

ITmedia エンタープライズ まとめ読み eBook

「英数・記号の混在」はもう古い NIST が禁じたパスワード慣行と組織のリアル

パスワード設定における「大文字・小文字・数字・記号の混在」や「定期的な変更」は、もはや過去の常識となりつつある。米国国立標準技術研究所（NIST）が策定したガイドラインの改訂版は、旧来の慣行を明確に禁止し、認証ポリシーの基準を刷新した。NIST はなぜ、これまでの常識を真っ向から否定したのだろうか。

本ブックレットでは、この NIST の新要件を基に、従来のパスワード運用が見直しを迫られる背景や、新たに義務化、禁止された具体的な認証要件を解説する。併せて、アークティックウルフジャパンの最新調査から見えた、新基準と逆行する企業のリアルを紹介する。

従業員の意識改革や厳罰に頼るのではなく、人間の心理や行動に即した「仕組みとしての防御策」をいかに築くか、これからの組織セキュリティの設計図を提示する。

「英数・記号の混在」はもう古い NIST がパスワードポリシーの要件を刷新

NIST はパスワードポリシーに関するガイドライン SP800-63B を更新した。従来のパスワード設定で“常識”とされていた大文字と小文字、数字、記号の混在を明確に禁止し、新たな基準を設けた。

米国国立標準技術研究所（NIST）は、パスワードポリシーに関するガイドライン「NIST Special Publication 800-63B」（以下、SP800-63B-4）を更新した。SP800-63B-4 では認証方式やパスワード管理の在り方を実質的に改訂しており、ただ新しい要素を追加したのではなく、これまで「推奨（should）」とされていた事項を「必須（shall）」へと格上げし、旧来の慣行の一部を明確に禁止した。

従来のパスワードの常識は“崩壊”している NIST が定める新要件とは？

SP800-63B-4 は主に政府機関や認証サービス提供者（Credential Service Provider：CSP）を対象とした技術的基準を定義している。認証プロセスにおいて、利用者の本人性を確認し、確立した信頼レベルに応じたアクセス制御を目的にしている。

従来、NIST はパスワードの複雑性を重視し、大文字と小文字、数字、記号を組み合わせた構成ルールを推奨していた。しかし「混在ルールを課してはならない」と明確に定義し、特定の文字タイプを強制する慣行を禁止した。

NIST はなぜこれまでのパスワードの常識を真っ向から反対しているのだろうか。

NIST はその理由として、形式的な複雑性が実際の安全性を高めるとは限らず、むしろ利用者に予測可能なパターン（例：「Password1!」など）を選ばせてしまう傾向があることを挙げている。

定期的なパスワード変更の義務付けも廃止された。「侵害が確認されている場合のみ変更を強制せよ」と明記されており、定期的な更新を強要する運用は推奨されていない。これまで一般的だった「90 日ごとの変更」といったルールは、むしろ利用者の負担を増やし、安全性を損ねる要因になっていたと判断されている。

パスワードの長さに関しても要件が引き上げられた。単 1 要素認証（パスワードのみで本人確認する場合）ではこれまで最低 8 文字以上を義務付け、15 文字以上を推奨としていたが、最低 15 文字を義務付けている。また、多要素認証（MFA）の場合においては最低 8 文字が求められている。最大長については少なくとも 64 文字を許容するよう指示されている。64 文字以上の長いパスフレーズを推奨する方針は旧版から存在していたが、今回はこれが明確に必要と規定されている。

この他、既知の漏えいパスワードとの照合（ブロックリスト方式）が正式に義務化された。検証機関および CSP は、パスワード設定時に過去の侵害データや一般的に使われやすい単語、サービス名やユーザー名を含むものなどを自動的に拒否しなければならない。これは利用者が形式上「複雑」なパスワードを設定しても、既に流出済みのものを使っている可能性を防ぐ目的がある。

旧来のセキュリティ質問（KBA）やパスワードヒントも全面的に排除された。新版では「ユーザーヒントを保存してはならない」「知識ベース認証を使ってはならない」と定義されており、こうした方法がもはや安全でないことが明確にされている。個人情報容易に入手可能な現代において、生年月日や出身地などを使った質問が攻撃者に突破される危険が高いためだ。

今回の改訂は、NIST がここ数年示してきた方向性の延長線上にあるが、表現の「義務化」と「禁止化」によって、実運用上の影響は大きいと考えられる。特に従来の複雑性ルールや定期変更の慣行を維持している組織は、今後のセキュリティポリシーの修正が必要となる。

NIST のガイドラインは米国連邦政府の基準となるが、その内容は国際的に広く参照されている。多くの企業や教育機関、クラウドサービス事業者が NIST の基準を事実上の業界標準として採用しており、今回の改訂も世界的な認証ポリシーの見直しに影響を及ぼす可能性がある。

初出：2025 年 10 月 17 日

著者：後藤大地, ITmedia

<https://www.itmedia.co.jp/enterprise/articles/2510/17/news027.html>

NIST が禁じたパスワード慣行、いまだ多数派 要件に逆行する企業の現実

アークティックウルフジャパンは年次セキュリティレポートの2025年版を公開した。同調査では、多くの企業がNISTの定める強力なパスワードポリシーと逆行している実態や、日本企業特有のセキュリティホールが存在が明らかになった。

アークティックウルフジャパンは2025年10月22日、年次セキュリティレポート「人的リスクレポート」の2025年版を公開した。

同報告書は、日本を含めた世界の1700人以上のITリーダーやエンドユーザー（管理職）を対象に2025年7月に実施したものだ。回答者が所属する業界としては、製造業や金融サービス、テクノロジーなどが多くを占めている。企業規模としては40%が従業員数50～499人、そして約30%が500～2999人、28%が3000人以上となっている。なお、日本の回答者は75人だった。



Arctic Wolf のリサ・テトロロー氏（Security Services 担当シニア・バイス・プレジデント）

同日に開催された説明会では、Arctic Wolf のリサ・テトロロー氏（Security Services 担当シニア・バイス・プレジデント）が調査結果について詳細に解説し、日本企業のセキュリティ課題とその背景にあるものを浮き彫りにした。

NIST のパスワード新要件に対応できていない企業が多数を占める実態

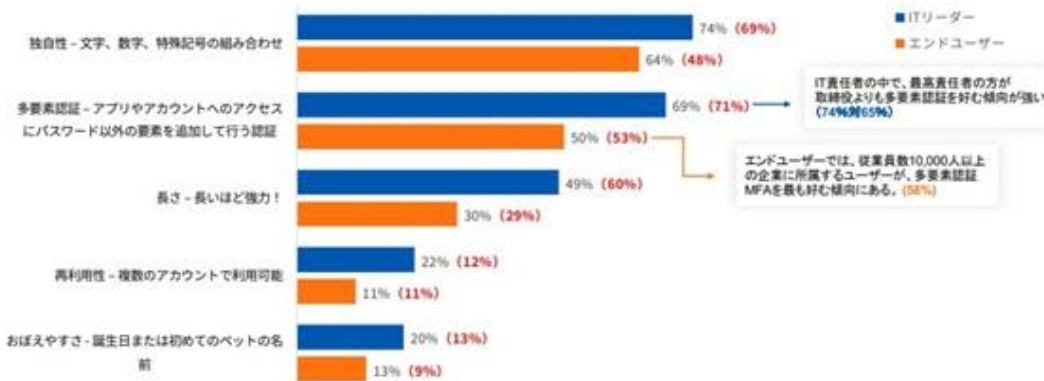
今回注目すべきはパスワードに関連した調査だ。「強力なパスワードの条件」について聞いたところ、「独自性（文字や数字、特殊記号の組み合わせ）」「多要素認証（MFA）」「長さ」が上位に挙がった。

独自性についてはITリーダーが74%（日本では69%）、エンドユーザーが64%（日本では48%）。MFAについてはITリーダーが69%（日本では71%）、エンドユーザーが50%（日本では53%）。長さについては、ITリーダーが49%（日本では60%）、エンドユーザーが30%（日本では29%）となった。

強力なパスワードの特徴

日本での数字は赤で表示

ITリーダー（74%（日本では69%））とエンドユーザーの5人中3人以上（64%（日本では48%））が、強力なパスワードの優れた特性として「独自性」を挙げています。多要素認証が2番目に優れた特性と見なされており、IT責任者の69%（日本では71%）がこれを選択しています。



Q1. 強力なパスワードの条件として、以下のうち該当するものすべてを選択してください

© 2019 Arcus Global Research Inc. All rights reserved. Page 10

対象: 300名のIT責任者、300名のエンドユーザー | 25

強力なパスワードの条件（出典：アークティックウルフジャパン提供資料）

米国国立標準技術研究所（NIST）は最近、パスワードポリシーに関するガイドライン「NIST Special Publication 800-63B」（以下、SP800-63B-4）を[更新](#)し、大文字と小文字、数字、記号を組み合わせた「混在ルールを課してはならない」と明確に定義し、特定の文字タイプを強制する慣行を禁止した。形式的な複雑性が安全性につながらず、むしろ利用者に予測可能なパターンを選ばせてしまう傾向があるためだ。

一方で今回の調査結果は、多くの企業の間でこうした混在ルールが依然として有効であるという誤解が解けていないことを示唆している。なお、同 NIST のガイドラインはパスワードの長さについても言及しており、パスワードのみでの単一要素認証の場合、最低 15 文字を義務付けている。調査ではグローバルと比較して日本の回答者はパスワードの長さを重視しており、良い傾向だといえるだろう。

この他、パスワード共有については日本ではより慎重な傾向が顕著だ。世界では 40% の IT リーダーが「同僚や家族とパスワードを共有したことがある」と答えたのに対し、日本ではわずか 13%。エンドユーザーも 36%（グローバル）に対し、日本は 15%にとどまった。

では日本のセキュリティ意識が高いかといわれるとそうともいえない。

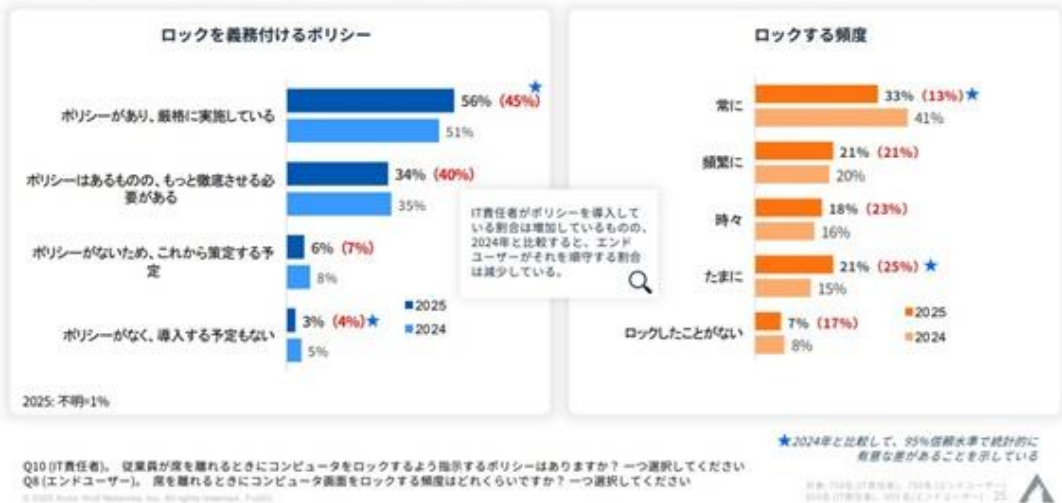
日常的なセキュリティ対策については日本とグローバルで大きな差が出た。IT リーダーの 90%（日本では 85%）が「従業員が席を離れるときに PC をロックするように指示するポリシーがある」と回答した。一方で「席を離れるときに PC をロックするか」という質問では、グローバルでは 33%のエンドユーザーが「常にロックしている」と答

えたのに対し、日本ではわずか 13% だった。テトロー氏はこの背景に「文化的な信頼の深さ」があると分析する。

席を離れる時にコンピュータをロックするか

日本での数字は赤で表示

ITリーダーの90%（日本では85%）が、従業員が席を離れるときにコンピュータをロックするよう指示するポリシーがあると回答しているものの、常にロックしていると回答したのはエンドユーザーの33%（日本では13%）のみにとどまる



席を離れるときに PC をロックするかどうか（出典：アークティックウルフジャパン提供資料）

「日本社会は信頼関係が非常に強固です。カフェで席を確保するためにスマートフォンやバッグを机に置く行為は、他国では考えられません。特に西洋文化圏では、そんなことをしたならテーブルに戻ったら持ち物が持ち去られているでしょう。そうした文化が「油断」としてセキュリティ意識にも影響しているとみられます」（テトロー氏）

一方でテトロー氏は「信頼は日本の強みでもある」としつつ、「職場では個人の信頼よりも、仕組みとしての防御策を優先すべきです」と強調した

セキュリティ意識が高い方が、生成 AI に機密情報を共有する？

この他、調査によると、グローバル平均では IT リーダーの約 3 分の 2、エンドユーザーの約半数が「悪意あるリンクをクリックした経験がある」と回答している。さらに、リンクを誤ってクリックした IT リーダーのうち 5 人に 1 人が「その事実を報告していない」ことも判明した。

一方で日本では、リンクをクリックした経験を持つのは IT リーダーで 38%、エンドユーザーで 36% と、グローバル平均よりも低い結果になった。ここから日本の従業員は比較的慎重である傾向が見られるが、これは「安心してよい」という意味ではない。また、フィッシング被害に遭わない自信の有無を尋ねた質問では、グローバルの 76% が「自信がある」と答えたのに対し、日本では 43% にとどまった。

従業員の努力だけではフィッシング被害を完全に防ぐのは困難である中、企業側としては被害に遭った従業員が迅速かつ事態を隠ぺいせずに被害報告を上げられる風土や仕組みを整えることが重要だろう。

また、同調査では「ChatGPT」などの生成 AI ツール利用に潜むリスクについても取り上げている。IT リーダーの 87%（日本では 84%）、エンドユーザーの 63%（日本では 52%）が業務で生成 AI ツールを使用している。この結果は前回調査と比較しても増加傾向にあるが、その使い方には注意も必要だ。

IT リーダーの 60%（日本では 51%）、エンドユーザーの 41%（日本では 46%）が「ChatGPT などの大規模言語モデル（LLM）に機密情報を共有したことがある」と答えていることが分かった。

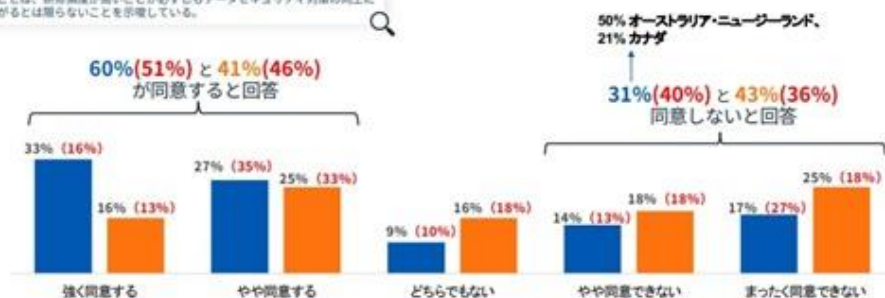
LLMに機密情報を共有

日本での数字は赤で表示

ITリーダーはLLM（大規模言語モデル）に機密情報を共有する傾向が強く、利用経験者の5人に3人（60%）が共有を認めている一方で、エンドユーザーでは41%（日本では46%）でした。

「ChatGPTなどのLLMで機密情報を共有したことがある」

毎週セキュリティ意識向上研修を受けている人は、LLM（大規模言語モデル）で機密情報を共有したと報告する割合が高い（85%対73%）。
その一方で、年1回以下しか研修を受けない人の割合は低い（34%対21%）。
このことは、研修頻度が高いことが必ずしもデータセキュリティ対策の向上につながるとは限らないことを示唆している。



Q4a. 「私はChatGPTなどのLLMで機密情報を共有したことがある」ことにどの程度同意しますか？1つ選択してください

© 2023 Arc42 Inc. All rights reserved. Privacy

※本調査は、2023年11月14日～15日に行われた調査結果に基づいています。



ChatGPT などの LLM に機密情報を共有したことがあるかどうか（出典：アークティックウルフジャパン提供資料）

これは従業員向けの AI 利用ポリシーに関する研修を実施することで解決できると考える人もいるかもしれない。しかし調査からは意外な結果も明らかになった。毎週セキュリティ意識向上研修を受けている人は「LLM に機密情報を共有した」と報告する割合が高い傾向が分かった（グローバルで 85%、日本では 73%）。一方で年に 1 回以下しか研修を受けない人の割合はグローバルで 34%、日本では 21%と低い結果になった。

研修頻度が高いことが必ずしもセキュリティやガバナンスの向上に結び付くわけではないというのは興味深い調査結果だ。

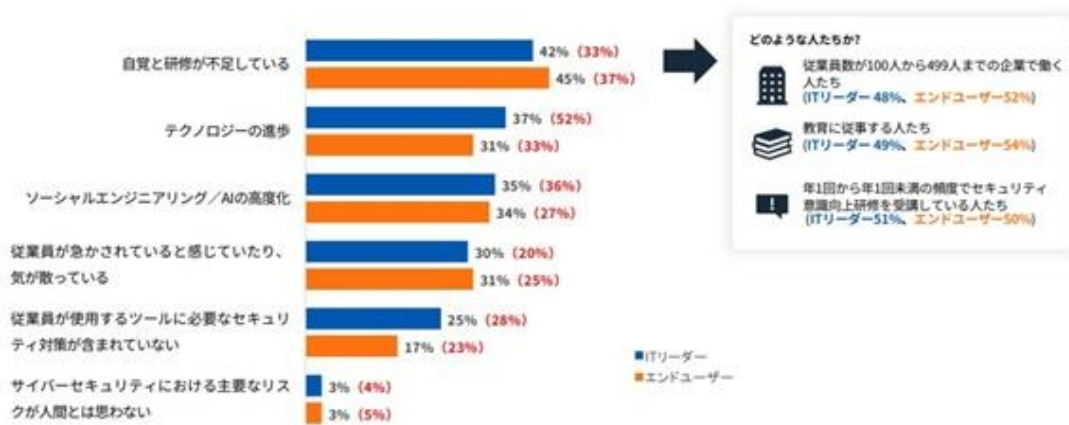
さすがにやりすぎ？ 詐欺被害に遭った従業員を解雇するケースも

調査では、多くの企業がセキュリティにおいて人間が主要なリスクになると考えていることも分かった。97%（日本では96%）のITリーダーが人間を主要なセキュリティリスクと認識しており、その理由として「自覚と研修の不足」を挙げた。

サイバーセキュリティにおいて人間が主要なリスクとなる理由

日本での数字は赤で表示

97%のITリーダーとエンドユーザー（日本では96%/95%）が人間を主要なリスクと認識しており、その最大の理由は自覚と研修が不足していることです



Q19 (IT責任者)/Q13 (エンドユーザー)。サイバーセキュリティにおいて人間が主要なリスクとなる理由は何ですか？上位2つを選択してください

© 2025 Arc42 All Rights Reserved. Japan

対象: 300名 (IT責任者) / 300名 (エンドユーザー) 25

サイバーセキュリティにおいて人間が主要なリスクとなる理由（出典：アークティックウルフジャパン提供資料）

興味深いのは、ITリーダー自身もセキュリティ対策を「無効化」するケースがあることだ。ITリーダーの51%（日本では43%）が「自社のシステムでセキュリティ対策を無効化した経験がある」と回答した。理由として最も多かったのは「対策が効率的な業務の妨げになっている」（グローバルで25%《日本で28%》）だった。これはまさに「人間こそがセキュリティリスクである」という懸念を裏付ける結果といえるだろう。

こうした人間起因のセキュリティリスクにどう対処すればいいか。調査からは極端な措置を講じる企業も確認された。「フィッシング詐欺などの被害に遭った従業員を解雇したことがあるか」という質問に対して、ITリーダーの58%（日本では45%）が「従業員が詐欺被害に遭ったことを理由に解雇したことがある」あるいは「非常に強い是正措置を講じた」と答えた。

調査によると、オーストラリアやニュージーランドの企業（74%）または、金融サービスに携わる企業（67%）はその傾向が強いことが明らかになっている。一方で「被害に遭った従業員に解雇以外の何かしらの是正措置を講じたかどうか」という問いでは、日本のITリーダーは「従業員のアクセス権限を変更あるいは制限した」（61%）や、「再

教育」(64%)といった対策を講じており、その多くが「一定の効果があった」としている。

テトロ氏には最後に「従業員への啓発やエンドポイントセキュリティの強化、定期的なインシデントレスポンス計画の見直しは非常に重要です。かつ被害に遭った従業員が安全な気持ちで報告できる環境や文化を構築することも忘れてはいけない」と締めくくった

初出：2025 年 10 月 24 日

著者：田淵聖人, ITmedia

<https://www.itmedia.co.jp/enterprise/articles/2510/24/news045.html>

