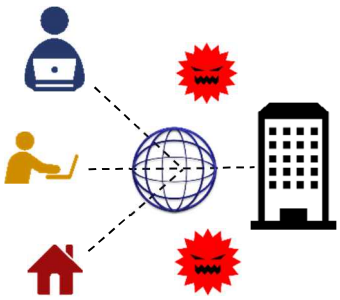
滋賀県警からのサイバーセキュリティに関するお知らせ

«テレワーク時代のセキュリティ»
VPN やリモートデスクトップのセキュリティ対策について

新型コロナウイルス感染対策及び DX（デジタルトランスフォーメーション）の推進により、テレワークの導入が進んでいますが、テレワークにおいて VPN（Virtual Private Network）やリモートデスクトップのシステムは欠かせません。

しかしながら、これらのシステム等の脆弱性を狙ったサイバー攻撃が確認されており、情報が流出するなどの被害が発生しています。

現に利用されている場合や導入を予定されている場合は、セキュリティ対策の確認や強化をお願いします。



VPN とは

VPN は、通信事業者のネットワークやインターネット等の公共ネットワーク上でつくられる、仮想的な専用ネットワークの総称です。

VPN には通信事業者がサービス化している VPN、インターネット等の公衆網を用いる VPN、スマートフォンや PC から利用する VPN のように、様々な種類があります。

【メリット】
- ・暗号化による安全な通信が可能
- ・社内ネットワークへの安全なアクセスが可能
- ・運用コストの削減

VPN は、安全性が高いことが特徴ですが、適切に設定することが重要です。

また VPN 専用ルータの脆弱性を悪用した不正アクセス事件が発生しています。

【確認・対策】
- **・VPN の専用機器やソフトウェアの脆弱性情報を確認して、適宜アップデートを実施してください。**
- **・VPN 利用時のパスワードは推測されにくいものになっているかを確認し、適切に管理して下さい。**

リモートデスクトップとは

リモートデスクトップとは、あるコンピュータをネットワーク接続された別のコンピュータで遠隔操作する技術の総称です。

Windows に標準で搭載されているほか、様々なリモートデスクトップサービスが提供されておりインターネットで利用できます。

【メリット】
- ・自宅やその他の場所から職場のコンピュータにあるデータの編集やアプリの利用が可能
- ・性能が低いコンピュータでも職場のコンピュータを遠隔操作でき、コストの低減や業務効率化が図れる

リモートデスクトップは、導入しやく用途も多岐にわたりますが、外部からアクセスする仕組みのため、攻撃対象となりやすいというリスクもあります。

【確認・対策】
- **・アクセスできる人（接続元 IP アドレス）を制限して、アクセスを管理して下さい。**
- **・VPN を併用して安全性を高めてください。**
- **・リモートデスクトップ利用時のパスワードは、推測されにくいものにし、二段階認証を採用することも検討してください。**

・・・・・・・・・・・・・・・・ランサムウェアによるサイバー攻撃に注意・・・・・・・・・・・・・・・・

国内外でランサムウェア感染による業務支障が多く報道されています。特に、事前にネットワークに侵入し窃取したデータを公開すると脅迫し、仮想通貨を要求する手法や、ネットワークに侵入して重要情報が格納されたサーバ等を暗号化する攻撃が確認されています。

重要なデータは必ずバックアップをとり、さらにオフラインで保管するようにしてください。

また、機微データや個人情報等は、特別なアクセス制御や暗号化を実施するなどの措置を行うようにして下さい。

参照：内閣サイバーセキュリティセンター「ランサムウェアによるサイバー攻撃について【注意喚起】
https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf

［お知らせ］ ウイルス感染対策を装った詐欺にご注意願います。ギフトカードでの費用請求は詐欺です。

滋賀県警察本部サイバー犯罪対策課　（代表）077-522-1231