

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>

○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>

○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>

○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/>

○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

○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>

○ランサムウェア対策特設サイト（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>

○「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>

○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>

○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>

○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/>

○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/>

○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>

○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](https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html)

○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](https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html)