



経産省：「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」の公表

UHY Tokyo ニュースレター / 2020年9月

経済産業省は2020年6月12日、「昨今の産業をめぐ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」を公表しました。本報告書は、経済産業省が2020年1月に発出した「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」）」に係る報告結果の取りまとめと、2019年度から実施している中小企業におけるサイバー攻撃発生後の初動対応を支援する「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た、中小企業を含めたサプライチェーン全体における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取りまとめたものとなります。また、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。概要は下記の通りであり、本報告書は下記URLからご確認いただけます。

<https://www.meti.go.jp/press/2020/06/20200612004/20200612004-2.pdf>

本報告書では、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・高度化しており、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であり、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が求められているとしています。以下3項目で構成されています。

1. 昨今のサイバーセキュリティに係る状況
サイバー攻撃による昨今の被害の特徴として、「標的型攻撃の更なる高度化」、「サプライチェーンの弱点への攻撃」及び「不正ログイン被害の継続的な発生」の3つを挙げ、日々高度化するサイバー攻撃への継続的な対応が重要であるとしています。
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
駆けつけ支援の対象となった特徴的な対応事例と

して、古いOSの使用や私物端末の利用、ホテルWi-Fiの利用、サプライチェーン攻撃などを紹介しています。

3. 今後の取組の在り方について
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として、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済産業省への報告、③適切な場合における（事案の）公表の3つを提示しています。

中小企業もサイバー攻撃の対象となっている実態が明らかになり、大企業・中小企業にかかわらず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とされている点に留意が必要です。また、サプライチェーン全体のセキュリティを確保するために求められる行動として、3つのアクション「共有」「報告」「公表」が示されており、各産業において連携した取組をどのように進めていくかが今後の課題と考えられます。

ご質問やご要望がございましたらお気軽にお問い合わせください。

※なお、本稿の意見に関する部分は、筆者の個人的な見解であることをあらかじめお断りします。



コンタクト

UHY東京監査法人

小野 琢司 - IT・内部統制 PG
Email: takuji.ono@uhy-tokyo.or.jp

〒141-0021 東京都品川区上大崎3-1-1 JR東急目黒ビル4F
Tel: +81 3 6417 0141 / Fax: +81 3 6417 0868
Website : <https://www.uhy-tokyo.or.jp/>