「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い」に対する報告結果及び「中小企業向けサイバーセキュリティ事後対応支援実証事業（いわゆる「サイバーセキュリティお助け隊」）」の事業報告を踏まえた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

経　済　産　業　省
商　務　情　報　政　策　局
サ イ バ ー セ キ ュ リ テ ィ 課
令　和　２　年　６　月　１２　日

内容

1. 本報告をとりまとめた趣旨

今年に入り、三菱電機、NEC 等が高度なサイバー攻撃を受けていたことが明らかとなり、また、サイバー攻撃により、企業情報が流出した可能性がある事例が続いていることなどについて、経済産業省はこの状況を重く受け止めているところです。

今年 1 月 31 日、経済産業省は、「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い（以下、「報告の依頼」という。）」を発出し、各産業団体に対して、機微情報を保有する企業に対して『サイバーセキュリティ経営ガイドライン Ver2.0』などの周知徹底を改めて求めるとともに、十分なセキュリティ対策が実施されていることを今一度点検するように依頼しました。特に防衛・宇宙関連や重要インフラ事業者との取引を行っている企業については、点検の結果、サイバー攻撃による重要な情報の漏えい等の可能性があった場合には、今年 2 月 14 日までに経済産業省まで報告するように求めました。

実際に経済産業省に届いた企業からの報告は、情報の漏えいに関わることに留まらず、サイバーセキュリティに係る自社の取組状況など、多様な内容を含むものでした。そうした報告内容の多様性は、情報漏えいの発生の有無を超えて、昨今のサイバーセキュリティに係る状況を把握するために有意なものであり、こうした報告内容をより適切に把握するため、2 月 14 日の報告の提出を受けた後、追加調査依頼やヒアリングなどを実施してきたところです。

また、「報告の依頼」に基づく企業からの報告とりまとめ作業と並行して、サプライチェーン全体におけるサイバーセキュリティ対策を強化するために取り組んできた「中小企業向けサイバーセキュリティ事後対応実証事業（以下「サイバーセキュリティお助け隊」）という。」に参加して、中小企業にセキュリティサービスを提供してきた事業者からの報告が、独立行政法人情報処理推進機構（以下「IPA」という。）を通じて、経済産業省に届きました。

「サイバーセキュリティお助け隊」では、中小企業に実際に事後対応支援サービスを実施する実証事業を通じて、中小企業に対するサイバー攻撃やそれに対する中小企業の具体的な支援ニーズを明らかにする取組が進められてきましたが、こうした活動の結果、実際にどのようなサイバー攻撃が行われ、どのような対処を行うことで被害の拡大を防ぐことができたか、という事例が明らかになってきています。

本報告は、「報告の依頼」の報告結果をとりまとめることに留まらず、「サイバーセキュリティお助け隊」で明らかになった事案も踏まえて、中小企業を含めたサプライ

チェーン全体を視野において、昨今の産業が直面するサイバーセキュリティに関わる状況について、経済産業省としての認識をまとめたものです。

　加えて、本報告では、昨今の状況に関する認識を踏まえた今後の取組の方向性についても提示しています。今後、ここで示した取組の方向性について、サプライチェーン全体のサイバーセキュリティ対策として具体化すべく、産業界等の関係者との調整に着手したいと考えています。

2. 本報告のとりまとめに当たって基礎となった取組

2.1. 「報告の依頼」について

① 趣旨

今年に入り、三菱電機、NEC 等が高度なサイバー攻撃を受けていたことが明らかとなりましたが、サイバー事案に対する社会的関心は非常に高く、これへの対応は、ステークホルダ等とのコミュニケーション等を間違えると会社の経営そのものに深刻な影響を与え得るという意味で経営問題そのものです。したがって、経営者の責任において、より広い視点から、関係機関への報告や対外公表などを含めて、リスクの適切な管理のためのマネジメントの確立とその適切な実施に努めていただく必要があることから、今年 1 月 31 日に「報告の依頼」を発出させていただきました。

② 依頼内容

1. 周知と点検
   - 機微情報を保有する企業に、『サイバーセキュリティ経営ガイドライン Ver.2.0』など[1]の周知徹底と、最新の攻撃手法やそれへの対策を理解の上、『サイバーセキュリティ経営ガイドライン Ver.2.0』などを踏まえた十分なセキュリティ対策が実施されていることを、今一度点検することを依頼。
2. 経済産業省への報告
   - 特に防衛・宇宙関連や重要インフラ事業者との取引を行っている企業に関しては、点検の結果、サイバー攻撃による重要な情報の漏えい等の可能性があったものについて、2 月 14 日までの経済産業省への報告を依頼。

[1] セキュリティ対策時に参照する文書等の例
経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0」
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
IPA「標的型サイバー攻撃対策」
https://www.ipa.go.jp/security/ta/index.html

3. 事案の公表

- その上で、機微情報を保有する企業全体でセキュリティ対策を高めていけるよう、攻撃側を利することのないよう検討した上で、適切な場合には、事案の公表を依頼。

2.2. 「サイバーセキュリティお助け隊」について

① 趣旨

多くの中小企業はサイバーセキュリティに対する意識が低く、自社がサイバー攻撃に遭うと思っていないため、サイバー攻撃に遭っていること自体に気付かず、その結果、サイバー攻撃の被害が拡大するケースも発生しています。また、多くの中小企業は IT やサイバーセキュリティに関する知識が十分でなく、IT に関するトラブルが発生した際にシステムの不具合が原因なのか、サイバー攻撃が原因であるか自社で判断することが困難です。

一方で、セキュリティサービス提供側は、中小企業の被害実態や中小企業支援に必要な人材スキル等を正確に把握出来ていないため、現状は中小企業のニーズに合った製品、サービスを十分に提供することができていません。

そのため、中小企業が使いやすいサイバーセキュリティ製品（事前対策）や、トラブル時に相談できる窓口、サイバー攻撃に遭った際に事後対応をするサービス（事後対策）に対する潜在的なニーズは存在するものの、需要側と供給側が上手くかみ合っておらず、中小企業のサイバーセキュリティ対策が思うように進まない状況にあります。

サイバーセキュリティお助け隊は、こうした状況を踏まえ、中小企業のサイバーセキュリティに対する意識の向上を図るとともに、中小企業の実態に合ったセキュリティ製品、サービスの開発や市場投入を支援し、中小企業にサイバーセキュリティ対策を定着させていくことを目的として取組が進められました。

② 事業内容

全国 8 地域（図 1 参照）において、地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした実証事業を実施しました。実証期間は 2019 年 6 月～2020 年 3 月で、実証に参加した中小企業は 8 地域合計で 1,064 社になりました。

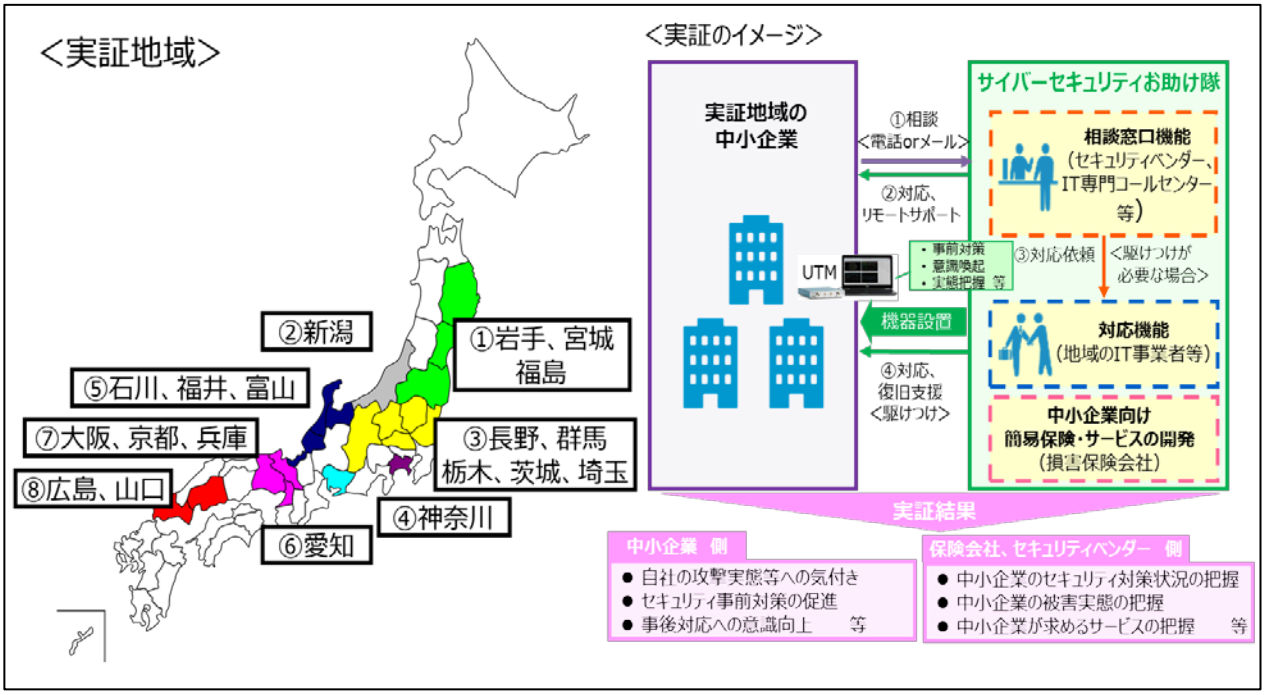

図 1:サイバーセキュリティお助け隊実証事業

3. 昨今のサイバーセキュリティに係る状況について

ポイント

- **標的型攻撃のさらなる高度化**
  ① マルウェア添付メール経由での感染等に加え、ネットワーク機器の脆弱性や設定ミスを利用することで、ユーザの動作を介さずに直接組織内のシステムに侵入する手法等が確認されています。
  ② さらに、侵入後もPowerShell 等を用いたファイルレスの攻撃や、C&C サーバ [2]との通信の暗号化、痕跡の消去など、攻撃の早期検知と手法の分析を困難にする攻撃手法が確認されています。

- **サイバー攻撃起点の変化（サプライチェーンの弱点を悪用した攻撃）**
  ① 海外拠点や取引先など、サプライチェーンの中で相対的にセキュリティが弱い組織が攻撃の起点となり、そこを踏み台にして、侵入拡大を図る事例も増加しています。

- **不正ログイン被害の継続的な発生**
  ① ID とパスワードのみで利用可能な会員制サイトや、クラウドメールアカウント等が、リスト型攻撃により不正ログインされる事案が継続的に発生しています。

- **中小企業に対するサイバー攻撃の実態**
  ① 地域や企業の規模にかかわらず、全国の中小企業もサイバー攻撃を受けていることが明らかとなりました。
  ② 想定被害額が 5,500 万円と算定される攻撃も確認されています。

3.1. 「報告の依頼」に基づく報告等を踏まえた状況の整理

3.1.1.報告結果

2 月 14 日を期限とする「報告の依頼」に応じて 40 件弱の報告がありましたが、軽微なインシデントの発生や既に公表した事案に関する内容で、重要情報の流出に関する報告はありませんでした。ただし、重要情報の流出は無かったものの、攻撃

[2] Command and Control サーバの略。攻撃者がマルウェアに対して指令となるコマンドを送信し、マルウェアが 仕掛けられたコンピュータの動作を制御するために用いられる。

を受けてマルウェアに感染した事例については報告がありました。また、期限後にインシデントを検知した事案についても報告を受けており、現在重要情報の流出がないかを調査中です。

報告の多くは、『サイバーセキュリティ経営ガイドライン Ver2.0』などの最新の攻撃手法やそれへの対策を理解の上、十分なセキュリティ対策が実施されているかどうかの点検を求めたため、点検結果に対する報告でした。

3.1.2.各企業におけるサイバーセキュリティの取組

点検結果について御報告いただいた概要は以下のとおりです。

① 過去に「サイバーセキュリティ経営ガイドライン Ver.2.0 付録 A サイバーセキュリティ経営チェックシート」に基づいて社内で点検を実施済だったが、今回改めて再点検を実施。過去の点検結果と比較を行い、既に対応している事項、改善されている事項、今後対応が必要な事項等をとりまとめ、不十分な事項については改善計画を立案したという報告。
② 「サイバーセキュリティ経営ガイドライン Ver.2.」の 10 個の指示事項に基づいてセキュリティ対策の点検を実施。対策が不十分と判定された事項については、以下の対応を実施予定という報告。
   - ✓ EDR[3]を導入する予定
   - ✓ セキュリティ教育を定期的に実施する予定
   - ✓ 今後 2 年間の体制・仕組みの整備計画を立てる予定
③ ISMS（JIS Q27001）で対応しているが、サイバー攻撃対策については、継続的に検討をしていくという報告。
④ グループ会社を含めて情報セキュリティ監査を年１回実施し、「サイバーセキュリティ経営ガイドライン Ver.2.0」に記載のセキュリティ対策が実施されていることを確認しているという報告。

3.1.3.サイバー攻撃による被害の状況

今回の「報告の依頼」に基づいて経済産業省に届けられた報告では、防衛・宇宙関連や重要インフラ事業者との取引を行っている企業において、サイバー攻撃によ

[3] Endpoint Detection and Response：エンドポイントでの検知・対応が行えるソリューション。

って重要な情報の漏えいが発生したとする報告はありませんでした。ただし、サイバー攻撃に係る攻撃者の技術が時々刻々と高度化する中、攻撃者が攻撃の痕跡を消すことなどによって、攻撃自体の秘匿や、被害が発覚した場合でも実際に行った情報窃取などの活動実態を分析できないようにするなどの仕掛けを施すことが常態化しています。

企業においては、こうしたサイバー攻撃の実態を認識し、引き続き、重要な情報の漏えい等がなかったかということについて、点検を行っていくことが肝要です。そして、もし、何らかの形で重要な情報の漏えい等の可能性があると思われる場合には、こうした「報告の依頼」の有無に関わらず、経済産業省に報告するよう、お願いします（詳細は P.19 4.2 ②を参照）。

今回の報告期間には、重要な情報の漏えいに関する報告はありませんでしたが、点検結果に対する報告及び昨今の三菱電機等の事案から把握された、特に注意が必要であると考えられることについて、以下に整理します。

① 依然として標的型攻撃に注意が必要

IPA が毎年公表する「情報セキュリティ 10 大脅威 2020[4]」（表 1 参照）では、「標的型攻撃による機密情報の窃取」が 2019 版に続いて 1 位となり、標的型攻撃が企業にとって依然として大きな脅威となっていることが分かります。

攻撃者は特定の企業を攻撃対象と定め、侵入経路を確立すべく、この対象に対して執拗に攻撃を繰り返します。侵入経路を確立する手法は様々で、標的型メールを使って攻撃対象の従業員等にマルウェア感染させるよう仕組むような手法のほか、通信機器の脆弱性や設定ミスを利用して侵入経路を確立する手法、攻撃対象の関連企業や取引先企業の情報システムを乗っ取り、そこを踏み台にして侵入経路の確立を図る手法（これは 4 位の「サプライチェーンの弱点を悪用した攻撃」に該当）など、あらゆる機会を使って侵入を図っていることが、サイバーセキュリティ専門家の報告なども含めた様々な事案から明らかになっています。

企業側の認識については、自社には絶対に守るべき機微情報はほとんどないので攻撃対象にはならないだろうなど、楽観的な見通しからサイバーセキュリティの取組の必要性を過小評価しているケースも見られます。しかし、既に述べたように、取

[4] https://www.ipa.go.jp/security/vuln/10threats2020.html

引先に攻撃するための侵入経路を確立するためにサイバー攻撃を仕掛けてくるおそれもあり、企業においては、取引先からの信用・信頼を維持し、自らの事業継続の安定性を高める観点から、自社がサイバー攻撃の対象になっている可能性があることを認識してサイバーセキュリティの取組を進めることが求められています。

表 1.　情報セキュリティ 10 大脅威 2020（組織向け）

順位	脅威
1 位	標的型攻撃による機密情報の窃取
2 位	内部不正による情報漏えい
3 位	ビジネスメール詐欺による金銭被害
4 位	サプライチェーンの弱点を悪用した攻撃
5 位	ランサムウェアによる被害
6 位	予期せぬ IT 基盤の障害に伴う業務停止
7 位	不注意による情報漏えい（規則は遵守）
8 位	インターネット上のサービスからの個人情報の窃取
9 位	IoT 機器の不正利用
10 位	サービス妨害攻撃によるサービスの停止

② 攻撃手法の高度化への対応を

侵入経路を確立する手法の多様化が進んでいることについては既に述べましたが、被害を受けた事案において専門家がフォレンジックなどを行って攻撃手法や被害実態などの分析を実施しても、必ずしも侵入経路を明確にすることができないケースが発生しています。これは、攻撃者が、侵入経路を確立した後、その痕跡を消すなどの技術的能力を持って、攻撃手法などの分析を妨害するための措置を施すことで、正確に分析することが困難であることが原因となっています。具体的には PowerShell 等を用いたファイルレスの攻撃や、C&C サーバとの通信の暗号化等の攻撃手法が使用される事案が確認されています。

こうした攻撃手法の高度化は、侵入経路の確立手法に加え、マルウェアの拡散技術にも見られます。攻撃対象企業のシステムに侵入後、マルウェアの特徴に基づいた検知システムを構築している場合でも、既存の検知システムに捕捉されずに組織内のシステムに拡散していくマルウェアの拡散技術が使用されています。このよう

な攻撃の典型的なケースといえる、正規のシステム制御の仕組みを悪用する攻撃は既に顕在化しており、ファイルレスの攻撃手法とあわせて実際に被害が報告された事案で利用されています。

こうした攻撃手法の高度化に対しては、まずは自らのシステムについて、資産構成をしっかりと把握してアクセス権限等を明確かつ適切に設定するとともに、システムを構成する機器・ソフトウェア等に関わる最新の脆弱性情報を把握し、速やかにパッチを当てるなどの取組を不断に継続していくことが重要です。こうした継続的な取組により、侵入経路の確立を防ぐとともに、仮に侵入をされたとしても、システム内部で水平・垂直に展開するために必要な起点となる機器等を乗っ取ることを難しくさせ、被害の拡大を防ぐことにつながります。

また、万が一、システムの侵入経路が確立され、サイバー攻撃がシステム内部に展開される事態になった場合には、こうした攻撃活動を早期に検知することが重要です。ただし、既に述べたように、攻撃手法が高度化する中で、既知のマルウェアや不正な通信先を検知したりする検知システムだけでは十分に対応できないケースも出てきていることから、システム内の振る舞いの異常から攻撃を検知する検知システムの活用などを検討することが適切です。

③ 海外の子会社等に対するサイバー攻撃の影響も視野に入れた体制の整備を

三菱電機の事案など、海外拠点等がサイバー攻撃の対象となったケースも明らかになっていますが、今回の「報告の依頼」に基づく報告の中でも、海外の現地法人がサイバー攻撃を受けたとの報告がありました。

攻撃者は、①で触れたような「標的型攻撃」を実施する中で、日本の本社等とはセキュリティ対応の状況が異なる海外の子会社などのシステムを乗っ取り、そこを起点にして日本の事業所のシステムに侵入して情報の窃取を行おうとしていた可能性も考えられます。

企業活動のグローバル化により、国境を越えてデータ等のビジネス資産を効率的に活用するためのシステム統合も進んでいますが、攻撃者の視点からは、こうした統合されたシステムは企業に対する攻撃の起点も拡がっていることになります。

企業の海外の子会社等は、自ら出資して設立をしているケースや現地法人を買収してグループに取り込んだケースなど事業体制が様々であり、かつ、海外のセキュリティビジネスの環境などが日本と異なることから、日本の事業所とは異なるサイバ

ーセキュリティ対策が採用されていることが少なくなく、そうしたセキュリティ対応状況の違いが、一旦侵入を許した場合に統合されたシステム全体の脆弱性として被害を拡大させてしまうおそれがあります。

グローバルにビジネス活動を拡大し、その活動内容の統合のレベルを上げていくほど、インシデントが発生した場合の被害も大きなものになるおそれがあることを認識し、ITシステム・ネットワーク構成を漏れなく特定した上で、影響範囲を限定するためのシステムの階層化などの構造変更を含め、海外の子会社等も含めたサイバーセキュリティの対応体制を整備することを計画的に進めていくことが一層必要になっています。

④ ウェブサービスに対するリスト型攻撃等への対応を

今回の「報告の依頼」の報告の対象とは異なりますが、ウェブサービスを行っているサーバが攻撃者に侵入され、個人情報が漏えいしてしまったという報告が増えています。

ウェブサービスは通常、顧客がブラウザを通じてサービスを提供するウェブサイトにアクセスし、ID/パスワードなどを入力して、購買などを行えるサイトへのアクセスや、自分のサービス利用履歴などを確認したり、クラウドメールを送受信することができるようにしたりするためのサービスです。

最近、こうしたウェブサービスを提供するウェブサイトに攻撃者がアクセスし、ID/パスワードの候補をリスト化した攻撃ツールを利用して様々な文字列等を入力してID/パスワードの一致を図り、ウェブサービスに本人になりすまして侵入する、いわゆるリスト型攻撃による個人情報の流出が報告されています。

被害を受けた多くのケースでは、ID/パスワードの入力だけで簡単にシステムにアクセスできるようになっていたり（いわゆる二段階認証となっていない）、個人に関わる情報が構造化されずに全てまとめて管理されていたりするため、一旦システムに入られると機微性の高いものも含めて全ての個人情報が盗み見られてしまうなどのシステム構成上の問題を抱えているケースが見られます。

多くのウェブサービスはインターネット経由で誰でもログイン画面のあるサイトにアクセスできるようになっていることから、こうした環境は攻撃者にとって侵入経路を確立するための入口が開いているような状況になっているという認識を持つ必要があります。ログインについては二段階認証、更に二要素認証を導入して、ウェブサービ

スのサイトへのアクセスに係るセキュリティ強化を図るとともに、個人に関わる情報について機微度に応じて分割して管理し、区分管理されたそれぞれのデータへのアクセス権を別に設定するなどのシステム構造の見直しなどを行うことが望ましいと考えられます。

3.2. 「サイバーセキュリティお助け隊」で対応したサイバー攻撃事例

サイバーセキュリティお助け隊では、全国 8 地域の 1,064 社の中小企業に UTM[5] や EDR 等の監視装置を設置し、重大なインシデントの可能性が検知された場合には、電話等による遠隔サポートや、現地への駆け付け支援を実施して対処を行いました。実証期間中にインシデント対応は合計で 128 件（12%の中小企業）発生しており、内訳は表 2 の通りです。

表 2:サイバーセキュリティお助け隊インシデント対応件数

対応種別	総数	内容	発生件数
インシデント対応	128 件	電話及びリモートによるインシデント対応 （訪問によるインシデント対応の一次対応を含む）	110 件
		訪問によるインシデント対応(駆け付け)	18 件

駆け付け対応が発生した 18 件のうち、特徴的な対応事例について、以下で説明します。

① 神奈川県の中小企業のインシデント事例（古い OS の使用）

- UTM 機器にて、社内から外部への不正な通信を検知し、駆け付け支援を実施。
- Windows XP でしか動作しないソフトウェア利用のために、マルウェア対策ソフト未導入の Windows XP 端末を使用。当該端末はインターネットに接続させていない認識だったが、社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。
- 当該端末を調査した結果、ワーム、トロイの木馬、迷惑ソフトその他計 25 ファイルの不正プログラムが発見されたため、駆除を実施。
- 検知・駆除できていなかった場合の想定被害額は 5,500 万円。

[5] Unified Threat Management：セキュリティ統合脅威管理ソリューション。

② 愛知県の中小企業のインシデント事例（私物端末の利用）

- UTM 機器にて、社内の特定の端末から不正な通信先への通信を検知し、駆けつけ支援を実施。
- 社員の私物 iPhone が会社の Wi-Fi に無断で接続されていたことが判明。
- 当該端末との不正通信先は過去にマルウェアの配布やランサムウェアの配布に利用されていることが確認されている攻撃者のサーバであった。
- 検知・駆除できていなかった場合の想定被害額は 4,925 万円。

③ 埼玉県の中小企業のインシデント事例（私物端末の利用）

- ランサムウェア[6]である WannaCry[7]の C&C サーバとの通信を検知し、駆けつけ支援を実施。
- 当該企業のネットワーク構成を確認し、不正通信元の IP が無線ルータであることを特定。本無線ルータにつながっている端末が感染している可能性が高いと推測された。
- 当該企業にヒアリングした結果、社長家族が個別に持ち込んだ無線ルータであると判明。
- 当該無線ルータに接続した可能性のある全 PC に対してウィルススキャンを実施するように依頼。

④ 群馬県の中小企業のインシデント事例 1（私物端末の利用）

- UTM 機器にて、社内から社外 Web サーバや社外 FTP サーバに対して、脆弱性を突くサイバー攻撃の通信を検知し、ブロックしている状況が判明。社内 PC がマルウェアに感染し、サイバー犯罪の踏み台にされている（他社サーバを攻撃させられている）可能性が高く、駆けつけ支援を実施。
- 不正通信の発信源となっている端末の IP（3 台分）を特定。3 つの IP のうち、該当端末を特定できたのは業務用 PC1 台。残り 2 台は特定に至らなかったが、社内無線 LAN に社員がプライベート端末を自由に接続できる環境（DHCP）であるため、それらの端末である可能性がある。
- 特定した 1 台については、OS を再インストールして初期化。

---

[6] https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
[7] https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

⑤ 岩手県の中小企業のインシデント事例

- マルウェアである Emotet[8]への感染が確認され、駆け付け支援を実施。
- 社員が出張先ホテルの Wi-Fi 環境でなりすましメールを受信し、添付のマルウェアを実行したことが原因で感染したことが判明。
- Emotet 感染により悪性 PowerShell コマンドが実行され、アドレス情報が抜き取られる。その後、当該企業になりすまして、抜き取られた取引先等のアドレス宛に悪性メールが送信された。
- 対策として、PowerShell の禁止設定、不正通信先ホストの IP アドレスのブロック、アンチウィルス・OS・ブラウザの最新版へのバージョンアップを実施。

⑥ 群馬県の中小企業のインシデント事例 2（サプライチェーン攻撃）

- UTM 機器にて、マルウェア添付メール 100 件を集中検知し、駆け付け支援を実施。
- 当該企業と取引のある会社のメールサーバがハックされたことによりメールアドレスが漏えいし、複数アドレスから当該企業に対してマルウェア付きメールが送付されていたことが判明。
- メール内容は賞与支払い、請求書支払い等を装うなりすましメールであり、サプライチェーンを通じた標的型攻撃を受けていたことが判明。
- UTM でブロックしている状況のため、実害は無し。

⑦ 大阪府の中小企業のインシデント事例

- UTM 機器にて、オンライン銀行詐欺ツール型マルウェア(UPATRE/DYRE)への感染の疑いがある通信が検知されたため、駆け付け支援を実施。
- 監視配下の全 PC にウィルススキャンを実施したところ、2 台の PC でマルウェアを検出したため、駆除を実施。

[8] https://www.ipa.go.jp/security/announce/20191202.html

4. 今後の取組の在り方について

4.1. 本報告をとりまとめる中で浮かんできた課題

本報告をとりまとめるべく、昨今のサイバーセキュリティを巡る状況を整理していく中で、いくつかの課題が明らかになってきました。

「報告の依頼」に関連して様々なコメントが寄せられましたが、その中で最も留意すべきと思われるコメントが、

- 自社とサプライチェーンを深く共有している企業がサイバー攻撃を受けて被害が発生していた可能性があったにも関わらず、自社に何ら伝えられていなかったことは遺憾
- 自社が関係している重要な情報の流出や自社のシステムへの影響等について対応する必要があった可能性があるにも関わらず、連絡を受けなければ対応に着手できない

というものでした。

サプライチェーンのどこからサイバー攻撃が展開され、どのような形で影響が発生し、拡散していくのかを正確に予測することが難しくなっている中、そもそも自社が関わるサプライチェーンにおいてサイバー攻撃による被害が発生している可能性があることすら把握できないような場合に対し、決して少なくない企業が不安・不満を感じるようになっています。

また、今回の「報告の依頼」では、「防衛・宇宙関連や重要インフラ事業者との取引を行っている企業」に対して「重要な情報の漏えい等の可能性があったものについて」は経済産業省に報告することを依頼しましたが、その際、「重要な情報」についての判断基準が曖昧であるとのコメントも寄せられています。

「サイバーセキュリティお助け隊」の活動では、中小企業に対して常時監視を含めた支援体制を提供し、サイバー攻撃があった場合には駆けつけて対処するサービスも実施したことで、サイバーセキュリティ対策として高い効果が確認できました。その一方、こうした支援サービスを有償化した場合に中小企業がコストをかけてまで取組を継続してくれるのか、その動機付けをどのように行うのか、ということが大きな課題として認識されています。

こうした課題認識を踏まえ、

- サプライチェーンを構成するモノとして、また、機微な情報を扱うモノとして、各企業に求められる行動
- 我が国の産業活動の信頼性を高めるための活動

という観点から、今後求められる取組の方向性を整理していきます。

4.2. 各企業に求められる行動

企業が様々なサイバー攻撃に晒される中で安定的な事業活動を確保するためには、自らの責任でサイバーセキュリティ対策にしっかりと取り組んでいかなければならないことは論を待ちませんが、企業が担うべき責任は自らの事業継続の確保に留まらなくなってきています。

サプライチェーンを他の企業とともに構成していることに伴うサプライチェーンのセキュリティを確保する責任や、企業が負っている社会的な責任、例えば安全保障環境に大きな影響を与える可能性があるため適切な管理が法令で求められている機微技術情報の管理責任など、様々な形で企業に求められる責任を果たしていくための、具体的な行動を取ることが期待されています。

しかし、実際には、サイバーセキュリティに関わるこうした責任を果たすための具体的な行動につながっていないケースが、本報告をとりまとめる過程で寄せられたコメントなどから浮かび上がってきました。

経済産業省としては、特に以下の3つの観点から、企業に実際にアクションをとってもらうことを訴えていくことが必要であると考えています。

①サプライチェーンを共有する企業間におけるサイバー事案に関する高密度な情報共有の実施

サイバー攻撃によって実際に被害が発生するようなケースは、各企業にとって、株価など自社の価値に対する判断にも影響を及ぼす重大な事態であり、そうした情報を外部に提供することについて慎重になることは理解できるものです。しかしながら、上記 3.1.3②で触れたとおり、攻撃手法は日々高度化しており、攻撃者は攻撃の痕跡を消すことで、攻撃手法や実際の被害状況を正確に分析して把握することを困難にさせることが常態化しています。そのため、サイバー攻撃による被害が自社に留まるものと断定することが難しくなっており、実際には、把握した攻撃の影響範囲を

超えて、サプライチェーンを共有する他の企業にも何らかの影響が出ている可能性が排除できなくなってきています。

ビジネスメール詐欺（いわゆるBEC（Business E-mail Compromise））の事案では、取引先企業のメールアカウントが乗っ取られ、そのアカウントから送られてきた詐欺メールにひっかかって金を振り込んでしまったケースで、詐欺に引っかかった企業が、取引先企業がサイバーセキュリティ対策を怠ったことでメールアカウントが乗っ取られたことを証明し、それによって自社が被害にあったことを主張したことで、取引先企業が損失の一部負担の和解に応じたという事例が出てきています。今後、自社の被害によって他社をサイバー事案に巻き込んだ場合に責任を問われるような動きが増えていくことが予想されます。

すなわち、攻撃手法の高度化やサイバー事案に巻き込まれた企業の対応などの状況を踏まえると、サイバー攻撃を受けて影響が及んでいる可能性があることを隠すことは大きなリスクにもなってきているということです。

したがって、少なくとも、重要なサプライチェーンを共有する企業間では、深刻なサイバー攻撃を受けて影響が及んでいる可能性がある場合にはお互いに情報を速やかに共有する、高密度な情報共有を行う仕組みを共有することが望ましいと考えられます。特に、サプライチェーンの中核を担う産業界をリードする企業が具体的な行動を起こしていくことが期待されます。

こうした高密度な情報共有は、参加する主体間における高い信頼感があって初めて成り立つものであり、簡単に構築が進むと考えることはできません。したがって、問題意識、情報管理の在り方や責任関係について共有できる小グループからの取組となることが想定されますが、これにより、重要なサプライチェーンの防御の強化と自社が他の企業をサイバー事案に巻き込んでしまった場合のリスクの軽減を図ることができるということが明確になっていくことで、こうした高密度な情報共有が産業界に拡がっていくことが期待されます。

なお、技術的助言を必要とする場合には、自社のシステム調達に関わっているシステムベンダやセキュリティベンダ等のほか、IPA J-CRAT[9]、JPCERT/CC[10]へ相談することが有効です。

[9] https://www.ipa.go.jp/security/J-CRAT/
[10] https://www.jpcert.or.jp/form/

②機微技術情報の流出懸念がある場合の経済産業省への報告

今回の「報告の依頼」に対するコメントの中で、「重要な情報」をどのように定義すべきかについて問い合わせるものがありました。

情報の重要性については、使うモノによってその価値が変わってくるものではありますが、例えば、個人情報は法令で厳格な管理を求められており、仮に流出の懸念が高い場合には個人情報保護委員会等に報告することが求められているような、社会として保護すべきものとして認識され、官民が協力してその保護に取り組むべき情報の区分もあります。

産業分野においても、このように官民で協力して保護に取り組むべき情報の区分は存在しており、その典型的なものが機微技術に関わる情報です。

機微技術は、産業全体の競争力を維持・強化する観点から重要なものとして位置づけられる場合や、安全保障環境に影響を与える可能性があるために重要なものとして位置づけられる場合など、いくつかの観点から、その重要性を説明することが可能ですが、安全保障環境に影響を与える可能性があるものとしては、外国為替及び外国貿易法で輸出管理対象とされている技術に関わる情報があります。これらの技術は、国際輸出管理レジーム等において、軍事目的に転用される可能性のあるものとして特定されている技術です。こうした技術がサイバー攻撃により流出した場合には、国際的な安全保障環境に影響を与える可能性があります。

したがって、こうした軍事転用可能な技術に関する情報が流出した可能性がある場合には、経済産業省に対して報告することが望ましいと考えられます。（報告先については文末に記載）

③情報漏えい等の被害が取引先等不特定多数の関係者に影響するおそれがある場合における関係者の影響緩和の取組促進のための公表の実施

サイバー攻撃による被害などの情報は株価など自社の価値に対する判断にも影響を及ぼす可能性のあるものであり、そうした情報について、サプライチェーンを共有する信頼できる企業の小グループで共有することを超え、世の中に公表することについては、抵抗感があることは想像に難くありません。

一方、サイバー事案が日常的に発生し、社会に大きな影響を及ぼすようになる中で、どのようなサイバー攻撃が実際に発生し、自分たちがどのように対処すべきか

ということを把握することに対する世の中の関心も高まっています。サイバー攻撃が高度化・大規模化し、サイバー攻撃の影響範囲も拡大していることから、社会的な対応能力を強化していく観点からも、実際のサイバー事案が速やかに公表されることに対する期待も増加しています。

サイバー攻撃の実態及びその被害を公表することの社会的意義は確実に増大しており、その期待も強くなっていることから、企業が守らなければならない価値とサイバー事案を公表することによる社会的な意義の間のバランスを如何に確保して、抵抗感なく公表を行える環境を実現するかが重要な課題となっています。

経済産業省としては、まずは上記①で示した考え方と同様、サプライチェーンを防御することを目的に、サイバー事案に対して影響を受ける可能性のある者がその影響を最小限に抑え込むことができるようにするということを目的とし、そのための手段として公表を捉える必要があると考えます。

すなわち、サイバー攻撃による被害が甚大で影響する範囲の特定が難しく、広く関係者を巻き込んでしまう可能性があり、上記①で触れたような小グループでの情報共有では被害拡大の抑制を図ることが難しいと考えられる場合には、速やかにサイバー事案について公表をすることが好ましいと考えます。

4.3. 中小企業を含めたサプライチェーン全体のサイバーセキュリティ対策の強化

既に述べたとおり、「サイバーセキュリティお助け隊」の活動等を通じて、中小企業が直面するサイバー攻撃の状況がより具体的に把握されるようになってきました。

我が国の産業構造は、海外の事業者と連携しつつも、材料から最終製品に至る厚みのあるサプライチェーンが国内に広く展開していることが特徴となっていますが、昨今のサイバー攻撃では、こうした広く展開したサプライチェーンのあらゆる脆弱性を使って標的とする企業への攻撃侵入経路を確立しようという動きが見られます。

したがって、日本の産業に対する信頼を維持・強化していくためには、単に各企業が自らについて最善を尽くすのみならず、サプライチェーンを共有する事業者、特にサイバーセキュリティの取組がなかなか進まない中小企業を如何に動機付けし、サプライチェーン全体を通したサイバーセキュリティ対策の取組に巻き込んでいくのかが重要になります。

「サイバーセキュリティお助け隊」の取組では、様々な技術を活用した中小企業に対する常時監視サービスの実施やサイバー攻撃によるシステムへの侵入が発生し

た場合の初期支援活動などが、中小企業のサイバーセキュリティ対策に効果があることが確認されました。その一方、「サイバーセキュリティお助け隊」が有償サービスに切り替わる場合、コストの観点から、継続してサービスの利用を求める中小企業の割合はそれほど高くないことから、サイバーセキュリティ上の効果は確認できるものの、それが自らの事業にどのように積極的な効果があるかについて確信を持てていない様子が伺われます。

こうした状況を打破するためには、サプライチェーンを共有する産業毎に、中小企業を含め、産業全体でサイバーセキュリティ対策を推進していく方針を明らかにし、その問題意識を広く共有して、サイバーセキュリティに資する行動を促す運動を開始し、中小企業に取組の意義を認識してもらい、動機付けていくことが必要です。

また、中小企業が取り組んでいるサイバーセキュリティ対策については、取引先が好ましい活動に取り組んでいる中小企業を認識できるよう、その取組を可視化していくことが有効です。

経済産業省・IPA では、中小企業が自らのサイバーセキュリティの取組を自己点検したことを自己宣言し、そのことをマークで示す「セキュリティ・アクション」の活動を推進し、既に 9 万事業者以上が自己宣言を行い、セキュリティ・アクション・マークを利用しているところです。

今後更に、自らのリスクアセスメントの努力のみでなく、サイバー事案の発生の際に初期対応支援サービスなどを受けることができるなど、専門サービスを受けられる体制を整えていることを可視化し、取引先がより高い信頼を持って産業活動を連携できるようにすべく、「サイバーセキュリティお助け隊」の経験を基礎に、専門サービス利用者の可視化について検討をしたいと考えています。

こうした中小企業のサイバーセキュリティ対策の取組を可視化し、それを各産業におけるサイバーセキュリティ対策の取組と連動させる体制を整えていくことで、産業界全体のサイバーセキュリティの推進運動にしていきたいと考えています。

5. 終わりに

本報告では、昨今のサイバー攻撃の状況と、それを踏まえた今後の対応の方向性についてまとめています。

サイバー攻撃については、「報告の依頼」や「サイバーセキュリティお助け隊」の結果等を踏まえて、事例や特徴をまとめていますが、サイバー攻撃の手法、攻撃者の意図は極めて多様であり、本報告で報告されている攻撃が全てではありません。また、サイバー攻撃は日々高度化し、システムや機器の新たな脆弱性が毎日発見される中で、状況は常に変化していきます。

したがって、企業におかれては、本報告を活用しつつ、IPA や JPCERT/CC などから公表される最新のサイバーセキュリティの状況に関する報告に注意を向け、サイバーセキュリティ対策を不断に進めていくことが期待されています。

また、本報告で示した今後の対応の方向は、産業界自らの取組として推進していくことが期待されることであり、経済産業省では、こうした取組を進めていくための環境の整備を行うことで、産業界の取組が加速していくことを支援していきたいと考えています。

本報告で示した対応の方向を実現していくべく、今後、経済産業省では、産業界との対話を強化して、具体的な取組の内容について検討し、官民の協力の下、サイバーセキュリティ対策の推進運動へとつなげていきたいと考えています。

本報告は、こうした今後の産業全体のサプライチェーンのサイバーセキュリティ対策の強化に向けた第一歩としての役割を果たすものと期待しています。

（機微技術情報の流出懸念がある場合等の連絡先）
商務情報政策局サイバーセキュリティ課
電話：03-3501-1511(内線　3964)
03-3501-1253（直通）
メール：itsec-public@meti.go.jp