お詫び：
印刷期限に資料準備が間に合いませんでした。
資料は以下のホームページからダウンロードしてください。
http://yosihiro.com/go/2005-07-01

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

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

高橋郁夫弁護士の着目点（推定）

個人情報保護対策の一環として、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技術が検討されることがある。

しかし、モニタリングは従業員のプライバシーを侵害してしまう側面を持つ。

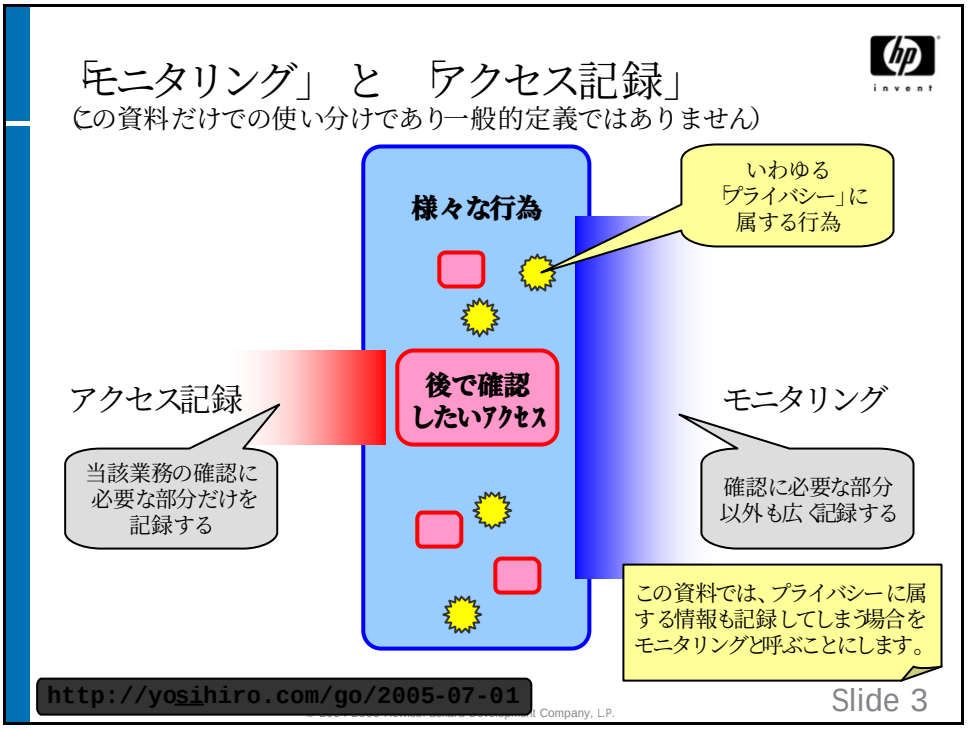
つまり、
顧客のプライバシーを保護しようとする対策のひとつが、
従業員のプライバシーを侵害してしまうかもしれない。

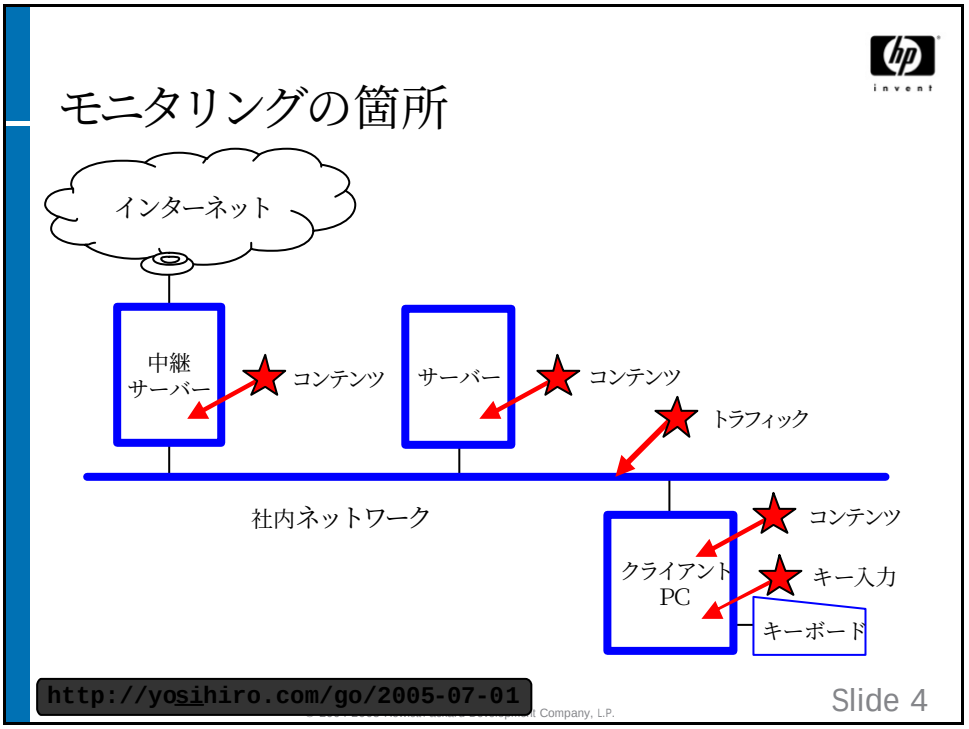
プライバシー保護がプライバシー侵害を招くことになるのか？

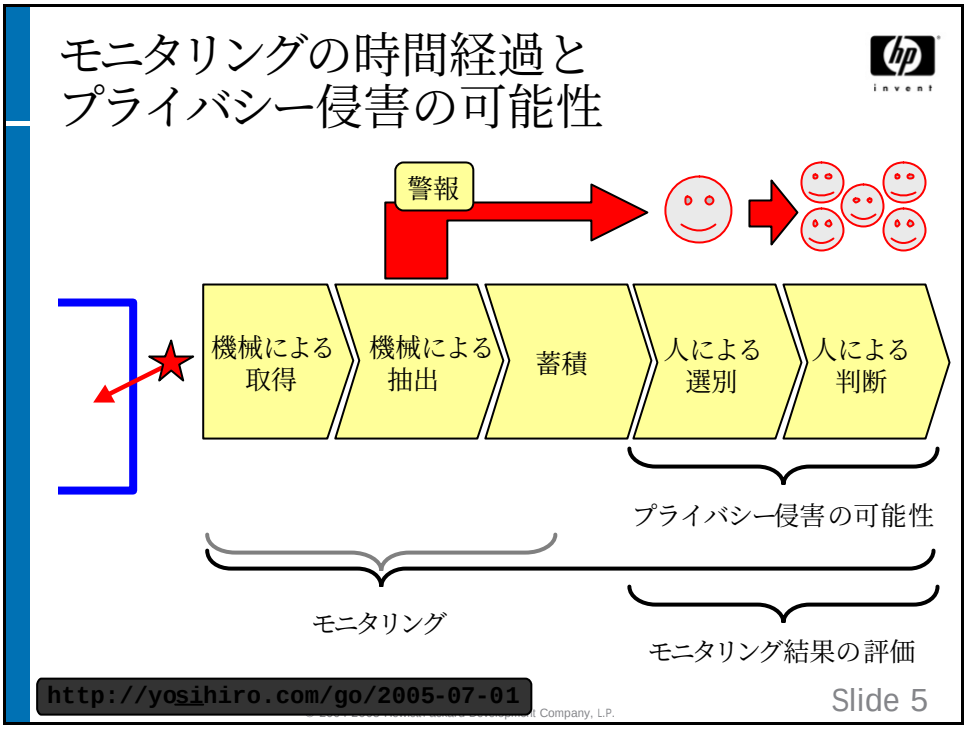
が気になるらしい・・・

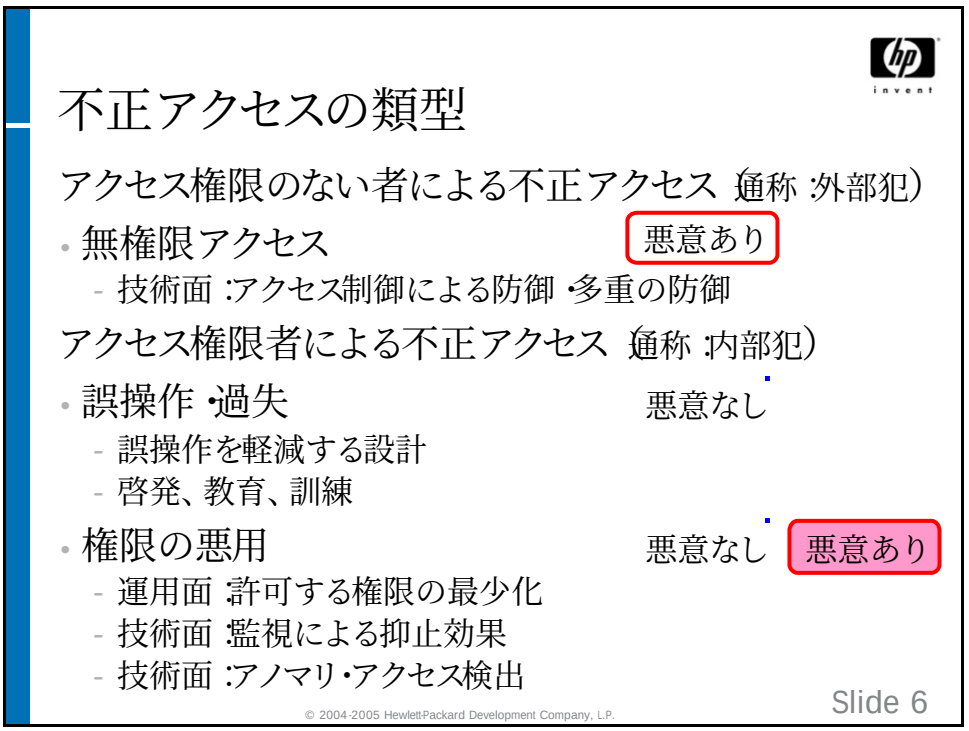
http://yosihiro.com/go/2005-07-01

Slide 2

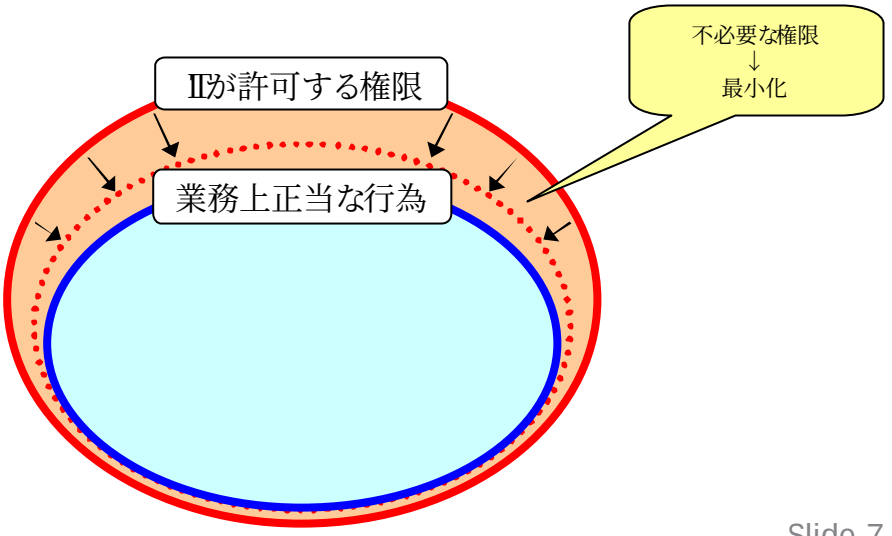








アクセス権限の最小化



Slide 7

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 8

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

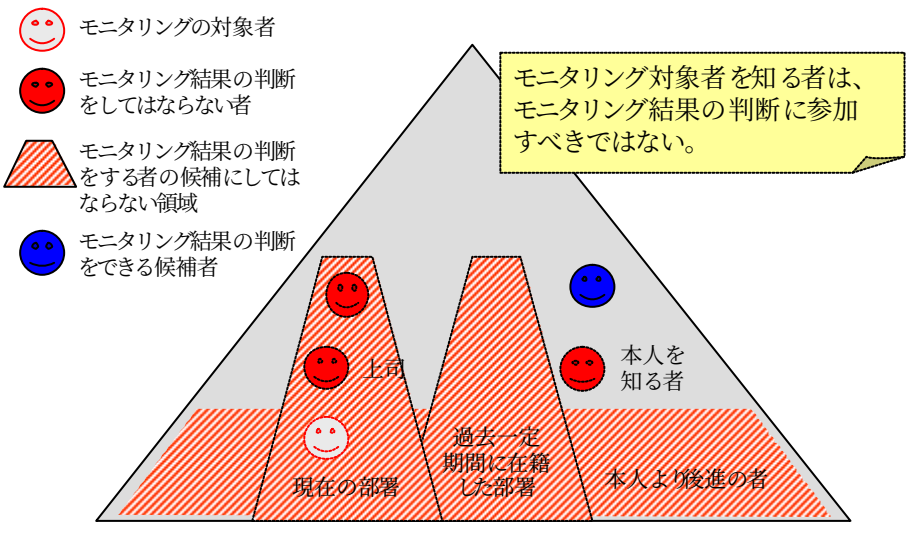
●掲げてはならないこと：

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、最終兵器であって、最終兵器として使わなければならない

Slide 9

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 10

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 11

最終兵器としての「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

最終兵器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兵器ほど恐ろしいものはない

最終兵器

Slide 12