資料６

「テレワークセキュリティガイドライン（案）概要」

ガイドラインの狙い

○　ガイドラインは、大企業に限らず中小企業にとっても、内容が簡単に分かり、活用しやすいものとする。

○　ガイドラインは、基本的な実施すべきセキュリティ対策について紹介し、より詳細な内容・事例・セキュリティ対策事項については、「ガイドライン解説書」を作成し、対応する。

1.セキュリティ対策のポイント

○　ガイドラインの作成に当たっては、「ルール」、「人」、「技術」の対策をバランスよく保つことをポイントとする。

2.「ルール」についての対策

○　セキュリティ対策として、「何を守るのか」「誰から守るのか」「優先順位は」「どのように実施するか」をルールとして定めることは重要である。各種ルールはセキュリティポリシーの基本方針に基づき作成される必要があり、理解し易く、実施し易いものでなければならない。また、ルールの効果について定期的にチェックし、内容を見直すことにより適合性の向上を図ることも重要である。

○　ガイドラインでは、テレワーク環境を「テレワーク端末」、「通信経路」、「社内システム」に区分し、それぞれに対する行動規範について例示する。

3.「人」についての対策

○　適切なルールがあっても「人」すなわちテレワーク勤務者やシステム管理者等が定めた事項を遵守しなければ意味がない。ルールを定着させるためには、「セキュリティ教育・啓発活動」や「定期的なチェック（監査）」を行う必要がある。また、セキュリティ事故による影響を抑えるためにも、セキュリティ事故発生後の対応方法や、事前の抑止力として罰則規定などを定めておくことが効果的である。

○　ガイドラインでは、それぞれの対策について具体例を記述する。

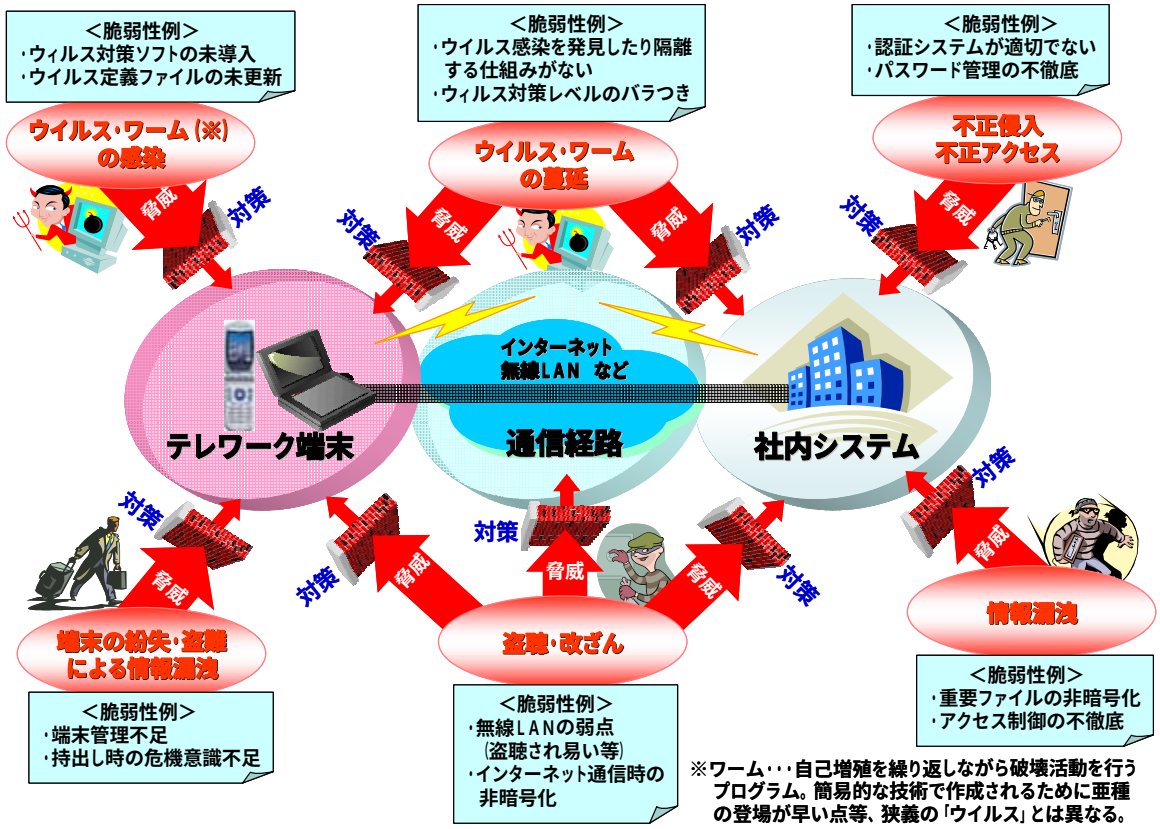
4.「技術」についての対策

○　技術的対策は「ルール」や「人」では対応できない脆弱性を補完するものであり、種々の脅威に対して「認証」「検知」「制御」「防御」を自動的に実施するものである。

○　ガイドラインでは、「ルール」同様、テレワーク環境を「テレワーク端末」「通信経路」「社内システム」に区分し、それぞれセキュリティ維持のために最低限実施すべきことを例示する。

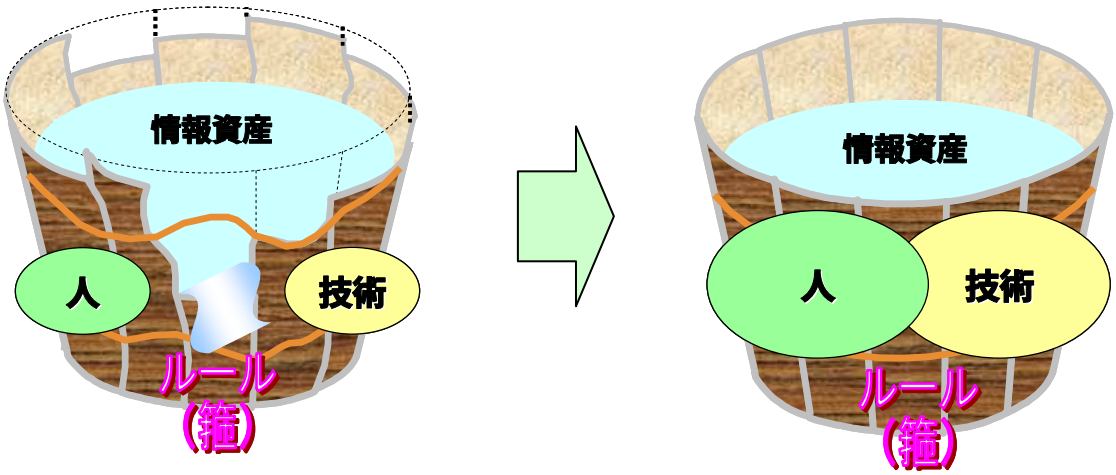
【参考】

○テレワークにおける脅威と脆弱性



○テレワークセキュリティ対策のポイント

・バランスが悪いセキュリティ対策　　・バランスがとれたセキュリティ対策



土台となる「ルール」が適切に定められていないと、「人」、「技術」の対策の効果が不十分となり、情報資産を守ることができない。

樽の箍（たが）となる「ルール」と、「人」、「技術」の対策がバランスよく保たれていれば、情報資産を守ることができる。