

計算科学研究センター（ネットワーク担当）

大野人侍（准教授）（1996年4月1日着任，2019年10月1日昇任）

A-1) 専門領域：情報科学，ネットワーク運用技術及びサイバーセキュリティ

A-2) 研究課題：

- a) ソフトウェアを用いたネットワークの自動制御
- b) ログ解析等によるネットワーク／サイバーセキュリティの自動最適化及び認証

A-3) 研究活動の概略と主な成果

- a) ORION2022（Okazaki Research Institutes Organization Network）において，Google Workspace等のパブリッククラウドサービスの利用を前提としたゼロトラスト・アーキテクチャを取り入れたシステム構築を行い，従来のORION主認証システムを拡張し，ゼロトラストを実現する認証基盤とした。ORION主認証システムは，FIDO規格に準拠した多要素認証（MFA）を利用した新しい統合認証システム（IdP）に改修し運用している。ORION2022主認証システムは，ORIONへのネットワーク接続時の定期的な端末及びユーザ認証，VPN接続時ユーザ認証及びGoogle Workspace等のユーザ認証に利用されMFA及びシングルサインオン機能を提供している。また，MFAを行う事により確実に本人確認が行えるようになった。2023年度の早い段階でMicrosoft365の認証も統合できるように開発を進めている。

更に，アンチウイルス・ソフトウェアに代わり新たに端末向けにEDR（Endpoint Detection and Response）の導入や端末の脆弱性検査機能の導入など，ゼロトラストを実現する上で重要な本人認証及び端末健全性の担保を行えるようにしている。

- b) ORION2022で導入した器機及びサービスではAPIの提供を原則求めており，提供されたAPIによりログやイベントなどの自動取得や処理の自動化，器機／サービス間連携を行えるようになっている。また，標準で提供されていない機能についてもAPIとローカルプログラムを組み合わせる柔軟に提供している。

C) 研究活動の課題と展望

ユーザや端末の認証と認可の統一化を推進していく。ORION2022は，クラウド等ORION外部のサービスを含んだ統合型ユーザ／端末管理・認証基盤，現在のログ解析基盤を拡張発展させクラウド・ログを取り込みORIONとクラウドの一貫した取扱と分析を可能とする情報セキュリティ・インシデント対応基盤やそれらを統合し自動制御するシステムとして設計，仕様化し調達を行い運用を開始している。更に，APIによるシステム間連携が行えるようになっているため，APIを用いた各システム間の連携や独自機能の開発と運用開始しており，今後機能拡張を行っていく。