

セキュリティと
業務効率UPを
ワンストップで実現!

統合認証プラットフォーム

Pass Logic

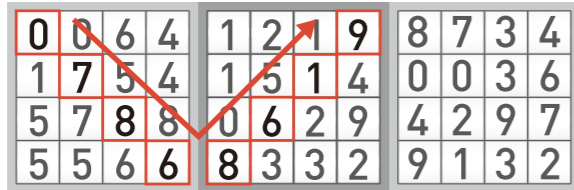
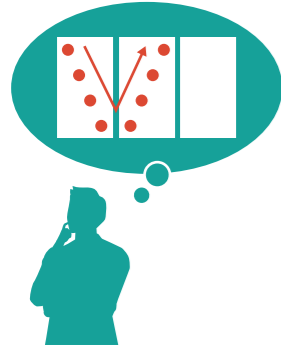
パスロジック



※トークンレス部門において(自社調べ)

■ トークンレス・ワンタイムパスワードで強固な本人認証

「パターン」を覚えるだけ。認証用デバイス不要のワンタイムパスワードです。高セキュリティな本人認証を低コストで実現します。



Password * * * * * * * * ログイン

→ 07868619

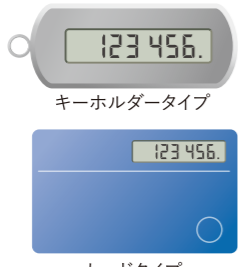
- ユーザーはマス目の位置と順番(パターン)を覚えるだけ。
- ログインのたびに乱数表が更新されるので、パスワードも毎回更新されます。
- パスワード入力画面を後ろから見られても、問題ありません。
- 認証用デバイスが不要。持ち歩き・取り出しの必要がなく、管理コストも削減できます。

■ ソフトウェアトークン・ハードウェアトークンにも対応

ソフトウェアトークンアプリ「パスクリップ L」(無償)や、OATH 規格のハードウェアトークンに対応。ポリシーに合わせて認証方式を選択できます。



ベーシック表示 ビンゴ型表示



キーホルダータイプ カードタイプ



パスクリップ L iOS/Android

クライアント証明書にも対応

■ Windowsへの認証をワンタイムパスワード化

Windows端末起動時のサインインをトークンレス・ワンタイムパスワードにすることができます。



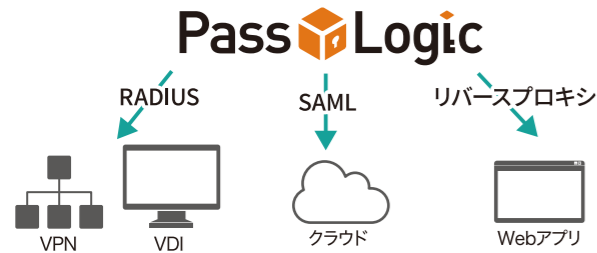
専用アプリケーション「PassLogic for Windows Desktop」

■ 対応OS: Windows 8.1、10、11、Windows Server 2016、2019

■ 豊富な連携方式でSSO (シングルサインオン) を実現

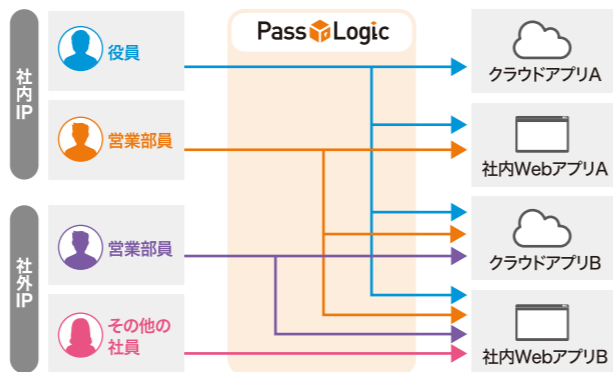
一度のログイン操作で、複数の業務システムに一括ログインできるSSO (シングルサインオン) 機能を備えています。

連携方式として、SAML2.0、RADIUS、リバースプロキシ方式などのプロトコルに対応。REST API による組み込みも可能です。



■ 個人やグループ単位でアクセスコントロール

ユーザーの所属グループや接続元のIPに応じて、接続可能なアプリケーションをコントロールできます。



高セキュリティ&高ユーザビリティも低コストで。

パスロジ インフォ

[Passlogy Co., Ltd. information]

vol.01



» インタビュー

テレワークに不可欠な不正ログイン対策 三重県庁が選択した 認証システムとは?

三重県デジタル社会推進局 スマート改革推進課 情報基盤班 班長 岡本 悟 氏

- ✓ トークンレスの認証システムはBCP (事業継続計画) 対策に最適
- ✓ SDGsに貢献 (産業と技術革新の基盤づくり)
- ✓ ショルダーハッキングを防ぐ不正ログイン対策のしやすさ
- ✓ 低コストでSSO (シングルサインオン) を実現



パスロジック 検索 <https://passlogic.jp>



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
©Passlogy Co., Ltd. 2022



PROFILE
三重県デジタル社会推進局
スマート改革推進課
情報基盤班 班長
おかもと ひとし
岡本 悟氏

安全なテレワーク環境を実現するには、 万全の不正ログイン対策が必要不可欠。 三重県庁が選択したのは、 純国産の認証システム 「パスロジック」だった。

全職員6,500人のテレワーク環境をわずか1か月で緊急配備！ 懸念されていた不正ログイン対策は、コストをかけずに誰でも簡単に使いこなせる「パスロジック (PassLogic)」を採用し、認証強化を実現。

新型コロナウイルスの感染が拡大し、全国に緊急事態宣言が発令された2020年4月、三重県庁では緊急対応として「登庁する職員を最低でも5割以下に削減」という方針が示された。とはいえ登庁しないと進まない業務もあるため、出勤する職員と在宅の職員をローテーションさせる必要がある。つまり、全職員6,500人が在宅勤務の対象なのだ。しかし、これまで在宅勤務の仕組みはほとんど検討していなかったため、その方法も、予算も、安全性も未知の世界だった。そんな混乱した状況から約1か月後、三重県庁の全庁テレワークは大成功することになる。果たして、どんな魔法を使ったのか。その中でパスロジックはどのような役割を果たしたのか。大逆転のストーリーを追っていこう。

Challenge 1

緊急事態宣言を受けて、未整備だったテレワーク環境をフルスピードで導入

2020年4月、緊急事態宣言が発令されると、もうコロナウイルスはすぐそこまで迫ってきている印象になった。職員が一人でも感染したらその部署の業務はストップしてしまう。行政サービスを止めずに職員の安全を守るには、在宅でも庁内と同じレベルで仕事ができるテレワークの仕組みを

導入することが急務だった。しかし、そこには大きな壁が立ちはだかっていた。

三重県デジタル社会推進局スマート改革推進課情報基盤班班長の岡本氏は、当時の様子を次のように振り返る。「三重県ではこれまで、出張など外出先でのモバイルワークを想定した実証研究は行っていたものの、在宅勤務についてはまったく検討していなかったんです。当時スマート改革推進課で保有していたモバイルワーク実証環境とそこで使用できるモバイルPCは、最大でも数十台程度で、システム環境も端末数も、在宅勤務に対応するには到底不可能でした」。いまある環境はまったく使えず、一から立ち上げなくてはならない。「時間も無いし、予算もない。かといって議論している余裕もない。細かいことは走りながら考えるしかありませんでした」。

そこでまず検討したのは、庁内の業務用PCを自宅に持ち帰るという案。しかしこれは情報漏えいの懸念などデメリットの方が大きいことから却下。また、VDI基盤を構築して専用端末を全職員に割り当てるには莫大な費用と時間がかかり、これも現実的ではない。残された方法は、職員の私物PCを使って業務を行うBYOD*とリモートデスクトップの組み合わせだった。

「個人所有のデバイスを流用するのでセキュリティリスクの問題がありましたが、構築ベンダーから提案されたリモートデスクトップの仕組みは、職場PCから私物PCへ画面

だけが転送されるので、私物PCには業務データが一切残らないのです」。低コストで導入までのスピードが速く、安全性の高いBYOD+リモートデスクトップの仕組みは三重県庁のニーズにぴったりマッチしたのだ。

※BYOD
Bring Your Own Deviceの略。個人で所有しているノートパソコンなどの端末を業務に利用すること。

Challenge 2

不正ログインを完全に阻止するためには認証の強化が必須

テレワーク体制が整えば、多くの職員が一気に在宅ワークへ突入する。そうなると懸念されるのは、リモートデスクトップでログインする際に使うIDやパスワードの不正利用だ。IDとパスワードが第三者に知られてしまえば、簡単にセキュリティが突破され、業務システムへの侵入を許してしまう。システム上、私物PCにデータは残らないとしても、県庁の業務用PCが操作できてしまう。不正ログインを絶対に阻止して重要な情報を守るためには、ログインする際、IDとパスワードだけではなく、もうひとつの認証方法を組み合わせることでセキュリティを強化することが急務だった。

ではどのような認証方法を追加すべきか？ iPhoneなどに搭載されていて何となく身近なのは指紋や顔で判断する生体認証

だが、指紋認証や顔認証は読み取り装置が必要になり全庁規模で導入するにはとんでもなくコストがかかる。ハードウェアトークンを利用するワンタイムパスワードも候補に上がったが、ハードウェアトークン端末の費用、全職員に配布する手間など、これも無理だという結論になった。さまざまな認証方法から、どの仕組みを組み合わせることで認証を強化するのがベストか？を議論していく中で、モバイルワークの実証研究で試験的に導入したパスロジ社のトークンレスのワンタイムパスワードがかなり使い勝手が良かったことから、第一候補となった。

Solution

リモートデスクトップサービスの認証に「パスロジック」を採用し、低コストですぐに使える強靱な認証を実現

「最終的に、認証方法はパスロジ社のトークンレスのワンタイムパスワードを選びましたが、もし従来のハードウェアトークン、ソフトウェアトークンのワンタイムパスワードしかなかったら、これだけのスピードでテレワーク環境を実現することは不可能だったと思います」と岡本氏は言う。

キーホルダー型やカード型の専用機器を必要とするハードウェアトークンは、人数分の購入コストが莫大で、紛失や故障、電池切れなどに対応する運用の手間もかかってしまう。一方、スマートフォンに入れた専用のアプリで認証するソフトウェアトークンについても、アプリのインストール方法がわからない人もいるし、そもそもスマートフォンを保有していない職員もいる。

認証用のデバイスを使わずに、6,500人の職員がだれでも簡単に使えること。さらにセキュリティ強化の必要性は絶対だが、コストと時間はかけられないこと。その要望を叶えた認証セキュリティのソリューションが、パスロジ社のトークンレス・ワンタイムパスワード「パスロジック」だった。

Benefit

三重県庁の大逆転！ わずか1か月で全庁 テレワーク環境が実現した

その後、システム構築は順調に進み、契

約手続きからおよそ1か月後の2020年6月、全職員を対象としたテレワークが開始された。パスロジックは、乱数表のマス目に表示された数字を自分が設定したパターンに沿って抜き出すという独特の方法を用いる（下図を参照）ため、岡本氏曰く「使い始めは質問攻めだろうと覚悟していた」そうだが、驚いたことに使い方がわからないという問い合わせはほとんどなかったそうだ。時間的に試用期間を設ける余裕がなく、庁内のイントラネットに簡単なマニュアルを用意しただけだが、大きな混乱もなくスムーズに全庁テレワーク体制がカットオーバーできた。

振り返ると、岡本氏にとっては怒涛の1か月だったに違いない。限られた時間の中で、徹底したセキュリティ対策、ITリテラシーの低い職員でも簡単に使える仕組み、そしてコストなど数々の条件をクリアする解決策を検討。仕組みがシンプルで、コストがかからず情報漏洩の危険性の少ないリモートデスクトップにトークンレスのワンタイムパスワードを組み合わせることで、緊急事態宣言下でも行政サービスが滞ることなく乗り切ることになった。何も決まっていなかった状態からたった1か月で全庁テレワーク環境を実現することができたのは、奇跡に近い。

Future

県庁DXや三層対策の見直しなど、デジタル社会推進局のミッションは目白押し。パスロジックの豊富な機能にも期待

岡本氏は、デジタル技術の利活用やセ



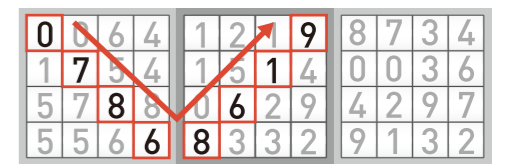
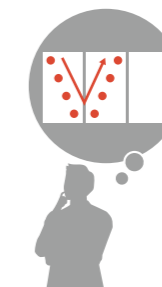
キュリティ対策を、いままでにない考え方でさらに進化させたいと話す。「今回、なんとかテレワークをこなせる基盤が構築できましたが、これが完成形ではなく、クリアすべき課題もまだ多くあります。また、県庁DXの推進や三層対策の見直しなど、やるべきことは目の前に山積み状態です」。

現状を踏まえ、パスロジックへの期待を次のように結んだ。

「今回は「1か月以内に、しかも低コストで、強靱な認証システムを構築する！」という非常に難易度の高い課題を解決でき、緊急事態を乗り越えることができました。今後テレワークが浸透していく中で、さらに強化した認証システムの仕組みが求められることと思います。我々がまだ使っていないパスロジックの機能、たとえばシングルサインオンやアクセスコントロールなども、今後のDX推進で活用していきたいと思っています。今後のご提案やアドバイスを期待しています」。

パスロジックのトークンレス・ワンタイムパスワードのしくみ

「パターン」を覚えるだけ。認証用デバイス不要のワンタイムパスワードです。低コストで高セキュリティな本人認証を実現します。



Password ***** ログイン

➔ 07868619

- ✓ ユーザーはマス目の位置と順番（パターン）を覚えるだけ。
- ✓ ログインのたびに乱数表が更新されるので、パスワードは毎回変わります。
- ✓ スマホのパターン認証と異なり、パスワード入力画面を後ろから見られても、問題ありません（ショルダーハッキングの心配なし）。