

安全管理措置WGの検討状況について

平成21年11月17日(火)

安全管理措置WG

● 安全管理措置WG 親会への報告のポイント

- 基本的論点(安全管理措置の必要性、保護措置のなされたPC等に係る手続の簡略化)の確認。
- 次回親会までに4回程度のWGを開催して、論点整理、提言案の策定を行う。

背景1 ノートPCの持ち出しニーズの増加

- ワイヤレスブロードバンドネットワーク接続環境の整備
 - ノートパソコン等の機能向上
- ↓
- 個人情報の入ったPCの外部への持ち出しの増加

背景2 安心して持ち出せるPC環境対策

- 平成20年以降、個人情報の漏えいに対応するための技術的対策の登場
 - リモートデータ消去・PCロック
PCの紛失時に、遠隔操作によって情報を消去、操作をロックする。
 - シンクライアント端末
ネットワーク上に情報を集中させ、PCには必要最小限の情報しか残さない
- ↓

WGの目的

個人情報漏えい事故による利用者(消費者)の被害を減少させるため、外部に持ち出したPCなどの情報端末機器の安全管理措置(情報漏えい対策など)の在り方について検討を行う。

基本的論点

- **事業活動を行う上で、個人情報の社外持ち出しが増加することが想定されるため、個人情報の漏えい時における利用者(消費者)の被害を減少させるため、安全管理措置が必要ではないか。**
- 暗号化等の保護措置が講じられている個人情報の入ったノートPC、可搬型記録媒体を紛失した場合等、本人への被害のおそれがない場合又は極めて少ないと考えられる場合には、個人情報ガイドラインの求める所定の手続き(本人への通知、公表等)の簡略化、省略をすることに合理的理由が認められるのではないか。

今後のスケジュール(予定)

○ 第1回(平成21年11月11日)

事業者からのヒアリング①

→親会(平成21年11月17日)に報告

○ 第2回(平成21年11月30日)

事業者からのヒアリング②、海外状況調査

○ 第3回(平成21年12月中旬)

論点整理

○ 第4回(平成22年1月中)

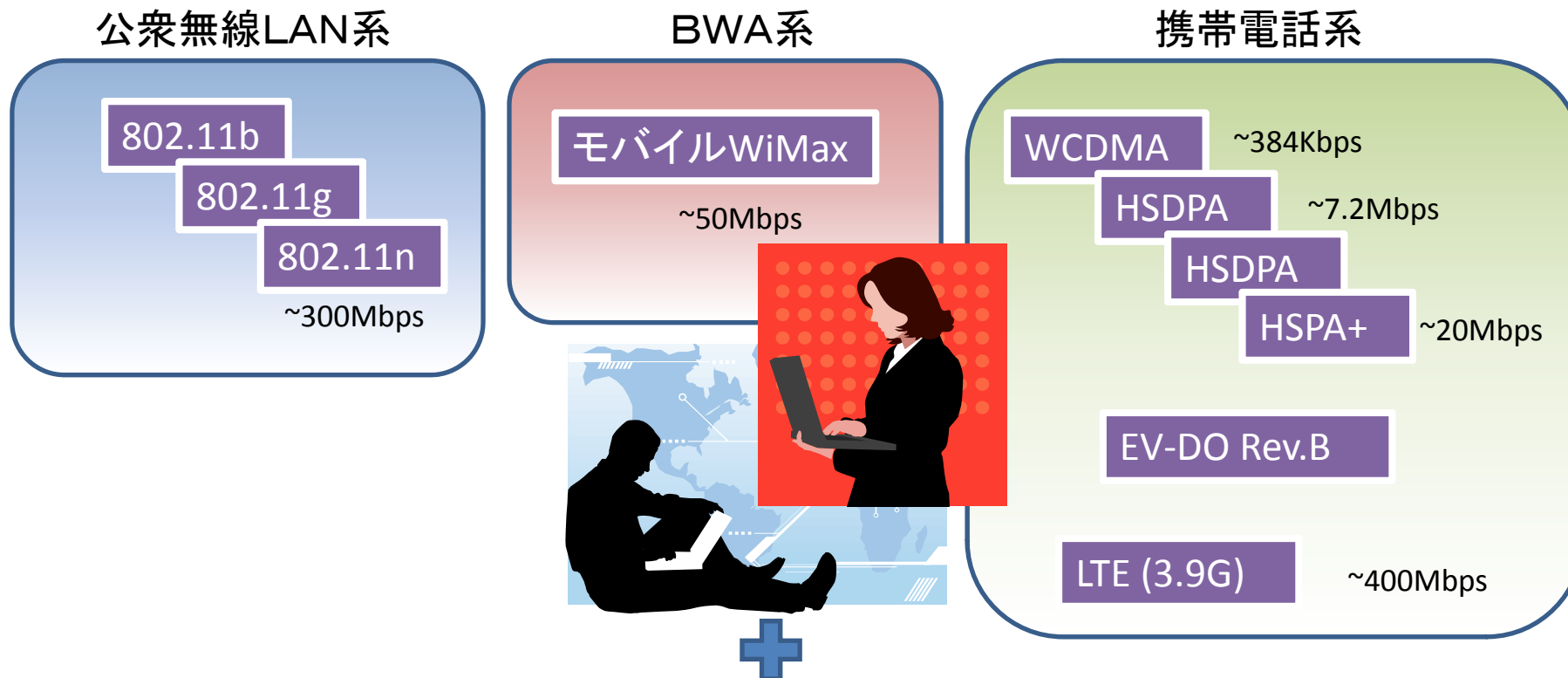
WGとしてのまとめ

→ 親会に報告

(必要に応じ上記以外に会合を開催)

(参考) 背景1(ノートPCの持ち出しニーズの増加①)

- ワイヤレスブロードバンドネットワーク接続環境の整備の進展



- 処理能力の向上、小型化・省電力化により、従来以上に持ち出して利用しやすいノートパソコン等の端末の登場

24Hバッテリー

超軽量・超薄型

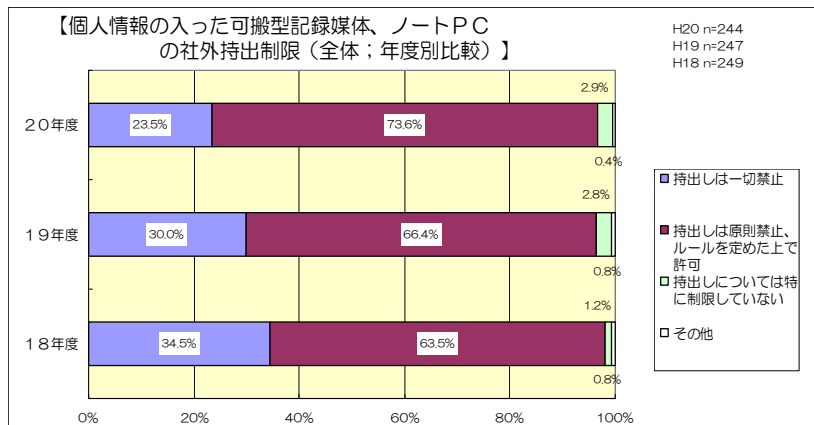
低価格モバイルPC

通信装置(モジュール)の内蔵化等

ワイヤレスブロードバンドネットワーク接続環境の整備・モバイルPCの普及により、場所にとらわれず、効率的に業務を行える環境が整いつつある

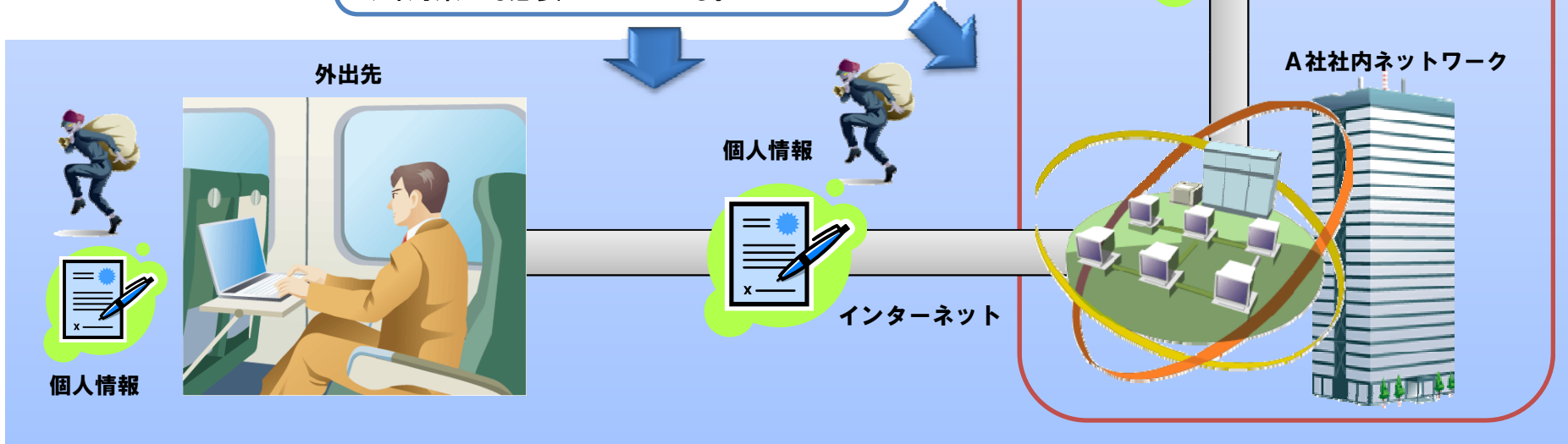
(参考) 背景1(ノートPCの持ち出しニーズの増加②)

モバイルPCの利用によりセキュリティ対象範囲が拡大



今までは、社内・支店間におけるセキュリティ対策が中心

個人情報の入ったノートPCの外部への持ち出しの増加等※によって、オフィス外でのセキュリティ対策にも必要が生じている。



※ パンデミック対策として、社員が出社できないことを想定したモバイルPCを活用する企業も存在

(参考) 背景2(安心して持ち出せるPC環境対策)

個人情報の漏えいに対応するため、以下のような技術的対策が進んでいる。

リモートデータ消去、PCロック、追跡サービス等

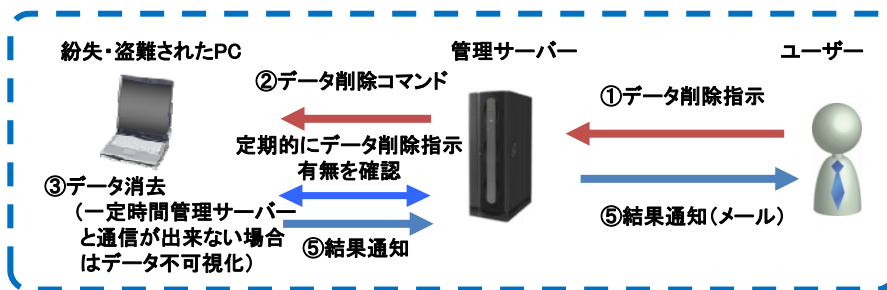
- 端末の紛失時に、遠隔操作によって情報を消去したり、操作をロックする等、情報漏えいを防止するソリューションが多数登場。

シンクライアント端末

- ネットワーク上に情報を集中させ、端末には必要最低限の情報のみ持たせることにより、情報漏えい対策として高い効果を持つ。

【ソリューション事例】(KDDI株式会社)

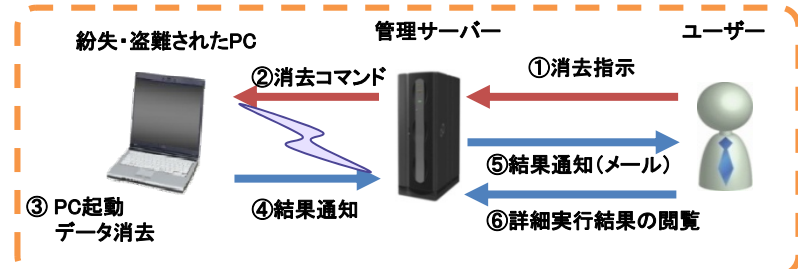
遠隔操作によって該当データの上書きを指示し、データを削除



- PCの指定されたデータを遠隔操作で削除(データの上書きを指示)
- インターネット接続中は、定期的に管理サーバーと認証し、データ削除指示有無を確認
- インターネット接続がない環境でも、PCIにKDDIの通信カードが挿入されている、または、通信機能搭載PC(KDDIの通信モジュール内蔵PC)をご利用であれば、電源ON時等に強制的に管理サーバーと通信し、データ削除指示有無を確認
- 一定時間管理サーバーと通信が出来ない場合は、指定されたデータを不可視化

【ソリューション事例】(富士通株式会社、株式会社ウィルコム)

遠隔操作によってデータの暗号鍵を消去し、ハードディスク内データを消去



- 遠隔操作でPCのハードディスク内の全データを即時消去(暗号鍵の消去)
- PCが電源オフ状態でも実行可能(専用の通信モジュールを搭載)
- 消去結果や、PCへのアクセス履歴を含むレポートを発行

高度に暗号化等された技術的措置が漏えいデータになされていれば、利用者への被害リスクは大幅に減少。