IPA

2024 年度 未踏 IT 人材発掘・育成事業 採択案件評価書

1. 担当 PM

竹迫 良範
（株式会社リクルート データ推進室 アドバンスドテクノロジーラボ 所長）

2. クリエータ氏名

小林 麟太郎
（The University of Edinburgh College of Arts, Humanities and Social Sciences）

3. 委託金支払額

2,880,000 円

4. テーマ名

ゼロトラストネットワークアクセスの導入を容易にするクラウド型プロキシの開発

5. 関連 Web サイト

なし

6. テーマ概要

本プロジェクトでは従来の境界型防御の問題点を補うゼロトラストセキュリティを容易に導入するクラウド型プロキシをフルスクラッチで開発した。既存のポリシー記述言語と異なり、大規模言語モデル（LLM）と連携し、日本語による自由記述可能な制御ポリシーを記述できるようにした点が特徴である。

7. 採択理由

近年テレワークが普及した日本において、より安全なセキュリティを担保するために、従来のプライベートネットワーク＋VPN によるアクセスではなく、ゼロトラストネットワークアクセス（ZTNA）を新規に導入する企業が増えてきている。ZTNA を実現するソリューションはいくつか存在するが、そのほとんどが外国製のシステムやクラウドサービスを使うことを前提としていることが多い。業務中に謎の通信不具合に遭遇して従業員が困ってしまうケースもあると聞く。このようなソリューションをブラックボックスのままで導入すると、自社の組織で可用性や情報取得・破棄をコントロールできる範囲が限定さ

れてしまうリスクも存在する。
　本提案は、令和 4 年 6 月 30 日にデジタル庁が公表したゼロトラストアーキテクチャ適用方針に準拠したアイデンティティー認識型プロキシ（IAP）をフルスクラッチで開発するという野心的なプロジェクトである。サーバやネットワークの構築からソフトウェアの開発導入までをすべて自前で行うことによって、ブラックボックスの要素を極力排除した柔軟性の高いシステムの構築が可能となる。IAP の実現には複数の要素技術を適切に組み合わせる必要があり、同時にパフォーマンス上の課題も解決しなければ現実的な導入は難しくなる。実現のためには多くの試行錯誤が必要となるプロジェクトになると思うが、日本企業への ZTNA 普及へ一石を投じる挑戦になることを期待する。

8. 開発目標

　テレワークの普及により、企業ネットワークへの社外からの接続が一般化し、ネットワーク内外の境界が曖昧になる中で、サイバー攻撃が急増している。特に VPN 機器を経由した侵入が多く、従来の境界型防御モデルでは対応が難しくなっている。このような状況を受けて注目されているのが、アクセス元や場所を問わず厳格な認証と最小権限の原則に基づくゼロトラストセキュリティである。一方で、ゼロトラストの導入には費用や運用の複雑さ、高度な知識の要求、外国製品への依存といった課題がある。特に中小企業や地方自治体など、リソースの限られた組織では導入のハードルが高く、より手軽で柔軟、かつ国産のシステムが求められている。
　このような背景から本プロジェクトでは以下の 3 つを開発目標とした。

(1) オールインワンのクラウド型プロキシの開発
　ゼロトラストアーキテクチャの最低要件を満たす機能をクラウド上で提供する。専門的な導入作業を必要とせず、ユーザが簡単に安全なネットワークを構築できる環境を実現する。

(2) 低コストかつ柔軟性の高いシステムの実現
　ソフトウェアを低レイヤーからアプリケーションレイヤーまで自前で開発し、サーバ・ネットワークのバックボーン技術も自ら構築し運用する。ブラックボックス化を避け、外部製品への依存を極力低減する。それにより現場に応じた柔軟な構成・運用が可能なシステムを提供する。

(3) 最低限の知識で運用可能な分かりやすいシステムの構築
　複雑なネットワーク機器操作やポリシー記述言語の習得を不要にする。エンジニア経験の少ない情報システム管理者でも運用に参加でき、容易に状態を監視・管理できる UI/UX 設計を目指す。

9. 進捗概要

本プロジェクトでは令和 4 年にデジタル庁が公表した「ゼロトラストアーキテクチャ適用方針」に適合することを前提とし、次の 4 つのシステムをそれぞれフルスクラッチで開発した。

(1) ユーザ・デバイス認証基盤システム

ユーザアカウント・デバイス情報を一元的に管理するためのシステムを、ユーザ管理機能、ユーザグループ管理機能、デバイス管理機能を中心に開発した。ユーザ管理機能では、組織内メンバに対してユーザアカウントを発行し管理するとともに、ユーザグループ管理機能として同じ役職等に属するユーザどうしをグループとして管理する。これは主にロール管理の用途で利用することを想定している。デバイス管理機能では、ユーザが保有する Windows デバイスの情報を取得し、一元的に管理する。デバイス情報を取得するため、Rust 1.82.0 をベースにネイティブアプリケーションを設計・実装した。これを通じて、搭載 OS の詳細情報や接続中のネットワーク情報、Trusted Platform Module の有無、BitLocker によりドライブが暗号化されているかどうか、Windows Hello に対応しているかどうか等のセキュリティ要件情報、位置情報、インストール済みのすべてのアプリケーション情報などを取得する。ここで取得する情報についても、後述するシステムのポリシーの要素として利用することができる。これにより統合エンドポイント管理（Unified Endpoint Management, UEM）の一部機能を代替することが可能である。また位置情報をもとに、ジオフェンシング等に用いることができるようにした。

(2) アクセス制御ポリシーシステム

ユーザ・デバイス認証基盤システムや外部 IDaaS（Identity as a Service）で管理されているユーザの身元やデバイス情報に基づき、保護リソースに対するアクセスを制御するアクセス制御ポリシーを作成、施行することで安全な接続を実現するシステムを開発した。クラウドサービスへのアクセスを制御する SaaS モード、ファイアウォール等により隔てられ外部からはアクセスすることができない機密性の高い社内システムへのアクセスを制御するトンネリングモードの 2 つを開発し、多様なニーズに応えられる環境を構築した。SaaS モードでは、SAML 2.0 に基づいて認証を実施し SaaS へのアクセスを制御する。このモードでは、自社のクラウドエンジニアがクラウドサービスにアクセスする際に、クラウドサービスのログイン機能だけでは賄うことができない、高度なアクセス制御を行いたいといったニーズを主に想定している。Google が提供する大規模言語モデル API である Gemini API と連携することで、日本語による自由記述式のアクセス制御ポリシーの作成を実現した。各アプリに対し、必須条件（～を満たさなければアクセスすることができない）と、拒否条件（～を満たしたら

ばアクセスすることができない）を設定することができる。例えば必須条件として「アクセス元の国名が日本であり、所有するデバイスは TPM が有効で、ドライブが BitLocker により暗号化されていること」という文章を設定することができる。この場合、外国からのアクセスや、セキュリティ要件の低いデバイス所有者からはアクセスさせたくないという場面に対して有効である。認証フローとしては、本システムがいわゆる IdP プロキシとして動作することで保護リソースに対する認証を実行する（図 1）。

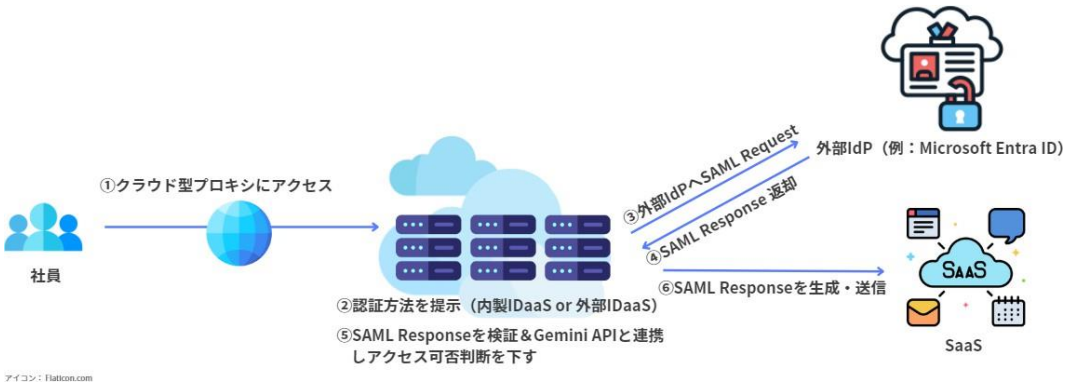

図 1：アクセス制御ポリシーシステム SaaS モードの概要図

トンネリングモードにおいては、社内システムへの安全なアクセスを実現するためのトンネリングサーバとエージェントソフトウェアを Rust 1.82.0 をベースにフルスクラッチで開発した。これらはファイアウォールや NAT 超えを同時に実現することで、導入の際にファイアウォールやルータの設定をする必要がなくなる。またユーザは VPN ソフトウェアをインストールすることなく、ブラウザから簡単にアクセスできる。認証フローは SaaS モードと同じであり、Gemini API と連携した日本語によるアクセス制御が利用できる。エージェントソフトは CLI コマンドとして実装しており、Rust のクロスコンパイルにより Windows の他、Linux および macOS 等の環境にも対応している。HTTP アプリケーションへのトンネリングを想定しており、独自ドメイン tunneling.me のサブドメインを各トンネルに割り当てることで、ドメインでアクセスできるようにした。加えて、会社等の独自ドメインを用いてアクセスしたいというケースに対応するため、ZeroSSL REST API と連携することで、アプリ内で SSL/TLS 証明書の発行認証から発行・適用までの処理を完結することに成功した。ドメインごとに証明書を発行し割り当てるため、サブドメインのサブドメインなど、ワイルドカードでは保護できない様々な独自ドメイン環境下において HTTPS 化を実現した（図 2）。

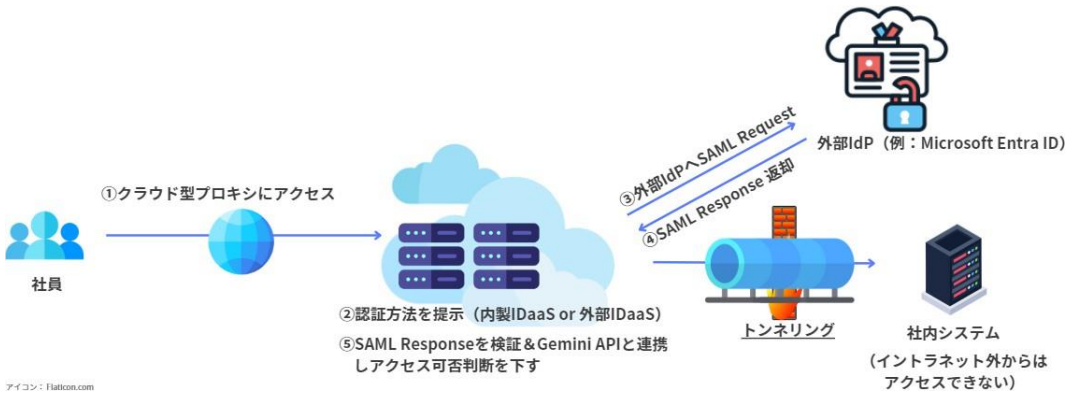

図 2：トンネリングモードにおけるトンネリングシステムの概要図

(3) インターネット制御監視システム

アクセス制御ポリシーシステムが情報資産の入り口側を保護するアプローチであったのに対し、インターネット制御監視システムはユーザ側からインターネット側へのアクセスをアクセス制御ポリシーにより制御する。インターネット制御監視システムも Rust 1.82.0 をベースに実装した（図 3）。ポリシーは必須条件と拒否条件を 1 つずつ設定することができ、日本語による自由記述が可能である。SOCKS5 プロトコルに対応しているため、デバイスのプロキシ設定に入力することで接続手続きが完了する。設定で「DNS もプロキシを利用する」を選択することで、アクセス先のドメイン名をポリシーの要素として利用することができる。具体的な利用例として、拒否条件に「アクセス先のドメイン名が deepseek.com であること」を設定すれば、いかなるユーザも deepseek.com にアクセスすることはできなくなる。情報漏えいの危険性があるウェブサイトや業務と関係のないウェブサイトにアクセスさせたくないというニーズに応える、ウェブフィルタリングの用途で利用することを想定している。

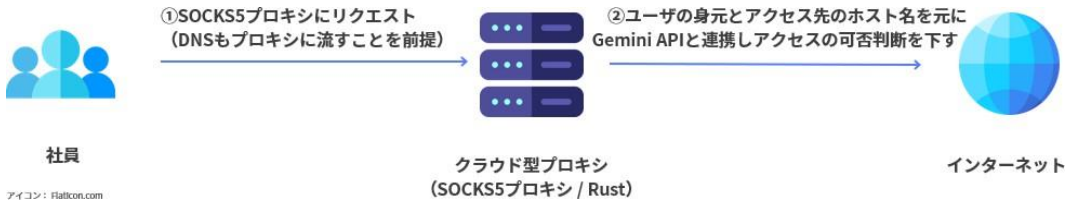

図 3：SOCKS5 プロキシの概要図

(4) アクセスログ総合管理システム

アクセスログ総合管理システムはアクセス制御ポリシーシステムから得られたアクセスログと、インターネット制御監視システムから得られたゲートウェイログを一元的に管理する。ログとして保管される情報は、アクセス先のアプリ名またはドメイン名（IP アドレス）、アクセス元のユーザ ID、アクセスの許可・不許可情報、その理由、アクセスした際に利用した認証方式情報、アクセス元の国名、発生日時である。許可・不許可となった理由については Gemini API によ

り生成される。またログを保管するだけでなく、収集したログをもとに、動的に新規アクセスが不審かどうかを判断する機能についても実装した。具体的には直近 10 件のアクセスログを随時呼び出し、新規アクセスが疑わしいかどうか Gemini API と連携して判断する。疑わしいと判断された場合は、アクセスが遮断され、当該ユーザに対してメールによる即時通告を行う。この即時通告では、検出したアクティビティの詳細情報のほか、アクティビティが疑わしいと判断された理由を Gemini API が生成し、合わせて通知する。この機能により、先述のシステムではカバーできていない、いわゆる出口対策についてもある程度有効であると考えられる。

10. プロジェクト評価

本プロジェクトでは、ゼロトラストアーキテクチャに必要な主要機能を備えたオールインワンのセキュリティシステムをフルスクラッチで開発し、既存の複雑なシステム導入作業の手間を大幅に削減した点が高く評価できる。特に、アクセス制御ポリシーを日本語で直感的に記述できる仕組みを導入したことは、ポリシー記述言語に不慣れなユーザにとって大きな利便性をもたらし、より多くの人がセキュリティシステムを利用できる環境の構築に貢献できると考えられる。また、システム全体がデジタル庁のゼロトラストアーキテクチャ適用方針に適合していることもあるため、日本国内における市場ニーズに対応した実装がなされている点も評価が高い。こうした成果の社会実装を通じて、将来的にはイントラネットや VPN 接続に依存しない、柔軟でセキュアなゼロトラストネットワーク環境の構築が日本中で行われることを期待したい。

11. 今後の課題

プロジェクト期間中に実際にユーザにシステム導入してもらい組織の中で使えるかどうか評価を行うことができなかった。今後は、本システムの実用性と信頼性の実証検証のために、バックボーンネットワークを整備し、実際にこのサービスを導入する組織に評価してもらうことが重要となる。現時点では、実際の業務環境への導入例がまだないため、通信事業者や NOC 運営者などと連携してフィールドテストを拡充する必要がある。また、オールインワン型のセキュリティシステムとしての機能を維持しながらも、ユーザの多様な利用ケースに対応できるよう、カスタマイズ性や拡張性をどう確保するかが課題である。加えて、開発が国産であることに価値を見出している一方、将来的には国際的な標準や他製品との連携を視野に入れた互換性の確保も検討する必要がある。Google Gemini API など一部海外のクラウドサービスに依存している部分もあるので、これらも国内のオンプレミス環境で運用できるような仕組みを整える必要がある。これらを踏まえた継続的な開発と、事業化に向けた実証実験の体制の整備が今後の課題となる。