昨今、身代金として金銭を得ることを目的に、企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを一斉に暗号化して使用できなくしたり、データを窃取して公開すると脅迫したりする「ランサムウェア攻撃」と呼ばれるサイバー攻撃が多発しています。大量のデータやシステム全体が被害に遭い、事業継続が脅かされる可能性があるため注意が必要です。こうした被害を未然に防ぐため、以下のような対策を講じることが推奨されます。

【一般的に推奨される対策等】

○ 有事への備え

・インターネットからアクセス可能な機器を必要最小限にする。

- テレワーク導入時の設置機器や事業部門が独自に設置した機器等、システム管理部門が把握できていない場合もあるので全社的な調査をしましょう。

・使用機器やソフトウェアの脆弱性を解消する。

- ソフトウェアを適宜最新に更新した上で、適切な設定がされているか確認しましょう。

・定期的に重要なデータをバックアップする。

- ランサムウェア感染時にバックアップデータが削除されることがあるため、バックアップ時以外はシステムから切り離すなど、バックアップデータの保全を再確認しましょう。

・原因究明、被害調査のためのログを確保する。

- システムの運用を外部委託している場合でもログを取得できるかを確認しましょう。

○ 被害発生時の対応想定

・取引先や関係機関へ、速やかに事情を説明する。

- 調査の結果や事業への影響を報告するよう要請されるケースもあります。

・警察へ被害を報告する。

・対応費用を調達する。

- 事業の機会損失が発生するほか、調査や復旧費用など緊急で費用が必要になることがあります。

・経営計画・体制を見直す。

・再発防止策を実施する。

- 適切に再発防止をするには、適切に原因を把握する必要があり、ログの保管や調査体制が必要です。

攻撃手法や影響の詳細や、上記以外の対策等については、独立行政法人情報処理推進機構（IPA）が下記 URL にて公開しているレポートなどをご参照ください。

https://www.ipa.go.jp/security/announce/2020-ransom.html#REPORT

〔参考情報サイト〕

＊サイバーセキュリティ経営ガイドライン

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

＊サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

https://www.ipa.go.jp/security/keihatsu/sme/sc3/index.html

＊経産省からの注意喚起

https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

◇ 産業サイバーセキュリティセンター（人材育成事業）

【中核人材育成プログラム（1 年間の教育プログラム）】

https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html

【戦略マネジメント系セミナー（4 日間の講演・講義）】

https://www.ipa.go.jp/icscoe/program/middle/strategic_management/index.html