物理セキュリティアーキテクチャの戦略的設計論
― サイバー・軍事防衛原則の応用による多層防御フレームワークの構築 ―
（ドラフト）

成田浩志*
Koji Narita
2025 年 9 月 16 日

要旨： 民間組織の物理セキュリティは、場当たり的な対策の継ぎ足しに陥りやすく、体系的な戦略設計が欠如しているという課題を抱える。本稿は、この課題を克服するため、サイバーセキュリティや軍事研究において実証されてきた普遍的な防衛原則、特に「多層防御（Defense in Depth)」や「指揮・統制・インテリジェンス」の概念を物理セキュリティの文脈に「翻訳」し、応用する。これにより、組織全体の防衛体制を設計するための、新たな戦略的フレームワークを提案する。本フレームワークは、①戦略・インテリジェンス層、②能動的対応層、③抑止・検知層の 3 層で構成され、組織が構築すべき防衛アーキテクチャの合理的かつ再現性のある青写真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 , 戦略的設計論 , 多層防御 , サイバーセキュリティ , 軍事原則 , リスクマネジメント , 組織防衛

Abstract：Physical security in private organizations faces the challenge of often resorting to a patchwork of ad-hoc countermeasures, lacking a systematic strategic design. To overcome this issue, this paper ″translates″ and applies universal principles of defense proven in cybersecurity and military research-specifically the concepts of ″Defense in Depth″ and ″Command, Control, and Intelligence″-to the context of physical security. By doing so, it proposes a new strategic framework for designing an organization's overall defense posture. This framework consists of three layers: (1) the Strategy and Intelligence Layer, (2) the Active Response Layer, and (3) the Deterrence and Detection Layer, and aims to provide a rational and reproducible blueprint for the defense architecture that organizations should build.

Keywords: Physical Security , Strategic Design , Defense in Depth , Cybersecurity , Military Principles , Risk Management , Organizational Defense

---

* SIP(Security Innovation Project)代表