MAKINO
LAW OFFICE
PROFESSIONAL CORPORATION

会社の「脱ハンコ」化～電子契約システム導入の手引き（その1）

ここでは、企業が電子契約を導入するに際しての基本的な考え方や導入の仕方について解説します。

Ⅰ　電子契約システムの選択

電子契約につき、電磁的記録を介して締結された契約であると解したとしても、その内容は、さまざまである。もっとも、現在、複数の企業において導入され、また、多くの企業が興味を持っている電子契約とは、B to B において、紙の契約書を用いて行われていた契約行為を、ペーパーレスで行うというものである。

そして、この電子契約類型には、大きく２つに分けられる。以下では、便宜上、オープン型電子契約とクローズド型電子契約と言う。

オープン型電子契約とは、不特定多数の者との間で行う電子契約である。この場合、契約当事者同士は、相手方の素性を良く知らない場合があり、本人確認を厳格に行わなければ、電子契約の有効性を担保できない。

そこで、オープン型電子契約では、通常、電子署名法上に規定される認定認証業務を行う認定認証局が利用される。**認定認証業務**とは、後述の特定認証業務が、電子署名法第 4 条により主務大臣の認定を受けた認証業務であり、電子署名法第 6 条に則り、認証業務に使用する設備が電子署名法施行規則第 4 条で定める基準に適合し、認証業務における利用者の真偽の確認が電子署名法施行規則第 5 条で定める方法により行われ、認証業務が電子署名法施行規則第 6 条で定める基準に適合する方法によって行われるものを言う。つまり、厳格な基準を満たした設備が用意され、厳格な基準を満たした本人確認方法がとられ、厳格な基準を満たした業務運営がなされていることが必要となる。

以上のように、オープン型電子契約では、厳格な本人確認手続を行った上で、電子証明書及び秘密鍵の登録が行わることになり、電子証明書の信用性が高まるが、他方で、電子証明書登録及び発行の費用が高くつくというデメリットがある。

他方、**クローズド型電子契約**とは、特定の者との間で行う電子契約である。クローズド型電子契約では、通常、取引の相手方が特定の者に定まっており、契約当事者は、相手方の素性を知っている場合が多い。そのため、厳格な本人確認は不要となり、簡便な方法を採用することが可能である。

そこで、電子署名法上の認定認証局を利用する必要はなく、電子署名法上に規定される特定認証業務を行う特定認証局を利用すれば足りる。**特定認証業務**とは、電子署名法第 2 条第 3 項に規定された認証業務であり、電子署名法施行規則第 2 条に基づく電子署

名の技術的安全性をクリアできれば足りるとされている。

そのため、電子署名の技術的安全性以外の本人確認手続などは簡便化することができ、特定認証局との合意により、ある程度の自由な制度設計が可能となり、費用を抑えることができる。

以上のように、クローズド型電子契約では、本人確認手続などにおいて簡便な手続とすることができ、柔軟な制度設計が可能であるが、他方、厳格な本人確認方法などがなされない結果、電子証明書の信用性は、認定認証業務における電子証明書と比べ低くなるというデメリットがある。

電子契約を導入する場合、それぞれの契約の性格や当事者間の関係等に応じて、適切な契約形態を選択する必要がある。

Ⅱ　クローズド型電子契約の仕組み

現状では、電子契約は、B to B で利用される例が多く、また、不特定多数の取引先を対象とするのではなく、すでに素性がわかっている特定の取引先との契約（クローズド型電子契約）で利用されているケースが多数である。

そこで、以下では、クローズド型電子契約を中心に、その仕組みを説明すると共に、導入の段取り、確認事項等を説明する。

紙の契約書を取り交わす場合、契約の一方当事者が、契約書を作成し、自ら（通常は代表者）が署名・押印し、契約の他方当事者に送る。契約書を受け取った他方当事者は、契約内容を確認し、他方当事者も署名・押印する。通常、契約書は２通作成され、各１通ずつを当事者が保管する。

これを電子契約で行うと、以下のようになる。

まず前提として、通常のクローズド型電子契約を導入する場合は、一方当事者（以下、「**統括企業**」という。）が、複数の他方当事者（以下、「**関係企業**」という。）を主導して行われるケースが多い。電子契約を利用するには、契約の一方当事者のみならず、他方当事者をも巻き込んで同じシステムを導入する必要がある。そのため、これまで取引を主導してきた統括企業により、電子契約の導入手続が進められる。そこで、後述の電子証明書の登録業務・発行業務についても、統括企業が外部事業者の委託を受けて行うことがある。

実際に、電子契約を締結する際には、一方当事者（仮にＸとする。統括企業の場合が多いが、関係企業の場合もある。）が契約書を電子データで作成し、他方当事者（仮にＹとする。関係企業の場合が多いが、統括企業の場合もある。）に送信する。ただし、このまま送信したとしても、Ｙとしては、この契約書が本当にＸにより作成されたものであるか、また、インターネット回線を経由してＹに送信する場合、途中で契約書が偽造さ

れていないかを判断できない。そこで、Ｘは、公開鍵暗号方式を利用して暗号化する。**公開鍵暗号方式**とは、一対の公開鍵と秘密鍵を利用する暗号方式であり、公開鍵で暗号化した電子データは秘密鍵でしか復号できず、秘密鍵で暗号化した電子データは公開鍵でしか復号できない。公開鍵は、相手方に広く公開するのに対し、自己の秘密鍵は自己で管理し、他人に秘匿しておく。例えば、ＡがＢに対し電子データを送信する場合、Ａは、Ｂの公開鍵で電子データを暗号化しＢに送信する。Ｂは、自己の秘密鍵を用いて、Ａから送られてきた電子データを復号する。

このような公開鍵暗号方式を利用し、本人確認、偽造確認を行えるようにしたのが電子署名制度である。前述の通り、秘密鍵で暗号化した電子データは、対となる公開鍵でしか復号できない。そこで、Ｘが関係企業にインターネット回線を利用し電子契約書を送信する場合、電子契約書（電子データ）からハッシュ関数を利用しハッシュ値（ダイジェストメッセージとも言う。）を求める。**ハッシュ関数**とは、あるデータから固定長の値を生成する関数のことで、あるデータ（文書）が同じであれば、ハッシュ値は同じになり、文書が違えば、ハッシュ値は異なる。

Ｘは、ハッシュ関数を利用し求められたハッシュ値を、自己の秘密鍵で暗号化し暗号文にすると同時に、電子契約書も自己の秘密鍵で暗号化する（通常の公開鍵暗号方式では、相手方の公開鍵で暗号化するが、電子署名では、自己の秘密鍵で暗号化することに特徴がある。）。そして、Ｘは、暗号化した電子契約書とハッシュ値を、Ｙに送信する。またＸは、認証局から発行されたＸの電子証明書もあわせＹに送信する。

ここで**電子証明書**とは、認証業務（認証局）から、本人確認手続を経て発行された公開鍵についての証明書であり、公開鍵と対をなす秘密鍵の有効性も証明される。もっとも、クローズド型電子契約の場合、統括企業が主導して導入され、また、契約当事者が特定の者に定まっており、統括企業は関係企業の素性を知っていることから、本人確認手続を簡素化すべく、統括企業自身が電子証明書の登録業務・発行業務を行うことが多い。

電子契約書及びハッシュ値の暗号文並びに電子証明書（Ｘの公開鍵が付されていることもある。）を受け取ったＹは、Ｘの公開鍵を用いて、電子契約書とハッシュ値を復号する。Ｙが有するＸの公開鍵で復号できれば、この電子契約書が、Ｘ本人により作成されたことが確認できる。

次に、Ｙは、復号された電子契約書からハッシュ関数を用いてハッシュ値を求める。前述の通り、同じ文書であれば、同じハッシュ値が求められることから、Ｘが送信したハッシュ値と、送られてきた電子契約書からＹが求めたハッシュ値が一致すれば、Ｘにより作成された電子契約書と、受け取った電子契約書が同一であり、偽造されていないことが確認できる。

また、Ｙは、同時に送信されたＸの電子証明書を利用し、認証局（実際には、検証局）のＣＲＬを閲覧し、公開鍵が失効していないかを確認する。**CRL**（Certificate Revocation

List）とは、検証局が有する失効した公開鍵のリストであり、証明書のシリアル番号が記載されている。このＣＲＬを確認することで、当該公開鍵（及び公開鍵と対をなす秘密鍵）の有効性を確認できる。また、ＯＣＳＰを利用することも考えられる。**OCSP**（Online Certificate Status Protocol）とは、電子証明書の失効状態を取得するためのプロトコルであり、ＯＣＳＰのやり取りを行うサーバ（ＯＣＳＰレスポンダ）から当該電子証明書の状態についての回答を得ることができる。

これらの手続を経て、Ｘが真正に電子契約書をＹに送信したことが確認できれば、Ｙにおいて契約書の内容を確認し、今度はＹがＸに対し、電子契約書を送信する。ＹからＸに送信する際も、Ｙの秘密鍵（Ｘの秘密鍵ではないことに注意。）を使い、電子契約書および電子契約書から求めたハッシュ値を暗号化し、Ｙの電子証明書を付す。Ｙから電子契約書の暗号文等や電子証明書を受け取ったＸは、ハッシュ値の一致を確認し、また、Ｙから送信されてきたＹの電子証明書を用いてＣＲＬを確認したりＯＣＳＰを利用して、Ｙの電子証明書の失効状態を確認する。

以上の手続を経て、契約が成立し、あとは、統括企業が指定したサーバに、電子契約書が格納され保存される。

会社の「脱ハンコ」化～電子契約システム導入の手引き（その 2）に続きます