サイバーセキュリティフォーラムin大阪
情報セキュリティ＆危機管理セミナー

大阪商工会議所における サイバー攻撃対策支援の 取組について

2020年2月25日

大阪商工会議所
経営情報センター　課長　古川 佳和

大阪商工会議所

大阪商工会議所の紹介

「商工会議所法」という法律に基づいて設立された地域総合経済団体
【創　立】1878年(明治11年)8月27日
【所　管】大阪市
【会員数】約３万会員
【代表者】会頭　尾崎 裕（大阪ガス株式会社　代表取締役会長）
【組　織】本部・５支部・大阪企業家ミュージアム

経営情報センターの紹介

【大阪商工会議所　経営情報センター】
- 1971年(昭和46年)開設
- 全国の商工会議所でも数少ないIT事業専門部署
- 中小企業の経営ニーズをいち早く捉え、「情報化」「IT」を活用した経営支援に取り組む
- 2017年からサイバー攻撃対策支援の事業を開始

中小企業の実態をアンケート調査
(2017年3月～6月実施)

日々巧妙化するサイバー攻撃。特に中小企業・小規模零細企業においては、何ら対策を講じていない企業ばかり。実際に被害にあってしまうと、情報漏えいによる信用失墜や業務の停止など、取り返しのつかない事態に。
実際のところどうなのかを調査し、何等か対策を打つためにも、中小企業におけるサイバー攻撃対策の実情を把握し、サイバー攻撃対策支援事業実施の基礎データならびに国に対する要望建議などの基礎資料とするために、関西を中心とした商工会議所に協力をいただきアンケートを実施。

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
◆調査期間：2017年3月～6月
◆調査方法：Ｗｅｂならびにファクシミリによる依頼、回収
◆調査対象：大阪、福井、敦賀、八日市、京都、綾部、宮津、亀岡、東大阪、高槻、岸和田、貝塚、茨木、吹田、豊中、池田、北大阪、守口門真、松原、高石、神戸、尼崎、明石、伊丹、西脇、相生、三木、龍野、加古川、小野、和歌山、田辺商工会議所会員の中小企業や団体など
◆有効回答数：315社

アンケート調査の結果わかったこと

中小企業の１／４は実際に被害にあっていたという事実

中小企業であっても標的型攻撃メールの受信（１８％）やランサムウエアによる被害（７％）にあっていることがわかりました。

中小企業にはセキュリティー対策の専門人材がいない！経費がかけられない

担当者がいないのが５０％。専任の担当者を置く中小企業は４％に止まり、兼任の担当者がいるが４４％。担当者がいない理由として多くの中小企業は適任者がいない（４４％）と回答。「現在実施している情報セキュリティー対策で十分ではない」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％）をあげた回答が多く挙げられました。

約８割の中小企業で情報セキュリティーにかける経費は年間５０万円以下

５０万円以下と回答する企業が７９％と一番多く、次いで５１万円～１００万円が１１％、１０１万円～５００万円が３％、５０１万円から１０００万円までが１％と続く。
情報漏えい賠償責任保険等に加入している中小企業は９％と低い。

サイバー攻撃による被害にあった場合の相談先は
取引先のＩＴ企業に相談するのが6割。公的機関の利用が少ない

警察(１４％)、商工会議所等支援団体（１０％）、情報処理推進機構(IPA)（１０％）など公的機関は相談先としてあまり考えられていない。

サイバー攻撃対策支援サービスの実施

- ホームページの巡回（サイバーパトロール）
- 標的型攻撃メールの訓練
- e-ラーニングによるセキュリティー教育
- 情報セキュリティー啓発セミナー
- サイバーセキュリティーに関する専門相談窓口の設置
- 一般財団法人関西情報センターと人材育成事業の共催実施

中小企業のサイバーセキュリティー対策強化に関する要望 (2017年7月)

1. 情報処理推進機構（ＩＰＡ）の活動・体制強化
   - ＩＰＡの活動拠点を関西に設置と体制強化

2. サイバーセキュリティー対策を実施する企業への補助金や税制優遇措置などのインセンティブの付与
   - サイバーセキュリティーをＩＴ導入補助金の対象に
   - サイバーセキュリティーへの投資促進のためのインセンティブを

3. サイバーセキュリティー人材の確保・育成支援
   - ＩＴ人材を採用する経費、社内で人材育成する経費、アウトソーシングなどで人材を確保する経費を助成

サイバー攻撃の実態を調査分析
(2018年度)

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、一定数の中小企業からネットワーク上の通信データ等を一定期間にわたり収集し、サイバー攻撃の実態に関する調査・分析を共同で実施。

【実施内容】
社内ネットワークにセンサを設置。
社内ネットワークの通信内容を観測し、不正なサイトへ通信をしていないかどうかを調査・分析。

【スケジュール】
○2018年6～9 月 調査対象先の募集
○2018年9 月～2019年1 月 サイバー攻撃実態調査の実施
○2019年7 月　 調査結果の公表

（つづき）実態調査の分析結果

調査した**30社すべてで何者かからサイバー攻撃を受けていた**ことを示す不審な通信が記録され、このうち少なくとも５社では悪意のあるサイトとの間でデータのやり取りが繰り返されていることが判明
(2019年2月17日 NHK ニュース7にて報道)

＜調査結果(2019年7月3日公表)＞

- 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種類のサイバー攻撃の実態が複数企業に対して確認**
- 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、またウイルス（マルウエア）に感染した社内のコンピューター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
- 今回のほとんどの協力企業では何らかの**ウイルス対策ソフトの導入ならびに運用がされていた**
- 中小企業も大企業と同様、**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
- 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

サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査（2019年2月～3月）

✓ 2019年2月～3 月調査 全国の従業員100名以上の事業所118社より回答
✓ 商取引の結節点に位置する大企業・中堅企業が、サプライチェーン上の取引先のサイバーセキュリティにつき、どの程度把握・関与しているか、取引先に由来してどの程度サイバー攻撃被害に遭っているか、今後、取引先に対しどのような要求事項を有しているか等を調査

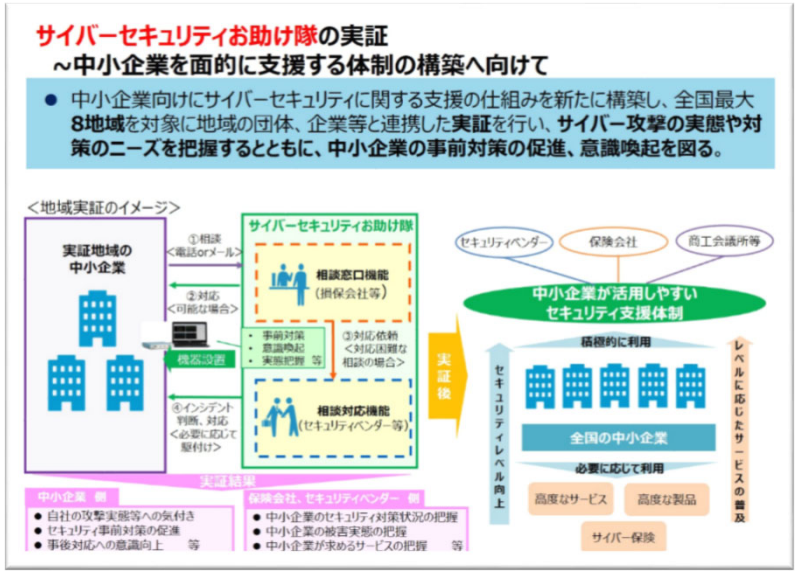
- **大企業・中堅企業の約７割（68%）は**、「仕入・外注・委託先（買い先）」「販売・受注・受託先（売り先）」における**サイバーセキュリティやサイバー攻撃被害について「あまり把握していない」**
- 取引先のサイバーセキュリティへの**「関与・管理等」につき**大企業・中堅企業の**半数強（56%）は「何も（殆ど）していない」**
- 「取引先に今後求めていきたいこと」は「口頭や文書での注意喚起」（42%）、「契約締結の依頼／要件化」（34%）。「何も（殆ど）せず」の企業も約２割（19%）存在。
- **４社に１社が取引先がサイバー攻撃被害を受け**、それが自社に及んだ経験がある
（その結果、**情報漏洩、システムダウン、データ破損**などの実害も）
- 「取引先がもしサイバー攻撃を受け、その被害が自社にも及んだ場合、採り得る対処」としては、「口頭や文書での注意喚起」（51%）、「損害賠償請求」（47%）、「セキュリティソフト・ハード導入の依頼／要件化」（37%）、「取引停止」（29%）。
- 「中小企業は今後どうしていくべきか」については、**「中小企業自身が自衛すべき」（60%）**、「国や自治体が支援すべき」（45%）、「IT企業や損保会社が安価・簡便なセキュリティサービスを提供すべき」（30%）、「商工会議所などが支援すべき」（27%）

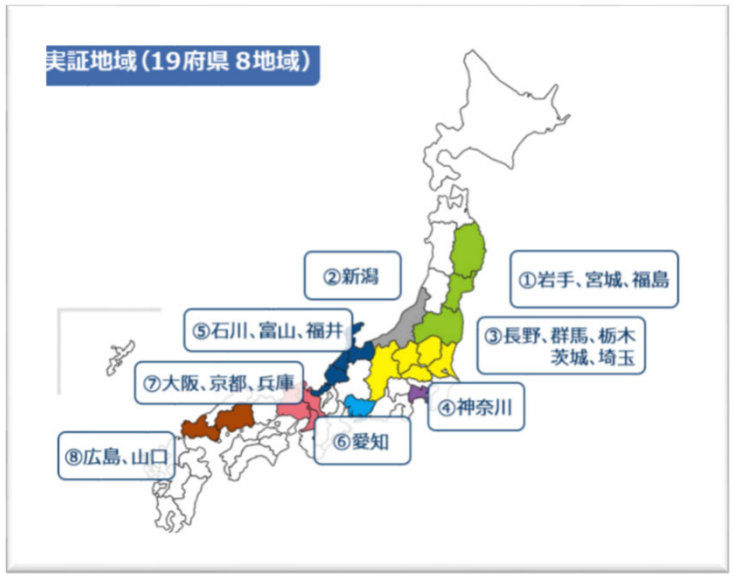
サイバーセキュリティお助け隊

(2019年度)

中小企業のサイバー攻撃の実態や対策のニーズを把握するため「実証実験」として、実証実験に参加する中小企業に対し、保険制度を活用した「セキュリティ機器の設置」「電話相談」「地元IT事業者の駆け付け」など、より具体的なサービスを見越した対策サービスを実施

IPAのホームページより

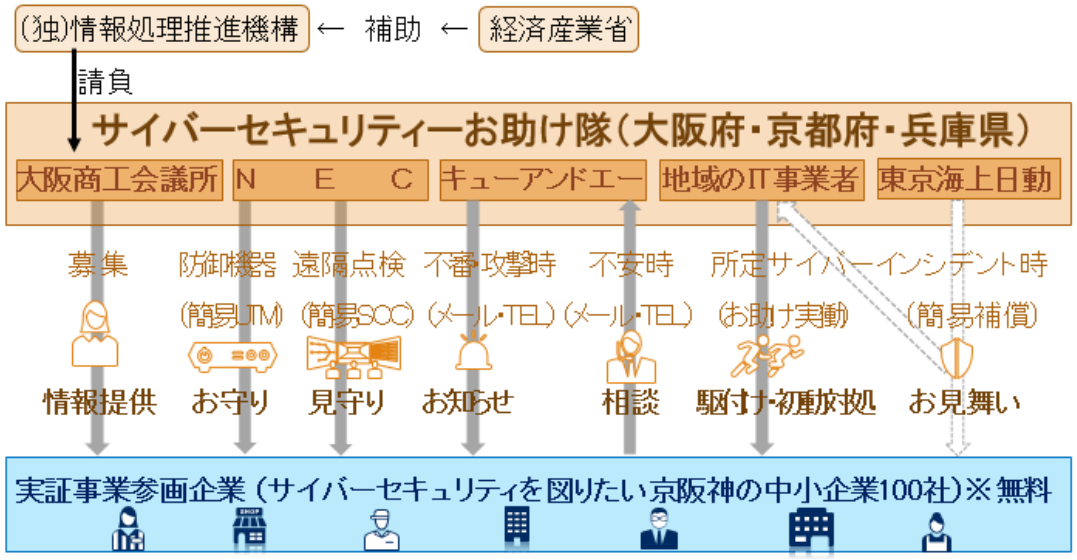




- 全国８地域で実証
- 2020年2月頃まで実施
- 1地域100社～200社
- 大阪商工会議所は「大阪・京都・兵庫」にて実施。
  （実施主体として「大阪商工会議所」「東京海上日動」「NEC」「キューアンドエー」「地域IT事業者」で構成）

サイバーセキュリティお助け隊（大阪・京都・兵庫）

下記のような総合支援サービスを提供した場合、その運営体制、価格・市場面を含め成立し円滑に機能するか否かを実証

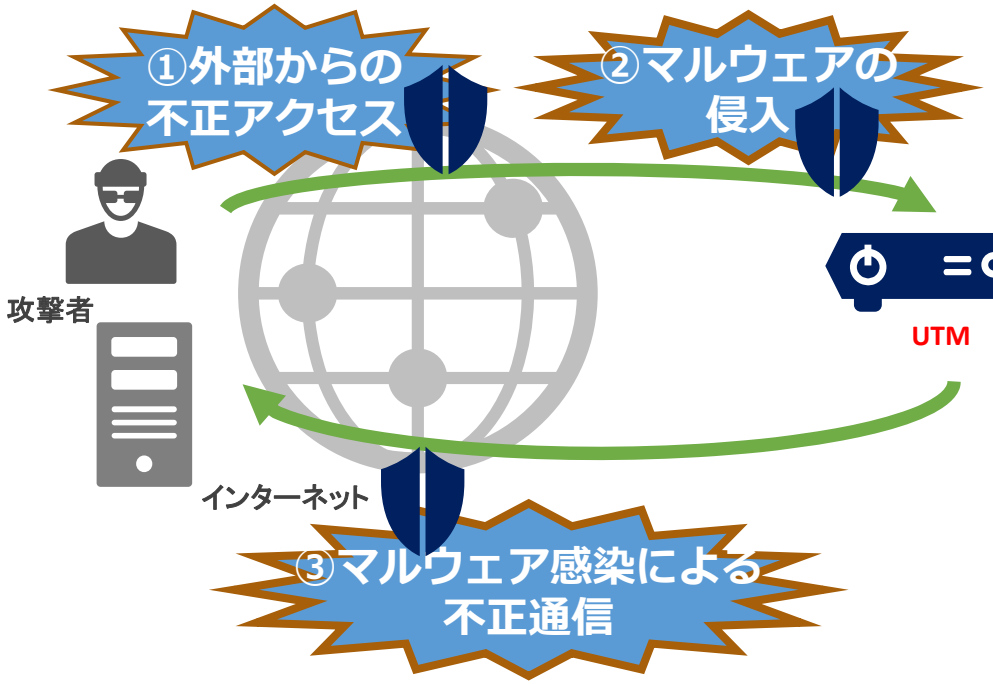


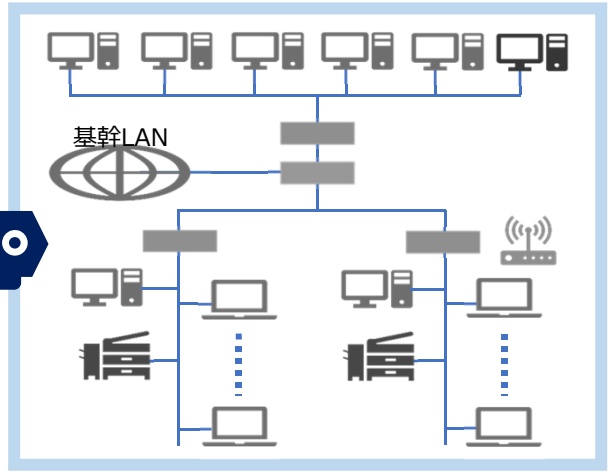
◎実　績：１１２社（うちＵＴＭ設置（監視）企業１１２社）
◎地　域：京都３（３%）、大阪９５（８５%）、兵庫１４（１２%）
◎業　種：製４４（３９%）、サ３５（３１%）、卸１８（１６%）、建８（７%）、小飲６（５%）、運１（１%）
◎規　模：社員値平均２９人、中央値１１．５人
◎その他：サプライチェーン構成８９（７９%）、　非構成２３（２１%）

スケジュール
・7月3日 発表記者会見
・7月5日 実施説明会、順次実証開始
・11月6日 中間報告会
・1月20日 実証終了
・2月12日 最終報告会

（つづき）実証の手法について

○UTMを設置して攻撃を防ぐ
①外部（インターネット）からの不正アクセスを防御
②外部（インターネット）からのマルウェアの侵入を防御
○UTMを設置して事前に防御できない攻撃から被害拡大を防ぐ
③マルウェア感染による外部（インターネット）への不正通信を防御





企業内

※UTMで防御できない脅威例
- 未知の手法を用いた外部からの攻撃
- ネットワークを経由しないマルウェア感染
  USBメモリ内のファイルにマルウェアが感染している等
- 暗号化されたファイルや、パスワード付きで圧縮されたファイルにマルウェアが含まれる
- UTM設置前からマルウェアに感染

サイバーセキュリティお助け隊最終報告（2020年2月）

項目	企業数	件数	件数/社月
外部からの侵入を防ぐ	64社	19,100件	56件
IPS(不正侵入通知)	48社	18,325件	72件
アンチウイルス	34社	775件	4件
被害拡大を防ぐ	31社	692件	4件
IPS(不正侵入通知)	31社	683件	4件
アンチウイルス	1社	1件	0.1件
Webガード	5社	8件	0.1件

※1回のインシデントで複数件検知することもある

重複を除くと
74社

(つづき)サイバーセキュリティお助け隊最終報告

■ UTMで検知・駆除したマルウェアは、
大半がOfficeファイル(Word, Excelなど)に仕込まれたマクロウィルス

マルウェア種類	検出件数	割合
Officeファイルに仕込まれたマクロウイルス	682	88%
マルウェアをダウンロードさせるWebスクリプト	62	8%
Windows端末内のファイルを暗号化して身代金を要求するマルウェア（ランサムウェア）	16	2%
PDFファイルに組み込まれた攻撃コード	15	2%
合計	775	100%

■ UTMにより、多数の攻撃を防御し、被害拡大を防ぐことができた
■ 防御だけでなく、ネットワークの問題（脆弱性)も見つけることができ、改善につながった
■ アンチウイルス機能も効果あり
- 更なるセキュリティを強化するために端末側でのマルウェア対策を推奨

サイバーセキュリティお助け隊・参加者の声

お助け隊実証に参画し良かった点		備考
社員のサイバーセキュリティ意識・知識が向上した	**21%**	・IPAセキュリティアクション診断受講し二つ星宣言準備中／情報セキュリティ５か条の周知 **・危機感を持つようになった／攻撃は常にあるという意識を徹底できた** **・事象があって初めて社員に啓発することが出来た／セキュリティへの重要性が伝わった** ・怪しいメールへの警戒感が高まった／必要事項以外は使用しないように徹底 ・勉強会を開催しレポートを作成した／セキュリティの勉強会のテーマとしてUTMを紹介した ・役員を含め必要を感じるきっかけとなった ・第三者に評価してもらうことが良かった
自社へのサイバー攻撃動向が把握できた	**21%**	**・アラート通知が実際にあり、他人事ではないとの意識につながった** ・アラート通知にて動向が確認できた／メール通知での把握ができた ・規模に関係なく何らかの攻撃があると分かった／攻撃が有るらしいと大雑把には分かった ・攻撃内容が解った／攻撃の有無実態を把握できるようになった ・重篤なマルウェア感染は自社では把握することが出来なかったと思う ・サイバー攻撃は無かった事が分かった（３）
自社のサイバーセキュリティやネットワーク環境を把握・改善することができた	**18%**	・UTMを含む新ネットワークを構築中 ・ウイルス対策ソストの無いPCにウイルス対策ソフトをインストールした ・ネットワーク設定の問題点の把握ができた／**問題があるＰＣを確定し対応できた** ・マニュアル作成中 ・メインＨＵＢのスペックに問題があることが分かった（交換予定）
自社へのサイバー攻撃・情報流出等が防げた	**17%**	・トロイの木馬を発見し駆除することが出来た／メール攻撃が無くなった ・不正アクセスを防いだ形跡があった／不正アクセスに対するアラートを受信 ・外部からのポートスキャン等を見つけることが出来た ・週１回程度何らかの攻撃が有ることが分かった **・セキュリティソフト未検知案件もUTMで防止できた** ・今までマルウエアが作動していても全く判らないという状況が改善された
自社の社会的信用が向上した	**6%**	・実証を機にSecurity Actionに登録 **・自社がこのような対策を行っていることをHP更新や名刺更新時にアピールする予定** ・小企業で対策を行っていることを評価されている
その他	**39%**	

中小企業のサイバーセキュリティー対策強化に関する要望 (2019年12月)

1.中小企業サイバーセキュリティー対策支援促進事業の予算確保

今年度の地域実証事業の空白地域(北海道、首都圏、四国、九州)を確実に埋めるなど、重要インフラや重要産業のサプライチェーンを守る支援体制モデルの早期構築と今年度実証事業の民間事業化を進めるために、必要かつ十分な予算措置を講じられたい

2.サイバーセキュリティお助け隊等民間サービスの普及拡大支援

① **SECURITY ACTION３つ星の新設と宣言要件への組み込み**
宣言要件に「お助け隊サービス等の利用」を設定されたい

② **「サイバーセキュリティ経営ガイドライン」への組み込み**
同ガイドライン指示９「サプライチェーン全体の対策」における「望ましいこと」の事例として、「お助け隊サービス等の利用」を追加されたい

③ **ＩＴ導入補助金の加点要件へ追加**
申請書を審査する際、「お助け隊サービス等の利用」を加点要件として追加されたい

④ **「サイバーセキュリティお助け隊」の商標登録とブランド化**
「サイバーセキュリティお助け隊」をＩＰＡ等にて商標登録し、実証実施事業者に通常使用権を許諾され、分かり易い統一ブランド化による普及を推進されたい

⑤ **民間事業化されたサービス利用者への補助金**
事業化されたサービスを利用する中小企業に対し、利用料の一部を補助されたい

⑥ **独占禁止法及び下請法の規制との関係明確化**
サプライチェーンを守るために大企業が取引先の中小企業に対し、事業化されたサービスの利用を促すにあたって、独占禁止法及び下請法に抵触しない範囲を明確化されたい

大阪商工会議所が実施するサイバー攻撃対策支援について（まとめ）

- **「自社には関係ない」と考えている中小企業の経営者に対して、セキュリティーの意識をもってもらいたい**
  - 対策セミナーの実施などによる啓発活動
  - 相談窓口の設置

- **国や関係機関に対しての中小企業向けサイバーセキュリティー施策の要望**
  - 今回の実証実験やアンケートの結果により、中小企業の実情に応じたサイバーセキュリティー施策を国や関係機関に対して働きかけ

- **中小企業の方々が利用できる安価で簡便なセキュリティー対策サービスの紹介や提供を実施**
  - 標的型攻撃対策の訓練メールサービス
  - 情報セキュリティシリーズe-ラーニング
  - **「商工会議所サイバーセキュリティお助け隊サービス」の開始（４月～）**

→UTMの機器レンタルならびに監視、コールセンターの設置
→セキュリティー事故（インシデント）が発生した場合でもコスト下が軽減できるよう、初期対策・簡易対策費用を損害保険で給付（上限５万円程度）

ご清聴ありがとうございました

大阪商工会議所はこれからも
中小企業のサイバー攻撃対策を支援します

大阪商工会議所　経営情報センター
cybersecurity@osaka.cci.or.jp