

## あなたは、クラウドサービスの 安全を信じますか？

2011.05.28

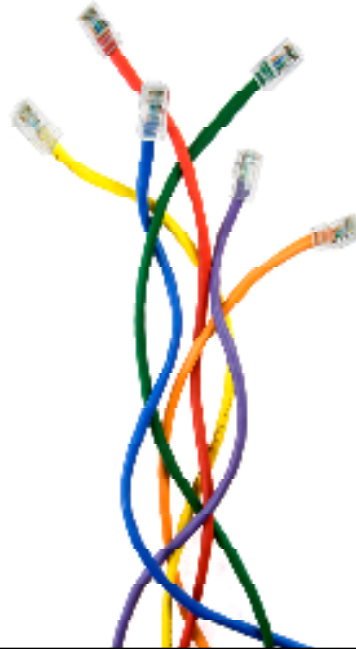
デロイト トーマツ リスクサービス株式会社

パートナー

公認会計士(CPA)

公認情報システム監査人(CISA)

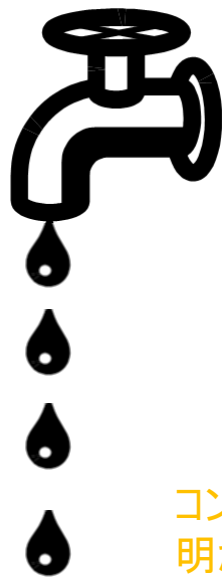
丸山 満彦



- パブリッククラウドサービスを社会インフラとして普及するための考え方
- 水道
- 株式市場

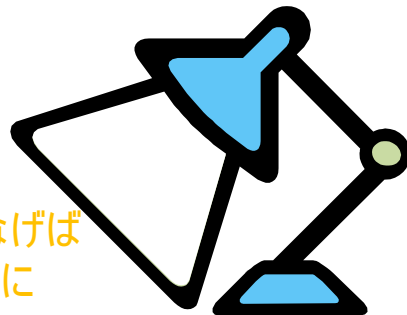
# クラウド・コンピューティング

ユーザーから見ればこんな感じ？

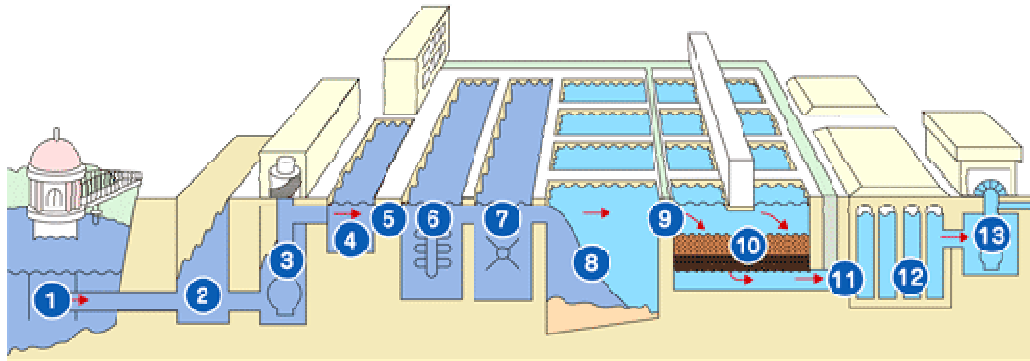


蛇口をひねれば  
水がでるように

コンセントにつなげば  
明かりがつくように



蛇口の向こう側は



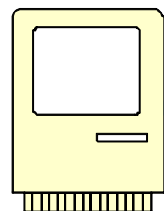
スライドに記載された事項は講演者の所属する法人、関連する団体の公式見解ではありません。

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved.

5

ユーザからみたらこんな感じ？

コンピュータを買ってきて...



ネットワークにつなげば...



がすぐに使える。。。

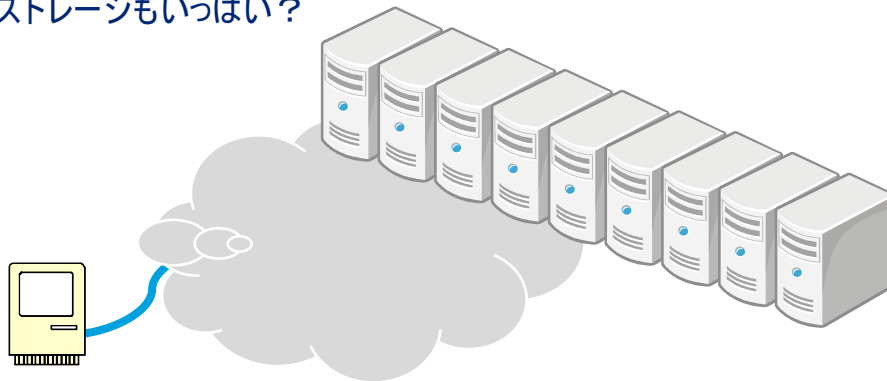
スライドに記載された事項は講演者の所属する法人、関連する団体の公式見解ではありません。

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved.

6

## クラウドの向こう側は？

- サーバーがいっぱい？
- いろいろなソフトが動いている？
- ストレージもいっぱい？



We  
don't  
care!

# We care...

## 安定供給

## 品質・安全性

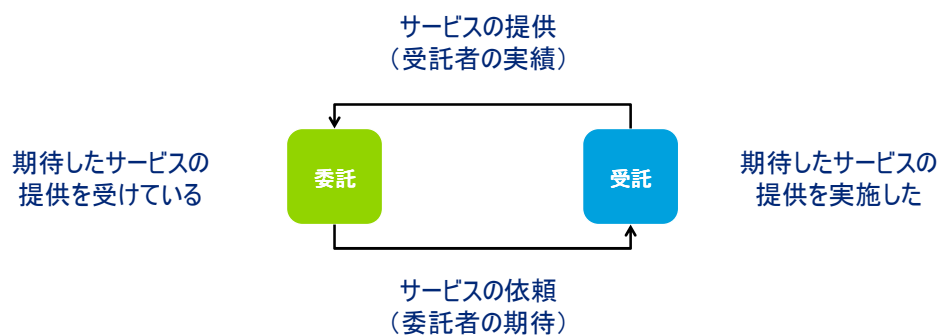
## コスト

フッター

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved.

9

### 何がポイントか？



フッター

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved.

10

# 品質・安全性

## 社会調整機能としてのリスクコミュニケーションツール(規制や開示)

- **最低限基準型 (Yes or No)**  
(最低限の品質のための基準を規定する)
  - ✓ 水道水の規制
  - ✓ 株式上場基準
- **開示基準型**
  - **情報開示基準型 (グラデーション)**  
(開示する項目を規定し、その項目を開示する)
    - ✓ 財務報告基準
  - **実態保証基準型 (Yes or No)**  
(評価する基準を規定し、それを達成していることを開示する)
    - ✓ 内部統制基準 (US-SOX)

## Yes or No型とグラデーション型の長所・短所

- **Yes or No型**
  - 単純でわかりやすい
  - Yes Noを分ける基準の合意が必要だが、一意に決めるのは難しい。
  - 柔軟な期待に対する対応が困難
- **グラデーション型は、**
  - 尺度のメッシュが細くなるほど
  - 尺度の数が増えるほど細くなるほど素人ではわかりにくくなる。

## 水道水が安全なのは、様々な仕組みのおかげ

- **法律（水道法）**
  - 水道水質基準
    - ✓ 水質基準項目と基準値（50項目）
    - ✓ 水質管理目標設定項目と目標値（28項目129物質）
    - ✓ 要検討項目と目標値（44項目）
- **適切な運営体制**
- **適切な運営設備**
- **適切な運営母体**

## (参考)水質基準

項目	基準	項目	基準
一般細菌	1mlの検水で形成される集落数が100以下	総トリハロメタン	0.1mg/L以下
大腸菌	検出されないこと	トリクロ酢酸	0.2mg/L以下
カドミウム及びその化合物	カドミウムの量に関して、0.01mg/L以下	プロモジクロメタン	0.03mg/L以下
水銀及びその化合物	水銀の量に関して、0.0005mg/L以下	プロモホルム	0.09mg/L以下
セレン及びその化合物	セレンの量に関して、0.01mg/L以下	ホルムアルデヒド	0.08mg/L以下
鉛及びその化合物	鉛の量に関して、0.01mg/L以下	亜鉛及びその化合物	亜鉛の量に関して、1.0mg/L以下
ヒ素及びその化合物	ヒ素の量に関して、0.01mg/L以下	アルミニウム及びその化合物	アルミニウムの量に関して、0.2mg/L以下
六価クロム化合物	六価クロムの量に関して、0.05mg/L以下	鉄及びその化合物	鉄の量に関して、0.3mg/L以下
シアン化物イオン及び塩化シアン	シアンの量に関して、0.01mg/L以下	銅及びその化合物	銅の量に関して、1.0mg/L以下
硝酸態窒素及び亜硝酸態窒素	10mg/L以下	ナトリウム及びその化合物	ナトリウムの量に関して、200mg/L以下
フッ素及びその化合物	フッ素の量に関して、0.8mg/L以下	マンガン及びその化合物	マンガンの量に関して、0.05mg/L以下
ホウ素及びその化合物	ホウ素の量に関して、1.0mg/L以下	塩化物イオン	200mg/L以下
四塩化炭素	0.002mg/L以下	カルシウム、マグネシウム等(硬度)	300mg/L以下
1,4-ジオキサン	0.05mg/L以下	蒸発残留物	500mg/L以下
シス-1,2-ジクロロエチレン及びトランス-1,2-ジクロロエチレン	0.04mg/L以下	陰イオン界面活性剤	0.2mg/L以下
ジクロロメタン	0.02mg/L以下	ジェオスミン	0.00001mg/L以下
テトラクロロエチレン	0.01mg/L以下	2-メチルイソボルネオール	0.00001mg/L以下
トリクロロエチレン	0.03mg/L以下	非イオン界面活性剤	0.02mg/L以下
ベンゼン	0.01mg/L以下	フェノール類	フェノールの量に換算して、0.005mg/L以下
塩素酸	0.6mg/L以下	有機物(全有機炭素の量)	3mg/L以下
クロロ酢酸	0.02mg/L以下	pH値	5.8以上8.6以下
クロロホルム	0.06mg/L以下	味	異常でないこと
ジクロロ酢酸	0.04mg/L以下	臭気	異常でないこと
ジブロモクロメタン	0.1mg/L以下	色度	5度以下
臭素酸	0.01mg/L以下	濁度	2度以下

©2010 Deloitte Touche Tohmatsu, LLC. All rights reserved.

15

## 水道水の品質

一定の品質を維持していれば、後はどのように表示してアピールするか？

**景品表示法**

健康のために必要と考える**最低限のレベル**

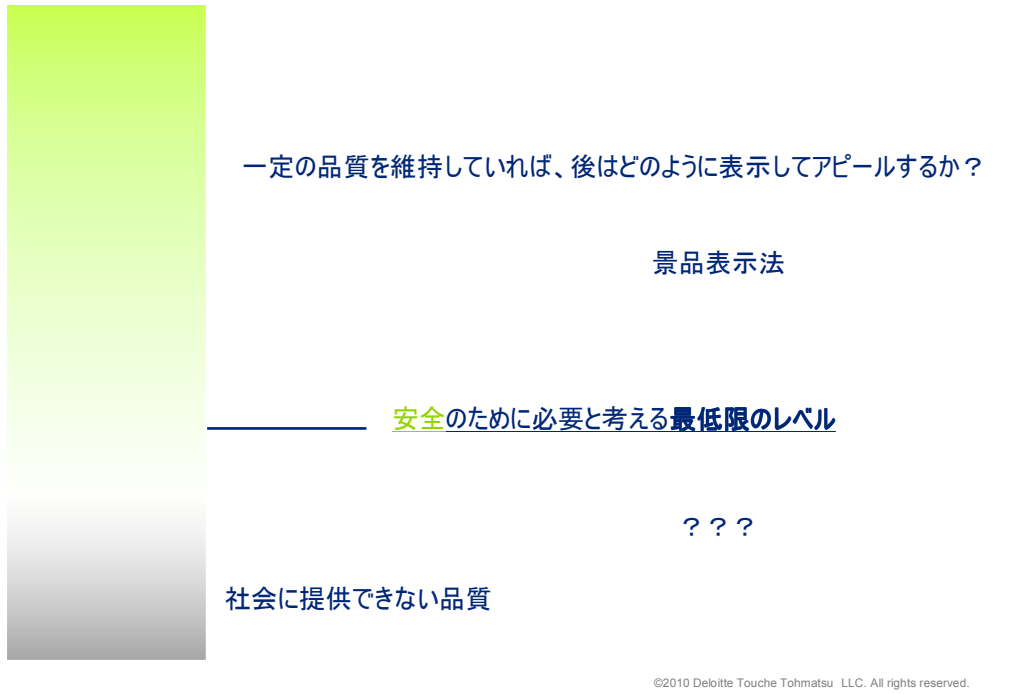
**水道法**

社会に提供できない品質

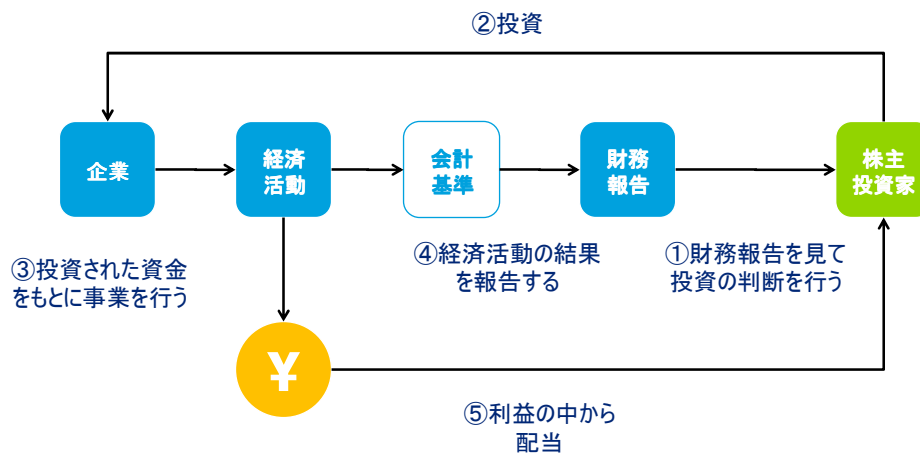
©2010 Deloitte Touche Tohmatsu, LLC. All rights reserved.



## クラウドサービスの品質？



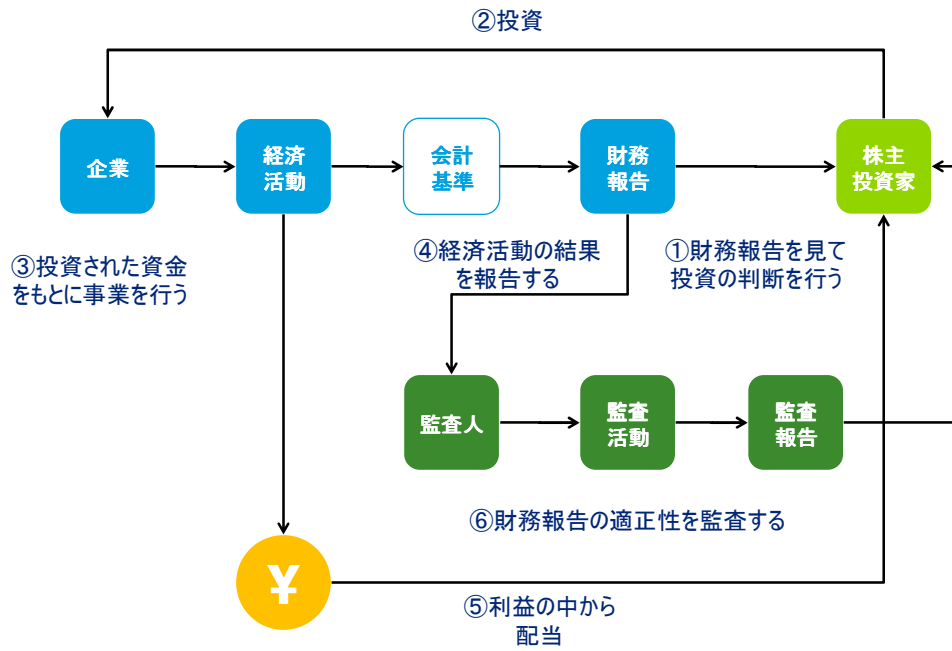
## 結果が重要な会計データの開示



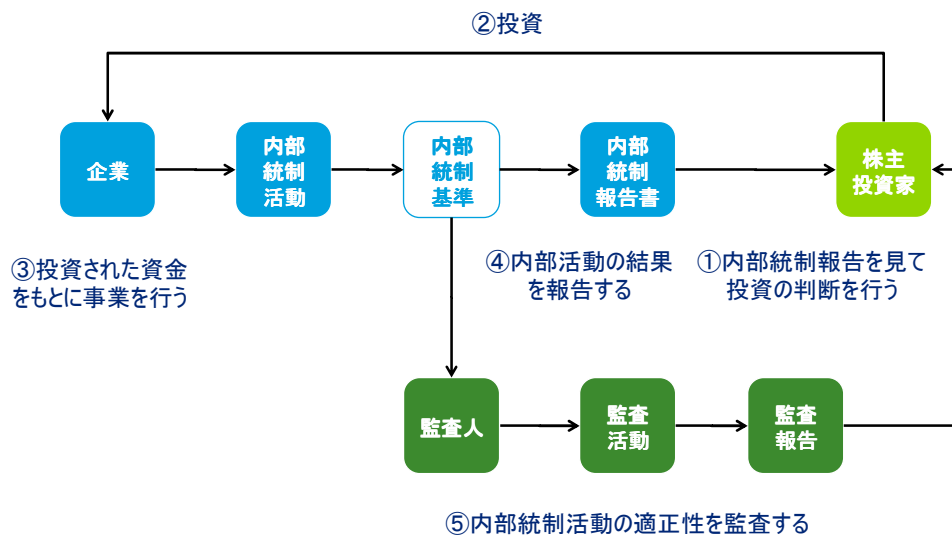
財務報告＝経済活動を投資家等に伝達するための手段

会計基準＝経済活動を財務報告に変換するための函数

## さらに監査による報告情報の信頼性の向上

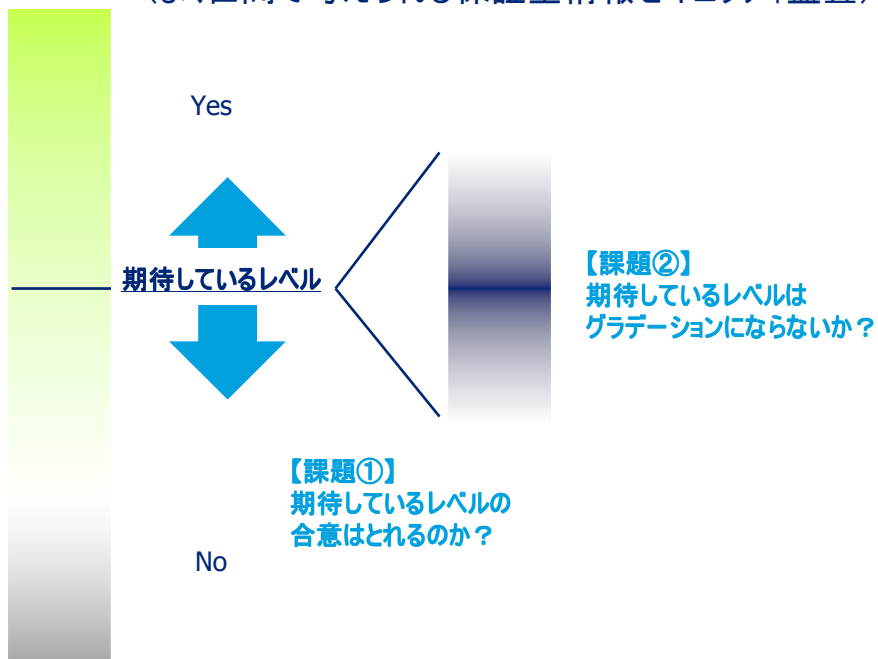


## 実態保証型 (US-SOX)

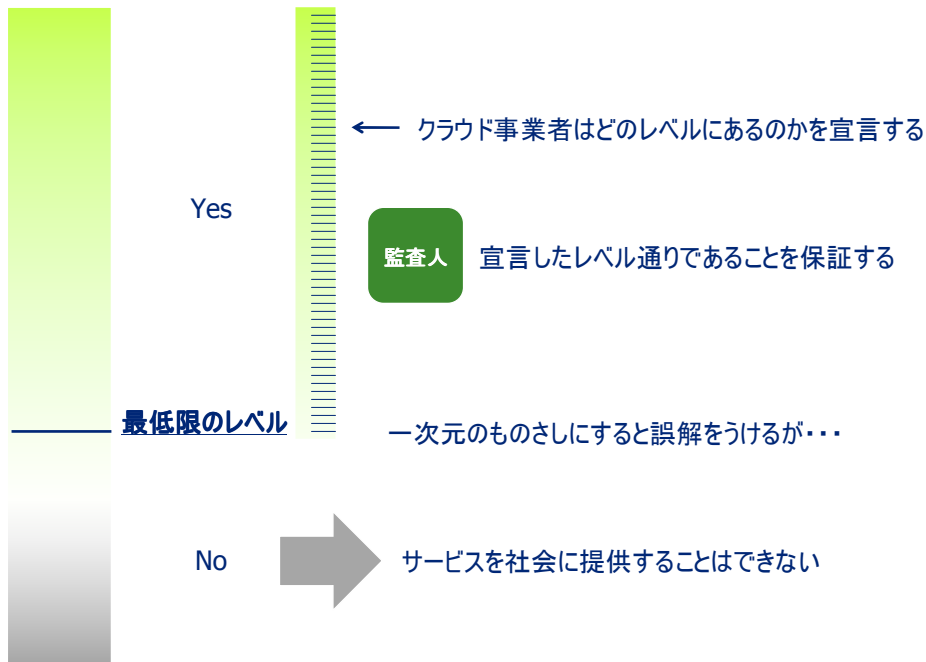


# クラウドサービスの安全性を信頼する 仕組み

仮説1：情報セキュリティ基準を準拠しているかどうか式  
(よく世間で考えられる保証型情報セキュリティ監査)



## 仮説2:最低基準方式と情報開示基準型を組み合わせた仕組み



フッター

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved. 23

## 仮説2-1:評価の基準は会計基準のようなものが現実的ではないか

- 事業者の信頼性に関する基準
- サービス品質に関する基準
  - 実施している対策
  - 実施した結果
    - ✓ サービス停止時間
    - ✓ .....
- 安全性に関する基準

やっていることだけでなく

結果も開示

フッター

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved. 24

## 実はそういう制度はすでにある

- ASP・SaaS安全・信頼性に係る 情報開示認定制 by マルチメディア振興センター
  - <http://www.fmmc.or.jp/asp-nintei/gaiyo.html>

表 一定の要件を考慮すべき項目の内容	
【対策・措置などを行っていない場合に非認定とする項目】	
コンプライアンス	情報セキュリティに関する規程などの整備
サービス基本特性	サービス(事業)変更・終了に係る問合せ先
アプリケーション、プラットフォーム、サーバ・ストレージ等	死活監視(ソフトウェア、機器)
	ウイルスチェック
	記録(ログ等)
	セキュリティパッチ管理
ネットワーク	ファイアウォール設置等
	ID・パスワードの運用管理
	ユーザ認証
	管理者認証
サービスサポート	連絡先
	メンテナンスなどの一時的サービス停止時の事前告知
	障害・災害発生時の通知
【最低水準数値以下の場合に非認定とする項目】	
サービス基本特性	サービス(事業)変更・終了時の事前告知時期

フッター

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved.

25

## 開示すべき基準は、社会的な合意でつくるべき (一般に公正妥当)



情報を理解できるほど賢くなる必要がある

提供者の不都合な情報も開示すべき  
(有価証券報告書をみてみる！)

フッター

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved.

26

## 監査を有効にするための前提

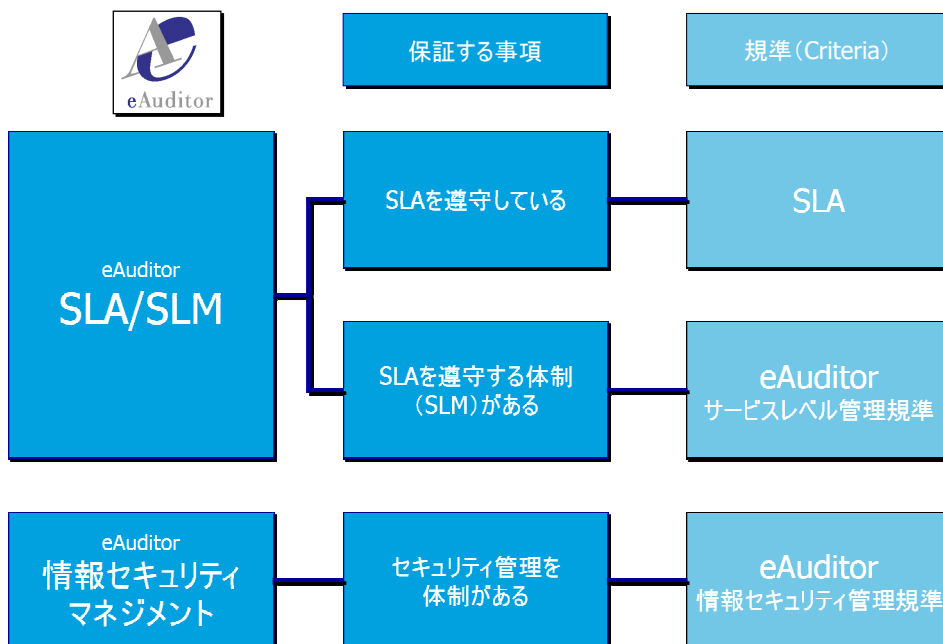
- 評価者についての前提
  - 信頼＝倫理観、客観性
  - 能力＝評価の対象や基準を理解し、論理的に結論を導ける  
ある評価者の存在を前提としている。
- 評価基準(Criteria)についての前提
  - 測定尺度が設定可能（判断がぶれないようにする必要がある）
    - ✓ 例えば、「サービス停止時間」とは何か？
  - 利害関係者が同意をしている

## Some more thought

- 情報開示
  - 「守秘義務契約を締結した上で開示する情報」と「公開できる情報」と区分する
- 第三者監査（カッコ内は財務諸表監査）
  - 事業者を一律に監査を義務付ける必要はない（上場企業、大会社）
  - すべての情報を監査対象とする必要はない（有価証券報告書）
  - 保証水準も段階をつけれる（監査報告書、レビュー報告書）

# まとめ

実は私が10年前に考えていたスキーム  
eAuditor監査の種類と規準(Criteria)



課題は、監査コストを社会的に負担する覚悟があるのか

- 低コストの監査 => 監査の信頼性が低い => 使えない
- 信頼性が高い監査 => 高コストの監査 => 使わない



ご静聴ありがとうございました・・・



# Deloitte. トーマツ.

トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファーム各社(有限責任監査法人トーマツおよび税理士法人トーマツ、ならびにそれぞれの関係会社)の総称です。トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャル アドバイザーサービス等を提供しております。また、国内約40都市に約7,000名の専門家(公認会計士、税理士、コンサルタントなど)を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はトーマツグループWebサイト([www.tohmatsu.com](http://www.tohmatsu.com))をご覧ください。

Deloitte(デロイト)は監査、税務、コンサルティングおよびファイナンシャル アドバイザーサービスをさまざまな業種の上場・非上場クライアントに提供しています。全世界150ヶ国を超えるメンバーファームのネットワークで、ワールドクラスの品質と地域に対する深い専門知識により、いかなる場所でもクライアントの発展を支援しています。デロイトの約170,000人におよぶ人材は"standard of excellence"となることを目指しています。

Deloitte(デロイト)とは、デロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)およびそのネットワーク組織を構成するメンバーファームのひとつあるいは複数指します。デロイト トウシュ トーマツ リミテッドおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。その法的な構成についての詳細は[www.tohmatsu.com/deloitte](http://www.tohmatsu.com/deloitte)をご覧ください。

© 2010 Deloitte Touche Tohmatsu LLC

Member of  
Deloitte Touche Tohmatsu Limited

©2010 Deloitte Touche Tohmatsu LLC. All rights reserved.