TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2022年
第17号

# 不正アクセス被害に注意！

報道によると、12 月３日に石川県内の医療機関が不正アクセスの被害を受け、県内においても 11 月 12 日に教育機関で不正アクセスがあったことを確認しています。

こうしたサイバー攻撃は、容易に県境・国境を越えて実行されるため、地域、企業・団体の規模を問わず攻撃の対象となり得ます。

攻撃者は、企業や組織のサーバや情報システムへ侵入するために、

○　パスワードの総当たり攻撃を行う

○　OS やソフトウェアの脆弱性、設定の不備等を突いて攻撃する

など様々な方法で不正アクセスを試みます。

一たび侵入を許せば、ホームページの改ざん、顧客情報や機密情報の窃取、新たなサイバー攻撃の踏み台等に利用されるおそれがあります。


## 被害の未然防止対策

### ○ 修正プログラムは、常に最新の状態にアップデートする

サーバやパソコン等の OS、各種ソフトウェアに修正プログラムを適用し、最新のバージョンに更新してください。ルータ、VPN 機器等は最新のファームウェアに更新してください。

### ○ セキュリティ対策ソフトの導入

セキュリティソフトの定義ファイルは、常に最新の状態になるよう設定し、定期的にフルスキャンを実施してください。

### ○ パスワードの適切な設定・管理

パスワードは、大小英字、数字及び記号を混在させた複雑なものとし、使い回しはしないようにしてください。

### ○ 多要素認証の導入

複数の要素（記憶情報、所持情報、生体情報のうち２つ以上）を使用して認証することで、セキュリティ強化を図りましょう。

### ○ バックアップはネットワークから切り離して保管

ランサムウェア等によるデータ破壊に備えて、定期的に外部記録媒体等へバックアップを行ってください。バックアップしたデータはネットワークから切り離して保管してください。

**不正アクセス被害を受けた場合は、**
**警察への通報をお願いします！**

参考　IPA：日常における情報セキュリティ対策
https://www.ipa.go.jp/security/measures/everyday.html
不正ログイン対策特集ページ
https://www.ipa.go.jp/security/anshin/account_security.html
総務省：国民のための情報セキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_risk_06.html