経済産業省

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

2020年６月12日

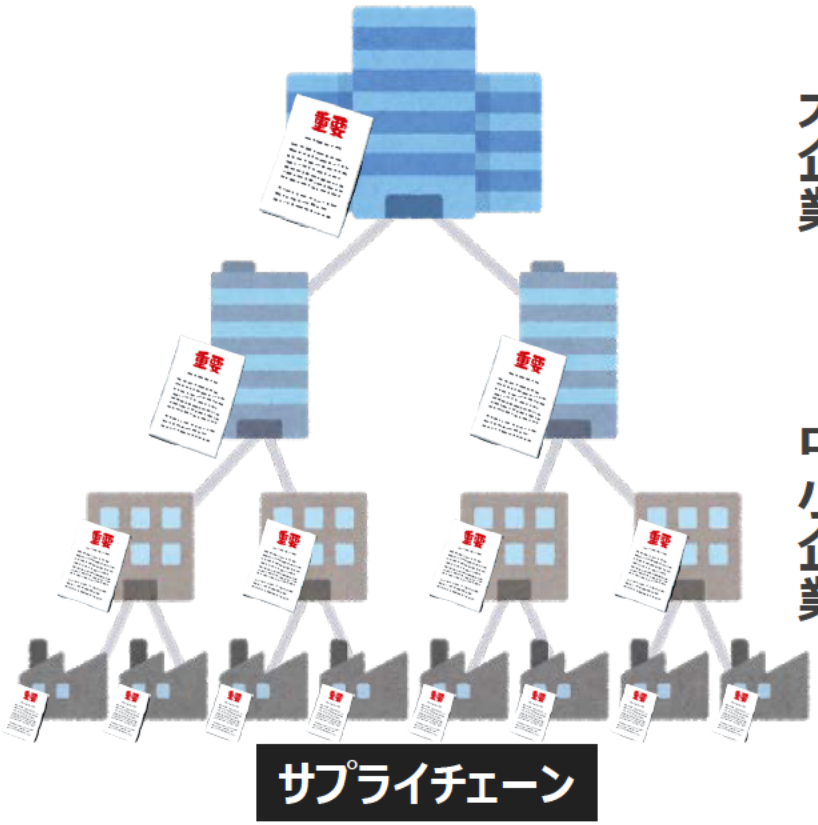
経済産業省

商務情報政策局

サイバーセキュリティ課

とりまとめの趣旨：サプライチェーン全体のサイバーセキュリティ対策が急務に

- **大企業から中小企業まで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化。**
  - 2020年1月以降、国内の複数の防衛関連の大企業が高度なサイバー攻撃の被害に遭っていたことが明らかに。
  - 「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（サイバーセキュリティお助け隊）」を通じて、中小企業に対するサイバー攻撃の実態も明らかに。
- 本報告では、サイバー攻撃の特徴や具体的事例を整理。
- 今後の取組の方向性をあわせて提示。産業界等の関係者等と調整しながら、サプライチェーン全体のサイバーセキュリティ対策を具体化していく方針。



- 2020年1月以降、三菱電機、NECなど、防衛省と取引関係にある企業が過去に高度なサイバー攻撃被害に遭っていたことが明らかに。防衛機微情報が狙われた可能性。

- サイバーセキュリティお助け隊を実施。
- 地域・企業規模に関わらず中小企業もサイバー攻撃の対象となっていることが判明。

昨今のサイバーセキュリティに係る状況：
日々高度化するサイバー攻撃への継続的な対応が肝要に

- 2月14日〆切の「報告の依頼」に基づく企業からの報告では、**サイバー攻撃によって重要な情報が漏えいしたとの報告はなかった**（ただし、〆切後に検知した事案で現在継続調査中の案件はあり。）。
- 一方、報告の内容や昨今のサイバー事案からは、**サイバー攻撃が日々高度化**していることが明らかになっており、**継続的にサイバーセキュリティ対策の状況を点検していくことがますます重要**に。

＜サイバー攻撃による昨今の被害の特徴＞

標的型攻撃の更なる高度化

・**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して侵入経路を確立するなど、メール開封等の**ユーザー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を確認**。

・加えて、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**を確認。

サプライチェーンの弱点への攻撃

・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、そこを踏み台に侵入拡大が図られる事例が増加。

・企業がグローバルにビジネス活動を拡大し、活動内容の統合レベルを上げていくほど、インシデント発生時の被害も大きくなるおそれ。影響範囲を限定するためのシステムの階層化など、**海外子会社等も含めた対応体制の整備が一層必要**に。

不正ログイン被害の継続的な発生

・ID・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、流出したID・パスワードのリストを利用した「**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**。

・ログイン機能に二段階認証や二要素認証を導入することで**ウェブサイトへのアクセスに係るセキュリティを強化**したり、個人情報を機微度に応じて分割して管理し、各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**が大切に。

「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：中小企業もサイバー攻撃の対象となっている実態が改めて浮き彫りに

- 1,064社が参加した実証期間中に、全国８地域で**計910件のアラート**が発生。重大なインシデントの可能性ありと判断し、**対処を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**5,000万円**近くなる事案も。

＜駆け付け支援件数＞

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※**	**110件**
		訪問によるインシデント対応	**18件**

※電話及びリモートによるインシデント対応には、訪問によるインシデント対応の一次対応を含む。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用

・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**。

・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。

・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**。

私物端末の利用

・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。

・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバと通信していた。

・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**。

ホテルWi-Fiの利用

・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、添付されたマルウェアを実行したことで**Emotetに感染**。

・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た後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

・実証参加企業でマルウェア添付メールを集中検知。

・**取引先のメールサーバがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。

・メールは賞与支払い、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**であった。

サプライチェーン全体のセキュリティ確保のために求められる行動

- 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い。
  - 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
- 企業が取るべき、**3つのアクション**「**共有**」「**報告**」「**公表**」の方向性を提示。
- 同時に、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のために、**中小企業のサイバーセキュリティ対策の取組の可視化**を検討。
- 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ることで、**産業界全体のサイバーセキュリティの推進運動**につなげていく。

3つのアクション

共有（Share）	報告（Report）	公表 （Announcement）
①サプライチェーン共有主体間での高密度な情報共有	②機微技術情報の流出懸念時の経産省への報告	③適切な場合の公表
◘ 重要なサプライチェーンを共有する企業間で、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、お互いに高密度な情報共有をすることが望ましい。	◘ 軍事転用可能性のある技術情報（輸出管理対象を目安）の流出は安全保障環境に影響を与えるおそれ。 ◘ 流出の可能性がある場合は、経済産業省への報告が望ましい。	◘ 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、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望ましい。

＋

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

⇒中小企業のサイバーセキュリティ対策の取組を可視化