

デジタル・フォレンジック・コミュニティ2007

## 保証型監査とフォレンジック

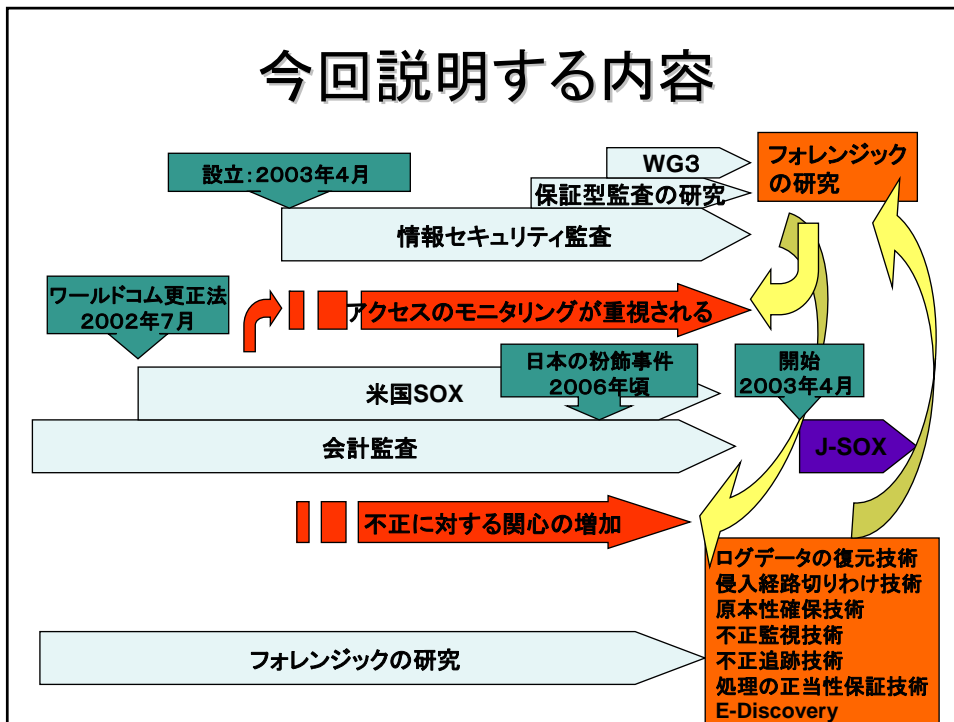
～フォレンジックは内部統制の構築と監査  
をどのように変えるのか～

JASA 日本セキュリティ監査協会  
調査研究部会長 長尾慎一郎

## 概要

- JASAでは情報セキュリティの内部統制の保証型監査を推進しております。
- ここでは、内部統制を広くとらえ、経営者・企業の不正に対して取り組んできた過去の歴史から、内部統制の限界について考えます。
- そして、内部統制にフォレンジック技術を利用することにより可能となる将来的な内部統制の構築を考えます。
- 内部統制に必要なログの準備も含め、事前に対応すべき内部統制について提案します。

# 今回説明する内容



## アウトライン

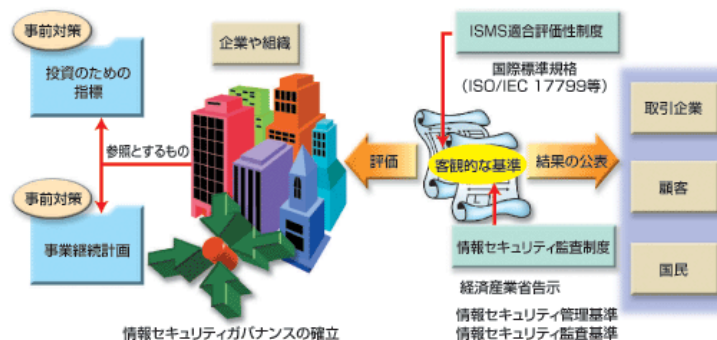
- JASAについて
  - 情報セキュリティ監査
  - 保証型監査
- 監査・内部統制と不正
  - 会計監査、セキュリティ監査、フォレンジック
  - 会計監査とデジタルフォレンジック
  - 情報セキュリティ監査とデジタルフォレンジック
- フォレンジック技術の利用
  - 内部統制に必要な技術
  - 将来期待される監査
- JASA 調査研究部会WG3活動

# JASAについて

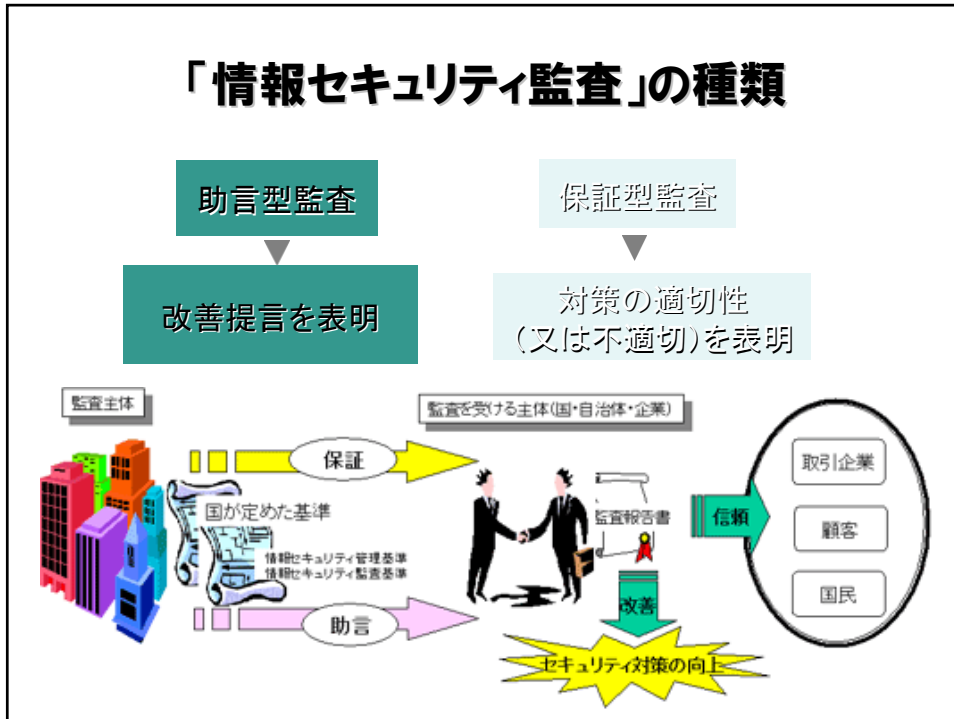
## 「情報セキュリティ監査」とは

情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動

～経済産業省「情報セキュリティ監査報告書」



## 「情報セキュリティ監査」の種類



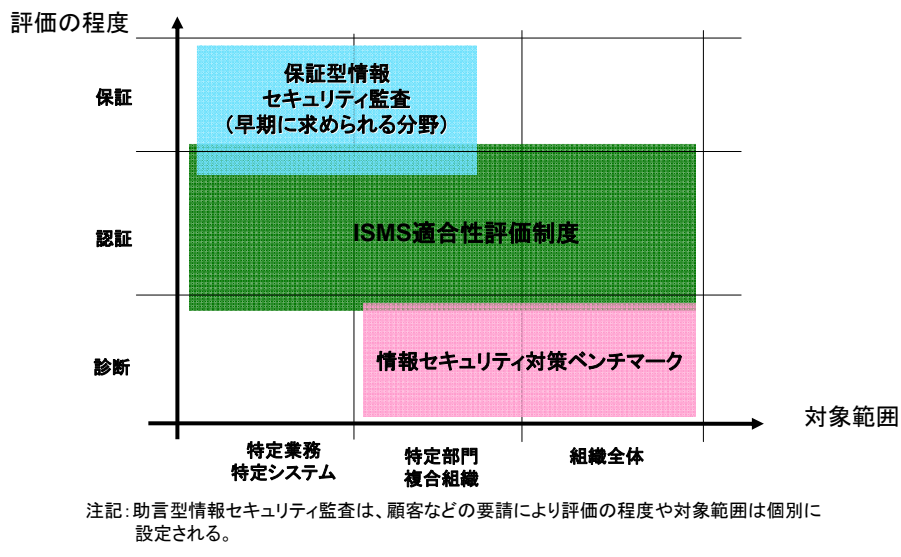
## 情報セキュリティ監査と他制度の関係

評価の程度	診断	認証	保証
制度	情報セキュリティ対策ベンチマーク	ISMS適合性評価制度	情報セキュリティ監査*2
制度利用の目的	組織の情報セキュリティ対策の整備・運用状況の自己評価	情報セキュリティマネジメントシステムの認証	顧客等が期待する情報セキュリティマネジメントの整備・運用状況の保証
目指すべきセキュリティ水準	経営者が目指す水準	経営者が目指す水準	顧客等が期待する水準
対象範囲	組織体*1	組織体*1、特定業務・サービスなど	特定業務・サービス又は組織体*1
評価尺度	JISQ27001を参照し作成された25の評価項目 (簡易的・固定)	JISQ27001 (包括的)	情報セキュリティ管理基準等を参照し作成された個別管理基準 (個別的)
評価者	経営者、管理者	審査員	監査人
評価のアウトプット	散布図、レーダーチャート、スコア、助言	ISMS認証登録証	保証意見
費用	無料	有料	有料

\*1: 組織体とは、組織の全部・一部・複合組織を指す。複合組織とは、複数の連携した組織群をグループとして評価するケースである。

\*2: 保証型情報セキュリティ監査。

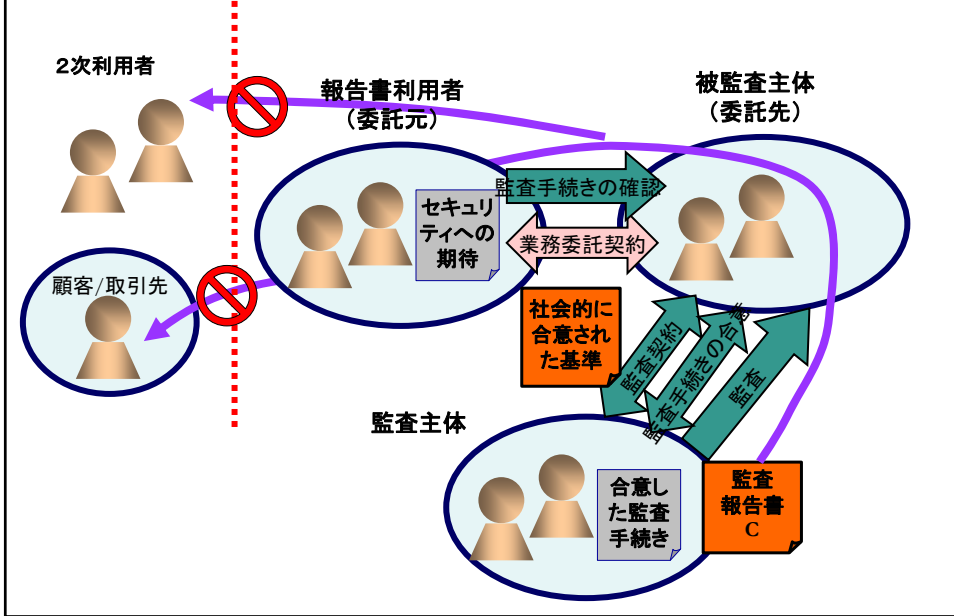
## 情報セキュリティ監査と他制度の関係



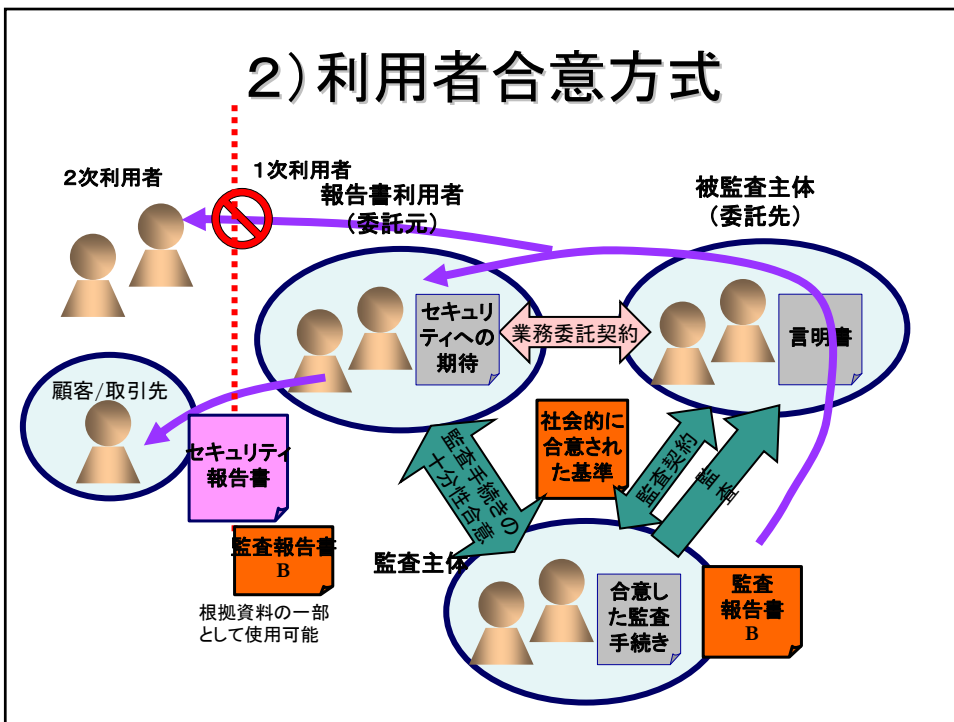
## 保証型監査

- この概念フレームワークの整理では、特に重要なポイントとして、情報セキュリティ監査人が実施する監査手続きの十分性と監査報告書の利用者との関係に注目
- その結果として、保証型情報セキュリティ監査を次の三つに大きく区分する
  - 1) 被監査主体合意方式
  - 2) 利用者合意方式
  - 3) 社会的合意方式

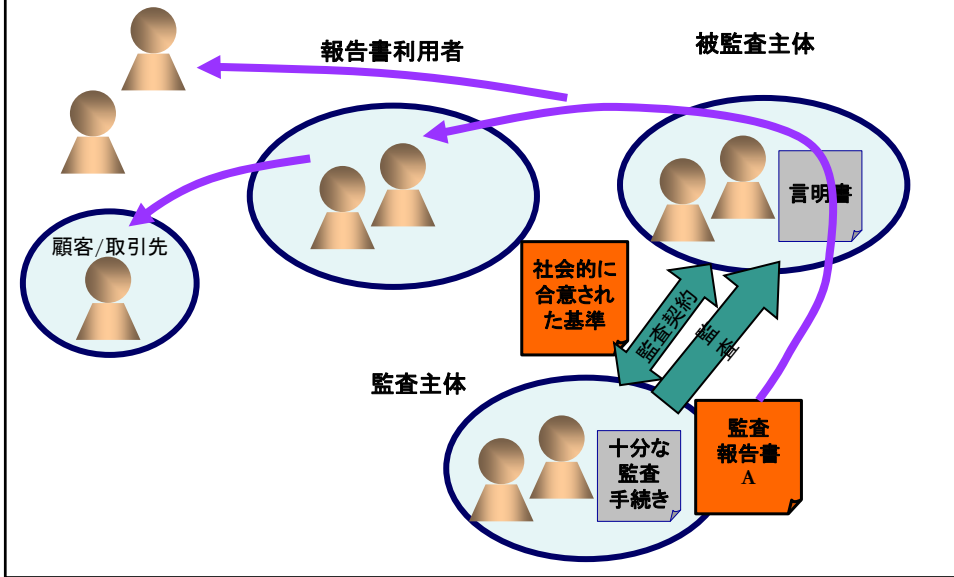
# 1) 被監査主体合意方式



# 2) 利用者合意方式



### 3) 社会的合意方式

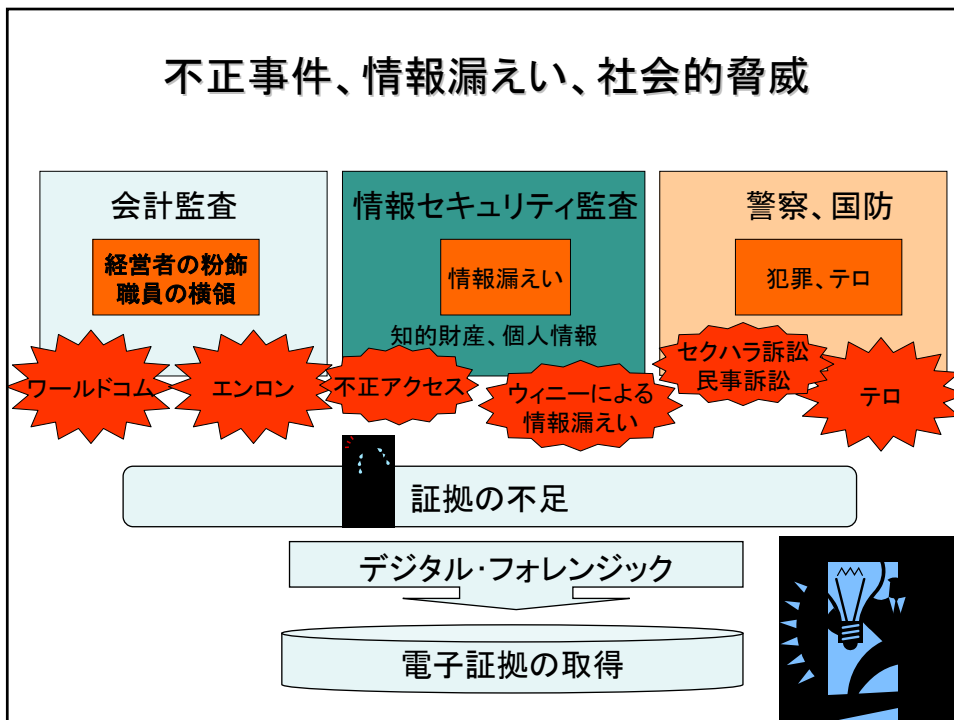


監査・内部統制と不正

## 会計監査、セキュリティ監査、フォレンジック

	会計監査(企業)	セキュリティ監査	一般社会 国防、警察
目的	会計情報の信頼性付与	情報の保護	国防、警察 市民の安全
脅威 不正事件	会計不正(エンロン、 ワールドコム) 株価操作 インサイダー取引	営業機密情報の漏洩 個人情報漏洩	テロ 犯罪 セクハラ訴訟
フォレンジック の利用 技術的対策	電子メールの解析 会計データの解析 ログの監視 データマイニング 統合監視ツール	ネットワークの追跡 ログの監視 統合監視ツール	空港の監視 Nシステム 電話の盗聴 GPS

## 不正事件、情報漏えい、社会的脅威



## 会計監査、セキュリティ監査、フォレンジックの差異

	会計監査	セキュリティ監査	フォレンジック
主な不正事例	経営者の粉飾 職員の横領	情報漏えい	刑事訴訟 民事訴訟
不正の行為者	内部者	外部者	内部者 外部者
目的	早期発見	早期発見	事故が起こって から追跡し、 証拠の確保
対策	・企業のガバナンス ・会計監査の強化 ・その他？	・ISO27001 ・情報セキュリティ監査	追跡技術 証拠確保
継続性	継続的なコントロール	継続的なコントロール	個別的な調査
コストと効果	投資家の損失の回避	漏洩による損失の回避	訴える側の利益

## ワールドコム的事件と内部監査人の活躍

- 1983年のAT&Tの解体と自由化により、利益の拡大を目指す。
- 90年代にM&Aを繰り返して拡大
- 1997年にMCIを\$370億ドルで買収。
- 2000年にSprintの買収を試みるが失敗。
  - 内部監査人Cooperが2001年Aug.にCapital Expenditureの監査を始める。
  - 2002年3月SECの調査が始まる
  - Cooperが内部監査の拡大を始める
  - Cooperが電子データの確保
  - 2002年6月20日、Cooperが\$30億ドルの不正な費用を発見。監査委員会に公表
  - 2002年6月26日からSECが調査
- 2002年7月に会社更生法を申請。

# ワールドコム の財務報告と修正額

単位: 億ドル

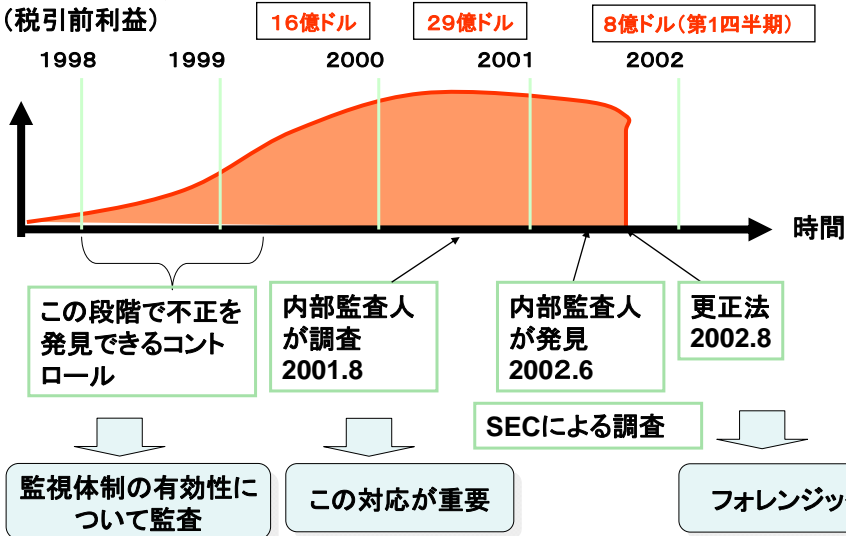
	Line costの資産化			税引前利益		
	財務報告	実際	費用の過小	財務報告	実際	利益の過大
2000年	155	167	12	76	60	16
2001年	147	178	31	23	-6	29
2002年 第1四半期	35	43	8	2	-6	8

US District Court

## 早期発見と監査

ワールドコムのケース

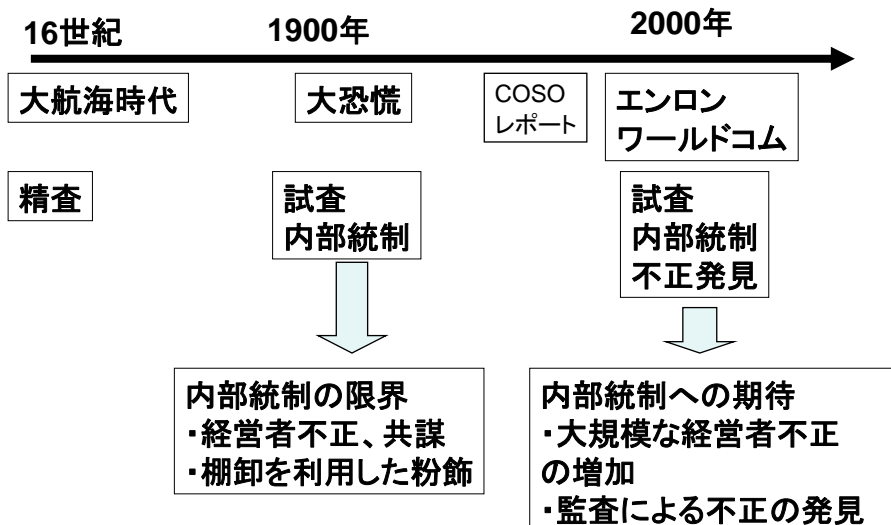
不正による金額の大きさ  
(税引前利益)



## 会計監査とフォレンジック

- 会計監査と不正の歴史
- 内部統制監査 (J-SOX)
- 企業が行う不正の発見
- フォレンジック技術の利用

## 会計監査と不正の歴史 (長期)



## 会計監査と不正の歴史(短期)

- 公認会計士監査と不正の歴史
  - 1985年トレッドウェイ委員会が設立
  - 1987年同委員会がCOSOLレポートを報告
  - SAS53号
  - SAS82号:不正を財務諸表の意図的な虚偽記載と定義。
    - 経営者による詐欺的な財務諸表の作成・報告を経営者不正 (Management Fraud)
      - 会計記録の偽造・改ざん
      - 取引の捏造や意図的な除外
      - 会計処理または開示に関する意図的な会計基準の不適切な適用
    - 資産の横領などの流用 (Defalcations)
  - 2002年10月SAS99号「財務諸表監査における不正の検討」

## 内部統制監査(J-SOX)

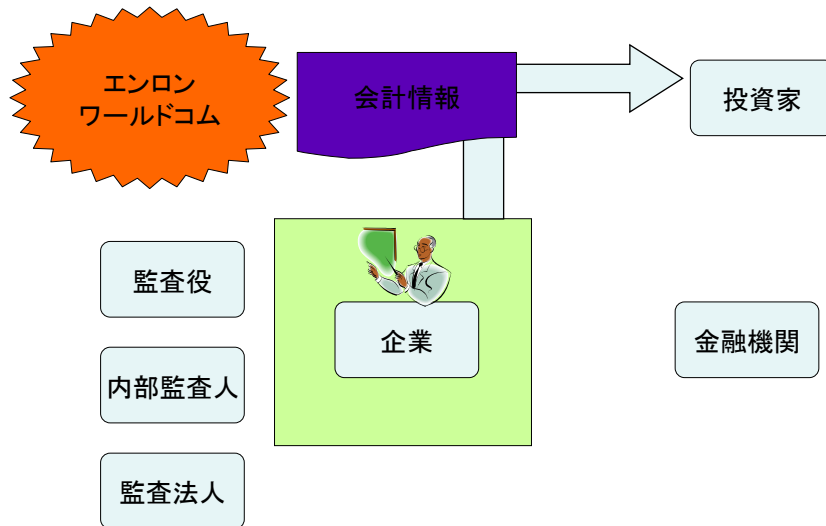
### 財務報告に係る内部統制の強化

昨今の開示をめぐる不適切な事例

⇒ 財務報告に係る内部統制の強化の必要性

- 有価証券報告書等の適正性について経営者の「確認」を義務付け
- 内部統制に関する経営者による「評価」と公認会計士による「監査」を義務付け

## 企業が行う不正の発見



## フォレンジック技術の利用

- 監査役、内部監査人がメールをリアルタイムに監視することができるか？
- フォレンジックとして、インサイダーの取引チェックのためにメール、IP電話を調査することがある
- EncaseのEnterpriseを導入すると、ネットワークを流れるパケットを保管、パターンマッチによる検索からデータを分析できる。  
e-Discovery対応のために、サーバをとめなくても情報を提供でき、かつデータの真正性を保証できる。
- ACLの利用

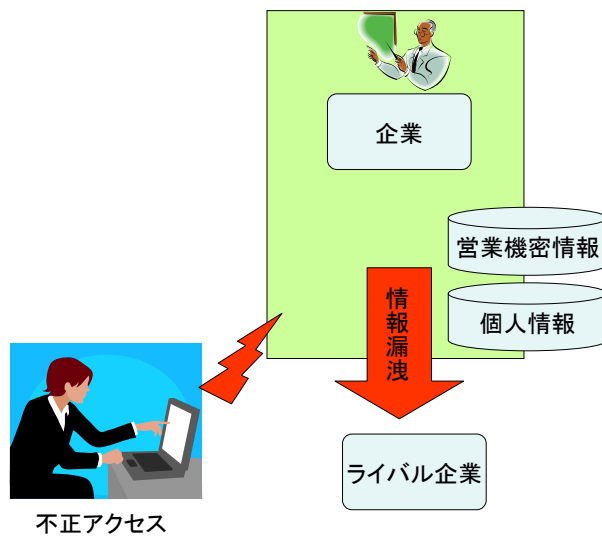
### マイナスの要因

- ・監視の効果が見えない
- ・小さな不正を発見されたくない

## 情報セキュリティ監査とフォレンジック

- 情報漏えいのリスク
- フォレンジック技術の利用

## 情報漏えいのリスク



## フォレンジック技術の利用

- 情報セキュリティ監査
  - 入力チェック、改ざん防止
  - ログの監視
  - 媒体管理
  - 資産管理
  - 物理的セキュリティ
  - 開発と運用の分離
  - 教育
  - アクセス管理
  - ※権限者の不正
  - ※業務側の職務権限の分離の確認

## フォレンジック技術の利用

- 内部監査人またはセキュリティ監査人がメール、ネットワーク等をリアルタイムに監視するか。
- 監視ツールを導入する。
- 内部監査人またはセキュリティ監査人が、監視ツールの設定をチェックする。

## 具体的な例： フォレンジック技術の利用

- 書類の持ち出し
  - 書類にICタグをつけて持ち出しを探知する。(ただし、コピーされると発見できない)
- 不正なアクセスと送信
  - 内部から外部への送信を監視する。ログによる監視が有効
- 写真撮影
  - 監視ビデオで監視する。デジタルカメラに剥がすと記録が残るシールを貼る。社員が発見することも多い。
- USBメモリスティック
  - 監視ツールをPCにインストールすれば、何をコピーしたかを管理部署で監視できる。
- SDカード
  - 同様。
- 内部者の不正アクセス発見のために、監視ツールの導入
  - ログの監視ツール、ネットワーク、クライアント等を監視するツール：SIM、統合監視ツール

## 具体的な例 フォレンジック技術の利用

- PCや個人にICタグをつけて監視する。
- 電子透かしをデータに挿入し、途中経路の追加をチェックすることができる。
- メールの送信を制限するため、送信者を事前登録した者に限定する。

## フォレンジック技術の利用

### 現在の監査の限界

- 監査権の限界
  - 強制捜査権がない
  - 反面調査ができない
- 内部統制の限界
  - 経営者不正や共謀に弱い
  - 内部統制の整備運用は完全ではない

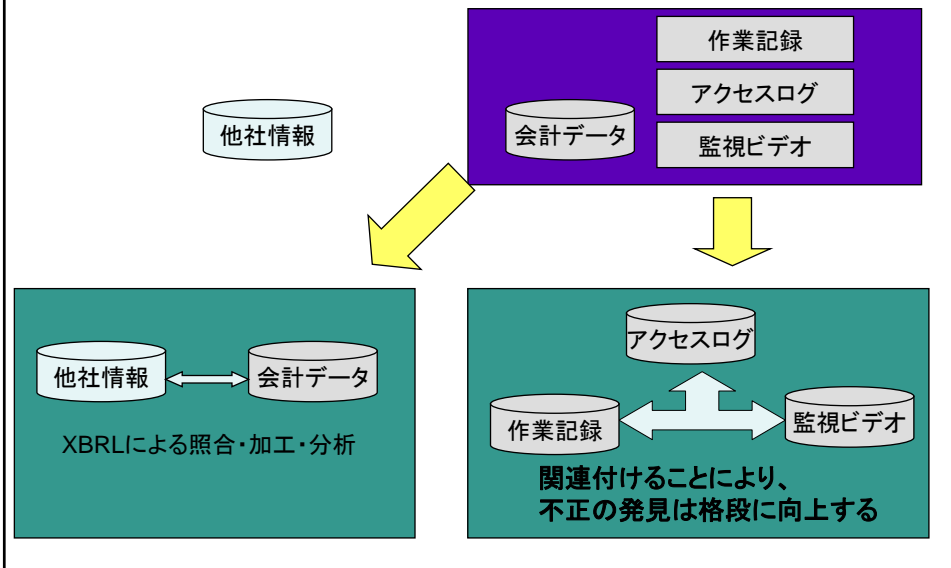
## 将来期待される会計監査

- 会計数字の異常の発見
- 不正の兆候の発見
- 不正の証拠の確保
  
- 新しい手法
  - 膨大なデータの確保とデータマイニングの技術利用
  - XBRLによるデータ照合の拡大

## 内部統制に必要な技術

- 多様なデータの蓄積
  - 会計データ
  - データへのアクセスログ
  - 電子メール
- 関連づけの技術
  - データマイニングの技術
  - 統合監視ツール

## 情報の関連付けの効果



## 将来期待される情報セキュリティ監査

- 内部者による違法行為の発見
- ISO27001の管理策にフォレンジック技術の活用
- 新しい手法
  - ログモニタリングの活用
  - 統合監視ツールの活用

## 今後利用が考えられる技術

### 画像の利用

- ① 衛星画像の利用
- ② 監視カメラ
- ③ PC画面のスクリーンショットを取れる。
- ④ カメラ映像から、本人の顔を認識する。

※画像データと職員の行動記録を組み合わせることにより、不正な行動を迅速に発見することが可能となる。

### GPSの利用

- ① GPSによる証拠や犯人の追跡
- ② 携帯電話の位置確認

※職員、営業員にGPS機能付き携帯を貸与し、不正な行動を把握。

## 今後利用が考えられる技術

### 携帯電話の盗聴

米国ではテロ対策として携帯電話の盗聴が認められ、プライバシー侵害の問題が懸念されている。日本では、捜査令状が必要。

※IP電話は暗号化されていないため、容易に盗聴しやすい。

### 暗号化

暗号化は不正のための手段として利用されることがある。不正の発見のためには、暗号化された文書、通信の解読が必要な場合もある。

### 暗号の解読

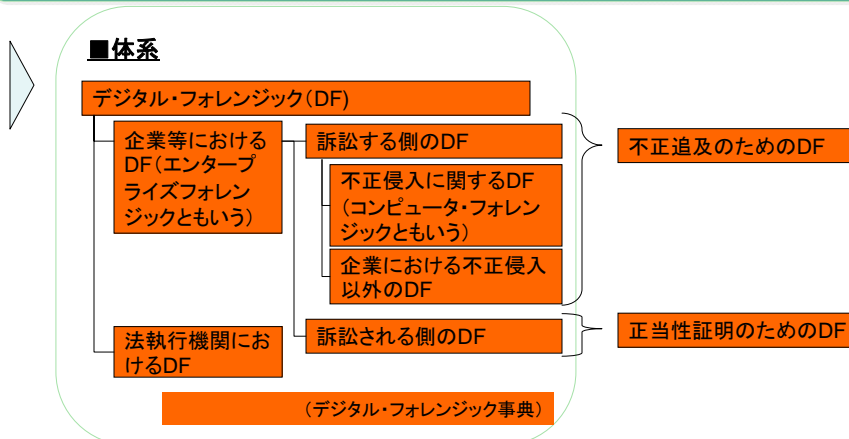
暗号化ソフトにはマスターキーが存在していることが多い。  
※企業内では暗号化して通信されるが、内部監査部等の特定の部署ではすべての暗号を戻せる共通マスターキーのような技術

## JASA 調査研究部会WG3活動

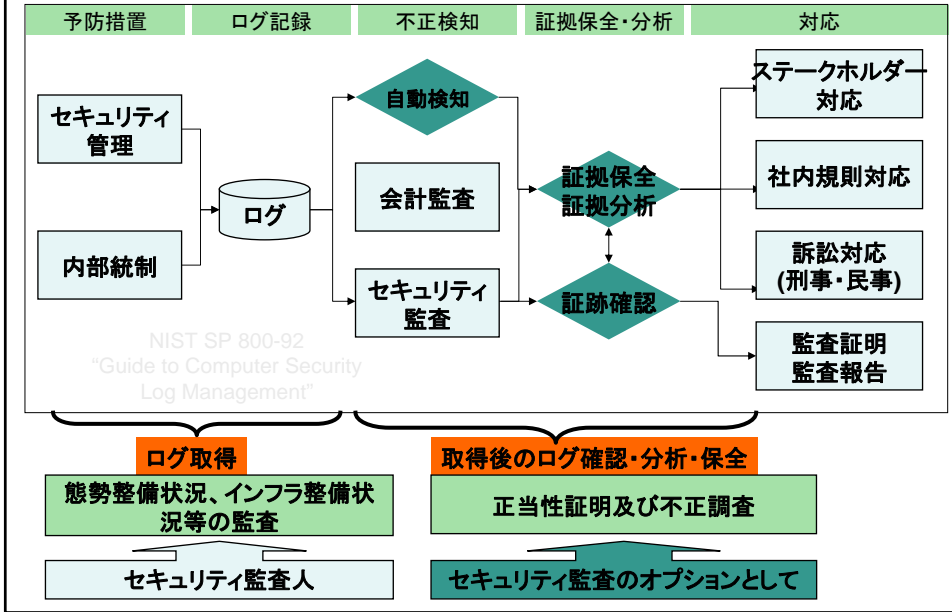
- 情報セキュリティ管理基準、監査基準を拠り所とする情報セキュリティ監査人の立場から、DF(デジタルフォレンジック)に関して検討することを本WG活動の一つのテーマとする。
- デジタルフォレンジックは「事前の準備」と「事後の分析・調査(捜査)」の両面があるが、上記で対象とするのは「事前の準備」フェーズとする。

## WG3におけるデジタルフォレンジックに関する認識

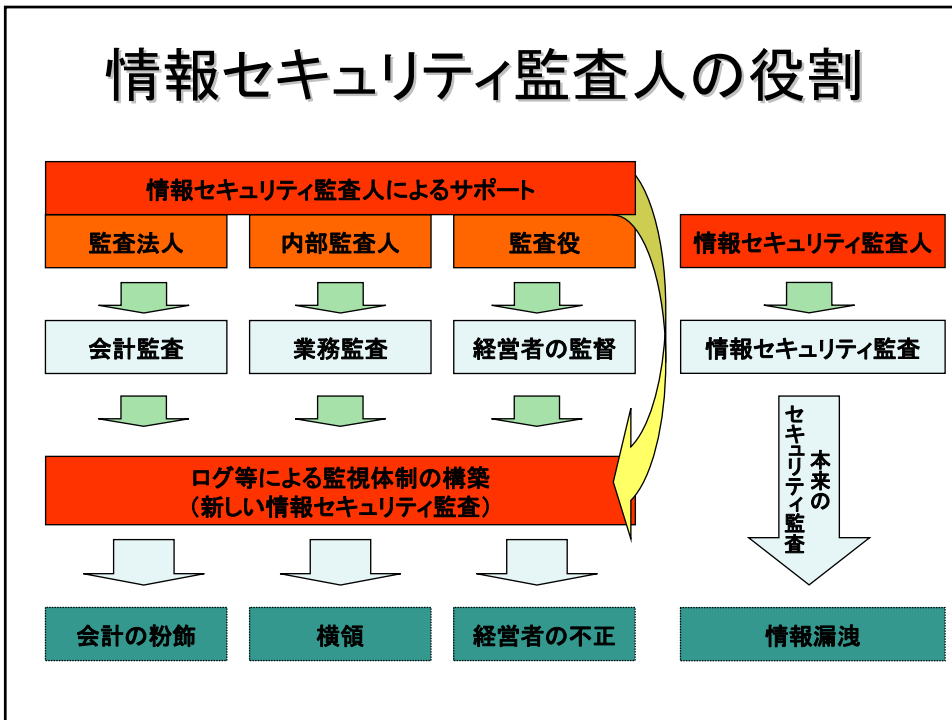
企業等においては、訴訟に至らないまでもフォレンジックを活用するケースが想定される。このため、企業等におけるDFを、訴訟する側・される側ではなく、フォレンジック活用の目的に着眼して、不正追及・正当性証明の2つに大別する。



## デジタルフォレンジックの流れとログの取扱い



## 情報セキュリティ監査人の役割



## まとめ

- 情報セキュリティ監査人は、
  - ISO27001の管理だけでなく、技術的な監視も重視すべきである。
  - 統合監視ツールを利用することで企業の内部統制強化に貢献できる。
  - 監査役、内部監査人、監査法人と協力することにより、企業の不正の発見に貢献することができる。

ご清聴ありがとうございます