よろず相談会第3回

2024年11月6日 10：00～12：00

一般社団法人　日本自動車工業会
総合政策委員会　ICT部会　サイバーセキュリティ分科会

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

本日の進行について

本日の進行	事前に頂いたご質問に対し、一問一答形式で進めさせて頂きます。
	一問一答の中で関連する質疑については口頭にてお願い致します。
	事前に頂いたご質問につきまして、個社の情報等を省き、一般化しております。
注意事項	進行上マイクとカメラは必ずオフにしてください。
	発言される際には挙手ボタンを押していただき、指名されましたら、 マイクをオンにして発言をお願いします。発言が終わりましたら必ずマイクをオフにしてください。
	話しの流れによっては個社ごとの状況を回答させて頂く場合もございます。
	運営管理上、本日の会議はレコーディングさせて頂きます。
	本資料は後日、メール、及び自工会HPにて展開いたします。ただし、本日の相談会の中で 個別にやり取りさせて頂いた内容は反映いたしませんので、ご注意ください。

本日取り上げさせて頂くご質問一覧

No.	質問
1	セキュリティ対策の予算の確保を、経営層に理解・納得していただく方法について教えてほしい。
2	情報セキュリティ対応方針(ポリシー)や規程はどのように作ればよいでしょうか？ また、組織だった体制を構築する際どのように進めればよいでしょうか？
3	セキュリティ・IT部門以外の部門は、あまり積極的に行動してくれていません。 他部門を巻き込んで、セキュリティ対策を推進するためのアプローチについて知りたい。
4	EDR製品の導入を行いたいが費用が大きく難しい。代わりに行われている対策があればお聞きしたい。
5	停止が難しいサーバー機へのアップデート対応をどのように進めて行けばよいか知りたい。
6	高い機密区分の情報資産（情報）の一覧化について、デジタル情報の生成速度の高速化など、実際に正しい状況を維持することが困難な状況が見えてきています。ベストプラクティスがありましたら教えてください？

時間が足りない場合は、すべての質問に対してお話できない可能性がございます。
時間が余った場合は、その他の質問に対しても取り上げますので、ご発言頂ければ幸いです。
活発な議論の場としたく、ご理解の程よろしくお願い致します。

IPAセキュリティプレゼンター
自己紹介

氏名	徳永 雅彦 （とくなが まさひこ）市川市在住
所属	（株）ナレッジシェア　代表取締役 日本技術士会　会員／市川商工会議所　会員　IT相談員 NPO法人ITCちば経営応援隊　理事
連絡先	tokunaga@kshare.jp
得意分野	・経営戦略・IT戦略策定支援、情報セキュリティ対策、情報セキュリティ監査、情報システム開発支援。 ・テキストマイニング、ナレッジ共有化支援。 ・IT系研修講師。
経歴・主な経験	・システム開発会社にて開発SE、開発部長、取締役を経て2011年独立。2015年（株）ナレッジシェア設立。 ・東京都中小企業振興公社、千葉県産業振興センター等支援事業にて、中堅・中小企業の経営改革とDX改革の支援中
資格等	・技術士（情報工学部門）　・情報処理安全確保支援士 ・公認システム監査人 ・ITコーディネータ

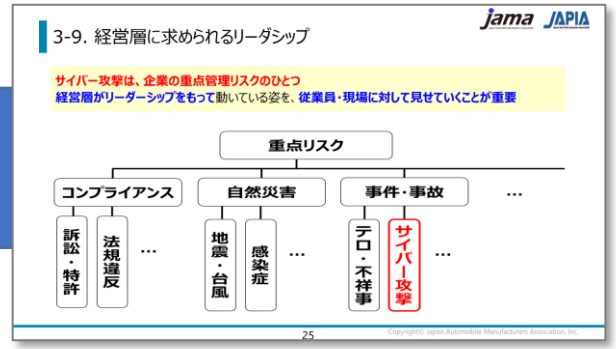
公益社団法人 日本技術士会
The Institution of Professional Engineers, Japan

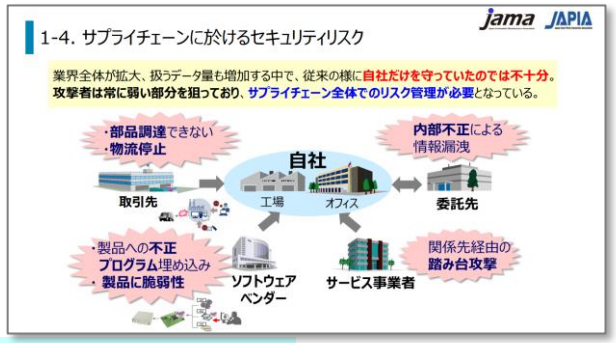
第008136号

質疑応答

質問①

セキュリティ対策の予算の確保を、経営層に理解・納得していただく方法について教えてほしい。



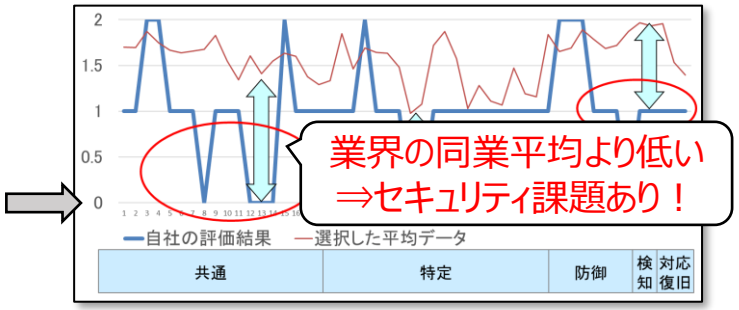


回答：
サイバーセキュリティ対策は、経営課題です。
経営者が正しい経営判断を実施いただけるようにするために、セキュリティ推進部署の皆さんは、適宜経営者へ判断情報を報告することが大切です。

例えば、2024年度 自己評価の実施・展開及び経営層向け説明会資料等をご活用いただきながら、下記情報を報告し、経営リスクへの構えを取っていただくことが重要と思います。

・セキュリティ事故被害により自社業務が停止する事例が発生しており、**セキュリティ強化はビジネス継続に重要**になっていること
・**企業規模に関係なく**、自動車業界の会社においても**セキュリティ事故被害が増加**しており、**他人事ではない**こと
・自社の業務影響が、**自動車業界サプライチェーンに関わる会社のビジネス継続に与える影響・損害額**

また、セキュリティ対策予算の確保の取組み例としては、
自動車業界平均比較テンプレート（自己評価提出会社へ送付）を活用し、他社の対策状況（規模別、業種別）と自社の対策状況とのギャップから、強化対策計画を作成して、優先付けを行い対応されている会社もあります。



【参考】JUAS：IT予算に占める情報セキュリティ関連費用の割合（P.43）

質問②

情報セキュリティ対応方針(ポリシー)や規程はどのように作ればよいでしょうか？また、組織だった体制を構築する際どのように進めればよいでしょうか？

回答：サイバーセキュリティポリシーおよび手順については、IPA殿のWebサイトに掲載された「中小企業の情報セキュリティ対策ガイドライン」（以下リンク参照）等にその雛形となる情報が掲載されております。
これらを参考に、自社の状況に合致した形にアレンジすることにより、比較的容易に相応のポリシー／手順を作成することができますので、参考としてください。

付録2：情報セキュリティ基本方針（サンプル）（全1ページ）（Word:35 KB）

付録5：情報セキュリティ関連規程（サンプル）（全45ページ）（Word:167 KB）

但し、単純に会社名などを埋めていくのではなく、その記載内容を正しく理解・把握したうえで、実行可能なものを策定することは必要です。以下の手順で進めることを推奨します。
①公開されているテンプレートを入手する
　（例：「情報機器の利用ルール」では規定サンプル「IT機器利用」（※）を活用）
②内容を鑑みて適切な管轄部署（所管部門）を検討し、規定やルールの責任者を決定する
　（例：「情報機器の利用ルール」では、機器提供／管理を行うIT部門長）
③管轄部署にて自社の事情／環境を考慮し、自社の状況に合わせて修正する
　（例：情報機器では、どんな端末／ソフトウェアを支給しているか）

質問②

情報セキュリティ対応方針(ポリシー)や規程はどのように作ればよいでしょうか？また、組織だった体制を構築する際どのように進めればよいでしょうか？

回答：セキュリティの体制を整備にあたっては、IT部門のような特定の部門に特化せず、全社横断的な体制を組むことが重要です。全社横断的な体制を構築し役割を明確にすることにより、それぞれの部門が主管する範囲が明確になり、規定やルールの整備やセキュリティの実務を行っていけるようになるかと思います。

特にポイントとしては各部門に関連した役割を明確にすることで合意が得られやすくなるかと思います。
例：システム管理者⇒IT部門、教育責任者⇒総務部門
　　部門責任者⇒部門が保有している機密情報（顧客情報、図面・・・など）の管理

【表６】情報セキュリティ管理のための役割と責任分担(例)

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

参考
IPA 中小企業の情報セキュリティ対策ガイドライン
本編：第二部４　（１）管理体制の構築（P24）より

質問③

セキュリティ・IT部門以外の部門は、あまり積極的に行動してくれていません。他部門を巻き込んで、セキュリティ対策を推進するためのアプローチについて知りたい。

回答：体制づくりと教育・啓蒙活動が重要と考えます。

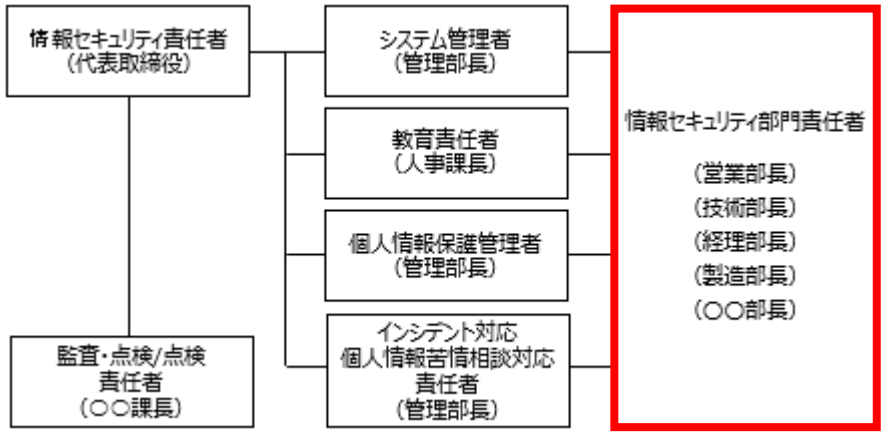
＜体制づくり＞

・経営層、CISOをトップとし**各部門に**情報セキュリティ責任者、情報セキュリティリーダーを配置した**全社横断的な体制**を構築する。
・情報セキュリティ対策を推進する**情報セキュリティ委員会**を設置する。
・情報セキュリティ部門は**定期的に各部門**責任者に施策展開を行い、**各部門自ら**推進する体制をつくる。

＜教育・啓蒙活動＞

・情報セキュリティ部門は、教育の雛形を各部門に提供し、**各部門自ら**部門教育を実施する工夫を行う。
・情報セキュリティ部門は、**階層別教育**や**全社員への**セキュリティ通信などの啓蒙活動を並行して行い底上げを図る。

【参考】IPA中小企業の情報セキュリティ対策ガイドライン
記載の情報セキュリティ委員会体制図サンプル



【ご参考資料】 中小企業の情報セキュリティ対策ガイドライン第3.1版　付録5：情報セキュリティ関連規程（サンプル）1 組織的対策
000055794.docx (live.com)
教育・学習（企業・組織向け）｜ここからセキュリティ！ 情報セキュリティ・ポータルサイト (ipa.go.jp)
自動車産業サプライチェーンへの推進活動 | JAMA - 一般社団法人日本自動車工業会

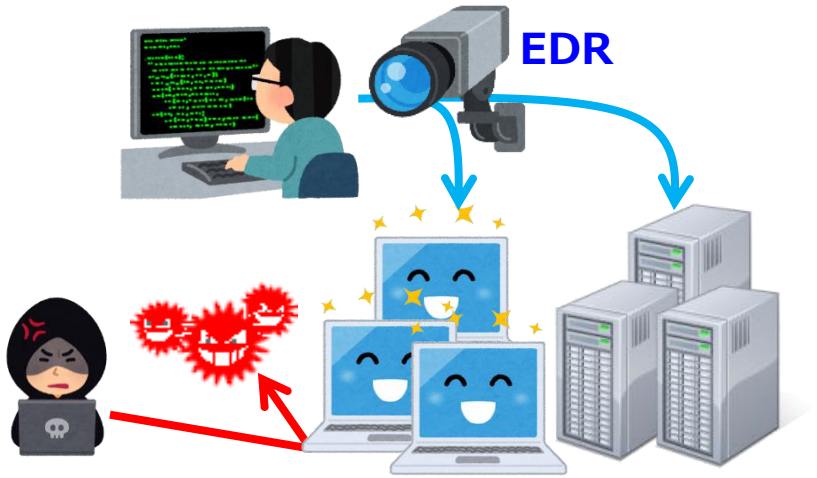
質問④

EDR製品の導入を行いたいが費用が大きく難しい。代わりに行われている対策があればお聞きしたい。
（Endpoint Detection and Response）

回答：
EDR製品は、高額な対策と思います。しかし、セキュリティ事故被害に合った会社は、再発防止策としてEDR製品の導入を真っ先に考えられるなど、**投資してでも必要な重要対策**と考えます。 **EDRの代わりとなる対策は現状ありません。**

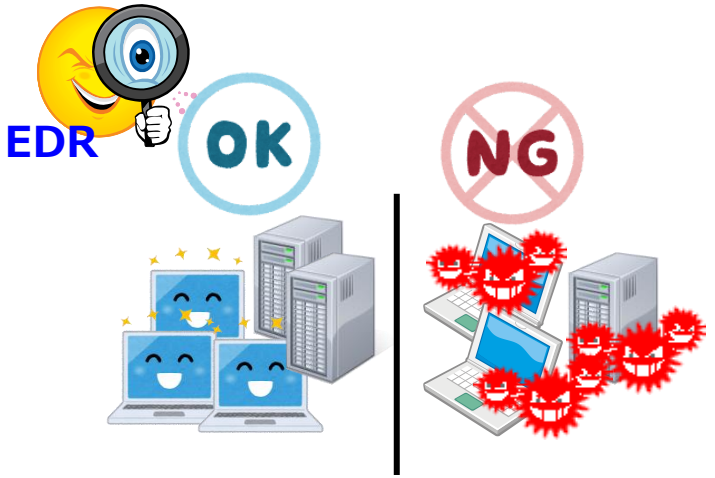
①サイバー攻撃被害から守る

エンドポイントのログを収集・分析し、怪しい挙動や攻撃を
検知＆隔離して脅威を除去
※未知ウィルスにも対抗



②マルウェア被害範囲の特定

万が一侵入を許してしまった場合においても、
被害端末を一台ずつ通信ログを分析せずに、
統合管理的に被害範囲を把握可能



③セキュリティ事故復旧対応時、
クリーンなサーバ・端末であることを判別

【参考】IPA a)お助け隊 制度説明、b)お助け隊サービス基準（ネットワーク監視型（UTM）と端末監視型（EDR））（概要： P.3、P.6-P.7、P.10-P.21）

※製品によって機能差があります。

質問⑤

停止が難しいサーバー機へのアップデート対応をどのように進めて行けばよいか知りたい。

回答：
停止が難しい＝停止することで業務への影響が大きいということかと思います。
そのためアップデートを行うには業務停止リスクを下げる施策が必要になります。
考えられる施策としては以下があります。
・テストサーバ、バックアップサーバで事前にアップデートし、問題が無いか確認する。
　⇒事前にアップデートを行い、搭載しているシステムが正常に動作することを確認する。

・切り戻し（アップデート前に戻す）方法を準備する。
　⇒切り戻し手順の確認、サーバの全体バックアップ及びリストア手順の確認・実施など。

・業務時間外にアップデートを実施する。
　⇒アップデート＋テスト時間＋切り戻し時間を計算し、業務に影響が出ないように計画する。
　　関係者への通知を行う。
※例えば毎月第１土曜日は定期アップデートの日のように事前に決めておくことで実施し易くなる場合があります。

その他：利用システムのクラウドサービスへの移行を進めることでサーバOS等のセキュリティ対策工数を低減することが出来る場合があります。※クラウドサービスのセキュリティ対策状況の確認が前提

質問⑥

高い機密区分の情報資産（情報）の一覧化について、デジタル情報の生成速度の高速化など、実際に正しい状況を維持することが困難な状況が見えてきています。ベストプラクティスがありましたら教えてください？

回答：

高機密情報の一覧化（台帳管理）を正しい状態に維持するには、まずは基本的なポイントを押さえることが必要です。

① 機密区分の定義や分類方法を出来るだけ明確で分かり易くする（例えば定型文書は、どの機密区分か決めておく）。
一覧化すべき**高機密文書を必要十分に絞り込む**ことが出来ます。⇒判断の効率化、自動化準備。

② 高機密文書の保管先を絞り込んで、その保管先へのアクセス権や移動制限などのルールを決めて設定します。
会社で準備した**クラウドに保管して一元管理するのも一つの方法**です。⇒保管・取扱い設定・棚卸の効率化。

③台帳**１行に記入する情報単位を最適化**します。例えば経営情報を自動で集計分析するシステムでは生成物一つ一つを台帳記入するより生成物種類ごとに書く方が現実的です。⇒システムでセキュリティ対策を担保する。

④機密区分の定義や高機密情報の扱いに関するルールを**社員に教育**します。情報資産の作成時、日常的および定期的な台帳メンテ・棚卸を正しく出来る様にすることが必要です。⇒セキュリティ品質の均一化と向上。

⑤上記の基本を押さえた上で、高機密文書が多くある場合や生成が頻繁な場合は、ツール導入が有効になると思います。
高機密情報のセキュリティ対策をシステム的に行う機密管理ツールとして**IRMやデジタルラベリング**があります。
（IRM：Information Rights Management。暗号化や利用権限制御などを実現する機密情報ファイル保護・管理システム）
クラウドでの一元管理とデジタルラベリングが実現できれば、機密情報の自動的なリスト化も可能になると考えられます。

参考情報

独立行政法人情報処理推進機構（IPA）
サイバーセキュリティに関する業務概要

■ 平時からインシデント発生時まで、サイバーセキュリティのマネジメントからオペレーションまでトータルな施策・対応を実施。

普及啓発・リテラシー向上支援

- 情報セキュリティ10大脅威、情報セキュリティ白書
- 経営者、社内担当者向け各種ガイドライン・教育コンテンツ
- 地域・中小企業支援
- 情報セキュリティ安心相談窓口
  10,923件（2023年）

SECURITY ACTION
セキュリティ対策自己宣言
累計宣言数約30万者（2023年10月）

サイバーセキュリティ お助け隊

サイバー事案対応（検知・分析・対処調整）

- サイバー情勢分析
- 国家支援型サイバー事案対策
- 情報共有（サイバー攻撃情報・脆弱性）
- セキュリティ監視（独法等）
- サイバー事故原因究明

IPA J-CRAT
2011年創立　341件支援（2023年）

J-CSIP Initiative for Cyber Security Information sharing Partnership of Japan

JVN iPedia
脆弱性データベース
約20万件登録（2024年3月）

セキュリティ基準・評価認証

＜製品・サービスのセキュリティ評価・認証＞

CRYPTREC Cryptography Research and Evaluation Committees

- 暗号技術調査/IT製品ISOセキュリティ認証
- IoT製品セキュリティラベリング（JC-STAR）
- クラウドサービスセキュリティ評価（ISMAP）

＜セキュリティ基準・分析・監査等＞

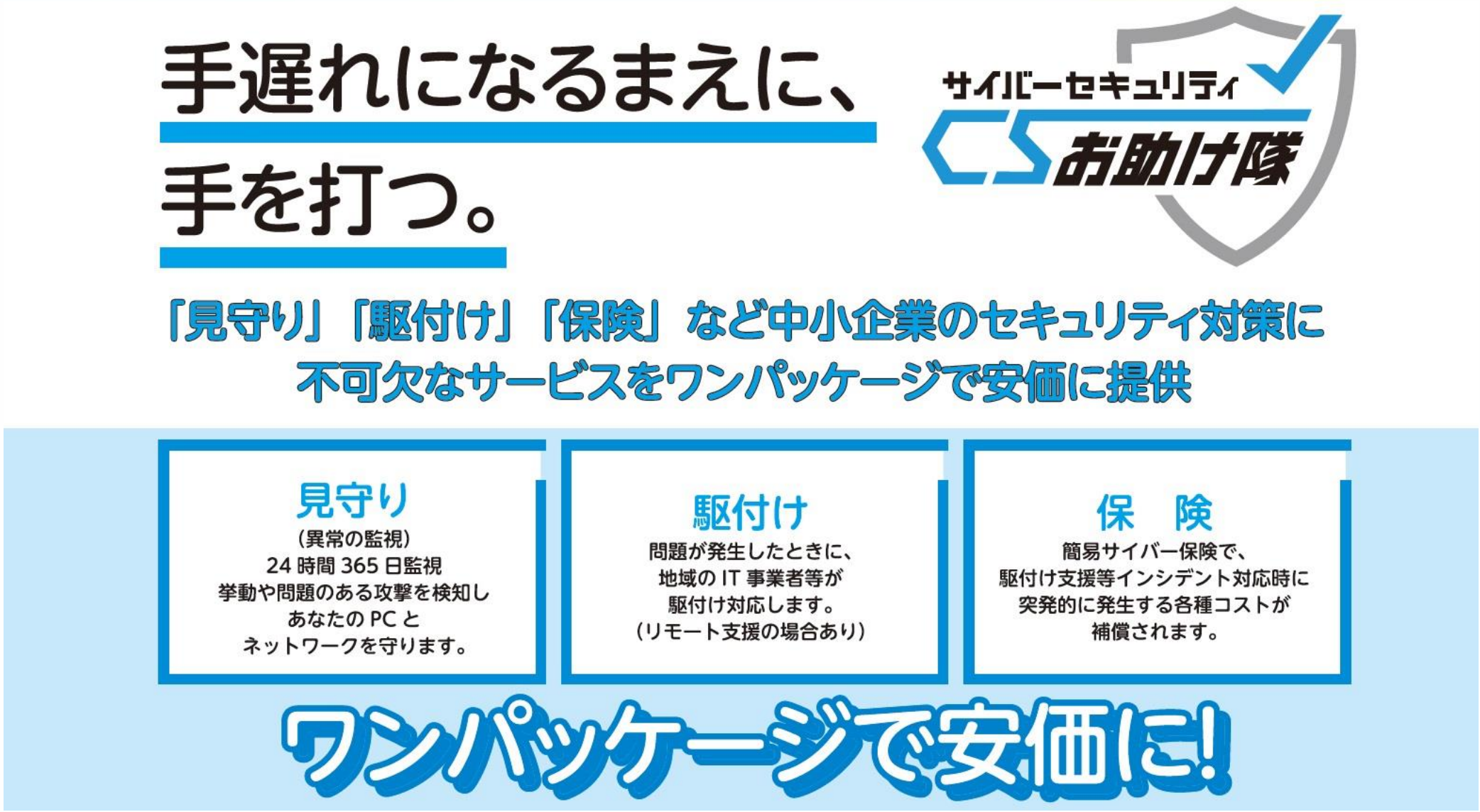
JC-STAR

- 制御システムセキュリティリスク分析
- サプライチェーンセキュリティ評価
- 独法等情報セキュリティ監査、政府システム監査

人材育成

- 国家資格「情報処理安全確保支援士」
  登録者数21,727名（2023年10月1日時点）
- 中核人材育成プログラム
  累計435名受講（2017年～）
- 若手人材発掘（セキュリティ・キャンプ）
  累計1,073名受講（2004年度～）
- 情報セキュリティコンクール
  応募約５万点（2023年度）

サイバーセキュリティお助け隊サービスの活用を！



サイバーセキュリティお助け隊サービス制度

https://www.ipa.go.jp/security/sme/otasuketai-about.html

- 中小企業に対するサイバー攻撃への対処として不可欠なサービス要件を、ワンパッケージとしてサービス基準にまとめ、これを満たすことが所定の審査機関により確認された民間サービスをIPAが「**サイバーセキュリティお助け隊サービス**」として登録・公表する制度。

◇「サイバーセキュリティお助け隊サービス基準」の主な内容

主な要件	概要
相談窓口	ユーザーからの**相談を受け付ける窓口**を設置／案内
異常の監視の仕組み	ネットワーク又は端末を**24時間見守る仕組み**を提供
緊急時の対応支援	インシデント発生などの**緊急時には駆け付け支援**
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：**月額１万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）**
簡易サイバー保険	インシデント対応時に突発的に発生する駆付け費用等を補償する**サイバー保険を付帯**

相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

本サービスを採用することを通じて、取引先企業に対する**自社の信頼性をアピール**

・ワンパッケージのサービスとして登録

・マーク提供
・ブランド管理・普及促進

➢ 各地域の「サイバーセキュリティお助け隊サービス」として**40事業者**が**57サービス**を登録。（2024年4月時点）

サイバーセキュリティ CSお助け隊

マーク付きの民間サービス

中小企業

E N D