電子署名法の課題と未来

―Society5.0時代を支えるトラスト技術と電子署名法--

2020年12月18日

セコム（株）IS研究所　松本　泰

松本の自己紹介　セコム（株）IS研究所　ディビジョンマネージャー

信頼される安心を、社会へ。
SECOM

- 1984年　UNIX上のビデオテックス・パソコン通信システムの開発に従
- 1994年　各種インターネットサービスの設計、開発、運用に従事
- 1999年　サイバーセキュリティ事業の立ち上げに従事
- 2003年-2007年　工学院大学「セキュアシステム設計技術者の育成」プログラム客員教授
- 2007年　経済産業省 商務情報政策局長表彰「情報セキュリティ促進
- 2007年-2012年　IPA 情報処理推進機構 情報セキュリティ分
- 2011年-2012年
  - 社会保障・税に関わる番号制度　情報連携基盤技術WG　構
  - 社会保障・税に関わる番号制度　社会保障分野サブWG　構成員
- 2013年-2014年
  - 内閣官房　パーソナルデータに関する検討委員会・技術検討WG　構成員
- 2008年-2018年　JDCC 日本データセンター協会　セキュリティWGリーダ
- 2020年12月現在
  - CRYPTREC 暗号技術検討会構成員、暗号技術評価委員会　委員、暗号技術活用委員会　委員
  - 日本ネットワークセキュリティ協会　PKI相互運用技術WGリーダ
  - 日本ネットワークセキュリティ協会　標準化部会　副部会長
  - 日本トラストテクノロジー協議会（2017年11月設立）副代表
  - JST/RISTEX 公私領域アドバイザー
  - QST SIP光・量子技術評価委員会委員
  - 津田塾大学総合政策学部非常勤講師（情報セキュリティ論）

サイバーセキュリティと情報プラットフォームを担当

この時期に、公開鍵暗号技術に基づく電子署名技術等について携る

2001年からJNSA PKI相互運用技術WGで活動
最近は、もっぱら主にIoTデバイス等で利用する公開鍵暗号技術などを中心に活動

電子署名法の課題と未来
―Society5.0時代を支えるトラスト技術と電子署名法--

- 未来のイメージ
- 電子署名法の（歴史的）成り立ちと立て付け
- プラットフォーム的視点からの電子署名法の課題

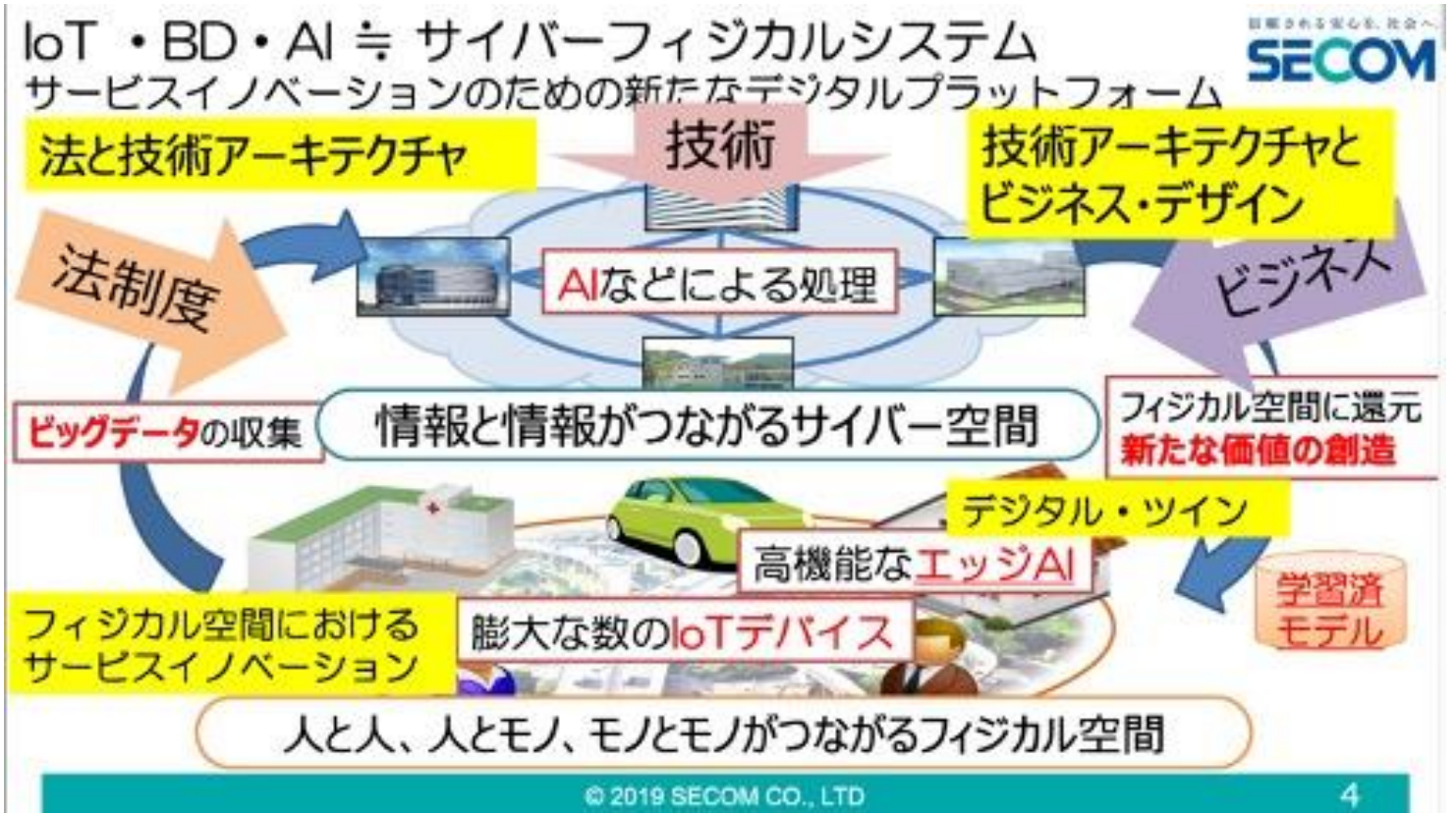
付録
- 過去からの議論
- 電子署名法の立て付けと課題

未来のイメージ

Society5.0時代を支えるトラスト技術的視点

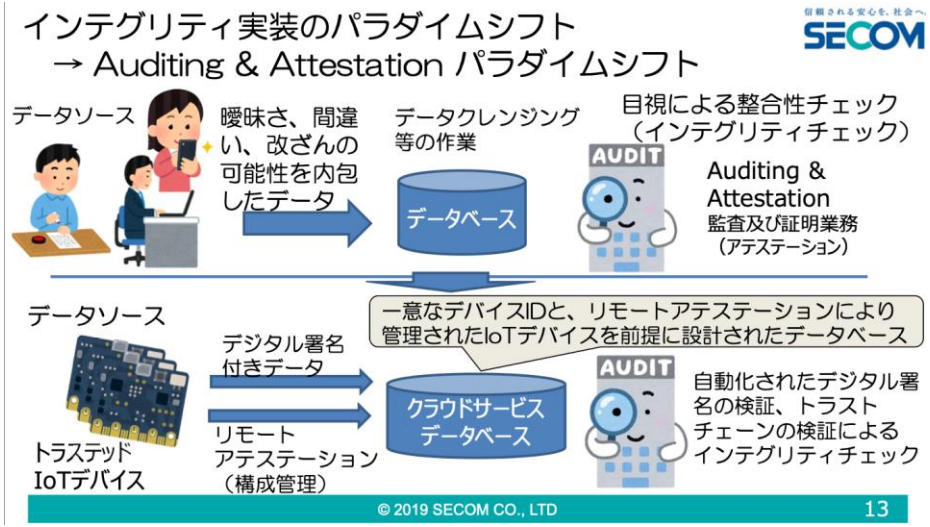
10年後をイメージして喋った昨年の「データ戦略の課題と未来」シンポジウム「データ戦略のためのITシステム」

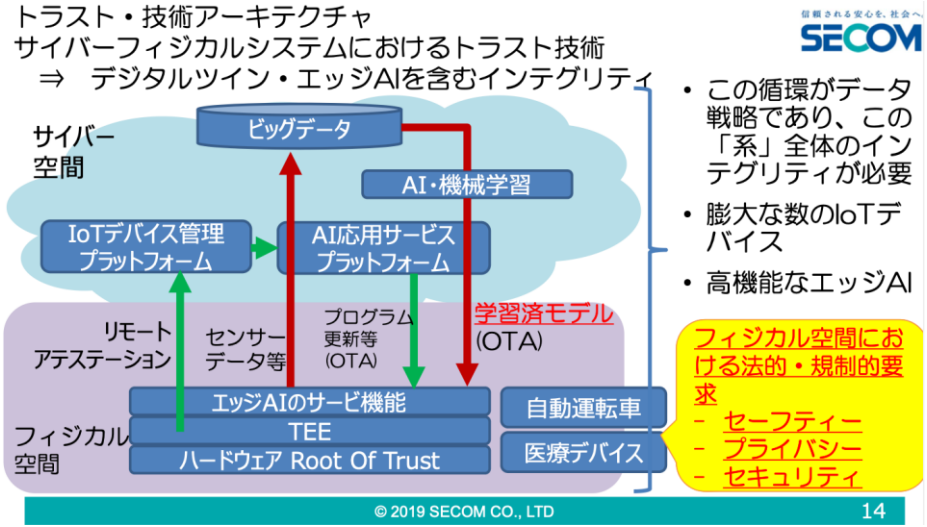
https://www.jlf.or.jp/assets/work/pdf/kenshu_190910_04.pdf



10年後をイメージして喋った昨年の「データ戦略の課題と未来」シンポジウム「データ戦略のためのITシステム」

https://www.jlf.or.jp/assets/work/pdf/kenshu_190910_04.pdf

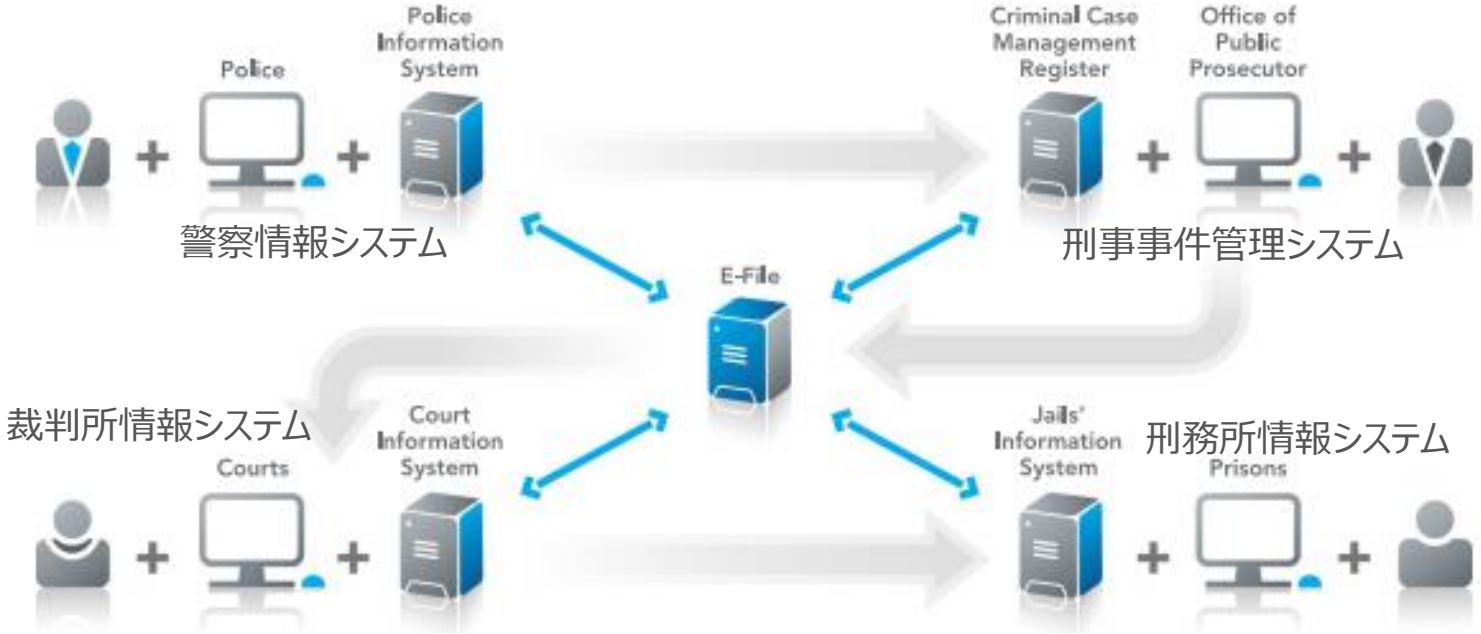




様々な主体（自然人、法人、サービス、IoTデバイス、AIエッジ）が、様々な証明などのために、様々なデータ・オブジェクト（書面、時刻、プログラムコード、 AI学習モデル）にデジタル署名を施し、リアルタイムに様々な連携のために、様々な場所からデジタル検証に基づいたトラストな自動化・スマート化が行われると言った世界

様々な連携？
Estonian e-File system(2008年から)

出典 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/07/29/Estonian+e-File+system



e-Fileは、訴訟の当事者とその代理人が電子的に文書を裁判所に提出し、それらに関連する訴訟の進行状況を観察できるようにするオンライン情報システムです。たとえば、ひとり親は、郡庁舎に行かなくても扶養手当を申請できます。

たぶん、欧州のeIDASの目指す世界観に近い。機微な情報の共有のためには、高い保証レベルの識別・認証（Identification＆authentication)と資格に応じたアクセス制御が必要。そして（機微な情報を扱うための）高い透明性であり、その高い透明性に必要なインテグリティと否認防止性

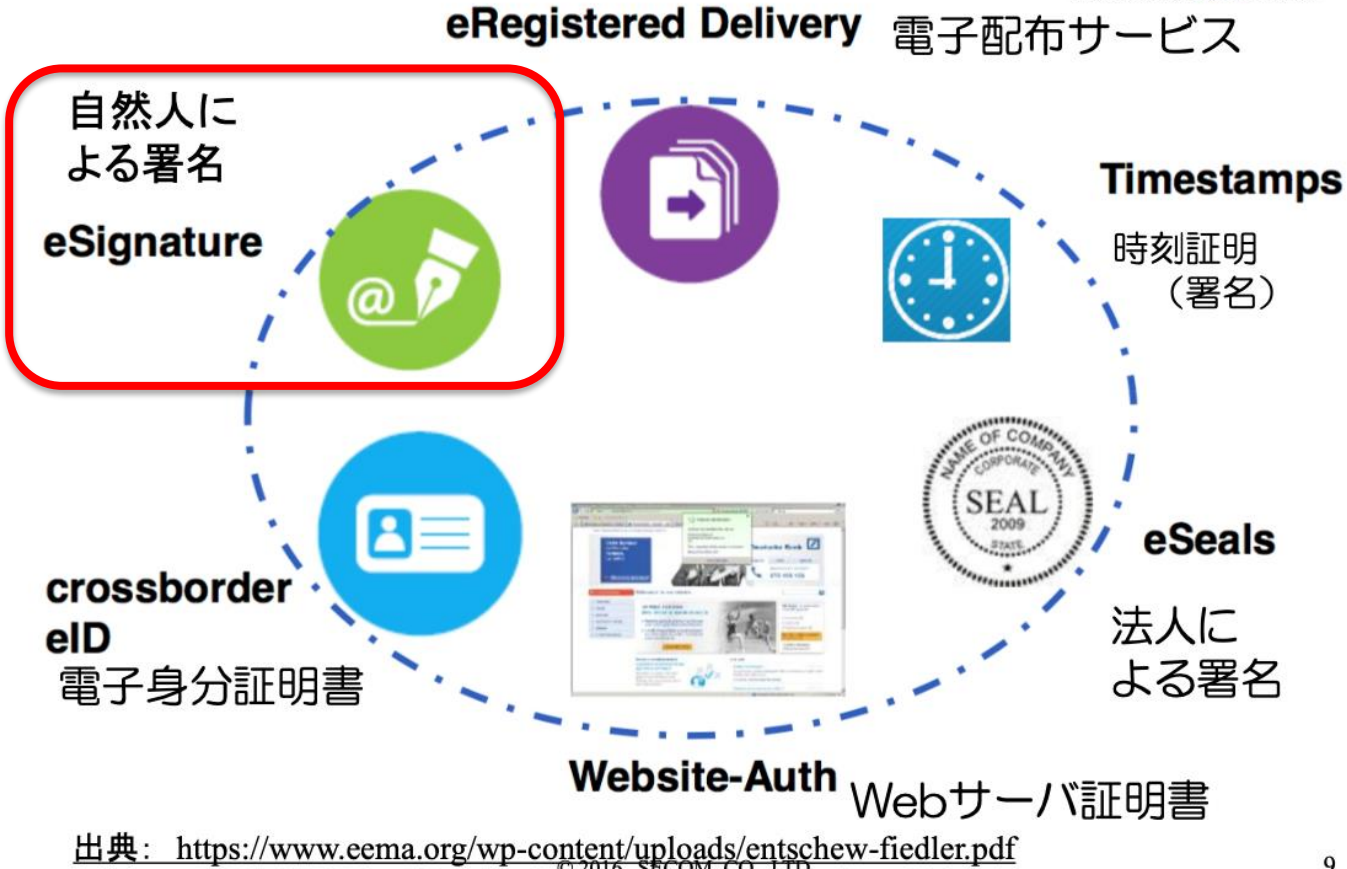
電子署名法の（歴史的）成り立ちと立て付け

2000年に成立した電子署名法
成立当時の状況と今日の状況

欧州と日本の電子署名法と個人情報保護法の動向

- 1995年　EUのデータ保護指令
- 1999年　EUの電子署名指令
  - →　日本の電子署名法に大きな影響を与えていたが。。。
- 2001年　電子署名法施行
- 2005年　個人情報保護法全面施行
- 2016年　EU eIDAS規則施行
  - 指令から規則へ。枠組み自体が大幅に変更された。
- 2017年　改正個人情報保護法施行
  - 主務官庁制度から個人情報委員会へ、4年毎の見直し
- 2018年　EU一般データ保護規則施行（GDPR）
  - 指令から規則へ。eIDASと同じく、欧州の単一市場戦略の影響が大きい。
- 2020年　20年ぶりの電子署名法の議論？？
- 202x年　電子署名法の未来？？？？？

欧州のeIDAS規則によるトラストサービス



9

出典：
2019年　トラストサービスの調査ワークショップ
EUの技術標準（松本）
https://itresearchart.securesite.jp/19ws207/docs/s03.pdf

技術的観点、相互運用性の観点からは、「自然人による署名が eSignature」が単独で存在しているわけではなく、深く連携している」

規制モデルの欧州と市場モデル米国の電子署名法

出典：2010年　PKI Day 2010 <社会基盤としてのPKI/PKIの10年>
https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

電子署名法の”Teething problem”？？
この認識がないと将来は”long-term problem”に苦しむ？

セコムIS研究所 Intelligent Systems Laboratory

Continental European Approach

Prevention through
comprehensive pre-implementation checks for
- products,
- technical, administrative and organisational aspects of certification activities, and
- reliability and specialised knowledge of staff.

- Development costs (evaluation of products and security concepts)
- More time-intensive in initial stages

"Teething problem"

Anglo-Saxon Approach

Ensuring adequate minimum level of
- competition in the market, and
- liability.

Liability depends on
- ability and willingness to assume liability in cases of damage, and
- recognised cases of damage.

Long-term problem

http://www.efpe.eu/upload_module/downloads/efpe/2006/prezentacje/2/06_JSchwemmer_BNetzA.pdf

28

米国の電子署名法

セコムIS研究所 Intelligent Systems Laboratory

James Bond	[*Digitized image of handwritten signature*]
/s/ James Bond	[*Typed name*]
007	[*Number or PIN*]
X	[*"X" or other random letter*]
☺	[*Smiley face or other picture*]
I Agree to these terms	[*Words typed in box*]
I AGREE	[*Button clicked with mouse*]

-----BEGIN SIGNATURE-----
iQCVAwUBMARo7vgyLN8bw6ZVAQF6ygP/fDnuvdAhGlDWsSMXUIR
MuNHYzdZ00cqkDb/Tc2+DuhuEa6GU03AgZY8K9t5r9iua34E68pCxo
gUz009b1OcjNt6+o+704Z3j1YY9ijYM8BWNaSp9L2W4nUuWBdlyIWy
ol/2PjjRVNZEtqtSRQnPEpJ2IHtz9iGovHf0Sqh
-----END SIGNATURE-----

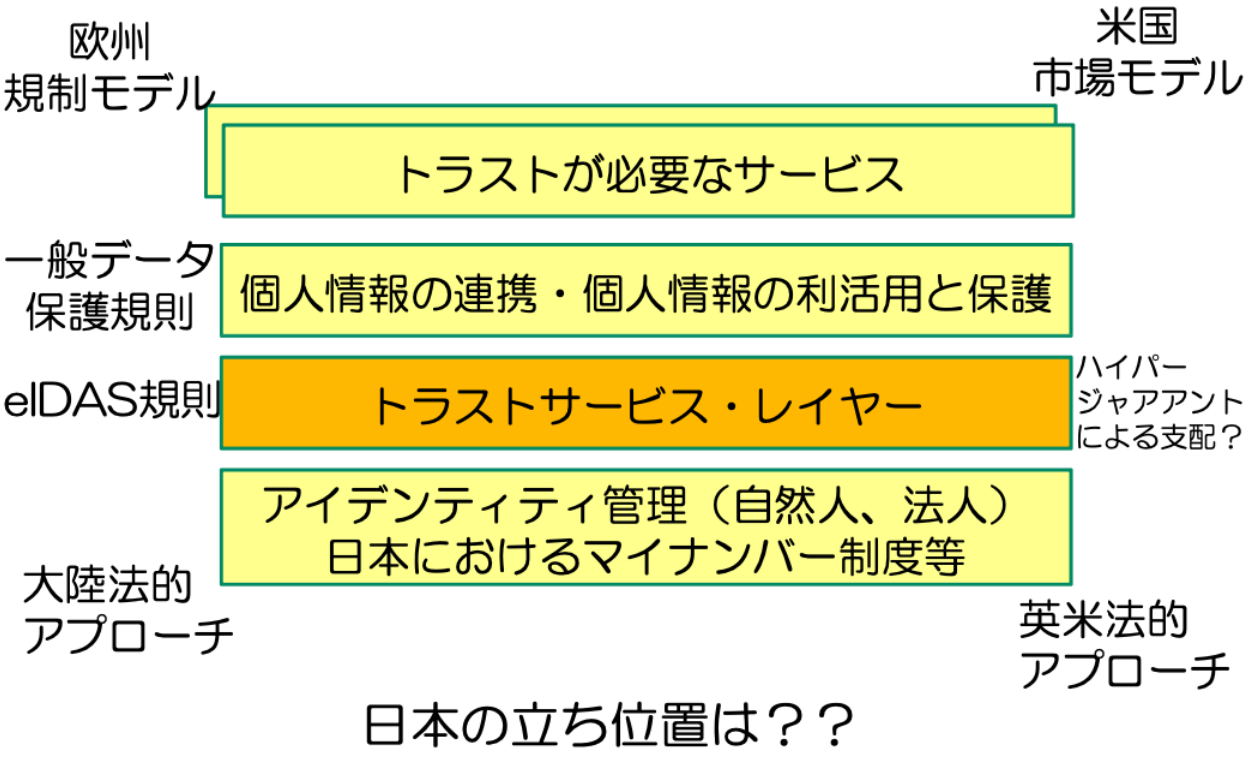
[*Digital signature*]

http://www.fips201.com/resources/audio/iab_0210/iab_022410_smedinghoff.pdf

29

欧州・米国・日本

セコムIS研究所
Intelligent Systems Laboratory



出典：
暗号技術によるトラストの確立に向けて
2015 年　松本
http://c-faculty.chuo-u.ac.jp/~tsujii/pdf/160606matsumoto.pdf

電子署名法の第一条　→　目的が最も重要

- 第一条
  - この法律は、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とする。

「特定認証業務に関する認定の制度その他必要な事項を定めること」は、

本当に

国民生活の向上及び国民経済の健全な発展に寄与したのか？？

電子署名の定義・特定認証業務・認定認証業務

付録：電子署名法の立て付けと課題

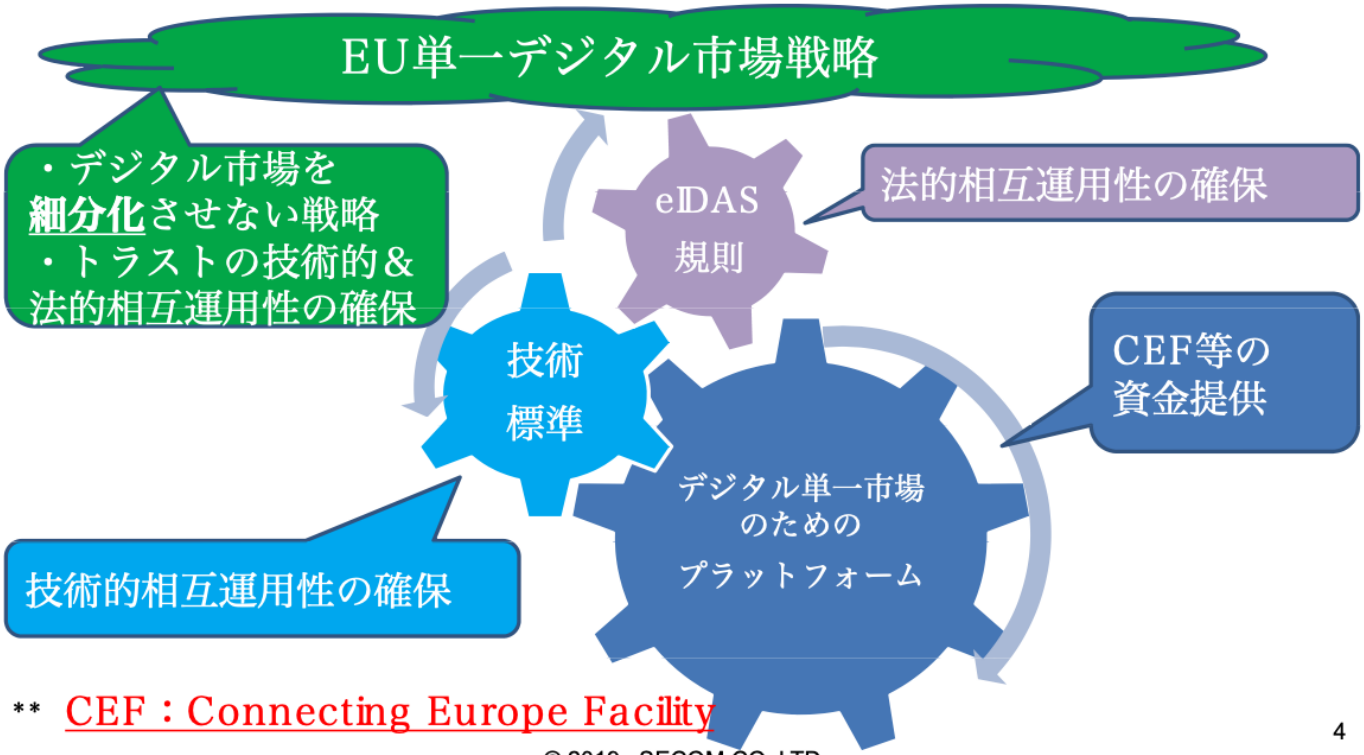
- 電子署名の定義
  - ２条　　→ 割となんでも良い？
- 特定認証業務
  - 署名法２条－３　この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。
  - 主務省令で定める特定認証業務の基準
    - 「平成十三年総務省・法務省・経済産業省令第二号電子署名及び認証業務に関する法律施行規則」　→ ほとんど基準と言えるものは、何も書かれてない。記述されているのは「暗号アルゴリズムのみであり、認定認証業務で要求される、設備、運用、本人確認などの記述は皆無。
- 認定認証業務
  - 署名法４条から47条は、認定認証業務関連
    - 設備、運用、本人確認などに、厳しい基準を課している。
    - 1999年のEU電子署名指令における「適格電子署名Qualified Electronic Signature 」の影響を強く受けている。

信頼される安心を、社会へ。
SECOM

プラットフォーム的視点のからの
電子署名法の課題

欧州のeIDAS規則

ＥＵの技術標準とデジタルプラットフォームの関係



** CEF：Connecting Europe Facility

4

出典：
2019年　トラストサービスの調査ワークショップ
EUの技術標準（松本）
https://itresearchart.securesite.jp/19ws207/docs/s03.pdf

電子署名(eSignature)と電子認証(eAuthentication)のLoA(Level Of Assurance)と統合

出典：2006年　社会基盤としての電子認証と電子署名
https://www.jstage.jst.go.jp/article/nig/43/5/43_5_324/_pdf

総説　特集「認証技術とその応用」

社会基盤としての電子認証と電子署名

Electronic Signature and Authentication for Social Infrastructures

Yasushi MATSUMOTO*　松本　泰*
*SECOM Co.,Ltd.
8-10-16, Shimorenjyaku, Mitaka-shi, Tokyo, 181-8528 JAPAN

1. 基盤としての電子署名と電子認証

IT 技術が社会に深く浸透していく中，これからの社会の共通基盤として，ネットワーク基盤と認証基盤（電子署名と電子認証の基盤）の必要性が言われ続けている．たとえば 2006 年夏に発表された e-JAPAN 重点計画 2006 でも，ネットワークと認証に関わる多くの記述があるが，重点分野の最初に取り上げられている医療福祉分野においても，以下のような記述がある[1]．

これらの課題のもと，医療・健康・介護・福祉分野の情報化に関する横断的なグランドデザインを速やかに策定した上で，まず医療の情報化の共通基盤である安全かつ安価な大容量ネットワークの構築や，医療機関・従事者・患者等の認証の仕組みの確立等に着実に取り組む．

ここでは，医療情報等を高度に利活用するため，共通基盤としてのネットワークと認証の必要性を説いている．こうしたことは医療福祉分野に限らず必要とされているが，安全なネットワークとそのネットワークを利用するための認証基盤の構築ということに関しては，まだ大きな課題がある．

様々な分野で必要とされている認証基盤であるが，現時点で一般的に認証基盤と認識されている公的個人認証サービスの普及と利用は低迷しており，電子署名も普及しているとは言いがたい状況にある．認証基盤の必要性の理解や，実際の認証基盤の構築を行なう上において，電子署名，電子認証（e-Authentication），認証（Certification）といった言葉の意味を正確に理解する必要がある．電子署名は，作成した文書等の責任を明確にするために必要になり，電子認証は，こうした文書等を適切な権限を持った人が参照等を行なうために必要になる．

電子署名と電子認証を理解する上で認証（Authentication）と認証（Certification），2 つの「認証」という用語は，多くの混乱の元になっている．多くの法律用語において「認証」は，英語の Certification を意味する．それに対して，サーバ等によるユーザの真正性の確認を意味することも認証（Authentication）と呼ばれる．Certification は，何らかの権威者が発行する証明書により何らかのことを証明する．公としての行政機関は従来からこの Certification を数多く行っており，その証としての証明書の発行を行なってきた．そのため法制度等において「認証」は Certification を意味することが多い．そのため Certification の電子化自体も多くの場合，電子署名の技術を用いて実現される．

1984年 UNIX上のビデオテックスの開発に従事
1990 年 UNIX 上の大規模パソコン通信システムの開発に従事
1994 年各種インターネットサービスの開発に従事
1998 年サイバーセキュリティ事業の立ち上げに従事
2006 年 9 月現在，NPO 日本ネットワークセキュリティ協会 PKI 相互運用技術 WG リーダ，電子署名・認証利用パートナーシップ (JESAP) 利用促進部会長，工学院大学「セキュアシステム設計技術論の高度」プログラム客員教授　IPA 情報システム等の脆弱性情報の取扱いに関する研究会 委員　CRYPTREC 暗号技術検討会メンバー．ECOM セキュリティ WG/ 電子署名認証 SWG サブリーダ．

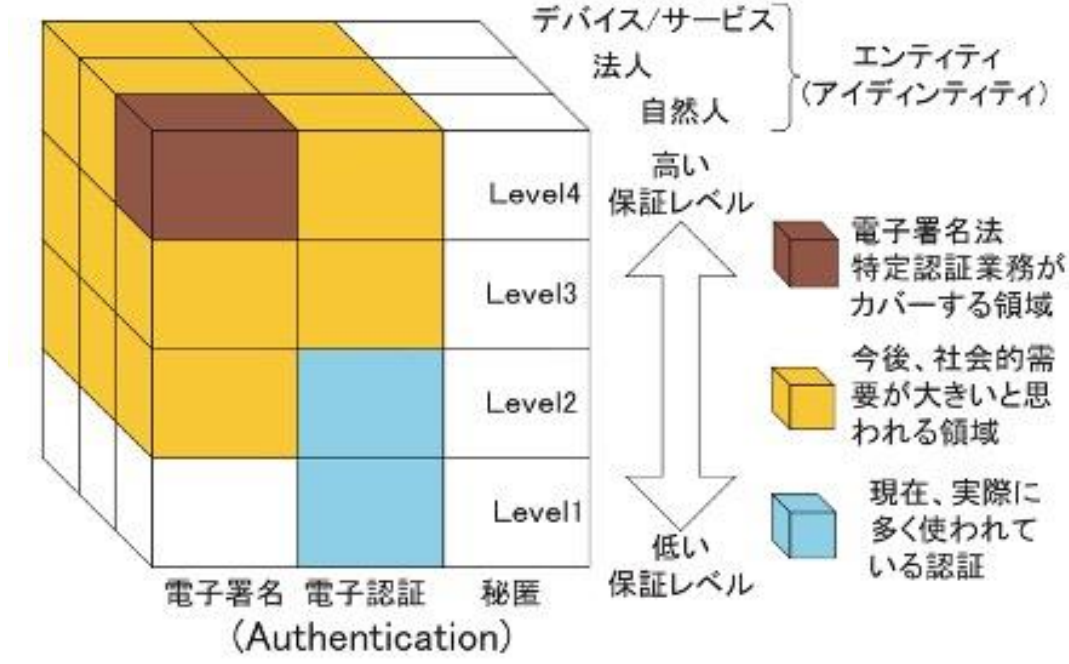
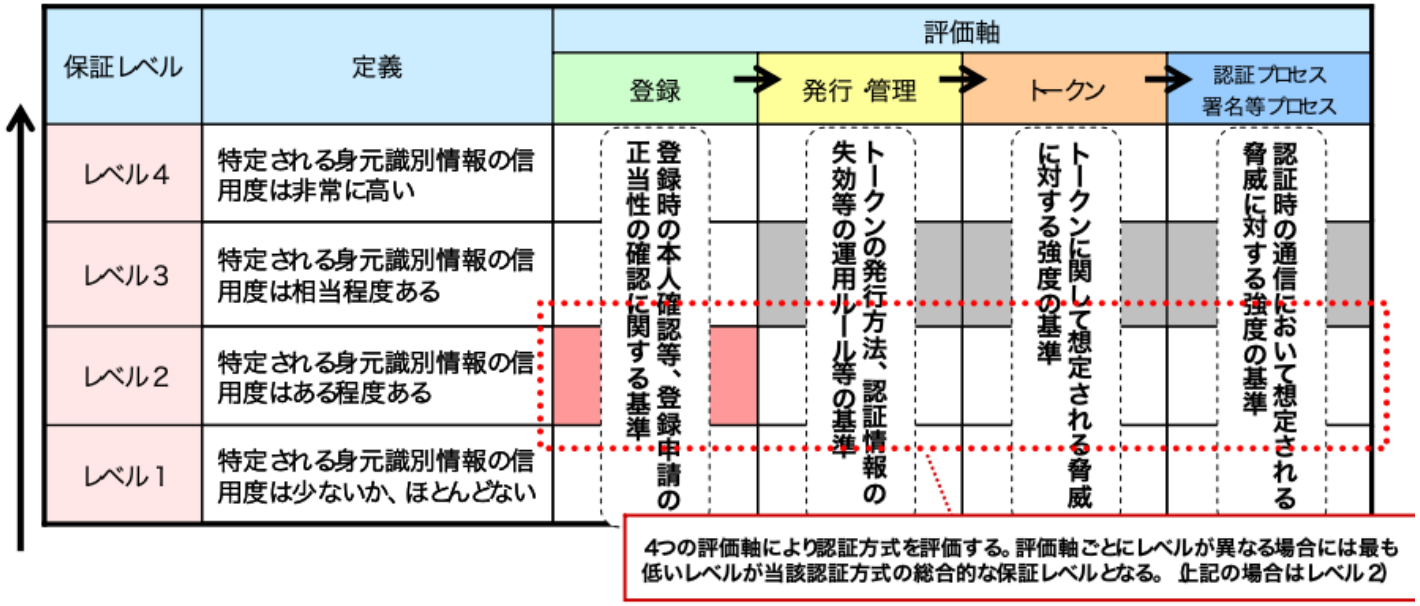


図3　トラストキューブ

2008年-2010年　電子政府ガイドライン作成検討会 セキュリティ分科会
オンライン手続における リスク評価及び電子署名・認証ガイドライン (2010年)
https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf
電子政府ガイドライン作成検討会 セキュリティ分科会報告書(2010年)
https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

電子政府ガイドライン作成検討会
セキュリティ分科会報告書

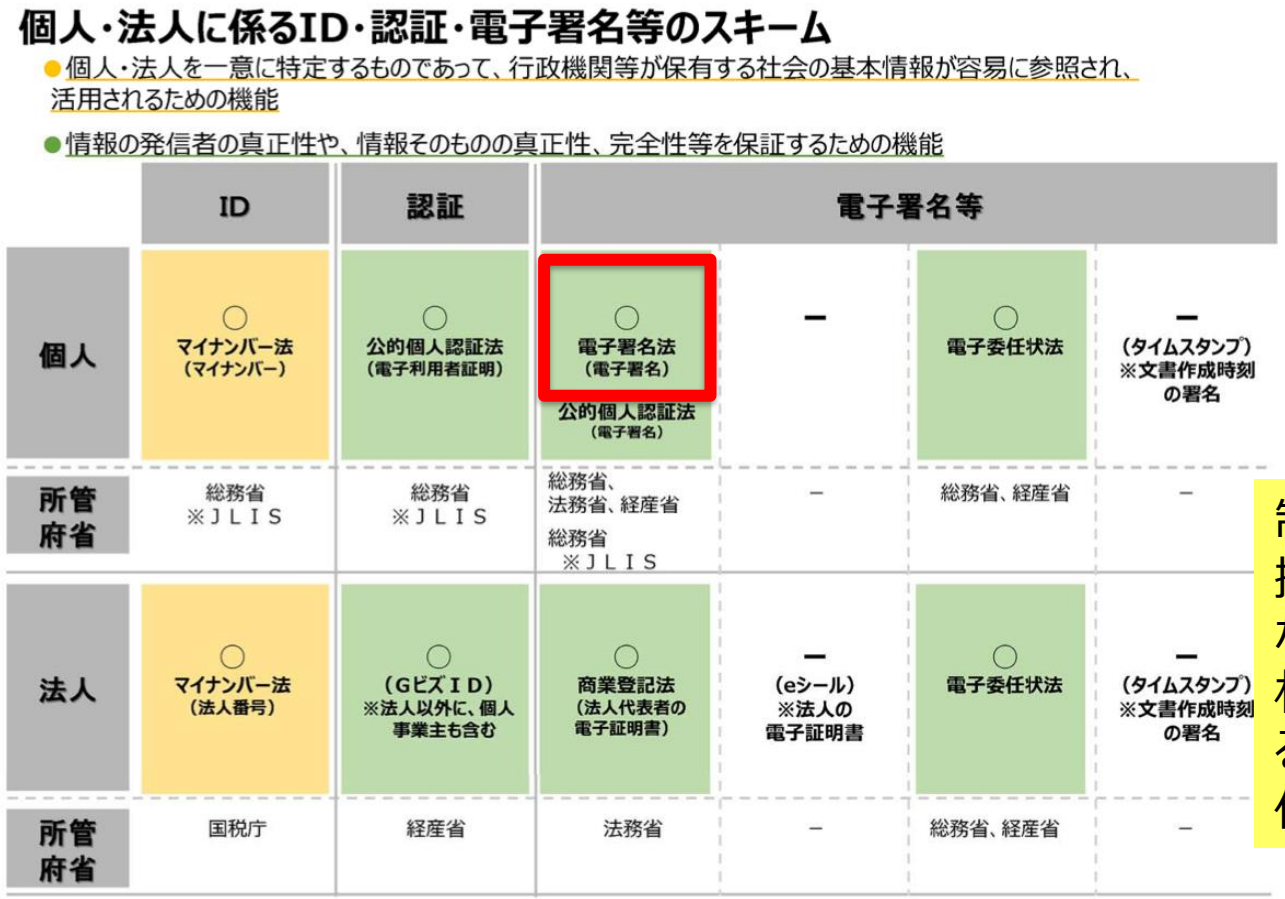


平成 22 年 2 月
電子政府ガイドライン作成検討会 セキュリティ分科会

図 54 電子署名 認証の保証レベルの考え方

署名（signature）と認証（authentication)の統合を目指したガイドライン

8．個人・法人に係るＩＤ・認証・電子署名等のスキーム



個人・法人に係るID・認証・電子署名等のスキーム

- 個人・法人を一意に特定するものであって、行政機関等が保有する社会の基本情報が容易に参照され、活用されるための機能
- 情報の発信者の真正性や、情報そのものの真正性、完全性等を保証するための機能

	ID	認証	電子署名等			
個人	○ マイナンバー法 （マイナンバー）	○ 公的個人認証法 （電子利用者証明）	○ 電子署名法 （電子署名） 公的個人認証法 （電子署名）	－ （eシール） ※法人の電子証明書	○ 電子委任状法	－ （タイムスタンプ） ※文書作成時刻の署名
所管府省	総務省 ※ＪＬＩＳ	総務省 ※ＪＬＩＳ	総務省、法務省、経産省 総務省 ※ＪＬＩＳ	－	総務省、経産省	－
法人	○ マイナンバー法 （法人番号）	○ （GビズＩＤ） ※法人以外に、個人事業主も含む	○ 商業登記法 （法人代表者の電子証明書）	－ （eシール） ※法人の電子証明書	○ 電子委任状法	－ （タイムスタンプ） ※文書作成時刻の署名
所管府省	国税庁	経産省	法務省	－	総務省、経産省	－

48

出典：
デジタル改革関連法案ワーキンググループ作業部会 とりまとめ
令和2年11月20日 デジタル改革関連法案ワーキンググループ作業部会
https://www.kantei.go.jp/jp/singi/it2/dgov/houan_wg/dai4/siryou2.pdf

制度的なパーツは、それなりに揃っているように見えるかもしれないが、技術の観点からは、相互運用性が決定的に欠ける。その原因は、ボトムアップに作られてきた制度にある。

2012年　PKI Day 2012我が国における信頼基盤の連携に向けて

https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

2012年頃における
個人情報保護法制の
ラググメンテーション（細分化）問題??

ラググメンテーション（細分化）問題のひとつが「個人情報保護法制2000個問題」

電子署名、及、関連する制度もも同様ではないかという疑問

様々な連携が要求される時代の本人確認(Identity proofing)の課題

信頼される安心を、社会へ。 SECOM

引き落とし口座の紐付けを行なっているのは金融機関

資金移動サービス事業者本人確認義務は？？？
金融機関が行っている本人確認が、金融機関の本人確認を満足しており、その口座との紐付けにより本人確認を行ったと見做した？？（らしい）

金融機関

引き落とし口座の紐付け

d口座

資金移動サービス事業者

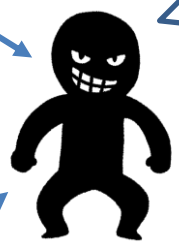
・資金移動サービス事業者の口座を作成
・金融機関のWeb口座振替受付サービスを利用して、口座を紐付け

金融機関の本人確認法

d回線ユーザ

キャリアの本人確認法

キャリアフリー
（＝d回線以外の方）



出し子のアルバイト？？

メールアカウント取得

メールサービス事業者

口座情報購入？？？

ダークウェブ

論点？？対立軸？？

- 技術的中立性　vs. 標準化＆相互運用性
- 米国の電子署名法　vs. 欧州のeIDAS
  - GDPRに関する議論と類似
  - フラグメンテーション問題
- 自己責任　vs. トラストサービス・トラストフレームワーク
- 利便性　vs. セキュリティ
  - リスクに応じた電子署名＆電子認証のLoA(Level of Assurance)と本人確認(Identity proofing)

vs. ではなく、バランスの良い社会実装への努力が重要

付録

- 過去からの議論
- 電子署名法の立て付けと課題

過去からの議論

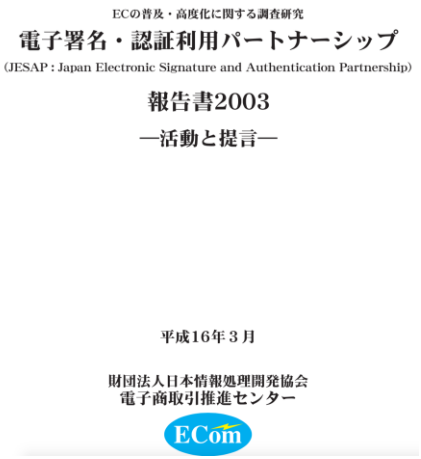
20年前（2020年12月7日）のセミナー -- 第2回 セキュリティ・フォーラム レポート
https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

信頼される安心を、社会へ。 SECOM

- 日本インターネット協会(IAJ)セキュリティ部会主催の第2回セキュリティフォーラムが、2000年12月7日午後1時30分よりIAJの会議室で開催されました。
- （中略）
- 今回は「PKIの相互運用とOpen PKIの流れ」と題して、セコム株式会社の松本泰さんにお話いただきました。PKIはeビジネスの広がりや電子政府への取り組みの中で、ネットワーク上での本人確認と、取引や情報の真実性等の確認と保証のための基本的枠組みを提供するもので、様々なソリューションが提供されだしていると共に、共通性・互換性を持った社会基盤としての有効性・利便性等の実現に向けて様々な試みや開発が進められている分野です。
- 松本さんのお話はまず「ボブはいかにしてアリスを信用するか」という設問の下に、夫々の信頼ポイントである自己のCA(電子認証局)同士の間での相互認証の仕組みという基本構造の解説からスタートし、X.509を中心とする技術基準の動向と証明書のクラス(信頼性レベル)の問題、信頼ドメインの概念とその相互認証・相互接続の仕組みや例、証明書失効リストの関係へと進みました。そして相互認証証明書と証明書パスの構築による信頼の連鎖の仕組みが解説され、さらに、複数PKI間の相互接続・相互運用のモデルと様々な技術課題の紹介にまで展開されて終りました。
- 普段なにげなく考えている電子署名やCAの問題がいかに複雑で奥が深く、世界規模でのシームレスな運用のためにはまだまだ解決すべき問題が、単に技術だけでなく経済主体や社会基盤、法整備や国際間のルールの確立も含めて多くあることが理解できました。

2003年　電子署名・認証利用パートナーシップ報告書2003　活動と提言

https://www.jipdec.or.jp/archives/publications/J0004195



3. 電子署名推進方法に対する提言

3.1 電子署名と実印/認印と対応付けて説明することの課題

（中略）

(1)　印鑑証明書と公開鍵証明書は同等な仕組みか(実印制度と PKI)？

(2)　実印と三文判

(3)　三文判 PKI について

インターネットを飛び交う文書の真正性を確保するためには「改ざんの検出」と「本人性確認」 の仕組みを欠かすことができない。リアルの世界で三文判がいかに多く使われていても、サイバーの世界ではこれと同等なものとして改ざん検出、本人性確認ができない電子署名は大きなリス クを伴う。三文判 PKI というとき考えなければならないのは基本的な PKI の仕組みを維持しなが らリスクや脅威に何処まで対応できるかのセキュリティ基準(ポリシー)を明確にすることであ る。

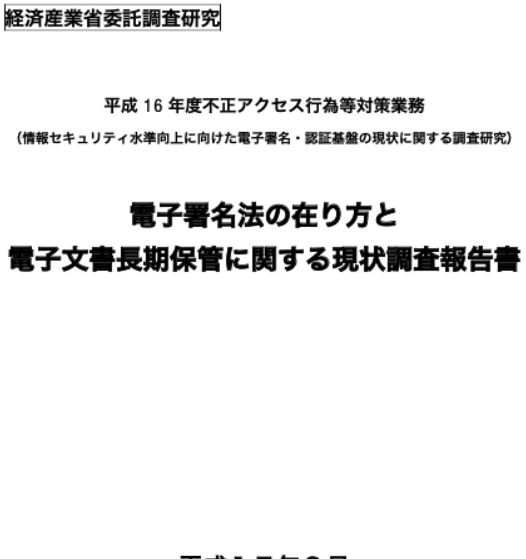
（中略）

三文判PKIというとき、このカナダ政府や米国政府が採用している初級または基本レベルのPKI を対応付けるべきと思われる。このレベルのポリシーでは認証局の厳格な運用は求めていなく、 鍵管理も HSM(ハードウェアセキュリティモジュール)は必要としない。また本人確認も厳格な 審査をしなくてよい。問題が起こってもそのリスクはそれほど大きなものにならない用途を想定 している。従って運用コストもかなり安いものとなる。

日本ではポリシーのレベル分けについてあまり議論されてこなかった。政府の GPKI でもポリシ ーは 1 つで(米政府の中級に相当)下位のレベルや複数の証明書の使い分けについて検討されていない。三文判 PKI の提起を契機として PKI の証明書ポリシーの議論が深まることが期待される。

「3.1 電子署名と実印/認印と対応付けて説明することの課題」の執筆は、2005年7月に亡くなられた鈴木優一氏

2005年　電子署名方の在り方と電子文書長期保管に関する現状調査報告書



経済産業省委託調査研究

平成 16 年度不正アクセス行為等対策業務

（情報セキュリティ水準向上に向けた電子署名・認証基盤の現状に関する調査研究）

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

平成１７年３月

(財)日本情報処理開発協会

出典：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
**この報告書は、以前、公開されていましたが2020年現在、公開されていません。

- 2.2. 特定認証業務の規定の明確化
- 2.2.1.特定認証業務の基準
- 現在、電子署名法による認証業務の認定を受けるには告示(指針)で規定された厳格な基 準を満たさなければならず、また指定調査機関の示す適合例の合致が求められ、これらをクリアするハードルはかなり高く、設備、本人確認方法、運用基準を満たすために多大なコス トがかかるようになっている。したがって、この認定認証業務で発行する証明書の価格が高 く利用普及の阻害にもなっていると言われる。多くの認証事業者は、義務として認定認証業 務の発行する証明書を使わなければならない政府への電子申請や電子入札のために認定を受 けているが、民間利用のために認定認証業務の証明書発行を行っているところは少なく、む しろ認定を受けない「特定認証業務」として安価な証明書発行サービスを行っているところ が多い。ハイリスクなビジネスでは厳格な基準を満たした認定認証業務の証明書を使うべき だが、それほどリスクの高くない分野での利用のために、安価でより安全な証明書を望む声 は大きい。（中略）
- ドイツの電子署名法では認定を受けない認証事業者についても認証業務の守るべき基準を示し、この基準に沿った認証事業を届出制で認知させている。さらにこれらの認証業務に一 定の条件を加味することで任意の認定も受けられるとしている。

「2.2　特定認証業務の規定の明確化」の執筆は、2005年7月に亡くなられた鈴木優一氏

2006年　社会基盤としての電子認証と電子署名

https://www.jstage.jst.go.jp/article/nig/43/5/43_5_324/_pdf

総説　　特集「認証技術とその応用」

社会基盤としての電子認証と電子署名

Electronic Signature and Authentication for Social Infrastructures

Yasushi MATSUMOTO*　　松本　泰*
*SECOM Co.,Ltd.
8-10-16, Shimorenjyaku, Mitaka-shi, Tokyo, 181-8528 JAPAN

1. 基盤としての電子署名と電子認証

IT 技術が社会に深く浸透していく中，これからの社会の共通基盤として，ネットワーク基盤と認証基盤（電子署名と電子認証の基盤）の必要性が言われ続けている．たとえば2006年夏に発表された e-JAPAN 重点計画 2006 でも，ネットワークと認証に関わる多くの記述があるが，重点分野の最初に取り上げられている医療福祉分野においても，以下のような記述がある[1]．

> これらの課題のもと，医療・健康・介護・福祉分野の情報化に関する横断的なグランドデザインを速やかに策定した上で，まず医療の情報化の共通基盤である安全かつ安価な大容量ネットワークの構築や，医療機関・従事者・患者等の認証の仕組みの確立等に着実に取り組む．

ここでは，医療情報等を高度に利活用するため，共通基盤としてのネットワークと認証の必要性を説いている．こうしたことは医療福祉分野に限らず必要とされているが，安全なネットワークとそのネットワークを利用するための認証基盤の構築ということに関しては，まだ大きな課題がある．

様々な分野で必要とされている認証基盤であるが，現時点で一般的に認証基盤と認識されている公的個人認証サービスの普及と利用は低迷しており，電子署名も普及しているとは言いがたい状況にある．認証基盤の必要性の理解や，実際の認証基盤の構築を行なう上において，電子署名，電子証（e-Authentication），認証（Certification）といった言葉の意味を正確に理解する必要がある．電子署名は，作成した文書等の責任を明確にするために必要になり，電子認証は，こうした文書等を適切な権限を持った人が参照等を行なうために必要になる．

電子署名と電子認証を理解する上で認証（Authentication）と認証（Certification），2つの「認証」という用語は，多くの混乱の元になっている．多くの法律用語において「認証」は，英語の Certification を意味する．それに対して，サーバ等によるユーザの真正性の確認を意味することも認証（Authentication）と呼ばれる．Certification は，何らかの権威者が発行する証明書により何らかのことを証明する．公としての行政機関は従来からこの Certification を数多く行っており，その証としての証明書の発行を行なってきた．そのため法制度等において「認証」は Certification を意味することが多い．そのため Certification の電子化自体も多くの場合，電子署名の技術を用いて実現される．

松本　泰
1984年 UNIX 上のビデオテックスの開発に従事．
1990年 UNIX 上の大規模パソコン通信システムの開発に従事．
1994年各種インターネットサービスの開発に従事．
1998年サイバーセキュリティ事業の立ち上げに従事．
2006年9月現在，NPO 日本ネットワークセキュリティ協会 PKI 相互運用技術 WG リーダ，電子署名・認証利用パートナーシップ（JESAP）利用促進部会長，工学院大学「セキュアシステム設計技術者の育成」プログラム客員教授．IPA 情報システム等の脆弱性情報の取扱いに関する研究会 委員．CRYPTREC 暗号技術検討会メンバー．ECOM セキュリティ WG/ 電子署名認証 SWG サブリーダ．

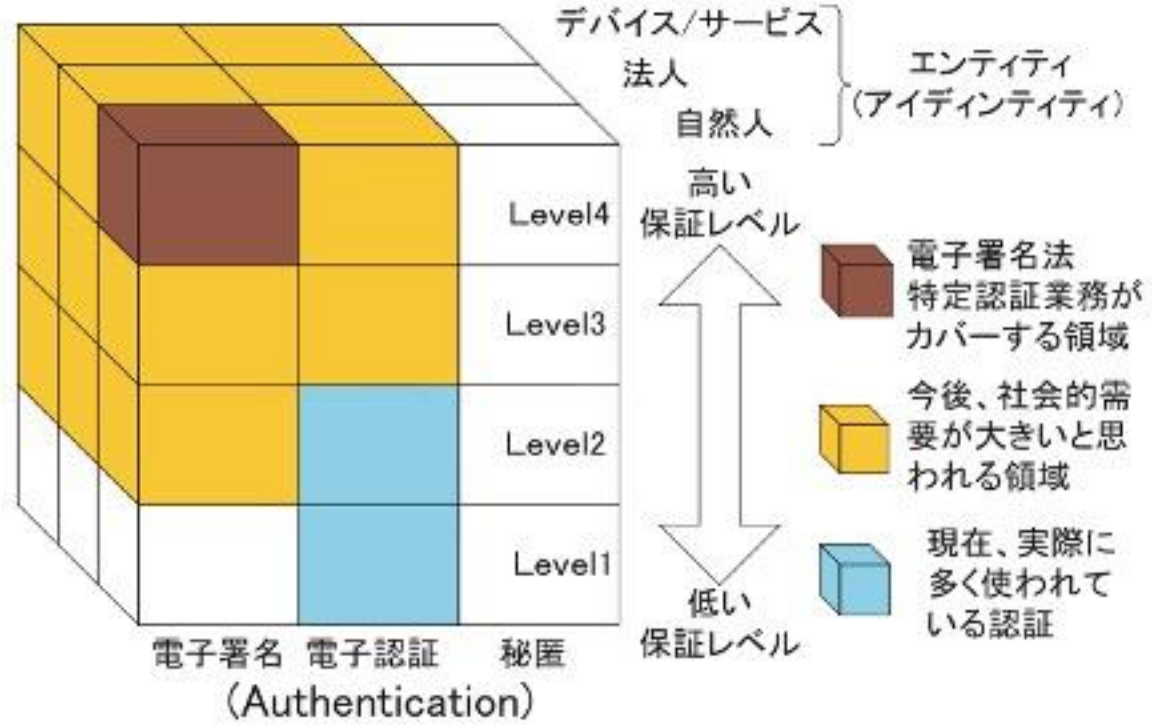


図3　トラストキューブ

* セコム（株）IS 研究所
〒181-8528　東京都三鷹市下連雀 8-10-16　セコム SC センター内）

2006年　社会基盤としての電子認証と電子署名

https://www.jstage.jst.go.jp/article/nig/43/5/43_5_324/_pdf

- 6.まとめ
- ビジネスはネットワーク社会への移行という環境変化に より、今では顔を突き合せなくてもリアルタイムの取引ができるような状況になりつつある。これまで契約者同士の 取引の時間的地理的な距離のために紙ベースの処理(署名) が必要だった業務であっても、オンラインの電子認証によ りその大部分が解決される.またビジネススキームからして抜本的に変わってしまえば署名ではなく電子認証で済む 場合もある。のようなネットワーク社会では、サービス 自体が信頼のおけるものであれば、認証およびその後の手 続きのログなどを証跡とするといったことが一般的だと考 えられる。
- 2001 年施行の電子署名法をはじめとする現行 の IT 技術の関連した法制度は、こうした環境の変化に追随できていない側面がある。こうしたなか、認証における 基準等は未整備であり、たとえばこれらにも起因するインターネットバンキング等における犯罪は「サービス自体が 信頼のおけるもの」といったことに対して疑問を抱かせ、インターネット上のサービスに対する信頼を揺るがしている。
- 電子署名が役に立たないかというと、まったくそういっ たことはない。「認証とログ」は特定のシステムに依存す るため、長期間のセキュリティ(たとえば重要文書の長期 保存など)や、組織を超えた広域のセキュリティに対応す るといったことが難しい。また、コストがかかるといった 問題もある。
- 標準化されたデータフォーマットを使い電子 署名が施されたデータは、特定のシステムに依存しない独立したデータとしての普遍性を持つが、これは社会基盤として非常に重要な意味を持つ
- IT 化、ネットワーク化は、利便性のみならず、新たな不正行為をも招いているが、電 子署名はこうしたことに対抗する技術である。しかし、電 子署名の普及には、競争原理だけではなく、適度な強制力 も必要ということが認識されるべきである。
- 電子署名と認証の違いを中心に説明してきたが、安心・ 安全なネットワーク社会を構築するためには、これらの技術を適切に使い分けるための技術・法制度・ビジネスの三 位一体となった検討がなされるべきである。電子署名の普及が思うように進まないのは、技術・法制度・ビジネスモ デルのバランスの悪さに起因しているように思われる。
- 今後、安心・安全なネットワーク社会を目指していく上では、電子署名・認証の更なる技術開発、法制度の整備、新たな ビジネスモデル創造などの更なる努力が求められる。

2008年-2010年　電子政府ガイドライン作成検討会 セキュリティ分科会
オンライン手続における リスク評価及び電子署名・認証ガイドライン (2010年)
https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf
電子政府ガイドライン作成検討会 セキュリティ分科会報告書(2010年)
https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

電子政府ガイドライン作成検討会
セキュリティ分科会報告書

平成 22 年 2 月

電子政府ガイドライン作成検討会　セキュリティ分科会

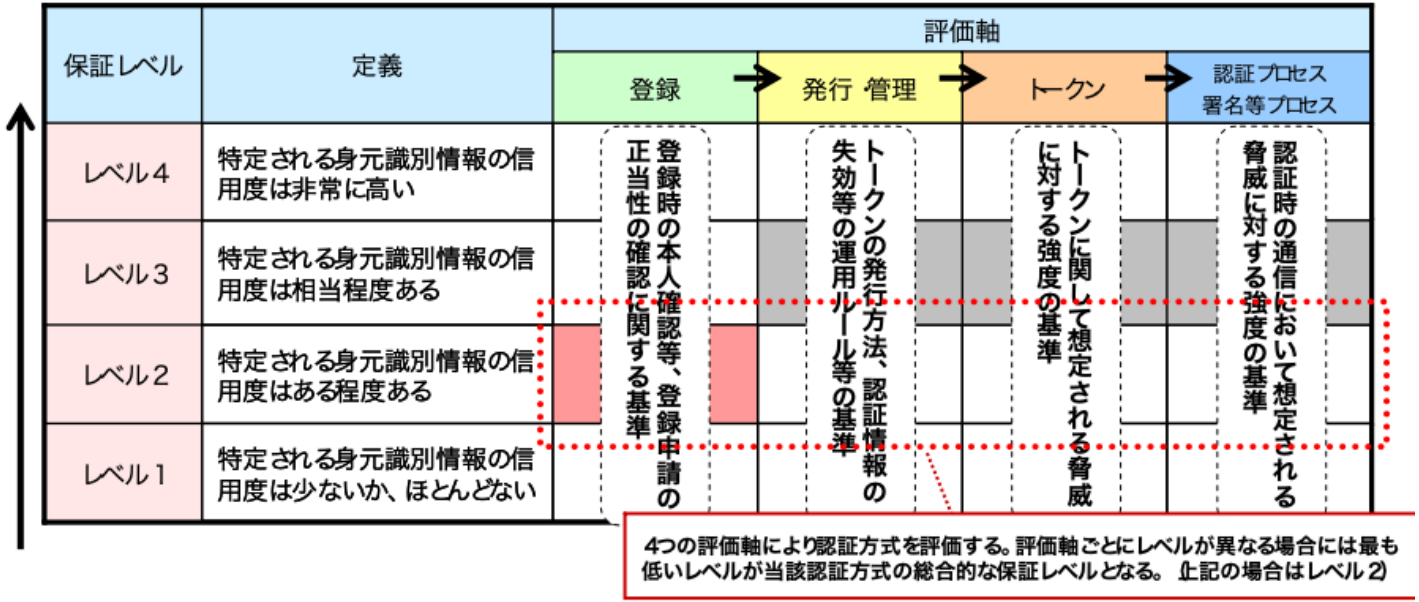


図 54 電子署名 認証の保証レベルの考え方

オンライン手続における リスク評価及び電子署名・認証ガイドライン（2010年）

https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

表 A.4-3 署名等プロセスの保証レベル

対策基準(※1)	保証レベル(※2)			
	1	2	3	4
電子政府推奨暗号リストに記載された公開鍵暗号による署名方式を用いること。			◎	◎
「表 A.3-9 トークンの保証レベル」の保証レベル3と同等の対策基準を満たすトークンを用いて署名等プロセスを実行すること。			◎	
電子署名用の証明書の用途を電子署名のみに限定すること。				◎
「表 A.3-9 トークンの保証レベル」の保証レベル4と同等の対策基準を満たすトークンを用いて署名等プロセスを実行すること。				◎

※1 上記は、電子署名を用いる場合の対策基準である。本ガイドラインでは、認証及び証跡管理技術を用いる場合の対策基準について特に規定せず、別途検討すべき課題として位置づけるとともに、関連事項について A.5.5 節にて述べる。

※2 「◎」は各保証レベルへの準拠にあたり必須の対策基準であることを示す。

オンライン手続における リスク評価及び電子署名・認証ガイドライン（2010年）

https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

- A.4. 署名等に係る対策基準
- A.4.1. 署名等フレームワーク
- A.2 章にて述べた通り、電子署名は、「改ざん」「事実否認」の脅威に対する有力な対策技 術である。
- 一方、A.3 章にて述べた認証は「なりすまし」に対する対策技術であると同時に、必要十 分な信頼性を備えた証跡管理技術を組み合わせることによって、改ざん、及び事実否認の 脅威に対しても一定の対策効果を得ることが可能である。例えば、電子政府のオンライン 手続において、申請者の認証を行なった上で、認証結果、及び当該申請者の申請内容と申 請事実を証跡として記録・保管することを考える。この証跡に対して、セキュリティ技術（タイムスタンプ等）、あるいはセキュリティ基準に基づく厳格な運用によって、サービス 提供にあたり必要十分な信頼性を確保することを想定すれば、認証を用いる場合でも、申請内容の改ざん、申請事実の否認といった脅威を軽減することが可能となる。
- なお、技術的視点から見れば、電子署名による「改ざん」「事実否認」の対策効果と、認証と証跡の組み合わせによる対策効果は必ずしも等価ではない。したがって、これらの技 術をサービスに適用するにあたっては、当該サービスにおいて想定される各脅威の対処方 針(どの脅威に対処し、どの脅威は許容するか)を慎重に検討する必要がある。
- 以降、本ガイドラインでは、以上のような申請内容の完全性、及び申請事実の非否認性を確保するための措置を「署名等」と総称する。
- 表 A.4-1 に示すように、署名等フレームワークと表 A.3-1 に示した認証フレームワーク の差異となる要素は「署名等プロセス」であると捉えると分かりやすい。そこで、「登録」 「発行・管理」「トークン」の対策基準については、A.3 章の「認証」の対策基準に準ずる こととし、ここでは「署名等プロセス」の対策基準に関して述べる。

オンライン手続における リスク評価及び電子署名・認証ガイドライン（2010年）

https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

- A.5.5. 証跡管理
- 証跡(ログ)管理は、本ガイドラインで定めた電子認証及び電子署名においてプロセス がどのように行われたかについての証拠を残すための手段として利用される。特に認証に おいては、署名以上に、証跡を電子文書として正しく取得管理することによって、完全性 及び非否認性を証明することにつながる。
- このような電子文書の管理を行うための目安が、総務省行政管理局 共通課題研究会によ ってまとめられた「インターネットによる行政手続の実現のために 第5章 電子文書の原本性」(平成 12 年3月)において下記のように整理されている。(以下抜粋)
- 電子文書の保存・管理上の問題点をふまえ、電子文書の原本性を確保するために充足 すべき要件としては、次の3つに整理することができる。
  ア 完全性の確保
  - 電子文書が作成された際、電子文書に対する改変履歴を記録すること等により、 電子文書の改ざん等を未然に防止し、かつ、改ざん等の一時角有無が検証できる ような形態で、保存・管理されること。
- イ 機密性の確保
  - 電子文書へのアクセスを制限すること、アクセス履歴を記録すること等により、 アクセスを許されない者からの電子文書へのアクセスを防止し、電子文書の盗難、 漏洩、盗み見等を未然に防止する形態で、保存・管理されること。
- ウ 見読性の確保
  - 電子文書の内容が必要に応じ電子計算機その他の機器を用いて直ちに表示でき るよう措置されること。
- また、この中では、要件担保のための措置の内容が示されており、アクセス管理のあり 方や保管場所の決定その他の電子文書の管理に関するルールを整備することが必要である と述べられている。一方、このような証跡や署名を施した文書は、長期間の利用/保存が 見込まれる場合がある。この場合、アルゴリズムの危殆化などの別の脅威が生じる可能性 を持つ。そこで、長期保存した文書の完全性及び非否認性を示すためには、タイムスタン プ署名を定期的に施すなどの処置をすべきである。

電子政府ガイドライン作成検討会 セキュリティ分科会報告書(2010年)
https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

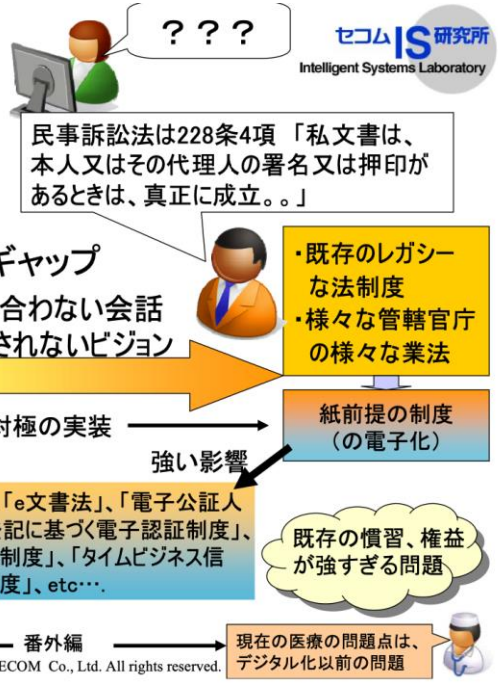
- 6.2. 制度的な課題
- (1) 本人確認に関する横断的な制度設計
  - 2003 年(平成 15 年)、CIO 連絡会議において決定された「電子政府構築計画」のなかで IT 化に対応した業務改革が提唱され、業務・システムの最適化への取組が始まったものの、 依然として我が国の制度は、情報通信技術の利活用を前提としたものとはなっておらず、本 格的な EA(Enterprise Architecture)は取り組まれていないのが現状である。
  - このため、2009 年(平成 21 年)8 月から IT 戦略本部の下に「デジタル利活用のための重 点点検専門調査会」が設置され、デジタル技術・情報の利活用を阻むような規制・制度・慣 行、サービスの仕組みそのものの在り方や運用などを国民にとって利益となる形で抜本的に 見直すための点検が行われているところである。
  - 本人確認については、今回、ガイドラインによりオンライン手続におけるリスク評価手法 及び対策基準を規定したところであるが、制度的には個別手続毎にそれぞれの機関がリスク と利便性を斟酌して判断している状況にあり、国民 ID や個人情報の取り扱いと合わせて、横 断的な制度設計に着手することが望まれる。(例えばエストニアにおいては、個人情報保護法 により、機密性に応じて個人情報を3段階に分類している。)
- (2) 代理人の扱い
  - 紙申請の場合において、代理人が申請する場合の本人確認手法については、委任状により行っているが、オンライン手続における委任の確認手法について検討されることが必要であ る。家族による代理申請など、代理申請は頻繁に行われていることから、オンラインにおい ても紙と同等な簡便さで代理申請ができるよう、委任されたことの確認が可能となるような システム設計をするべきである。
- (3) 認証の法的位置づけ
  - 電子署名については、電子署名法によりその法的効力が規定されているものの、認証については、各主体のリスク判断により運用されているところである。今後、より信頼できるネ ットワーク社会の構築に向けた環境整備の一環として、「誰が」の保証について、どのような 制度的裏付けが適切であるのか、関係者間による検討が望まれる。
- (4) CC 認証の取得促進に向けた環境整備
  - IC カードのセキュリティ評価については、世界的に ISO/IEC15408(コモンクライテリア)に基づくセキュリティ評価・認証を取得することが、一般的である。このため、現在国内に IC カード等のシステム LSI のセキュリティ評価・認証体制の整備に向けた取組が行われているところである。今後、このような取組がより一層促進されることが望まれる。
- (5) 術語
  - 我が国の既存法令等においては「認証」が Certification(証明、検定)の意味で使われており、Authentication(認証)に充てる適切な術語がなく、認証方式に関する議論を難しくし ている。このため、さらなる制度検討にあたっては、認証に関する分かりやすい術語につい て、検討することが望まれる。

2010年　PKI Day 2010 <社会基盤としてのPKI/PKIの10年>

https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

標準化と法制度の関係

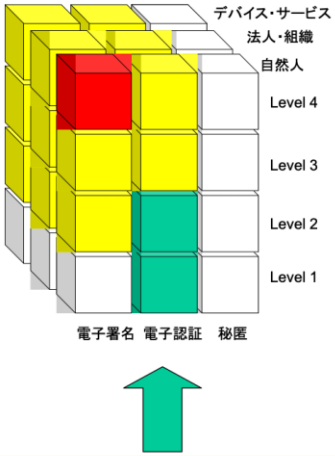
セコムIS研究所 Intelligent Systems Laboratory



情報セキュリティに関連する制度の課題
電子署名法の功罪

セコムIS研究所 Intelligent Systems Laboratory

- 「電子署名法」の認定制度は、「推定効」の呪縛（および、無謬性を求める電子政府のサービス）等からリスクを許容しない非常に厳しい基準を課している。そのため、電子署名法の認定基準自体は、世の中で署名が使われるべき全ての領域に対してベストプラクティスを提供している訳ではない。
- 現状の電子署名法のカバーしている領域は、非常に狭く、各種の厳しい基準が、電子署名は使いにくい、高価、運用が難しいというイメージを与えている面がある。
  - 非常にニッチなビジネス領域の社会的なインパクトがない分野にしてしまっている。。。。
- セキュリティの視点だけ追及してきたこと自体が、逆に「TRUSTの確立」を妨げている可能性がある。



無謬性的な要求がなされた電子署名法の世界と混沌としたビジネスのレモン市場の世界の同居？？

2010年　PKI Day 2010 <社会基盤としてのPKI/PKIの10年>

https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

電子署名法の”Teething problem”？？
この認識がないと将来は”long-term problem”に苦しむ？

セコムIS研究所 Intelligent Systems Laboratory

Continental European Approach	Anglo-Saxon Approach
Prevention through comprehensive pre-implementation checks for - products, - technical, administrative and organisational aspects of certification activities, and - reliability and specialised knowledge of staff.	Ensuring adequate minimum level of - competition in the market, and - liability.
- Development costs (evaluation of products and security concepts) - More time-intensive in initial stages "Teething problem"	Liability depends on - ability and willingness to assume liability in cases of damage, and - recognised cases of damage. Long-term problem

http://www.efpe.eu/upload_module/downloads/efpe/2006/prezentacje/2/06_JSchwemmer_BNetzA.pdf

28

米国の電子署名法

セコムIS研究所 Intelligent Systems Laboratory

James Bond	[*Digitized image of handwritten signature*]
/s/ James Bond	[*Typed name*]
007	[*Number or PIN*]
X	[*"X" or other random letter*]
☺	[*Smiley face or other picture*]
I Agree to these terms	[*Words typed in box*]
I AGREE	[*Button clicked with mouse*]

-----BEGIN SIGNATURE-----
iQCVAwUBMARo7vgyLN8bw6ZVAQF6ygP/fDnuvdAhGIDWsSMXUIR
MuNHYzdZ00cqkDb/Tc2+DuhuEa6GU03AgZY8K9t5r9iua34E68pCxo
gUz009b1OcjNt6+o+704Z3j1YY9ijYM8BWNaSp9L2W4nUuWBdlyIWy
ol/2PjjRVNZEtqtSRQnPEpJ2IHtz9iGovHf0Sqh
-----END SIGNATURE-----

[*Digital signature*]

http://www.fips201.com/resources/audio/iab_0210/iab_022410_smedinghoff.pdf

29

2012年　PKI Day 2012我が国における信頼基盤の連携に向けて

https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

「信頼基盤」と「個人情報保護法」の共通点？？

セコムIS研究所 Intelligent Systems Laboratory

- 現在の法律の成立時期
  - （目標を間違えていた？？）世界最先端電子政府が検討されていた2000年前後に検討された頃に、法律（個人情報保護法、電子署名法）が成立
- 現在の制度は、欧州の制度と米国の制度の折衷案？
  - 欧州 vs. 米国
  - 日本における制度の立ち位置は？
- 現時点での状況　－連携のためのポリシ不整合？？
  - 制度間、管轄官庁間の不整合？？
  - 制度と技術の成り立たない会話？？
  - 日本と世界の不整合？？
    - 個人情報保護法であれば、データの越境問題

12

デジタル時代のビジョンの共有は可能か？

セコムIS研究所 Intelligent Systems Laboratory

20

2012年　PKI Day 2012我が国における信頼基盤の連携に向けて

https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

2012年頃における
個人情報保護法制の
ラググメンテーション（細分化）問題??

ラググメンテーション（細分化）問題のひとつが「個人情報保護法制2000個問題」

電子署名、及、関連する制度もも同様ではないかという疑問

2019年　トラストサービスの調査ワークショップ

https://itresearchart.securesite.jp/19ws207/docs/s03.pdf

トラストサービスの調査ワークショップ2019

EUの技術標準

-- デジタル単一市場戦略の中核となるトラスト --

2019年　2月　7日

松本　泰　　セコム（株）ＩＳ研究所

© 2019 SECOM CO. LTD.

1

ＥＵの技術標準とデジタルプラットフォームの関係

© 2019 SECOM CO.,LTD.

4

2019年　トラストサービスの調査ワークショップ

https://itresearchart.securesite.jp/19ws207/docs/s03.pdf

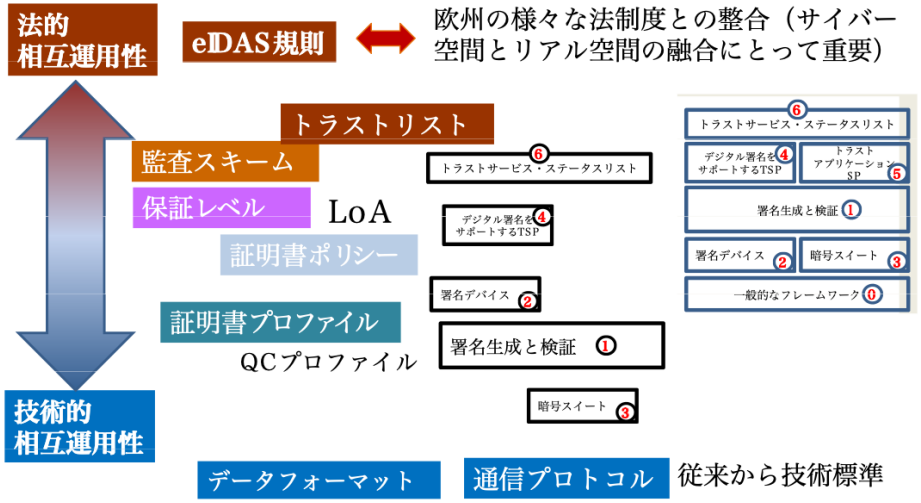
eIDAS前文 -- 技術標準の意味するところ

- 「欧州デジタルアジエンダ」と題した2010年8月26日の欧州委員会コミュニケーションでは、デジタル市場の細分化、相互運用性の欠如、そしてサイバー犯罪の増加を、デジタル経済の良好な循環にとって大きな障害となるものとして認定した。
- 委員会はさらに、２０１０年の「Dismantling the obstacles to EU citizens' rights (EU市民に対する障害の排除)」と題したEU市民活動レポートにおいて、連合市民がデジタル単一市場や国境を越えたデジタルサービスの恩恵を受けることの妨げとなっている問題を解決することの必要性について強調した。
- The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy.
- In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying

- 欧州においてデジタル単一市場のためのデジタルプラットフォーム構築の障害となるのは、デジタル市場の細分化、相互運用性の欠如
- この障害を取り除くためには「トラスト」に関わる相互運用性を確保した技術標準が必要であり、更に、デジタル市場を細分化（fragmentation）させないための規則（eIDAS規則）が必要だった。
- eIDAS規則は、従来の紙台帳時代の法制度の単なるリプレースの話ではなく、デジタルプラットフォーム構築のための法制度。

© 2019 SECOM CO.,LTD. 5

技術的相互運用性に対して法的相互運用性の重要性
Technical interoperability & Legal interoperability



ICTが社会基盤化するほどに、技術的相互運用性と法的相互運用性の整合が重要になっている　-> EU技術標準を理解する上で非常に重要

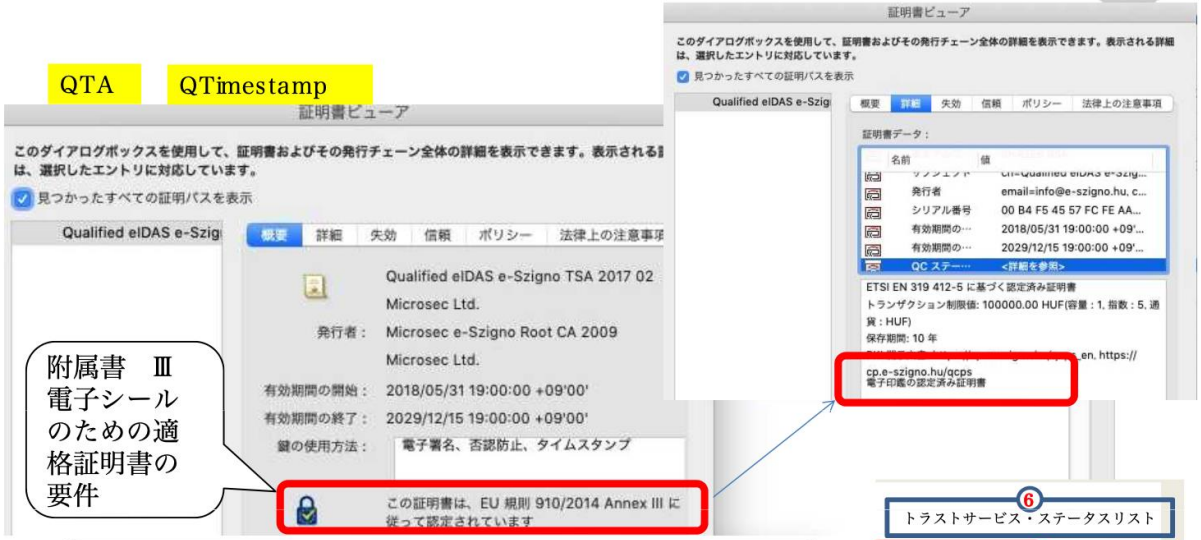
© 2019 SECOM CO.,LTD. 10

https://itresearchart.securesite.jp/19ws207/docs/s03.pdf

信頼される安心を、社会へ。
SECOM

Acrobat Readerによる適格タイムスタンプの検証

セコムIS研究所 Intelligent Systems Laboratory



附属書　Ⅲ
電子シールのための適格証明書の要件

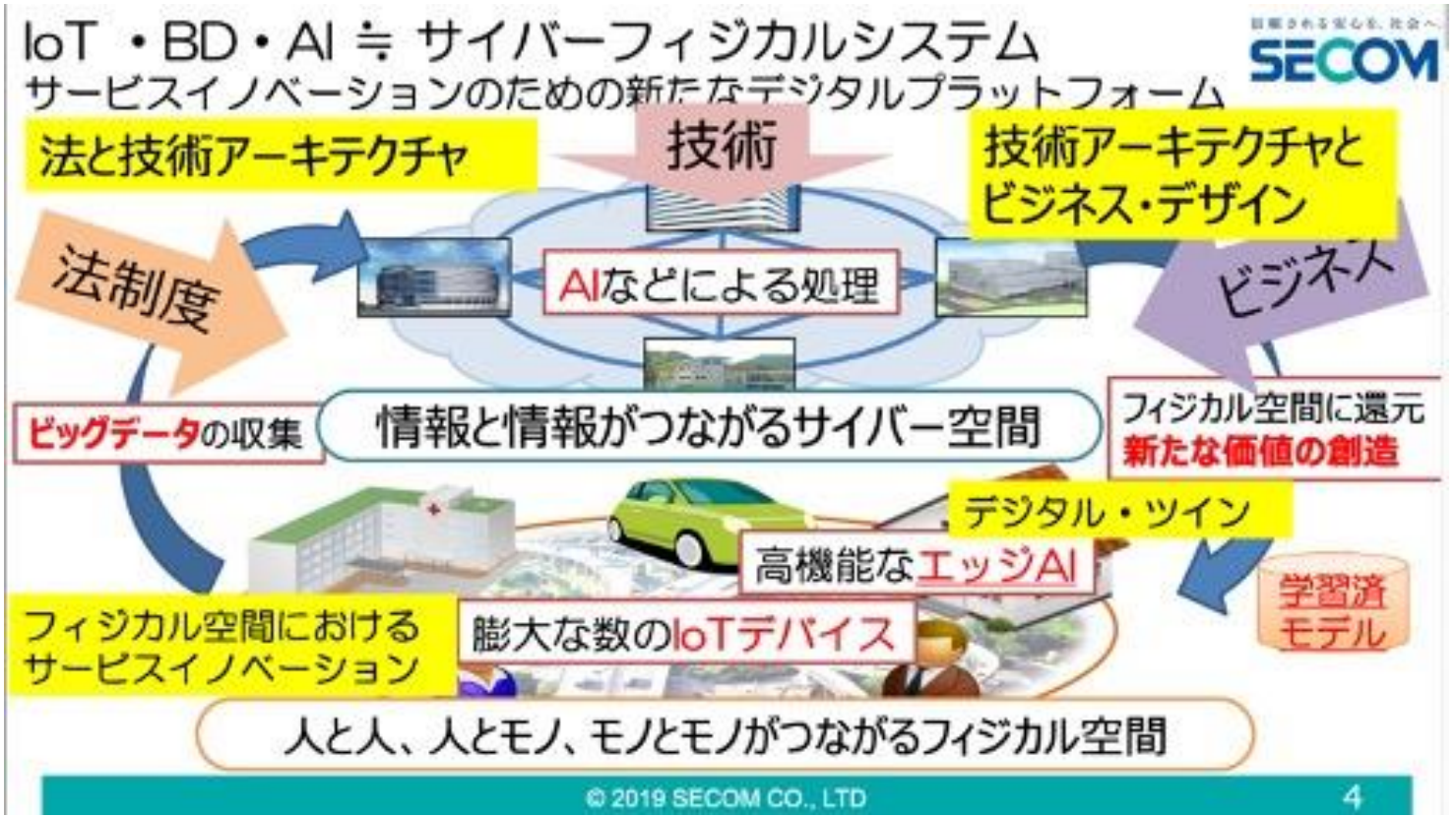
ETSI EN 319 422
Time-stamping protocol and time-stamp token profiles
ETSI EN 319 421
Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

サンプル署名ドキュメント：https://static.e-szigno.hu/docs/hr--min--bel--EN--v2.8.pdf

28

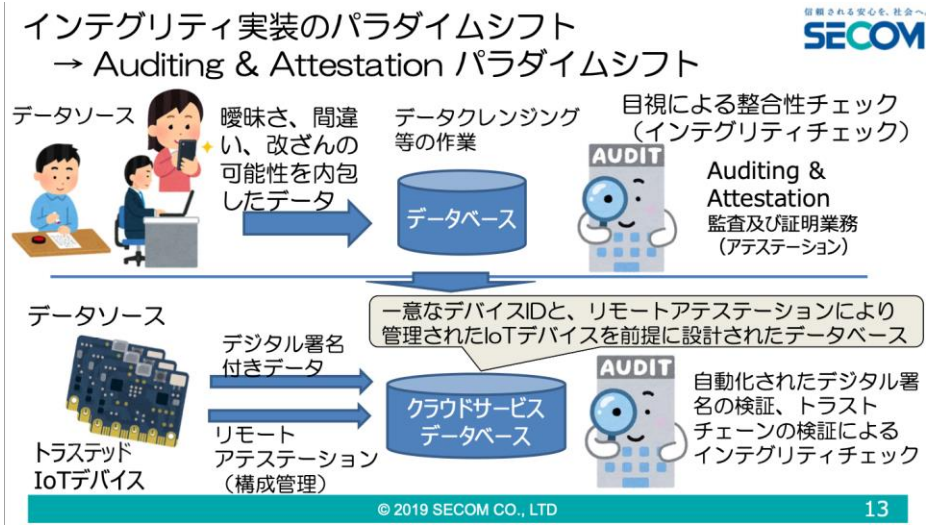
10年後をイメージして喋った昨年のシンポジウム
2019年　データ戦略の課題と未来

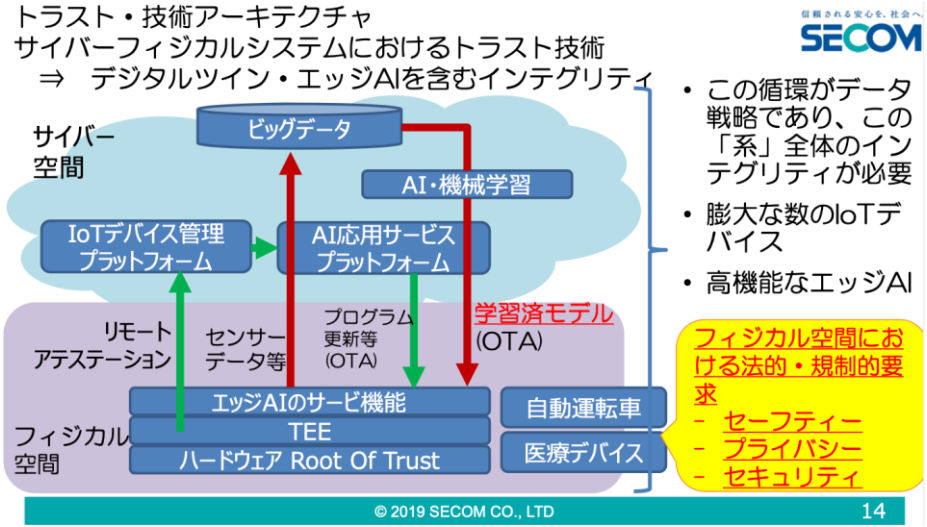
https://www.jlf.or.jp/assets/work/pdf/kenshu_190910_04.pdf



10年後をイメージして喋った昨年の「データ戦略の課題と未来」シンポジウム「データ戦略のためのITシステム」

https://www.jlf.or.jp/assets/work/pdf/kenshu_190910_04.pdf





様々な主体（自然人、法人、サービス、IoTデバイス、AIエッジ）が、様々な証明などのために、様々なデータ・オブジェクト（書面、時刻、プログラムコード、 AI学習モデル）にデジタル署名を施し、リアルタイムに様々な連携のために、様々な場所からデジタル検証に基づいたトラストな自動化・スマート化が行われると言った世界

参考資料

- 2000年　-- 第2回 セキュリティ・フォーラムレポート
  - https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html
- 2003年　電子署名・認証利用パートナーシップ報告書2003　活動と提言
  - https://www.jipdec.or.jp/archives/publications/J0004195
- 2005年　電子署名方の在り方と電子文書長期保管に関する現状調査報告書
  - #2020年現在　非公開
- 2006年　社会基盤としての電子認証と電子署名
  - https://www.jstage.jst.go.jp/article/nig/43/5/43_5_324/_pdf
- 2010年　オンライン手続における リスク評価及び電子署名・認証ガイドライン
  - https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf
- 2010年　電子政府ガイドライン作成検討会 セキュリティ分科会報告書
  - https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf
- 2010年　　PKI Day 2010〈社会基盤としてのPKI/PKIの10年〉
  - https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf
- 2012年　　PKI Day 2012我が国における信頼基盤の連携に向けて
  - https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf
- 2019年　トラストサービスの調査ワークショップ　Uの技術標準
  -- デジタル単一市場戦略の中核となるトラスト --
  - https://itresearchart.securesite.jp/19ws207/docs/s03.pdf
- 2019年　データ戦略の課題と未
  - https://www.jlf.or.jp/assets/work/pdf/kenshu_190910_04.pdf

信頼される安心を、社会へ。
SECOM

電子署名法の立て付けと課題

電子署名法の第一条　→ 目的が最も重要

- 第一条
  - この法律は、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とする。

「特定認証業務に関する認定の制度その他必要な事項を定めること」は、

本当に

国民生活の向上及び国民経済の健全な発展に寄与したのか？？

第二条

- この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）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をいう。
  - 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。
- 2　この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）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をいう。
- 3　この法律において「特定認証業務」とは、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をいう。

「特定認証業務」の主務省令で定める基準
ー＞　　これが、とっても重要なはずだけど。

第二章　電磁的記録の真正な成立の推定　　第三条

- 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。

- （認定の基準）
- **第六条**　主務大臣は、第四条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。
  - 一　申請に係る業務の用に供する設備が主務省令で定める基準に適合するものであること。
  - 二　申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること。
  - 三　前号に掲げるもののほか、申請に係る業務が主務省令で定める基準に適合する方法により行われるものであること。
- ２　主務大臣は、第四条第一項の認定のための審査に当たっては、主務省令で定めるところにより、申請に係る業務の実施に係る体制について実地の調査を行うものとする。

「認定の基準」は、2000年当時、非常に労力をかけて作成されていた。
しかし、少なくも2000年当時は、非常に敷居が高い（高過ぎる）基準だった。

主務省令
平成十三年総務省・法務省・経済産業省令第二号
電子署名及び認証業務に関する法律施行規則

- （特定認証業務）
  - **第二条**　法第二条第三項の主務省令で定める基準は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。一　ほぼ同じ大きさの二つの素数の積である二千四十ハビット以上の整数の素因数分解
  - 二　大きさ二千四十ハビット以上の有限体の乗法群における離散対数の計算
  - 三　楕円曲線上の点がなす大きさ二百二十四ビット以上の群における離散対数の計算
  - 四　前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの

- 「認定の基準」には、設備、本人確認方法、運用基準について、非常に厳しい基準が示されている。
- その一方、「特定認証業務」に関しては、暗号アルゴリズム以外の基準は、何も示されていない。ここに大きな課題がある。
  - 暗号アルゴリズムということに関しては、 2003年2月20日に「電子政府」における調達のための推奨すべき暗号のリスト(電子政府推奨暗号リスト)を公表したCRYPTRECの活動の影響を色こく受けている？？