

メールアドレスの乗っ取りに注意！

～自社メールサーバーから大量の迷惑メールが…～

メールアドレスに
ログインできない

エラーメッセージが
大量に届いている

不特定多数の宛先に、
迷惑メールが送信されて
いるとの連絡が…

機密情報の流出

他のサービスの更なる乗っ取り

スパムメール送信



それ、メールアドレスの乗っ取りが原因かも!?

⚠ 乗っ取られてしまったらとるべき対応 ⚠

メール アカウント の設定を確認

- アカウントにログインできるか
- 転送設定、署名のURLやメールアドレス等におかしいところはないか

パスワード の変更

- 使いまわししない
- 複雑なパスワードを設定
- 二段階認証を有効化

登録アドレスへ の連絡

- 登録連絡先へ、アカウントが乗っ取られた旨を報告
- 不審なメールやリンクへの注意を呼び掛け

ウイルス チェック の実施

- セキュリティソフトでスキャンする
- マルウェアが検出された場合、再度パスワード変更と設定内容の確認を行う

- 被害予防のため、日頃から上記「パスワード」の対策を行うとともに、不審なメールや不審なファイルを開封しない等の対策を実施してください。
- 万が一、サイバー攻撃の被害が疑われる場合は、警察にご連絡ください！



簡易的にメールアドレスの流出診断ができます！

『Have I Been Pwned?』は、流出したメールアドレスやパスワードが確認できるサイトです。注) 確認結果は判断の参考としてください。

<https://haveibeenpwned.com/>

〈流出として登録されていない場合〉

Good news — no pwnage found!

〈流出として登録されている場合〉

Oh no — pwned!

流出が確認された場合は、
直ちにアカウントパスワードを変更
してください。



埼玉県警察 サイバーセキュリティレポート

R6.6

サイバー局サイバー対策課