タイトル：ブルートフォース攻撃とは？ その被害事例と3つの対策を解説！

ブルートフォース攻撃とは？

ブルートフォース攻撃は、悪意を持った者が、個人や企業のサーバー等に不正にアクセスし、主にデータや金銭を盗むことを目的としたハッキング手法のひとつです。

まずは、その定義から解説します。

ブルートフォース攻撃の定義

「ブルートフォース攻撃」は、日本では「総当り攻撃」と訳されます。

ブルートフォース攻撃は、ログインIDやパスワードなどを総当たりで試行し、本人になりすましてログインするハッキング行為です。個人や組織のネットワークシステムに不正にアクセスする、シンプルかつ効果的な手法です。

ハッカーは、ユーザー名とパスワードを繰り返し試すことで、ログインに必要な情報を見つけ出します。

ブルートフォース攻撃は、古くからあるサイバー攻撃であるにもかかわらず、ハッキングの戦術としてとても効果的です。

ブルートフォース攻撃の種類

ブルートフォース攻撃には様々な種類があります。攻撃方法がわかれば、防御法もわかります。

ここでは、代表的なブルートフォース攻撃を3つ紹介します。

単純なブルートフォース攻撃

ブルートフォース攻撃は、ログインIDを固定し、異なるパスワードを総当たりで入力することで、サーバーログインを狙う手法です。

単純なブルートフォース攻撃は、ソフトウェアを使用し、機械的に総当たりでユーザーのパスワードを推測します。

多くの人が、いまだに単純で脆弱なパスワードを使用しています。また、複数のウェブサイトで同じパスワードを使い回していたり、パスワードを紙に書いて机に置いていたりします。

こうしたずさんなパスワード管理に対して、ブルートフォース攻撃は簡単で効果的です。

まず、攻撃者はターゲットを選択し、そのアカウント名とパスワードでログインを試みます。

推測が容易なパスワードであれば、比較的短時間でハッキングに成功します。

辞書攻撃

「辞書攻撃」とは、あらかじめよく使われるパスワードを辞書として保存しておき、それを利用してログインを試みる手法です。

たとえば、「password123」、「012345」、「誕生日」などパスワードに使用されることの多いキーワードを辞書化し、それを優先的に試すのです。

「辞書攻撃」という名称は、ハッカーがパスワードとして使われそうなキーワードの辞書を作成し、それを利用することに由来します。

ハイブリッドブルートフォース攻撃

ハイブリッドブルートフォース攻撃とは、単純なブルートフォース攻撃と辞書攻撃を組み合わせた手法です。

この攻撃は、ハッカーがターゲットのユーザー名を知ることから始まります。そして辞書攻撃でパスワードの組み合わせを総当たりで試行します

攻撃者は、パスワードとしてよく使われる単語、人気のある単語、数字、年号、またはランダムな文字を組み合わせたパスワードを辞書として保存しておきます。それを元に総当たりでログインを試みるのです。

ユーザーが単純で脆弱なパスワードを設定している場合は、ハッキングの成功率が高まります。

リバースブルートフォース攻撃

リバースブルートフォース攻撃は、パスワードを1つに固定し、ログインIDを変えながら繰り返しログインを試行する手法です。

前述のブルートフォース攻撃は、ログインIDを固定し、異なるパスワードを入力することで、サーバーログインを狙う手法でした。この手法は、ターゲットが定まっている場合に用いられます。

リバースブルートフォース攻撃は、まずパスワードを固定します。そしてログインIDを変えながらハッキングを試行する方法です。この手法は、主にターゲットが定まっておらず、誰でもいいのでハッキングしたい場合に用いられます。

ブルートフォース攻撃の目的は何か？

ブルートフォース攻撃は、ターゲットのログインIDやパスワードを解読するのに数カ月から数年かかることもあり、忍耐力が必要です。しかし、その分、大きな報酬を得られる可能性があります。

ブルートフォース攻撃の主な目的を挙げてみましょう。

個人・企業情報の窃取

ユーザーのアカウントへ侵入すると、財務情報、銀行口座、クレジット情報、家族情報、医療情報など、さまざまなデータが手に入ります。攻撃者は本人になりすまし、金銭を盗んだり、第三者に情報を売り渡すことで利益を得ます。

企業の機密データにアクセスすることによって、企業財務、特許情報、新製品開発、社員や関連会社の個人情報などを取得できます。

また、脅迫、恐喝、悪評の流布など、より広範囲な攻撃を可能にします。

マルウェアの拡散

攻撃者は、ユーザーのコンピュータをマルウェアに感染させることで、接続されたシステムやネットワークに侵入し、組織に対してより広範囲なサイバー攻撃が可能になります。

悪意のある活動のため

ブルートフォース攻撃に成功すると、さらに広範な攻撃の土台になります。たとえば、DDoS攻撃、セキュリティ防御の突破、システム破壊などが可能になります。

企業やウェブサイトの評判を落とす

ブルートフォース攻撃は、経済的な損失だけでなく、風評被害も引き起こします。たとえば、ウェブサイトに卑猥なテキストや画像を掲載することで、企業やウェブ運営者の評判が低下し、サイトそのものを運営できなくするのです。

ブルートフォース攻撃を防ぐには

ブルートフォース攻撃は、シンプルなハッキング手法です。いくつかの方法を採用することで、攻撃を防止できます。

ブルートフォース攻撃を防止する代表的な防御策をご紹介します。

より強固なパスワードの使用

IDとパスワードがわからなければ、ブルートフォース攻撃は成功しません。ブルートフォース攻撃を防ぐには、パスワードの解読をできるだけ困難にすることが一番有効です。

パスワードの推測を困難にすることで、解読に時間がかかり、攻撃者を諦めさせる方法です。

パスワード強化は、自分と組織のデータを保護するために重要な役割を担っています。

また、最先端の暗号技術を用いたパスワード強化は、ブルートフォース攻撃からサーバーを保護するために有効です。

ユーザーパスワードの保護強化

ハッカーがログインに失敗するたびに、その記録はエラーログに記録されます。

ECサイトなどで適当なユーザーID、パスワードを入れて、「パスワードが間違っています」と表示されれば、IDは存在することをハッカーに知らせることになります。

そうならないために、「ユーザーID、パスワードのどちらかが間違っています」というように推測されないようにします。

セキュリティとパスワードに関する継続的なサポート

サイバー攻撃の脅威を認識し、パスワードを強化するためには、利用者への定期的な教育が必要です。さらに、企業のパスワード管理ツールなどを導入すれば、企業データを危険にさらすリスクを排除できます。

ブルートフォース攻撃は、総当たりでログイン試行を繰り返したり、新しいデバイスや通常とは異なる場所からのログインなどの兆候によって発見できます。企業は、システムやネットワークを常に監視することで、疑わしいアクセスや異常な行動を即座にブロックできます。

FAQ（よくある質問）

ブルートフォース攻撃とは何ですか？

ブルートフォース攻撃とは、ユーザーのログインIDやパスワードなどを推測し、総当たりでログインを試みるハッキング行為です。ブルートフォース攻撃は、IT初心者でも時間をかければ成功の確率が高まるハッキング戦術で、とても効果的です。

ブルートフォース攻撃は違法ですか？

ブルートフォース攻撃は違法です。組織が自分たちのセキュリティ強化のために侵入テストを実行するなどの場合のみ、ブルートフォース攻撃は合法となります。

ブルートフォース攻撃は、よく使われるハッキング手法ですか？

ブルートフォース攻撃は、一般的なハッキング手法です。Verizonの調査によると、2017年の全データ侵害の約5%を占めています。

2019年の調査では、どんなに複雑な8文字のパスワードでも、わずか2.5時間で解読されることがわかっています。

まとめ

ブルートフォース攻撃は、ログインIDやパスワードを総当たりで試しログインを試みるハッキング行為です。IT初心者でも、時間をかければ成功の確率が高まる効果的な手法です。

現在も、ブルートフォース攻撃によってさまざまな被害が発生しています。

ブルートフォース攻撃の手口は単純なので、ログインIDやパスワードの管理を徹底し、アクセス制限をかけることで対処できます。

ハッキング被害を注意喚起し、定期的な社内教育やシステム保守などで、ブルートフォース攻撃を回避しましょう。