サイバー防衛戦略の物理的セキュリティへの応用に関する理論的考察
―境界防御からゼロトラストへの進化を援用した多層防御フレームワークの提案―

成田浩志*
Koji Narita

要旨：
物理・人的セキュリティ分野では、現場担当者の直感への依存や、複雑化する脅威への対応遅延といった課題が存在する。本稿は、サイバーセキュリティ分野における防衛戦略の進化、すなわち「境界防御モデル」から「ゼロトラスト・アーキテクチャ」への移行プロセスを理論的基盤として援用し、物理空間における対人リスクを段階的に評価・判断するための新たな多層防御フレームワークを提案するものである。本フレームワークは、「安全性」「法律」「コミュニケーション」の３つの防御層を通じて、明白な物理的脅威から、ルール違反、そして文脈的な異常へと段階的に検証を行う。この理論的試論を通じ、物理セキュリティ分野に、再現性と汎用性のある新たな判断構造を提供することを目的とする。

キーワード：物理セキュリティ、サイバーセキュリティ、ゼロトラスト、多層防御、対人リスク、判断プロセス

Abstract：
In the field of physical and human security, challenges persist, such as an over-reliance on the intuition of front-line personnel and delays in responding to increasingly complex threats. This paper draws upon the evolution of defense strategies in the cybersecurity domain-specifically, the shift from the ″perimeter defense model″ to the ″Zero Trust Architecture″-as a theoretical foundation. It proposes a novel multi-layered defense framework for systematically assessing and making judgments about interpersonal risks in physical spaces. This framework conducts a phased verification process across three defensive layers-″Safety,″ ″Legality,″ and ″Communication″-to evaluate threats ranging from overt physical dangers and rule violations to contextual and behavioral anomalies. Through this theoretical exploration, the paper aims to provide the field of physical security with a new, reproducible, and versatile judgment structure.

Keywords: Physical Security, Cybersecurity, Zero Trust, Multi-layered Defense,