

『内部統制』の“いつ”に有用な “変更不可能な時計”

内部統制で“いつ”がなぜ重要か？

内部統制には監査が必要です。

監査とは、「ある対象について、基準に照らし証拠を収集して、その証拠に基づいて何らかの評価を行うこと」という定義になります。すなわち、ある対象に対して監督し検査することを意味します。

「基準」とは、社内の規定や業務のフロー、情報システムの利用規定・運用規定のことで、これらが守られていることを証明することが必要になります。社内の情報漏洩の対策として利用規制や証拠をとることにより違反行為の抑制を行うことが上げられます。この際に重要であるとされたのが「だれが、いつ、どこで、なにを」したかです。内部統制の構築においても信頼性の確保という観点からこれらの対応が重要です。

具体例で“いつ”の重要性を説明します。ある行為が“いつ”行われたかを知ることは重要です。本来は先月行うべき入力操作が、今日行われたのではないということが正しく確認できないようでは、入力された情報の正当性が確保されたとは言えません。このため、利用者が操作を行った時刻を管理しておくことは重要です。

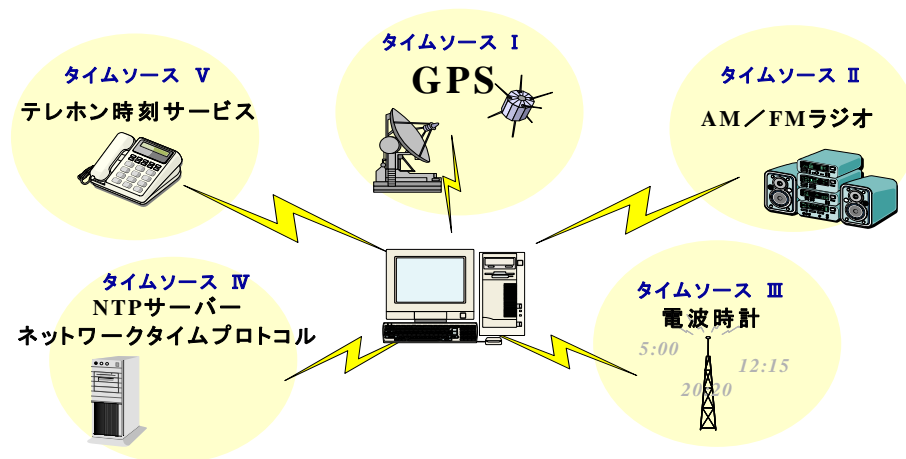
そのためには処理に係る各コンピュータの時刻を正確に合わせておく必要があります。

正確な信頼性のある“いつ”を作る方法

条件

1. 時刻取得元の特定(証明)ができること (時刻取得元は **第三者時刻**)
2. 協定世界時 UTC(NICT)とのトレーサビリティが確保できること
3. 時刻差の監視ができ、改ざんができないこと
4. 後日、時刻取得の事実が証明可能なこと

一般的な時刻配信の問題点

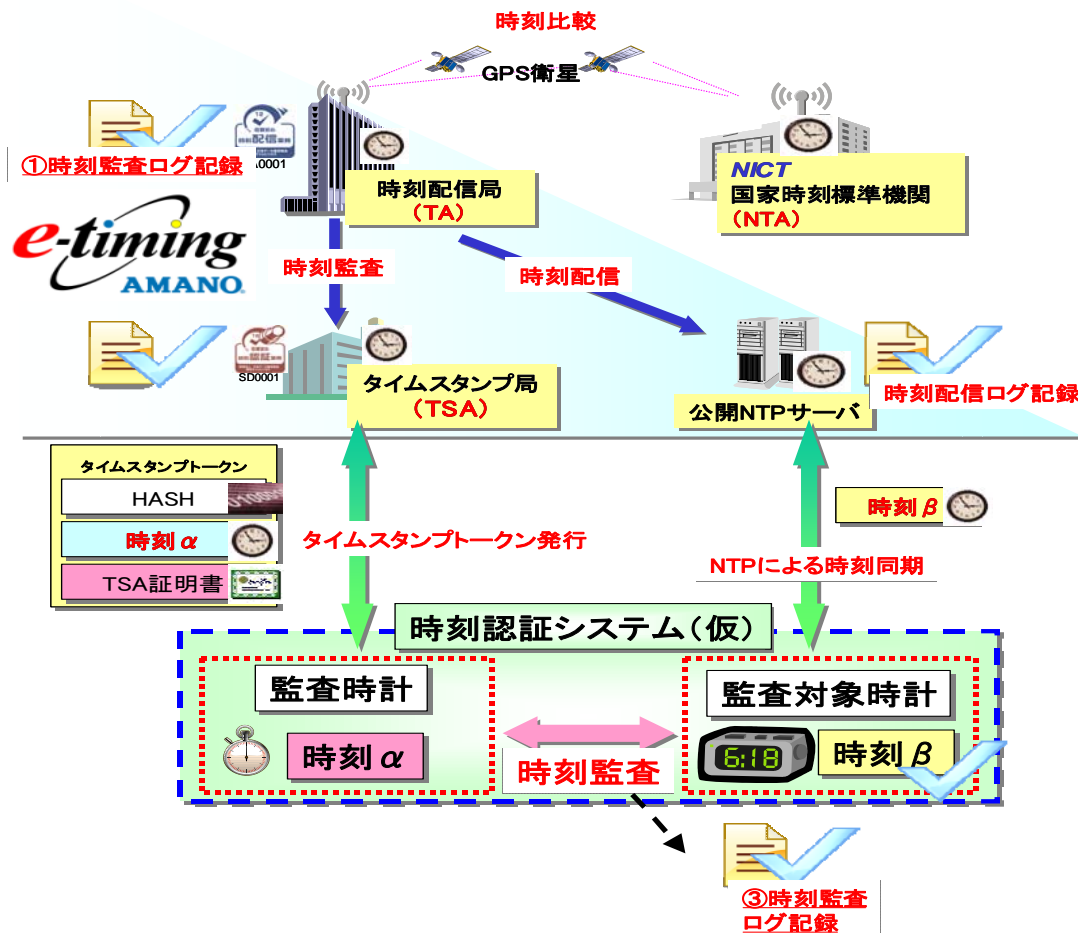


1. 後日、時刻取得元の特定(証明)ができない → I、II、III、IV
2. 協定世界時 UTC(NICT)とのトレーサビリティが確保できない
→ I、II、III、IV
3. 通信上での改ざんが可能 → I、II、III、IV
4. Client側の時刻を取得間隔の間で改ざんが可能 → I、II、III、IV、V

解決手段

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。



問題点ごとに解決方法を記します。

1. 後日、時刻取得元の特定(証明)ができない

解決策 監査時計はタイムスタンプトークンを元にしていますので TSA 証明書により時刻源であるタイムスタンプ局(TSA)の特定が可能となります。

2. 協定世界時 UTC(NICT)とのトレーサビリティが確保できない

解決策 タイムスタンプトークン内の時刻αは国家時刻標準機関から紐づいた時刻を保持している時刻配信局(TA)から時刻監視を受けたタイムスタンプ局(TSA)の時刻から作成している。時刻認証システムでは、この時刻αを受け取り監査時計を補正した際のログを保持しているため、そのログとタイムスタンプ局(TSA)のタイムスタンプトークンの発行ログ、時刻配信局(TA)の監査記録を追うことにより国家時刻標準機関とのトレーサビリティを確保できます。

3. 通信上での改ざんが可能

解決策 時刻認証システム内でタイムスタンプトークンの検証を行うことにより改ざんを検知が可能となります。

4. Client 側の時刻を取得間隔の間で改ざんが可能

解決策 監査時計はソフト的に変更ができないような仕組みにすることにより改ざんができない仕組みになります。例、OS からは時計セットできない。

特徴

2 種類の時計を持つことの意味

- ・ タイムスタンプトークンから取得した時刻 α の信頼性は高いのですが取得した時点では通信時間や、システムの処理時間が加わり時刻認証システムで受け取った時には遅れています。これを補うために NTP プロトコルを利用して時刻を取得する監査対象時計が必要になります。
あるルールに則り、監査時計が監査対象時計を監査することにより精度の高い時刻を監査対象時計から本システムを組み込んだ仕組みに供給可能となります。
- ・ 一般的な時刻同期システムでは、組み込み機器が時刻を要求した際に監査をせずに時刻を引き渡します。このため、組み込み機器内で時刻が改ざんされていても検知することができません。本システムでは組み込み機器から監査対象時計への時刻の要求毎に監査時計で監査を行います。これにより極めて信頼性の高い時刻を機器に供給することが可能となります。

最後に

信頼性の高い時刻の必要性については、取引時間が重要な銀行や証券会社等の金融機関、ネットオークション、電子入札、病院の電子カルテ、ネットゲーム、リアルマネートレーディング、バーチャルマネー等への適用も考えられます。

本時刻認証システムは技術的な提案段階です。今後、お客様からご意見等をいただき具現化を検討していこうと考えています。

ご興味のある方は、下記の Mail アドレスまでお問い合わせくださいますようお願い申し上げます。