被害防止へ 対応事例紹介

サイバー攻撃について1117社の実態把握

独立行政法人情報処理推進機構（IPA）は5月31日、「令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊）」の報告書を公表した。

本事業は、13地域（24道県）と2産業分野の中小企業を対象に、サイバー攻撃被害の実態などを把握するとともに、サイバーインシデントが発生した際の支援体制の構築に向けた実証事業である。

1117社の中小企業が参加し、延べ1190社に対してUTM機器（統合脅威管理）などのセキュリティー機器を設置することで、サイバー攻撃の実態把握を行った。

本事業を通じ、業種や規模を問わず多くの企業がサイバー攻撃の脅威にさらされており、ウイルス対策ソフトなどの既存対策だけでは防ぎきれていない実態が明らかとなった。

また、インターネット上に公開しているホームページやサービスサイトなどの脆弱性（ぜいじゃくせい）診断において、対象企業のほとんどで何らかの脆弱性が発見され、そのうちおおむね2割の企業においては、重大なインシデントにつながる可能性があると診断された。

これらの結果、合計293件のインシデント対応ほか技術的支援が発生し、そのうち電話およびリモートなどによるインシデント対応ほか技術的支援を291件、訪問によるインシデント対応（駆け付け対応）を2件実施した。インシデント対応を行った事例を紹介する。

■事例①

UTMサービスを導入した企業において、同一ホストにて断続的に要注意検知が発生していることが確認されたため、お助け隊事業者が駆け付け支援を実施。対象のマルウェアと判定されたプログラムは、インターネットからダウンロードしたフリーソフトであったことが判明、駆除を実施した。

■事例②

UTMサービスを導入した企業において、PCの「ウイルス対策ソフト」を導入済みであったものの、「不正なIPアドレスへの通信」が成立していることが確認されたため、緊急度「高」のアラートを発報、支援を実施した。被害は確認されていないが、仮に情報漏えいなどの被害に至っていた場合の被害試算額は、5476万円であった。

■事例③

EDRサービスを導入した企業において、不正プログラム「ブラウザハイジャッカー」をEDRで検知、駆除方法を案内したが自力で対応できなかったため、お助け隊がリモート支援により駆除を実施した。

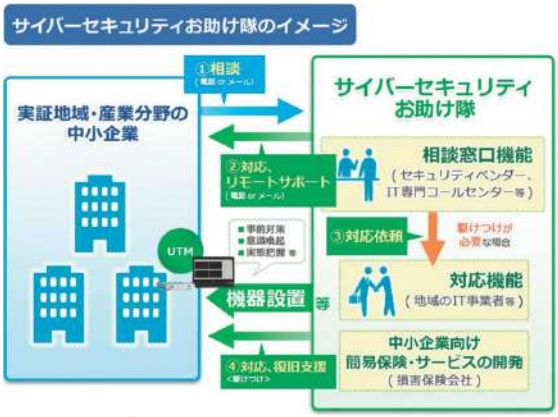
優良支援サービスにマーク付与

成果報告書ではこれ以外のインシデント対応事例のほか、組織的なセキュリティー対策の実態や人的リソースの状況などのアンケート結果が掲載されている。自社のセキュリティー対策実施の参考にしてほしい。

実証事業の過程で中小企業のニーズにマッチした民間サービスの開発が進められる中で、IPAでは、本実証事業の結果などを踏まえ、相談窓口、異常の監視、緊急時の対応支援、簡易サイバー保険などの各種サービスをワンパッケージで安価に提供することを要件としてまとめた「サイバーセキュリティお助け隊サービス基準」を2月に策定・公表した。

同基準を満たすサービスには、「サイバーセキュリティお助け隊マーク」の利用を許諾し、ブランド管理を行うとともに普及を促進している。

自社のセキュリティー対策強化に向けて活用を検討してほしい（成果報告書の詳細については、QRコードを参照）。（独立行政法人情報処理推進機構・江島将和）



サイバーセキュリティお助け隊のイメージ

2021年6月21日 会議所ニュース（日本商工会議所） （C）日本商工会議所 無断複製転載を禁じます。