先ず損保代理店様自身を守り、次にお客様を護る！サイバー攻撃対策＆お客様へのサイバー保険提案力強化セミナー

大阪商工会議所　経営情報センター　課長　野田幹稀

最近のサイバー攻撃の概要

サイバー攻撃の「攻撃する側」

現状

攻撃者の変容

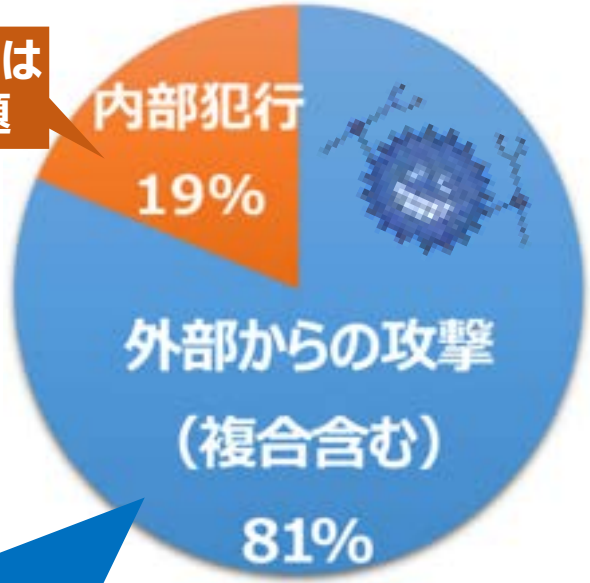
個人・愉快犯

気付かせることで
自己顕示欲を満たす

組織・経済犯

※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

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」

攻撃対象の増加

- 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**

対策

※上図：経済産業省サイバーセキュリティ課
2022年11月

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

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	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%）

業種的な差異はあるか？

	UTM検知通信	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%
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！

様々な攻撃の手口と基礎的対策

サイバー攻撃の攻撃手法

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

概要

ランサムウエア（PC・サーバ・バックアップ等の不正暗号化）

※上図：大阪府警HP　ランサムウェア「Wannacry」

◎以前：①暗号化（身代金要求）　支払うと？

◎少し前：①暗号化（身代金要求）＋②窃取＆暴露・売り飛ばし（身代金要求）
（支払わないと／二重脅迫）

◎最近：ノーウエアランサム　②窃取＆暴露・売り飛ばし（身代金要求）

∵ 犯罪者：(a) バックアップ普及で身代金支払減少　(b) 攻撃作業の工数削減

◎最新：ノーウエアランサム　②窃取＆暴露・売り飛ばし　身代金の要求すら“してくれない”

∴ 被害者：(a) 事象検知の困難化　(b) 情報流出で他者にも被害が

サイバー攻撃の攻撃手法

対策

ランサムウエア（組織1位）

【事前対策】

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」

- 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自体のバックアップも要），クラウド，リストア訓練

※上図　IPAの事故対応手引き

【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「No More Ransom」公式ウエブサイト

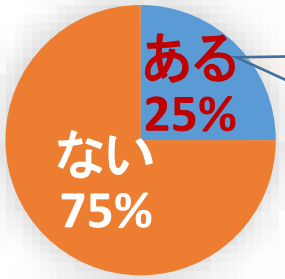
サイバー攻撃の攻撃手法

サプライチェーン攻撃（2位）

概要

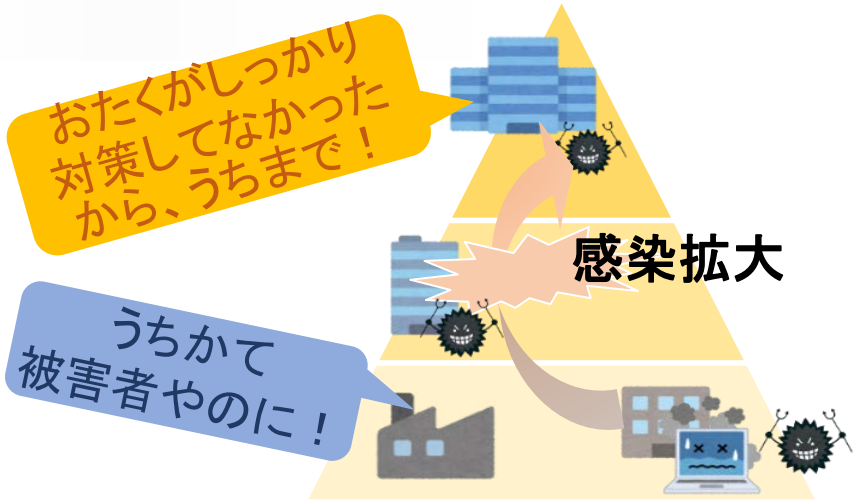
大企業・中堅企業(全国118社)

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

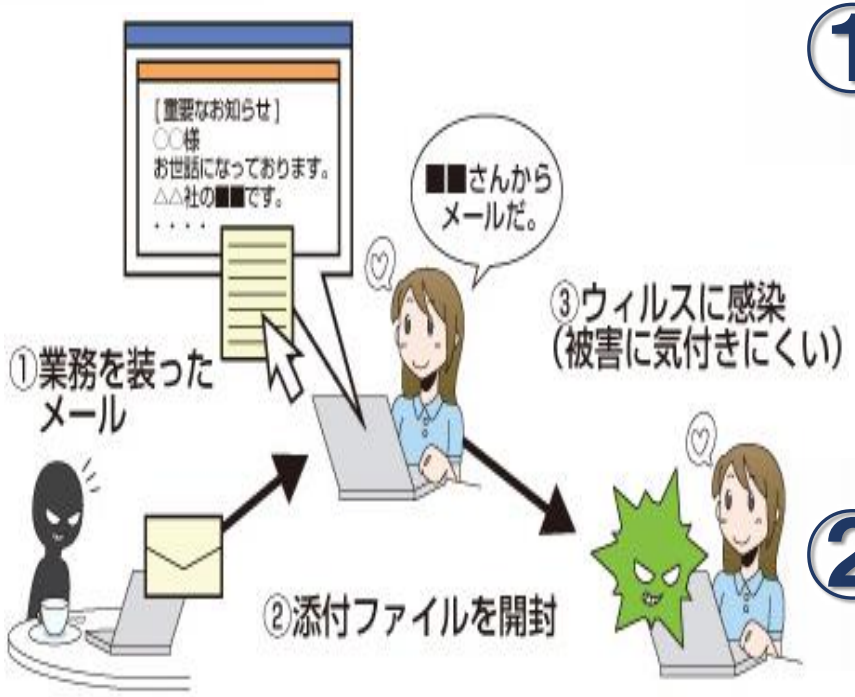
②親事業者の協力としてセキュリティ対策の助言・支援を行う

・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

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

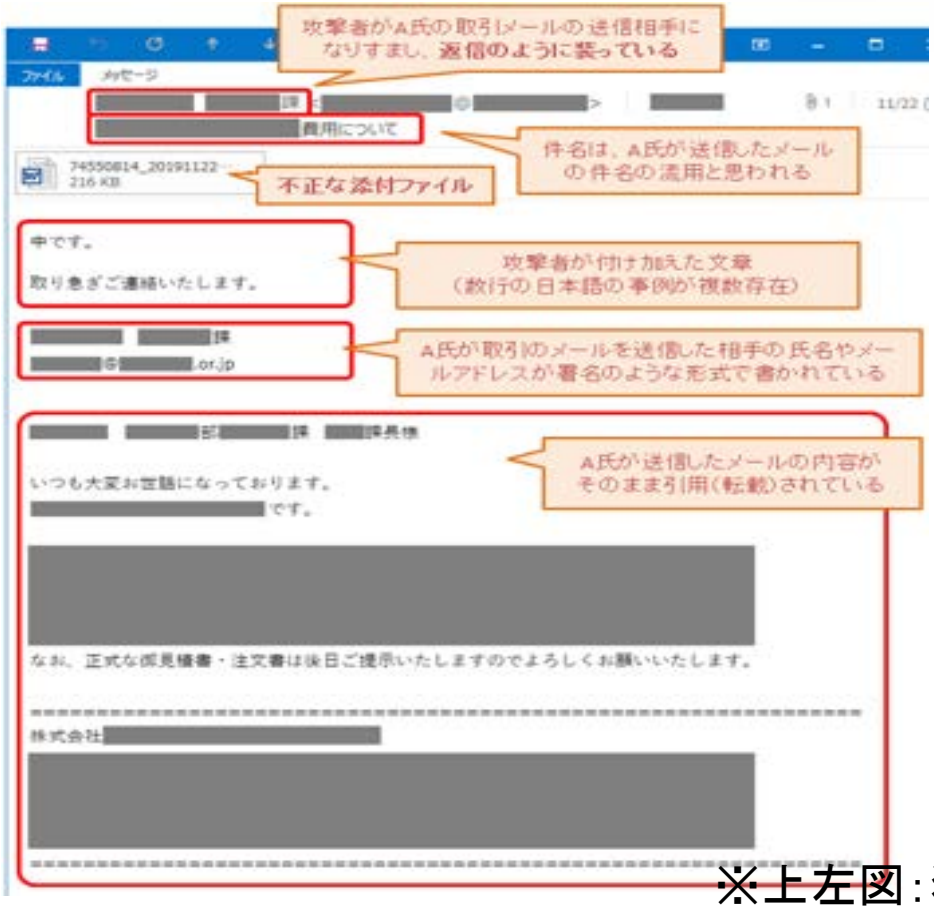
- **金銭**の窃取
- 「さっき送った振込先、間違ってました。変更願います」

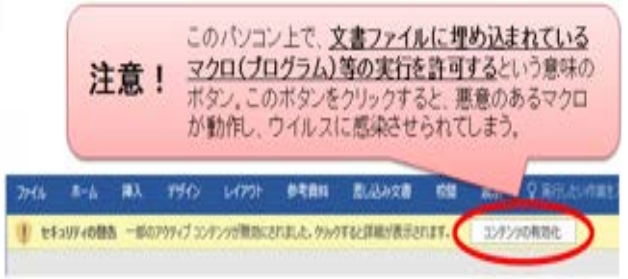
サイバー攻撃の攻撃手法

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

標的型攻撃メール・ビジネスメール詐欺・フィッシング

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

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！

you tú 你

⑥直接的原因を作った人を責めない！

サイバー攻撃の攻撃手法

テレワーク等の働き方を狙った攻撃（組織5位）

概要

BYOD（個人所有のPCを利用）の場合テレワーク端末は、攻撃者から見て「間口が広く垣根の低い入口」

VPNの場合、暗号化通信の上陸地点は、攻撃者の入口となる。

対策

テレワPCは可能な限り**仕事専用**にし、家族に使わせない。
OS・**ウイルス対策ソフト**（OFFにしない）は最新化しておく。
不明なアプリ、ソフトはインストールしない、使用しない。
ネット検索はほどほどにする。怪しい広告はクリックしない

職場側に設置するVPN装置の**脆弱性をなくし、パスワードを複雑なものに**しておく。職員側のパスワードも複雑なものに。

不注意による情報漏えい等の被害（組織9位）

概要

BCCで送るべきところTO, CCで送信してしまう

- メール**転送**時、下方に個人情報が残っていたり、添付ファイルが残ったまま送信。
- **同一内容の文章**を別人に送信する時、宛先のメルアドは変更したがメール本文の宛名を元の人のまま送信

対策

複数のドメインに**TO, CCでは送信できぬようにしておく。**
エクセル等のメルアドリストやPCのディスプレイの余白付近に巨大な字で「BCCで送信」など注意書きしておく。

- 組織内や外部の懇意な関係者（A氏）のみで（TO, CCで）送信し合っていたメールを、**あるタイミングで外部の部外者（B氏）に転送することになった場合は要注意。**
- 同じ内容のメールを不特定多数に送信する場合は、**一斉送信サービス**などを使用する。

サイバー攻撃の攻撃手法

ウイルス感染詐欺・パソコンサポート詐欺

実例

※独立行政法人情報処理推進機構（IPA)公式Webサイトより

※大阪府警察本部　公式Webサイトより

対策

👉通常のセキュリティソフトや OSでは、不審サイトや不正アプリを検出した事実の**通知を表示するだけ！**
電話問い合せ、アプリのダウンロードを促すことはない！

警告画面を閉じる方法

①左上のESCキーを３秒程押す　②右上に表示された×を押す

※独立行政法人情報処理推進機構（IPA)公式Webサイトより

IPA「情報セキュリティ安心相談窓口」

03-5978-7509

anshin@ipa.go.jp

10:00～12:00･13:30～17:00（土曜日曜祝日･年末年始除く）

実在する中小企業での
サイバー攻撃・被害の実例

実在中小企業での攻撃・被害実例

実例		対策
A社（大阪府） 金属製品製造業 従業員10～20人	●ラトビア共和国内から管理者パスワードでログインされPCが遠隔操作されていた。 ●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い	●リモートデスクトップ機能の無効化／3389番ポート閉鎖 ●接続端末の限定化(利用IPアドレスを限定)
B社（大阪府） 土木工事業 従業員70～80人	●PCがコンピュータウイルスを配布するとしてブラックリストに掲載されている悪性サイトと通信していた	●ネット広告のクリック、不明ツールのインストールを避ける ●不審メールの添付ファイルやURLを開かない
C社（大阪府） 医療用器具製造業 従業員80～90人	●バックドアを作るために利用されるコンピュータウイルスGh0stRATによる悪性サーバからの指令の通信検知	●UTMによる出入口防御 ●EDRによる端末での早期検知・隔離

※大阪商工会議所・神戸大学他「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）

実在中小企業での攻撃・被害実例

実例		対策
D社（大阪府） 機械製造業 従業員100～150人 ※大阪商工会議所での相談事例（2020年7月）	●ファイアウォールの脆弱性からランサムウエアに感染し不正暗号化。 ●復旧2000万円を要した ※大手ITベンダに丸投げだった	●事前対策：バックアップ(オフライン)・リストア訓練 ●渦中対策：即LAN線を抜く ●事後対策：「NoMoreLansom」で復号を試みる
E社（大阪府） 化学品卸売業 従業員70～80人 ※大阪商工会議所への会員企業からの情報提供（2020年）	●社員のメルアドでスパムメールが大量にばらまかれ、取引先のメールサーバにて同社ドメインが迷惑メール登録されてしまいメール受信拒否が発生	●怪しい添付ファイルは開かない。マクロは有効にしない ●定期的なメール訓練の実施
F社（大阪府） 印刷物卸小売業 従業員10～20人 ※大阪商工会議所での相談事例（2023年12月）	●WordPressで作成されたHPが乗っ取られ、他社の通販サイト（これも乗っ取られている）に改竄された ※大阪府警からの連絡で発覚	●対症対策：現サーバを捨て新サーバーをたてる（契約する） ●根治対策：ユーザリストやログインページを非公開設定にする。

実在中小企業での攻撃・被害実例

	実例	対策
G社（愛知県） 自動車部品製造業 従業員約1700人 ※新聞報道から（2022年3月1日）	●トヨタのサプライチェーンTier1の子会社のVPN機器の脆弱性から侵入 → 子会社から同社に侵入 → サーバ・PCがランサムウエア感染 → サーバ・部品供給管理システム停止 → ネットワーク遮断 → 部品納入停止 → トヨタ全工場（14工場28生産ライン）が停止 → サプライチェーン全体が被害 ●翌日から再稼働。トヨタのレジリエンスは凄い！	●VPN機器の脆弱性情報を常に情報収集 （IPA） https://www.ipa.go.jp/security/security-alert/
名古屋港湾協会 （愛知県） 	●システム業者の遠隔保守用VPN機器から侵入 → ランサムウエアがサーバのデータを暗号化 → 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衣類の入荷遅延等 → 紙によるマニュアル作業で荷役継続 → 約60時間で完全再開 ※2023年7月4日発生　国土交通省の「中間取りまとめ」要約	●VPN機器に接続できるPC（IPアドレス）を限定しておく ●VPN機器への接続時のID・パスワードを強固化

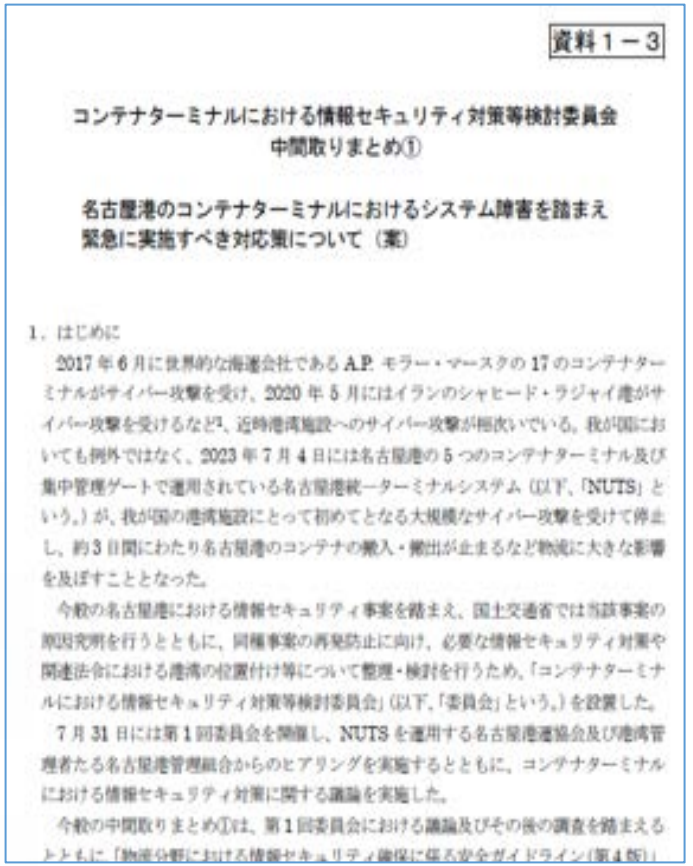
中小企業が持つべき視点と実践すべきこと

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

ＢＣＰの視点！

- 徳島県の町立半田病院のランサムウエア被害（2021年10月31日）で当時、病院事業管理者として現場対応した須藤氏（現院長）
  - 👉「これは災害だ」（朝日新聞の取材に対し）
- 「名古屋港統一ターミナルステム」のランサムウエア被害（2023年7月4日）による停止をふまえた国土交通省「緊急に実施すべき対応策」（同年9月）
  - 👉「（自然）災害用の事業継続計画（BCP）は事前に整備されていたものの、システム障害発生時のBCPが事前に整備されていなかった。**サイバー攻撃も対象としたシステム障害発生時のBCP を整備すべきである**」



資料１－３

コンテナターミナルにおける情報セキュリティ対策等検討委員会
中間取りまとめ①

名古屋港のコンテナターミナルにおけるシステム障害を踏まえ
緊急に実施すべき対応策について（案）

1．はじめに

2017 年 6 月に世界的な海運会社である A.P. モラー・マースクの 17 のコンテナターミナルがサイバー攻撃を受け、2020 年 5 月にはイランのシャヒード・ラジャイ港がサイバー攻撃を受けるなど[1]、近時港湾施設へのサイバー攻撃が相次いでいる。我が国においても例外ではなく、2023 年 7 月 4 日には名古屋港の 5 つのコンテナターミナル及び集中管理ゲートで運用されている名古屋港統一ターミナルシステム（以下、「NUTS」という。）が、我が国の港湾施設にとって初めてとなる大規模なサイバー攻撃を受けて停止し、約 3 日間にわたり名古屋港のコンテナの搬入・搬出が止まるなど物流に大きな影響を及ぼすこととなった。

今般の名古屋港における情報セキュリティ事案を踏まえ、国土交通省では当該事案の原因究明を行うとともに、同種事案の再発防止に向け、必要な情報セキュリティ対策や関連法令における港湾の位置付け等について整理・検討を行うため、「コンテナターミナルにおける情報セキュリティ対策等検討委員会」（以下、「委員会」という。）を設置した。

7 月 31 日には第 1 回委員会を開催し、NUTS を運用する名古屋港運協会及び港湾管理者たる名古屋港管理組合からのヒアリングを実施するとともに、コンテナターミナルにおける情報セキュリティ対策に関する議論を実施した。

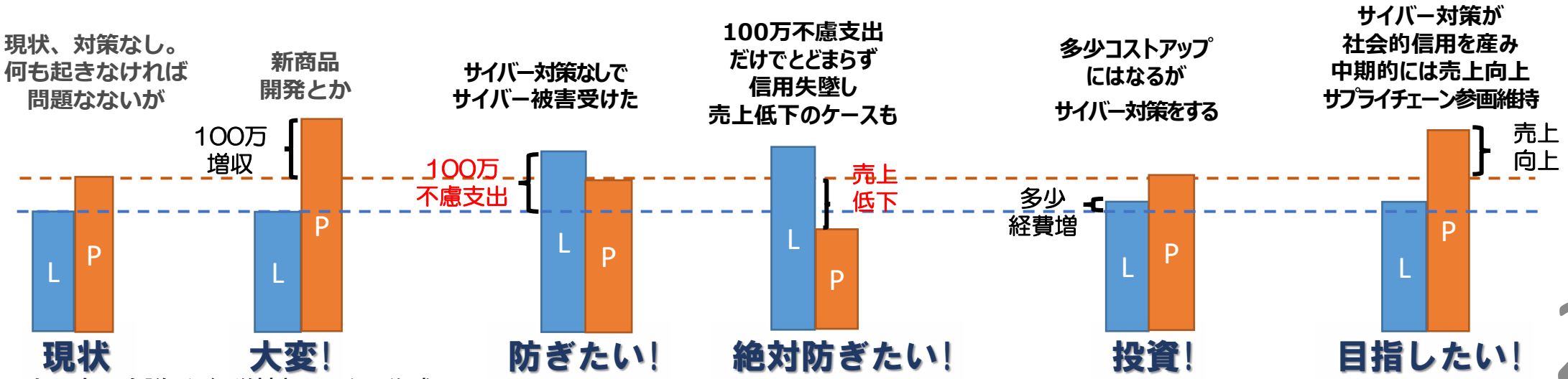
今般の中間取りまとめ①は、第 1 回委員会における議論及びその後の調査を踏まえるとともに、「物流分野における情報セキュリティ確保に係る安全ガイドライン（第４版）」

※上図:2023年9月
国土交通省の「コンテナターミナルにおける情報セキュリティ対策等検討委員会間取りまとめ①」

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



※上図:大阪商工会議所　経営情報センター作成

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

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

「投資」の「相場」は？

- セキュリティベンダ
  - 👉売上の１％
- (一社)日本サイバーセキュリティ・イノベーション委員会
  - 👉**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

- Ｇｏｒｄｏｎ－Ｌｏｅｂモデル（米国メリーランド大学）
  - 👉想定被害額の36％相当額

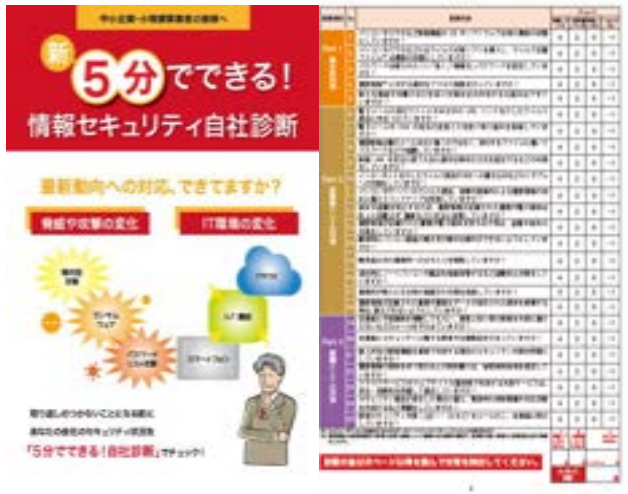
何から始めたらいいのか？

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

①「長く」「複雑に」「使い回さない」

1. 目安として**10文字(桁)**以上
2. **大文字(26)、小文字(26)、数字(10)、記号(31)の4文字種**
3. 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
4. **使い回さない（下記②参照）**
5. 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**

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）

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「コア・パスワード」を先ず作り「利用サービスごとの固有文字列」を合体

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）　26の13乗通り（解読に287日）
3．数文字を大文字に　**kyojinWAkirai**　52の13乗通り（解読に6,445年）
4．記号と数字を追加　**kyojinWAkirai!4**（コアパスワード）　93の15乗通り（解読に1,067億年）
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）

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地商工会議所で開催する

中小企業の経営者・社員・支援機関職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！

各地商工会議所・商工会が、会員・役員(常議員会)・女性会・青年部・事務局職員向けにサイバーセキュリティセミナーを実施する場合、大阪商工会議所が無償で講師派遣！

1. 概要

・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「わが社は狙われない」と考えがちで対策が遅れています。
・大阪商工会議所が、各地商工会議所・商工会様に、無償で講師を派遣させて頂き、中立的・普遍的立場から、専門用語を排した平易な内容で、中小企業の生々しい具体事例を盛り込んだ内容にて、分かり易く解説します。

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：貴商工会・商工会議所（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管理職）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、ハイブリッド開催。これだけのために単独でセミナーを開催頂くのはご負担ですので、既存会合（総会、役員会、部会、女性会役員会、経営指導員研修等）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（20分、30分、45分、60分、90分など。リアル出講60分又は90分がオススメです）

4. 開催経費

・講師料：無償（講師リアル登壇の場合のみ交通費だけ負担下さい。格安航空券の場合、遠地でも往復1～3万円）
・その他　：会場代・備品代・案内経費・資料印刷代・その他経費は、貴団体のご負担でお願い申し上げます。

5. その他

・開催実績は裏面をご覧下さい。受講者満足度は多くの場合95%以上です。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）
〒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

御社名、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	
メルアド		セミナー時間・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にのみ使用します。これにより同意頂いたものとして取り扱わせて頂きます。

大阪商工会議所 2023/6/8		
満足	15	52%
おおむね満足	14	48%
やや不満	0	0%
不満	0	0%

大阪管工機材商業協同組合 2024/5/28		
大変参考になった	36	61%
まあまあ参考になった	23	39%
どちらとも言えない	0	0%
参考にならなかった	0	0%

松浦商工会議所 2024/6/6		
とても満足	11	58%
満足	8	42%
どちらでもない	0	0%
やや不満・不満	0	0%

- 危機感を高めるきっかけになった
- 年々サイバー攻撃も増えており情報のアップデートが必要と感じた

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）

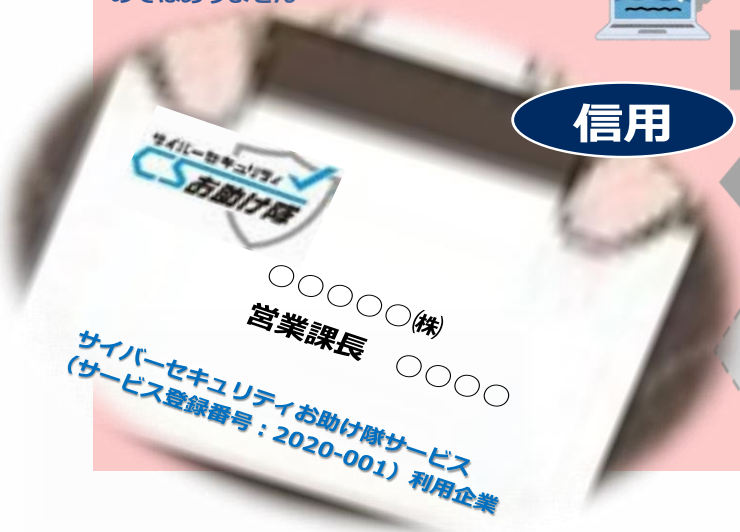
対策　国に登録されているUTM（多機能防御装置）レンタルサービス

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

これだけ揃って　月額
商工会議所　会員6600円
非会員8250円

損害保険会社代理店様へのご提案
（大阪商工会議所との顧客紹介契約）

顧客紹介（広報協力）契約（任意）

大阪商工会議所

①顧客紹介（広報協力）契約

（③紹介）

損保代理店
地方銀行
信用金庫
地域のITベンダー

詳しいことは
大阪商工会議所
に聞いて下さい

②案内

③説明希望連絡票送信

④詳細説明（訪問・オンライン）

⑤「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

⑥顧客紹介手数料支払い

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！**

“本格的な”賠償型の保険（2階建て部分）は別途必要

- ☞損害賠償請求・訴訟費用への対応
- ☞フォレンジック調査・再発防止費用への対応
- ☞利益損害・営業継続費用の補償

「商工会議所サイバーセキュリティお助け隊サービス」に付帯しているのは、あくまで費用保険で駆け付けサービスという現物給付（1階建て部分）

大阪商工会議所は「サイバー攻撃の調査・分析」や「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貢献」したことをご評価頂き、2020年 **「サイバーセキュリティに関する総務大臣奨励賞」を受賞**しました。
今後も中小企業のサイバー攻撃対策を支援します！**サイバーセキュリティセミナーに無償で講師派遣します！**

大阪商工会議所　経営情報センター（野田・登坂）
〒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/