Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Password Managers Usage Recommendations
(パスワードマネージャ利用に関する M³AAWG 推奨)

March 2017

この文書への URL: www.m3aawg.org/Password-Managers-BP

注釈：M³AAWG はここにリストされる教育的情報を産業向けのサービスとして提供している.
しかしながら, M³AAWG は特定のパスワードマネージャの製品やプロバイダを支持あるいは推奨するものではない.

I. はじめに

パスワードマネージャについてはユーザとサイバーセキュリティの専門家などの間に賛否両論があり，パスワードマネージャの利用が全てのオンラインアカウントに対する一意の強度の高いパスワードの適用に貢献していると主張する人がいる一方で，パスワードマネージャは単一障害点であり，それが提供する価値についてはあまり確かなものではないと主張する人もいる．この「M³AAWG 推奨」は，パスワードマネージャの利用についての産業界での一般的なコンセンサスを反映したものである.

多くのユーザが，login を要求する異なる Web サイトやポータルサイトなどに対する大量のユーザ名／パスワードの管理と格闘している(例えば，ローカルコンピュータに login するときなど). ユーザのリアクションは次のようなものである:

- 単に 1 件のレポートにアクセスする目的，あるいは 1 件の買い物をするために新たなアカウントを登録するように要求されると尻込みし，作業を放棄する.
- 同じユーザ名とパスワードを複数サイトで使い回す．このことは，いずれかのサイトでセキュリティの侵害があった場合に，それら認証情報が，それまでに利用してきた全てのサイトで侵害されたと見なされることを意味する.
- 長くて強度を持ったパスワードを使うことは，非常に多くの個別のユーザ名とパスワードを覚えておかなければならないという問題をいっそう困難にするため，長くて強度を持ったパスワードよりも短くて弱いパスワードを選びがちになる.
- ユーザ名とパスワードを覚えようと試みるよりは，サイトにアクセスするたびに「忘れた」パスワードを繰り返しリセットする.

多くのユーザは明らかに個別の ID が多過ぎて記憶だけに頼ることはできないが，上記のような典型的な回避策は安全ではない.

II. パスワードマネージャの効果

この問題に対する最も一般的な解答はパスワードマネージャの利用である．典型的なパスワードマネージャは以下のような多くの機能を提供する:

- 暗号で保護された安全なパスワード格納域(及び, 簡単なメモ用の安全な格納域)
- Web ブラウザとの緊密な統合(例えば, ログインフォームへの自動記入機能など)
- 新しいサイトで利用する複雑なパスワードの生成
- ユーザパスワードのオフサイトバックアップ(例えば, 「クラウド」への格納)
- 複数のユーザデバイスやサービス間でのパスワードの同期

パスワードマネージャの格納内容へのアクセスは通常, ユーザの記憶しておかなければならない別のパスワードで制限される. 数十のパスワードを覚えておく代わりに, ユーザは 1 つのパスワードだけを覚えておけば, 安全でない手法に頼る必要もなく, 数十の安全なパスワードにアクセスできる.

III. M^{3}AAWG による推奨

- M^{3}AAWG は, 多くのユーザがパスワードの大部分を管理するためにパスワードマネージャを利用することを推奨する.
- M^{3}AAWG は, ISP と企業が, そのユーザとスタッフと顧客に対して, パスワードマネージャの利用を促進することを推奨する.

M^{3}AAWG は, 特別なセキュリティ上の懸念や物理的な現実によって, パスワードマネージャの利用にそぐわないユーザが存在することを理解している(例えば, パスワードマネージャ自体が格納されているマシンのように, ユーザがそのパスワードを記憶しておかなければならないローカルマシンへの login など). このようなケースではユーザは個々の要求に沿った適切な代替手法をとる必要がある
.

IV. 結論

M^{3}AAWG 推奨は, テクノロジーの「勝者」と「敗者」を選ぶものではなく, ある環境に適した技術が異なる環境ではうまく適合しないかもしれないという事実を受け入れるものである.

M[3]AAWG はまた, パスワードマネージャの利用にリスクがないとは言えないことも理解している. もしパスワードマネージャが侵害された場合, さまざまなシステム上のアカウントが影響を受ける可能性がある.

ユーザは仕事用またはプロフェッショナルなパスワードと家庭用あるいは個人用のパスワードを混在させるかも知れない. ユーザは分離をサポートした製品を実行したり, それぞれ別のブラウザに紐付けられた 2 つの異なる製品を利用することで, これらの認証情報を分離しておきたいかも知れない.

それでも M[3]AAWG は, 多くのユーザがパスワードマネージャを利用し, ISP や企業がそのユーザ, スタッフ及び顧客に対してパスワードマネージャの利用を促進することを強く推奨する.

V. 参考文献

1. "Basic security practices regarding passwords and online identities,” https://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities

2. "Guide to Enterprise Password Management (Draft)," particularly section 4.3, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

3. "Password Managers," https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_en.pdf

4. "Password Security, Protection, and Management," https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf

5. “Review: Best Password Managers for the Enterprise," http://www.networkworld.com/article/3011735/security/review-best-password-managers.html

6. “The Best Free Password Managers for 2016," http://www.pcmag.com/article2/0,2817,2407168,00.asp

7. "Top Password Managers Compared,” http://www.csoonline.com/article/2877613/identity-access/top-password-managers-compared.html

8. Wikipedia List of Password Managers https://en.wikipedia.org/wiki/List_of_password_managers

---

M[3]AAWG が公開している全てのベストプラクティスと同様, この文書の更新については M[3]AAWG Web サイト (www.m3aawg.org)をチェックして下さい.