令和４年２月２３日
経済産業省

昨今の情勢を踏まえたサイバーセキュリティ対策の強化について
（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案の潜在的なリスクは高まっていると考えられます。

各企業・団体においては、経営者のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

不審な動きを把握した場合は、早期対処のために速やかに経済産業省やセキュリティ関係機関に御相談ください。

１．リスク低減のための措置

〇パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。

〇IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。　※下記 URL 参照

〇メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

２．インシデントの早期検知

〇サーバ等における各種ログを確認する。

〇通信の監視・分析やアクセスコントロールを再点検する。

３．インシデント発生時の適切な対処・回復

〇データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

〇インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

そのほか、サイバーセキュリティ対策については、以下 URL を御参照ください。

- 独立行政法人情報処理推進機構（IPA）
  - セキュリティ関連情報サイト
    https://www.ipa.go.jp/security/
  - 情報セキュリティ安心相談窓口
    https://www.ipa.go.jp/security/anshin/
  - その他（届出・相談・情報提供）窓口一覧
    https://www.ipa.go.jp/security/outline/todoke-top-j.html

- JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)
  - 注意喚起サイト
    https://www.jpcert.or.jp/at/2022.html
  - インシデント対応依頼
    https://www.jpcert.or.jp/form/
  - 侵入型ランサムウェア攻撃を受けたら読む FAQ
    https://www.jpcert.or.jp/magazine/security/ransom-faq.html
  - ※ Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について
    https://www.jpcert.or.jp/newsflash/2020112701.html

- 経済産業省
  - 2021 年 4 月 2 日 「2020 年 12月18日発出「注意喚起」の Update ～最新事例から得られる教訓」
    https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/006_03_00.pdf
  - 2020 年 12 月 18 日 「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」
    https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html
  - 2020 年 6 月 12 日 「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書」
    https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html
  - 2020 年 4 月 17 日 「産業界へのメッセージ」
    https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf

以上