

企業のゼロトラスト・アーキテクチャ導入におけるベストプラクティスの検討

Examining best practices of zero-trust architecture implementations for enterprise network

岡本 優 マネジメント分科会 情報セキュリティ大学院大学

Abstract: In recent years, the term "Zero Trust" or "Zero Trust Architecture (ZTA)" has come to be widely used due to the expansion of cloud services in enterprises and the spread of remote work. Although the introduction of Zero Trust is being considered in the context of DX in enterprises, it has not been widely adopted. Based on the results of a market survey, companies are considering the introduction of Zero Trust, but the introduction has not progressed very much. This paper presents the results of our research and investigation into the background of the lack of progress in implementation, and the possibility of using the latest zero-trust technology and implementation methods to promote zero-trust implementation and propose "best practices".

研究の背景

最近の企業ネットワークの取り巻く環境

- ・クラウドシフト
- ・DXや働き方改革の推進
- ・コロナ禍におけるリモートワーク普及
- ・VPN製品におけるボトルネック・脆弱性

既存の境界防御の限界⇒「境界型からゼロトラストへ」

- ・近年日本国内でもゼロトラストのソリューションを導入する企業・組織が増えているが、市場調査からZTAが導入はあまり進んでいないのが現状

導入の進まない背景を掘り下げ、最新のゼロトラスト技術・導入手法により、ゼロトラスト導入を推進できる手法を検討

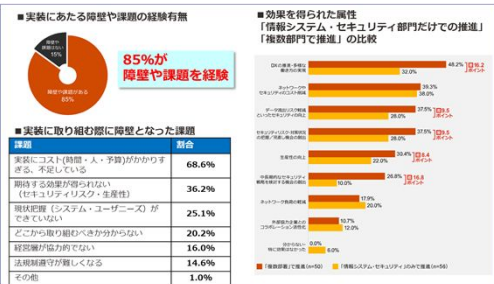


ベストプラクティスを提案できないか研究調査を実施

先行研究

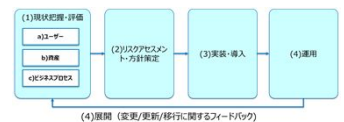
①市場調査

導入の障壁：コスト面・導入効果・経営者の協力
組織横断的に推進する企業がZTAの効果が出ている



③導入プロセス

NIST 800 207
導入ステップを繰り返しZTAを段階的に導入



導入の目的を明確化

⇒あるべき姿に近づけるための検討・計画

- ・企業での経営課題に対してZTをどのように導入するか目的を明確化
- ・セキュリティ強化観点のみ実施すると費用対効果が見込めず頓挫する可能性がある

②事例調査・技術調査

Google BeyondCorp

10年かけて数万人の従業員に対してVPNを使わないネットワークアクセスを実現。導入を進めるために企業によって守るべき情報資産、利用するユーザー・デバイスなどのインベントリ調査を行うことから導入が始まる

認証認可技術

- ①多要素認証(MFA)+シングルサインオンSSOが基本
- ②コンテキストアウェア、継続的認証にも課題がある

④ゼロトラスト導入関連研究

ゼロトラスト成熟度モデル

企業や組織がゼロトラスト計画を立案する際に、自分たちが今どこにいて、どこを目指すべきなのか明示



今後の研究

- ・ゼロトラストにおける重要要素の認証認可技術の深堀・課題抽出
- ・導入における課題について、事例などの継続的な調査・実際の企業へのヒアリングを実施
- ・導入におけるベストプラクティス(あるべき姿)を検討