一般社団法人大阪損害保険代理業協会　様

中小企業におけるサイバー攻撃の実態とその現実的な対策

本資料の著作権は大阪商工会議所に帰属しますが、損害保険代理店様におかれて、お客様に対し、本資料の一部又は全部を、そのまま又は適宜加工・編集を加えてお客様等にご提供頂いても構いません（文意は変えず、出典元をご明記願います）

2023年1月25日

大阪商工会議所　経営情報センター

中小企業における サイバー攻撃の実態 （攻撃の種類と基礎的対策）

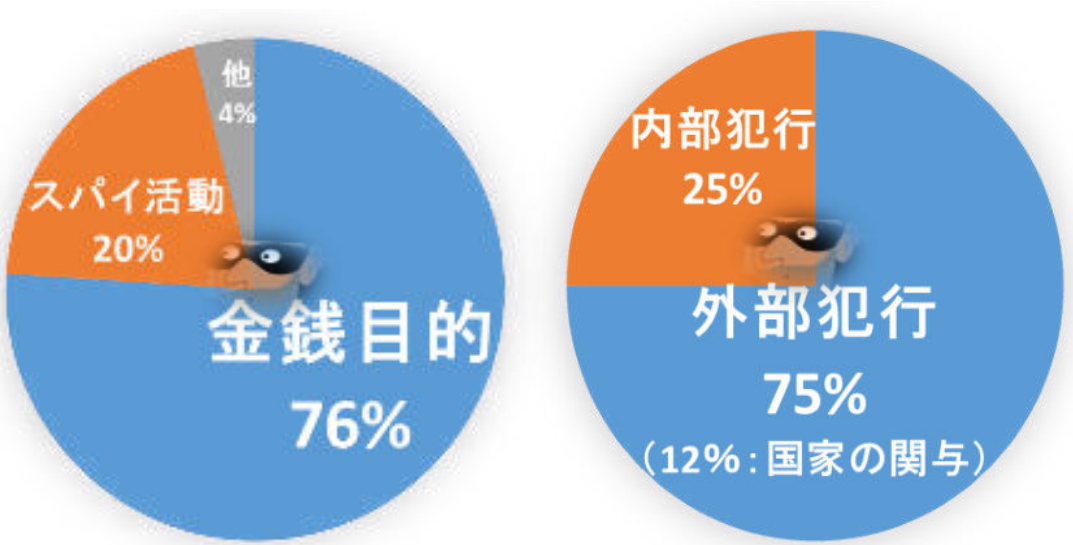
サイバー攻撃の「攻撃する側」

攻撃者の変容

個人・愉快犯

気付かせることで
自己顕示欲を満たす

組織・経済犯



気付かせないことで
利益の最大化を図る

※米国の大手通信会社ベライゾン社の調査（2018年）

サイバー攻撃の「攻撃される側」

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

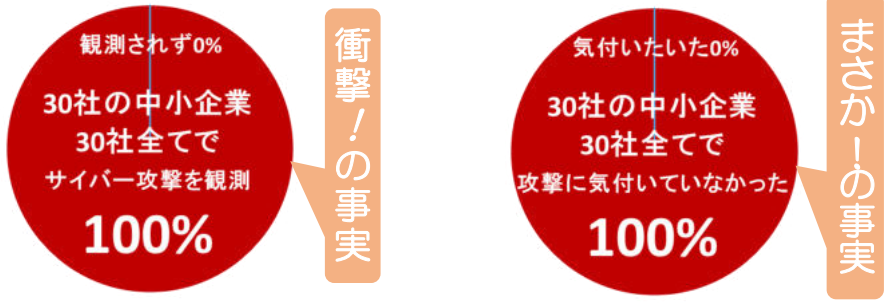
対策してないIoTをネットにつないだ
↓
最短38秒で感染
※横浜国立大学2016年調査

☞セキュリティ脆弱　→　攻撃の踏み台に

中小企業って狙われてるの？

①中小企業30社中30社（100％）で攻撃を観測！

※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／大阪30社）



②攻撃を受けていた中小企業では

１社あたり平均、月56件の「外→内」の攻撃
１社あたり平均、月　4件の「内→外」の不審通信

※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／京阪神110社）

☞「ウチなんか狙われへんって！」って考えることは危険！

どんな中小企業に攻撃が？（地域）

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	64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%）

※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

☞地域と攻撃の関係性は、ほぼ無し！どの地域でも攻撃は（結構多く）ある！

どんな中小企業に攻撃が？（業種）

検知	UTMが検知した通信	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
		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%
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%
なし		9	8	5	1	1	0

※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／京阪神110社　※UTM不適切設置2社除く）

☞業種と攻撃の関係性は、ほぼ無し！どの業種でも攻撃は（結構多く）ある！

サイバー攻撃の攻撃手法（総論）

攻撃手法の多様化

2021年	個人	2022年	組織	2021年
2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
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4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	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4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	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7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	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

※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2022」

☞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）

ランサムウエア（組織1位） 概要

- ファイルが暗号化され使用不能に
- 復号と見返りに身代金要求
- 身代金の支払手段は仮想通貨
- 身代金の額は？
- 身代金は値引交渉できる？
- 身代金を支払うと？
- 身代金を支払わないと？

※上画像：大阪府警察HPより　ランサムウェア「Wannacry」

☞日本のランサムウエアの被害額は世界２位との統計情報も

サイバー攻撃の攻撃手法(各論)

ランサムウエア（組織1位） 対策

【事前対策】

- 検知と防御
  - 出入口：UTM
  - 各端末：EDR
- 定期的なバックアップ
  - ローカル（保存先HDDとのLAN線は逐一抜く）
  - クラウド（「CCI Back up」など）

【事後対策】

- 即ＬＡＮ線を抜く

一瞬というほどでもない！　今さら抜いても遅い！と思わない！

（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？
- 民間の復号サービスも（無料･有料）

トレンドマイクロ「ランサムウェア ファイル復号化ツール」
https://esupport.trendmicro.com/support/vb/solution/ja-jp/1114210.aspx

※上図:大阪府警察HPより

tú

サイバー攻撃の攻撃手法(各論)

標的型攻撃メール(組織2位)・ビジネスメール詐欺(組織8位) 概要

※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**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」

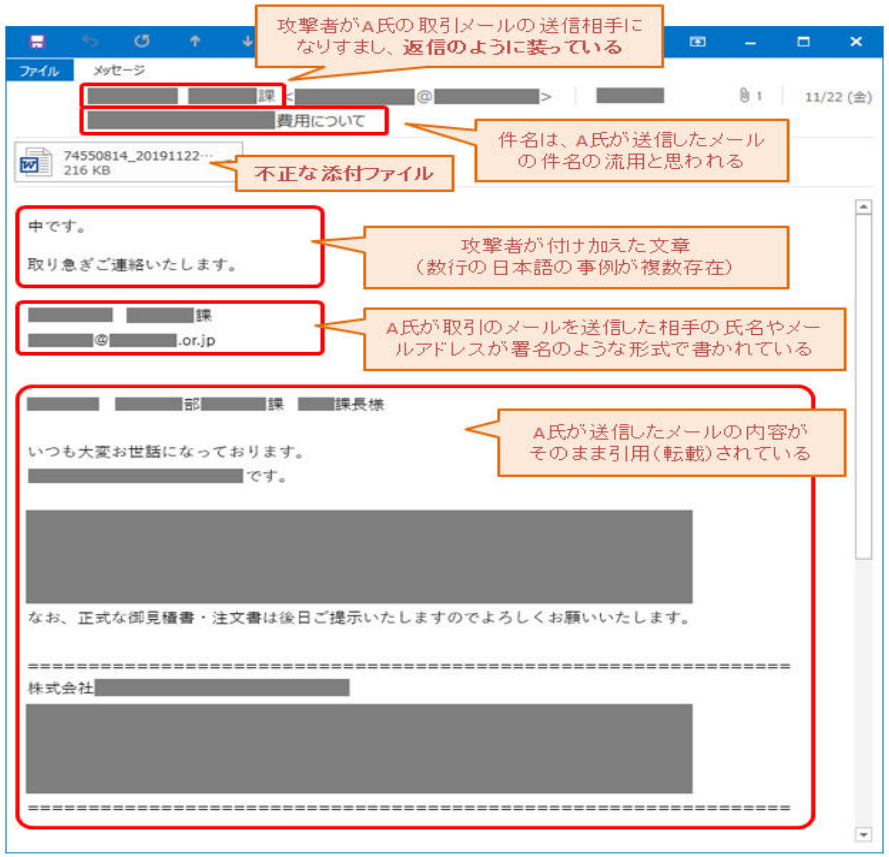
②ビジネスメール詐欺

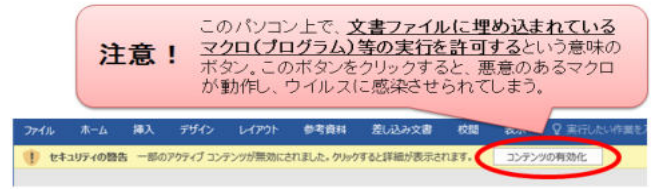
- **金銭**の窃取
- 「さっき送った振込先、間違ってました。変更願います」

サイバー攻撃の攻撃手法（各論）

標的型攻撃メール（組織2位）実例

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
  ↓
- 自分の執筆し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）

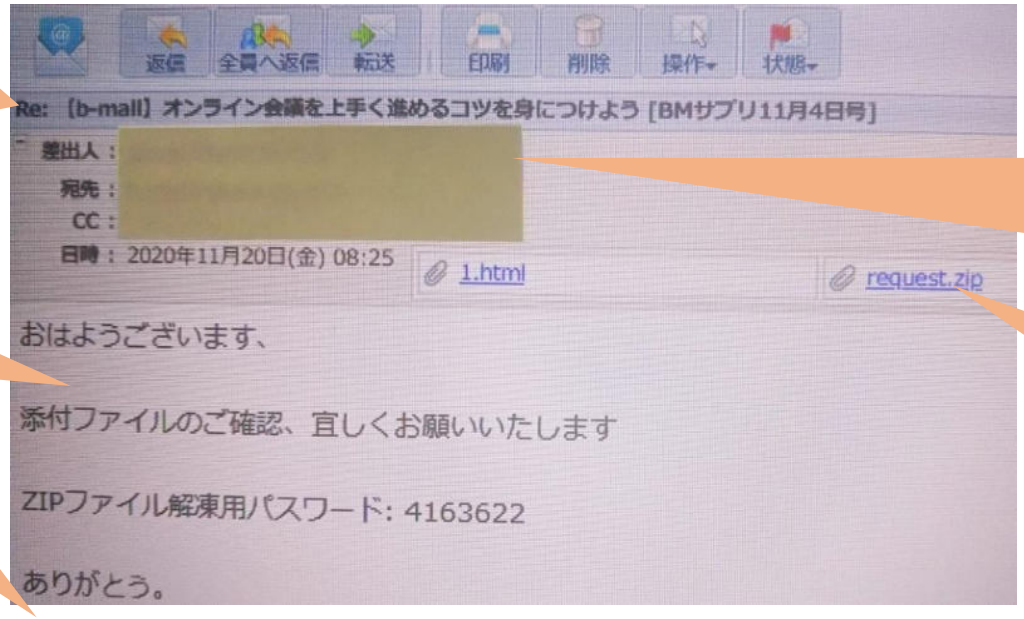
標的型攻撃メール（組織2位）実例

ウイルスメール「Ｅｍｏｔｅｔ（エモテット）」の別の手口（パスワード付き圧縮ファイル）「ＩｃｅｄＩＤ（アイスドゥ・アイディー）」

大阪商工会議所が実際に送信したメールの返信として送信されてきた

あいかわらず稚拙な日本語、抽象的な表現、変な句読点

メール後半に、自分が実際に送信（執筆）した本文が残されているケースも



大阪商工会議所が実際に送信したメールの送信先が差出人となっている（この会社のPCが感染し当該PCのメールボックス等の中の情報を元に感染が拡大したものと推定される）

Zipファイルを開けると「Emotet」と同じような文書ファイルがあり そのマクロ実行で感染

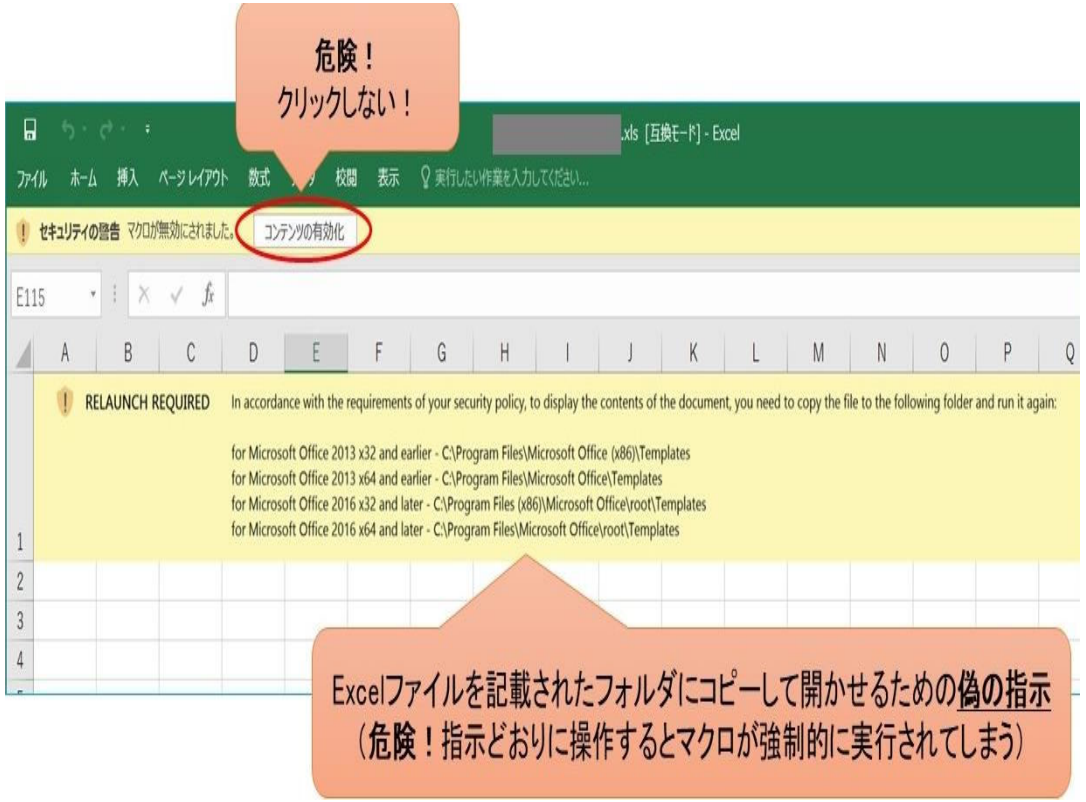
※大阪商工会議所に実際に着信したメール（2020年11月20日）

☞最近は日本語が上達しているので要注意！ショートカットファイルも要注意

サイバー攻撃の攻撃手法（各論）

標的型攻撃メール（組織2位） 実例

ウイルスメール「Emotet（エモテット）」の最新の手口（2022年11月2日）



- 2022年11月2日から、メールに添付のExcelファイル内に書かれている偽の指示が、コンテンツの有効化を促す内容だったものから左図のように変化
- Excelファイルを、記載されたTemplatesフォルダにコピーして開くと、マクロを無効化する設定にしていても、ファイルに含まれている悪意あるマクロが強制的に実行されてしまう（コピー先のTemplatesフォルダが“信頼できる場所”としてデフォルトで設定されているため同フォルダに格納されたファイルは安全性の高いファイルとみなされ、マクロが実行可能に

※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

tú

サイバー攻撃の攻撃手法(各論)

標的型攻撃メール(組織2位)・ビジネスメール詐欺(組織8位) 実例

こんなタイトルは注意！

【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＞
【最終警告】au PAY マーケット からの緊急の連絡
【au PAY マーケット】個人情報確認

※JNSA提供情報

☞金融機関、大手小売業、宅配便が多い

tú

サイバー攻撃の攻撃手法(各論)

標的型攻撃メール(2位)・ビジネスメール詐欺(8位) 対策

×そのメールを開き、URLや
添付ファイルをクリック
してはいけない

○その案件を、検索エンジンで
能動的に手入力し調べてみる

○その会社の公式Webサイトに
その案件が掲載されているか確認

tú

サイバー攻撃の攻撃手法(各論)

標的型攻撃メール(2位)・ビジネスメール詐欺(8位) 対策

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！

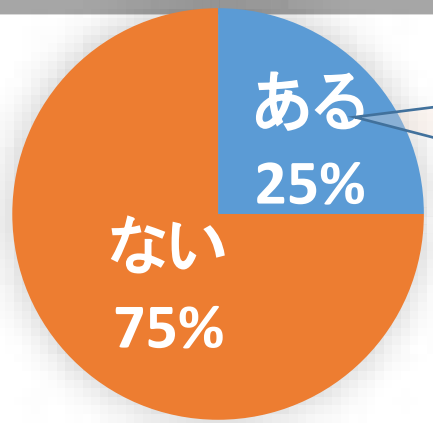
you tú 你

サイバー攻撃の攻撃手法(各論)

サプライチェーン攻撃（3位） 概要

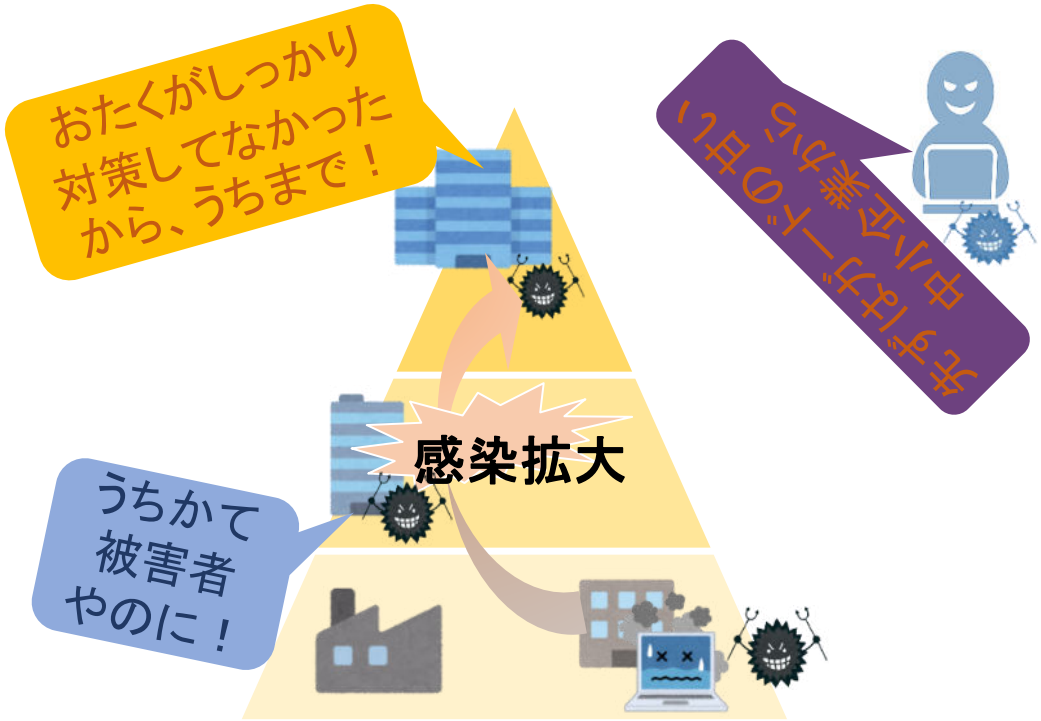
大企業・中堅企業(全国118社)

取引先の中小企業が受けたサイバー攻撃被害が自社に及んだことが



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！

tú

サイバー攻撃の攻撃手法（各論）

フィッシングによる個人情報等の詐取（個人１位）
偽警告によるインターネット詐欺（個人６位）

実例

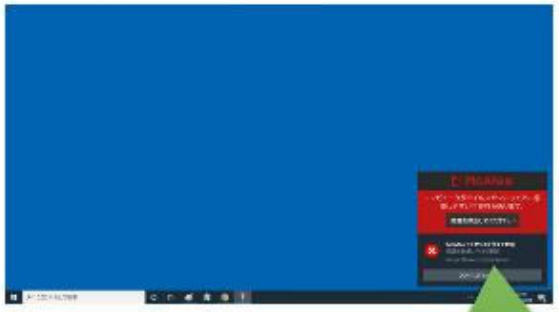
■Amazonのフィッシングの手口

フィッシングメール

フィッシングサイト

URLリンクをクリックしない！！

■ブラウザ通知悪用の手口



不審な通知画面

偽のセキュリティ警告サイト

URLリンクをクリックしない！！

※上図：独立行政法人情報処理推進機構（IPA）HPよりそのまま引用

対策　フィッシングサイトの見分け方

☞見分けようとしないこと！（似せて作ってある、というより、そのままコピーされている！）

中小企業における
サイバー攻撃の実態
（中小企業における被害事例）

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／建築材料卸売業／従業員30～40人）

実例

・**D-DoS攻撃**（多数の外部端末から大量の通信を送られることによるサービス運用妨害）

対策

・異常通信を遮断するUTMやIPS（不正通信防御）を導入
・DDoS攻撃元IPアドレスからの通信をFW等で遮断
・特定の国からのアクセスをFWやWAF等で遮断
・社内でNTP（時刻同期）サーバを公開している場合、脆弱性対策済のバージョンにアップデート

※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）

④Ｄ社（大阪府／医療用器具製造業／従業員80～90人）

・**バックドア**（サイバー攻撃者のユーザーPCへの裏口）として利用されるコンピュータウイルス「GhOstRAT」による**悪性サーバーからの指令等の通信**が検知された。

※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）

⑤Ｅ社（大阪府／機械製造業／従業員100～150人）

・**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** ※大阪商工会議所での相談事例（2020年7月）

中小企業にどんな攻撃が？（実例）

⑥Ｆ社（大阪府／化学品卸売業／従業員70～80人）

- **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）

⑦G社（事務用品･文具の製造･販売／従業員約900人）

- **自社の通販サイトが不正アクセスを受け、顧客のクレジットカード情報が漏えい。同サイトは４か月閉鎖逸失利益が約４千万円発生**

※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）

中小企業にどんな攻撃が？（実例）

⑧H社（愛知県／自動車部品製造業／従業員約1700人）

- 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Ｆ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！

中小企業における サイバー攻撃対策の実情

中小企業のサイバー対策実情（人）

情報システム担当者がいるか？

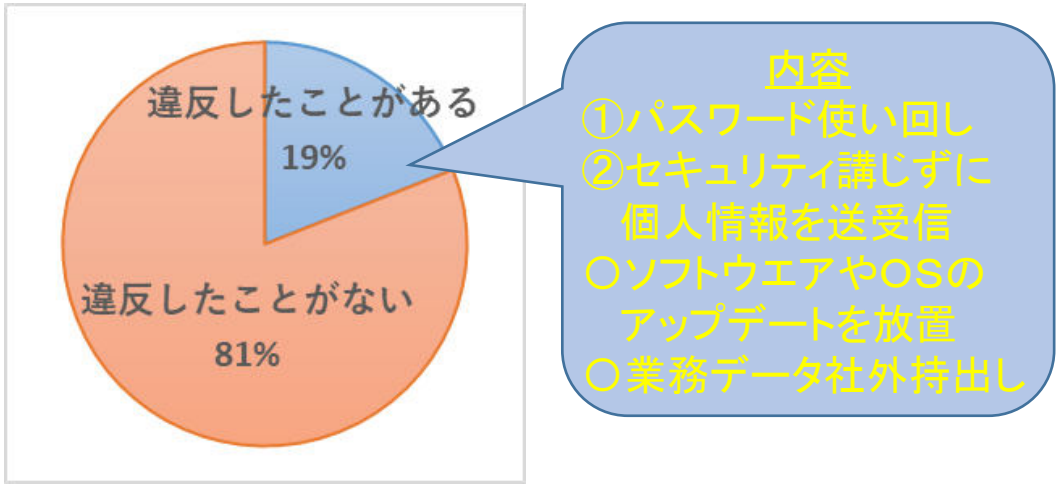
情報システム担当者の有無	令和2年度サイバーお助け隊実証 参加企業（2020年10月）n=50 滋賀・奈良・和歌山の中小企業 【平均30.8人・中央10.0人】	令和元年度サイバーお助け隊実証 参加企業（2020年1月）n=105 大阪・京都・兵庫の中小企業 【平均29.3人・中央11.5人】
専任者がいる	3(6%)	9(9%)
兼任者しかいない	17(34%)	34(32%)
1人もおらず経営層が直轄	22(44%)	52(50%)
1人もおらずIT業者に外注	7(14%)	10(10%)
回答なし	1(2%)	ー

※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

☞３割が「兼任情シス」、６割が「ゼロ情シス」
一般的に課題視される「ひとり情シス」ですら、中小企業では“最上位クラス”

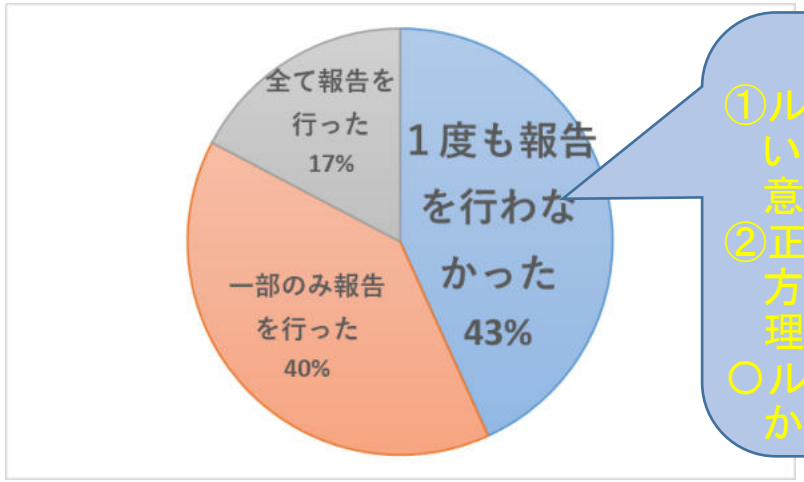
中小企業のサイバー対策実情（人）

従業員が会社の情報管理ルールに違反したことがあるか？



内容
①パスワード使い回し
②セキュリティ講じずに個人情報を送受信
〇ソフトウエアやOSのアップデートを放置
〇業務データ社外持出し

従業員はルール違反を会社や上司に報告したか？



理由
①ルールは理解していたがそれを守る意識が稀薄だった
②正しい手順や対応方法等の知識や理解が不足してた
〇ルール自体知らなかった

※独立行政法人情報処理推進機構　中小企業の従業員へのアンケート調査（2021年12月8日）

☞“かくれサイバートラブル”が相当数発生か？！そして、責任の所在は、、、

中小企業のサイバー対策実情（お金）

サイバー対策に年どれくらいお金をかけているか？

サイバー対策年間経費 （正社員情シス担当者人件費除く）	令和2年度サイバーお助け隊実証 参加企業（2020年10月）n=50 滋賀・奈良・和歌山の中小企業 【平均30.8人・中央10.0人】	令和元年度サイバーお助け隊実証 参加企業（2020年1月）n=105 大阪・京都・兵庫の中小企業 【平均29.3人・中央11.5人】
5万円未満	32(64%)	76(72%)
5～10万	8(16%)	8(8%)
11～20万	5(10%)	9(9%)
21～50万	4(8%)	7(7%)
51万以上	0(0%)	4(4%)
回答なし	1(2%)	1(1%)

※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

☞８割が「年１０万円以下」（月額では１万円未満）
金額が大きくなるほど少ない傾向

中小企業のサイバー対策実情（対策）

どんなサイバーセキュリティを実施しているか？

サイバー攻撃対策の セキュリティ実施状況 ※複数回答あり	令和2年度サイバーお助け隊実証 参加企業（2020年10月）n=50 滋賀･奈良･和歌山の中小企業 【平均30.8人・中央10.0人】	令和元年度サイバーお助け隊実証 参加企業（2020年1月）n=105 大阪･京都･兵庫の中小企業 【平均29.3人・中央11.5人】
アンチウイルスソフト	46(92%)	91(87%)
ファイアウオール	14(28%)	40(38%)
UTM	1(2%)	8(8%)
その他ITベンダー提供のセキュリティサービス	1(2%)	3(3%)
データのパスワード設定	6(12%)	16(14%)
データの暗号化	3(6%)	6(6%)
物理的管理の徹底	0(0%)	6(6%)
社員教育・研修	6(12%)	14(14%)
専門人材育成	0(0%)	1(1%)
SECURITY　ACTION	4(8%)	11(11%)
サイバー攻撃損害保険	1(2%)	0(0%)
取引先との情報管理契約	2(4%)	3(3%)
サプライチェーンでの規定等の制定・参画	0(0%)	1(1%)
特に実施していない	2(4%)	3(3%)

アメリカでは、半数以上がサイバー保険に入っている

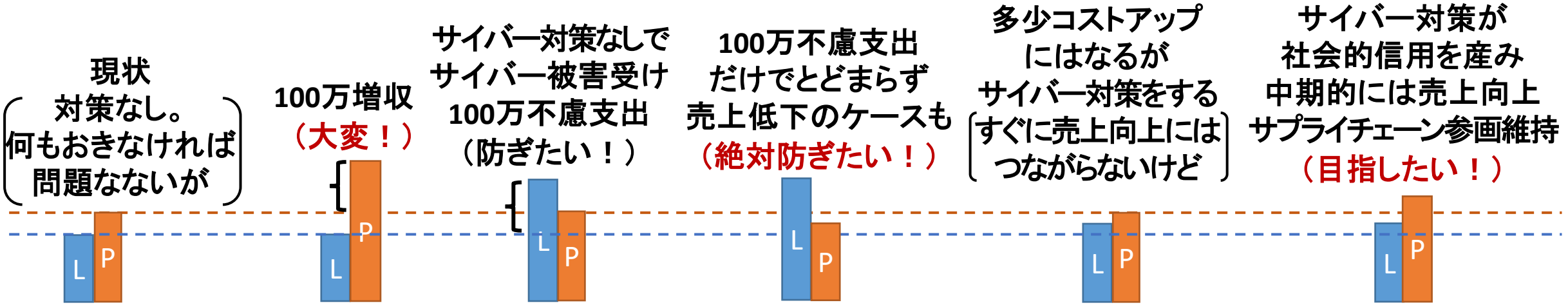
※大阪商工会議所が実施したサイバーセキュリティお助け隊実証（2019年・2020年）での調査結果

では、中小企業はどういう視点を持てばいいのか？（概論）

中小企業のサイバー対策に必要な視点

①「費用」でなく「投資」と！ 対策の前提となる考え方

- 100万円の売上を創るより、100万円の「無駄な支出」防止
- 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

②実例で見る「費用」と「投資」の関係性

対策の前提となる考え方

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（ｺﾝｻﾙﾃｨﾝｸﾞ･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）

中小企業のサイバー対策に必要な視点

③「相場」は？

対策の前提となる考え方

- セキュリティ投資（費用）は、
  - ☞セキュリティベンダ推奨……売上の１％
  - ☞現実的には……売上の０．５％

売　上	ベンダー推奨	現実的には、、、
年商5億円	500万円	250万円
年商1億円	100万円	50万円
年商5千万円	50万円	25万円

☞ウイルス対策ソフト＋α（何ができるか？）

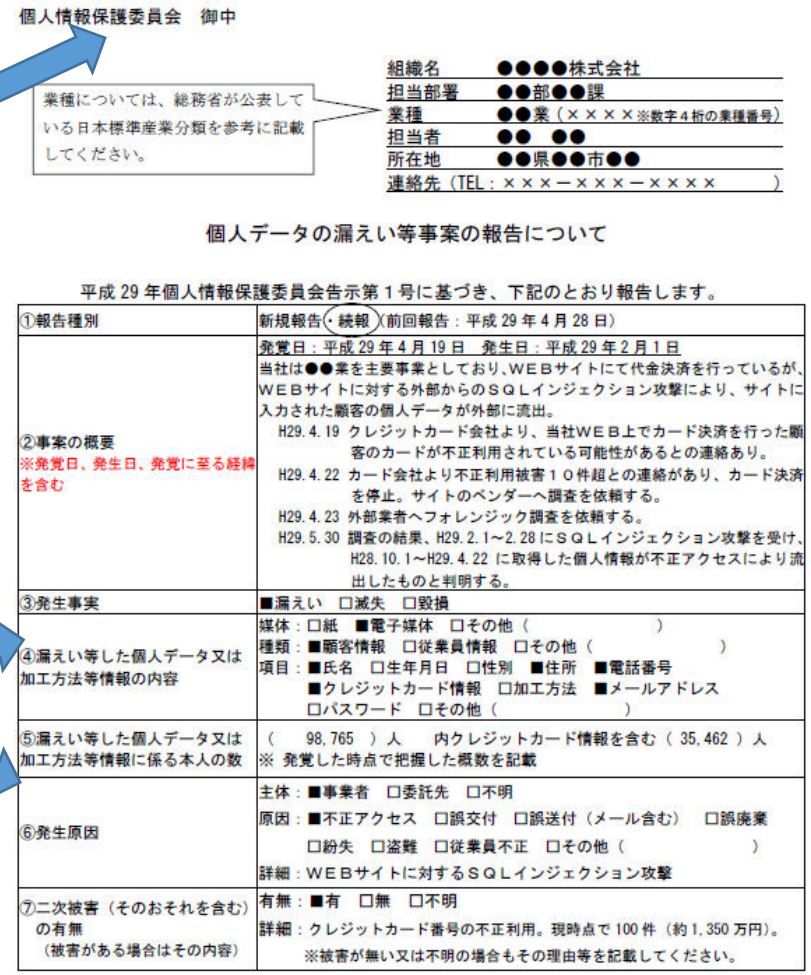
中小企業のサイバー対策に必要な視点

2022年4 月施行の改正個人情報保護法

企業は（サイバー攻撃などの不正アクセスに
より情報漏洩が発生した場合を含め）
被害者（漏洩した本人）・当局への通知・報告が
原則義務化（改正前は努力義務）！
報告義務違反には、罰則（罰金）も！

☞**いつ、どんなサイバー攻撃をされ、**
どんな個人情報が、どのくらい、
何が原因で漏えいしたかを**報告する必要**があります。

☞こうした情報を日常的に「把握」「記録」する体制や
ツールやサービス利用が必要。
さもなくば**「調査」に多額の費用が発生。**



個人情報保護委員会　御中

業種については、総務省が公表している日本標準産業分類を参考に記載してください。

組織名	●●●●株式会社
担当部署	●●部●●課
業種	●●業（××××※数字4桁の業種番号）
担当者	●●　●●
所在地	●●県●●市●●
連絡先（TEL：×××－×××－×××× ）	

個人データの漏えい等事案の報告について

平成 29 年個人情報保護委員会告示第 1 号に基づき、下記のとおり報告します。

①報告種別	新規報告・続報（前回報告：平成 29 年 4 月 28 日）
②事案の概要 ※発覚日、発生日、発覚に至る経緯を含む	発覚日：平成 29 年 4 月 19 日　発生日：平成 29 年 2 月 1 日 当社は●●業を主要事業としており、ＷＥＢサイトにて代金決済を行っているが、ＷＥＢサイトに対する外部からのＳＱＬインジェクション攻撃により、サイトに入力された顧客の個人データが外部に流出。 H29. 4. 19 クレジットカード会社より、当社ＷＥＢ上でカード決済を行った顧客のカードが不正利用されている可能性があるとの連絡あり。 H29. 4. 22 カード会社より不正利用被害１０件超との連絡があり、カード決済を停止。サイトのベンダーへ調査を依頼する。 H29. 4. 23 外部業者へフォレンジック調査を依頼する。 H29. 5. 30 調査の結果、H29. 2. 1～2. 28 にＳＱＬインジェクション攻撃を受け、H28. 10. 1～H29. 4. 22 に取得した個人情報が不正アクセスにより流出したものと判明する。
③発生事実	■漏えい　□滅失　□毀損
④漏えい等した個人データ又は加工方法等情報の内容	媒体：□紙　■電子媒体　□その他（　　） 種類：■顧客情報　□従業員情報　□その他（　　） 項目：■氏名　□生年月日　□性別　■住所　■電話番号 ■クレジットカード情報　□加工方法　■メールアドレス □パスワード　□その他（　　）
⑤漏えい等した個人データ又は加工方法等情報に係る本人の数	（　98, 765　）人　　内クレジットカード情報を含む（ 35, 462 ）人 ※ 発覚した時点で把握した概数を記載
⑥発生原因	主体：■事業者　□委託先　□不明 原因：■不正アクセス　□誤交付　□誤送付（メール含む）　□誤廃棄 □紛失　□盗難　□従業員不正　□その他（　　） 詳細：ＷＥＢサイトに対するＳＱＬインジェクション攻撃
⑦二次被害（そのおそれを含む）の有無 （被害がある場合はその内容）	有無：■有　□無　□不明 詳細：クレジットカード番号の不正利用。現時点で 100 件（約 1, 350 万円）。 ※被害が無い又は不明の場合もその理由等を記載してください。

商工会議所
サイバーセキュリティ
お助け隊サービス
（サービス概要）

商工会議所サイバーセキュリティお助け隊サービス（趣旨）

- 国（経済産業省・IPA）の実証事業を通じて事業化
- NEC・東京海上と連携し大阪商工会議所がサービス提供
- 人・お金が不足がちな中小企業に特化した格安・簡便なサイバーセキュリティ・パッケージサービス
- 国（経済産業省・IPA）の「サイバーセキュリティお助け隊サービス」の基準を満たし、国に登録されたサービス
- 利用企業は「わが社は、中小企業として最低限のセキュリティ対策やってます」と公言できる！
- IT導入補助金の対象（２年分の利用料を1/2補助）

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）

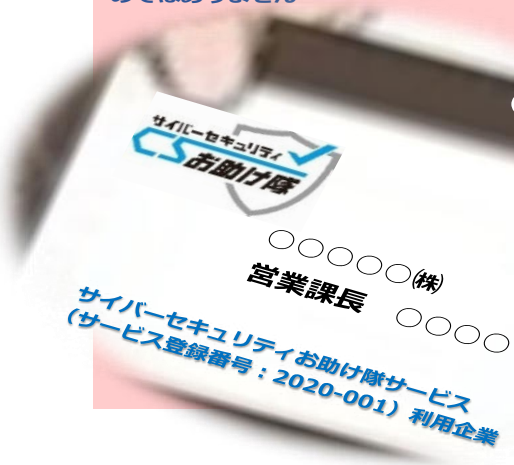
レンタルUTMの「お守り」＋常時「見守り」＋困った時「相談」
攻撃時「お知らせ」＋事故時「駆け付け（保険）」＝「信用」

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

顧客紹介

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）

駆け付け
（初動対処）

信用

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

「商工会議所サイバーセキュリティお助け隊サービス」ユーザ概況

①契約社数	計281社　【大商直販】217社 【再販】64社（2年残留：94%、３年残留：91%）
②契約台数	計354台　【大商直販】263台 【再販】91台（2台:17社、3台:8社、4台1社、5台:3社、10台以上:2社）
③都道府県 本社所在地　社数	大阪61%、兵庫8%、東京5%、和歌山5%、千葉3%、京都3%、奈良3%、新潟2%、滋賀2%、 群馬、茨城、神奈川、長野、静岡、愛知、福井、三重、香川、岡山、広島、山口、大分、熊本、宮崎、鹿児島…1%
④業種	製造業29%、サービス業27%、公的機関11%、建設・工事業10%、卸売業8%、小売業6%、 情報通信業3%、病院・社会福祉3%、宿泊飲食業2%、不動産業1%、運輸業1%、不明1%
⑤規模	平均値57人、中央値16人（～5人18%、6～10人9%、11～20人13%、 21～50人12%、51～100人9%、101～200人4%、201人～4%、不明31%）

製造販売業（社員100人）
クライアント数に対して利用料金が安価

製造業（社員3人）
規模拡大に伴い、機器ごとの個別対策実施が煩雑になるため、出入口での一括対策が必要

サービス業（社員8人）
UTMでウイルスが検知され、相談窓口に相談。その日のうちに駆け付け対応してもらい、ウイルスを駆除できた

建設業（社員12人）
使い勝手がよい

卸売業（社員68人）
費用が高額でなく、実際に攻撃が週1回程ありそれを防げているため、利用を継続したい

製造業（社員6人）
今後ネットショップを開業予定。セキュリティを強化させたい

製造業（社員17人）
セキュリティ被害にあった場合、社内対応が不可能に近い駆け付け対応を含む一次対応があるので助かります

商工会議所サイバーセキュリティお助け隊サービス（ユーザ実例）

α社様（大阪/建設業/80～90人） 実例

本サービス利用前

・偽の請求書メール（Emotet）を開封してしまったことにより、PCがウイルス感染した。（2019年12月発生）

本サービス利用の理由

・すぐに対応してくれる（できる）安心感＋安価
・何も対策を講じず情報漏洩等で取引先様にご迷惑をおかけするわけにはいかない
・ウイルス感染時に、どんなウイルスがいつ侵入したか情報提供がある

本サービス利用後

・再び偽の請求書メール（Emotet）が届いたが本サービスのUTMが水際で防御。被害無。（2020年7月発生）

目に見えないウイルス対策に投資することへの必要性について社長を説得することに苦労しました。最終的には経費削減・ウイルス対策（UTM）の必要性について理解してもらった上でサービス利用となりました。

商工会議所サイバーセキュリティお助け隊サービス（ユーザ実例）

β社様（大阪/製造業/40～50人） 実例

実証参加中にUTMが不審な通信を観測

・会社PCから社外の悪性サーバーへの不審通信をUTMが観測（IPS）。
・コンピュータウイルスが高い確率で入り込んでいる可能性あり。
（2019年11月発生）

お助け実働隊 地域IT事業者が駆け付け支援

・駆け付けても被疑端末が見つからなかったのでその日は何も出来ず終了。
・後日、被疑端末（管理されていない“シャドーIT”）が見つかったとの連絡があり、再び駆け付け。
・そのPCから474件のウイルスが見つかり、駆除。

なにが問題だったか？放置するとどんなことが起きた？

・社長の親族の管理下にあるPCだった点。それを会社のLANに接続していた点。
・駆除したウイルスは個人情報を窃取するタイプのもの（Dorkbot）。放置は被害拡大をもたらした可能性大。

サイバーセキュリティお助け隊サービス　メディアも注目

NHK「おはよう日本」（2022.6.17）

読売新聞（2022.6.19）

2022年(令和4年)6月19日(日曜日)　読売新聞

サイバーテロII　企業の危機　5

監視の目強化 国が支援

朝日新聞（2022.2.3）

個人情報流出 備えは

サイバー保険 損保販売強化

報告義務化

■情報流出の最近の主な事例（時期は発表年月）
2020年1月　NECの社内サーバーに不正アクセス
1月　三菱電機がサイバー攻撃を受け情報流出
6月　ホンダがサイバー攻撃、米国など9工場停止
11月　カプコンにサイバー攻撃、内部情報流出
21年7月　川崎汽船子会社のシステムに不正アクセス
11月　日本政策投資銀行の海外法人にサイバー攻撃
（各社の発表内容をもとに作成）

個人情報の流出事故を起こした企業に報告義務を課す法改正を4月にひかえ、経済界に対応に乗り出す動きが広がってきた。中小企業では対策の遅れが目立ち、商工会議所などが加盟企業の支援に乗り出しているほか、損害保険大手は好機とみて、「サイバー保険」の販売を強めている。

改正個人情報保護法が4月に施行され、規模の大きな流出事故などは被害者や国の個人情報保護委員会への報告が義務化される。流出した情報の内容や原因、二次被害の恐れなどを伝える必要がある。対応に不備があれば、最大1億円の罰金が科されたり、個人情報保護委員会の命令に従わない場合、社名を公表されたりすることもある。

被害者数が多いなど、一定の要件を満たせば、大企業だけでなく中小企業も対象だ。そこで、中小の加盟企業が多い大阪商工会議所では、法改正や必要な対策などに関する情報提供に力を入れているほか、提携先のサイバーセキュリティー会社によるシステムの見守りサービスも提供している。ただ、「中小企業の多くは売り上げを生まない『守りのIT投資』をコストとみて、なかなか広がらない」（担当者）と話す。

大阪日日新聞（2021.5.19）

大商、サイバー対策で認定

IPA審査 中小企業向けサービス強化へ

産経新聞（2022.10.23）

資金・人材不足、大商が支援も

コーディネーションセンター」（東京）によると、ネットの不正に関する報告件数は平成30年度の1万6639件から右肩上がりで、令和3年度は5万801件だった。

企業の間で対策は急務と意識されている。帝国データバンクが5月に近畿2府4県の企業を対象に実施した調査では、事業継続計画（BCP）を策定する意思があるとした企業（970社）のうち、想定するリスクとして「情報セキュリティー上のリスク」は37・4％で、自然災害と感染症に次ぐ3番目の高さだった（複数回答）。

国の対応必要

ただ、大手企業と比べてセキュリティーが甘く、標的になりやすいとの指摘もある中小企業では対策が進まない。大阪商工会議所経営情報センターの野田幹稚課長によると、サイバー対策に必要な費用は事業の売上高の0・5～1％とされるが、中小には重い負担となる。野田氏は「複雑化する手口に対応できる情報システム担当者が中小に入る人は少なく、経営者が担当を兼ねるケースは珍しくない」と話す。同会議所は中小向けに定額制のセキュリティーサービスを用意。サービスを開始した令和2年度で約70社だった利用者は3年度に約150社、4年度は10月時点で約280社と増え続ける。

中小がとる対策について、帝国データバンク大阪支社の昌木裕司情報部長は「不審なメールは開かないという基本を守り、最新のセキュリティーソフトを常備することの徹底が重要。サイバー保険を利用することで不測の事態への補償を確保することもできる」と指摘。一方で「一企業でできることには限界があり、国家レベルでの対策を取らなくては、日本経済にとって大きなリスクとなる恐れがある」と警鐘を鳴らしている。（井上浩平）

公明新聞（2022.7.18）

サイバー攻撃から会社を守る

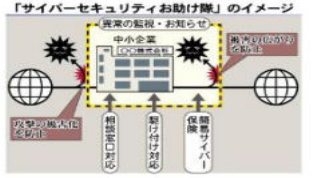
安価、簡便に導入できる「お助け隊サービス」

月額6600円で提供

"経営の重要課題"と推進

大商の取り組み

「サイバーセキュリティお助け隊」のイメージ



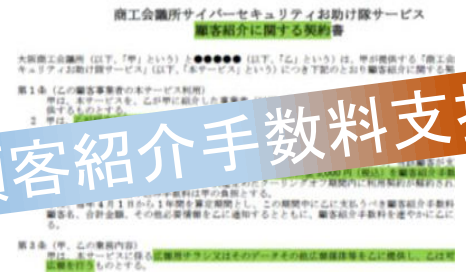
損害保険会社代理店様へのご提案
（顧客紹介手数料支払い契約）

サイバー保険と親和性の高い本サービスのご活用

- **本格的なサイバー保険（賠償型）を拡販するうえでのドアノックツールに「お助け隊サービス」をご利用下さい！**

損害保険会社代理店様と大阪商工会議所との協業

- 「商工会議所サイバーセキュリティお助け隊サービス」顧客紹介手数料支払い契約のご提案


商工会議所サイバーセキュリティお助け隊サービス
顧客紹介に関する契約書

①顧客紹介手数料支払い契約

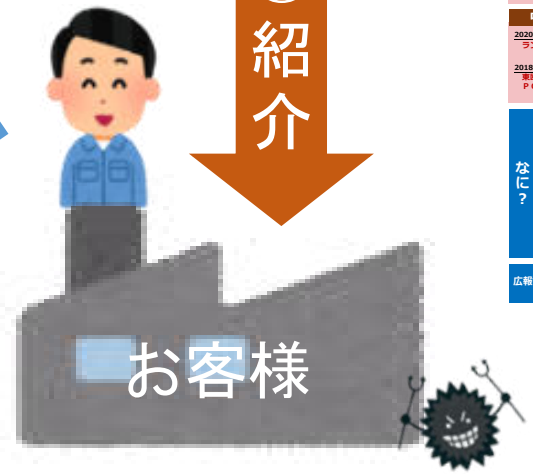
⑤顧客紹介手数料支払い

③詳細説明

④「商工会議所サイバーセキュリティお助け隊サービス」申込

詳しいことは大阪商工会議所からご説明させて頂きます

②紹介



- ✓ 会社の規模や業種に関係なく、
  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、
  事業継続の実現を！

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

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/