

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跡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。

↑このパートは「内部統制と監査の説明」になっているため、「監査時計」について説明したい文書の冒頭で書くのには重い（難解な）内容です。

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。

↑これでは具体例になっていないので、「ある行為」の実例を出しましょう。領収書を出すとか、資料請求データを入力するとか、業務イメージの湧くような具体例が欲しいところ。

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。

↑「正確に合わせておく必要があります。ところが、これが意外に難しいのです」・・・のよう一言足しておくと、読者に親切です。

冒頭部分について少々補足します。

この文書の主たるストーリーは下記4行のはずですね。

- S1) コンピュータの時刻は正確に合わせておかなければなりません
- S2) そして、時刻が正確であったことを過去に遡って立証できなければなりません
- S3) ところがこれが実は難しいのです。
- S4) そのために当社は「監査時計」方式を提案します。

一方、オリジナル原稿では

- S0) 内部統制には監査が必要であり、監査とはこれこれこういうものだ

という説明から始まっていました。

もし、内部統制と監査について知識を持っている人が読むと、S0の内容は当たり前すぎてうっとうしく感じます。

逆にあまり知識を持っていない人が読むと、S0の内容は難しそうで抵抗感を覚えます。

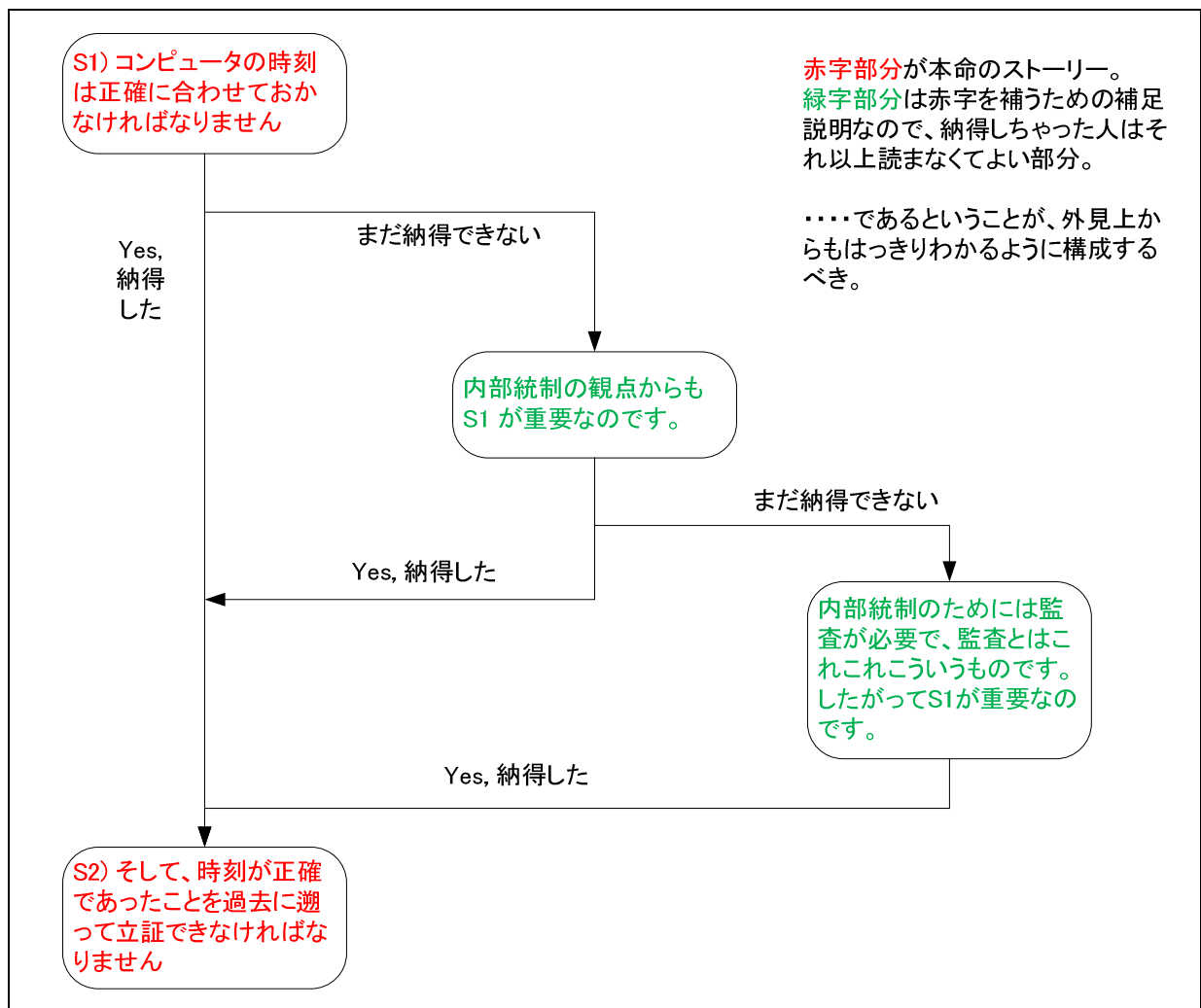
さて、ここでS0とS1を並べてみましょう。

S0) 内部統制には監査が必要であり、監査とはこれこれこういうものだ

S1) コンピュータの時刻は正確に合わせておかなければなりません

この文書を先に読み進めるにあたって、より重要なのはS0とS1のどちらでしょうか？

と考えると、もっとも重要なのはS1であり、S0はそれを補強するための補足説明に当たるものです。要するにS0は本来飛ばして読んでもいいところなので、「ここは飛ばして読んでもいいよ」ということがハッキリわかるように構成しましょう。そうなってれば、読者は安心してとばし読みすることができます。



■対応関係があるならある、ないならないでハッキリさせるべき

正確な信頼性のある時刻を作る条件として以下の4項目が挙がっています。

- A 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)
- A 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
- A 3. 時刻差の監視ができ、改ざんができないこと
- A 4. 後日、時刻取得の事実が証明可能なこと

一方、一般的な時刻配信の問題点として以下の4項目が挙がっています。

- B 1. 後日、時刻取得元の特定(証明)ができない → I、II、III、IV
- B 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
- B 3. 通信上での改ざんが可能 → I、II、III、IV
- B 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

これは一見すると A 1～A 4がB 1～B 4にそれぞれ対応しているように見えますが、内容を良く読むと A 3=B 3+B 4 という対応関係になっていて、A 4はどこに行ったんだろう? という混乱を招きます。改善を求めたいところです。

■タイムソースを5種類出すのは多すぎる

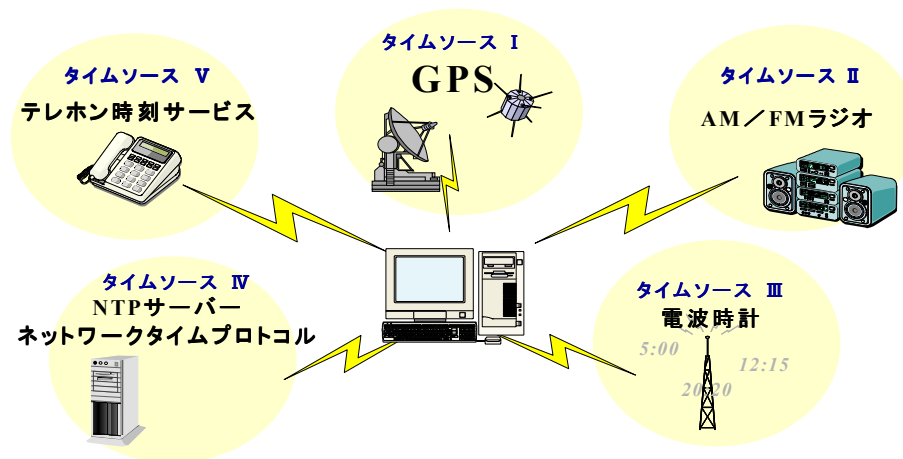
タイムソースの例として I～V まで5種類が挙がっていますが、現実にはI VのNTP以外はコンピュータシステムの時間管理メソッドとしては非現実的でしょうから、ここは格差をつけて扱うべきでしょう。

事実上、「監査時計」の仕組みは「NTP」を補完する形で機能するんですよね？ であれば、

NTPだけではコンピュータシステムの時間監査は不可能だ。
だから当社の監査時計を合わせて使ってくれ

というメッセージが主役になるはずで、NTP以外のタイムソースは「その他大勢」扱いでいいです。
ハッキリ差をつけて扱きましょう。

また、この図↓は少々問題で、



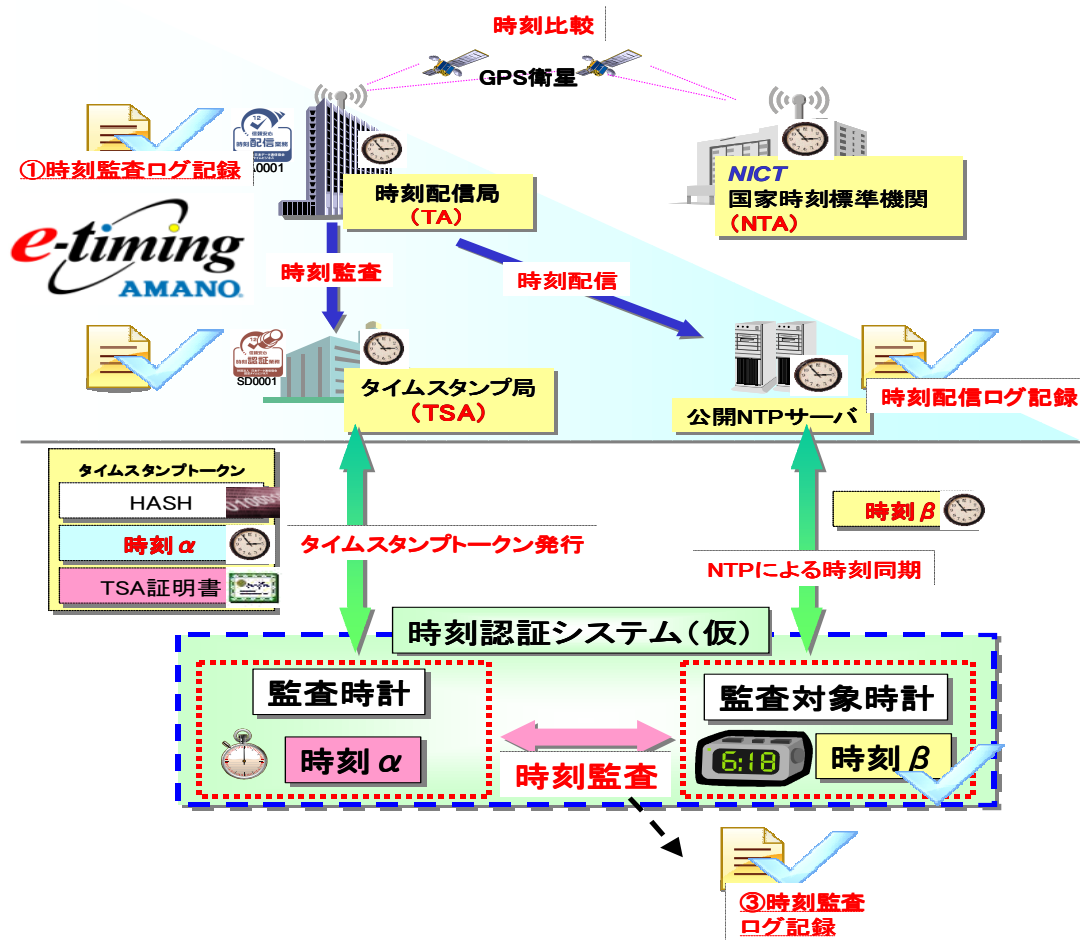
この種の「中心があってその周囲を取り巻く」タイプの配置をする場合、読者の視線は中心の左上 (V テレホン) または真っ直ぐ上 (I GPS) を出発点にして右回りに進みます。実際には上記のレイアウトなら左上のVから見始める人が大半と考えられるため、

あれ？ 最初がV？ で次がI？ なんじゃこれ

となってしまう可能性が高いです。レイアウトを変えましょう。

その際、「NTP」と「その他大勢」という差をつけるべきなので、NTPをもっとも目立つ位置に大きく持ってきて、その他は小さくひとかたまりにしておくことをオススメします。

■この図はなかなか良くできていると思います。(若干、色を使いすぎの気はしますが)



■「TSA」の解説を始めるタイミングは難しい

「TSA」のように純然たるテクノロジーの説明を始めると、どうしても技術的専門用語が多発するため、読者に「新しい用語を理解する」負担をかけがちになります。できるだけ、TSAのような「実装技術」に対する上位の枠組みである「要求事項」のイメージを読者に持たせてから、実装技術の説明をするほうが良いと思われます。

■仮称でいいのでシステム名が欲しい

「時刻認証システム(仮)」だと一般名称っぽいので記憶に残りにくいです。このシステムの固有名があるほうがいいですね。仮称でもいいので。「アマノ〇〇〇〇システム」とか「××××メソッド」とか、名前をつけて何度も使うことは重要です。とりあえず書き直し案のほうでは「監査時計方式」と呼んでおきました。

Amano Digital Time Stamp Service というのがその名前なのでしょうか？