認証の失敗は顧客の喪失につながることが判明

～ Ponemon Institute の新レポートより ～

ユーザーがサービスにアクセスできないことがデジタル変革の取り組みに悪影響を及ぼすというリスクについて、IT 部門と事業部門の責任者の間には、その理解や対応の面で大きなギャップが存在

カリフォルニア州サンノゼ発　- 2022 年 3 月 29 日

本人確認およびパスワードレス顧客認証のための最も拡張性の高いプラットフォームを提供する Nok Nok Labs（以下 Nok Nok™）が後援し、プライバシー、データ保護、および情報セキュリティ・ポリシーを専門とする著名な研究機関である Ponemon Institute（以下、ポネモン研究所）が作成した新しいレポートでは、認証の失敗やその弱点がビジネスに多大なコストをもたらしていることを浮き彫りにしています。

Nok Nok が独自に初期調査を行ったところ、今日のシステム認証プロセスに関する状況や、その状況下で認証の失敗がビジネスに与える影響を示すようなビジネスデータはほとんどないことがわかりました。そこでこのギャップを解消するための初めての取り組みとして、ポネモン研究所は Nok Nok と共同で、デジタル変革プロジェクトを現在推し進めている企業を対象とした業界調査を実施しました。

システムで起こる認証の失敗は、組織の認証プロセスに弱点があるため、ユーザー全体の中からあるユーザの本人確認を行えない場合に起こります。 1,007 人の IT 部門のセキュリティ・スタッフやセキュリティ責任者、事業部門の責任者を対象とした調査によると、様々な認証の弱点に起因するビジネス損失の平均は、3,900 万ドルから 4,200 万ドルにも昇ることがわかりました。また、特に重大なビジネス上の混乱をもたらすような認証の弱点についていえば、ビジネス損失は追加で最大平均 3,400 万ドルから 4,000 万ドルも増えてしまうということがわかりました。さらに この調査で明らかになったのは、社内外のユーザーがシステムの認証失敗によって組織の商品やサービスにアクセスできなくなったとき、IT セキュリティ部門と事業部門との内部連携の際に大きなギャップが存在することです。

システムの認証の弱点がもたらす影響や経済的損失には、アカウント回復やパスワードリセットが過度に行われることや、攻撃者が有効なユーザー名とパスワードの認証情報のリストを使って行うクレデンシャル・スタッフィングなどの自動化された攻撃を被りやすいことなどが挙げられます。システムの認証の弱点がコストにつながってしまうのは、多くのユーザーが認証できなくなる問題を解決するのにダウンタイムのコストがかかったり、業務プロセスの中断が起きたり、第三者とのビジネス関係に悪影響があったりするためです。**この調査から得られた重要な発見は、「システムで認証に失敗すると、顧客を失うことになる」ということについて、社内の利害関係者の間で共通の認識があるということでした。**

ポネモン研究所の会長兼創設者である Larry Ponemon（ラリー・ポネモン氏）は、次のように語っています。「驚くことではありませんが、システムで認証に失敗することが組織にとっていかに高いものにつくのかが

明らかになりました。潜在的なコストの大きさを知れば、このレポートのデータによって、組織が啓発されると共に関心が高まり、セキュリティプロセスやアクセス制御方法の再検討がされ、システム認証の弱点とそれに伴うビジネスリスクを軽減するための戦略的調整が行われることになるでしょう。」

社内ユーザー認証と社外顧客認証との関係

従業員の本人確認や認証を行うようなユースケースでは、認証の弱点によって生じるリスクに対処する際、システムの認証についての理解における社内のギャップやズレが障害となることがあります。この調査で浮き彫りになったギャップには、次のようなものがあります。

- **認証プロセスの全体的なコントロールについて**

組織における認証プロセスを高いレベルでコントロールできていると回答しているのは、IT 部門のセキュリティ・スタッフの 32%とセキュリティ責任者の 44%だけである一方、事業部門の責任者の 67%は認証プロセスのコントロールに自信を持っています。**内部の認証のコントロールについて、その認識には組織間で 2 倍の差があります。**

- **認証失敗のリスクを低減できる自信について**

事業部門の責任者の 66%は、組織は認証失敗のリスクを低減するためにとてもよく準備ができている、または非常によく準備ができていると回答しているのに対し、IT 部門のセキュリティ・スタッフは 40%しかそのように回答していませんでした。**こういった失敗への対処について自信にズレがあり、1.6 倍も差があることは、システム全体への問題が将来起こることを予見させるものです。**

- **認証の失敗の回数や頻度が増加していることの認識について**

IT 部門のセキュリティ・スタッフの 71%と事業部門の責任者の 55%が、認証の失敗が大幅に増加していると回答しています。**認証の失敗について、内部部門間の評価には大きな隔たりがあります。**

- **盗取した認証情報を使った犯罪者のなりすましと、「本物の」従業員、顧客、ユーザーとを見分けられるかについて**

盗取した認証情報によるなりすましを防ぐことは非常に困難または困難であると、IT 部門のセキュリティ・スタッフの 66%が回答したのに対し、事業部門の責任者は 48%でした。**両グループとも、信頼できるユーザーの認証情報とサイバー犯罪者が提示する認証情報を区別することは、組織にとって非常に困難であるということを認めています。**

Nok Nok の CEO である Phillip Dunkelberger（フィリップ・ダンケルバーガー）は次のようにコメントしています。「このデータは、システムのプロセスやワークフローから生じる認証の失敗に組織が適切に対処しないと、いかに大きなリスクやコストが生じうるのかを明らかにしてくれています。事業部門と IT 部門の間に存在するギャップは警戒すべきものです。企業がセキュリティ環境を適切にコントロールしている、すなわち従業員の認証ハードウェアやプラットフォームをコントロールしているとしても、社内エンドユーザーの認証に失敗すると、多大なリスクやコストが発生することは明らかです。ましてや使用するデバイスやプラッ

トフォーム、ネットワーク接続を、企業がほとんど、あるいは全くコントロールできていないような、何百万人もが利用する顧客向け認証アプリケーションの場合、同等のリスクが存在するのはもちろん、コストはさらに掛かってしまうことになるでしょう。」

ダンケルバーガーはさらにこう続けます。「企業全体のシステムの認証の失敗を解決するために、経営層はリーダーシップをもっと発揮し、この両部門を結びつける必要があります。そうしないと、この傾向は悪化し、コストは上昇し続けるでしょう。Nok Nok は現在、顧客の認証に関する問題解決に注力しており、認証こそが顧客の信頼につながる玄関口であると常に信じています。今回の調査結果は、消費者向けの認証のユースケースにも当てはまりますが、企業にとってシステム認証の弱点は、顧客を失ってしまうことも含め、非常に大きなコストになりうることを示唆しています。つまり、ユーザーの本人確認と認証について、企業はこれまでとは異なる考え方をしなくてはならないことを、今回の組織内部のギャップやズレに関するデータが示しているのです。またこれこそが、我々が Nok Nok を起業した理由の一つなのです。我々は組織の IT 部門と事業部門が求めるものに包括的なアプローチを提供し、デジタル変革を実現させ、これを加速させるエンドユーザー認証ソリューションを提供しています。」

Ponemon Risks and Cost of Authentication Report(ポネモン研究所による認証のリスクとコストに関するレポート)はこちらからダウンロード可能です。

Nok Nok のパスワードレス認証ソリューションについての詳細はこちらをご参照下さい。
https://noknok.com/solutions/
https://jp.noknok.com/products/s3-authentication-suite-jp/

Ponemon Institute（ポネモン研究所）について
Ponemon Institute（ポネモン研究所）は、企業や政府が責任ある情報およびプライバシー管理の実践を推進できるように取り組んでいます。この目的を達成するために、当研究所は 独立した研究を行い、民間および公共部門のリーダーを教育し、そして、さまざまな業界の企業のプライバシーおよびデータ保護の実践を検証しています。

Nok Nok Labs について
Nok Nok Labs は、FIDO 標準のパイオニアであり、次世代のアイデンティティおよびパスワードレス認証ソリューション分野の信頼のおけるリーダーです。Nok Nok™ S3 Authentication Suite は、最新のアイデンティティとパスワードレス認証を活用することにより、企業の顧客体験、トランザクション、ビジネスプロセス、ワークフローを変革することを支援します。Nok Nok™ S3 Authentication Suite は、既存のシステムレベルのワークフローや従来のセキュリティ・インフラにインテグレーション可能な、最もスケーラブルで機能豊富なパスワードレス・ソリューションを提供します。Nok Nok Labs の次世代パスワードレス・プラットフォームを導入した企業には、99%以上の認証成功率、オンボーディング・コンバージョンにおいて 10%以上の改善、アカウント回復リクエストの 90%以上の削減を実現している例もあり、運用コストを大幅に削減することができます。カリフォルニア州シリコンバレーに本社を置く Nok Nok Labs は、堅牢なグローバル特許ポートフォリオによって保護されている独自の発明とイノベーションを提供しています。FIDO Alliance の創設メンバ

ーであり、FIDO 仕様の発案者である Nok Nok Labs は標準ベースの認証の導入におけるエキスパートであり、BBVA、Cigna、DDS、Ericsson、富士通、日立、Intuit、Lenovo、三菱 UFJ 銀行, MTRIX、NTT DATA、NTT ドコモ、OneSpan、ソフトバンク、Standard Bank、T-Mobile、Verizon を含む顧客およびパートナーと連携しています。 詳細は、jp.noknok.com をご参照ください。