

家庭用ルーターのセキュリティ対策

- ルーターの管理画面パスワードが初期設定のままになっていませんか？
- 最新のファームウェアにアップデートされていますか？
- サポートが切れたルーターを使用していませんか？
- 見覚えのない設定変更がなされていませんか？

⇒ 詳しくは中のページをCheck!

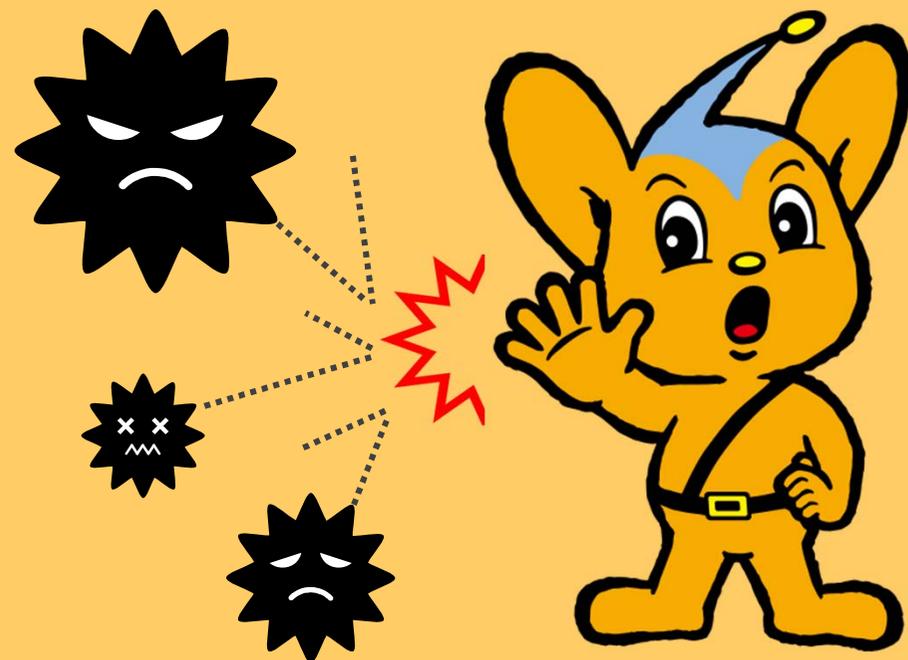
警視庁では

サイバー犯罪やサイバーセキュリティに関する情報発信を行っています。

警視庁 サイバーセキュリティインフォメーション 検索

YouTube / 警視庁公式チャンネル

サイバー攻撃に注意！



家庭用ルーターもセキュリティ対策を！



セキュリティの弱い家庭用ルーターがサイバー攻撃に悪用されています！



警視庁サイバー攻撃対策センター



警視庁 サイバーセキュリティインフォメーション 検索

街とともに。人とともに。FOR MORE COMMUNICATION

けいしちょう

家庭用ルーターのセキュリティ対策（点検事項）

ルーターの管理画面パスワードが初期設定のままになっていませんか？

古いルーターの初期設定パスワードは、推測しやすいものが多く、危険です。
パスワードは、単純なものではなく、英大文字、英小文字、数字、記号を含めた複雑なものに変更してください。

サポートが切れたルーターを使用していないですか？

メーカーのサポート（ファームウェアの提供）が終了している場合、ぜい弱性が改善されずに危険です。
ルーターのサポート期間は、各メーカーのホームページを確認できます。
サポート切れのものは買替えを検討してください。

最新のファームウェアにアップデートされていますか？

ルーターもアップデートが必要です。
各メーカーから更新プログラムが配信されていますので、常に最新のものにアップデートしてください。
また、ルーターの自動アップデート機能を活用することで高いセキュリティが保たれます。

見覚えのない設定変更がなされていないですか？

身に覚えのない設定（VPN機能、DDNS機能など※）がされていたり、知らないユーザーが追加されている場合は、ルーターを初期化し、最新のファームウェアにアップデートした上、複雑なパスワードに再設定してください。
※：VPN機能やDDNS機能が搭載されていないルーターもあります。

セキュリティ対策をしていないルーターは、犯罪インフラとしてサイバー攻撃者に悪用される可能性があります。セキュリティをより高めるために、定期的に自宅のルーターの状態を確認してください。

