

アカウント情報の流出時に連鎖的な被害を招く パスワードの使い回しは危険！

サイバースキュリティ・ニュース

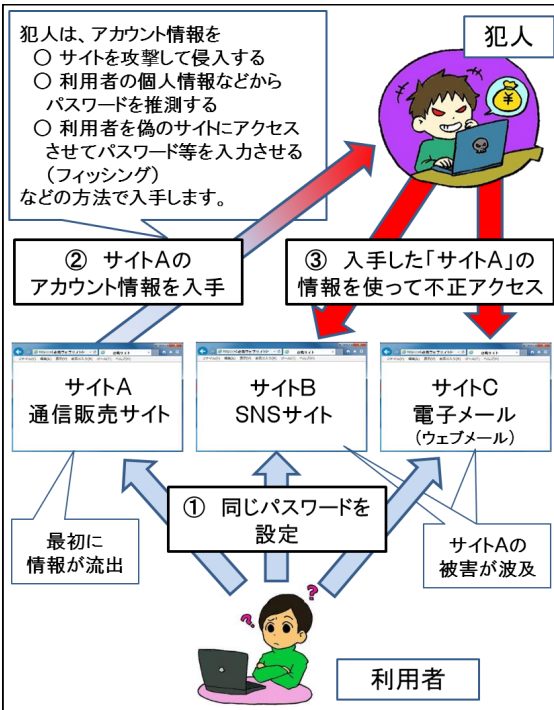
サイバー犯罪対策課
H30.11.8

**パスワードはサイトやサービスごとに
変えて被害を最小限に**

防ぎ切れない流出、使い回しで被害が拡大

パスワードを含むアカウント情報は、常に流出の危険にさらされています。あなたが使用しているパソコンからだけでなく、利用しているサイトから流出してしまうこともあります。もし、同じパスワードを他の

サイトでも使い回している場合、左の図のように、通信販売サイトから流出したパスワードを使ってSNSから不正にメッセージを送信される、メールをのぞき見される、といった連鎖的な被害が起きてしまいます。



連鎖的な被害の例

安易なパスワードは被害の危険大

「1234」「abc」などの単純なものや、誕生日、電話番号、名前などを使ったパスワードは、他人が簡単に推測できてしまうため危険です。下図の例を参考に、覚えやすく推測されにくいパスワードを作りましょう。

情報流出に便乗した脅迫メールに注意

要求は無視してパスワードを変更

実際に使用しているパスワードとともに「あなたのアカウントをハッキングした。仮想通貨を払えば情報を消す」などと書かれた脅迫メールが県内でも多数確認されています。このようなメールが届いても応じる必要はありません。支払いせずに、速やかにパスワードを変更して、警察に相談してください。

こんにちは！

あなたは私を知らないかもしれませんが、なぜあなたはこの電子メールを受け取っているのかわかっていますか？この瞬間、私はあなたのアカウント(●●●●@●●●.ne.jp)をハッキングし、そこからメールを送りました。私はあなたのデバイスに完全にアクセスできます！

今私はあなたのアカウントにアクセスできます！たとえば、●●●●@●●●.ne.jpのパスワードは●●●●です

実際に、私は大人のvids(ポルノ資料)のウェブサイトにマルウェアを置きました。あなたは何をしていますか、あなたはこのウェブサイトを訪れて楽しんでいました。あなたがビデオクリップを見ている間、インターネットブラウザはRDP(Remote Desktop)として動作するようになりました。それは私にあなたのスクリーンとウェブカメラへのアクセスを提供するキーロガーを持っています。その直後に、私のソフトウェアプログラムはあなたのメッセージ、ソーシャルネットワーク、そして電子メールから連絡先全体を集めました。

私は何をしましたか？私は二重スクリーンビデオを作った。最初の部分はあなたが見ていたビデオを表示しています(あなたは良いと奇妙な味を持っている)、2番目の部分はあなたのウェブカメラの記録を示しています。まさにあなたは何をすべきですか？

脅迫メールの例

- ①危険なパスワードの例
「mie110」
短くて単純(名称と電話番号を使用)
- ②安全性を増したパスワードの例
「M!eAnzen+110」
・なるべく長く(12文字以上が目安)
・文字、数字、記号を組み合わせる
・英単語より日本語のローマ字が安全
- ③使い回し対策の例
サイトごとに違う部分と、共通して使う部分を組み合わせる
例：通販サイト～ Ath M!eAnzen+110
SNSサイト～ Bsn M!eAnzen+110
サイトごとに違う部分 共通して使う部分

パスワードの作り方