



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://yoshihiro.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・パッカー株式会社
個人情報保護対策室 室長
佐藤 慶浩

© 2004-2005 Hewlett-Packard Development Company, L.P.
本書に含まれる情報は、予告なく変更されることがあります。



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://yoshihiro.com/go/2005-07-01>

© 2004-2005 Hewlett-Packard Development Company, L.P.

Slide 2

「モニタリング」と「アクセス記録」
(この資料だけでの使い分けであり一般的定義ではありません)

The diagram shows a central blue box labeled '様々な行為' (Various actions) containing several yellow starburst icons. A red box labeled '後で確認したいアクセス' (Access I want to check later) is highlighted within this box. A red arrow labeled 'アクセス記録' (Access record) points to this red box, with a callout stating '当該業務の確認に必要な部分だけを記録する' (Record only the parts necessary for confirmation of the business). A blue arrow labeled 'モニタリング' (Monitoring) points to the entire blue box, with a callout stating '確認に必要な部分以外にも広く記録する' (Record broadly, not only the parts necessary for confirmation). A yellow callout points to the starbursts, stating 'いわゆる「プライバシー」に属する行為' (Behaviors belonging to so-called 'privacy'). A yellow callout at the bottom states 'この資料では、プライバシーに属する情報も記録してしまう場合をモニタリングと呼ぶことにします。' (In this document, we will call cases where information belonging to privacy is also recorded 'monitoring').

hp invent

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

Slide 3

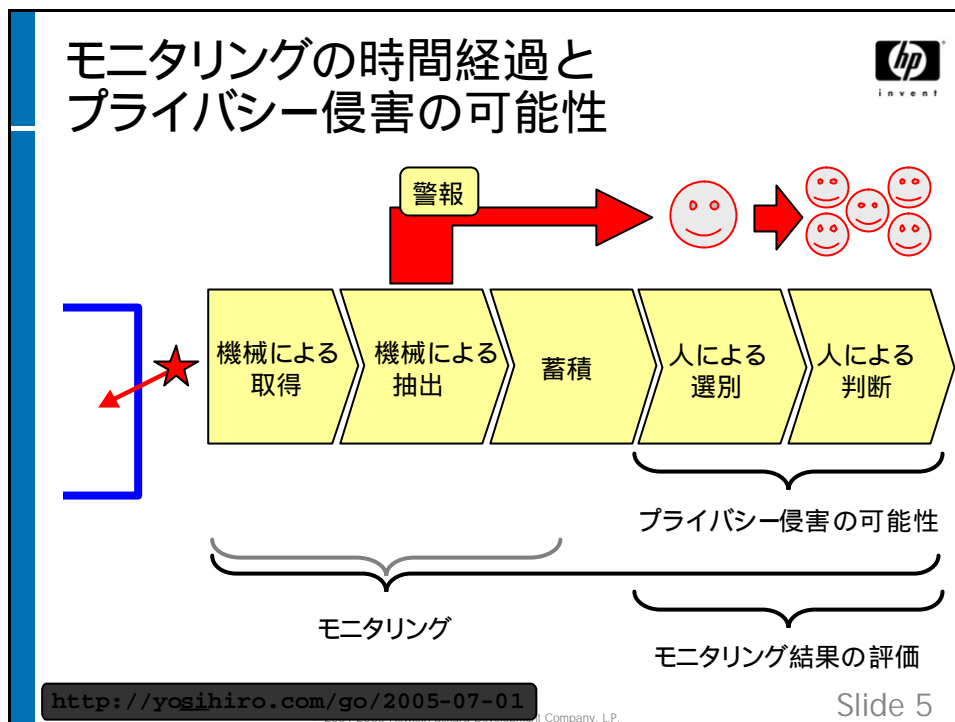
モニタリングの箇所

The diagram illustrates the flow of data through a network. At the top, a cloud labeled 'インターネット' (Internet) is connected to a '中継サーバー' (Relay server) and a 'サーバー' (Server). Red arrows labeled 'コンテンツ' (Content) show data moving from the Internet to the relay server, then to the main server, and finally to a 'クライアント PC' (Client PC). A red arrow labeled 'トラフィック' (Traffic) shows data moving from the Internet to the client PC. The client PC is connected to a '社内ネットワーク' (Intranet network). A callout for the client PC lists 'コンテンツ' (Content), 'キー入力' (Key input), and 'キーボード' (Keyboard). The HP logo is in the top right corner.


hp invent

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

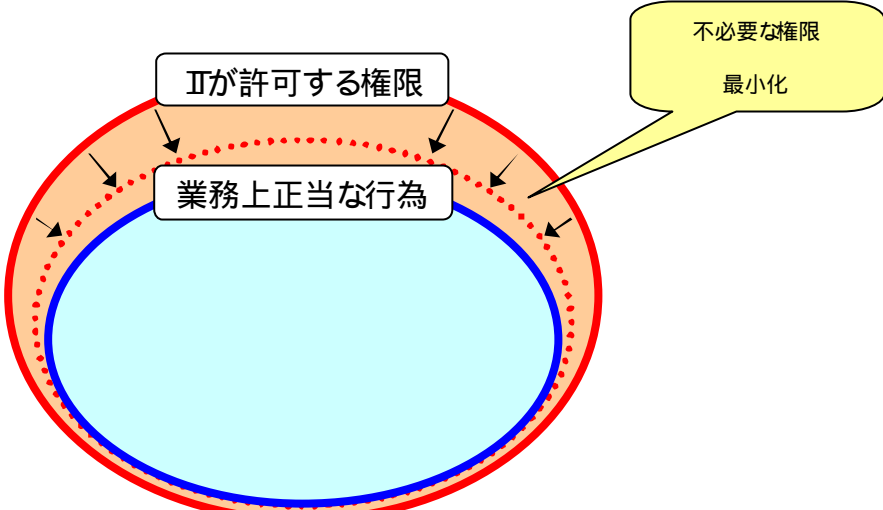
Slide 4



- ### 不正アクセスの種類
- 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
- hp invent
- Slide 6
- © 2004-2005 Hewlett-Packard Development Company, L.P.



アクセス権限の最小化




ITが許可する権限

業務上正当な行為

不必要な権限
最小化

© 2004-2005 Hewlett-Packard Development Company, L.P.

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、
従業員と会社と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。


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。

ウソつきは
信頼されない


© 2004-2005 Hewlett-Packard Development Company, L.P.

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

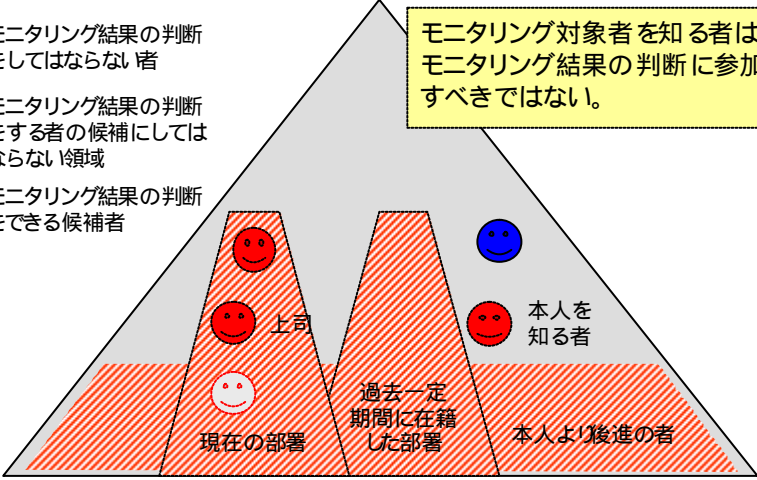
モニタリングは、最終兵器であって、最終兵器として使わなければならない

© 2004-2005 Hewlett-Packard Development Company, L.P. 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



-  モニタリングの対象者
-  モニタリング結果の判断をしてはならない者
-  モニタリング結果の判断をする者の候補にしてはならない領域
-  モニタリング結果の判断をできる候補者




モニタリング対象者を知る者は、モニタリング結果の判断に参加すべきではない。

現在の部署 (White smiley face)
過去一定期間に在籍した部署 (Red sad smiley face)
本人より後進の者 (Blue smiley face)

上司 (Red sad smiley face)
本人を知る者 (Red sad smiley face)

© 2004-2005 Hewlett-Packard Development Company, L.P. 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？

© 2004-2005 Hewlett-Packard Development Company, L.P. 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

←

© 2004-2005 Hewlett-Packard Development Company, L.P. Slide 12