

個人情報を守る身近なセキュリティ対策

企業等から流出した個人情報を使い、別のサービスへの不正ログインを試みる手口があります。日頃の備えで、被害拡大を防ぎましょう。

1 今日からできる基本的なサイバーセキュリティ

パスワードを使い回さない
サービスごとに長く複雑なものを設定
流出したパスワードは再利用しない

多要素認証を設定する
パスワードに加え、認証アプリ、
ワンタイムパスワード、パスキーを
設定。

端末とアプリを最新に更新
OS・アプリの自動更新をON
ウイルス対策機能を有効にしよう

不審なメール・SMSは開かない
リンクを不用意にクリックしない
差出人をよく確認



2 フィッシング被害防止

フィッシング: 実在の企業を装ったメールや偽サイトから誘導し、パスワードやカード情報を盗む手口

「至急」「利用停止」など不安を煽る記載情報漏えいのお知らせを装う場合もあります。

差出人名やロゴだけで本物と判断しない。

From: XYZ銀行
件名: 【重要】取引停止のお知らせ

本人かどうか確認が取れない取引がありましたので停止しました。
確認してください。
<http://example1.jp>



From: XYZカード
件名: 【緊急】不正アクセスを検知しました

第三者からの不正なアクセスを検知しました。
確認してください。
<http://example2.co.jp>



 050xxxxxxx

お荷物のお届けがありましたが、不在の為持ち帰りました。
<http://example3.ne.jp>



メールやSMS内のリンクは開かず、普段使う公式アプリなどから確認。

※詳細なフィッシング対策はこちら⇒

<https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html>

