「テレワークセキュリティガイドライン概要」

１．　本ガイドラインの狙い

○　本ガイドラインは、基本的に実施すべき情報セキュリティ対策について紹介するものであり、情報セキュリティ対策について初めての方にとっても、内容が簡単に分かり、活用しやすい構成とすることにより、民間のテレワーク導入を支援し、普及促進を図るものである。

２．　情報セキュリティ対策のポイント

○　情報セキュリティ対策を行うにあたり、企業などの組織が重要視すべきことは、情報資産を洗い出し、どのような脅威や脆弱性、リスクがあるのか十分に把握、認識した上で、体系的な対策を実施することである。

○　本ガイドラインでは、テレワーク（※１）を実施するうえで必要となる情報セキュリティ対策を「ルール」、「人」、「技術」という３つの要素に分類し、それぞれについて具体的な方策を紹介する。セキュリティの高いテレワーク環境構築のポイントは、「ルール」、「人」、「技術」の対策をバランスよく保つことである。

＜テレワークセキュリティ対策１９か条＞

３．「ルール」についての対策

① 情報セキュリティ管理体制（管理者の選任、情報資産の管理方法の策定等）を構築する。

② テレワーク環境においても情報セキュリティポリシー（※２）が正しく遵守されているか、定期的なチェック（監査）を実施する。

③ 社内システムへアクセスするためのアカウント（※３）については、管理方法を明確に定め、厳格に管理する。

④ テレワーク端末を貸与する際には、「氏名」「担当業務」「パソコン機種」「連絡先」「返却期限」「情報セキュリティ対策状況」等を把握しておく。

⑤ テレワーク用に貸与された業務用パソコンは許可された目的内で利用条件に従って適切に用いる。

⑥ 一時的に職場外に持ち出すデータは原本ではなく原本からの複製とする。

⑦ 私物のパソコンを業務に利用する場合には、インストールされているソフトを確認するなど定められた利用条件に従う。

⑧ ネットワークを用いてテレワークを実施する際には、指定された通信手段を用いる。

４．「人」についての対策

⑨ トップダウンにより情報セキュリティポリシーを周知・徹底する。

⑩ テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、日々、教育・啓発活動を実施する。

⑪ 就業規則や外部委託契約に機密保持規定や罰則規定を設ける。

⑫ セキュリティ事故発生時は、直ちに定められた担当者に連絡する。

５．「技術」についての対策

⑬ ウイルス対策ソフトをインストールし、最新の定義ファイルに定期的に更新する。

⑭ ＯＳ（※４）及びソフトウェアにおいては、パッチ（※５）の更新を定期的に行う。

⑮ 外部メディアへ保存する等、定期的にデータのバックアップを実施しておく。

⑯ ＯＳのログイン時等のパスワードは、他人に推測されにくいものとし、定期的に更新を行う。

⑰ 機密性の高いデータを保存・送信する際には必ず暗号化する。

⑱ 社内システムとテレワーク環境の境界線にはファイアウォール（※６）やルータ（※７）等を設置し、不必要なアクセスを遮断する。

⑲ 社内システム内にある重要データは、安全な領域（※８）に格納するとともにアクセス権限の付与は必要最低限とする。

※１　テレワーク…情報･通信技術の利用により時間･空間的束縛から解放された多様な就労業形態をいい、本ガイドラインでは、在宅による就労に限らず、施設に依存しないモバイル型などの多様な就労・作業形態を総称する用語として用いている。

※２　情報セキュリティポリシー…企業で行うべき「情報セキュリティに関する方針や行動指針」を意味し、組織として統一のとれた情報セキュリティレベルを保つために策定される文書。

※３　アカウント…ネットワーク及び社内システムにログインする際の権利（ユーザ ID 等）。

※４　ＯＳ…メモリやハードディスクの管理やキーボードなどの入出力機能など、パソコンに基本的な動作をさせるために必要なソフト。

※５　パッチ（差分）…不具合の修正等への対応を行うため、アプリケーションの一部分を書き換えるプログラム。

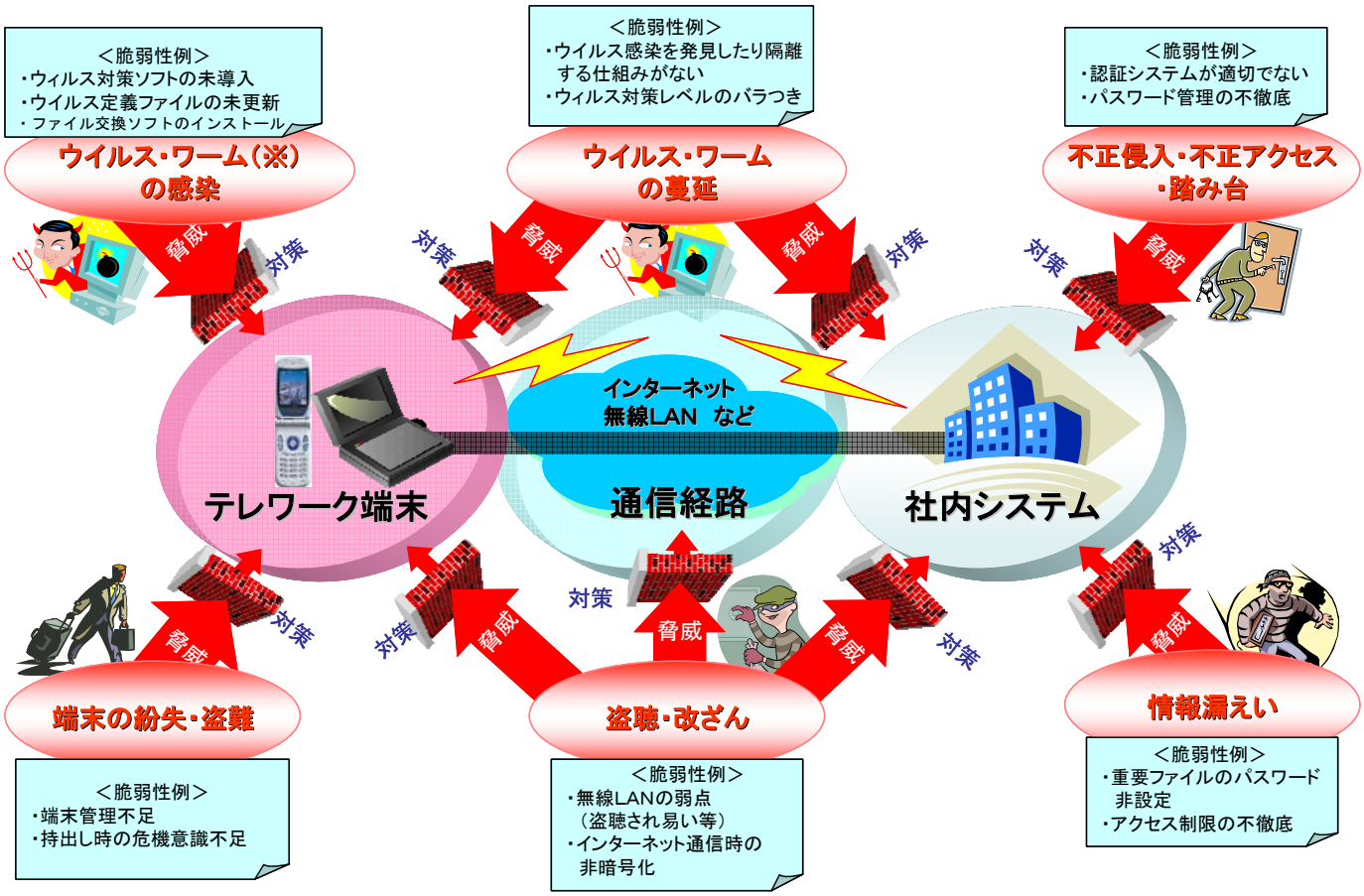
※６　ファイアウォール…不正アクセス等からサーバやパソコンを保護するための機器のこと。

※７　ルータ…通信経路の管理を実施しているネットワークを構成する機器のこと。

※８　安全な領域…守るべき重要な情報資産が、危害や損傷などを受けずに正常な状態でいられる領域のこと。情報セキュリティの三大要素である機密性、完全性、可用性が適切に確保されている必要があり、耐震設備や入退出管理設備などの「物理的」なものだけでなく、アクセス制御や認証など「論理的」な情報セキュリティ対策も含めて検討すべきである。

【参考】

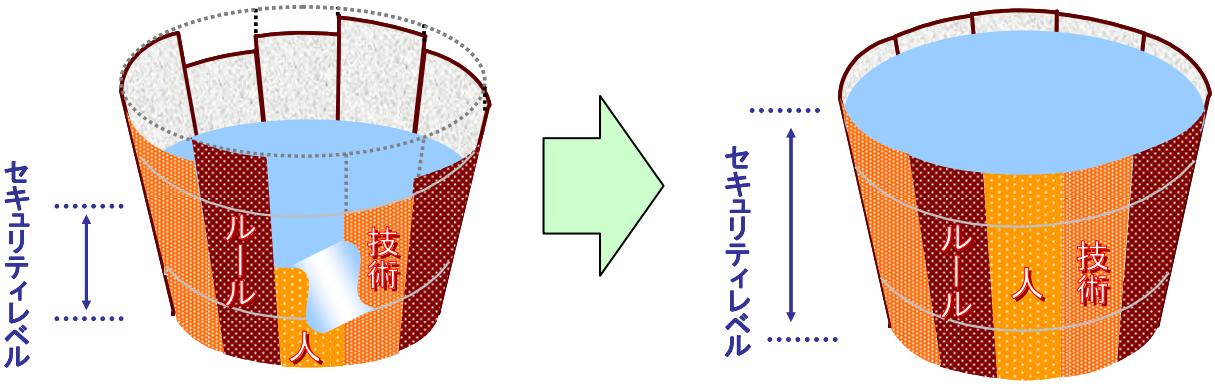
○テレワークにおける脅威と脆弱性



※　ワーム･･･自己増幅を繰り返しながら破壊活動を行うプログラム。

○テレワークセキュリティ対策のポイント

・バランスが悪い情報セキュリティ対策　　・バランスがとれた情報セキュリティ対策



「ルール」、「人」、「技術」のバランスが悪いと、対策として不十分になり、全体の情報セキュリティレベルは低下してしまう。

「ルール」、「人」、「技術」の対策がバランスよく保たれていると、高い情報セキュリティレベルを維持できる。