電子署名・認証・タイムスタンプ

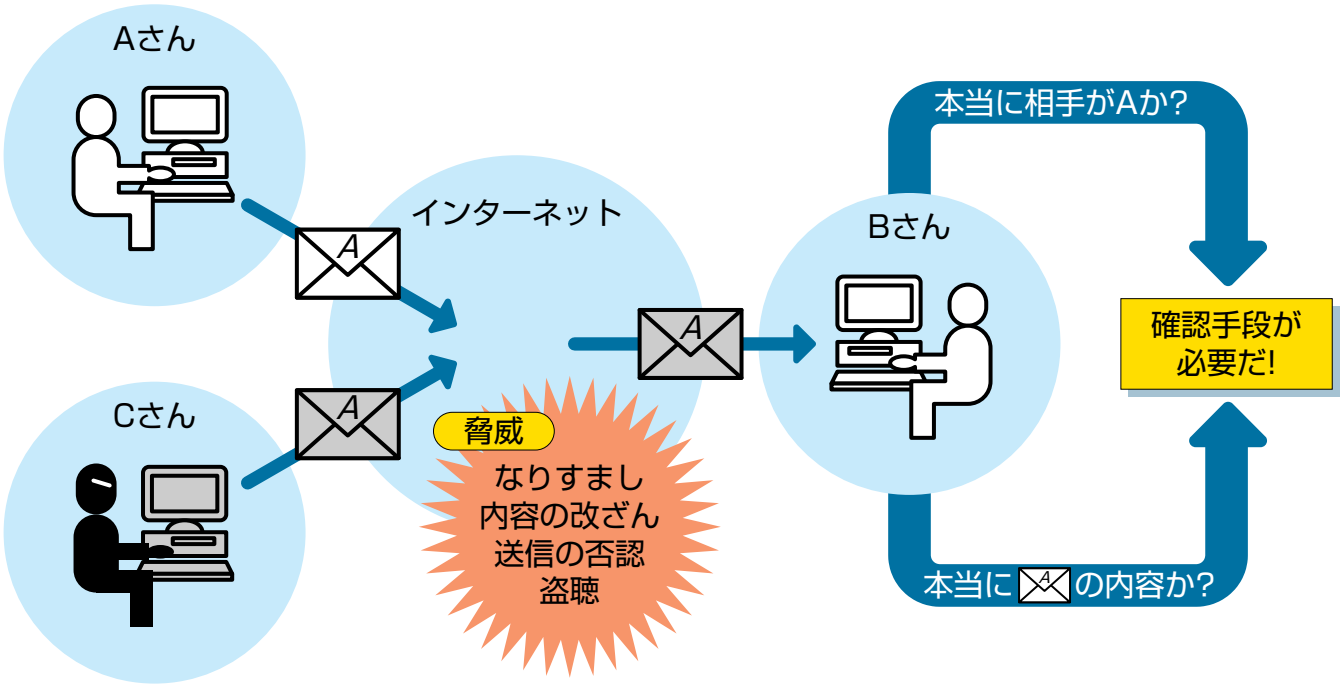
その役割と活用

総務省は、ICT（Information ＆ Communication Technology）が安心して利用できる社会の実現を目指して、電子署名、認証業務、タイムスタンプに対する国民の理解を深めていくための取り組みを行っています。

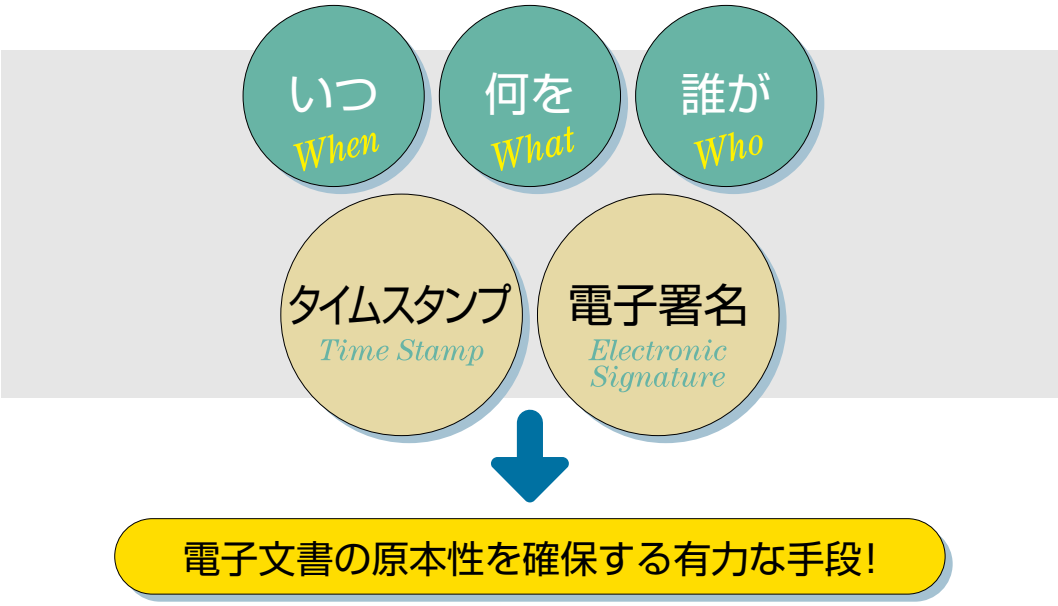
総 務 省

❶インターネット社会における認証とは

インターネットを利用した日常業務に潜む様々な脅威！



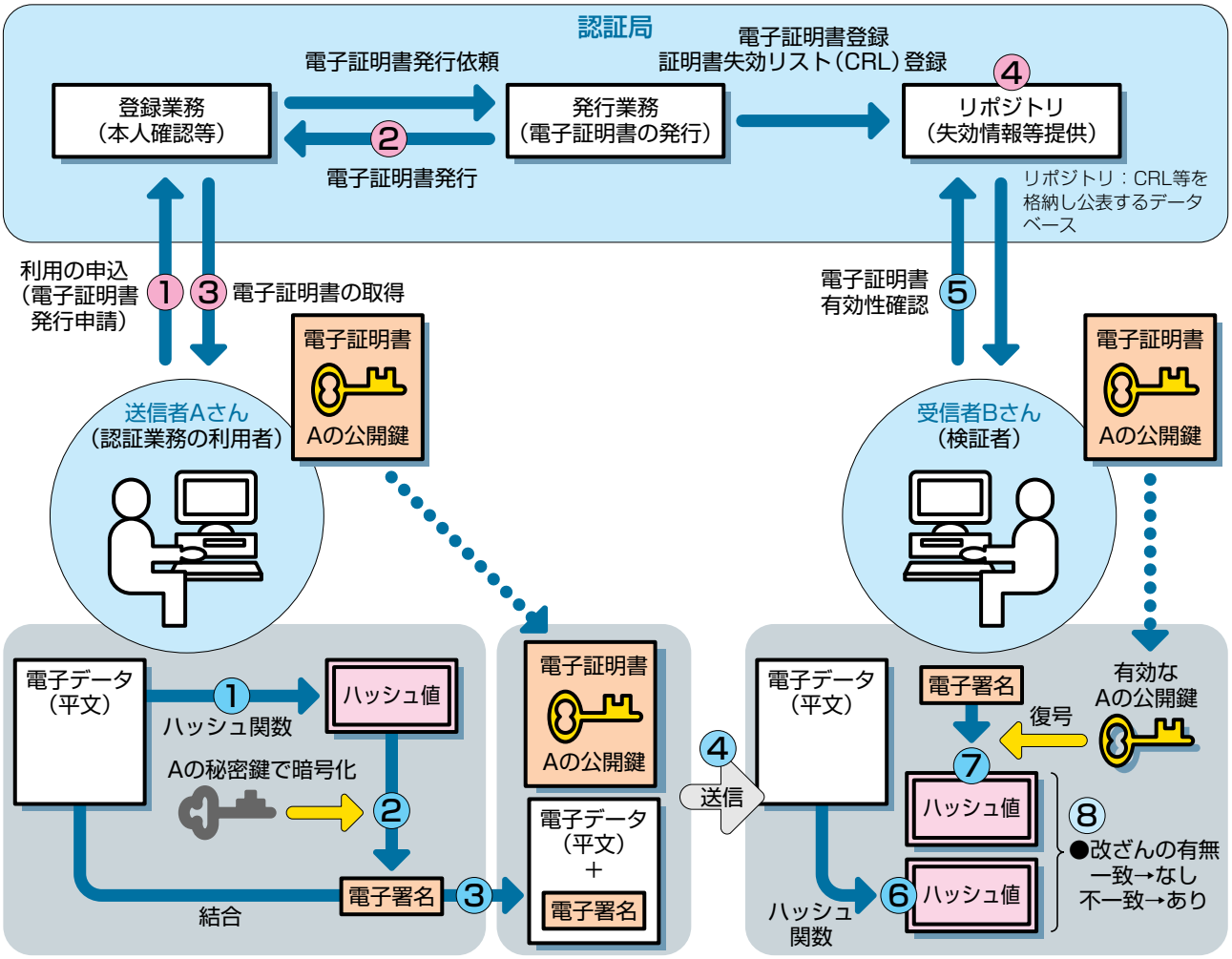
インターネット上の電子文書に関して「いつ」「何を」「誰が」を担保するには



電子署名・タイムスタンプは、インターネット社会における「いつ」「何を」「誰が」を担保するための「証拠」であり、電子文書の原本性が確認できる有力な手段です。

❷電子署名・認証のしくみと活用

電子署名・認証のしくみ（公開鍵暗号方式）



ハッシュ関数：文字や数字などのデータ（入力値）を一定の長さのデータ（出力値）に変換する関数

上段は、電子証明書の発行処理及び認証局の働きを示しています。

① Aさんは、認証局に電子証明書の利用を申し込みます。
② 認証局は、Aさんの本人確認、秘密鍵と公開鍵の対応付けの確認などを行ったのち、Aさんが登録した公開鍵の電子証明書を発行します。
③ Aさんは、認証局から電子証明書を受理します。
④ 認証局は、発行した電子証明書が何らかの理由により失効された場合、その情報をリポジトリに掲載します。

下段は、電子証明書を利用しての電子データの安全な送信方法を示しています。

① 送信者Aさんは、電子データをハッシュ関数により変換してハッシュ値（メッセージダイジェストともいう）を生成します。
② このハッシュ値を電子証明書で証明されている公開鍵に対応する秘密鍵で暗号化します。（この行為を「電子署名」といいます。）
③ 電子データ（平文）と電子署名を結合し、④ 電子証明書とともに受信者Bさんへ送信します。
⑤ 受信者Bさんは、電子証明書が失効されていないかなど電子証明書の有効性を確認します。
⑥ 受信したデータを電子データ（平文）と電子署名にわけ、電子データ（平文）から送信者Aさんと同じハッシュ関数を用いてハッシュ値を生成します。
⑦ 電子署名をAさんの公開鍵を用いて復号し、ハッシュ値を取得します。
⑧ ⑥と⑦で得たハッシュ値を比較し、一致していれば、電子データが途中で改ざんされていないこと並びにAさんからの電子データであることが確認できたことになります。

利用分野

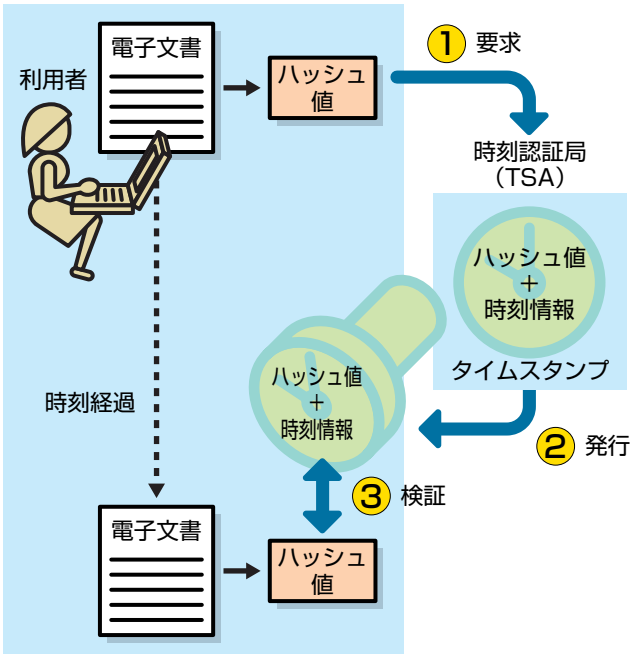
1. 電子入札　2. 電子申請・申告　3. 電子契約　4. 電子商取引　5. 電子メールへの電子署名　6. 電子決裁　等

❸タイムスタンプのしくみと活用

タイムスタンプのしくみ

タイムスタンプ（TS）は、TSに刻印されている時刻以前にその文書が存在し（存在証明）、その時刻以降文書が改ざんされていないことを証明する（非改ざん証明）ものです。

●タイムスタンプの仕組み



タイムスタンプサービスは、①TSの要求、②発行と③検証の過程から構成されています。要求・発行は、利用者が原本データのハッシュ値（電子文書の指紋に相当）を時刻認証局（TSA）に送付し、TSAがこのハッシュ値に時刻情報を付与したTSを利用者に送付する過程です。

検証は、原本データのハッシュ値とTSのハッシュ値を比較する過程で、一致していれば改ざんされていないことを証明できます。

TSそのものの信頼性を確保するため、例えばデジタル署名を使用する方式では、TSにTSAがデジタル署名をし、TSがTSAから発行され、改ざんされていないことを保証しています。

タイムスタンプの時刻情報は、日本標準時に基づいており、時刻の信頼性が確保されています。

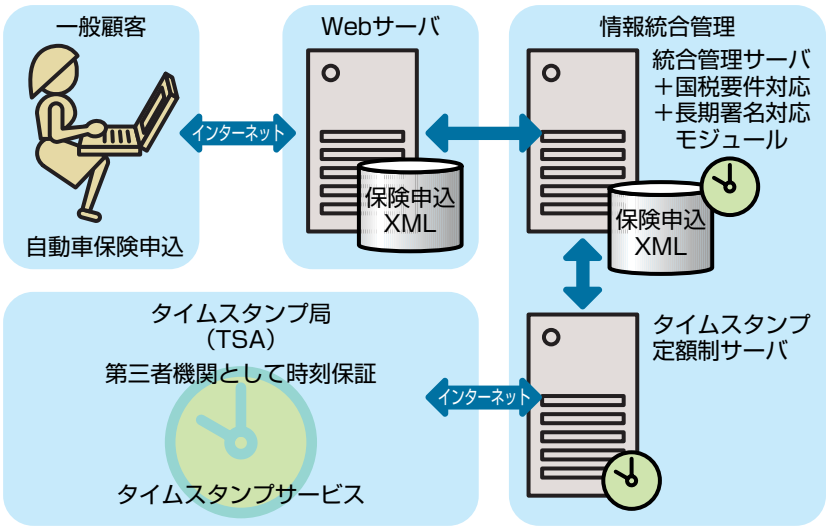
タイムスタンプの活用

電子文書化は、業務プロセスの改革、顧客サービスの向上等業務効率化の基盤となっています（例：e-文書法関連）。最近では、内部統制の観点からも、電子文書化による記録と管理の重要性が増大しています（例：J-SOX法）。電子文書の証拠性を高める上で、タイムスタンプの利用は、今後ますます進むものと期待できます。主な利用例を列記します。

①電子署名との併用による利用⇒原本性確保
- 申込書･契約書の電子化・電子保存（図参照）
- 電子商取引（EDI）
- 電子カルテ

②タイムスタンプ単独での利用⇒時間的順序の証明
- 特許における先使用権制度での利用

③基盤技術として
- 電子文書長期保存のための「長期署名フォーマット」での利用



インターネット自動車保険申込システム利用例　参考：月刊IM,2007年7月号

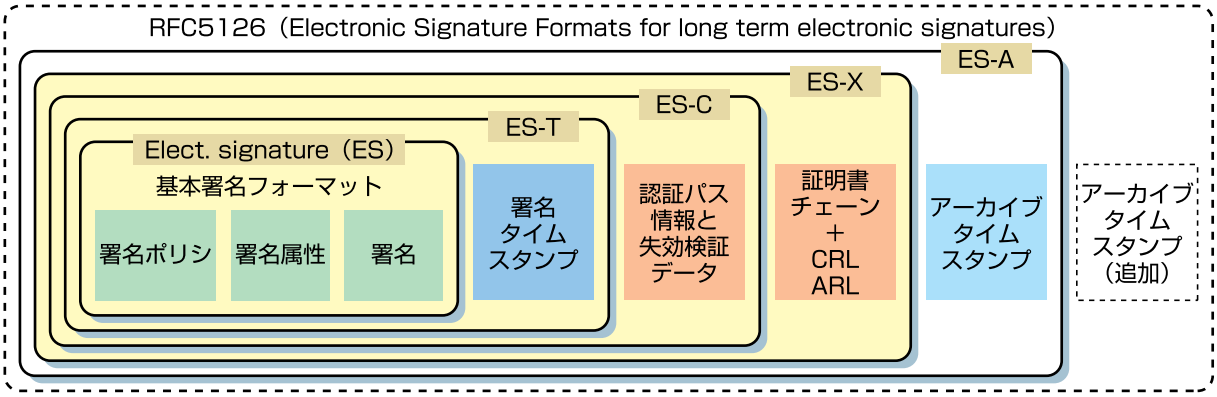
XML：文書やデータの意味や構造を記述する言語

❹電子署名の長期利用

長期署名フォーマットの国際標準（RFC5126）

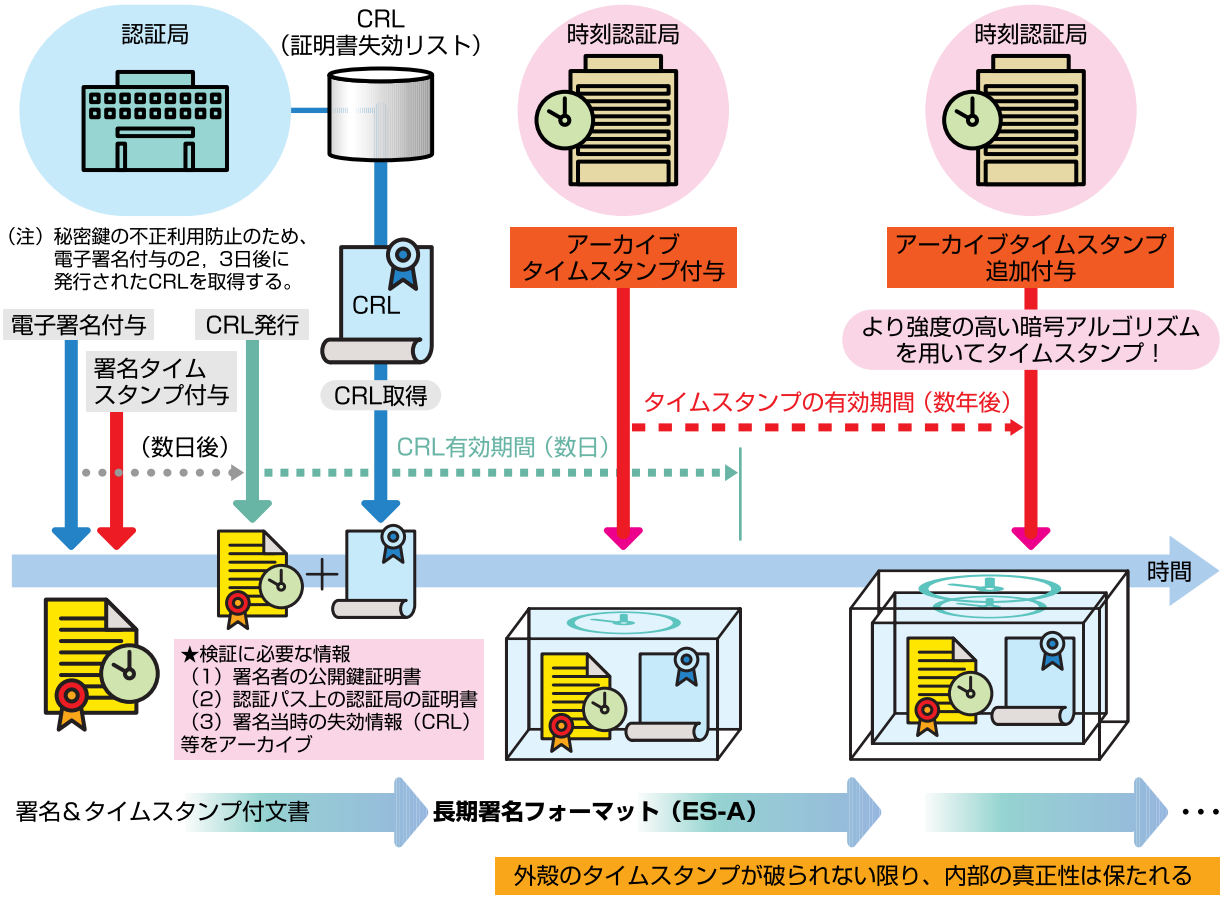
電子署名の長期利用のための長期署名フォーマットが国際標準（RFC5126）として、またJIS X 5092として策定されており、以下のような効果があります。

・署名タイムスタンプにより署名時刻の証拠性を確保
・失効情報や証明書を署名データ内に格納し、証明書検証の継続性を確保
・アーカイブタイムスタンプの暗号アルゴリズムにより、署名データや失効情報等を保護
（署名アルゴリズムの脆弱化による署名偽造を防ぐ）



ES-T：Electronic Signature with Time stamp　ES-X：Electronic Signature eXtended　ARL：認証局証明書失効リスト
ES-C：Electronic Signature with Complete validation data　ES-A：Electronic Signature Archive
アーカイブタイムスタンプ：電子文書、デジタル署名、署名タイムスタンプ及び検証情報全体を改ざんできないようにアーカイブ（保管）するために付加されるタイムスタンプ

長期署名フォーマット構築例



タイムビジネス信頼・安心認定制度

本制度（時刻配信業務と時刻認証業務の認定）については、
財団法人 日本データ通信協会が行っております。

認定制度の概要

目的

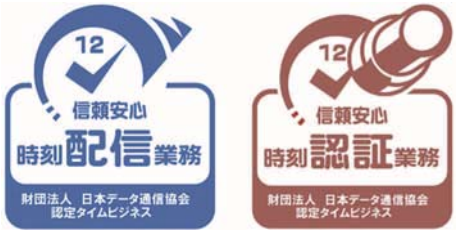
タイムスタンプサービスを安心して利用できる環境の実現とICT社会の基盤への貢献

概要

「タイムビジネスに係る指針」（総務省、2004年11月策定）を踏まえて、
タイムビジネスが当協会で定めた基準を満たし厳正に業務が実施されているかを認定

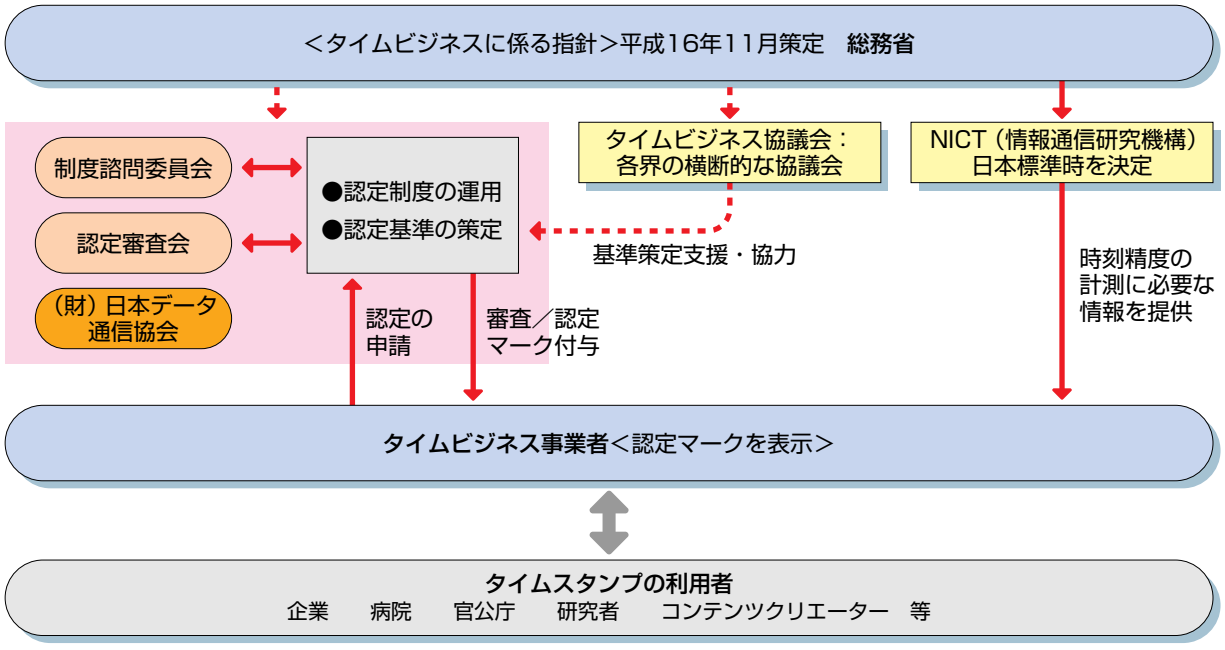
認定事業者

認定証が交付され、認定マークを使用可



認定マーク

認定制度の枠組み



総務省

〒100-8926　東京都千代田区霞ヶ関 2-1-2
TEL. 03-5253-5111（代表）　URL: http://www.soumu.go.jp/

発行年月　2009年3月