Googleセキュリティ通知の対処法は？セキュリティ強化法も紹介

藤川大

2022.06.09（最終更新：2022.06.09）

Googleから「セキュリティ通知」というメールが届いた……。このとき、内容を見て、もし心当たりがない場合は気をつける必要があります。本記事で、その理由や適切な対応方法、合わせて今後困らないためのセキュリティ強化方法を現役の情報セキュリティエンジニアがご紹介します。

目次

1 Googleのセキュリティ通知が届いたときに最初に確認したい2つのこと

Googleアカウントを利用していると、下図のようなセキュリティ通知が届くことがあります。

セキュリティ通知メール

焦る方が多いかもしれませんが、届いたからといって、やみくもに対応するのは危険です。落ち着いて、以下の2点を確認してください。

1. Googleのセキュリティ通知が届くような操作をしたか
2. そのGoogleのセキュリティ通知は本物か

1-1 Googleのセキュリティ通知が届くような操作をしたか

まずは、Googleのセキュリティ通知が届くような操作をしたか確認しましょう。

Googleのセキュリティ通知は、以下のような場合に届きます。

> ・新しいデバイスでのログインなど、重要な操作を検知した場合
> ・大量のメールが送信されるなど、不審なアクティビティが検知された場合
> ・保存したパスワードの表示など、重要な操作をブロックした場合

セキュリティ通知への対応 | Google アカウント ヘルプ

よくあるのが、新しいデバイスでのログインです。いつもと異なるパソコンやスマートフォン、タブレットなどからGoogleアカウントへログインすると、セキュリティ通知が届きます。

また、その派生系として、いつもと異なるブラウザからGoogleアカウントへログインしたり、Googleログインに対応したアプリに初めてログインしたりするときにも、セキュリティ通知が届きます。

つまり、あなたのGoogleアカウントに対して、あなた以外の人がログインした可能性がある場合に、「このような操作がされてますけど、大丈夫ですか？」という意味を込めて、通知が届くのです。

1-2 そのGoogleのセキュリティ通知は本物か

セキュリティ通知メールを受信した場合、そのメールが本物かどうか確認してください。

本物そっくりの偽物のメールで、あなたにGoogleアカウントのパスワードを入力させて盗むというフィッシングメールの可能性もあります。

うっかりパスワードを入力してしまうと、パスワードが漏えいしていないにも関わらず、あなた自身の手で漏えいさせることになります。

セキュリティ通知メールが本物かは、以下の方法で確認できます。

1. Googleアカウント へログイン
2. 左側のナビゲーションパネルで [セキュリティ] をクリック
3. [最近のセキュリティ関連のアクティビティ]欄に記載されている時刻・内容と、メールの受信時刻・内容を照合する

例えば、17時31分に、「Macでの新しいログイン」と本文に書かれたメールを受信したとき、[最近のセキュリティ関連のアクティビティ]欄に以下のような表示がなければ、セキュリティ通知メールが偽物の可能性があります。

最近のセキュリティ関連のアクティビティ

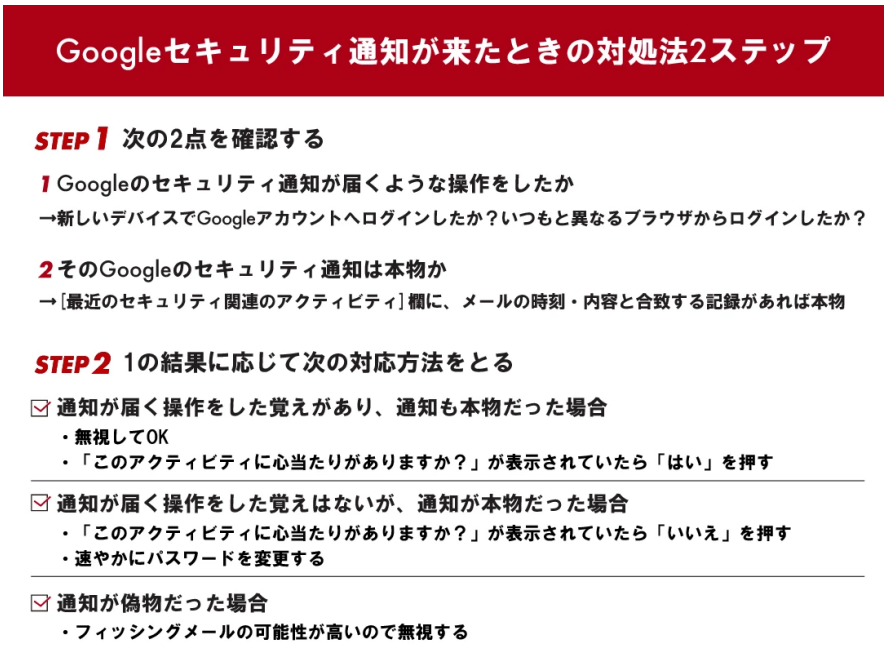
2 Googleのセキュリティ通知が届いたときの対処方法

Googleのセキュリティ通知への対応方法は、「Googleのセキュリティ通知が届くような操作をしたか」「そのGoogleのセキュリティ通知は本物か」によって変わります。

以下で、

1. 通知が届く操作をした覚えがあり、通知も本物だった場合
2. 操作をした覚えはないが、通知が本物だった場合
3. 通知が偽物だった場合

という3つのパターンに分けて、それぞれの対処方法をご紹介します。



Googleからセキュリティ通知が来たときの対処法2ステップ（デザイン：吉田咲雪）

2-1 通知が届く操作をした覚えがあり、通知も本物だった場合

何も問題ありませんので、通知を無視して構いません。

もし、「このアクティビティに心当たりがありますか？」と表示されていたら、「はい、心当たりがあります」を押してください。

2-2 通知が届く操作をした覚えはないが、通知が本物だった場合

あなたのGoogleアカウントへ、誰かが不正アクセスした可能性があります。

もし、「このアクティビティに心当たりがありますか？」と表示されていたら、「いいえ、アカウントを保護します」を押してください。

そして、速やかにパスワードを変更してください。不正にログインした人がパスワードを変更してしまうと、あなたがログインできなくなるためです。

パスワードを変更する手順は次の通りです。

1. Googleアカウント へログイン
2. 左側のナビゲーションパネルで [セキュリティ] をクリック

3. [Googleへのログイン]の中にある[パスワード]をクリック
4. 現在のパスワードを入力
5. 新しいパスワードを入力して、[パスワードを変更]をクリック

2-3 通知が偽物だった場合

フィッシングメールの可能性が高いので、通知メールは無視しましょう。

3 Googleから「重大なセキュリティ通知」が届いた場合は？

Googleからはセキュリティ通知の他、以下のような「重大なセキュリティ通知」という件名のメールが来ることもあります。

重大なセキュリティ通知

この場合も、心当たりがあるか、本物の通知かどうかの2点を確認の上、セキュリティ通知の場合と同様の対応を行ってください。

「重大なセキュリティ通知」は不正なログインをブロックした時などに届くもので、セキュリティ通知と比較して不正アクセスの可能性が高いため、くれぐれも無視しないように気をつけましょう。

4 Googleのセキュリティを高める方法

不正アクセスを防ぐには、普段からセキュリティを高めておくことが大切です。ここでは、4つの方法を紹介します。

4-1 2段階認証の設定

2段階認証は、パスワード（1段階）に加えて、もう1段階の認証を設けることで、セキュリティを強化するものです。

以下から設定できますので、もしまだ設定していない方は、必ず設定するようにしましょう。

1. Googleアカウント へログイン
2. 左側のナビゲーションパネルで [セキュリティ] をクリック
3. [Googleへのログイン]の中にある[2段階認証プロセス]をクリック
4. 以降、ナビゲーションに沿って進める

この設定を行うことにより、ログイン時にパスワードだけでなく、電話へテキストメッセージ（SMS）もしくは自動音声で届くコードの入力が必要となります。

パスワードのみでログインできる状況では、それが漏えいした場合に、世界中の誰でもログインできてしまいますが、2段階認証を設定しておけば電話を持っている人でないと基本的にはログインできません。

毎回コードを入力するのが面倒な場合は、ログイン時に [このコンピュータでは次回から表示しない] チェックボックスをオンにすれば、そのデバイスではコードが聞かれず、パスワードのみでログインできるようになります。

ただし、他人と共同利用するデバイスでは、このチェックボックスをオンにするのはやめましょう。あくまで、あなただけが利用するデバイスでのみオンにしてください。

4-2 Googleアカウント推奨のセキュリティ対策を行う

以下の画面のように「アカウントの保護手続きを完了してください」や「おすすめのセキュリティ対策があります」と表示されている場合は、それぞれナビゲーションに従って設定を完了させましょう。

4-3 パスワードは誰にも教えない、入力時の覗き見に注意

これはGoogleアカウントに限らず、一般的なパスワード管理に関する対策です。

警察庁が公開している「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」によると、2020年（令和2年）における不正アクセス行為（識別符号窃用型）の手口別検挙件数の第2位が、「言葉巧みに利用権者から聞き出した又はのぞき見たもの」で、20%を占めます。

うっかり相手の口車に乗ってパスワードを漏らさないようにしましょう。

また、パスワード入力時に、背後から覗き見られないようにすることも重要です。

オフィスやカフェで仕事をしているときはもちろん、電車内でもパスワードの取り扱いには十分に注意してください。

4-4 パスワードは見えるところにメモしない、推測されやすいパスワードを設定しない

警察庁が公開している先ほどの資料によると、「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」が第3位で、17.2%を占めます。

パスワードを書いた付箋をパソコンに貼っていたり、パスワードを書いた手帳をパソコンと一緒に持ち歩いたりしていませんか？

これは、銀行通帳と印鑑をセットで持ち歩くようなもので、意味がありません。すぐにやめましょう。

もしパスワードが覚えられないのであれば、覚えられるパスワードへ変更しましょう。

ただし、IDとパスワードが同じであったり、電話番号や誕生日をそのままパスワードにしたりすることは危険です。

危険なパスワードの例や、安全なパスワードの作り方について、IPA（情報処理推進機構）が案内していますので、以下をご覧ください。

今、パスワードが危ない! チョコっと+パスワード あなたは大丈夫? | IPA

5 セキュリティ通知が来たら落ち着いて適切な対応を

Googleアカウントがもし乗っ取られてしまうと、あなただけの問題では済みません。

もしGmailを取引先とのコミュニケーションに利用していたら、取引先の信頼を失う可能性があります。
もしGoogleドライブに大切なデータを保存していたら、データを取り戻せないかもしれません。
もしGoogleフォトでプライベートな写真を保存していたら、写真に写っている人たちに迷惑がかかるかもしれません。

そうなる前に、あらかじめセキュリティを高めておき、いざセキュリティ通知が来た際は、落ち着いて、本記事の通りに対応しましょう。

この記事を書いた人

藤川大

ITエンジニア&IT顧問

2007年からIT業界一筋。現職では社内向けITを担当し、ひとりでも多くの人をITの力で働きやすくするため、日々奮闘中。その傍ら、2020年から副業（複業）で個人事業主として活動開始。中小企業のIT顧問、IT研修事業。仕事の依頼はTwitterのDMへ。

藤川大の記事を読む