令和４年３月２４日
経済産業省
総務省
警察庁
内閣官房内閣サイバーセキュリティセンター

現下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）

昨今のサイバー攻撃事案のリスクの高まりを踏まえ、政府においては、２月 23 日に「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（別添１）」、３月１日に「サイバーセキュリティ対策の強化について（別添２）」注意喚起を行っております。

その後も、国内では、ランサムウェアによる攻撃をはじめとするサイバー攻撃事案の報告が続いており、また、エモテットと呼ばれるマルウェアの増加も見られるところです。また、米国では、３月 21 日に、バイデン大統領が、国内の重要インフラ事業者等に対して、ロシアが潜在的なサイバー攻撃の選択肢を模索しており警戒を呼びかける声明を発表するとともに、企業等に対してサイバーセキュリティ対策を強化する具体策を提示しています。

このような現下の情勢を踏まえ、政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部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、上記の２月 23 日及び３月１日の注意喚起にある対策（①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復）の徹底をあらためてお願いいたします。また、ランサムウェアやエモテットについては、これまで専門機関等において公表している情報・サイトを確認の上、対応を講じるようお願いいたします。あわせて、不審な動き等を検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して情報提供いただくとともに、警察にもご相談ください。

【参考】
＜これまでの注意喚起＞
〇２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）」
https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf

〇３月１日　経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、ＮＩＳＣ「サイバーセキュリティ対策の強化について（注意喚起）」
https://www.nisc.go.jp/press/pdf/20220301NISC_press.pdf

＜ランサムウェア対策＞
〇ストップ！ ランサムウェア　ランサムウェア特設ページ　STOP! RANSOMWARE
https://security-portal.nisc.go.jp/stopransomware/

〇ランサムウェア対策特設ページ（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

〇侵入型ランサムウェア攻撃を受けたら読む FAQ（一般社団法人 JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

〇ランサムウエア対策特設サイト（一般社団法人 JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html

＜エモテット＞
〇「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/announce/20191202.html

〇マルウェア Emotet の感染再拡大に関する注意喚起（一般社団法人 JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/at/2022/at220006.html

＜中小企業向け対策＞
〇サイバーセキュリティお助け隊（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/otasuketai-pr/

＜外国の動向＞
〇３月 21 日　米国「国家によるサイバーセキュリティに関する声明」（英文）
https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

〇３月 21 日　米国ホワイトハウス「[ファクトシート]潜在的なサイバー攻撃から身を守るために今すぐ行動しよう。」（英文）

https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

〇３月 18 日　英国国家サイバーセキュリティセンター（NCSC）による注意喚起（英文）
https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences

〇３月４日　ドイツ連邦情報技術セキュリティ庁（BSI）による注意喚起（独文）
https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html

〇３月 15 日　ドイツ連邦情報技術セキュリティ庁（BSI）によるカスペルスキー社製アンチウイルス製品の使用に関する注意喚起（独文）
https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html

別添１

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

別添２

令和４年３月１日
経済産業省
金融庁
総務省
厚生労働省
国土交通省
警察庁
内閣官房内閣サイバーセキュリティセンター

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リスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部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、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、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。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

１．リスク低減のための措置

○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。

○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。

○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

○サーバ等における各種ログを確認する。

○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

○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。

○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。