氏　　名	乗松　隆志
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第　　７２７５　　号
学位授与の日付	２０２５年　３月　２５日
学位授与の要件	自然科学研究科　　産業創成工学専攻 （学位規則第４条第１項該当）
学位論文の題目	A Study on Information Security for End-to-End Communication by TCP/IP Internet Protocol Suite （TCP/IP インターネットプロトコルスイートを利用したエンドツーエンドの通信の情報セキュリティの研究）
論文審査委員	教授　山内　利宏　　教授　太田　学　　准教授　乃村　能成

学位論文内容の要旨

As smart devices become increasingly sophisticated, collaboration between SNS applications and financial service APIs, known as open banking, has become common through the TCP/IP protocol suite. This trend heightens the importance of information security in end-to-end communication between user applications on devices and server-side services. According to ISO/IEC 27000:2018, information security involves maintaining confidentiality, integrity, and availability.

To ensure secure API access, Transport Layer Security and OAuth 2.0 are employed; however, unauthorized API access remains a concern. The Financial-grade API (FAPI) security profile is proposed to mitigate this risk, but its implementation relies heavily on configuring an OAuth 2.0 authorization server. This process often requires significant man-hours, leading to potential misconfigurations and inefficiencies in the development cycle.

In response, we developed a policy-based method for applying security profiles, featuring two modules: a Profile module that implements the security profile and a Policy module that determines when and which profile to apply based on request context. Our analysis showed that this method can significantly reduce the man-hours required for configuration.

We also created a conformance test execution platform designed to streamline the testing of FAPI security profiles against Keycloak, an open-source identity and access management solution. This platform automates the setup of necessary server programs, formalizes testing procedures, and allows for parallel execution of conformance tests, thus maintaining the efficiency of Keycloak's CI/CD processes. We verified that the platform can effectively run tests for multiple security profiles, ensuring compliance without extending the CI/CD cycle.

Lastly, we explored bandwidth control strategies within networks using PROFINET to manage latency effectively in both real-time and best-effort communications. Our mathematical model derived from queuing theory provides insights into traffic volume thresholds, helping to maintain optimal availability.

Through this research, we addressed critical issues in securing end-to-end communication for API access. Our contributions, including the implementation of policy-based security profiles and the conformance testing platform, have been integrated into the OSS Keycloak, ensuring free access to these enhancements for the community.

論文審査結果の要旨

スマートデバイスの高性能化と普及に伴いAPIアクセスによるアプリケーション間連携が一般的となり、アプリケーションとサーバ間のエンドツーエンド通信の情報セキュリティ（機密性、完全性、可用性の維持）の重要性が高まっている。

論文提出者は、APIアクセスによるアプリケーション連携において、TLSとOAuth 2.0の適用に加えて、セキュリティプロファイルを適用することにより、エンドツーエンド通信の機密性と完全性を保つ手法を実現した。機密性について、認可サーバの設定ミスが生じる可能性があるという課題については、セキュリティプロファイルを適用することで、設定ミスと設定工数を低減できることを示した。また、完全性について、セキュリティプロファイルの実装の正しさをテストするための工数が大きく、処理時間が長いという課題に取り組み、複数のテストを並列自動実行できる開発環境を構築し、課題を解決し、かつその有効性を示した。論文提出者は、これらの方式をオープンソースソフトウェアであるKeycloakに実装し、本研究成果を誰でも利用可能な形式で公開している。

さらに、可用性の観点では、エンドツーエンド通信の可用性の中でもレイテンシに着目し、リアルタイム通信とベストエフォート型のネットワークが混在するネットワークにおいて、可用性が失われることを防止する方法として、リンク層におけるレイテンシとネットワークに流入する通信量の間の関係を数理モデルで分析した。この分析により、ベストエフォート型通信の可用性を維持するために、ネットワークに流入する通信量をどの量以下にすべきかを明らかにし、この値を帯域制御の閾値に利用できることを述べた。

以上のように、本論文は、アプリケーションとサーバ間のエンドツーエンド通信環境において、機密性、完全性、可用性を維持するための課題を解決しており、情報工学に寄与するところが大きい。また、研究成果の大部分をオープンソースソフトウェアとして公開し、実際のサービスで利用されている点も評価できる。よって、本論文は博士（工学）の学位に値すると認める。

なお、論文発表会では、適切な説明が行われ、質疑に対する応答も適切であった。これにより、十分な学力を有すること、及び自立した研究者として活動を行う能力を有することが確認できた。