Rocket® software

メインフレームへの自動サインオンを実現するオプションを比較する

目次

02 メインフレームセキュリティをモダナイズする必要性

03 メインフレームのパスワードに関する問題

04 どのソリューションを採用すべきか？

04 エンタープライズSSO

06 高速ログオン機能

07 メインフレームへの自動サインオン機能のアドオン

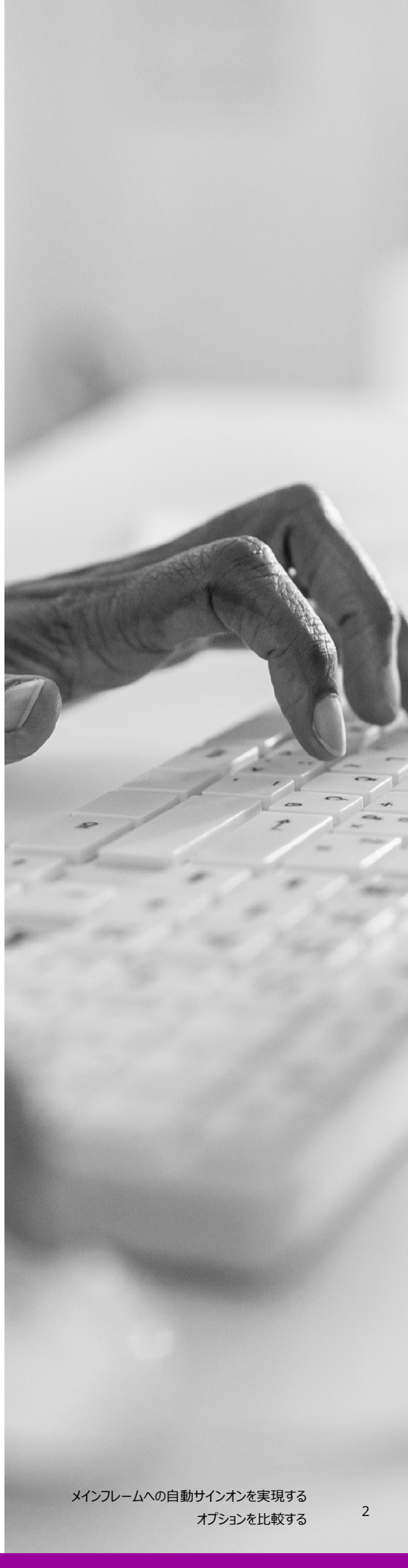
09 メインフレームを他のビジネスと連携させる

← 目次に戻る

メインフレームセキュリティをモダナイズする必要性

巨大なメインフレームは決して過去のコンピューティングではありません。現在でも、この強力な大容量マシンが企業で最もミッションクリティカルなアプリケーションの多くを支えています。つまり、当面なくなることはないのです。問題は、数十年前に構築されたメインフレームアプリケーションの多くが、大文字と小文字を区別しない8文字の脆弱なパスワードを処理するようにハードコードされている点にあります。当時は問題ありませんでしたが、今はそれでは通用しません。

ますます巧妙化する現代のセキュリティ脅威には、これまでよりもはるかに強力でありながら管理しやすいアプローチが必要です。今後に向けて時代遅れのパスワードの問題を解決する方法はありますが、どのように自社に適したソリューションを判断すればいいのでしょうか。本書では、主な選択肢の詳細と選定に役立つガイドラインを提供します。



メインフレームのパスワードに関する問題

あなたが最近ATMからお金を引き出したか、保険金を請求したことがあるとしたら、その取引はおそらくメインフレームで処理されたはずです。しかし、そのような機能があるにもかかわらず、メインフレームには特異な特徴があり、現代の企業環境では異端扱いされています。その特徴の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。以下のような問題を抱えています。

現代のセキュリティニーズを満たしていない

かつてネットワークやハッカーは、私たちの日常生活とは無関係の存在でした。今では状況が変わり、ほとんどのデバイスやアプリケーションへのアクセスにパスワードが必要になっています。しかしパスワードだけでは不十分です。パスワードの効果はその基準と管理方法にかかっています。

パスワードについては、付箋にメモしてモニターを貼るといった行為を避け、大文字と特殊文字が最低でも1文字ずつ含まれる10～12文字のものにすることが推奨されています。管理の点からは、1つのパスワードでメインフレームアプリケーションを含むすべてのネットワークリソースにアクセスできれば非常に便利です。しかし、社内のパスワードをすべて8文字に簡略化したいと思う人は誰もいません。

パスワード管理が煩わしい

大抵の人は、すべてのパスワードを覚えるのに苦労しています。忘れるたびにシステム管理者にパスワードをリセットしてもらう必要がありますが、これは平凡ながら手間のかかる作業であり、システム管理者の注意をより重要なITプロジェクトから奪ってしまいます。

ガートナー・グループによると、ヘルプデスクへの問い合わせの20～50%はパスワードリセット依頼です。またフォレスター・リサーチは、パスワードリセット1件あたりのヘルプデスク人件費は平均して約701ドルと述べています[1]。さまざまな統計がありますが、普遍的な事実があります。パスワードの管理は時間と費用の無駄です。

ユーザーは時代遅れの余計なステップを踏まなければならない

ユーザーがコンピューターにログインすると、通常はメインフレームを除き、アクセス権限を持つすべての企業リソースにアクセスできるようになります。メインフレームアプリケーションにアクセスする場合は、再度サインオンを強いられます。メインフレーム上のアプリケーションごとに、その都度サインオンを求められるのです。ネットワークリソースへの即時アクセスが期待されている現代において、この余計な手間は過去の遺物と言えます。

ガートナー・グループによると、ヘルプデスクへの問い合わせの20～50%はパスワードリセット依頼です。

セキュリティリスク、IT管理上の煩わしさ、利便性などの問題を踏まえ、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。しかし、実現可能なアプローチをどのように選べばいいのでしょうか。

[1] https://www.linkedin.com/pulse/does-password-reset-service-desk-cost-us-money-yes-wake-vijay-shankar/

← 目次に戻る

どのソリューションを採用すべきか？

セキュリティの強化、IT部門におけるパスワード管理業務の解消、利便性の向上を実現する方法はいくつかあります。以下のセクションでは、それらのオプションと、それぞれの主な特徴、検討すべき事項、選定上のガイドラインを併せて紹介します。

01

エンタープライズSSO

エンタープライズシングルサインオン（エンタープライズSSO）は、ユーザーがメインフレームアプリケーションを含むネットワークリソースにアクセスするたびに認証情報を入力する手間を解消する技術です。ユーザーは企業の標準的な認証方法を通じて一回だけ認証を行います。一旦認証されたら、各種ネットワークリソースへのアクセスを試みるたびに、エンタープライズSSOソリューションによって自動的にサインオンされます。

仕組み

エンタープライズSSOの認証情報ストアに、社内のすべてのユーザーおよびリソースのログオン情報（ユーザー名とパスワード）が安全に保管されます。ユーザーがログオンが必要なリソースへのアクセスを試みるたびに、エンタープライズSSOのデスクトップエージェントがログオンプロンプトを傍受し、そのリソースへのアクセスに必要なユーザーの認証情報を認証情報ストアから取得して、アプリケーションに渡します。これはユーザーとアプリケーションにとって透過的なプロセスです。

エンタープライズSSOとメインフレームの統合も同様の仕組みです。エンタープライズSSOのデスクトップエージェントが、端末エミュレータのHLLAPIインターフェースを介してメインフレームのアプリケーションと通信します。メインフレームがサインオン画面を表示すると、エージェントが認証情報ストアから取得したユーザーの認証情報をその画面に入力します。

← 目次に戻る

主な特徴

メインフレームのアプリケーションに変更を加える必要がない

メインフレームのアプリケーションは、ユーザーサインオンプロセスの背後にいるエンタープライズSSOソリューションの存在を認識しません。ユーザーにIDとパスワードの入力を要求し、クライアントから認証情報を受け取るだけです。受領後はメインフレームのセキュリティアクセスフレームワークに基づいて、その認証情報を検証し、通常通りにユーザーを認証します。

既存のエンタープライズ認証方法を活用する

メインフレームへのサインオンに義務付けるべき唯一の認証方法などありません。エンタープライズSSOは企業の標準的な認証方法を通じてユーザーの本人確認を行った後、認証情報ストアからそのユーザーのメインフレーム認証情報を読み取ります。ユーザーは8文字のパスワードを使用してメインフレームのアプリケーションへサインオンされますが、事前にユーザー名とパスワード、デジタル証明書、またはワンタイムトークンを使用してエンタープライズSSOソリューションから認証されていなければなりません。

追加コストなしでメインフレームアプリケーションへのアクセスを実現できる

エンタープライズSSOソリューションのライセンス形態によっては、追加コストをかけることなく、メインフレームへのサインオン機能を追加できるかもしれません。統合とメンテナンスには費用が発生しますが、ほとんどのエンタープライズSSOソリューションのライセンスは、ソリューションに接続されるアプリケーションに関わらず、ユーザー単位で供与されます。

検討すべき事項

静的なパスワードを使用する

ユーザーが手入力することはありませんが、メインフレームアプリケーションへのサインオンには静的なパスワードが使われます。したがって、メインフレームのセキュリティのためには、やはりユーザーがパスワードを保護し、IT部門がメインフレームのパスワード管理責任を負わなければなりません。

全社的なインフラソリューションとして実装される

エンタープライズSSOはメインフレームへのアクセス専用として導入されることはほとんどなく、むしろすべての企業リソースへのアクセス用に導入されるものです。そのため、通常エンタープライズSSOプロジェクトは多くのITインフラタイプにまたがる大規模でコストがかかる取り組みとなり、完了までに数年を要します。メインフレームへのアクセスは、長期にわたるエンタープライズSSOプロジェクトの最終段階に実装されるか、実装されないこともあります。

デスクトップエージェントと端末エミュレータの統合が必要になる

エンタープライズSSOによって、メインフレームへのアクセス基盤は煩雑化します。エンタープライズSSOのデスクトップエージェントはHLLAPI経由で端末エミュレータと統合する必要があるため、デスクトップ上で管理すべきホストアクセス関連のソフトウェアが増えるからです。たとえば、端末エミュレータをアップグレードするたびに、端末エミュレータとエンタープライズSSOのデスクトップエージェント間の統合が正常に機能していることを確認しなければなりません。端末エミュレータのアップグレードによっては、統合の微調整や全面的な再コーディングが必要になる可能性があります。

エンタープライズSSOを選ぶべきか？

あなたの組織ではエンタープライズSSOソリューションをすでに導入済みですか。そのエンタープライズSSOソリューションはメインフレームアプリケーションに対応していますか。セキュリティポリシーで、メインフレームへの認証に静的な8文字のパスワードを使用することは認められていますか。これらの条件に当てはまるならば、あなたの組織でメインフレームへのサインオンプロセスを自動化するにあたり、エンタープライズSSOは有効な選択肢となり得ます。

エンタープライズSSO：主なポイント

エンタープライズSSOソリューションを導入済みの場合は、そこから始めてください。ただし、静的なパスワードの使用を完全に廃止する必要がある場合は、時間制限付きのワンタイムPassTicketsを使用するソリューションを探してください。

← 目次に戻る

02

高速ログオン機能

高速ログオン機能（ELF）は、X.509証明書を持つユーザーをメインフレームのアプリケーションへ自動的にサインオンさせることができるIBM®のソリューションです。証明書高速ログオンとも呼ばれています。

仕組み

端末エミュレーションクライアントがTelnetサーバーとのSSL／TLS接続を確立し、メインフレームセッションを開始します。その後、エミュレーションクライアントはログオンマクロを実行し、ユーザーIDとパスワードのフィールドにプレースホルダーを挿入します。TelnetサーバーはSSL／TLSハンドシェイク時に提供されたクライアント証明書に基づき、ユーザーのメインフレームユーザーIDと、Resource Access Control Facility（RACF）から取得した時間制限付きのワンタイムPassTicketを要求します。その後、Telnetサーバーはログインマクロから取得したメインフレームユーザーIDとPassTicketをプレースホルダーに挿入し、ユーザーをメインフレームのアプリケーションに自動的にサインオンさせます。

主な特徴

パスワード管理の必要性が解消される

ELFはPassTicketsを使用してユーザーを単一のメインフレームアカウントにサインオンさせるため、そのアカウントにおける静的なパスワードの管理負担が解消されます。つまり、パスワード忘れでヘルプデスクへ問い合わせる必要がなくなるということです。

2層アーキテクチャに対応している

ELFが2層アーキテクチャであるということは、ミドルウェアを追加する必要なく、自社環境にメインフレームへの自動サインオンを追加できるということです。

RACFでID情報をマッピングできる

ユーザーのエンタープライズIDとメインフレームユーザーIDのマッピングを管理するために、別途データストアやLDAPディレクトリを実装する必要はありません。RACFのユーザーアカウント情報にユーザーのデジタル証明書を直接追加することができます。

検討すべき事項

ユーザー認証にはX.509証明書が必要である

デジタル証明書を用いた二要素認証方式はとても安全ですが、実装と管理には高いコストがかかります。現在、ほとんどの組織はユーザー名とパスワード方式の認証を採用していますが、これはELFとの相互運用性がありません。

ユーザーごとに1つのメインフレームユーザーIDしか持てない

ユーザーの証明書はRACFで単一のメインフレームIDにしかマッピングできないため、ELFの自動サインオン機能を採用する場合はユーザーにメインフレームユーザーIDを1つしか持たせることはできません。つまり、以下の2種類のユーザーには対応できなくなります。

1. 複数のメインフレームアプリケーションへのアクセス権限を持つユーザー：すべてのメインフレームアプリケーションでユーザーIDを統一させればELFを機能させることはできますが、それはすべての環境で可能なことではないかもしれません。
2. 特定のメインフレームアプリケーションに対して複数のIDを持つユーザー：担当するタスクに応じて、1人のユーザーにさまざまなレベルの権限が与えられている場合に、このような状況が発生します。

証明書が更新されるたびに再マッピングが必要になる

RACFにおけるユーザー証明書とメインフレームIDのマッピングは、ユーザーIDではなく証明書自体に紐付けられるものです。そのためクライアントの証明書が更新されるたびに（セキュリティ上の理由から通常2～3年ごと）、RACFでユーザーのメインフレームIDを新しい証明書に再マッピングしなければなりません。

← 目次に戻る

ELFを選ぶべきか？

ユーザーがメインフレームユーザーIDを1つしか持たず、セキュリティインフラにデジタル証明書が組み込まれている場合は、ELFが有効な選択肢かもしれません。この条件に当てはまらない場合は、もっと柔軟なソリューションを探してください。

ELF：主なポイント

ELFはPassTicketsによる高度なセキュリティを実現するほか、業界をリードする端末エミュレーションクライアントでサポートされているアプローチです。ただし、ユーザーが認証にX.509証明書を使用していない場合、または複数のメインフレームユーザーIDを保有している場合には、もっと柔軟なソリューションを探す必要があります。

03

メインフレームへの自動サインオン機能のアドオン

Rocket® Secure Host Accessは、IBM® 3270アプリケーションへの自動　サインオンを実現する、セキュリティを最優先に設計された端末エミュレータです。静的なパスワードの必要性を解消するだけでなく、再コーディングの必要なく、 さまざまな認証方式と連携してメインフレームアプリケーションのセキュリティを強化します。

仕組み

ユーザーがメインフレームのセッションを開始すると、端末エミュレータのログオンマクロがRocket Secure Host Accessからユーザーのメインフレーム認証情報を要求します。このツールはユーザーのエンタープライズIDを利用してメインフレームユーザーIDを取得します。その後、IBM® z/OS® Digital Certificate Access Server（DCAS）と連携し、RACFから対象アプリケーション向けの時間制限付きのワンタイムPassTicketを取得します。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、マクロが認証情報をメインフレームに送信し、ユーザーはメインフレームのアプリケーションにサインオンされます。

PassTicketsについて

PassTicketsは、ユーザーがメインフレームアプリケーションへのサインオンを試みるたびに、RACFによって動的に生成されます。静的なパスワードとは異なり、PassTicketsは一度しか使用できないため、リプレイ攻撃を防ぐことができます。またPassTicketsには有効期限があるため、一度も使用されていない場合でも一定時間（デフォルトでは10分）が経過すると失効します。

← 目次に戻る

主な特徴

パスワード管理の負担が解消される

Rocket Secure Host Accessは静的なパスワードに代わり、PassTicketsを使ってユーザーをメインフレームアプリケーションへサインオンさせます。メインフレームのパスワードは不要になるため、ITスタッフはパスワードの紛失または忘却によるリセット作業から解放されます。

さまざまな認証方式に対応できる

Rocket Secure Host Accessは、ディレクトリベースのユーザー名とパスワード認証方式からデジタル証明書を利用する認証方式（デジタル証明書は必要ありませんが）までさまざまな方式に対応しているため、どのようなID・アクセス管理（IAM）システムを利用していてもシームレスに連携させられます。

1人のユーザーが複数のメインフレームユーザーIDを持てる

Rocket Secure Host Accessでは複数のメインフレームユーザーIDを単一のユーザーにマッピングできるため、複数のメインフレームアカウントを持つユーザーを、それらすべてのアカウントに自動サインオンさせることができます。

検討すべき事項

3層アーキテクチャを採用している

Rocket Secure Host Accessは、ワークステーション上の端末エミュレーションクライアントとメインフレーム上のアプリケーションとの間に位置するミドルティアサーバーに展開され、z/OS DCASサービスからPassTicketを取得するものです。

メインフレームIDとエンタープライズIDのマッピングに基づいている

ユーザーが認証されると、IAMシステムはユーザーのエンタープライズIDをRocket Secure Host Accessに提供します。メインフレームへの自動サインオンを機能させるには、IT部門がRocket Secure Host Accessシステムでユーザーのエンタープライズ IDとメインフレームIDをマッピングしておく必要があります。

DCASサービスを使用する

メインフレーム上でIBMのDCASを有効にする必要があります。DCASはz/OS通信サーバー（z/OS TCP/IPネットワークスタック）のコンポーネントです。z/OSとともに提供されますが、デフォルトではインストールされていません。

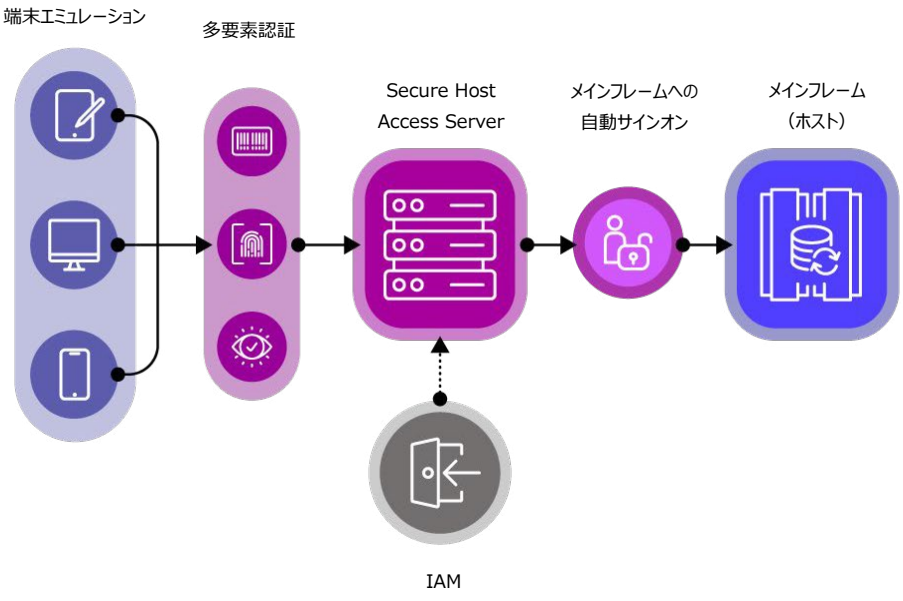


図1. ユーザーはRocket Secure Host Accessへ認証後、メインフレームアプリケーションへログインする際にパスワードを入力するという余計な手順を踏む必要がなくなります。パスワードの入力は、このツールが自動的に処理します。

← 目次に戻る

Rocket Secure Host Accessを選ぶべきか？

ミッションクリティカルなメインフレームアプリケーションのセキュリティ強化は要件とされていますか。メインフレームのパスワード管理業務から解放されたいですか。証明書を使用しない認証方法や、単一のユーザーに複数のメインフレームIDを付与するといった柔軟性は必要ですか。メインフレームへの自動サインオン機能をアドオンとして追加すれば、メインフレームアプリケーションを再コーディングする必要なく、安全かつ効果的にメインフレームのセキュリティを強化することができます。

ROCKET SECURE HOST ACCESS：主なポイント

ELFと同様に、Rocket Secure Host AccessはPassTicketsを利用するため、高度なセキュリティが実現されるアプローチです。ELFとの違いは柔軟性にあります。Rocket Secure Host Accessはさまざまな認証方式に対応しており、単一のユーザーに複数のメインフレームユーザーIDを割り当てることが可能です。

メインフレームを他のビジネスと連携させる

メインフレームは絶滅しません。いずれなくなるものとして扱わないでください。メインフレームを現代のセキュリティフレームワークに組み込み、時代遅れの8文字パスワードから脱却する方法はあります。本書で紹介したソリューションの仕組みを理解し、あなたの組織に最適なアプローチを選択してください。

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。

*formerly Micro Focus® products

Modernization. Without Disruption.™

詳細はこちらをご覧ください ›

詳細はこちら

Rocket software

MAR-12520_WP_CompOfAutoSignOnOptMainframe_V1

RSWPSHA02-202603-KA