複数の道内企業が被害に！！

今年に入ってから道内企業のランサムウェアの感染被害が増加傾向にあります！
ランサムウェアの感染被害は、地域や業種・規模を問わず発生しています！

複数の道内企業がランサムウェア感染被害に

ランサムウェアとは、金銭を脅し取ることを目的としたソフトウェアで、コンピュータ内のファイルが暗号化されたり、あらかじめ情報が盗まれたりして「暗号化の解除」や「機密情報の公開を止める」などの名目で「身代金」を要求されます。

主な発生要因/手口

①VPN機器等の脆弱性によりネットワークに不正侵入されて感染
②リモートデスクトップのID・パスワードを不正利用されて感染

加えて、最近の被害傾向として、VPN機器等に対する不正アクセスが確認されています。
原因は、VPN機器等に設定されたパスワードが安易なものであったり、使用していないアカウントが残ったままになっていることなどが挙げられます。

感染リスクを減らすため

①VPN機器等のファームウェア、パソコンのOS、ウイルス対策ソフトなどは、適宜修正プログラムを適用し、常に最新の状態にアップデートする。
②VPN機器等のアカウントについて、パスワードの複雑化や多要素認証を導入し、**使用していないアカウントが設定されていないか、管理画面でよく確認する（あれば確実に削除）**。
③リモートデスクトップのパスワードの複雑化や多要素認証の導入など、不正アクセス対策を行う。

万が一感染した場合に備えて

①重要なデータは必ずバックアップを取り、バックアップを取った媒体は、必ずネットワークから切り離して保管する。
②バックアップを使って復元する手順の確認と訓練を実施する。
③有事に備えて担当部門(CSIRT)を設置し、対応手順の策定や教育等を行う。

被害に遭った場合は、所在地を管轄する警察署に通報してください

北海道警察サイバーセキュリティ対策本部