

主催：総務省沖縄総合通信事務所 様
サイバーセキュリティセミナー沖縄 in ResorTech EXPO 2026

中小企業における サイバー攻撃・被害の実態 と現実的な対策

令和8年（2026年） 秋

大阪商工会議所 経営情報センター 次長 兼 経営情報担当課長 野田幹稀
(IPA登録セキュリティプレゼンター)

サイバー攻撃の「攻撃する側」(攻撃者の変容)

概要

※「Verizon 2026 Data Breach Investigations Report (ベライゾン データ漏洩/侵害調査報告書) エグゼクティブサマリー」(2026年5月19日)

	金銭目的	スパイ活動	外部からの攻撃	内部の犯行・ミス
製造業	87%	15%	95%	5%
建設業	97%	5%	99%	1%
不動産・リース業	100%	—	79%	22%
金融・保険業	98%	3%	88%	12%
情報産業	84%	16%	89%	11%
教育サービス	78%	21%	78%	22%
その他サービス	78%	23%	81%	19%

個人による愉快犯から
国家を含む組織・経済犯に

ビジネス!

国家による関与を含む!
ベライゾン
(Verizon社によると40%が「国家支援型」攻撃者)
国家サイバー統括室「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

中国は、政府機関や重要インフラ事業者、先端技術保有者によるサイバー攻撃を行っていると考えられ、最近では、同国が支援する

ロシアはサイバー攻撃を軍事的・政治的目的達年のウクライナ侵略前に、同国の政府機関や重

IT・技術の問題
というより
人(人事・労務)の問題

※独立行政法人情報処理推進機構(IPA)
「組織における内部不正防止ガイドライン」



人が
AIの助力を得て
サイバー攻撃

2026年1月頃

この時代は短すぎたので特筆事案が僅少



AIが
人の助力を得ず
(自律的に)
サイバー攻撃

2026年4月頃

全員 注意!

経営層 注意!

2026年4月7日
米国Anthropic(アンソロピック)社
「Claude Mythos」
(クロード・ミュトス)

- 脆弱性の発見能力が著しく高い
- 攻撃コードを自動生成し、人手を介さず自律的に攻撃
- 「デジタル核」と形容する専門家も
- 詳細はP14参照

価値観を共有
しない国・企業が
同等のAIを開発
(6~12か月の差と言われる)

- 散発的・局所的だった攻撃・被害が同時多発的・面的なものに
- 情報漏洩・システム破壊の件数や経済的損害が甚大化
- 国家やインフラ機能(物理面も)が麻痺(戦争レベル)

メモ欄

サイバー攻撃の「攻撃される側」(攻撃対象の変容)

概要



パソコン
ルータ
サーバ

+ a

「Society 5.0」

①狩猟→②農耕→③工業→④情報→⑤今

「5G (ファイブジー)」

第5世代移動通信システム。ジエネーションのG。ギガではない

「Connected Industries」

データを介し機械・技術・人など様々がつながること

「サイバーフィジカルシステム」

サイバー空間と物理空間を融合させて上手く運用するやり方

「DX」

デジタル技術で人々の生活をより良いものに変革すること

「IoT」

モノがネット経由で通信すること。またそのモノ自体



Bring Your Own Device
= 社員の個人所有端末を使わせる

- ・パソコン (BYOD含む)
ルータ、サーバ自体
の**絶対数増**
- ・無線LANによるスマホ、
タブレット等の**接続増**
- ・各種機器の**IoT化**
- ・スマート工場、
コネクティッドカー等の**出現**

A
I

全員 注意!

情シス 注意!

- ・職場で許可なくA Iを
業務利用 (情報漏えい)
- ・実在しない情報を
対話型A Iが生成
(ハルシネーション)
- ・A Iがソフトウェアやシス
テム等の脆弱性を探索し、
攻撃してくるのに対し、
ユーザ(端末)側もA Iで対抗
し防御(プログラム修正・
パッチを適用)すべきだが、
それが追い付かない場合も
(ゼロデイ攻撃)

事例 対策していないIoTをネット接続 → 最短38秒で感染

※横浜国立大学2016年調査

対策

経済産業省・IPA「セキュリティ要
件適合評価及びラベリング制度」
(IoT製品のセキュリティ機能を
★1～★4で評価・可視化する
国の制度) 2025年3月～



↓ 先進事例 2025年5月
(株)バッファロー公式Webサイトより)



経済産業省「工場システムに
おけるサイバー・フィジカル・
セキュリティ対策ガイドライン」



メモ欄

どんな中小企業に攻撃が？

実例

地域的な有意差はない！

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ヵ月	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
Intrusion Prevention System (不正侵入防止)	22社 7,906件	48社 18,325件
ウイルス遮断	12社 524件	34社 775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
危険サイトアクセス遮断	0社 0件	1社 1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%)

全員 注意！

業種的な有意差はない！

	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%
外→内の攻撃	26	22	8	5	2	1
内→外の不正通信 (両方検知した社数)	15 (11)	9 (7)	2 (1)	4 (2)	1 (0)	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）

※大阪商工会議所が独立行政法人情報処理推進機構(IPA)から請け負い、NEC他と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

サイバー攻撃の手口・事例・対策（概略）

概要

全員 注意!

独立行政法人情報処理推進機構（^{アイピーエー}IPA）「情報セキュリティ10大脅威2026」（2026年1月29日）

	「組織」向け脅威	「個人」向け脅威
1	ランサム攻撃による被害	インターネット上のサービスからの個人情報の窃取
2	サプライチェーンや委託先を狙った攻撃	インターネット上のサービスへの不正ログイン
3	AIの利用をめぐるサイバーリスク 【2026年初選出】	インターネットバンキングの不正利用
4	システムの脆弱性を悪用した攻撃	クレジットカード情報の不正利用
5	機密情報を狙った標的型攻撃	サポート詐欺（偽警告）による金銭被害
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	スマホ決済の不正利用
7	内部不正による情報漏えい等	ネット上の誹謗・中傷・デマ
8	リモートワーク等の環境や仕組みを狙った攻撃	フィッシングによる個人情報等の詐取
9	^{ディードス} DDoS攻撃（分散型サービス妨害攻撃）	不正アプリによるスマートフォン利用者への被害
10	ビジネスメール詐欺	メールやSNS等を使った脅迫・詐欺の手口による金銭要求

攻撃の 多様化&巧妙化、高度化&容易化、高速化&同時多発化

ランサムウェア

実例



※上図：ワナクライ=want to cry=泣きたいか？の意
大阪府警HP ランサムウェア「Wannacry」

概要

◎以前：①暗号化(復号してほしかったら身代金を払え)
encrypt decrypt=元に戻す ransom (ランサム)

◎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 支払うと？
二重脅迫 (82.6%)

※警察庁「令和6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」

◎最近：①ノーウェアランサム 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：①ノーウェアランサム ②窃取&暴露・売り飛ばし
↓ 身代金の要求すらしてこない
∴ 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

最近は ソース SaaS や パース PaaS 等の言葉をモジった ラース RaaS という“悪のエコシステム(ランサムウェア犯罪分業)”も存在
Software as a Service Platform as a Service Ransomware as a Service

※大阪商工会議所 経営情報センター 作文

メモ欄

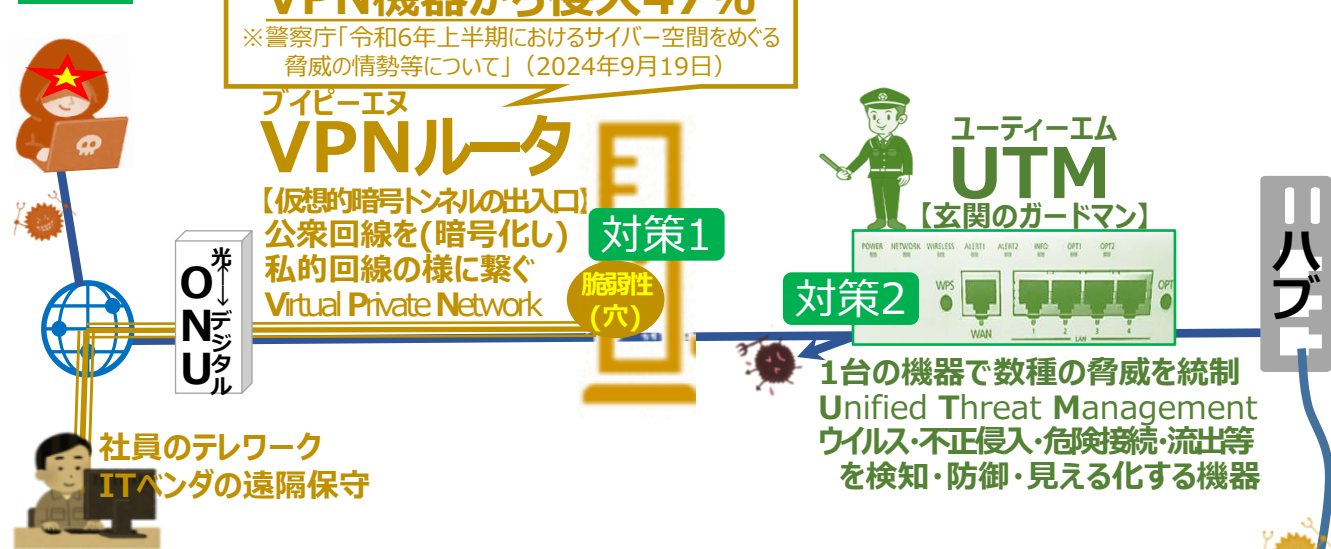
ランサムウェア

※大阪商工会議所 経営情報センター 作文・作図

全員 注意！

情シス 注意！

対策



やるべきこと → **へんな画面が出てきたら、即、LAN線を抜く**
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(約50GB)暗号化に中央値42分(最速約6分)
※Deep Instinct社およびSplunk Blogs(March23,2022)より抜粋

やめてはいけないこと → **身代金は支払わず 復号を試みる**
①「No More Ransom」で無料復号化ツールを入手し復号する
② 警察庁は「Lockbit3.0」「Phobos」「8Base」暗号の復元が可能
復号はできても『改ざんされていない』という証明は得られない！

やめてはいけないこと → **電源を切る/切らない！**
本格的(フォレンジック)調査 しない予定(そんな予算・内規・外圧がない)なら電源を切る！
する予定なら、切らないで現場保全・ログ(通信記録)を温存

今後の対策 **ゼロトラスト前提でクラウドで守るSASE (SWGなど) 等**
サッシー：ネットワークとセキュリティをクラウドで統合

- 対策0 **適切なバックアップ運用！**
※大阪府警察本部の公式Webサイトから引用・大阪商工会議所にて一部編集
- ① 業務データのみならず、システムの稼働に必要な設定ファイルやプログラムも含めてバックアップ対象を選定
 - ② バックアップ用の外部記憶装置はバックアップ時以外は物理的に接続しないようにする(逐一線を抜く＝オフラインバックアップ)
 - ③ 潜伏期間を持つランサムウェアもあることから、最新だけでなく過去の複数の地点に復旧できるようにする
 - ④ 対象データごとに適切な取得日時、間隔を検討する

今後の対策		※経済産業省の公式ウェブサイト(2026年3月27日)から抜粋
SCS 評価 制度 ★3	4-3-4-1	取得対象、取得頻度及び保管期間を定めて自社で取り扱うデータのバックアップを取得すること
	4-3-4-2	重要な機密情報については、4-3-4-1におけるバックアップに加えて、遠隔地バックアップを実施すること
	4-3-4-3	バックアップ対象ごとにリストア(バックアップがちゃんと戻るか確認)手順書を整備すること
	4-3-4-3	

実例 岐阜県の自動車部品製造業 従業員約900人

※同社Webサイトを抜粋・大阪商工会議所にて要約・一部編集・補足（2025年10月）

10/1(水)19:31 ID・パスワードが不正利用され(VPNの脆弱性ではなく)社員用VPNアカウント経由で社内ネットワーク侵入
(10/4のVPN切断までの間、組織内探索、クライアント端末の制御権窃取、データ窃取)

10/3(金)20:58 システム破壊、ファイル暗号化、サーバ初期化

10/4(土)01:21 ランサムウェアの脅迫文が社内フォルダに置かれる

10/4(土)02:25 サイバー攻撃を確認

10/4(土)04:45 VPN切断

10/4(土) 顧客、関係各所、警察へ連絡

10/4(土) 受注・生産・出荷のシステム確認。復旧開始

10/4(土) 資金決済のシステム確認。復旧開始

10/7(火) 外部への接続制限を開始

10/8(水) 個人情報流出の可能性を個人情報保護委員会へ報告

10/10(金) 詳細解析(フォレンジック調査)開始(300GB程度の、顧客情報・個人情報の流出を含む不正通信を確認)

10/28(火) ダークサイト(通常のブラウザでは閲覧不能なネット上の闇サイト)で情報漏洩の事実を確認(翌日閉鎖)

12/12 同社副社長が地元商工会議所で会員企業向けに自社の被害状況や教訓について講演

12/25 安全宣言(ウィルス根絶、侵入経路・攻撃手法特定、新たな侵入の可能性排除等の確認をふまえ)

2026/2/19 Webサイトに(本件に関する最終的な)「個人情報漏えいの可能性に関するご報告」を掲載

ドメインコントローラー(ActiveDirectory)、仮想化基盤を含む業務系サーバー、PC等の暗号化、ファイルサーバーからのデータの搾取

多要素認証、パスワードロック、NW分割があれば防げたかも

検知まで48時間以上

一時的な利用を目的に2025年4月に作成された正規VPNアカウントが悪用された。一時利用ゆえ非常に容易なID・パスワードだった(例…ID:temp PASS:password1msys1)。利用終了後も抹消せず残存。2025年5月時点で最初の不正アクセス・ログイン(この時点では攻撃無し。その後の侵入者と同一か否か不明)

これは尊敬されるべきこと！他社に同様の被害に遭ってほしくない！との強い思いと使命感がないと、できないこと

対策 事案後の対策：①EDR導入、②振る舞い検知の導入、③より高度なアンチウイルスソフトによる全サーバ・端末のスキャン、④全IDのパスワード変更、⑤VPNを含む入口の全封鎖(事案後当面)、⑥外部とのアクセス制限(システムと切り離したクリーン端末にて接続)、⑦外部機関による詳細解析、⑧24時間監視体制 など

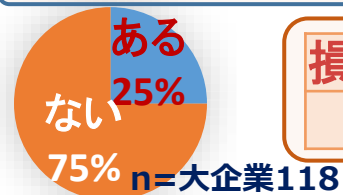
サプライチェーンや委託先を狙った攻撃

概要

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）

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？

今後同じようなことが起きたらどう対処する？



損害賠償請求	55社(47%)
取引停止	34社(29%)

被害者なのに加害者(踏み台)になってしまう！

大阪商工会議所・経済産業省共同調査「サイバーセキュリティ費用の価格転嫁に関するアンケート」（2025年7月／全国の中小企業129社）

セキュリティ対策費用を価格転嫁できたか？



セキュリティ対策の費用は価格転嫁できない？！

メモ欄

経営層 注意！

実例 アスクル(2025年6月)

業務委託先に付与の管理者アカウントの認証情報(多要素認証なし)を悪用

おたくが、しっかり対策してなかったから、うちまで！

そやかて、うちかて被害者やのに！

感染拡大

実例 名古屋港運協会(愛知県)※2023年7月4日発生 国土交通省「中間とりまとめ要約」

システム業者の遠隔保守用VPN機器から侵入 → ランサムウェアがサーバのデータを暗号化 (ア)船舶37隻が約24時間遅延 (イ)コンテナ約2万本の搬入出遅延 (ウ)トヨタの愛知・岐阜4拠点が稼働停止 (エ)アパレルメーカーで衣類の入荷遅延 → 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

対策

- ①受託中小企業基本法「振興基準」(2026.1.1改正)
 - ・中小受託事業者の努力 必要なセキュリティ対策を行う
 - ・委託事業者の協力 セキュリティ対策の助言・支援を行う
 - ②各業界ごとに「サイバーセキュリティガイドライン」策定
 - ③サイバー攻撃対策に要した経費の価格転嫁を円満に行えるような(受託者と委託元との)相互理解が必要
- (一社)日本自動車工業会・(一社)日本自動車部品工業会・(一社)日本建設業連合会などのガイドライン↑



サプライチェーンや委託先を狙った攻撃

今後の対策 経済産業省・IPA「サプライチェーン強化に向けたセキュリティ対策評価制度」

情シス 注意!

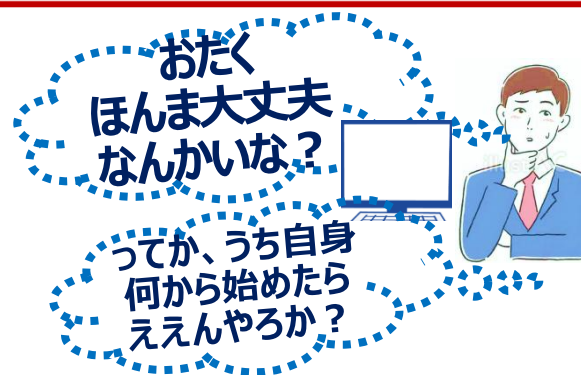
経営層 注意!

2027年3月～開始

※大阪商工会議所にて作成

(1)可視化・客観化が必要!

サイバー攻撃は目に見えない。サイバー攻撃対策も目に見えない

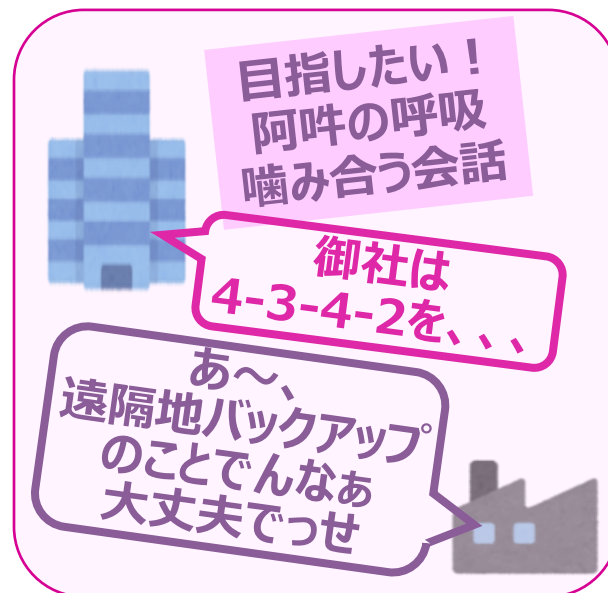
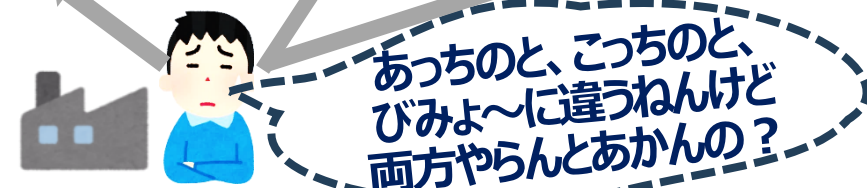


ってか、うち自身
何から始めたら
ええんやろか?

(2)標準化・共通言語化が必要!

元請会社における 情報セキュリティガイドライン	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	X協会 ガイドライン
2.2版 2010年06月 初版 2024年02月 修正	2024年8月1日	
(法人)日本建設業連合会 産業委員会 ICT推進部会 情報セキュリティ専門部会	jama JAPIA	

業種横断的なものが必要!



御社は
4-3-4-2を、...

あ〜、
遠隔地バックアップ
のことでんなあ
大丈夫でっせ

(3)難しすぎず、易しすぎず

ISO27001(ISMS)

情報資産保護がメイン・マネジメントのシステム
PDCAを回す・内部監査員・お金が結構かかる

この中間くらいが必要!
もう少し技術寄りの対策も必要!



セキュリティ対策自己宣言

情報セキュリティ方針策定&公開



セキュリティ対策自己宣言

自己宣言だけやったら
事故るでえ〜

自己宣言・登録

情報セキュリティ6か条

- ① OS・ソフトを最新状態に
- ② ウィルス対策ソフトを導入
- ③ パスワードを強化
- ④ 共有設定を見直す
- ⑤ 脅威・攻撃の手口を知る
- ⑥ バックアップを取ろう

サプライチェーンや委託先を狙った攻撃

今後の対策		経済産業省・IPA「サプライチェーン強化に向けたセキュリティ対策評価制度」		情シス 注意!	経営層 注意!
大分類		★3	2027年3月～開始	★4	
ガバナンスの整備	企業として最低限のリスク管理体制の構築	継続的改善に資するリスク管理体制の構築			メモ欄
	・ 自社のセキュリティ担当の明確化 [No.1-2-1] ・ セキュリティ対応方針の策定 [No.1-3-1]	・ 定期的な経営層への報告、不備の是正等 [No.1-4-1]			
取引先管理	取引先に課す最低限のルール明確化	取引先の管理・把握及び取引先との役割・責任の明確化			
	・ 他社との機密情報の取扱い明確化 [No.2-1-2] ・ 接続している外部情報サービスの把握 [No.3-1-3]	・ 機密情報共有先の把握 [No.2-1-1] ・ 重要な取引先等の対策状況把握 [No.2-1-3] ・ インシデント発生時の他社との役割等の明確化 [No.2-1-4]			
リスクの特定	自社IT基盤や資産の現状把握	脆弱性など最新状況の把握と反映			
	・ 情報資産やネットワークの把握 [No.3-1-1,3-1-2] ・ 外部情報サービスの管理 [No.3-1-3]	・ 脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]			
攻撃等の防御	不正アクセスに対する基礎的な防御	多層防御による侵入リスクの低減			
	・ ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] ・ パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] ・ 内外ネットワーク境界の分離・保護 [No.4-5-1]	・ 重要な保管データの暗号化 [No.4-3-1,4-3-2] ・ ログの収集・定期的な分析の実施 [No.4-4-3] ・ 社内システムにおける適切なネットワーク分離 [No.4-5-1] ・ 社外への不正通信の遮断(出口対策) [No.4-5-2]			
	端末やサーバーの基礎的な保護				
	・ 適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] ・ 端末等へのマルウェア対策 [No.4-4-1,4-4-4]				
攻撃等の検知	ネットワーク上の基礎的な監視等	迅速な異常の検知			
	・ ネットワーク接続・データの監視[No.5-1-1]	・ 情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]			
インシデントへの対応	インシデント発生に備えた対応手順の整備				
	・ インシデント対応手順の作成 [No.6-1-1]	*大分類「インシデントへの対応」において、★4での追加項目はなし			
インシデントからの復旧	インシデント発生から復旧するための対策の整備	インシデントからの復旧手順等の整備			
	・ インシデント発生から復旧するための対策の整備[No.7-1-1]	・ 復旧ポイント、復旧時間を満たす手順等の整備[No.7-1-1]			

AIの利用をめぐるサイバーリスク

※独立行政法人情報処理推進機構「情報セキュリティ10大脅威2026解説書
【組織編】四版」(2026年4月11日)をもとに、大阪商工会議所で一部編集

全員 注意!

情シス 注意!

経営層 注意!

概要		事例	やるべきこと → やってはいけないこと	対策
①職場で許可なくAIを業務利用し、情報漏えい		米AI企業の調査 (NEW Research: AI Is Already the #1 Data Exfiltration Channel in the Enterprise) によると、業務において、生成AIにデータをコピーしてプロンプト(指示文)として入力している利用者が77%。うち82%が組織に管理されていないアカウントによるもの		(イ)未許可のAIサービス利用(シャドーIT・シャドーAI)の禁止 (ロ)個人アカウント(ID・パスワード)による業務利用の制限 (ハ)AIのサービス利用規定の整備と従業員教育の徹底 (ニ)個人情報・会社の機密情報を安易にAIに入力させないこと (ホ)生成物(画像等)の外部公開時は著作権侵害に留意すること (ヘ)外部サービス利用時には入力データを「学習対象」から除外する オプトアウト(事後拒否)設定の徹底 (ト)通信ログ・CASB(キャスビー: Cloud Access Security Broker)等で、AIサービス利用状況を把握
②実在しない情報に対話型AIが生成(ハルシネーション)		2025年1月、米国で、弁護士が生成AIを用いて作成し、提出した意見書に実在しない判例が引用されていた		(チ)AI悪用による不正アクセスに備え、多要素認証の徹底 (リ)IT資産管理、OS・ソフトウェアのアップデート、脆弱性のパッチ適用 (ヌ)多層防御(端末と玄関の両方)とふるまい検知の導入 (ル)オフライン(線が繋がっていない状態)でのバックアップ
③AIに助力を得たサイバー脅威の増長		中国の国家支援型アクターが、偵察・脆弱性発見・認証情報窃取・データ分析など一連の攻撃プロセスの8~9割をAIが自律的に実行して高度な諜報活動を行った		
SCS 評価 制度 ★3	4-4-4-1	システム、情報機器及びソフトウェアは以下の状態とすること。 - ライセンスが付与され、サポートされている。 - サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。 - 可能であれば、自動アップデートが有効化されている		
	4-4-4-2 (抜粋)	利用している機能又は設定に関して、以下のいずれかに該当するアップデートプログラムがリリースされてから14日以内に、アップデートすること - 当該アップデートが、ベンダーにより「重大」(Critical)又は「高リスク」(High Risk)と説明される脆弱性を修正するものである - 当該アップデートが、CVSSの基本値が7.0以上の脆弱性を修正するものである		

2026年4月7日
米国のAnthropic(アンソロピック)社
「Claude Mythos(クロード・ミトス)」

- ①27年間、世界中の専門家や専門機関が気付かなかったシステムの脆弱性を僅か数時間で発見!
- ②16年間にわたる数百万回の自動テストでも検出できなかった深刻なバグ(不具合)を自律的に発見!
- ③あまりに危険なためアンソロピック社は一般公開を封印!

- 👉松尾豊 東大教授「核兵器並みのインパクトがある技術」
- 👉片山さつき財務大臣「今、そこにある危機」(2026.04.24)
- 👉木原稔官房長官「サイバー攻撃のスピードと規模が劇的に増加」
- 👉平将明前デジタル大臣「価値観を共有しない国の手に渡ったら、」
- 👉アンソロピック社タリオ・アモディCEO「中国が追いつくのは6~12か月」

標的型攻撃メール・ビジネスメール詐欺・フィッシング

全員 注意!

概要

● 標的型攻撃メール

機密情報・個人情報・認証情報の窃取

● ビジネスメール詐欺・フィッシング(Phishing)

ソックリな偽サイトに誘導し
金銭の窃取 (クレカ情報・認証情報含む)

※イラスト：総務省HPより



メモ欄

対策

※大阪商工会議所 経営情報センター 作文・作図

① メルアド・拡張子は最後の最後まで確認 (但しメルアドは容易に偽装可能)

(ファイルの種類の識別子：ワードは .doc エクセルは .xlsx など)

② メール件名が短文・抽象的な場合は開封/送信しない

③ “微妙に懐かしい人”からのメールは開封しない

④ 添付ファイルは開かない (特に .lnk .exe .scr .cpl)

⑤ マクロやコンテンツの有効化は押さない

(エクセル等の便利な処理自動化機能)

⑥ 二人称が「あなた」はアウト

⑦ ミスった社員を責めない

⑧ 受動的× 能動的○

- 御礼
- 議事録
- ご連絡

microsoft.com
rnmicrosoft.com

添付ファイル: form 04.25.2022.lnk 4.0 KB
form 04.25.2022.lnk 4.0 KB

文書.doc
exe

First, we are apologize for the delayed reply and bring you so much trouble.

Our bank has refuse to credit your remit to our account due to the account is not a USD account we are sorry for the trouble we have caused you.

A I 翻訳

まず、ご連絡が遅くなり、あなたに大変迷惑をおかけしたことをお詫ひします。

口座が米ドルではないため、当銀行はあなたの送金を入金することを拒否しました。ご迷惑をおかけして申し訳ございません。

(但し、今後、A I 翻訳の精度・自然さは、加速度的に改善される見込み)

今後の対策

DMARC (送信者のドメイン認証を行い、怪しい場合はゴミ箱に入れてくれる。送信者側が実施)

標的型攻撃メール・ビジネスメール詐欺・フィッシング

全員 注意!

概要 フィッシング(Phishing)
送信者を詐称したメールやSMSを送りつけ、
貼り付けたリンクをクリックさせて Short Message Service : 携帯同士で電話番号を宛先にしメッセージをやり取りするサービス
偽のホームページに誘導することで、
クレジットカード番号やID・パスワード
などの重要な情報を盗み出す詐欺 ※総務省のHPより（一部編集）

実例 こんなタイトルのメールは要注意

マスターカード・・・【マスターカード】重要なお知らせ
PayPay・・・・・・2025年5月04日請求金額のお知らせ
（請求がない方にもご案内しています）
マネックス証券・・・お客様の資産安全のため、
登録情報の定期更新をお願いします
Appleサポート・・・アカウント保護のためのご案内
今年もこの暑さに耐えるつもりですか？
【TSITE.jp会員限定】24,897円のお支払いで47,920pt進呈
【機密】2026年度下半期の人事評価および昇進対象者
リストの先行公開について

※大阪商工会議所(講師のメール)で受信した実例（主に2025年5月～2026年5月）

対策

やってはいけないこと

やるべきこと

受動的に開封しない

能動的に手入力

能動的に公式HPで確認

フィッシングサイトの見分け方

見分けようとしないうこと

受動的にクリック
能動的に手入力しググる

【マスターカード】重要なお知らせ

Google

【マスターカード】重要なお知らせ

すべて ニュース 画像 ショッピング 動画 もっと見る

約 6,720,000 件 (0.27 秒)

https://internet.watch.impress.co.jp/docs/news

件名「【Mastercard】重要なお知らせ」の不審なメール

2021/11/18 — 件名「【Mastercard】重要なお知らせ」の不審なメール、マスターカードをかたるフィッシングに注意。偽サイトに誘導してカード情報を詐取。山田 貞幸。

https://www.mastercard.co.jp/get-support/phishing

フィッシング詐欺にご注意ください | Mastercard®

不審な電話がございましたら一切お答えになりませんよう、十分お気をつけください。万が一被害に遭

世界で最も多くの
場所で使える
Mastercard®

メモ欄

標的型攻撃メール・ビジネスメール詐欺・フィッシング

全員 注意!

概要

2段階式フィッシング(メール)

1 通目の (いかにも不審そうな) メールを見破った (開封しなかった) 人に対して、

2 通目として、その人 (同じ受信者) の「課題意識の高さ」を逆手に取ったメールを送りつけるもの

※右図：警視庁サイバー攻撃対策センターの「X」から
(2026年6月11日)

実例

二段階式フィッシングメールの例

1 通目

From：本社会計係
件名：【重要】通勤手当申請
通勤手当未申請の方へ
[このリンクから申請](#)ください。



あれ？
このメールはおかしいな。
僕は騙されないぞ。

さっきの不審なメールに
気付いたからシステム
担当者に報告しなくちゃ。

2 通目

From：本社システム担当
件名：【注意】不審メールについて
全社員向け
社員に不審なメールが送信されています。
不審なメール受信状況を調査しますので、
[ここから回答](#)ください。



しまった！
2通目もフィッシング
メールだったのか・・・



対策

やるべきこと

メール送信者の表示は攻撃者側で表示を変えることができる！不審な場合は、メルアド自体を確認！
「URLのクリック」や「添付ファイルの開封」の前に、関係者にアナログ(電話等)確認！

やってはいけないこと

「返信」や「転送」は絶対に避ける！

メモ欄

内部不正による情報漏えい等（情報って、誰のもの？）

全員 注意！

情シス 注意！

経営層 注意！

概要

実例

対策

自分の足で集めた名刺		退職の記念に家に持って帰ろう！私のサラリーマン人生の集大成！ 独立した時の顧客候補として活用するの！私のコミュカの戦利品！	会社の情報資産！ 個人情報でもある！ 名刺交換相手の視点で考えて！
自分の汗で作った顧客名簿		前の部署で作った500社のリストを使おう！俺が作ったんやから俺のもんやん！ この名簿、将来「何か」に役立つやろうな。USBで保存しとこ！	会社の情報資産！ 共有設定を見直そう！ (Security Action★1)
自分の頭でまとめあげたプレゼン資料		この資料、私自身の知識と抽象化能力の結晶！MBAの修論に引用しよつと！ ノーベル賞級の発明(青色LED)ですら「発明者(社員)の貢献度」は 日亜化学50%：中村修二氏50%（東京地裁2004年一審判決） 日亜化学95%：中村修二氏5%（東京高裁2005年二審和解）	会社の情報資産！ 著作権法第15条「職務著作」 契約や規約で定めておくべき！
自分のスマホに保存してある仕事のデータ		そもそも、従業員の個人所有端末に、会社のデータを保存することは原則NG 個人所有端末に搭載のAIに会社のデータを食わせることは絶対NG 個人所有端末で撮影した会社の風景・書類・PC画面をSNSにUPすることは原則NG （憲法13条「自己決定権」も21条「表現の自由」も、盾には出来ない！）	BYODは注意！ 持込許可する場合はルール厳格化を！ 持込禁止の場合は論外！

SCS 評価 制度	★3	1-2-3-1	役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。
		1-2-3-2	入社時又は社外要員の受入れ時に守秘義務のルールを説明すること。
	★4	1-2-3-3	自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。(社外要員を除く。)
		1-2-3-4	派遣社員及び受入出向者について、派遣元及び出向元の会社と業務開始前に守秘義務を締結すること。
		3-1-4-5	退職時及び任期満了時には機密情報及び情報機器を回収すること。 - 回収物には、情報(印刷物及び記憶媒体)、パソコン、スマートデバイス及びアクセス権(ID及び鍵)を含めること。

「内部不正」「不注意」「教育不足」等による情報漏えい等

※大阪商工会議所 経営情報センター 作文・作図

全員 注意!

経営層 注意!

概要

①BCCで送るべきところTO,CCで送信
ブラインドカーボンコピー (Blind Carbon Copy) Carbon Copy

②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、
下の方に (B氏が知らない) A氏等の個人情報等が
残っていたり、秘密事項の添付ファイルが残存。

③同一内容の文章を別人に送信する時、宛先のメールアドレス
は変更したがメール本文の宛名を元の人のまま送信

④SNS投稿 (「インスタのストーリー」「BeReal(ビーリアル)」など)
(a)「通知から○分以内に投稿」という圧(「BeReal」の場合)
(時間との闘い! 分別なく、手あたり次第、目の前のモノや風景を投稿しようとする)
(b)「○時間で消える」という穴
(ストックでなくフローだと思ってしまう! 時間は短くてもストック! デジタルタワー)
(c)「公開範囲は友達のみ」という罠
(「友達」「友達の友達」がスクショや撮り出し拡散するかも! 「友達の友達」は友達でない!)
(d)「自分の日常(Real)を誰かに伝えたい」という欲
(e)本人は「悪気はなかった」、会社は「研修はしていた」の轍

事例

メール画面の送受信先が「株式会社B商事」になっているが、宛先は「株式会社A 代表取締役 A」になっている。これは「BCC」で送信されていることを示している。

メール本文には「株式会社A 代表取締役 A」という情報が残っている。

添付ファイルには「株式会社A 代表取締役 A」という情報が残っている。

メール画面の送受信先が「株式会社YYY会」になっているが、宛先は「株式会社YYY会」になっている。これは「BCC」で送信されていることを示している。

メール本文には「株式会社YYY会」という情報が残っている。

添付ファイルには「株式会社YYY会」という情報が残っている。

※西日本シティ銀行の「お詫びとお知らせ」(2026年4月30日)

対策

①複数のドメインにTO,CCでは送信できないように
しておく。エクセル名簿の1行目やファイル名に
「BCCで送信」など、自身に対する注意喚起を!

顧客名簿 (BCCで
送信する!) .xlsx

BCCで送信する!

②そのままの転送は原則しない

③同内容のメールを不特定多数に送信する場合、
一斉送信サービスなどを利用

④情報管理(SNS投稿を含め)のルール策定と徹底
(イ)スマホその他機器の持込の可/不可の具体的明示
(ロ)アプリやサービス利用の可/不可の具体的明示
(ハ)モノ・コト・情報・人の開示の可/不可の具体的明示
(ニ)ユーザごとの設定状況の定期的確認の徹底
(ホ)私用アカウントでもダメなモノはダメと徹底
(ヘ)人間の「自己顕示欲」や「想像力の低さ」に向き合う
(ト)デジタルネイティブ世代を過信しない

メモ欄

18

分散型サービス妨害攻撃(DDoS)^{ディードス}・犯罪のビジネス化

情シス 注意!

経営層 注意!

概要 Distributed Denial of Service

複数の(乗っ取った)PCやIoTに攻撃作業を分散的に(Distributed)担わせ、攻撃先の会社等に対し、**大量のアクセス**(7Mbps～100Gbps※警察庁調査)を行い攻撃先のネットワーク機器やサーバ等に**過負荷**をかけ、

その会社等の顧客や利用者が**HP等**を閲覧・利用すること(Service)を邪魔(Deny)し、**機会損失**や**イメージダウン**を行う。

かつては政治目的や嫌がらせがメインだったが、最近は「DDoS攻撃をされなくなったら、金を払え」といった経済犯的「ランサムDDoS攻撃」も。

※大阪商工会議所 経営情報センター 作文

実例 ※産経新聞・日本経済新聞・NHKの報道(2024年12月)等をもとに要約

- ①2024年9月、**京都市内の夫妻が、スポーツジム検索サイト(京都の中小企業が運営)**に対し、中国の代行業者に(SNS「WeChat」^{ウィーチャット(「微信」)}経由で) **750元(15,000円)**で“委託”し**DDoS攻撃**。サイト閲覧が不能に。広告契約解除等により数十万円の経済的損失。電子計算機損壊等業務妨害で逮捕
- ②2024年10月、**日本国内の中学生2人が、「IPストレッサー」というネットサービスを用い、自分の学校に関係するウェブサイトに対しDDoS攻撃。**
「YouTubeでDDoS攻撃の動画を見て、カッコいいと思った」などと供述。

対策

※警察庁「DDoS 攻撃への対策について」
(令和5年5月1日) から抜粋・要約

- ①**海外からのアクセスを遮断**
インターネット上の住所
(攻撃元のIPアドレスは99%が海外に割り当てられたもの)
- ②**WAF (Web Application Firewall) 等の導入**
ウェブ アプリケーション
ファイアウォール(火の壁)
- ③**サーバの設定で、同一IPアドレスからのアクセス回数制限・タイムアウト設定**

メモ欄

全員 注意!

概要

① クイッシング (Quishing)

メール等に記載の QR コード (悪性サイトへのURLを変換したもの) から誘導するフィッシング (パスワード・クレジットカード情報・個人情報が詐取される)

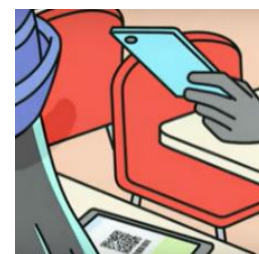
QRコードは、真贋判定がほぼ不可能
(URLなら文字列で場合により真贋判定できるが)

② 正規のQRコードの上に偽QRコードのシールが貼られている

繁華街、店舗、電車内などの広告・案内用の(正規の)QRコードの上に、悪性サイトへのアクセスが設定された偽QRコードのシールをペタッと貼り付ける

③ キャッシュレス決済のQRコードを撮影されてしまう

飲食店や小売店等で、スマホに(キャッシュレス決済の)QRコードを表示したまま置きっ放しにしておくと、悪意ある第三者に物理的に画面撮影され、使われてしまう



※上記イラスト：警視庁の公式Webサイト 「QRコードトラブル編」アニメーション映像より

対策

やってはいけないこと

- (1) QRコードを無警戒に読み取る
- (2) リンクを受動的に押す
- (3) 自分のスマホに表示されたQRコードを置きっ放しにする

やるべきこと

- (1) 急がば回れ！サイバーセキュリティって面倒臭いものだとか諦観する
- (2) シールが上から貼られていないか、手で触って確認する

※大阪商工会議所 経営情報センター 作文

ウイルス感染詐欺・パソコンサポート詐欺サポート詐欺(偽警告)

全員 注意!

実例



※IPA公式Webサイトより

クリックすると偽のセキュリティ警告が表示される「不審な広告」事例

※大阪府警察本部 公式Webサイトより

その警告画面・警告音は偽物です!!

①警告の画面が次々と重なって開く。
「閉じる」ボタンが隠されてしまい、画面を閉じる事ができない事例が多い。

②警告音やアナウンスが流れる
けたたましい警告音や、テクニカルサポートを名乗る「ウィルス感染」等の警告アナウンスが大音量で流れる事があります。

③実在する企業やサービスのロゴなどが表示される
マイクロソフト、マカフィー等「企業名やロゴ」、またWindowsの標準機能からの警告を装った表示が繰り返し表示される。

④サポート窓口の電話番号の表示!
問い合わせ先の電話番号が、繰り返し表示されます。

⑤焦らせるような表現が目立つ
「今すぐ対応しないと、個人情報情報が漏洩する」「無視すると被害にあう」など、ユーザーに切迫感を与え、動揺させて電話をかけさせようとする。

×(閉じる) 消滅

警告

注意

安全

山梨県の商工会 地域経済団体 従業員約20人
※朝日新聞報道・同商工会公式Webサイトから抜粋・要約 (2024年3月)

業務用PCで仕事をしていたところウイルス感染の警告画面が消えなくなった。表示の電話番号に電話した。

↓
マイクロソフトを名乗る男の日本語の指示に従いウイルスを除去すると称するソフトをインストール。ネットバンキング取引のIDとパスワードを教えた。「PCの電源は切るな」と言われ、その通りにした。

↓
口座から計3回計1千万円が不正送金(窃取)された。2台のPCが遠隔操作されており、当該PCは個人情報情報を保存してあるファイルサーバーに接続できる状態にあったことから、個人情報情報が漏洩した可能性が否定できない

「とにかく実行」も「安全に戻る」も、両方とも押下してはいけない!
「安全」なはずあらへん! 次ページの通り対応すること!

ウイルス感染詐欺・パソコンサポート詐欺サポート詐欺(偽警告)

全員 注意!

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！ 電話問い合わせ、アプリやソフトウェアのダウンロードを促すことはない！

※大阪商工会議所 経営情報センター 作文

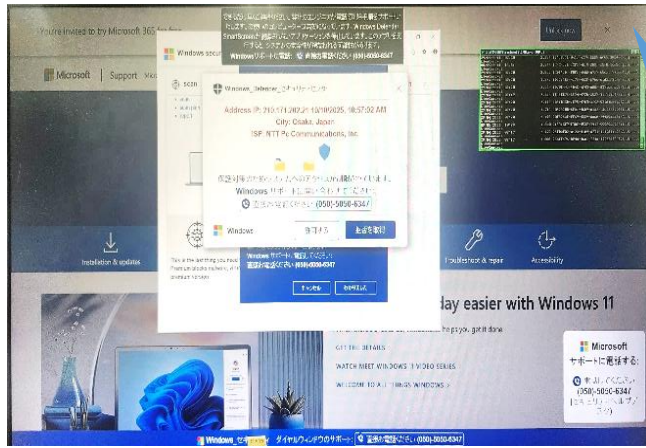
やってはいけないこと

- ① アプリやソフトはダウンロードしない！
- ② 電話番号に電話をかけない！
- ③ 個人情報・クレカ情報を入力しない！
- ④ 画面上のアイコン等を押下しない！

やっても良いこと

- ① (×(閉じる)ボタンが消滅しているケースが多いため) 先ず「×(閉じる)ボタン」を復活させ、警告画面を閉じる (下図参照)
- ② 「CTRL」「ALT」「DELETE」で強制終了
- ③ 電源ブチ切りで強制終了

※講師自身のPC(大阪商工会議所)に現れたウイルス感染詐欺の画面(2025年10月)



×(閉じる)消滅

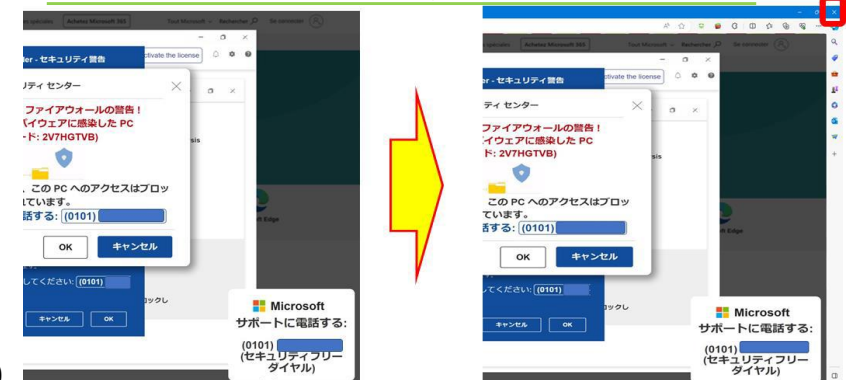
エスケープ
ESCキーを3秒程押す



落ちて着く

大丈夫!

右上に表示された × を押す



※上・右図：独立行政法人情報処理推進機構公式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

メールやSNS等を使った脅迫・詐欺の手口による金銭要求

全員 注意!

経営層 注意!

概要

- ・社長、部長などのエライ人を騙り、社員にニセメールを送り付け、お金を窃取する（この振込詐欺的手口は昔からあったが、2025年末から、SNSグループを作らせるパターンが出現）
- ・経理担当者等を含んだSNSグループを作らせて、支払い名目でお金を振り込ませる手法

実例

「LINEグループに招待して」詐欺（エライ人からの振込詐欺）

「業務プロジェクトに対応するためにLINEグループを作って招待してください」
「取引相手の振込先情報を送るから今すぐお金を振り込んでくれ」

実例

「『LINEグループに招待して』というメールを信用するな」詐欺

「私の名前を騙ってLINEグループを作成するメールが頻繁に届いています。絶対に信用しないでください。添付ファイルはメール遮断ツールです。直ちにダウンロードし(以下略)」

※2026年1月9日 警視庁 匿名・流動型犯罪グループ対策本部 発表

対策

やってはいけないこと

・エライ人を無条件に信じること。エライ人に後からイヤミ言われることを恐れること

やるべきこと

・エライ人に対してでも、勇気を出して事実確認を行うこと
・振り込む前に、上司や同僚に相談すること

※大阪商工会議所 経営情報センター 作文

中小企業のサイバー対策に必要な視点

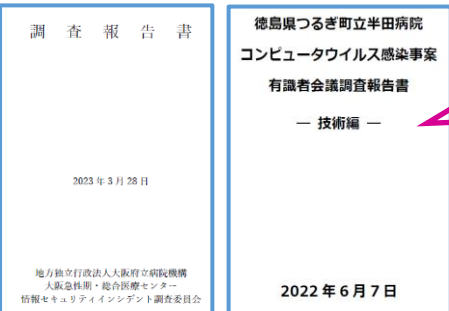
BCPの視点！ Business Continuity Planning(事業継続計画)

情シス 注意！

経営層 注意！

実例

①徳島県の町立半田病院の
ランサムウェア被害(2021年10月31日)
で現場対応した須藤氏(現院長)



「幹部職員も参集し災害相当と判断。(中略)災害対策本部を設置、BCPに基づく対応を行った。災害と判断したことが功を奏し(中略)、情報共有と連携を図ることができていた」

閉域网？ そんなの幻想よ！
想定外？ そんなの死後(語)よ！

👉「これは災害だ」
※朝日新聞の須藤氏(現日経新聞)の2021年11月取材

※大阪急性期総合医療センター・半田病院 調査報告書

②「名古屋港統一ターミナルシステム」ランサムウェア被害(2023年7月4日)
に係る国土交通省「緊急に実施すべき対応策」(同9月)

👉「(自然)災害用の事業継続計画は事前に整備されていたものの(中略)システム障害発生時のBCPがなかった。システム障害発生時のBCPを整備すべき」

③株式会社関通のランサムウェア被害(2024年9月12日)

👉「サイバー攻撃 その瞬間 社長の決定～被害企業のリアルストーリー」
同社社長(達城久裕氏)が著し、同社自身が発行 (2025年6月20日初版)
※(株)関通/Cyber Governance Lab(株)の許諾を受け掲載



中小企業の経営者・情シスは、是非読むべき！
分刻みの推移、各登場人物が思ったこと、やったこと、
その結果どうなったか、何が本当に重要だったか、
初動対処、被害額、リーダーの決断、事業継続、教訓

対策



※日本ネットワークセキュリティ協会西日本支部
「今すぐ実践できる工場セキュリティハンドブック サイバー対応IT-BCP編 第1.0版」



※IPA「中小企業のためのセキュリティインシデント対応の手引き」

SCS 評価 制度 ★3	7-1-1-1	事業継続上重要なシステムについて、サイバー攻撃を念頭に、業務の目標復旧レベルを定めたうえで、当該レベルまで業務を回復するために必要な対策を、以下の例を参考として整備すること [復旧のための対策(例)] - システムによる業務継続(例:予備機、クラウド環境等により待機系を整備する) - 人手による業務継続(例:電話、FAX等による連絡又は業務の実施に備え、影響のある取引先の連絡先及び複数の連絡手段を整備する)
	7-1-1-2	事業継続上重要なシステムについて、サイバー攻撃を念頭に、以下の対策を構想すること。 - 目標復旧時点への復旧ができるようにNo.4-3-4-1及びNo.4-3-4-2で取得したバックアップを保管すること - No.4-3-4-3で定めたリストア手順書どおりに、かつ、目標復旧時間内でバックアップの復元ができることを確認すること

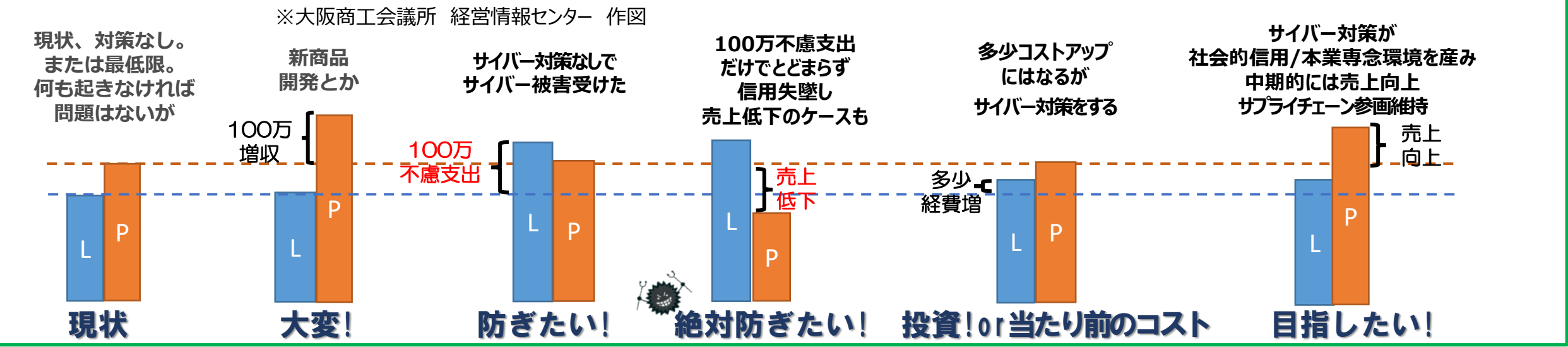
中小企業のサイバー対策に必要な視点

「コストではなく、投資！」or「投資ではなく、組織を守るための“当たり前の必須コスト”」 経営層 注意！

- 対策**・100万円の「新たな売上」をつくるより100万円の「無駄な支出」を防ぐ方が一般的には容易（神戸大学 森井昌克名誉教授）

・セキュリティは、何も起きなかったことこそが最善の成果（大阪大学 猪俣敦夫教授）

・セキュリティの向上により、売上や生産性が直接向上することは少ないが、少なくとも低下することは回避できる



「セキュリティ投資(当たり前の必須コスト)」の「相場」は？

対策 (一社)日本サイバーセキュリティイノベーション委員会

「企業規模・業種別に見るセキュリティ投資・人員数の目安値」(2026年2月13日)

ゴードン ローブ

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

IT投資…売上の2%と想定 うち「攻めのIT」85%、「守りのIT」15%と想定
∴「守りのIT」は売上の2%×15%

中堅企業 : 売上の0.3%

利益でなく売上!

中小企業のサイバー対策に必要な視点

どんな費目に、どれくらいお金がかかるか？

経営層 注意！

事例	甲社（30人サービス業）
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化。 PC 1 台がウイルス感染 ・外部に偽装メール送信
原因・被害範囲調査費	364万円
再発防止・事態収拾費 （ITコンサルティング・弁護士等）	44万円
再発防止費 （システム導入等）	214万円
社会的信用低下	？
合計被害額	622万円 + ？

※東京海上日動火災保険(株)
「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）
をもとに大阪商工会議所が作図

乙社(200人食品メーカー)
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
1320万円
1155万円
1000万円
？
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...

何から始めたらいいのか？

IPAの無償ツールや無償テキストや支援策を活用！

全員 注意！

情シス 注意！

経営層 注意！

対策 経営層・・・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・・・「情報セキュリティ6か条」を実践し「Security Action」宣言

読む

中小企業の
情報セキュリティ対策
ガイドライン
第4.0版



IPA 情報処理推進機構

調べる

中小企業・小規模事業者の皆様へ

5分でできる！
情報セキュリティ自社診断

最新動向への対応、できてますか？

脅威や攻撃の変化 IT環境の変化



取り返しのつかないことになる前に
あなたの会社のセキュリティ状況を
「5分でできる！自社診断」でチェック！

診断項目	No	診断内容	チェック			
			実施 している	一部実施 している	実施 していない	わからない
Part 1 基本的対策	1	パソコンやスマートフォンなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
	2	パソコンやスマートフォンなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル ^{※1} は最新の状態にしていますか？	4	2	0	-1
	3	パスワードは破られにくい「長く」「複雑な」「パスワード」を設定していますか？	4	2	0	-1
	4	データの共有設定を必要人に限定していますか？	4	2	0	-1
	5	故障や誤操作、ウイルス感染などによる重要情報 ^{※2} の消失に備えて定期的にバックアップを取っていますか？	4	2	0	-1
	6	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1
Part 2 従業員としての 対策	7	電子メールの添付ファイルや本文中心URLリンクを介したウイルス感染に気をつけていますか？	4	2	0	-1
	8	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	-1
	9	重要情報の受け渡しは、暗号化など安全な手段で行っていますか？	4	2	0	-1
	10	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1
	11	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルの対策をしていますか？	4	2	0	-1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机の上に放置せず、書庫などに安全に保管していますか？	4	2	0	-1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	-1
	14	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	-1
	15	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	-1
	16	関係者以外の事務用への立ち入りを制限していますか？	4	2	0	-1
	17	退社時にノートパソコンや備品を施設保管するなど盗難防止対策をしていますか？	4	2	0	-1
Part 3 組織としての 対策	18	内部ネットワークを守るため、不正アクセス対策機能を設定していますか？	4	2	0	-1
	19	ウェブサイトや公開すべきでない情報を公開していませんか？	4	2	0	-1
	20	従業員に情報セキュリティに関する教育や注意喚起を行っていますか？	4	2	0	-1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	-1
	22	重要情報の提供を行う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	-1
	23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	-1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	-1
	25	情報セキュリティ対策（上記1～24など）をルーラ化し、従業員に明示していますか？	4	2	0	-1

※1 コンピュータウイルスを発生させるためのデータベースファイル。「バックアップファイル」とも呼ばれます。
※2 重要情報とは、営業秘密など事業に必要で漏洩によって被害のある情報や、顧客や従業員の個人情報など流出した場合に組織のイメージダウンや損害賠償責任を問われるなどの管理責任を伴う情報のことです。

診断の後は次ページ以降を読んで対策を検討してください。

A+B+C
合計

点

相談する

情報セキュリティ方針
策定&公開する

デジタル化・AI導入補助金(旧IT導入補助金)
受給資格獲得

社会的信用UP 社員士気UP

自己宣言・登録する

情報セキュリティ6か条

- ① OS・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
- 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
- ⑥ バックアップを取ろう

中小企業向けサイバーセキュリティ対策支援者リスト

【独立行政法人情報処理推進機構（IPA）作成】
国家資格「情報処理安全確保支援士」の資格者のうち、中小企業向けサイバーセキュリティ対策支援が実施できる専門家のリスト。支援可能なテーマ、支援実績、得意業界、支援可能形態、支援料金、保有資格、保有スキル等を記載メールで直接連絡を取り、相談や依頼を行う

都道府県	支援可能なテーマ	支援可能な形態	支援可能な料金	支援可能なスキル	支援可能な資格	支援可能な実績	支援可能な得意業界	支援可能な支援者
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策
北海道	セキュリティ対策	相談・調査・対策	相談・調査・対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策	セキュリティ対策

取引先も含めて守る

◎サプライチェーン強化に向けたセキュリティ対策評価制度(SCS評価制度)
(★3・★4・(★5))

国際認証

ISMS (ISO/IEC27001)

※独立行政法人情報処理推進機構（IPA）2026年3月29日

パスワード強化の方法（情報セキュリティ6か条③）

全員 注意！

対策 ※大阪商工会議所 経営情報センター 作文

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. 固有名詞(人名・社名)、誕生日、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簡単なパスワとなってしまう！下記②で作成し、手帳に記載&鍵のかかるロッカーに保管

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！で解売）
👉大文字+小文字で6桁…197億通り（秒殺！で解売）
👉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（解売に15年）



内閣サイバーセキュリティセンター
(現国家サイバー統括室)
「パスワードノート」

P@ssw0rd 等は一応4文字種だが**絶対NG**

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

大阪商工会議所が「巨人が嫌い」なわけではありません
講師個人が選定した、大阪弁で言うところの「ネタ」です

- 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（解読に最大287日）
- 3. 数文字を大文字に **kyojinWAKirai**
52の13乗通り（解読に最大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=4.47×10²⁹通り（解読に最大1,067億年）
- 5. 利用サービス名を追加 **kyojinWAKirai!4ama**（某世界的小売業の場合）
kyojinWAKirai!4neko（某大手宅配便の場合）
使い回しリスク減少

今後の対策 パスキー(Passkeys：生体情報と所有による認証)等のパスワードレスの認証（パスワそのものが盗まれることを想定）

パスワード強化の方法（SCS評価制度での評価基準）

情シス 注意！

経営層 注意！

対策

※経済産業省の公式ウェブサイト(2026年3月27日)から抜粋

SCS 評価制度★3	パスワード 設定 ルール	4-1-5-1	パソコン、サーバ、スマートデバイス及びクラウドサービスの利用者又は管理者は、それらにおける デフォルトパスワードを変更 するよう 社内ルールを定めること
		4-1-5-2	ユーザ認証にパスワードを利用する場合、 推測されやすい単語の設定を禁止 するよう 社内ルールを定めること
		4-1-5-3	ユーザ認証にパスワードを利用する場合、以下のいずれかの保護対策を講じるよう 社内ルールを定めること - No.4-1-3-3で示す認証要素を利用した 多要素認証 を使用するか、又は 試行が少なくとも10回失敗した場合にアカウントロック するように制限したうえで、パスワードの長さを8文字以上とする。 - 上記のとおり 多要素認証又は試行回数 の制限を実施できない場合、パスワードの長さは、 英大文字・小文字、数字を含めた10文字以上とする。
		4-1-5-4	ユーザ認証にパスワードを利用する場合、情報機器及びサービス間での パスワードを使い回さない よう 社内ルールを定めること
		4-1-5-5	No.4-1-5-1からNo.4-1-5-4までで 定めたパスワード設定に関するルール について、役員、従業員、派遣社員及び受入出向者を対象に 周知すること
SCS 評価制度★3	パスワード 管理 ルール	4-1-6-1	紙媒体への記載及び施錠保管 、パスワード管理アプリの利用等により、パスワードを安全に保管するよう 社内ルールを定めること
		4-1-6-2	パスワードの漏洩 が判明した場合、又はその疑いがある場合に速やかにパスワードを 変更 するための 手順を定めること
		4-1-6-3	No.4-1-6-1及びNo.4-1-6-2で定めた パスワードの管理に関するルール について、役員、従業員、派遣社員及び受入出向者を対象に 周知すること

経営層 注意!

30

脅威や攻撃の手口を知る（SCS評価制度での評価基準）

情シス 注意！

経営層 注意！

対策 ※経済産業省の公式ウェブサイト(2026年3月27日)から抜粋

SCS 評価制度★4	セキュリティの意識向上のための教育・研修	4-2-1-1	経営層が情報セキュリティに関する役割及び責任を理解するための機会を設けること
		4-2-1-2	セキュリティに関する職場特有のリスクの理解及びルールへの遵守が必要な場合、職場単位で重要なルール及びリスクについて、年1回以上の頻度で周知すること
		4-2-1-3	以下のトピックについて、役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時、かつ、年1回以上、教育資料配布・掲示、eラーニング、集合教育等による教育・研修を実施すること - 電子メールによるマルウェア感染の予防 - Web 閲覧によるマルウェア感染の予防 - 機密区分の定義と取扱い
		4-2-1-4	No.4-2-1-3で実施した教育・研修の実施状況を記録し、保管すること
		4-2-1-5	年1回以上の頻度でセキュリティの意識向上のための教育・研修の実施内容について点検すること
SCS 評価制度★3	セキュリティインシデント発生時の教育・訓練	4-2-2-1	役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時、かつ、年1回以上の頻度で、セキュリティインシデント発生時の対応について、教育資料の配布・掲示に加え、eラーニング又は集合教育による教育・訓練を実施すること
		4-2-2-2	No.4-2-2-1で実施した教育・訓練の実施内容、実施方法、実施時期及び受講状況を記録し、保管すること
		4-2-2-3	年1回以上の頻度でセキュリティインシデント発生時の対応に関する教育・訓練の実施内容について点検すること

攻撃等の検知 (SCS評価制度 1-2-2-2/5-1-1-1/5-1-1-2/5-1-1-3/6-1-1-1)

国の「お助け隊サービス」登録第1号「商工会議所サイバーセキュリティお助け隊サービス」

情シス 注意!

経営層 注意!

対策 ※大阪商工会議所 経営情報センター 作図



※全国のいずれかの商工会議所・商工会
※非会員 月8600円
※「サブライティエーション強化に向けたセキュリティ対策評価制度」の
を少なくとも下記の5つの評価基準を満たす

メモ欄

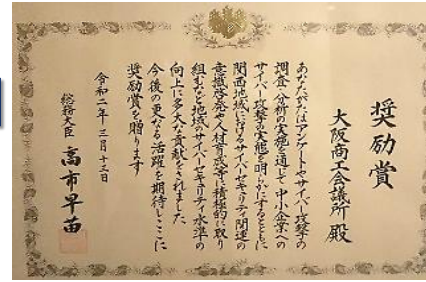


SCS 評価 制度	★4	1-2-2-2	入手した情報又はログの相関分析等により、 サイバー攻撃の予兆及びインシデントの発生 の検知を可能とし、 インシデントの防止及びインシデントが発生した場合の対応 が導き出せる 体制を整備 すること ①【お守り(防止)】②【見守り(予兆・分析)】③【お知らせ(発生検知)】④【駆け付け(対応)】
	★3	5-1-1-1	社内外ネットワークの境界又は端末において、インターネットから社内への通信及び社内から不正なサーバへの通信の双方について、不正アクセスをリアルタイム検知・遮断する仕組みを導入すること ①【お守り(リアルタイム検知・遮断)】
	★3	5-1-1-2	ネットワーク機器のログ及びアラートを分析し、セキュリティ担当部署の担当者又は管理者により不審な事象が発見された場合に、それが セキュリティインシデントに該当するかが判断 されること ①【見守り(分析)】②【お知らせ・相談(インシデントに該当するかどうか判断)】
	★3	5-1-1-3	No.5-1-1-1で設置したネットワーク機器又はサービスについて、以下の要件を満たす 異常時に通知する仕組みを導入 すること。 -アラートが速やかに 発報 されること -インシデントの 速報レポート が作成され、 通知 されること ①【お知らせ(アラート発報・速報レポート)】
	★4	6-1-1-1	以下の手順を含んだ セキュリティインシデントへの対応手順を定める こと ①発見報告 ②初動 ③調査・対応 ④復旧 ⑤最終報告 ①【お知らせ(①)】 ②【駆け付け(②～⑤)】 ※サービス利用＝手順制定

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」
を高市早苗総務大臣(当時)から、受賞しました。
今後も全国のサイバー攻撃対策セミナーに、無償で
講師を派遣し、意識啓発・人材育成に貢献します！



高市内閣「日本成長戦略本部」 (2025年11月4日)

「危機管理投資」「成長投資」戦略分野

- ① A I ・半導体 ②造船 ③量子 ④合成生物学・
バイオ ⑤航空・宇宙 ⑥デジタル・サイバーセキュリ
ティ ⑦コンテンツ ⑧フードテック ⑨資源・エネルギー
安全保障・G X ⑩防災・国土強靱化 ⑪創薬・先端医療
⑫フュージョンエネルギー ⑬マテリアル（重要
鉱物・部素材）⑭港湾ロジスティクス
⑮防衛産業 ⑯情報通信 ⑰海洋

「分野横断的課題」

- ①新技術立国・競争力強化 ②人材育成
③スタートアップ ④金融を通じた潜在力の解放
⑤労働市場改革 ⑥介護、育児等の外部化など負担軽減
⑦賃上げ環境整備 ⑧サイバーセキュリティ

大阪商工会議所 経営情報センター（野田）

〒540-0029 大阪府中央区本町橋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/>

本日の講演を受講された皆さん！
この二次元コード読み取りますか？
ええんですか？ほんまに？

