

IT時事ネタキーワード「これが気になる！」(第126回)

Google、2年放置のアカウントを削除する方針へ

2023.06.23



米Googleは5月16日、「アクティブでないアカウントに関するポリシーをアップデートした」とブログで述べた。これに関連して5月19日の「[Google Japan Blog](#)」によれば、ユーザーにオンラインで使用する製品やサービスを安全に使用してもらうためのリスク軽減措置として、無効なGoogleアカウントに関するポリシーをすべてのサービスで「2年間」へと更新したという。

Google、悪用される危険性から2年放置のアカウントを削除へ

この流れを受け早くても2023年12月から、2年以上使用されていない、またはログインされていないGoogleアカウントとそのアカウントで使用されているコンテンツ(例えば、GmailやGoogleドキュメント、Googleドライブ、Google Meet、Googleカレンダー、YouTube、Googleフォトなど)が削除対象となる。ただし、Googleのサブスクリプションに加入している、ウォレットに残高がある、YouTubeに動画をアップしているアカウントの削除予定はないという。

具体的な変更内容は「無効なGoogleアカウントに関するポリシー」を参照してほしい。これによれば、アカウントが2年間使用されなかった場合、アカウントは無効とみなされ、アカウントとデータがすべて削除される可能性があるが、Googleは措置を講じる前に、Googleアカウントにメール通知を送信、もしくは再設定用のメールアドレス(存在する場合)に通知を送信している。

こうしたアカウント削除を防ぐには、まず該当のアカウントでログインを行う。その後「メールを読む、送信する」「Googleドライブを使用する」「YouTube動画を見る」「写真を共有する」「アプリをダウンロードする」「Google検索を使用する」の他、「Googleでログイン」機能でサードパーティ製のアプリやサービスにログインする、といった操作を2年間に一度以上行う必要がある。

筆者も以前に遭ったオークション詐欺。休眠アカウント悪用の可能性

筆者は、以前ネットオークションで詐欺に遭った。補償制度などで事なきを得たが、その時使われていたのが、「なりすましアカウント」だった。以前アクティブだったものの2年近く使わず放置されていた、いわゆる「休眠アカウント」だった、と、あとで警察から知らされた。

ネットオークションでは「信用」が物を言う。取引の際は、今まで誠実な取引を行ってきたユーザーかを過去の評価数で判断して取引する。新規アカウントでは警戒され、入札が控えられる傾向がある。そこで休眠アカウントが使われるのだ。

当時、筆者は、相手が誠実な取引をある程度重ねている事実を確認して取引を行った。しかし、「以前は盛んに取引していたようだが、しばらく取引がなかった。久しぶりにまた始めたのだろう」と思う程度で、まさか「なりすまし」アカウントだとは全く思わなかった。こうした休眠アカウントについて、パスワードを解析して盗んだり闇取引で購入するなど、犯罪に利用したりするケースは近頃頻繁に行われているという。

放置されたアカウントは、長期間パスワードが変更されず、パスワードは使いまわされている可能性が高く、二段階認証などの安全対策もなされていない場合が多く、悪意ある者に簡単に利用されてしまいがちだ。Googleによると、休眠アカウントはアクティブなアカウントに比べ、二段階認証が設定されている割合が10倍も低く、多くの場合セキュリティが脆弱(ぜいじゃく)で、侵害されると個人情報の盗難、スパムなどの望ましくないコンテンツ、悪意のあるコンテンツの媒介などに使用される可能性があるという。「こうしたリスクを軽減するため、無効なGoogleアカウントに関するポリシーをすべてのサービスで2年間へと更新」する、というわけだ。

この一方、Twitterでは、イーロン・マスクCEOが5月9日、「数年間まったく活動がなかったアカウントを削除しているため、フォロワー数が減少する可能性があります」とツイート。これもなりすましなどへの安全対策と思われる。なお、Twitterのヘルプセンターの「[Inactive account policy](#)」には、アカウントをアクティブに保つには、少なくとも30日ごとにログインしてください、という記述があるので参考にしてほしい。

アカウント管理の必要性。悪用を防ぐにはどう管理すべきか

悪意ある者による危険を避けるためには、しばらく使っていない休眠しているアカウントは基本的に削除するのが一番だ。使う可能性があるなら、二段階認証やパスワード変更などの安全対策を施したのち、定期的にログインし、不審なログインや利用がないかなど状況をチェックしつつ運用していくのが適切だ。

定期的に、というのは、少なくともTwitterの「30日に1回」を目安とするのがよいだろう。管理が難しい場合は、アカウントを削除してしまったほうが賢い。使いたくなったら再度アカウントを作ればよい。アカウントの管理は、悪意ある者に利用されないよう、ユーザーが主体的に行うことが望ましい。誰も、自分のアカウントが乗っ取られて悪事に使われるのは愉快ではない。これを防ぐためには、自分の使っているアカウントをすべてリストアップして早めにチェックを行おう。

今のところ、アカウント管理で最も有効なのは二段階認証だ。利用しているサービスが多要素認証などに対応している場合は必ず設定しておこう。GoogleやApple、Twitter、Yahoo!、[Facebook](#)などたいいのサービスは対応している。都度二段階認証するのは骨が折れるが、安全には替えられない。なお、二段階認証は、常用メールアドレスへのメールや携帯電話番号へのSMS(ショートメッセージ)を使うのが基本だが、携帯電話が盗まれる可能性もある。自身の顔や指紋などの生体認証に対応している場合はなるべくそちらを使う(それでも指紋など盗まれる可能性はなくはない)と、さらに安全性を高められるだろう。

今後の傾向と対策は？ 他サービスの動向にも注視したい

今後、GoogleやTwitterに倣い、休眠アカウントおよび休眠アカウントの保持するデータを定期的に削除することをうたうサービスも増えてくるとされる。利用するサービスは、ポリシーや規約をよく読んだ上、Webページやメールなどで定期的な情報をチェックし、情報に応じて早めに対策を行おう。

ただ、休眠アカウント削除の情報のチェックはもちろんだが、サービスそのものが終了する可能性もあるので注意が必要だ。サービスそのものに不具合が生じることもあり、最悪の場合、不具合を抱えたままサービス終了、というケースも筆者の知る限り過去にはあった。もしもに備えて、アカウント情報をはじめ、クラウド上のデータなど定期的にバックアップを取る習慣を付けよう。当たり前だが、アカウント情報(ID、メールアドレス、パスワード)を記したファイルやメモなどは厳重に管理する必要がある。

基本的なことだが、複数サービスでのパスワードの使い回しは避けたほうがいい。情報が盗まれた場合、アカウントの使いまわしの可能性が想定され、複数サービスにおいて悪用される可能性があるからだ。パスワードは定期的に変更したほうがいいのは、言うまでもない。常に最新のITニュースやセキュリティ専門サイトなどの情報をチェックし、いざという場合に備えよう。

※掲載している情報は、記事執筆時点のものです