永久保存版

情報通

2004. October 10月号
発行日：平成16年10月1日
発　行：東京税理士会
　　情報システム委員会
題　字：金井塚　清（豊島）

時刻認証とアリバイ証明−『何時？』は大丈夫か？

私たちは、これまでに電子申告とネットワーク社会の安全性を保つ仕組みである公開鍵基盤(PKI)について勉強してきました。これにより、申告データという大変秘匿性の高い情報を、インターネットを通じて面識のない他人間でも安全に受け渡しすることが可能になる、ということを知りました。

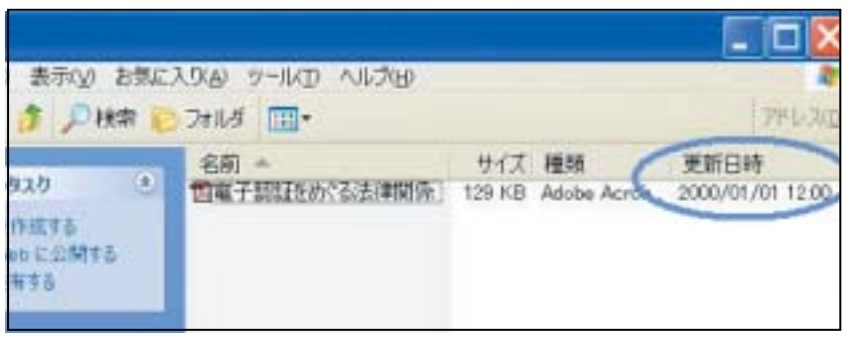
さて、私たちはお客様のデジタルデータを取り扱うという観点から更に一歩を進めましょう。「申告データの前提である帳簿組織とその前の証憑書類が信頼のおけるデジタルデータになりうるか？」というのが今回の話題です。端的には会計記録の検証可能性の問題です。手書き帳簿の時代では、検証可能性は転記の後を容易に追うことができたので特に問題にはなりませんでしたが、複製の容易なデジタルデータは、遡及訂正を痕跡無く可能としますので、悪意には改竄の可能性が常につきまとうのです。この不信感を払拭する手だてとしてデータの「時刻認証」という方法があるのですが、今回の情報通は時刻認証（タイムスタンプサービス）についてスポットを当ててみましょう。

1．時刻認証とは

前号の情報通（9月1日発行）では「『誰』がその電子情報を作成したのか？」を電子証明書を利用した電子署名によって明らかにしました。一方、電子情報のうち『何』が「どの時点（以下『何時？』という）」に存在し、それ以降、変更・改ざんが行われていない、ということを証明する時刻認証（デジタルタイムスタンプ）という技術があることをご存知でしょうか。

パソコンの時計の精度はそれほど高くないことは周知の事実です。税理士業務で一分、一秒という精度が必要な場面はそうはありません。しかし重要なのはパソコンの時計は所有者によって簡単に変更できるということです。紙文書のように指紋、しみ、日焼けなど物理的な痕跡が残るものと違って、コピーが容易で痕跡を残さず改ざんが可能な電子文書では時刻という唯一絶対の基準として時刻自体の信頼性が重要となるわけです。電子データにおける原本性の要件のひとつである真正性確保に『その時点での原本として確定し、それ以降内容が変わっていないこと』という考え方があります。そもそも電子の世界ではどれが原本でどれが副本かという議論自体意味の無いものとされています。

エクスプローラ画面にあるログファイルの更新日時はその一例です。この更新日時はパソコンの時計から持ってきているもので、ファイルの更新日時をファイルのアリバイの証拠として第三者に提示しても上記の理由から証拠能力が低いというわけです。



（例1：　ファイルの更新日時、タイムスタンプ）

2．サイバーの世界でアリバイは示せるか

自分が作成した電子文書のアリバイを作成者が証明するためには、パソコンの時計を変更していないという証明を行うことが必要ですが、これが些か厄介なのです。俗に言う、悪いこと（無実）をしていないと言う証明が大変困難であるのと同じわけです。電子情報の発信時刻、到着時刻を証明するログの時刻についても同様のことが言えます。電子メールを受け取ったという事実よりも何時受け取ったかを証明できれば、より証拠性が高くなるというわけです。第三者に証拠としてある事実を証明、或いは主張する際に、証拠能力は大変重要で、時刻証明を第三者に行う場合には時刻認証が有効となります。

次に電子署名の属性情報の中にある電子署名が付与された時刻はどうでしょうか。

（例2：電子署名とデジタルタイムスタンプが付与された電子文書）

上記の電子文書の右上にある電子署名が付与された時刻も例1と同様、パソコンの時計に依存しています。ということは、本人が電子文書の変更をして、パソコンの時計を好きな時刻に直し（バックデート）、電子署名をして古いファイルを消去してしまえば、作成者本人の電子情報の改ざんや不正は誰も見抜くことはできず、電子署名付き電子文書を受け取った相手に間違ったものを送付したと言って作成日が古い改ざんした文書を送付することが可能になります。電子署名付きの電子文書を受け取ったからと言って喜んでばかりはいられないわけです。電子署名の改ざん検知が可能というのはあくまで、作成者本人以外の改ざんであって本人はやりたい放題だということにご留意下さい。かくて特定期間保存する義務のある電子文書などの保存期間を証明することは電子署名では出来ないのです。

3．アリバイ確保の時刻認証

そこで、デジタルタイムスタンプ（時刻認証）の出番となる訳です。パソコンやサーバのローカル時計に依存せず、信頼のおける第三者の時刻を利用して、デジタルタイムスタンプを付与することで、電子文書原本性の証拠性は高まり、アリバイ証明が可能となります。電子文書の存在証明と非改ざん証明が保存期間を証明する際に重要な要件になります。データを受け取った、受け取ってないなどの否認防止と言う観点からも、受け取った時刻を特定する時刻認証はたいへんに有効な手段だと言えます。

時刻認証といっても、電子データのハッシュ値と時刻を暗号化したタイムスタンプトークンというデータを時刻認証局（TSA）が発行し、オリジナルの電子データとタイムスタンプトークンを使って検証を行うのであって、公開鍵暗号方式を用いた電子署名技術を利用している仕組みであり、電子署名のように作成者本人が電子署名を行うのではなく、第三者が当局の時刻情報を利用し署名を行うことが大きく異なる点であり、証拠性が高いと言われている理由です。法務省が行っている確定日付や郵政庁の消印のように、第三者の日時を利用して存在証明することはリアルの世界（紙文書）では一般的です。しかし、24時間365日エンドレスに発生する電子情報の存在証明を行うには価格、使い勝手の面で現行の方法はサイバーの世界にはそぐわない、ということなのです。

4．近い将来には

電子情報の証拠性の確保、言い換えれば、紙文書と電子文書を同等に扱えるようにする為には『誰』、『何』、『何時』の三要素を担保する必要があり、従って電子署名と時刻認証とはセットになって利用することが肝要です。サイバーの世界に信頼を確立するために遠からずこの組み合わせが求められることになると思います。

現在のところこの時刻認証については、アマノ㈱社や㈱NTTデータ社などから提供されているようですが、今月号の情報通は、アマノ㈱社より原稿の監修をいただきました。製品等の照会については下記のURLをご参照下さい。

http://www.e-timing.ne.jp

納税者の保有する電子証明書の取扱について

−ICカードを預かってはいけません−

納税者が電子申告を行うには、「利用者識別番号」、「暗証番号」「納税用確認番号」、「電子証明書（ICカード）の暗証番号」の4つが必要となります。このうち、税務に係る代理人である税理士といえども下記の通り知ってはいけないモノがあるということを強く認識して下さい。

税務代理の際、上記の納税者の「暗証番号」と「ICカードの暗証番号」は、税理士であっても知ってはいけません。これらの情報は極めて秘匿性の高い重要な個人情報であり、顧問先管理の名の下にこれを知った途端、インターネットセキュリティの主役PKIの信頼基盤は崩壊してしまうのです。

また、e-Taxの受付システムにおいて、なりすまし防止に「利用者識別番号及び暗証番号」の2つの情報を利用します。税務代理のためにはそのうち納税者の「利用者識別番号」は不可欠です。しかし、顧問税理士が納税者の「利用者識別番号と暗証番号」の2つの情報を管理するということは「なりすまし」の可能性を自ら招き入れ、ニセ税理士行為の手段を許容することにもなりかねないのです。

従って、電子申告に係る税務書類に納税者の電子署名を付与する際は、以下の方法によって処理されるようお願いします。

①納税者からメール等で電子署名を付与した申告データをもらう
②パソコンとリーダライタを持参して納税者のところへ出向く
③納税者に来所を求めて電子署名を付与してもらう。

ＩＣカードはリーダライタがなければ読めません