

タイムビジネスに係る指針

～ ネットワークの安心な利用と電子データの安全な長期保存のために ～

平成16年11月5日

総 務 省

1. 目的

現代社会では、至るところで時刻の整合性が必要とされており、“時計”がなければ社会が成り立たないと言っても過言ではない。特に、情報通信ネットワークを支えるコンピュータシステムや身近となったパソコンや携帯電話においても時計が内蔵されており、各システムはこの時計に同期して動作している。

近年の情報通信技術(ICT)の進展に伴い、ネットワーク経由で流通する情報量の増加とともに、高い利便性が伴う電子化した情報の保存が普及しつつある。しかし、紙で記録される文書とは異なり、電子化されたデータは容易に複製や改ざんができてしまうため、原本の区別が本質的に不可能である。その対策として、これらの電子データそのものに第三者が証明可能な時刻情報を付与するシステムの実現が、電子データの原本性確保や改ざん防止に寄与することとなった。

また、ブロードバンドに代表されるインターネットの利用拡大により、地理的・時間的制約を受けずに情報の流通が可能となり、国際的な電子商取引も増加している。その際、異なるシステムで運用される時計に大きな誤差が生じている場合のトラブル発生を防止するには、各システムの時刻を正確に保つことが必要であり、その正確性を第三者が証明するサービスのニーズも生まれている。

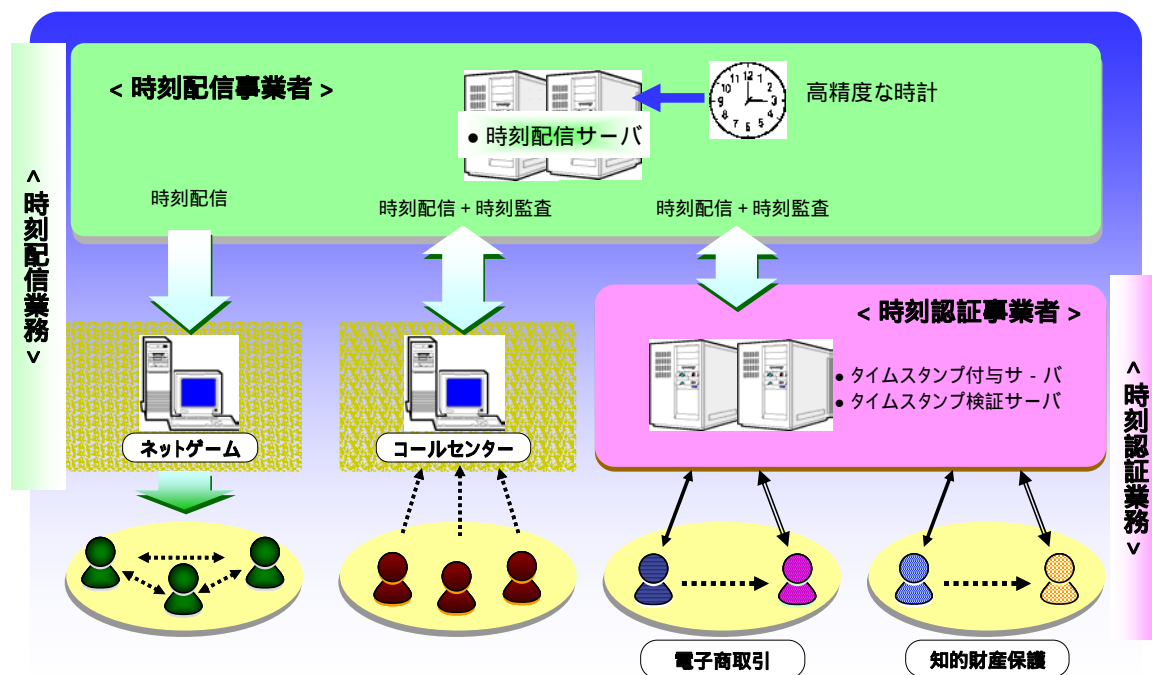
このように、誰もが安心して利用できるネットワーク環境の構築と情報の流通、並びに安全に電子データを長期保存することが求められており、ネットワーク上で正確な時刻情報を配信する“時刻配信”や、電子データの存在した時刻及びその時刻以降に当該電子データの非改ざんを証明できる“時刻認証(タイムスタンプの付与及び有効性証明)”の必要性が高まってきている。

総務省では、インターネット上で高精度に時刻情報を配信するとともに後ほどその配信経路や時刻精度を確認できる技術と、高い安全性と時刻精度を有するタイムスタンプを実現する技術を確立する研究開発を平成15年度から3ヶ年計画で実施しているところであるが、今後、技術の確立に伴って民間事業者において様々な“時刻配信”や“時刻認証”に関する業務(以下「タイムビジネス」という。)の実施が期待される。その本格普及のためには、利用者がタイムビジネスを信頼して利用できるための適切な措置を講じることにより、タイムビジネスが円滑に社会に受け入れられるようにすることが必要である。

そのため、関係者合意のもとでタイムビジネスに求められる要件を取りまとめる意義があるとの考えに立ち、タイムビジネスの必要性に関する解説と併せて、本指針を策定することとした。

なお、タイムビジネス事業者は、本指針に沿った上で、更に自らの事業実態に応じてタイムビジネスの信頼性向上に努めることが望まれる。

2. タイムビジネスのイメージ



3. タイムビジネスの必要性

インターネットの利用拡大に伴い、ネットワークにつながるシステムが増加するため各システムで扱われる時刻の正確性が重要となる。また、電子データは記録を残さずに改変することが容易であるため、電子商取引の拡大や紙文書の電子化に伴って増加する電子データに対する信頼性の確保も重要となっている。

システムで扱われる時刻は、そのシステムの管理方法によってある程度の精度を維持することは可能であるが、過去のある時点におけるシステムで扱われた時刻の正確性について確認を求められると、その情報を提供することは困難である。そのため、時刻配信業務によって精度の高い時刻の提供を受けてシステムを運用することや、システムで扱われた時刻の精度について、後日、証明できることが求められている。

また、インターネット等を通じてやり取りされる電子データに対して、その作成者を確認する措置が必要となり、電子署名が用いられるようになっている(電子署名及び認証業務に関する法律(平成12年法律第102号)に基づき、本人による電子署名が行われているとき、当該電子データの真正性を推定でき、電子データの作成に係る者を特定できる)。しかし、電子署名は、電子データが“いつから存在していたのか”、“ある時点から内容に変更が生じていないか”を確認できる機能を有しないため、これらを証明するタイムスタンプの利用が求められる。

以上のように、時刻配信やタイムスタンプに係る業務が必要とされており、これら業務に対する信頼性の確保が重要となっている。

[参照 【参考】タイムスタンプ利用によるメリット](#)

4.用語

この指針における用語は、次のとおりである。

(1) 時刻配信業務

情報通信ネットワークを利用する上で必要となるサーバ等の電気通信設備に用いられる時刻に高い信頼性を与えるため情報通信ネットワークを通じて時刻情報を配信する業務、更に配信先の時刻精度を計測して報告を行う時刻監査業務をいう。

(2) 時刻認証業務

電磁的記録(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。)に記録された情報(以下「電子データ」という。)に係る情報について行われる措置であるタイムスタンプの付与及び当該タイムスタンプの有効性を証明する業務をいう。

タイムスタンプ[#]

電子データがある時刻に存在していたこと及びその時刻以降に当該電子データが改ざんされていないことを証明できる機能を有する時刻証明情報。

(3) タイムビジネス

「時刻配信業務」及び「時刻認証業務」の総称を指す。

(4) 検証者

タイムスタンプが付与された電子データを有し、かつ当該タイムスタンプの有効性を確認する者をいう。

(5) 標準時

独立行政法人情報通信研究機構法(平成11年法律第162号)第13条第1項第3号に基づき、独立行政法人情報通信研究機構が通報する標準時を指す。

なお、時刻配信業務のうち、標準時に準拠した時刻情報を配信する業務を特に標準時配信業務という。

[#] 既に一般で使用されているタイムスタンプ・トークンという用語は、本指針で定義するタイムスタンプと同義で扱われていることがあり得る。

5. タイムビジネスに求められる事項

(1) 時刻配信業務

ア) 時刻情報は、高い精度を有する時計^(注)を用いることによって生成されるものであって、標準時と比較して、その差が一定の範囲にあること。

注: 高い精度を有する時計は、原子時計であることが望ましい。

イ) 時刻情報は、情報通信ネットワークを通じて、配信先である時刻認証業務の用に供する設備等の電気通信設備に対し、安全な方法により十分な精度で配信すること。

ウ) 時刻監査を行う場合には、配信先の設備を特定してその時刻精度を定期的に計測するとともに、その結果を当該設備に送信又は時刻監査を求めた者に報告すること。

エ) 時刻配信業務に関する監査を受けること。

なお、時刻配信業務では、時刻監査を求めた者その他の者の求めに応じ、時刻情報の配信元とその維持精度に係る情報を提示できることが望ましい。

(2) 時刻認証業務

ア) タイムスタンプに用いる時刻情報は、標準時に準拠した時刻情報であることが望ましく、その誤差は一定の範囲にあること。

イ) タイムスタンプの付与は、時刻認証業務の利用者であることを確認した後、当該利用者の有する電子データに係る情報に対して行うこと。

ウ) 利用者に対してタイムスタンプ及び当該タイムスタンプの有効性検証に必要となる情報(以下「検証必要情報」という。)を確実に渡すこと。これらはタイムスタンプを付与する対象となる情報の基になる電子データに対応することを要する。

エ) 時刻認証において暗号技術を用いる場合には、暗号の強度を十分に考慮すること。

なお、暗号鍵を用いる場合には、利用者その他の者からの求めに応じ、暗号鍵に係るアルゴリズムと有効期間、並びに暗号鍵を用いて時刻認証業務を行う者の名称を含む情報について証明できること。

オ) 上記エ)における暗号鍵は、高い安全性が見込まれる期間内に更新を行うこと。

カ) 時刻認証業務で用いる暗号技術の脆弱性や暗号鍵の危殆化が判明した場合には、速やかに当該業務を停止するとともに、その旨をすべての利用者に対して通知すること。

なお、当該業務は、高い安全性が見込まれる暗号技術又は暗号鍵に切り替えた後に再開すること。

キ) 時刻認証業務を利用しようとする者に対して、次の事項に関する説明を適切に行うこと。

- ・ 業務の内容
- ・ タイムスタンプの有効期間

- ・ 電子データとそれに係るタイムスタンプ及び検証必要情報の適切な保存
 - ・ 暗号鍵を用いている場合には、当該暗号鍵に係るポリシー
- ク) 検証者に対して、次の事項が理解できるように情報を適切に提供すること。
- ・ 時刻認証業務の概要（上記キ)に記載した説明事項の概要)
 - ・ 電子データとそれに係るタイムスタンプ及び検証必要情報、並びに検証結果に係る情報の適切な保存
- ケ) 時刻認証業務に関する監査を受けること。

また、時刻認証業務を行う事業者は、当該業務で付与したタイムスタンプの有効性を保証する期間内において業務を継続することが困難となった場合には、速やかにすべての利用者に対して、その旨を通知するとともに、当該タイムスタンプの有効性が確保できるように努めること。

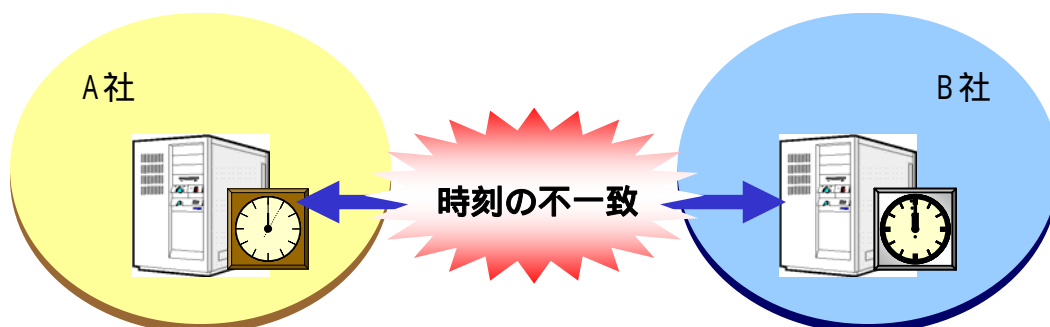
なお、時刻認証業務では、利用者又は検証者の求めに応じ、時刻情報の配信元とタイムスタンプに用いた時刻情報の維持精度に係る情報を提示できることが望ましい。

以上

【参考】

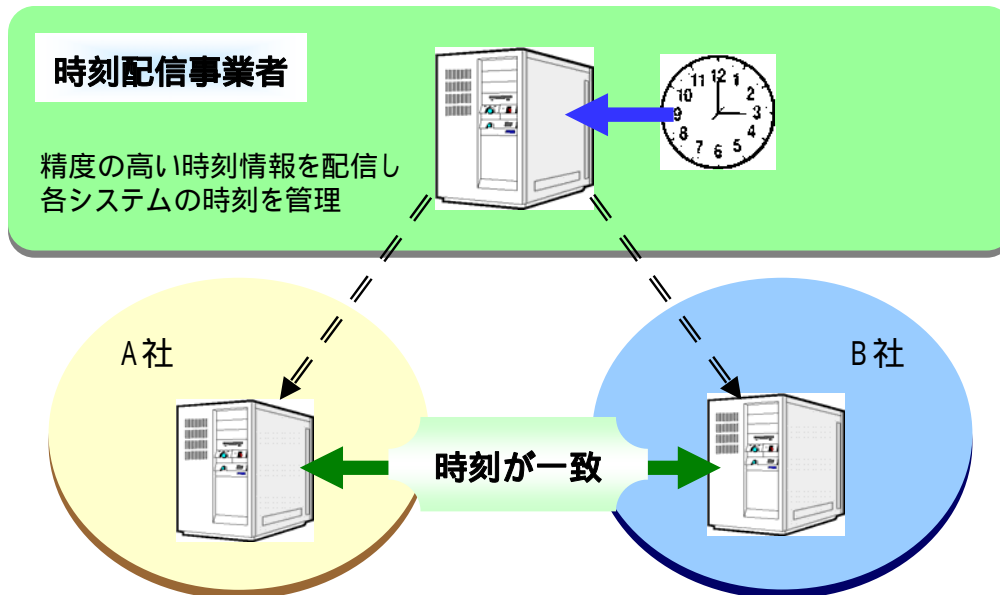
タイムビジネス利用によるメリット

【例1】 時刻配信サービスを利用しない場合に生じる不安



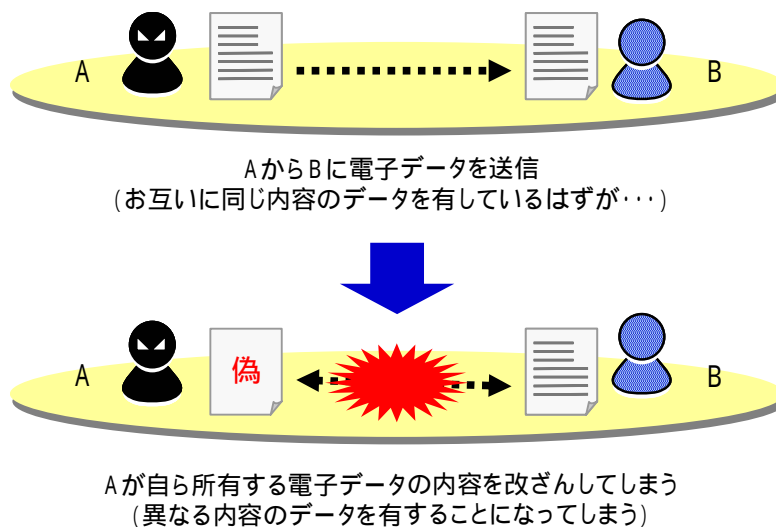
各社の所有するシステムの時刻管理が別々に行われている場合、適切に時刻管理を行っていない社があると、その社と電子データの交換を行った際に時刻情報に整合性がとれなくなる可能性がある。例えば、A社で処理した情報をB社に送信した際、それを受け取ったB社の時計が遅れていると、その情報に係る記録時刻そのものが遅れてしまい、一連の情報の発生順序が不正確となり、全体として情報の信頼性の低下につながる。

【例1への対応】 時刻配信サービスを利用することで不安解消



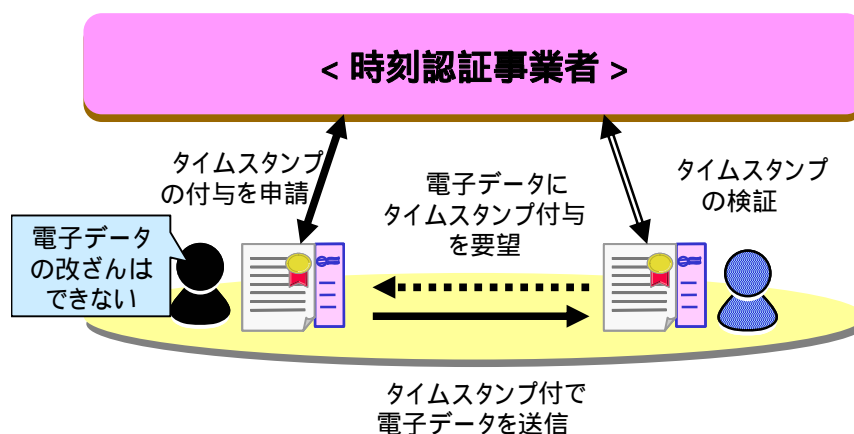
各社の所有するシステムの時刻管理を時刻配信事業者が行うことにより異なるシステム間でも時刻が一致しているので、電子データに係る時刻情報に対する信頼性が高くなる。

【例2】 タイムスタンプを電子データに付けていない場合に生じる不安



AがBに電子データを送付したとき、お互いが同じ内容のものを持ち合うことになるが、Aが悪意を持っている場合、自分の所有するシステムの時計を戻して、あたかもその時刻に作られたように電子データを作成、あるいは元のデータを改ざんしてしまう。このときAとBが有する電子データが異なることになり、その電子データを巡って問題が発生する可能性がある。

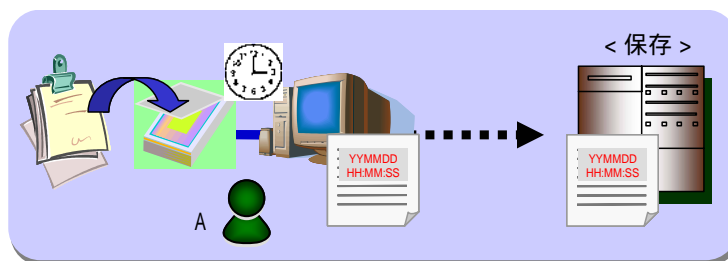
【例2への対応】 タイムスタンプを電子データに付けてもらうことで不安解消



Bは受信する電子データに対してタイムスタンプの付与を条件としておけば、当該電子データに関し、タイムスタンプの付与時点から検証までの間に改ざんがなされていないことを時刻認証事業者証明してもらえるので、安心して電子データを取り扱うことができる。

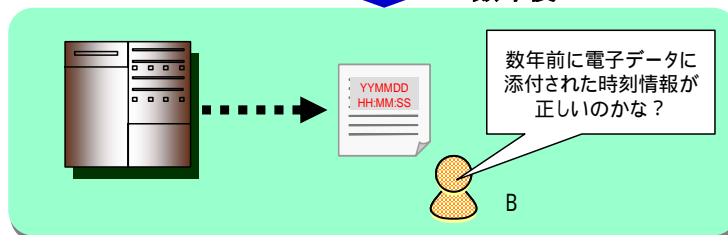
【例3】 電子データを長期に保存する場合に生じる不安

Aは紙ベースの資料を電子化し、
所有するシステムの時計を用いて
時刻情報を付加した後に保存。



数年後...

BがAの保存している電子データを
確認するとき、付加されている時刻
情報の信頼性を得る方法がない。

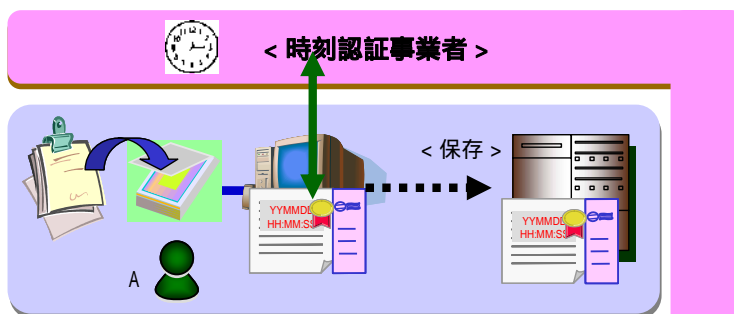


**A自身が行う改ざんを防止
できない。**

Aが紙文書を電子データ化して(最初から電子データで作成しても同じ)長期に保存する場合、
電子化に用いるAのシステム時計で時刻情報を付加して保存していると、後日、当該時刻情報
が正しいものであるか第三者に証明してもらえないため、Bは時刻情報を信用できない。

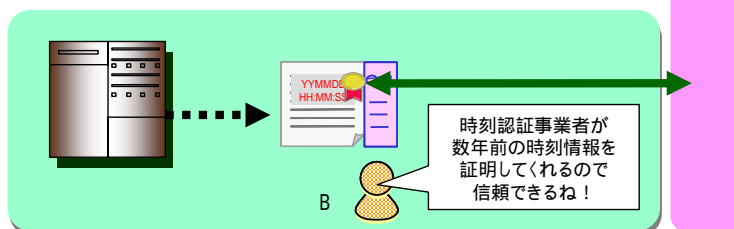
【例3への対応】 電子データの長期保存にタイムスタンプを用いることで不安解消

Aは、紙ベースの資料を電子化し、
時刻認証事業者にタイムスタンプ
を付与してもらった後に保存。



数年後...

Bは、Aの保存している電子データ
に付与されているタイムスタンプを
時刻認証事業者を確認。



**時刻認証事業者が、電子データに
付与されたタイムスタンプの時刻以
降、当該電子データに改ざんがない
ことを証明。**

Aが紙文書を電子データ化した(最初から電子データで作成しても同じ)直後に第三者である
時刻認証事業者にタイムスタンプを付与してもらって保存しておく、後日、Bが当該時刻情
報を検証する場合に時刻認証事業者が証明してくれるので信頼できる。