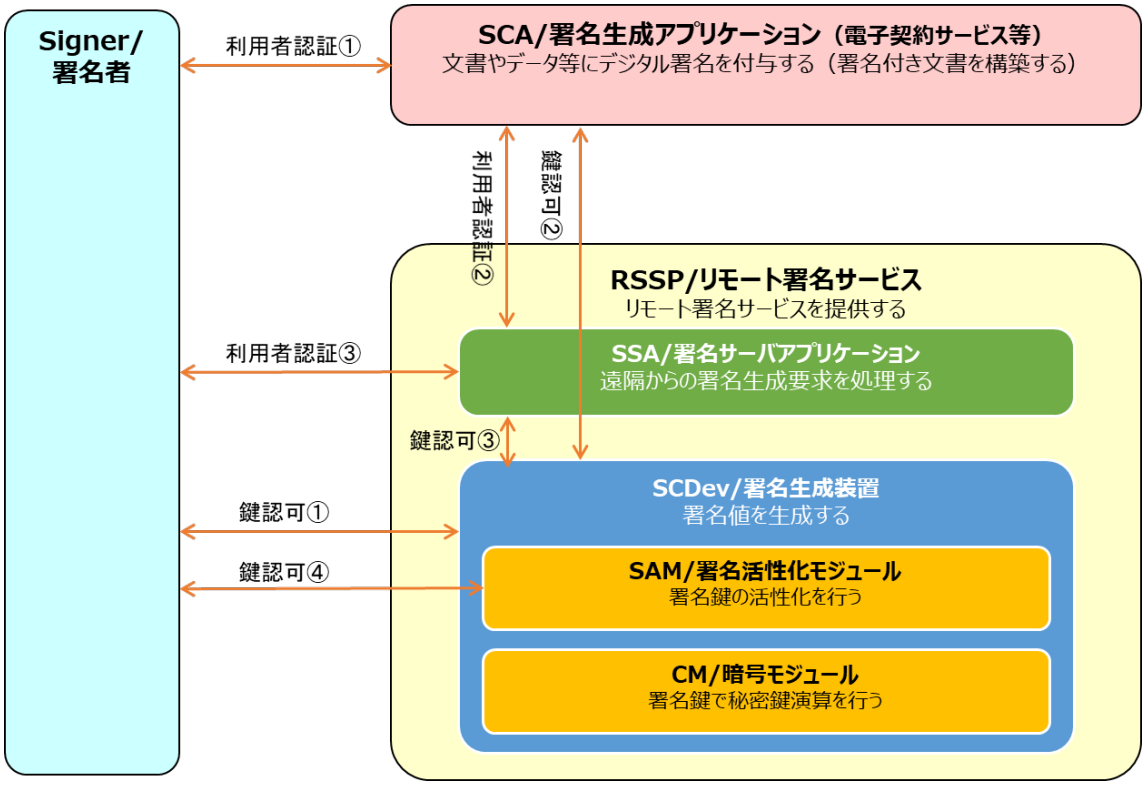


図 3-1　リモート署名サービスの構成例

なお、本ガイドラインでは、署名生成アプリケーション（SCA）や利用シーンの多様性を考慮し、鍵認可については表 3-1 及び上記に示したが、利用者認証の対策については、参考資料[6]などを基に、リモート署名の対象となる情報の重要度やリスク分析の結果を考慮して検討する必要がある。

4 リモート署名の概要

経済産業省の電子署名研究会の平成 28 年度の事業報告書では、リモート署名を以下のように定義している。

> リモート署名とは、一般にリモート署名事業者のサーバに利用者の署名鍵を設置・保管し、利用者の指示に基づきリモート署名サーバ上で自ら（利用者）の署名鍵で電子署名を行うことをいう。

本ガイドラインにおいても、これに基づいて記述する。

4.1 ローカル署名とリモート署名の違い

日本における“電子署名”は、紙媒体に対する署名や捺印と同様に利用者が署名鍵を手許に保管し、利用者の手許で行うモデルであった。ここではこれを「ローカル署名」と呼ぶことにする。

一方で、デジタル化とネットワークの発展は、クラウドサービスなどデータ処理の形態を多様化し、電子署名の利用環境も大きく変化した。従来の電子署名は、署名鍵の取得の手間や、耐タンパデバイスによる安全な保管の面倒さなどが普及の妨げとなっていたが、署名鍵をサーバ等に預け、遠隔から利用する形態（リモート署名）がこの課題の一つの解決策となることが期待される。リモート署名は、単に鍵の場所をローカルからリモートにした以上に大きな意味を持つ。そのメリットは、一般のクラウドサービスと同様に、デバイスフリー化、いつでもどこでも利用可能なこと、所有（管理）から利用への転換である。これにより、紙では手許でしかできなかった“署名“が、リモートで可能となることでビジネスモデルの変革につながる可能性を秘めている。さらに“電子署名法”は自然人を対象としているが、マシンや組織の“署名”も含め、電子署名の発展につながると考えられる。

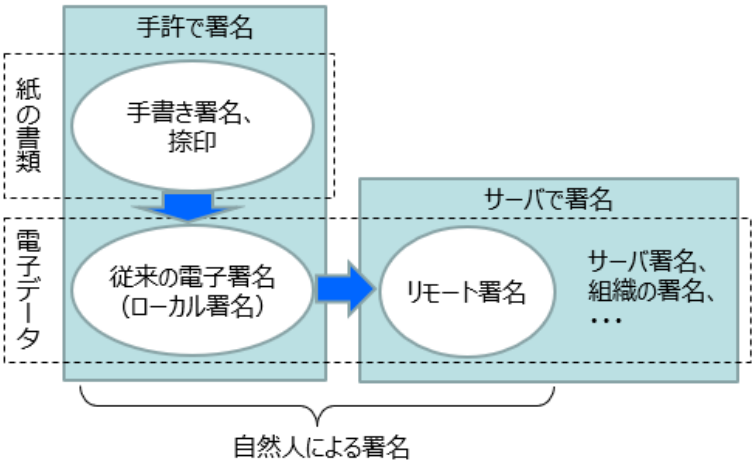


図 4-1　署名形態の進開

実際にはリモートで署名鍵を預ける先としての事業者（以後、「リモート署名事業者」(RSSP)と呼ぶ）の存在が必要となる。その場合のリモート署名と、ローカルで署名を行う場合の対比を下図に示す。

リモート署名を安全に利用するために重要であり、検討すべき点は、リモート署名事業者が保管している署名鍵の安全性と署名鍵と署名者の結びつき（署名鍵登録時と署名鍵利用時）である。

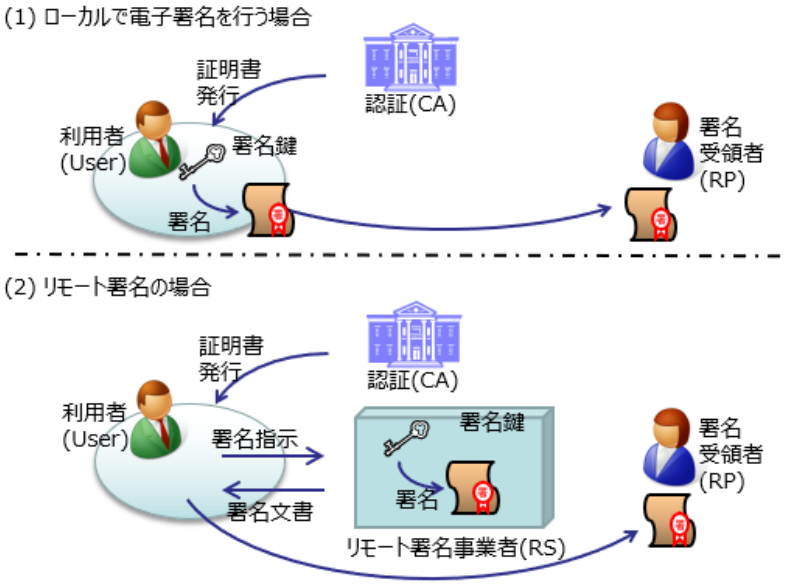


図 4-2　ローカルな電子署名とリモート署名の比較

4.2 リモート署名の利用形態

リモート署名をビジネスに利用する場合、特定のサービスのアプリケーションと密接に連携する形態が考えられる。実際、現状のリモート署名の利用例の多くは、電子契約及び電子契約を含む保管サービスである。これは、汎用的な署名鍵をリモート環境（外部）に置いて汎用的な用途で利用するケースより、リモート署名のニーズの牽引役となることが期待される。この場合、利用者が行う手続き等をアプリケーションが仲介して進める形態が想定されるが、あくまでも利用者の意思の下の処理とみれば処理の流れは同様である。

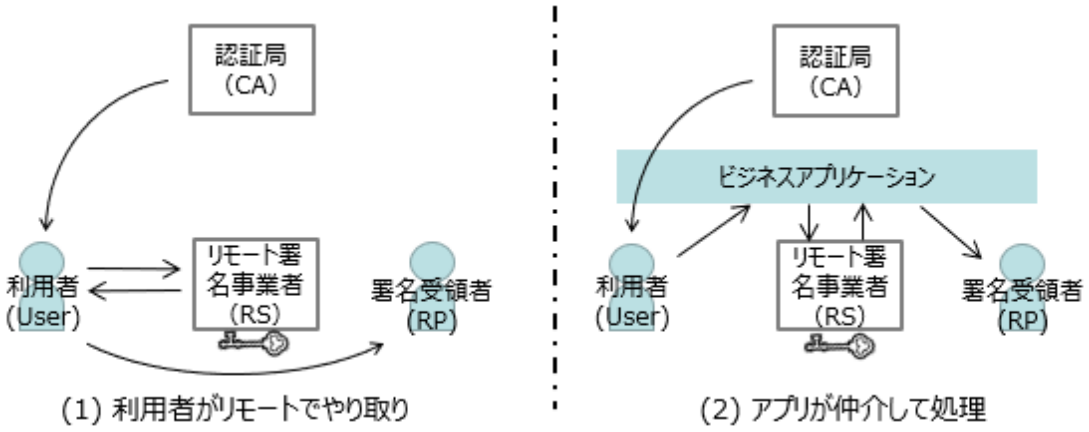


図 4-3　リモート署名の利用形態の例

さらに、電子契約等のビジネスアプリケーション提供者が汎用のリモート署名事業者を利用するケースと、アプリケーション提供者が自社サービス用にリモート署名機能を提供するケースも考えられ、論理的には、別の構成要素と位置付けとなるもののリモート署名を行ううえで満たすべき機能にかわりはなく、5 章や 6 章では、リモート署名で満たすべき機能について説明する。

4.3 リモート署名に関連するプレイヤと役割

前節で述べたリモート署名に関連するプレイヤについて、その役割を下表にまとめる。

表 4-1 リモート署名のプレイヤ

プレイヤ	役割
リモート署名事業者 （Remote Signature Service Provider：RSSP）	利用者の署名鍵を設置・保管するサーバとそのサーバ上で利用者の指示に基づき、電子署名を行う機能を提供する者
署名生成アプリケーション （Signature Creation Application：SCA）	署名対象ドキュメント等の準備と、リモート署名を利用して長期署名等を生成するサービス等
クレデンシャル発行者 （Credential Service Provider：CSP）	リモート署名事業者のサーバを利用するための認証クレデンシャルを発行する者
認証事業者 （Certification Authority： CA）	利用者の署名鍵に紐づく電子証明書を発行する機関
利用者（署名者） （User：U）	リモート署名サービスを利用して署名を行う者（署名者）
署名受領者 （Relying Party：RP）	署名の受領者

利用者が電子契約等のリモート署名アプリケーション（サービス）を利用して電子署名をおこなうことを前提としている。リモート署名アプリケーションとリモート署名事業者が同一の場合もあるが、この２つを分離してサービス提供することも可能となっている。リモート署名事業者は、署名者の署名鍵を用いて署名対象に対する署名値を提供する。署名値を受けたリモート署名アプリケーションは、署名値と署名対象とを組み合わせることにより最終的な署名済み文書を提供する。

ここで本来、署名鍵を持つのは利用者であるが、鍵を生成するのは利用者とは限らない。電子署名法施行規則第６条第３号及び第３号の２では、認証事業者が署名鍵を作成する場合及び利用者が署名鍵を作成する場合における基準について規定している。さらに、鍵の移送の便を考えると、リモート署名事業者も鍵生成の候補となる。

いずれの場合も一定の条件を満たすものであれば、電子署名法施行規則に適合するものであるといえる。 これらの具体的な要件については、6 章において述べる。

従来のローカル署名のモデルとリモート署名のモデルによる役割と保有情報の違いを図

4-5 に示す。従来のローカルで署名を行うモデル（図の(1)）では、利用者が署名鍵と署名鍵を活性化する署名鍵のクレデンシャル（CM-C）及び公開鍵証明書を保有する。一方、リ モート署名のモデル（図の(2)）では、利用者は署名鍵のクレデンシャルと公開鍵証明書及びリモート署名（RSSP）のサービスを利用するためのサービス ID とサービス ID に対応する認証クレデンシャル（RS-C）を保有する。さらに、RSSP は、署名サービスを提供する正当な利用者であるかを認証するために利用者の認証情報（認証クレデンシャル検証情報（RS-CV））と認証情報に対応した利用者の署名鍵を保有する。

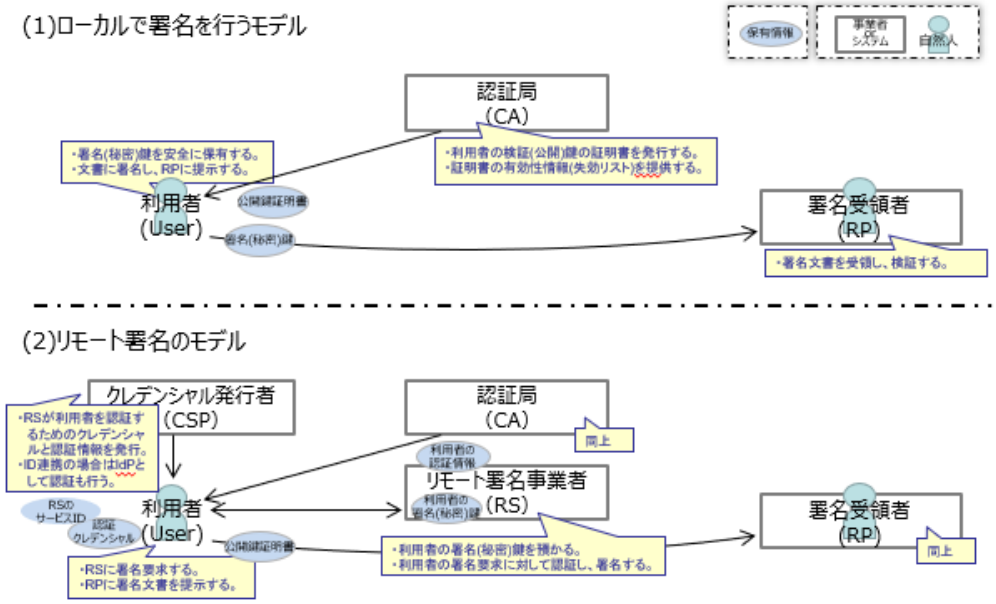


図 4-4　ローカル署名モデルとリモート署名モデルの比較（プレイヤと役割、保有情報）

参考として、電子署名法（認定認証業務含む）がカバーする範囲と定める要件を下図に、赤枠で示す。リモート署名の場合に、それらに追加して担保すべき範囲を青枠で示す。

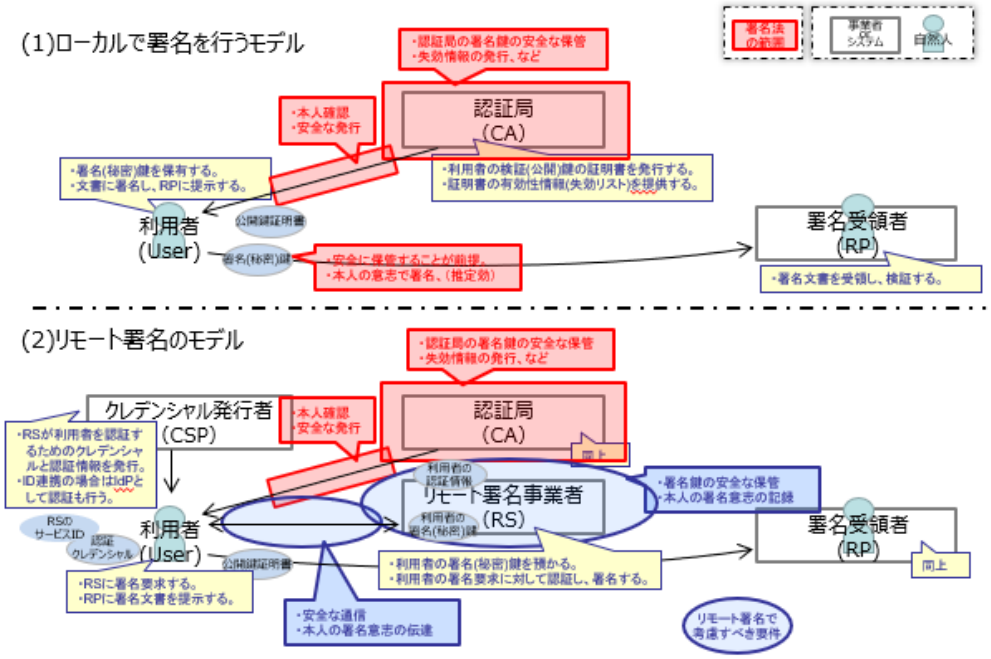


図 4-5　ローカル署名モデルとリモート署名モデルの比較（電子署名法要件との関係）

4.4 リモート署名鍵のライフサイクルと関連する処理

リモート署名鍵のライフサイクルに着目し、それに関連する処理と要件を整理する。リモート署名鍵のライフサイクルは、鍵生成登録フェーズ、署名利用フェーズ、利用停止フェーズで構成される。鍵生成登録フェーズは、署名鍵ペアを生成し CA が証明書を発行するとともに、リモート署名サービスを利用するための各種手続きと署名鍵のリモート署名サーバへの登録を行うフェーズ、署名利用フェーズは利用者がリモート署名サービスにアクセスし、署名対象データとリモート署名鍵を指定して電子署名を指示するフェーズ、利用停止フェーズは、利用者が利用中止する場合や鍵の期限切れ（更新の場合も含む）、失効などにより、リモート署名鍵に関する情報を廃棄するフェーズである。各フェーズとその時のリモート署名関連の処理を図 4-7 に示す。

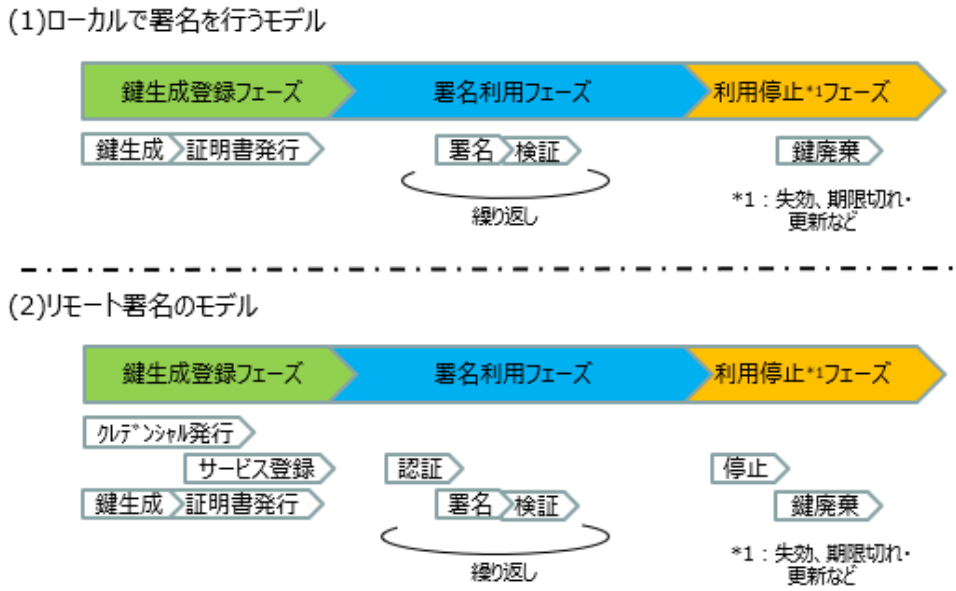


図 4-6　署名鍵のライフサイクルと関連の処理

これらの処理を、ローカル署名とリモート署名のモデルに表すと下図となる。以下、それに基づいて説明する。

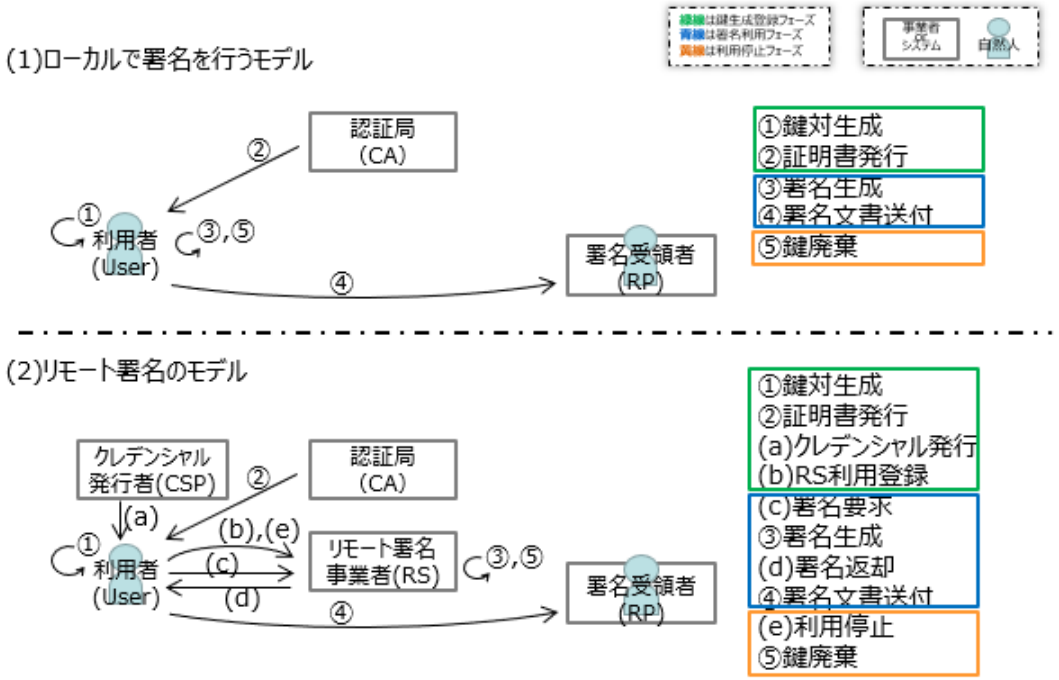


図 4-7　ローカル署名モデルとリモート署名モデルの比較（処理フロー）

(1) 鍵生成登録フェーズの処理

鍵生成登録フェーズにおいてローカル署名のモデルでは、①署名鍵生成・IC カード等への格納、② 公開鍵証明書発行を行うが、リモート署名のモデルではそれに加えて、(a) 利用者認証用 クレデンシャルの発行、(b) RSSP へのサービス利用のためのアカウント開設や署名鍵登録（インポート）、公開鍵証明書登録を行う。

(1A) 鍵生成処理

前述のように、鍵生成する主体は 3 通り考えられるが、いずれも利用者の申請がトリガーとなって行われる。CA に生成依頼した場合は、生成された鍵を利用者がいったん受け取って RSSP に登録する場合と、CA から直接 RSSP に（利用者の指示の下で）渡す場合が考えられる。RSSP で鍵生成した場合は、いったん公開鍵（検証鍵）を利用者が受け取ってから CA に証明書発行依頼するケースと、RSSP から直接 CA に依頼するケースが考えられる。利用者が鍵生成した場合も、証明書発行申請は RSSP に代行してもらうケースも考えられる。いずれも、利用者の意思のもとで行われることが必要である。

また、既存の鍵を利用することも可能である。（鍵重複や脆弱性などをどう確認するかは RSSP の課題である）

なお、署名鍵の移送による漏えいや鍵重複が発生し得ることを考慮した場合、RSSP で署名鍵を生成し移送しないことで安全な運用が可能になる。

(1B) 各種登録処理

利用者は、リモート署名サービスを利用するために必要な各種手続きと、署名鍵の RSSP への登録を行う。まず、利用者の本人性担保のための認証クレデンシャルを発行してもらう。RSSP から発行された ID で認証することでもよいが、保証レベルを高めるには第三者の発行するクレデンシャル（マイナンバーカードなど）を用いることが望ましい。リモート署名利用のために取得するものでなく、既存のクレデンシャルでもよい。

次に、RSSP に利用者登録（アカウント開設）を行い、署名鍵と公開鍵証明書を登録するとともに、本人と登録する署名鍵の紐付け（PIN の発行）を行う。(1A)の鍵生成を RSSP が行う場合は、登録（アップロード）は不要となる。

RSSP 側では、リモート署名事業者が管理するサーバ（以下「リモート署名サーバ」という）に、適切に保管、管理する必要がある。（5.5 節 に詳細を示す。）

(2) 署名利用フェーズの処理

ローカル署名のモデルでは、対象を選択して③署名生成を行うが、 リモート署名のモデルでは、リモート署名を利用するために RSSP にログインした後、(c)署名要求として署名対象データと署名指示（鍵の活性化）をリモート署名事業者に送信し、リモート署名事業者が③署名生成し、(d)署名（署名付き文書）が返却される。その際、利用者は意図したとおり

の署名がなされているか、署名検証することがある。

(2A) 認証処理

利用者が登録フェーズにおいて登録した利用者本人であることをクレデンシャル RS-C で認証する。RSSP は必要に応じて、CSP に確認を行う。

(2B) 署名処理

利用者は署名対象データのアップロードと署名する鍵の指定、署名指示を行い、RSSP では、署名鍵の活性化、署名対象データへの電子署名を行う。この際、署名指示として対象文書ごとに CM-C(PIN)を送信する場合と、あるまとまりの単位で署名アプリに委ねる場合がある。

署名対象データの送信の代わりに、そのハッシュ値のみを送信することも、RSSP のサービス仕様によっては可能である。

(2C) 署名検証処理

署名実施後、署名文書は利用者に返却され、利用者は RP に送付するなどに利用を行う。

ここで、利用者は、意図した文書に意図したとおりの署名が付与されているか、署名検証を行って確認する場合がある。

(3) 利用停止フェーズの処理

これは、何らかの理由により、そのリモート署名鍵の利用を停止するフェーズである。その理由としては、有効期限の終了（更新を伴う場合もある）、失効（更新または新規発行を伴う場合もある）、リモート署名サービスの利用終了、リモート署名事業者都合による終了がある。

利用者は RSSP に停止申請するとともに、場合によっては認証局に失効申請を行う。

リモート署名事業者は、登録されていた各種の利用者情報を破棄し、利用者の指示に基づき、リモート署名サーバ上に保管されている利用者の署名鍵等の安全な破棄などが必要である。

4.4.1 電子契約サービス等を想定したライフサイクルと処理

以下に電子契約サービス等を想定したシステム構成及び各段階における手順を示す。署名者が認証サービスに対して登録を行う際、詳細には CSP（クレデンシャル発行者や ID プロバイダ）とともに、RA（登録局）、CA（認証局）が連携する。さらに電子契約サービス等を想定した場合、SCA（署名生成アプリケーション）のサービス認証要求に対して正しい認証情報（アクセストークン）を提示することで電子契約サービスが利用できる。また、リモートで署名を行う場合には、RSSP（リモート署名サービス）の署名認可要求に対して正しい認証情報（アクセストークン）を提示することで署名鍵が活性化し、SCA から署名要求としてハッシュ値が RSSP に送信され、RSSP から署名値が SCA に送信される。

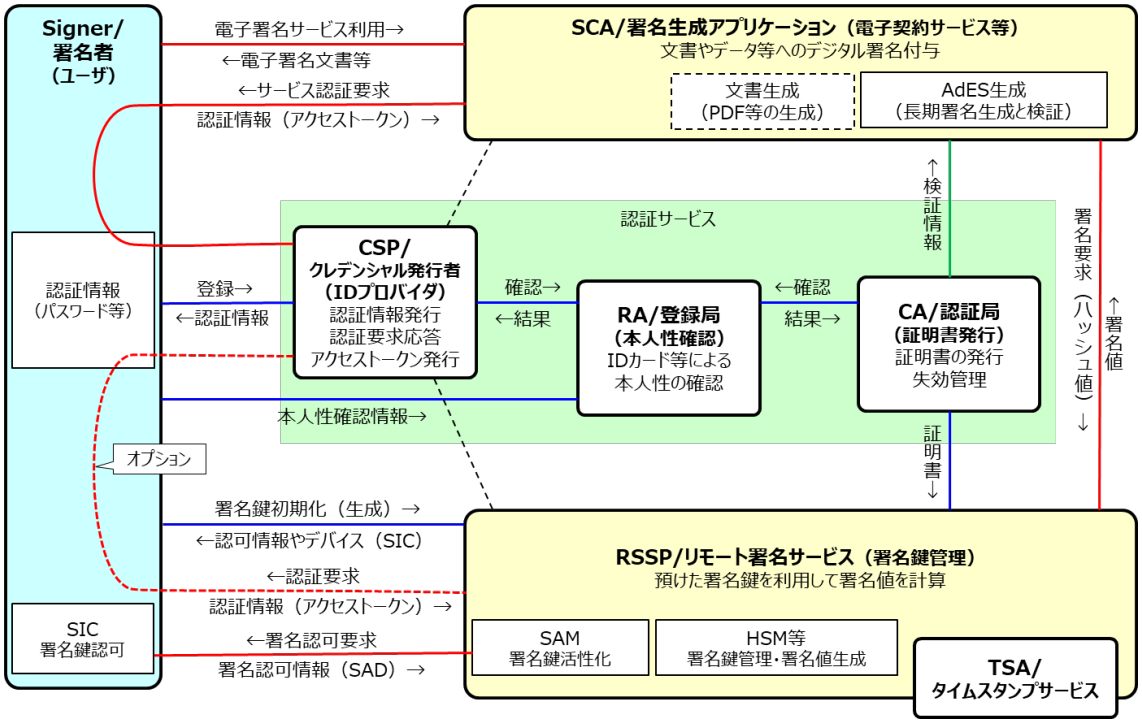


図 4-8　リモート署名モデルのシステム構成例

上記に関する登録、利用、停止の具体的な手順を以下に示す。

表 4-2 リモート署名の一般的な項目と手順

段階	項目	説明
登録	利用者登録	本人性を確認した上で署名サービスへ登録
	利用者クレデンシャル発行	利用者（認証用）クレデンシャルを発行

段階	項目	説明
	署名鍵登録（初期化）	利用者のみアクセス可能な署名鍵を登録 ※ 利用者登録時と兼ねる場合あり
	署名鍵クレデンシャル発行	署名鍵（認可用）クレデンシャルを発行 ※ 利用者クレデンシャル発行と兼ねる場合あり
利用	利用者認証	利用者クレデンシャルを確認して認証
	署名サービス利用	電子署名を必要とするサービスの利用
	署名鍵認可（署名処理）	署名時に署名鍵クレデンシャルを確認して認可
	署名結果取得	署名済み文書や署名完了の結果を発行
停止	署名鍵失効（削除）	署名鍵の利用の終了
	利用者退会	署名サービスの利用の終了

4.5 リモート署名のリファレンスモデル

4.5.1 リファレンスモデルの概要

この節ではリモート署名サービスの代表的なモデルを示す。基本的なモデルとして署名者が電子契約サービス等を介してリモート署名サービスの利用を開始する基本モデル 1 と、署名者のローカル環境で実行される署名アプリからリモート署名サービスを利用する基本モデル 2 を定める。また、参考として基本モデルの派生型をいくつか例示する。

4.5.2 基本モデル 1(SCA からのリモート署名サービス利用)

このモデルでは署名者は SCA(電子契約サービス等)からリモート署名サービスの利用を開始する。SCA を経由したリモート署名サービス利用は様々なバリエーションがあり得るが、このモデルはその基本形として定める。このモデルの派生形を 4.5.4 で例示する。

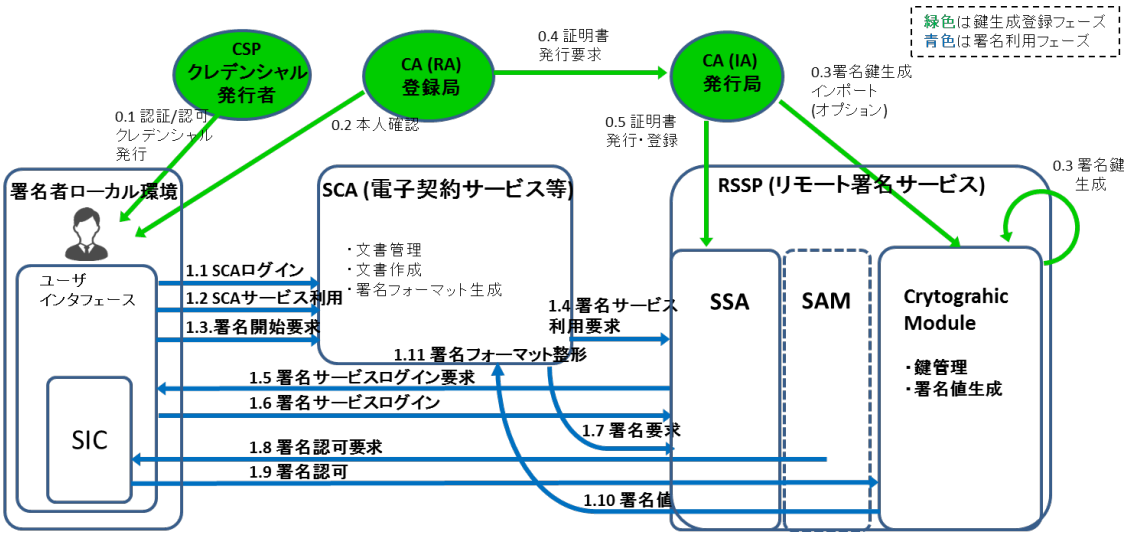


図 4-9　基本モデル 1 (SCA からのリモート署名サービス利用)

署名者は鍵生成登録フェーズにおいて、署名鍵の生成と登録、リモート署名サービス利用のための認証クレデンシャルの発行、署名実行のための認可クレデンシャルの発行、RA による本人確認を経た証明書発行を行う。リモート署名サービス利用のための認証クレデンシャルと、署名実行のための認可クレデンシャルは複数要素の認証方法の組み合わせもあり得る。各クレデンシャルの発行者が別の主体であることもあり得る。

また、SCA の利用に関しても、署名者は SCA 自身の要求に従った利用登録と SCA のサービスにログインするための認証クレデンシャルの発行を受ける。

署名利用のフェーズでは、署名者はまず SCA のサービスを通じて、署名対象文書を選択し、SCA に対して署名指示を行う（図 4-9 1.1～1.3)。そして、SCA から RSSP に対し

てその署名者に対する署名サービス利用開始を指示する（図 4-9 1.4）。その後、RSSP は、例えば HTTP のリダイレクション等の手法を用いて、署名者のユーザーインタフェースを通じてリモート署名サービスへのログインを要求する（図 4-9 1.5）。署名者はリモート署名サービスログイン用の認証クレデンシャルを用いてログインし、リモート署名サービス利用のセッションを開始する（図 4-9 1.6）。その後、SCA から RSSP に対して署名要求が行われる（図 4-9 1.7）。この署名要求には署名対象文書のハッシュ値が指定されることが考えられる。RSSP は署名実行の認可を署名者に対して求める（図 4-9 1.8）。署名者は署名認可のためのクレデンシャルを用いて、署名実行を認可する（図 4-9 1.9）。この署名認可用のクレデンシャルは PIN や、PIN を含んだ複数要素の認証方法を採用することがある。署名認可の後、RSSP は Cryptographic Module で管理されている署名者の署名鍵を活性化し署名対象のハッシュ値に対して署名演算を行う。そして、その署名値を SCA に返却する（図 4-9 1.10）。その後、SCA はその署名値を署名フォーマット等に格納するなどによって文書と対応付けて管理する（図 4-9 1.11）。

リモート署名サービスへのログインから署名要求に至るフローについては、サービスによって異なる。異なるバリエーションについては 4.5.4 節を参照されたい。

4.5.3 基本モデル 2（アプリからの直接利用）

このモデルでは署名者はスマートフォンや PC、デバイスのローカル環境にインストールされた署名アプリからリモート署名サービスに接続し署名値生成を行う。

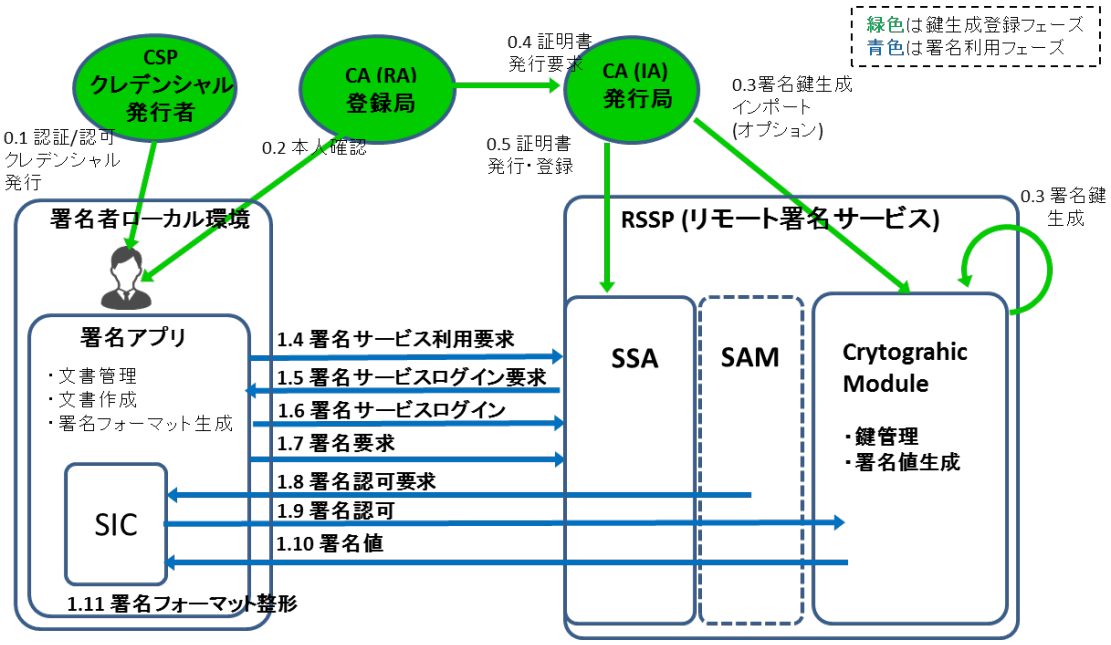


図 4-10　基本モデル 2 (アプリからの直接利用)

署名登録フェーズは基本モデル 1 と同様である。

署名利用のフェーズでは、署名者はまず署名アプリを起動し、RSSP にログインする（図 4-10 1.4～1.6)。その後、署名者は署名対象文書を選択し、RSSP に対して署名要求を行う（図 4-10 1.7)。このとき、署名アプリは署名対象文書を持ち、その文書データからハッシュ値を演算し、そのハッシュ値を署名要求に含めることが考えられる。その後、RSSP は署名実行の認可を署名者に対して求める（図 4-10 1.8)。署名者は署名認可のためのクレデンシャルを用いて、署名実行を認可する（図 4-10 1.9)。図 4-10 1.7～1.9 のフローはサービスにより、一組の要求応答メッセージとなっている場合も考えられる。

この署名認可用のクレデンシャルは PIN や、PIN を含んだ複数要素の認証方法を採用することがある。署名認可の後、RSSP は Cryptographic Module で管理されている署名者の署名鍵を活性化し署名対象のハッシュ値に対して署名演算を行う。そして、その署名値を署名アプリに返却する（図 4-10 1.10)。その後、署名アプリはその署名値を署名フォーマット等に格納するなどによって文書と対応付けて管理する（図 4-10 1.11)。

4.5.4 【参考】基本モデルの派生形

4.5.4.1 SCA を介した認証認可のケース

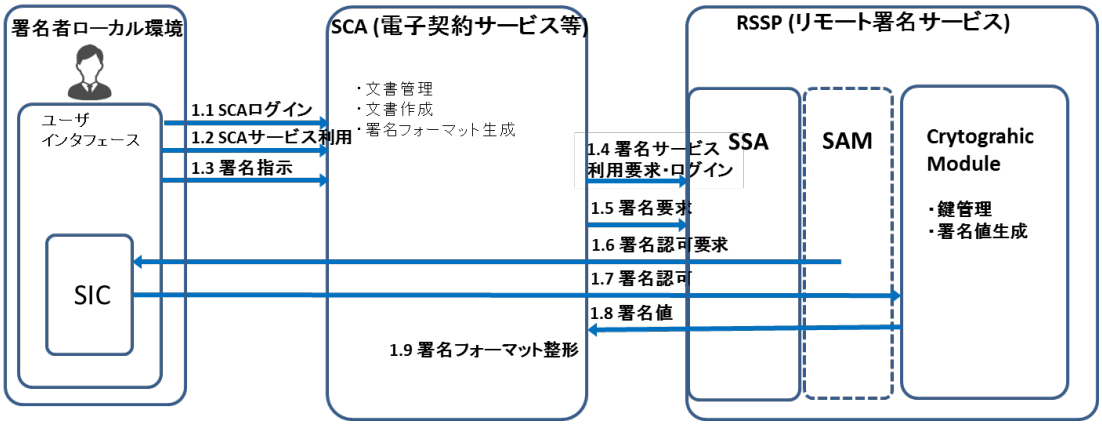


図 4-11　SCA を介した認証認可のケース

このモデルは RSSP のログイン時の認証や署名認可のフローを SCA が仲介するケースである。この場合、SCA が、認証クレデンシャルを用いた RSSP のログインや、署名者と RSSP の間のセッション、署名認可などの通信内容、クレデンシャルに関連する秘密の情報を SCA によって知られる可能性があるため、RSSP による技術的な対策や SCA での適切な運用が求められる。

図 4-11 1.4 での SCA から RSSP へのログイン要求は、署名者ごとの ID を使う場合もあれば、SCA と RSSP との間で契約された契約ごとの ID(例えば、あるユーザーグループごとに割り振られた ID や、企業や組織ごとに割り振られた ID など)が用いられることもが考えられる。一方、署名認可については署名者ごとに割り当てられた署名認可用クレデンシャルが用いられる。

4.5.4.2 認証連携を用いるケース

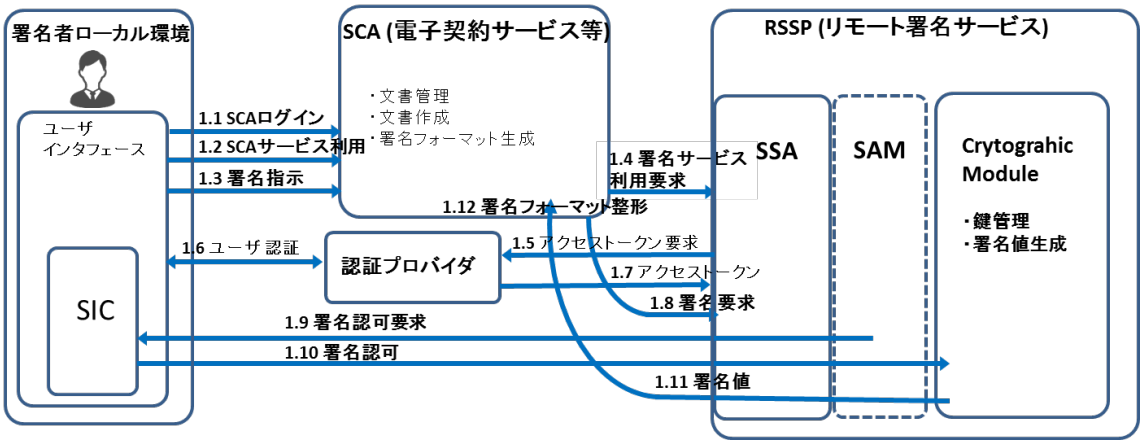


図 4-12　派生形（認証連携の例）

図 4-12 は RSSP のログイン時に外部の認証プロバイダを用いた認証連携を行う場合のモデルを示したものである。基本モデル 1 とほぼ同じフローであるが、RSSP のログイン時に認証プロバイダによるアクセストークンを使用する点が異なっている。RSSP は署名者のログインのために認証プロバイダにアクセストークンを要求する。署名者の認証やアクセストークン発行の認可が必要な場合には、認証プロバイダは署名者に認証やアクセストークン発行の確認を行った上で、RSSP に対してアクセストークンを発行する。RSSP はそのアクセストークンをもって署名者に対し RSSP のサービス利用を許可する。このモデルは SCA と異なる主体が認証プロバイダを運営する場合、4.5.4.1 の派生型のように、RSSP のログインのための秘密の情報を SCA に知られることがないことが利点である。

5 セキュリティ検討事項

5.1 電子署名の要件

電子署名には一般的に以下の性質が要求される。

- 電子署名によって意思を示す本人（署名者）を特定できること。
- 電子署名の対象となった文書が署名者本人の意図したものであること。
- 署名者本人が意図しない文書に対して電子署名が作成されないこと。

電子署名を PKI によって実現する場合、上記の性質は以下のより具体的な要件で示される。

- 署名鍵は署名者本人と対応づけられ、それ以外の者とは対応づけられない。
- 署名者本人はその署名鍵を用いて、意図したデータに対して署名を生成することができる。
- 署名者本人以外の者がその署名鍵を用いて、署名者本人が意図しないデータに対して署名データを生成することができない。

4 章で述べたように、リモート署名は署名鍵を第三者機関が管理するモデルであり、認証局からの署名者証明書の発行やリモート署名サービスでの署名鍵管理、署名鍵利用などで複数のシステム要素にまたがった処理フローによって成り立っている。各システム要素や処理フローの過程において、上記の電子署名として成立するための要件が覆される脅威への対策が必要となる。次節以降では、4.5 節の基本モデル 1 と基本モデル 2 を前提として、電子署名として成立するための要件を覆す要因となる脅威について整理する。

なお、SCA 及び署名者のローカル環境（署名アプリなど）については今後の課題である。

5.2 登録フェーズにおける脅威

登録フェーズにおける脅威は、署名者登録、署名者管理、証明書署名要求、署名鍵のインポートがある。

5.2.1 署名者登録等における脅威

5.2.1.1 RSSP において、RSSP の利用者 ID と RS-C を対応づける過程で、攻撃者が RS-C を不正取得する。[1]

5.2.1.2 攻撃者は、RA または CA への送信中に署名検証データを変更する。

5.2.1.3 攻撃者は登録中に登録情報を取得する。

5.2.1.4 攻撃者は登録時に署名者になりすます。

（注記１）認証局に対する一般的な脅威について
認証局における署名者証明書発行時の本人確認時におけるなりすましや、不正な証明書発行などといった認証局に対する脅威分析やリスク評価、それらを踏まえた運用規定の議論は従来からなされており、リモート署名固有ではないため、本書ではスコープ外とする。
認証局運用規定に関する別の文書を参照のこと。

5.2.2 署名者管理における脅威

5.2.2.1 攻撃者は特権ユーザを偽装し、登録情報を更新する。

5.2.2.2 攻撃者は更新中に認証情報を開示する。

5.2.3 証明書署名要求における脅威

5.2.3.1 攻撃者が CSR のデータを変更する。

5.2.3.2 攻撃者が詐称して CSR を行う。

[1] これらの脅威は「署名鍵は署名者本人と対応づけられ、それ以外の者とは対応づけられない」の性質を覆す要因となる。

5.2.4 署名鍵のインポートにおける脅威

5.2.4.1　署名鍵と署名鍵情報（鍵の属性や利用目的など）があり、攻撃者はこれらを扱い不正にインポートする。

5.2.4.2　攻撃者が他人の署名鍵を自らの鍵情報でインポートする。

5.2.4.3　攻撃者が自分の鍵を他人の鍵情報でインポートする。

5.2.4.4　攻撃者が同じ鍵を複数回インポートする。

なお、利用者属性等を割り当てた署名鍵もインポート可能である。

5.3 署名利用フェーズにおける脅威

署名利用フェーズにおける脅威は、署名利用フェーズ全般、鍵利用・管理における脅威と内部不正者による脅威がある。

5.3.1 利用フェーズにおける脅威

5.3.1.1　攻撃者は、認証情報を変更する。

5.3.1.2　攻撃者は、（SAP の 1 つ以上の）ステップをバイパスし、署名する。

5.3.1.3　攻撃者は、（SAP の 1 つ以上の手順を）再生し、署名する。

5.3.1.4　攻撃者は、偽造された認証情報を使用して署名者に偽装し、署名する。

5.3.1.5　攻撃者は、SAM への転送中に R.DTBS / R または R.SAD の情報を得る。

5.3.1.6　攻撃者は、SAM への転送中に R.DTBS / R を偽造し、署名する。

5.3.1.7　攻撃者は、（SAP での転送中に R.SAD を）偽造し、署名する。

5.3.1.8　攻撃者は、作成中または作成後または転送中に、署名を SAM 外で修正する。

5.3.1 鍵利用・管理における脅威

5.3.1.1 攻撃者は平文の共通鍵／秘密鍵に不正にアクセスし開示する。

5.3.1.2 攻撃者は共通鍵／秘密鍵を導出する。

5.3.1.3 攻撃者は CM 格納時に、鍵及び鍵の属性を不正に変更する。

5.3.1.4 攻撃者は CM 管理時に、鍵を誤用（許可されてない暗号機能・署名機能に利用）する。

5.3.1.5 攻撃者は鍵を乱用（許可されていない鍵を利用）する。

5.3.1.6 攻撃者はクライアントアプリケーションデータからの送信中の機密データを不正に開示する。（R.ClientData、および場合によっては R.RAD）

5.3.1.7 攻撃者はクライアントアプリケーションデータからの送信中の機密データを不正に変更する。（DTBS/R などの R.ClientData、認証/承認データ、または公開鍵（R.PubKe））

5.3.1.8 攻撃者は CM ハードウェアまたはソフトウェアの機能不全を発生させる。（温度、電力、HW の故障、SW の破損）

5.3.2 内部不正者による脅威

5.3.2.1 攻撃者（内部者）が運用管理者に詐称し署名鍵を利用する。

5.3.2.2 攻撃者（内部者）が監査者に詐称しログを得る。

5.3.2.3 攻撃者（内部者）が署名鍵の活性化情報を得る。

5.4 利用停止(破棄)フェーズにおける脅威

5.4.1.1 攻撃者（本人以外）が利用停止（破棄依頼）する。

5.4.1.2 利用停止の再送攻撃（利用停止依頼を傍受し、変更して再送する）。

6 セキュリティ対策事項

5 章のセキュリティ検討事項に対するセキュリティ要件を示す。セキュリティ対策事項は、一般的なセキュリティ要件（本ガイドライン・パートⅠの 6.1 節）、セキュリティ機能要件として署名鍵活性化モジュールに関する要件（本ガイドライン・パートⅡの 3 章）、署名値生成モジュールに関する要件（本ガイドライン・パートⅡの 3 章）で構成する。

6.1 一般的セキュリティ要件

6.1.1 役割・組織の管理

6.1.1.1 リモート署名サービスは異なる特権をもつ役割をサポートすること。

6.1.1.2 リモート署名サービスは少なくとも次の特権を持つ役割をサポートすること。

セキュリティ統括責任者（Security Officers）： セキュリティポリシーの確実な実施に対する責任を有し、セキュリティ関連情報を管理する者。

システム管理者（System Administrators）：リモート署名サービス関連システムのインストール、設定及びメンテナンスの権限を有する者。セキュリティ関連情報へのアクセス権はない。

システム運用担当者（System Operators）：リモート署名サービスの運用に関する責任を有し、システムバックアップ及びリカバリの権限を有する者。

システム監査者（System Auditors）：システム運用がセキュリティポリシーに従った運用であるか監査し、其の為にアーカイブや監査ログを確認する権限を有する者。

6.1.1.3 リモート署名サービスは少なくとも以下の特権をもたない非特権役割をサポートすること。

署名者（Signer）：SAP によって SAD をリモート署名サービスに受け渡すことにより、文書又は DBTS/R に署名する者。
秘密鍵と公開鍵をリモート署名プロバイダに送ることが認められている。

SCA：署名者による署名を得るために、リモート署名サービスに DTBS/R リクエストを送ることが認められている。

RA：CSR（証明書発行要求）に対して、リモート署名サービスに公開鍵

証明書を送ることが認められている。

CA：署名者からの要請に従い、リモート署名サービスプロバイダに署名者の秘密鍵と公開鍵を送ることが認められている。

6.1.1.4 全ての特権をもつ役割を一人で担ってはならない。また、一人で二つ以上の特権を持つ役割を担うべきではない。

6.1.1.5 特権を持つ役割のユーザと特権を持たない役割に係るユーザは互い関与しないこと。

6.1.1.6 リモート署名サービスはセキュリティ統括責任者とシステム監査者を兼任しないことを保証すること。

6.1.1.7 リモート署名サービスは、システム管理者の役割及び/又はシステム運用者の役割を担うユーザがシステム監査者及び/又はセキュリティ責任者の役割を担うことないことを保証すること。

6.1.1.8 特権を持つ役割のユーザは適切に指名を受け、訓練を受けたものであること。

6.1.1.9 特権をもつ役割のユーザのみが、ハードウェアへの物理的にアクセス可能であり、リモート署名サービスの管理ができること。

Note：非特権ユーザのアクセスの際には、特権を持つ役割を担う者が同行し監視すること。

6.1.1.10 特権をもつシステムユーザのみが全ての関連するアプリケーション及びインターフェースを通してリモート署名サービスを管理する広範な権限をもつこと。

6.1.1.11 システム運用

6.1.1.11.1. リモート署名サービスは以下を実現する為に必要な内容を含むマニュアルを提供すること。

- 正しく安全な運用
- システム故障のリスクが最小限となるような方法での設置
- システム及び扱う情報の完全性を保証するために、ウィルス及び悪意のあるソフトウェアから保護

6.1.1.11.2. リモート署名サービスのプロバイダは、6.1.1.2 で要求されている 4 つの特権

をもつ役割の責任を対象とするシステム文書を提供すること。それには次を含むべきである。

- インストールガイダンス
- 管理ガイダンス
- ユーザガイダンス

6.1.1.12 時刻同期

電子署名の生成と検証には時刻が重要な要素となっている為、リモート署名サービスが標準時刻に適切に同期していることが必要である。

6.1.1.12.1. リモート署名サービス提供者は、リモート署名サービスの時刻精度とその確認方法を表明すること。

6.1.1.12.2. 監査済みイベントの時刻精度を確認するために、標準時刻源と適切に同期している時刻源を使用するべきである。

6.1.1.12.3. 証明書の有効期限が切れているかどうかを確認するために、UTC と適切に同期している時刻源を使用すること。

6.1.2 識別及び認証

6.1.2.1 リモート署名サービスは各ユーザがリモート署名サービスに対してアクションを認める際に、各ユーザの識別と認証を実施すること。

6.1.2.2 ログアウト後の再認証を必須とすること。

6.1.2.3 認証データの組み合わせを使用する場合、容易に予測できないものであること。

6.1.2.4 特権ユーザについては、有効なセッションの時間を定義し、一定時間以上の経過によってセッションを停止する等の措置を取り、セッション乗っ取りのリスクを低減すること。

6.1.2.5 認証失敗

6.1.2.5.1. ユーザ認証エラーの回数を管理し、限度を超えたユーザ認証エラーが発生した

場合、一定期間或いは管理者によるアンロックが行われるまで、同一ユーザによるユーザ認証を認めないこと。

6.1.3 システムへのアクセスコントロール

6.1.3.1 リモート署名サービスは、特定のユーザだけがアクセスを許可されたシステム及びユーザオブジェクトに対し、アクセスコントロールを実施すること。

6.1.3.2 リモート署名サービスは機密性の高い残存情報へのアクセスコントロールを実施すること。

6.1.4 監査及びログ

6.1.4.1 少なくとも以下のイベントを記録すること。

- 重要なリモート署名サービス環境、鍵管理イベント（生成、使用及び破壊）
- ユーザ署名イベント（署名者の署名鍵を使った正常な署名及びDTBS/Rリクエスト管理）
- SAP中のユーザ認証
- リモート署名サービスによる署名者のSAD管理
- 監査データ生成機能の開始及び停止
- 監査パラメータの変更

ユーザ署名イベントには、署名鍵の関連証明書に関する情報を含むこと。
リモート署名サービスへのすべてのアクセス試行をログするべきである。

6.1.4.2 リモート署名サービスは、外部記憶装置への監査情報伝達に失敗した場合の措置を定めること。

6.1.4.3 監査データ可用性の保証

6.1.4.3.1. リモート署名サービスは監査データを保持し、すべての監査データを保管する措置をとること。

6.1.4.3.2. 監査機能は情報を追記するのみであること。

6.1.4.3.3. リモート署名サービスは、監査証跡に保存された監査レコードに不正削除が行われないよう保護すること。

6.1.4.3.4. 監査レコードは、外部記憶装置にアーカイブしたときに削除することができる。

6.1.4.4 監査データパラメータ

6.1.4.4.1. すべての監査レコード（サービス別監査ログを含む）は、次のパラメータを含むこと。

- イベントの日時
- イベントのタイプ
- アクションに対して責任を負う実体（ユーザ、管理者、プロセス等）の識別
- イベントの成否

6.1.4.5 選択可能な監査レビュー

6.1.4.5.1. リモート署名サービスは、イベントの日付、タイプ及び/又はユーザ ID による監査ログの検索を可能にすること。

6.1.4.5.2. 監査レコードは、システム監査者が理解しやすい形式で処理及び提示が可能であること。

6.1.4.6 制限付き監査レビュー

6.1.4.6.1. リモート署名サービスは、監査記録へのアクセスについて、システム監査者等一部のユーザを除きデフォルト設定で拒否すること。

6.1.4.7 警告の生成

6.1.4.7.1. リモート署名サービスは、リモート署名システムの本章で識別されているセキュリティ要件を満たす能力に影響を与える可能性のある異常イベントに対して通知する警告を適時に生成すること。

その他の異常イベントについても検知されたときに警告を発するメカニズムを実行するべきである。警告は関連のある管理者への通知のきっかけとなるべきである。

警告はまた、潜在的な攻撃パスをカットするなど、潜在的な攻撃に対応する措置を始動させることができる。

ユーザアクティビティに関係する異常イベントの例には次があげられる（がこれに限られるものではない）：

- 標準的な使用時間を超えたユーザアクション
- 異常速度で行われるユーザアクション（人以外の介入を検知するため）
- 規定プロセス内の標準的なアクティビティを省いたユーザアクション
- 重複するユーザセッション

6.1.4.8 監査データの完全性の保証

6.1.4.8.1. リモート署名サービスは、監査データの完全性を保証すること。

6.1.4.8.2. リモート署名サービスは、監査データの完全性を検証する機能を提供すること。

6.1.4.9 監査タイミングの保証

6.1.4.9.1. 監査イベントの時刻精度を保証するために、要件 SRG_SO.2.2J を適用する。

6.1.5 アーカイブ

6.1.5.1.1. リモート署名サービスは、外部メディアでのアーカイブ生成の能力をもつこと。保存及び情報提供の観点から適切な外部メディアを選択するべきである。

6.1.5.1.2. すべての監査ログをアーカイブすること。

6.1.5.1.3. 各アーカイブエントリにはアーカイブの時刻を含むこと。

6.1.5.1.4. アーカイブには、リモート署名サービスユーザパスワードなどの機密性の高いセキュリティパラメータを含まないこと。

6.1.5.2 アーカイブデータの完全性

6.1.5.2.1. アーカイブにおけるエントリの不正変更が行われないよう防止すること。不正変更を検知するために、完全性を検証するメカニズムを実行すること。

6.1.6 内部不正対策

内部不正対策は、6.1.1 役割・組織の管理及び 6.1.4 監査及びログを参照。

6.1.7 バックアップ・リカバリ

6.1.7.1 バックアップ情報の完全性及び機密性

6.1.7.1.1. バックアップ情報の完全性の検証を可能にするメカニズムによる変更からバックアップを保護すること。

6.1.7.1.2. 高感度のセキュリティパラメータ及びその他機密情報は、機密性及び完全性を確保するために保護された形で保管すること。

6.1.7.2 リカバリ

6.1.7.2.1. リモート署名サービスは、バックアップからシステムの状態を復元できる回復機能をもつこと。

6.1.7.2.2. 十分な特権を持つ役割にリンクしているユーザは、要求に応じてバックアップからの回復機能を起動することができること。

6.1.8 コアコンポーネント

6.1.8.1 署名鍵活性化

対策レベル	対策事項
最低限	• 署名鍵の活性化（鍵認可）を行うために、単要素認証しなければならない。 • 利用者認証で鍵認可を行ってもよい。
推奨	• 署名鍵の活性化（鍵認可）を行うために、複数要素認証しなければならない。 • 利用者認証と別に鍵認可を行わなければならない。
附帯	• 上記の推奨に追加して、本ガイドライン（パートⅡ）で示した要件に適合認証した署名鍵活性化モジュールでの署名鍵の活性化（鍵認可）しなければならない。

6.2 組織・運営

組織のセキュリティ対策及び運営に関しては、主に ISO/IEC27002（JIS Q 27002）の「6 情報セキュリティのための組織」に規定する管理策の推奨基準を適用するものとする。以下に、リモート署名事業に係る管理対策を示す。

リモート署名に関係するプレイヤであるリモート署名事業者、クレデンシャル発行者、認証事業者については、組織・運営のために ISO/IEC27002 を参照して情報セキュリティ管理策を実施する。
なお、以下に ISO/IEC27002 に記載されていない詳細を以下に説明する。

6.2.1 職務の分離

リモート署名に関係するプレイヤであるリモート署名事業者、クレデンシャル発行者、認証事業者については、同一法人がすべての機能の提供を行う事が可能である。また、リモート署名事業者においては特に重要な職務の権限の分離を行う必要がある。（詳細は 6.1.1 管理、参照）

6.2.2 事業継続管理

リモート署名事業者は、困難な状況（adverse situation）（例えば，危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。特に、利用者の秘密鍵の管理については、危殆化が疑われる状況を生み出さないよう必要な要求事項をあらかじめ定めておく必要がある。（例示：危殆化が疑われた状況では、鍵を失効する等の対策を行うこと）

6.2.3 コンプライアンス

リモート署名の利用分野は、電子商取引、電子契約、電子申請など様々であるが、リモート署名の応用分野は、電子署名済みデジタルドキュメントの長期的な保存などもあり、利用分野の個別法を遵守する必要がある。リモート署名事業者やリモート署名を利用したアプリケーションサービス提供者などは、自らのサービスが個別法の、どの要件に対してどのように対応しているか、また利用者に対しては、どのような運用や追加的対策が求められるか示す必要がある。自らのサービスポリシーに重要項目を記載し、利用者に対して自らのサービスの理解を促す必要がある。

7 参照情報

[1] EN 419 241-1 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

[2] EN 419 241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

[3] EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

[4] ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

[5] ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

[6] NIST Special Publication 800-63 Revision 3 Digital Identity Guidelines

[7] Cloud Signature Consortium (CSC), Architectures, Protocols and API Specifications for Remote Signature applications

[8] 日本データセンター協会、 Japan Data Center Council（JDCC)、データセンターセキュリティガイドブック、データセンターファシリティスタンダード

[9] ISO/IEC 27002 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範 Information technology -- Security techniques -- Code of practice for information security management

[10] ISO/IEC 27017:2015 情報技術－セキュリティ技術－ISO/IEC27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[11] 電子署名及び認証業務に関する法律

[12] 電子署名及び認証業務に関する法律施行規則

[13] 電子証明書に格納された属性情報の信頼性と利用に関するガイドライン、電子認証局会議

[14] 行政手続におけるオンラインによる本人確認の手法に関するガイドライン、2019 年（平成 31 年）2 月 25 日、各府省情報化統括責任者（ＣＩＯ）連絡会議決定

[15] 電子契約活用ガイドライン Ver.1.0（2019 年 5 月)、公益社団法人日本文書情報マネジメント協会

[16] 電子文書の信頼性向上ガイドライン第 1 版（2019 年 3 月)、公益社団法人日本文書情報マネジメント協会

附録

リモート署名の検討については、経済産業省の「平成２８年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））報告書」において、リモート署名のガイドラインを作成する際には、より詳細な検討を行うことが示されている、この重要検討項目は、リモート署名の利用を考えるうえでも重要な項目であるため、以下にこれらの重要検討項目について、本ガイドラインで検討した結果を説明する。

1　署名結果の確認

リモート署名では、利用者（署名者）が意図した署名対象文書に正しく署名されたことを確認する必要がある。少なくとも、誰が（利用者 ID)、何に（署名対象)、署名処理を行った（処理結果）であるかを表示する。その他、署名時刻や検証結果等も表示して署名結果を利用者（署名者）に確認させる。これらの確認項目の詳細化を検討し、必要応じて求められる要件を検討する必要がある。

表 A-1 署名結果の表示項目

項目	要求	概要
処理結果	必須	正常に署名処理が完了したかどうか
利用者 ID	任意	認証クレデンシャル（RS-C）のうち利用者識別の ID 等 ※ ただし利用者 ID が秘匿対象であれば表示しない。
署名対象	任意	署名の対象となるファイル名、または署名する内容等
署名文書	任意	生成された署名文書のファイル名等
署名時刻	任意	リモート署名を行った時刻 ※ タイムスタンプの時刻が望ましいがシステム時刻でも良い。
署名者名	任意	署名証明書の Subject 要素等 ※ 判別が付く場合には CN 項目だけでも良い。
検証結果	任意	署名の検証結果（改ざん有無や署名フォーマット準拠等）を表示 ※ 第三者による検証（認証局による検証等）が望ましい。 ※ 必要に応じて検証レポートを表示できるとなお良い。

2　利用停止処理について

利用停止の要因としては、有効期限の終了（更新を伴う場合もある）、失効（更新または新規発行を伴う場合もある）、リモート署名サービスの利用終了、リモート署名事業者都合による終了がある。

(1) 有効期限の終了（更新を伴う場合もある）の場合
RSSP は、鍵の有効期限を管理している場合、期限前に利用者に通知し、更新を要求される場合は、旧鍵を廃棄し、鍵生成登録時の手順に従い新鍵を生成・登録する。旧鍵の署名を継続する必要がある場合、新鍵による旧鍵の証明書の相互認証証明書を発行してもらうケース等もある。

(2) 失効（更新または新規発行を伴う場合もある）
利用者または CA 等から何らかの要因（危殆化など）で鍵の失効を通知された場合、RSSP は速やかに旧鍵を廃棄する。（要検討）

(3) リモート署名サービスの利用終了
利用者からリモート署名サービスの利用終了を通知された場合、RSSP は速やかに鍵を廃棄、または利用者に引き渡して廃棄する。（要検討）

(4) リモート署名事業者都合による終了
RSSP のサービス終了やインシデント（漏洩など）が発生した場合、鍵が継続利用できる場合は利用者に引き渡し、鍵の継続利用不可の場合は速やかに廃棄するとともに然るべき措置を講じる。（要検討）

いずれの場合も、リモート署名事業者は使用しなくなった利用者の署名鍵等の重要情報を安全かつ確実に破棄（削除）する必要がある。

3　システムログと監査ログ

リモート署名は、電子契約や電子申請などの利用も想定されている為に、自動的に保存されるシステムログの他に、監査ログが必要となる。監査ログでは監査人が調査を行う際に必要となる情報、つまり「いつ」「だれが」「何をしたか」を確認できる必要がある。また法規制や運用ポリシーに違反をしていないか、また標準に準拠しているかを判断する材料となる情報である。

自動的に保存されるシステムログは、例えば NIST SP 800-92 「コンピュータセキュリティログ管理ガイド」等の標準仕様を参考にして適切かつ必要な情報が保存されるように設定と運用を行う。SP 800-92 ではセキュリティログとして、「セキュリティソフトウェア」「オペレーティングシステム」「アプリケーション」の 3 種類が定義されているが、これらがシステムログの分類と言える。

表 A-2 NIST SP 800-92 によるシステムログの分類

システムログの分類	概要
セキュリティソフトウェア	認証サーバ、侵入検知、ウイルス・マルウェア対策等の独立したセキュリティソフトウェアが生成するログ。
オペレーティングシステム	システムイベント等のログ。適切な OS 設定により必要なログを出力する。
アプリケーション	利用されるアプリケーションと連携する全サーバ・システムの利用ログ。利用者の要求とその応答、アカウントの情報操作（認証成否や変更等）、利用状況（トランザクション数等）、重要な運用アクション（アプリケーション起動・終了や運用状況、設定変更情報等）を保存。

システムログを保護する為には、システム時刻の同期、改ざん防止策、アーカイブとローテーション等のポリシーを適切に設定して運用を行う必要がある。またパスワード等の認証秘匿情報は保管してはならない。

監査ログは大別すると、利用者や管理者の行動を追う為の「トランザクションログ」と、リソースアクセスに関する「アクセスログ」に分けられる。時間帯や ID 等を指定して監査ログの生成を可能にすべきである。監査ログは、なりすましや改ざんの有無等の判断材料となる情報である。

表 A-3 監査ログの分類

監査ログの分類	概要
トランザクション	利用者および管理者の行動を追跡する為のログ情報。
アクセス	システムイベント等のログ。適切な OS 設定により必要なログを出力する。

システムログから監査ログを生成する際のシステムログの項目等は、事前に検討を行い決めておく必要がある。またシステムログを解析するツールの利用も検討すべきである。監査人は監査証跡の 1 つとして監査ログを利用することができる。監査証跡は監査ログ以外にも、入手可能なあらゆる情報を使い構成された情報である。

4　設置・環境

電子署名を行うために必要な符号類 を適正に管理できるようにするという観点からリモート署名サーバの設備環境の詳細を検討した。なお、詳細化の検討については、ISO/IEC 27002、ISO/IEC 27017 をベースに特定認証業務の認定に係る調査表（一般財団法人日本情報経済社会推進協会)、データセンターセキュリティガイドブック（日本データセンター協会、 Japan Data Center Council（JDCC)）を参照した。これらの参照文献を基に検討した結果、物理的及び環境的セキュリティについては、以下を前提とする。

- 該当する地域標準、国内標準及び国際標準が要求するレベルの抵抗力を確立するために、隔壁と併せて、警報機能を備え、監視し、試験する。
- ハウジング、クラウド環境の両方においては、本事項は契約等によりサービス提供企業にて対応されるものとする。

4.1　物理的セキュリティの考え方

利用者の署名鍵、または利用者の署名鍵の暗号化で使用する共通鍵を保護するために、署名を行う装置（CM を構成するための設定済みソフトウェアまたはハードウェア）は、通常のデータセンター環境よりも高いセキュリティが必要である。このため、一般のコンピュータラックを設置する環境を「コロケーションエリア」と定義する。この「コロケーションエリア」よりも高いセキュリティの環境を定義して、当該エリア（または領域）を「CM 設置室」（仮称）と呼んで明確に区別する。

なお、上記の高いセキュリティの環境で CM をハードウェア（HSM）またはソフトウェアで構成する場合に、以下の考え方があるが、ビジネスモデルに基づき検討が必要。

1. 高いセキュリティの「CM 設置室」の領域に設置することが望ましい。
2. HSM を組み込むサーバ類は一般環境である「コロケーションエリア」に置いても良いものとする。
3. CM をソフトウェアで構成する場合には、不正アクセスを行おうとすると自己破壊（署名鍵などの重要情報のゼロ化）を行う HSM の耐タンパ性の特性と同等のレベルでのデータ保護が可能かをリモート署名事業者が検討する必要がある。

4.2　情報セキュリティポリシーセキュリティを保つべき領域

4.2.1　物理セキュリティの境界

「リモート署名サーバ」を設置する建物、当該建物内の「CM 設置室」、及びその「コロケーションエリア」を物理的セキュリティ境界として定める。「リモート署名サーバ」を設置する建物（又は敷地)、当該建物内の「CM 設置室」、及び「CM 設置室」の「コロケーションエリア」を物理的セキュリティ境界として定める。「CM 設置室」に、より高いセキュ

リティレベルが要求される場合に「コロケーションエリア」を設けることがある。「CM 設置室」と「コロケーションエリア」がある場合、「コロケーションエリア」を通過しなくては「CM 設置室」にアクセスすることはできないものと定義する。

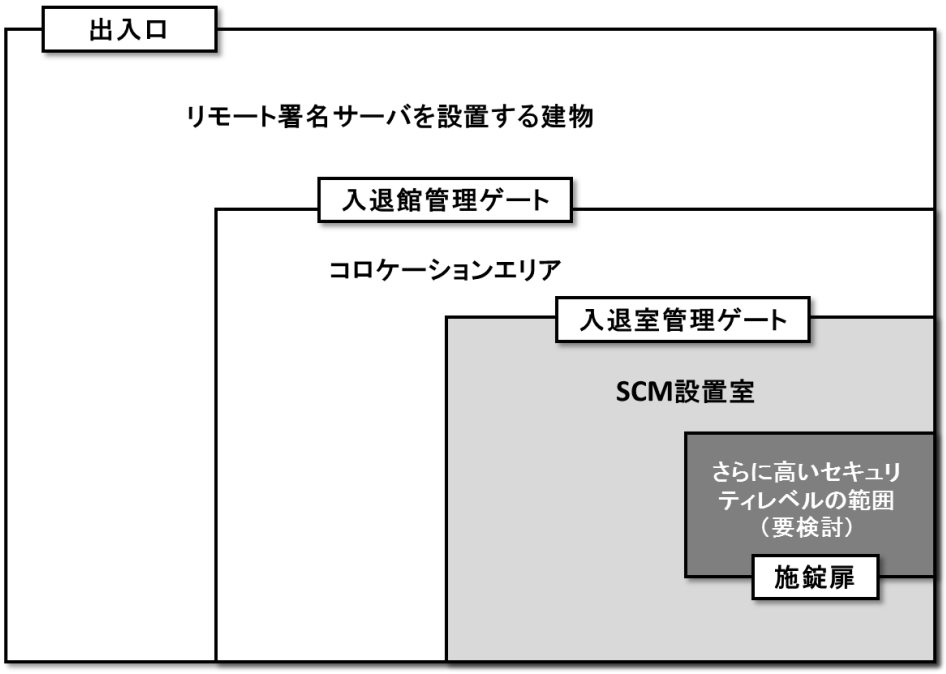


図 A-1 物理的セキュリティ境界のイメージ図

4.2.2 物理的入退管理策

「リモート署名サーバを設置する室」には、認可されたものだけにアクセスを許可するために以下の事項を考慮することが望ましい。

イ　入室する二以上の者の身体的特徴の識別（あらかじめ登録された指紋、虹彩その他の個人の身体的特徴の照合を行うことをいう。）によって入室が可能となること。

ロ　入室者の数と同数の者の退室を管理すること。

4.2.3 オフィス、部屋及び施設のセキュリティ

「リモート署名サーバ」の設備の所在を示す掲示をしてはならない。

4.2.4 外部及び環境の脅威からの保護

自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計し，適用しなければならない。

イ 「リモート署名を行うサーバを設置する室」を建築物の 2 階以上に設置することが望ま

しい。建築物の 1 階以下に設置する場合には、水害に対して十分な対策を講じる。特に、過去に水害がある場合又は海抜ゼロメートル地帯等である場合には、浸水対策を講ずる。

4.2.5　セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関して手順を設計し、適用することが望ましい。

イ　「リモート署名サーバを設置する室」から利用者の署名鍵、または利用者の署名鍵の暗号化で使用する共通鍵を作業者が取得できない対策を講じることが望ましい。

5　装置

5.1　装置の設置及び保護

装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し，保護しなければならない。

5.2　資産の移動

「リモート署名サーバ」は「リモート署名サーバを設置する室」から事前の許可なしで持ち出してはならない。又、事前の許可なしに「リモート署名サーバを設置する室」に持ち込みを行ってはならない。

5.3　構外にある装置及び資産のセキュリティ

構外にある資産に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用しなければならない。

5.4　無人状態にある利用者装置

利用者の署名鍵、または利用者の署名鍵の暗号化で使用する共通鍵を保管している記憶媒体は、物理破壊することが望ましい。又、「リモート署名サーバを設置する室」内で実施することが望ましい。

5.5　装置のセキュリティを保った処分又は再利用

利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない。

イ　退室完了後、認証設備室内はモーションセンサを働かせるなどで、無人の「リモート署名サーバを設置する室」内で動きを検出した場合に警報が発せられる。

ロ　遠隔監視カメラで撮影している映像及び記録された映像は被写体が明確に確認できる。無人の場合にも常夜灯を点灯させて、被写体が明確に確認できるようにする。

リモート署名ガイドライン(案)

パートⅡ．署名活性化モジュール

日本トラストテクノロジー協議会（JT2A）

2019 年 12 月 18 日時点版

目　　次

1 署名活性化モジュールの概要

リモート署名サービス（RSSP）で実装する署名活性化モジュール（SAM）の概要を以下に示す。署名活性化モジュールは、署名者または署名生成アプリケーション（SCA）の鍵認可要求を処理し、署名鍵を活性化するモジュールである。なお、下図は論理的な構成例である。

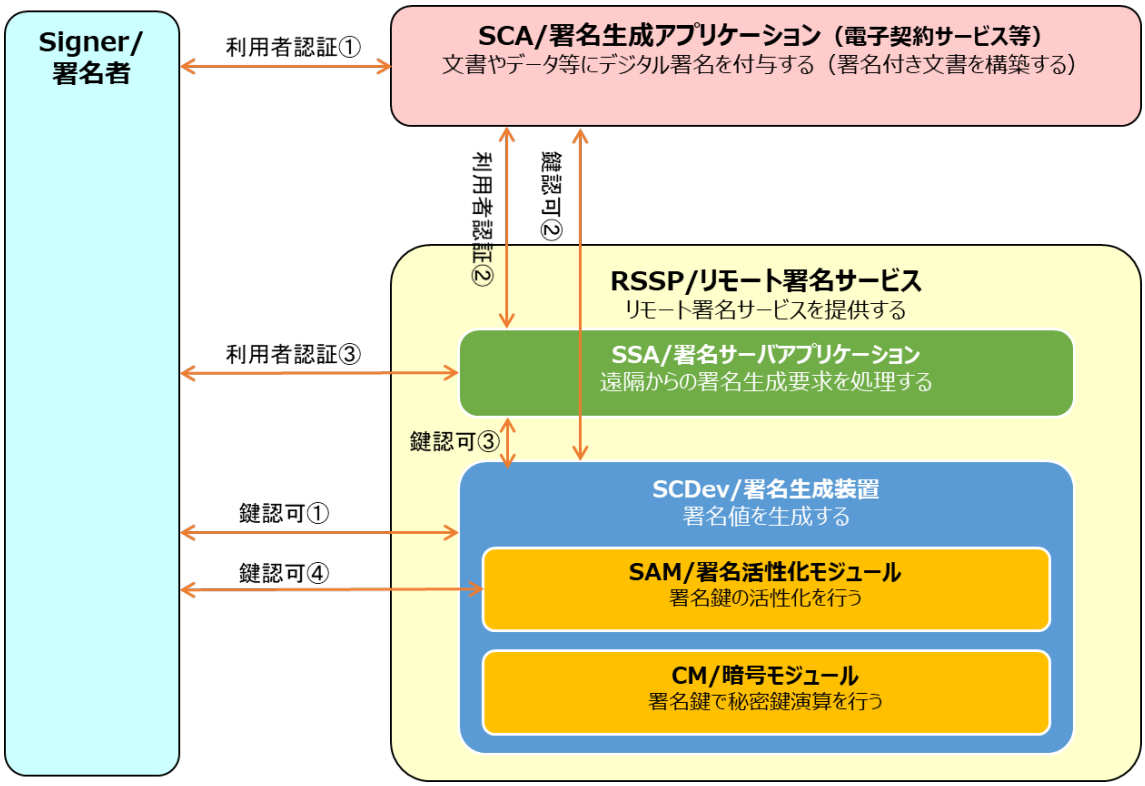


図 1-1　リモート署名サービスの構成例

2 セキュリティ検討事項

以下に本ガイドライン・パートⅠの 6 章のセキュリティ検討事項から署名活性化モジュールに関する脅威のみを示す。

2.1 登録フェーズにおける脅威

2.1.1 署名者登録等における脅威

2.1.1.1　RSSP において、RSSP の利用者 ID と RS-C を対応づける過程で、攻撃者が RS-C を不正取得する。[2]

2.1.1.2　攻撃者は、RA または CA への送信中に署名検証データを変更する。

2.1.1.3　攻撃者は登録中に登録情報を取得する。

2.1.1.4　攻撃者は登録時に署名者になりすます。

2.1.2 署名者管理における脅威

2.1.2.1　攻撃者は特権ユーザを偽装し、登録情報を更新する。

2.1.2.2　攻撃者は更新中に認証情報を開示する。

（注記１）認証局に対する一般的な脅威について
認証局における署名者証明書発行時の本人確認時におけるなりすましや、不正な証明書発行などといった認証局に対する脅威分析やリスク評価、それらを踏まえた運用規定の議論は従来からなされており、リモート署名固有ではないため、本書ではスコープ外とする。認証局運用規定に関する別の文書を参照のこと。

2.1.3 証明書署名要求における脅威

2.1.3.1　攻撃者が CSR のデータを変更する。

2.1.3.2　攻撃者が詐称して CSR を行う。

2.1.4 署名鍵のインポートにおける脅威

[2] これらの脅威は「署名鍵は署名者本人と対応づけられ、それ以外の者とは対応づけられない」の性質を覆す要因となる。

2.1.4.1　署名鍵と署名鍵情報（鍵の属性や利用目的など）があり、攻撃者はこれらを扱い不正にインポートする。

2.1.4.2　攻撃者が他人の署名鍵を自らの鍵情報でインポートする。

2.1.4.3　攻撃者が自分の鍵を他人の鍵情報でインポートする。

2.1.4.4　攻撃者が同じ鍵を複数回インポートする。

なお、利用者属性等を割り当てた署名鍵もインポート可能である。

2.2 署名利用フェーズにおける脅威

署名利用フェーズにおける脅威は、署名利用フェーズと内部不正者による脅威がある。

2.2.1 利用フェーズにおける脅威

2.2.1.1　攻撃者は、認証情報を変更する。

2.2.1.2　攻撃者は、（SAP の 1 つ以上の）ステップをバイパスし、署名する。

2.2.1.3　攻撃者は、（SAP の 1 つ以上の手順を）再生し、署名する。

2.2.1.4　攻撃者は、偽造された認証情報を使用して署名者に偽装し、署名する。

2.2.1.5　攻撃者は、SAM への転送中に R.DTBS / R または R.SAD の情報を得る。

2.2.1.6　攻撃者は、SAM への転送中に R.DTBS / R を偽造し、署名する。

2.2.1.7　攻撃者は、（SAP での転送中に R.SAD を）偽造し、署名する。

2.2.1.8　攻撃者は、作成中または作成後または転送中に、署名を SAM 外で修正する。

2.2.2 内部不正者による脅威

2.2.2.1　攻撃者（内部者）が運用管理者に詐称し署名鍵を利用する。

2.2.2.2　攻撃者（内部者）が監査者に詐称しログを得る。

2.2.2.3　攻撃者（内部者）が署名鍵の活性化情報を得る。

2.3 利用停止(破棄)フェーズにおける脅威

2.3.1.1　攻撃者（本人以外）が利用停止（破棄依頼）する。

2.3.1.2　利用停止の再送攻撃（利用停止依頼を傍受し、変更して再送する)。

3 署名活性化モジュール（Signature Activation Module）のセキュリティ機能要件

2 章のセキュリティ検討事項に対する署名鍵活性化モジュールに関するセキュリティ機能要件を示す。

3.1 登録

3.1.1 署名者登録等における機能要件

3.1.1.1 SAM は、R.Signer に関連するデータが完全性で保護され、必要に応じて機密性が保護されることを保証しなければならない。
※この対策方針は 6.1.3 の一部として求められる対策である。

3.1.1.2 SAM は、R.Signer の一部として署名認証データ R.Reference_Signer_Authentication_Data をセキュアに扱うことができなければならない。

3.1.1.3 SAM は、署名モジュール署名鍵ペアを生成するために暗号モジュールを安全に使用でき、R.Signing_Key_Id と R.SVD を R.Signer に割り当てることができなければならない。

3.1.1.4 SAM は、R.SVD が認証前に変更されていないことを保証するものとする。

3.1.2 署名者管理における機能要件

3.1.2.1 SAM は、SAM に対するアクションが実行される前に特権ユーザを持つ管理者が認証されることを保証しなければならない。
※この対策方針は 6.1.1 の一部として求められる対策である。

3.1.2.2 SAM は、署名者又は特権ユーザの制御下で、R.Signer、R.Reference_Signer_Authentication_Data、R.Signing_Key_Id 及び R.SVD に対する変更が行われることを保証しなければならない。
※この対策方針は 6.1.1 の一部として求められる対策である。

3.1.3 証明書署名要求における機能要件

3.1.3.1 CSR はセキュアチャネルで通信をする。

3.1.3.2 本人と CSR の内容を確認する。

3.1.4 署名鍵のインポートにおける機能要件

対策レベル	対策事項
最低限	• 署名者を確認した署名鍵をインポートしなければならない。
推奨	• 上記の最低限に追加し、署名鍵のインポートは、信頼できる CA(認証局)からのみに限定しかねればならない。
附帯	• 署名鍵をインポートしてはならない。

3.2 署名利用時

3.2.1 署名利用（一般）の機能要件

3.2.1.1 SAM は、SAD を検証しなければならない。つまり、SAD 要素間にリンクが存在することを確認し、署名者が強く認証されていることを確認する必要がある。
※この対策方針は 6.1.2 の一部として求められる対策である。

3.2.1.2 SAM は、以下を提供するシグネチャアクティベーションプロトコル（SAP）のサーバ側エンドポイントを実装しなければならない。
- 署名者認証
- 送信された SAD の整合性
- 少なくとも機密情報を含む SAD の要素の機密性
- リプレイ、バイパス、偽造からの保護

3.2.1.3 SAM は、SAM への送信時に、認証用データの使用を危うくする攻撃に対してシグネチャ認証データが確実に保護されることを保証しなければならない。

3.2.1.4 SAM は、R.DTBS/R が SAM に送信されたときに完全性を保証されることを保証しなければならない。

3.2.1.5 SAM は、SAM 内部で署名を改変できないことを保証しなければならない。

3.2.1.6 SAM は、特権ユーザーの制御下で R.Privileged_User 及び R.Reference_Privileged_User_Authentication_Data の変更が行われることを保証するものとする。
※この対策方針は 6.1.1 の一部として求められる対策である。

3.2.1.7 SAM は、R.Privileged_User に関連するデータが完全性で保護され、必要に応じて機密性が保護されることを保証しなければならない。

3.2.2 共通（システム）における機能要件

3.2.2.1　SAM は、特権ユーザーが SAM の操作を実行するときに、SAM が特権ユーザーを認証することを保証しなければならない。
※この対策方針は 6.1.1 の一部として求められる対策である。
※この対策方針は 6.1.2 の一部として求められる対策である。

3.2.2.2　これらの目的のために使用される別の乱数発生器のプロトコルまたはシードデータにおいて、鍵として使用するために SAM によって生成された乱数は、乱数が予測できず、十分なエントロピーを有することを保証するために定義された品質基準を満たさなければならない。

3.2.2.3　SAM は、特権ユーザにより R.TSF_Data の改変が許可され、不正な改変が検出されることを保証しなければならない。
※この対策方針は 6.1.1 の一部として求められる対策である。

3.2.2.4　SAM は、R.AUDIT に対する改変が検出されることを保証しなければならない。
※この対策方針は 6.1.4 の一部として求められる対策である。

3.3 利用停止

3.3.1　利用停止を依頼した利用者を確認しなければならない

3.3.2　利用停止の再送攻撃への耐性がなければいない

4 参照情報

[1] EN 419 241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

[2] ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

[3] ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

[4] Cloud Signature Consortium (CSC), Architectures, Protocols and API Specifications for Remote Signature applications

[5] 電子署名及び認証業務に関する法律

[6] 電子署名及び認証業務に関する法律施行規則

附録

リモート署名の検討については、経済産業省の「平成２８年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））報告書」において、リモート署名のガイドラインを作成する際には、より詳細な検討を行うことが示されている、この重要検討項目は、リモート署名の利用を考えるうえでも重要な項目であるため、以下にこれらの重要検討項目について、本ガイドラインで検討した結果を説明する。

1　署名鍵活性化

リモート署名で署名を行うためには、リモート署名の利用者認証後に、署名対象文書と署名指示及び署名鍵を活性化するクレデンシャル（CM-C）を利用するアクセス認可が必要である。リモート署名の具体的なサービスを想定した場合、利用者はリモート署名サービスにログインして署名を行うが、多量の署名を行う場合に、署名の都度 CM-C の入力を行う場合と、一度の CM-C の入力で多量の署名を処理する場合が考えられる。理想を言えば署名の都度 CM-C の入力を行うことが望ましいが、ここでは複数署名を 1 回の CM-C により行う処理に関して整理する。なお同じ CM-C の利用は 1 回のみに限定すべきであり、同じ CM-C を繰り返し利用可能とすることは、中間者攻撃等を容易くする可能性があり推奨されない。

SCA が CM に対して CM-C を使って署名鍵活性化する場合、一度に複数の署名対象文書（ハッシュ値）と署名指示を指定する方法と、CM-C から SAD のようなトークンを生成し SAD を更新しつつ繰り返し署名要求を行う方法の、2 通りが考えられる。また両方を組み合わせることでより多量の署名要求に応えることも可能となる。

方法１）一度に複数の署名対象文書と署名指示を指定する方法

SCA が複数の署名対象文書のハッシュ値を計算して、CM へ対する署名要求時に複数のハッシュ値を指定する処理方法。結果として SCA は複数の署名値を受け取り、各署名値を利用して複数の署名文書を作成する。なお先に CM-C からトークン（SAD）を発行して利用しても良い。

図 B-1 一度に複数の署名対象を指定する場合のシーケンス図

方法 2）トークンの更新を利用して繰り返し署名要求をする方法

最初の CM-C からトークン（SAD）を生成して、署名要求にはトークンを利用する。CM に対する 1 回の署名要求の終了後に、利用済みトークンから新たなトークンを更新して取得することで、繰り返し署名要求を行えるようにする処理方法。

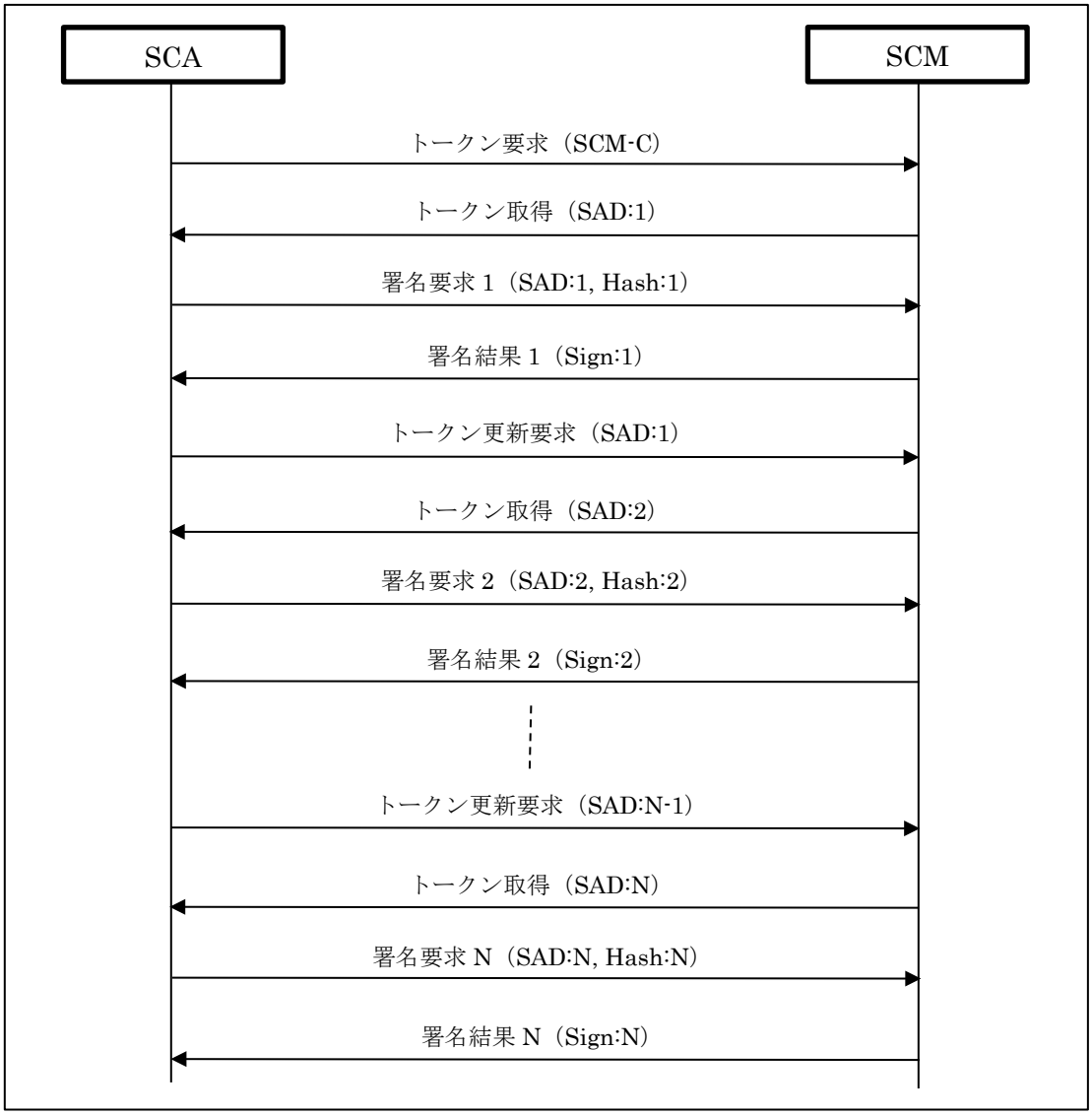


図 B-2 トークンを更新しつつ複数の署名対象を指定する場合のシーケンス図

2　CSC クラウド署名コンソーシアムの API 仕様

クラウド署名コンソーシアム（CSC）は、ソリューション、テクノロジー、トラストサービスプロバイダを含む業界や学術界の専門家から成る国際的な協力グループによって設立された団体で、以下を目的として活動している。CSC の API 仕様書はメールアドレスを登録することで、無償で取得できる。

(1) 共通のアーキテクチャ設計と構成要素構築によって、ソリューション、テクノロジー、トラストサービスプロバイダ間の相互運用性を実現
(2) サービス間の連携を相互運用可能にするべくプロトコルと API の技術仕様開発
(3) オープンスタンダードとして API 仕様を公開
(4) クラウド署名のコンセプトを促進

CSC の API 仕様は、署名利用フェーズのみとなっている。将来的には鍵生成登録フェーズと利用停止フェーズも追加される可能性はあるが、現時点では標準化されていない。CSC の API 仕様に準拠することで、署名サービスとトラストサービスプロバイダ等のサービス間の署名利用フェーズにおける相互運用性が保証される。API 仕様は HTTP/HTTPS を使った RESTful な API と JSON の電文から構成される。

CSC の API 仕様は、欧州の eIDAS に準拠している。この為に CSC の API 仕様を eIDAS 準拠の実装例として見ることもできるが、Qualified（認定）レベルだけでは無く、Advanced（高度）レベルでもあり、レベルによって要求される仕様が異なる点には注意して読み解く必要がある。CSC 仕様に準拠したサービスは、欧州以外の米国や日本でも既に提供されている。その点ではグローバル仕様に対応していると言える。リモート署名を検討する際には目を通すべき API 仕様の 1 つであるだろう。

リモート署名ガイドライン(案)

パートⅢ．署名値生成モジュール

日本トラストテクノロジー協議会（JT2A）

2019 年 12 月 18 日時点版

目　　次

1 署名値生成モジュールの概要

リモート署名サービス（RSSP）で実装する署名値生成モジュール（CM）の概要を以下に示す。署名値生成モジュールは、署名者または署名生成アプリケーション（SCA）の鍵認可要求の処理に基づいて、署名活性化モジュール（SAM）によって署名鍵が活性化した状態で署名値を生成するモジュールである。なお、下図は論理的な構成例である。

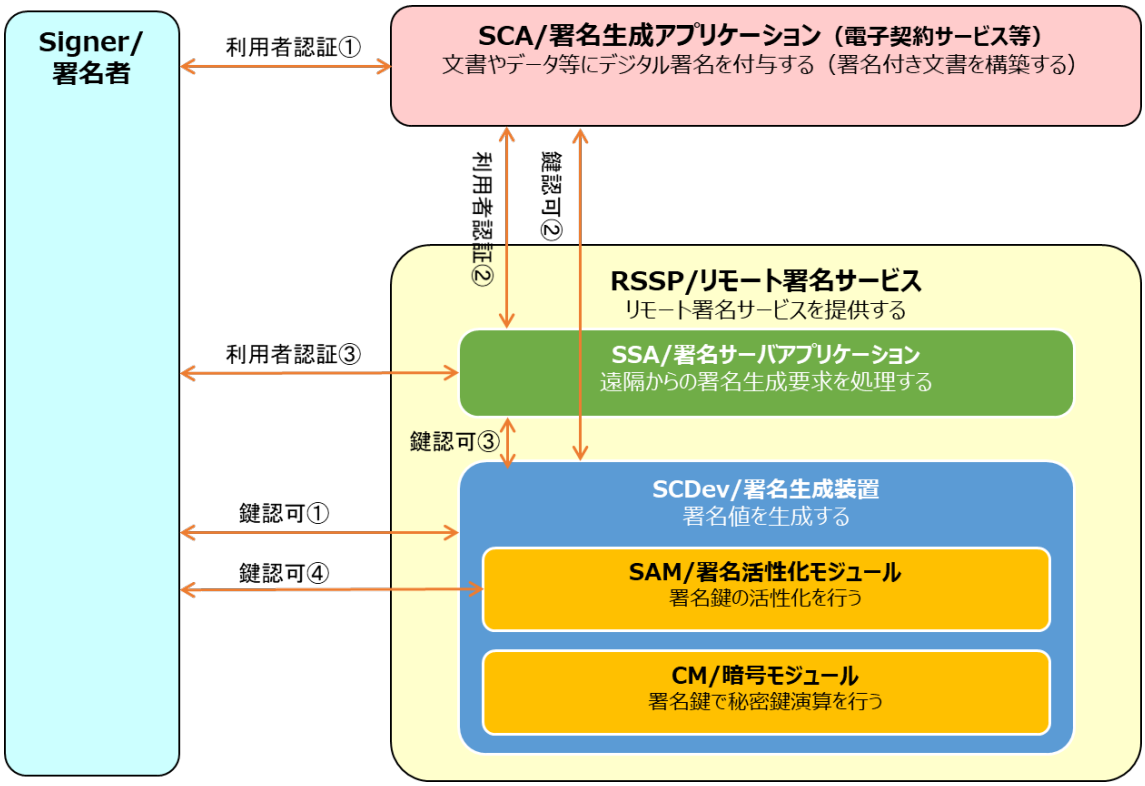


図 1-1　リモート署名サービスの構成例

2 セキュリティ検討事項

以下に本ガイドライン・パートⅠの 6 章のセキュリティ検討事項から署名値生成モジュールに関する脅威のみを示す。

1. 攻撃者は平文の共通鍵／秘密鍵に不正にアクセスし開示する。
2. 攻撃者は共通鍵／秘密鍵を導出する。

3. 攻撃者は CM 格納時に、鍵及び鍵の属性を不正に変更する。
4. 攻撃者は CM 管理時に、鍵を誤用（許可されてない暗号機能・署名機能に利用）する。
5. 攻撃者は鍵を乱用（許可されていない鍵を利用）する。
6. 攻撃者はクライアントアプリケーションデータからの送信中の機密データを不正に開示する。（R.ClientData、および場合によっては R.RAD）
7. 攻撃者はクライアントアプリケーションデータからの送信中の機密データを不正に変更する。（DTBS/R などの R.ClientData、認証/承認データ、または公開鍵（R.PubKe））
8. 攻撃者は CM ハードウェアまたはソフトウェアの機能不全を発生させる。（温度、電力、HW の故障、SW の破損）

3 署名値生成モジュール（Cryptographic module）のセキュリティ機能要件

2 章のセキュリティ検討事項に対する署名値生成モジュールに関するセキュリティ機能要件を示す。

1. 平文の秘密鍵を CM の外部に持ち出し利用できないようにしなければならない。（鍵が後述する 9 の方法で安全にエクスポートされている場合を除く）。

2 CM は、信頼できる第三者機関によって使用に適していると認められ承認された暗号アルゴリズム※を提供しなければならない。
※電子署名法施行規則第二条、及び CRYPTREC 暗号リスト等

3 鍵の価値および重要な属性（秘密または公開）は、その完全性が許可なく変更されることがないよう、CM によって保護しなければならない。

4 CM は、CM の使用を許可する前に、すべてのサブジェクトに対して認証/許可チェックを実行しなければならない。
- CM の管理者
- CM 暗号機能の利用者（セキュアチャネルを使用するクライアントアプリケーション）。
- 秘密鍵のユーザー

※この対策方針は本ガイドライン・パート I の 6.1.2 の一部として求められる対策である。

5　任意の鍵（秘密または公開）は、それが使用されることが許可されている暗号機能または操作（例えば暗号化または署名等）の目的が定義されていなければならない。

6　CM は、秘密鍵を使用するために承認と再承認が必要とされる場合に、明確に規定された制限を定義し適用することを要求しなければならない。
※この対策方針は本ガイドライン・パート I の 6.1.2 の一部として求められる対策である。

7　CM は、クライアント間の伝送中に機密データ（認証/許可データなど）の機密性を保護するために使用できるクライアントアプリケーションへの安全なチャネルを提供しなければならない。
※この対策方針は本ガイドライン・パート I の 6.1.3 の一部として求められる対策である。

8　CM は、クライアントアプリケーションと CM の間の伝送中に機密データ（署名されるデータ、認証/許可データ、または公開鍵証明書など）の保全性を保護するために使用できる安全なチャネルをクライアントアプリケーションに提供しなければならない。
※この対策方針は本ガイドライン・パート I の 6.1.3 の一部として求められる対策である。

9　CM は、送信中のデータの機密性と完全性を保護する安全な方法を使用することによってのみ、秘密鍵のインポートとエクスポートを許可しなければならない。なお、割り当てられたキーはインポートまたはエクスポートできないことが望ましい。
※この対策方針は本ガイドライン・パート I の 6.1.3 の一部として求められる対策である。

10　秘密鍵を含む、利用者データをバックアップするために CM によって提供されるいかなる方法も、データのセキュリティを保護し、許可された管理者によって制御されなければならない。
※この対策方針は本ガイドライン・パート I の 6.1.3 の一部として求められる対策である。

11　使用される鍵、認証/許可データ、または他の乱数ジェネレータのシードデータとして使用するために生成され、クライアントアプリケーションに提供される乱数は、乱数が予測不可能であり、十分なエントロピーがなければならない。

12　CM は、改ざんからセキュリティ機能を保護するための機能を提供しなければならない。特に CM は、意図された環境の範囲内でのあらゆる物理的操作を CM の管理者が検出できるようにしなければならない。

13　CM は、以下のような他のセキュリティプロパティの弱体化または失敗を引き起こす可能性のある障害を検出しなければならない。

- 通常の動作範囲外の環境条件（温度および電力を含む）。
- 重要な CM ハードウェアコンポーネント（RNG を含む）の故障。
- CM ソフトウェアの破損。

また、障害が検出されると、CM はそのセキュリティと、それに含まれ管理されているデータのセキュリティを維持するための措置をとらなければならない。

14　CM は、セキュリティ関連イベントの監査記録を作成し、イベントの詳細とそのイベントに関連するサブジェクトを記録しなければならない。
CM は、監査ログの改ざん防止（防止または検出）を提供することによって、監査レコードが偶発的または悪意のあるレコードの削除または変更から保護されることを保証しなければならない。
※この対策方針は本ガイドライン・パート I の 6.1.4 の一部として求められる対策である。

15　署名鍵生成

対策レベル	対策事項
最低限	• 署名鍵ペアの生成は、本ガイドライン 3.2 で指定した暗号アルゴリズム、鍵長、パラメータで生成しなければならない。
推奨	• 上記の最低限に追加し、署名鍵ペアの生成は、CMVP 等の認証取得の HSM で生成しなければならない。
附帯	• 署名鍵ペアの生成は、欧州の署名生成デバイスの要件及び本ガイドライン（パートⅢ）の要件に適合したデバイスで生成しなければならない。

4 参照情報

[1] EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

[2] ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

[3] ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

[4] Cloud Signature Consortium (CSC), Architectures, Protocols and API Specifications for Remote Signature applications

[5] 電子署名及び認証業務に関する法律

[6] 電子署名及び認証業務に関する法律施行規則

附録

リモート署名の検討については、経済産業省の「平成２８年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））報告書」において、リモート署名のガイドラインを作成する際には、より詳細な検討を行うことが示されている、この重要検討項目は、リモート署名の利用を考えるうえでも重要な項目であるため、以下にこれらの重要検討項目について、本ガイドラインで検討した結果を説明する。

1　鍵管理について

鍵管理は、CM で実施する内容であり、以下の CM は論理的なコンポーネントである。そのため、実際には複数のハードウェアやソフトウェアで構成される場合もある。

1.1　鍵の生成

- 安全なアルゴリズム(電子署名法施行規則第二条、及び CRYPTREC 暗号リスト等)を利用して鍵生成を行う必要がある。
- 鍵生成時に鍵の属性を考慮に入れて生成を行う必要がある。

1.2　鍵のインポート

- 署名アプリケーション（SAP）と署名生成モジュール（CM）間はセキュアチャネルを利用することが望ましい。
  - 例）通信の暗号化（TLS）等のセキュリティプロトコルを利用する。デバイスドライバと CM 間のデータについて暗号化機能などを検討する。
- インポート対象の鍵は暗号化されていることが望ましい。
  - 例）PKCS#11 が定義しているラップ（暗号化）を利用する。HSM が提供するインポート機能を利用する。
- 暗号化に利用する鍵は暗号対象の鍵と同等のセキュリティ強度を持つことが望ましい。

1.3　鍵の属性管理

- 鍵は、アルゴリズム、利用用途、許可設定などを特定する属性情報と紐付けた状態で管理する。
- 例えば、署名鍵は署名のみ利用可能とする等、鍵の属性を設定することで用途を限

定的にする。

1.4 鍵の利用

- CM 内の鍵を利用する場合は CM に対して認証処理が必要であること。
- 鍵は認定された暗号アルゴリズム（電子署名法施行規則第二条、及び CRYPTREC 暗号リスト等）で処理すること。
- 暗号処理の演算過程で生成される中間値には CM 外部からアクセスできないこと。

1.4.1 鍵の保管

鍵の保管に関しては、ISO/IEC 27002 と同等の対策が必要である。

- 全ての暗号鍵は、改変及び紛失から保護することが望ましい。さらに、署名鍵及びプライベート鍵は、認可されていない利用及び開示から保護する必要がある。
- 鍵の生成、保管及び保存のために用いられる装置は、物理的に保護されることが望ましい。

1.4.2 鍵に関する設定変更

HSM において鍵を利用可能または利用不可にする等の設定変更については、別の管理策が必要となる（この管理策は、技術的な対策だけではなく、組織・運用の対策も含まれる）。以下に詳細を示す。

- HSM を利用可能に設定変更する場合、及び HSM を利用不可に設定変更する場合には、複数の者によって行う必要がある。
- 一方、上記以外のすべての HSM に関する作業を複数人で作業しなくともよい。
  - 例えば、署名者本人の署名鍵の HSM へのインポートが必要と仮定すると、その作業（インポート作業）はシステムやアプリケーションで対応する場合も想定できる。

1.5 鍵のエクスポート

- 署名アプリケーション（SAP）と署名生成モジュール（CM）間はセキュアチャネルを利用することが望ましい。
  - 例）通信の暗号化（TLS）等のセキュリティプロトコルを利用する。
- エクスポート対象の鍵は暗号化されることが望ましい。
  - 例）PKCS#11 が定義しているラップ（暗号化）を利用する。HSM が提供するエクスポート機能を利用する。

1.6 鍵の破棄

- 利用廃止時に鍵は廃棄され、鍵が不正利用されるリスクをなくすこと。

  - 例えば、HSM を用いている場合に、HSM 内部の鍵を廃棄する場合は、HSM が提供する鍵消去方法を利用すること。
- バックアップした鍵については、鍵が不正利用されるリスクをなくすこと。

1.7 鍵の利用に関するログ

- 以下の作業時には CM を利用する署名アプリケーション(SAP)もしくは CM(HSM 等）が提供するログ機能を利用してログを取得することが望ましい。
  - HSM 設定（HSM 設定ポリシー等など含む）
  - 鍵生成
  - 鍵廃棄
- HSM 自体にログをアーカイブ保存する機能がない場合には、アーカイブされたログを管理するシステムを用意する必要がある。

署名鍵の生成環境の区別

署名鍵の生成環境により、署名鍵の存在場所すなわち署名の生成場所（リモート署名事業者かそれ以外か）を明らかにできる場合があり、このことが、署名への信頼性、署名時刻への信頼性、不正な署名があった場合の責任の所在などに影響を及ぼす。

署名鍵の存在場所がリモート署名事業者に限定される場合、次の効果が期待できる。

効果１：リモート署名事業者が署名鍵を安全に管理することにより利用者による署名鍵の杜撰な管理に起因した不正署名の可能性が排除されるため、署名への信頼性が高まる。

効果２：リモート署名事業者が署名生成処理が取得する時刻の発生源である時計を厳密に管理していることにより、署名生成時に付与される時刻への信頼性が高まるため、長期署名における署名タイムスタンプの取得を省略できる可能性がある。

効果３：不正な署名が生成された場合、署名鍵の存在場所がリモート署名事業者に限定される場合は責任の所在をリモート署名事業者に求めることができるが、そうでない場合、責任の所在を明らかにすることは困難になる。(そもそも、リモート署名事業者により署名鍵が安全に管理されている場合、不正な署名が生成されるリスクが生じる機会は極めて小さくなるはずである)

本ガイドラインではリモート署名で利用する署名鍵の 3 通りの生成パタンにおいて、署名鍵が存在する場所に対する考え方は次の通りである。

①リモート署名事業者が生成する場合

i 一定の要件を満足する HSM を利用する場合、署名鍵の唯一性（HSM 内にのみ存在すること）が保証される。

ii HSM を利用しないが安全な鍵の運用管理がなされている場合、署名鍵の唯一性（リモート事業者内のみに存在すること）が保たれていると考えて良い。

②認証事業者が生成する場合

i 署名鍵が認証事業者からリモート署名事業者のみに送付する場合、認証事業者が安全な鍵の運用管理を行なっていれば、署名鍵の唯一性（リモート事業者内のみに存在すること）が保たれていると考えて良い。

ii 署名鍵が認証事業者から利用者を経由してリモート署名事業者に渡す場合、署名鍵の唯一性は保証されない。

③利用者が生成する場合

i 署名鍵の唯一性は保証されない。

つまり、署名鍵を①リモート署名事業者が生成する場合、及び②-i 認証事業者が生成する場合でかつ署名鍵が認証事業者からリモート署名事業者のみに送付される場合には、署名鍵の存在場所はリモート署名事業者に限定される。

ただし、リモート署名事業者内で署名を生成する場合、利用者の署名に対する多重署名としてリモート署名事業者の署名を付与することにより、②-ii や③の場合であっても、署名の生成場所を明らかにできるため、効果１～３が生じることとなる。

このように署名鍵の生成環境は重要な要素である。リモート署名を安全に利用するためには、リモート署名事業者の HSM で鍵生成したものか否かについて利用者や署名検証者及び第三者から区別できるような対策を検討する必要がある。また、署名鍵の生成環境の情報や設定を変更できないようにする必要も考えられるため、これらに求められる要件を具体化し、対応方法を検討することが必要となる。さらに、既存の認定制度や監査制度においても、これらの情報を監査や認定の対象とし、監査結果や認定結果を公表することも検討する必要がある。