



SNSやメールの 乗っ取り・なりすましに 注意!!



不正アクセス被害にはこのような原因があります

Case1 簡単なパスワードを設定していた



Case2 不正なアプリをインストールした



Case3 フィッシングメールに引っかかった



対策

- 推測されにくい複雑なパスワードを設定する。
- パスワードを使いまわさない。
- 多要素認証や二段階認証を設定する。

対策

- 公式ストア以外からアプリをインストールしない。
- 不審なアプリに端末の権限を許可しない。
- セキュリティソフトを導入する。

対策

- メールリンクは安易に開かない。
- 内容を確認する際は、公式サイト・アプリから直接ログインする。
- ID・パスワード・認証コードは安易に入力しない。

他にもこんな危険があります



公共Wi-Fiの利用

公共のフリーWi-Fiは、盗聴されるリスクがあります。



プレゼント企画やキャンペーン

応募を装った偽企画で、アカウント情報を求められ、乗っ取られるおそれがあります。



知人を装ったメッセージ

乗っ取られた友人のアカウントから偽サイトへ誘導するメッセージがくるおそれがあります。

乗っ取り・なりすましの被害に遭ったときは

- ログインできる場合は、新しいパスワードに変更する。
- ログイン中の端末を確認し、見覚えのない端末は全てログアウトさせる。
- アカウントの登録情報や認証方法が変更されていないか確認する。
- SNS等の交流相手に注意喚起する。
- サービス提供会社に相談する。
- 同一のパスワードを使っているサービスが他にある場合、そのサービスのパスワードを変更するなどの対策をする。

被害拡大を防ぐためにすぐ対応しましょう



不審に感じたら
すぐに警察に通報・相談を!

警察相談電話

#9110



北海道警察公式HP
サーバ-セキュリティひろば

北海道警察



YouTube動画
サーバ-セキュリティ講座

