サイバーセキュリティ対策についての産業界へのメッセージ

2022 年４月 11 日
産業サイバーセキュリティ研究会

《経営者の皆様へのメッセージのポイント》

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
２．感染が確認された場合には、適時、報告・相談・対応を行う
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
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

昨今、ランサムウェアや Emotet（エモテット）と呼ばれる不正プログラムをはじめとして、サイバー攻撃による被害が増加傾向にあります。

ランサムウェアは、感染したパソコンやサーバ機器のデータを暗号化することで使用できない状態にし、復号する（元に戻す）ことの見返りとして金銭を要求する不正プログラムです。2021 年に全国の都道府県警察から警察庁に報告があった件数は 146 件であり、前年と比較可能な７～12 月だけで４倍に増加しています。また、実際には報告、公開されない事案も相当数ある可能性もあります。

Emotet は、情報の窃取や他の不正プログラムへの感染に悪用される不正プログラムの一種で、取引先との正当なやりとりを装うなど不正なメールによる攻撃が行われます。また、Emotet が起点となり、他のサイバー攻撃に発展する可能性があります。Emotet は 2021 年１月にテイクダウン（押収）及び無害化されましたが、2021 年 11 月以降活動の再開が確認されており、３月に入り 2020 年の感染ピーク時の約５倍以上に増加しているとのデータも確認されています。

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講じることにより、対策の強化に努めていただくとともに、被害を受けた場合の適切な対応が必要です。（経営者が認識すべき原則、及び経営者が指示すべき重要項目は、サイバーセキュリティ経営ガイドラインにまとめられています。）

IT サービス等提供事業者（機器やサービス等を提供する事業者）においては、提供する機器やサービス等の脆弱性が侵入口となり大きな被害となるケースがありますので、提供する機器やサービス等のセキュリティが確保されるよう留意が必要です。また、被害組織から助言を求められるケースが想定されるため、独立行政法人情報処理推進機構（以下、IPA）や一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）等の公開資料を参考にする等、適切な助言ができるように留意が必要です。

取引先や子会社などを含むサプライチェーンに留意した対応が必要であることはもちろんですが、海外支店や子会社などを保有する企業においては、海外拠点のシステム等についても国内と同様に具体的な支援・指示等によるセキュリティ対策が必要です。

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

- 保有資産を IT 部門や情報セキュリティ部門が全社を対象に洗い出すとともに、最新のセキュリティパッチを当てるなど、脆弱性対策を徹底する。VPN 機器（リモート接続機器）を含め、

保有資産へのアクセス経路となり得る外部公開資産には特に留意する。(VPN 機器の脆弱性を悪用されパスワードを盗まれることがあり、その場合はバージョンアップに加え、パスワードを変更することが必要。)

- 受信したメールの添付ファイルを開く前に送信元を確認する、利用環境で添付ファイルのマクロが自動実行されないような設定を確認するといった教育を行うことに加え、メールサーバで不正な添付ファイルや本文の不正な URL を検出・削除する機能を導入する。(マクロとは、複数の操作を一括で実行するための機能で、不正プログラムの実行にも使用される場合があります。)
- システムに多要素認証を適用する等により認証を強化する。
- あらかじめ重要な情報を暗号化することで、保有資産が窃取された場合であっても、外部環境では復号できないようにする。
- 感染に備えパソコンやサーバ機器内にある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バックアップデータを保管するとともに、バックアップからシステムを復旧できることの確認・訓練を定期的に実施する。
- 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。
- 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・訓練を行うとともに、事前のインシデント対応計画の策定と、被害を最小限に抑えるための迅速対応の態勢(特に、経営層への報告)を確立する。

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(下記 URL 参照)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。
- ランサムウェアの場合、金銭を支払ったとしても復号できたり、機密情報の暴露を止めたりできる保証はないため、ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎む。
- 取引先を含めた関係者に状況を共有する。特に Emotet の場合は、取引関係者間などで感染が拡大することから、早急な連絡が望まれる。
- 警察、個人情報保護委員会(個人情報の漏えいが疑われる場合)、所管省庁等への報告・届出を実施する。特に、関連法令等の則った適切な措置を講じる。

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、その影響は自社にとどまらず、サプライチェーン全体の事業活動に及ぶ可能性があることを踏まえ、中小企業も積極的なサイバーセキュリティ対策に取り組むことが必要。
- 中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度である「SECURITY ACTION」を活用ことで、情報セキュリティ５か条から取組を始め、対策のステップアップを進めていくことが可能。
- 「サイバーセキュリティお助け隊サービス」など中小企業向けに開発された支援パッケージを活用することも推奨。(なお、中小企業向けに、サーバ等の異常監視や、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について、独立行政法人情報処理推進機構(IPA)が「サイバーセキ

ュリティお助け隊サービス」として認定し、12 事業者がサービスを提供しています。）
参考、中小企業の情報セキュリティ：https://www.chusho.meti.go.jp/keiei/gijut/security.htm

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

- 顧客の情報資産やプライバシーを保護するために、提供する製品・サービスにセキュリティ対策を実施する。また、製品・サービスの重大な脆弱性が公表された場合には、例えば顧客へ連絡する等の対応を行う。
- 認証された開発者のみが使用できる環境でソフトウェアを開発する。
- ソースコードレビューの実施やエラーチェックツールを用いて、開発工程や出荷前に、既知および潜在的な脆弱性の有無を確認する。使用しているオープンソースソフトウェア等について、提供元のコミュニティ等を確認し、バグやセキュリティ関連情報、サポート情報を確認する。

そのほか、サイバー攻撃への対応の専門機関である IPA や JPCERT/CC からもランサムウェアや Emotet 等に関する情報が発信されておりますので、以下 URL を御参照ください。

➢ これまでの注意喚起
- ✧ 2022 年３月 24 日　経済産業省、総務省、警察庁、NISC
  「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
- ✧ 2022 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、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
- ✧ 2022 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）」
  https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf

➢ 経済産業省／独立行政法人情報処理推進機構（IPA）
- ✧ 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/
- ✧ ランサムウェア対策特設ページ
  https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
- ✧ 「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
  https://www.ipa.go.jp/security/announce/20191202.html
- ✧ 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

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