中小企業における サイバーセキュリティの 「実態」と「現実的対策」

2023年11月28日　蒲郡商工会議所常議員会

大阪商工会議所　経営情報センター　登坂　文香

最近のサイバー攻撃の概要【総論】

サイバー攻撃の「攻撃する側」

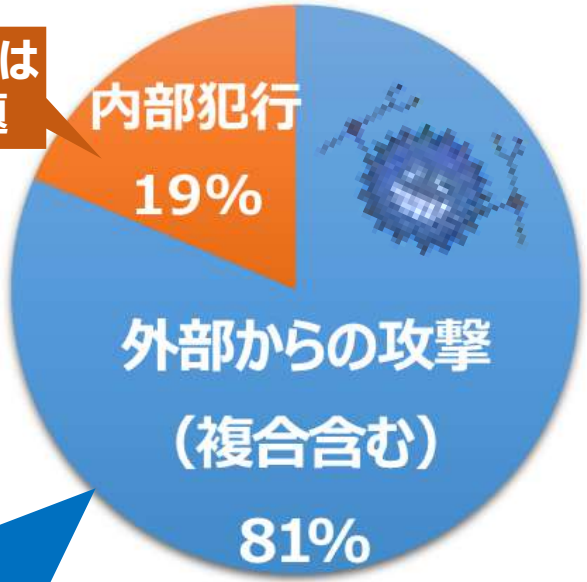
【攻撃者の変容】

一昔前　個人・愉快犯　　現在　組織・経済犯

気付かせることで
自己顕示欲を満たす

※米国の大手通信会社ベライゾン社「データ漏洩／侵害調査報告書」（2023年7月）

ビジネス！



気付かせないことで
利益の最大化を図る

国家による関与を含む
日本国政府「サイバーセキュリティ戦略」
では、中国・ロシア・北朝鮮を名指し

サイバー攻撃の「攻撃される側」

現状

【攻撃対象の増加】

パソコン
ルータ
サーバ
+α

「Society5.0」
「5G」「IoT」
「Connected Industries」
「サイバーフィジカルシステム」
「DX」
「コロナ起因デジタル化」

- パソコン,ルータ,サーバ等自体の**絶対数増**(BYOD含む)
- 無線LANによるスマホ,タブレット等の**接続増**
- 複合機,カメラ,各種デバイス等の**IoT化**
- スマート工場,コネクティッドカー等の**出現**

☞セキュリティ脆弱 → 攻撃の踏み台に

対策してないIoTをネットにつないだ
↓
最短38秒で感染
※横浜国立大学2016年調査

対策

※上図:経済産業省サイバーセキュリティ課
2022年11月

どんな中小企業に攻撃が？

現状

地域的な差異はあるか？

攻撃種別	令和2年度サイバーお助け隊実証 参加企業(2020年10月)53社 滋賀・奈良・和歌山の中小企業 【平均30.8人・中央10.0人】約3か月		令和元年度サイバーお助け隊実証 参加企業(2020年1月)110社 大阪・京都・兵庫の中小企業 【平均29.3人・中央11.5人】約5ヵ月	
外→内の攻撃	30社	8,430件	54社	19,100件
IPS	22社	7,906件	48社	18,325件
アンチウイルス	12社	524件	34社	775件
内→外の不正通信	23社	2,366件	31社	692件
IPS	17社	2,290件	31社	683件
アンチウイルス	0社	0件	1社	1件
Webガード	12社	76件	5社	8件

重複除くと38社（71%）

重複除くと74社（67%）

業種的な差異はあるか？

		製造業 44社	サービス業 35社	卸売業 18社	建設業 8社	小売飲食 6社	運輸業 1社
	UTM検知通信	全体中の参加率 39%	全体中の参加率 32%	全体中の参加率 16%	全体中の参加率 7%	全体中の参加率 5%	全体中の参加率 1%
検知あり	外→内の攻撃	26	22	8	5	2	1
	内→外の不正通信	15	9	2	4	1	0
	(両方検知した社数)	(11)	(7)	(1)	(2)	(0)	(0)
	合計	41	31	10	9	3	1
	合計(重複を除く)	30 全体中の検知率 42%	24 全体中の検知率 32%	9 全体中の検知率 12%	7 全体中の検知率 9%	3 全体中の検知率 4%	1 全体中の検知率 1%
	内部の脆弱性	16	16	6	5	4	0
	検知あり合計（重複を除く）	35(79%) 全体中の検知率 40%	27(77%) 全体中の検知率 31%	13(72%) 全体中の検知率 15%	7(母数少) 全体中の検知率 8%	5(母数少) 全体中の検知率 6%	1(母数少) 全体中の検知率 1%
検知なし		9	8	5	1	1	0

各業種の全体の中での「実証参加率」と「検知率」がほぼ同一（＝業種による差異なし）

※大阪商工会議所が実施したサイバーセキュリティお助け隊実証（2019年・2020年）での調査結果

☞**地域・業種に有意差は、ほぼ無し！どの地域・業種でも攻撃は(結構多く)ある！**

様々なサイバー攻撃の手口と基礎的対策【各論】

サイバー攻撃の攻撃手法（各論）

現状

攻撃手法の多様化

2022	個人	2023	組織	2022
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	8位	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不当請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

※独立行政法人情報処理推進機構（ＩＰＡ）「情報セキュリティ10大脅威2023」

☞**攻撃者の変化に伴い、攻撃手法も変化し、多様化・高度化・巧妙化**
→単一のセキュリティ機器や対策では防げない

サイバー攻撃の攻撃手法(各論)

概要

ランサムウエア(組織1位)

被害の6割が
中小企業！

※上図：大阪府警HP　ランサムウェア「Wannacry」

- PCやサーバのファイルが暗号化される
- 復号と見返りに身代金(仮想通過)要求
- 身代金の額は最近「値上がり」気味
- 身代金は値引交渉できる？
- 身代金を支払うと？支払わないと？
- 最近は身代金を要求してこない場合も
- VPN装置(FortiGate等。その存在自体をユーザが知らないケースも)の脆弱性や接続制限定が原因で侵入されることも
- ウイルス対策ソフト無効化・認証窃取

☞「不正暗号化」「情報の窃取」「情報の闇市場での暴露・販売」の3重脅威

サイバー攻撃の攻撃手法(各論)

対策

ランサムウエア(組織1位)

VPN機器(FortiGate等)から侵入71%、リモートデスクトップから侵入10%
※警察庁「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」

【事前対策】

- 検知と防御･･･出入口にUTM,端末にEDR,VPNの接続限定･脆弱性対応
- バックアップ･･･外付けHHD,NAS(NAS自体バックアップも要),クラウド,リストア訓練

【事後対策】

暗号化されたデータを(バックアップにより)復旧できたのは**約50%**
平均の被害額**2,386万円**(身代金含まず)、対応工数**27.7人月**
※特定非営利活動法人日本ネットワークセキュリティ協会「インシデント損害額調査レポート第2版」(2023年10月)

- 即LAN線を抜く
  (例:感染1.5秒後に活動開始→3秒後に暗号化開始→20秒後に他端末に伝染→10万ファイル暗号化に中央値42分)
  ※上データ：ウイルス対策ソフトCPMSのHPより
- 警察にPCを預けると？
  (2023年1月警察庁サイバー警察局がロシア系Lockbit3.0が暗号化したデータの復元に成功)
- 身代金は支払わず、復号を試みる
  (「No More Ransom」等から無料の復号化ツールを入手。復号できないものもあり)

※上図　IPAの事故対応手引き

※上図「No More Ransom」公式ウエブサイト

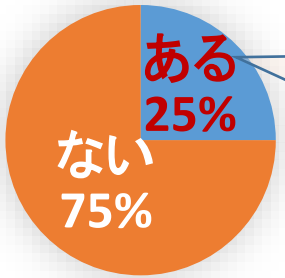
サイバー攻撃の攻撃手法(各論)

概要　サプライチェーン攻撃(2位)

対策が脆弱な企業から狙う！

大企業・中堅企業(全国118社)

取引先の中小企業が受けたサイバー攻撃の被害が、自社に及んだことがあるか？



今後の対処として

損害賠償請求	55社(47%)
取引停止	34社(29%)

※大阪商工会議所「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5月／全国の大企業・中堅企業118社）

☞被害者なのに、加害者（踏み台）になってしまう！

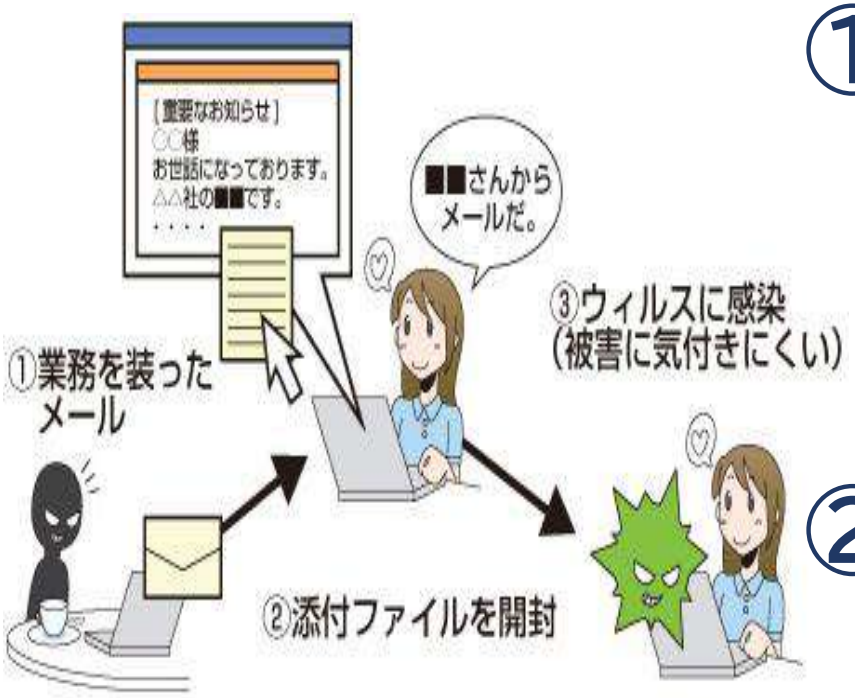
対策

- 「下請振興基準」(下請中小企業振興法第3条第1項)2020.1.31改正
  - ①下請事業者の努力として必要なセキュリティ対策を行う
  - ②親事業者の協力としてセキュリティ対策の助言・支援を行う
- 各業界ごとに「サイバーセキュリティガイドライン」策定

※左図：
自工会
部工会
ガイドライン

サイバー攻撃の攻撃手法(各論)

概要 **標的型攻撃メール(組織3位)・ビジネスメール詐欺(組織7位)**



※イラスト：総務省HPより

☞**最近の標的型攻撃メールは標的を定めずやってくる**

①標的型攻撃メール

・機密情報・個人情報の窃取
・「うちなんか、標的になるほど値打ちある会社ちゃうし」

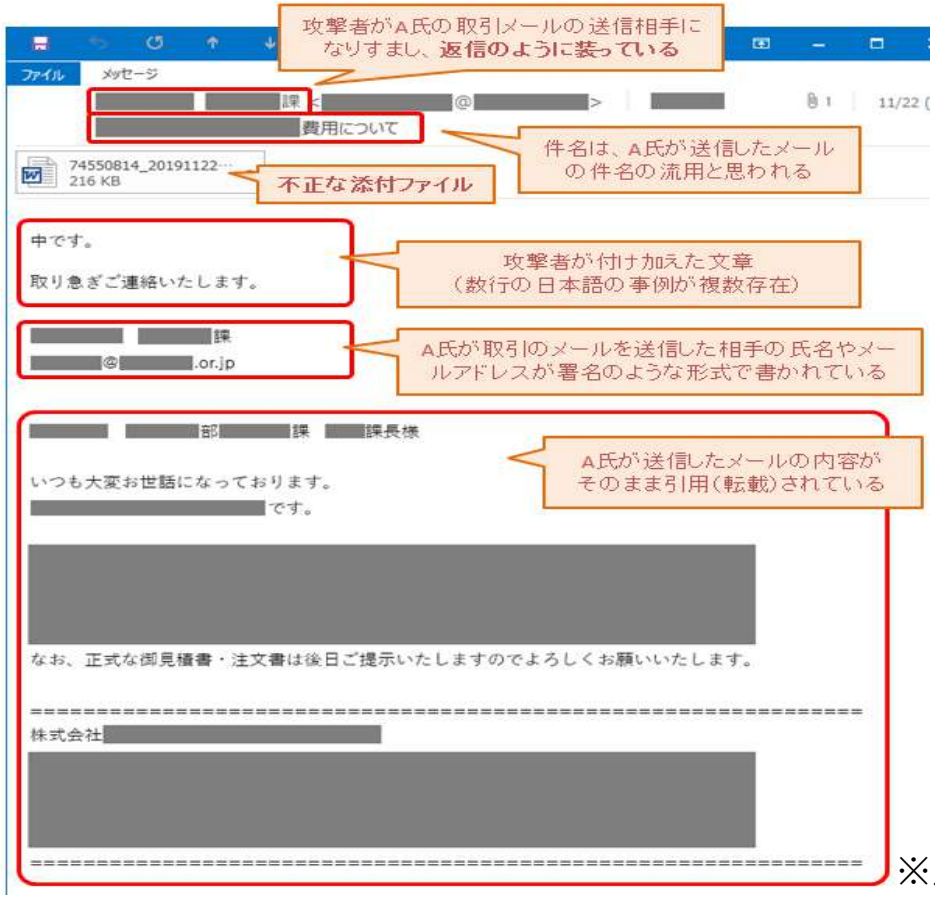
②ビジネスメール詐欺

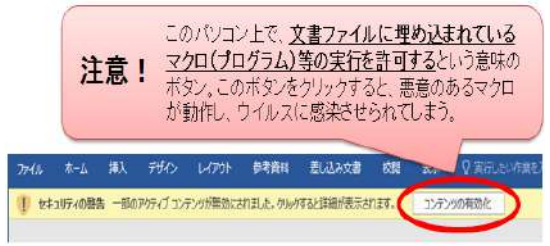
・金銭の窃取
・「さっき送った振込先、間違ってました。変更願います」

サイバー攻撃の攻撃手法(各論)

実例　標的型攻撃メール(組織3位)等

ウイルスメール「Emotet(エモテット)」





- 取引先や知人がEmotetに感染
  ↓
- 自分が過去にその取引先や知人に送信したメールの返信を装うメールが(犯罪者から)送信されてくる
  ↓
- 自分の書いた文書が載っているので安心してしまう
  ↓
- 添付のワードやエクセルを開きマクロ実行してしまう
  ↓
- こんどは自分が感染しEmotetの発信源になってしまう

※上左図：独立行政法人情報処理推進機構（ＩＰＡ）の公式ウエブサイトより

サイバー攻撃の攻撃手法(各論)

標的型攻撃メール(3位)・ビジネスメール詐欺(7位)・フィッシング(個人1位)

実例 こんなタイトルのメールは要注意

【JCBカード】カード年会費のお支払い方法に問題があります
【My Jcb】重要なお知らせ
【VISAカード】お支払い金額確定のご案内
VISAカード【重要:必ずお読みください】
【Mastercard】カード年会費のお支払い方法に問題があります
【マスターカード 】重要なお知らせ
【イオンカード】カード年会費のお支払い方法に問題があります
【イオンカード】重要:必ずお読みください
【重要】AEON CARD重要なお知らせ
【重要】イオンカード本人確認のお知らせ[メールコードA●●]
【重要なお知らせ】三井住友カード ご利用確認のお願い
【最終警告】三井住友カードからの緊急の連絡[メールコードS●●]
【三井住友カード】事務局からのお知らせ
<緊急!三井住友カード 重要なお知らせ>

※ＪＮＳＡ提供情報

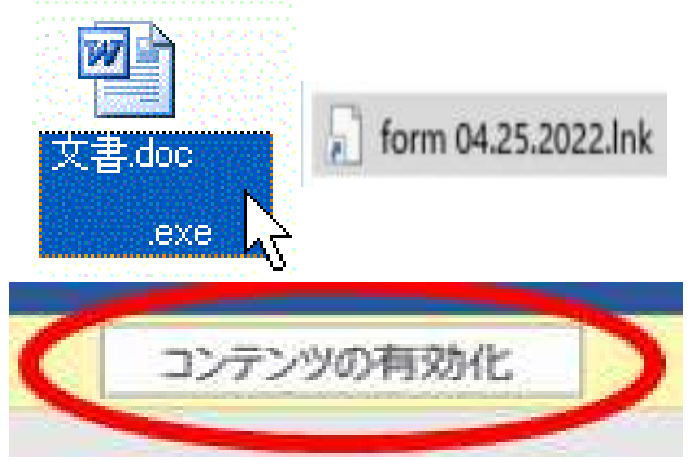
対策 クリック・開封せずに能動的に手入力しググる

サイバー攻撃の攻撃手法(各論)

対策　標的型攻撃メール(3位)・ビジネスメール詐欺(7位)

①メルアド、添付ファイルの拡張子は最後の最後まで確認！
　ショトカはクリックしない！不審な添付ファイルは開かない！

②添付ファイルの「コンテンツ有効化」「マクロ有効化」は押さない！



③実在する取引先や知り合いの人物名やメルアドに安心しない！
　その人から今このタイミングでメール受信する予定や必然性ある？
　「久しぶり」「なつかしい」「一体何の連絡？」の誘惑に負けない！

④重要メールの送受信は、相手に事前or直後にアナログ的に電話連絡！
　正規メールをウイルスメールと思い削除した場合「ごめん。再送して！」
　自分の送信メールを相手が削除した場合、快く再送信してあげましょう！

⑤文中の二人称が「あなた」の場合、ウイルスメール！

実在する中小企業でのサイバー攻撃被害【事例】

中小企業にどんな攻撃が？（実例）

①A社（大阪府／金属製品製造業／従業員10～20人）

実例

・ラトビア共和国から管理者パスワードでログインされ
パソコンが遠隔操作されていた。
・同社にはラトビアに営業所も現地工場も取引先もなく
社員の出張経験も無し。同国のITサービス利用も無い

対策

・リモートデスクトップ機能の無効化
・リモートデスクトップで使用の3389番ポートを閉じる
・接続端末の限定化（利用IPアドレスを限定）

※大阪商工会議所・神戸大学・東京海上日動火災保険㈱による「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」（2018年）

☞ラトビア共和国が悪いわけではない！そういう問題ではない。

中小企業にどんな攻撃が？（実例）

②B社（大阪府／土木工事業／従業員70～80人）

実例

・社内端末がコンピュータウイルスを配布するとして世界的にブラックリストに掲載されている悪性サイトと頻繁に通信していた

対策

・不用意なWeb上のネット広告をクリックしたり、発行元不明なツールのインストールは避ける
・不審メールの添付ファイルやURLを開かない
・悪性サイトとの通信をブロックするUTM等を導入
・バージョンアップ不可の場合は脆弱性ある機能を無効化

※大阪商工会議所・神戸大学・東京海上日動火災保険㈱による「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」（2018年）

中小企業にどんな攻撃が？（実例）

③C社（大阪府／機械製造業／従業員100～150人）

実例

・ランサムウエア被害に遭い復旧のために
2000万円の被害が出た

※大阪商工会議所・神戸大学・東京海上日動火災保険㈱による
「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」（２０１８年）

④D社（大阪府／化学品卸売業／従業員70～80人）

実例

・社員のメルアドでスパムメールが大量にばらまかれた。
・取引先のメールサーバに、F社ドメインが迷惑メール
登録されてしまい、メールを受信して頂けなくなった

※大阪商工会議所への会員企業からの情報提供（２０２０年）

中小企業にどんな攻撃が？（実例）

⑤E社（愛知県／自動車部品製造業／従業員約1700人）

実例

・大手自動車メーカーのサプライチェーン（Tier1）
・子会社のリモート接続機器の脆弱性から不正侵入
→ 子会社から同社に侵入 → サーバ、PCがランサムウエア感染（身代金払わず）→ サーバ、部品供給管理システムが停止 → ネットワーク遮断 → 部品納入を停止 → 納入先の大手自動車メーカの全工場（14工場28生産ライン）が停止

※2022年2月発生　新聞報道等を編集

☞大手自動車メーカーの工場は翌日から再稼働。 その危機管理能力は高く評価されるべき！

中小企業にどんな攻撃が？（実例）

⑥名古屋港湾協会（愛知県）

※2023年7月4日発生　国土交通省の「中間取りまとめ②」を要約

実例

- システム業者が遠隔保守を行うためのVPN機器から侵入。サーバのデータ全てがランサムウエアに暗号化された。
- VPN機器は①接続できるIPアドレス（インタネット上の住所）に制限がかけられていなかったのでIDとパスさえ合致すれば誰でもアクセス可能だった。②VPN機器の脆弱性が公開されていたのに未対応だった。
- 影響は①船舶37隻が約24時間遅延、②コンテナ約2万本の搬入出が遅延、③トヨタの愛知・岐阜4拠点が稼働停止、④アパレルメーカーでの衣類の入荷遅延等
- 名古屋港統一ターミナルシステムの停止により、紙などのマニュアル作業で荷役を継続。約60時間で完全再開

☞本事案はサプライチェーン攻撃でもある！
保守業者などの身内に潜むリスクも！

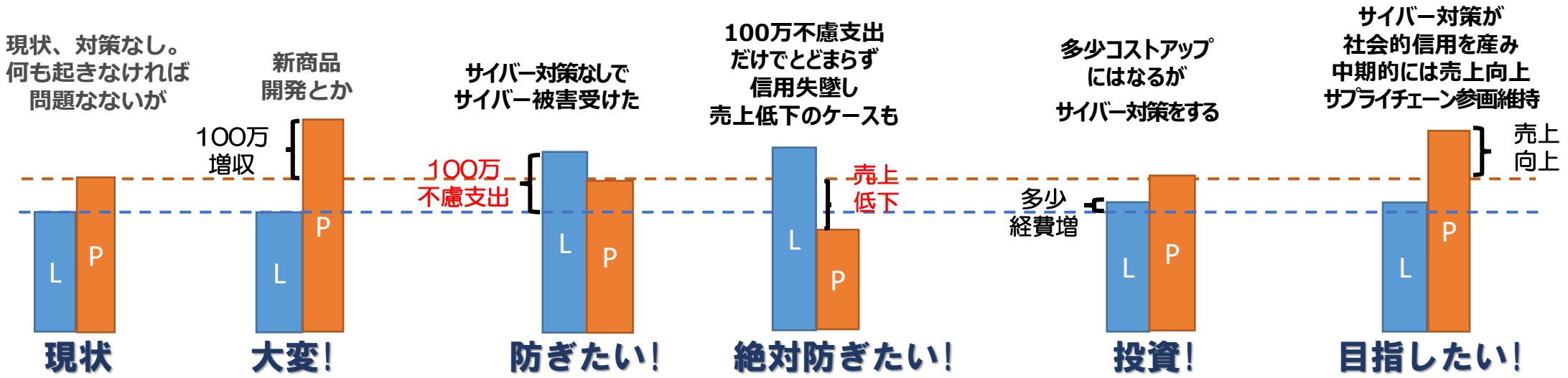
人もお金も不足がちな中小企業が持つべき視点と実践すべきこと

中小企業のサイバー対策に必要な視点

対策の前提となる考え方　「費用」でなく「投資」！

・100万円の「新たな売上」を（新商品を開発し）つくるより
　100万円の「無駄な支出」防ぐことの方が、一般的には簡単

・社会的信用の向上（少なくとも低下回避）により売上UP



中小企業のサイバー対策に必要な視点

対策の前提となる考え方

実例で見る「費用」と「投資」の関係性

実例

	甲社（30人サービス業）	乙社（200人食品メーカー）
事故の事象（被害と実害）	・不審メールに添付のワード文書のマクロを有効化。PC1台がウイルス感染 ・外部に偽装メール送信	・260台のPCがウイルス感染。社員をかたる「なりすましメール」が取引先に15万件/日送信されてしまった
原因・被害範囲調査費	364万円	1320万円
再発防止・事態収拾費（コンサルティング・弁護士等）	44万円	1155万円
再発防止費（システム導入等）	214万円	1000万円
社会的信用低下	？	？
合計被害額	622万円＋？	3475万円＋？

事故がなかったら発生していなかった「無駄な費用」
甲社400万円　乙社2475万円

「無駄な費用を未然に防ぐための投資」
甲社200万円　乙社1000万円

甲社
２００万の投資で
４００万の被害防止

乙社
１０００万の投資で
２４７５万の被害防止

「他山の石」にせねば！

結果論やん

※東京海上日動火災保険㈱「サイバーリスク保険インシデント事例集」（2021年11月大阪商工会議所への個別提供）

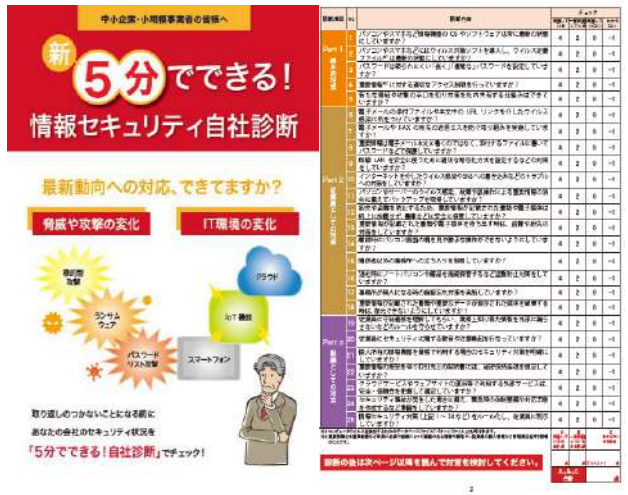
何から始めたらいいのか？

対策

経営者 IPA「中小企業の情報セキュリティ対策ガイドライン」を読む

情シス IPA「5分でできる！情報セキュリティ自社診断」をやる

全社で IPA「情報セキュリティ5か条」を実践し「Security Action」宣言



①ＯＳやソフトウェアを最新状態に

②ウィルス対策ソフトを導入する

③パスワードを強化

④共有設定を見直す

⑤脅威や攻撃の手口を知る

自己宣言・登録

サンプル SECURITY ACTION セキュリティ対策自己宣言

※独立行政法人情報処理推進機構（IPA）公式ウェブサイトから

情報セキュリティ5か条③（パスワード）

対策

攻撃者は1秒間で約1千億通り試行できる！
- 数字のみで4桁・・・10,000通り（瞬殺！で解読）
- 大文字+小文字で6桁・・・197億通り（秒殺！で解読）
- ４文字種全て(93個)使い10桁・・・93の10乗通り 48,388,230,717,929,320,352通り（解読に15年）

①「長く」「複雑に」「使い回さない」

- 目安として10文字（桁）以上
- 大文字(26)、小文字(26)、数字(10)、記号(31)の4文字種
- 人名、地名、社名、著名な固有名詞、誕生日、電話番号、英単語、よくあるパスワなどは使わない
- 使い回さない（下記②参照）
- 忘れることを恐れると、短く簡単なパスワードとなってしまうので、下記②にて作成し、手帳に記載

P@ssw0rd などは一応4文字種だが絶対NG

鍵のかかるところに保管

②パスワードの作り方例

- 「コアとなるパスワード」を先ず作り「利用サービスごとの固有の文字列」を合体させる

1. 自分なりの短いコトバを作る　巨人は嫌い（座右の銘、校歌の一節など、忘れない自分固有の「句」や「節」）
2. ローマ字に　kyojinwakirai（巨人をgiantsなど英語にしない）
3. 数文字を大文字に　kyojinWAkirai
4. 記号と数字を追加　kyojinWAkirai!4（コアパスワード）
5. 利用サービス名を追加　kyojinWAkirai!4ama（アマゾンの場合）
   kyojinWAkirai!4neko（ヤマト運輸の場合）

26の13乗通り（解読に287日）

52の13乗通り（解読に6,445年）

93の15乗通り（解読に1,067億年）

使い回しリスク減少

サービス名の部分は複雑でなくていい

情報セキュリティ5か条⑤（手口を知る）

対策　サイバー攻撃対策セミナーを各社、各協同組合で開催する

中小企業の経営者・社員が知っておくべき

サイバー攻撃対策セミナー に

大阪商工会議所から無償で講師を派遣します！

協同組合・工業組合・支援機関・士会・中小企業が、組合員(経営者)・会員・社員向けに
サイバー攻撃対策セミナーを実施する場合、大阪商工会議所から無償で講師を派遣します

1．趣旨

・サイバー攻撃は年々増加・巧妙化しており、中小企業も狙われています。
・データ損壊や個人情報漏洩はもとより、ウイルスの中継点とされてしまい、「被害者なのに加害者」となり、損害賠償請求を受けることもあります。
・中小企業の多くは「わが社狙われない」と考えがちで対策が遅れています。
・そこで大阪商工会議所が、協同組合・各種団体・支援機関・中小企業に無償で講師を派遣し、中立的・普遍的立場から、専門用語を排した平易な内容で、サイバー攻撃の現状と対策について分かり易く解説致します。

2．講演テーマと内容案

・テーマ例：「中小企業におけるサイバー攻撃の手口・被害事例・現実的対策」など（自由設定）
・内容例：攻撃の手口、中小企業の被害事例、被害最小化の視点、現実的・具体的対策法など

3．セミナーの開催形態等

・主催者：貴組合・貴団体・貴社（大阪商工会議所は主催者・共催者ではなく、あくまで講師派遣の立場です）
・講　師：大阪商工会議所　経営情報センター　職員（サイバーセキュリティ担当者）を講師として無償派遣します
・形　態：リアル開催、オンライン開催、リアル・オンラインのハイブリッド開催。これだけのために単独でセミナーをご開催頂くのはご負担かと存じますので、既存の会合（総会、役員会、勉強会等）に付設されるのも一手かと存じます。
・時　間：ご希望により調整します（20 分、30 分、45 分、60 分、90 分など）

4．開催経費

・講師料：無償（交通費は、講師リアル登壇の場合のみ、実費ご負担願います。但し京阪神都市部の場合は不要）
・その他　：会場代、備品代、案内経費、資料印刷代、その他経費は、貴団体・貴社のご負担でお願い申し上げます。

5．その他

・過去の開催実績は裏面をご覧下さい。テキストのイメージは別添をご覧下さい。事前のオンライン打合せも対応致します。
・大阪商工会議所は「サイバーセキュリティに関する総務大臣奨励賞」を受賞するなど、この分野では先進的取組みに努めています。

本件担当：大阪商工会議所　経営情報センター　（担当：野田・登坂）
〒540-0029　大阪市中央区本町橋 2-8　TEL：06－6944－6353

サイバーセキュリティセミナー　講師無償派遣　申込シート

大阪商工会議所　御中
cybersecurity@osaka.cci.or.jp　へ PDF 送信　or　FAX06-6946-7214

組織名、会社名		セミナー主催者	
担当者氏名		セミナー趣旨・名称	
担当者部署・役職		セミナー受講対象者	
メルアド		セミナー時期・時間	＿＿月　上旬・中旬・下旬　＿＿分間くらい
TEL		講師の出講形態	講師はリアル登壇希望　・　講師はオンライン登壇希望

ご記載の個人情報は、大阪商工会議所が本講師無償派遣事業運営のためだけに使用します。これにつき同意頂いたものとして取り扱わせて頂きます。

【刈谷モノづくり大学講習会（刈谷市委託事業）】

【セミナー案内】

中小企業における サイバーセキュリティの「実態」と「現実的対策」

受講料 無料

サイバー攻撃は年々増加・巧妙化しています。昨今は犯行側も効率性を重視するため、難攻不落な大企業より、容易に侵入しやすい中小企業を先ず狙う傾向があります。そこで今回、全国の商工会議所の中でも先駆けてサイバー攻撃対策支援事業を行っている大阪商工会議所の職員より、中小企業で実際に発生しているサイバー攻撃の生々しい実態とその対策状況を紹介していただきます。そして実際に当地域で「サイバーセキュリティお助け隊」として活動をされている当所会員事業所の(株)PCワールド様より実際の事例をお聞きします。
自社が被害にあわないために、また、知らないうちに加害者となってしまわないように、まずは、サイバー攻撃の実態とその手口を知り、今後の対策の考え方を整理してください。

講　師　野田 幹稚 氏　大阪商工会議所 経営情報センター 課長
事例紹介　早川 雅治 氏　(株)PCワールド 代表取締役
日　時　令和5年7月21日(金) 14:00~15:30
受講方法　以下の①か2のどちらかをお選びください。
①会場（刈谷商工会議所会議室）での受講
②オンライン受講(Zoom)
申込方法　下部の申込書をFAX(0566-24-6049)にて送りいただくか、右にあるQRコードよりGoogleフォームにてお申込ください。

主な内容
○サイバーセキュリティの現状
○サイバー攻撃による中小企業の被害実例
○IT導入補助金を活用したセキュリティ対策
○サイバーセキュリティお助け隊について
など

QRコードからも申込可能です

主　催　刈谷商工会議所中小企業相談所、(公社)刈谷法人会刈谷支部
問合せ　TEL 0566-21-0370

セミナーの内容	回答数	割合
満足	8	57.1%
どちらかといえば満足	5	35.7%
どちらかといえば不満足	0	0.0%
不満足	0	0.0%
未回答	1	7.1%
計	14	100.0%

ご意見・ご感想
・とてもわかりやすかったです。ありがとうございまし
・非常に興味のある内容であり、分かり易い講習で

商工会議所サイバーセキュリティお助け隊サービス(概要)

対策 国に登録されているUTM(多機能防御装置)レンタルサービス

中小企業・中小組織（全国）

お金ないし、人おらへんし、
時間ないし、面倒くさいし、
IT苦手やし、狭いし、
そやけど怖いし・・・

お守り【レンタル UTM】
ウイルス遮断〔外→内、内→外〕
IPS(不正通信遮断)〔外→内、内→外〕
危険サイトアクセス遮断
業務外サイトアクセス検知
アプリ動作検知

本サービスはサイバー攻撃・被害の低減と早期対応支援を目的としたものであり、サイバー攻撃・被害を完全に防ぐことを保証するものではありません

契約/サービス提供
情報提供/セミナー

近畿以外は再販事業者

見守り(監視)
お知らせ(通報)

相談
（メール・電話）

信用

駆け付け
（初動対処）

保険

保険は所定サイバーシンシデント時に大阪商工会議所契約のお助け実働隊地域 IT 事業者が初動対処する際にのみご利用いただけ、その上限は年２回まで、上限各 15 万円相当額までとなります（現金給付はなし）

大阪商工会議所

大手IT企業・大手損保・ITに強いコールセンター会社・地域の中小IT事業者と連携

24H365D 監視
（日本電気㈱（ＮＥＣ））

相談窓口

お助け実働隊地域 IT 事業者

簡易サイバー保険
（東京海上日動火災保険㈱）

これだけ揃って 月額
商工会議所 会員6600円
非会員8250円

- ✓ 会社の規模・業種に関係なく、サイバー攻撃はやってきます！
- ✓ サイバー攻撃の手口を知って対策し、事業継続・本業専念を！

大阪商工会議所は、2020年
「サイバーセキュリティに関する総務大臣奨励賞」受賞
これからも中小企業の
サイバー攻撃対策を支援します！
出前セミナーは講師料無料です！


奨励賞
大阪商工会議所殿
あなたがたはアンケートやサイバー攻撃の調査・分析の実施を通じて、中小企業へのサイバー攻撃の実態を明らかにするとともに、関西地域におけるサイバーセキュリティ関連の意識啓発や人材育成等に積極的に取り組むなど地域のサイバーセキュリティ水準の向上に多大な貢献をされました。
今後の更なる活躍を期待してここに奨励賞を贈ります
令和二年十二月十七日
総務大臣 高市早苗

大阪商工会議所　経営情報センター
〒540-0029　大阪市中央区本町橋2-8
お問合せ：050-7105-6004　又は　cybersecurity@osaka.cci.or.jp
紹介動画：https://www.youtube.com/watch?v=TVn5KF4hubY
お申込み：https://www.osaka.cci.or.jp/cybersecurity/utm/