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）

ここでは、電子契約システムを実際に導入するにあたってのポイントを解説します。

Ⅲ 電子契約導入の段取り

電子契約の利用は、以上の通り、これまでの紙での契約とは全く異なるシステム、段取りを経ることになる。そのため、初めて電子契約を導入する場合には、予定通りに手続きが進められるか、あらかじめ確認しておく必要がある。

具体的には、①電子契約を導入する対象契約の選定、②業務フローの明確化、③当事者及び外部事業者の役割分担、④電子契約を導入した際のリスクの洗い出し、⑤テスト環境におけるテスト及び点検・検査を行う必要があろう。

そこで、以下、電子契約導入の大まかな段取りを説明する。

1 対象契約の選定

電子契約導入にはいくつかのメリットがあるが、全ての契約においてメリットがあるというものでもない。契約の中には、電子契約に向いているものと、向いていないものがある。そこで、**電子契約を導入する際、最初に検討すべき事項は、電子契約を利用する契約の選定である**。

電子契約の特徴から、以下の場合は、電子契約に向いていないものと考えられる。

まず、法律上、明確に紙の書面を要求している契約が挙げられる。例えば、定期借地契約（借地借家法第 22 条）、定期建物賃貸借契約（借地借家法第 38 条第 1 項）、訪問販売、電話勧誘販売、連鎖販売、特定継続的役務提供、業務提供誘引販売取引（特定商取引法第 4 条等）などである。そもそも電子契約は、従来の紙の契約から電子の契約へ移行するものであるが、ここで挙げた契約は、法律上、紙の書面を要求していることから、電子契約導入のメリットは少ない。

次に、契約書面に多数の付属書類がある契約が挙げられる。多数の書類を作成し、これらをすべて契約当事者双方で点検し、それぞれに対し契約当事者が署名し、電子データとして保存することが必要となるため、かえって確認手続きが煩雑となり、簡素な手続きが行えるという電子契約のメリットは減殺されてしまう。

また、契約時において、現場確認を行う必要のある契約も挙げられる。そもそも電子契約は、契約当事者がそれぞれ遠隔地にいる場合、対面で署名・押印したり、契約書原本を双方に郵送するなどする手間を省き、インターネット上で契約書のやり取りを瞬時に行う点に導入するメリットがある。そのため、契約当事者がある場所に参集し、現場

確認を行う必要がある場合には、その場で、契約を締結すれば足りるのであり、電子契約導入のメリットが減殺されてしまうのである。

このように、電子契約を利用する契約の内容を精査し、電子契約導入のメリットがあるかどうかを検討し、対象となる契約を選別する必要があるのである。

2 業務フローの明確化

次に、電子契約を導入した際に、どのような方法で電子契約のやり取りを行うのか、業務フローを明確化する必要がある。業務フローの確認が不十分で、手続に不備がある場合、電子署名や電子契約書の有効性に被疑が生じ、電子契約が有効に成立しているのか争いとなる場合があるのである。業務フローの明確化の際には、以下の点を重点的に確認する必要がある。

① 誰（どの部署）がどのようなケースにおいて、電子契約方式を利用し、電子契約を利用（契約の申込み）を行うのか
② どのような方法で電子契約を作成し、どのような方法で契約の相手方に送信（通知）するのか
③ 契約の相手方のどの部署・担当者に電子契約を送信（通知）するのか
④ 電子契約を受け取った契約の相手方は、どのような方法で、電子契約の内容の正確性、送信元の真正性を検証するのか
⑤ 契約の相手方は、誰（どの部署）が、どのような方法で電子契約の利用（契約の承認）を行い、一方当事者に送信（通知）するのか
⑥ 契約の相手方から送信された電子契約は、どのように保管し、その内容の正確性はどうやって検証するのか
⑦ 全体を通じて、どのように安全管理を講ずるのか

3 役割分担

電子契約を利用する際には、作成・成立した電子契約を安全に保管するサーバが必要である。また、電子契約が本当に権限のある本人により作成されたこと、内容が正確であることを担保するための制度も必要である。そこで、通常、電子契約を保管するサーバを提供する外部事業者や、電子署名の有効性を担保するための電子証明書を発行する外部事業者が必要となる。つまり、電子契約書を保管する外部事業者、電子証明書を発行する外部事業者（認証局と言う。）など、契約当事者以外の外部事業者の利用が必要となる。そのため、電子契約導入に際して、電子契約書を保管し、又は電子証明書を発行する外部事業者をどのように利用するのか、どの程度まで利用するのかについて明らかにしておく必要がある。契約当事者が電子契約に関する業務のほとんどを行い、外部事

業者のシステム（サーバ）や個別サービス（電子証明書の登録・発行など）だけを利用させてもらうのか、それとも、外部事業者に電子契約に関する業務手続の全体を委託し、全面的に外部事業者を利用するのかということである。前者の場合であれば、契約当事者の作業が増えるものの、コストを低く抑えることが可能となる。他方、後者の場合であれば、コストがかかるものの、作業の多くを外部事業者に任せることが可能となり、外部事業者の専門的知識を利用することもできる。

また、前述の通り、クローズド型電子契約の場合、電子証明書の登録業務・発行業務を契約の一方当事者である統括企業が行うことがあることから、外部事業者と統括企業との役割分担を明らかにしておくとともに、責任分担も明確にしておくべきである。

電子契約を利用する際にも、コストと契約当事者の手間を考慮して、どの程度、外部事業者を利用するのかを決定する必要がある。

4 リスクの洗い出し

また、あわせて、電子契約を導入する際のリスクの洗い出しを行う必要もある。電子契約は、インターネットを利用し、契約書という重要な電子書面のやり取りを行うものであり、また、電子契約書は、通常、サーバに保管される。そのため、インターネット上でのスニッフィング（データ傍受）やなりすまし、サーバダウンによる契約書データの消失などの危険性が常に付きまとう。また、後述する電子署名で使用される秘密鍵については、ＰＩＮコード（暗証番号）付きのＩＣカードや契約当事者のＰＣまたはサーバに格納され、ＰＣやサーバへのアクセスは、通常、ＩＤ、パスワードを利用して行われる。そのため、ＩＣカードを適切に保管したり、ＰＩＮコード、ＰＣやサーバのアクセスに利用されるＩＤ、パスワードの厳重管理が必要となる。

そこで、明確化された業務フローをもとに、脅威、脆弱性、リスクの洗い出しを行い、リスクの分析と評価を行う必要がある。そして、評価されたリスクをもとに、リスク対応を行う。リスク対応には、通常、リスクの回避、リスクの低減、リスクの移転、リスクの保有がある。リスクの回避とは、例えば、そもそも電子契約取引を行わないということであり、リスクの低減とは、費用をかけ電子契約をやり取りするインターネット環境を専用回線にすることなどであり、リスクの移転とは、主に、保険をかけ、万が一に備えることなどであり、リスクの保有は、特段何も対策を取らず、リスクを受け入れることである。

評価されたリスクの大きさや発生率の高さなどを考慮し、どのような方法がベターなのかを検討する必要がある。

5 テスト環境におけるテスト及び点検･検査

対象となる契約を確定し、業務フローを明確化し、外部事業者の利用を含め役割分担を決め、リスク対応をし、いざ、電子契約導入が決まったとしても、インターネット環境やシステムにおいて不具合が生じることが多々ある。そこで、電子契約のやり取りが業務フローに則り、安全・確実に運用できるかどうかをテスト環境においてテストする必要がある。

後述する通り、契約当事者同士ではシステム（ＯＳやソフトウエアなど）が異なっている場合があり、文字化けしたり、送信できなかったり、検証ができないなど、正確に運用できないことがある。そのため、必ず、テスト環境においてテストを行うことが必要である。そして、テスト結果をもとに、点検・検査を行い、どのような環境が必要かを確認し、最終的に電子契約が導入できるかを決定する。

以上の段取りを経て、電子契約を導入することになる。それでは、導入までの段取りにおいて、具体的にどのような点に注意をし、契約当事者間において、どのような取り決めをしておくべきか。以下では、電子契約導入の際に確認すべき事項を説明する。

Ⅳ　電子契約導入の際の確認事項

1　契約当事者間での電子契約利用契約

電子契約とは、ある契約（例えば売買契約など）を締結する際の契約方式に過ぎない。もっとも、これまで、紙をベースとしたアナログの契約方式を、インターネット等を利用したデジタルの契約方式へと移行するものであることから、契約当事者間において契約を締結する際には電子契約を利用するという合意をする必要がある。これを、ここでは、便宜上、電子契約利用契約と言う。

その際には、アナログの契約にはない、**電子契約特有の確認事項**がある。以下では、その確認事項を説明する。

(1) システムの確認、送信条件の確認

電子契約は、契約当事者が直接対面せず、また郵便による送付を行うこともなく、インターネットを利用し瞬時に相手方に契約書を送信し、締結することが可能なものであり、インターネットを含めたコンピュータシステム利用が前提である。ところが、契約当事者双方のＯＳ（オペレーティングシステム）や各種ソフトウェアが異なっていることがある。また、同じＯＳやソフトウェアであっても、バージョンが異なっていることもあり得る。さらに、契約当事者間で利用している通信サービスが異なっていることもある。これらの状況においては、各システムの不整合性から、思うような動作ができないことがあり得る。

そのため、電子契約を導入するに際しては、各契約当事者が利用しているコンピュータシステム、通信システムをあらかじめ確認し、不具合が起こらないようにしなければならない。そこで、前述のテスト環境におけるテストが重要となるのである。

（2）契約の成立時期の確認

電子契約を利用する場合、通常、インターネットを介し、契約当事者間で契約書をやり取りすることになる。また、契約書（電子データ）はサーバに保管されるが、契約書が保管されるサーバは一方当事者（統括企業）が管理しているサーバの場合もあるし、また、専門の外部事業者が管理しているサーバの場合もある。

ここで、どの段階で契約が成立するのか争いとなる可能性がある。例えば、統括企業がサーバを管理している場合、統括企業が作成・署名した電子契約書を受けとった関係企業が、署名して統括企業が管理しているサーバに契約書を送信したとする。統括企業が、まだ契約書を確認していない段階で、関係企業が、サーバ内で保管されている契約書のデータを削除した場合、契約は成立したといえるのであろうか。また、外部事業者が管理するサーバであった場合はどうであろうか。

この点、民法上、契約は承諾の通知を発したときに成立するとされているが（民法第 526 条）、電子消費者契約及び電子承諾通知に関する民法の特例に関する法律第 4 条では、電子契約について特例を設け、承諾が相手方に到達したときに成立するとされている。

電子契約では、申込者が、電子契約書を作成し、電子証明書を付して、これを相手方に送信し、相手方も、自身の電子証明書を付して、申込者に電子契約書を送信する。

したがって、相手方が電子契約書を申込者に送信し、申込者に到達した段階で契約が成立することになる。

そして、民法上、承諾の「到達」とは、申込者が相手方の意思表示を了知し得べき客観的状態を生じたこととされており、例えば、郵便物が申込者の郵便ポストに投函された場合は、申込者の勢力範囲内に入ったとして到達に当たるとされている。この考えを敷衍すれば、相手方が電子契約書を送信し、申込者が保管しているサーバ内に入れば、申込者の勢力範囲内に入り、申込者はこれを了知し得べき客観的状態を生じたとされることから、承諾の到達があったと言える。したがって、統括企業がサーバを管理している場合であれば、関係企業がサーバ内に保管されている電子契約書を削除したとしても、すでに、統括企業が了知し得べき客観的状態を生じたとされることから、承諾の到達が認められ、契約は成立したということになるであろう。他方、外部事業者のサーバで管理している場合、統括企業の勢力範囲内に入ったといえるかどうかは微妙である。もっとも、電子契約書が関係企業からサーバに送信された場合、統括企業に対しその旨通知が送信されることから、統括企業が関係企業の意思表示を了知し得べき客観的状態を生じたと言えそうである。

電子契約についてはこのような問題が生じ得ることから、あらかじめ契約当事者間において、いつ契約が成立するのか明確にしておくとともに、システム上もその対策（例えば、契約当事者双方の電子署名が行われ、一旦サーバに契約書が保管されれば、一方の当事者のみでは削除できないなど）をとっておくべきであろう。

（3）電子署名の有効性の確認

電子契約では電子署名（秘密鍵）が使用される。すなわち、電子契約書からハッシュ関数を用いて電子契約書からハッシュ値を求め、電子契約書とともに、秘密鍵で暗号化する。そこで、この秘密鍵が本当に本人のものであるかどうかを確認する必要がある。またあわせ、電子契約の内容が改ざんされていないかどうかを確認する必要もある。

前述の通り、電子契約では公開鍵暗号方式がとられ、秘密鍵で暗号化した文書は、これと対をなす公開鍵でしか復号できない。したがって、他方当事者（例えば、Y）が、一方当事者（例えば、X）の公開鍵で復号できるということは、秘密鍵が本人（X）のものであるということが確認できるのである。

また、電子契約では、Xは、電子契約書を秘密鍵で暗号化すると同時に、ハッシュ関数を用いて電子契約書からハッシュ値（メッセージダイジェストともいう。）を求め、これもあわせYに送信するのが通常である。Yは、Xから送信された暗号化された電子契約書を復号し、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出力し、公開鍵で復号したハッシュ値を比較し、一致していれば、改ざんもされていないことが確認できる。

このように、他方の当事者（例えば、Y）は、一方の当事者（例えば、X）から電子契約書が送信された場合には、

ⅰ　公開鍵で暗号文を復号できれば、秘密鍵はX本人のものであることが確認できる

ⅱ　公開鍵で復号したハッシュ値と、復号した電子契約書から求められたハッシュ値が一致すれば、電子契約書に改ざんがないことが確認できる

ことになる。

この手続は、電子契約書の有効性を支える重要な手続であることから、契約当事者は、相手方から電子契約書の受信した場合には、これらの手続きを確実に行うようにしておかなければならない。

（5）電子署名（秘密鍵）の管理責任

すでに説明している通り、電子契約では、契約当事者が対面して契約を締結するのではなく、インターネットを介してのやり取りとなることから、相手方が、本当に契約当事者であるのかの確認が必要となる。そのために、秘密鍵を用いた電子署名が用いられるが、これが他人に利用されては意味が無い。

前述の通り、秘密鍵については、ＩＣカードに格納する方法、契約当事者のＰＣに格納する方法、サーバに格納する方法などがあり得る。秘密鍵が他人に利用されないように、ＩＣカードについては、保管場所、保管者を明確にし、保管方法を決めておく必要がある。また、ＩＣカードの場合、通常、ＰＩＮコード入力が必要となるため、ＰＩＮコードも厳格に管理しなければならない。秘密鍵をＰＣやサーバに格納する場合も、ＩＤやパスワードを入力しないと秘密鍵が使用できないように設定し、ＩＤ、パスワードを厳格に管理する必要がある。

また、電子契約も契約である以上、会社の代表が秘密鍵を利用し、電子契約を締結するのが原則であるが、大規模事業者の場合、毎日のように契約を締結する必要があり、個々の支店・事業所の責任者が、代表に代わり電子契約を締結することも考えられる。そのため、秘密鍵を利用し電子契約を締結できる者を特定し、この者に秘密鍵を渡さなければならない。これとあわせ、会社内でも権限の無い者により秘密鍵が利用されないように管理・ルール化する必要がある。すなわち、秘密鍵の管理が杜撰で、複数の従業者が秘密鍵を利用できる状態であるとなると、**全く契約締結権限がない者による契約申込みや承諾がなされる危険がある**のである。

以上のように、秘密鍵の管理方法を明確にしておく必要があるが、仮に、全くの無権限者が秘密鍵を利用したとしても、他方の当事者は、相手方の内情等を知らず、権限を有している者により秘密鍵が利用されたものと考える。そこで、他方の当事者の不利益とならないよう、秘密鍵が無権限者により利用されたとしても、他方の当事者に対し対抗できないようにしておく必要がある。すなわち、契約当事者間の電子契約利用契約において、秘密鍵の厳格管理を相互に義務付け、万が一、秘密鍵が無権限者により利用され、電子契約が締結されてしまったとしても、この効果を否定できないとする文言を入れておくべきである。

（6）電子証明書の取得

電子契約の締結は対面でのやり取りではないため、相手方が本当に権限のある者であるかどうかの判断がつきづらい。そのため、当の本人であることを確認する仕組みが必要であり、それが電子署名（秘密鍵）であるが、電子署名（秘密鍵）は失効していることもあり得る。そこで、電子証明書を利用する。**電子証明書**とは、認証局が、電子契約を利用しようとする者の公開鍵が真正であることを証明するものであり、いわば印鑑証明書のようなものである。もっとも、そもそもの前提として、電子契約書については、当該本人により申請されていることが必要である。そこで、電子証明書の申請において、本人確認の手続きを明確に定めておく必要がある。

まず前提として、電子契約は通常Ｂ to Ｂ取引において利用され、契約当事者は会社対

会社であるが、電子証明書の名宛人は、通常、会社ではなく個人となっている点に注意が必要である。これは、会社が契約当事者であるとしても、実際に契約を締結するのは個人（通常は代表）であること、また、会社の中には、契約締結権限を有する者と有しない者がおり、契約締結権限を有しない者が勝手に電子契約を締結しないようにする必要があるためである。

本人確認方法としては、住民票の写しや戸籍謄本、写真付きの証明書等の提示を受けるという方法が一般的である。もっとも、オープン型電子契約であれば、不特定多数の者との間の取引を想定しているため、電子契約導入の段階において、このような厳格な本人確認が必要となるが、他方で、クローズド型電子契約であれば、通常は、取引先が複数あるとしても、特定の会社であることが多く、また、これまでも取引実績があるなどして、契約締結権限を有する者が誰であるのかについて知っていることが多いであろう。したがって、オープン型電子契約よりも緩やかな本人確認手続が認められる。例えば、会社の登記事項証明書を添付させるとともに、会社への電話聞き取りにより、意思確認を行うという方法も考えられる。クローズド型電子契約においては、それまでの相手方との取引実績や取引態様、当事者間の関係等を勘案し、手続の手間やコストを考慮し、当事者が考える手間と安全性のレベル感にあわせた方法を採用することになる。

次に、電子契約の契約当事者は会社であるが、実際、契約に署名・押印するのは個人であり、通常は代表が行う。ところが、大規模事業者となると、日々多数の契約を締結する必要があり、各事業所ごとの担当者が契約を締結しているのが実情である。その際に、電子契約だけは、すべての契約手続きに代表が関与し、代表が自ら電子署名を行わなければならないとすると、かえって業務の効率を妨げることになる。他方で、無権限の一般社員が社長に黙って勝手に契約書を作成されないようにする必要もある。
そこで、代表以外に電子署名を行える者の範囲を明確に決めておく必要がある。

また、通常、企業内においては、定期的に人事異動が行われ、電子契約（電子署名）を利用する職務から離れ、別の職務に変わることもありうる。その場合、前任者の電子契約利用権限をはく奪し、後任者の電子契約利用権限を付加する手続きが必要となる。

したがって、これらの手続きにいても明確にしておくことが望ましい。

また、認証局に発行申請した電子証明書（及び秘密鍵）については、認証局で本人確認が終了するすると、電子証明書を申請した本人に渡すことになる。電子証明書については、ＩＣカードに格納する方法、契約当事者のＰＣに格納する方法、サーバに格納する方法などがある。電子証明書の本人に対し、どのような方法により受け取るのか、あらかじめ明確にしておく必要がある。

（7）相手方よる電子証明書の受領

電子契約を利用する際には、一方当事者であるＸが作成した電子契約書を、ハッシュ関数を用いてハッシュ値（ダイジェストメッセージ）を求め、これを秘密鍵で暗号化するが、他方当事者であるＹは、この秘密鍵に対応するＸの公開鍵を用いて暗号文を復号することになる。しかしながら、この公開鍵が本当にＸのものであるかどうかわからないことから、Ｘは、自身の公開鍵における電子証明書をＹに送り、Ｙは、受領したこの証明書の有効性を確認することになる。

電子証明書の送信方法としては、電子契約利用契約等により異なり、メールで直接相手方に送信する方法や、サーバを設け、ここに電子契約や電子証明書をアップロードして、相手方にその旨連絡し、相手方がこのサーバにアクセスして、電子証明書を閲覧することなどが考えられる。いずれにしても、この手続きを明確に定めておく必要がある。

（8）電子証明書の有効性の確認（失効していないこと）

電子契約を利用しようとする者は、電子契約に際し公開鍵暗号方式を利用することから、認証局に対し、電子証明書の発行申請を行うことになるが、電子証明書の発行には、本人確認が必要となる。前述の通り、この認証局には、電子署名法に規定される認定認証局による厳格な手続と、特定認証局による自由な手続があり、そのどちらを利用するのか、手間、コスト、電子契約の内容、当事者間の関係等を勘案して決定する。その上で、本人確認手続を含めた電子証明書発行の手続を明確にしておく必要がある。

一方当事者（例えば、Ｘ）は、電子契約書の暗号文等を送信すると同時に、Ｘの公開鍵の電子証明書を付し、Ｙに送信する。そして、Ｙは、送られてきた電子証明書が有効であるかどうかの確認を行う。

その確認方法としては、主にＣＲＬとＯＣＳＰがある。前者の**CRL**とは失効リストのことであり、検証局において、失効した電子証明書のシリアル番号を確認することができる。電子証明書を受け取った者は、このＣＲＬを確認することにより、受け取った電子証明書が有効か失効しているかを知ることができる。他方、**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。

大量の取引がある場合、検証を行うのは手間がかかる。特に、ＣＲＬについては、失効リスト一覧から、当該証明書のシリアル番号がないか、逐一確認しなければならない。

クローズド型電子契約の場合は、取引の相手方が限定されており、相手方の現状を理解している場合も多いであろう。そこで、証明書検証を行うのか、行うとしてどの

範囲まで検証を行うのか、あらかじめ当事者間で決めておくべきである。

（9）契約データの確認

電子契約は、契約書を紙で保管せず、すべて電子データとして保管する。しかるに、契約は締結したらそれで終わりと言うわけではなく、契約後も、争いとなった場合や、争いとならなくても疑義が生じた場合などにおいて、契約書の内容を確認する必要がある。そのため、電子契約であっても契約内容を確認できる方法をあらかじめ明確にしておく必要がある。

電子契約は、電子データとしてサーバなどに保管されているのが通常であろうことから、サーバにアクセスし、電子データをダウンロードできるようにしておくべきである。もっとも、ダウンロードした電子契約のデータは、サーバ内に保管されている電子契約のデータのコピーのようなものであろう。したがって、ダウンロードした電子契約のデータは、原本ではなく写しとしての性質であると考えられる。

また、電子データをダウンロードできるとしても、契約書の内容に手をつけられるようでは、偽造の危険性がある。そこで、データの変更ができないようにしておくと同時に、**タイムスタンプ**を利用することも検討すべきである。

（10）電子契約の放棄とアナログ契約への回帰

電子契約とはあくまで、ある契約を締結する際の契約方法に過ぎない。したがって、一般的に、契約当事者間において電子契約を利用する合意があったとしても、アナログの紙の契約方法を排除していないであろう。

そこで、契約当事者間において、電子契約利用契約を締結した場合でも、通常の紙の契約方法で契約が締結できるようにするかどうかを明確にしておくべきである。

2 外部事業者の電子契約サービス、契約書保管サービス

（1）契約内容の確認

契約当事者間において電子契約を利用するに当たり、外部事業者を利用することが考えられる。オープン型電子契約であれば、電子署名法に規定されている認定認証局を利用することになる。他方、クローズド型電子契約については、自由に制度設計が可能であるものの、確実な電子契約取引の運用を行うためにも、外部事業者による電子契約サービス、契約書保管サービス等を利用するのが望ましいであろう。

クローズド型電子契約を利用する場合でも、当事者が自ら、契約書を保管するサーバを用意し、個別・任意に認証機関（認証局）から証明書を取得することも考えられるが、現在、複数の事業者から、電子契約におけるパッケージサービスが提供されており、また、プライベート証明書と呼ばれる電子証明書が取り扱われており、これら

を利用するのが便利である。

したがって、電子契約を利用する際には、どのレベルまで、外部事業者のサービスを利用するのかを、まず確認することになる。

ここで、確認すべき重要な内容について指摘する。

① 契約書の保管方法と保管者の確定

電子契約は電子データをサーバ等に保管するが、その保管する方法としては、契約当事者の一方（通常は、統括企業）が用意したサーバにおいて保管する方法と、第三者である専門の外部事業者が用意したサーバにおいて保管する方法が考えられる。前述の場合、外部事業者に対する費用が発生しない代わりに、統括企業において保管されることから、相手方当事者（通常は、関係企業）から見れば、統括企業による保管契約書の偽造・差し替えの懸念が考えられる。したがって、この方法を採用する場合には、関係企業の懸念を払拭すべく、一度、双方の電子署名がなされ、契約が締結された以降は、データに変更を加えることができないようにシステムを設定する、また、適宜、タイムスタンプを付し、万が一、偽造がなされたとしても検出できるようなシステムにしておく必要がある。他方、後者については、外部事業者に対する費用をどのように分担するのか、また、外部事業者が倒産したり、サービス提供を停止した場合にどのようにするのかについてあらかじめ決めておく必要がある。

② 証明書の発行方法と発行者の確定

電子証明書の発行には、電子署名法に規定する認定認証業務による厳格な手続により行われる証明書と、緩やかな手続により行われる、いわゆるプライベート証明書が考えられる。

電子署名法に規定する認定認証局が行う証明書の発行は、厳格な手続きが必要となる上、証明書登録・発行費用も高くつくものの、安全性が高く、高い信用度が得られる。他方、プライベート証明書については、認定認証業務と比べ厳格な手続きはなされず、当事者の責任である程度自由に厳格さのレベルを選択でき、また費用を抑えることもできるが、信用度は認定認証局による証明書ほど高くない。もっとも、プライベート証明書においても、暗証強度や仕様については、認定認証局によるそれとほぼ同レベルであり、安全性が問題となる例は少ないであろう。

前述の通り、クローズド型電子契約においては、取引先が特定されており、どのような取引先であるのかが分かるような状況である。したがって、契約内容や当事者間の関係等を勘案し、どのような証明書を利用し、どのように発行するのかを確定しておく必要がある。

また、クローズド型電子契約のうちでも、特に、一方当事者（統括企業）が主導し

で電子契約を導入しようとするような場合、本人確認手続を含め、電子証明書の登録業務・発行業務を外部事業者に委託するよりも、統括企業自らが行った方が簡便であることが多い。

そこで、このような場合は、認定認証局による厳格な手続ではなく、いわゆるプライベート証明書を利用し、また、その電子証明書の登録業務・発行業務についても、統括企業が代行することが考えられる。もっとも、統括企業も契約当事者であることには違いが無く、一方の契約当事者である統括企業が、契約手続の大部分を行うとなると、他方の契約当事者である関係企業は、統括企業が偽造その他不正なことをするのではとの懸念をいだくことも考えられ、この懸念を払拭する必要もある。そこで、手続を明確にした上で、電子契約を締結する部門と、電子証明書の登録業務・発行業務部門を明確に区分し、この両部門間にはチャイニーズウォールを設置すべきであろう。

③ データ保管の安全性

専門の外部事業者を利用し、電子契約書を外部業者のサーバで保管する場合、または、専門の外部事業者を利用し、電子証明書の登録業務・発行業務を行う場合、いずれにしても、サーバのセキュリティが確保されることが必要となる。電子契約においては、紙での契約書は存在せず、すべては電子データとして保存されている。また、電子証明書についても、電子契約の有効性を担保する重要な制度であることから、正確性・真正性が要求される。

したがって、電子契約サービスや契約書保管サービスを利用する場合、かかるサービスを提供している外部事業者のセキュリティ体制が重要であり、利用の際にはこれらをあらかじめ確認し、適切な外部事業者を選定する必要がある。

④ バックアップ

また、データのバックアップ体制も重要である。外部事業者のサービスを利用する際には、かかる外部事業者のセキュリティ体制の確認とともに、万が一に備え、どのようなバックアップ体制がとられているのかについても確認する必要がある。

これは、一方当事者である統括企業においてサーバを用意し、統括企業がサーバを管理している場合も同様である。この場合は、統括企業が、データをバックアップできる体制を検討し、実行しなければならないであろう。その際には、バックアップデータのみを外部事業者のサーバで保管するという方法も考えられる。

（2）当事者の契約関係

外部事業者の電子契約サービス、契約書保管サービスを利用する際の契約関係をまとめると、以下の通りとなる。

まず、一方当事者である統括企業と他方当事者である関係企業は、対等な契約当事者関係であり、電子契約利用契約を締結する。

また、電子契約書を保管するために外部事業者のサーバを利用する場合や、外部事業者においてプライベート証明書の登録業務・発行業務を行わせる場合など外部事業者を利用する場合には、統括企業及び関係企業がそれぞれ、外部事業者と、外部事業者のサービス利用契約を締結することになる。

統括企業が主導して、電子契約を利用する場合であっても、上記契約関係が原則となる。

統括企業が外部事業者のプライベート証明書の登録業務・発行業務を代行する場合であっても、統括企業は、外部事業者が本来行う登録業務を代わりに行っているだけにすぎず、登録業務・発行業務についての契約は、統括企業及び関係企業と外部事業者との間に成立するにすぎない。統括企業と外部事業者との間は、統括企業が外部事業者の登録業務・発行業務を受託するという関係になる。もっとも、プライベート証明書については、本人確認手続を緩やかにするケースが多く、外部事業者としては、関係企業の素性について詳細にまで了知していないことも考えられる。それにもかかわらず、外部事業者は、登録業務の委託者としての責任を負わせられることになるとすると、本システムはうまく稼働しなくなることもあり得る。そこで、関係企業の本人確認については、外部事業者から委託を受けた統括企業が責任をもって行うという、統括企業と外部事業者との間の合意が必要となるであろう。