Cisco Secure Access by Duo 導入事例

株式会社 CAMPFIRE

信頼性を高める包括的なセキュリティ強化の皮切りとして全社に多要素認証（MFA）を展開

製品 & サービス

- Cisco Secure Access by Duo

課題

- IT ベンチャーとしてのスピード感と金融事業提供企業としての信頼性を共存すべく、包括的なセキュリティ強化を検討
- クラウドシフトやリモートワーク拡大などの変化に伴い、従前のセキュリティ対策では不安
- 会社が管理していないクラウドサービスやデバイスの利用は、大きなインシデントにつながる

ソリューション

- 社員 140 名、約 200 台の社給 PC とスマートフォンを対象に多要素認証とデバイスヘルスチェック機能としての利用を開始
- Push 通知やモバイルパスコードなど複数の方式を提供、ユーザビリティも直感的でわかりやすい
- 展開後はトラブルもなく、順調に利用中

結果～今後

- ID とパスワード依存から脱却し、確実に安全性が高まった実感
- Cisco Umbrella も活用し、適切なクラウド利活用を促したい
- 最終的には Cisco SecureX による自動化と統合管理を目指す

「資金集めを民主化し、世界中の誰しもが声をあげられる世の中をつくる」のスローガンを掲げ、国内最大※の購入型クラウドファンディング「CAMPFIRE」をはじめ、融資型、株式投資型など多彩なクラウドファンディング事業で急成長を続ける株式会社 CAMPFIRE。同社は IT ベンチャーとしてのスピード感と金融事業提供企業としての信頼性を共存すべく、包括的なセキュリティ強化の皮切りとして今回、Cisco Secure Access by Duo を導入。ゼロトラストの考え方に基づく多要素認証（MFA）により安心、安全なテレワーク環境整備を進めています。

SecureX による統合的なセキュリティを目指し、最初のステップとして Cisco Secure Access by Duo による多要素認証を導入しました。

―― 株式会社 CAMPFIRE 情報セキュリティチーム マネージャー 木下 氏

国内最速で流通総額 440 億円突破、延べ支援者数 510 万人、プロジェクト掲載数 51,000 件（2021 年 5 月時点）を誇る国内最大の購入型クラウドファンディング「CAMPFIRE」をはじめ、グループ会社運営の融資型クラウドファンディング「CAMPFIRE Owners」、株式投資型クラウドファンディング「CAMPFIRE Angels」など多彩なサービス展開により急成長を続ける株式会社 CAMPFIRE。COVID-19 感染拡大の影響により経営に支障をきたした事業者の資金調達手段としても、さらにクラウドファンディングのニーズが高まっています。

課題

今回のプロジェクト推進の背景を株式会社 CAMPFIRE 情報セキュリティチーム マネージャーの木下氏は、次のように話します。「当社の特徴は、スピード成長を目指す IT ベンチャーであり、高い信頼性が求められる金融事業を行う企業でもあるという点です。加えてクラウドサービスの利用やリモートワークの拡大など業務環境も大きく変化し、従来型のセキュリティ対策を抜本的に見直す必要に迫られていました。その中で当社としては、今回の Cisco Secure Access by Duo（以下、Duo）による多要素認証の導入は、包括的なセキュリティ強化策の第 1 ステップである、と捉えています。将来的に目指す姿は、多様なアクセスやデバイスの全体を俯瞰して見ることができて、何か事象が発生したときに素早く影響範囲を特定、被害を最小化できる統合的なセキュリティ環境です。

※クラウドファンディング年間支援成立件数（自社調べ）

株式会社 CAMPFIRE
情報セキュリティチーム
マネージャー
木下 氏

そこで着目したのが Cisco SecureX であり、段階的に実現を目指す最初のステップとして今回実行したのが、Duo による多要素認証ということになります。」
Cisco SecureX とは、エンドポイント、クラウド、ネットワーク、アプリケーションにわたって、シンプルで一貫性のあるエクスペリエンスを実現する、オープンかつクラウドネイティブのプラットフォームです。木下氏は「多彩なサービスラインナップでクラウドからエッジ、エンドポイントまでを統合的に管理でき、自動化により効率的に運用できる点に期待しました。」と語ります。
そうした将来のセキュリティ全体像を見据えたうえで、最初のステップに Duo による多要素認証を選んだ理由について、木下氏は次のように話します。「企業のセキュリティ強化にはさまざまな対策を講じる必要がありますが、クラウドシフトとリモートワーク主体の働き方においては、会社が管理していないクラウドサービスやデバイスの利用は、大きなインシデントにつながります。そのため、まずはここの認証を正しく保つ必要性が高いと考え、最初のステップに定めました。従来の ID とパスワードによる認証にはリスクが伴いますので、ゼロトラストの考え方に基づいて本人であるかどうかも含め、正しいデバイスかを認証することが重要だと考えました。」

クラウドシフトとリモートワーク主体の働き方においてユーザとデバイス認証を正しく保つ必要性が高いと考え、多要素認証を最初のステップに定めました

ソリューション

Cisco Secure Access by Duo はゼロトラストの考え方を基本とした、アプリケーションにアクセスするユーザとデバイスの信頼性を検証し、正しいアクセスのみに許可を与えるクラウドベースのセキュリティ ソリューションです。同社では 2020 年秋より導入に向けた検討を進め、機能評価と検証を経て同年末から利用が開始されました。

丁寧な説明とマニュアル配布で全社員への展開を推進

現時点では社員 140 名、約 200 台の社給 PC とスマートフォンを対象として、デバイス認証を除く多要素認証とデバイスヘルスチェック機能としての利用を展開しているとのこと。「展開時のオペレーションは ID およびパスワードの発行と、ユーザに Duo のデバイスヘルスチェックのアプリケーションをインストールしてもらうのみですので、さほど大変ではありませんでしたが、全社員が実際に使い始めるまでは少し時間がかかりました。マニュアルを配布し、何のために多要素認証が必要なのかを説明。いただいた質問に都度回答するなどして、理解を深めてもらいました。」

シンプルなユーザビリティで利用上のトラブルもなく多要素認証を実現

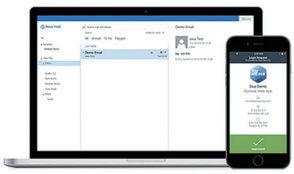
Duo によりログイン前にデバイスの健全性がチェックされ、認証された後に SSO（シングルサインオン）で業務上必要な正規のクラウドサービスにのみ、接続が許可されます。「多要素認証としてはユーザに Duo Push 通知やモバイルパスコードなど複数の方式を提供し、選択して利用できるようにしています。ユーザビリティも直感的でわかりやすいので展開後はトラブルもなく、順調に利用されています。」

結果～今後

木下氏は現状の手応えとして「以前からインシデントにつながりかねない外部からの不正なアタック攻撃を把握しており、ID とパスワードのみに依存した状態に不安がありましたが、Duo での多要素認証と IP アドレス制限が実行できることで、確実に安全性が高まった実感があります。コロナ禍でさらにリモートワークが拡大したこともあり、引き続きデバイス認証も早期に実施して、より確実なものにしていきたい。」と語ります。

Cisco Secure Access by Duo

「ゼロトラストセキュリティ」の考え方に基づき、多要素認証（MFA：Multi-Factor Authentication）を
実現する、クラウドベースのセキュリティサービスです。
社員が業務利用するデバイスやアプリの状態の可視化と、社内イントラだけでなく
外部クラウドサービス利用時の安全性も実現します。



デバイスの健全性を確認し、テレワークの安全性を高める

アプリケーションや VPN アクセス時に、多要素認証による本人確認とデバイスの健全性を検証し、アクセス可能なユーザおよびデバイスを識別したうえで「信頼」を確立。適切な権限を付与することにより、パスワード漏えいやマルウェアに侵害されたデバイスから不正アクセス・情報漏えいを防ぐことができます。

ストレスのない多要素認証を提供

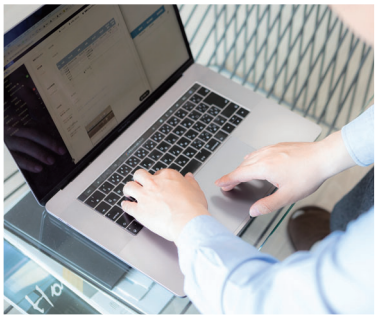
ユーザ自身が認証方式をカスタマイズ可能。スマートフォンやウェアラブルなど好みのデバイスを登録管理して、多要素認証をストレスなく利用できます。ユーザは認証画面で Duo Push を選択できます。数秒後にスマートフォンで受信するプッシュ通知で［承認］を押すだけで、アプリケーションに安全にストレスなくアクセスできます。

クラウドサービスとの高い親和性

Office 365 や Outlook、BOX、Dropbox、AWS、Azure、Active Directory など、さまざまなクラウドアプリケーションやプラットフォームとの統合が可能です。

クラウドベースで導入しやすい

組織の大小を問わず簡単に導入および運用できる、SaaS モデルで提供されます。クラウドベースのセキュリティサービスのため、既存の IT インフラへの影響を最小限に抑えて導入することが可能です。ユーザの自己登録機能や自動連携機能により導入時間を短縮。導入ステップは標準化、公開されたガイダンス資料と動画により、導入工数が大幅に削減可能です。



そして次なるステップとしては「Cisco Umbrella を用いてクラウドサービスの利用状況を可視化し、リスクのあるものはブロックするなどして適切な利活用を促していきたい。また、DLP（Data Loss Prevention）機能との連携による個人情報など機密情報保護の仕組み化も検討しています。その次に Cisco SecureX による自動化および統合管理を実現させたいと考えています。」とのことです。

最後に木下氏は、シスコへの期待についてこう結びました。「常にご担当者のレスポンスも早く、正確かつ丁寧に対応いただき非常に助かっています。シスコには当初からの目的である Cisco SecureX による統合的な管理性はもちろん、さらに各サービスのシームレスな連携を強化いただき、利便性と管理性、安全性を高めるソリューション提供に期待しています。」

その他の詳細情報

Cisco Secure Access by Duo シリーズ の詳細は、
https://www.cisco.com/c/ja_jp/products/security/duo を参照してください。

株式会社CAMPFIRE

設立 2011 年 1 月 14 日
所在地 東京都渋谷区渋谷 2 丁目 22-3 渋谷東口ビル 5F
資本金 67 億 8,106 万円（資本剰余金含む）
従業員数 140 名（2021 年 3 月末時点）
URL https://campfire.co.jp/

事業内容：購入型クラウドファンディング事業、寄付型クラウドファンディング事業、融資型クラウドファンディング事業、株式投資型クラウドファンディング事業、それらに付帯する事業の企画・開発・運営

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日10:00-12:00, 13:00-17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

2247-2108-01A-F