ゼロトラストセキュリティにおける ICT システムの運用管理要件に関する研究 －CSF の識別に着目したゼロトラストセキュリティの問題発生の未然防止－

アブストラクト

1. はじめに

テレワークの普及とクラウドシフトに伴い、企業のセキュリティ環境は大きな変化を遂げている。

この背景から、従来のイントラネットからゼロトラストネットワークへの移行を進める企業が増えているが、その導入における問題を抱えている企業も少なくない状況である。

2. 仮説の設定

本研究では、ゼロトラストセキュリティ（ZTA）の導入以降で企業が直面する苦労や失敗を分析し、主要な要因に焦点を当てることで、これらの問題の未然防止に向けた有益な提言を行うことができるという仮説を立てた。

3. 研究アプローチと提言

セキュリティのフレームワーク（CSF）を用いて企業が直面している問題の要因を整理した。その結果、CSF の中で「識別」というセキュリティ対策に関連する問題を多くの企業が抱えていることが明らかになった。そして、本研究では「識別」の中でも特に重要なセキュリティ対策である「資産管理」に焦点を絞り、次の提言を行った。「本研究で提示する「外部情報システム台帳」を中心に資産管理を確実に実施することで、ZTA 導入以降のインシデント対応における運用負荷を軽減できる。

4. 提言の検証・評価

ロールプレイを実施することで提言の検証を行った。ロールプレイではまず、仮想企業と仮想インシデントを定義した。そして資産管理が適切に実施されているパターンと、実施されていないパターンの 2 パターンの比較検証を実施した。

ロールプレイの結果、従来「資産管理」で考慮されてこなかった、あるいは変化が反映されていない「外部情報システム台帳」を管理することの重要性が増加していることが明らかになった。そして、本研究で提案した「外部情報システム台帳」フォーマットを使用して資産管理を行うことで、ゼロトラストセキュリティ導入以降のインシデント対応における運用負荷を軽減できることを示した。資産管理を適切に実施することで、セキュリティインシデント対応において、トリアージや対応の計画、事象の分析などの定量的・定性的な負荷削減効果が認められることが確認できており、提言の有用性を示すことができた。

5. まとめ

本研究では、企業における ZTA 導入以降で発生する問題を収集し、CSF を用いて分析を行った。その結果、「識別」に分類されるセキュリティ対策が問題の主な原因であることが明らかになった。そして、「識別」の中から「資産管理」に焦点を当て研究を行った。その結果、「外部情報システム台帳」などの台帳を活用することで、ZTA 環境におけるセキュリティインシデント対応の負荷を軽減する効果があることを明らかにした。