

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●7億7300万件のアカウント情報流出か…平文パスワードも出回る

<http://www.itmedia.co.jp/news/articles/1901/18/news077.html>



このニュースをザックリ言うと…

- 1月17日（現地時間）、セキュリティ研究者のトロイ・ハント氏より、多数のWebサイトから流出した大量のアカウント情報（メールアドレス・パスワード）がハッキングフォーラムに掲載されていると発表されました。
- 発表によれば、アカウント情報はオンラインストレージサービス「MEGA」に12,000本以上のファイル（計87GB超）としてアップロードされ、重複や無関係のデータを含めると11億6000万件以上に上っており、ハッシュ化されていたパスワードが平文に戻されていたケースもあったとされています。
- ハント氏は入力したメールアドレスのアカウントが流出しているかどうかを確認できるサービス「Have I Been Pwned (HIBP)」(※参照)を運営しており、**流出データから重複等を除き整理したメールアドレス約7億7300万件およびパスワード約2122万件を反映した**とのこと。
- また、流出が確認されたパスワードは決して使用せず、パスワードの使い回しを避ける等の自衛策を講じるよう注意を呼び掛けています。

AUS便りからの所感等

- 流出したアカウント情報をもとに様々なサービスへの不正ログインを試みる、いわゆる「リスト型攻撃」の脅威により、パスワードの設定については、かつて安全とされてきた「定期的な変更」が危険とされ、**「使い回しをしないこと」**の他、**「今回のように流出が発覚した場合は速やかに変更する」**ことが重要とされています。
- 前述のとおりHIBPには入力したパスワードが流出していないか確認するサービスもあり、パスワードそのものを外部に送信しない形で確認ができる模様です。
- ともあれ、自分が利用している全てのアカウントの棚卸しを行い、「被害を受けた可能性があるアカウントがないか」のみならず「放置しているアカウントがないか」等をも確認し、適切に管理することが重要です。



7億7300万件の流出情報、問フォーラムで流通 平文パスワードも出回る

さまざまなWebサイトやサービスから流出した電子メールアドレスとパスワードの組み合わせ情報が、大量にハッキングフォーラムに掲載されているが見つかった。アカウント情報の流出を確認できる無料サービス「Have I Been Pwned (HIBP)」を運営するセキュリティ研究者のトロイ・ハント氏が1月17日に明らかにした。

HIBPは、自分のメールアドレスやパスワードが流出被害に遭っていないかどうかをユーザーが確認できるサービス。ハント氏は、今回発見された流出情報のうち、メールアドレス約7億7300万件と、パスワード約2122万件を同サービスで検索できるようにした。



一方、パスワードの一部はハッシュが解除され、平文に戻されていた。HIBPでは、電子メールとは別に、流出したパスワードを検索できる「Pwned Passwords」のサービスも提供しており、ハント氏は今回の流出情報に含まれていたパスワードのうち2122万2975件を、このサービスで検索できるようにした。

今回見つかった情報の中には、ハント氏自身が過去に使っていた電子メールとパスワードも含まれていたという。ただし、いずれも今は使っていないパスワードだった。

こうした形で流出したメールアドレスとパスワードの組み合わせを、通報サイトやSNSなどネット上のあらゆるサービスで自動的に試し、適用するかどうかをチェックするツールも存在しているという。ハント氏はユーザーに対し、流出が確認されたパスワードは決して使用せず、パスワードの使い回しを避けるなどの自衛策を講じるよう促している。

文春オンライン

(※参照) <http://bunshun.jp/articles/-/8908>

「わたしのパスワードも流出している！」をクリック1回で確かめる方法

漏えいした5億件のパスワードデータをチェックできるサイト



山口 真実

genie: タイフ、チタノログ

トップページでメールアドレスを入力するだけ！

使い方は、サイトトップページのフォームにメールアドレスを入力して送信するだけ。パスワードの漏えいしなければ「Good news — no pwnage found!」、見つければ「Oh no — pwned!」というメッセージが表示されます。実際に漏えいが確認できた場合は、漏えい元のサイトに加えて、どんなデータが漏えいしたのか、その種類を教えてください。

漏えいした5億件のパスワード

こうした場合に試してみたいサイトです。このサイトは、過去に、メールアドレスを入力したパスワードを手軽にチェックできま

筆者が使っているプライベートのアドレスで確認したところ、すでに退会したサービスを含む、5つのサイトからデータの漏えいが確認できました。すべてに共通するのはメールアドレスとパスワードで、ほかにはユーザー名や、パスワードのヒントが漏えいしているケースもありました。



●「インターネットの安全・安心ハンドブック」最新版、NISCが無料公開

<https://internet.watch.impress.co.jp/docs/news/1165158.html>



このニュースをザックリ言うと…

- 1月18日（日本時間）、内閣サイバーセキュリティセンター（NISC）より、サイバーセキュリティの重要性を周知するための「**インターネットの安全・安心ハンドブック Ver4.00**」が公開されました。
- 2016年2月に「ネットワークビギナーのための情報セキュリティハンドブック」として公開されたもので、ほぼ毎年、最新のサイバー攻撃の事例を反映して改訂されています。
- NISCのWebサイトからPDFファイルが無料でダウンロードでき、各種電子書籍サイトからも同じく無料で入手可能になっています。

AUS便りからの所感等

- 同ハンドブックでは「サイバー攻撃ってなに？」から始まり、「基本的なセキュリティのポイント」「**最新の攻撃の手口(PC等に乗っ取られることで起こり得ること等)**」「パスワード・Wi-Fi・Web・メールのセキュリティ」「スマホ・パソコンのより進んだ使い方」あるいは「**SNS・インターネット関連の犯罪やトラブル**」まで広く取り上げられています。
- あらゆる情報機器のユーザはもちろん、システム管理者等においても、利用者に対する教育の題材として、またシステム・ネットワークの見直しやセキュリティソリューションの導入の際にも、「有用な視点」の一つとして活用できることでしょう。



●指令の送受信にGoogleドライブを用いるトロイの木馬を確認

<https://japan.zdnet.com/article/35131576/>



このニュースをザックリ言うと…

- 1月16日（現地時間）から18日にかけて、中国360 Threat Intelligence Center (360TIC) および米 Palo Alto Networks社より、「**Googleドライブ**」を経由して**指令のやり取りを行うトロイの木馬**の活動について報告されています。
- 報告によれば、トロイは主に中東をターゲットとする攻撃者グループ「DarkHydrus」によるもので、**不正なVBAマクロが埋め込まれたExcelファイル**の形をとっています。
- 指令のやり取りや、感染したPC上で収集した情報の送信する等の際、特殊なDNSリクエストを用いた通信の他、その代替としてGoogleドライブ上のファイルを用いる機能を持つとされています。

AUS便りからの所感等

- マルウェアが外部からの指令を受ける通信手段も様々で、GoogleドライブのようにHTTPSによる暗号化通信が行われるものもあり、特定のプロトコルを監視するというだけでは完全に防ぎきれないでしょう。
- **外に出ていくあらゆる不審な通信を検知し、時には遮断するような出口対策**の採用により、マルウェアの行動を止めたり、機密情報の流出を抑止したりすることが期待できますが、今回のようなことがあったからと、安易にGoogleドライブ等へのアクセスをブロックすることはユーザの利便性を大きく損ねることに注意が必要です。

