滋賀県警察からのお知らせ

サイバーセキュリティ情報 CSI

事業者の皆さまに、注目のサイバーセキュリティに関する情報をお届けします。

R３年度No.１

狙われるデジタル社会
VPNやクラウドのセキュリティ対策の確認を

デジタル社会の進展に伴い、VPNやクラウドサービスの利用が拡大していますが、VPNやクラウドサービスに対する攻撃が発生しています。
また、設定ミスや確認不足による情報漏えいが発生していますので、注意してください。

VPNが狙われる

VPN（Virtual Private Network）は、暗号化を用いることにより安全な通信が可能となる技術で、自宅等から社内ネットワークにアクセスする場合等に使用されています。
ところが、VPNは暗号化等により安全であるものの、外部との出入口を作ることになるので、攻撃者側から見ると侵入するチャンスとなります。
VPNを利用した社内ネットワークへのアクセスは、適切な設定が必要です。

VPNのセキュリティ対策

◆ **VPN機器のアップデート情報を確認しましょう。**
旧型のVPN機器の脆弱性をつかれて社内ネットワークに侵入された事案が発生しています。
VPN機器のアップデートやセキュリティパッチの適用状況を確認してください。

◆ **パスワード設定や認証方法を確認しましょう。**
複雑なパスワードを利用することは当然ですが、トークンやSMS認証を組み合わせる「多要素認証」を導入してください。

クラウドサービスが狙われる

企業向けのクラウドサービスが数多く展開されており、事業に関する様々な情報が外部のサーバで管理できるようになっています。
一方で、クラウドサービス事業者は、ユーザのニーズに応じてサービスを提供しているものの、サービス内容によっては、安全性が低くなる場合があります。
また、クラウドサービスも外部サーバですので、攻撃者側から見ると出入口となり得ます。
脆弱性や設定の不備は侵入される原因となります。

クラウドサービスのセキュリティ対策

◆ **サービス内容を確認しましょう。**
クラウドサービスは、様々な種類がありますので、セキュリティ面において必要なサービスが提供されるかどうかを確認してください。

◆ **クラウドサービスも適切に設定しましょう。**
アップデートされると、ユーザ側で再設定が必要になる場合があります。

◆ **アクセス権の設定を適切に行いましょう。**
アクセス権の設定は必要最小限の範囲で設定するようにしてください。

脆弱性情報のチェックサイト
機器やソフトウェアの脆弱性情報が公開されています。
脆弱性がある機器等は攻撃されるリスクが高まりますので、アップデート等を行いましょう。
JVN･･･https://jvn.jp
JPCERT/CC ･･･https://www.jpcert.or.jp

メール誤送信に注意してください。
メールの誤送信による情報流出事案も発生しております。
特に重要情報を添付して送付する場合は、送信先メールアドレスをしっかり確認するようにしてください。

«ビットコインを請求する架空請求メールが多数確認されていますのでご注意願います。»

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）