PassLogic 導入事例 株式会社サイバーエージェント

PASSLOGY

サイバーエージェント社のサービスは「PassLogic」で守られている?!

データセンターとのVPN接続に、ソフトウェアトークン型OTP認証機能を採用

ブログサービス「アメブロ（https://www.ameba.jp/）」や、コミュニティサービス「アメーバピグ（https://pigg.ameba.jp/）」、ポイント交換サービス「ドットマネー by Ameba（https://d-money.jp/）」など、数々のインターネットサービスを手掛けるサイバーエージェント社では、エンジニアが各サービスを提供するサーバ群に接続する際の認証に、「PassLogic」の認証機能のひとつ「ソフトウェアトークン型 OTP（ワンタイムパスワード）認証」を利用しています。
このシステムの構成と、認証システムとして PassLogic を採用した理由について、今回の導入製品選定に携わられたサイバーエージェント社 技術本部の東様と梶澤様にお話を伺いました。

株式会社サイバーエージェント
CyberAgent, Inc.

設立：1998 年 3 月 18 日
従業員数：約 4,000 人 ※2016年9月30日時点
URL：https://www.cyberagent.co.jp/


技術本部 東様


技術本部 梶澤様

導入の背景・課題

- ☐ VPN接続開始時の認証における2要素認証環境の確保
- ☐ ユーザトラブル対応が頻発する状況の改善

導入後の改善効果

- ✔ ユーザ側の導入・利用手順がシンプルになり、管理コストが削減された。
- ✔ インシデント発生時の状況把握が容易になった。

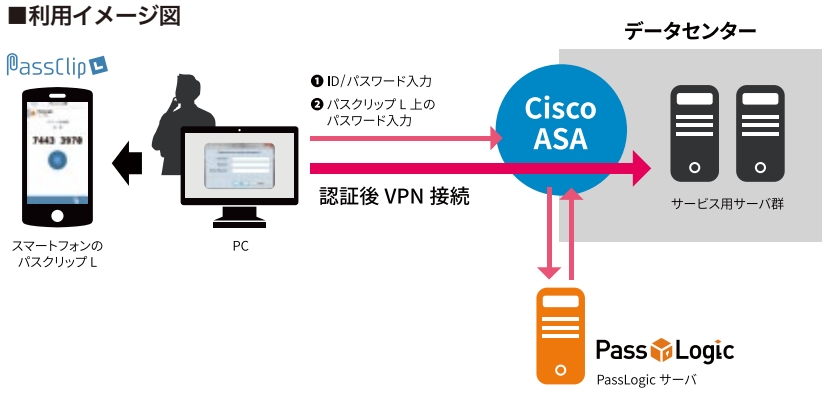
数多くのサービスを支えるサーバ群には VPN で接続

サイバーエージェント社が運営するインターネットサービスは、データセンター内のサーバ群から提供されています。このサーバ群には当社の約 800 名のエンジニアたちが社内もしくは社外から接続し、各サービスの運用を行っています。
当社ではこのデータセンターとの通信にインターネットを利用した VPN 接続を採用しています。専用線による運用も検討したのですが、当社は複数の建物にオフィスが分散しており、部署や社員の拠点移動もよく発生するため、そのたびに管理者が再設定を行うのは管理コストが高くなってしまうという判断がありました。そこで VPN で、どの拠点からでも、また社外からでもフレキシブルに接続し、業務ができる環境が整備されました。

セキュリティを向上し、ユーザビリティを担保する2要素認証

この VPN 接続は、当社のサービスを支える重要なインフラ基盤でありながら、インターネットを通じてどこからでも接続できる柔軟性も持ち合わせているので、セキュリティには十分留意する必要があります。認証においては、ID とパスワードだけでは不十分なので、セキュリティポリシーとして、2要素認証を必須としています。PassLogic導入前も ID &パスワードに、海外製のソフトウェアトークン型 OTP 製品も加えた2要素認証を採用していました。しかし、この海外製 OTP 製品は、ユーザ側での導入手順が煩雑だったことや、OTP参照時に PIN コード入力が必要なうえ、PINコードの入力ミスでロックアウトした際には管理者が対応する必要があるという問題があり、認証システムの見直しを実施しました。
見直しにあたっては、以前と同じ認証方式のソフトウェアトークン型 OTP を採用する方向で検討開始しました。ユーザは日常的にサーバへの接続を何度も行います。認証方式を大きく変えてしまうと、ユーザが対応しきれず、業務が滞る可能性があるので、できるだけ利用時の感覚が変わらない製品の選択を意識しました。
PassLogic は、トークンレスOTPの認証システムとしてフィーチャーされている製品ではありますが、スマートフォン用アプリを利用したソフトウェアトークン型OTPとしても利用できると知り、候補として挙がりました。

■利用イメージ図



PassLogic のソフトウェアトークン型 OTP 認証機能の解説

PassLogic と連携するスマートフォン用アプリ「パスクリップ L（iOS/Android・無償）」に表示された OTP を入力して認証します。

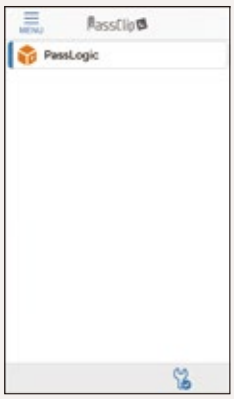
■利用開始手順

❶ App Store/Google Play から「パスクリップ L」をダウンロード&インストール

❷ 管理者から送信される利用開始メール内のリンクをタップ

❸ ブラウザ上に表示される連携画面でリンクをタップ

❹ パスクリップ L 上に「PassLogic」スロットが出現し、連携完了



■認証手順

❶ スマートフォン上の「パスクリップ L」を起動し、「PassLogic」スロットをタップ

❷ 表示されるOTPを確認
※30秒ごとに変更
※ベーシック型表示とビンゴ型表示を管理者側で選択可能

ベーシック型表示

ビンゴ型表示

❸ 認証するシステム / サービスの認証画面に確認した OTP を入力

「Cisco AnyConnect」の場合、Second Passwordとして入力

ブラウザで PassLogicの認証ポータルからのログインも可能

接続成功／失敗

PassLogic 導入の理由

PassLogic を採用した主な理由は以下になります。

❶オープンソースソフトウェアによる開発

当社では、システムを開発する際には、積極的にオープンソースソフトウェアを利用しています。PassLogic も、PostgreSQL や Apache といった当社エンジニアたちが理解しているオープンソースソフトウェアで開発されているため、インシデントが発生した場合、PassLogic もしくは PassLogic と何かの間で、何が起こったのかを推測することができる安心感があります。

❷「OpenLDAP」サーバとのID同期が可能

当社では社内アカウント管理に「OpenLDAP」を使用しています。そして、PassLogic は OpenLDAP との ID 同期機能を持っており、使用中の OpenLDAP サーバをそのまま利用できました。

❸コスト面で優位

当社では、従業員が業務にスマートフォンを使用する体制が整っています。個人所有のスマートフォンの業務利用（BYOD）が認められていますし、希望者が申請すれば会社から業務用スマートフォンが支給されます。

PassLogic のスマートフォンアプリ型の OTP に変更したとしても、新たに認証用デバイスを用意する必要はないため、新たなデバイス購入コストがかかりません。

スマートフォンアプリも無償ですし、サーバソフトウェアとライセンスの費用に関してもリーズナブルだと判断できる価格でした。

❹ AWS上に仮想アプライアンスが用意されている

今回は PassLogic を AWS（アマゾン・ウェブ・サービス）上に構築しました。PassLogic は AWS マーケットプレイスに仮想アプライアンスとして用意されているので、AWS の管理画面からの操作だけで、手軽にサーバを準備することができました。

PassLogic 採用後の状況と今後の予定

導入検討時のテスト環境構築の問合せから、導入決定後の本番環境構築においても、パスロジ社からは早急かつ丁寧に対応していただきました。

運用においては、ユーザ側で行うソフトウェアトークンアプリの設定手順も、利用時の OTP 参照手順も、以前よりシンプルになったため、管理者の運用コストが大きく削減されました。

今のところは、ソフトウェアトークン型 OTP 認証機能を VPN 接続にのみ採用している状況ですが、今後シングルサインオン機能についても検討し、Web サービスやクラウドサービスへの認証にも採用すべきか考える予定です。

PASSLOGY™
パスロジ株式会社
www.passlogy.com
パスロジック事業部
03-5283-2263
受付時間 10:00〜17:00［土・日・祝休］
E-MAIL：sales@passlogy.com
セキュリティ情報サイト
せぐなべ 検索
www.segunabe.com
お問い合わせ先