テレワーク拡大で懸念されるランサムウェア犯罪について(注意喚起)

テレワークのためには、多くの場合、セキュリティ対策として VPN 機器が利用されています。VPN 機器の脆弱性を放置した場合、VPN 機器の脆弱性を活用して認証情報を不正に取得し、認証情報を活用して、組織内のネットワークやシステムに不正にアクセスされ、機密情報を窃取される被害のリスクがあります。さらに、窃取した機密情報を暗号化して復号と引き換えに金銭を要求するケースやそれに加え窃取されたた機密情報をインターネット上に公開すると脅迫して金銭を窃取しようとする攻撃(いわゆるランサムウェアによる攻撃)が増加していると言われています。

今般、脆弱な Pulse Secure 製機器（VPN サーバー）から窃取したと見られる認証情報のリストが 2020 年８月３日にロシア語のダーク Web フォーラムに公開された旨の記事（注 1）が８月４日付け「米 ZDnet」に掲載されました。これを踏まえ、内閣サイバーセキュリティセンター(NISC)にて、当該データを入手し、解析したところ、厚生労働省所管行政分野に属する業務を実施していると考えられる企業の情報が含まれている旨の連絡がありました。

攻撃対象とされた VPN サーバーの脆弱性情報は、「Pulse Connect Secure の認証回避の脆弱性（CVE-2019-11510）に関する情報」（注 2）に掲載されていますのでご確認ください。

医療機関等でも同様の事案が発生する可能性がありますので、同機器を利用している情報システムを持っているかご確認頂き、当該システムについては更新プログラムが最新版となっているか点検を実施し、適用されていない場合は更新プログラムを適用する等、不備のないよう対応をお願いします。また、ID、パスワードによる認証だけでなく、多要素認証の導入も不正アクセスのリスクを低減する上で、有効な手段となりますのでご検討ください。

ひとたび、サイバー攻撃の被害が発生した場合、技術的相談を受けることや、他の医療機関への横展開対策等の早急な対応が必要な場合もあるため、当該事案についてご認識いただくとともに、サイバー攻撃被害時の対処手順、連絡体制の再確認をお願いします。

注１：８月４日付け「米 ZDnet」記事
https://japan.zdnet.com/article/35157986/

同記事では、リモートアクセスツールの脆弱性を攻撃することにより認証情報を取得し、企業内のシステムやネットワークに不正侵入することで、機密情報を窃取、それらの情報を暗号化して復号と引き換えに金銭を要求するケースやそれに加え、窃取した機密情報をインターネット上に公開すると脅迫して金銭を窃取しようとする攻撃(いわゆるランサムウェアによる攻撃)が増加している旨が掲載されています。

注２：Pulse Connect Secure の認証回避の脆弱性（CVE-2019-11510）に関する情報
（JPCERT コーディネーションセンター）
https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html