Okta 導入支援サービス EIAM（企業向け ID 認証）事例

株式会社タイミー 様

急成長に伴い社員数が5年で32倍に増えたタイミー、Oktaの導入でゼロトラストを加速

タイミー社は、「一人ひとりの時間を豊かに」というビジョンのもと、「『はたらく』を通じて人生の可能性を広げるインフラをつくる」をミッションに掲げ、有料職業紹介事業として「働きたい時間」と「働いてほしい時間」をマッチングするスキマバイトサービス「タイミー」を全国へ展開している。スマホアプリ上で申し込み・勤怠・報酬確定までを一気通貫で完結させ、最短即日で働ける体験を実現している。こうしたスピードと手軽さを武器に、タイミーはスキマバイト市場を切り拓いたパイオニアとして、圧倒的なユーザー数を誇る。

今回は、タイミーが Okta を導入した背景や詳細について、同社の情報システム部 コーポレート IT G マネージャーである小池 光亮氏に話を伺った。

株式会社タイミー
情報システム部 コーポレート IT G
マネージャー
小池 光亮氏

急成長で顕在化した ID 管理の課題

急成長する中で、タイミーでは大きな課題が顕在化していた。スピードを武器に事業を拡大する一方で、管理の仕組みが追いつかなくなり始めていたのである。

「2019 年には 38 名だった社員数が、2024 年には 1,224 名になっていました。実に 5 年で 32 倍になったわけです。そこで問題になったのが ID の管理でした。」

こう語る小池氏は、タイミー全社のシステム基盤や、社員が使う端末や SaaS の管理、監視を業務としており、セキュリティ製品などの選定や提案も行っている。

「当時はベンチャー企業として急成長しており、毎月数十人という単位で社員が増えていました。そのため、アカウントの発行・権限付与・棚卸しといった運用が急速に複雑化していきました。」

タイミーは創業当時からオンプレミスのサーバーを社内に持たず、全てのシステムを SaaS で管理している。同社にとって、ID は業務そのものを支える存在とも言える。その管理が揺らげば、利便性だけでなくセキュリティにも直結するリスクとなる。

「セキュリティインシデントが増加する中で、従来の VPN などによる境界防御に限界を感じていました。どこからアクセスしても安全であることを前提にするのではなく、ユーザーやデバイス単位で信頼性を検証する、ゼロトラストでの防御にシフトしていくことになりました。」

ゼロトラスト構築の最優先事項は IdP 導入

ゼロトラストの体制を構築するにあたり、最優先となったのが ID 管理だ。タイミーでは、その中核を担う仕組みとして Identity Provider（以下、IdP）を導入することになった。以前より、社員の端末管理に MDM や、エンドポイントセキュリティ対策として EDR を導入していたが、急速な組織拡大の中で運用が追いつかず、リスクになりかねない状態だった。IdP の導入は、認証基盤を再設計し、分散した管理を一元化するための打ち手でもあった。

IdP を選定する際の要件については、現実の運用に耐えうるかが重視された。

「まず、SaaS と接続ができること。そして、導入・構築後も自分たちで管理できるよう、リファレンスが充実していること。加えて、生体認証などのシームレスな認証機能を持っていることを求めました。」と小池氏は語る。

生体認証を希望した背景は、社員が端末などに ID/ パスワードを打つという行為をなくし、利便性とセキュリティを同時に引き上げたいという狙いがあった。

さらに、同社特有の要件もあった。オンプレミスを持たない構成ゆえに、自社で証明書を発行・管理することができない。そのため、「IdP 側で認証局を持っていること」も不可欠な条件だったという。こうした要件をもとに複数のベンダーを比較・検証した結果、すべてを満たしたのは Okta のみだった。

ラックの選定理由と導入の難所

そこで Okta 社に導入支援が可能なベンダーについて相談し、候補となる数社を紹介された。選定にあたって重視したのは、有事を前提にした対応力だ。ゼロトラストを導入しても、セキュリティインシデントは起こり得るという前提に立ち、セキュリティベンダーであることを最優先条件とした。加えて、日本企業であることも重要な要件だった。

「そうした条件で絞るとラックが残りました。実は私、前職でのつながりもあり、ラックの知見や技術力を肌で感じていたので、一番信頼がおける企業としてお願いしました。これは運命ですね、きっと。」

導入はコーポレート IT の中でのプロジェクトとして進められ、小池氏がリーダーを務めた。選定はスムーズだったものの、導入では設計と配布の 2 つの段階で苦労があったという。

まず設計では、何をデータのマスターにするのかという問題があった。創業からの急成長により、データは複数システムに分散し、完全なマスターが存在しない状態だった。人事労務的なデータをそのまま流用できず、断片的な情報を突き合わせながら統合していく必要があったという。さらに、権限設計やグルーピングも一筋縄ではいかず、ラックの助言を受けながら何度も見直しを重ねた。この設計フェーズが、結果として最も時間を要した。

配布の段階では、2 つの課題があった。1 つは、Okta では MDM を活用して証明書を配布するが、配布対象となるサービスの整理が不十分で、事前の統制から手を付ける必要があった。そしてもう 1 つはシステムの浸透だった。「配布するので対応をお願いします」と周知しても、約 30 名が対応しないまま残った。「理由を聞くと、やり方が分からないのではなく、自分が対象だと思っていなかったというケースでした。最後の敵は急激な組織拡大ゆえのコミュニケーションの難しさ = 当事者意識の醸成でした。」

最終的に未対応者に対し、セキュリティ品質を一律に担保するためやむなくシステムへのアクセス一時停止をするなど、毅然としたガバナンス対応を実施し完了させた。技術的な課題だけでなく、人の行動や認識も含めて乗り越えて導入は完了したが、スケジュールは当初想定より約 1 か月の遅延となった。

導入効果とゼロトラスト運用への手応え

導入後約 1 年が経過しているが、運用は引き続きコーポレート IT グループが担当している。

小池氏は、「基本基盤の 9 割は完了し、現在はより高度な統制に向けた次のフェーズへ移行している状態ですね。」と振り返る。現在は運用開始後に加わったグループ会社への展開も検討中だ。単体導入から、組織全体への統制へとスコープが広がりつつある。

導入後の効果として最も大きかったのは、「IdP があることを社内に宣言できたこと。そして社員がそれを認識して動いてくれるようになったこと」だという。また、SSO の実現や、グルーピングの効率化といった機能面のメリットもあるが、一方で既存 ID との差分吸収など、運用の手間が劇的に減ったわけではないという現実もある。

ユーザー側の体験も変わった。生体認証に対応したことで指紋や顔でログインできるようになり、日常的なストレスが軽減された。一方で、パスワードを覚える必要がなくなったことで、生体認証ができなかったときの復旧は難しくなった。ただし、端末認証や SASE 製品と組み合わせることで、社用端末以外からのアクセスを遮断できており、この点については「安心感がまったく違う」と小池氏は強調する。

また、エンジニアから SSO などの活用に関する相談が増えたことも、副次的な効果だった。個別に散在していた認証や管理の課題が、IdP を軸に統制できるようになり、部門をまたいだコミュニケーションが生まれている。「結果として、管理と開発の間にシナジーが生まれたと感じています。」

運用する上で必要な機能に大きな不足はないものの、今後の拡張としては EDR に加え、SASE との連携に期待を寄せる。デバイスの状態に応じてアクセスを制御する仕組みに、ネットワーク側の要件も組み込めれば、ゼロトラストの実効性はさらに高まるという見立てだ。

一方で、導入時にお試しで組み込んだワークフロー機能は、今になって活用が進んでいる。「結果的に非常に助かっています。」と小池氏は評価する。また可用性の高さも大きな安心材料だ。日常的な問い合わせはあるものの、基盤そのものが止まることはなく、認証基盤としての信頼性は高い水準で維持されている。ゼロトラストの中核を担うプラットフォームとして、安定性は運用の質を大きく左右する。

伴走支援で定着させるゼロトラスト、次は検知と対応へ

ラックの支援について小池氏は、「権限設計の初期フェーズでは試行錯誤がありましたが、それ以外は非常にスムーズでした。」と振り返る。テスト工程の伴走や、保守フェーズにおける Okta 社との定例会議への同席など、導入後も継続的な支援が提供されている点を評価する。「サポート窓口は Okta 社とラックの双方にありますが、リファレンスが充実しているため、多くは社内で自己解決できています。」外部ベンダーに依存しすぎない運用が実現できている点も、大きな安心材料となっている。

ゼロトラスト基盤の導入を振り返り、小池氏は今回の取り組みの意義をこう語る。「セキュリティを強固にするだけでなく、生体認証によって社員の日常のわずらわしさを無くすことができました。これこそが自社が掲げる『一人ひとりの時間を豊かに』というビジョンを、コーポレート IT の側面から体現した形だと考えています。」

今後は、ワークフロー活用による運用効率化や、グループ会社への統制拡大を推進していく構えだ。「今が完成形とは思っていません。より安心・安全な環境を目指し、継続的にブラッシュアップしていきます。」と小池氏は語る。

この先のロードマップの 1 つにセキュリティ監視・対応体制のさらなる高度化がある。同社では現在もプロダクトとコーポレートのセキュリティチームが連動し、日々の検知・インシデント対応体制を稼働させている。今後は事業の急成長や脅威の高度化を見据え、SIEM の導入などを通じて、この監視体制をより高度で専門的な SOC へと機能強化していく方針だ。「現状の監視・対応体制から更に一段上のフェーズへ引き上げるため、内製化の範囲や既存チームとの役割分担も含めて、最適な SOC 体制の設計を進めているところです。」と語る小池氏。

Okta によって安全かつ利便性の高い認証基盤を整えた同社は、今後も予防だけでなく検知・対応力まで含めたセキュリティの実効性を高め、「はたらく」を支えるインフラの安定的な成長を支えていく考えだ。

［お問い合わせ］
株式会社ラック
サービス紹介ページ　https://www.lac.co.jp/solution_product/okta_eiam.html