

其の四、使い回すべからず！

あなたのID・パスワードは
すでに流出しているかも！？



忘れちゃうから
全部同じパスワード
にしよう

パスワード
使い回してはならぬ！

使い回しの危険性を知るべし

犯人は、流出しているID・パスワードのリストを元に、不正なログインを試みる。パスワードを使い回していると、芋づる式に他のサービスもログインされてしまう。

ID	パスワード
yyyy@xxx	bbb00
aaaa@xxx	ap110
uuuu@xxx	pp123
.....

流出しているID・パスワードのリスト

不正ログイン

別々のパスワードにするでござる！

インターネット セキュリティ五箇条

- 其の一、押すべからず！**
フィッシングメールかもしれぬ
メール本文中のURLは押さずに
公式サイトなどからアクセスすべし
- 其の二、慌てるべからず！**
偽ショッピングサイトかもしれぬ
個人情報を入力する前に確認すべし
- 其の三、かけるべからず！**
警告画面は偽物かもしれぬ
表示された電話番号は疑うべし
- 其の四、使い回すべからず！**
不正にログインされるかもしれぬ
サービスごとに別々のパスワードにすべし
- 其の五、すぐに相談すべし！**
一人で悩んではならぬ
サイバー犯罪に関して、困ったことが
あれば、周りの人や最寄りの警察署
に相談すべし



ちよつとまって！

確認したかい？

この五箇条



サイバー犯罪対策課のホームページはこちら
<https://www.pref.aichi.jp/police/anzen/cyber>

愛知県警察本部 サイバー犯罪対策課
☎ 052-951-1611 (代表)

この標語は、大学生サイバーボランティアが考えてくれたものです。

其一、押すべからず！

あなたのスマホやパソコンに届くメールは偽物かも！？



フィッシングの実態を学ぶべし

- 1 偽メール（フィッシングメール）が届く。有名企業、金融機関、公的機関などを装っている。
- 2 メール本文中にあるURL（https://...）を押すと、本物そっくりの偽サイト（フィッシングサイト）が表示され、ID・パスワードや個人情報等の入力を求められる。
- 3 フィッシングサイトに入力した情報が犯人に盗まれる。
- 4 盗まれた情報が犯人に不正利用される。

フィッシングメールの例でござる！

- ・パスワードが失効しました
- ・荷物のお届けがあります
- ・当選しました 等

其二、慌てるべからず！

そのショッピングサイト詐欺サイトかも！？



購入手続きする前にチェックすべし

<input type="checkbox"/>	どこでも売切れであるような人気商品が「在庫有り」となっている
<input type="checkbox"/>	会社概要がデタラメ又は他社の概要が使われている
<input type="checkbox"/>	決済方法が銀行振込みのみである
<input type="checkbox"/>	代金振込先名義が個人名である

※会社概要をインターネット検索してみると、別の会社であったり、詐欺サイトであるとの口コミが表示されたりすることがある。

個人情報（クレジットカード情報等）を盗む目的のサイトもあるため、入力する前にチェックするでござる！

其三、かけるべからず！

突然の警告画面それ偽物のサポート会社かも！？



手口を知って被害を防ぐべし

パソコンでサイトを閲覧していたら…

警告画面・警告音！
すぐに問い合わせよう記載が！
「050-xxxx-xxxx」「03-xxxx-xxxx」等

- 1 パソコンに不具合が発生したとの偽警告で不安をあおられる。
- 2 画面に表示された電話番号に問合せをしてしまう。
- 3 電話の相手から、復旧と継続サポートのためとして高額料金を請求される。

このような事態が起きても焦らずに！
警告画面を閉じるだけで解消されることがあるでござる！