インターネット 10分 講座

リモート時代の電子署名を巡る技術動向

1 はじめに

コロナ禍のもと多くの皆さんがリモートワークを余儀なくされていることでしょう。リモートワーク時における問題の一つが「押印」や「署名」ではないでしょうか。でも「押印」や「署名」の本質とは何でしょう[※1]。民訴法第228条第4項には「私文書は、本人（中略）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。」という規定があります。ここから見ると「押印」と「署名」の効果は同じであると言えそうです。また民訴法第228条第4項のこの推定はその前提として「自分の印鑑を第三者が勝手に持ち出して使うことはないという経験則からの推定。」があり、合わせて「二段の推定」と呼ばれます。以上から「押印」や「署名」には以下の二つの条件（二段の推定）が必要ということになります。

押印／署名の条件：
1. ハンコ（署名）が利用できるのは所有者のみ（本人性）
2. ハンコで押印する（署名する）ことで真正に成立する（意志確認）

「電子署名」は「電子的」に「署名」を実現したもので、電子署名法により法的にも認められています。世界を見ると各国に「電子署名法」がありますが、そのほとんどは「電子署名された文書は紙に署名した場合と同等の扱いとする。」ということになっています。次に「電子署名」とは何でしょうか。日本においては電子署名法の第2条第1項の電子署名において「デジタル情報（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、以下のいずれにも該当するもの。」となっています。該当条件は以下の二つです。

- ●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（同項第１号）
- ●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（同項第２号）

最初の条件は「二段の推定」と同じと言えますが、追加として「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」という条件があります。現実世界では押印済みの紙をコピーすることは困難である前提がありますが、電子世界ではコピーが容易であり、かつ見分けがつかない点から追加されたと考えられます。以上から「電子署名」には以下の三つの条件が必要と言えます。

電子署名の条件：
1. 電子署名が利用できるのは本人のみ（本人性）
2. 電子署名することで真正に成立する（意志確認）
3. 改変が行われていないこと（非改ざん性）

電子署名においては技術と法が密接に関係するために長い前置きになりましたが、法的な解説はここまでとして、以降は「電子署名」を実現する技術動向について紹介します。

※1　押印に関するQ&A（内閣府 法務省 経済産業省）　https://www.meti.go.jp/covid-19/ouin_qa.html

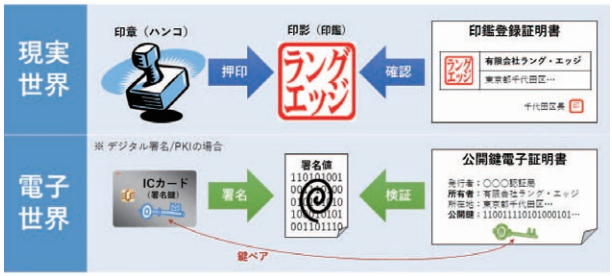
2 リモート時代の電子署名

2.1 リモート時代以前（ローカル利用）

クラウド発展の前から電子署名は使われてきました。電子署名法が施行された時（2001年4月）に、前提となっていたのは「デジタル署名」と「公開鍵基盤（PKI）」の組み合わせでした。「デジタル署名」にはRSA公開鍵暗号技術が使われてきましたが、「署名鍵（秘密鍵・私有鍵とも呼ばれる）」を利用して対象データの「署名値」を計算します。「署名値」は「署名鍵」とペアになった「公開鍵（検証鍵とも呼ばれる）」で検証することで、改ざんが検知できる仕組みとなっています。「公開鍵基盤（PKI：Public Key Infrastructure）」では「公開鍵」を含む「公開鍵電子証明書」を署名値の検証のために配布します。

これをハンコで考えると、押印する「印章（ハンコ）」そのものが「署名鍵（ICカード等に格納）」であり、押印により生じる「印影（印鑑）」が「署名値」であり、印影を保証する「印鑑登録証明書」が「公開鍵電子証明書」と言えます。デジタル署名と公開鍵基盤（PKI）を利用すると、従来の仕組みをそのまま電子的に実現できます。

公的な「公開鍵電子証明書」は、認証局（CA：Certification Authority）と呼ばれる組織から発行されます。「公開鍵基盤（PKI）」の認証局では、「公開鍵電子証明書」の発行申請時に「身元確認（Identity Proofing）」を行ってから発行することで、「署名鍵」の所有者を保証します。「署名鍵」はいろいろな物に格納されま



押印と電子署名（デジタル署名）の比較

すが、一番身近な例ではマイナンバーカードのような、ICカードに格納して使われることが一般的でした。しかしながら、ICカードを使うにはPCに「ICカードリーダー」を接続して「ドライバソフトのインストール」が必要となり、決して使い勝手が良い利用方法ではなく、電子署名はなかなか普及してきませんでした。

2.2 リモート時代以降（クラウド利用）

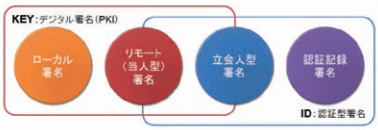
リモート時代である現在は、クラウドサービスの利用が前提となることが多くなりました。一般的にクラウドサービスの利用には「電子認証（ID認証）」が要求されます。「電子認証」と言うと先ほど出てきた公開鍵基盤（PKI）の「認証局」と混同されがちですが、この二つの「認証」はまったく異なる意味です。英語で言えば「電子認証（ID認証）」の認証は「Authentication（立証）」であり、「認証局（PKI）」の認証は「Certification（認定）」です。「電子認証（ID認証）」を利用する目的は「身元確認された利用者当人であることを当人認証により確認する」ことです。電子認証するためにID発行を行いますが、一般的にID発行申請時に「身元確認」を行ってからID発行することで、「ID」の所有者を保証します。なお、ID発行時にIDと認証要素（認証クレデンシャル、例：パスワード）の発行や紐付けが行われます。

サービスを利用する時にIDやパスワードを入力する操作は「当人認証」です。「電子認証（ID認証）」ではID発行時に「身元確認」を、サービス利用時に「当人認証（Authentication）」を行います。そして「身元確認」の保証レベルと「当人認証」の保証レベルは別の定義となりますが、米国のNIST SP 800-63で定義された保証レベルが広く使われています。「身元確認保証レベル」は「IAL（Identity Assurance Level）」と呼ばれ、匿名・属性確認・対面確認のような項目でレベル分けされます。「当人認証保証レベル」は「AAL（Authenticator Assurance Level）」と呼ばれ、単要素・2要素・ハード利用の2要素のような項目でレベル分けされます。

見方を変えると、電子署名の条件のうち「電子署名が利用できるのは所有者のみ（本人性）」に関しては、「電子認証（ID認証）」を利用しても実現することができる時代になったと言えます。このように電子署名のクラウド化に関しては、ID認証の技術を取り込んだ新しい電子署名技術が生まれてきて使われています。

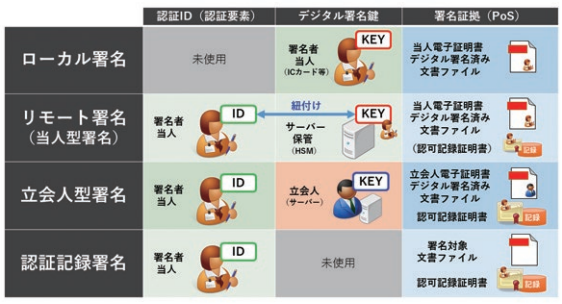
3 電子署名技術方式

リモート時代の電子署名技術は、従来の「デジタル署名（PKI）」と「電子認証（ID認証）」の二つの技術の組み合わせとして実現されています。大きく「署名鍵（KEY）」を主としたデジタル署名（PKI）と、「電子認証（ID）」を主とした認証型署名に分けられます。



電子署名方式の分類

「リモート署名」と「立会人型署名」は「デジタル署名」と「電子認証」の両方を使うハイブリッド型となりますが、署名鍵と認証IDの利用方法と、署名結果として取得される署名証拠（後述）が異なります。



各署名方式の比較

3.1 ローカル署名

「署名鍵」を署名者当人が所有して管理することで「本人性」を保証します。デジタル署名の付与には、ローカル環境で実行される「署名アプリ」を操作して「署名鍵」を使用することで「署名意志」を示します。当人のデジタル署名を利用することで「非改ざん性」も保証されます。署名者の「身元確認」はPKIの「認証局」が行います。必要に応じて当人署名済みの文書をメールで検証者に送信するか、クラウドにアップロードして利用します。ICカードに署名鍵を格納している場合にはPCにICカードリーダーやドライバソフト等の専用ソフトウェアをインストールする必要があり、使い勝手の面で面倒な面があります。

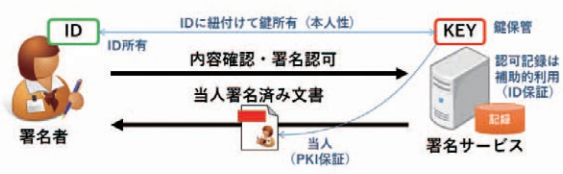
ローカル署名方式は歴史が古く、デジタル署名や認証局の技術や運用についてそのほとんどがRFC/ISO/W3C/JIS/ETSI等で標準化されています。実績という面では最も信頼できる署名方式と言えます。

ローカル署名の仕組み

3.2 リモート（当人型）署名

「認証ID（と認証要素）」を署名者当人が所有して管理し、「認証ID」に紐付いたクラウド上の「署名鍵」をデジタル署名に利用することで、「本人性」と「署名意思」を保証します。認証IDと署名鍵の紐付けは強固である必要があるために、一般に「当人認証」には2要素等の高い保証レベルが要求されます。当人のデジタル署名を利用することで「非改ざん性」も保証されます。なおID認証に依存する認可記録も重要であり、別途「認可記録」から「認可記録証明書」を発行することで「本人性」を強化することができます。

ローカル環境に「署名鍵」を持たないのでICカードリーダー等が不要となり、ローカル署名よりも手軽にデジタル署名を利用することが可能となります。署名者の「身元確認」はローカル署名と同じくPKIの「認証局」が行うことで、ローカル署名と同等の本人性が保証できます。

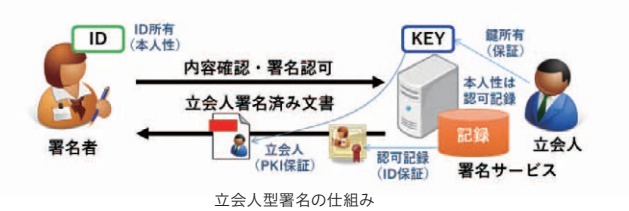


リモート（当人型）署名の仕組み

リモート署名の技術標準に関してはJT2A（日本トラストテクノロジー協議会）※2が「リモート署名ガイドライン※3」を公開しています。他にもCSC（クラウド署名コンソーシアム）※4やEUのETSIでもAPI等の技術仕様や運用ポリシーが標準化されています。

3.3 立会人型署名

「認証ID（と認証要素）」を署名者当人が所有して管理し利用することで、「署名認可」時に当人認証を行い「本人性」と「署名意志」を保証します。署名行為を保証するために、クラウド環境で実行される「署名サービス」にて「立会人」の「署名鍵」を使用してデジタル署名を付与します。立会人のデジタル署名を利用することで「非改ざん性」も保証されます。なおPKIの認証局が保証するのは「立会人」であり、本人性の保証のために別途「認可記録」から「認可記録証明書」を発行する場合もあります。「身元確認」を簡易にする（例：メール到達性のみ等）とサービス利用が容易であるという利点がありますが、身元確認のレベルは低くなるのでリスクを検討して利用する必要があります。



立会人型署名の仕組み

3.4 認証記録署名

「認証ID（と認証要素）」を署名者当人が所有して管理し利用することで、「署名認可」時に当人認証を行い「本人性」と「署名意志」を記録します。本人性の保証のために別途「認可記録」から「認可記録証明書」を発行する場合もあります。文書の「非改ざん性」に関しては、原本文書をアクセス制御されたサーバーに保管する等の方法で別途保証する必要があります。データ保管や電子申請等のサーバー側に文書を保管する場合等に向いており、簡易な電子署名として認められている場合もあります。立会人型署名とは文書にデジタル署名を付与するかどうかの違いとなります。

認証記録署名の仕組み

※2　JT2A（日本トラストテクノロジー協議会）
http://www.jt2a.org/

※3　リモート署名ガイドライン（JT2A リモート署名タスクフォース）
https://www.jnsa.org/result/jt2a/2020/index.html

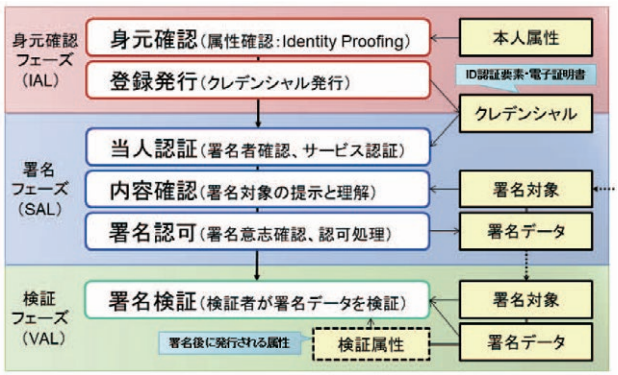
※4　CSC（Cloud Signature Consortium）
https://cloudsignatureconsortium.org/

電子署名保証レベルの考え方

いろいろな電子署名技術があることが分かりました。次に問題となるのは「どの電子署名技術を使えば良いのか？」でしょう。電子署名を利用するシーンを考えると大金が関係する重要契約の場合もあるでしょうし、上司が部下の勤怠管理を承認する場合もあるでしょう。保証レベルという考え方を電子署名に当てはめると、「大金が関係する重要契約」には高い保証レベルの電子署名が必要ですし、「社内事務承認」には低い保証レベルの電子署名で十分と言えます。一般的に保証レベルが高くなると利便性は低下します。やみくもに高い保証レベルをめざすのではなく、利用目的に合った保証レベルの選択が必要となります。

4.1 電子署名のフェーズと利用手順

どのような電子署名方式を使っても、電子署名の利用プロセスは基本的に同じとなります。電子署名は、利用開始時の「身元確認フェーズ」と、署名付与時の「署名フェーズ」と、後から署名結果を確認する「検証フェーズ」の三つに分けることができます。
「署名認可」の前に何に署名するか確認する「内容確認」を置くことは電子署名としては必須となります。



電子署名のフェーズと利用手順

4.2 米国NIST SP 800-63-3（電子認証保証レベル）

電子認証には米国NIST SP 800-63-3※5にて保証レベルが決められています。SP 800-63-3では三つの保証レベル「IAL:身元確認保証レベル」「AAL:当人認証保証レベル」「FAL（Federation Assurance Level）:連携情報保証レベル」が決められています。なお2022年には後継のSP 800-63-4が出る予定ですが、この中では定義が変更される可能性がありますので注意が必要です。FALに関しては電子署名とは関連が無いのでここでは説明しません。
電子認証では主に「サービス利用時の本人性」が求められるのに対して、電子署名では後で（例えば裁判で）「過去の署名時点の本人性」が求められるという違いがあります。このような違いがあるので、電子認証の保証レベルをそのまま使うことはできません。

4.3 電子署名保証レベル（eSignAL）

電子署名に関してもSP 800-63-3同様に指針となる保証レベルを策定すべく、JNSA（日本ネットワークセキュリティ協会）※6電子署名ワーキンググループの保証レベルタスクフォース※7にて作業中で、2022年には「電子署名保証レベル（eSignAL）」のガイド（仮）を公開する予定です。ここではその中から基本的な考え方を説明します。
電子署名保証レベルは三つの保証レベル「IAL:身元確認保証レベル（身元確認フェーズ）」「SAL:署名プロセス保証レベル（署名フェーズ）」「VAL:検証可能データ保証レベル（検証フェーズ）」に分かれます。NIST SP 800-63-3と策定中の電子署名保証レベル（eSignAL）のどちらも「身元（Identity）」「プロセス（Process）」「データ（Data）」の三つの保証レベルで構成されます。
電子署名保証レベル（eSignAL）のうち、最初の「IAL」は電子認証のSP 800-63-3AのIALと基本的に共通です。IALのレベルは電子認証と電子署名の両方においてサービスの前提となるも

のであり、非常に重要な保証レベルです。IALに関して、詳しくはNIST SP 800-63-3Aに記載されています。

NIST SP 800-63-3と策定中の電子署名保証レベルの比較

4.4 SAL：署名プロセス保証レベル

「SAL（Signing process Assurance Level）」は、署名フェーズで使われる技術の保証レベルです。基本的にはNIST SP 800-63-3Bで説明されている「AAL」を利用しますが、AALの各要件に加えて「サービス認証」と「署名認可」の2段階認証や、デジタル署名を利用する場合には署名鍵の保管にHSM（Hardware Security Module）の利用を要求する点が追加されています。

4.5 VAL：検証可能データ保証レベルとPoES（署名証拠）

「VAL（Verifiable data Assurance Level）」は新しく造語として考えた「PoES（署名証拠：Proof of Electronic Signatures）」の強度を保証するレベルです。PoESは第三者が検証できるデータ（Verifiable data）である必要があり、証拠データとして利用できる情報がPoESです。
例えば署名時に生成されるデジタル署名データはPoESと言えますし、クラウド上の認証ログと操作ログが別途提供されその内容に整合性と非改ざんが保証できればPoESと言えます。ただし、当然ですがデジタル署名データの方が標準化されているということもあり、VALの保証レベルとしては高くなります。標準化されているということは、多くの専門家がチェックをした仕様という意味で信頼性が高くなります。

4.6 技術標準と認定制度の関係（トラストとは）

電子署名保証レベル（eSignAL）はあくまで技術的な保証レベルをまとめたものであり、「技術標準」をめざしています。一方で、最近では「トラスト（信頼）」と言う言葉がよく使われますが、トラストには「認定制度」による公的機関の保証が必要となると考えています（ただしトラストにはいろいろな考え方があります）。認定時に利用されるものが「技術標準」です。「認定制度」と「技術標準」は別々に存在するのではなく、両方が揃って「トラスト」を達成できます。トラストを実現する両輪とも言えるでしょう。
日本の電子署名法は署名技術に関しては具体的に書かれておらず、いろいろな署名方式が認められています。また電子署名法には、検証に関しては何も記述がありません。そのために、電子署名法の準拠性だけでトラストされた電子署名を実現することは困難だと言えます。まずは技術標準としての電子署名保証レベルを策定し、他の技術標準と組み合わせた要件を利用した公的な認定制度が望まれます。

※5　NIST SP 800-63-3　https://pages.nist.gov/800-63-3/
※6　JNSA（日本ネットワークセキュリティ協会）　https://www.jnsa.org/
※7　JNSA 電子署名ワーキンググループ 署名保証レベルタスクフォース　https://www.jnsa.org/result/e-signature/2021/esal/index.html

5 世界と日本の動向

欧州と米国においてもクラウド利用の電子署名が普及しつつありますが、アプローチ方法が異なります。欧州は域内のID認証と電子署名の規則（レギュレーション）として「eIDAS※8」を施行しています。「eIDAS」には「技術仕様」と「認定制度」が含まれており、標準化されたID認証と電子署名（デジタル署名方式）の環境を実現しています。欧州は大陸法ベースの事前に規定された法や規則に従うことで保証するアプローチと言えます。
米国では裁判に勝てるだけの証拠が重要視されています。米国の電子署名サービスは標準化されておらず、しいて言えば電子認証方式のサービスが多いようです。米国は英米法ベースの裁判による判例重視のアプローチと言えます。
日本においては判例重視の英米法に近いのですが、実際の「技術仕様」として「デジタル署名方式」と「電子認証方式」の両方が使われており標準化がされていない状況です。利用目的ごとに電子署名の保証レベルを選択し、必要なら海外との相互運用性を考慮して利用する必要があるでしょう。

※8　eIDAS Regulation　https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

6 おわりに

電子署名技術とひとことで言っても、いろいろな方式があることはご理解いただけましたでしょうか。ただし、どのような技術を使ったとしても電子署名として必要な要件である「本人性」「署名意志」「非改ざん性」は変わりません。法的な側面もあり分かりにくいと言われている電子署名技術ですが、本稿にて少しでも理解が深まったのであれば幸いです。
なお今後も保証をPKIではなくBC（BlockChain）を使った電子署名や、ID Wallet・VC（Verifiable Credentials）※9・DID（Decentralized IDentifie）のように、そもそも署名鍵や属性情報の持ち方も変わってくることが予想されます。電子署名技術の進化もまだまだ続きそうです。

（有限会社ラング・エッジ　宮地直人）

※9　Verifiable Credentials Data Model（W3c）　https://www.w3.org/TR/vc-data-model/