次世代電子署名認証法制に向けた検討課題

―eIDAS等最近の動向をも視野に入れて―

神戸大学大学院法学研究科

米丸恒治

セミナー内容

- 署名法、認証法研究の経緯（はじめに）
- １　電子署名法のあるべき課題（整理）
- ２　次世代認証基盤法制へ向けて
- ３　わが国の電子署名認証法の課題
- ４　おわりに

署名法、認証法の調査（経緯紹介）

- 約20年前から電子署名法を調査研究
  2000年日本署名法　← ドイツ　デジタル署名法等
  行政手続オンライン化法・e文書法等により電子(化)文書の利用等を原則解禁
- 電子署名法制、電子認証法関連のテーマ
  デジタル署名＋デジタル・タイムスタンプ等
- 電子署名付き文書の長期保存等の法制度(必須)
- 電子署名付き文書の文書形式の変換　(必須のはず)
- 法的に安全な電子化プロセス、標準化動向
  ドイツ、EUを中心とした調査研究
  特に、ドイツの新身分証明書法、De-Mail法とそれに至るシミュレーション・標準化等は、その構想段階から注目して調査・研究してきた。

電子署名法の骨子

- 「電子署名及び認証業務に関する法律」
- 2条　定義「電子署名」
  電磁的記録に対する措置であり、
  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。　⇒署名者の本人確認
  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。　⇒対象データの非改ざん・完全性
- 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。

※電子署名のアルゴリズムの定義規定は、政令で定める。
　署名用ソフトウェアや、署名用デバイスの認定（認証）の規定はない。
※主要な部分は、指定認定機関等に関する規定である。

1　電子署名法のあるべき課題（整理）

(1) 特定認証業務の基準
　　特定認証業務の基準をより明確にすべき。

(2) 電子署名の利用性向上のために、認証基準のレベルを分けるべき。　Cf. EU指令、eIDAS規則でも。
登録印、認印、メール署名など用途に応じて。

(3) 特定認証業務を最低限届出制にして、主務官庁の監督権を明示すべき。　(現行法、認定認証業務のみ)
※報告要求、立入検査権等を明記し、安全・安心な利用環境を整備　→　普及を!!

(4) 認証業務休廃止時の業務承継・検証環境確保措置を明記し、保障体制を構築すべき。
※利用者の保護のため、検証環境長期確保は重要な課題

1　電子署名法のあるべき課題（整理）

(5) 署名鍵の安全性を明確にすべき
　HSMは、多様化しうる。モバイル署名、ローミング鍵の利用等も、多様に想定される中で、署名用途に応じた安全性＋柔軟性の最適化

(6) 署名付文書の長期的な検証可能性の実現
　①署名付文書の長期的な保存→検証可能性確保の重要性を法制的に支援すべき。
　Cf.ドイツ署名法では、当初から想定していた。
　②長期保存に際しユーザへの教示を！
　③想定される暗号アルゴリズムの危殆化等への対応について、法制度で明示＋適格暗号アルゴリズム等の公示（移行プラン）⇒　適格認証サービス全体の移行を
　④電子保管サービス(証明サービス)への移管・保存

1　電子署名法のあるべき課題（整理）

(7) 認証業務についての責任の明確化
①損害賠償責任の明示、担保の確保
②損害賠償についての立証責任の転換を
事業者側での無過失の証明が必要では
③証明書中の利用限度額設定とのバランス
日本法では想定せず　要検討！

(8) 「属性」認証、「資格」認証の法制化
属性等RAとCAの協働を認める法整備

1　電子署名法のあるべき課題（整理）

(9) 個人情報保護の明示と「仮名pseudonym」

①個人情報保護の厳格化は必須

②個人情報保護の観点からの「仮名」利用

※「本人確認がされたID/識別名」の利用

⇒　証明書への「仮名利用」明示を

⇒　「仮名」の開示手続の整備も必要になる

※プロバイダ責任制限法の開示手続が参考

(10) 相互運用性の確保

1　電子署名法のあるべき課題（整理）

(11) 時刻認証の定義、信頼性要件等整備

※電子署名とタイムスタンプの組み合わせ

電子署名＝電子データについての責任

①誰が、②どのデータに署名(押印)したか

タイムスタンプ＝①いつ、②どのデータが存在

※ドイツ等では、電子署名法中にタイムスタンプ業務を組み込んできた！　日本法には欠如！

※タイムスタンプのみでも、多様な用途が想定される。　Cf. 各種医療データ、実験データの存在証明

※タイムスタンプについても、長期的な検証確保を!

２　次世代認証基盤法制に向けて

(1) 電子書留メールの法制的支援

電子書留メールの要件、(関連サービス　例：保管・保存)

※ドイツDe-Mail法制とその実証実験での構想

＝電子書留メール(セキュアな意思表示手段)

＋構想段階

暗号化・復号化のサービス

長期保存サービス(長期署名フォーマット/LTANS・ERS)

注）De-MailとE-Postbrief(DP)の囲い込み

注）ドイツ電子政府法　電子訴訟手続促進法

適格署名、eID、De-Mailを手書き署名と同等扱い

※eIDAS規則で、電子書留(送達)サービス規定

２　次世代認証基盤法制に向けて

(2) Webサイト認証の法制的支援

※サイトのなりすまし、別サイトへのジャンプ等からのユーザの保護

※eIDAS規則でもWeb認証サービスにつき規定

※ユーザに分かりやすい表示（ブラウザ等）

(3) 今後の欧州各国等の動向のフォローアップ

◎eIDAS規則では、各国の電子署名・認証法制がすべて置き換わるわけではない点に注意！

例：ドイツでは、従来の電子署名法制を生かしつつ、eIDAS規則で「上書き」される部分を改正する方向か。

３　次世代電子署名認証法へ

(1) 各省の権限を越えて次世代へ
　次世代電子署名認証法制は、官公民を通じた基盤法制であり、省庁の垣根を越えた法制化が必要

(2) 官民の役割と責任の明確化
　民間事業者への多様なサービス展開の機会確保
　信頼性確保・責任体制の明確化は、必要！
国は、法制化を通じて、多様なサービスの可能化
最終的な長期的責任体制の構築の責任を負うべき。

(3) 民間によるサービスの多様化・可用性拡大と信頼性確保　　多様なビジネスモデルはあるが、信頼性・安全性の問題はさらに別問題では。

(4) ICT技術の発展への柔軟性＋信頼性の確保
モバイル署名、自動刻印等々

主要参考文献(署名法概説書割愛)

- 拙稿「ドイツ・デジタル署名法と電子認証」立命館法学256号31-73頁（1998年）
- 拙稿「〔資料〕EU電子署名指令」(立命館法学268号276-292頁)　その後一部改訳版あり。
- 拙稿「〔資料〕ドイツ新電子署名法」(立命館法学279号163-180頁)2002年
- 拙稿「電子署名法の課題」(Law&Technology No.19, 15-27頁) 2003年
- 拙稿「電子署名法制とタイムスタンプに関する規定の整備(タイムビジネス推進協議会『タイムビジネスに関するドイツ動向調査報告書』3-27頁、法令等資料1-39頁)」2004年
- 第1部 電子署名法制度の在り方に関する調査研究(日本情報処理開発協会(経済産業省委託調査)『電子署名法の在り方と電子文書長期保管に関する現状調査報告書』2005年

主要参考文献

- 拙稿「電子カルテ等の証拠性の長期的な確保について－電子署名およびタイムスタンプの利用と長期保存の課題を中心に－」(年報医事法学21号22-29頁) 2006年
- 拙稿「電子署名の安全な利用と電子署名法の課題－施行状況検討の年にあたって－」(情報ネットワーク・ローレビュー5巻150-160頁) 2006年
- 拙稿「電子署名済文書の証拠性確保と長期保存－その法的要求事項と対応策の現状と課題－(Law & Technology 33号26-36頁) 2006年
- 拙稿「ドイツにおける電子署名付行政文書の長期保存対策(行政＆ADP2007年1月号32-41頁) 2007年
- 拙稿「ドイツにおけるeIDカード(電子身分証)の概要と特徴－eIDの官民共用と個人情報保護のしくみ－(行政＆情報システム46巻1号32-37頁) 2010年
- 拙稿「電子取引における認証と個人情報保護－ドイツ新電子身分証明書における認証と個人情報保護技術－(Law&Technology誌51号54-63頁) 2011年
- 拙稿「ドイツDe-mailサービス法の成立－安全で信頼性ある次世代通信基盤法制としてのドイツ版電子私書箱法制－(行政＆情報システム2011年6月号30-35頁) 2011年
- 拙稿「ドイツDe-Mailサービス法案の概要－インターネット上の安全で信頼性ある通信基盤法制整備の試みとして－(情報ネットワーク・ローレビュー第10巻149-158頁) 2011年
- 拙稿「ドイツDe-Mailサービス法－安全で信頼性ある次世代通信基盤法制としての認証付メール私書箱法制－(多賀谷一照・松本恒雄編『情報ネットワークの法律実務』第一法規、加除式)2731-2741頁（）2011年

主要参考文献

- 拙稿「ドイツDe-Mailサービス法の概要とEUへの波及－安全で信頼性ある次世代通信基盤法制へ向かう独欧－(『日本データ通信』2013年3月号)18-24頁）2013年
- 拙稿「電子認証(eID)の導入動向―欧州とドイツ((多賀谷一照・松本恒雄編『情報ネットワークの法律実務』第一法規、加除式) 2013年
- 拙稿「先端研究を支えるエビデンスがない!?(Law＆Technology64号60-61頁（2014年
- 拙稿「行政文書の電子化と一元的管理に向けた動向と課題―ドイツの電子政府法・標準化動向等の紹介を中心に―(行政＆情報システム2014年10月号) 2014年

ご静聴ありがとうございました。

- 最適化された電子署名認証法制の実現に向けて議論を進めましょう！
- 技術と法制度の最適な組み合わせにより、日本版「適格電子署名認証法制」実現に向けて、議論が求められています！