令和４年９月５日
製造産業局　生活製品課
商務情報政策局　サイバーセキュリティ課

サイバーセキュリティ対策の強化について（注意喚起）

昨今においてはサイバー攻撃被害のリスクが高まっており、ランサムウェアをはじめとするサイバー攻撃被害が国内外の様々な企業・団体等で続いています。

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、以下に掲げる対策を参考に、サイバーセキュリティ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とともに、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もあるため、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．サイバーセキュリティ対策を徹底し、持続可能な体制を確立する

- ○保有する情報資産を漏れなく把握する。
- ○不審なメールへの警戒や、機器等に対して最新のセキュリティパッチを当てる等、脆弱性対策を徹底する。
- ○多要素認証（※1）等により認証を強化する。
- ○データ滅失に備えデータのバックアップを取得し、ネットワークから切り離された場所に保管する。
- ○サイバー攻撃を受けた際の対応について、普段から役員および職員に対して教育・訓練を行う。
- ○システムが停止した場合に、業務を止めないための計画（BCP）を策定し、代替手段を整備する。

２．感染が確認された場合には、適時、報告・相談・対応を行う

- ○感染拡大防止に留意するとともに、専門機関やセキュリティベンダー等へ支援を依頼しつつ、早期の業務復旧を図る。
- ○サイバー攻撃者への金銭の支払いは厳に慎む。
- ○Emotet（※2）の場合、取引関係者間などで感染が拡大することから、取引先を含めた関係者に状況を共有する。
- ○警察、所管省庁等への相談・報告・届出を実施する。報告義務のある事案については、正確かつ迅速に行う。

※1　本人確認のために、ID・パスワードに加えて指紋認証を行う等、２つ以上の異なる認証要素（記憶情報、所持情報、生体情報のうち２つ以上）を用いて認証する方法。
※2　Emotet（エモテット）は、情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大が試みられる。

３．中小企業においては「サイバーセキュリティお助け隊サービス（※）」などの支援パッケージを活用する

- ○自社がサイバー攻撃による被害を受けた場合、その影響は、サプライチェーン全体の事業活動や経済全体に及ぶ可能性があることを踏まえ、「サイバーセキ

ュリティお助け隊サービス」の活用など積極的なサイバーセキュリティ対策に取り組む。

※異常監視や、サイバー攻撃を受けた初動対応支援、被害を受けた場合の簡易保険など、中小企業に必要な対策をワンパッケージにまとめたサービス。また「IT 導入補助金」で当サービス利用料の 1/2 を補助します。
・サイバーセキュリティお助け隊サービス　https://www.ipa.go.jp/security/otasuketai-pr/
・IT 導入補助金　セキュリティ対策推進枠　https://www.it-hojo.jp/security/

４．IT サービス等提供事業者は、製品・サービスのセキュリティ対策に責任を持つ

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
  - 中小企業向け情報セキュリティ対策
    https://www.ipa.go.jp/security/keihatsu/sme/index.html
  - IPA 情報セキュリティセミナーのコースと関連資料のご案内
    https://www.ipa.go.jp/security/seminar/isec-semi/standard_course_guide.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（製品名：FortiGate） 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
  - 2022 年 8 月 8 日 「夏季の長期休暇において実施いただきたい対策について（注意喚起）」
    https://www.meti.go.jp/press/2022/08/20220808003/20220808003.html
  - 2022 年 4 月 25 日 「春の大型連休に向けて実施いただきたい対策について（注意喚起）」
    https://www.meti.go.jp/press/2022/04/20220425003/20220425003.html
  - 2022 年 4 月 11 日 「産業界へのメッセージ」
    https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20220411.pdf
  - 2022 年 3 月 24 日 「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）」
    https://www.meti.go.jp/press/2021/03/20220324008/20220324008-1.pdf

- 中小企業庁
  - 中小企業の情報セキュリティ
    https://www.chusho.meti.go.jp/keiei/gijut/security.htm

- 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・ポータルサイト
    https://security-portal.nisc.go.jp/

（参考）繊維業界における被害例

○A社における不正アクセス事案

A社ECサイトに対する不正アクセスの被害が発覚。約25万人分の個人情報（氏名、電話番号、住所、生年月日、性別、メールアドレス）が流出。

公開不要なサーバーへのアクセス制限がなかったこと及びECサイトから会員情報を呼び出すプロセスの脆弱性を悪用されたことが原因。

攻撃元IPアドレスのブロック、監視強化、会員情報取得処理の変更などの対策を実施。

○B社における不正アクセス事案

B社ECサイトに対する不正アクセスにより、約1万5,000人分のクレジットカード情報（カード名義人名、クレジットカード番号、有効期限、セキュリティコード）が流出。

同社ECシステムの脆弱性をついた第三者の不正アクセスにより、決済システムの改ざんが行われたことが原因。

同社に対して一部のクレジットカード会社より、情報漏洩の懸念について連絡があり、同日にECサイトの運用及びカード決済を停止。その後、第三者調査機関による調査を開始し、調査結果を受け、セキュリティ対策を強化した新システムを構築中。