中小企業におけるサイバー攻撃の実態と対処能力の向上

2022年8月

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 実態と対策（個別対策）

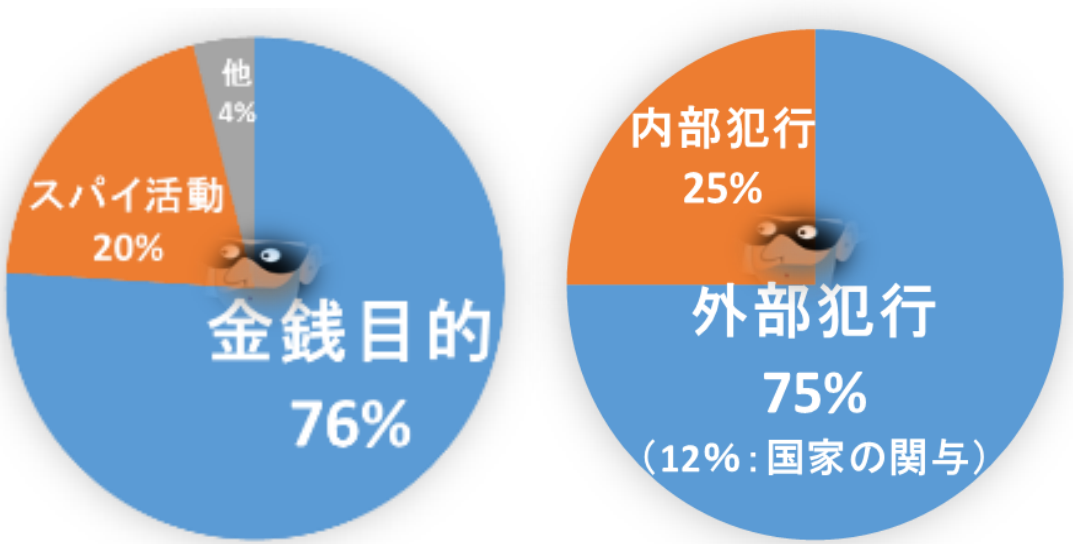
サイバー攻撃の「攻撃する側」

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

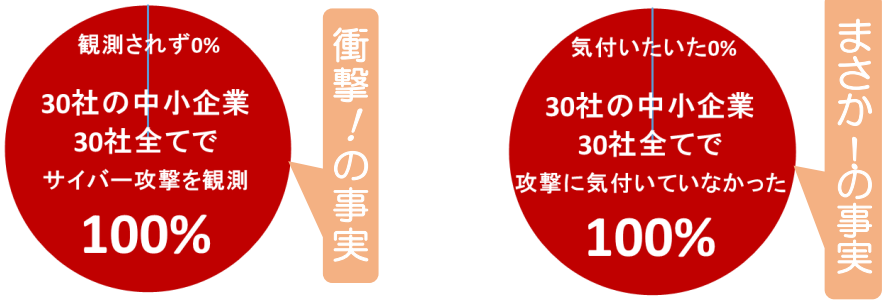
対策してないIoTをネットにつないだ
↓
最短38秒で感染
※横浜国立大学2016年調査

☞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 全体中の参加率 39%	サービス業 35社 全体中の参加率 32%	卸売業 18社 全体中の参加率 16%	建設業 8社 全体中の参加率 7%	小売飲食 6社 全体中の参加率 5%	運輸業 1社 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（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（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（松本商工会議所「CCI Back up」など）

【事後対策】

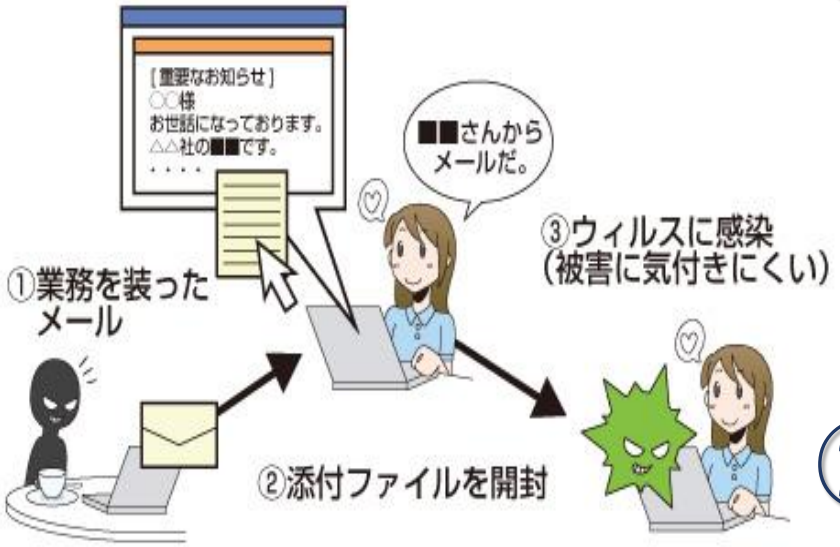
- すぐにLAN線を抜く。電源は落とさない
- 警察にPCを預けると？
- 民間の復号サービスも（無料･有料）

※下図：大阪府警察HPより

☞暗号化は「一瞬」ではなく一定時間かかる。不審を感じたら直ぐにLAN線を抜く

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) 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）

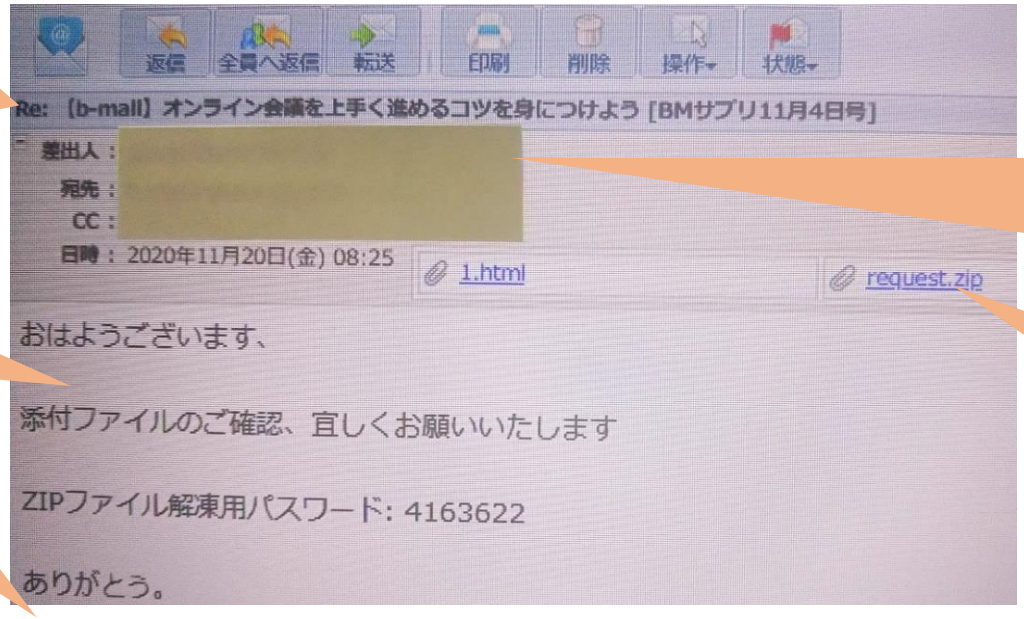
標的型攻撃メール（2位） 実例

ウイルスメール「Ｅｍｏｔｅｔ（エモテット）」と、その新手法（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

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) 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

〇その案件を、検索エンジンで
能動的に手入力し調べてみる

〇その会社の公式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！

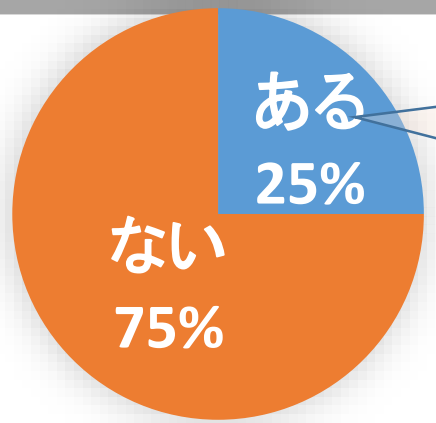
you tú 你

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

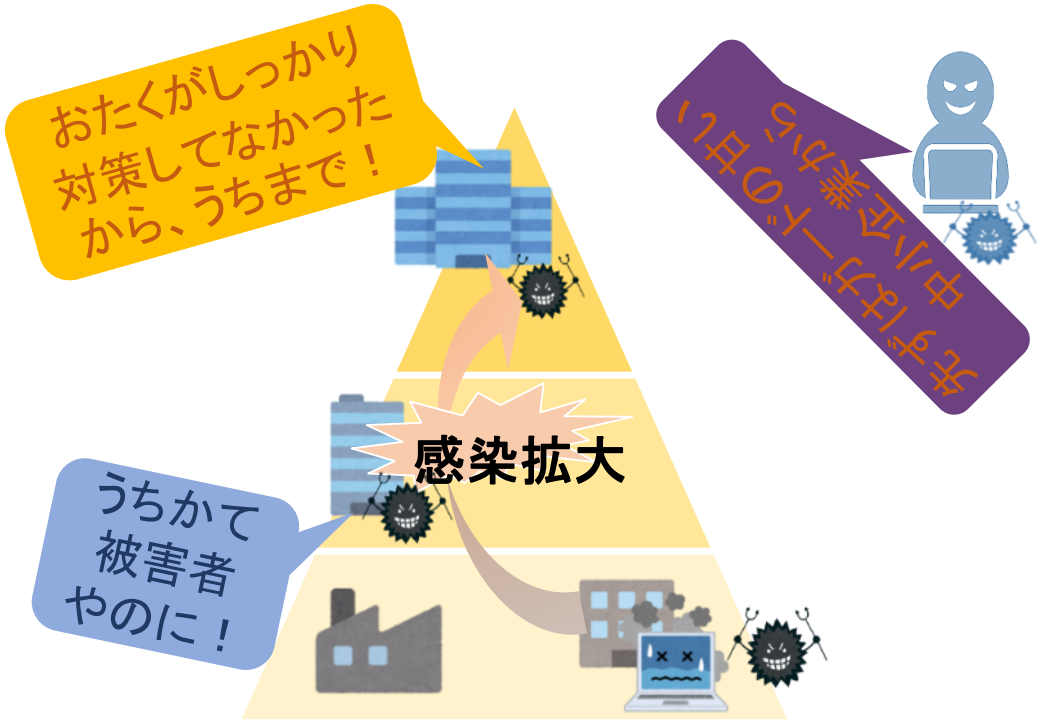
大企業・中堅企業(全国118社)

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！**

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）対策

・技術的な意味では「サプライチェーン攻撃に特化した対策」というのは、ない

【国の動向】

・「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


JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

1.0 版

2020年12月1日

jama
Japan Automobile Manufacturers Association, Inc.

JAPIA
Japan Auto Parts Industries Association

一般社団法人 日本自動車工業会
電子情報委員会
サイバーセキュリティ部会

一般社団法人 日本自動車部品工業会
IT対応委員会
サイバーセキュリティ部会

【業界の動向】

・サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）＜経産省主導＞

・各業界ごとに「サイバーセキュリティガイドライン」等を策定

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）

実例

・**バックドア**（ユーザーPCの攻撃用裏口）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

※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）

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）

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。**
・**取引先メールサーバに、同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）

実例

・**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）

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ーの全工場（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？

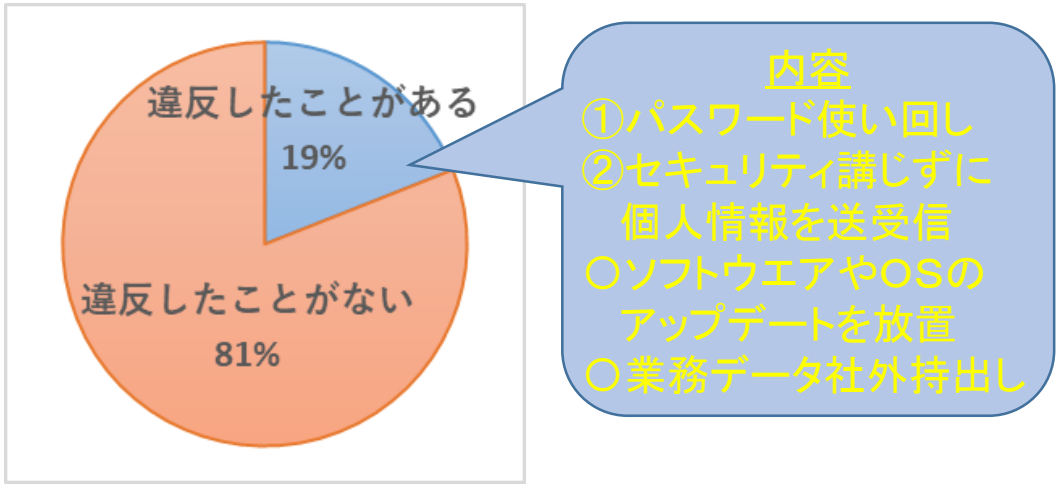
情報システム担当者の有無	令和2年度サイバーお助け隊実証 参加企業（2020年10月）n=50 滋賀・奈良・和歌山の中小企業 【平均30.8人・中央10.0人】	令和元年度サイバーお助け隊実証 参加企業（2020年1月）n=105 大阪・京都・兵庫の中小企業 【平均29.3人・中央11.5人】
専任者がいる	3(6%)	9(9%)
兼任者しかいない	17(34%)	34(32%)
1人もおらず経営層が直轄	22(44%)	52(50%)
1人もおらずIT業者に外注	7(14%)	10(10%)
回答なし	1(2%)	ー

※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

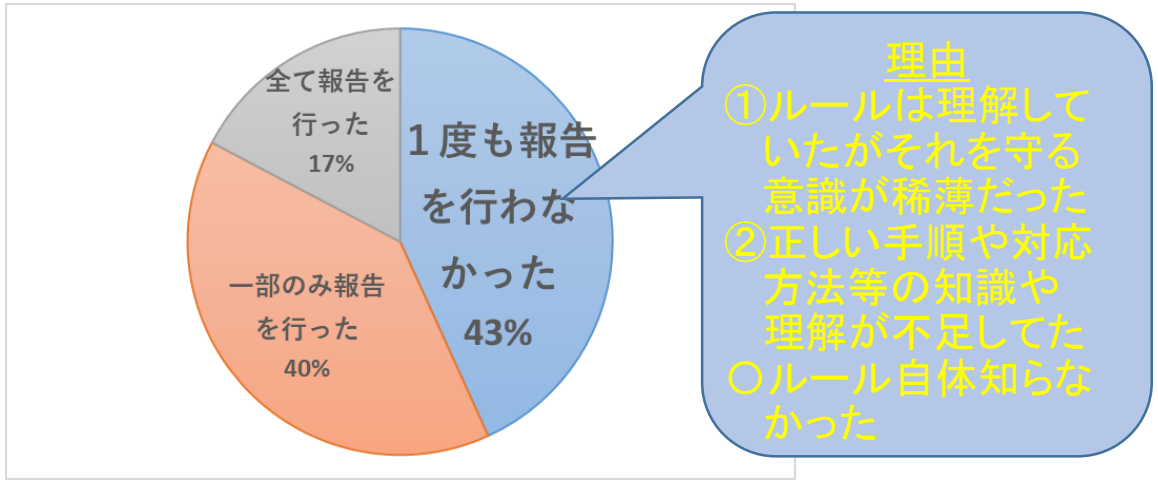
☞３割が「兼任情シス」、６割が「ゼロ情シス」
一般的に課題視される「ひとり情シス」ですら、中小企業では“最上位クラス”

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？



従業員はルール違反を会社や上司に報告したか？



※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

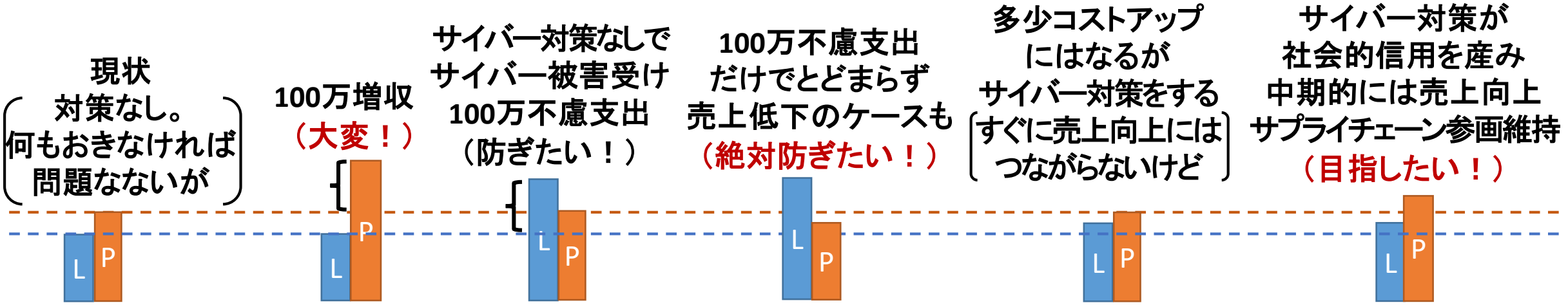
☞８割が「年１０万円以下」（月額では１万円未満）
金額が大きくなるほど少ない傾向

では、中小企業はどうすればいいのか？（全体的な対策）

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」対策の前提となる考え方

実例

	甲社（30人サービス業）	乙社（100人警備業）
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にしたことでPC1台がウイルス感染 ・お客様を含む外部に、偽装メールが送信されてしまった	・ウイルス感染により、社員のアカンウトに不正ログイン。 ・客先約180社に530通のウイルス付きメールが送信された
原因･被害範囲調査費	364万円	1257万円
再発防止費（ｺﾝｻﾙﾃｨﾝｸﾞ等）	44万円	27万円
再発防止費（ｼｽﾃﾑ導入等）	214万円	93万円
社会的信用低下	？	？
合計被害額	622万円＋？	1377万円＋？

「歴史のIF」を言ってもしゃーないけど。。。
後悔、先に立たず。。。

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1300万円

「無駄な費用を未然に防ぐための投資」

甲社200万円　乙社100万円

甲社
200万の投資で
400万の被害防止

乙社
100万の投資で
1300万の被害防止

「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？（経営層）

対策　**お金をかけずに、先ずは、経営者が**

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

- 中小企業の経営者がセキュリティに関して考えないといけないことが書かれています
- 具体的な対策の進め方について書かれてあります

※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

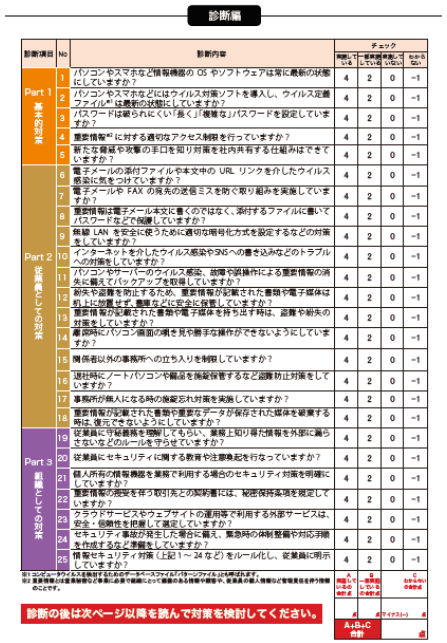
☞経営者、総務担当者、情報システム担当者向けに平易に書かれている良書

何から始めたらいいのか？（情シス）

対策 お金をかけずに、先ずは、情報システム担当者が

IPA「5分でできる！情報セキュリティ自社診断」をやる

- 25の設問に回答
- 得点に応じた対策が示されている
- オンライン受診もできる



※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

☞先ずは足元のチェック。点数化により「何を優先すべきか」が見えてくる

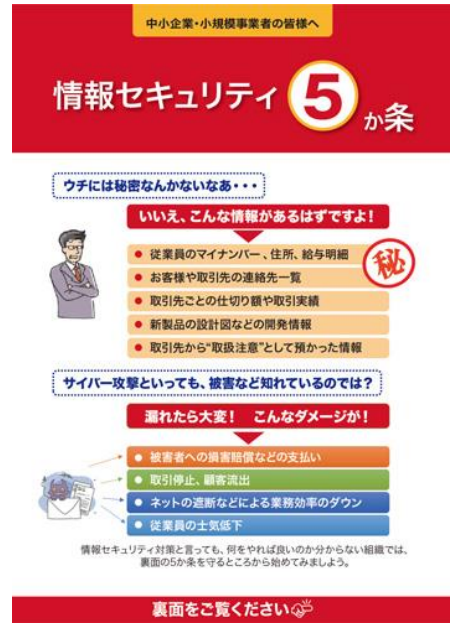
何から始めたらいいのか？（社員も）

対策

次に、少しだけ社員をまきこんで

IPA「情報セキュリティ5か条」を実践する

- **OSやソフトウェアを最新の状態に**
- **ウィルス対策ソフトを導入する**
- **パスワードを強化**
- **共有設定を見直す**
- **脅威や攻撃の手口を知る**



※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

☞これらを「実践的に取り組むことを宣言する（第三者機関の審査や認定は不要）」のが「Security Action」1つ星（IT導入補助金の申請要件。名刺などにも宣言の事実を、そのロゴマークを入れることにより、謳えます。それだけでも社員の意識は高まります。

商工会議所サイバーセキュリティお助け隊サービス（趣旨）

- 国（経済産業省・IPA）の**実証事業を通じて事業化**
- 大阪商工会議所（組成者）と、大手損保、大手IT企業、各地域IT事業者、各地商工会議所など**約50社が公民連携**
- 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！**

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）

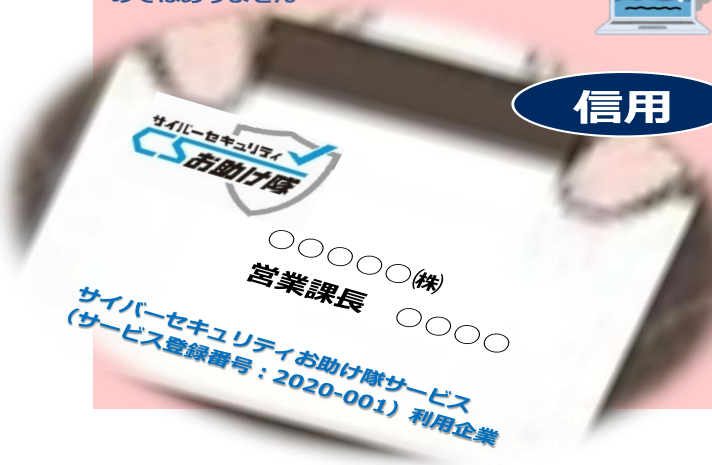
対策 レンタルUTMの「お守り」＋常時「見守り」＋困った時「相談」
攻撃時「お知らせ」＋事故時「駆け付け（保険）」＝「信用」

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

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

商工会議所サイバーセキュリティお助け隊サービス（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（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。

- ✓ 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/