ランサムウエア対策を万全に

22年上期の被害件数は過去最多

ランサムウエアが猛威を振るい、事業活動の停止や遅延など、社会経済活動に大きな影響を及ぼしている。ランサムウエアとは、感染すると端末上のデータなどが暗号化され、そのデータを復号する（元に戻す）対価として金銭を要求する不正プログラムのこと。2022年は、自動車関連企業にてサプライチェーン全体が影響を受ける事案や、医療機関にて新規患者の受け入れを停止する事案などが発生し報道でも大きく取り上げられた。警察庁が9月に公表した資料によると、22年上期の被害件数は過去最多の114件、うち59件（52％）が中小企業からの相談であったことから、中小企業にとっても他人事ではない。ランサムウエアに関しては本誌連載でも度々取り上げているが、最近は連載ｖｏｌ・42（QRコード参照）で解説した標的型サイバー攻撃と同様の攻撃手法を駆使して企業のネットワークに侵入し、暗号化する前にデータを窃取しておき、支払わなければデータを公開するなどと脅迫するタイプ（以下、侵入型ランサムウエア攻撃）が多く確認されている。そこで今回は、もしも侵入型ランサムウエア攻撃を受けた場合にどのように対処すべきかを解説する。

侵入経路をふさぎ原因究明を

データが暗号化されて開けなくなったり、金銭を要求するポップアップが表示されるなどランサムウエア感染被害を確認した場合、まずは被害拡大を防ぐために、感染した端末をネットワークから切り離す。複数の端末で同時に被害が発生した場合は、ドメインコントローラーなど管理サーバーの管理者アカウントの権限を悪用してランサムウエアの一斉配布・実行が行われた可能性があるため、管理者アカウントの侵害調査やパスワードの変更などを行う。

次に、被害の原因を特定し対処する。データの復元などを実施する前に被害の原因となった侵入経路をふさがないと、再度攻撃を受ける恐れがある。

原因を特定するためには、端末やネットワーク機器のログ調査や解析が必要となる。最近の被害では、リモートアクセス（遠隔操作など）の出入り口を経由した侵入や、ＳＳＬ－ＶＰＮ（仮想専用回線）など外部から接続可能なシステムの脆弱性を悪用した侵入などが多く報告されているので重点的に確認していただきたいが、自社の担当者では確認が難しい場合は、外部専門組織に相談してほしい。

被害からの復旧に当たっては、隔離した端末をネットワークに戻す前に、攻撃者が仕掛けた他の不正プログラムや不正な設定がないか確認する。その後、バックアップからデータを復元する。バックアップが取れていない場合は、復号ツールが公開されていないかランサムウエアの被害低減を目指す国際的なプロジェクト「ＮｏＭｏｒｅ Ｒａｎｓｏｍ」（QRコード参照）で確認してもよいであろう。攻撃者に対して身代金を支払うことは推奨されない。判断や対応に迷った際は、外部専門組織や警察などへ相談してほしい。

独立行政法人情報処理推進機構（ＩＰＡ）では、ランサムウエア対策の特設サイトを公開している（QRコード参照）。平時の備えや有事の対応方法、外部参考サイトの情報などをまとめているので参考にしてほしい。

（独立行政法人情報処理推進機構・江島将和）

「ランサムウエアによる被害」のイメージ

中小企業のセキュリティ対策 vol.42

NoMore Ransom ポータルサイト

ＩＰＡランサムウエア対策特設サイト