KEEPER

JTP株式会社 | Case Study

AIエージェントを含む特権アクセス管理の刷新とエンドポイント特権管理の導入で

セキュリティ強化とクラウド運用サービスの効率向上を実現

JTP株式会社

https://www.jtp.co.jp/

設立：1987年10月31日

本社：東京都品川区北品川4-7-35 御殿山トラストタワー 14階

従業員：480名

事業内容：セキュリティ・生成AIの導入・運用、システムの構築・保守運用、医療機器の輸入販売・保守



JTP株式会社
システムコンサルティング事業部
執行役員 兼 事業部長
岡本 拓也 氏



JTP株式会社
システムコンサルティング事業部
クラウドソリューション部 部長
小林 知夏 氏

導入ソリューション

- パスワード管理
- 特権アクセス管理
- エンドポイント特権管理

クラウド運用サービス「Kyrios（キリオス）」を通じて、24時間365日体制で企業システムの運用・保守を支援するJTP株式会社。同社は、お客様の描く未来を実現可能にする「Enabler（イネイブラー）」を掲げ、セキュリティや生成AIの導入・運用をはじめ、幅広いITサービスを提供している。その運用現場では、顧客ごとに異なる環境や認証方式に対応するなか、認証情報、とりわけシステム管理者が利用する特権IDの管理が重要なテーマとなっていた。サイバー攻撃が高度化する現在、万一のリスクに備えながら、セキュリティと運用効率をさらに高める仕組みが求められていた。
JTPは、自社の運用基盤にKeeper Securityを導入。パスワード管理と特権アクセス管理を一元化するとともに、自ら運用で培った知見を、お客様への提案や導入支援にも生かしている。

導入前の課題

- ☑ 顧客ごとに異なる認証情報管理による運用負荷
- ☑ 特権ID管理の複雑化とセキュリティリスク
- ☑ エンドポイントにおける特権管理の強化
- ☑ AI時代を見据えた認証情報管理基盤の必要性

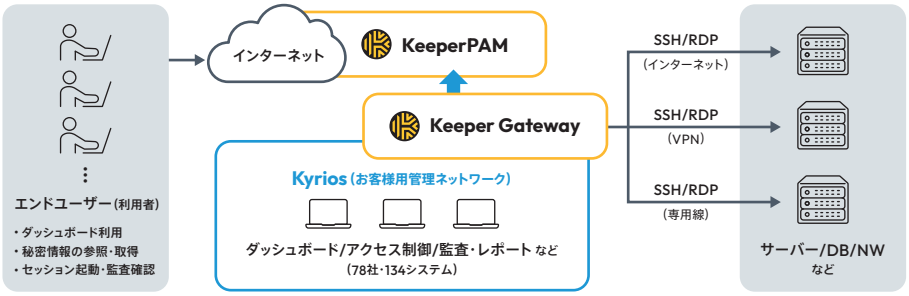
導入効果

- ☑ 140以上のシステムの特権IDを一元管理し、運用工数を大幅削減
- ☑ 顧客環境への変更なしに特権IDを管理できる「エージェントレス」構成
- ☑ アプリ単位のアクセス制御と権限昇格の最小化を見据えたEPM活用
- ☑ AIエージェントのNHI管理を見据えた認証情報管理基盤の整備

> ***AIエージェントが当たり前になる時代は、人だけではなくAIの認証情報まで管理しなければならない。だからこそ、認証情報管理の重要性はさらに高まると考えています。***

JTP株式会社 システムコンサルティング事業部 執行役員 兼 事業部長　岡本 拓也 氏

■ 利用構成図



運用サービスを支える現場で、認証情報管理をさらに高度化

JTP株式会社は、海外ITメーカーの国内展開を支えるアウトソーシング事業で培った技術力を基盤に、現在ではシステム構築から運用までを一貫して支援するソリューション事業を展開している。その中核となるサービスが、クラウド運用サービス「Kyrios」である。

Kyriosが目指しているのは、単にシステムを運用することではない。JTPが掲げる「Enabler（イネイブラー）」の考え方のもと、お客様が本来注力すべき業務に集中できる環境を整え、目指す姿の実現を支援することにある。そのため、運用設計や手順書なども積極的に共有し、お客様自身が将来、自走できる状態まで見据えた支援を行っている。

現在、Kyriosでは約70社・140システムを対象に、約50名の運用チームが24時間365日体制で監視・運用を提供している。マルチクラウドやハイブリッド環境が拡大するなか、お客様ごとに異なる認証方式やアクセスルールに対応しながら、安全な運用を継続することが求められる。なかでも管理者権限を持つ特権IDは、万一漏えいすれば重大なインシデントにつながるおそれがあるため、特に厳格な管理が求められる情報だ。JTPでは、将来のリスクにも備えながらセキュリティと運用品質をさらに高めるため、認証情報管理の高度化を進めることにした。

AI時代を見据えた認証情報管理基盤と、特権アクセス管理の導入しやすさが決め手

システムコンサルティング事業部 執行役員 兼 事業部長の岡本拓也氏は、「ランサムウェアなどの攻撃では、認証情報が侵入口になるケースが非常に多く、一つの特権IDが奪われるだけで組織全体へ被害が広がる可能性があります。だからこそ、人が利用する特権IDだけでなく、AIエージェントやマシンなどのNon-Human Identity（NHI）も含め、認証情報を適切に管理する仕組みが必要でした」と振り返る。

JTPでは生成AIやAIエージェントの導入支援にも取り組んでおり、人だけでなくAIエージェントやサービスアカウントなど、人以外の認証情報が急速に増えていく時代を見据えていた。「従業員一人が数十、あるいは数百のAIエージェントを利用するようになれば、人の認証情報だけでは管理しきれません。AIがどのシステムへ、どの権限でアクセスするのかまで含めた認証情報管理が必要になります」と岡本氏は語る。

数あるPAM製品の中でKeeper Securityを選んだ最大の理由は、顧客環境へ大きな変更を加えることなく、自社側で特権アクセスを安全に管理できることだった。パスワード管理と特権アクセス管理を単一のプラットフォームで実現できる点も、運用代行サービスを提供する同社のニーズと合致し、将来を見据えた認証情報管理基盤として採用を決定した。

段階的な導入と一元管理で、安全性と運用効率を向上

導入時に最も時間を要したのは、認証情報の整理だった。「誰が、どのシステムに、どの権限でアクセスしているのかを一つずつ洗い出しました。他社の特権アクセス管理製品と異なり、Keeperはアクセスするユーザーを起点に整理できるため、段階的に導入を進めやすかったですね」とシステムコンサルティング事業部 クラウドソリューション部 部長の小林知夏氏は振り返る。

現在では、運用担当者はKeeper Vaultから必要なシステムへ1クリックで安全にアクセスでき、認証情報を意識することなく作業を行えるようになった。セッション単位で証跡が残るため、監査対応や運用状況の把握も容易になり、運用品質の向上と管理負荷の軽減につながっている。

さらに、お客様先やJTP社内に設置するKeeper Gatewayでは、エンドポイント特権管理（EPM）の活用も進めている。アプリケーション単位でのアクセス制御や、必要に応じた管理者権限の一時的な付与など、権限昇格を最小限に抑える運用を検討している。

今後は、EPMのより詳細な設計・設定を進めることで、必要最小限のアクセス権限のみを付与する運用を目指し、さらなるセキュリティ強化につなげていく考えだ。



JTP株式会社
マネージド&セキュリティサービス事業部
執行役員 兼 事業部長
小林 智文 氏

お客様の挑戦を支えるEnablerとして、自社で培った知見を生かし、導入から運用までをご支援します。

私たちは、Keeper Securityを販売する前に、自社で導入し、実際の運用で活用しています。
導入時にどのような準備が必要なのか、どこでつまずきやすいのか、運用をどう定着させればよいのか。実際に経験しているからこそ、お客様にも具体的なノウハウをご提供できます。
製品をご提案するだけではなく、導入後の運用まで見据えて伴走することが私たちの役割です。これからも、自ら実践して得た知見をお客様へ還元し、安心してKeeper Securityをご活用いただける環境づくりを支援していきたいと考えています。

Keeper Security APAC株式会社
〒105-0001 東京都港区虎ノ門4-1-13 プライムテラス神谷町4F
https://www.keepersecurity.com/ja_JP/

●お問い合わせ
JTP株式会社
東京都品川区北品川4-7-35 御殿山トラストタワー14F
TEL：03-6408-2488
https://solution.jtp.co.jp/contact