The Bulletin of Seisa Dohto University
No.7, 209－213, 2026

研究ノート

eスポーツとセキュリティに関する研究：包括的セキュリティフレームワークの提案

鷹　田　勇　智

要約

近年のeスポーツ市場の急速な拡大に伴い，プレイヤー，観客，運営組織が直面するセキュリティリスクが深刻化している。本研究では，eスポーツエコシステムにおける多層的なセキュリティ脅威を体系的に分析し，技術的脅威から社会的リスクまでを包含する包括的セキュリティフレームワークを提案する。DDos攻撃，チート行為，個人情報漏洩，ハラスメントなどの具体的事例を検証し，現行の対策の限界を明らかにした。提案フレームワークは，予防的セキュリティ，リアルタイム監視，インシデント対応，教育・啓発の四層構造からなり，産業界と学術界の協働による持続可能なセキュリティ環境の実現を目指す。本研究の成果は，eスポーツ産業の健全な発展と参加者の安全確保に寄与することが期待される。

キーワード：eスポーツ，サイバーセキュリティ，オンラインゲーム，情報セキュリティ

1．はじめに

21世紀に入り，eスポーツ（Electronic Sports）は単なる娯楽から，世界的な競技スポーツへと発展を遂げた。複数の調査機関の報告によれば，世界のeスポーツ市場規模は2023年に約23億ドルに達し，視聴者数は5億人を超えている。この急速な成長の背景には，デジタル技術の進歩，インターネット環境の整備，そして新型コロナウイルス感染症による在宅時間の増加がある。

しかしながら，eスポーツの発展と同時に，様々なセキュリティ上の課題が顕在化している。内閣官房　国家サイバー統括室（2025）は，オンラインゲーム環境における脅威が従来のサイバーセキュリティの範疇を超えて多様化していることを指摘している。特に，大規模な国際大会においては，競技の公正性を脅かすチート行為，配信インフラを標的とするサイバー攻撃，プレイヤーの個人情報を狙った不正アクセスなど，複合的なリスクが存在する。

従来のサイバーセキュリティ研究は，主に企業や政府機関を対象としたものが多く，eスポーツという新しい分野特有の課題に対する包括的な分析は限定的である。本研究では，eスポーツエコシステム全体を俯瞰し，技術的脅威から社会的リスクまでを統合的に分析することで，実効性の高いセキュリティフレームワークの構築を目指す。

2．eスポーツの現状と発展

eスポーツの歴史は1970年代のアーケードゲーム競技会に遡るが，現代的なeスポーツの基盤が形成されたのは2000年代以降である。高速インターネットの普及とストリーミング技術の発達により，地理的制約を超えた大規模な競技環境が実現した。特に，Twitch，YouTube，中国の

Douyu 等のプラットフォームの登場は，e スポーツの観戦文化を確立し，産業化を加速させた。

現在の e スポーツ市場は，複数のステークホルダーによって構成される複雑なエコシステムを形成している。プレイヤー，チーム，リーグ運営者，スポンサー企業，配信プラットフォーム，観客が相互に関連し合い，それぞれが異なるセキュリティリスクを抱えている。Andrea *et al.*（2023）は，このような多層構造がセキュリティ管理を複雑化させる要因であると分析している。

地域別に見ると，アジア太平洋地域が最大の市場を形成しており，特に韓国，中国，日本における政府レベルでの支援策が目立つ。韓国では 2019 年に e スポーツ振興法が制定され，中国では国家体育総局が e スポーツを正式なスポーツ競技として認定している。一方で，これらの地域では政府による規制も強化されており，セキュリティ要件の厳格化が進んでいる。

3．e スポーツにおけるセキュリティ脅威の分析

3.1　技術的脅威

e スポーツにおける技術的脅威は，主に四つのカテゴリに分類される。第一に，ゲーム内不正行為（チート）がある。これには，自動操作ボット，ウォールハック，エイムボットなどのソフトウェア型チートと，専用ハードウェアを用いた物理的改変が含まれる。実際に 2014 年に開催された Counter-Strike: Global Offensive（CS：GO）の大会「DreamHack CS:GO Championship」への出場停止処分が下されている。他にも，2024 年に開催された Apex Legends の公式世界大会「Apex Legends Global Series（ALGS）」にて，出場選手たちへ勝手にチートを付与するといったハッキング被害が発生している。

第二に，DDoS 攻撃による配信インフラの妨害が挙げられる。近年の大規模大会では，配信サーバーやゲームサーバーを標的とした DDoS 攻撃が頻発しており，競技の中断や視聴体験の悪化を引き起こしている。

第三に，マルウェアとランサムウェア攻撃がある。これらは，ゲームプラットフォーム，トーナメントシステム，運営組織のネットワークに重大なリスクをもたらす。

第四に，フィッシング詐欺とソーシャルエンジニアリング攻撃である。攻撃者は公式の開発者やサポートチームを装い，プレイヤーから機密情報を詐取する手法を用いている。

3.2　情報セキュリティ脅威

個人情報の保護は，e スポーツにおいて特に重要な課題である。プロプレイヤーは，本名，住所，収入情報などの機密情報を複数のプラットフォーム上で管理する必要があり，情報漏洩のリスクが高いと考えられる。また，一部 web 上の報告では，ゲーム業界におけるウェブアプリケーション攻撃の件数が 2021 年に約 2 倍に増加し，プレイヤーの機密データに影響を及ぼしている可能性があるとの指摘もある。

また，ソーシャルエンジニアリング攻撃も深刻な問題となっている。攻撃者は，プレイヤーの SNS アカウントを詳細に調査し，個人的な情報を利用してなりすましやフィッシング攻撃を行う。特に，若年層のプレイヤーは，セキュリティ意識が低く，被害に遭いやすい傾向がある。

3.3　社会的・心理的脅威

e スポーツ特有の脅威として，オンラインハラスメントとスウォッティング（偽の緊急通報による実住所への警察派遣）が挙げられる。Sky Broadband（2023）が 4000 人の女性ゲーマーを対象に行った調査によると，49％の女性がオンラインゲームのプレイ中やゲーム配信中にハラスメントを受けたことがあると回答していた。回答者の年齢層を 18～24 歳に絞ると，75％まで上昇していた。

4．セキュリティ対策の現状と課題

4.1　現行の技術的対策

現在，eスポーツ業界では様々な技術的対策が講じられている。アンチチートシステムについては，Valve Anti-Cheat（VAC），BattlEye，Easy Anti-Cheatなどの商用ソリューションが広く採用されている。これらのシステムは，機械学習アルゴリズムを用いて不審な行動パターンを検出し，リアルタイムでの対応を可能にしている。

しかしながら，マルウェアと同様にこれらの対策は常にチート開発者との「いたちごっこ」の状況にあり，完全な解決には至っていない。特に，AIを活用した高度なチートツールの登場により，従来の検出手法の限界が露呈している。

4.2　法的・制度的対策の限界

法的な観点では，各国でeスポーツに関する規制整備が進んでいるものの，国際的な統一基準の欠如が課題となっている。韓国のゲーム産業振興法や中国のネットワークセキュリティ法など，先進的な取り組みも見られるが，グローバルなeスポーツ大会においては，複数の法域にまたがる複雑な問題が生じている。

また，プラットフォーム事業者の自主規制に依存する部分が大きく，統一的なセキュリティ基準の策定が急務である。

4.3　教育・啓発活動の不足

セキュリティ意識の向上については，組織的な取り組みが不十分である。多くのプレイヤー，特に若年層は，基本的なセキュリティ知識を欠いており，簡単な攻撃の被害に遭うケースが多い。

5．提案する包括的セキュリティフレームワーク

5.1　フレームワークの基本構造

本研究では，eスポーツエコシステム全体をカバーする包括的セキュリティフレームワーク（Comprehensive Esports Security Framework：CESF）を提案する。CESFは，予防的セキュリティ層，リアルタイム監視層，インシデント対応層，教育・啓発層の四層構造からなる。

5.2　予防的セキュリティ層

予防的セキュリティ層では，脅威の発生を未然に防ぐための基盤的対策を実装する。この層には，セキュアなアカウント管理システム，多要素認証の義務化，定期的なセキュリティ監査，プライバシー設定の最適化などが含まれる。

特に重要なのは，ゼロトラスト原則に基づくアクセス制御の実装である。全てのデバイス，ユーザー，アプリケーションを潜在的な脅威として扱い，継続的な認証と認可を行う。これにより，内部脅威や侵害されたアカウントによる被害を最小化できる。

5.3　リアルタイム監視層

リアルタイム監視層では，AIと機械学習を活用した高度な脅威検知システムを構築する。このシステムは，ゲーム内行動分析，ネットワークトラフィック解析，ソーシャルメディア監視を統合し，多角的な脅威検知を実現する。

提案するシステムでは，ブロックチェーン技術を活用した改ざん防止機能も実装する。競技結果やプレイヤーデータの完全性を保証する。

5.4　インシデント対応層

インシデント発生時の迅速な対応を可能にする専門的な対応体制を構築する。この層では，24時間365日体制のセキュリティオペレーションセンター（SOC），自動化されたインシデント対応システム，法執行機関との連携体制などを整備する。

また，被害者支援プログラムも重要な要素である。ハラスメントやサイバー攻撃の被害を受けたプレイヤーに対し，心理的支援，法的助言，技術的復旧支援を提供する包括的なサポート体制を構築する。

5.5　教育・啓発層

持続可能なセキュリティ環境の実現には，全ステークホルダーのセキュリティ意識向上が不可欠である。年齢層や役割に応じたカスタマイズされた教育プログラム，定期的なセキュリティトレーニング，最新脅威情報の共有システムなどを実装する。

6．おわりに

本研究では，急速に発展するｅスポーツ業界における多様なセキュリティ脅威を体系的に分析し，包括的セキュリティフレームワーク（CESF）を提案した。提案フレームワークは，技術的対策，制度的対策，教育的対策を統合したホリスティックなアプローチを採用し，ｅスポーツエコシステム全体の安全性向上を目指している。

今後の課題として，実環境での実証実験の実施，コスト効率の最適化，国際標準化の推進などが挙げられる。また，AI 等の新技術の発展に伴う新たな脅威への対応も継続的に検討する必要がある。

ｅスポーツが社会に広く受け入れられ，持続可能な産業として発展するためには，セキュリティの確保が前提条件である。本研究の成果が，安全で公正なｅスポーツ環境の実現に貢献することを期待する。

参考文献

1）Andrea Czakó, Orsolya Király, Patrik Koncz, Shu M Yu, Harshdeep S Mangat, Judith A Glynn, Pedro Romero, Mark D Griffiths, Hans-Jürgen Rumpf, Zsolt Demetrovics (2023), J Behav Addict, 12(1), 1–8

2）Anna-Greta Nyström, Brian McCauley, Joseph Macey, Tobias M. Scholz, Nicolas Besombes, Joaquin Cestino, Julia Hiltscher, Stephanie Orme, Ryan Rumble, Maria Törhönen. (2022). Current issues of sustainability in esports, International Journal of Esports, 1(1), 1–10

3）Denysova Lolita, Lavrov Vitaliy (2024), Esports and Cybersecurity: Modern Digital Solutions, Sport Science and Human Health, 11(1), 1–13

4）小孫康平（2021），ｅスポーツを学校に導入する際の課題と情報モラル教育，AI 時代の教育論文誌，４，13–18

5）内閣官房 国家サイバー統括室（2025），新たなサイバーセキュリティ戦略の方向性，国家サイバー統括室（2025/7/1），chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.nisc.go.jp/pdf/council/cs/n01/01document1.pdf，（アクセス日：2025/8/24）

6）望月拓実（2021），我が国に求められるｅスポーツ研究：文献レビューによる検討，国際研究論叢：大阪国際大学紀要，34(2)，75–96

Research on Esports and Security: Proposal for a Comprehensive Security Framework

KOMODA Yuchi

Abstract

The rapid expansion of the esports market in recent years has led to increasingly severe security risks for players, spectators, and organizing bodies. This study systematically analyzes the multi-layered security threats within the esports ecosystem and proposes a comprehensive security framework encompassing threats ranging from technical vulnerabilities to social risks. We examined specific cases such as DDoS attacks, cheating, personal information leaks, and harassment, revealing the limitations of current countermeasures. The proposed framework consists of a four-layer structure: preventive security, real-time monitoring, incident response, and education/awareness, aiming to achieve a sustainable security environment through collaboration between industry and academia. The outcomes of this research are expected to contribute to the healthy development of the esports industry and the safety of its participants.