（外部公開用）

平成３０年度
中小企業に対するサイバー攻撃実情調査
（報告）

令和元年７月３日
大阪商工会議所

（共同研究実施者）
国立大学法人神戸大学、東京海上日動火災保険株式会社

大阪商工会議所

1.調査の概略

　中小企業におけるサイバー攻撃が危惧される現在において、その現状を把握することは重要かつ危急の問題となっている。本調査では中小企業の社内ネットワークに出入りするパケットを直接調べることによって、その現状を把握することが目的である。

　調査対象は大阪市内を中心とした多種多業種の中小企業30社とし、サイバー攻撃の現状とその被害について実態調査を行った。

2.調査の背景

大阪商工会議所では平成29年度から3年間にかけて取り組む中期計画「たんと繁盛大阪アクション」の事業の一環として、「サイバー攻撃対策支援事業」を実施している。

大阪商工会議所が平成29年3月～6月にかけて実施した「中小企業におけるサイバー攻撃対策に関するアンケート調査」により、中小企業であっても標的型攻撃メールの受信（18%）やランサムウェアによる被害（7%）にあっていることがわかった。そして、「現在実施している情報セキュリティ対策で十分でない」と回答した企業は約7割（68%）となっており、その理由として「経費がかけられない」（60%）、「専門人材がいないのでわからない」（48%）を挙げた回答が多くあった。

また、神戸大学大学院森井研究室の協力の下、大阪商工会議所では平成29年7月より独自のネットワーク監視システムにより、会員企業や関係団体約７０社に対して、webサーバを監視するなど、サイバー攻撃対策の支援を行っており、より多くの中小企業にサイバー攻撃の実態を知ってもらうことにより、独自の啓発活動を実施している。

大阪商工会議所の調査により、多くの中小企業がサイバー攻撃を受け、その被害を危惧している。一方で、人材がいない、経費がかけられないといった理由から対策が十分に行われず、サイバー攻撃受け、不正アクセスの被害を受けている事自体を把握していない可能性がある。本調査では、対象となる協力企業の社内ネットワークにセンサを設置し、パケット情報を収集、直接分析することで、各協力企業に対するサイバー攻撃の有無を調査し、中小企業に対するサイバー攻撃の現状を把握することを目的としている。その過程で、サイバー攻撃の実態を把握や、適切な早期対策が期待できる。

3.本調査の実施手法

調査対象企業にセンサを設置し、パケット情報を収集し、それを直接分析する。本調査では、神戸大学が準備した侵入検知システムを利用したセンサを用いて、パケット情報を収集。さらに、解析システムを構築することによって、サイバー攻撃の分析を行う。センサで取得したパケット情報は、定期的に係員が蓄積媒体（外付けハードディスク等）でコピーして収集。収集したデータを分析して、レポートとして中小企業に送付。調査期間の中間及び終了後に、全体の詳細解析を行い、サイバー攻撃の現状を分析した。

なお、本調査で設置するセンサは、各協力企業の現有ネットワークに流れるパケットを複製、分岐させ収集するため、現有ネットワークには影響を与えない。

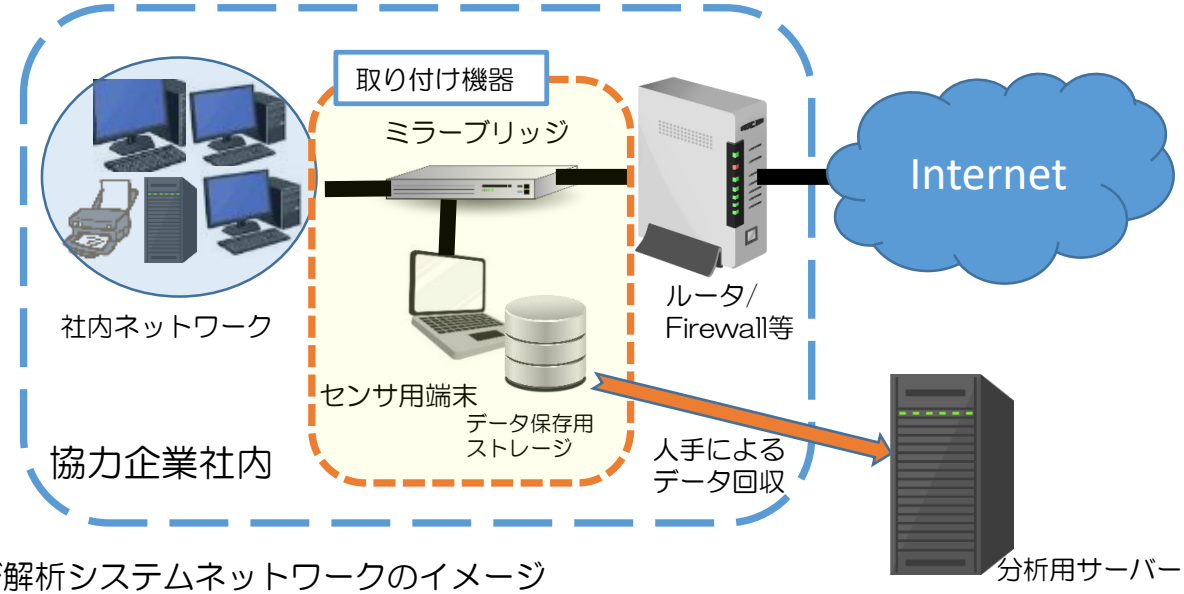


図3.1 センサ及び解析システムネットワークのイメージ

4.アラートログの分析結果

アラートログを分析した結果、複数企業に対して主な重度のアラートとして下記の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た。

- OpenSSLの脆弱性「HeartBleed」に関するアラート
- リモートデスクトッププロトコル（RDP）に関するアラート
- ネットワークタイムプロトコル（NTP）を利用した攻撃のアラート
- SSL3.0の脆弱性である「POODLE」に関するアラート
- 不正なファイルの送受信に関するアラート
- Server Message Block(SMB)の脆弱性に関するアラート
- Gh0st RATに関するアラート
- エクスプロイトキットに関するアラート

4.アラートログの分析結果（つづき１）

脆弱性やポートを狙って攻撃されている事例から、大きく３つの種類のサイバー攻撃の実態が確認された。

①外部から社内の端末をリモート操作の可能性

海外から管理者権限でのパスワードアクセスを繰り返し、リモートデスクトップによる接続が成功している。以下の脆弱性を突いたアラートを検出している。

A) ET POLICY RDP connection confirm

B) ET POLICY MS Remote Desktop Administrator Login Request

C) ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Outbound)

考えられる対処案)
・リモートデスクトップの機能を無効にする
・リモートデスクトップで使用するポート番号(3389番)を利用できないようにする
・接続する端末を限定的にする(利用するIPアドレスを限定)
・VPNを利用して安全な回線でローカルネットワークに接続した後にリモート接続する
など

4.アラートログの分析結果（つづき２）

脆弱性やポートを狙って攻撃されている事例から、大きく３つの種類のサイバー攻撃の実態が確認された。

②社内端末と悪性サイトとの通信

いくつかの事業所でマルウェア等を配布する悪性サイトとの通信が確認されており、マルウェアを社内ネットワークへダウンロード、または社内ネットワークから外部へ何等かのデータが漏洩された可能性がある。また、長期間に渡りアラートが検出している組織もあり、恒常的に通信している可能性が高い事業所もあった。

例えば、利用された脆弱性は平成26年に発見されたOpenSSL通信の脆弱性であるHeartBleedや同じく平成26年に公開されたSSL3.0の脆弱性であるPOODLEなど、既に広く周知され対策が公開されているものも存在した。セキュリティ人材不足やセキュリティ経費がかけられないなどの理由から**多くの中小企業では既知の脆弱性が放置されている**と考えられる。

また、バックドアの機能を持つマルウェアの一種(GhOst RAT)も検出された。マルウェアに感染した端末をコントロールするために利用される。キーの入力操作情報やオペレーティングシステム（OS）のバージョン、CUPの性能などのシステムに関連する情報などを収集し、GhOst RATが管理するコマンド＆コントロール（C&C）サーバに送信されている。

考えられる対処案）
・不用意なWeb上のネット広告をクリックしたり、発行元が不明なツールのインストールなどは避ける
・送信元が不明なメールに添付されたファイルやURLを開かない
（怪しいメールを開かない、開いた場合もLANケーブルを抜き、管理者にすぐ連絡するような訓練を実施することも有効）
・悪性サイトとの通信をブロックするような対策ツール(ウィルス対策ソフト等)を導入
・Windows Updateを含め使用するソフトウェアを最新のものとし、脆弱性に対応したバージョンに更新する
・システムの都合によりすぐにバージョンアップできない場合は脆弱性のある機能を無効するなどの対応を実施する
など

４.アラートログの分析結果（つづき３）

③DDoS攻撃を目的としたパケットを受信

いくつかの協力企業にてNTPのmonlist機能を用いたDDoS攻撃を受けていたことを確認した。

Network Time Protocol（NTP）は正確な現在時刻を取得するためのプロトコルである。複数のNTPサーバから攻撃対象にデータを送りつけて、大量の処理負荷を与えることでサービスを停止させるDDoS攻撃が行われる。また、脆弱性のあるNTPサーバを運用している場合、第三者を攻撃する際の踏み台として利用される場合もある。

考えられる対策案）
・異常な通信があれば、その通信をブロックするようなDDoS攻撃の対策ツール(IPS等)を導入
・DDoS攻撃をしていると疑われるIPアドレスからの通信を遮断
・特定の国からのアクセスを遮断する
・社内でNTPサーバを公開している場合は、脆弱性対策済のバージョンにアップデートする

5. 送信元もしくは宛先IPに着目した分析

共通のIPアドレスから複数企業からの、もしくは複数企業へ向けた通信でアラートが複数検出されている。一つのIPアドレスから複数企業からの、もしくは複数企業へ向けた通信でアラートが検出されるのは、通信が悪性である可能性が高い。

対象とした中小企業３０社については人的にもネットワーク的にも無関係、つまり交流はない企業である。したがって攻撃元からも、大阪市内の企業であるという以外に相関はなく、攻撃の有無についても相関があるとは通常考えられない。しかしながら、同一の攻撃元、つまり悪性サイトのIPアドレスから調査対象の中小企業３０社の中で複数の企業と通信が行われ、攻撃対象となっている事実が明らかとなった。

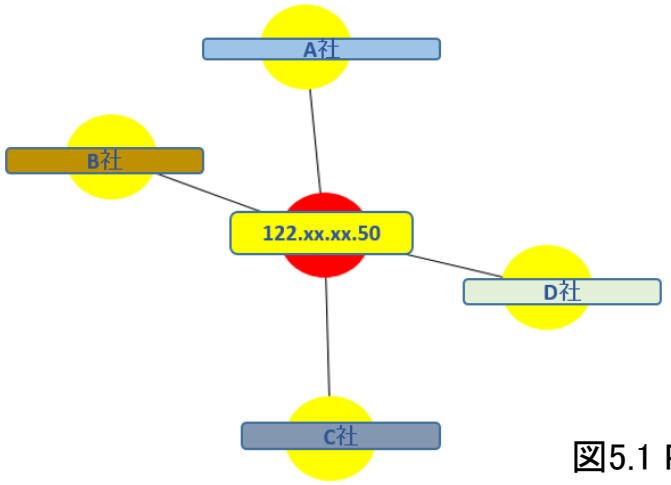


図5.1 Pアドレスとその宛先企業

６．企業別に着目した分析

それぞれの企業に到達したパケットのIPアドレスに着目した分析を行なっている。いかなるIPアドレスから、いつ、どれだけ、どのようなパケットが到達し、そのパケットによる脅威を分析している。

協力企業のうちA社では、インバウンド通信（企業外から企業内への通信）はアメリカが約60%、ルーマニアが約25%、日本が約15%を占める。アウトバウンド通信（企業内から企業外への通信）は日本が約50%、アメリカが約25%、ルーマニアが約20%を占める。他の企業と比較して、ルーマニアと通信が多く見られている。この企業では外部から社内のPCにアクセスし、リモートで操作を試みるための通信が検知されていた。

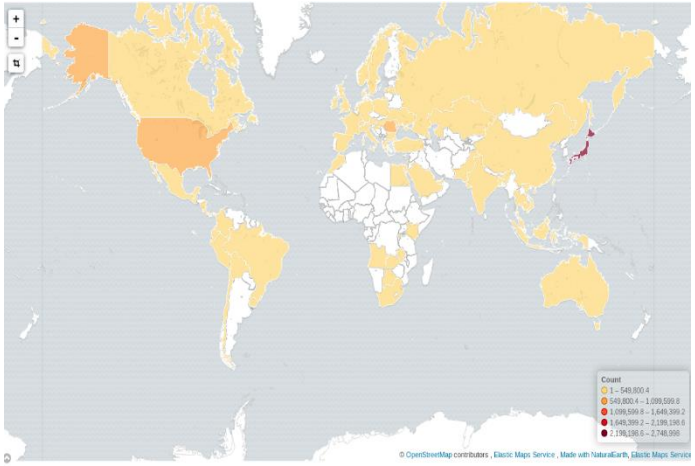
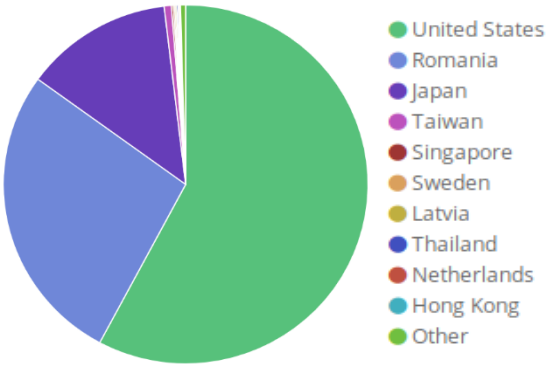


図6.1：A社における通信を行う端末の所在国



geoip.country_name.keyword:	Count
United States	860043
Romania	403948
Japan	195489
Taiwan	9457
Singapore	2529
Sweden	2126
Latvia	2072
Thailand	2019
Netherlands	1823
Hong Kong	1326
United Kingdom	1166
Canada	702
China	567
Cambodia	488
Brazil	439
Russia	427
France	400
Israel	371
Iran	166
Ukraine	163
Republic of Moldova	135
Ireland	125
Republic of Korea	120
Bulgaria	111
Panama	101
Costa Rica	91
Germany	90
Italy	81
Nicaragua	80

図6.2：A社における観測数上位の内訳

7. まとめ

平成29年度において、アンケート形式によって大阪市内の中小企業に対するサイバー攻撃実態調査を行った。サイバー攻撃に理解を示す中小企業が少ない中で、アンケートに回答した１／４の事業所が少なからず何等かのサイバー攻撃を受けたことを自覚しており、特にランサムウェアによる被害が７％に及んだことで、その実態が明らかになった。ただし、目に見えるランサムウェア等の被害ではなく、目に見えないサイバー攻撃の被害、たとえば情報流出やバックドア等の設置、あるいはBot等のリモート操作の被害については企業の自覚がないゆえに実数に現れないことが予想されていた。セキュリティ関連会社の技術者、有識者の知識、経験から、中小企業の少なくとも1割はすでにサイバー攻撃の被害、つまり不正アクセスに遭遇しているということが言われているものの、実際の調査事例はなく、その実態は不明のままであった。

今回、種々の業種での大阪市内を中心とした中小企業３０社に協力を依頼し、約４ヶ月という長期間、しかも各中小企業の社内ネットワークにセンサを設置し、出入りしているパケットを全て観測するという過去に例を見ない調査を実施した。中小企業に対するサイバー攻撃の現状だけでなく、不正アクセスの可否についても詳細に調査を行った。その結果、重度な不正アクセスを許容している中小企業の実態が明らかになっている。

7． まとめ（つづき）

外部からのリモート操作に関しては、海外からのアクセスであり、通常ではありえないアクセス手法を取っていることから、正常な企業活動とは程遠く、悪意のある端末（パソコン）操作であると考えられる。悪性サイトとの通信に関しても、公に悪性と認定されているサイトであり、正常な企業活動としてアクセスすることはまずあり得ないと考えている。アクセスサイトとの通信では、ほとんどが双方向の通信であり、社内情報が漏洩している可能性も否定できない。 DDoS攻撃に関しても、それに全く気づかない状況である。攻撃としては、ポートスキャンやSSH等へのサービスへのパスワード試行といった攻撃だけではなく、OpenSSLの脆弱性「HeartBleed」を狙った攻撃や、SSL3.0の脆弱性「POODLE」を狙った攻撃、あるいはエクスプロイットキットというハッキングツールを利用した高度な攻撃手法も観測されている。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も明らかになった。

今回の調査結果として、多くの中小企業で被害を受けている実態が明らかとなった。また各社に対するサイバー攻撃も単純な攻撃ではなく、高度な攻撃を含む多種多様な攻撃を受けていることも分かった。今後のさらなる調査に委ねられるものの、不正アクセスを受け、知らない間に不正な通信が行われている最大の原因は、サイバー攻撃を含む情報通信技術(ICT)や機器管理知識が乏しい中小企業が多いことが考えられる。中小企業に身の丈にあった不正アクセスへの対抗措置、そして、現実的に可能なサイバー攻撃対策を希求する。

平成３０年度中小企業に対するサイバー攻撃実情調査（報告）

令和元年7月3日作成

実情調査実施者
大阪商工会議所
国立大学法人神戸大学
東京海上日動火災保険株式会社