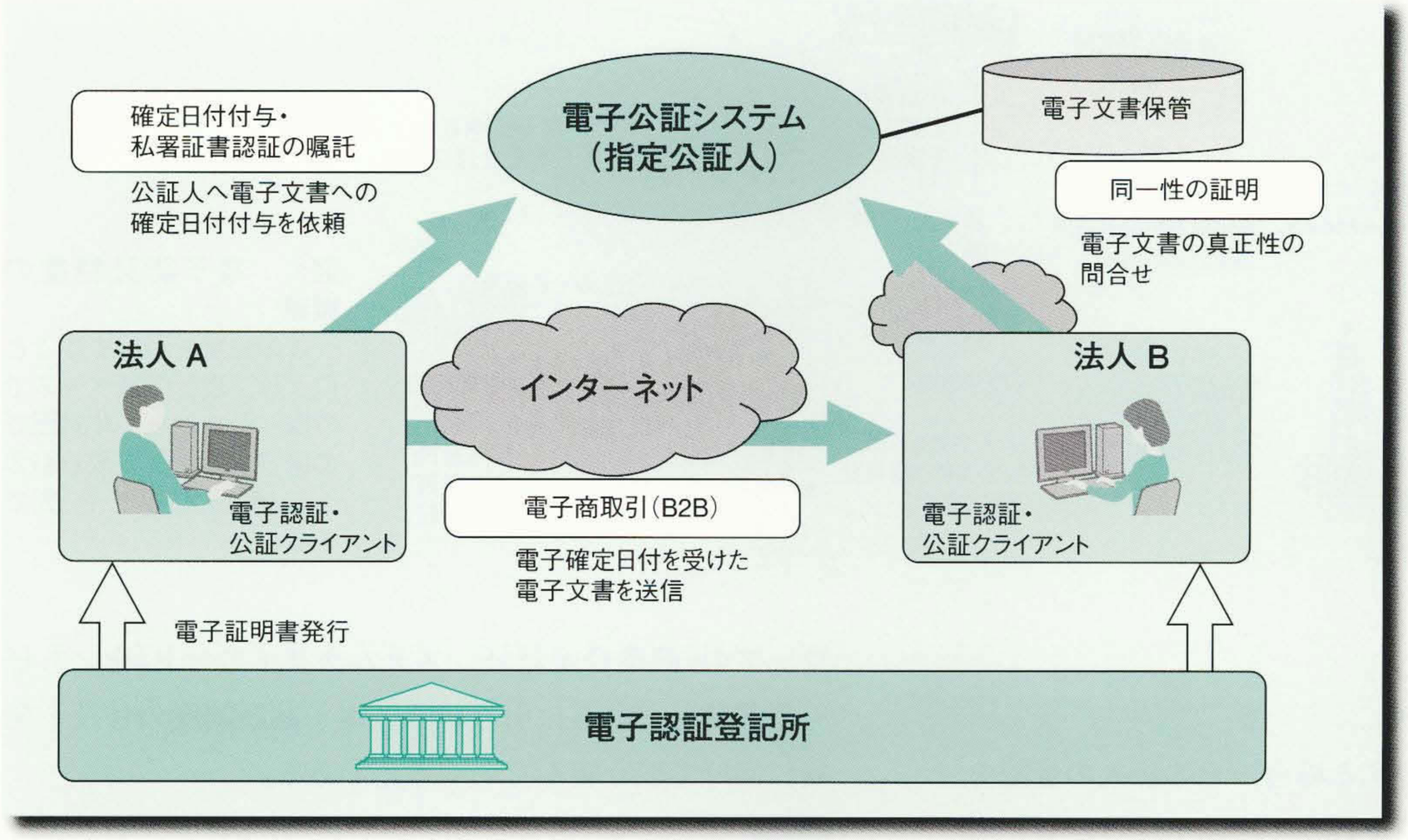
法務省の電子認証・公証システム

Certification/Notary System by Ministry of Justice

宮崎　豊　*Yutaka Miyazaki*
石井晶一　*Shôichi Ishii*
高橋昌行　*Masayuki Takahashi*
押田晋作　*Shinsaku Oshida*



注：略語説明
B2B（Business to Business）

電子認証・公証システムの全体イメージ

法務省の電子認証・公証システムの全体像を示す。法人は，電子認証登記所が発行する電子証明書を利用して各種電子申告・申請ができる。電子公証もその業務アプリケーションの一つである。

法務省は，「商業登記に基礎を置く電子認証制度」と「公証制度に基礎を置く電子公証制度」を2000年4月に創設し，インターネットを通じた電子取り引きや電子申請の制度的な基盤を整備してきた。このうち電子認証制度については，2000年10月から法人に対する電子証明書の発行を開始している。また，電子公証制度についても，日本公証人連合会と連携してシステムを整備し，2002年1月から業務サービスを開始する予定である。

日立製作所は，これらの制度の普及・発展に向けて，認証局などのシステム構築と運用に参画するとともに，実際に両制度を利用する法人・嘱託人のためのクライアントソフトウェアを開発している。これらの製品群は，今後活発化する電子商取引や電子申請などの業務アプリケーションと密接に連携して稼動する。

1　はじめに

政府・自治体への電子申告・申請や法人どうしの電子商取引などをインターネットを利用して行うには，セキュリティを確保する必要があり，そのために電子認証技術が活用されている。

法務省は，いち早く電子認証制度や電子公証制度などの法的な基盤整備を行い，電子化の分野でも，紙の世界と同等の業務遂行を可能とし，電子化の長所を生かした効率化や活性化を図ろうとしている。

日立製作所は，セキュリティ関連技術の開発・製品提供を積極的に展開しており，電子政府実現に向けての認証基盤整備にも深くかかわってきた。

ここでは，法務省の電子認証・公証システムのうち，特に，2002年にサービス開始が予定されている電子公証システムと，日立製作所が開発したクライアントソフトウェア「電子公証クライアント」について述べる。

2　電子認証システム

2.1　電子認証制度

従来の企業間取り引きなどでは，取引相手方の「本人性」，「法人の存在」，「代表権限の存在」を確認するため，登記所が発行する印鑑証明書・資格証明書が広く利用されていた。電子認証制度は，これらの証明書の代わりに，法人の登記情報に基づいて電子証明書を発行するものである。

この電子証明書を利用することで，インターネットなどのオープンなネットワーク上での相手の存在確認，送付された電子文書の真正性の証明などの法的保証，成り済ましや改ざんなどのトラブル防止，セキュアな文書交

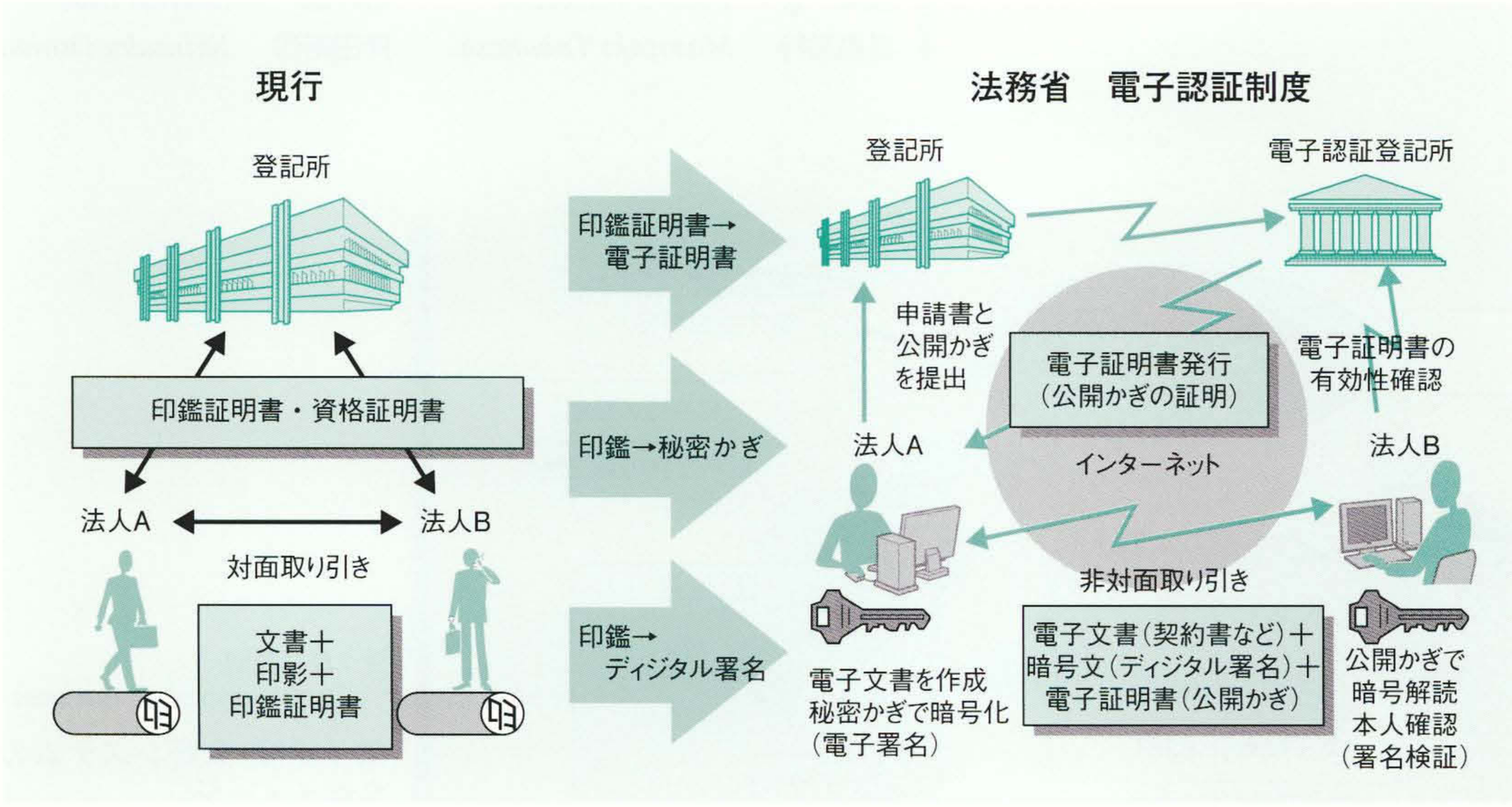


図1　電子認証制度の概略

この制度を利用することにより，現行の紙ベースでの取り引きから，非対面での電子文書による取り引きへと移行することができる。

換などが可能となる。

2.2　電子証明書の利用方法

法人が電子証明書を取得する場合，その法人の登記を管轄する登記所へ発行申請を行う。申請を受けた登記所は，所定の審査の後，電子認証登記所へ登録手続きを行い，電子認証登記所から電子証明書が発行される。

法人は，電子証明書の取得や取引相手方の電子証明書の有効性確認を，インターネットを通じて自分のクライアント端末から電子認証登記所へ，リアルタイムに行うことができる。

この仕組みを利用すると，法人は，電子証明書を取得し，電子文書に対するディジタル署名を行い，政府・自治体への電子申告・申請や法人どうしの電子商取引などを行うことができる(**図1**参照)。

2.3　電子証明書の適用

電子認証制度に基づいて発行された電子証明書は，現在，政府や自治体が実施している各種電子申告・申請システムの実証実験などで利用されている。政府認証基盤(GPKI：Government Public Key Infrastructure)でも，電子認証登記所はGPKIのブリッジ認証局と相互認証を行っており，申請･申告者側の存在証明として今後広く認められる見込みである。

次に述べる電子公証制度を利用するうえでも，この電子証明書が適用される。

2.4　日立製作所の取組み

日立製作所は，電子認証制度に基づいた電子認証登記所のシステム構築に参画するとともに，この制度を利用するために必要となる法人のためのクライアントソフトウェアの「商業登記認証システムクライアント」をいち早く製品化している。引き続き，電子認証制度の普及・発展に向けて取り組んでいく考えである。

3　電子公証システム

3.1　電子公証制度

電子認証制度に基づいて発行された電子証明書で利用できるサービスの一つに，2002年1月から開始される電子公証制度がある。

現在は，認証や確定日付付与の事務を，公証人が紙の文書で行っている。電子公証制度では，指定公証人と呼ばれる電子公証業務を取り扱う公証人が，電子文書により，電子私署証書の認証や電子確定日付の付与を行う(**図2**参照)。

さらに，電子公証制度では，電子私署証書や電子確定日付付与文書のハッシュ(特殊関数)値を指定公証人が保管することにより，電子文書の真正性を指定公証人にあとで確認できるサービスも実施する。

3.2　電子公証クライアント

日立製作所は，電子認証制度に基づいて発行された電子証明書を所有する法人が電子公証制度を利用するための，「電子公証クライアント」というクライアントソフトウェアを開発している。

電子公証クライアントでは，電子文書に嘱託人のディジタル署名を行い，電子確定日付の付与や私署証書の認証を依頼するための嘱託文書を作成することができる。また，指定公証人によって嘱託文書に日付情報と認証文が付与され，指定公証人のディジタル署名が行われた電

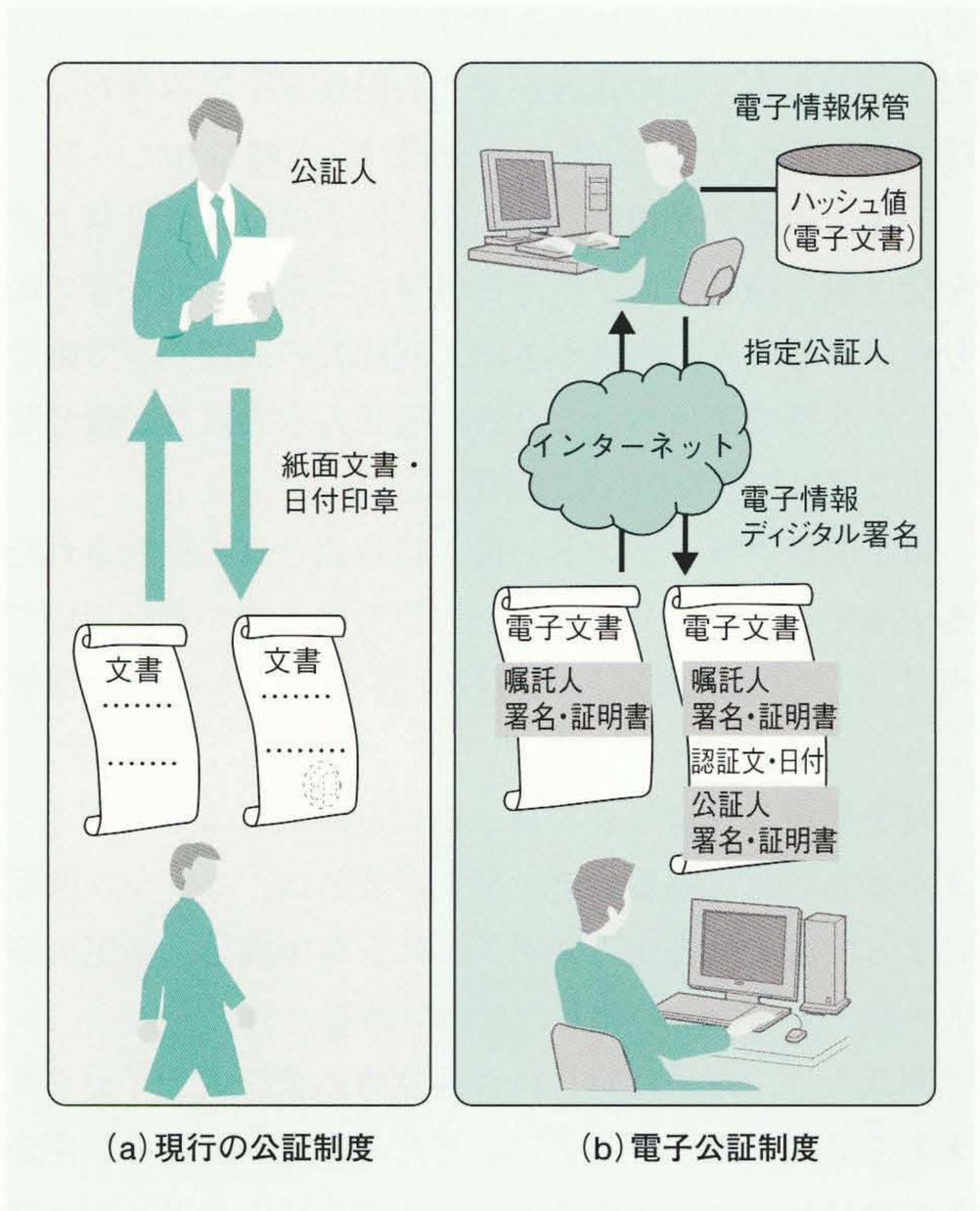


図2　電子公証サービスのイメージ
電子公証制度のサービスイメージを示す。インターネットを通じ，電子文書への確定日付付与などを公証人に依頼することができる。

子確定日付付与文書，電子私署証書の取得と内容確認を行うことができる。

電子公証クライアントを用いて電子公証制度を利用することにより，従来は公証人役場に赴き，公証人に確定日付付与や認証を依頼していた書類を電子化することが可能となる。また，取り引きの過程で公証制度を利用していた商取引や申請に関しても，電子化が可能となる。

例えば，「小口債権の譲渡に関する第三者への対抗要件は，公証人により確定日付が付与された通知または承諾」と民法で定められている。しかし，電子公証制度を利用すれば，小口債権を電子文書化し，電子確定日付を付与することにより，従来と同等の法的効力を留保したまま，小口債権に関する譲渡処理の電子化が可能となる。

電子確定日付付与業務については，電子情報に日付情報を付した電子文書が保管されることから，従来の「公証」制度に限定されないさまざまなニーズに対してもサービスが提供される。

B2B(Business to Business)やB2G(Business to Government)でやり取りされる電子情報の真正性を保証する基盤として，電子証明書を発行する認証局とともに，この電子公証制度は必要不可欠なものとなる。

3.3　ディジタル署名

電子公証制度では，嘱託人は，インターネットを介して指定公証人に確定日付付与を依頼することができる。

秘匿性が高く，法的効力を持つ電子情報を，インターネットを介してやり取りするためには，送信相手の確認(成り済まし，否認の防止)を行うとともに，送信経路での盗み見や改ざんなどから守る技術が必要である。

電子公証制度では，送信相手を確認したり，送信経路での安全性を高めるために，「公開かぎ暗号方式」によるディジタル署名や暗号化の技術を用いている。

公開かぎ暗号方式では，秘密かぎと公開かぎという二つのかぎを用いる。これら二つのかぎは，一方のかぎで暗号化した情報が他方のかぎでしか復号化できないという関係にある。

秘密かぎは所有者が他者に知られないように管理するが，公開かぎは，所有者の情報とともに認証局に登録し，電子証明書の形式で公開する。

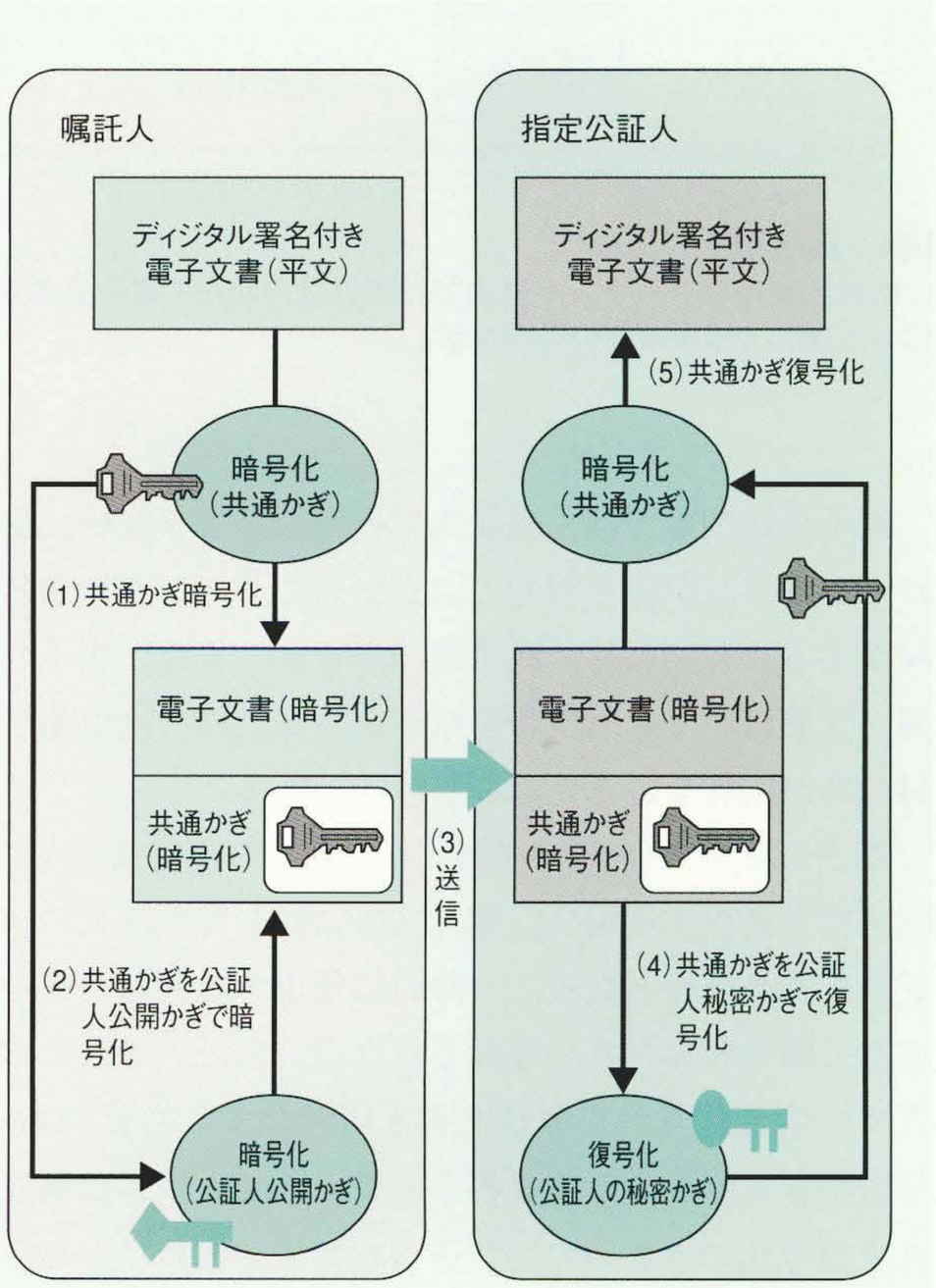


図3　暗号化の原理
嘱託人から指定公証人に対する，インターネットを通じた電子文書送信時の暗号化の原理を示す。

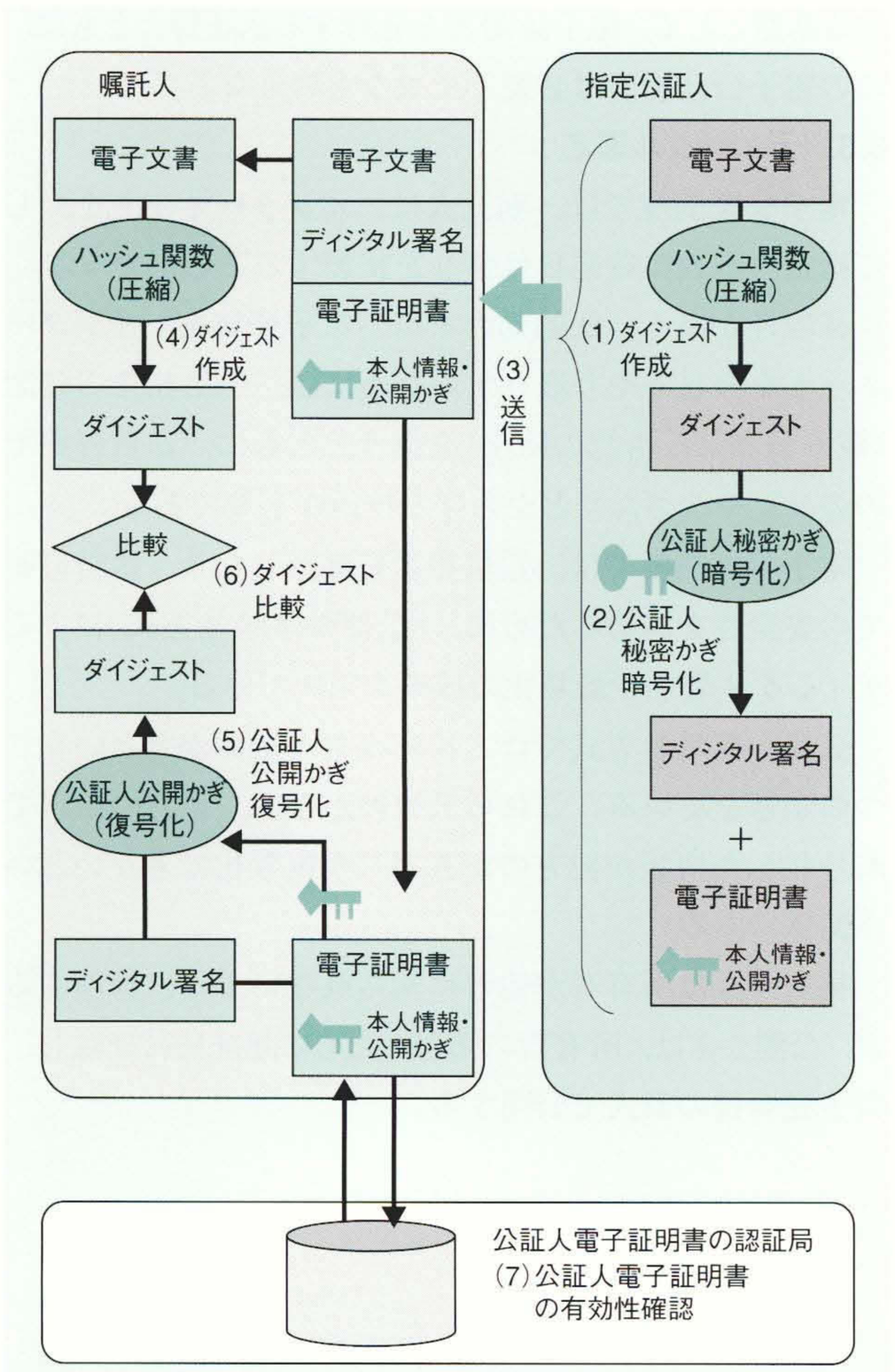


図4　相手確認の原理
嘱託人がインターネット経由で指定公証人からの電子文書を受信した場合の相手確認の原理を示す。

電子公証制度では，嘱託人と指定公証人が互いに秘密かぎと電子証明書を所有し，送信者のディジタル署名を検証することにより，相手確認を行う。また，相手の公開かぎを用いて送信情報を暗号化するため，送信相手以外の者が内容を盗み見ることができない。

電子公証クライアントでは，嘱託人から指定公証人に嘱託文書を送信する場合，嘱託文書に対して嘱託人のディジタル署名を行った後，一時的に使用する共通かぎを生成して暗号化を行う。嘱託された指定公証人は，そのかぎで，暗号化された嘱託文書を復号化する必要がある。秘密かぎを所有する嘱託相手の指定公証人以外は嘱託文書を復号化できないので，送信経路での盗み見から守ることができる。

ここで，嘱託文書の暗号化を指定公証人の公開かぎではなく，共通かぎで行っているのは，共通かぎによる暗号化処理が公開かぎによる暗号化処理よりも数百倍高速だからである。この共通かぎと公開かぎを組み合わせて暗号化を行う方法は「ディジタル封筒」と呼ばれている。

一方，嘱託人が指定公証人から電子確定日付付与文書を受け取る場合，電子確定日付付与文書は共通かぎで暗号化される。この共通かぎは，嘱託人の公開かぎで暗号化した状態で送信されるため，嘱託人本人以外が復号化することはできない(**図3**参照)。

電子公証クライアントでは，暗号化されて送信された電子確定日付付与文書を嘱託人自身の秘密かぎを用いて復号化し，電子確定日付付与文書を嘱託人端末に保管する。

電子確定日付付与文書は，指定公証人によってディジタル署名されている。ディジタル署名は，ハッシュ関数によって電子文書からダイジェストを作成し，指定公証人の秘密かぎで暗号化したものである。

嘱託人は，電子確定日付付与文書の公証人ディジタル署名を公証人電子証明書に含まれる指定公証人の公開かぎで復号化し，電子文書から改めて生成したダイジェストと比較する署名検証処理を行う。ディジタル署名が指定公証人の公開かぎで復号化できることから，指定公証人の秘密かぎで暗号化されたことがわかる。

公証人の秘密かぎは，指定公証人しか知りえない情報であるため，指定公証人によって処理されていることがわかる。また，ハッシュ関数によって生成されるダイジェストは，元の電子文書の内容が一部分でも変われば異なる値になるため，送信されてきた電子文書の内容が改ざんされていないことが確認できる(**図4**参照)。

署名検証に用いた公開かぎの真正性は，この公開かぎが含まれている公証人電子証明書の有効性を，OCSP(Online Certificate Status Protocol)により，公証人電子証明書の認証局に確認することができる。

これら指定公証人のディジタル署名に関する署名検証や電子証明書の有効性確認を行うことにより，嘱託人は，受け取った電子確定日付付与文書が公証人によって作成されたものであることを確認することができる。

電子公証制度では，電子認証技術として相手確認のためにディジタル署名を用いるだけでなく，ディジタル署名が従来の私文書への押印と同等の効力があると認められている。

従来の公証業務では，嘱託人が公証人に書類の認証を依頼する場合，文書に嘱託人の押印を行った後，公証人役場に赴き，公証人の内容確認を受ける。公証人が認証

を行う場合，嘱託文書に対して認証日付，公証人氏名，認証文を追記し，公証印を押印して私署証書が完成する。

電子私署証書の作成でも，同様の手順が必要である。嘱託人は電子文書に対して嘱託人のディジタル署名を行い，指定公証人が電子文書に対して認証日付，公証人氏名，認証文を追加し，指定公証人のディジタル署名を行い，電子私署証書が完成する。

私署証書では，複数の嘱託人が連名で押印する場合がある。この場合，電子私署証書でも，一つの電子文書に対して複数人のディジタル署名を行うことが必要である。

電子公証クライアントでは，電子私署証書嘱託文書に対して，複数名の嘱託人が順次ディジタル署名を行うことにより，連名の電子私署証書嘱託文書を作成することができる。

3.4 同一性の証明

電子公証制度では，指定公証人がディジタル署名を行って作成した電子確定日付付与文書や電子私署証書そのものに対するハッシュ値を，20年間保管するサービスを開始する予定である。

PKI(Public Key Infrastructure)に基づくディジタル署名の真正性は，ディジタル署名された電子文書を署名者の電子証明書に含まれる公開かぎを用いて検証し，この署名検証に用いた電子証明書の有効性を，CRL(Certificate Revocation List)や，OCSPなどの方法で認証局に確認する。しかし，この方法による電子証明書の有効性確認は，おおむね電子証明書の有効期限の近傍では可能であるが，電子証明書失効後長時間経過した時点では，このようなサービスが継続されているかどうかは不確定である。契約書を電子文書で作成し，ディジタル署名を行うとき，電子文書の作成から十数年後に電子文書の真正性を確認する必要が生じる可能性があり，その確認方法が問題となる。

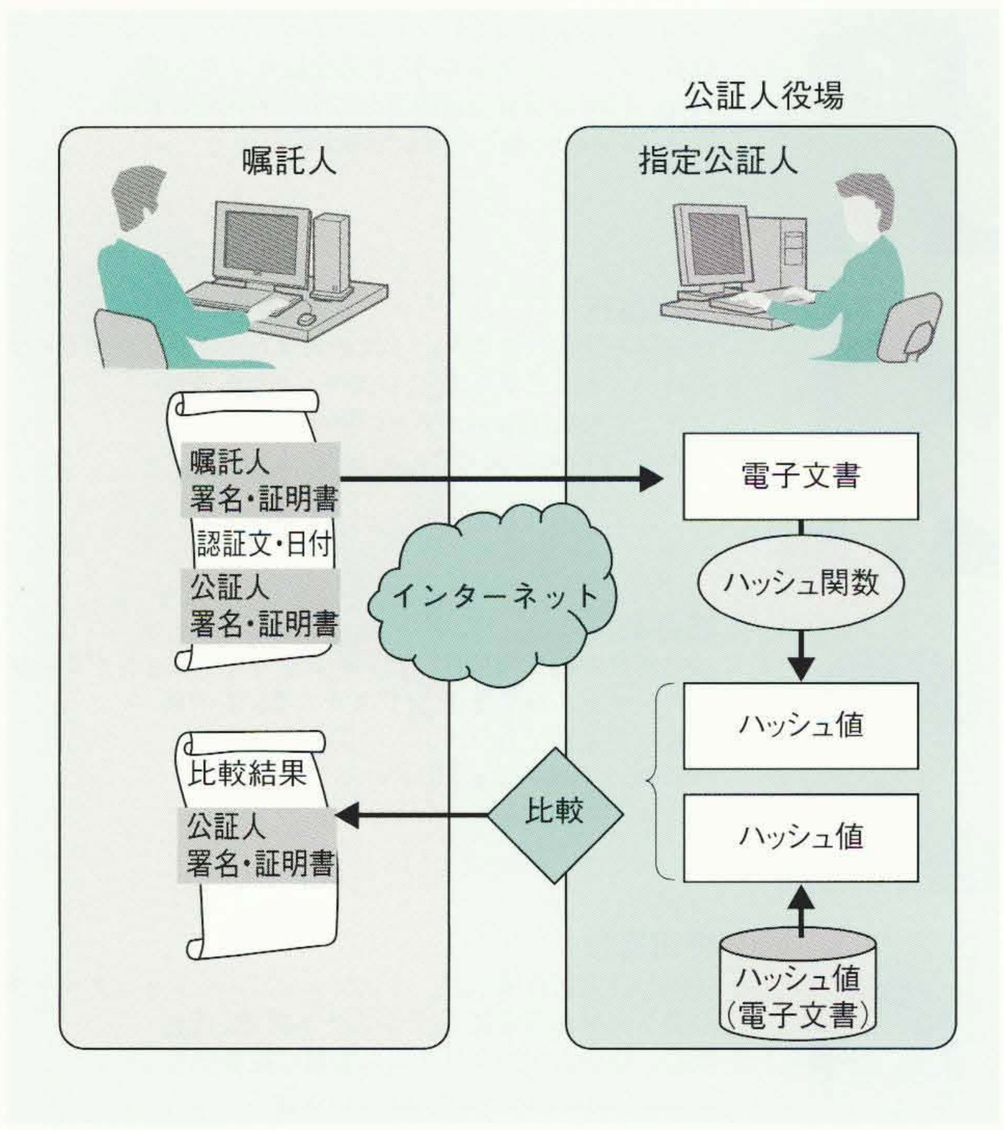


図5 同一性の確認の原理

同一性の確認の原理を示す。送信されてきた電子文書のハッシュ値と指定公証人が保管しているハッシュ値を比較することにより，電子文書の真正性を確認することができる。

電子公証制度では，電子確定日付付与文書や電子私署証書を作成していれば，そのハッシュ値を20年間保管するため，電子文書の真正性を確認することができる。

同一性の証明を行う場合，嘱託人は電子公証クライアントから，電子確定日付付与文書，または電子私署証書を指定公証人にインターネットを介して送信する。

指定公証人は，送信されてきた電子文書のハッシュ値と，指定公証人が保管しているその電子文書のハッシュ値を比較したうえで，結果通知にディジタル署名を行い，嘱託人に返信する。これにより，この文書が指定公証人によって確定日付付与，認証されたものであることが証明される(**図5**参照)。

送信されてきた電子文書が指定公証人によって作成された電子確定日付付与文書や電子私署証書でなければ，算出されるハッシュ値は，指定公証人が保管している電子文書のハッシュ値とは異なる。そのときは，指定公証人から，確定日付付与や認証を行った電子文書ではないことが通知される。

このように，電子公証制度を利用して電子文書に確定日付付与，または認証を受けることにより，電子証明書の有効期間を過ぎたディジタル署名付き電子文書に関しても真正性を確認することができる。

3.5 電子公証クライアント

電子公証クライアントの画面イメージを**図6**，**7**に示す。

電子認証制度・電子公証制度を利用することで，電子申請や電子商取引に用いる電子情報そのものの真正性を証明することができるようになった。

日立製作所は，今後，電子公証クライアントをはじめとする，商業登記電子証明書を活用した業務アプリケーションモデルを開発していく考えである。

3.6 電子公証サービスの今後

電子公証制度は，現行の公証制度を基盤にしているた

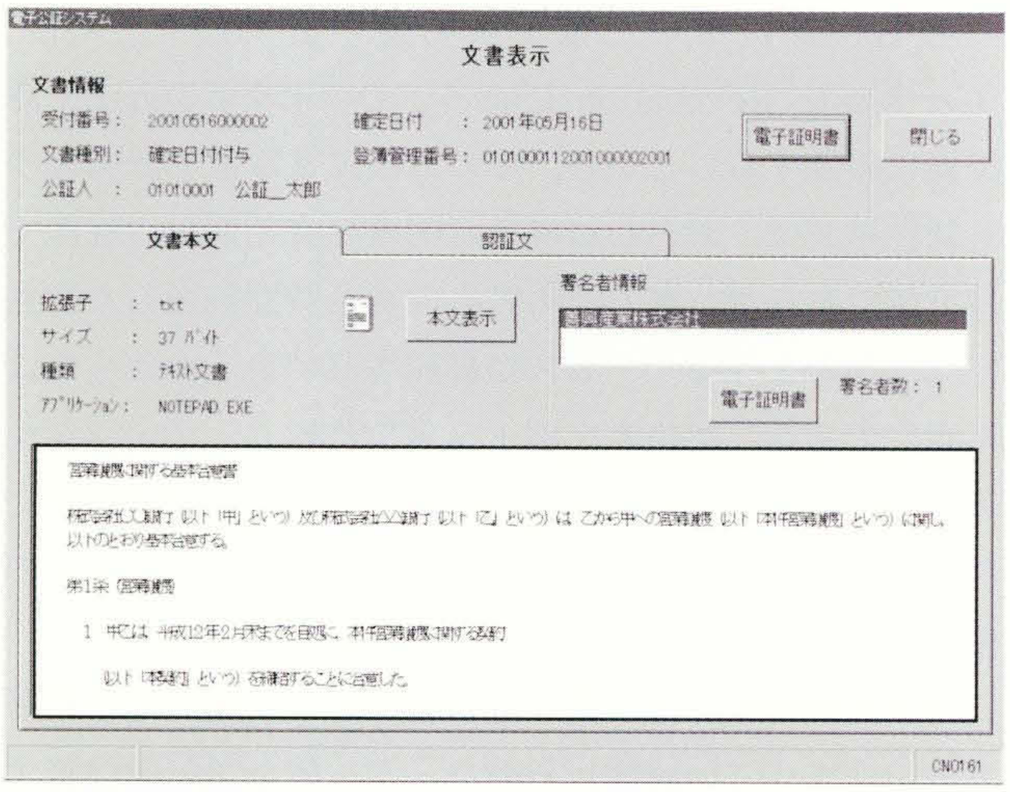


図6　電子公証クライアントの画面例(1)

ディジタル署名された電子文書から，署名対象である電子文書部分と電子証明書部分を表示する。

図7　電子公証クライアントの画面例(2)

電子公証クライアントから，インターネット経由で嘱託文書の進ちょく状況の確認ができる。公証人による処理が完了していれば，そのまま電子文書を取得することができる。

め，現時点では，例えば電子確定日付の付与によって証明される対象は日付情報であり，時間情報は証明対象ではない(ただし，指定公証人が管理する確定日付付与簿には，秒単位まで記録される。)。しかし，今後，公証人が電子情報の真正性を保証するTTP(Trusted Third Party)となるためのマーケットニーズとしては，時間情報も含めた証明も必要となる。また，電子申請や取引業務の中に公証機能をスムーズに結合させる必要もあると考える。

今後，電子公証サービスを広く活用するため，日立製作所は，法務省や日本公証人連合会との連携により，さらに使いやすい電子公証サービスの開発を行っていく考えである。

4　おわりに

ここでは，法務省の電子認証・公証システムについて，特に電子公証システムとクライアントソフトウェア「電子公証クライアント」を中心に述べた。

政府や自治体の電子システムでは，PKIの定着とともに，その基盤を利用した業務アプリケーションが次々と現われてきた。ここで述べた電子公証システムもその一例であり，「時間や空間にとらわれないサービスの実現」がいっそう現実味を帯びてきた。

日立製作所は，今後も，インターネットを利用した各種サービスの普及に取り組んでいく考えである。

参考文献

1) 中上，外；電子行政を支えるセキュリティ基盤技術，日立評論，9月増刊号，53～56(平12-9)

執筆者紹介

宮崎　豊
1984年日立製作所入社，システムソリューショングループ
公共システム事業部 GPKI事業推進センタ 所属
現在，認証局基盤技術関連システムの開発に従事
E-mail：y-miyazaki @ itg. hitachi. co. jp

高橋昌行
1984年日立製作所入社，システムソリューショングループ
公共システム事業部 官公システム第5部 所属
現在，中央官庁系システムの開発に従事
E-mail：mtakahasi @ itg. hitachi. co. jp

石井晶一
1995年日立製作所入社，システムソリューショングループ
公共システム事業部 官公システム第5部 所属
現在，中央官庁系システムの開発に従事
E-mail：s-ishii @ itg. hitachi. co. jp

押田晋作
1998年日立製作所入社，システムソリューショングループ
公共システム事業部 官公システム第5部 所属
現在，中央官庁系システムの開発に従事
E-mail：s-oshida @ itg. hitachi. co. jp