

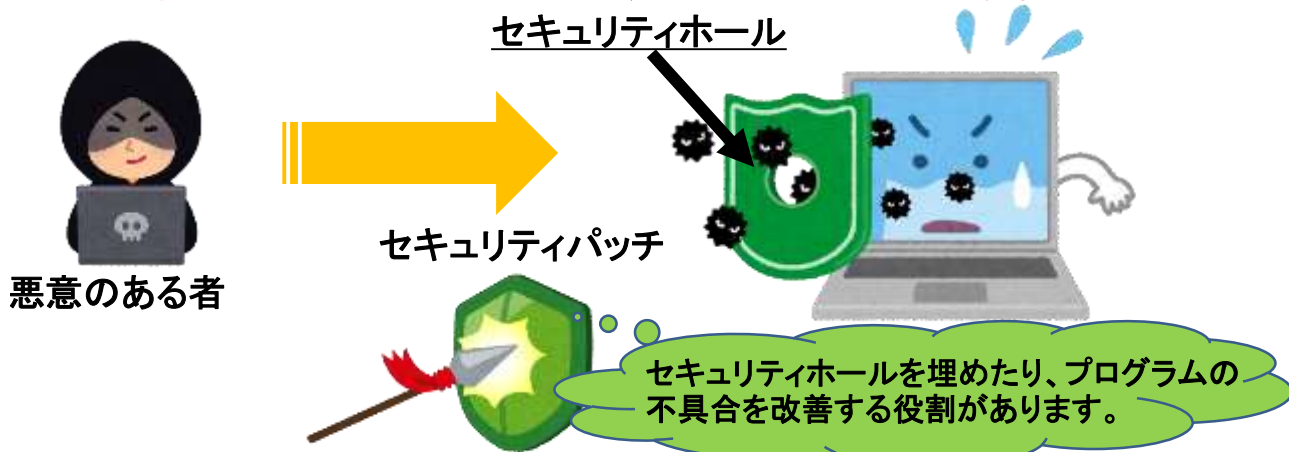


# セキュリティパッチの管理・運用の徹底を！！

## ～ 脆弱性を狙った攻撃に注意 ～

- ・システムを導入した後、メンテナンスをしていますか？
- ・業務への影響を恐れ、サーバ等の脆弱性を放置していませんか？

**脆弱性(セキュリティホール)は、システムの弱点です。**



**セキュリティパッチを適用しないと・・・**

**不正アクセス・マルウェア等の悪意のある攻撃の対象に！**

### VPN機器のセキュリティ対策

◎SSL-VPN機器(いわゆる次世代ファイアウォール)を導入している場合、脆弱性の影響を受けないように、対策(セキュリティパッチの更新)が実施済みか必ず確認し、さらに『パスワードを変更し、不審な接続ログ等がないか確認』をお願いします。

### セキュリティパッチの管理・運用の徹底

リモートワーク等、働き方が変化するなか企業や団体が利用するシステムへリモートアクセスする需要が増えていますが、システムの脆弱性は不正アクセス・マルウェア等の攻撃による情報流出事案の要因となります。

脆弱性を狙った攻撃手法等は、インターネットで公開されている場合もあり、悪意ある者は脆弱性のあるシステムを探しています。

セキュリティパッチの管理・運用ルールを策定し、特にクリティカルな脆弱性のセキュリティパッチの適用は、確実に実施してください。