

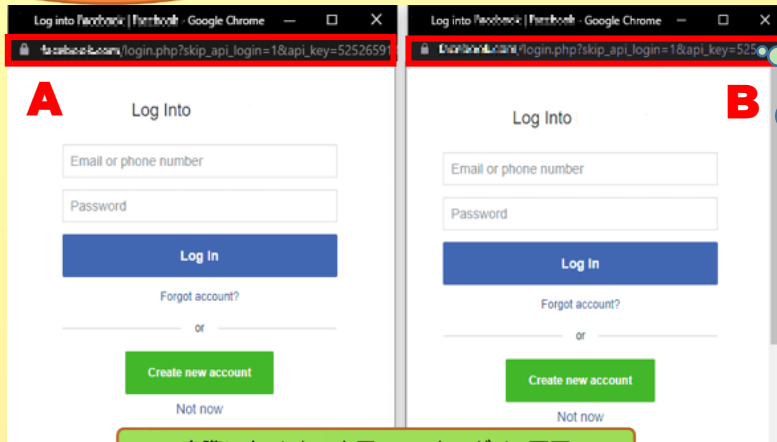


# サイバーニュース

R 4 年 第 5 号  
奈良県警察本部  
サイバー犯罪対策課

## 注意『偽装URL』によるフィッシングにご用心！

### 問題 どちらが正規サイトのログイン画面？



どちらも画面上に表示されているURLは全く同じです！

PASSWORD



実際にネット上で出回っていたログイン画面

答えは、  
**Aが偽のフィッシングサイト**  
**Bが正規サイト**  
のログイン画面です！



1 2  
3 4

え？どっちも全く同じログイン画面じゃないか…！？

どうやって偽サイトを見破れば良いんだ！



でも、表示されるURLまで正規サイトと全く同じURLに設定することなんて本当に可能なんですか？



残念ながら可能なんです(泣)  
犯人はポップアップウィンドウとして表示されるページを偽装して正規サイトのログイン画面とそっくりな偽のログイン画面を作成し、パスワードなどの情報を盗みとろうとします！



**注意**

フィッシング対策としては...

## 正規サイト、アプリから接続(ログイン)する

といった基本的な対策が一番効果的と考えられます！

インターネットを利用する際にURLを確認する方法は対策として非常に有効な方法ですが、今回紹介したように『偽装URL』が存在するように、URLを確認するだけでフィッシングの被害を100%防げる訳ではありません。

★無理に偽サイトを見破ろうとせず、最も安全な方法でインターネットを利用しましょう！

