Rocket® software

グリーンスクリーンからレッドアラートへ：メインフレームのセキュリティを強化する

悪意のあるAI、フェイクITワーカー、高額な罰金からグリーンスクリーンを守る方法

目次

はじめに

ITチームは長年、Linuxなどのマシンよりもメインフレームの方が「保護しやすい」という考えを信じ、メインフレームで「十分である」と考えてきました。

そのような時代は過ぎ去りました。

データ侵害の課題とコストは増加しています。脅威はこれまでよりも広範囲で大胆に活動しており、サイバー攻撃の手段は増え、AIも使われるようになっています。調査において、メインフレームの脆弱性に対する積極的な対策に高い自信を持っていると答えたITリーダーがわずか28%であったのも頷けます[1]。

このホワイトペーパーでは、メインフレームのセキュリティを抜本的に見直すことなく、増大するリスクを低減し、オペレーションを保護する方法を紹介します。

具体的には、以下の点をまとめました。

- 現在メインフレームを脅かしている3つの重大なリスク
- それらのリスクを解消するための5つのベストプラクティス
- 役立つテクノロジーと手法

夜は安心して眠れるように、今すぐ簡単に取り入れられる方法があります。**今すぐ始めてください。**

← 目次に戻る

メインフレームのリスクが高まっている理由

高度に発達したハイパーコネクテッドな現代社会において、メインフレームは格好の標的です。

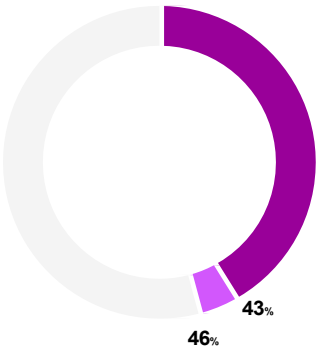
ユーザーが端末エミュレータを使用してメインフレームのアプリケーションに直接アクセスすることはよくあります。驚くことに、その際のログイン認証は、大文字と小文字を区別しない8文字のパスワードであることが一般的です。以前はそれでも問題ありませんでしたが、現代において、会社で最も重要な資産であるメインフレームのデータを適切に保護するにあたり、このような認証方法では不十分です。

メインフレームのデータは、極めて重大なリスクを抱えています。

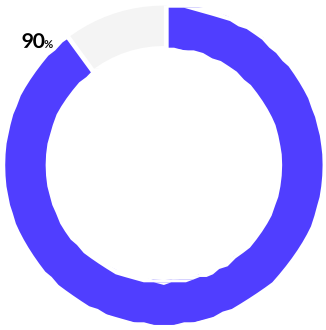
- データ侵害によるコストは前年比10%増加し、パンデミック以降で最大の伸び率を記録しました。2024年の侵害1件あたりのコストは、世界平均で488万米ドルに達しています[2]。侵害のほぼ半数（46%）で顧客の個人識別情報（PII）が、43%で知的財産（IP）のレコードが関係していました。いずれも規制違反であり、罰金の対象です[3]。
- クレジットカード取引の約90%はメインフレーム上で処理されています。メインフレームには、社会保障番号、生年月日、住所、電話番号、クレジットカード番号を含む大量（正確な数値で示すことはできませんが）のPIIが保存されています。金融サービス、政府機関、公益事業、非営利 団体が最も多くのPIIを保有している傾向があります。
- 2024年、認証情報の窃盗または侵害によるサイバー攻撃件数が前年比71%増加しました[4]。2024年に発生したセキュリティインシデントの40%で、アプリケーションレベルの攻撃が行われていました[5]。一方ダークウェブでは、ますます多くのパスワードや認証済みブラウザセッションのトークンが公開されています[6]。
- IBM®のデータ侵害コストに関する2024年のレポートによると、2024年に確認されたすべての攻撃ベクトルの中で被害額が最も高かったのは悪意のある内部関係者による攻撃であり、平均499万米ドルでした。それ以外に、ビジネスメール詐欺、フィッシング、ソーシャルエンジニアリング、認証情報の窃盗または侵害などの攻撃ベクトルも高額な被害額につながっています。これらのフィッシング攻撃の一部では、生成AIが使われている可能性があります[7]。

ユビキタスAIなどの新技術が、ハッキングや窃盗といった攻撃活動への参入障壁を下げています。このような新技術により、IDを偽装したり数秒でパスワードを解読したりするほか、キーを押す音からパスワードを特定することさえ可能になりました。

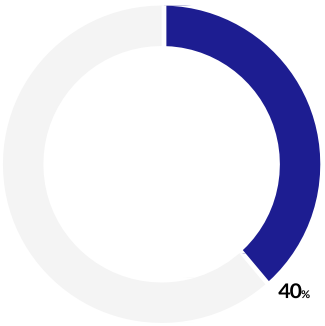
組織には、悪意のあるアクターを排除し、データとオペレーションを攻撃から守り、メインフレームを円滑に稼働させるための新たなベストプラクティスが必要です。



データ侵害の46%でPIIが、43%でIPが関係している



クレジットカード取引の90%はメインフレーム上で処理されている



2024年に発生したセキュリティインシデントの40%で、アプリケーションレベルの攻撃が行われている

← 目次に戻る

メインフレームを脅かす3つの重大なリスク

メインフレームは、執念深いハッカーや不満を抱えた従業員から、競合他社や妨害を企てている国家支援型のアクターに至るまで、あらゆる者にとって魅力的な標的となっています。しかも現代では、クレデンシャルスタッフィング、パスワードスプレー攻撃、フィッシングなどのツールを簡単に利用できてしまいます。

一方で、アクセスに関する新たなデータセキュリティ規制も急増しており、違反には罰則が科せられます。

これらのすべてが、メインフレームを含む複雑なIT環境を管理するCISOにとって、過大なコストを伴う懸念事項になっています。

警戒すべき3つのリスク領域は以下のとおりです。

01 内部脅威とフェイクワーカー

02 AI、ChatGPT、Copilotなど

03 コンプライアンス要件の肥大化

← 目次に戻る

内部脅威とフェイクワーカー

「犯人は家の中にいる！」などと言えば、低俗なホラー映画の台詞のように聞こえるかもしれませんが、内部脅威は現実に存在するどころか、ますます蔓延し、巧妙化しています。よくあるのは、権限を持つ従業員や契約業者が意図せずセキュリティを侵害する過失です。また、不満を持つ従業員が意図的に不正を働くケースもあります。悪意のある人物をたった1人採用しただけでも、その人物の組織内での立場によっては、個人的な利益や金銭のために暴走されることは少なくないのです（同等職への人事異動ですら、大きな被害をもたらすことがあります）。

このような事態には認証情報の紛失、共有、窃盗、失効が関係していることが多く、想像以上に頻繁に発生しています。

そして状況は悪化します。

「幽霊社員」が会社の給与台帳に現れるかもしれません。給与台帳やその他の記録を改ざんするアクセス権と能力を持つ内部の不正行為者が、実際には存在しない社員の給与明細を作成し、現金化するのです。

極端な（しかし、実際に起こり得ます）例として、北朝鮮の「ラップトップファーム」スキャンダルのような精巧な標的型攻撃法が挙げられます。この事例では、組織化された実行犯らが北朝鮮の利益のために、数千件の盗まれた認証情報を利用し、米国の市民や居住者になりすました300人以上の海外の情報技術（IT）ワーカーを米国企業のリモート職に就けたとされています[8]。

この犯行グループは、米国の決済プラットフォーム、オンライン求人サイトのアカウント、米国内のプロキシコンピューター、米国人や米国法人（攻撃に加担していることを認識していない場合もあります）を悪用して企業を騙したとされています。米政府の勧告によると、このサイバー犯罪者は従業員が職務を通じて得た特権的アクセス権限を悪用して侵入したとされており、サイバーセキュリティ専門企業であるマンディアントなどの組織も、この見解を裏付ける所見を発表しています。

マサチューセッツ州では、攻撃者が巧妙な偽の給与支払サイトによって州職員を騙し、個人情報や金融データを盗むというインシデントが発生しました。この犯人は、同州の職員向けセルフサービス勤怠管理　システムに対する「認証情報収集キャンペーン」を行っていた可能性が高いと考えられています[9]。フィッシング詐欺の極みと言えます。

高度な技術を持つテクノロジー企業でさえ例外ではありません。ロシアの国家支援型アクターがパスワードスプレー攻撃（脆弱なパスワードといった脆弱性を悪用する手法）によってマイクロソフトをハッキングし、最終的に同社メールアカウントの一部を侵害するというインシデントが発生しています[10]。

要するに、内部脅威は増加傾向にあります。攻撃はますます容易になり、幅広いアクターに利益をもたらしているのです。

「幽霊社員」が会社の給与台帳に現れるかもしれません。給与台帳やその他の記録を改ざんするアクセス権と能力を持つ内部の不正行為者が、実際には存在しない社員の給与明細を作成し、現金化するのです。

← 目次に戻る

AI、ChatGPT、Copilot など

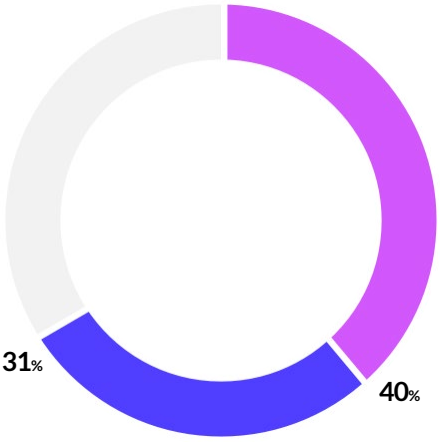
AIはビジネスのあり方を一変しています。製品の設計、開発、製造、販売、サービス提供の方法から、顧客、見込み客、従業員、ベンダー、パートナーとの関わり方まで、あらゆる側面を変えているのです。企業はソフトウェア開発を含む業務の全域にAI（生成AIを含む）を導入することを急いでいます。

AIはテクノロジー主導の攻撃だけでなく、ソーシャルエンジニアリングでも利用されるようになっています。ソーシャルエンジニアリングとは、人間の特性を悪用し、機密情報や個人データ（認証情報を含む）の提供、金銭の支払いや預け入れといった行動に誘い込む攻撃です。ベライゾン・ビジネスによると、2023年には3,600件以上のソーシャルエンジニアリングインシデントが発生し、そのうち3,032件でデータ漏洩が確認されています[11]。ソーシャルエンジニアリング攻撃で最も多い手法はプレテキスティングで40%以上を占めており、次いでフィッシング（31%）、恐喝、ベイト攻撃が多数確認されました[12]。

プレテキスティングとは、ソーシャルエンジニアリング攻撃者が被害者を脆弱な状況に追い込み、個人情報を差し出す理由（シナリオ）を作り出す技法です。（リバースソーシャルエンジニアリングでは、被害者に攻撃者へ連絡させるように仕向けます。）

AIの普及とともに、人間側もIDの詐称に抵抗できなくなってきています。AIが、建設的なヘルプデスクボットから、一夜にして現れたかのようなTikTokインフルエンサーや多数のフォロワーを持つLinkedInプロフィールまで、人間になりすますことがますます容易になっているからです。AIによるなりすましやIDの盗用は、新たな内部脅威、詐欺、金融犯罪、社会的・政治的な構造変化、さらには金銭的損失や名誉毀損といった被害までもたらす可能性があります。

もちろん、賢明な企業や組織は、データ侵入や流出対策として、セキュリティを絶えず更新しています。メインフレームはこれまで守られてきたものの、メインフレームを所有している企業は、AIが人間になりすましている可能性について警戒を怠ってはなりません。



ソーシャルエンジニアリング攻撃の40%はプレテキスティングで、フィッシング（31%）、恐喝、ベイト攻撃がそれに続く

← 目次に戻る

コンプライアンス要件の肥大化

コンプライアンス対策は万全だと思っているかもしれませんが、今後の規制環境は予想以上に厳しいものとなるでしょう。トムソン・ロイターによると、一般的な金融機関は平均して1日あたり223件の規制動向に対処しなければなりません[13]。

データとITのセキュリティに関する規制は着実に進歩しており、メインフレームも含めたコンプライアンス対応には期限が設けられ、違反すれば罰則が科されます。

現在メインフレームも対象となっているのは、Payment Card Industry Data Security Standard（PCI DSS；ペイメントカード業界データセキュリティ基準）、一般データ保護規則（GDPR）、カリフォルニア州消費者プライバシー法（CCPA）などの規制です。これらすべての規制で多要素認証（MFA）のようなより厳格な個人情報の保護がすでに義務付けられているか、まもなく義務付けられます。2025年1月17日に施行されたデジタルオペレーショナルレジリエンス法（DORA）も同様です。DORAは、欧州連合（EU）域内で事業を行う金融機関にデータの暗号化を義務付けています。

米国各州も同様の動きを見せています。ニューヨーク州のサイバーセキュリティ規制（23 NYCRR Part 500）は、州法銀行、民間銀行、国際銀行、住宅ローン仲介業者、保険会社など、ニューヨーク州で事業を行う金融機関の顧客データとITシステムを保護することを目的として制定されました[14]。この規制はMFAを義務付けており、違反した場合には民事制裁金が科される可能性があります[15]。

米国政府もさまざまなコンプライアンス規制を定めています。サイバーセキュリティ国家行動計画の一環として、すべての連邦政府のウェブサイトにMFAを義務付けています。同様に、国税庁は税理士に対し、MFAキーの保護による機密データの保護を義務付けています。

これらはメインフレームに影響する規制のほんの一例です。ユーザー認証に関する要件は、ますます厳重化されています。

← 目次に戻る

今すぐ取り入れられる5つのベストプラクティス

課題は増え続けていますが、この先組織を守るために実践できる5つの簡単な対策を紹介します。

01

「グリーンスクリーン」と言えば「セキュリティ」と考えるようにする

自然にそう考えるようになるべきです。グリーンスクリーンアプリケーションは、PIIなどの機密データを含む重要なデータを提供するものです。他のIT部分と同様に、グリーンスクリーンアプリケーションも過剰なほど保護する必要があります。

本質的に安全なウェブベースの端末エミュレータを提供するか、ユーザーにVPN経由でアクセスさせてください。また、端末エミュレータがTLS 1.3やMFAなどの標準的なセキュリティ機能に対応していることを確認してください。

まだ参加されていない場合は、IT-ISAC（情報技術情報共有分析センター）の全国レベルやトピックごとの活動に参加してください。脅威の最新情報を得られるほか、他の会員から学びを得られます。

02

グリーンスクリーンへのログイン認証を既存のIAMソリューションに統合する

ID・アクセス管理（IAM）は、企業のリソースやデータへのアクセスを制御するポリシー、テクノロジー、プロセスのフレームワークです。これは現代のサイバーセキュリティにおいて極めて重要なコンポーネントであり、機密データ、システム、アプリケーションへのセキュアなアクセスを実現します。

← 目次に戻る

IAMは、ID管理、アクセス管理、認証、認可、プロビジョニング／デプロビジョニング、ガバナンス／コンプライアンス、監視／レポートなどの機能を提供します。セキュリティを強化し、規制コンプライアンスを支援するほか、業務を効率化して、ユーザーにとっての利便性を向上させます。

IAMシステムの標準的な構成要素であるMFAは、アカウントへのアクセスにパスワードに加えて他の要素を要求するセキュリティ手法です。通常は第二の要素として、(1) 知識情報（パスワードやPINなど）か (2) 所持情報（トークンなど）に該当する認証要素を2つ以上提供しなければなりません。第三の要素を求める場合は、指紋や虹彩スキャンなど、ユーザーの生体情報が採用されています。一般的なMFAは、ユーザーがデバイスやアプリでアカウントにサインインする際に、第二の要素を要求します。

MFAを実装しておけば、パスワードが侵害されてもアカウントへの不正アクセスを防げます。また、脆弱なパスワードや盗まれたパスワードを使用してデータへのアクセスを試みるサイバー犯罪を防ぐ上でも効果的です。

IAMを利用すれば、外部環境とメインフレーム接続の間に、さらなる防御層が追加されることになります。

03

異常な行動を警戒する

監視と行動分析を自動化し、継続的に行動の変化を警戒してください。たとえば、インドの従業員が深夜に突然、初めての場所からログインするといった変化です。直接接続されているすべてのメインフレームユーザーを含めて、監視範囲を拡大させてください。事前にアクセスを制限するほか、制御を常に最新の状態に保ってください。

通常、企業のIAMシステムを利用すれば、認証情報に基づいて行動をブロックまたは許可するルールを細かく設定し、この課題を解決することができます。また、メインフレームへのアクセスにIAMを活用すれば、メインフレームに接続される前に悪意のあるアクターを阻止することができます。

← 目次に戻る

04

常に監査証跡を残す

将来的に発生し得る悪意のある行動パターンを特定し防止するためには、誰がいつ、どこで、なぜ、どのように接続し、何を行ったかを把握する必要があります。優れたIAMシステムには、このために利用できる測定機能が備わっています。メインフレームオペレーションのバックグラウンドで動作するランタイムプロセス検出ツールも、ヒートマップなどのテクノロジーを用いて、ユーザー操作をリアルタイムに細かく追跡できます。

グリーンスクリーンにおけるユーザー活動のログを記録し、組織内ですでに取り入れられているレポート機能に集約する作業は、IAMに任せてはいかがでしょうか。

05

すでに堅牢なSDLを確立済みのベンダーを探す

堅牢で確立済みのセキュア開発ライフサイクル（SDL）を実証できるベンダーと協力してください。開発中やアップデート時には、どのアクセス権限を付与したのか、どのアクセス権限をはく奪したのか、それをどのように確認できるのかを把握する必要があります。

ソフトウェアベンダーは、企業のサプライチェーンにおいて安全なパートナーでなければなりません。たとえば、事業を展開している業界における新たなセキュリティ規制の動向と、それが顧客（あなた）に与える影響を監視できるベンダーを探すべきです。

IBM®のデータ侵害コストに関する2024年レポートによると、予防策にセキュリティAIと自動化を幅広く活用するというのは　有効なアプローチであり、実際に展開している組織は、平均して年間222万米ドルのコスト削減を実現しています[16]。

← 目次に戻る

新たなリスク、新たなルール、新たな価値

メインフレームも、もはやハッカーや窃盗犯、犯罪者のレーダーから逃れられません。

私たちは、IDの偽装、窃盗、売買がますます容易になった、急速に進化するオープンインターネットの世界を生きています。情報の保護とアクセス許可にパスワードだけでは不十分です。組織の脅威プロファイルは悪化の一途をたどり、ハッカー（人間とAI）はますます独創的な手法を導き出しています。

グリーンスクリーンへのアクセスを保護することは、モダナイゼーション戦略において極めて重要でありながら、見過ごされがちな要素でもあります。

今すぐ導入可能なテクノロジーと上記のベストプラクティスを取り入れることで、このセキュリティ問題を解消し、増大するリスクを低減させることができます。

必要なツールと手法は揃っています。想像よりも簡単にできるはずです。今すぐ始めてください。

[1]The State of Mainframe Security, 2023 Survey Report by Rocket Software

[2]Cost of a Data Breach Report 2024, IBM

[3]Cost of a Data Breach Report 2024, IBM

[4]IBM X-Force Threat Intelligence Index 2024

[5]Gartner

[6]"Stolen passwords are a goldmine now," Axios, March 5, 2024

[7]Cost of a Data Breach Report 2024, IBM

[8]"Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea," Office of Public Affairs/U.S. Department of Justice, May 16, 2024

[9]"State employees fooled by fake payroll website farming their data," Boston.com, October 10, 2024

[10]"Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard," Microsoft, March 8, 2024

[11]Verizon Business 2024 Data Breach Investigation Report

[12]Verizon Business 2024 Data Breach Investigation Report

[13]"Establishing Resiliency through a Modern Regulatory Change Management Strategy," IDC blog, March 22, 2021. https://blogs.idc.com/2021/03/22/establishing-resiliency-through-a-modern-regulatory-change-management-strategy/

[14]New York Department of Financial Services, https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

[15]"DFS Announces $1 Million Cybersecurity Settlement With First American Title Insurance Company" https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311281

[16]Cost of a Data Breach 2024, IBM https://www.ibm.com/reports/data-breach

目次に戻る

Rocket® Secure Host Access

Rocket® Secure Host Accessは、重要なホストアプリケーションへの安全で、フィッシング対策が施された、パスワード不要のアクセスを提供します。既存のエンタープライズIAMを活用し、最小限の労力でホストアプリケーションへのアクセスを上位のITセキュリティ戦略に統合することができます。

Rocket® Secure Host Accessは、以下をサポートします。

- SSO、SSH、MFAなどのセキュリティのベストプラクティスを拡大させる。
- 組織のエンドユーザーロールに基づいて機密データを削除する。
- サイバー攻撃の脅威と罰金を低減させる。

ロケットソフトウェアは、メインフレームアプリケーションへのアクセスにおいてセキュリティファーストのアプローチを貫く唯一の端末エミュレーションパートナーです。既存の戦略とツールを活用してグリーンスクリーンへのログインを保護することをお手伝いします。

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。

詳細はこちらをご覧ください

Modernization.
Without Disruption.™

Rocket software

MAR-12201_WP_SecureHostAccess_V4　RSWPSHA02-202603-KA