Rocket® software

メインフレームの パスワードを使わないという 新しいアプローチ

目次

← 目次に戻る

はじめに

メインフレームのパスワードを使わないという新しいアプローチ

パスワードは企業にとって不可欠なものです。許可されたユーザーのみが最も貴重な資産である情報にアクセスできることを保証します。このような重要な役割を考えると、どのようなパスワードでもいいわけではありません。長く複雑なパスワードであることが理想的です。それもアプリケーションごとに変えるべきです。そして定期的に更新する必要があります。

パスワードは企業にとって脅威でもあります。ユーザーは、パスワードの作成、記憶、そして絶え間ない変更という負担を強いられています。IT部門は、パスワードポリシーの管理と強制という負担を負わなければなりません。幸いなことに、現代的なNetIQのID・アクセス管理（IAM）システムとシングルサインオン（SSO）によって、この負担を軽減することができます。ユーザーは1回ログインするだけで、社内のほとんどのリソースにアクセスできるようになるのです。

しかし、すべてのリソースではありません。残念ながら、IAMとSSOのアプローチは、実際にビジネスを稼働させている最も重要なシステム、つまりメインフレームには使えないのです。

「いつでも、どこでも、どのデバイスからでもメインフレームにアクセスできるようにしてほしい」

現代のユーザーは、メインフレームを含むすべての企業リソースに、いつでも、どこでも、あらゆるデバイスからアクセスできることを期待しています。しかし、メインフレームへのアクセスを無制限に認めれば、ITネットワーク管理者やメインフレームシステム管理者は夜も眠れません。

なぜなら、安全なアクセスを提供する上で、ネットワークとメインフレームはまるで2つの独立した島のようなものだからです。それぞれに独自のアクセス制御システムがあり、それぞれに独自のルールがあります。そしてどちらの管理者も、相手側に合わせて自らのルールを変えようとはしません。

相互に依存関係があり、連携することにメリットがあるにもかかわらず、どちらの島の管理者も統合を阻む課題の解決方法を見出せないのです。

パスワードは企業にとって脅威でもあります。ユーザーは、パスワードの作成、記憶、そして絶え間ない変更という負担を強いられています。

← 目次に戻る

ネットワーク側の主張

ITネットワーク管理者はメインフレームへのアクセスを可能にする端末エミュレーションアプリケーションを管理しているため、そのセキュリティ強化に強い関心を持っています。しかし、IAMで実現される強力なパスワードによる堅牢なネットワークセキュリティを「メインフレーム側」にも拡大させるための現実的な方法はありません。

大多数のメインフレームアプリケーションは、数十年前の今よりも安全な時代に開発されたものです。その時代には、オープンネットワーク、サービス中心のアーキテクチャ、ハッカーなどのサイバー脅威はまだ存在していません。そのためメインフレームアプリケーションは、脆弱な8文字のパスワードを使うようにハードコードされました。当時はそれで十分だったからです。しかし、時代は変わりました。

たとえ現役のメインフレームプログラマーを見つけられたとしても、今メインフレームアプリケーションを書き換えるのは危険です。業務が混乱するだけでなく、費用もかかります。メインフレームを含むすべてのネットワークリソースへのアクセスに単一のパスワードを強制するには、社内のすべてのパスワードを8文字に簡素化するしかありませんが、誰もそのようなアプローチを採りたくはありません。

メインフレーム側の主張

メインフレームシステム管理者は、長年ハッカーたちのレーダーから外れていたメインフレームが、今は標的とされていることを認識しています。メインフレームにはIAMが備わっていませんが、アクセス認証や認可はResource Access Control Facility（RACF）やTop-Secretで実現することができます。それ自体は問題ありませんが、依然として脆弱な8文字のパスワードに縛られているのが現状です。

メインフレームシステム管理者はパスワードやアクセス制御を強化したいと考えていますが、断固として譲れないことが1つあります。メインフレームが誇る99.999%という信頼性を決して損なうことはできないということです。しかし、メインフレームへのアクセスをネットワーク側のネットワークサーバーに統合すれば、まさにその信頼性が損なわれると考えています。また、ネットワーク側ではセキュリティ問題に伴い頻繁に障害が発生しますが、それは到底許容できるものではありません。

大多数のメインフレームアプリケーションは、数十年前の今よりも安全な時代に開発されたものです。その時代には、オープンネットワーク、サービス中心のアーキテクチャ、ハッカーなどのサイバー脅威はまだ存在していません。

← 目次に戻る

メインフレームのパスワードに関する問題

メインフレームは高性能である一方、特異な側面があり、現代の企業環境では異端扱いされています。そのような特異性の1つがメインフレームアプリケーションのパスワードです。以下の問題を抱えています。

- **脆弱な認証**
  セキュリティ専門家に、「大文字と小文字を区別しない8文字のパスワードは機密データを保護するのに十分な強度であるか」と尋ねてみてください。答えは断固として「NO」でしょう。企業のパスワードには厳格なポリシーが適用されています。しかし前述の理由から、厳格なポリシーをメインフレームへのアクセスに適用することができません。
- **危険なユーザー行動**
  この即時アクセスの時代において、メインフレームへのアクセスには別途ログインが必要というのは、ほとんどのユーザーにとって時間の無駄です。考えてみてください。個々のアプリを開くたびに異なるパスワードを入力したいと思う人がいるでしょうか。特に、一日に5〜6回も開くアプリであればなおさらです。このような状況が、ログアウトを怠ったり席を離れる際にワークステーションの電源を入れたまま（無防備な状態で）放置したりするなど、ユーザーをセキュリティよりも利便性を優先する行動に走らせています。
- **煩わしいメインフレームパスワードのリセット**

  複数のメインフレームアプリケーションにアクセスするユーザーは、複数のパスワードを記憶しなければなりません。しかし、それは不可能なので、パスワードを付箋に書いて貼っておくか、パスワードの更新時には微細な変更しかしないといった、セキュリティ上の悪しき習慣に頼るのです。それでもユーザーは結局忘れてしまい、パスワードをリセットせざるを得なくなります。ネットワークのパスワードとは異なり、メインフレームのパスワードはユーザー自身でリセットできません。高給取りのITスタッフが手元の作業を中断 して、この単調で時間のかかる作業を行う必要があります。

セキュリティリスクからユーザビリティやIT管理上の煩わしいタスクまで、8文字のパスワードでメインフレームにログインする慣行は変える必要があります。

優れたセキュリティのための架け橋

両者の主張は並行して進化してきませんでした。ネットワーク側の主張では巧妙化する脅威に対抗するため、業務 アプリケーションへのアクセスを保護するセキュリティが強化されてきました。一方、メインフレーム側では、何十年も前に重要アプリケーションに組み込まれたセキュリティ対策が、数十年間そのままの状態です。

幸いなことに、業務に悪影響を及ぼすことなく、強力な集中管理型のセキュリティをメインフレームアプリケーションにも拡大させられる方法がついに登場しました。Rocket® Secure Host Accessです。 メインフレームとIAMシステムをつなぎ、両者の主張の架け橋となります。

具体的には、Rocket Secure Host AccessはIAMシステムと連携し、端末エミュレータを介したメインフレームへのアクセスの一元管理および保護を実現します。ユーザーとメインフレームの間に展開され、既存のLDAP認証構造を利用してユーザーの認証情報を検証した後、メインフレームへのアクセスを許可します。つまり、ユーザーは強力な認証情報（強固で複雑なパスワード）を使ってIAMに認証・認可されるまで、メインフレームのログイン画面に近づくことすらできません。

Automated Sign-On for Mainframeの仕組み

Automated Sign-On for Mainframeは、IBM® z/OS® Digital Certificate Access Server（DCAS）と連携し、Rocket Secure Host Accessから対象のアプリケーションへのアクセスに必要な時間制限付きのワンタイムPassTicketを取得します。取得したメインフレームユーザーIDとPassTicketを端末エミュレータのログオンマクロに返すと、同マクロが認証情報をメインフレームに送信してユーザーをアプリケーションにサインオンさせます。

← 目次に戻る

また、信じられないかもしれませんが、Rocket Secure Host Accessによってメインフレームのパスワードが不要になります。Rocket Secure Host Accessによって認証されたユーザーは、メインフレームアプリケーションへのログイン時にパスワードを入力するという追加手順を踏む必要がなくなるのです。このツールが 代わりに入力するからです。ユーザーは8文字の危険なパスワードを覚える必要がなくなり、セキュリティ意識の高いIT部門はパスワード管理業務から解放されるため、双方にメリットがあります。

Rocket Secure Host Accessは、ビジネスに合わせてサーバーにもメインフレームにもインストールできます。メインフレームへのアクセスに柔軟で拡張性が高く、高度なセキュリティを備えたソリューションを提供し、メインフレームのパスワードを使う必要性を解消します。

IBM Z MFAによるゼロトラストアーキテクチャを支える追加の防御層

Rocket Secure Host AccessはIBM Z MFAと完全統合され、追加のセキュリティ層を提供します。zOSへのあらゆるアクセスポイントが、多要素認証（MFA）で厳重に保護されます。

安全で、管理性が高く、経済的なソリューション

かつて貴重なメインフレームのデータは、守られた専用経路を通って信頼できる端末へと転送されていました。しかし、それは過去の話です。今日のインターネットという誰もが走れる高速道路においては、悪意のある者からデータを保護するには最強の防御策が必要です。脆弱な8文字のパスワードは過去の遺物として手放すべき時が来ました。パスワードに代わり、最強の認証システムへの架け橋を築き、許可されたユーザーのみが最も重要なデータにアクセスできるようにしましょう。Rocket Secure Host Accessは、これを実現するための安全で、管理性が高く、経済的な手段を提供します。

脆弱な8文字のパスワードは過去の遺物として手放すべき時が来ました。パスワードに代わり、最強の認証システムへの架け橋を築き、許可されたユーザーのみが最も重要なデータにアクセスできるようにしましょう。

Rocket Software について

Rocket Software は、モダナイゼーションにおけるグローバルテクノロジーリーダーであり、コアシステムからクラウドまで、世界有数の企業のモダナイゼーションの取り組みを支援するパートナーとして選ばれています。12,500 社を超える顧客と 750 社のパートナーから信頼され、世界中に 3,000 人以上の従業員を擁する Rocket Software は、顧客がデータ、アプリケーション、インフラストラクチャを最大限に活用して、現代の世界を支える重要なサービスを提供できるよう支援しています。Rocket Software は、ボストン地域に本社を置く非公開の米国企業で、世界中に中核的研究開発拠点を戦略的に配置しています。Rocket Software は、Bain Capital Private Equity のポートフォリオ企業です。

LinkedIn と X で Rocket Software をフォローしてください。

Modernization. Without Disruption.™

詳細はこちら

Rocket software

MAR-12833_WP_NewApproachMainframePassword_V1

RSWPSHA03-202603-KA