

要旨

**初心者による初心者のためのゼロトラストセキュリティ
～初心者がIPAを評価してみた～****1. はじめに**

テレワークの普及やクラウドの活用の拡大により、近年では社外にいながら入社時と同様の環境を使って業務することが珍しくなくなった。

社外で業務に従事するにあたり、従来の境界型のセキュリティではなくゼロトラストセキュリティの考え方が重要視されている一方で、ゼロトラストセキュリティという言葉を知っていても、中身がよくわからない、どうすれば導入できるのか、といった疑問を多くの方が感じているのではないかと推察される。

IE06では、そういった疑問を解消すべく、ゼロトラストセキュリティを導入するにはどうしたらよいか、何ができれば安全なのかを研究し、ゼロトラストセキュリティの導入プロセスを実践して検証を試みた。

2. 研究内容

セキュリティの専門業務担当ではない上、ゼロトラストセキュリティに対する知識ゼロの5名のメンバーが、ゼロトラストセキュリティの概念や導入プロセスを一から学び、わかりやすい解釈を示しつつ、実際に発生したセキュリティインシデント事案（重要データの入ったUSBの紛失による情報の流出）を題材にして課題を洗い出し、架空のゼロトラストセキュリティ導入を実践してみた。

実践の結果、過程で生じた気付きや留意すべき事項をまとめ、今後ゼロトラストセキュリティの導入を検討する方々への参考材料として掲示する。

3. 研究手順

ゼロトラストセキュリティの知識習得の手掛かりとして、IPAが公開する『ゼロトラスト導入指南書』に記載されている概念や考え方、技術的な構成要素を理解したのち、架空の世界をチームメンバーで創り出し、独自の解釈を交えゼロトラストセキュリティの概要をまとめた。

その後、同じくIPA公開の『ゼロトラスト移行のすゝめ』に記載されている導入プロセス従い、セキュリティインシデント事例の再発抑止に必要な架空のゼロトラストセキュリティ導入を以下の手順で検討し実践した。

(1) 導入事例の選定

インシデント事例の設定に際し、シンポジウム出席者を含め課題や導入をイメージしやすい事例を選定。

要旨

(2) As-Is分析

現状の課題がどこにあるのかを以下の観点で分析し、ありたい姿を検討。

- ・セキュリティ観点
- ・ユーザー利便性観点
- ・IT環境の運用効率化観点

(3) グランドデザイン作成

As-Is分析からAs-Is構成（現状の構成）、そこからTo-Be構成（ありたい姿を実現するための構成）を作成。

そこから具体的な導入ソリューションの検討を実施。

(4) 投資判断

今回の研究では投資判断を諮る経営者や予算が示されていないため、移行に際して必要となる費用を概算で示すまでに留めた。

(5) 環境構築

グランドデザイン作成で検討した具体的なソリューションを組み込んだモデルケースを作成。

(6) 研究活動の振り返り・評価の実施

(1)～(5)を経ての気づきや改善事項等をまとめ、IPAの『ゼロトラスト移行のすゝめ』や『ゼロトラスト導入指南書』の内容に対する我々の評価を示した。

4. 研究結果・考察

実際のゼロトラストセキュリティ導入現場では期間、予算、企業のセキュリティポリシー等の制約がある中で対応するところだが、研究会という特性上、これらの制約なく技術や製品の導入を検討したため、仮説や架空の前提を置いて導入検討を実施した。その結果、実際の企業が実施するゼロトラストセキュリティ導入とは異なる手法やアプローチになっている可能性が高く、また実用性評価までを検証することが期間的にも困難な結果となった。

一方で、これからゼロトラストセキュリティ導入を検討される企業や団体が、導入プロセスを検討する上での参考事例として活用できる内容となっているものとする。

- 参考文献

- 独立行政法人情報処理推進機構（IPA）『ゼロトラスト移行のすゝめ』
<https://www.ipa.go.jp/files/000099778.pdf>
- 独立行政法人情報処理推進機構（IPA）『ゼロトラスト導入指南書』
<https://www.ipa.go.jp/files/000092243.pdf>

- 文章内の記載の会社名および製品名は、各社の登録商標または各社に帰属する標章もしくは商号です。