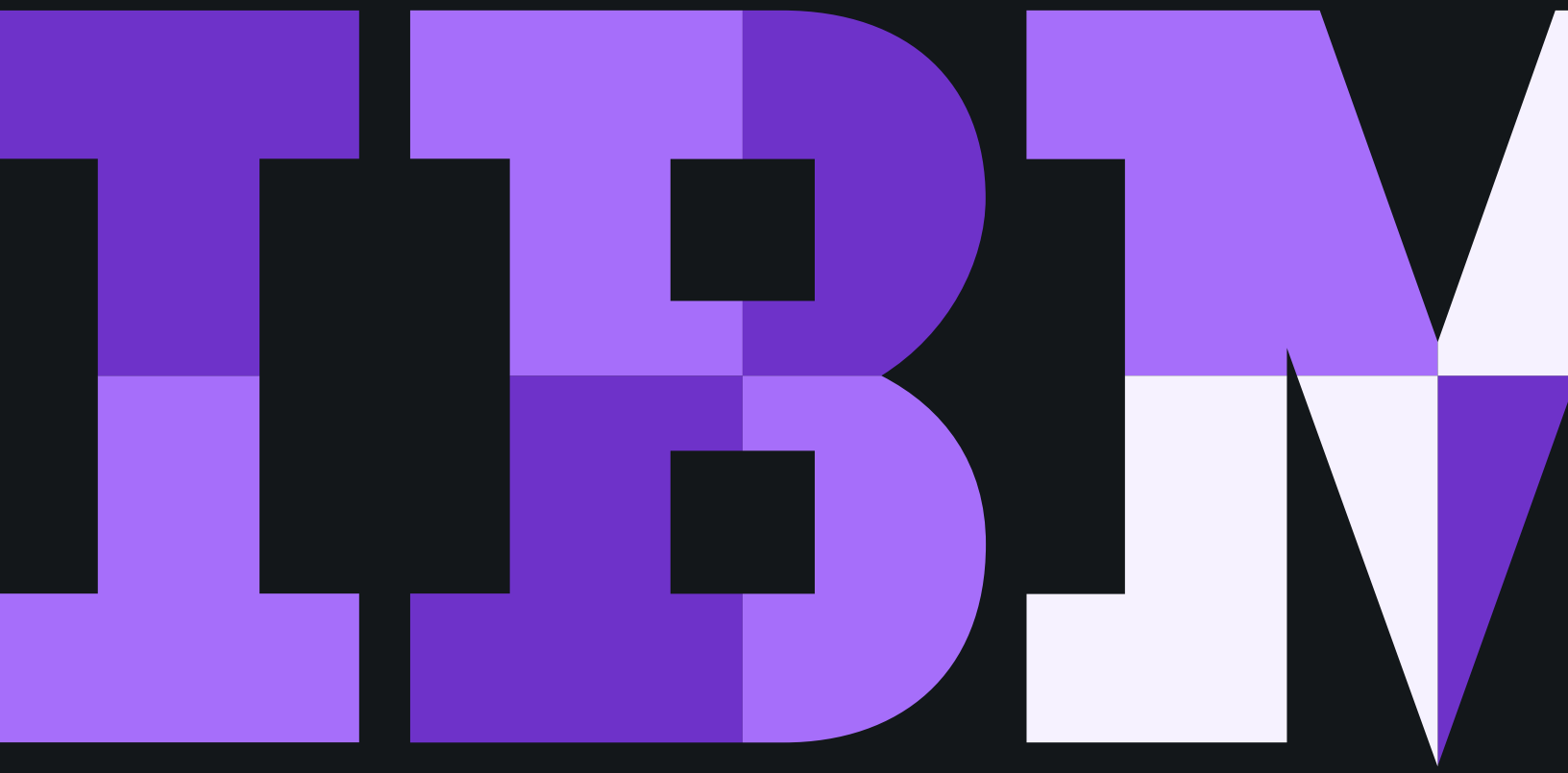
IBM Security

2020 年 1 月

デジタル体験を改善するためのデジタル・トラストの構築

シームレスでセキュアなデジタル・トラストによるビジネス機会の開拓



IBM

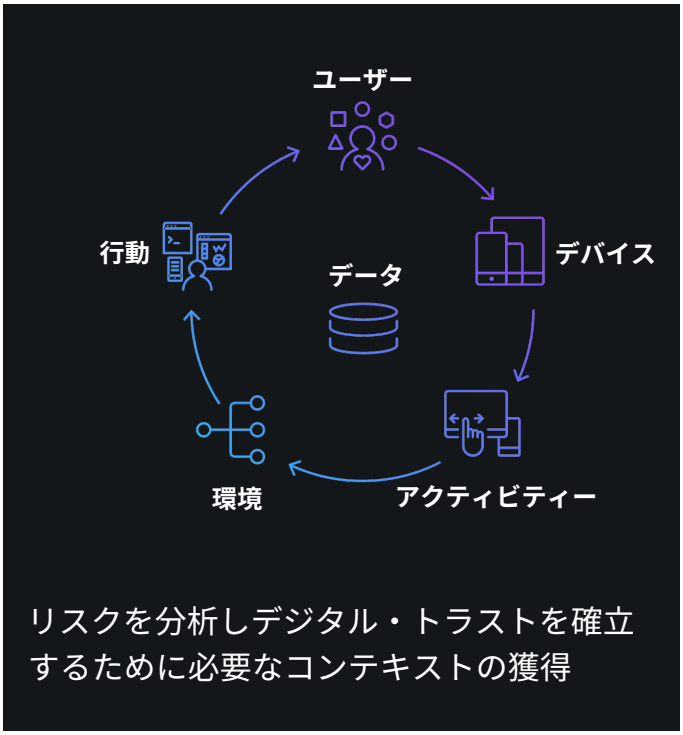
目次

3 デジタル世界における信頼の構築
3 信頼を確立するためのコンテキストの活用
4 信頼確立のために企業セキュリティーとの連携
5 ビジネスを安全に維持
6 信頼の基盤を通したデジタル変革の推進
7 セキュリティーによるビジネス機会の開拓

デジタル世界における信頼の構築

人間は、五感、記憶、知性を使って信頼を確立します。しかし、これらの手段が奪われたとしたらどうでしょうか。デジタル世界では、信頼を確立するために、情報、アイデンティティー、セキュリティー・ツールを複雑に組み合わせることが必要になります。

デジタル・トラストは、適切なユーザーが適切な理由と目的で適切なデータに適切にアクセスする際に発生するプライバシー管理と特権が組み合わさって構成されます。デジタル・トラストのメリットはセキュリティーだけではありません。ユーザー体験を考慮に入れ、一貫して実装されたデジタル・トラストにより、生産性の向上と増収の機会につながるエンゲージメントの向上が達成できます。



リスクを分析しデジタル・トラストを確立するために必要なコンテキストの獲得

信頼を確立するためのコンテキストの活用

顧客は、個人情報の保護を求めています。さらに、セキュリティーの専門家には、企業を守る義務があります。考慮に入れるべきプライバシーおよびコンプライアンス要件が存在し、それに伴って企業も変化する必要がありますが、その間にも、世界的なサイバー犯罪者のコミュニティーから発せられる、ますます高度なサイバー攻撃に耐えなければなりません。一方、ユーザーは、シームレスでわかりやすいセキュリティー・メカニズムを要求します。

企業は、かつては、ID およびアクセス管理 (IAM) ソリューションを使って信頼性を構築することができたかもしれません。**ただ、デジタル・トラストは、単にアイデンティティーを確立しただけでは得られません。それは、以下を考慮することにより、アイデンティティーの上にコンテキスト知見の層を重ねて分析し理解することから**生まれます。

- ユーザーと、そのユーザー固有の属性
- デバイス、およびデジタル指紋などのエンドポイント固有の認証
- データ、アプリケーション、ユーザーに関連するアクティビティー
- ユーザーの環境とネットワーク環境
- 利用状況の分析によって規定されるユーザーの行動

信頼確立のために企業セキュリティーとの連携

他のあらゆる関係と同様、デジタル・リレーションシップは、長期間にわたる多くの小さなやり取りの積み重ねで構成されています。そのやり取りを総合することにより、私たちの行動、利益、責任、役割で構成される、アイデンティティーに対する蓄積された知見が得られます。ただし、デジタル世界では、企業は個人がデバイス、ネットワーク、アプリケーション、チャネル間を移動するたびにこの関係を常に検証し確認する必要があります。このため、ユーザーにパスワードの入力を求めるプロンプトを繰り返し表示し、追加の認証手続きを要求したり、アプリケーションに対する正当なアクセスが拒否されるといった摩擦が生じます。

デジタル・トラストの目標は、ユーザーのためのセキュアで摩擦のない体験を構築することであるべきです。これを達成するには、組織は、手動のコントロールに頼るのではなく、適切なセキュリティー・テクノロジーとプロセスを組み合わせて信頼性メカニズムを自動化する必要があります。たとえば、アプリケーションごとにパスワードの入力を求める代わりにシングル・サインオンを導入する、またはユーザーの体験の質を損ねることなく、セキュリティー・コントロールを有効に設定する効果的な方法として、高度なアナリティクスを使用してステップアップ認証を開始することができます。

IBM Security Identity & Access Management によるサイレント・セキュリティーの実現

企業は、適切なタイミングで適切なユーザーがデータに適切にアクセスできるようにする必要があります。IBM Identity & Access Management を使って、社員に必要なものを提供できます。

動画を見る

適切なデジタル・トラストのフレームワークによって、AI が組み込まれた詐欺検知、強力でシームレスな ID およびアクセス管理、機能スイートが統合されたデータ・セキュリティー、マルチデバイス管理が統合された モバイル・セキュリティーなどの最新のテクノロジーを活用できます。これらのテクノロジーを組み合わせることによって、お客様は以下を実現できます。

- オンプレミスとクラウドベース・システムの間でセキュリティーとアイデンティティーをシームレスに拡張
- レガシー・テクノロジーと新しいテクノロジーを統合して共有された信頼性の基盤を構築
- セキュリティー・コストを削減し、組織全体のセキュリティー・プロセスを合理化
- 部署を超えた可視性をセキュリティー・チームに提供し、チームの結束力を強化

IBM Security のソリューションとサービスを利用することによって、世界最高級のデジタル・トラスト・プラットフォームを構築できます。IBM Security Guardium は、データを守りコンプライアンスを保証します。IBM Security Identity & Access Management は、アイデンティティーを効率的に管理しユーザーの行動を検証します。IBM Security MaaS360 は企業内外のモバイル・セキュリティーを管理します。

ビジネスを安全に維持

お客様が何年もかかって築いてきた顧客との信頼関係を維持する必要があります。コンプライアンス要件に適合し、不正行為を防止することにより、お客様の評判を守るだけでなく、収益率を引き上げることも可能です。プライバシー、同意、コンプライアンスの制約があっても、セキュリティーを強化し、ログインおよび認証プロセスを簡易化することが可能です。人工知能や行動分析などの最新技術を活用することで、デジタル・トラストを確立するためのサイレント・メカニズムを確立することができます。

アイデンティティーは、場所、デバイス、アプリケーション間を常に移動するため、セキュリティー・コントロールは俊敏で透明である必要があります。この俊敏で透明性の高いセキュリティーは、以下を含むさまざまな形体で実装できます。

- 簡単に実装できる単一および多要素認証統制によるシームレスな体験の提供
- リスクの高いユーザーのみに適用できる、厳重で高度な認証メカニズム
- 複数のデバイスやアプリケーション間のアクセスを簡素化するシングル・サインオン画面および統合されたアプリケーション起動パッド

IBM Security は、高品質のユーザー体験を維持しながらお客様のビジネスを守ります。IBM Security サービスは、重要なデータを特定、分類、保護します。IBM Security Guardium ユーザー・アクティビティーを監視し、不正なアクセスをセキュリティー・チームに警告し、暗号化、マスキング、トークン化などのセキュリティー・コントロールを通してデータを守ります。IBM Security Identity & Access Management 規制遵守 (FFIEC、2FA、PSD2 など) を支援し、アクセス証明書を中央管理し、ログイン、ログアウト・プロセスを簡素化するため、新しい規制要件が発生してもすぐに適応できます。IBM Security Trusteer は AI およびデータ・コンソーシアムを使用した最新式の不正行為防止機能を提供し、異なる組織にわたる不正行為の傾向を追跡し、保護するデータを共有し、防衛線を構築します。

IBM Security Guardium でよりスマートなデータ保護を

スマートなデータ保護は、知見に基づいて監視し、企業のイノベーションに伴って変化する目的と規模に合わせて自動化します。IBM Security Guardium がお客様の世界をどのように保護できるか詳しく見る

動画を見る

IBM Security Guardium は、ユーザーのアクティビティーを監視し、不正なアクセスをセキュリティー・チームに警告します

信頼の基盤を通したデジタル変革の推進

デジタル変革は、イノベーション、効率性、体験の改善を約束することで促進されます。この約束には、セキュリティーと信頼の存在が暗黙的に含まれています。**セキュアでシームレスなデジタル体験を提供できる企業は、従業員の生産性を改善し、顧客ロイヤリティーを向上でき、デジタル市場の勝者となります**。反対に、セキュリティー・メカニズムをユーザーの期待に適合できなかった企業は、デジタル変革に大きな痛みが伴います。

デジタル・ユーザーが期待するものは、簡素化されたセキュリティーです。ユーザーは、何回も手動で認証する必要がない、多要素認証による保護を求めています。財布やパスワードを失くしたときでも簡単に使用できるセルフヘルプ・ツールが必要です。また、ユーザーは、デバイスやアプリケーションが変わっても、同じ ID 情報がシームレスに付いてくることを期待します。

IBM Security は、信頼のデジタル基盤の構築をお手伝いできます。IBM Security Identity & Access Management は、セキュアなシングル・サインオンを提供するため、一旦アプリケーションにログインしたユーザーに繰り返しパスワード・プロンプトが表示されることはありません。IBM Security MaaS360 を使用すると、ユーザーはセキュリティーを犠牲にすることなく、どこからでもアプリケーションにアクセスできます。IBM Security Trusteer は、リスク要素がある場合のみステップアップ認証をインテリジェントに開始するため、シームレスなオンボーディングとログインを提供しながら不正行為を防止します。

IBM Security Trusteer によるデジタル ID の信頼性を構築

IBM Security Trusteer を導入すると、顧客の ID とその信頼関係がデジタル体験と共に移動します。

動画を見る

セキュリティーによるビジネス機会の開拓

デジタル・トラストに対する正しいアプローチは、セキュリティーを超えて、より高い品質のユーザー体験を構築することから発掘できる商機を見据えることです。これまでは、長い登録手続きや複数のパスワード・プロンプトを提示するセキュリティーは、ユーザーにとって、快適な体験を妨げるものでした。ユーザーが本当に必要としているものは、複数のデバイスを移動しても付いてくるデジタル ID であったり、ユーザーによるデバイスの持ち方といった、小さな異常でも見逃さない行動分析など、背後で実行されるセキュリティー・メカニズムです。

今日、デジタル・トラストがどのように確立されるか考えてみましょう。多くの場合、パスワードの入力、ID の入力、プロンプトに反応するなど、**身元を証明する行為をユーザー側から実行する必要があります。これとは異なり、ユーザーが触ったり見たりすることがなく、パスワードを入力する必要がない、より広範囲なコンテキスト信頼性メカニズムの一部としてサイレント認証が自動的に実行される** 体験を想像してみてください。すべてのユーザーに同じ信頼性問題を提示するのではなく、リスクのあるごく少数のユーザーのみに問題が提示されます。すべてのユーザーが潜在的な脅威として扱われる否定的な経験を味わわせることなく、データを保護し続け、アカウントを安全に守り、信頼性を確立できます。

デジタル・トラストを適切に獲得した企業は、ユーザーとより強固で長期的な、より有益な関係を構築できる可能性があります。

IBM Security のデジタル・トラスト・ソリューションは、このような信頼関係を構築し、複数のデバイスやアプリケーションにシームレスに拡張できます。IBM Security は、以下の機能を備え、データ検知、データ保護、アイデンティティーおよびアクセス管理、認証、リスク管理、不正行為検知、グローバル脅威インテリジェンスが統合された総合的なデジタル・ソリューションを提供します。

IBM Security Trusteer – クラウド・インテリジェンス、AI および機械学習を統合することにより、シームレス認証と強力な不正行為検知機能による、継続的なデジタル・アイデンティティー保証を提供できるようお客様を支援します。

IBM Security MaaS360 – データを保護し、プライバシーとコンプライアンスを支え、セキュアでシームレスなモバイル体験を提供するために設計され、AI を使用してクラウドに統合されたエンドポイントを管理するソリューション

IBM Security Guardium – プライバシーおよびコンプライアンス・リスクを分析し、データを守り、脆弱性を継続的に監視する完全な保護プラットフォーム

IBM Security Identity & Access Management – シングル・サインオン、多要素認証、アクセス・コントロールなどの透過的なアイデンティティーおよびアクセス管理機能によりサイレント・セキュリティーを提供

IBM セキュリティー

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in Japan
January 2020

WAGXLGAJ