2010 年 1 月 7 日

関西大学法科大学院　法と社会２「法とメディア」第 13 回

電子メディアにおける署名・認証制度

弁護士・弁理士　近　藤　剛　史

tsuyoshi@kondolaw.jp

Ⅰ　電子メディアにおける暗号

1) いろは歌　　作者空海？　柿本人麻呂？

「色は匂へど　散りぬるを　我が世誰ぞ　常ならむ

有為の奥山　今日越えて　浅き夢見じ　酔ひもせず」

いろはにほへ**と**

ちりぬるをわ**か**　　小野小町の暗号　「沓冠（くつかむり）」

よたれそつね**な**

らむうゐのお**く**　　→　　「咎無くて死す」

やまけふこえ**て**　　（無罪で死ぬ）

あさきゆめみ**し**

ゑひもせ　　**す**

2) 暗号の歴史

BC1900 年頃　エジプトにてヒエログリフで暗号を使用

http://ja.wikipedia.org/wiki/%E3%83%92%E3%82%A8%E3%83%AD%E3%82%B0%E3%83%AA%E3%83%95

BC5－60 年頃　シーザー暗号(Julius Caesar)

1460 年代　アルベルティが多表式暗号、トリテミウスの多表式暗号

さらに鍵を付加した「ヴィジュネル方陣」　→ 1800 年代まで破られず

1930 年代　独エニグマ暗号

http://ja.wikipedia.org/wiki/%E3%82%A8%E3%83%8B%E3%82%B0%E3%83%9E_(%E6%9A%97%E5%8F%B7%E6%A9%9F)

日本のパープル暗号（AF=ミッドウェイ、「ニイタカヤマノボレ」）

1970年　ＤＥＳ(Data Encryption Standard)暗号

1971年　ＤＥＳが米国商務省において標準化

1976 年　「公開鍵暗号」(スタンフォード大の Whitfield Diffie,Martin Hellman)

1977 年　RSA 暗号(MIT の Ronald Rivest,Adi Shamir,Leonard Adleman)

1985 年　楕円曲線暗号（ECC 暗号）

2007 年　ＭＤ５（ハッシュ関数）が解読？

3) 現在のＩＴ社会における暗号（電子署名）の利用

イ）電子メールの受信

電子メールのヘッダ情報

「Content-Type: text/plain; charset=ISO-2022-JP」

メール用暗号ＰＧＰ(Pretty Good Privacy)

ロ）ＰＯＰ３（メールサーバー）

POP3(Post Office Protocol Version 3)とは、MD5 という暗号アルゴリズムによる APOP(Authentified Post Office Protocol)というプロトコルを用いた通信手順。

ハ）ウェブサイトにおける「ＳＳＬ(Secure Sockets Layer)」

ネットスケープ社が提唱した TCP プロトコル（ハイブリッド暗号）

① クライアントは、乱数１と自分が使用可能な暗号方式をサーバーへ送信

② サーバーからは、乱数２と実際に使う暗号方式を決めてクライアントへ返答

③ サーバーは証明書と署名を付けて、公開鍵を送信

④ クライアントは署名などを検証し公開鍵を受け取って、公開鍵暗号方式による暗号通信の準備を行う

⑤ この時点で、クライアントが公開鍵を持っていれば、クライアントからサーバーへも証明書付きで公開鍵が送信

⑥ クライアントから公開鍵が送信されなくても処理は継続され、クライアントは Pre Master Secret と呼ばれる乱数を作り、暗号化してサーバーへ送信

⑦ クライアントとサーバーは、決められた手順に従って、Pre Master Secret 、乱数１、乱数２から Master Secret を作成

⑧ Master Secret と乱数１、乱数２から、共通鍵１、MAC Secret 1、共通鍵２、MAC Secret 2 を作成

⑨ この生成した共通鍵１と共通鍵２を利用して、共通鍵暗号で暗号化された秘匿通信が開始される（共通鍵が２つなのは、両方向からの通信に対応するため）

Cf.インターネット・エクスプローラー）の場合

「ツール」 → 「インターネットオプション」 → 「コンテンツ」タブの「証明書」ボタン → 「信頼されたルート証明機関」

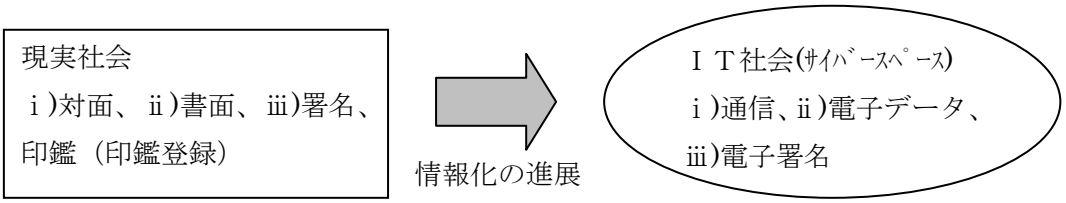
つまり、サーバーの証明書が、あらかじめブラウザに登録された認証局から発行されたものであれば、信頼できる認証局から発行された証明書として処理する。

そうでない場合には、「このサーバー証明書を発行した認証局は信頼できるかどうかわからないが、処理を継続するか」というメッセージが表示される。

→ いわゆるフィッシングに対する防御となる

Ⅱ　現実社会の法と電子メディアにおける法

1)　メディアの変容



高度情報通信ネットワーク社会形成基本法

2) 電子メディアにおける法基盤

ⅰ）契約合意の成立

講義にて既述。

ⅱ）書面（紙媒体）vs 電子データ

イ）現実社会の場合

書面交付には、次のような効果があるとされている。

①情報提供を書面で行うことにより、顧客に対し当該情報が確実・明確に伝わり、また、後日、情報の内容を再確認できるという「情報提供機能」

②顧客に説明を行う際、書面を用いることにより説明を補うこと等が期待される「説明補完機能」

③顧客に対し主要なリスクなどの重要情報の警告等を行う際、書面を用いることにより顧客に対する一層の注意喚起を期待する「警告機能」

④顧客の行った取引の内容・条件を書面で通知することにより、顧客が当該取引の内容・条件等を事後的に確認できるという「確認機能」

⑤この他、取引の証跡としての「証拠保全機能」

ロ）電子メディアの場合

書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律（平成 12 年法律第 126 号、いわゆる「ＩＴ書面一括法」）

証券取引法（現金融商品取引法）、保険業法、割賦販売法、訪問販売等に関する法律（現特定商取引法）、旅行業法、宅地建物取引業法等に関する改正。

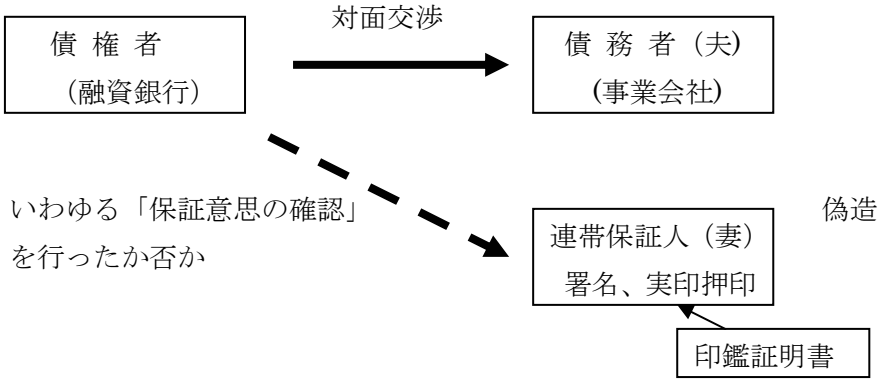
・電子媒体を利用して書面交付（厳密には情報の交付）を行うに際しては、交付された情報について、従来の書面による交付と同等の利用可能性が確保される必要があり、そのためには、「書面」を用いることによる明確性・確実性・保存性が電子媒体による交付においても確保されるようにする必要がある。

iii）署名(記名)捺印 vs 電子署名・電子認証

イ）現実社会の場合

いわゆる「保証否認」のケース

Cf.文書の成立を否認するときは、その理由を明らかにしなければならない（民訴規則 145 条）



①身分証明書の提示、印鑑登録、②印鑑登録カードの自宅住所地への郵送、③印鑑登録カード提示により印鑑登録証明書の交付

Q いわゆる「保証否認」のケースは、何が法律上の争点となるのか？

Q その場合、どういう間接事実が重要だと考えられるか？

Q 例えば、2000 年 4 月 1 日に、妻が夫のために貸金に関する包括根保証を行っていた場合、債権者は連帯保証人である妻に対して連帯保証債務の履行請求をなし得るか？

ロ）電子メディア

電子署名及び認証業務に関する法律（2000 年 5 月 31 日公布）

自筆署名 → 電子署名、　市役所 → 認証局(Certificate Authority)

Ⅲ　公開鍵暗号を用いた電子署名

1) 電子署名の必要性

・データの信頼性・安全性とセキュリティの強さは比例する

・①本人の属性であることを示すデータとの照合に成功していること、②そのデータが本人のものであることの確認作業が既になされていること、の２つが必要。

・ここで言う「証明」とは、自然科学的な証明ではなく、証明の程度（証明度）という概念を含んだ社会科学的なもの。

・匿名性を維持しつつ、改竄やなりすましを防止しつつ、本人であることを証明することが求められている。

2) 電子文書の原本性の確保

最良証拠法則(Best Evidence Rule)　　cf.書証原本の確認

①内容の同一性の保証

②作成者の保証

③作成日時の保証

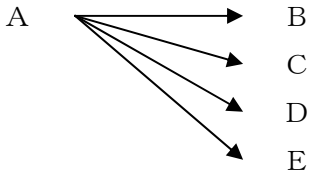
3) 共通鍵（対称鍵）暗号システム、秘密鍵暗号システム

（メリット）暗号システムの構築が容易

（デメリット）いくつもの鍵が必要

鍵を別途安全な方法で送る必要

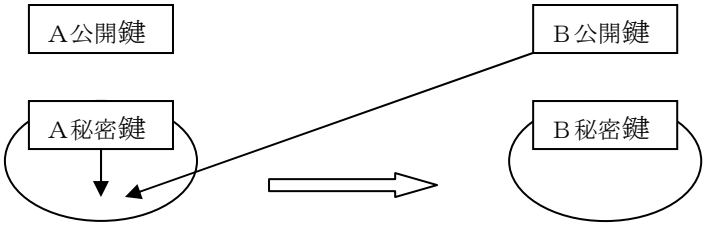
ある暗号を持っているのが１人だけだという保証がない



4) 公開鍵（非対称鍵）暗号システム

イ）仕組み

公開鍵と秘密鍵は、ペアになっている鍵であるが、同一の鍵ではなく、相互に他方の鍵を推測することができないようにして生成される



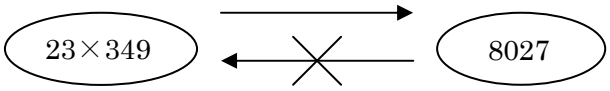
送信者Ａの秘密鍵で暗号化し、さらにＢの公開鍵で暗号化して送信すると、①Ａだけが暗号文として送信することができ（Ａの本人性の確認）、かつ、②Ｂだけが復号して読むことができる（安全性の確保）。

ロ）ＲＳＡ暗号

1977 年、ロナルド・リベスト(Ron **R**ivest)、アディ・シャミア(Adi **S**hamir)、レオナルド・エーデルマン(Len **A**dleman) によって、発見された。

RSA 暗号とは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つ。暗号(Cipher)とデジタル署名(Digital signature)を実現できる方式として公開されたもの。

（参考）RSA 暗号方式、一方向関数



ｐ、ｑ　ランダムに選んだ５１桁の素数

Ｎ：ｐとｑの積　　Ｌ：ｐ－１とｑ－１の最小公倍数

ｅ：Ｌと素な数　　ｄ：Ｌ、ｅに対して下記(＊)式を満たす数

１＝Ｌｃ＋ｅｄ　（＊）を満たすｃ、ｄが存在することが知られている。

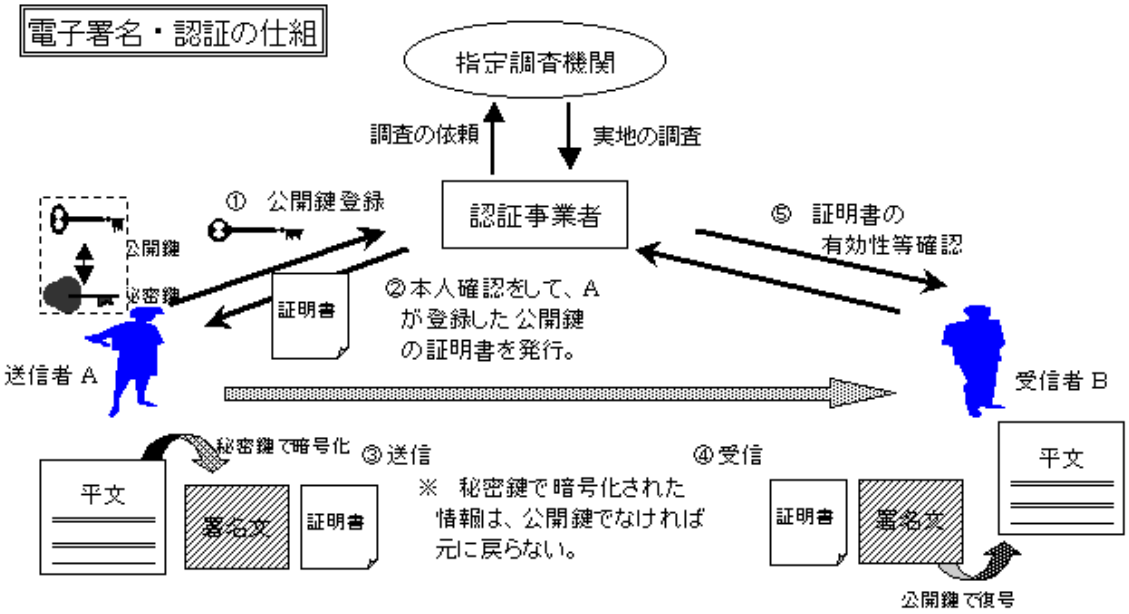
暗号鍵：（ｅ、Ｎ）　復号鍵：ｄ

Cf.素数の発見法

「エラトステネスのふるい」

総当たり方式（ブルート・フォース法）

5) 認証機関(CA)の存在理由



6) デジタル署名(Digital Signature)

公開鍵暗号方式とハッシュ関数とを利用して、メッセージ認証と本人認証の両方を行う仕組みをデジタル署名と呼ぶ。

Cf.東京証券取引所のデジタル署名サービス

http://www.tse.or.jp/listing/disclosure/signature.html

電子データに関係する技術の普及に伴い、上場会社が作成した開示資料は、その複製、修正が容易に行い得る状態にあり、上場会社のホームページ等に掲載された会

社情報が改ざんされ、投資者に誤った判断が提供されるおそれがあるため。

Ⅳ　電子署名及び認証業務に関する法律（電子公証システム）

1)電子署名及び認証業務に関する法律の概略

・2000 年 5 月 31 日公布、2001 年 4 月 1 日施行

・電子署名の効力（民訴法の補完）と認証機関の運営主体について規定

・「指定公証人の行う電磁的記録に関する事務に関する省令」の一部が改正され、2007 年 4 月 1 日から新しい電子公証制度が導入された。

2)「電子署名」の定義

・「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、次の要件のいずれにも該当するものをいう」（2 条 1 項）

①「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」（本人性の確認）

②「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」（非改ざん性の確認）

・「技術的中立性（technological neutrality）」

3)効力

・電磁的記録の情報に本人による一定の電子署名が行われているときは、真正に成立したものと推定する旨の規定

イ）従来文書におけるいわゆる「二段の推定」

① 印影が本人又は代理人の印章により顕出された場合

↓↓（最高裁昭和39年5月12日判決）

② 当該印影は本人又は代理人の意思に基づき成立したもの

↓↓（民事訴訟法 228 条 4 項）

③ 文書が真正に成立したと推定される

↓

④ その文書（契約条項）に記載されている法的効力が認められる。

ロ）デジタル文書における取扱

② 本人による電子署名が行われている

↓（電子署名認証法 3 条）

③ デジタル文書が真正に成立したものと推定する

↓

④ そのデジタル文書に記載されている法的効力が認められる。

・ちなみに、公文書の場合には民事訴訟法 228 条 2 項が「方式」による推定を認めているので、電子の文書の場合であっても、同条項を直接に適用して、その真正な成立を推定することが可能

4)認証機関の運営主体

・民間認証機関の安全・信頼性を確保するため、「特定認証業務」と定義して（2 条 3 項)、特定認証業務を行おうとする者は、主務大臣の認定を受けることができるとしている（4 条）

・主務大臣は、認証業務の認定をする際に、その指定する者（指定調査機関）に調査の全部又は一部を行わせることができる（17 条～32 条）

・業務に関する帳簿書類の作成・保存義務（11 条）

・利用者の真偽の確認に関します情報の目的外使用の禁止（12 条）

・主務大臣による報告徴収及び立入検査などを受ける義務（35 条）

5)電子署名法の問題点

①認証業務を行う際に認証機関がどのような手続で本人確認するのか

現在認められている電子署名の種類（5 種類）

イ） 商業登記に基づく電子証明書（電子認証制度を運営する電子認証登記所）

ロ） AccreditedSign パブリックサービス２（日本認証サービス株式会社）

ハ） ビジネス認証サービスタイプ１－G（日本商工会議所）

ニ） 公的個人認証サービス（地方公共団体）

ホ） 日本司法書士会連合会認証サービス（日本司法書士会連合会）

②認証内容が誤っていた場合における認証機関の責任

③個人情報、プライバシーの問題

電子署名の場合、誰でも認証機関から自由に取得できたり、取引の際に電子店舗側が必然的に電子署名を要求するといった運用がなされると、必要以上の個人情報が電子署名に関する認証の記載事項として漏洩したり、個人情報が悪用される危険性がある

④国際的な電子商取引に関するルール作り

⑤ デジタル文書と従来の文書との棲み分け

6) 電子公証制度

イ）経過及び概要

・2002 年 1 月 15 日より、電子公証制度の運用を開始。

・公開鍵暗号基盤（PKI, public key infrastructure)」に基づくデジタル署名

・現行の公証制度で紙の文書に対して行われている公証業務の中で「私署証書を認証する」、「会社設立の際に必要となる定款を認証する」、「文書に確定日付を付与する」ことを、電子文書（電磁的記録）に対しても行うことができるように創設されたのが「公証制度に基礎を置く電子公証制度」

それに付随してこれらの電子文書を「２０年間保存」することや、「謄本の作成等」にも応じることができます。

・電子公証サービスは、法務大臣によって任命された公証人のなかから、特に指定

された公証人（「指定公証人」と呼ばれます。）が運用。

・これまでの制度では、公証人役場にデータを入力したフロッピーディスクを提出して嘱託等を行う必要があったが、2007 年 4 月 1 日以降、原則として、法務省オンライン申請システムを経由して嘱託等を行うことになった。また、住民基本台帳の情報に基づいて発行される「公的個人認証サービス」における電子証明書が新たに利用可能となった。

ロ）サービスの主な内容

a）電子確定日付の付与

インターネットを介して、嘱託人（クライアント）である企業が作成した電子文書の成立時期及び内容を証明する電子確定日付（日付情報）を付与します。債権の譲渡などについては法律上確定日付が必要。また、契約の中身や成立の日付に争いが生じるおそれがあるような場合には確定日付を受けておくと有利。

b）電子私署証書の認証

紙文書に捺印するように、電子文書にデジタル署名を行い、電子私署証書を作成し、これに指定公証人の認証を受けることができる。指定公証人は、認証を行うに際し、法律家の立場から文書の内容が違法でないことを審査する。

なお、一般の文書については、作成者が公証人の認証を受けるかどうかは任意であるが、株式会社などの設立の際に作成する定款については、公証人が認証を行わないと無効。

ハ）付随的サービス

a）同一性の証明

電子確定日付文書、電子私署証書が、確かに指定公証人により認証されたものと同一であることを証明してもらうサービス。手数料は 1 件当たり 700 円

b）同一情報《複製》の取得

作成した電子文書の原本保存サービスを行い、指定公証人に保存依頼した電子確定日付文書、電子私署証書の原本の複製を依頼し、その結果を取得するサービス。このような原本の保存サービスによって、これにより後日紛争が生じた際に電子文書の存在･内容を証明することができ、紛争の解決に役立つことから、公証制度に基礎をおく電子公証制度においては、公証人が信頼できる第三者機関（ＴＴＰ：Trusted Third Party）としての役割を担うことが期待されている。

ニ）適用外

a）公正証書の取扱

金銭の貸借、土地・建物の賃貸借等の契約や遺言などの公正証書の電子化はまだ実現せず。

このような契約や遺言は、公証人が当事者の面前で意思確認を行う必要がある場合が多いことなどがその理由。

Q　家の明渡しに関するいわゆる執行受諾文言付きの公正証書（執行証書）を作成した場合、その公正証書を債務名義として強制執行を行うことは、可能か？

b）利用者

電子公証サービスは、現在のところ、法人として登記された企業を対象としており、個人を対象としていない

7）暗号の強度

電子署名及び認証業務に関する法律施行規則（平成 13 年 3 月 27 日総務省・法務省・経済産業省令第 2 号）

第 2 条（特定認証業務）

法第 2 条第 3 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 1024 ビット以上の整数の素因数分解

二　大きさ 1024 ビット以上の有限体の乗数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 160 ビット以上の群における離散対数の計算

四　前 3 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

以　上