

『内部統制』の“いつ”に有用な“変更不可能な時計”

書き直しサンプル

■「時刻」は正確でなければなりません

業務を遂行していくと、その過程でさまざまな「業務記録」が発生します。「業務記録」には、たとえば注文書や領収書のようなものもあれば、ミーティング議事録やメールでの業務連絡のようなものもあります。

それらの記録には通常、「時刻」が記載されます。あたりまえの話ですが、その「時刻」は正確なものでなければなりません。時刻が正確でないと下記のような困った事態が起こります

<時刻が正確でないと起こる、困った事態>

(略)

しかし、「時刻が正確である」とはいったいどのようなことを意味するのでしょうか？

■「時刻」の正確さを保証することは難しい

たとえばここにある鉄道の切符があり、「発行日時：11月11日11時11分11秒」と印字されていたとしましょう。このようなゼロ目の切符はオークションで高値がつく可能性があります。しかし果たしてこの切符は本当に間違いなく「11月11日11時11分11秒」に発行されたものであると言えるでしょうか？

たとえば、切符自体は本物だったとしても、その切符を発行したマシンの内部時計が狂っていたら、券面に表示された時刻と、実際に発行された時刻は違っている可能性があります。

実は、「記録」に記載されている時刻が「正確な時刻である」と主張することは意外に難しいのです。

■「時刻」の正確性とはいったい何か？

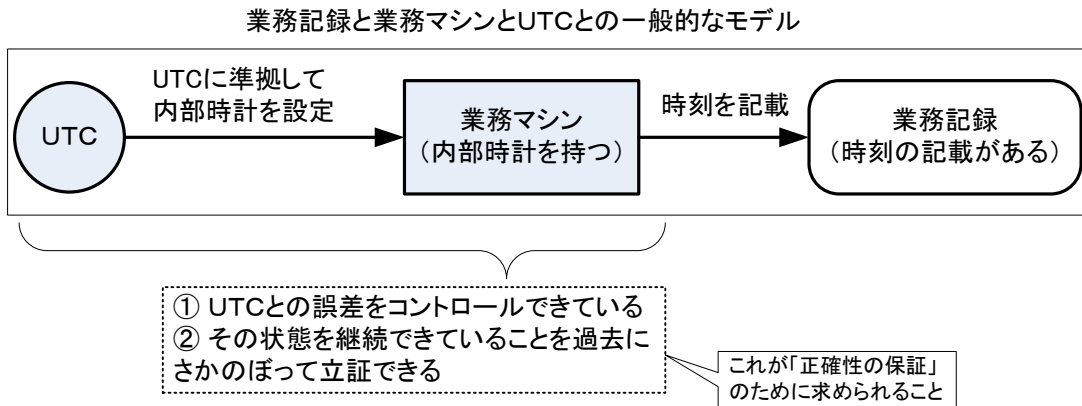
ここでいったんモデルを整理しておきましょう（図1）。

一般的に言って、業務を遂行するためには何らかの「業務マシン」が使われており、そこには内部時計があります。内部時計はUTC（または、UTCを基にそれぞれの地域において国家が定める標準時刻）に準拠して設定されていなければなりません。業務マシンは業務記録を発行生成するにあたってその「内部時計」の時刻を記載します。

一方、業務記録に記載されたその特定の「時刻」の正確性が問われるのは、それよりも未来のある時

点であり、場合によっては1年以上後ということもありえます。

図1：「時刻の正確性の保証」とはどのようなことか？



以上、これらを考慮しますと、「業務記録に書かれた時刻の正確性を保証する」ためには、下記2要件が満たされなければなりません。

<時刻の正確性保証要件>

- ① 業務マシンの内部時計と UTC との誤差をコントロールできていること
- ② その状態を継続できていることを過去にさかのぼって立証できること

「誤差をコントロールできている」というのは、具体的には次の各項が成り立つことです。

<誤差のコントロールの条件>

- a) 定期的に UTC（または、UTC を基にそれぞれの地域において国家が定める標準時刻）を基準として内部時計を補正できていること
- b) 補正を行う際に、その時点での誤差を記録できていること

また、「過去にさかのぼって立証」できなければならないのは、「業務記録」がそもそも「過去」のものだからです。「過去の業務記録」を監査証跡として利用するためには、「現在、業務マシンの内部時計が正確である」ことがわかっていても意味がありません。「過去のその時点で業務マシンの内部時計が正確であった」ことの信頼に足る根拠が必要になります。

■時刻の正確性保証に対する障害とは？

しかし、実際には通常の時刻管理方式で「時刻の正確性保証要件」を満たすことは困難です。

< N T P 以外の時刻管理方式の場合 >

たとえば（タイムソースの例）など、N T P 以外の時刻管理方式を使用するものは、下記の理由により実用になりません。

理由：略

< 公開 N T P サーバーを使用する場合 >

N T P サーバーを用いて業務マシンの時刻補正を行う方式はもっとも実用的ですが、以下の理由により時刻の正確性保証要件を満たすことができません。

R1) 後日、時刻取得元の特定(証明)ができない

R2) UTC とのトレーサビリティが確保できない

↑上記 2 項目は、「正しい時刻が維持されていたとしても、それを証明できない」ことを意味します。

R3) 通信上での改ざんが可能

R4) Client 側が時刻を取得する間隔の間で改ざんが可能

↑上記 2 項目は、「時刻が不正に改ざんされていたとしても、それを発見できない」ことを意味します。

これらの理由はいずれも時刻の正確性保証要件の②を不可能とするものです。

< 時刻の正確性保証要件（再掲） >

① 業務マシンの内部時計と UTC との誤差をコントロールできていること

② その状態を継続できていることを過去にさかのぼって立証できること

N T P は簡便に時刻の配信・補正を行うためのシステムであるため、監査に耐えうる証拠能力や不正行為（R3,R4 項）からの防衛はそもそも想定されていません。

特に問題なのは業務マシン側の管理権限を（正当・不当にかかわらず）持つ人員による改ざんの可能性（R3,R4 項）です。したがって、このような可能性をも排除しうる時刻監査の仕組みが必要です。

そのために当社が提案しているのが「監査時計」方式です。

■解決策：「監査時計」方式の導入

「監査時計」方式の要点は以下のようなものです。

2 種類の時計を持ち、一方の時計（監査時計）が、もう一方の時計（監査対象時計）を監査す

ることにより、一般的な時刻配信の問題点を解決します。

監査時計は 財団法人 日本データ通信協会から認定を受けたタイムスタンプをもとに時刻を作成します。

「監査対象時計」とは、通常の業務マシン側の内部時計のことを言います。こちらはこれまで通りNTPによる時刻同期方式を使うことができます。

一方、「監査時計」が、新しく導入される仕組みです。

「監査時計」は以下のような方式により正確な時刻を保持することが保証されます。

<監査時計の正確性を保証する仕組み>

ATM-1 NTPとは別の時刻配信方式(TSA方式)によりUTCとのトレーサビリティを確保

ATM-2 監査時計の管理権限を業務システム側の管理権限と分離する

したがって、あとは「監査時計」を基準にして「監査対象時計」の監査を行うことが可能になります。

<監査対象時計の時刻監査を行う仕組み>

ATM-3 監査時計を基準にして監査対象時計の監査を行う

ATM-4 そのログを安全な形で保存する

「監査対象時計の監査」とは、具体的には2つの時計の差異を記録することを意味します。

監査時計の正確性は保証されているため、それとの差異をたどることにより監査対象時計の正確性を検証することができます。

■TSA方式

TSA方式とは、UTCとのトレーサビリティを確保しつつ時刻配信を行う方法の一種です。TSA方式は以下の各装置により構成されます。

時刻配信局(TA)

タイムスタンプ局(TSA)

TSAクライアント

「時刻配信局(TA)」は、(UTCに準拠する)国家時刻標準機関から紐付いた時刻を保持しています。

タイムスタンプ局(TSA)はTAから時刻配信および時刻監査を受けています。このためTSAについても時刻の正確性が保証されています。

一方、TSAクライアントはタイムスタンプ局から時刻配信を受けますが、このときのデータ形式として、改ざんを検出可能な「TSA証明書」を含む「タイムスタンプトークン」を使用します。このタ

タイムスタンプトークンは、発行したタイムスタンプ局と受け取ったT S Aクライアントの双方の記録を
付き合わせて追跡検証することができるため、最終的にT S Aクライアントの時刻の正確性も保証され
ます。

