

ケーススタディ

アトラシアン・ウィリアムズF1チーム、開発拠点から
レース現場まで機密データを保護

背景

アトラシアン・ウィリアムズF1チームは、1977年にサー・フランク・ウィリアムズとパトリック・ヘッドによって創設された、F1屈指の名門チームです。英国オックスフォードシャー州グローブを拠点とし、コンストラクターズチャンピオンシップ9回、ドライバーズチャンピオンシップ7回の優勝を誇るなど、F1史上屈指の実績を築いてきました。優れたエンジニアリングと挑戦し続ける姿勢で知られる同チームは、急速に進化するモータースポーツの世界で競争力を維持するため、最先端のテクノロジーとデータ分析を活用し、イノベーションとパフォーマンスを追求しています。

業種
モータースポーツ

従業員数
1000人以上

ソリューション
keeper 企業向け
パスワードマネージャー

課題

F1は世界で最もデータ集約型のスポーツの一つであり、サイバー攻撃の格好の標的となっています。アトラシアン・ウィリアムズF1チームでは、レースウィークごとに1TBを超える車両データや空力データ、シミュレーションデータを生成しています。各マシンには400を超えるセンサーが搭載され、3万ものデータチャンネルから収集された情報が、サーキットのエンジニアと英国グローブの本拠地ヘリアルタイムで同時に送信されます。こうしたデータへのアクセスを保護する認証情報は、データそのものと同等の戦略的価値を持っています。

「F1はチームスポーツです。チーム全員が同じ目標に向かって連携しなければ、何も成り立ちません。だからこそ、セキュリティが障害になってはならないのです。必要な人が、必要なときに、必要なものへアクセスできることが重要です。」

クリス・ヒックス | アトラシアン・ウィリアムズF1チーム
シニア情報セキュリティエンジニア

組織全体では約1,200人が働いており、風洞施設からレース現場まで、それぞれが役割に応じた適切なアクセス権限を必要としています。また、シーズン中は20か国以上を転戦するため、こうしたアクセスを適切に管理することが不可欠です。一方で、F1には各チームの年間支出を制限するコストキャップ制度があり、人件費、設備投資、運営費を含むあらゆる支出が厳しく管理されています。そのため、セキュリティへの投資は、マシンの性能向上に直結する開発投資とのバランスを慎重に見極めながら判断する必要があります。

「セキュリティツールを導入するか、それとも新しいフロントウイングや新たなメカニカルエンジニアに投資するか。本当にそうした比較検討をしています。だからこそ、ツールを提案する際には、その価値を明確に示さなければなりません。」

クリス・ヒックス | アトラシアン・ウィリアムズF1チーム
シニア情報セキュリティエンジニア

Keeperのソリューション

アトラシアン・ウィリアムズF1チームは、Keeperの企業向けパスワードマネージャーとBreachWatch®を導入し、認証情報管理を一元化しました。その中核となるのは、あらゆるチームや部門で安全なコラボレーションを実現することと、現在および将来の脅威に対応する業界最高水準の暗号化を提供することの2つです。

スピードを支える安全な情報共有

Keeperの共有フォルダとロールベースの権限管理により、業務に必要な認証情報のみを各担当者へ自動的に付与できます。また、ワンタイム共有を利用すれば、請負業者やサードパーティにも有効期限付きのアクセスを提供でき、有効期限が切れると自動的にアクセスが無効化されるため、手動で管理する必要はありません。Keeperは管理対象のあらゆるブラウザ、デバイス、オペレーティングシステムに対応しており、必要な認証情報へ、必要なときに、必要な場所からアクセスできます。サーキットで活動するチームからマーケティングチームまで、あらゆるユーザーの業務を円滑にします。

「認証情報はすべてKeeper内で生成され、対象サイトを自動で認識して瞬時に自動入力されます。」

ジェームズ・イエクスリー | アトラシアン・ウィリアムズF1チーム ソーシャルメディアエグゼクティブ

重要データを守る高度な暗号化

Keeperの**ゼロ知識・ゼロトラストアーキテクチャ**では、暗号鍵はクライアント側で生成され、Keeperのサーバーには保存されません。楕円曲線暗号方式、**AES 256ビット暗号化**、PBKDF2をボルト、フォルダ、レコードの各階層で組み合わせ、すべてのシステムで多要素認証 (MFA) と生体認証を実施しています。

「暗号化されたデータを解読するには、サイバー犯罪者でも2,000年以上かかります。暗号鍵はアトラシアン・ウィリアムズF1チーム側のクライアントで生成されます。Keeperが保存するのは、0と1のデータだけです。」

ダレン・グッチョーネ | Keeper Security CEO兼共同創業者

Keeperはさらに、**Kyberアルゴリズム**による耐量子計算機暗号を採用し、「Harvest Now, Decrypt Later (今収集して後で解読する)」攻撃への対策も講じています。これは、量子コンピューターの実用化を見越して、攻撃者が現在の暗号化データを保存し、将来解読を試みる脅威に対応するものです。

「F1では、常に次の規則改定を見据えて行動する必要があります。これから訪れる脅威から私たちをどう守るかを見据え、Keeperも同じ考え方で将来を見据えた取り組みを進めていることを心強く感じています。」

クリス・ヒックス | アトラシアン・ウィリアムズF1チーム
シニア情報セキュリティエンジニア



組織への影響

Keeperにより、ウィリアムズの各チームは必要な認証情報へすぐにセルフサービスでアクセスできるようになり、ITサポートの負担が軽減され、より価値の高い業務に注力できるようになりました。さらに、プロビジョニングとプロビジョニング解除が自動化されたことで、ITチームは日常的なアクセス要求への対応に費やす時間を減らし、チームの競争力向上につながる重要な技術課題により多くの時間を割けるようになりました。

「各チームがKeeperを使い始めると、サービスデスクに問い合わせる必要がなくなり、自分たちで必要なことに対応できるようになります。その結果、サポートチームはマシンの性能向上に直結する、より重要な業務に集中できるようになります。」

クリス・ヒックス | アトラシアン・ウィリアムズF1チーム
シニア情報セキュリティエンジニア

レース現場を支えるセキュリティ

レース現場では、インフラを迅速にセットアップできることで、データ分析やレース戦略により多くの時間を割けるようになります。まさに、こうしたわずかな積み重ねが勝敗を左右します。サーキットに到着したエンジニアは、必要な認証情報にすぐアクセスできるため、自信を持ってシステムを迅速に立ち上げることができます。

「サーキットでインフラの立ち上げが早く終われば、その分の時間をエンジニアはレース戦略の立案やデータ分析に充てられます。レースウィークでは、そうしたほんのわずかな時間の差が大きな違いを生み出すのです。」

クリス・ヒックス | アトラシアン・ウィリアムズF1チーム
シニア情報セキュリティエンジニア



世界中で変わらない安心のセキュリティ

グローブの本拠地でも、世界各地のサーキットでも、一貫したポリシー準拠のアクセスを、あらゆる国、ネットワーク、デバイスで実現できます。さらに、BreachWatchによるダークウェブの継続的な監視と、ゼロ知識暗号化によるすべての認証情報の保護により、ウィリアムズは妥協することなく戦い続けるための強固なセキュリティ基盤を確立しています。

「認証情報管理は、もはや改善が必要な領域ではありません。」

クリス・ヒックス | アトラシアン・ウィリアムズF1チーム
シニア情報セキュリティエンジニア

すべてのチームを支える強固なセキュリティ基盤

Keeperがもたらした効果は、IT部門だけにとどまりません。ウィリアムズでは、ゲストエクスペリエンス、ソーシャルメディア、出張管理、コストエンジニアリングなど、さまざまな部門の担当者が共通して、その価値を実感しています。それは、日々利用するあらゆる認証情報を、安全かつ一元的に管理できる環境です。セキュリティは、業務を妨げるものではなく、意識することなく安心して使えるものへと変わりました。

「F1では、セキュリティが極めて重要です。私たちは多くのお客様のデータを扱っているため、それらを一元管理し、Keeperによって安全に保護したいと考えています。」

トム・アイバーソン | アトラシアン・ウィリアムズF1チーム
シニアHQゲストエクスペリエンスマネージャー



KeeperPAM

多くの企業では、従業員のパスワード管理の実態を十分に把握できておらず、そのことがサイバーリスクを大きく高めています。パスワードの利用状況やポリシー遵守状況を把握しなければ、サイバー衛生を改善することはできません。Keeperは、優れたセキュリティ、可視化、管理機能を提供することで、この課題を解決します。

データは、Keeperのゼロ知識セキュリティアーキテクチャと世界最高水準の耐量子計算機暗号によって保護されています。ゼロ知識とは、マスターパスワードおよび情報の暗号化・復号に使用される暗号鍵を知り、アクセスできるのはユーザー本人だけであることを意味します。

Keeperは、企業規模を問わず直感的に操作でき、容易に導入できます。Active DirectoryやLDAPサーバーとの連携により、プロビジョニングやオンボーディングを効率化します。さらに、**SSOコネク**®は既存のSSOソリューションと連携し、FedRAMP High認証およびGovRAMP High認可を取得しています。

Keeperは、あらゆる規模の組織に対応できるよう設計されています。ロールベースの権限管理、チーム共有、部門別の監査、委任管理といった機能により、組織の成長を継続的に支援します。**Keeperコマンダー**は、既存システムおよび将来的なシステム連携を可能にする強力なAPIを備えています。

KeeperPAMのビジネス活用事例

- 認証情報に起因するデータ侵害やサイバー攻撃を防止
- パスキーに対応し、スムーズな認証を実現
- コンプライアンスの強化
- 従業員の生産性向上
- パスワードポリシーと運用ルールの徹底
- ヘルプデスクのコストを削減
- 短期間でセキュリティを確保し、トレーニングの手間を最小限に抑える
- 従業員のセキュリティ意識と行動を向上させる

Keeperについて

Keeper Securityは、150以上の国で幅広い企業や利用者を守る、急成長中のサイバーセキュリティソフトウェア企業です。ゼロ知識とゼロトラストを基盤とし、あらゆるIT環境に対応できるセキュリティの先駆けとして知られています。主力製品のKeeperPAM®は、AIを搭載したクラウドネイティブのプラットフォームであり、ユーザーやデバイス、インフラを包括的にサイバー攻撃から保護します。特権アクセス管理 (PAM) の分野では、ガートナー社の「Magic Quadrant (マジック・クアドラント)」において革新性が高く評価されました。Keeperではロールベースのポリシー、最小権限、ジャストインタイムアクセスを組み合わせることで、パスワードやパスキー、インフラのシークレット、リモート接続、エンドポイントを安全に管理しています。

Keeperは、世界各地の企業や利用者から高い信頼を得ています。

Gartner

Keeper Security®は2026年、世界で2番目に急成長しているセキュリティソフトウェア企業として評価されました



Cybersecurity Stars Awards 2026

AIセキュリティ・イノベーター・オブ・ザ・イヤー、企業向け
最優秀特権アクセス管理プラットフォーム



Cybersecurity Excellence Awards

特権アクセス管理



Global InfoSec Awards

AI搭載サイバーセキュリティソリューション、サイバーセキュリティ企業、特権アクセス管理 (PAM)



Globe Awards 2026

サイバーセキュリティ部門シルバー受賞