TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2021年 第12号

コロナ禍で急造したネットワーク環境に注意！

【被害事例】

1 ランサムウェア感染被害

国内の事業者がランサムウェアの被害に遭っている事例が複数確認されています。被害に遭った事業者の中には、**業務が一時停止せざるを得ない状況**に追い込まれた事例や、被害が自社だけでなく取引先企業に影響を及ぼした事例も確認されています。

被害事例の中には、新型コロナウイルス感染症対策として、急遽構築したテレワーク環境の不備を突かれて被害に遭った可能性が指摘されています。

2 サプライチェーン攻撃による情報流出

サプライチェーン攻撃は、企業間の供給網の弱点を狙った攻撃です。本社に比べてセキュリティ対策がぜい弱な出先機関や子会社、関連企業などを狙って攻撃し、本社等の企業内ネットワークに侵入して、**企業の機密情報を窃取**するものです。

被害事例では、海外の拠点（子会社）を踏み台として、本社の企業内ネットワークに侵入された事例が確認されています。

Check!

被害原因として、**「新型コロナウイルス感染症対策のため急造したネットワーク環境のぜい弱性」**が指摘されており、

◎　従来の業務形態で設計されたネットワークセキュリティのルールを一時的に変更したが、そのまま継続利用していないか。

◎　テレワークの利用促進のため、一時的に旧式のネットワーク機器を再利用したが、セキュリティ対策がぜい弱なままとなっていないか。

◎　過去に利用していた外部からのネットワーク接続ポイントが、閉じられないまま放置されていないか、失念していないか。

など、コロナ禍の一時的対応とした変更点等について、確認をお願いします。

今後益々、社会のデジタル化が進み、外部から企業内ネットワークにアクセスする機会は増加すると考えられることから、**コロナ禍における自社の業務形態に応じたネットワーク管理やセキュリティ対策**をお願いします。