電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価

宇根正志（うねまさし）

要　旨

インターネットを活用した電子商取引を展開するうえで、契約書等、商取引関連の文書を電子的かつ安全に取り扱いたいというニーズが、金融分野をはじめとする幅広い分野で高まっている。交信データの安全性を確保するためには、データの暗号化や取引相手の認証に加えて、後々の係争等に備えて、「だれが、いつ、どのような電子文書を、送信（あるいは受信）した」という事実を証明可能にする技術が必要とされている。

電子文書の送受信証明を行うためのプロトコルは、このようなニーズに対応する技術であり、その概念や枠組みはISO13888に規定されている。ISO13888はいくつかの送受信証明の実現形態を規定しており、特定のデータが特定時刻に存在したことを証明するタイムスタンプ・プロトコルも、その中の1つに含まれている。

送受信証明のプロトコルに関する研究は従来から進められており、最近では一部で商用サービスも開始されている。しかし、プロトコルに関する安全性評価手法は、現在研究途上にあり、十分に確立されているわけではない。今後、電子文書の送受信証明のサービスを安心して利用するためには、各サービスに採用されているプロトコルの安全性評価が必要である。

本稿では、電子文書の送受信証明プロトコルの概念や枠組みについてISO13888に沿って説明した後、各種研究・商用サービスの動向を紹介し、今後検討が必要な課題を提示する。そのうえで、送受信証明プロトコルの実現形態の1つであるタイムスタンプ・プロトコルの安全性評価について最新の研究成果を紹介する。

キーワード：安全性評価、暗号プロトコル、送受信証明、タイムスタンプ、電子商取引、電子認証、ISO13888

本稿は、2000年11月22日に日本銀行で開催された「第3回情報セキュリティ・シンポジウム」への提出論文として作成されたものである。本稿の作成に当たっては、櫻井幸一助教授（九州大学大学院システム情報科学研究院情報工学部門）から、貴重なコメントを頂戴した。ここに記して感謝したい。もっとも、本稿のあり得べき誤りはすべて筆者に属することはいうまでもない。また、本稿に示された意見はすべて筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

宇根正志　日本銀行金融研究所研究第2課（E-mail: masashi.une@boj.or.jp）

1．はじめに

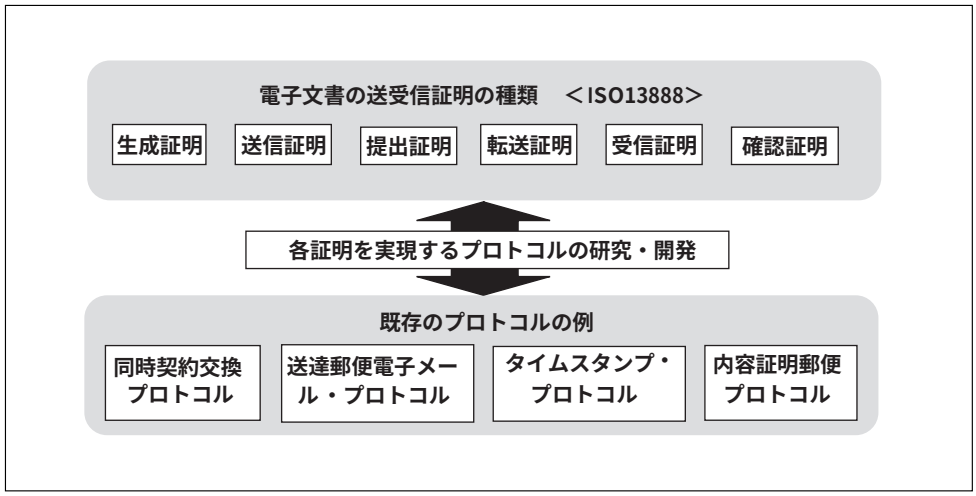
インターネットの急速な拡大に伴い、オンライン証券取引や電子オークション等、各種電子商取引が行われるようになってきている。インターネット上で安全な電子商取引を実現するためには、通信相手がだれか、送受信されるデータが通信途中で改ざんされていないか等、通信データの安全性確保が問題となる。既存の各種サービスの中には、電子文書の機密性・一貫性をSSL（Secure Sockets Layer）等の暗号プロトコルを用いて確保するほか、取引相手の本人確認を認証機関が発行する公開鍵証明書によって実現しているものも存在する。

しかし、電子商取引の安全性を確保するための対応は、それだけに尽きるわけではない。取引相手に正しく電子文書が届いたとしても、例えば、受信した相手が「自分はそうした電子文書を受け取っていない」と主張したり、送信者が「自分はそうした電子文書を送っていない」と主張した場合には、その真偽を確認することは極めて困難となる。具体的な一例として、インターネット上での電子商取引で購入した商品について、インターネット上でクーリング・オフによる契約解除を要求するといった状況を想定すれば、受信者が電子文書の受信を否認したり、受取日付を偽ったりする可能性を考慮しておくことが必要であることが理解できよう。このような問題に対応するためには、電子文書について、「受信者が電子文書を特定時刻に受信した」という事実を証明するプロトコルや、「送信者が電子文書を特定時刻に送信した」という事実を証明するプロトコルが必要である。このようなプロトコルについては、従来から理論的な研究が進められており、送受信証明の商用サービスが開始されているものの、電子文書の送受信証明を実現している電子商取引はごく一部に限られているとみられる。

では、具体的にどのような種類のプロトコルが送受信証明を行うためのプロトコルに含まれるのであろうか。送受信証明を行うプロトコルの概念や基本的な枠組みは、ISO13888（ISO/IEC［1997a, 1998, 1997b］）に規定されている。ISO13888では、電子文書の送受信証明の種類として、生成証明、送信証明、提出証明、転送証明、受信証明、確認証明を規定している。これらの証明を実現するものとして、同時契約交換プロトコル、送達郵便電子メール・プロトコル、タイムスタンプ・プロトコル、内容証明郵便プロトコル等が提案されている（図1参照、なお、各プロトコルについては3章～5章で説明）。

現在、電子文書の送受信証明に関する商用サービスが一部で開始されており、今後もさまざまなサービスが提案されていくと予想される。そうしたサービスを利用したいと考える利用者サイドでは、どのサービスを選べばよいかを検討する際に、各サービスが本当に安全かを確認しておく必要がある。しかし、現時点では、各種送受信証明プロトコルの安全性を評価するための手法は十分に確立されていない。電子文書の送受信証明を行うプロトコルは暗号技術等の各種要素技術から構成されており、プロトコルの安全性を評価するためには、個々の要素技術を評価したうえで、総合的な評価が必要である。今後は、こうしたプロトコルの

図1　電子文書の送受信証明の種類とプロトコル



安全性評価手法を確立し、利用者が安心してサービスを利用できるように、利用者に評価結果を適切に伝えることが重要である。また、送受信証明プロトコルの安全性評価手法の確立は、他の暗号プロトコルの評価にも有益な情報を提供しうるものと考えられる。

金融分野においても、電子文書の送受信証明プロトコルは、ネットワーク上で行われる取引の安全性を一層高めるうえで有用な技術である。今後、インターネット上での電子商取引が一層拡大し、さまざまな形態で金融サービスを利用したいというニーズが高まってくると考えられる。その場合、金融機関が重要な電子文書をネットワーク経由で取引相手に送付するに当たり、電子文書の送受信証明プロトコルを活用していくことも考えられよう。

本稿では、まず2章において、送受信証明プロトコルの基本的な枠組みをISO13888の内容に沿って説明する。3章および4章では、理論研究動向と実装研究・商用サービス動向についてそれぞれ整理し、今後検討が必要となる主な技術的課題を示す。5章では、送受信証明プロトコルの実現形態の1つであるタイムスタンプ・プロトコルを取り上げ、その安全性評価に関する最新の研究成果を紹介する。

2．電子文書の送受信証明プロトコルの枠組み －ISO13888を参考に

電子文書の送受信証明プロトコルの概念や基本的な枠組みは、国際標準ISO13888（non-repudiation）[1]に規定されている。ISO13888は、TTP（trusted third party）[2]が電子文書の送受信時に介在するケースを主として前提にしている。以下では、ISO13888の内容に沿ってプロトコルの基本的な枠組みについて説明する。

（1）送受信証明の種類・目的

電子文書の送受信証明の概念を規定するISO13888-1（ISO/IEC［1997a］）は、送受信証明の種類として以下の6つを規定している。

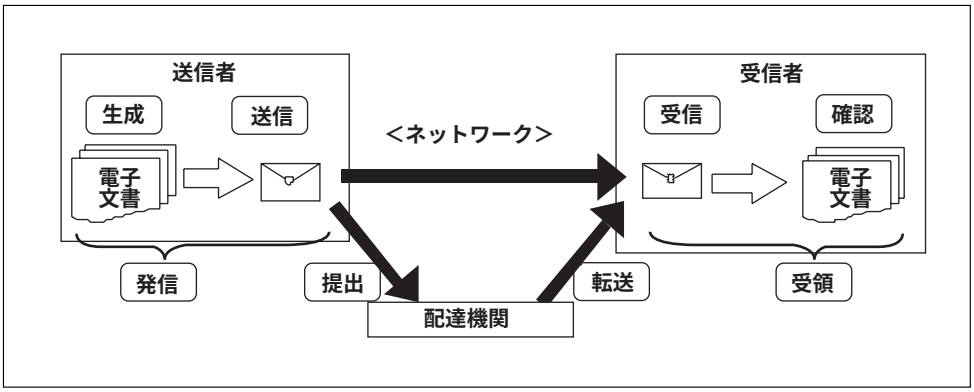
①生成（creation）証明：「だれが、いつ、どんなデータを生成したか」を証明
②送信（sending）証明：「だれが、いつ、だれに対して、どんなデータを送信したか」を証明
③提出（submission）証明：「特定の配達機関（delivery authority）が、いつ、だれから、だれに対して送信される、どんなデータを受信したか」を証明
④転送（transport）証明：「特定の配達機関が、いつ、だれから受信した、どんなデータを、だれに対して転送したか」を証明
⑤受信（receipt）証明：「だれが、いつ、だれから送信された、どんなデータを受信したか」を証明
⑥確認（knowledge）証明：「だれが、いつ、だれから送信された、どんなデータの内容を確認したか」を証明

さらに、生成証明および送信証明の両方を含むものとして発信（origin）証明が規定されているほか、受信証明および確認証明の両方を含むものとして受領（delivery）証明が規定されている。これらの各種証明は、データを送受信する際の各プロセスに対応している（図2参照）。データを送信する場合、TTPである配達機関を経由せずに直接受信者に送信するケースと、配達機関を経由するケースが想定される。配達機関を経由しないでデータを送信するケースでは、データの発信、受領の2つの証明を考慮する必要がある。一方、配達機関を経由する場合には、データの提出、転送、受領の証明を考慮する必要がある。

これらの各種証明を実現するサービスの実用化を考える場合、プロトコルが備えるべき要件を明確にしておくことが有用である。ただし、ISO13888においては、そうした要件に関する規定は存在しない。

1 ISO13888で用いられている“non-repudiation”には、「否認防止」「否認拒否」といった訳語が当てられることが多いが、本稿では、「電子文書（あるいはデータ）の送受信証明」という表現を統一的に用いることとする。
2 TTPは、ISO13888-1では、「情報セキュリティ関連業務の管理・運用状況について他のエンティティから高い信頼を寄せられているエンティティ」と定義されており、データの送受信者や、トークンの検証者等から高く信頼されていることが前提とされている。ただし、TTPの業務要件や組織の特徴等については、本標準には規定されておらず、現在ISO14516（TTPの利用や管理に関する指針）やISO15945（デジタル署名を活用するためのTTPサービスの仕様）として標準策定が進められている。

図２　電子文書の送受信証明の種類・構成



（2）各種TTP

ISO13888は、各種証明内容に関する情報、および、証明の正当性を示す情報を含むトークンと呼ばれるデータを用いる方法を規定している。証明内容に応じたトークンを生成・保管し、必要に応じてトークンを提示することで、自分の主張の正当性を裏付けることができる。トークンの生成は、TTPが行う場合とデータの送受信者が行う場合とが規定されている。ISO13888-1に規定されている各種TTPの機能は、表1のとおり（相互関係については図3を参照）。

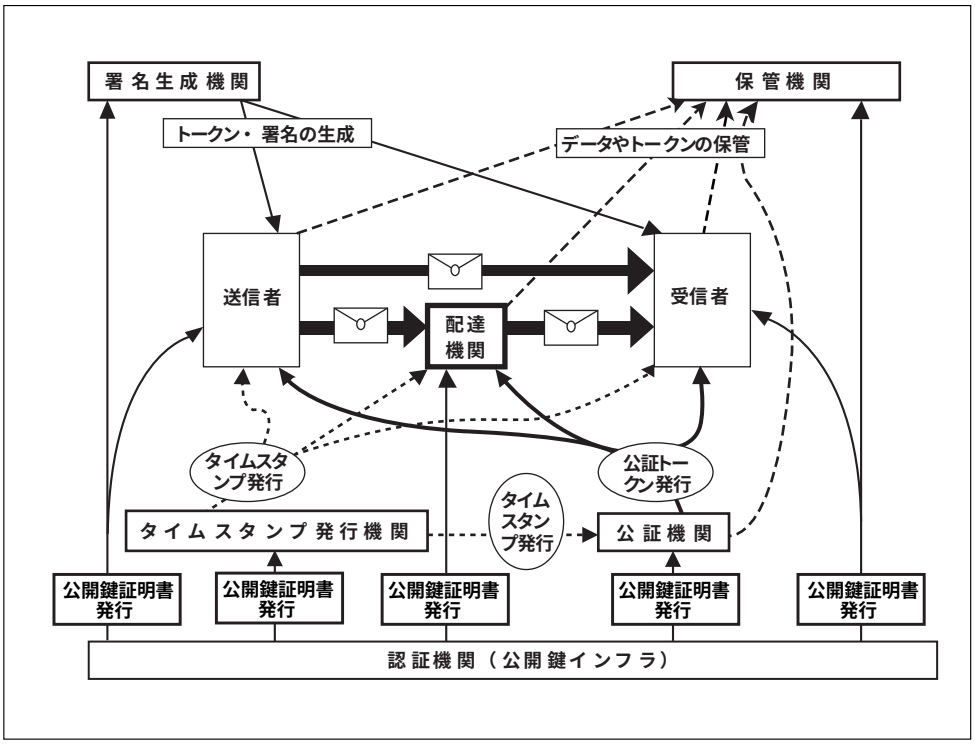
表１　各種TTPとその機能

TTP	機能
配達機関（delivery authority）	交信データを中継し、その内容や交信の事実を証明するトークンを生成。データ提出証明トークン*NRST*（non-repudiation of submission token）とデータ転送証明トークン*NRTT*（non-repudiation of transport token）の2種類のトークンを生成。
署名生成機関（digital signature generating authority）	配達機関を介さず直接データを交信するケースで、データの送受信者の代わりに、トークンや、その生成に用いられるデータのデジタル署名を生成。
監視機関（monitoring authority）	特定の事象・行為の発生を監視し、それらを証明するトークンを生成。
トークン生成機関（token generation authority）	既存のトークンを要素として利用し、それらを含む別のトークンを生成。
タイムスタンプ発行機関（time stamping authority）	事象・行為が発生した時刻を証明するタイムスタンプを生成。各TTPが各種トークンを生成する際に、信頼できる精度の時刻情報を入手困難な場合に利用される。
公証機関（notary authority）	保管・交信されたデータとそれらを取り扱った送受信者を特定する公証トークンを生成。
保管機関（evidence recording authority）	トークンやデータを受付日時に関する情報とともに安全に保管。

表1に示される複数の機能を1つのTTPが実現するケース（例えば、配達機関がタイムスタンプも発行するケース）も想定されている。

なお、ISO13888では、公開鍵証明書を発行する認証機関（certification authority）についても、デジタル署名を用いる場合に必要なTTPとして規定されている。認証機関は、データの送受信者だけではなく、デジタル署名を利用する各種TTPに対して公開鍵証明書を発行する。認証機関と公開鍵インフラ（PKI：public key infrastructure）については、ISO13888では詳しく規定されていないものの、データ送受信証明サービスの土台となる重要なインフラとして位置づけられている[3]。

図3　各種エンティティの関係・位置づけ



3 ISO13888で公開鍵インフラについて触れられていないのは、公開鍵インフラに関連する各種標準が既に存在する、あるいは、現在他の標準として策定が進められているためと考えられる。例えば、公開鍵証明書や公開鍵証明書廃棄リスト等に関する国際標準ITU-T X.509（ITU-T＜国際電気通信連合・通信標準セクタ＞が策定）が既に存在するほか、X. 509の公開鍵証明書を用いた公開鍵インフラを利用する各種技術仕様が、IETF PKIX（Internet Engineering Task Force, Public-Key Infrastructure X.509：インターネットにおける公開鍵インフラ関連技術の標準化を行うワーキンググループ）において策定されている。また、デジタル署名を活用するためのTTPサービスの仕様に関する国際標準案ISO15945の策定や、金融分野における公開鍵証明書の管理方法等に関する国際標準案ISO15782の策定も進められている。認証機関や公開鍵インフラに関する検討動向については、谷口［2000］を参照。

(3) トークン

トークンの基本型として、以下の*GNRT*（generic non-repudiation token）が規定されている。

> *GNRT* = *text* ‖ *z* ‖ *CHKx*(*z*)（‖：データの結合を表す）
> ・*text*：トークン自体の識別情報等のデータ（必須）
> ・*z* = *Pol* ‖ *f* ‖ *IDs* ‖ *IDg* ‖ *IDc* ‖ *IDr* ‖ *IDo* ‖ *Tg* ‖ *Ti* ‖ *Q* ‖ *Imp*(*m*)
> ・*CHKx*(*z*)：*x*（TTPの識別情報）によって生成されるデータ*z*の一貫性（integrity）を検証するデータ（MAC[4]もしくはデジタル署名）（必須）
> 　・*Pol*：トークンの生成・検証方法に関する情報（必須）
> 　・*f*：トークンによって提供されるサービス内容を示す情報（必須）
> 　・*IDs*：事象・行為を行った者の識別情報
> 　・*IDg*：トークン生成者の識別情報
> 　・*IDc*：事象・行為を行った者の相手となる者の識別情報
> 　・*IDr*：トークンの生成要求者の識別情報
> 　・*IDo*：その他の者の識別情報
> 　・*Tg*　：トークンの生成日時を表す情報（必須）
> 　・*Ti*　：事象・行為が発生した日時を表す情報
> 　・*Q*　：その他のデータ
> 　・*Imp*(*m*)：事象・行為に関するデータ*m*やそのハッシュ値等（必須）

上記*GNRT*に含まれる情報のうち必須なのは、*text*、*Pol*、*f*、*Tg*、*Imp*(*m*)、*CHKx*(*z*)の6つであり、その他はサービスの種類によって含まれる場合がある。各種トークンに含まれる情報を整理すると表2のとおり。

表2から、どのトークンにおいても、その生成日時に関する情報が必ず含まれることがわかる。また、タイムスタンプについては、タイムスタンプ発行機関と生成日時に関する情報が必須であるほか、公証トークンの場合、これらに加えて、トークンの発行依頼者の識別情報も必須となる。ただし、データの送受信の事実に関する係争等が後日発生した場合、その事実を証明するデータとしてトークンを利用するためには、トークンをどのように管理・保管するかが問題となる。この点については、ISO13888では保管機関について規定するにとどまっており、トークンの管理方法に関する要件等は規定されていない。

4 MAC（message authentication code）：メッセージの受信者がその一貫性（integrity）と送信者確認を行うためにメッセージに添付されるデータ（認証子）。共通鍵暗号アルゴリズムを用いてメッセージを圧縮変換して生成され、元のメッセージを1 bitでも変更すると異なるMACが生成される。

表２　各種トークンに含まれる情報

		トークンの種類					
		発信	提出	転送	受領	タイムスタンプ	公証
トークン生成者		送信者や署名生成機関	配達機関	配達機関	受信者や署名生成機関	タイムスタンプ発行機関	公証機関
トークン保管者		送信者や受信者	送信者や配達機関		送信者、受信者、配達機関	トークンの生成依頼者・生成者	
トークンの情報	*IDs* :送信者の識別情報	○	△	△	△	―	―
	IDg :トークン生成者の識別情報	送信者の場合は△、署名生成機関の場合は○	○	○	受信者の場合は△、署名生成機関の場合は○	○	○
	IDc :受信者の識別情報	△	○	○	○	―	―
	IDr :トークン生成依頼者の識別情報	―	―	―	―	―	○
	IDo :その他の主体の識別情報	―	△	△	―	―	―
	Tg :トークンの生成日時の情報	○	○	○	○	○	○
	Ti :事象・行為発生日時の情報	△	○	○	△	―	―

備考：○：必須、△：オプション、―：規定なし

（4）トークン生成プロトコル

各種トークンの一貫性を確保する手段については、デジタル署名を利用する場合（ISO/IEC 13888-3, ISO/IEC［1997b］）とMACを利用する場合（ISO/IEC 13888-2, ISO/IEC［1998］）が規定されている。MACを利用するためには、データの送受信者間で秘密の暗号鍵を共有する必要があり、通信相手が特定されている環境での利用に限定される。一方、デジタル署名では、事前に鍵の共有が不要なため、インターネット等不特定多数の相手と通信を行う場合に便利である。このように、MACとデジタル署名では利用環境が異なっている。本稿では、オープンなネットワークにおけるデータの送受信証明を検討対象とすることとし、以下、デジタル署名を用いるプロトコル（ISO/IEC 13888-3［1997b］）について説明する。

イ．配達機関を利用しないプロトコル

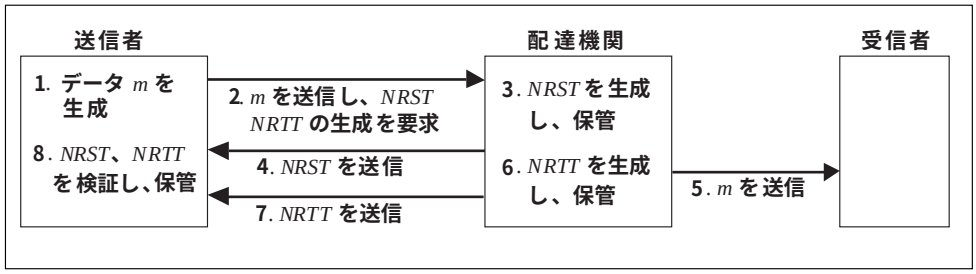
配達機関を利用しないケースでは、データ発信証明トークン*NROT*（non-repudiation of origin token）とデータ受領証明トークン*NRDT*（non-repudiation of delivery token）の生成プロトコルが規定されている（図4参照）。送信者は、送信データ*m*に対する*NROT*を生成・保管し、*m*と*NROT*を送信するとともに、*NRDT*の生成を受信者に要求する。受信者は、*NROT*のデジタル署名を検証したうえで*NROT*を保管し、*m*を受領した証となる*NRDT*を生成・保管したうえで送信者に送信する。送信者は、*NRDT*のデジタル署名を検証し、*NRDT*を保管する。

図４　データ発信・受領証明トークン生成プロトコル

ロ．配達機関を利用するプロトコル

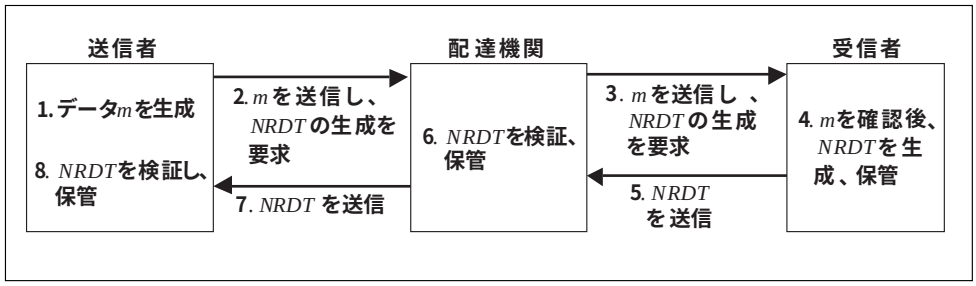
配達機関を利用するプロトコルでは、送信者が配達機関へデータを提出したことを証明するトークン*NRST*と、配達機関が受信者へデータを転送したことを証明するトークン*NRTT*の生成プロトコルが規定されている。これらのプロトコルは図5のとおり。

図５　データ提出・転送証明トークン生成プロトコル



データ受領証明トークンの生成プロトコルでは、送信者は、配達機関を経由してデータ*m*を受信者に送信すると同時に、*NRDT*の生成を受信者に要求する。受信者は、データ*m*を確認して*NRDT*を生成・保管し、配達機関経由で*NRDT*を送信者に送信する（図6参照）。

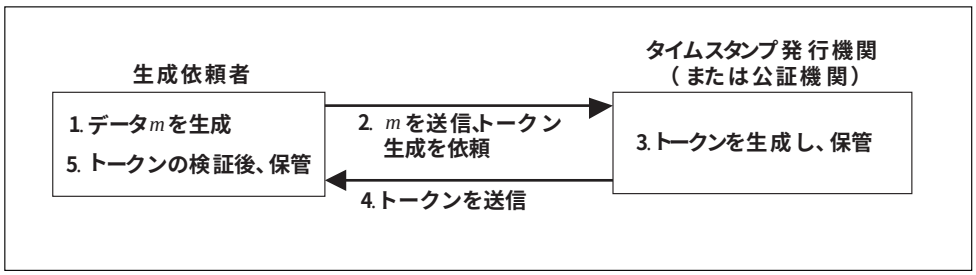
図６　データ受領証明トークン生成プロトコル



ハ．タイムスタンプ・公証トークンのプロトコル

この他、タイムスタンプ[5]や公証トークンの生成プロトコルについても例があげられており、それらの手順は図7のとおり。プロトコルの内容は同一であるが、タイムスタンプには生成依頼者の識別情報が含まれない一方、公証トークンには生成依頼者の識別情報が含まれる。

図7　タイムスタンプや公証トークンの生成プロトコル



（5）配達機関を利用しないプロトコルの問題点

ISO13888-3の配達機関を利用しないプロトコルに関して、ジョウ（Zhou）とゴールマン（Gollman）は、受信者による選択的受領（selective receipt）と送受信者による時刻情報の不正操作の可能性を示し、配達機関の必要性を指摘している（Zhou and Gollman［1996］）。

イ．選択的受領

配達機関を利用しないプロトコルでは、データ受領証明トークン*NRDT*を生成するかは受信者本人に委ねられる。このため、受信したデータが都合の悪いものであった場合、受信者が*NRDT*を生成しない可能性がある。ジョウらはこの問題を選択的受領と呼んでいる。

また、選択的受領によって、送信者は情報を受信者に提供したにもかかわらず、受信した証となる情報を受信者から得ることができないという意味での不公平な状況が生まれることになる。このような不公平な状況をどのようにして回避するかというテーマについて、既にさまざまな理論研究が行われている（詳細は3章1節）にて説明）。

5 タイムスタンプについては、IETFやISOにおいて標準の策定が進められている。IETF PKIXでは、タイムスタンプの生成の際にタイムスタンプの発行依頼者と発行者間で交信されるデータ・フォーマットを規定する標準の策定が進められている（Adams［2000］）。ISOでは、汎業界向けの情報セキュリティ技術の標準化を担当するSC27が、タイムスタンプ・プロトコルの基本的な枠組みや発行者の役割等を規定する国際標準案ISO18014の策定を進めている。

ロ．時刻情報の不正操作

ジョウらは、第2の問題点として、受信者が*NRDT*に含まれる時刻情報を正しく生成しない可能性がある点を指摘している。具体的には、受信者が、送信者から受け取ったメッセージの内容を確認し、その直後に*NRDT*を生成せず、後になって*NRDT*を生成するという不正行為である。たとえ*NRDT*に含まれる日時情報の生成をタイムスタンプ発行機関が行う場合においても、受信者がタイムスタンプで示される特定日時以前にデータを受け取っていたことが証明されるだけであり、実際にいつ受信者が受信したかを特定することは困難である。

また、同様の問題が、送信者のデータ送信時刻に関しても発生する。すなわち、送信者は、*NROT*に含まれる日時情報を不正に操作し、送信日時を実際よりもさかのぼって偽ることが可能である。タイムスタンプ発行機関を利用したとしても、タイムスタンプは送信者があるデータを特定日時よりも前に持っていたことを証明するのみであり、実際の送信日時は特定困難である。

3．各種プロトコルの理論研究動向

データ送受信証明プロトコルに関する最近の理論研究の動向をみると、代表的な研究テーマとして、「公平」なデータ交換を実現するプロトコル研究があげられる。これらの研究における「公平」とは、「送信者と受信者のいずれか一方がデータを相手に持ち逃げされて不利益を被る、という問題が発生しないこと」と定義される。公平なデータ交換を行うためのプロトコル研究は、①TTPを利用するプロトコルの研究と、②TTPを利用しないプロトコルの研究、の2つに分類される。

また、その他のプロトコルの中で近年注目されているものの1つとして、タイムスタンプ・プロトコルがあげられる。タイムスタンプ・プロトコルの分野では、「タイムスタンプの発行者はTTPである」という前提をはずした場合（TTPの信頼性の前提が崩れた場合）でも、タイムスタンプの安全性を確保できるような各種プロトコルが提案されており、その安全性評価に関する研究も進められている。以下では、最近のこれらの理論研究動向を紹介する。

(1) 公平な情報交換を行うためのプロトコルに関する研究

イ．TTPを利用するプロトコル

TTPを用いるプロトコルに関する研究は2つの方向に分けられる。1つは、送受信者が通信する際に必ずTTPを経由して行うプロトコルを対象とするものである。こうしたプロトコルの場合、交信データがすべてTTPを通過するため、データの送受信処理等の負荷がTTPに一極集中し、その処理速度が低下するという問題が存在する。したがって、TTPの関与をなるべく少なくし、TTPの処理の負荷を小さくすることが望ましい。このような観点から、第2の方向として、通常の送受信者間の通

信はTTPを経由せずに行い、送信者と受信者のどちらか一方が相手から受け取るはずの情報を受信できない等の問題が生じた場合にのみ、TTPを利用して不公平な状況を解消するというプロトコルに関する検討が行われている。

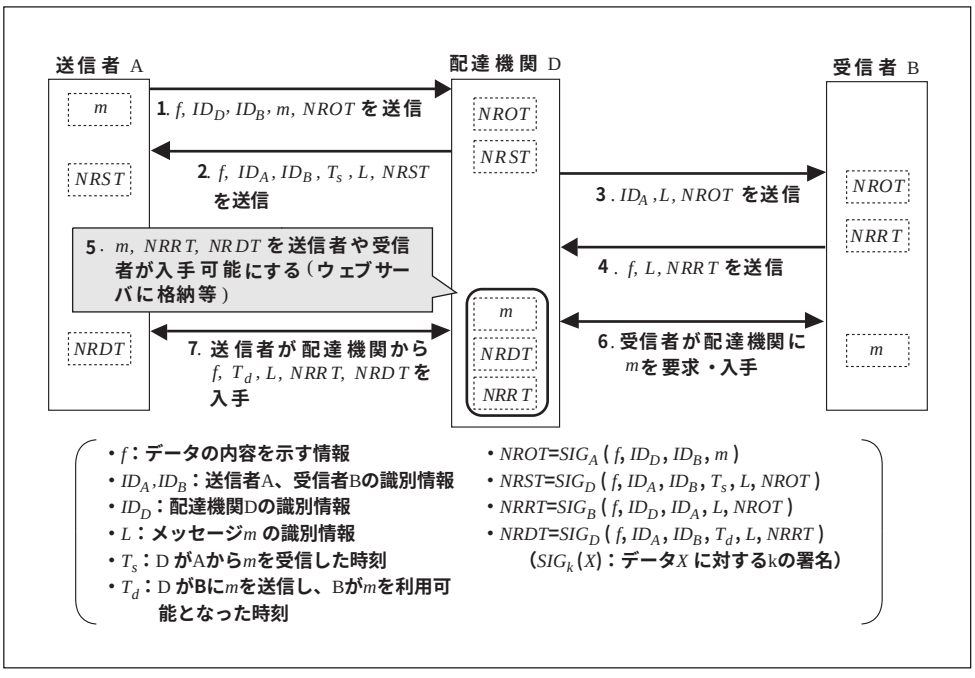
（イ）TTPが送受信データを中継するプロトコル

TTPが交信データを中継する代表的なプロトコルとして、ジョウ・ゴールマンのプロトコル（Zhou and Gollman［1997］）、佐本・中原のプロトコル（佐本・中原［1999］）があげられる。

①ジョウ・ゴールマンのプロトコル

本プロトコルの特徴は、TTPである配達機関が、メッセージmを送信する前に、mに対して一意に決定される識別情報Lを受信者に送信し、受信者からLに対するデータ受信証明トークン$NRRT$（non-repudiation of receipt token）を入手することによって、選択的受領を防止している点である。本プロトコルでは、受信者は、「自分がLに対応するmを入手できるようになった時点でmを受領したとみなす」ということを予め配達機関に対して承諾していることが前提となっている。受信者は、配達機関からLや$NROT$を受信し、mを入手するために配達機関に$NRRT$を送信する。配達機関は、受信者から$NRRT$を受信した後、Lを知っている者だけがネットワーク経由でmにアクセスできるようにする（例えば、アクセス制限を設けたうえでウェブサーバにmを格納する）。この時点で、受信者は配達機関からmを入手可能となり、

図8　ジョウ・ゴールマンのプロトコル



配達機関は、受信者が*m*を受領した証となる*NRDT*を生成する。配達機関は、*NRRT*や*NRDT*等についても、*m*と同様に、送信者がネットワーク経由で入手可能な状態にする。プロトコルの概要は図8のとおり。

配達機関Dは、受信者Bから*L*に関する*NRRT*が到達しない（手続4が完了しない）限り、受信者Bが*m*を入手できる状態にしない（手続5を実行しない）ことによって、受信者Bによる*m*の持ち逃げを防止する。また、本プロトコルでは、データの受領証明だけではなく、発信証明、提出証明、受信証明のトークンも生成され、これらの事実を証明することができる。

②佐本・中原のプロトコル

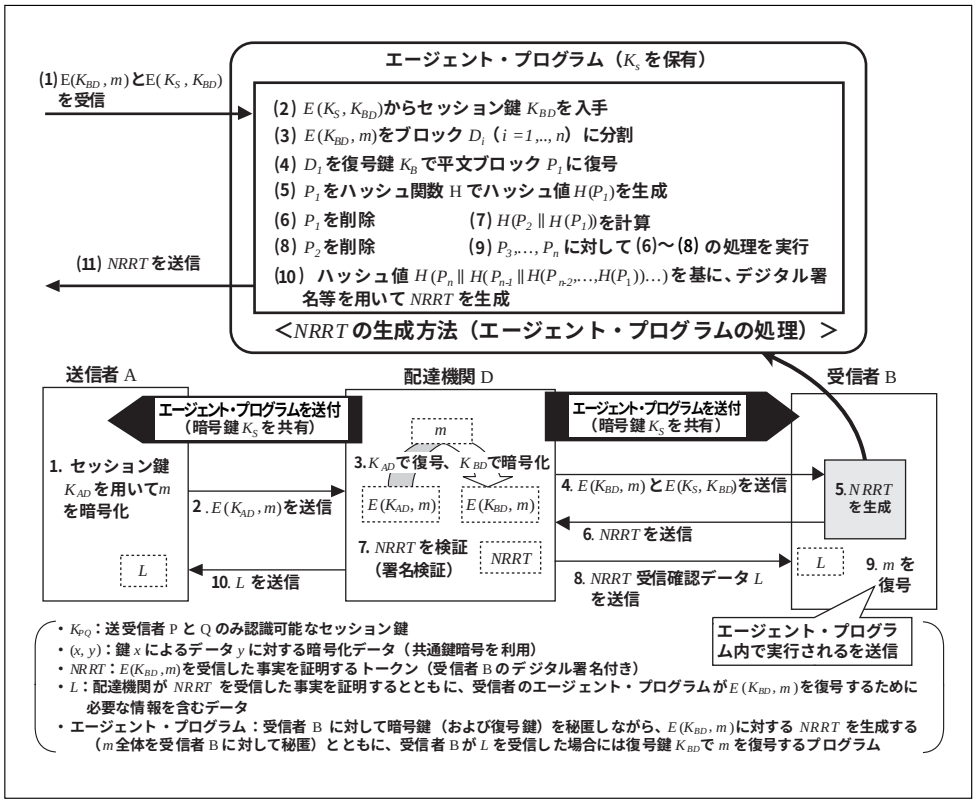
佐本・中原［1999］は、データの送受信における公平を「送信者と受信者のどちらか一方に不利益を生じることがない状態」とし、具体的には、「事実否認が発生しないこと」および「受信者がその電子データを受け取るだけで、電子データに対する対価を支払わないという状況に陥らないこと」としている。

このような条件を満足するために、本プロトコルでは、配達機関が送信者から送信されたデータ*m*を暗号化して受信者に送信し、受信者から受信証明トークン*NRRT*を受け取った後で、暗号化された*m*を復号するために必要な情報*L*（*NRRT*受理確認データ）を受信者に送信する、という手順を採用している。*NRRT*は*m*に依存したデータとなっており、受信者が*NRRT*を配達機関に送信することなく*m*を復号するという状況を避けるために、受信者が不正操作困難なエージェント・プログラムにおいて、*NRRT*の生成や配達機関への配送が行われる。エージェント・プログラム内で利用される復号鍵は、耐タンパー性を有するデバイスに格納されて受信者に配送され、受信者に対して秘匿される。本プロトコル全体の処理の流れは図9のとおり。

送信者Aと受信者Bは、最初に配達機関Dからエージェント・プログラムを受信する。配達機関Dは、送信者からセッション鍵K_{AD}で暗号化されたデータ*m*を受信した後、セッション鍵K_{BD}で暗号化しなおしたうえで受信者Bに送信する。*NRRT*の生成は、エージェント・プログラムにおいて実行され、暗号化された*m*を複数のブロックに分割し、平文*m*全体への復号が一度に生じないように各ブロックを順番に復号しながら、ハッシュ関数やデジタル署名を用いて行われる。配達機関は、*NRRT*を受信した後に、*NRRT*受理確認データ*L*を送信する。*L*を受け取った受信者は、エージェント・プログラムにおいて*m*の復号を行う。

本方式は、NTTの電子公証システムTrust-CYNOS（cyber notary system）に採用されており（竹内・村田［2000］、中原［2000］）、現在実装研究が進められている。

図９　佐本・中原のプロトコル

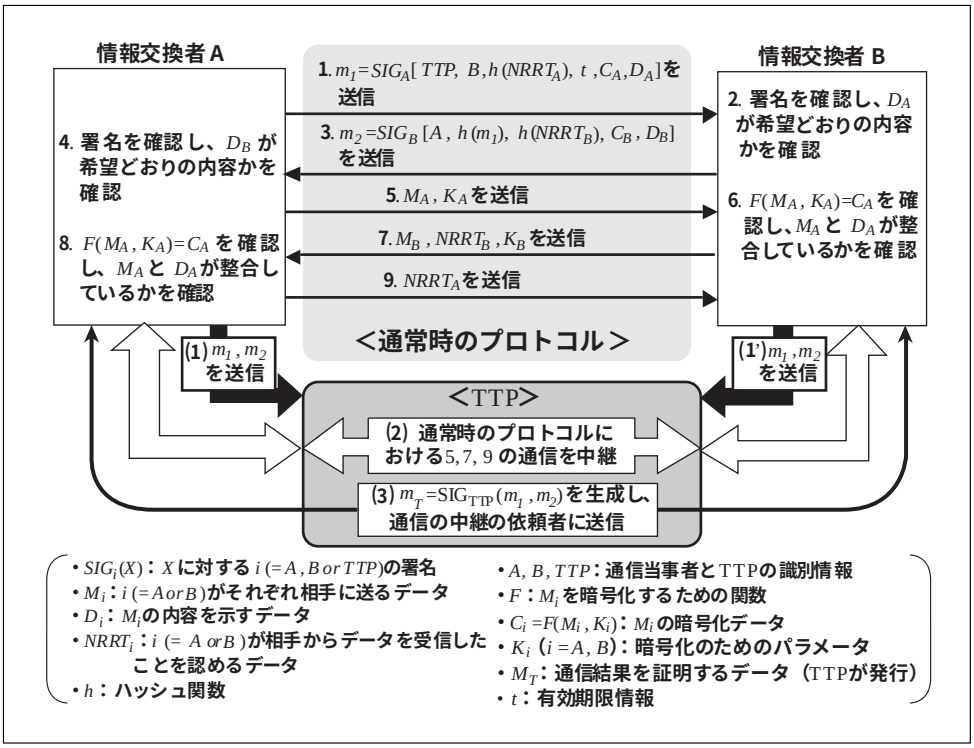


（ロ）不公平な状況が発生した場合にのみTTPを利用するプロトコル

二者間の情報交換において不公平な状況が発生した場合にのみTTPが関与するプロトコルとして、アソカン・シュンター・バイトナー（Asokan, Schunter and Waidner［1997］）のプロトコルがあげられる。本プロトコルは、二者間の公平なデータ交換を実現すると同時に、互いに相手から送信証明トークン*NROT*と受信証明トークン*NRRT*を入手可能にする。送信データが不正な場合や、どちらか一方がプロトコルの最中に処理を行わない場合、TTPは、通信者双方と交信してプロトコルを継続させ、不公平な状態を解消するほか、プロトコルが正常に終了しなかった場合、その事実を証明するトークンを生成する。本プロトコルの概要は図10のとおり。

情報交換者双方は、まず、暗号化された交換対象データやその内容を表すデータ等にデジタル署名を添付して、相手に送信する。最初にデータを送信する者は、プロトコルの有効期限に関する情報や、不都合が生じた際に利用するTTPの識別情報も相手に送信する。プロトコルの有効期限を定めるのは、相手が意図的にプロトコルの処理を実行せず、プロトコルが長時間中断する状況を回避するためである。次に、情報交換者は、交換対象データとその暗号化に利用されたパラメータをそれぞれ相手に送信し、最初に受信した暗号化データとの整合性を確認する。そのうえで、互いに交換対象のデータを受信した証として、*NRRT*を送信する。

図10　アソカン・シュンター・バイトナーのプロトコル



このプロトコルの最中に、一方の情報交換者が、交換対象となるデータとそれを暗号化する際に利用したパラメータを相手に送信した結果、その相手から何らデータを受信できない（例えば、図10の手続7が実行されない）場合を考える。このようなケースでは、不公平な状況に陥っている者が、予め決めていたTTPに情報の仲介を依頼する。TTPは、情報交換者間の通信を中継し、中断されていたプロトコルを継続するように機能する。その場合でも、情報交換者の一方がプロトコルの有効期限中にデータを返信しない際には、プロトコルはその時点で終了し、TTPは、「プロトコルが正常終了しなかった」ことを示す情報を生成する。

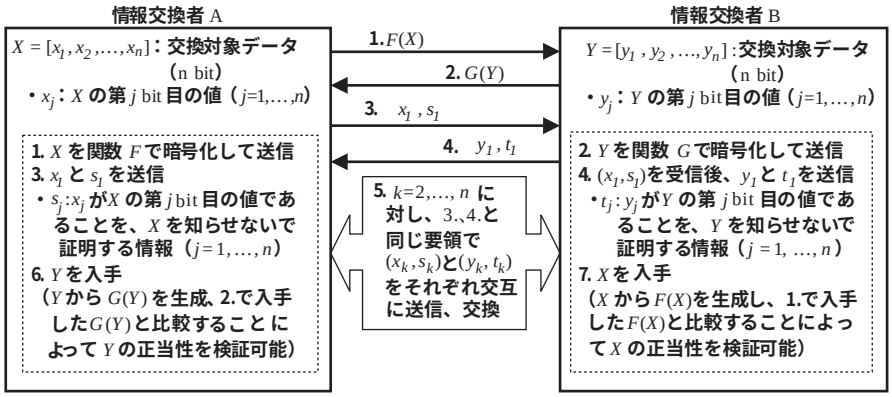
このほか、アソカンらは、上記プロトコルを拡張し、デジタル署名を公平に交換するプロトコル（Asokan, Shoup and Waidner［1998, 1999］）を提案している。これらの研究は、欧州議会傘下のプロジェクトSEMPER[6]において活用されており、同プロジェクトの実証実験に採用されている（SEMPER Consortium［1996］、Lacoste［2000］）。

6 SEMPER（Secure Electronic Marketplace for Europe）：1995年9月から2000年5月にかけて実施された欧州域内の電子商取引に関する実証実験プロジェクト。インターネット上において、安全かつ公平な商取引を実施するために必要な技術的要件の検討や技術研究・開発が行われた。特に、公平なデジタルデータの交換をどのようにして実現するかが第一の技術的要件として位置づけられた。本プロジェクトには、フランス（フランステレコム）、ドイツ（コメルツ銀行）、スイス（IBMチューリヒ研究所）、ベルギー（バンクシス）等欧州7カ国の企業が参加した。

ロ．TTPを利用しないプロトコル

一方、TTPを利用しないプロトコルの研究も進められている。TTPを利用するプロトコルの場合、その安全性や効率性はTTPの業務運営状況に大きく依存するため、TTPを利用しないで公平なデータ交換ができないかという問題意識によるものである。ただし、TTPを利用しない場合には、送信者がデータ全体を一度に受信者に送信すると、そのデータを受信者に持ち逃げされる可能性が生じる。そこで、データ全体を一度に交換するのではなく、交換対象のデータを細かく分割したデータをそれぞれ交互に送信することによって、情報交換者のどちらか一方だけが相手のデータ全体を持ち逃げすることを困難にする、という「段階的秘密交換プロトコル（gradual secret exchange protocol）」が研究されている（代表的な研究成果として、Even, Goldreich and Lempel［1985］、Brickell *et al.*［1987］、Cleve［1989］、Damgård［1993］、Okamoto and Ohta［1994］があげられる）。段階的秘密交換プロトコルの概要は図11のとおり。

図11　段階的秘密交換プロトコル



（*F*,*G* については、逆関数を求めることが同程度に困難な関数とする）

まず、情報交換者AとBは、交換対象データXとYをそれぞれ$F(X)$と$G(Y)$に暗号化して相手に送信する。XとYがそれぞれn bitのデータであるとし、XとYの第i bitデータをそれぞれx_iとy_i（$i = 1, ..., n$）とする。Aは、「x_iがXの第i bit目のデータである」ことを証明するデータs_iを生成し、(x_i, s_i)をBに送信する。Bは、x_iがXの第i bit目のデータであることを確認したうえで、「y_iがYの第i bit目のデータである」ことを証明するデータt_iを生成し、(y_i, t_i)をAに送信する。データs_iとt_iの構成方法については、紛失通信[7]を用いた方法（Even, Goldreich and Lempel［1985］）や一方向性関

7 紛失通信（oblivious transfer）：受信者は一定の確率Pでデータを受信できるが、送信者は受信者がそのデータを受信したかどうかを確認することができない、という性質を持つ通信方法。

数に基づく方式（Okamoto and Ohta［1994］）等が提案されている。上記の要領でXとYは1 bitずつ交互に送受信され、プロトコルが最後まで正常に行われると、AとBはそれぞれYとXを入手できる。

本プロトコルでは、例えば、BがAからx_i（$1 \leqq i \leqq n$）を入手したままAにy_iを送信しない場合、BはAよりも1 bit多くデータを入手することができる。しかし、両者が得たデータ量の差はたかだか1 bitであるため、AとBが同じ計算能力を持つと仮定した場合、Bがそれまでに得たデータからXを計算するためにかかる時間は、AがYを計算する時間のたかだか2分の1である。したがって、Bが一方的にXを得ることは困難であり、データ交換における公平性が確保される。ただし、データの交換が1 bitずつ実行されることから、大量のデータを交換するときには、効率的とはいえないケースがある。

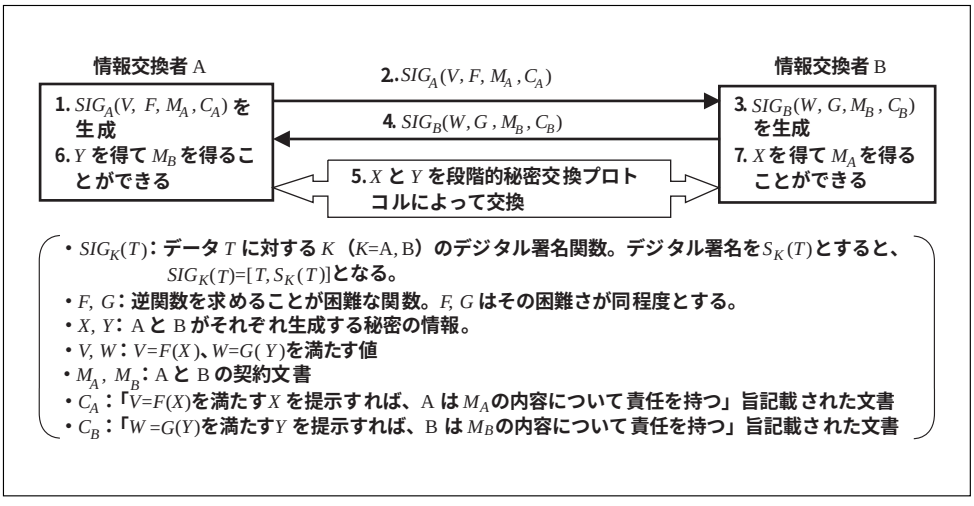
この段階的秘密交換プロトコルの代表的な応用例として、同時契約交換プロトコル（Even, Goldreich and Lempel［1985］）や、送達確認電子メール（certified electronic mail、Goldreich［1982］）があげられる。これらのプロトコルの概要は以下のとおり。

①同時契約交換プロトコル

契約文書を交わしたいAとBは、それぞれ契約文書M_AとM_Bに自分のデジタル署名を付けて、相手の署名付き契約文書を受け取る前に自分の署名付き契約文書を相手に持ち逃げされることがないように交換したい。このような場合に利用されるのが同時契約交換プロトコルである（図12参照）。

本プロトコルのアイデアは、まずAとBが、それぞれ相手にデータX、Y（XとYは同一サイズのデータ）を提示した場合に契約を締結する旨を記載した文書を契約文書とともに送信し、その後段階的秘密交換プロトコルによってデータX、Yを交換

図12　同時契約交換プロトコル



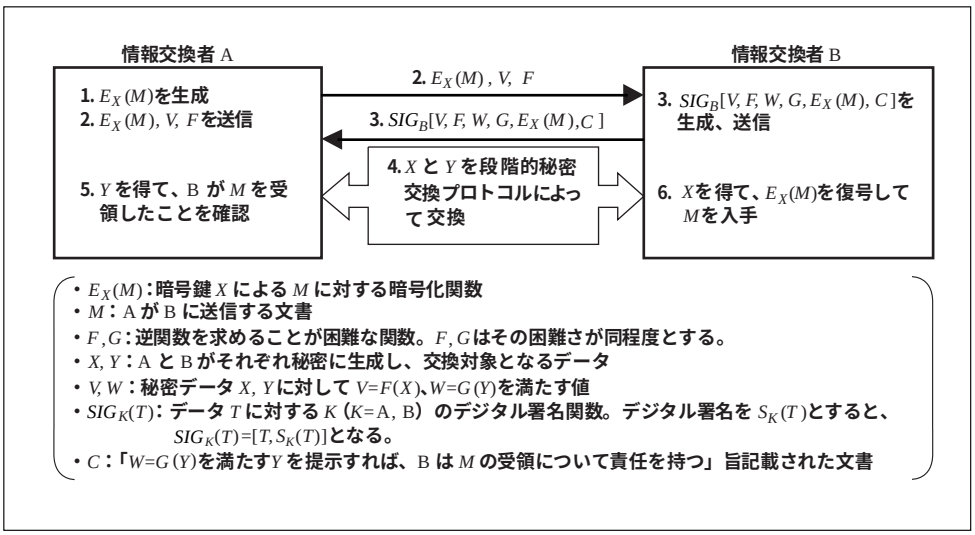
する、というものである。例えば、Aが手続5.の途中でプロトコルを中止し、Bが得たXよりもYを1 bitだけ余計に入手することができたとしても、AがY全体を得るために必要となる計算量は、BがX全体を得るための計算量よりもたかだか2分の1にすぎず、AとBが同程度の計算能力を有するという前提のもとでは、Aが一方的にYを得ることは困難である。

②送達確認電子メール

AがBに文書Mを送信し、BはMを受信したことを認めるデジタル署名SをAに送信する場合を考える。送達確認電子メールは、AがSを入手する前にMをBに持ち逃げされたり、BがMを入手する前にSをAに持ち逃げされることを防ぐことを特徴とする。このために、まずAはMを暗号鍵Xで暗号化したデータをBに送信し、これに対してBは「あるデータYを提示した場合にのみMの受領を認める」旨を内容とする文書Cにデジタル署名を添付してAに送信する。そのうえで、AとBがXとYを段階的秘密交換プロトコルによって交換する。本方式の概要は図13のとおり。

本方式において、例えば手順4. でAが途中で処理を中断した場合、AはBの受領確認を得るために必要なデータYに関して既にBに送信したXよりもたかだか1 bit 多く入手できるにすぎず、AとBが同程度の計算能力を有するという前提のもとでは、Aだけが一方的にY全体を入手することは困難である。

図13　送達郵便電子メール



（2）タイムスタンプ・プロトコルに関する研究

タイムスタンプ・プロトコルについては、タイムスタンプ発行機関がTTPであることを前提とする簡素なプロトコルがISO13888において規定されている（これをsimple protocolと呼ぶ）。一方、タイムスタンプ発行機関がTTPではない（十分に信頼でき

ない）場合でも、タイムスタンプの安全性を確保するためにはどのような仕組みが必要か、という観点からも研究が進められており、これまでに連鎖型プロトコル（linking protocol）と分散型プロトコル（distributed protocol）の2種類が提案されている。

イ．連鎖型プロトコル

連鎖型プロトコルは、他のタイムスタンプに含まれる情報を用いてタイムスタンプを生成する方式であり、タイムスタンプを時系列的に結び付ける連鎖情報（linking information）と呼ばれるデータを利用する形態が一般的である。連鎖情報は、タイムスタンプが生成されるたびに生成され、対応するタイムスタンプに含まれる情報（例えば、タイムスタンプ対象データのハッシュ値や時刻情報）と直前の連鎖情報等から、一方向性ハッシュ関数によって生成される。また、タイムスタンプ検証時には、連鎖情報が正しく再生されるか否かが確認される。ハッシュ関数が安全であり、再生した連鎖情報が正しいか否かを確認するための情報（以下、検証情報）を改ざん困難な状況で保管する場合、タイムスタンプ発行機関を十分信頼できなくても、タイムスタンプの改ざん等不正行為は極めて困難であると考えられる。

タイムスタンプ発行機関による検証情報の改ざんを困難にする方法として、これまでに以下の2つの方法が提案されている。

①検証情報を大勢の人々の目に触れるメディア（新聞等）に掲載する。
②複数のタイムスタンプ発行機関の存在を前提とし、検証情報を適宜他のタイムスタンプ発行機関に送信してタイムスタンプを入手する。

前者の方法を採用した主なプロトコルとして、ベイヤー（Bayer）らのプロトコル（Bayer, Haber and Stornetta［1992］）、エストニアの国家プロジェクトの成果として提案されたCuculus（Buldas *et al.*［1999］）[8]、ベルギーの国家プロジェクトの成果として提案されたTIMESEC（Quisquater *et al.*［1999］）があげられる。また、後者を用いたプロトコルとして、欧州議会傘下のプロジェクトの成果として提案されたPKITS（Fabrica Nacional de Moneda y Timbre［1998］）があげられる。

ロ．分散型プロトコル

分散型プロトコルのアイデアは、個々のタイムスタンプ発行機関を信頼できなくても、多数のタイムスタンプ発行機関が結託する可能性は比較的小さいと考えられるため、一定数のタイムスタンプ発行機関が結託しない限り安全なタイムスタンプを構成するというものである。このため、実装には複数のタイムスタンプ発行機関が必要となる。代表的なプロトコルとして、秘密分散技術を利用したNTTの分散時

8 エストニアのプリバドール（Privador）社（http://www.privador.com/）は、現在タイムスタンプ機能付き公開鍵インフラ・システムTrueSignの開発を進めており、そこで利用されるタイムスタンプ・プロトコルの原型としてCuculusが採用されている（Privador［2000］）。

刻署名システム（Takura, Ono and Naito［1999］）があげられる。本プロトコルでは、一定数以上のタイムスタンプ発行機関の署名が集まらないとタイムスタンプを生成できず、逆に一定数より少ない数のタイムスタンプ発行機関が結託してもタイムスタンプを偽造・改ざんすることが困難である。

ハ．プロトコルの安全性評価

タイムスタンプ発行機関への信頼に関する要件を緩和するために、連鎖型プロトコルをはじめとしてさまざまなプロトコルが提案されている。このため、プロトコルの形態が多様化しており、各種プロトコルの安全性を体系的に評価するためには、プロトコルの概念整理から検討を行うことが必要となっている。このような問題意識に基づき、宇根・松本［2000a, b］は、タイムスタンプ・プロトコルの概念整理およびプロトコルの分類方法を提案しており、一部のプロトコルについて安全性の評価を実施している。これらの研究成果については、5章で説明する。

4．実装研究および商用サービス動向

（1）海外の動向

海外では、電子文書の送受信証明プロトコルに関する実証実験に加え、既にいくつかの商用サービスが開始されている。いずれの実証実験および商用サービスにおいても、TTPが利用されている。

代表的な実証実験として、欧州議会のプロジェクトSEMPERやスイフト（SWIFT）[9]のデータ送受信証明サービスTrustActのほか、タイムスタンプ・プロトコルの実証実験として、PKITS（スペイン）、TIMESEC（ベルギー）、Cuculus・TrueSign（エストニア）があげられる。

一方、商用サービスに関しては、データ送受信証明サービスとして、米国郵便公社（USPS：United States Postal Service）の$Post_e$CS、米UPS社のUPS Document Exchange、米ヒルグリーブ（Hilgraeve）社のHyperSend等があげられる。タイムスタンプ・サービスに関しては、シュアティ・ドット・コム（Surety.com）社のDigital Notary、米ドキュメント・オーセンティケーション・システムズ（Document Authentication Systems）社、米タイムスタンプ・ドット・コム（Timestamp.com）社、米ファーストユース・ドット・コム（Firstuse.com）社等もサービスを提供している。また、データ保管サービスとしては、米ザンタス（ZANTAZ）社、米ユーザートラスト（USERTrust）社、米オーセンティデート・ドット・コム（AuthentiDate.com）社等

9 SWIFT（Society for Worldwide Interbank Financial Telecommunication）：クロスボーダー銀行取引におけるペーパーレス化を、同一のネットワーク、標準化された手続により推進することを目的として1973年に欧米15カ国239銀行の出資によって設立された非営利協同組合（本部はベルギー）。日本の金融機関は1976年より参加している。

もサービスを展開している。金融分野における電子文書の送受信証明プロトコルの例として、全米証券業協会（NASD：The National Association of Securities Dealers）のOATS（Order Audit Trail System）があげられる（NASD Regulation［1999］）。

これらの実証実験および商用サービスのうち、スイフトのTrustAct、米国郵便公社の$Post_e$CS、全米証券業協会のOATSの概要を紹介する。

イ．スイフトのTrustAct

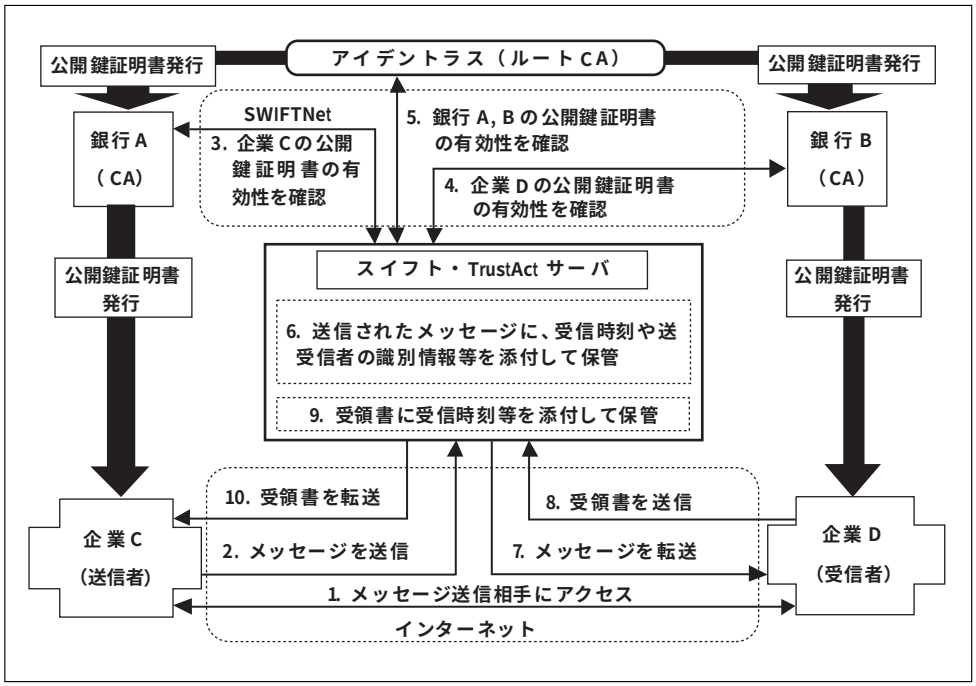
TrustActは、スイフトが米アイデントラス（Identrus）社[10]と共同で開発を進めている企業間データ配達サービスであり、ISO13888で規定される提出・転送・受領証明に対応するサービスを提供することが目的である。TrustActでは、スイフトが配達機関の役割を果たし、送受信者の本人確認を行ったうえで受信者にデータを転送するとともに、その際にデータの送受信証明に必要な各種トークンを生成、保管する。現時点では、本サービスを利用できるのはアイデントラス社がルートCAとなる公開鍵インフラに認証機関として参加する銀行から公開鍵証明書を取得している企業のみであり、スイフトは、データを中継する際にこの公開鍵証明書を用いて送受信者の本人確認を実行する仕組みとなっている。本人確認の際に利用されるネットワークは、スイフトが開発を進めているクローズドなネットワークSWIFTNet[11]が予定されている。TrustActにおける利用者のメリットとしては、電子商取引の際に必要な本人確認をスイフトが利用者に代わって実行してくれることや、スイフトが利用者に代わってデータの提出・転送・受信証明トークンを生成、保管してくれること等があげられる。TrustActにおける企業間データ送受信の手順を説明する（図14参照）。

送受信者となる企業CおよびDは、まず、それぞれアイデントラス社（ルートCA）より公開鍵証明書を入手している銀行AとB（いずれもCA）から公開鍵証明書を入手していることを前提とする。そのうえで、送信者である企業Cは、売買注文や伝票等のデータをスイフトのTrustActサーバ（以下、サーバ）に送信する。サーバは、企業C、Dの公開鍵証明書の有効性をそれぞれ銀行A、Bに確認する。次にサーバは、企業Cから受信したデータに受信時刻情報や送受信者の識別情報等のデータを添付して保管し、企業Cから受信したデータを企業Dに転送する。企業Dは企業Cからのデータを受領した旨を記載した受領書をサーバに送信し、サーバは、受信時刻等を受領書とともに保管した後、企業Cに転送する。後日、企業CとDとの間で取引の事実に関する問題が発生した場合、サーバにおいて記録されているデータを確認することによって、その事実の真偽を確認する。

10 アイデントラス（identrus）社：1999年3月に設立された、公開鍵インフラをベースとした電子認証サービスを提供する会社。同社は、米エントラスト（Entrust）社、米ボルチモア・テクノロジーズ（Baltimore Technologies）社、米コンパック（Compaq）社等と技術提携しており、同社がルートCAとなって参加金融機関（2000年9月時点で35社）に公開鍵証明書を発行し、各金融機関が認証機関としての業務を実施可能にする。

11 SWIFTNet：スイフトが現在検討を進めている次世代ネットワークであり、TCP/IPを通信プロトコルとして採用するほか、公開鍵インフラ（スイフトがCAの役割を果たす）を利用した情報セキュリティ対策を装備する等の特徴を有している。

図14　スイフトのTrustAct



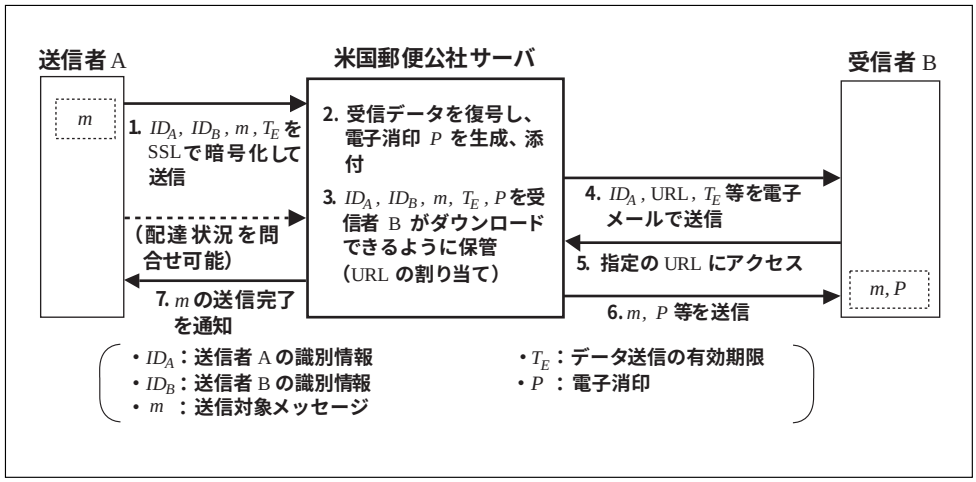
現在、スイフトはTrustActの実証実験を進めており、2001年中のサービス開始を目指している。

ロ．米国郵便公社のPost$_e$CS

米国郵便公社のPost$_e$CS は、インターネット経由でのデータ配達証明サービスであり、米国郵便公社のサーバ（以下、サーバ）が通信データを中継し、送信者が特定の受信者宛にデータを送信した事実や、指定されていた受信者がデータを受け取った事実を証明することを目的としている。また、送信者は、データの配達状況を米国郵便公社のウェブサイト経由で随時確認することが可能であり、受信者がデータを受け取っていないうちにデータの送信を取りやめることも可能となっている。また、送信者はデータの受信期限を設定することもできる。

サーバは、SSL（Secure Sockets Layer）によって暗号化された送信データを復号した後、受信時刻情報を含むタイムスタンプとして電子消印（Electronic Postmark）Pを生成・添付し、保管する（図15参照）。電子消印は、送信データのハッシュ値に時刻情報を結合したものに対するデジタル署名として生成される。サーバは、送信データの保管場所を示すURL、送信者の識別情報、データ入手可能期限T_E、データにアクセスするための情報等を含む電子メールを暗号化し、受信者に送信する。受信者は、指定されたURLにアクセスして送信データmを入手することができる。この結果、受信者がいつデータを入手したかが明確となり、データ受信証明が可能となる。最後にサーバは、受信者がmを入手した事実を送信者に伝える。

図15　米国郵便公社のPosteCS



本サービスでは、データの提出・転送証明のトークンは生成されないものの、サーバから受信者に送信される電子メールがデータ提出証明のトークンに相当すると考えることができるほか、最後に米国郵便公社から送信者に送られる通知のデータがデータ転送証明のトークンに相当すると考えることができる。

ハ．全米証券業協会のOATS

OATSは、全米証券業協会が、ナスダック市場での証券取引の源となる各種取引指図に関する情報（全米証券業協会会員証券会社に顧客から寄せられる売買注文、注文変更、キャンセル等の情報）を、取引当事者や取引時刻等のデータとともに電子媒体で保管するシステムである。OATSのプロジェクトは、1996年8月、米国証券取引委員会（SEC：The Securities and Exchange Commission）がナスダック市場での証券取引の監視を強化する目的で全米証券業協会規則を改正したことが契機となっている。OATSのシステムは、1999年3月1日より、顧客から会員証券会社にオンラインで寄せられた取引情報を対象に運用が開始されており、顧客から紙面で寄せられた取引情報についても、今後適用対象となる予定である。

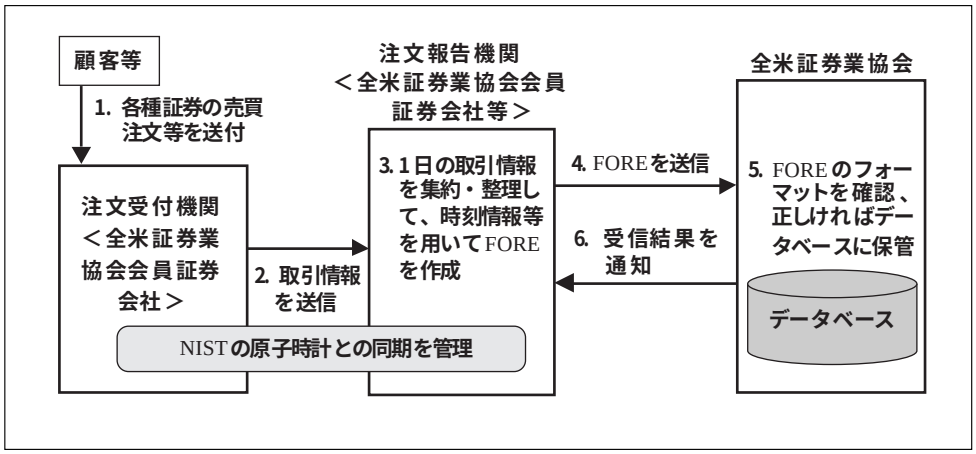
OATSによる取引情報の保管は、以下の手順で行われる（図16参照）。顧客から証券取引に関する各種注文を受けた注文受付機関（ORF：order receiving firm）は、時刻情報等とともに取引の内容を注文報告機関（OSO：order sending organization）に送信する。注文報告機関は、各種取引情報を集約し、会員証券会社の識別情報、取引が発生した時刻に関する情報（秒単位）、取引内容に関する情報等を含むデータFORE（firm order report file）を作成する。注文報告機関は、毎日最低1回、専用回線もしくはインターネット経由でFOREを全米証券業協会に送信する。FOREは、（例えば火曜日の）ナスダック市場の取引終了時刻の1秒後（火曜日の16:00:01）から翌日（水曜日）のナスダック市場の取引終了時刻（水曜日の16:00:00）の間に行われたあらゆる取引に関する情報を含んでおり、注文報告機関は、このFOREを

翌々日（木曜日）の4:00:00までに全米証券業協会に報告することが義務づけられている。全米証券業協会は、受信したFOREのフォーマットを確認したうえで、FOREをデータベースに保管するとともに、その結果を1時間以内に注文報告機関に通知する。

注文受付機関や注文報告機関は、最終的に全米証券業協会に送信されたFOREに含まれる時刻情報とNISTの原子時計との誤差が3秒以内になるよう、時刻生成装置の精度を管理することが要求されている。

このように、OATSは、特定の主体が特定時刻に特定の行為を行ったことを証明するものであり、ISO13888の送受信証明の枠組みに照らし合わせると、公証サービスの一種として位置づけることができる。

図16　全米証券業協会のOATS



（2）わが国の動向

わが国では、いくつかの実証実験が進められているものの、既に開始されている商用サービスはごく一部である。これらに採用されているプロトコルは、いずれもTTPを用いたものである。

まず、実証実験の対象となっているシステムをみると、各産業分野における電子データ交換（EDI：Electronic Data Interchange）のシステムに電子文書の送受信証明機能を組み込んだタイプのものがほとんどである。代表的な実証実験として、貿易金融EDIに関する検討（広瀬・山崎・佐藤［1999］、ECOM［2000］）があげられるほか、情報処理振興事業協会のエレクトロニック・コマース推進事業（1995年度補正予算）や電子商取引共通基盤整備事業（1996年度補正予算）の一環として実施された各種実証実験があげられる。情報処理振興事業協会関連の実証実験の代表例として、リース会社とその代理店間でのデータ通信における送受信証明機能を備えたシステムに関する検討（多田［1998］）等があげられる。一方、特定のアプリケーションを前提とせず、各種データの送受信証明を実現する汎用的なシステムに関す

る実装研究も一部ではあるが進められており、郵政省の電子内容証明サービス実験[12]や、NTTの電子公証システムTrust-CYNOSの実装研究があげられる。

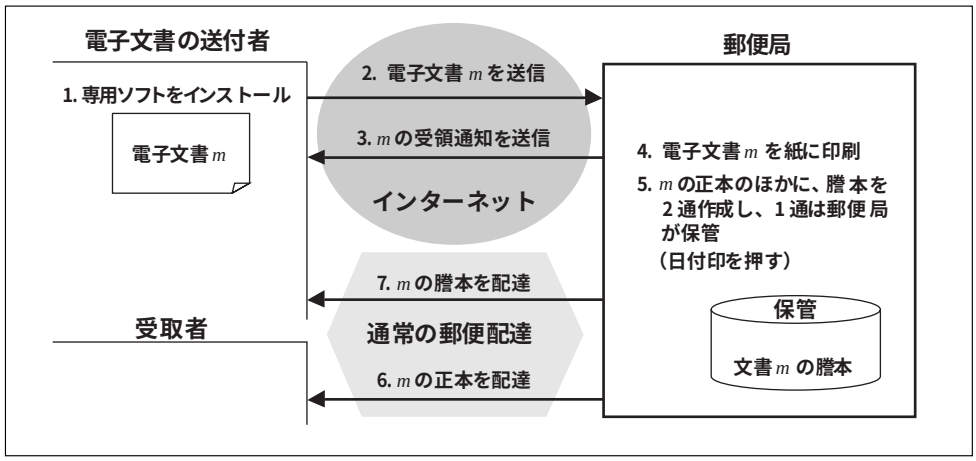
商用サービスについては、データ配達証明のサービスの提供事例は現時点では見当たらない。これに対して、タイムスタンプ・サービスについては、NTTデータがSecureSealというサービスを2000年4月より開始しているほか、現在検討が進められているものとして、法務省の電子公証制度（法務省［1998］、原［2000］）があげられる。その他、データ保管サービスに関しては、富士通のセキュア・アーカイバ（黒田ほか［1998］）をはじめとしていくつかの商用サービスが開始されている（森［2000］）。

以下では、郵政省の電子内容証明サービス実験と、NTTデータのSecureSealの概要について説明する。

イ．郵政省の電子内容証明サービス実験

電子内容証明サービス実験は、送付者が郵便物を郵便局に持参して内容証明郵便サービスを受ける代わりに、送付者がインターネット経由で郵便局（新東京郵便局）に電子文書を送信し、郵便局が電子文書をプリント・アウトして内容証明郵便の処理を行ったうえで郵便物を受取者に配達する、というものである（図17参照）。本実験は2000年3月中に既に行われており、「はいぶりっどメール」[13]に内容証明処理を追加する形で、2001年2月1日から実サービスが開始されている。

図17　電子内容証明サービス実験



12 詳細については、郵政省のサイトhttp://www.mpt.go.jp/pressrelease/japanese /yubin/000605j201.htmlを参照。

13 はいぶりっどメール：郵便業務における①手紙やはがきの投函、②郵便局間の文書転送、③指定された受取者への配達、というプロセスのうち、①の手続を、利用者が自宅や企業のパソコンから電子文書を郵便局（新東京郵便局）へインターネット経由で送信するという手続に置き換えたサービス。電子文書を受け取った郵便局は、最寄りの郵便局（現在は全国12の郵便局に限定）に電子文書を転送し、その後電子文書はプリント・封緘・配達される。印刷された電子文書は削除される扱いとなっている。詳細は、http://www1. hybridmail.go.jp/を参照。

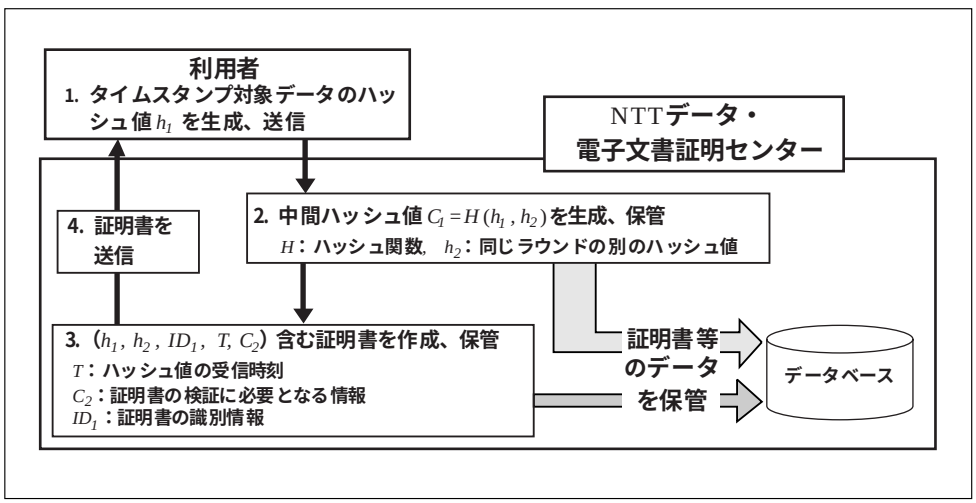
本サービス実験では、電子文書を受信した郵便局は、受領通知をインターネット経由で送付者に送信した後、通常の内容証明郵便と同様に、指定された受取者に配達する正本を作成するほか、送付者宛および郵便局保管分の謄本を合計2通作成する。この結果、正本および謄本には日付印（法律上の確定日付となる）が押され、文書の送信・提出・転送・受信の事実が証明される。

なお、電子文書の送付者と郵便局との間で交信されるデータは、実験では専用ソフトウェアによって暗号化されていたが、「はいぶりっどメール」ではSSLによって暗号通信が行われているため、内容証明郵便サービスが実用化される際には、専用ソフトウェアではなくSSLによる暗号通信が行われるとみられる。

ロ．NTTデータのSecureSeal

SecureSealは、特定のデータが特定時刻に存在したことを証明するものであり、米シュアティ・ドット・コム社のサービスDigital Notaryと同じシステムによって運用されている[14]。SecureSealの主な特徴は、タイムスタンプの検証を全面的にタイムスタンプ発行機関に依存している点である。検証者は、タイムスタンプを検証する場合、NTTデータの電子文書証明センター（以下、センター）にタイムスタンプを送信し、センターは検証者に検証結果のみを送信する。ただし、センターが適切に運営されていることを確認するための情報として「集約ハッシュ値」と呼ばれるデータが、毎週金曜日に日経産業新聞エレクトロニクス面に掲載される。集約ハッシュ値は、1週間センターが受信したすべてのタイムスタンプ対象データ（ハッシュ値）から生成される。まず、タイムスタンプに相当する証明書の生成手続は以下のとおり（図18参照）。

図18　SecureSealにおける証明書の生成手順

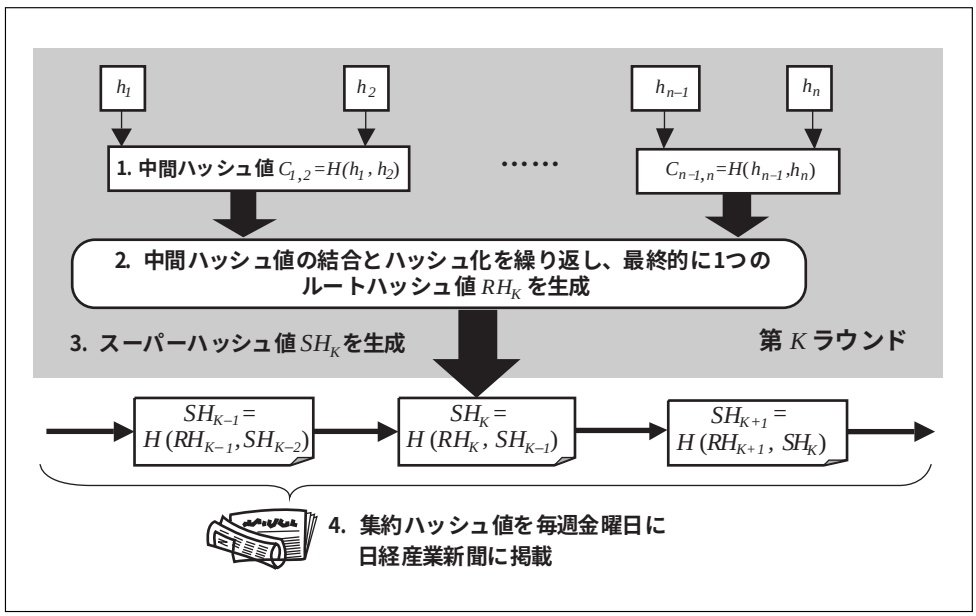


14 NTTデータのサイト（http://www.nttdata.co.jp/）およびSurety.com社のサイト（http://www.surety. com/）を参照。

1. 利用者は、専用ソフトウェアを利用してタイムスタンプの対象となる文書のハッシュ値h_1（ハッシュ長は288 bit）を生成し、NTTデータの電子文書証明センターに送信。
2. センターは、h_1と同じラウンド（ラウンドは1秒ごとに更新される）で受信した別のハッシュ値h_2を利用して中間ハッシュ値C_1（ハッシュ長は288 bit）を生成し、データベースに保管。
3. センターは、（h_1, h_2 ID_1, T, C_2）を内容とする証明書を生成し、データベースに保管。なお、Tはハッシュ値の受付時刻情報、C_2は証明書の検証に必要な情報（時刻Tにおける他の中間ハッシュ値や、後述するルートハッシュ値等が含まれる）、ID_1は証明書の識別情報。
4. センターは、証明書を各利用者に送信。

このようにして生成される証明書は、スーパーハッシュ値と呼ばれる情報によって時系列的に関連づけられる。スーパーハッシュ値の生成方法は図19のとおり。

図19　第Kラウンドにおけるスーパーハッシュ値の作成方法



1. 第Kラウンド内に受信したハッシュ値（h_1,...,h_n）（288 bit）を2組ずつ結合・ハッシュ化し、288 bitの中間ハッシュ値（$C_{1,2}$,...,$C_{n-1,n}$）を生成。
2. 複数の中間ハッシュ値を再び結合・ハッシュ化し、最終的に288 bitのルートハッシュ値RH_Kを生成。
3. 第Kラウンドのルートハッシュ値RH_Kと、第$K–1$ラウンドのスーパーハッシュ値SH_{K-1}を結合・ハッシュ化して、第Kラウンドのスーパーハッシュ値SH_Kを生成。

4. スーパーハッシュ値は、センターのデータベースに記録され、1週間分のスーパーハッシュ値が結合・ハッシュ化されて集約ハッシュ値が生成される。集約ハッシュ値は毎週金曜日に日経産業新聞[15]に掲載される。

SecureSealでは、証明書の検証はセンターによって実行される。検証者は、検証対象の証明書をセンターに送信する。証明書を受信したセンターは、自分のデータベースの情報を基に証明書の一貫性を検証し、検証結果を検証者に回答する。

(3) 残されている検討課題

データ送受信証明のプロトコルは、理論・実証両面で検討が進められており、既に一部では商用サービスが開始されている。しかし、それらのサービスは、現時点では幅広い分野において利用されるまでには至っていない。今後サービスの普及に向けて検討が必要になると考えられる主な技術的課題として、次の3つがあげられる。

①TTPの業務要件の確立と適正な管理・運営体制の維持

既存の実証実験や商用サービスでは、交信データを中継する配達機関等がTTPとして適切に業務を遂行することが前提となっている。したがって、TTPとしての業務要件を明確にしたうえで、それらを常に満足できるように管理・運用体制を整備・維持することが必要となる。

このような業務要件の明確化については、わが国ではECOM等で検討が進められている[16]ほか、ISOにおいても汎用的なTTPに関するガイドラインの策定[17]が進められている。これらの検討結果や各種標準に基づいて、具体的にどのようにサービスの管理・運営を行えばよいかを今後明確化していく必要がある。

②各種プロトコルの安全性の確保

送受信証明の各種プロトコルにおける安全性の確保も課題である。既存の実証実験や商用サービスではTTPの利用を前提としており、そのようなプロトコルにおいては、まず、TTP自体の信頼性を前提とした場合に十分な安全性を確保できるようにセキュリティ対策を講じることが必要であることは、当然である。

しかし、TTP自体に何らかのセキュリティ侵害が生じる可能性がないわけではない。したがって、「TTPが信頼できる」という前提が崩れた場合においても、プロトコルの安全性に対する信頼が揺らぐことのないように予めセキュリティ対策を講じておくことが望ましい。

15 ちなみに、Digital Notaryでは、集約ハッシュ値が毎週日曜日にニューヨーク・タイムズ紙に掲載される。
16 例えば、ECOMの電子公証システムガイドライン（電子商取引実証推進協議会［1998］）があげられる。
17 TTPの業務内容に関する指針として、ISO14516の策定が進められている。

また、電子文書の送受信証明には、後々の係争や情報公開等に備えて電子文書や各種トークンを数十年という長期間保管しておくことが求められる。送受信証明プロトコルに利用されるデジタル署名やハッシュ関数等暗号技術の安全性は時間の経過とともに徐々に低下するものであり、電子文書に関する各種証明が必要となる時期が到来する前に、暗号技術の安全性が十分なものではなくなる可能性がある。この他、サービスを利用した時点では十分な安全性が確保されているとみられた暗号技術であっても、その後強力な暗号解読法が発表され、十分な安全性を維持できなくなる可能性もある。

このように、TTPの利用を前提とするプロトコルであっても、TTPの前提が崩れた場合や、採用されていた暗号技術の安全性が低下した場合も考慮してセキュリティ対策を検討することが求められる。

③利用者にとって利便性と透明性の高いサービスの確立

電子文書の送受信証明サービスを有用なものとするためには、利用者にとって使い勝手がよく、安心して利用できるものでなければならない。そのためには、サービスの内容はもちろん、サービスのシステムにおけるセキュリティ対策や管理・運用体制等の情報を公開し、サービスの透明性を確保することが重要である。

ただし、システムの構造やセキュリティ対策の内容等は、専門的な知識が必要となるケースが多いため、専門知識を有しない利用者に対してどのようにわかりやすく伝えるかが問題となる。現在、整備が進められているセキュリティに関する第三者評価・認定の枠組み（ISO15408やBS 7799等）が利用可能となれば、高い技術力を有する評価・認定機関による客観的な評価結果は、そのシステムの安全性を判断するうえで有用であると考えられる。

5．電子文書の送受信証明プロトコルの安全性評価 －タイムスタンプ・プロトコルを例に

電子文書の送受信証明プロトコルが、社会のインフラとして高く信頼され、幅広い分野で利用されるようになるためには、そのプロトコルの安全性評価が適切に行われることが必要であると考えられる。しかし、現時点では、安全性評価を行うための手法が十分に整備されておらず、そのような手法の確立は今後の重要な研究課題の1つである。

最近の電子文書の送受信プロトコルに関する安全性評価研究の一例として、タイムスタンプ・プロトコルを対象とした安全性評価の研究があげられる。宇根・松本［2000a, b］は、タイムスタンプ・プロトコルの概念整理を行ったうえで、タイムスタンプ発行機関が不正行為を行う可能性や、タイムスタンプの生成に利用されるハッシュ関数の安全性低下の可能性を考慮した安全性評価の研究を行っている。本章では、これらの研究成果を紹介する。

（1）プロトコルの安全性評価に関する課題

従来のタイムスタンプ・プロトコルの安全性評価研究では、タイムスタンプ発行機関を信頼できない場合にどのようにしてタイムスタンプの安全性を確保するかに重点が置かれてきた。しかし、各種プロトコルが提案された結果、ISO13888の枠組みでは十分な概念整理が困難となり、新たなプロトコルの枠組み整備等が必要となってきた。現在、プロトコルの安全性評価の課題として、以下の3つがあげられる。

イ．プロトコルの概念整理

プロトコルの体系的な安全性評価を行うためには、まずプロトコルの概念整理を行う必要がある。例えば、タイムスタンプに含まれる情報の種類、タイムスタンプの生成・検証方法、検証に利用される情報の保管方法等にはさまざまな形態が想定される。このようなプロトコルの属性に関する分類を行い、各種プロトコルの特徴や長所・短所を明確にすることが必要である。

ロ．プロトコル構成者の不正行為を前提とした評価

従来のタイムスタンプ・プロトコルでは、タイムスタンプ発行機関の不正行為や攻撃者との結託に対して安全性を確保することが主たる目的であった。しかし、提案プロトコルの中には、タイムスタンプ発行機関の不正行為による影響について十分な評価が行われていないものも存在する。例えば宇根と松本は、代表的なタイムスタンプ・プロトコルの1つであるPKITSについて、攻撃者が少なくとも2つのタイムスタンプ発行機関と結託すれば、タイムスタンプを改ざんできることを示している（宇根・松本［2000a］）。また、プロトコル構成者として、タイムスタンプの発行依頼者、タイムスタンプ発行機関、検証者以外のものが想定される場合もあるが、攻撃者がだれと結託した際に攻撃が成功するかといった観点から評価を行う必要もある。

ハ．暗号技術の安全性低下を前提とした評価

タイムスタンプの要件の1つとして、数十年の長期間にわたって有効性を維持できることがあげられる。しかし、タイムスタンプの生成に利用されるデジタル署名やハッシュ関数等の暗号技術は、解読技術の進歩や事故等によって安全性が低下する可能性がある。そのような場合でもタイムスタンプの安全性が損なわれないか否かについて評価を行い、対応策を検討する必要がある。

(2) プロトコルの概念整理と種類

宇根・松本［2000b］は、まず、タイムスタンプ・プロトコルの構成者およびそれらの役割について整理を行ったうえで、プロトコルを10種類に分類している。その内容は以下のとおり。

イ．プロトコルの枠組み

(イ) タイムスタンプの定義

ISO13888は、タイムスタンプに含まれる必須の情報として、タイムスタンプ発行機関（以下、発行者）の識別情報ID_{TSI}、タイムスタンプ対象データMのハッシュ値H、発行者がタイムスタンプの発行依頼者（以下、発行依頼者）からハッシュ値Hを受信した日時・時刻に関する情報Tを規定している。

しかし、この規定に当てはまらないタイムスタンプ・プロトコルも考えられる。例えば、タイムスタンプ対象データMあるいはハッシュ値HをT等の属性情報と一緒に保管したうえで、発行依頼者に対してMあるいはHの保管場所に関する情報を含むものの、Tを含まないデータをタイムスタンプとして返信する、というものである。このような不都合を解消するために、タイムスタンプを新たに「少なくともID_{TSI}とHを含むデータ」と定義する。

(ロ) プロトコルの構成者

タイムスタンプ・プロトコルの構成者として、発行依頼者、発行者、証明者、タイムスタンプの検証者（以下、検証者）、証拠補強者の5つを定義する（表3参照）。

表3　プロトコル構成者とその役割

プロトコル構成者	役割
発行依頼者 (time stamp requester)	タイムスタンプ対象データMに対するハッシュ値Hを発行者に送信し、Hに対するタイムスタンプを入手。
発行者 (time stamp issuer)	タイムスタンプを生成し、その際に生成される検証情報（タイムスタンプの内容を検証するための情報）Eを保管。タイムスタンプ検証時に、検証者にEを送付する場合もある。
証明者 (prover)	データMが時刻Tに存在していたことを検証者に証明するために、Mのハッシュ値Hに対するタイムスタンプを検証者に送信。一般には、証明者は発行依頼者と同一となる。
検証者 (verifier)	タイムスタンプや発行者から入手した情報等から、ハッシュ値Hに対応するデータMが時刻Tに存在したか否かを検証。
証拠補強者 (evidence amplifier)	検証情報Eが改ざんされていないことを示すためにEを保管し、検証者にEを提供。検証情報の一部を公表するプロトコルも存在するが、公表に携わるプロトコル構成者も証拠補強者に該当する。

なお、ISO13888では、タイムスタンプ・プロトコルの構成者として、発行依頼者、発行者、検証者が規定されている。しかし、既存のプロトコルの中には、検証情報（タイムスタンプを検証する際に用いられる情報[18]）を保管する者が存在するケースもある。このようなプロトコルの代表例として、Digital Notaryがあげられる。Digital Notaryでは、検証情報の一部（公表対象のスーパーハッシュ値に対応）をニューヨーク・タイムズ紙に掲載しており、ニューヨーク・タイムズ社が証拠補強者になる。

（ハ）タイムスタンプの生成・検証手続

上記の各プロトコル構成者のもとで、タイムスタンプの生成手続は以下のとおり（図20参照）。

①発行依頼者は、タイムスタンプ対象データのハッシュ値Hを発行者に送信。
②発行者は、HやID_{TSI}等からタイムスタンプを生成し、これらの情報とタイムスタンプ発行過程で生成された検証情報Eをデータベースに保管。
③発行者は、発行依頼者にタイムスタンプを送信。
④発行者は、証拠補強者にEの一部または全部を送信。
⑤証拠補強者は、Eを保管。

ISO13888では、タイムスタンプの改ざん検出手段として、タイムスタンプにMACやデジタル署名を添付する方法が規定されている。

一方、タイムスタンプの検証手続は以下のとおり（図21参照）。

①証明者（発行依頼者）は、検証者にHとHに対するタイムスタンプを送信。
②検証者（もしくは検証代行者）は、必要に応じて発行者にタイムスタンプを送信し、検証に必要な情報を請求。
③発行者は、タイムスタンプの種類に応じて、TやE等の情報を検証者に送付。
④検証者は、発行者等から得た情報やタイムスタンプに含まれる情報を用いてタイムスタンプを検証。発行者が検証者にEを送るケースでは、そのEが改ざんされていないことを確認するために証拠補強者からEを入手し、発行者のEと比較する場合もある。

18 ここでは、検証情報をタイムスタンプの内容を検証するための情報と定義し、タイムスタンプの一貫性を確保するために生成されるデジタル署名および署名検証鍵に対する公開鍵証明書は検証情報に含めない扱いとする。

図20　タイムスタンプ生成手続

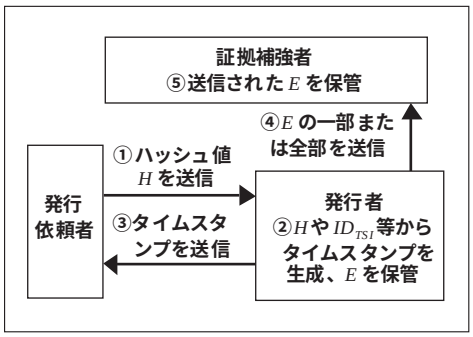
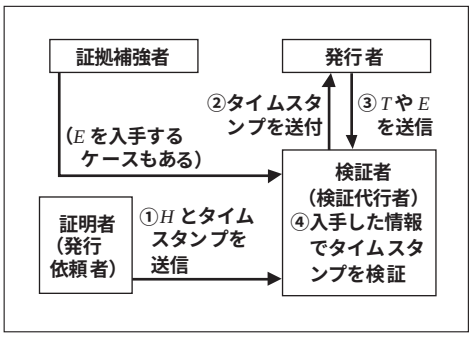


図21　タイムスタンプ検証手続



ロ．プロトコルの分類

タイムスタンプ・プロトコルは、一般に、連鎖型プロトコル、分散型プロトコル、ISO13888に規定されている簡素なプロトコル（simple protocol）の3つに分類される（Habor and Stornetta［1991］, Massias and Quisquater［1997］）。しかし、この分類方法は、タイムスタンプの生成方法の観点からの分類にすぎず、必ずしも適切とはいえない。例えば、1つの発行者がヒステリシス署名[19]（松本ほか［2000］）を利用してタイムスタンプを生成する場合、従来の分類方法では連鎖型プロトコルか簡素なプロトコルかの区別が定かではない。

前節の枠組みに基づいてプロトコルを分類する場合、タイムスタンプに含まれる情報の種類、タイムスタンプの生成方法、検証情報の保管方法、検証者が発行者から入手できる情報の種類、という4つの観点が検討の対象となる。ここでは、まず、①タイムスタンプの種類、②検証者による検証情報の取得可能性、③タイムスタンプの生成方法、の3つの観点からプロトコルを分類する。

（イ）タイムスタンプの種類

タイムスタンプに含まれる情報として、H、ID_{TSI}、T、Eが想定される。定義から、タイムスタンプにはHとID_{TSI}が含まれるため、TもしくはEが含まれるか否かでタイムスタンプを分類する。ただし、Tが含まれずEが含まれるタイムスタンプは常識的に考えにくいことから、そのようなタイムスタンプは想定しない。

①時刻・証拠無タイムスタンプ（time stamp with no time information and no evidence）：HとID_{TSI}を含み、TとEを含まない

②時刻付・証拠無タイムスタンプ（time stamp with time information and no evidence）：H、ID_{TSI}、Tを含み、Eを含まない

19 松本ほか［2000］が提案しているヒステリシス署名は、その署名者が過去にかかわった署名付き電子文書の圧縮データが履歴情報として埋め込まれる署名であり、ある署名が過去に本当に生成されたか否かをその履歴情報によって検証する（署名のアリバイを確認する）ことができるという特徴を持つ。

③時刻・証拠付タイムスタンプ（time stamp with both time information and evidence）：H、ID_{TSI}、T、Eを含む

（ロ）検証者による検証情報の取得可能性

時刻・証拠無タイムスタンプと時刻付・証拠無タイムスタンプの場合、検証者はTやEを発行者から入手可能か否かによって以下の2つのケースが存在する。

①取得型（evidence-available scheme）：検証者がEを発行者から取得可能
②非取得型（evidence-unavailable scheme）：検証者がEを発行者から取得不可能

（ハ）タイムスタンプの生成方法

第3に、タイムスタンプの生成方法に着目し、以下の連鎖型と個別型に分類する。

①連鎖型（linking scheme）：タイムスタンプが他のタイムスタンプに含まれる情報を用いて生成される
②個別型（individual scheme）：タイムスタンプが他のタイムスタンプに含まれる情報を用いずに生成される

（ニ）10種類のプロトコル

以上の分類方法によって、プロトコルは表4の10種類に分類できる。なお、時刻・証拠付タイムスタンプの場合、タイムスタンプにEが含まれていることから、検証者は発行者からEを取得する必要がなく、検証者による検証情報の取得可能性による分類は意味がない。

既存の主要な方式を表4の分類に当てはめると、PKITS、TIMESECは方式7に該当するほか、Cuculusは方式9、法務省の電子公証システムやNTTの分散時刻証明システムは方式6に該当する。また、NTTデータのSecureSeal（シュアティ・ドット・

表4　タイムスタンプ・プロトコルの分類

方式	タイムスタンプの種類による分類	検証者による検証情報の取得可能性による分類	タイムスタンプの生成方法による分類
1	時刻・証拠無タイムスタンプ	非取得型	連鎖型
2			個別型
3		取得型	連鎖型
4			個別型
5	時刻付・証拠無タイムスタンプ	非取得型	連鎖型
6			個別型
7		取得型	連鎖型
8			個別型
9	時刻・証拠付タイムスタンプ	——	連鎖型
10			個別型

コム社のDigital Notary）は方式5に該当する。従来は、タイムスタンプの生成方法にのみ着目した分類が行われていたことから、こうした詳細な分類が不可能であり、体系的な安全性評価も困難となっていた。上記の分類によって、タイムスタンプ・プロトコルの安全性評価が容易となると考えられる。

以下では、宇根・松本［2000b］で分析対象となっている方式7「連鎖・取得型の時刻付・証拠無タイムスタンプ方式」の安全性評価結果を紹介する。

（3）連鎖・取得型の時刻付・証拠無タイムスタンプ方式の概要

イ．主要な方式の特徴

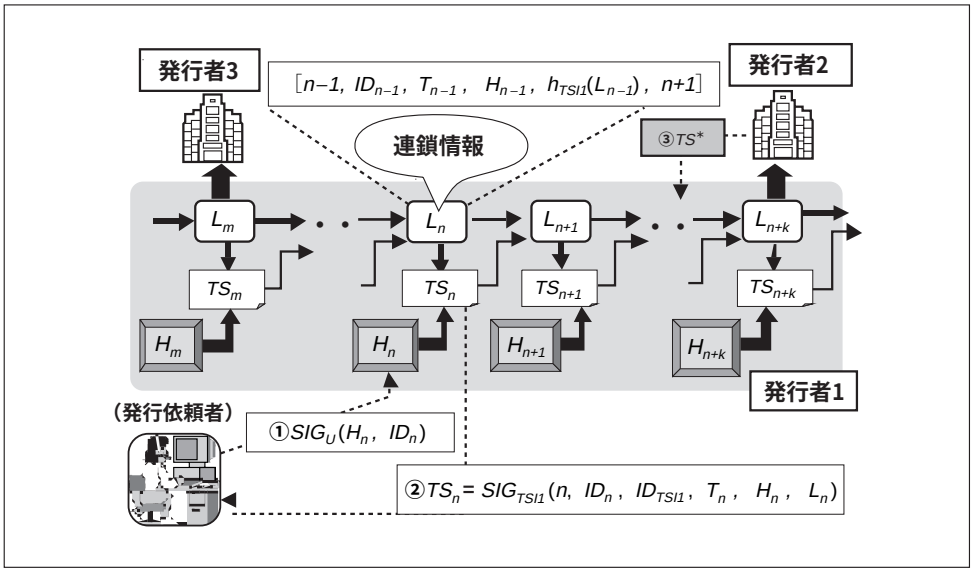
連鎖・取得型の時刻付・証拠無タイムスタンプ方式では、タイムスタンプに検証情報Eが含まれないため、その管理方法によっていくつかの方式に分類される。方式7に当たる代表的なタイムスタンプ・プロトコルのPKITSとTIMESECの特徴を整理すると、表5のとおり。

表５　PKITSおよびTIMESECに含まれる情報、検証情報、検証方法

	タイムスタンプに含まれる情報	タイムスタンプの改ざん検出手段	検証情報		検証方法
			確認情報	再生情報	
PKITS	H、T、ID_{TSI}、シリアル番号、連鎖情報、発行依頼者の識別情報	発行者によるデジタル署名を添付	一部の連鎖情報とそれに対するタイムスタンプ＜発行者が保管＞	タイムスタンプの系列＜発行者が保管＞	連鎖情報系列を再生、一部の連鎖情報に対する他の発行者のタイムスタンプを検証
TIME-SEC	H、T、ID_{TSI}、シリアル番号、ラウンド番号、連鎖情報、各ラウンドの複数のハッシュ値Hを集約する情報、発行依頼者の識別情報	発行者によるデジタル署名を添付	一部の連鎖情報＜ウェブ上等で公開＞	各ラウンドのHを集約した値（ラウンドハッシュ値）の系列と、検証対象となるラウンドの前に生成されたスーパーハッシュ値＜発行者が保管＞	連鎖情報系列を再生、一部の連鎖情報をウェブ掲載のものと照合

これらのプロトコルの検証情報は、タイムスタンプを時系列的に結び付ける連鎖情報を再生するための情報（再生情報、regeneration information）と、再生した連鎖情報の正当性を確認するための情報（確認情報、confirmation information）の2種類に分類することができる。これらの検証情報は発行者によって保管されるが、新聞やウェブサイトに掲載するプロトコルも方式の1つとして考えられる。以下では、このような検証情報の公表も検証補強者による保管形態の1つとして位置づける。なお、例としてPKITSのタイムスタンプの生成手続と検証手続を以下に示す。生成手続は以下のとおり（図22参照）。

図22　PKITSのタイムスタンプ生成手続



＜タイムスタンプ生成手続＞

①発行依頼者は、自分の識別情報ID_nとタイムスタンプ対象データのハッシュ値H_nにデジタル署名を添付したデータ$SIG_u(H_n, ID_n)$を発行者1に送信。本タイムスタンプ発行依頼がn番目（シリアル番号）であったとし、各記号の番号はシリアル番号に対応する。

②発行者1は、H_nに対する連鎖情報L_nとTS_nを生成してデータベースに保管した後、発行依頼者に送信。ただし、h_{TSI1}を発行者1のハッシュ関数、SIG_{TSI1}を発行者1のデジタル署名関数とする。

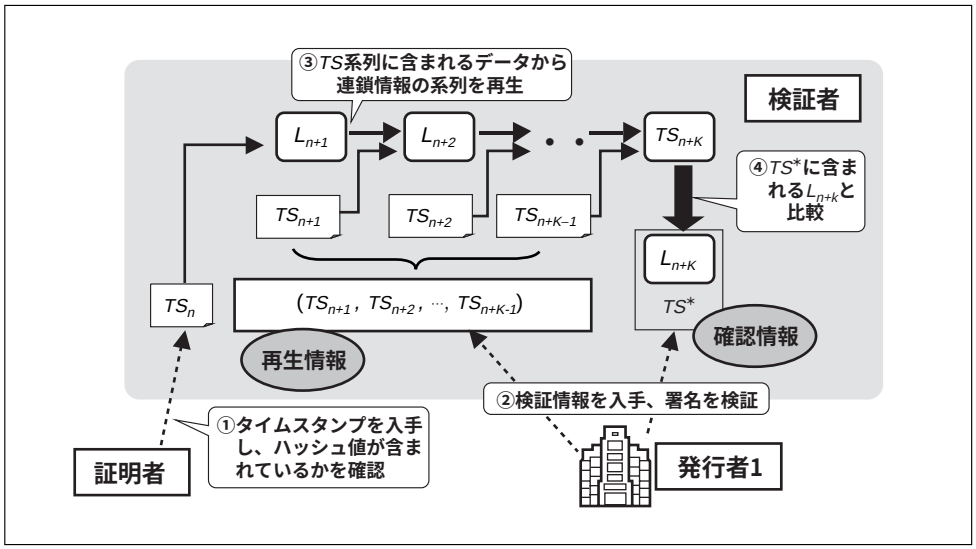
$$L_n = [n-1, ID_{n-1}, T_{n-1}, H_{n-1}, h_{TSI1}(L_{n-1}), n+1] \quad (1)$$

$$TS_n = SIG_{TSI1}(n, ID_n, T_n, H_n, L_n) \quad (2)$$

③発行者1は、L_{n+k}のハッシュ値$h_{TSI1}(L_{n+k})$を別の発行者2に送信し、タイムスタンプTS^*を得る。

一方、タイムスタンプの検証手続は以下のとおり（図23参照）。

図23　PKITSのタイムスタンプ検証手続



＜タイムスタンプ検証手続＞

①検証者は、タイムスタンプ対象データのハッシュ値を計算し、そのハッシュ値がTS_nに含まれているかを検証。

②検証者は、TS_nのデジタル署名を検証。

③検証者は、発行者1からTS_i（$i = n+1,..., n+k-1$）とTS^*を入手し、各署名を検証。

④検証者は、TS_i（$i= n+1,..., n+k-1$）に含まれる情報から連鎖情報系列L_i（$i=n+1,..., n+k$）を生成し、そのL_{n+k}がTS^*の対象となっているL_{n+k}と一致するか否かを確認。

タイムスタンプの検証は2つの手続から構成される。第1の手続は、連鎖情報系列の再生である。PKITSの例では、検証対象のタイムスタンプTS_nに対応する連鎖情報L_nを起点として、発行者が保管しているTS_i（$i=n+1,..., n+k-1$）を用いて順番に連鎖情報系列を再生する部分に相当し、TS_i（$i=n+1,..., n+k-1$）が再生情報に対応する。第2の手続は、再生した連鎖情報系列の真正性を確認情報によって確認するというものである。PKITSの例では、再生した連鎖情報L_{n+k} が真正か否かを他の発行者のタイムスタンプTS^*に含まれるL_{n+k}と比較することで検証する部分が相当する。

ロ．検証情報の保管形態

連鎖・取得型の時刻付・証拠無タイムスタンプは、2種類の検証情報をだれがどのように保管するかによってさらに分類される。検証情報を保管するプロトコル構成者（以下、保管エンティティ）としては、発行者と証拠補強者のいずれか、もしくは両者が想定される。一方、検証情報の保管方法については、ここでは保管エンティティによる検証情報の改ざん検出可能性によって以下の2つを想定する。

①**改ざん検出容易な方法：**保管エンティティが検証情報を改ざんしたとしても、後から改ざんの事実を容易に検出できる保管方法。一例として、PKITSにおいて採用されているように、発行者が、検証情報を他の発行者に送信し、その検証情報に対するタイムスタンプを発行してもらう、といった方法があげられる。

②**改ざん検出困難な方法：**保管エンティティが検証情報を改ざんした場合、後から改ざんの事実を容易に検出できない保管方法。例えば、他の発行者のタイムスタンプを添付する等の処理を施すことなく、データベースに記録するという方法があげられる。

本分類方法は、PKITSにおいて採用されている、「他の発行者が発行したタイムスタンプによって検証情報の一貫性を確保する」という手法にヒントを得て考案されたものである。

以上の結果、2種類の検証情報の保管形態として、表6の16の形態が考えられる。検証情報が発行者のほかに証拠補強者によっても保管される場合、タイムスタンプの検証時に、検証者は、証拠補強者からも検証情報を入手し、発行者から入手したものと比較する。

表６　検証情報の保管形態の分類

形態	確認情報		再生情報	
	方法	保管エンティティ	方法	保管エンティティ
1	改ざん検出困難	発行者	改ざん検出困難	発行者
2				発行者と証拠補強者
3		発行者と証拠補強者		発行者
4				発行者と証拠補強者
5		発行者	改ざん検出容易	発行者
6				発行者と証拠補強者
7		発行者と証拠補強者		発行者
8				発行者と証拠補強者
9	改ざん検出容易	発行者	改ざん検出困難	発行者
10				発行者と証拠補強者
11		発行者と証拠補強者		発行者
12				発行者と証拠補強者
13		発行者	改ざん検出容易	発行者
14				発行者と証拠補強者
15		発行者と証拠補強者		発行者
16				発行者と証拠補強者

（4）安全性評価の方法・結果

イ．評価の前提

各形態の安全性評価を行うに際して、以下の7つの前提を置く。

①**連鎖情報：**連鎖情報は、タイムスタンプが生成されるたびに生成され、直前に生成された連鎖情報とそのタイムスタンプの生成に利用された各種データを結合・ハッシュ化して生成される。
②**攻撃者：**攻撃者は、証明者の1人である。
③**攻撃目的：**攻撃目的は、既存のタイムスタンプの改ざんである。
④**攻撃方法：**攻撃者は、改ざんしたタイムスタンプの検証が成功するように、連鎖偽造攻撃（Fake Chain Attack、Just［1998］）やバイパス攻撃（Bypass Attack、宇根・松本［2000b］）によって検証情報の改ざんを実行する。
⑤**保管エンティティとの結託：**攻撃者は、検証情報を改ざんするためには、その検証情報を保管しているエンティティと結託しなければならない。
⑥**検証方法：**タイムスタンプの検証は、再生された検証情報の比較によって実施されるほか、証拠補強者も検証情報を保管する場合には、発行者が保管する検証情報と証拠補強者が保管する検証情報の比較も行われる。
⑦**交信データ：**交信されるデータにはいずれもデジタル署名等が添付され、改ざん検出容易な形態となっている。

連鎖偽造攻撃は、改ざんしたタイムスタンプの検証が成功するように検証情報を改ざんする攻撃であり、連鎖偽造攻撃の場合には確認情報が改ざんの対象となる。一方、バイパス攻撃は、改ざんしたタイムスタンプの検証が成功するように再生情報を改ざんする、という攻撃である。バイパス攻撃では、確認情報は改ざんしないため、同攻撃を適用するためには連鎖情報の生成に利用されるハッシュ関数のsecond-preimage[20]を探索することが必要となる。タイムスタンプへの攻撃目的および攻撃方法には上記前提③、④以外にもさまざまなケースが想定されるが、タイムスタンプ・プロトコルの安全性評価の出発点として、ここでは上記攻撃目的および攻撃方式に絞って検討を行う。

このように、プロトコルの安全性評価を行う際には、まず評価対象とするプロトコルの特徴点を整理したうえで分類を行い、そのうえで評価の前提条件を定め、各種プロトコルに対して前提条件を適用して網羅的に分析を行うことが必要である。以下では、具体的な分析方法の例として、PKITSやTIMESECのプロトコルが当てはまる形態9に対して連鎖偽造攻撃を適用するケースを想定し、攻撃が成功するための必要十分条件の導出手順を説明する。

20 second-preimageとは、あるハッシュ関数Fにおいて特定の入力値xが与えられたとき、$F(x) = F(y)$を満たす入力値y（$\neq x$）のことである。特定の入力値が与えられたときにsecond-preimageの探索が容易に可能か否かはハッシュ関数の安全性に関する性質の1つであり、second-preimageが容易に探索可能なハッシュ関数は安全性上深刻な欠陥が存在すると位置づけられる。一般に広く利用されているSHA-1、RIPEMD-160、MD5等のハッシュ関数は、これまでのところsecond-preimageを容易に探索する方法がみつかっていない。

ロ．形態9に連鎖偽造攻撃を適用するための必要十分条件

形態9は、発行者が、確認情報を改ざん検出容易な形態で保管するとともに、再生情報を改ざん検出困難な形態で保管する、というものである。PKITSでは、確認情報に他の発行者がタイムスタンプを発行することによって、確認情報を改ざん検出容易にしている（Fabrica Nacional de Moneda y Timbre［1998］）。また、TIMESECでは、確認情報をウェブサイト上等に公開して不特定多数の目に触れるようにすることによって、確認情報の改ざんを検出容易にしている（Quisquater *et al.*［1999］）。

（イ）必要条件の導出

連鎖偽造攻撃は、改ざんしたタイムスタンプの検証が成功するように、確認情報を改ざんするという攻撃である。確認情報を改ざんするためには、攻撃者は、まず確認情報を管理する発行者と結託することが必要である。また、確認情報は各保管エンティティの改ざんが検出容易な形態で保管されているため、攻撃者は、改ざんが検出困難になるように確認情報を改ざんすることが必要である。

このように、連鎖偽造攻撃を行うためには、発行者との結託（条件Aとする）、検出困難な形態での確認情報の改ざん（条件Cとする）、という2条件が必要となる。

（ロ）十分条件の導出

次に、条件Aと条件Cが十分条件となっていることを確認する。「条件Aと条件Cが同時に満足されるならば、連鎖偽造攻撃が成功する」という命題が真であるならば、その対偶である「連鎖偽造攻撃が成功しないならば、条件Aと条件Cのうち少なくともいずれか1つは満たされない」という命題も真である。

連鎖偽造攻撃が成功しないとは、タイムスタンプを改ざんしたとしてもその検証が成功しない、ということを意味する。検証が成功しないのは、「再生した連鎖情報と確認情報を用いた検証が成功しない」というケースである。

このケースでは、再生した連鎖情報と整合的に確認情報を改ざんできなかったケースに相当するが、そのようなケースとして次の3つがあげられる。

- **ケース1）**確認情報を検出困難な形態で改ざんすることが不可能であるケース（条件Cが満足されない場合）
- **ケース2）**確認情報を検出困難な形態で改ざん可能であるが、攻撃者が発行者と結託できないケース（条件Aが満足されない場合）
- **ケース3）**ケース1とケース2が同時に発生するケース（条件Aと条件Cが同時に満足されない場合）

以上より、検証が成功しない場合、少なくとも条件Aと条件Cのいずれか1つが満たされないことが示された。この結果、条件Aと条件Cは、形態9において連鎖偽造攻撃が成功するための必要十分条件でもあることが示された。

ハ．安全性評価結果

前節と同様の分析をすべての形態に適用し、各形態における連鎖偽造攻撃とバイパス攻撃のための必要十分条件を整理すると、表7のとおり。

表７　2つの攻撃が成功するための必要十分条件

形態	連鎖偽造攻撃			バイパス攻撃				4つの条件
1	A			A			D	条件A：攻撃者が発行者と結託。 条件B：攻撃者が証拠補強者と結託。 条件C：保管エンティティによる改ざんを検出容易な形態で保管されている検証情報を、検出困難なように攻撃者が改ざんする。 条件D：発行者のハッシュ関数が、second-preimageを容易に探索できる。
2, 4	A	B		A	B		D	
3	A	B		A			D	
5	A			A		C	D	
6, 8	A	B		A	B	C	D	
7	A	B		A		C	D	
9	A		C	A			D	
10, 12	A	B	C	A	B		D	
11	A	B	C	A			D	
13	A		C	A		C	D	
14, 16	A	B	C	A	B	C	D	
15	A	B	C	A		C	D	

検討結果から、連鎖偽造攻撃に対して最も安全と考えられる形態は、3つの条件A、B、Cが必要十分条件となる形態10、11、12、14、15、16の6つである。条件Bは、「攻撃者が証拠補強者と結託する」という条件である。上記の6つの形態では、発行者と証拠補強者の双方が、確認情報と再生情報のうち少なくとも一方を改ざん検出容易な方法で保管する。また、バイパス攻撃に対して最も安全と考えられる形態は、条件A、B、Cに加えて、「連鎖情報を生成するためのハッシュ関数がsecond-preimageを容易に探索できる」という条件Dも必要十分条件となる形態6、8、14、16の4つである。これらの形態では、発行者と証拠補強者の双方が、再生情報を改ざん検出容易な方法で保管する。以上の考察により、連鎖偽造攻撃およびバイパス攻撃の両方を考慮した場合、最も望ましい形態は形態14と形態16となる。なお、PKITSとTIMESECはともに形態9に属しており、安全性の観点から最も望ましい方式というわけではないことがわかる。

形態14と形態16は、確認情報と再生情報の両方を改ざん検出容易な方法で保管することに加え、少なくとも再生情報については、発行者だけではなく証拠補強者も保管するという形態となっている。このため、発行者は、検証情報全体を検出容易な方法で管理するための追加的な処理が必要となるほか、再生情報を証拠補強者に送信することも必要となる。形態16の検証情報の管理形態をPKITSのタイムスタンプ生成・検証手続に適用するならば、発行者は、①タイムスタンプを生成するたびに、再生情報となるタイムスタンプと、確認情報となる連鎖情報を他の発行者に送信し、それらの情報に対するタイムスタンプを入手することが必要となるほか、

②すべてのタイムスタンプおよび連鎖情報を、他の発行者が生成したタイムスタンプとともに証拠補強者に送信することも必要となる。

二．評価手法に関する考察

従来のタイムスタンプ・プロトコルに関する概念整理や分類方法は、タイムスタンプの生成方法のみに着目したものであり、体系的な安全性評価が困難であった。これに対して、本章で紹介した概念整理および分類方法は、タイムスタンプ・プロトコルをさまざまな観点から分類・整理し、肌目細かな安全性評価を可能にした。その結果、「連鎖・取得型の時刻付・証拠無タイムスタンプ・プロトコル」を検証情報の保管形態の観点から16に分類し、各形態と安全性との関連を評価することができた。

本章で紹介した安全性評価は、連鎖偽造攻撃およびバイパス攻撃という一部の攻撃法に限定したうえで行われたものであり、あらゆる攻撃法を前提としているわけではない。また、分析の対象となったプロトコルも、想定されるプロトコルの一部にすぎない。今後は、その他の攻撃法を前提とした安全性評価に拡張するとともに、残りのプロトコルについても同様の分析を行うことが課題である。

6．おわりに

電子文書の送受信証明は、安全な電子商取引を実現していくうえで重要な機能である。既にさまざまなタイプの電子商取引がインターネット上で実用化されているが、交信されるデータの送受信証明を実現しているものはごく一部とみられる。それ以外のものについては、送受信者のいずれか一方によるデータの持ち逃げや、データの送信あるいは受信の否認といった問題が発生し、そのサービスの信頼が損なわれるリスクがある。

金融機関がインターネット上での資金決済サービス等を提供する際には、金融機関はその顧客を電子認証や暗証番号等で確認したうえで取引を入力させており、かつ、取引の一方の当事者が金融機関という信頼できる機関であることから、データの持ち逃げや送受信の否認のリスクが深刻な問題とはなっていない。しかし、今後、金融機関が、より高度な電子商取引――例えば、大口金融取引や、複数の当事者間にまたがる複雑な取引――を実現するための新しい金融サービスを検討する場合、電子文書の送受信証明の重要性が高まるものと考えられる。また、その実現形態の1つであるタイムスタンプ・プロトコルも、後々の係争や情報公開等に備えて電子文書を長期間安全に保管する際に活用することができる。

本稿では、電子文書の送受信証明を行うためのプロトコルに関する研究・開発動向およびサービス動向について整理した。そのうえで、今後検討すべき主な技術的課題として、①TTPの業務要件の確立と適正な管理・運営体制の維持、②各種プロトコルの安全性の確保、③利用者にとって利便性・透明性の高いサービスの確立、

の3点を指摘した。また、これらのうち、②の課題に関連して、電子文書の送受信証明プロトコルの一形態であるタイムスタンプ・プロトコルの安全性評価に関する最新の研究成果を紹介した。

電子文書の送受信証明プロトコルに関する研究成果は、金融分野において暗号プロトコルを利用した各種サービスの検討を行う際に有用である。インターネットを利用した金融サービスが高い信頼を得るためには、こうした各種研究成果を参考にしながら、そのサービスに利用するプロトコルの安全性評価を行い、高い評価を得た技術を採用していくことが重要であると考えられる。

参考文献

宇根正志、松浦幹太、田倉 昭、「デジタルタイムスタンプ技術の現状と課題」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年、105～153頁

――――、松本 勉、「タイムスタンププロトコルCuculusとPKITSの安全性に関する一考察」、『情報処理学会研究報告』2000-CSEC-11、情報処理学会コンピュータセキュリティ研究会、2000年a、55～60頁

――――、――――、「連鎖型タイムスタンプの検証に用いられる情報の管理」、『コンピュータセキュリティシンポジウム2000論文集』、情報処理学会コンピュータセキュリティ研究会、2000年b、25～30頁

黒田康嗣、蒲田 順、吉岡孝司、岩瀬詔子、野田敏達、小野越夫、「電子原本管理システム・セキュアアーカイバ」、『コンピュータセキュリティシンポジウム'98論文集』、情報処理学会、1998年、113～118頁

佐本陽一・中原慎一、「公平な到達確認プロトコル」、『1999年コンピュータセキュリティシンポジウム予稿集』、情報処理学会、1999年、31～36頁

竹内宏典、村田祐一、「安全な情報流通社会を支える認証・公証プラットフォーム」、『NTT技術ジャーナル』2000年10月号、2000年、26～30頁

多田宜幹、「電子公証を含む電子商取引支援システムの実証実験」、『エレクトロニック・コマース推進事業最終成果発表会論文集』、情報処理振興事業協会、1998年、401～406頁

谷口文一、「金融業界におけるPKI・電子認証について －技術面、標準化に関する最近の動向を中心に」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年、15～54頁

電子商取引実証推進協議会、『電子公証システムガイドライン（Ver.1.0）』、1998年

――――、『貿易金融EDI実施ガイドライン』、1999年

――――、『貿易金融プロセスの電子化の普及に向けて 普及編、ルール編』、2000年

中原慎一、「安全な情報流通を支える認証・公証プラットフォーム」、『NTT R&D』2000年11月号、日本電信電話株式会社、2000年

――――、橋本正一、「電子公証システムの証明技術」、『1998年コンピュータセキュリティシンポジウム予稿集』、情報処理学会、1998年、249～254頁

橋本正一、中原慎一、「電子公証システムにおける証明サービスとその構成法の提案」、『1998年コンピュータセキュリティシンポジウム予稿集』、情報処理学会、1998年、279～284頁

原 司、「公証制度に基礎をおく電子公証制度の導入」、『NBL』No. 690、2000年6月、12～17頁

広瀬章子、山崎康彦、佐藤勝彦、「貿易管理手続き簡素化のための流通性書類の電子化プロジェクト ― Project EDEN ―」、『電子商取引共通基盤整備事業最終成果発表会論文集』、情報処理振興事業協会、1999年、99～102頁

法務省民事局、『電子取引法制に関する研究会報告書』、1998年3月

松本 勉、岩村 充、佐々木良一、松木 武、「暗号ブレイク対応電子署名アリバイ実現機構（その1）―コンセプトと概要―」、『情報処理学会研究報告』2000-CSEC-8、情報処理学会コンピュータセキュリティ研究会、2000年、13～17頁

森永 輔、「電子政府や電子商取引のトラブルを回避―文書の原本性を確保する商品が登場」、『日経コンピュータ』2000年9月25日号、日経BP社、2000年、26～31頁

Adams, Carlisle, Pat Cain, Denis Pinkas and Robert Zuccherato, "Internet X.509 Public Key Infrastructure Time Stamp Protocol(TSP)," October 2000.(http://www.ietf.org /internet-drafts/draft-ietf-pkix-time-stamp-11.txt)

Asokan, Nadarajah, Matthias Schunter and Michael Waidner, "Optimistic Protocols for Fair Exchange," *4th ACM Conference on Computer and Communication Security*, pp.6-17, 1997.

————, Victor Shoup and Michael Waidner, "Optimistic Fair Exchange of Digital Signatures (Extended Abstract)," *Proceedings of EUROCRYPT'98*, LNCS 1403, pp.591-606, Springer-Verlag, 1998.

————, ———— and ————, "Optimistic Fair Exchange of Digital Signatures," October 18, 1999.(http://www.shoup.com/papers/)

Bayer, Dave, Stuart Haber, Scott Stornetta, "Improving the Efficiency and Reliability of Digital Time-Stamping," *Sequences II*: *Methods in Communication, Security and Computer Science*, pp.329-334, Springer-Verlag, 1992.

Brickell, Ernest F, David Chaum, Ivan Bjerre Damgård, and Jeroen van de Graaf, "Gradual and Verifiable Release of a Secret," *Proceedings of CRYPTO'87*, LNCS 293, pp.156-166, Springer-Verlag, 1987.

Buldas, Ahto, Peeter Laud, Helger Lipmaa and Jan Villemson, "Time-Stamping with Binary Linking Schemes," *Proceedings of CRYPTO'98*, LNCS 1462, pp.486-501, Springer-Verlag, 1999.

Cleve, Richard, "Controlled Gradual Disclosure Schemes for Random Bits and Their Applications," *Proceedings of CRYPTO'89*, LNCS 435, pp.576-588, Springer-Verlag, 1989.

Damgård, Ivan Bjerre, "Practical and Provably Secure Release of a Secret and Exchange of Signature," *Proceedings of CRYPTO'93*, LNCS 765, pp.200-217, Springer-Verlag, 1993.

Even, Shimon, Oded Goldreich and Abraham Lempel, "A Randomized Protocol for Signing Contracts," *Communications of the ACM*, Vol. 28, No. 6, pp.637-647, 1985.

Fabrica Nacional de Moneda y Timbre, *PKITS: Deliverable D4 Time-Stamping Service Functional Specification and Protocols for Unstructured Data*, Revision Number: 16, July 30, 1998.

Goldreich, Oded, "A Protocol for Sending Certified Mail," *Technical Report*, Technion - Israel Institute of Technology, Comupter Science Department, 1982.

Habor, Stuart and Wakefield Scott Stornetta, "How to Time-Stamp a Digital Document," *Journal of Cryptology*, Vol. 3, No. 2, pp.99-111, 1991

International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 13888-1: Information technology - Security techniques - Non-repudiation - Part 1: General*, 1997a.

———— and ————, *ISO/IEC 13888-2*: *Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques*, 1998.

———— and ————, *ISO/IEC 13888*-3: *Information technology - Security techniques - Non-repudiation - Part 3: Using asymmetric techniques*, 1997b.

Just, Michael, "Some Timestamping Protocol Failure," *Proceedings of the Internet Society Symposium on Network and Distribute System Security*, 1998.

Lacoste, Gérard, Birgit Pfitzmann, Michael Steiner and Micheal Waidner, "Final Report of Project SEMPER," June 19, 2000.

Massias, Henri and Jean Jacques Quisquater, "Time and Cyptography," *TIMESEC Technical Report*, 1997.

NASD Regulation, Inc., *OATS Reporting Technical Specification*, July 29, 1999. (http://www.nasdr.com/3340.htm)

Okamoto, Tatsuaki and Kazuo Ohta, "How to Simultaneously Exchange Secrets by General Assumption," *Proceedings of 2nd ACM Conference on Computer and Communication Security*, pp. 184-192, 1994.

Privador, A.S., "Privador TrueSign^{TM} Technology Overview," Draft, May 25, 2000. (http://www.privador.com/)

Quisquater, Jean Jacques, Henri Massias, J. Serret. Avila, Bart Preneel and Bart Van Rompay, "Specification and Implementation of Timestamping System," *TIMESEC Technical Report WP3*, 1999.

SEMPER Consortium, "Basic Services, Architecture and Design, Deliverable D03 of ACTS Project AC026 Public Specification," September 24, 1996.

Takura, Akira, Ono Satoshi and Naito Shozo, "Secure and Trusted Time Stamping Authority," *Proceedings of IWS'99*, pp.123-128, 1999.

Zhou, Jianying and Dieter Gollmann, "Observations on Non-repudiation," *Proceedings of ASIACRYPT'96*, LNCS 1163, pp.133-144, Springer-Verlag, 1997.