たんと繁盛

記者発表資料

平成２９年6月３０日

大阪経済記者クラブ会員各位

「中小企業向けサイバー攻撃対策支援事業の開始」ならびに「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結果」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・中川・石田）
ＴＥＬ：０６－６９４４－６５８０

○ 大阪商工会議所は、ホームページのサイバーパトロール、情報セキュリティー対策に特化した相談窓口の開設、啓発セミナー・セキュリティー人材の育成――の３本柱で構成する中小企業向けサイバー攻撃対策支援事業を７月５日(水)に開始する。

○　インターネットのサイバー攻撃は日々巧妙化しており、被害にあった企業にとっては、情報漏えいによる信用失墜や業務の停止など様々なリスクが発生する恐れがある。

○　本会議所が今年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」では、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った。

○「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％）をあげた回答が多かった。（添付資料２）

○　神戸大学の協力で開発したシステムを利用し、会員事業所のホームページをパトロールし、サイバー攻撃を受けて改ざんもしくは閲覧できない状況になっていないかを発見・連絡し、対処策の相談に応じるサービスを開始する。またキックオフイベントとして、サイバーセキュリティーに関する知識を学ぶ「プラスＩＴセミナー」を７月５日（水）に開催する。

以　上

【添付資料】資料１　中小企業向けサイバー攻撃対策支援事業の概要
資料２　「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」結果について

たんと繁盛

資 料 1

中小企業向けサイバー攻撃対策支援事業の概要

1. サービス内容

(1) ホームページのサイバーパトロール

中小企業のホームページが改ざんやアクセス不能になるなどのサイバー攻撃にあっていないか、神戸大学の協力で開発したシステムを利用し、サイバーパトロールを行う。

具体的には事前に申請のあったホームページアドレス（ＵＲＬ）に対して１日２回、トップページを含めて２階層までパトロールを実施し、ホームページの改ざんや攻撃（ＤＤｏＳ攻撃）によるサービス不能を検知した場合、大商担当者から利用企業担当者へ電話ならびに電子メールで速やかに連絡する。

対応は平日午前９時から午後５時とし、休日や時間外に検知した場合は翌営業日に対応を行う。通知の際には、下記相談窓口を紹介する。

(2) サイバーセキュリティーに関する相談窓口の設置

日々の業務でどうすればサイバーセキュリティー対策ができるのか、もしホームページの改ざんや不正アクセスがあった場合にどうすればいいのか、情報漏えいや流出事案等があった場合にどのように対処すればいいのか等、サイバーセキュリティーに関する専用の相談窓口を経営情報センター内に開設する。

相談窓口は原則として毎週火・木の予約制とし、相談は基本的に経営情報センターにて対応するが、神戸大学や協力会社から派遣された専門スタッフが同席した対応も併せて実施する。

(3) サイバーセキュリティーに関する啓発セミナーによるセキュリティー人材の育成

経営者や担当者が必要とするサイバーセキュリティーの知識や最新情報を知るための啓発セミナーを実施。今年度はサイバーセキュリティーの最新事例・対応策に関する内容、ならびに中小企業が自社のセキュリティー対策の現状を診断する方法をテーマに２回開催予定。７月５日(水)に、第１回目となるキックオフイベント「プラスＩＴセミナー」を開催する。

2. サービスの運営について

○ 同サービスは、大商ならびに関西商工会議所連合会加盟会議所のうち、同事業に賛同する商工会議所の会員向けに実施する。

○ 利用期間は申込日の翌月から、今年度末(平成３０年３月末)まで。

○ サービス料金は、月額５００円（税込)。（平成３０年度以降はサービス料金を改めて設定する。）ホームページのサイバーパトロール、サイバーセキュリティーに関する相談窓口、啓発セミナー（大商が特に指定したセミナーに限る）が利用・参加できる。

たんと繁盛

資 料 2

「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」結果について

調査概要

◆**調査目的**：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。
◆**調査期間**：平成２９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

【調査結果のポイント】

●**電子メール（９５%）やホームページ（８７%）、ネットバンキング（６６%）、基幹業務等、ＩＴを利活用している中小企業は多くある中、サイバー攻撃対策として、アンチウイルスソフトの導入（７８%）、ファイアーウオールやＵＴＭの導入（５６%）、データ等へのパスワード設定（３７%）、民間企業が実施するセキュリティーサービス（３７%）が実施されているが、現在実施しているセキュリティー対策で十分でないと思っている企業が約７割（６８%）。**

●**十分ではないと思っている理由として、情報セキュリティーに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%）という回答。**

●**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感染（７%）など、実際にサイバー攻撃の被害にあっている。**

●**情報セキュリティーの担当者がいないと回答した企業が過半数。担当者がいても専任担当者（４%）ではなく、何かの業務の兼任（４４%）の担当者である。**

●**情報セキュリティーにかける経費として、８割弱（７９%）の中小企業が年間５０万円以下であり、中小企業は情報セキュリティーに、経費をあまりかけないという傾向にある。**

設問ごとのポイント

Ⅰ　ＩＴの活用について

１　ＩＴの活用状況について（複数回答）

～多くの中小企業でホームページや電子メール、ネットバンキング、内部基幹業務等でＩＴを活用

○電子メール（９５％）やホームページ（８７％）は、ほとんどの中小企業で活用され、ネットバンキング（６６％）や電子商取引（１７％）にも利用されている。

２　今後のＩＴ活用についての関心度合いについて（複数回答）

～クラウドやＩｏＴ、ビッグデータ、ＡＩに関心あり

○クラウドへの関心が最も多く（４５％)、次いでＡＩ（３２％)、ＩｏＴ（２９％)、ビッグデータ（２３％）と続く。

３　ＩＴ活用についてのリスク懸念（複数回答）

～サイバー攻撃に対する懸念、情報漏えいに関する懸念が多い

○ウイルスメールやホームページの改ざんなどのサイバー攻撃に対して懸念する中小企業は８割以上（８１％）ある。

Ⅱ　情報セキュリティー対策の実施について

１　情報セキュリティー対策の実施状況

～アンチウイルスソフトすら導入していない中小企業は約２割

○情報セキュリティー対策として、アンチウイルスソフトの導入と回答した中小企業は７８％にとどまった。

○ファイアーウオールやＵＴＭを導入している中小企業は５割強（５６％)。

○データ等への暗号化を実施している中小企業は１割強（１１％)、社員の教育・研修を実施している中小企業は２割（２１％）に止まる。

○現在実施している情報セキュリティー対策に対して十分でないと思っている中小企業は７割弱（６８％）と回答。

○情報セキュリティー対策が十分でないと思っている理由で一番回答が多かったのは、「経費がかけられないから（６０％)」と多く、「専門人材がいないのでわからないから（４８％)」と続く。

２　サイバー攻撃の実情

～中小企業であっても標的型攻撃メールやランサムウエアの標的に

○サイバー攻撃を受けたことがある内容として、標的型攻撃メールの受信（１８％)、ランサムウエアによる感染（７％）があった。

○具体的な被害例

・ホームページの問い合わせから、大量のメールが送られてきた
・ランサムウエアによる感染で、１部署のデータ全て暗号化された
・なりすましメールの添付資料を開いたことで、情報が漏洩した
・自社ホームページがアクセス不能になり、修復に１カ月ほどかかった
・メールアカウントが乗っ取られた
・ホームページのセキュリティーホールを突かれ、悪意のあるリンクを埋め込まれた

Ⅲ　社内における情報セキュリティー体制について

１　情報セキュリティー担当者について

～ほとんどの中小企業で専任の担当者が不在

○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％と回答。

○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（４３％）と回答。

２　サイバー攻撃による被害にあった場合の相談先について

～６割以上の中小企業で取引先のＩＴ企業に相談し、公的機関の利用が少ない

○サイバー攻撃による被害があった場合に相談する先として取引先ＩＴ企業と回答する中小企業が６割を越える（６３％）。

○警察（１４％）、商工会議所等支援団体（１０％）、情報処理推進機構（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。

３　情報セキュリティーにかける経費について

～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。

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（集計結果）

2017年3月～6月

集計サンプル数 315件　※印は複数回答可

	回答件数	率
【設問１】どのようなIT活用をされていますか※		
1.　ホームページ	273	87%
2.　電子メール	299	95%
3.　ネットバンキング	209	66%
4.　eコマース(企業・個人向け電子商取引)	55	17%
5.　SNS(プログ、フエイスブック、ツイッターなど)	99	31%
6.　内部管理システム(経理、給与計算など)	182	58%
7.　製造管理システム	42	13%
8.　受発注システム	119	38%
9.　特に何もしていない	3	1%
【設問２】今後どのようなIT活用に関心がありますか※		
1.　IoT	92	29%
2.　ビッグデータ	71	23%
3.　人工知能(AI)	100	32%
4.　FinTeck(ブロックチエーン、ビットコインなど)	25	8%
5.　シェアリングエコノミー	11	3%
6.　シンクライアント(デスクトップ仮想化など)	25	8%
7.　クラウド	141	45%
8.　仮想現実(VR)	27	9%
9.　特に何も関心がない	67	21%
【設問３】ITを活用する上で、どのようなリスクを懸念されておられますか※		
1.　情報漏えい	247	78%
2.　情報システムの停止、障害	231	73%
3.　サイバー攻撃(ウイルスメール、ホームページの改ざんなど)	254	81%
4.　設備や機器の更新などによるコスト増	125	40%
5.　特に懸念していることはない	5	2%
【設問４】サイバー攻撃対策としてどのような情報セキュリティーを実施しておられますか※		
1.　アンチウイルスソフトの導入	246	78%
2.　ファイアーウオールやUTMの導入	152	56%
3.　民間企業が提供するセキュリティーサービス	116	37%
4.　データ等へのパスワード設定	117	37%
5.　データ等の暗号化	36	11%
6.　社員の教育・研修	66	21%
7.　専門人材の育成	7	2%
8.　特に実施していない	12	4%
【設問５】現在実施している情報セキュリティーで十分と思われますか		
1.　十分である	94	30%
2.　十分ではないと思っている	214	68%
3.　無回答	7	2%
【設問６】前問で「2.十分ではないと思っている」と答えた方にお尋ねします。理由は、次のどれに近いですか※		
1.　経費がかけられないから	128	60%
2.　業務多忙で時間がないから	50	23%
3.　専門人材がいないのでわからないから	102	48%
4.　相談する相手がいないのでわからないから	35	16%
【設問７】サイバー攻撃対策に関して、どのような情報が知りたいですか※		
1.　最新のセキュリティーサービスの内容	124	39%
2.　サイバー攻撃の最新の手口や具体的な事例	171	54%
3.　被害に遭った時の対応策	210	67%
4.　特に知りたいことはない	22	7%

【設問8】次のようなサイバー攻撃を受けたことがありますか※		
1. 自社ホームページアクセス不能	6	2%
2. 自社ホームページの改ざん	8	3%
3. 標的型攻撃メールの受信	58	18%
4. 情報の盗聴・盗み見	3	1%
5. ランサムウェアによる感染（第三者によるファイルの暗号化）	22	7%
6. ネットバンキングによる不正送金	0	0%
7. 特になし・わからない	228	72%
【設問9】サイバー攻撃で実際に被害を受けられた方で具体的な内容と被害額等を差し支えない範囲でお答えください		
＜省略＞		
【設問10】社内に情報セキュリティーの担当者はいますか		
1. 専任の担当者がいる	14	4%
2. 兼任の担当者がいる	140	44%
3. 担当者はいない	159	50%
4. 無回答	2	2%
【設問11】前問で「3.担当者はいない」と答えた方にお尋ねします。理由は、次のどれに近いですか※		
1. 必要ないから	22	14%
2. 業務多忙だから	23	14%
3. 適任者がいないから	68	43%
4. 担当者を雇う経費がないから	42	26%
5. 担当者を育成する経費がないから	11	7%
6．無回答	10	6%
【設問12】サイバー攻撃による被害に遭われた場合、どこへ相談することを考えられていますか※		
1. 社内のセキュリティー担当者	69	22%
2. 取引先IT企業(セキュリティー会社、システム開発会社など)	200	63%
3. 自治体	4	1%
4. 警察	45	14%
5. 商工会議所等支援団体	31	10%
6. 情報処理推進機構(IPA)	32	10%
7. わからない	40	13%
【設問13】情報セキュリティーに年間どの程度の経費をかけておられますか		
1. 50万円以内	250	79%
2. 51～100万円以内	34	11%
3. 101～500万円以内	11	3%
4. 501～1000万円以内	3	1%
5. 1000万円以上	1	0%
6. 無回答	16	6%
【設問14】ホームページが改ざんされていないかパトロールするサービスに関心がございますか		
1. ある	82	26%
2. 特に必要ない	222	70%
3. 無回答	11	4%
【設問15】情報漏えい賠償責任保険等(商工会議所保険制度)に加入されていますか		
1. 加入している	14	4%
2. 加入していないが、関心がある	86	27%
3. すでに同等の保険に加入している	17	5%
4. 加入する予定はない	98	31%
5. わからない	90	29%
6. 無回答	10	4%