トラストセキュリティの概要と最近の話題

JNSA 電子署名 WG サブリーダー
有限会社ラング・エッジ
宮地　直人

1. はじめに

昨今では電子文書やデータのトラスト（信頼性）が問題になるケースが増え、「その文書が作成したのは誰なのか？またいつ存在していたのか？」と言う問いが新聞を賑わせている。これに対する1つの答えが、電子署名等の技術の利用である。

本稿では電子文書やデータの信頼性を守る電子署名のような技術を「トラストセキュリティ」と呼び、その概要と最近の関連トピックスを紹介する。なお「トラストセキュリティ」は造語であり一般的に使われ定義されている用語ではない。

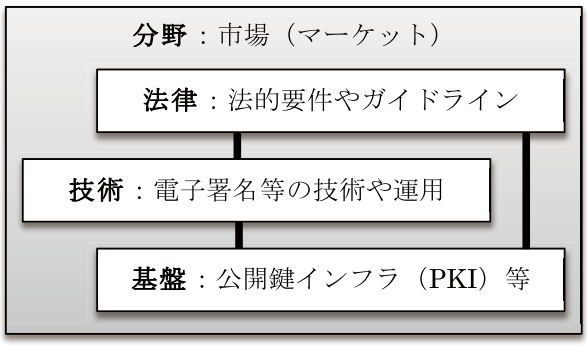
1.1. トラストセキュリティとは

電子文書等のコンテンツのセキュリティと言えば、暗号化やアクセス制御のようにコンテンツ自体を直接守る技術が一般的である。一方でコンテンツを第三者が閲覧する場合、そのコンテンツを誰がいつ作成し改ざんも無いと言うことを示す必要がある。この場合コンテンツ自体とは別に信頼性を守るセキュリティ、つまりトラストセキュリティが必要となる。

トラストセキュリティにおいて重要な点は「第三者」の存在と視点である。トラストセキュリティではトラストの証拠（エビデンス）を、第三者が検証できることが要求される。

2. トラストセキュリティの概要

トラストセキュリティは大きく分けて、「法律」「技術」「基盤」の3つの要素から構成される。これらの要素はターゲットとなる市場毎に要件が異なる。単純に技術だけの問題では無く、基盤と法律が絡むことが理解を難しくしている面があることは否めない。本稿ではトラストセキュリティの概要を要素毎に紹介する。



トラストセキュリティの構造図

2.1. 法律：法的要件やガイドライン

電子化以前において文書は紙として保存され、自筆署名や押印をすることで信頼性を担保していた。電子化された電子文書においては「電子署名」をすることで「紙の署名や押印と同等」と認める為の要件を定めた「電子署名法」やガイドラインを定めている国が多い。

◎ 日本

日本では「電子署名法」をはじめとして、「e文書法」「タイムビジネスに関わる指針」等の法律やガイドラインがある。ここではこれらの詳細は説明しないが、市場毎に関連する法律を確認することは必須と言える。日本では多くの法律においてPKIベースのデジタル署名（RSA署名等）が求められる。

◎ 欧州

欧州においては各国に電子署名法が存在しており、EUとして「電子署名指令」が定められていた。しかしより強い効力の「eIDAS規制」が施行された。適格な電子署名の法的有効性について手書き署名と同等と規定している。

eIDASはEUの「規制」である為に各国の電子署名法よりも強い拘束力を持つ。eIDAS規制では後述する「技術」や「基盤」についても明確に定義されており、現時点では最も整備されたトラストセキュリティと言える。欧州ではeIDAS規制に適合することで、電子署名

を利用した各国相互の電子取引が可能となっている。

Chapter III - Trust Services
Section 3 - Qualified trusted services
TSP:認証局やトラスト・リスト
Section 4 - Electronic Signatures
電子署名（XAdES/PAdES等）
Section 5 - Electronic seals
電子シール:組織や法人による電子署名
Section 6 - Electronic time stamps
電子タイムスタンプ

欧州eIDAS規制の電子署名関連部を抜粋

◎ **米国**

米国は欧州や日本とは少し事情が異なる。米国の電子署名法は「ESIGN Act」と呼ばれるもので、PKIベースのデジタル署名を要求しない。電子証拠（エビデンス）ベースの電子署名を認めている。既に多くのクラウド署名と言われるサービスがESIGN Actに準拠して使われている。

ESIGN Actでは細かい要件は求めておらず、必要に応じて証拠を提出する必要がある。具体的にはサービスの認証時や署名時の情報やログを保存し監査する運用が求められる。

なお米国においてもPKIベースのデジタル署名が求められる分野もあり、全てが非PKI電子署名と言う訳ではない。

Basic Requirements:
1. Intent to sign must be clear.
   署名する意図が明白でなければならない
2. The signature must be associated with the record.
   署名は記録と関係していなければならない
3. There must be clear consent to do business electronically.
   はっきりした電子取引の同意が必要
4. There must be access to records.
   記録へアクセスが可能でなければならない
5. No tampering of documents.
   文書の改ざんがされていないこと

米国ESIGN Actの基本要求

◎ **アジア**

アジアでは欧州eIDASのように国を跨り相互に有効な規制や法律を決める動きは無い。一方で中国や韓国においても電子署名やタイムスタンプは普及して来ており、アジア圏内における電子取引を活性化する為に今後相互運用についても検討されることを期待したい。

2.2. 技術：電子署名等の標準化技術

トラストセキュリティが第三者の検証を前提にしている以上、相互運用性の確保は必須となる。

日本と欧州は同じデジタル署名の技術を前提としていることから、10年以上前のECOM（次世代電子商取引推進協議会）の時代から共同して技術の標準化や相互運用性試験等を行ってきている。欧州ではETSI（欧州電気通信標準化機構）が電子署名技術の標準化を行ってきている。JNSAはETSIのアソシエート・メンバーであり、情報交換や仕様検討をおこなっている。

◎ **長期署名と検証**

「長期署名」は長期保管にも対応した電子署名の形式であるが、本来は「Advanced Electronic Signature」であり「先進署名」と呼ぶべき技術だ。例えばXML署名とXML長期署名のXAdESを比較すると以下の差異がある。

1. 署名証明書保護（XML署名ではオプション）
2. 署名タイムスタンプ：署名時刻を保証
3. 長期保管対応：検証可能期間の延長

1.と2.は長期保管しない場合でも有用な項目であり、XML署名よりもXAdESを通常利用すべきである。欧

州のeIDAS規制においても「適格署名」として長期署名形式が採用されている。XAdES以外にも、CMS形式のCAdESや、PDF形式のPAdES等がある。

長期署名は日本においても長期署名プロファイルとしてJIS化やISO化を推進してきた。しかしeIDAS規制では、欧州独自の長期署名仕様が標準化された。欧州の仕様は幾つかの点でJISプロファイルとは相容れない属性があり、今後別の道を進むのか歩み寄るのか検討が必要な状況にある。

また検証の標準化も課題である。署名自体は標準化されているが、検証手順に関しては決して明確になっていない。検証を標準化することで異なるベンダー間の相互運用が可能になる。

◎ 秘密鍵保管と利用

欧州のeIDAS規制では適格証明書と秘密鍵はSSCD（セキュア署名生成デバイス）に格納することが求められる。日本ではそこまでの要求はまだ無いが、SSCDに格納することが望ましい。

利用者の手元で利用するSSCDは、ICカードが最も一般的である。ICカードから秘密鍵を抜き出したり複製したりすることはできない。日本においてもマイナンバーカード（JPKI）やHPKIカード等で利用されている。

サーバーやクラウド側で使われるSSCDがHSM（ハードウェアセキュリティモジュール）である。最近ではクラウドHSMとして大量の利用者の秘密鍵を保管できるものが増えている。

◎ 電子認証

電子署名においてもサーバー連携して利用されるクラウド署名やリモート署名が使われはじめている。この時に重要となる技術が電子認証である。電子署名時には特に高い認証レベルが要求されることが多い。

欧州のeIDAS規制ではeIDとしてオンラインにおける公的個人認証のレベルも定義されている。日本では電子署名時の認証についてJNSAリモート署名TFにて検討と策定を進めている。

◎ 短期証明書（ワンタイム証明書）

電子署名時に短期間（1回）だけ有効な電子証明書と秘密鍵を発行し、署名後すぐ秘密鍵を破棄する電子署名の運用方法がある。署名時に必ず有効である為に「失効」の考え方を不要とできる利点がある。日本ではまだ事例は少なく標準化もされていないが、今後利用が進む可能性がある。

◎ 電子シール

電子シールは欧州のeIDAS規制で定義された利用方法であり、技術的には電子署名とほぼ同じであるが署名者が自然人では無く、法人や部署や組織である点が異なる。例えば電子領収書に用いられるが、コード署名も法人名の証明書で署名されるので電子シールの一種と言える。

日本においては法的な裏付けが無くまだ一般的では無いが、今後電子社会において必要性が高まることが予想される。

◎ 暗号スイート

現在電子署名で一般に使われている暗号アルゴリズムは、RSA-2048bitとSHA-2である。当面はこれで良いとしても次世代の暗号スイートとして、例えば量子コンピュータへの耐性を持つ、耐量子暗号の調査と検討は進めるべきである。

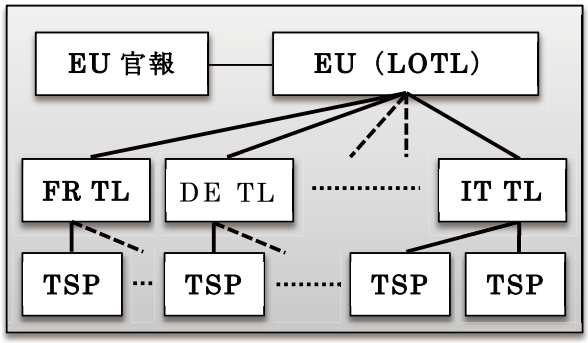
◎ 運用とエビデンス保管

特に米国ESIGN Actでは重視されるが、デジタル署名を行う場合であっても、運用ポリシーの策定とログ等の証拠の管理と保管は必須と言える。特にクラウド署名やリモート署名においてはサーバーが関与する為に運用や管理は特に重要となる。

2.3. 基盤：公開鍵インフラ（PKI）等

最後の要素は基盤である。日本と欧州ではPKIがベースになっている。PKIではルート証明書を頂点としたPKIドメインに分けられる。日本では公的なPKIドメインとしてGPKI・LGPKI・JPKI・商業登記・認定認証局があるが、これらはブリッジ認証局を介して並列的な構造で相互接続されている。

欧州のeIDAS規制ではトラストリスト（Trusted List）と言うツリー型の構造により登録各国のPKIドメインを相互接続している。まず国単位で認定された適格TSP（Trust Service Provider：認証局等）をまとめたトラストリストを作成、次にEUのEC証明書をトップとしたLOTL（リストオブトラストリスト）でトラストのツリー構造が作られる。既にAdobe Reader/Acrobatが対応している。

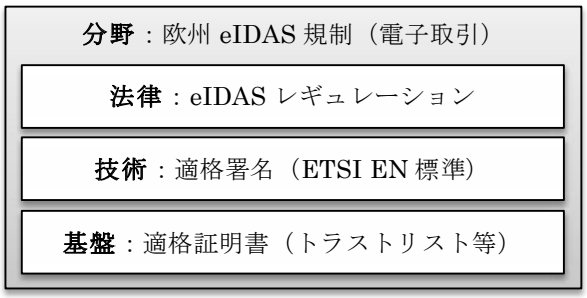


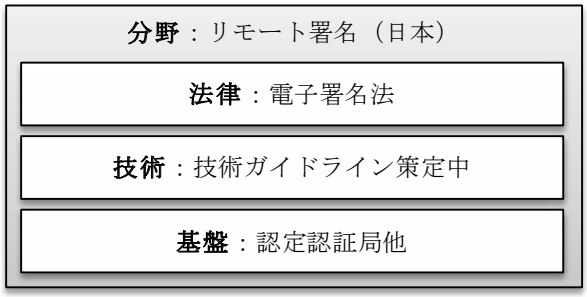
欧州eIDAS規制のトラストリスト

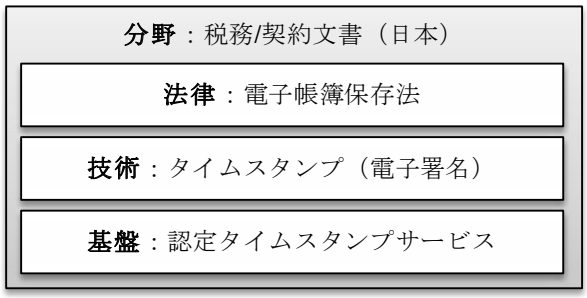
日本の基盤は国内に閉じており、海外との連携も検討が必要である。他に新たな基盤としてブロックチェーン利用の可能性もあるだろう。更にIoT時代にも対応したトラスト基盤も必要である。

3. トラストセキュリティ適用分野の分析

「法律」「技術」「基盤」をトラストセキュリティの適用分野（市場）毎に分析をした。







他にも色々な分野や市場があるが「法律」「技術」「基盤」がどうかと言う視点で見て頂きたい。

4. 最近の話題

4.1. マイナンバーカード（JPKI）

JPKIは住基カードからマイナンバーカードに変更となり、新たに認証用の利用者証明書が含まれた。これに

よりオンライン時の本人確認への道が開けた意義は大きい。例えば今秋正式開始予定のマイナポータルにおいてもマイナンバーカードを利用した認証や署名が可能となる。

マイナンバーカードの課題としては、個人情報となる4情報（氏名・性別・生年月日・住所）が含まれる署名用証明書の管理や、検証時の失効確認に申請と課金がかかる点がある。

オープンソースのICカードドライバであるOpenSCにて、マイナンバーカードへの対応が進んでいることも、新たな利用やサービスへの道を開く可能性があり期待される。

4.2. リモート署名とクラウド署名

欧州ではeIDAS規制対応のクラウド署名として、アドビシステムズ社が中心となりCSC（クラウド署名コンソーシアム）が設立された。CSCではAPIやプロトコルの技術仕様を標準化してクラウド署名の普及を目指している。

日本では2015～2016年度に、経済産業省の電子署名法研究会とJNSA電子署名WGメンバーが中心となり関係各団体が連携したリモート署名TFにてサーバーによる署名の技術仕様や運用ポリシーを検討してきた。2017年度は、これまでの検討結果をまとめた技術ガイドラインの公開を目標とし、新たにユーザー企業も加え、仮称JTSC（Japan Trusted Signature-service Consortium）の立ち上げを目指している。

4.3. 海外ベンダーや欧州ETSI/CENの動き

欧州のETSI/CENは日本や米国にeIDAS規制をベースにした相互運用を推進する為に動き出している。今年の3月8日には米国で「US Government and EU Workshop on Digital Signatures!」を、7月4日には日本で「日欧インターネットトラストシンポジウム」を開催している。また欧州のHSMベンダーや前述のCSCも春以降に相次いで担当者が来日してセミナーを開催している。

JNSAにおいてもリモート署名TFやJTSC（仮称）を中心に今後相互運用を含め対応していく予定である。

4.4. PDF/PAdESのISO標準

8年近くの歳月がかかったが、PDF 2.0であるISO 32000-2がやっと発行された。またJNSA電子署名WGの標準原案作成TFが参加してきたPAdESプロファイルISO 14533-3も発行段階をむかえている。ISOにおけるPDFの電子署名については基本的な仕様が出揃ったと言える。

4.5. 医療情報分野

電子処方箋の運用ガイドラインが2016年3月に厚生労働省より公開され、これをベースにJAHIS（一般社団法人保健医療福祉情報システム工業会）から2017年5月に「JAHIS電子処方せん実装ガイド Ver.1.0」が公開された。

医療情報では既にHPKIと言う基盤があり電子化が推進されている分野である。

5. おわりに（JNSA 電子署名 WG）

トラストセキュリティは今まさに色々な市場で必要とされ活況を呈してきている。eIDAS規制をベースに海外からも黒船が来ており日本としての対応も検討が必須となっている。

筆者としては若い技術者の皆さんにもトラストセキュリティの知識を持って頂きたいと考えている。本稿で示した通りクラウドへの展開も始まっており、地味かもしれないが新しい市場においてやりがいのある分野である。もしトラストセキュリティに興味があれば是非一度JNSAの電子署名WGに参加頂くか、勉強会も開いているのでそちらでも情報を得ることができる。JNSA電子署名WG実験サーバー（http://eswg.jnsa.org/）で勉強会の予定や各種情報を得ることができるので是非チェックや参加を検討して欲しい。

最後に、本稿の内容は、筆者の個人的見解であり、JNSA電子署名WGの見解ではない。内容に問題があれば筆者が全ての責を負うものである。