2025年
10月
OCTOBER

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

キヤノンマーケティングジャパン株式会社

はじめに

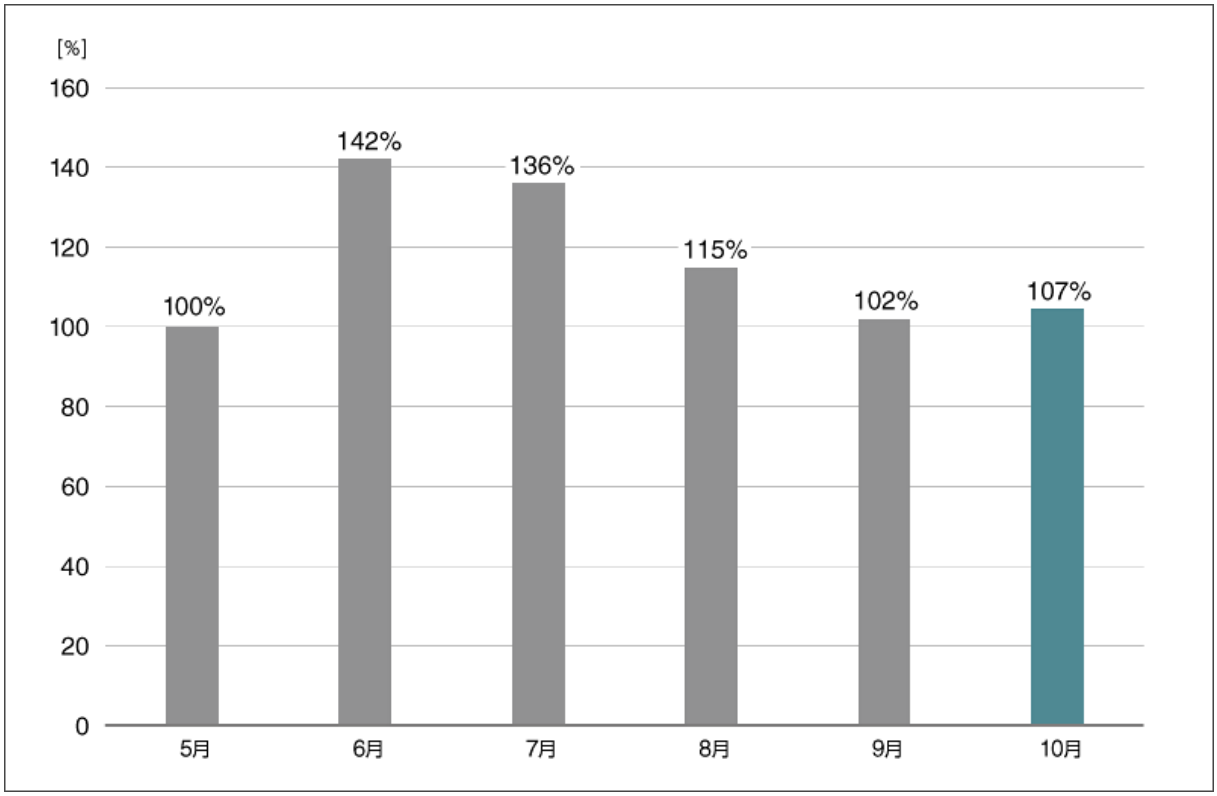
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

2025 年 10 月マルウェア検出状況

2025 年 10 月（10 月 1 日～10 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。



国内マルウェア検出数*1の推移

（2025 年 5 月の全検出数を 100%として比較）

*1 検出数には PUA（Potentially Unwanted/Unsafe Application；必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション）を含めています。

2025 年 10 月の国内マルウェア検出数は、2025 年 9 月と比較して増加しました。検出されたマルウェアの内訳は以下のとおりです。

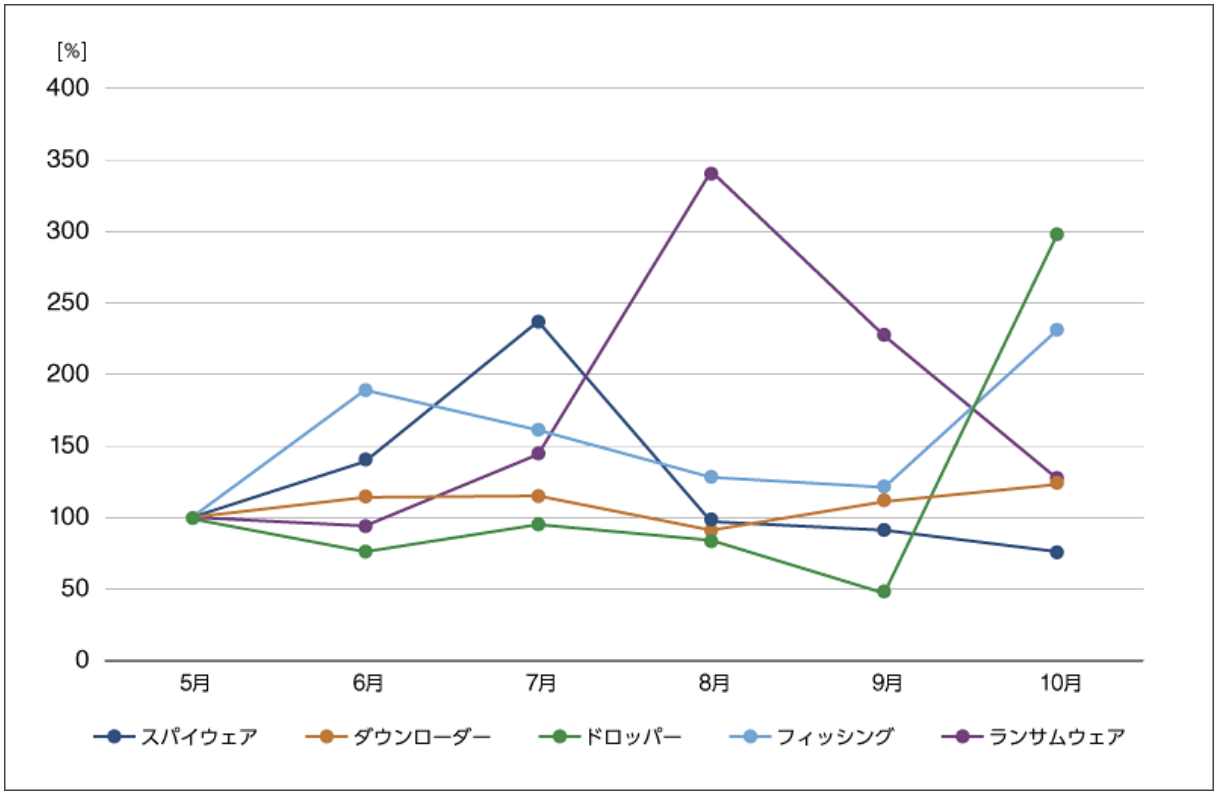
国内マルウェア検出数*2 上位（2025 年 10 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	39.3%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	14.4%	アドウェア
3	DOC/Fraud	9.2%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	HTML/Phishing.Gen	3.4%	フィッシングを目的とした不正な HTML ファイル
5	Win64/Agent	1.4%	不正な実行ファイルの汎用検出名
6	JS/Danger.ScriptAttachment	1.4%	ダウンローダー
7	HTML/Fraud	1.3%	詐欺サイトのリンクが埋め込まれた HTML ファイル
8	JS/Agent	1.3%	不正な JavaScript の汎用検出名
9	HTML/Nomani	1.0%	詐欺を目的とした不正な HTML ファイル
10	JS/Adware.Sculinst	0.6%	アドウェア

*2 本表には PUA を含めていません。

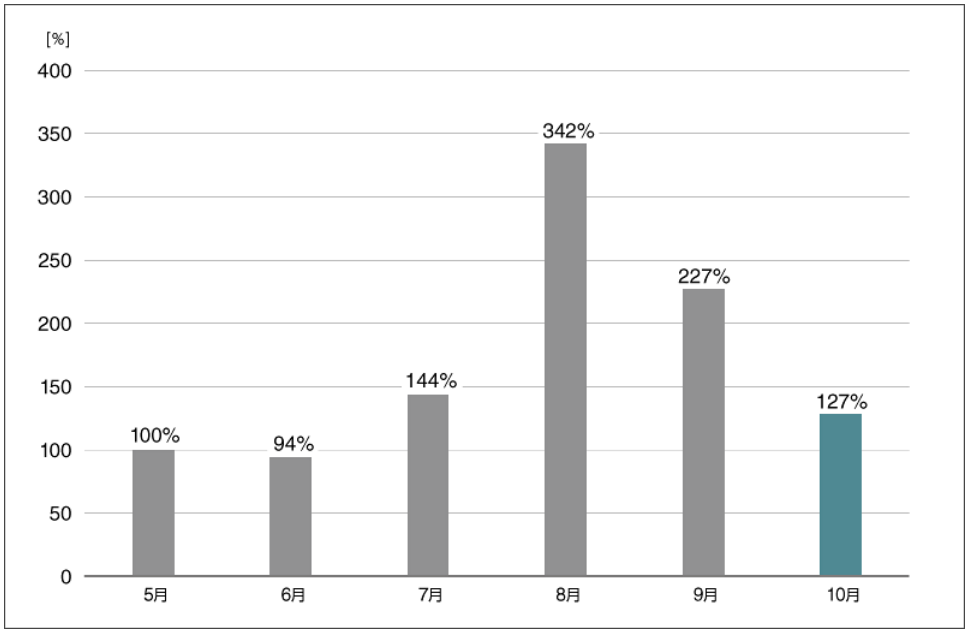
10 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL にアクセスすると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

2025 年 10 月に ESET 製品が国内で検出したマルウェアの種類別の推移は、以下のとおりです。以降のグラフには PUA が含まれています。



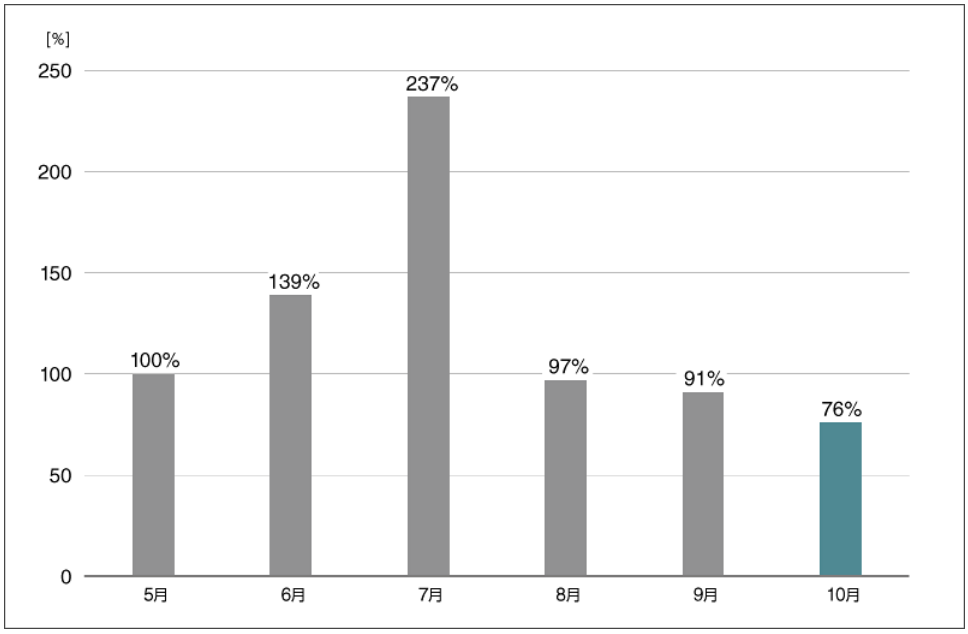
国内マルウェアの種類別検出数の推移
（2025 年 5 月の各検出数を 100%として比較）

2025 年 10 月は 9 月から引き続きランサムウェアの検出数が減少しました。一方、フィッシングやドロッパーの検出数は増加しました。



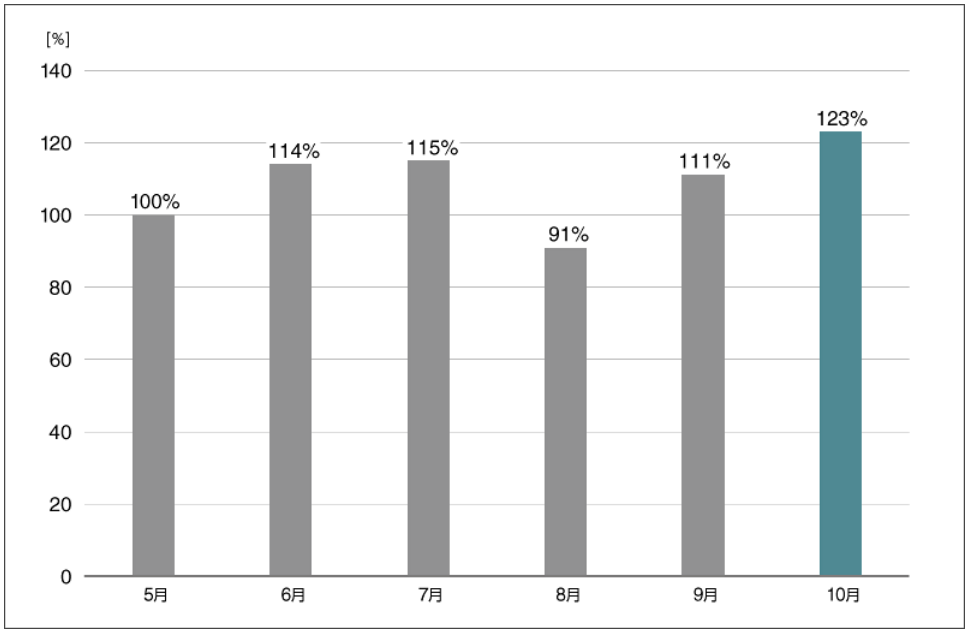
ランサムウェア検出数の推移（国内）

（2025 年 5 月の検出数を 100%として比較）



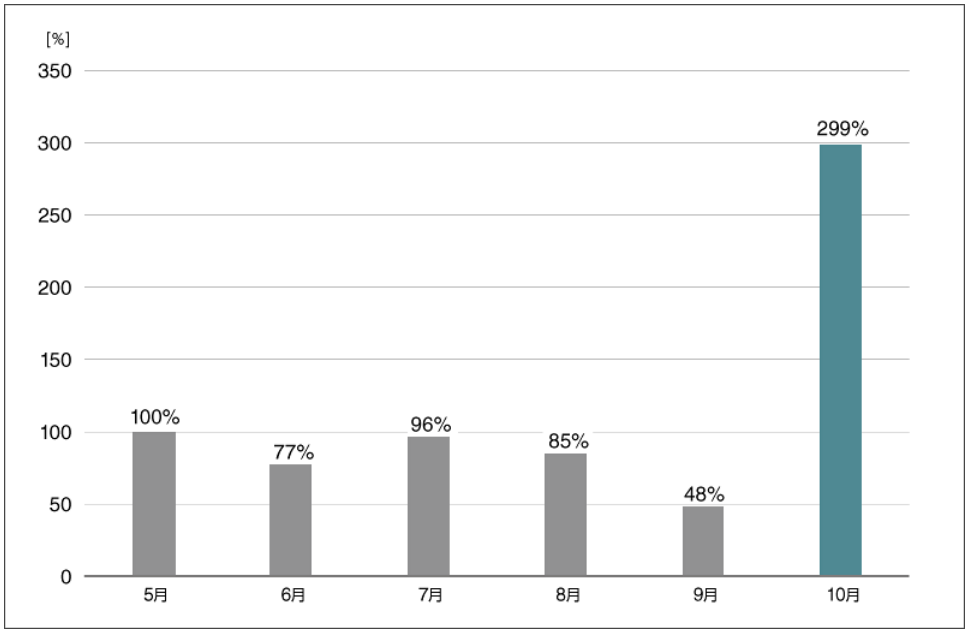
スパイウェア検出数の推移（国内）

（2025 年 5 月の検出数を 100%として比較）



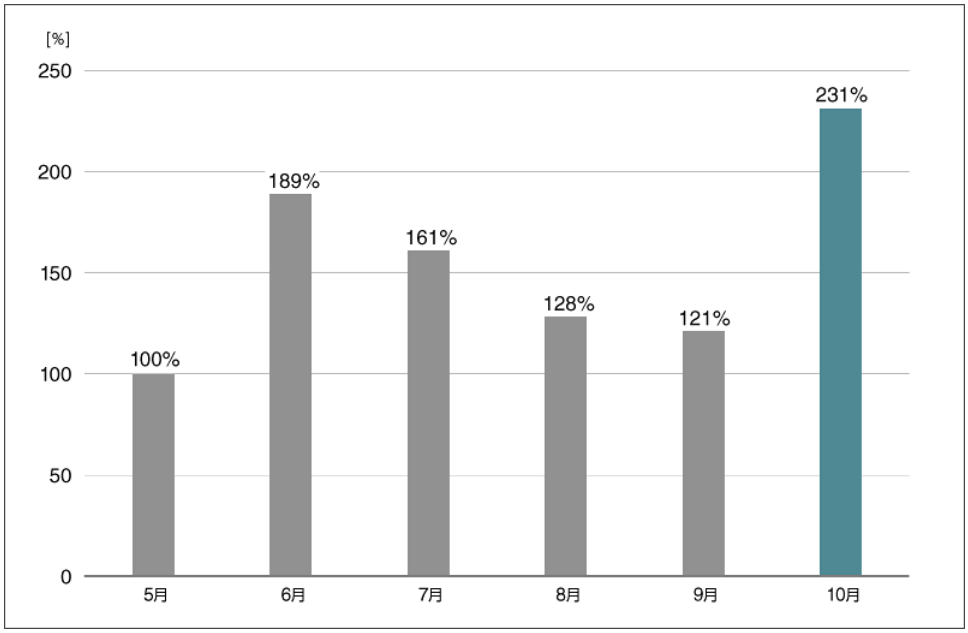
ダウンローダー検出数の推移（国内）

（2025 年 5 月の検出数を 100%として比較）



ドロッパー検出数の推移（国内）

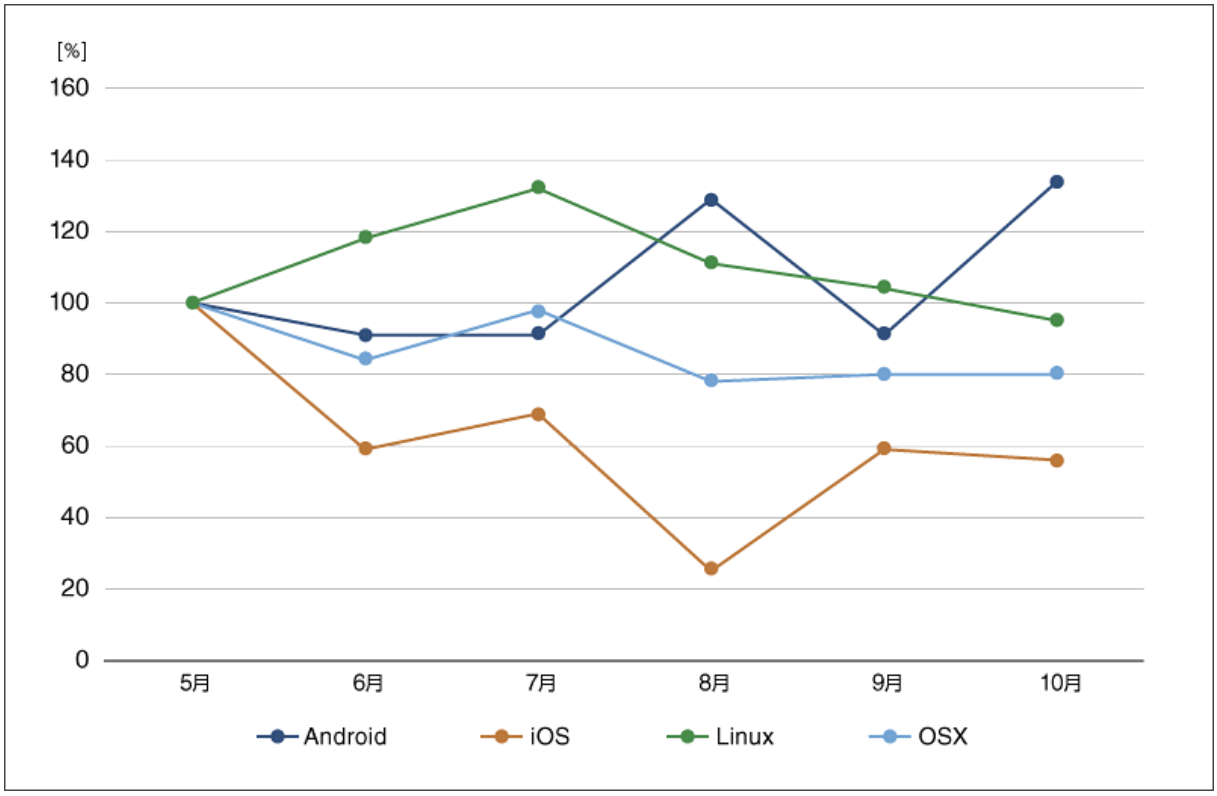
（2025 年 5 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 5 月の検出数を 100%として比較）

2025 年 10 月に ESET 製品が国内で検出したマルウェアの OS 別推移は、以下のとおりです。



国内マルウェアの OS 別検出数の推移（Windows を除く）
（2025 年 5 月の各検出数を 100%として比較）

2025 年 10 月は Android を狙ったマルウェアの検出数が大幅に増加しました。

米国のデジタルアイデンティティに関するガイドラインが更新

2025 年 7 月末に、デジタルアイデンティティに関するガイドラインである SP 800-63B が更新されました。これは NIST（米国標準技術研究所）が制定したデジタルアイデンティティ管理に関する基準です。デジタルアイデンティティ管理とは、「誰が」「どのシステムやデータに」「どんな方法で」アクセスできるのかを制御・証明する技術や運用方法を意味します。
SP 800-63B は今後米国の政府機関のシステムが従うべき基準として扱われるため、米国政府が企業にシステム開発やクラウドサービスを発注する時に要件として求めるケースが増えていくと予想されます。
EU サイバーセキュリティ庁や日本の独立行政法人情報処理推進機構、国家サイバー統括室など、多くの政府機関が、NIST の SP800 系ガイドラインをセキュリティルール策定の参考としてきました。SP 800-63B もまた、今後国際的なパスワード・認証設計のデファクトスタンダードとして扱われていくものと思われます。
日本国内のサービスを考えるうえでも、SP 800-63B は認証設計・ユーザー管理・パスワード運用の重要な指針となるでしょう。

SP 800-63B には、主に以下のような要素が含まれます。

- 認証に関する基本原則
- パスワードに関する要件
- 多要素認証の定義と要求

これらの基準は本来パスワードポリシーを制定する側が意識するべき基準であり、ユーザー側が意識しなければいけないものではありません。しかし、特にパスワードに関する要件については、最新の信頼できる基準を理解しておくことで、より安全かつ効率的にサービスを利用できるようになります。具体的には、最新のガイドラインに沿ったパスワードポリシーを設定していないサービスを利用する際に、管理しやすく強固なパスワードを自ら選択できるようになります。
なぜ安易なパスワードを利用してはいけないのか、安全なパスワードとはどういうものなのかを、NIST の新しいガイドラインを参考に再確認してみましょう。

SP 800-63B の概要

2025 年 7 月末に公開された SP 800-63B は、2017 年に公開された旧版を更新したものです。2017 年から 2025 年までの 8 年間で、パスワードに関する基準がどのように変化したのかを確認します。

要件	2017 年の旧ガイドライン	2025 年の新ガイドライン
最小文字数	最低 8 文字	最低 8 文字（多要素認証併用）、ただし推奨として 15 文字以上
最大文字数／許容長	少なくとも 64 文字まで受け付けるべき	少なくとも 64 文字まで受け付けるべき
構成ルール（文字種混在、記号の強制など）	ルールを課すべきではない（Should not）	ルールを課してはならない（Shall not）
定期的なパスワード変更	ルールを課すべきではない（Should not）	ルールを課してはならない（Shall not）
漏えい済みパスワードの扱い	既知の漏えいパスワードを使用させない	ブロックリストを用いて禁止する
パスワード入力／ユーザー利便性	空白文字・絵文字を許可することが望ましい	貼り付けを許可すべき 記号・空白文字・絵文字を許可すべき
ユーザー秘密質問	秘密質問・ヒントは推奨されない、可能なら廃止すべき	許容されない、強く制限される方式

ユーザーがパスワードを設定する上で参考になるのが、表内の最小文字数・最大文字数・構成ルールの三項目です。どの項目においても、2017 年から 2025 年で最低要件に変化はありません。しかし、より安全なパスワードが設定されるよう基準が明記されるようになりました。
パスワードの文字数や複雑さによって、パスワードの解析にかかる時間がどのように変化するのかを Hive Systems 社が調査しています。この調査でも、8 文字以下のパスワードは突破される危険性が高く、15 文字以上のパスワードは安全性が高いとされています。

現行のサービスでは、大文字や記号を混ぜたパスワードが強制されるケースが散見されます。しかし、新しいガイドラインでは、強制することでむしろパスワードがワンパターンになってしまうことから、ルールとして課すべきではないとされました。ユーザーは自分が管理できる範囲で、複雑かつ安易ではないパスワードを選ぶべきということです。

＜NIST 新基準における良いパスワードと悪いパスワードの一例＞
悪いパスワード: P@ssWord
（記号を使っているが、推測しやすい）
良いパスワード: HK480gam258a5k8lm0
（記号は使っていないが、ユーザー個人にしかわからない語呂合わせを含むもの）

また、同じく現行のサービスでよく採用されているルールとして、「定期的なパスワードの変更」ルールが挙げられます。このルールは「避けるべき」ではなく、明確に禁止されることになりました。ユーザーに定期的なパスワード変更を求めると、安易なパスワードの使いまわしが増えることがイギリスの調査で判明しています。そのため、パスワードの変更は侵害が発生したときのみ行い、強固なパスワードを継続的に使用してもらうことが推奨されています。
よく使用されるパスワードがどういうものであるかを理解して、他者に予想されにくい強固なパスワードを設定してください。

パスワードの漏えいで発生しうる被害

ここまで、NIST の新しいガイドラインを参考に、安全なパスワードについて考えてきました。ここからは、脆弱なパスワードを使用し続けることで発生しうる被害について紹介します。

IPA が開設している情報セキュリティ安心相談窓口には、毎月百件前後の不正ログインに関する相談が寄せられています。情報セキュリティ安心相談窓口への相談件数は 2025 年に入って大きく増加しました。特に 2025 年 7～9 月期は前年同期比で 3 倍以上の相談件数となっており、個人・企業を問わず不正アクセスを目的とした攻撃が苛烈になっている状況がうかがえます。
また、IPA は不正アクセスの要因の 1 つとして、「単純なパスワードが推測されること」を挙げています。

攻撃者がユーザーのアカウントに不正アクセスを行うと、アカウントの種類に応じて以下のような被害が発生します。

アカウントの種類	不正アクセスによって起こる被害
EC サイトのアカウント	クレジットカードの不正利用
SNS アカウント	SNS アカウントの乗っ取り
クラウドサービスの管理用アカウント	クラウドサーバー経由での機密情報流出
メールアカウント	友人や取引相手に対するスパムメール送信

また、海外では、1 人の従業員のアカウントが不正アクセスされ、それを起点として大規模なランサムウェア事案が発生した事例が報告されています。
個人の手を離れて、組織や家族に被害が及ぶこともあるため、上記の NIST のガイドラインを参考に今一度パスワードを見直してみてください。

まとめ

2025 年 10 月のマルウェアレポートでは、NIST のデジタルアイデンティティに関するガイドラインである SP 800-63B の更新について取り上げました。また、特にパスワードポリシーに関わる部分を紹介し、ユーザーがより安全なパスワードを設定するためのポイントを整理しました。
パスワードの文字数や複雑さは、パスワードに対する攻撃が高度化している今でも、依然として安全確保のために有効です。また、パスワードが利用中のサービスから流出していないかを確認し、侵害されたパスワードは別のパスワードに変更することも大切です。
前段で紹介したように、個人・団体を狙った不正アクセスは増加傾向にあります。パスワードの利用や設定に関して、NIST のガイドラインを参考に今一度見直しをしてみてください。

■常日頃からリスク軽減するための対策について
各記事でご案内しているようなリスク軽減の対策をご案内いたします。下記の対策を実施してください。

１．セキュリティ製品の適切な利用

1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しています。最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新の状態にアップデートしてください。

1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

２．脆弱性への対応

2-1. セキュリティパッチを適用する

マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。「Windows Update」などの OS のアップデートを行ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

３．セキュリティ教育と体制構築

3-1. 脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

3-2. インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

４．情報収集と情報共有

4-1. 情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

4-2. 情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

引用・出典元

●Are Your Passwords in the Green? | Hive Systems
https://www.hivesystems.com/blog/are-your-passwords-in-the-green
●The problems with forcing regular password expiry | National Cyber Security Centre
https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry
●情報セキュリティ安心相談窓口 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/index.html
●情報セキュリティ安心相談窓口の相談状況［2025 年第 3 四半期（7 月～9 月）］ | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/reports/2025q3outline.html
●インターネットサービスへの不正ログインによる被害が増加中 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

Canon

キヤノンマーケティングジャパン株式会社