F－CSNET通信かわら版

令和８年５月

「サプライチェーンリスク管理」

～自社と取引先を攻撃から守る～

攻撃者は防御の固い企業を直接狙うのではなく、サプライチェーンに含まれる中小企業を「踏み台」として悪用する場合があります。
警察庁の統計では、ランサムウェア被害の半数以上が中小企業で発生しており、その多くが取引先への納期遅延や機密情報の流出を招いています。

1　サプライチェーン攻撃の構図

攻撃者はいきなり大手を狙うのではなく、まず「守りの薄い中小企業」を狙う傾向があります。

【侵入】
脆弱なＶＰＮや、メールセキュリティを突破

→

【踏み台化】
侵入したＰＣから取引先に「なりすまして」侵入

→

【攻撃】
機密情報の窃取
サプライチェーン停止

2　実行させるべき３つの指示

多要素認証（ＭＦＡ）
パスワードだけでなくスマホ等での承認を必須化

脆弱性対応
ＯＳやＶＰＮ機器のアップデート、放置されたアカウントの削除

分離バックアップ
ネットワークから切り離したバックアップの定期的な確保

3　異常発生時の緊急対応フロー

ＳＴＥＰ１ 隔離	不審なＰＣのＬＡＮケーブルを抜き、Ｗｉ-Ｆｉをオフにする。電源は切らずにそのまま維持（証拠保全）する。
ＳＴＥＰ２ 報告	社内のセキュリティ担当及び経営層へ連絡し、被害範囲を特定する。
ＳＴＥＰ３ 外部連携	専門ベンダー、警察、ＩＰＡ、影響が懸念される「取引先」へ速やかに注意喚起を行う。

出典・参考：ＩＰＡ　中小企業の情報セキュリティ対策ガイドライン

◆ 福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止･拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などを、Ｘ（旧Twitter）やホームページに掲載していますので、ぜひご覧ください。

【Ｘ（旧Twitter）】

【ホームページ】