記者発表資料

令和元年7月3日

大阪経済記者クラブ会員各位
（同時提供：金融記者クラブ(東京)）

中小企業を狙ったサイバー攻撃の実態を調査・分析する実証事業＜平成30年度実証＞の実施報告について

【お問合先】
大阪商工会議所　経営情報センター
（古川・野田・中川）
ＴＥＬ：０５０－７１０５－６００４
東京海上日動火災保険株式会社　広報部
ＴＥＬ：０３－５２２３－３２１２

大阪商工会議所、神戸大学、東京海上日動火災保険株式会社（以下、東京海上日動）は、中小企業を狙ったサイバー攻撃の実態を調査・分析する実証事業を行った実施報告について、お知らせいたします。

１．背景

○ 大阪商工会議所が平成 29 年 3～6 月に行ったアンケート調査において、多くの企業がサイバー攻撃にともなう被害を危惧している一方で、中小企業においては、「対応できる人材がいない」、「経費がかけられない」といった理由で十分なセキュリティー対策が行われていないこと、サイバー攻撃や不正アクセス等を受けている事実自体を把握できていない可能性が高いこと、等が明らかになっています。

○ また、中小企業が直面するサイバー攻撃の実態やその被害状況については、現在その統計データ等が存在していないことから、その実態を正確に把握することは困難であり、中小企業のセキュリティー意識の向上や対策の普及促進の観点で大きな課題となっています。

２．実証事業の内容

○ 上記の環境認識のもと、大阪商工会議所、東京海上日動は、神戸大学の協力のもと、中小企業に対するサイバー攻撃の実態を把握するための実証事業として、中小企業 30 社に協力をいただき、ネットワーク上の通信データ等を平成 30 年 9 月から平成 31 年 1 月の約 3～4 か月間にわたり収集し、サイバー攻撃の実態に関する調査・分析を実施いたしました。

３．調査結果について

○ 神戸大学にて今回の実証事業に協力した中小企業 30 社の通信データを分析したところ、30 社すべてにおいて何等かの不正な通信があった旨を示すアラート（警告）の記録（ログ）がありました。

○ アラートのログを分析した結果、脆弱性（弱点）やポート（出入口）を狙って攻撃されている事例から、外部から社内の端末をリモート操作されているなど、大きく 3 つの種類のサイバー攻撃の実態が複数企業に対して確認されました。

○ 主な重度なアラートとして、暗号化通信の一部を解読できる状態になっている、またウィルス（マルウェア）に感染した社内のコンピュータシステムの情報やキーの入力操作情報などを悪意あるサーバーに送信するなど、8 種類の脆弱性やポートを狙って攻撃されている事例が存在することが判明しました。

○ 今回のほとんどの協力企業では何等かのウィルス対策ソフトの導入ならびに運用がされていました。

○ 中小企業だからと言って決して攻撃されていないわけではなく、また、常に高度な手法を用いた攻撃にさらされている実態が明らかになりました。

○ 人もお金もかけられない中小企業も多く、大企業や重要インフラ事業所のようなセキュリティー対応も行き届かないために攻撃者による侵入を回避できておらず、多くの中小企業はその事態に気付いていないという実態が浮き彫りになりました。

４．今後の取り組みについて

○ 今回の結果を踏まえ、中小企業においてどのようなサイバーセキュリティの事後対策が有用なのかを検証するため、平成 31 年度に新たに取り組む実証事業「サイバーセキュリティお助け隊」を実施につなげてまいります。

○ 大阪商工会議所は、中小企業に向けてセキュリティー対策の啓発を行うとともに、必要に応じて、政府や関連団体等への要望を行ってまいります。

【添付資料】実施報告書

http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/20190703cyber_h30.pdf

以上