資料１

トラストサービスに関する現状

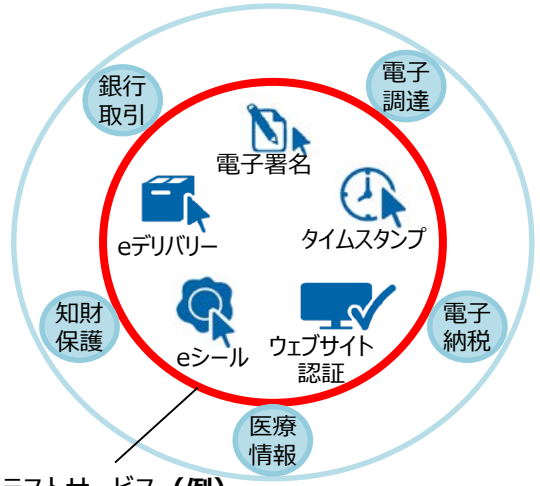
２０１８年１１月５日

事　　務　　局

トラストサービスの在り方

- 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。
- グローバルなプラットフォーム事業者が提供するIDを活用して様々なサービスを利用できるようにするID連携が進展している中、オンラインでのやりとりにおいて、**通信の相手先となる人や組織の正当性の確認や認証にとどまらず、ネットワークにつながるモノの認証やネットワーク上を流れるデータの完全性（Data Integrity）の確保等を実現するための我が国のトラストサービス（電子署名、利用者認証、タイムスタンプ等）の在り方について、**EUにおけるeIDAS規則の制定等の動きも踏まえつつ、**国際的なサービスの進展を視野に入れた相互運用性の確保の観点からも、包括的な検討を行う必要**。
- 我が国では、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）に基づく電子署名のサービスや、総務省「タイムビジネスに係る指針」の規定に基づくタイムスタンプのサービスが提供されているところ。
- EUでは、電子取引における確実性を確保し、市民、企業の経済活動の効率化を促進するため、2014年8月にeIDAS（electronic Identification and Authentication Services）規則を発効し、トラストサービスに関して包括的に規定。

EUにおけるトラストサービスのイメージ



トラストサービス（例）

電子署名

○ 電磁的に記録された情報について、本人により作成されたことを示すもの（リモート署名にも対応）。

タイムスタンプ

○ 電子データが、ある時刻に存在していたこととその時刻以降に改ざんされていないことを証明するもの。

ウェブサイト認証

○ ウェブサイトやサーバの管理主体を確認して発行される、一般に「SSL証明書」と呼ばれる電子証明書を用いるもの。

eシール

○ 文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの。

eデリバリー

○ 送受信者の識別と送受信データの完全性、送受信日時の正確性を保証するもの。

（出典）欧州委員会公表資料をもとに総務省作成
https://ec.europa.eu/cefdigital/wiki/download/attachments/55887082/Validation%20of%20QES%20v2.00.pdf

電子署名法の概要

※　総務省、法務省及び経済産業省の共管（平成13年4月施行）

目的

電子署名の円滑な利用を確保し、通信ネットワークを利用した社会経済活動の一層の推進を図ることとしたもの

内容

電子署名とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するもの（法第２条第１項）。

一　当該情報が**当該措置を行った者の作成に係るもの**であることを示すためのものであること。

二　当該情報について**改変が行われていないかどうかを確認することができるもの**であること。

（１）電磁的記録の真正な成立の推定

本人による一定の条件を満たす電子署名が付されている電子文書等の真正な成立の推定（法第３条）

（２）認証業務に関する認定制度

主務大臣は、主務省令で定める基準等に適合する特定認証業務を認定（法第６条）

認証業務	自らが行う電子署名について利用者その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務（法第２条第２項）
特定認証業務	電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務（法第２条第３項）
認定認証業務	主務大臣の認定を受けた特定認証業務（法第４条第１項）

電磁的記録の真正な成立の推定

［手書き署名・押印］

○　民事訴訟法第228条第４項

「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。」

「本人の署名又は押印」があるときは、

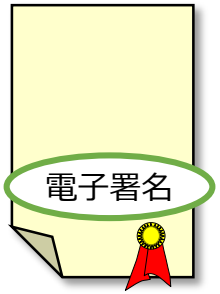
文書の真正な成立（本人の意思に基づき作成されたこと）の推定

類似の仕組みを導入

［電子署名］

○　電子署名及び認証業務に関する法律第３条

「電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について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。）が行われているときは、真正に成立したものと推定する。」



「本人による一定の条件を満たす電子署名」がされているときは、

電磁的記録の真正な成立の推定

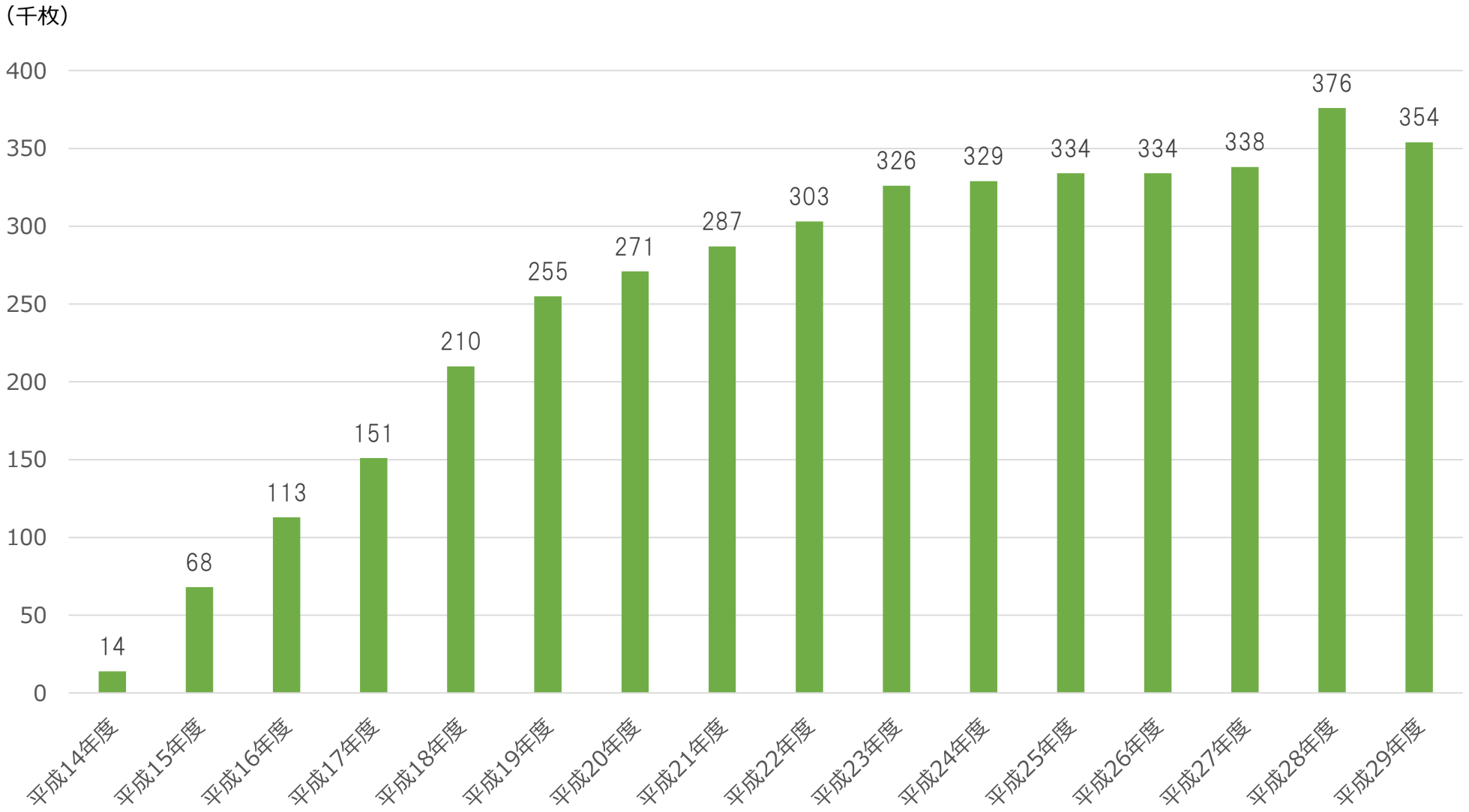
認定認証事業者一覧

■ 平成30年10月末時点で、８事業者11業務が認定されている。

	特定認証業務の名称	業務を行う者の名称	**認定日**
1	株式会社日本電子公証機構認証サービスiPROVE	株式会社日本電子公証機構	H13.12.14
2	CECSIGN認証サービス	株式会社コンストラクション・イーシー・ドットコム	H14.3.26
3	セコムパスポート for G-ID	セコムトラストシステムズ株式会社	H14.7.4
4	AOSignサービス	日本電子認証株式会社	H14.8.29
5	TOiNX電子入札対応認証サービス	東北インフォメーション・システムズ株式会社	H14.12.10
6	TDB電子認証サービスTypeA	株式会社帝国データバンク	H15.2.5
7	e-Probatio PS2 サービス	株式会社エヌ・ティ・ティネオメイト	H17.11.9
8	DIACERTサービス	三菱電機インフォメーションネットワーク株式会社	H26.2.6
9	AOSignサービスＧ２	日本電子認証株式会社	H26.7.31
10	DIACERT-PLUSサービス	三菱電機インフォメーションネットワーク株式会社	H27.1.21
11	e-Probatio PSA サービス	株式会社エヌ・ティ・ティネオメイト	H28.11.1

認定認証事業者から発行された電子証明書（有効枚数）の推移

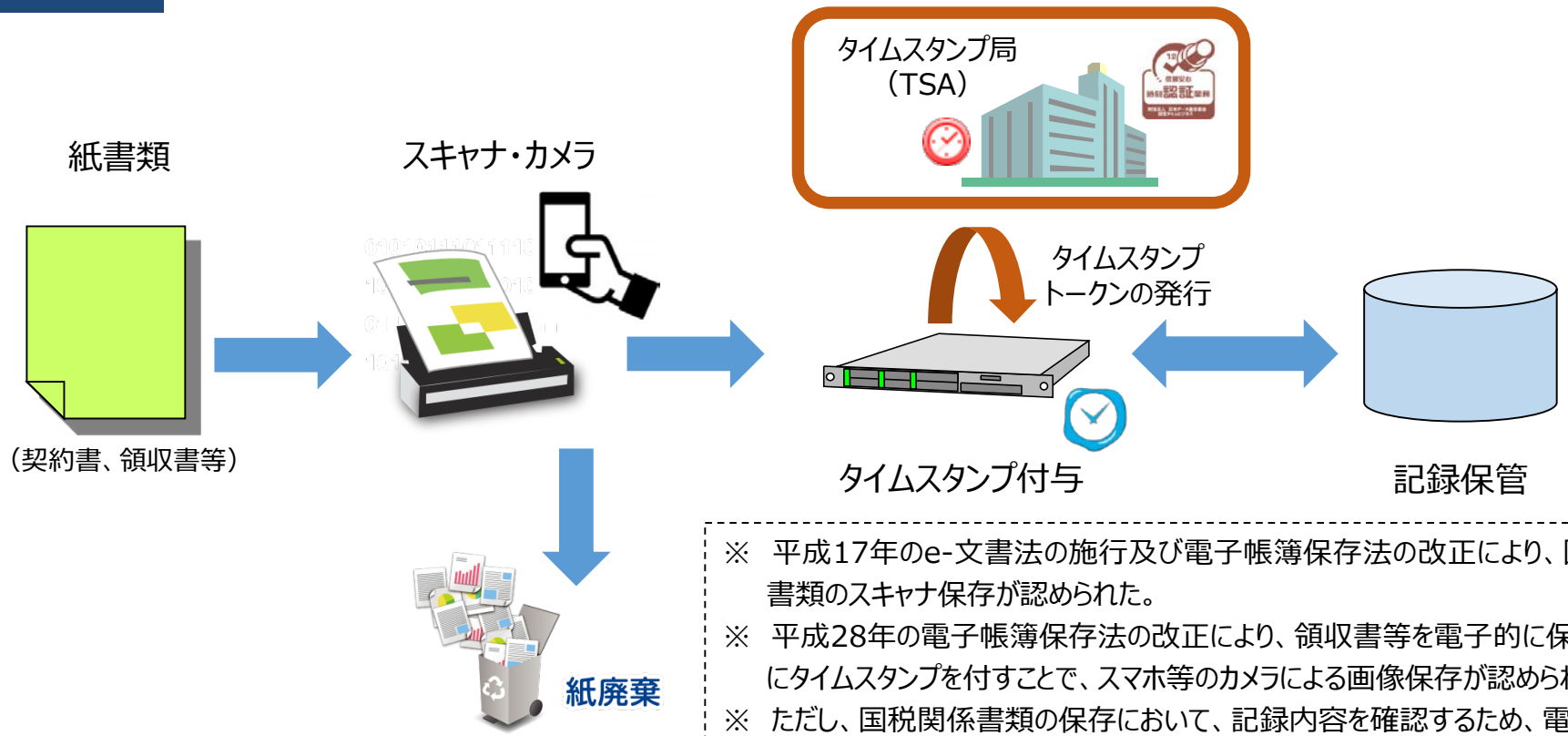
■　ここ数年の電子証明書の有効枚数は30万枚程度を推移（電子証明書の有効期間は最大５年間）。



タイムスタンプの概要と活用事例

- タイムスタンプを活用し、電子データと時刻情報を結合することで、**(1)その時刻にそのデータが存在したこと（存在証明）**と、**(2)その時点から現在に至るまでデータが変更・改ざんされていないこと（非改ざん証明）**を、証明することができる。
- 平成30年（1月～6月）の認定タイムスタンプ発行件数は、1億700万枚。例えば、国税関係書類のスキャナ保存等においては、タイムスタンプの付与が要件となるなど、タイムスタンプの普及・利用が進んでいる。

活用事例　電子帳簿保存法（国税庁）に基づく取引関係書類の電子データ化

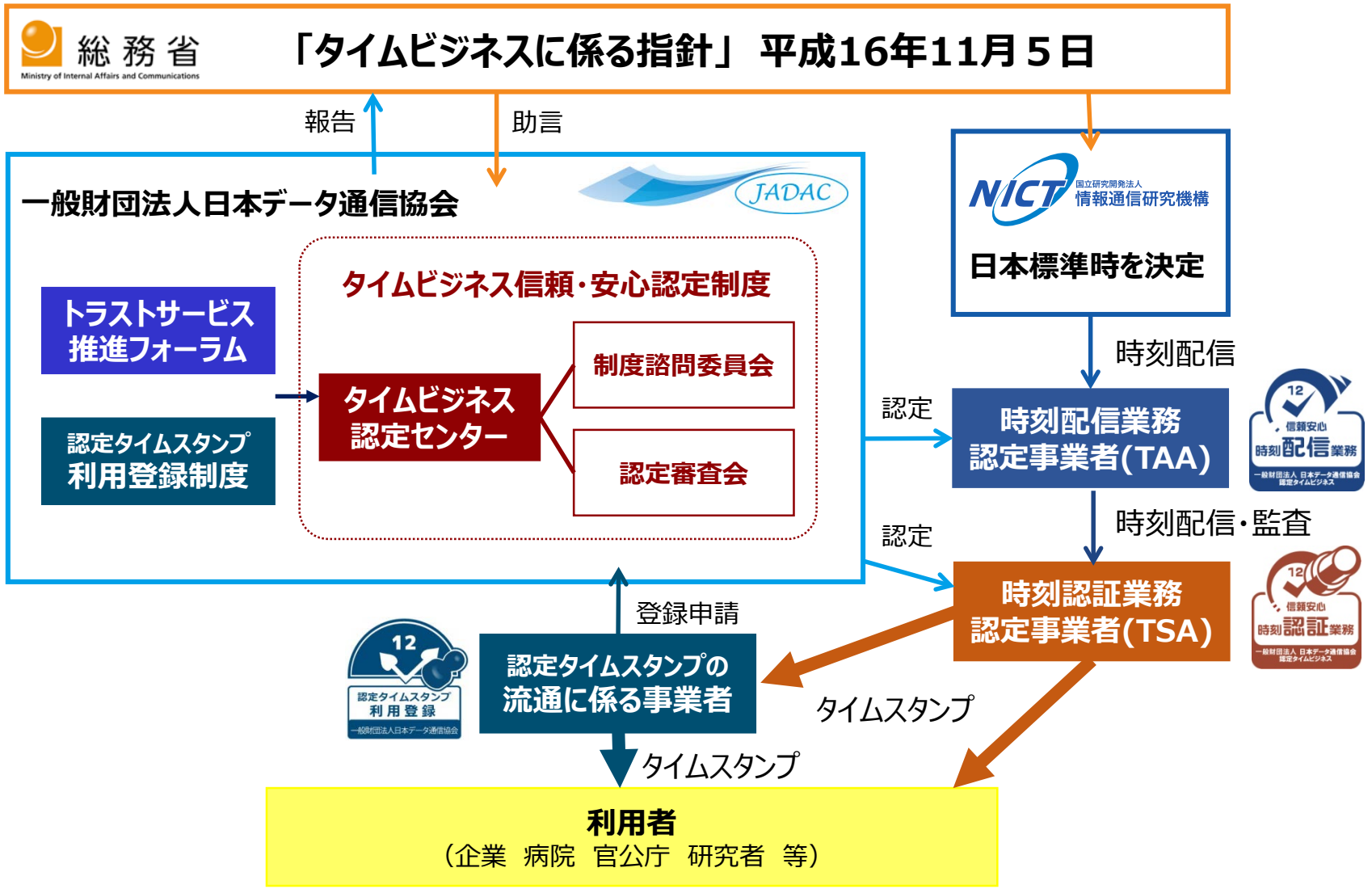


※　平成17年のe-文書法の施行及び電子帳簿保存法の改正により、国税関係書類のスキャナ保存が認められた。
※　平成28年の電子帳簿保存法の改正により、領収書等を電子的に保存する際にタイムスタンプを付すことで、スマホ等のカメラによる画像保存が認められた。
※　ただし、国税関係書類の保存において、記録内容を確認するため、電子化後も原本を一定期間保存することを義務付け。

※　上記事例のほか、医療情報システムの安全管理に関するガイドラインに基づき、電子カルテや検査データの医療情報等にも、タイムスタンプが利用されている。

タイムスタンプに関する認定制度

■ 総務省「タイムビジネスに係る指針」（平成16年11月公表）を受けて、一般財団法人日本データ通信協会が 「タイムビジネス信頼・安心認定制度」を運用。



認定事業者一覧

■ 平成30年10月末時点で、時刻配信業務認定事業者（※１）として２事業者、時刻認証業務認定事業者（※２）として７事業者が認定されている。

（※１）ネットワークを通じて時刻情報を配信する業務及び配信先の時刻精度を計測して報告を行う時刻監査業務を行う事業者

（※２）タイムスタンプの付与及びタイムスタンプの有効性を証明する業務を行う事業者

時刻配信業務認定事業者（TAA）：２事業者

サービスの名称	事業者の名称	最新の認定有効期間	初回認定取得日
アマノ時刻配信・監査サービス for TSU	アマノ株式会社	H29.3.22～H31.3.21	H17.3.22
セイコー時刻配信サービス	セイコーソリューションズ株式会社	H30.4.24～H32.4.23	H18.4.24

時刻認証業務認定事業者（TSA）：７事業者

（１）デジタル署名を使用する方式

サービスの名称	事業者の名称	最新の認定有効期間	初回認定取得日
アマノタイムスタンプサービス3161	アマノ株式会社	H29.３.31～H31.３.30	H17.３.31
セイコータイムスタンプサービス	セイコーソリューションズ株式会社	H30.４.24～H32.４.23	H18.４.24
テラダタイムスタンプサービス	寺田倉庫株式会社	H29.12.22～H31.12.21	H27.12.22
TKCタイムスタンプ	株式会社TKC	H28.11.10～H30.11.９	H28.11.10
サイバーリンクスタイムスタンプサービス	株式会社サイバーリンクス	H29.４.28～H31.４.27	H29.４.28
MINDタイムスタンプサービス	三菱電機インフォメーションネットワーク株式会社	H30.４.１～H32.３.31	H30.４.１

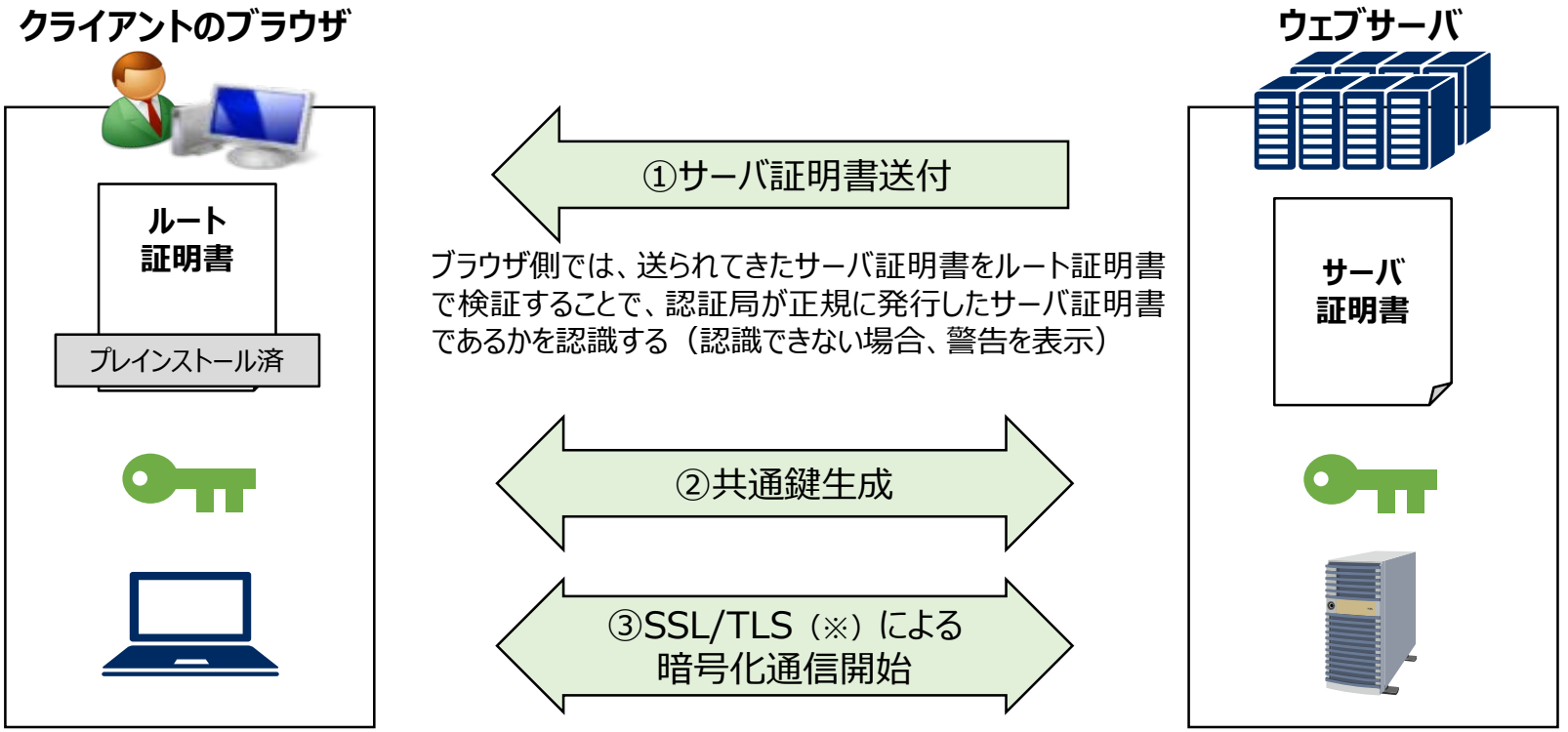
（２）アーカイビング方式（※）

サービスの名称	事業者の名称	最新の認定有効期間	初回認定取得日
SecureSeal® standard	株式会社エヌ・ティ・ティ・データ	H30.３.8～H32.３.7	H18.３.8

※ サービス利用者にタイムスタンプを発行するとともに、センタ側でも発行したタイムスタンプと同じデータを安全に記録・保管（アーカイブ保管）する方式

サーバ証明書による暗号化通信の仕組み

- WebブラウザがWebサイトとの通信を行う際には、このWebサイトから提示されたサーバ証明書の発行元を調べ、Webブラウザに格納されている発行元のルート証明書によってサーバ証明書の署名を復号し、正当なものであるか否かを判断。
- サーバ証明書に署名した認証局が中間認証局である場合には、ルート認証局が見つかるまで、上位の認証局をたどる。

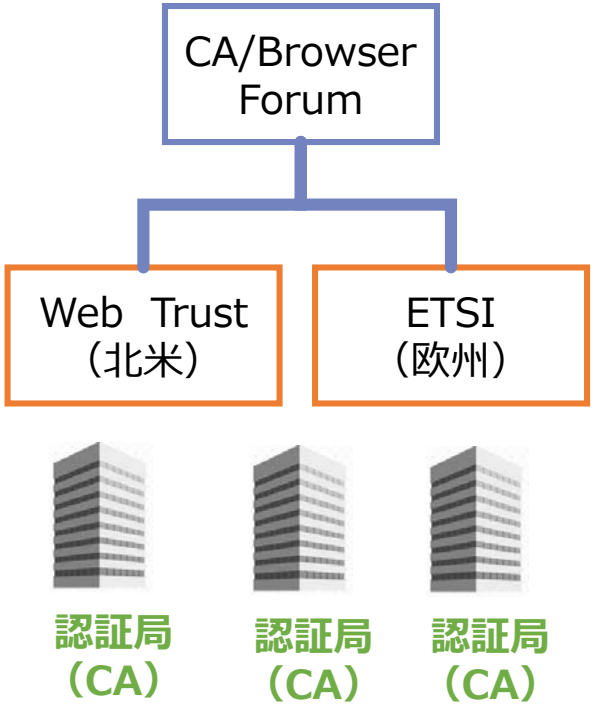


（※） SSL（Secure Sockets Layer）/ TLS（Transport Layer Security） とは、インターネット上で通信を暗号化し、第三者による通信内容の盗み見や改ざんを防ぐ技術。SSL/TLSを利用すると、ウェブサイトから入力する個人情報やクレジットカード情報等の大切なデータを安全にやりとりすることができる。 SSLとTLSは、大枠の仕組みは同じものであり、SSLがバージョンアップを重ねて「SSL3.0」となり、その次のバージョンから「TLS1.0」という名称で呼ばれている。SSLの名称は広く普及しているため、TLSを指していても、SSL又はSSL/TLSと表記することが多い。

CA/Browser Forumの概要

■ CA/Browser Forum（CAブラウザーフォーラム）は、電子証明書を使った通信の安全性やその利便性を向上させるためのガイドラインを策定している会員制の任意団体。DigiCert（旧：Symantec）やGlobalSignといった認証局事業者とApple、Google、Microsoft、MozillaといったWebブラウザを開発しているベンダ等からなる。

■ 組織関連図



■ トラスト的構造

Baseline Requirements	・ Baseline Requirementsとは、CA/Browser Forumが発行するパブリック証明書の発行及び管理に関する基本要件 ・パブリック証明書を発行する全ての認証局（CA）に適用される要求事項を定めている。
監査基準	・Baseline Requirementsに基づき、Web Trust, ETSIが発行する監査基準
CP/CPS	・CP（証明書ポリシ:Certificate Policy） 発行する電子証明書の利用目的、適用範囲、セキュリティレベル、認証局の責任等、認証局が電子署名を発行する際の運用方針を定めている。 ・CPS(認証局運用規定:Certification Practice Statement) 認証局がCPをどのように適用するかの手順を定めている。

※ EUでは、eIDAS規則に基づき、信頼できるサーバ証明書の認証局をトラストリストとしてリスト化し、当該リストに掲載されている認証局は、CAブラウザフォーラムにおいて要件を満たすものとして扱われている。

出典：「CA/Browser Forumとは」をもとに作成
https://www.nic.ad.jp/ja/basics/terms/ca_browser_forum.html
http://www.meti.go.jp/meti_lib/report/H28FY/000458.pdf