経済産業省

サプライチェーン・サイバーセキュリティ・コンソーシアムについて

2020年10月

経済産業省

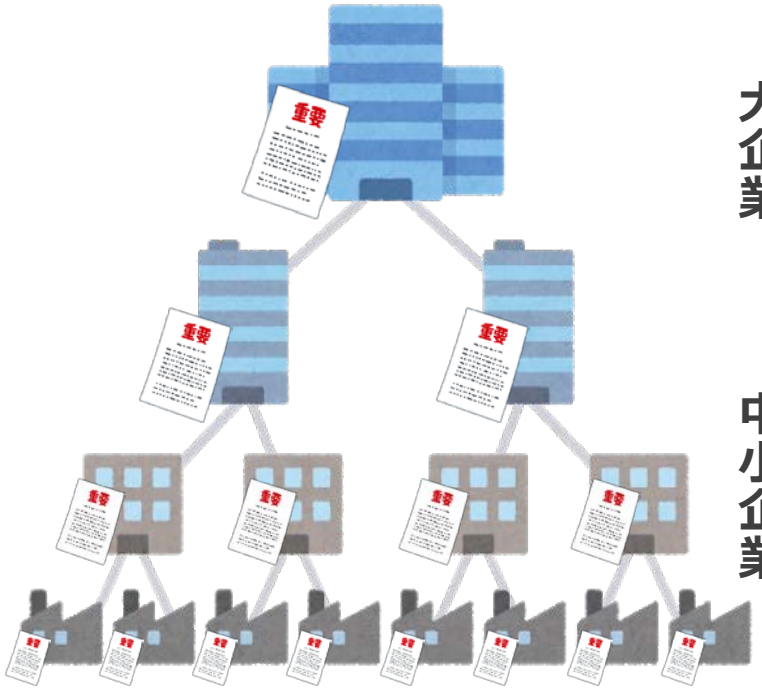
商務情報政策局

サイバーセキュリティ課

「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」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

2020年6月12日公開資料

- **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。



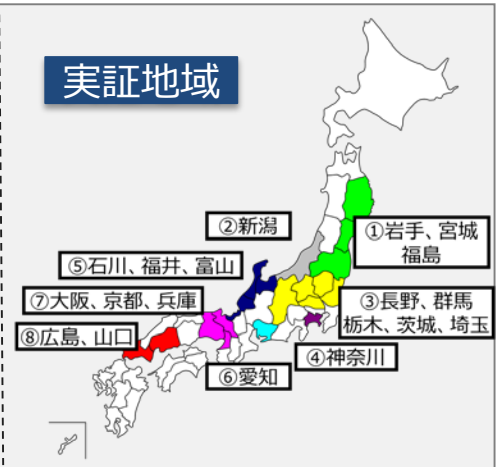
サプライチェーン

大企業

- 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。

中小企業

- 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。



https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

2020年6月12日公開資料

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。

https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

令和元年度の取組：お助け隊 実証事業の結果

- 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**5000万円**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ーと通信していた。
- 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ー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。

https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

産業界を挙げたサプライチェーン全体のサイバーセキュリティ強化運動の展開へ

1．企業のリスクマネジメント強化のための基本行動指針の設定

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 ☞ NDA関連情報が目安	②機微技術情報の流出懸念時の経産省への報告 ☞ 輸出管理対象技術が目安	③適切な場合の公表 ☞ 被害企業内での取締役会への報告事項(①の対象外のもの)が目安

2. 中小企業を含めたサプライチェーン・サイバーセキュリティ・コンソーシアムの立ち上げ

大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ。
－サイバーセキュリティ対策の取組を可視化し、マークを持つモノとの取引を望むことを明確化

- 「お助け隊」のブランド化
- 「SECURITY ACTION」加速

サイバーセキュリティ強化運動の全体像（コンソーシアムのイメージ）

- 大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、基本行動指針の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。

参加資格：コンソーシアムの取組方針や経産省の「基本行動指針」に賛同いただき、規約に同意いただける個人・法人

1．基本行動指針へのコミットメント

Supply-Chain Cybersecurity Consortium（SC3）

事務局：IPA

総会
年1回程度開催（WG報告、重要事項の決定等）

運営委員会

- 中小企業対策強化WG
- 地域SECUNITY形成促進WG
- 産学官連携人材育成WG
- ・・・・

経済産業省

6月12日発出
基本行動指針
※『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』（経済産業省サイバーセキュリティ課）

審査基準案・審査機関基準案の策定

IPA 独立行政法人 情報処理推進機構
審査基準・審査機関基準

審査機関の確認

お助け隊サービス審査機関

審査基準に基づきサービスを審査

匿名インシデント情報

- お助け隊サービスA
- お助け隊サービスB
- お助け隊サービスC

・一定の基準を満たすサービスに「サイバーセキュリティお助け隊」の**商標**利用権を付与

サービス提供

2．お助け隊サービス利用の推奨等の中小企業の取組支援

中小企業

・お助け隊マークを中小企業に付与して見える化


お助け隊マークイメージ

・SAとも併用可能

自社の信頼性をアピール

取引先（大企業等）

・分野別の下請ガイドラインの改訂を調整中

コンソーシアム　各ＷＧの議論内容（案）

中小企業対策強化ＷＧ

中小企業のサイバーセキュリティ対策強化のために、現状の課題や官民が取り組むべき施策や方向性について、幅広く検討。

地域SECUNITY　形成促進ＷＧ(P)

各地域におけるセキュリティ・コミュニティに関する取組について、プラクティスや課題を共有することにより、日本各地のサプライチェーンサイバーセキュリティ対策を底上げ・強化する。（原則オンライン開催）

産学官連携 人材育成促進ＷＧ(P)

産業界の求める人材像の共有、人材像を踏まえたカリキュラムの開発、各地域の高専等で生まれた産学官連携のプラクティスの共有を含む具体的な連携の促進などを通じ、サイバーセキュリティ分野における産学官連携での人材育成促進を図る。