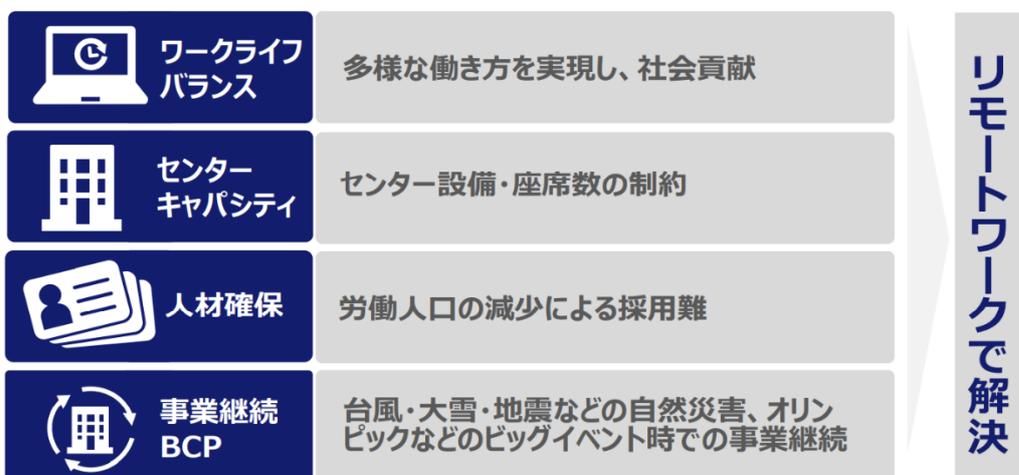


## 第114回 維持管理研究会 議事録

- 開催日時：2021年 1月21日（木）15:30～17:30
- 場所：Zoom リモート開催
- 出席者（敬称略） 14名  
相原、井上、小田、久保、澤田、清水、守護、菅谷、守護、田中、徳山、柳本、山下、中谷（記）
- 研究テーマ
  - ① リモートワークの対応事例（SCSK サービスウェア様）を田中さんから説明して頂いた。  
2017年から培ったノウハウを元に、インフラセキュリティマネジメントを間接部門からトライアルし段階的に業務範囲を拡大し、2020年に全部門への展開が完了した。

### <取り組みの背景>



テレワークでは十分なセキュリティが確保できないため、あくまで自宅でのリモートワークであることが、大きなポイントであり、下記の対応により十分なセキュリティを確保した対応となっている。

### <貸与 PC への対策>

**① 高レベルのセキュアPC**

リモートワーカーは  
当社の貸与PCで業務を行います



- リモート接続ツール
- 顔認証ツール
- WEB会議ツール
- コールセンターツール

当社貸与PC：業務以外には一切使用不可  
HDDにはデータを保存できず、盗難・紛失した場合も問題は発生しません。

- × 特定アプリ以外は利用不可  
(リモート接続・顔認証・WEB会議)
- × ローカルにデータ保存できない
- × コピー&ペーストでもHDDに保存不可
- × アプリケーションのダウンロードはできない
- × 印刷できない
- × インターネット接続を限定  
(ホワイトリスト管理)

**② 顔認証**

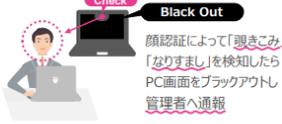
PC搭載のWEBカメラを使い  
顔認証による管理を実施

**在席管理**

本人がPC前に座っている時間を自動集計・管理



**セキュリティ事故抑制**

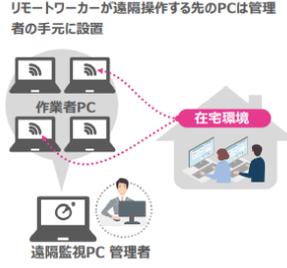


顔認証によって「覗きこみ」「なりすまし」を検知したらPC画面をブラックアウトし管理者へ通報

**③ 遠隔監視**

PC操作を常に監視

リモートワーカーが遠隔操作する先のPCは管理者の手に設置



作業PC 在宅環境 遠隔監視PC 管理者

- ① リモートワーカーのPC操作をいつでもモニタリング可能 → 牽制が働く
- ② 業務時間外は当社首都圏で管理する  
・作業PCの電源オフ  
・業務時間外のPC利用を制限
- ③ 操作ログは一定期間保管

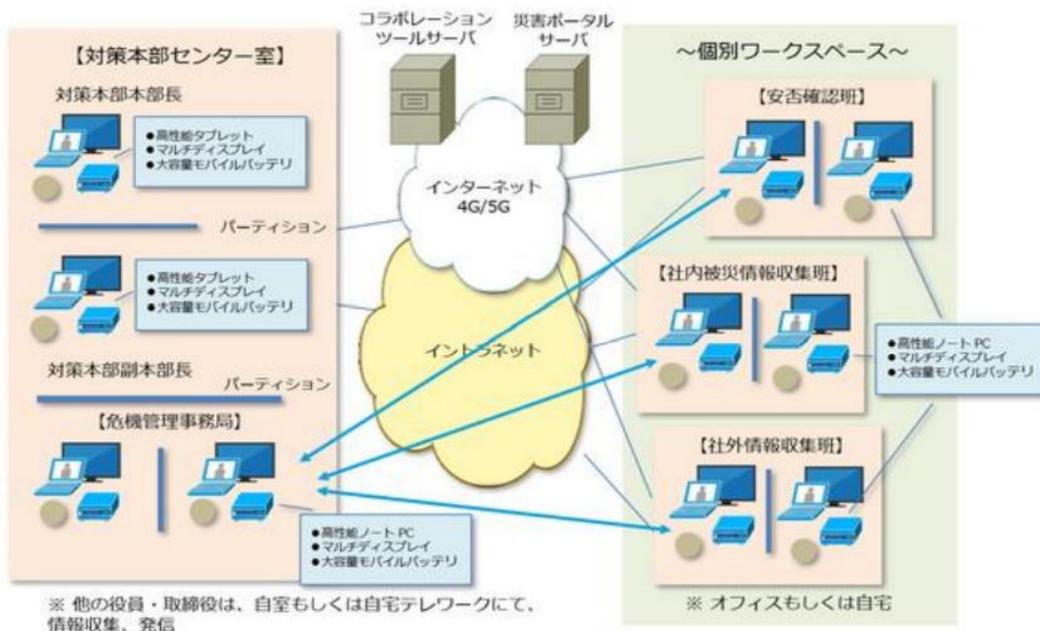
社内と遜色のない高セキュリティレベルを自宅で実現している。

## ② 複合型の対策本部の在り方について検討

危機管理担当部門はこのコロナ対応で四苦八苦しており、自然災害 BCP の訓練も十分にできず、PDCA もままならず、マニュアル類は塩漬け状態という企業が多く存在している。

一方でコロナ禍での強い不安感から、同時に起こる可能性が高い震災や自然災害に危機意識を感じ、複合災害 BCP への取り組みが必要となってきた。

<複合型対策本部の構成例>



災害時にいきなり上図のような仕組みに順応するのは、多くの時間と訓練が必須です。

まずはコミュニケーションをどのように取るのか、短時間でもよいので、仕組みに慣れてもらうことから始めて、慣れるまで繰り返し実施（PDCA）することが重要である。

また、停電しているという設定で、エンドポイント（PC やタブレット）端末は機能するのか、災害発生時に、リモート会議などの接続性や性能に問題ないか等の確認が必要である。

<次回開催予定>

2021年 2月18日（木）15:30～17:30

Zoomによるリモートで実施

以上