

Microsoft 365をはじめとするSaaS向け認証基盤をIP3-ACEで構築 「いつでもどこでもどんなデバイスからでも、安全に使える環境づくり」に成功

株式会社 イシダ様



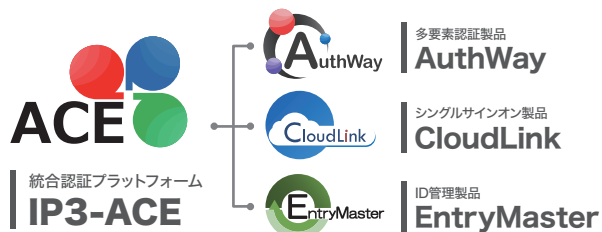
PROFILE

先進の計量技術を核に、包装・検査・情報などへ事業領域を拡げ、世界100カ国以上で「食の安全・安心」を支える自動省力化メーカー。

近年では、京都と滋賀にまたがる如意ヶ嶽にイシダグループが保有する森林を「イシダの森」として整備し、環境保全や自然体験を通じた次世代育成などのCSRに取り組んでいる。

●本社：京都府京都市左京区聖護院山王町44

●滋賀事業所：滋賀県栗東市下鈞959-1



株式会社イシダは、Microsoft 365の全社導入を契機に、SaaS向けの新しい認証のしくみが不可欠であると判断。シングルサインオン、電子証明書認証、ワンタイムパスワード認証を組み合わせた認証基盤を構築して、2019年7月からグループ全体約3800人で利用しています。

課題

Microsoft 365を全社導入するために、セキュリティ、利便性、グローバル対応、コスト、安定性などの要件を満たす新しい認証基盤が必要だった

効果

SSO、MFAを実現する「IP3-ACE」を導入。Active Directoryと認証基盤との二重メンテが不要で、運用管理の手間がきわめて少ないSaaS向け認証基盤を構築できた

SaaSを安全かつ便利に利用するために認証基盤を構築

株式会社イシダ（以下、イシダ）は、国内初の民間ハカリメーカーとして1893年に創業。創業から現在に至るまで、時代の変化に対応して数々の計量機器を開発し産業・経済を支えてきました。同社は1972年、世界初となる独自の『組み合わせ計量』技術を使った「コンピュータスケール」の開発に成功し、定量自動計量を実現。これまで不可能だった重さや形状がばらばらのものを高速で同じ重さに計量するシステムは、世界の食品工場に革命をもたらしました。イシダはこのコア技術に加え、包装や検査など常に新技術の開発にチャレンジし、食品から物流、小売りなど幅広い分野の自動省力化に貢献しています。

同社が、Microsoft Officeのサブスクリプションサービス「Microsoft 365」（旧Office 365）の全社導入を決めたのは2018年のことです。

「初めてのSaaS大規模利用に際し、認証をどうするかが課題となりました」と、株式会社イシダ 滋賀事業所 情報システム部 情報セキュリティ・ITインフラ課 課長の岡田雅之氏は語ります。

インターネット上では不特定多数がアクセス可能であり、ID/パスワードだけでは悪意のある攻撃を受ける可能性があります。一方で、オンプレミスからクラウドへの移行は大きな潮流であり、イシダのSaaS利用も拡大が避けられません。

株式会社イシダ
滋賀事業所
情報システム部
情報セキュリティ・ITインフラ課
課長
岡田 雅之 氏



「認証基盤は日々の業務を支える重要な『ビジネス・インフラ』です。セキュリティと利便性を兼ね備えた認証基盤の構築は、情報セキュリティ戦略から見ても極めて重要であると考えています。」

「Microsoft 365を安心して使えるよう、さらにSAML連携によりSaaSの利用範囲を広げられるよう、Active Directoryを含めた新たな認証基盤を構築することにしました」（岡田氏）。

電子証明書とワンタイムパスワードによる2種類の多要素認証を併用

「当社が認証基盤/ID管理で重視したのは、『いつでも、どこでも、どんなデバイスからでも認証が可能であること』です。さらに、セキュリティ、利便性、多言語対応、コスト、安定性といった様々な観点から、認証基盤のあり方を検討しました」（岡田氏）。

セキュリティと利便性の両立には、多要素認証（MFA）とシングルサインオン（SSO）が不可欠でした。しかし多要素認証の実現方法は、イシダ本体とグループ会社で変えることにしました。

「イシダ本体の約3,000人には、会社支給のPCから

の利用に限定し、電子証明書による厳重な本人確認を行う方式としました。利用者は従来どおりIDとパスワードを入力するだけで、電子証明書の照合が自動で行われ、多要素認証が成立するしくみです」（岡田氏）。

一方、グループ会社の国内外約800人には、ネットワーク環境が常時接続されているわけではないため、電子証明書を確実に配布・管理するのが困難です。そこでワンタイムパスワード（OTP）のソフトウェアトークンによる多要素認証を採用しました。

そして異なる多要素認証方式の両方に対応できる製品として、アイピーキューブの「IP3-ACE」を選定しました。

IP3-ACEは、多要素認証システム「AuthWay」、シングルサインオンシステム「CloudLink」、ID統合管理システム「EntryMaster」の3製品を組み合わせた統合認証基盤ソリューションです。電子証明書とOTPの両方による多要素認証に対応し、SAML連携したクラウドサービスに対してスムーズなシングルサインオンを実現します。

製品導入事例 株式会社イシダ様

イシダではMicrosoft製品で全てを実装することも検討しましたが、必要となるサーバー台数が多く、運用管理の手間が膨大になりそうだったので断念。IP3-ACEなら1台のサーバーに搭載でき、冗長化しても2台で済みます。Linuxサーバーならアップデートも自動処理され、運用管理の手間がほとんどかかりません。

また、IP3-ACEはユーザー数に応じた価格設定ではなく、大規模システム向けのスペシャルプライスが適用されたため、コストパフォーマンスに優れていました。「大規模ユーザー向けの価格設定は大変助かりました」(岡田氏)。

株式会社イシダ
滋賀事業所
情報システム部
情報セキュリティ・ITインフラ課
池田 大智 氏



「Active DirectoryとEntryMasterの自動連携は非常に便利です。人事からCSVファイルをもってEntryMasterに投入し、Active Directoryも自動同期されるという使い方にチャレンジしたいと思います。」

Active Directoryとの連携で、IDデータの二重メンテナンスが不要に

イシダのSaaS向け認証基盤は、約半年の構築期間を経て、2019年7月に本番稼働を開始しました。新規に構築したActive Directoryは、認証基盤のEntryMasterとデータ連携します。Active DirectoryでIDデータの追加や削除を行えば、データ変更が自動検知されEntryMasterに反映され同期が維持されます。Active Directoryと認証基盤の二重メンテナンスは不要になりました。イシダ本体で使う電子証明書については、セキュリティを最優先に、厳重な

管理体制を整備しています。「デバイスへの電子証明書の配布と運用ルールづくりでは、試行錯誤の末、1台ずつ確認する作業を行う時期もありました」と、情報セキュリティ・ITインフラ課の池田大智氏は振り返ります。一方、グループ会社では一定期間ごとにパスワード変更を義務付け、変更がない場合は自動的に無効化することにしました。利用者がEntryMasterでパスワード変更を行うと、変更データはActive Directoryへ

自動的に同期されます。パスワード変更を促すメールも、EntryMasterの機能で自動配信しています。また、グループ会社にはユーザーID数に応じて課金し、実費を請求しています。「課金することで、不要なIDが放置されずにグループ会社が精査してくれる効果もあります」(岡田氏)。IDの棚卸しとグループ会社別のユーザーID数のレポート作成・送信は、EntryMasterに機能を追加して自動化しました。

稼働から約5年、認証基盤に関するセキュリティインシデントは発生していない

2019年の稼働開始から5年近く経ちますが、クラウドサービスの認証に関するセキュリティインシデントは発生していません。IP3-ACEも安定稼働を維持し、業務をストップさせたことはありません。イシダ本体では、従来と同様のID/パスワード入力操作だけで多要素認証ができる、利便性の高い認証基盤を構築できました。「ほぼメンテナンスフリーと言えるほど、本当に手間がかかりません。IDaaSとは違ってオンプレミス運用ですが、Linuxサーバーは自動でセキュリティ更新を適用してくれるので、自社運用の負担を感じることはありません」(池田氏)。「一般的なIDaaSと比べて、コストパフォーマンスが非

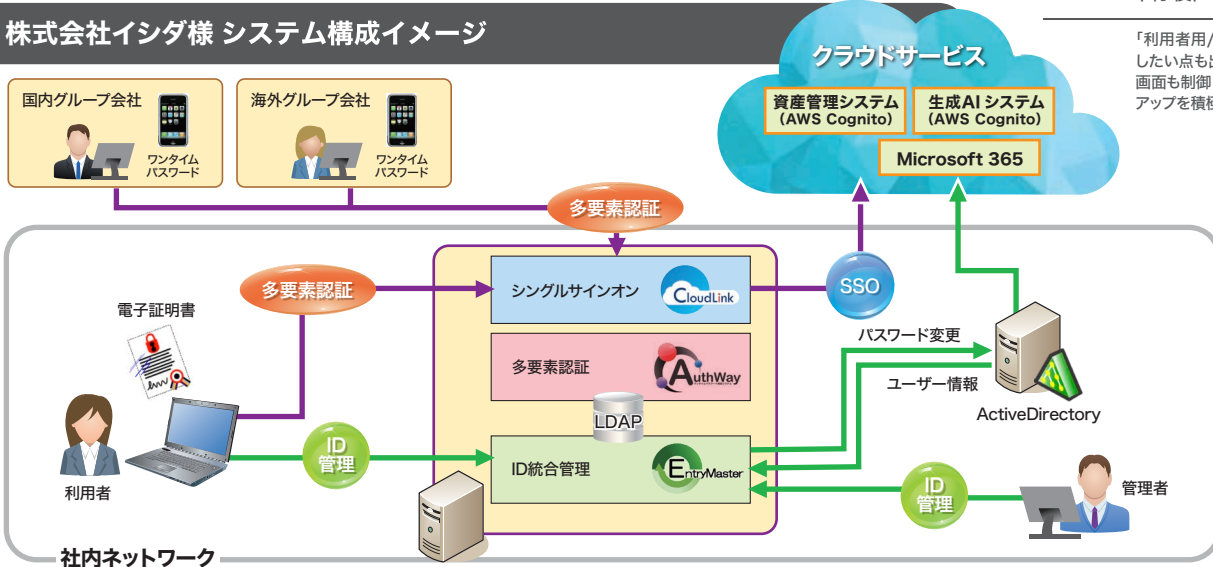
常に優れていることを5年が経って実感しています」と語るのは、情報セキュリティ・ITインフラ課の中村俊仁氏です。オプションやサポート費用を含めてIDaaSと比較した結果、5年間で5,000万円以上のコスト削減効果があったそうです。5年前の選択が正しかったことが証明されました。アイピーキューブの迅速なサポート体制にも満足しているとのこと。 「認証基盤に関する問題や新たな要求があれば、まずアイピーキューブに連絡すれば、ワンストップで迅速な対応を受けられます。特に、他システムのバージョンアップに伴うセキュリティ対策では、的確なアドバイス

を受けたことが印象に残っています」(岡田氏)。次の課題としては、グループ会社の多要素認証手段としてパスワードレス認証の導入も検討中。「いつでも、どこでも、どんなデバイスからでも、安全にアクセスできる認証基盤」は、今後も進化を重ね、イシダグループ全体の情報セキュリティレベル向上を支えていくことでしよう。

株式会社イシダ
滋賀事業所
情報システム部
情報セキュリティ・ITインフラ課
中村 俊仁 氏



株式会社イシダ様 システム構成イメージ



「利用者用/管理者用画面で、ブラッシュアップしたい点も出てきました。IP3-ACE最新版では画面も制御しやすくなるそうなので、バージョンアップを積極的に行いたいと考えています。」

※本製品には、OpenSSL Toolkitで使用するためにOpenSSL Projectによって開発されたソフトウェアが含まれています。(http://www.openssl.org/)