企業における デジタル・ フォレンジックの 位置づけと課題

日本ヒューレット・パッカード株式会社
個人情報保護対策室　室長
佐藤　慶浩

『デジタル・フォレンジック事典』の目次から

第6章　企業におけるデジタル・フォレンジック

6. 1 企業におけるデジタル・フォレンジックの基本的な考え方
6. 1. 1 デジタル・フォレンジックの対象となるデータとしての違い
6. 1. 2 デジタル・フォレンジックを使う局面による違い
6. 1. 3 デジタル・フォレンジックの対象が誰のものかによる違い
6. 1. 4 デジタル・フォレンジックを選択することの妥当性

6. 2 通信事業者
6. 3 公認会計士監査
6. 4 金融機関

Slide 2

6. 1企業における デジタル・フォレンジックの基本的な考え方

デジタル・フォレンジックはIT戦略策定時の重要課題である

非電子情報に対するフォレンジックと同等の対策が少なくとも必要である
非電子情報の規程を各自の解釈で電子情報に適用すべきではない
電子情報のフォレンジックにITを活用した手法を採用するのは自然である
非電子情報に非IT手法、電子情報にIT手法という1対1の関係ではない
インテリジェントな作業には、少しの人手を加えてIT工数を激減できる場合が多い

事業効率化のためのITと、IT化によるリスク対応のバランスを図る
後付のコンプライアンスは疎かになりやすい
コンプライアンス対策は組み込む（ビルトインする）べきである
怠るとリスク許容を潜在化させ、事故発生時には、事業効率の相殺では済まない悪影響を与える可能性がある

経営層がIT戦略策定時に組み込み、各事業部局がIT導入時にも組み込む必要がある

Slide 3

6. 1. 1 デジタル・フォレンジックの対象となるデータとしての違い

①電子文書等
　内容が証拠として意味を持つ
　データの完全性が求められる
　データをありのままに保全しておく必要がある
②ログファイル等
　行為の記録発生の事実が証拠として意味をもつもの
　データの否認不能性が求められる
　データをそのままではなく形式変換しても構わない場合がある

補足：電子文書の当事者間だけでの原本性確保は困難であることを認識しておくこと

Slide 4

6. 1. 2 デジタル・フォレンジックを使う局面による違い

①原告としての立場
追求する立場
・被害の事実を主張
②被告としての立場
防衛する立場
・加害の事実の誤りを主張
・加害の責任範囲の主張

・行為者の別
組織内の者による行為、組織外の者による行為
・作為・不作為の別
行為をしたこと、行為を怠ったこと

上記によりフォレンジックの目的が決定し、取るべき手法が定まる
それに備えた対策を事前に講ずることが必要となる

Slide 5

6. 1. 3 デジタル・フォレンジックの対象が誰のものかによる違い

①自社のもの
比較的制約なく調査可能

②自社以外の当事者のもの
利害関係で調査可能範囲が変わる

③当事者以外の第三者のもの
利害関係で調査可能範囲が変わる
加えて、守秘義務等の制約や、調査による新たな利害関係の影響

Slide 6

6. 1. 4 デジタル・フォレンジックを選択することの妥当性

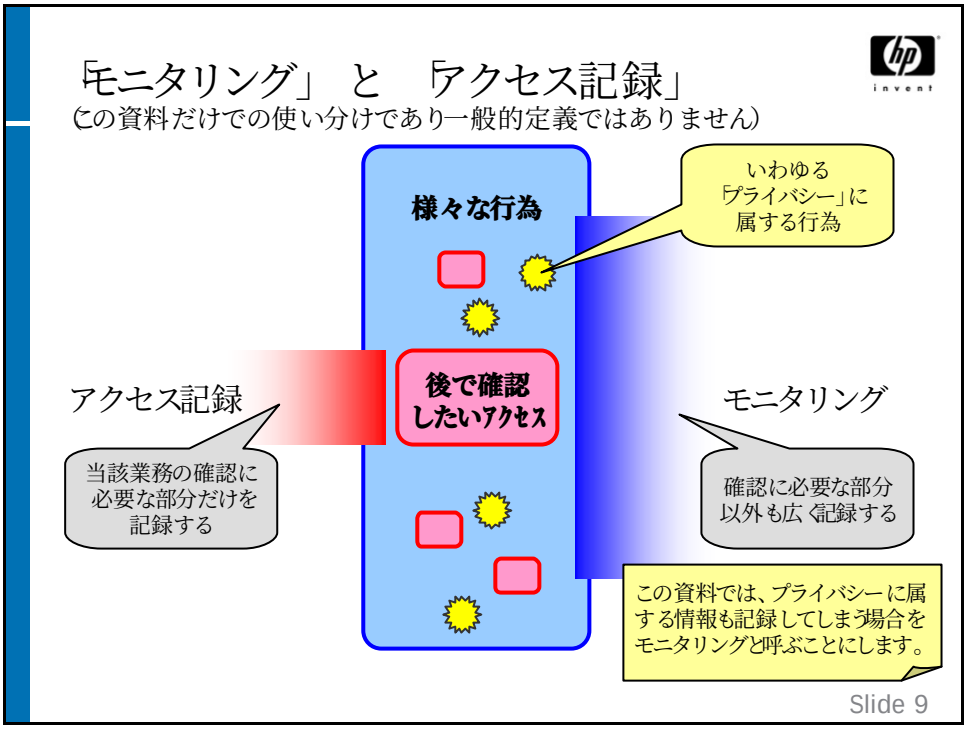
「フォレンジックとして、デジタル・フォレンジックを選択することの妥当性」

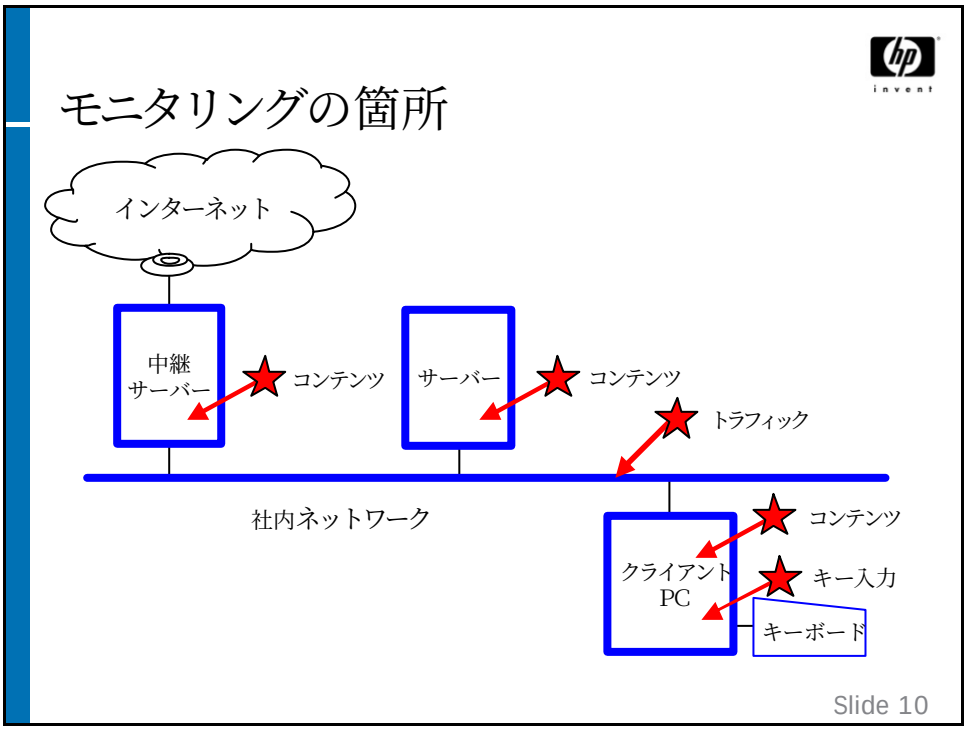
Slide 7

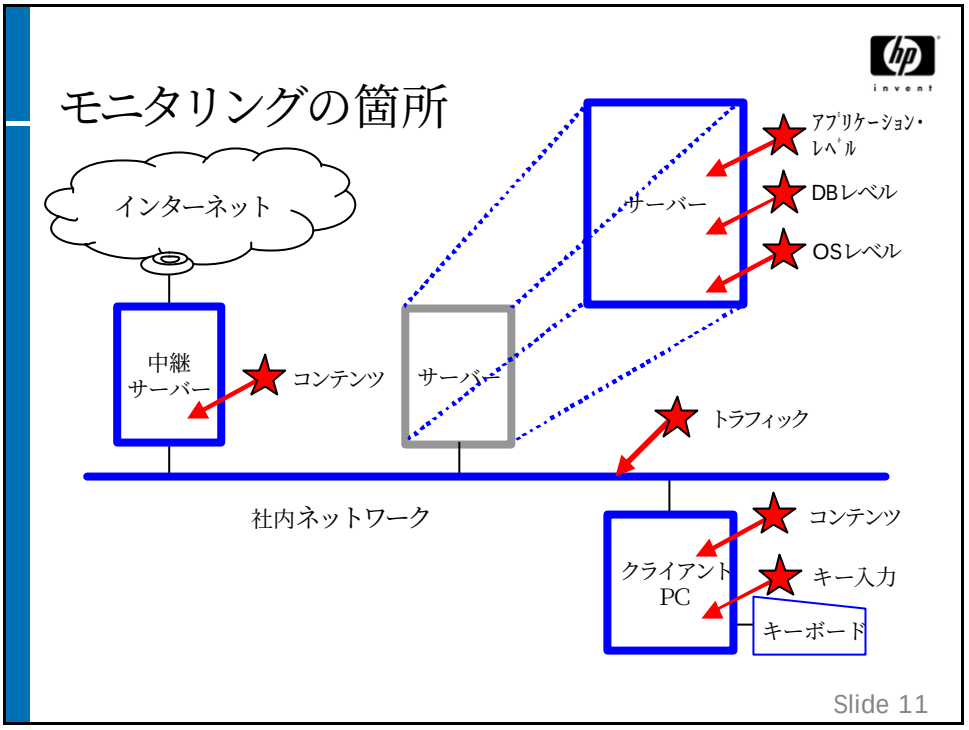
企業におけるコンピュータ・フォレンジックの課題の一例：

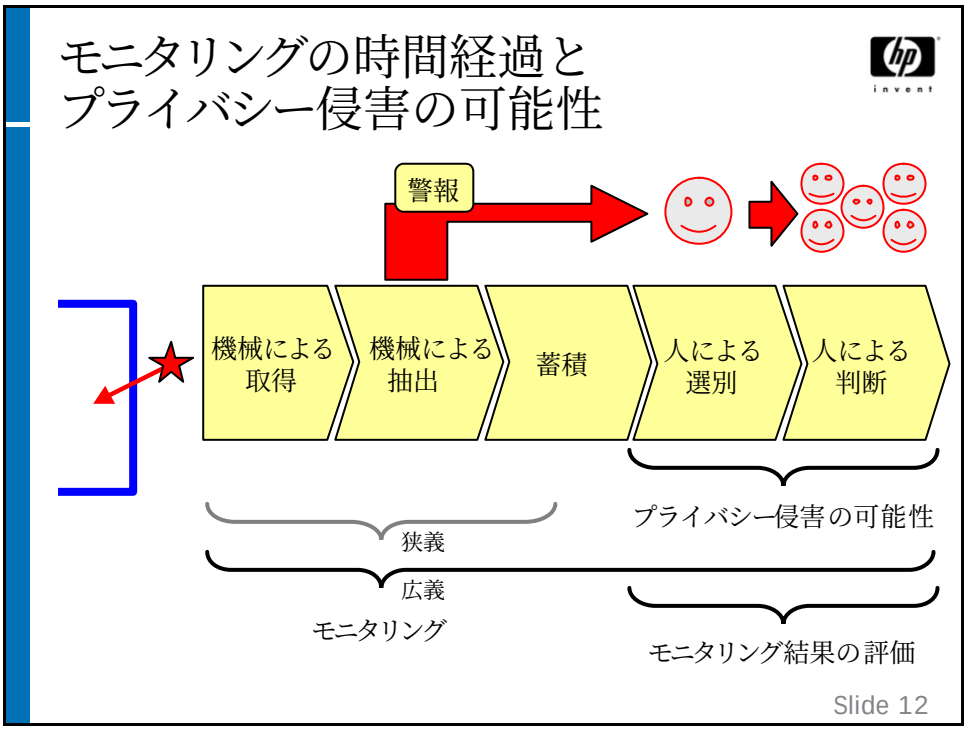
モニタリング実施上の注意点

Slide 8









不正アクセスの類型

アクセス権限のない者による不正アクセス（通称：外部犯）

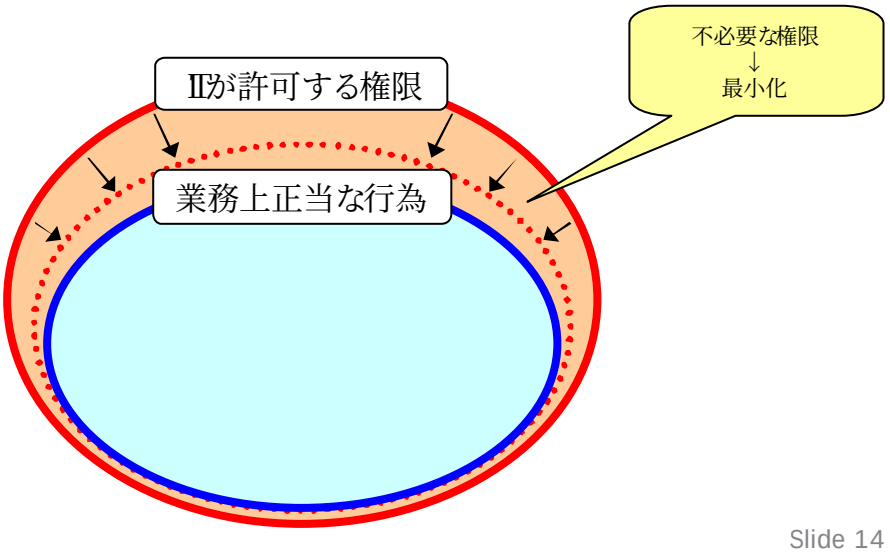
- 無権限アクセス　悪意あり
  - 技術面：アクセス制御による防御・多重の防御

アクセス権限者による不正アクセス（通称：内部犯）

- 誤操作・過失　悪意なし
  - 誤操作を軽減する設計
  - 啓発、教育、訓練
- 権限の悪用　悪意なし　悪意あり
  - 運用面：許可する権限の最少化
  - 技術面：監視による抑止効果
  - 技術面：アノマリ・アクセス検出

Slide 13

アクセス権限の最小化



Slide 14

会社における従業員のネット利用に対するモニタリングについて

モニタリングは、
従業員と会社の間の信頼関係なくしては、
プライバシー侵害以外の何ものでもない。

●従業員が会社を信頼するには？
会社はモニタリングするに際して、最大限の誠意を示さなければならない。

ウソつきは信頼されない

●最大限の誠意とは？
会社はモニタリング以外の手段ででき得る限りの対策を実施し、モニタリングについては、それ以外の手段ではできない場合に限定して実施しなければならない。
モニタリングの利用目的の達成には、プライバシーの尊重がなされなければならない。

Slide 15

会社における従業員のネット利用に対するモニタリングについて

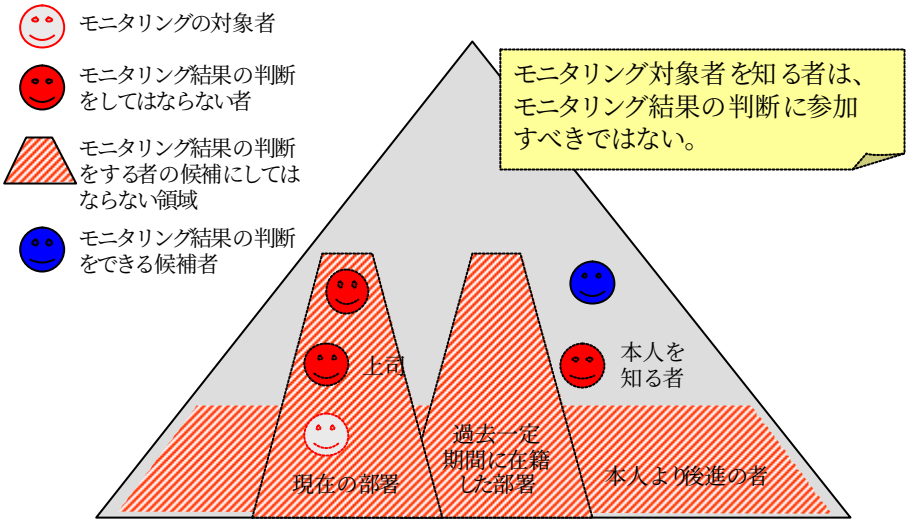
●モニタリングの大義名分
モニタリングは従業員の潔白を証明するために実施する
→モニタリングで無実ならば、無実としなければならない
なぜなら、モニタリングは最後の手段でなければならない
そうできないのであれば、モニタリングすべきではない
悪意のない過失の原因究明に役立ててもよい
悪意の抑止に役立ててもよい

●掲げてはならないこと：
犯人を見つけるための材料を得るためにすべきではない
犯人を問い詰める証拠を得るためにすべきではない

モニタリングは、最終手段であって、最終手段として使わなければならない

Slide 16

モニタリング結果の分析と プライバシー侵害の可能性



Slide 17

モニタリング結果の分析と プライバシー侵害の可能性

●小規模な会社

プライバシーを侵害しないでモニタリング結果を分析するための社内体制を構築することは困難。

●大規模な会社

プライバシーを侵害しないでモニタリング結果を分析するための社内体制を構築することは可能。
しかし、分析作業場所を社内に限定し、作業者を社外に依頼する資金もあるはず。
社外に依頼しない理由について熟慮する必要がある。
→身内の恥を外にだしたくないから?
→費用が安いから・・が論外であるのは明白。
→では、なぜ?

Slide 18

最終手段としての「モニタリング」
不正アクセスの類型

アクセス権限のない者による不正アクセス（通称：外部犯）

- 無権限アクセス
  - 技術面：アクセス制御による防御・多重の防御

アクセス権限者による不正アクセス（通称：内部犯）

- 誤操作・過失
  - 誤操作を軽減する設計
  - 啓発、教育、訓練
- 権限の悪用
  - 運用面：許可する権限の最少化
  - 技術面：監視による抑止効果
  - 技術面：アノマリ・アクセス検出

最終手段にどれだけの
経営資源を配分するかを
十分検討する必要がある
中途半端な最終手段ほど
恐ろしいものはない

最終手段

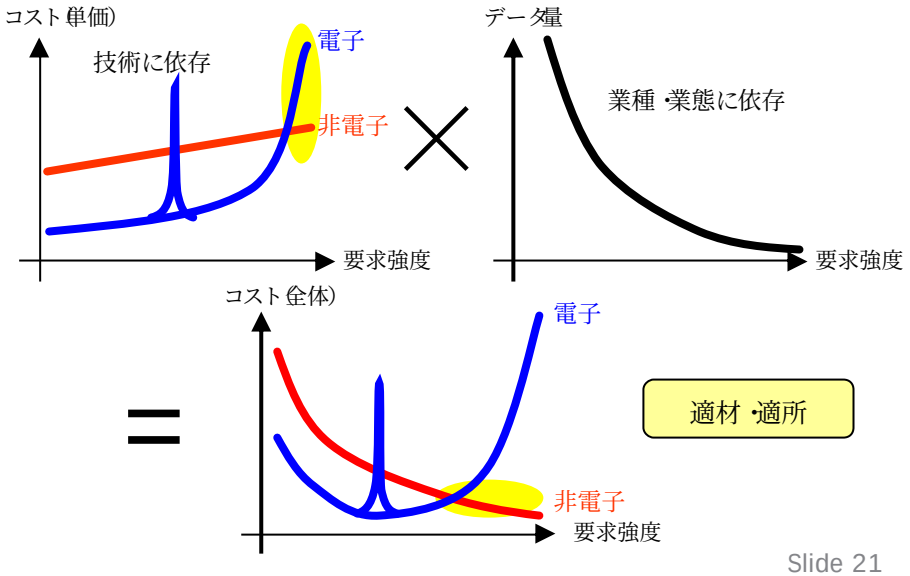
Slide 19

企業におけるコンピュータ・フォレンジックの
課題の一例：

要求事項とコストの関係

Slide 20

企業における情報の電子・非電子選択とフォレンジック要求強度とコストの関係



Slide 21

6. 1. 4 デジタル・フォレンジックを選択することの妥当性

「フォレンジックとして、デジタル・フォレンジックを選択することの妥当性」

フォレンジックはデジタルな手法だけではない
電子情報だからといって、すべてをデジタル・フォレンジックだけで解決する必要はない

フォレンジックの処理には人による判断が介在することが考えられる

デジタルでしか実施できないか？
なぜ、デジタルを採用するのか？
デジタルとしない場合、どのような処理となるか？
※業務手順の改訂にまで視野を広げることが重要
※文書の電子化は、完全性・原本性リスクを増大する場合が多い

不正なことをしていない立証が必要。という観点の欠如は危険。

Slide 22