よろず相談会 第6回

2024年11月22日 15：00～17：00

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	資産台帳　情報セキュリティ規定　等、初めの一歩から取り組むことになります。 情報情報資産台帳については、どのような情報を登録するのか、各情報の機密区分はどの様に決めていけば良いのか教えてください。
2	現状の自社内の対策状況がセキュリティレベルに対応できているのか確認方法が分からないので教えてください。
3	外部情報サービスが具体的に何を指すのか教えてください。 ｱﾌﾟﾘｹｰｼｮﾝやｸﾗｳﾄﾞｻｰﾋﾞｽ等の利用について、ｾｷｭﾘﾃｨ面の審査をどの様に実施すれば良いか、また各社どの様にしているのか知りたい。
4	従業員へのセキュリティ教育実施の施策について教えてください。また、以下の点について具体的に教えてください。 ・電子メール機能やWebブラウザ利用及び事故事例の教育で、利用者がより関心を持ってくれるコンテンツを紹介頂きたい。 ・自社環境でも影響が大きい注意喚起事例を、負担少なくタイムリーに社内共有する方法を知りたい。
5	自社でサイバー対策についての知識が薄く勉強しながらの状況です。知識のレベルアップ方法を教えてください。
6	No.17,24,50,53 各種ログに対する対処方法をどのようにされているのかをお聞きしたいです。 ・専門担当者がおらず、保存場所や機能が異なるﾃﾞﾊﾞｲｽに対して、ﾛｸﾞの収集から分析まで、どの様にすれば良いか教えてください。

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

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

第008136号

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

質疑応答

質問①（1/2）

資産台帳　情報セキュリティ規定　等、初めの一歩から取り組むことになります。
情報資産台帳については、どのような情報を登録するのか、各情報の機密区分はどの様に決めていけば良いのか
教えてください。

回答： IPA殿Webサイト上の 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　P54～58 リスク分析の【手順１】および 付録7：リスク分析シート（全7シート）(Excel:98 KB)　情報資産管理台帳Sheetが参考になります。
但し上記は厳格な方法なので敷居が高いかもしれません。もう少し やり易い方法例を下に記します。

１）機密区分を定義する ⇒ ２）高い機密区分の情報を抽出する ⇒ ３）情報資産 管理台帳に記入する

表１．達成条件No.54 機密区分の例

機密区分例	定義例（外部に漏洩した場合、会社の信頼や収益に）	取扱い方法例	台帳記載
極秘	極めて秘匿性の高い情報（著しい影響を及ぼす可能性がある）	コピー、移動等 禁止	要
秘 （マル秘）	厳格に選定された関係者のみに共有すべき秘匿性の高い情報 （影響を及ぼす可能性が高い）	コピー、移動は一定条件でのみ可。 保存時には暗号化	
関係者外秘 （社外秘）	関係者間で業務に利活用する情報 （影響を及ぼす可能性がある）	持ち出し時手続き要。保存時のアクセス制御、会社指定保管先のみ可	不要
（公開）	機密に当たらない情報（影響を及ぼさない）	ー	

※ 上記に並行して、個人情報か否か、顧客から預かった情報か否か、という視点での分類を併用する場合も多い。

質問①（2/2）

資産台帳　情報セキュリティ規定　等、初めの一歩から取り組むことになります。
情報資産台帳については、どのような情報を登録するのか、各情報の機密区分はどの様に決めていけば良いのか教えてください。

１）機密区分を定義する ⇒ ２）高い機密区分の情報を抽出する ⇒ **３）情報資産 管理台帳に記入する**

表２．達成条件No.56 情報資産(情報)一覧化の例

極秘情報資産一覧（例）

No.	対象情報	個人情報有無	管理者	部署	保管場所	保管期限	開示先（メールアドレス）	棚卸日	備考
1									
2									
3									
4									

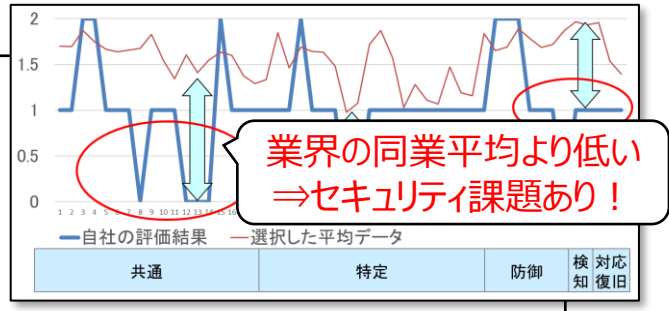
質問②

現状の自社内の対策状況がセキュリティレベルに対応できているのか確認方法が分からないので教えてください。

回答：

例えば、下記の様な確認方法があると思います。

1)自動車産業ガイドを活用した自己評価　（業種・規模別平均との違い）
2)診断ツールによるチェック（プラットフォーム診断、Web診断等）
3)外部ベンダーからの専門的な支援による確認



＜1)自動車産業ガイドを活用した自己評価　の注意点＞

対策完了とご判断いただくには、**「目的」**項目に書かれた**“何のために対応するのか？”**を認識いただいた上で、
“何を？”（「達成条件」の内容）、**“どれだけ対応するのか？”（「達成基準」の内容、対象、時期、頻度）**の
全てが満たせているのかを確認ください。
また、自動車産業ガイドの自己評価は、**自己評価の点数アップが目的ではありません。**
是非、**セキュリティレベルアップが必要なポイントの点検（気づき）**と**セキュリティレベルアップ**に繋げていただけますと幸いです。
（できていることを評価するのではなく、できていない所を見つけるツールとしてお使いください。）

次ページ参照

参考

分類	ラベル	目的	要求事項	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)
共通	1方針	会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる	自社の情報セキュリティ対応方針を策定し自組織内に周知していること	1	Lv1	**自社の情報セキュリティ対応方針(ポリシー)を策定している**	・自社の情報セキュリティ対応方針を策定し、文書化すること	【情報セキュリティ対応方針の記載事項の例】 ・経営者の責任：当社は、情報セキュリティを確保・維持、改善するための活動を、経営者主導で推進します ・法令遵守： 当社は、情報セキュリティに関連する法令を遵守します 【策定・文書化の責任者の例】 ・経営者 ・取締役会
				2	Lv2	**自社の情報セキュリティ対応方針(ポリシー)の内容を確認し、必要に応じて見直ししている**	【規則】 ・社内外の環境変化を踏まえて、内容を確認し、適宜見直ししていること 【頻度】 ・情報セキュリティ対応方針(ポリシー)の内容を確認、改善 -1回以上/年 ※別途、重大な変化が発生した場合には迅速に対応すること	【見直しの例】 ・会社規則に見直しについて規定している ・定期的にセキュリティ委員会で規定見直し状況を報告施している 【社内外の環境変化の例】 ・自社体制の変更 ・対象となる情報資産の変更 ・新たな脅威の検知・管理対象の変更時 ・情報セキュリティ事件・事故発生後
例えば	3法令遵守	会社として、情報セキュリティに関する法令を遵守する	情報セキュリティに関する法令を考慮し、社内ルールを策定すること (法令例：個人情報保護法、不正競争防止法)	9	Lv1	**情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している**	【規則】 ・情報セキュリティに関連する法令を守るための社内ルールを策定すること ・策定した社内ルールを教育・周知すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 （教育） ・新規受け入れ時、かつ、１回／年 （周知） ・定常的に、かつ、ルールの改正時に周知すること	【規則改定の例】 ・個人情報保護法、GDPR、不正競争防止法等の情報セキュリティに関する法令・規則の情報収集をを行い必要に応じ規則改定を行っている ・法令の変更内容がルールに則っているか関係部署で確認している（１回／年） ・策定したルールに、見直す頻度を記載している 【教育・周知の例】 ・策定したルールに、教育・周知頻度を織り込んでいる ・eラーニングで教育を実施している（年1回）

質問③

外部情報サービスが具体的に何を指すのか教えてください。
アプリケーションやクラウドサービス等の利用について、セキュリティ面の審査をどの様に実施すれば良いか、
また各社どの様にしているのか知りたい。

回答：
外部情報サービス・・・クラウドサービスを代表とする自社以外の情報サービスを指します。
その他、顧客・子会社・関係会社・外部委託先の情報サービスも外部情報サービスに該当します。

クラウドなどを利用する際のセキュリティ面の審査は下記の観点で実施するのがよいと思われます。

1．システム、事業者を選択する観点
・サービス提供事業者の情報セキュリティ方針と自社のセキュリティ方針の適合
・サービスの稼働率や障害発生頻度等の信頼性

2．運用する観点
・適切な利用者のみが利用できる認証設定の可否
・データのバックアップ取得可否

3．管理する観点
・セキュリティ対策や機能の有無
・データ保存先や保存期間の確認

＜参考資料＞　チェックシートと解説がセットになっており利用しやすいです。
中小企業のためのクラウドサービス安全利用の手引き (ipa.go.jp)

質問④（1/2）

従業員へのセキュリティ教育実施の施策について教えてください。また、以下の点について具体的に教えてください。
・電子メール機能やWebブラウザ利用及び事故事例の教育で、利用者がより関心を持ってくれるコンテンツを紹介頂きたい。
・自社環境でも影響が大きい注意喚起事例を、負担少なくタイムリーに社内共有する方法を知りたい。

回答：
①従業員へのセキュリティ教育実施の施策について教えてください。
自動車産業 セキュリティチェックシートの対象「教育・啓発」の項目（No.28～37）を実施されると良いと考えます。

分類	ラベル	目的	要求事項	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当 (回答者検討
	7日常の教育	マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する	従業員として注意することを教育していること	28	Lv1	電子メールのマルウェア感染に関する社内への教育を行っている	【規則】 ・電子メールによるマルウェア感染の予防について、教育資料配布・掲示、eラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等）における メール利用者 【頻度】 ・新規受け入れ時、かつ、1回／年以上	【教育の例】 ・新入社員教育・中途入社教育・社外要員受け入れ集合教育等 ・eラーニングによる教育 ・自社、IPAやセキュリティベンダー等の提供する映像教育コンテンツの視聴 ・自社、IPAやセキュリティベンダー等の提供する教育資料の配布・掲示 ・利用マニュアル等による電子メール利用のリスクと対処法等の解説 ・標的型メール訓練の実施とその解説 【教育頻度の例】 ・新入社員・中途社員・社外要員受け入れ時 ・1回／年 eラーニング による教育を実施 ・1回／年 更新内容を中心とした教育資料・マニュアル等の再確認の通知 ・1回／年 標的型メール訓練を実施	教育・啓発	情報セキュリティ／IT
				29	Lv1	インターネットへの接続に関する社内への教育を行っている	【規則】 ・Web閲覧によるマルウェア感染の予防について、教育資料配布・掲示、eラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等）における インターネット利用者 【頻度】 ・新規受け入れ時、かつ、1回／年以上	【教育の例】 ・新入社員教育・中途入社教育・社外要員受け入れ集合教育等 ・eラーニングによる教育 ・自社、IPAやセキュリティベンダー等の提供する映像教育コンテンツの視聴 ・自社、IPAやセキュリティベンダー等の提供する教育資料の配布・掲示 【教育頻度の例】 ・新入社員・中途社員・社外要員受け入れ時 ・1回／年 eラーニング による教育を実施 ・1回／年 更新内容を中心とした教育資料・マニュアル等の再確認の通知	教育・啓発	情報セキュリティ／IT
				30	Lv1	機密区分に応じた情報の取り扱いに関する教育を行っている	【規則】 ・機密区分の定義と取り扱いについて、教育資料配布・掲示、eラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等）	【教育の例】 ・新入社員教育・中途入社教育・社外要員受け入れ集合教育等 ・eラーニングによる教育 ・自社、IPAやセキュリティベンダー等の提供する映像教育コンテンツの視聴 ・自社、IPAやセキュリティベンダー等の提供する教育資料の配布・掲示 【教育頻度の例】 ・新入社員・中途社員・社外要員受け入れ時	教育・啓発	情報セキュリティ

質問④（2/2）

従業員へのセキュリティ教育実施の施策について教えてください。また、以下の点について具体的に教えてください。
・電子メール機能やWebブラウザ利用及び事故事例の教育で、利用者がより関心を持ってくれるコンテンツを紹介頂きたい。
・自社環境でも影響が大きい注意喚起事例を、負担少なくタイムリーに社内共有する方法を知りたい。

回答：

②電子メール機能やWebブラウザ利用及び事故事例の教育で、利用者がより関心を持ってくれるコンテンツを紹介頂きたい。

情報セキュリティ対策は、IPAから体系的に情報発信（無料）されていますので活用を推奨します。

・ビジネスメール詐欺のパターン、対策、啓発資料等
　ビジネスメール詐欺（BEC）対策特設ページ | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
・Webブラウザ利用含む情報セキュリティに関するさまざまテーマをピックアップして紹介
　安心相談窓口だより | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
・情報セキュリティ各種教材・ツールを掲載
　情報セキュリティ教材・ツール | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
・ランサムウェア攻撃や身近な攻撃の手口を紹介
　映像コンテンツ一覧 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

③自社環境でも影響が大きい注意喚起事例を、負担少なくタイムリーに社内共有する方法を知りたい。

・重要なセキュリティ情報、脆弱性対策情報、情報セキュリティ10大脅威など身近で重要な情報を提供
　情報セキュリティ | IPA 独立行政法人 情報処理推進機構
　重要なセキュリティ情報 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

質問⑤

自社でサイバー対策についての知識が薄く勉強しながらの状況です。知識のレベルアップ方法を教えてください。

回答：

セキュリティ知識レベルアップの方法は、下記のパターンがありそうです。

a) 独学で勉強
b) 外部ベンダーの力をお借りし、任せる
c) 外部ベンダーの力を借りるが、OJTにより自身のセキュリティ知識をレベルアップ

経験上、IPAの「情報セキュリティマネジメント試験」の資格取得にチャレンジいただくことも、取り掛かりの勉強として良いと思います。 https://www.ipa.go.jp/shiken/kubun/sg/index.html

また、独学で勉強される場合は、下記の様な教材もIPAから提供されています。

a) 5分でできる！情報セキュリティポイント学習(IPA)

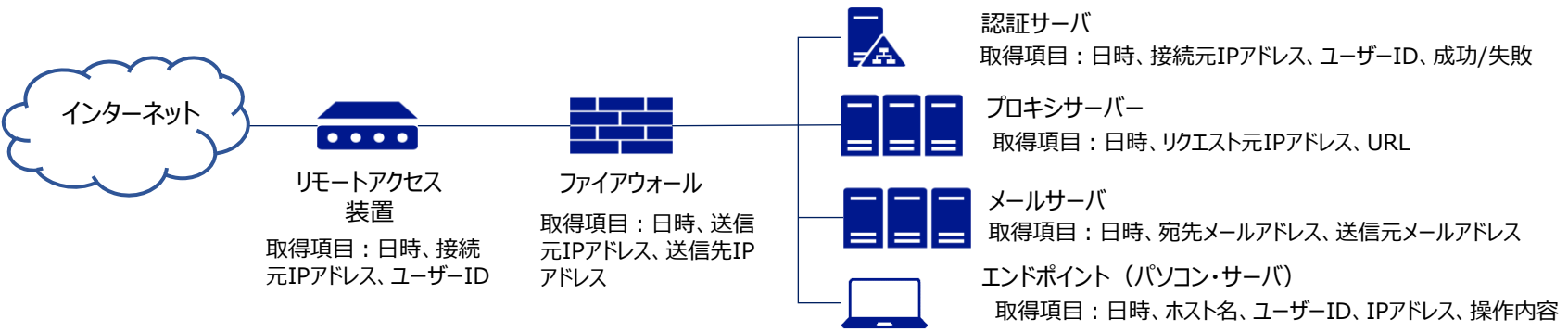
b)教育・学習（企業・組織向け）｜ここからセキュリティ！(IPA)

c) みんなのサイバーセキュリティコミック (JNSA)

質問⑥

【ガイドライン】No.17,24,50,53 各種ログに対する対処方法をどのようにされているのかをお聞きしたいです。
・専門担当者がおらず、保存場所や機能が異なるデバイスに対して、ログの収集から分析まで、
どの様にすれば良いか教えてください。

回答：
第一歩としては下記のようなログをマニュアルで取得することが考えられます。



No.	レベル	達成条件	達成基準
17	Lv2	**サイバー攻撃や予兆を監視・分析をする体制を整備している**	【規則】 ・サイバー攻撃や脆弱性に関する公開情報、非公開情報を活用する体制を構築している ・相関分析によりサイバー攻撃や予兆の検知を可能とし、その分析結果から適切な対応が導きだせる体制を構築している ※相関分析： 複合的なログなどで分析して情報セキュリティ事件・事故の予兆や痕跡を見つけ出す手法
24	Lv1	**情報セキュリティ事件・事故時の対応手順(初動、システム復旧等)を定めている**	【規則】 ・対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告
50	Lv2	**人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている**	【規則】 ・重要情報を扱うシステムは、アクセス権を付与するための条件を明確にする ・アクセス権の設定は、システム管理者の要件および設定手順を明確にし、厳格な管理下で実施する。 ・重要情報を扱うシステムは、情報利用者とシステム管理者の権限を分離するなど、個人に権限が集中しない環境とする。 ・重要情報を扱うシステムは、その運用／利用状況を監視する。
53	Lv2	**アクセスログは、安全に保管しアクセス制御された状態で管理されている**	【規則】 ・法規制等により要求される事項を満たす事ができるよう、適切な期間のログを保持する。 ・ログを脅威から保護するため、ログを保存するモノ、システムにアクセス制御等を適用すること

様々なネットワーク・セキュリティ機器からあげられるログ情報は多岐に渡るため、関連性を横断的に分析することができるSIEM（System Information and Event Management）と呼ばれる総合ログ管理の製品やサービスを導入する方法もあります。

ログ情報の分析においては、自社で体制を構築することも可能ですが、監視・分析体制を提供しているベンダーのサービスを活用する方法があります。
＜参考＞サイバーセキュリティお助け隊サービス ユーザー向けサイト | IPA

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＞

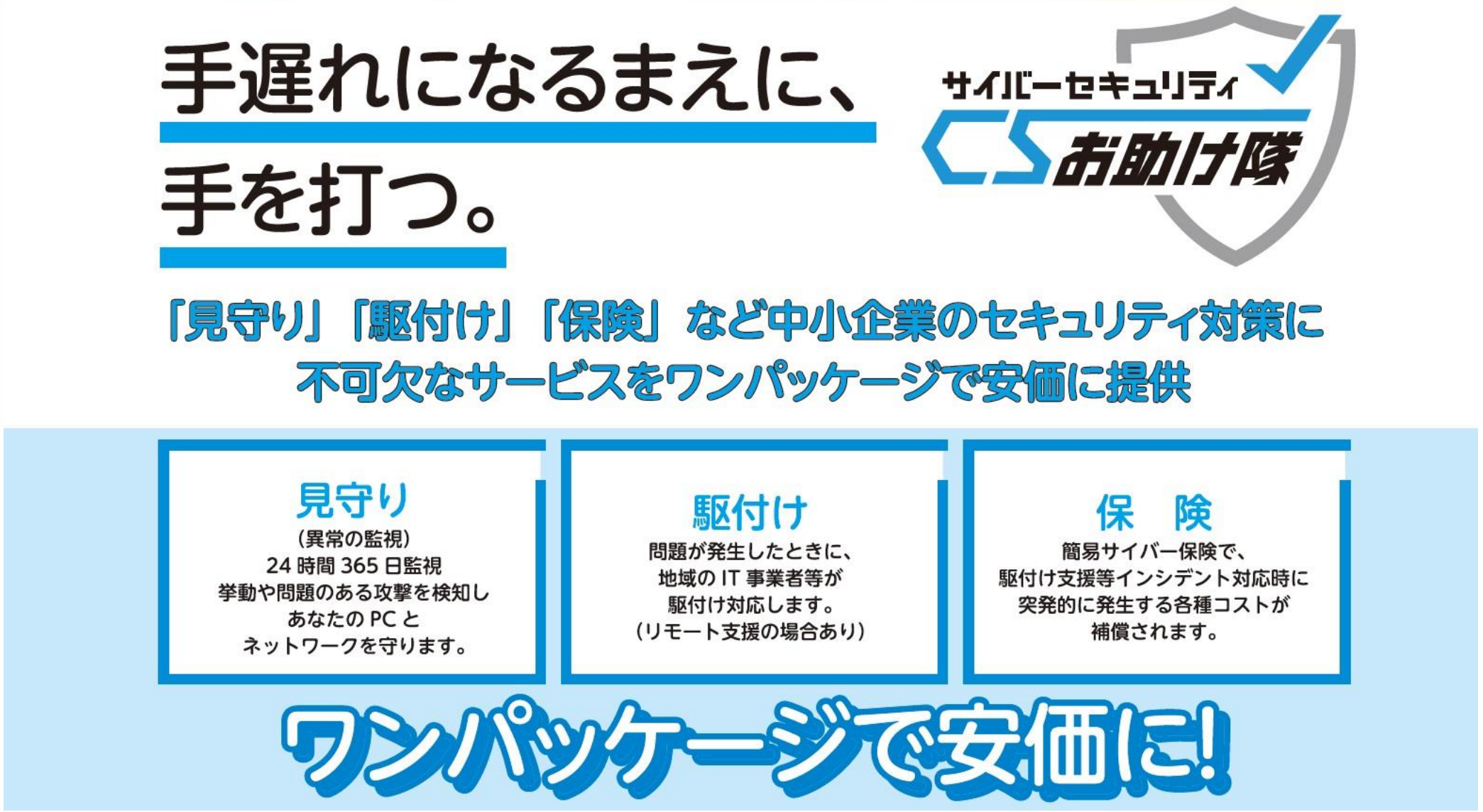
JC-STAR

- 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**

IPA ・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 → 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

➢ 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）

E N D