特集

NISTの新しいパスワードルールブック

更新版ガイドラインによる、メリットとリスクがあります

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

NIST Special Publication (SP) 800-63-3「デジタルアイデンティティガイドライン」[1]に掲載されているパスワードセキュリティに関する米国国立標準技術研究所 (NIST) の更新された基準は、情報セキュリティにおける最も弱いリンクの能力と限界、すなわちユーザー自身に対するものではなく、それらと共に機能するITセキュリティを向上させるための新しいアプローチです。更新版NISTのガイドラインは、ユーザビリティとセキュリティの面で多くのメリットをもたらします。また、一方で、新たなリスクと導入上の課題が発生します。これらの問題は、新しいガイドラインの導入前、導入中および導入後に慎重に検討する必要があります。

新しいガイドラインの概要

従来のNISTのガイドラインでは、厳格な複雑性ルール、定期的なパスワードのリセット、パスワードの再利用制限などのポリシーに基づいて、パスワードセキュリティに対する従来のアプローチを提唱していました。[2] NISTの新しい基準は根本的に異なるアプローチを採用しています。[3] 例えば、セキュリティ侵害の証拠がない限り、パスワードの変更は必要ありません。厳格な複雑性ルールは、構造の柔軟性、文字種類の拡大、長さの延長、および「悪い」（すなわち安全でない）パスワードの禁止に置き換わっています。NISTの新しいガイドラインは、ユーザーが不満を感じることが少ないパスワードベースの認証、ITリソースへのアクセスをより効果的に保護する可能性がありますが、トレードオフがあります。

更新版NIST SP 800-63-3ガイドラインのパスワード要件の基本は次のとおりです：[4]

- **長さ** - 8～64文字を推奨します。
- **文字タイプ** - 可能であれば、絵文字などの非標準文字も使用できます。
- **構造** - 長いパスフレーズを推奨します。禁止されているパスワード辞書の掲載項目と一致しないようにしてください。
- **リセット** - パスワードが漏洩または忘れた場合にのみ必要です。
- **マルチファクタ** - 最も機密性が低いアプリケーションを除き、すべてのアプリケーションに推奨されます。

Bachman Fulmer 博士 (CISA)
タンパ大学（米国フロリダ州）会計学の准教授です。EYの技術リスクおよび保証サービス部門で、技術、コンプライアンス、ビジネスプロセス改善に重点を置く内部監査人として従事していました。

Melissa Walters 博士
タンパ大学会計学の准教授です。システム導入、コントロールおよびサポート分野で勤務し、情報システムとそのコントロール/監査を教えています。

Bill Arnold (CISSP)
タンパ大学の情報セキュリティ担当理事であり、情報セキュリティ計画、導入、評価および管理の分野で活動している情報セキュリティアナリストです。

ユーザーの観点からのメリットおよびリスク

更新版NISTのパスワードガイドラインは、意図したパスワード保護を損なうような人的要因に対処することで、セキュリティを強化するように設計されています。従来のパスワード構築手法では、ユーザーは非常に複雑で推測が困難なパスワードを生成するよう求められます。これらのパスワードは定期的にリセットする必要があり、一般的にユーザーはパスワードを連続して再使用することはできません。また、複数のITシステムで同じまたは類似のパスワードを使用することを控えるように指示されます。すべてのユーザーが知っているように、これにより、パスワードを記憶することが非常に困難になります。他方で、悪意の無い個人が、アドバイスを無視して、より覚えやすいパスワード、以前に使用したパスワードの再使用、リセット間の変更を最小限にする、他の労力を最小限にする方法により、これらの問題に対処しがちです。[5] また、パスワードを書き留めて便利だけれども安全でない場所に掲示してしまうユーザーもいます。[6]

新しいガイドラインの下では、ユーザーはランダムな文字列よりも一貫性のあるフレーズを覚える方が簡単なため、複雑な構造規則を持つ分かりにくい文字列ではなく、より長く思い出しやすいパスフレーズを選択することが推奨されます。同様の論理により、ユーザーにとって意味があり、覚えやすいフレーズに基づく頭字語を介して安全なパスワードを生成する従来のアドバイス（例えば、「Robert has been a Spartans fan since 2010!」というフレーズの各単語の最初の文字を使用すると、「RhbaSfs2010!」が生成されます）につながりました。[7] この12文字の略語は、一般的に厳密なパスワードの作成要件を満たし、安全なセキュリティを提供します。しかし、新しいNIST標準では頭字語だけでなく、パスフレーズ全体の使用を推奨しています。44文字の元のフレーズは、12文字の頭文字よりもはるかに暗号化が強化されますが、ユーザーにとっては覚えやすいです。**図1**は、NISTのパスワードアプローチと従来のパスワードアプローチを比較したものです。

> 新しいガイドラインの下では、複雑な構造規則を持つ分かりにくい文字列ではなく、より長く思い出しやすいパスフレーズを選択することが推奨されています。

新しいガイドラインでは、ユーザーに安全なパスワードに関する概念を変更させることなく、柔軟性とセキュリティを強化しています。NISTガイドラインはより長いパスフレーズの使用を促進・推奨しますが、このガイドラインに基づいて唯一必

図1 - パスワード更新

NISTのパスワード	従来のパスワード
長く思い出しやすいパスフレーズが推奨されます。 例：「NIST passphrases make long passwords easy!（NISTのパスフレーズにより、パスワードを長くすることが容易になります！）」 例：「I really look forward to spring weather in Upstate New York.（「ニューヨーク州北部の春が本当に楽しみです。）」	長くなるとより複雑になるため、障害と見なされます。 例：「[z2#DSGDnr=[6y@g<q{@」 思い出しやすいパスワードは、簡単に推測されます。 例：「P@$$wORD」
問題のあるパスワードは、辞書により拒否されます。 例：「123456」または「qwerty」などの一般的なパスワード、および、マスコットまたはチーム名などの地域に関連したパスワード	厳密な構造規則によって、許容される選択が導かれます。 例：大文字および小文字、数字、句読点、またはこれらを組み合わせた最低8文字。
マルチファクタ認証は、セキュリティの特別の層を提供します （例えば、モバイルアプリケーション/ソフトウェアトークン、ハードウェアトークン、バイオメトリクス、キーフォブ）。	

Enjoying this article?

- Read *Implementing the NIST Cybersecurity Framework. www.isaca.org/US-cyber-implementation*
- Learn more about, discuss and collaborate on information and cybersecurity ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

要な制限は、パスワードの長さが8文字以上であることです。そのため、ユーザーは、従来の複雑なルールで慣れ親しんだものとかなり異なるパスワードを実際に作成する必要はありません。パスワードまたはパスフレーズが十分な長さであり、禁止されたパスワードの辞書にないものにする必要があります。

> 「また、NISTのガイドラインは、機密性が最も低いアプリケーション以外はすべて、マルチファクタ認証を推奨しています。」

また、ユーザーには、あらかじめ定義されたスケジュールでパスワードを変更する必要がないというメリットがあります。定期的にパスワードを変更することで、セキュリティが侵害されたパスワードをある期間を超えて使用することを防止できますが、新しいパスワードを継続して生成し、覚えておく必要があるという問題がユーザーに発生します。ユーザーは、パスワードを少し変更する（例えば、1文字の追加または置き換えなど）だけで補完する場合がありますが、これではポリシーの目的が損なわれています。特定アカウントのセキュリティが侵害されたと思う理由またはシステム侵害の証拠がない限り、ユーザーが強制的にパスワードを定期的に変更しなければならないことによる労力は、もたらされるメリットを上回る可能性があります。[8] これに対応して、NISTの新しいガイドラインでは、設定されたスケジュールで強制的にリセットするのではなく、疑わしい脅威がある場合にのみ、パスワードのリセットを推奨しています。

更新版ガイドラインにより、ユーザーはさまざまな方法で安全なパスワードを簡単に実行できるようになる一方で、問題や困りごとが発生する可能性もあります。例えば、NISTのガイドラインでは、特別なリストに基づいて、一般的に使用されるパスワードや安全でないパスワードが拒否される辞書検証ステップが必要になります。特定の構造規則または禁止リスト自体への透明性がない場合、連続的に拒否されると、ユーザーが不満を感じる可能性があります。更に、一部のユーザーにとっては、禁止リストに掲載されているため、希望のパスワードが受け入れられなかったというメッセージを単に表示させるだけでは、後の試行を成功させるのに十分な情報ではない可能性があります。ユーザーがセキュリティを強化する機会を十分に活用するには、対象となるトレーニングとサポートが必要な場合があります。少なくとも、新しいNISTのガイドラインの下で受け入れ可能なパスワードを選択する方法に関する基本的なガイダンスがユーザーには必要です。そうでない場合、ユーザーがプロセスに不満を感じる可能性があります。[9]

残存する脅威は、攻撃者が公開情報源からの個人情報を使用したり、ソーシャルエンジニアリング技術を採用して信用情報を推測したりするインテリジェントな能力です。パスフレーズの例「Robert has been a Spartans fan since 2010!」は、次のように良いパスワードとしての多くの特徴を有しています。ユーザーが覚えやすく、十分に長く、さまざまな文字タイプが含まれています。しかし、ユーザーが、Facebook（または他のソーシャルメディア）上に大学の所属、学校スポーツの興味、卒業日を投稿している場合、刺激された攻撃者は、この種の個人情報を簡単に収集・使用して、パスワードの推測が成功するまでの経路を短縮することができます。このタイプの脆弱性は、NISTのガイドラインに固有のものではありませんが、パスワードの構造に柔軟性を持たせることで、この弱点をより深刻な問題にする可能性があります。

セキュリティ専門家の観点からのメリットおよびリスク

セキュリティ専門家は、パスワードを推測しにくくするように設計された既存のガイドラインは、しばしば誤ったセキュリティ感覚を提供することを十分に認識しています。「Pa$$w0Rd12」は、従来の構造要件を満たしますが、攻撃者の標準ツールセットで推測される最初のパスワード群に含まれます。[10] NIST SP 800-63-3のガイドラインでは、ユーザーがセキュリティ上よくない決定を下すのを促す要因の

いくつかに対処することで、ユーザー自身が通常セキュリティの最も弱いリンクであるという事実が反映されています。このように、更新版NISTのガイドラインでは、情報セキュリティ専門家が、ユーザーの負担を増やすことなく、認証の安全性を高める手助けができる可能性があります。

暗号方式による複数の文字タイプを持つ長いパスワードはより安全ですが、従来の構造ガイドラインでは一般的に、複雑で長いパスワードを覚えるのが難しく、ユーザーがより安全なパスワードを作成することを妨げる可能性があります。[11] 従来システムの中には、パスワードの長さや、シンプルさのために文字種類を制限して、ユーザーに安全性の低いパスワードを強制するものもあります。[12] NISTは、少なくとも64文字以上のフレーズを許可し、扱いにくい複雑さのルールを強制することなく、より強力なパスワードを奨励するために、空白、句読点、さらには絵文字（可能な場合）などの非標準文字を含む拡張文字セットを受け入れるようにシステムを構成することを推奨しています。

また、NISTのガイドラインは、機密性が最も低いアプリケーション以外はすべて、マルチファクタ認証を推奨しています。新しいNISTガイドラインの他の側面と同様に、マルチファクタ認証は、ユーザーに対する影響を最小限に抑えながら、セキュリティを大幅に向上させることができます。バイオメトリクス、スマートフォン対応アプリケーション、キーフォブ、暗号化キーなど、マルチファクタ認証は、ユーザーに負担をかけることなく、認証セキュリティにおける第2の強力な防衛線を提供します。[13]

新しいガイドラインには大きなメリットがありますが、セキュリティ専門家は、これらのガイドラインを導入する上でのトレードオフを注意深く検討すべきであり、安全な認証のための簡単なソリューションを期待してはいけません。例えば、NIST SP 800-63-3のガイドラインで強化されたセキュリティの多くは、ユーザーがより長いパスワードを簡単に採用できるようにすることによりますが、実際には通常のパスワードの取り扱いを変更する必要はありません。ある個人は、8文字の英文字（または数字）の短いパスワードを作成する可能性があります。パスワードが禁止パスワードリストにより制限されない場合、ユーザーは、より簡単なパスワードを選択することが考えられ、そうすると従来の複雑性ルールでは解読されてしまいます。

禁止パスワード辞書は、NISTのガイドラインで提供されるセキュリティ強化の中心であり、セキュリティ専門家による特別な注意が必要です。重要な考慮点は、NISTは特定の禁止パスワードリストを規定していないので、導入者は自分自身で採用、展開、維持しなければなりません。専門的に管理された不正なパスフレーズ辞書を提供する数多くの商業サービスに加えて、Github[14]には「SecLists」のようなセキュリティが侵害されたパスワードおよび一般的に使用されるパスワードのオープンソースのリポジトリがあります。SecListsに基づくパスワード検証ツールの例、「NIST Bad Passwords」は、Github[15]で利用可能であり、辞書の導入に興味のあるユーザーのための概念の証明として評価することができます。しかし、問題のあるコンテキスト固有のパスワードに対処するようには設計されていないため、このようなリストは限られた用途しかありません。

> 「各組織は、合理的なユーザーおよび組織固有のパスワード制限を組み込み、定期的に再点検するための方針と手順を策定する必要があります。」

コンテキスト固有のパスワードを適切に制限することは、特に難しい課題です。例えば、ユーザー自身のユーザー名、ウェブサイト名、関連する組織名または他の関連する用語を含むと、関連するシステム上でユーザーを認証する際の安全性が低下します。大学のシステムを保護するという状況において、大学の名前、そのマスコット、またはその派生語をパスフレーズに含めると、攻撃者の推測がより簡単になる可能性があります。禁止パスワード辞書を慎重に構築すると、このリスクの一部が軽減される可能性があります。例えば、大学のマスコットが

Spartanである場合、この単語と関連する派生語を禁止辞書に追加することが賢明でしょう。結局、大学の卒業生は、所属はユーザーの個人的なアイデンティティーの重要な部分であることに変わりはないのに、同じ言葉を制限する明確な理由がない他の組織に加わることになります。したがって、一般的な辞書アプローチは、個々のユーザーに関連する容易に識別可能な所属および嗜好のすべてを合理的にブロックすることはできません。また、必ずしも良い考えとは言えません。あるユーザーにとっては容易に推測される種類の言葉は、別のユーザーにとっては、あいまいで比較的安全な選択である場合があります。

> 更新版NIST SP 800-63-3パスワードガイドラインは、すべての組織がユーザー認証ポリシーと実践を最新式にする機会を提案しています。

これらのタイプの「ローカル脆弱性」を標準辞書が処理できないため、これは重要な問題です。各組織は、合理的なユーザーおよび組織固有のパスワード制限を組み込み、定期的に再点検するための方針と手順を策定する必要があります。システムや組織が進化するにつれて、制限されるべきキーワードの種類やその他の関連情報が変化する可能性があり、新しい脅威に対する保護を追跡・実装するプロセスが必要になります。更に、セキュリティの侵害が発生した場合、侵害されたパスワードを速やかに禁止リストに追加する必要があります。[16] これらの追加制限を取り入れることは、NISTのパスワードガイドラインを導入する際に、技術的に最も困難でプロセス集中的な側面であると考えられます。

いずれにしても、NIST SP 800-63-3のガイドラインでは、禁止パスワード辞書によりブロックされているもの以外の安全でないパスワードの発見的問題解決法をユーザーが使用することを防止する必要があることが明確になっています。例えば、ユーザーは、繰り返しまたは連続した文字を使用することを許可すべきではありません。[17] これらの追加のパスワード構造の危険性は、辞書に潜在的に含まれる可能性がありますが、プログラムで導入する方が簡単かもしれません。

NISTのガイドラインでは、計画された義務的なパスワードのリセットを避ける代わりに、セキュリティの侵害の疑いがある場合にのみパスワードのリセットを要求しています。定期的なパスワードのリセットは、セキュリティが侵害されたアカウントに、システムがさらされる可能性のある期間を制限するために使用されます。[18] 実際は侵害されているという仮定の下でのみセキュリティを追加します。不要なパスワードのリセットは、ユーザーを苛立たせるだけでなく、管理者やサポート担当者の作業を増やします。パスワード変更が不要な場合、不正アクセスの脅威を迅速に処理できるように、侵害されたアカウントや侵害された可能性があるアカウントを特定するために、システム管理者がユーザーの活動を効果的に監視するためのツールとリソースを持つことが重要です。NISTガイドラインのこの側面には、注意深い考慮が必要です。セキュリティ専門家は、侵害監視およびパスワードリセットに関して、理にかなった判断を下すために、彼らのシステム、ユーザーおよび彼らが守る情報に関するリスクのプロファイルを知る必要があります。

結論

更新版NIST SP 800-63-3パスワードガイドラインは、すべての組織がユーザー認証ポリシーと実践を最新式にする機会を提案しています。多くの米国政府関連機関は、NISTの推奨を導入する必要がありますが、いずれの組織も基準に記載されている更新版のガイダンスを（全部または一部）自由に採用することができます。[19]

パスワードは、長期にわたり、ユーザーとセキュリティ専門家の両方にとって悩みの種でした。NISTのガイドラインは、パスワードの多くの問題点に対処する一方で、システムセキュリティの最も弱いリンク（ユーザー自身）を考慮して、セキュリティの実践を強化することを推奨しています。しかし、NIST SP 800-63-3ガイドラインを採用したか、または採

用しようとしている組織は、認証セキュリティ手順の変更の根拠とメカニズムについて十分に理解していることを確認する必要があります。また、NISTガイドラインのメリットの可能性だけではなく、従来のパスワードポリシーと比較して、新しいセキュリティガイドラインにより直接記述されていないユーザーセキュリティに対する残存リスクについても認識する必要があります。また、組織は、NISTのガイドラインに基づいてセキュリティを強化するための中心である、禁止パスワード辞書の開発と維持の課題および新しい規則にユーザーが適応するために必要な変更管理への投資の可能性を考慮する必要があります。

注釈

1 国立標準技術研究所 (NIST)、「Digital Identity Guidelines（デジタルアイデンティティガイドライン）」、NIST Special Publication (SP) 800-63-3、USA、2017年6月、*https://csrc.nist.gov/publications/detail/sp/800-63/3/final*

2 McMillan, R.、「The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1-d!（それらのパスワードルールを書いた人は新しいヒントを持っています：N3v$r M1-d!）」*ウォールストリートジャーナル*、2017年8月7日、*https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118*

3 リスクコントロール戦略、「The New NIST Guidelines: We Had It All Wrong Before（新しいNISTのガイドライン：我々はすべて間違っていた）」、2018年1月8日、*https://www.riskcontrolstrategies.com/2018/01/08/new-nist-guidelines-wrong/*

4 *前掲論文*NIST

5 *前掲論文*McMillan

6 Culp, S.、「The Ten Immutable Laws of Security（セキュリティの10の不変の法則）」、Microsoft Corporation、2003年、*www.wciapool.org/pdf/Tab_5_10Immutable_LawsofSecurity.pdf*

7 米国コンピュータ緊急対応チーム、「Security Tip（セキュリティのヒント）」、(ST04-002)、2009年5月21日、*https://www.us-cert.gov/ncas/tips/ST04-002*

8 Cranor, L.、「Time to Rethink Mandatory Password Changes（強制的なパスワード変更を再考する時）」、Federal Trade Commission、USA、2016年3月2日、*https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes*

9 Meyer, T.、「Training Your Users to Use Passphrases（パスフレーズを使用するようにユーザーをトレーニングする）」、*Medium.com*、2018年5月18日、*https://medium.com/@toritxtornado/training-your-users-to-use-passphrases-2a42fd69e141*

10 Mitchell, W.、「Password Cracking（パスワードクラッキング）」、*Web.cs.du.edu*、2018年、*http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html*

11 *前掲論文*McMillan

12 GNU C Library、「DES Encryption and Password Handling（DES暗号化とパスワード処理）」、2018年、*https://ftp.gnu.org/old-gnu/Manuals/glibc-2.2.3/html_chapter/libc_32.html#SEC661*

13 De Cristofaro, E.、H. Du、J. Freudiger、G. Norcie、「A Comparative Usability Study of Two-Factor Authentication（2ファクタ認証の比較可能性の検討）」、2013年、*https://arxiv.org/abs/1309.5344*

14 danielmiessler、「SecLists」、GitHub、*https://github.com/danielmiessler/SecLists/tree/master/Passwords*

15 Li, C.、「NIST Bad Passwords（NISTの悪いパスワード）」、2018年、*https://cry.github.io/nbp/*

16 *前掲論文*NIST

17 *同上*

18 Henry-Stocker, S.、「Periodic Password Changes—Good or Bad?（定期的なパスワードの変更 - 良い悪い？）」、*Network World*、2016年8月8日、*https://www.networkworld.com/article/3104015/security/periodic-password-changes-good-or-bad.html*

19 ISACA®、*Implementing the NIST Cybersecurity Framework（NISTサイバーセキュリティフレームワークの導入）*、2014年7月、*https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx*