資料２

SC3 第9回中小企業対策強化WG
事務局説明資料

２０２３年2月２０日
SC3事務局

議題１．業界ガイドライン等の共通項抽出について

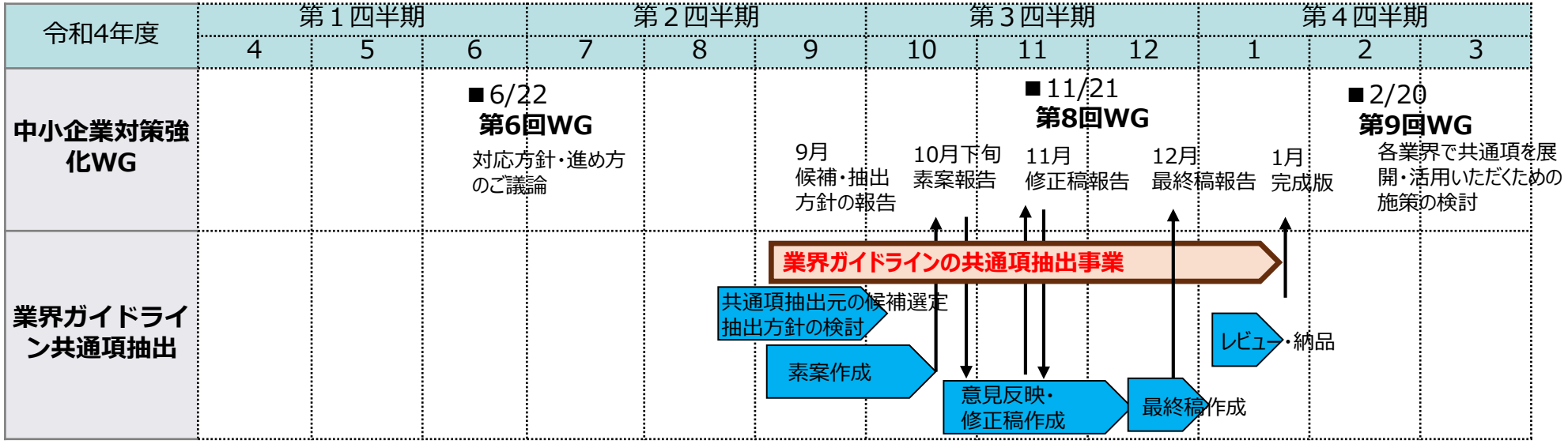
議題２．お助け隊サービス制度について

【参考】業界ガイドライン等の共通項抽出の対応方針とスケジュール

第6回中小WG資料を改版

検討事項	対応方針（案）
議題	共通項の元とすべきガイドライン等の検討した上で、共通項を抽出・整理する。
検討スキーム	6月22日　①第6回中小WGにて対応方針・進め方について確認 7月～　②SC3会員に業界ガイドラインの有無確認及び提供依頼 共通項抽出元候補選定、抽出方針の検討 9月　③候補・抽出方針の報告（メールベースでご意見を頂く） 10月下旬　④ガイドライン候補、抽出方針を元に共通項の素案を作成、委員に報告 11月21日　⑤**第8回中小WG**にてご意見照会 11月初旬～⑥頂戴したご意見を修正稿に反映（メールベースでご意見を頂く）複数回 12月末　⑦最終稿の確認 2月20日　⑧**第9回中小WG**で各業界でガイドラインの共通項を展開・活用いただくための施策の検討【今回】

スケジュール（修正）



共通項抽出結果のご報告①（共通項抽出の判断基準）

3．抽出結果

- 抽出結果に基づき、チェック項目ごとの記載傾向を確認し、共通項の抽出を行うため、チェック項目別のスコアの平均点を算出した。
- 今回、**①チェック項目別のスコアの平均点が「１」を超えるチェック項目**、もしくは、**②記載が確認できたガイドラインが半数以上（７つのガイドライン以上）のチェック項目**を、共通項として抽出することとした。

【（例）チェック項目：サイバーセキュリティリスクの認識、組織全体での対応方針の策定】

ガイドライン	抽出結果
自工会部工会・サイバーセキュリティガイドライン2.0版	○
ネットワーク機能付き事務機セキュリティガイドラインVer.1.00	－
通信ネットワーク機器セキュリティユーザーガイドラインVer. 2.0	－
制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）	－
スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	－
鉄道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	○
装備品等及び役務の調達における情報セキュリティ基準	○
ビル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第1版	○
電力制御システムセキュリティガイドライン JEAG 1111-2019	◎
スマートメーターシステムセキュリテ	◎
元請け会社における情報セキュリ	－
建設現場における情報セキュリテ	○
医療情報システムの安全管理に関するガイドライン 第5.2版	－
本チェック項目におけるスコアの平均点	**0.69**
記載を確認したガイドライン数	**7**

以下の場合に共通項として抽出する。
①：チェック項目別のスコアの平均点が「１」を超えた項目
②：①に該当しないものの記載が確認できたガイドラインが半数以上（７つのガイドライン以上）の項目

共通項抽出結果のご報告②（共通項として抽出した項目）

3．抽出結果

- **各ガイドラインのチェック項目別に、前述の評価基準をもとに評価を行い、抽出対象としたガイドラインにて記載が充実している項目、記載が多い項目について、共通項として抽出した。**
- **共通項として抽出されたチェック項目は以下のとおりである（赤字のチェック項目が共通項に該当）。**

カテゴリ	チェック項目	①チェック項目ごとの平均点が「１」を超えた項目	①に該当しないものの記載が確認できたガイドラインが半数以上の項目
①サイバーセキュリティリスクの認識、組織全体での対応方針の策定	(1)経営者のリスク認識	－	○
	(2)経営者によるセキュリティポリシーの策定・宣言	○	－
	(3)法律・業界ガイドラインの把握	－	○
②サイバーセキュリティリスク管理体制の構築	(1)サイバーセキュリティリスク管理体制の構築	○	－
	(2)関係者の役割と責任の明確化	○	－
	(3)リスク管理体制とサイバーセキュリティリスク管理体制の明確な規定	－	－
③サイバーセキュリティ対策のための資源（予算、人材等）確保	(1)対策の明確化・費用評価・予算確保	－	－
	(2)人材の確保、役割の理解	－	○
	(3)組織内の人材育成	－	－
	(4)セキュリティ人材のキャリアパス・待遇の設定	－	－
	(5)継続的なセキュリティ対策の実施	－	－
④サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	(1)情報資産の優先順位付け	－	－
	(2)経営戦略を踏まえたリスクの把握	－	○
	(3)リスクが事業にも足たらす影響の推計	－	－
	(4)リスク対応計画の策定	－	○
	(5)残留リスクの識別	－	－
⑤サイバーセキュリティリスクに対応するための仕組みの構築	(1)重要端末への多層防御の実施	○	－
	(2)脆弱性診断の実施・対応	○	－
	(3)検知すべきイベントの特定・迅速な検知のための体制構築	○	－
	(4)意図しないイベントへの対応計画の策定	－	－
	(5)サイバーセキュリティリスクへの対応内容の見直し	○	－
	(6)従業員に対する教育の実施	○	－

共通項抽出結果のご報告③（共通項として抽出した項目）

3．抽出結果

■ 前頁続き。

カテゴリ	チェック項目	①チェック項目ごとの平均点が「１」を超えた項目	①に該当しないものの記載が確認できたガイドラインが半数以上の項目
⑥サイバーセキュリティ対策におけるPDCA サイクルの実施	(1)経営者への対策状況の報告	－	－
	(2)外部監査の実施	－	－
	(3)環境変化に応じたPDCAの整備	－	－
	(4)リスクと取組状況の外部への公開	－	－
⑦インシデント発生時の緊急対応体制の整備	(1)組織内外の連絡先の整備	－	－
	(2)初動対応マニュアルの整備	－	○
	(3)インシデント対応専門チームの設置	－	－
	(4)経営者への報告ルート・公開内容等の設定	－	－
	(5)初動対応マニュアルの見直し	－	－
	(6)定期的な対応訓練の実施	－	－
⑧インシデントによる被害に備えた復旧体制の整備	(1)業務の復旧計画の策定	－	○
	(2)復旧計画の見直し	－	－
	(3)組織内外の連絡先の整備	－	－
	(4)定期的な対応訓練の実施	－	－
⑨ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	(1)システム管理の適切な委託の実施	－	－
	(2)委託先に実施を求めるセキュリティ対策の明確化	－	○
	(3)サプライチェーンのセキュリティ対策状況の把握	－	－
⑩情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	(1)業界団体を通じた情報共有の実施	－	－
	(2)関係団体への情報提供の実施	－	－

【1.業界ガイドライン等の共通項抽出について】

共通項抽出結果のご報告④（共通項の記載例）

- 共通項として抽出された項目について、各ガイドラインで記載されていた内容を整理し、段階別に記載例を整理。

ガイドライン未整備の業界における参考に

■ 共通項として抽出された項目について、各ガイドライン内で記載されていた内容例の一部を整理した。**記載内容が少ない水準の記載例を「第１段階」、記載が具体的であり望ましいと考えられる水準の記載例を「第２段階」、とレベル別に整理**している。

■ また、**サイバーセキュリティお助け隊サービスを用いることで対応が可能な項目についても個別に記載**した。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
サイバーセキュリティリスクの認識、組織全体での対応方針の策定	経営者のリスク認識	【第１段階】 （装備品等及び役務の調達における情報セキュリティ基準） ● 経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て、情報セキュリティ基本方針等の承認等を通して、自社における情報セキュリティの確保に努めるものとする。 【第２段階】 （電力制御システムセキュリティガイドライン） ● 経営層は、電力制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、電力制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、電気事業者が重要インフラとしての社会的責任を果たすためのセキュリティ対策が実行されない可能性がある。	本項目については、サイバーセキュリティお助け隊サービスを用いることにより24時間365日、挙動や問題のある攻撃を検知することが可能となる。
	経営者によるセキュリティポリシーの策定・宣言	【第１段階】 （元請け会社における情報セキュリティガイドライン） ● 情報セキュリティ対策として各項目の具体的な手順やルールを定めます。従業員および協力会社を含めた現場構成員に周知します。定期的に手順・ルールの見直しを行い、変更した場合はその都度、現場構成員に周知することも必要です。 【第２段階】 （電力制御システムセキュリティガイドライン） ● 経営層は、電力制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、電力制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、電気事業者が重要インフラとしての社会的責任を果たすためのセキュリティ対策が実行されない可能性がある。	－
	法律・業界ガイドラインの把握	【第２段階】 （鉄道分野における情報セキュリティ確保に係るガイドライン） ● 「安全ガイドライン」の形態 各重要インフラ事業者等は、当該事業分野に関する法制度の下、関係する基準に従い、業を営んでいる。 このことを踏まえ、「指針」においては、各重要インフラ事業者等の判断や行為に関する基準又は参考となる文書類を「安全基準等」と呼び、次の①～④に分類している。 ①関係法令に基づき国が定める「強制基準」 ②関係法令に準じて国が定める「推奨基準」及び「ガイドライン」 ③関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」 ④関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等 本ガイドラインは②に対応し、国が定める「ガイドライン」として推奨事項を列挙しているものであり、事業分野の特性に鑑み、重要インフラ事業者等が自らの情報セキュリティ対策を実施する際に参考資料として活用することを想定している。	－

【1.業界ガイドライン等の共通項抽出について】

共通項抽出結果のご報告⑤（共通項のチェックシート）

- 記載例に加えて、業界ガイドラインから得られた共通項について、対処できているかどうかを確認するためのチェックリストを別紙として取りまとめた。

【チェックシートイメージ】

カテゴリ	共通項として抽出されたチェック項目	チェックの視点	対応状況
サイバーセキュリティリスクの認識、組織全体での対応方針の策定	経営者のリスク認識	【第１段階】※達成していれば「○」 経営者がサイバーセキュリティリスクを認識している。 【第２段階】※達成していれば「◎」 認識したうえで、以下のような具体的な関与を行っている。 ① 経営者自身の責任の明確化。 ② 情報セキュリティの責任に関する方向性の検討。 ③ 自社のセキュリティ基本方針等の承認の実施	
	経営者によるセキュリティポリシーの策定・宣言	【第１段階】※達成していれば「○」 セキュリティポリシーを策定し、宣言している。 【第２段階】※達成していれば「◎」 セキュリティポリシーに以下のような視点が含まれているか。 ① 情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかについて、自社に適した情報セキュリティに関する基本方針を定めている。 ② 自社の経営において最も懸念される事態は何かを明確にしている。	
	法律・業界ガイドラインの把握	【第１段階】※達成していれば「○」 法律・業界ガイドラインについて把握している。 【第２段階】※達成していれば「◎」 法律・業界ガイドライン把握するにあたり、以下のような前提・認識を有している。 ① 情報技術の進化の早さゆえに実施を検討するべき対策は目まぐるしく変化するため、自社だけで把握することは困難であることから、情報セキュリティに関する最新動向を発信している公的機関などを把握し、常時参照することで備えるように情報セキュリティ担当者に指示を行っている。 ② 知り合いやコミュニティへの参加を通じ情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有することとなっている。	

		③ 組織の対応方針（セキュリティポリシー）に基づいたCISO等からなるサイバーセキュリティリスク管理体制を構築されている。 ② 情報セキュリティ上の事故などが発生した場合も含め、情報セキュリティ責任者から部門責任者を通じた従業員への情報の伝達経路を確立している。 ③ 既存の個人情報保護管理体制（特定個人情報事務取扱担当者、個人情報苦情申出先）等の管理体制との整合が取れている。	
	関係者の役割と責任の明確化	【第１段階】※達成していれば「○」 情報セキュリティに関わる関係者の役割と責任を明確化している。 【第２段階】※達成していれば「◎」 以下のように、役割に応じた情報の伝達方法が確立している。 ① 関係者の選定にあたっては、法的な義務を順守し、システム運用を担うにあたり適当な能力を有する者を選定している。 ② 情報セキュリティ上の事故などが発生した場合に、情報セキュリティの責任者へ状況が迅速に報告されるような連絡体制を整備している。	
サイバーセキュリティ対策のための資源（予算、人材等）確保	人材の確保、役割の理解	【第１段階】※達成していれば「○」 サイバーセキュリティを担う人材の確保に努めている。 【第２段階】※達成していれば「◎」 以下のような視点で人材確保を行っているか。 ① 複数の対策が必要という前提を持っている。 ② 実効性の観点から継続的な人材育成・配置を考慮している。 ③ 全社的なスキルアップに取り組んでいる。 ④	
サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	経営戦略を踏まえたリスクの把握	【第１段階】※達成していれば「○」 経営戦略を踏まえたサイバーセキュリティリスクの把握を実施している。 【第２段階】※達成していれば「◎」 以下のような観点でリスクを把握しているか。 ① 重要度の高い情報資産を把握している。 ② 有事の際の影響の程度の把握を実施している。 ③ サイバーセキュリティに係る事案から派生して生じる事象の把握を実施している。	
	リスク対応計画の策定	【第１段階】※達成していれば「○」 リスクへの対応計画を策定している。 【第２段階】※達成していれば「◎」 以下のような観点が計画に含まれているか。 ① リスクに備えた対処準備。 ② リスク発生時の報告・連絡方法	

共通項抽出結果のご報告⑥（抽出結果）

- 業界ガイドラインを策定されている業界へのフィードバックを行っていただけるよう各ガイドライン毎の得点を別紙(Excel）として取りまとめた。

（別紙） 共通項抽出結果詳細
チェック項目に基づき、各ガイドライン内の記載を確認した結果を記載する。また、チェック項目ごとにNISTが提供するサイバーセキュリティフレームワークとの対応関係も合わせて提示する。

抽出軸		NISTフレームワーク対応	共通項判断		自工会部工会・サイバーセキュリティガイドライン 2.0 版
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	記載有無
サイバーセキュリティリスクの認識、組織全体での対応方針の策定	経営者のリスク認識	(−)	0.69	7	1
	経営者によるセキュリティポリシーの策定・宣言	(ID.GV−1)	1.15	9	2
	法律・業界ガイドラインの把握	(ID−GV−3) (DE.DP−2)	1.00	7	2
	その他		0.00	0	0
サイバーセキュリティリスク管理体制の構築	サイバーセキュリティリスク管理体制の構築	(−)	1.23	9	2
	関係者の役割と責任の明確化	(ID.GV−2)	1.23	10	2
	リスク管理体制とサイバーセキュリティリスク管理体制の明確な規定	(ID−GV−4)	0.62	5	1
	その他		0.00	0	0
サイバーセキュリティ対策のための資源（予算、人材等）確保	対策の明確化・費用評価・予算確保	(−)	0.38	4	1
	人材の確保、役割の理解	(PR.AT−2) (PR.AT−3) (PR.AT−4) (PR.AT−5)	0.92	8	2
	組織内の人材育成	(PR.AT−1)	0.77	6	2
	セキュリティ人材のキャリアパス・待遇の設定	(−)	0.15	1	0
	継続的なセキュリティ対策の実施	(PR.AT−1)	0.62	6	1
	その他	(PR.AT−1)	0.00	0	0

ガイドラインを提供いただいた業界へのフィードバックに

共通項判断(オレンジ色)のスコアと比べて、低いチェック項目の見直しに

印刷可能なように、各業界ガイドライン毎のスコアのみをまとめた表も作成。

共通項抽出結果のご報告⑦（考察）

- 共通項の抽出結果を踏まえての考察として、共通項として抽出された項目や、ガイドライン内で記載の少ない項目、今後中小企業や業界に求められる対応について記載した。

４．考察

■ 共通項が抽出されたカテゴリについて

- カテゴリ別にみると、**「①サイバーセキュリティリスクの認識、組織全体での対応方針の策定」、「 ②サイバーセキュリティリスク管理体制の構築」、「④サイバーセキュリティ対策のための資源（予算、人材等）確保」「⑤サイバーセキュリティリスクに対応するための仕組みの構築」、「⑦インシデント発生時の緊急対応体制の整備」、「⑧インシデントによる被害に備えた復旧体制の整備」、「⑨ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」について、共通項として抽出されたチェック項目が存在した。**
- 特に、**「①サイバーセキュリティリスクの認識、組織全体での対応方針の策定」、「⑤サイバーセキュリティリスクに対応するための仕組みの構築」については抽出された共通項が多く、重要性の高いカテゴリとして認知されている傾向がある**と考えられる。

■ インシデント発生時の対応や復旧フェーズにおける記載が少ない。

- セキュリティに対する認識や体制構築に対する項目と比較すると、**インシデント発生時の対応や復旧体制にかかる記載が少ない傾向がみられた。**
- **今回、分析対象とした既存の業界ガイドラインにおいて、被害に遭うことを前提とした記載が少ないことは課題**といえる。たとえば、IPAが実施する既存調査で得られた事例集等も活用しつつ、業界ガイドライン内に、中小企業における被害事例を盛り込んでいただくよう働きかけ、業界団体や、業界ガイドラインの読み手に対して、情報セキュリティ被害が起こりえるものであるという認識を持っていただくことも有益ではないか。

【1.業界ガイドライン等の共通項抽出について】

共通項抽出結果を展開・活用いただくための施策検討（案）

- 前回（第8回中小WG）でもご意見いただいた通り、共通項抽出のアウトプットを展開しただけで未整備の業界へ展開・活用いただくのは正直難しい。
- 未整備の業界への活用いただくための施策として、**ガイドライン未整備**の**業界**で関心のある**団体**を選定し、**策定支援**を行い、その結果として手引きやチェックシートの作成等を行い、活用を促進するためのモデルケースを作りたいと考えるがいかがか。(異論なければ、令和5年度IPA調査事業として実施)
- 他方、共通項抽出結果について「**中小企業ガイドライン**※1」**へ反映**も行う。

【ガイドライン未整備の業界団体への策定支援事業（イメージ）】

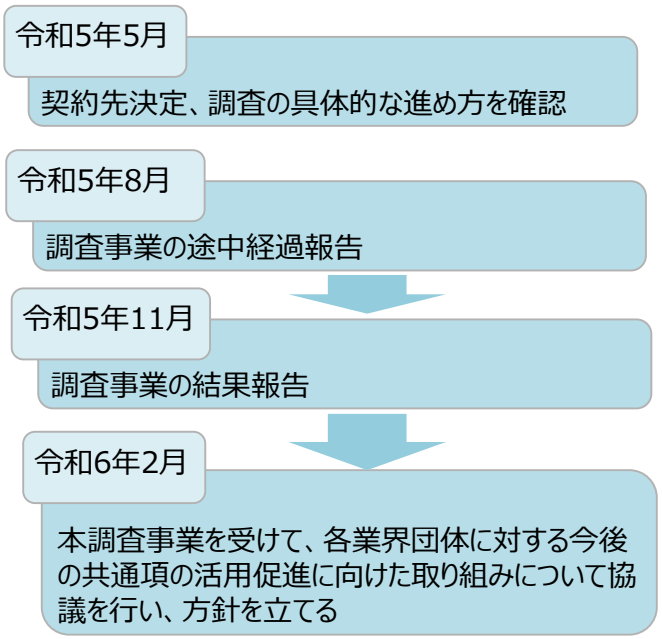
■目的
- ガイドライン未整備の業界が主体的に活用を促進するためのモデルケース作り

■調査内容

1．業界団体との連携による実証調査
  - SC3に加入する業界団体から、ガイドライン未整備で策定に関心のある３団体を選定し、当該業界団体に対してガイドライン策定委員会の実施支援や専門家による助言等による実証調査を行う。

2．調査結果の活用
  - 中小企業ガイドラインの改訂に向けた提言
  - 実証調査の結果をもとにしたガイドライン共通項を業界団体で活用促進するための手引きやチェックシート作成等

【スケジュールイメージ】



※1:「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

議題１．業界ガイドライン等の共通項抽出について

議題２．お助け隊サービス制度について

【2. お助け隊サービス制度について】

第４回お助け隊サービス事業者連絡会の報告

- 今年度最後の**第４回お助け隊サービス事業者連絡会**を1月26日(木)に実施。
- 今回の開催は、事業者間の交流ではなく、前回の中小WGでご議論いただいた「お助け隊サービスの普及に向けた取組」等についてご意見・ご要望をお伺いした。

＜第４回お助け隊サービス事業者連絡会開催要領＞

項目	内容
日時	2023年1月26日（木）16:00-17:30（オンライン）
対象	既登録サービス事業者（現状、２４事業者）
アジェンダ	1. お助け隊サービス制度の運用状況 2. お助け隊サービスの普及に向けた取組みについて （１）広報活動報告 （２）PRサイトの改修について 3. お助け隊制度検討委員会について 4. 情報共有の高度化について 5. R5年度お助け隊審査（更新審査）スケジュールについて 6. 経済産業省からの情報共有 7. 次回以降の事業者連絡会の開催について
その他	**今後のスケジュール（予定）：** ・2023年5月：第５回事業者連絡会（オンライン開催） ・2022年9月：第６回事業者連絡会（リアル開催）

【サービス事業者の主なご意見概要】

（お助け隊サービスの広報活動について）

- 申込者の内訳を確認すると、IPAの**PRサイトからの訪問者が一番多く、IPAの広報は有効。**
- 地域別の検索を新たに加えることは、見やすくて非常によい。

（情報共有の高度化について）

- インシデントの発生状況やその対応を把握できるのは助かるが、インシデントとなると抵抗もあるので取り扱いには注意が必要だと思うがどう考えているののか？→会社名など特定ができる情報は匿名化するのは当然として、センシティブに取り扱わなければならないものであると十分理解している。
- マルウェアに感染している状況など地域別に感染することもあるため、そういう情報を共有いただけると非常に助かる。（営業展開の一つとしての活用の期待も）

事業者の数が増え、双方向の情報発信や事業者同士の意見交換が難しくなってきたため、これまでの開催にとらわれず、開催形式や回数の見直しを今後検討。

お助け隊サービス広報活動報告①

- 経営層などビジネスユーザーが主たる読者である新聞等に広告を掲載し、対策を怠ることによって想定される被害や、中小企業に例外なく攻撃されている等の事例と合わせ、安価で対策可能なお助け隊サービスを訴求した。

掲載期間、掲載新聞及び掲載サイズ

- 11月7日（月）~12月6日（火）の期間
- 日経産業新聞：全5段2回、半5段3回
- 日刊工業新聞：全5段2回、半5段3回
- 会議所ニュース（日商）：全5段1回

全5段Aパターン

お助け隊サービス広報活動報告②

全5段Bパターン

半5段A,Bパターン

お助け隊サービスPRサイトの改善案①

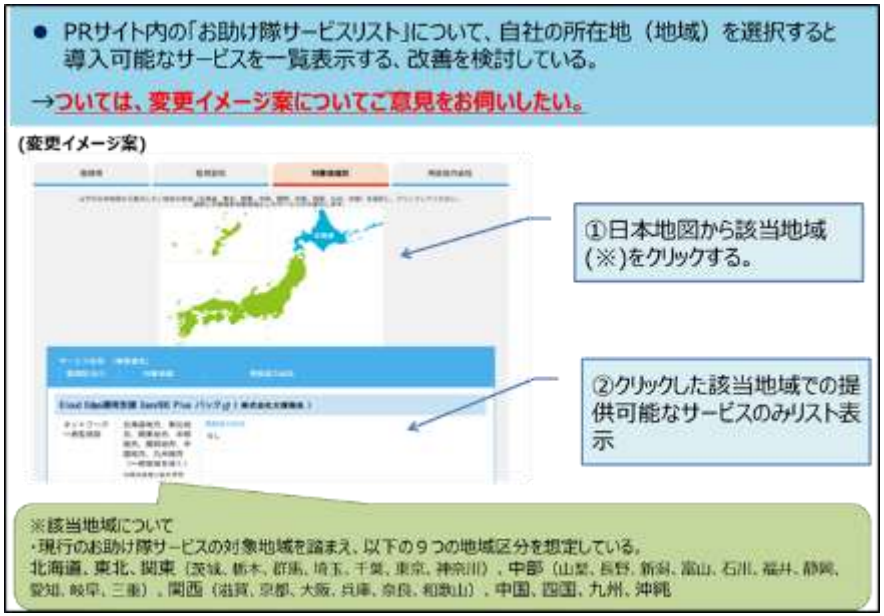
- 前回（第8回中小WG）で頂戴したご意見を踏まえ、改善案の検討及び事業者連絡会（前述）にて情報提供のお願いとご要望・ご意見をお伺いした。

（第8回中小WGで頂戴したご意見）

- 自社の所在地を選択すると、導入可能なお助け隊サービスが一覧表示されるとよい。
- サービス内容（具体的にどのようなことをしてくれるか）についてより具体的なものが分かると普及促進に繋がるのではないか。
- お助け隊サービスの普及の肝は、導入したことによって守られた・助かったなどの事例の積み重ねであり、事例を収集し、アナウンスすべき。

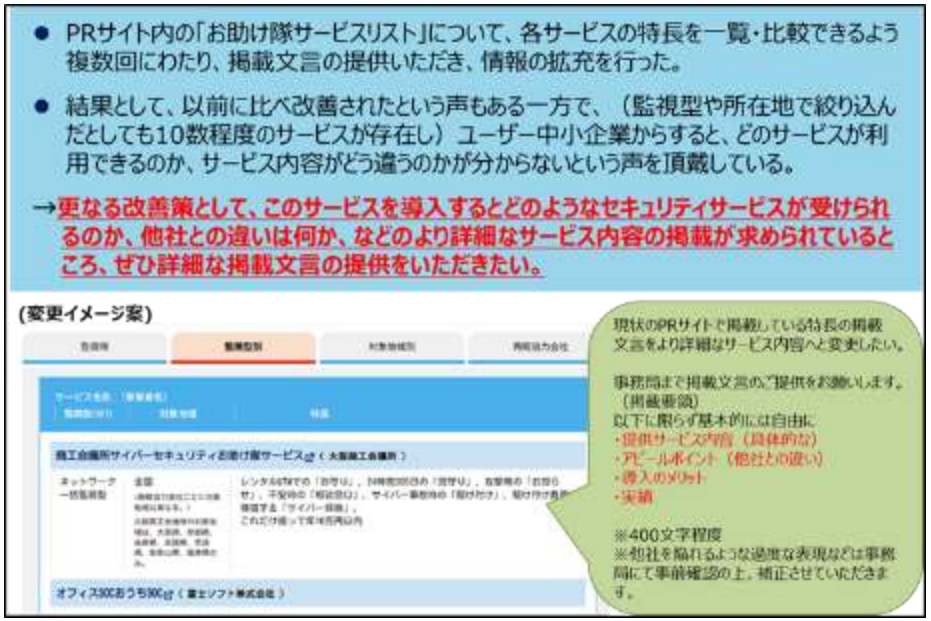
■ 対象地域選択

事業者連絡会配布資料抜粋



■ サービス内容の明確化

事業者連絡会配布資料抜粋



お助け隊サービスPRサイトの改善案②

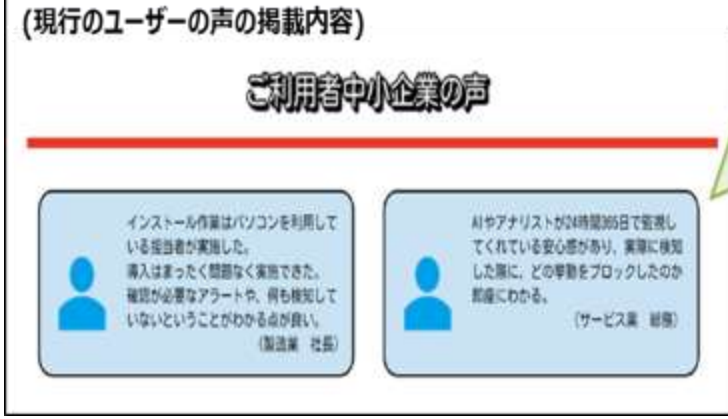
■ ユーザー中小企業の声の拡充

事業者連絡会配布資料抜粋

- PRサイト上、お助け隊登録事業者様から提供いただいた情報を元に、ユーザー中小企業の声として掲載。
- お助け隊サービスの導入数を増やすためには、やはり導入したことによって守られた・助かったなどという事例の積み重ねが大切であり、ユーザー中小企業の声の情報拡充を行いたい。

→**ユーザー中小企業の声やお助け隊サービス導入事例など、PRサイトに掲載可能な情報を提供いただきたい。**

(現行のユーザーの声の掲載内容)



(追加掲載情報案)

- 導入実績(導入したことによって守られた、良かった点などの事例)
- ユーザー中小企業の満足度(アンケートの集計結果)
  ⇒ユーザー中小企業に簡単なアンケートを実施していただき、その結果を掲載するなど。

情報提供をお願いしたところ、
1社から導入事例などの情報提供をいただけた。

やはり情報提供を呼びかけるだけではなかなか集まらないので、今後は、年2回の情報提供で入手している情報や、ウェビナーの開催での紹介したユーザー様の情報などを元にIPA側で原案を作成し、事業者に確認いただいた上で掲載するなどこちらから積極的なアプローチをしていきたい。

【情報共有】政府広報によるお助け隊サービスの紹介について

内閣府で、政府の重要施策を広く国民に知っていただくことを目的として行っている政府広報に「お助け隊サービス」が採用され、先月末に掲載されました。
■掲載期間：１月30日(月)～２月５日(日)
■掲載サイト名：Yahoo!ニュース
※スマホで「国内」及び「地域」タブに含まれる個別記事を開き、「記事全文を読む」をタップすると最上部に表示。

【2. お助け隊サービス制度について】

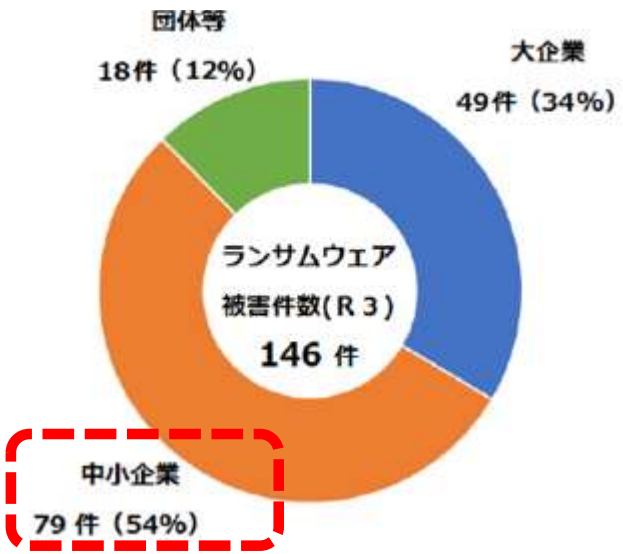
ランサムウェア脅威にさらされている中小企業の実態

- **ランサムウェアの被害は拡大**し、令和3年度においては**その半数が中小企業**であった。
- 中小企業であっても標的となる可能性が高く、お助け隊サービスとしてランサムウェア対策にどのような姿勢で取り組むかを検討いただきたい。

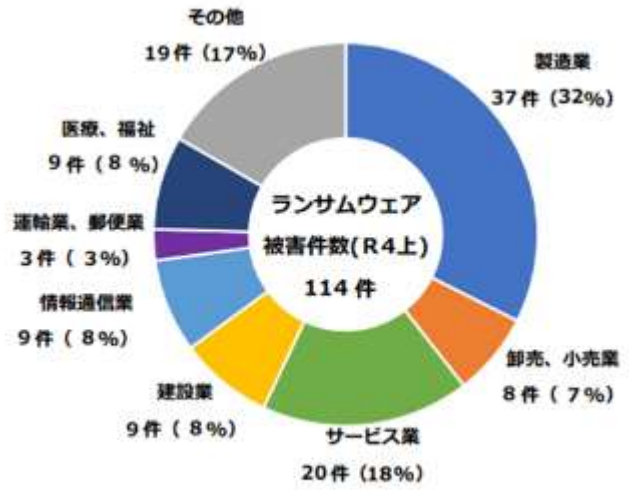
【参考資料】

- 令和3年中に警察庁に報告された国内のランサムウェアによる**被害件数は146件**で**中小企業がその半数以上（54%）**を占める。
- 様々な業界で被害が発生し、発注元、取引先企業への被害波及、攻撃の足掛かりとされる懸念

＜被害企業・団体等の規模別報告件数＞



ランサムウェア被害の被害企業・団体等の業種別報告件数



注　図中の割合は小数第1位以下を四捨五入しているため、総計が必ずしも100にならない。

【参考情報】【2. お助け隊サービス制度について】

ランサムウェア脅威にさらされている中小企業の実態

■お助け隊サービスで要求している技術要件

お助け隊サービス基準上は、**ランサムウェアの脅威対応を直接的には要求はしていない。**

異常の監視の形態としては、以下のどちらか、もしくはその両方を満たすよう求めている。

※ランサムウェア（マルウェア）対策を明確に求めてはいない。

（現状のお助け隊サービスの監視装置・サービスの仕様は次頁）

■ネットワーク一括監視型(第1章 2 (1))

- お助け隊サービスのうち，UTM（Unified Threat Management・統合脅威管理）等のネットワークセキュリティ監視装置を用いてユーザーのネットワーク通信の異常を監視する形態のものをいう。

■端末監視型(第1章 2 (2))

- お助け隊サービスのうち，EDR（Endpoint Detection and Response）等のエンドポイントセキュリティソフトウェアを用いてユーザーの端末内部の挙動の異常を監視する形態のものをいう。

異常監視サービスでの対策は求めていないものの、緊急時の対応支援により、対応可能と整理。

■緊急時の対応支援(第2章 1 (3))

- ユーザーと合意したサービス規約等に基づき，ユーザーから要請された場合， ユーザーの指定する場所に技術者を派遣することにより，緊急時の対応支援を行うこと（リモートによる対応支援が可能な場合には，リモートによる対応支援も可とする）。

■お助け隊サービスベンダーが提供している監視装置・サービスの仕様

監視機器			機能	ランサムウェア対策としての有効性
製造会社	Type	機器名		
NEC	UTM		・マルウェア対策、Webレピュテーション、不正侵入制御（IPS）	○
富士ソフト	SoC	-	・AIによる分析と専門技術者分析を実施して分析結果を定期的にインシデント通報としてお知らせ (目的の実行、C&C、デリバリー、エクスプロイト、偵察)	△(マルウェア配布サイトへの接続防止)
宝情報	UTM	Check Point	・ファイアウォール、IPS、アンチウイルス、アンチスパム、URLフィルターリング、アプリケーション制御、アンチボット、リモートVPN	○
トレンドマイクロ	UTM	Cloud Edge	・ウイルス対策、スパイウェア対策、ファイアウォール、URLフィルタリング、USB禁止設定	○
サクサ	UTM	HOME-UNIT／SS6000	・ファイアウォール、アンチウイルス、アンチスパム、Webフィルターリング、不正侵入検知／防御、リモートアクセスサービスを提供。	○
SOPHOS	UTM	XG86W	・ネットワークに潜むリスクを可視化、未知の脅威をブロック、インシデントに自動対処	○
	EDR	Intercept X Advanced with XDR	・ウイルス対策、マルウェア対策、ランサムウェア対策	○
チェック・ポイント・ソフトウェア	UTM	Quantum Spark1530	・UTMがC&C宛の通信を検知・ブロック・UTMから送信されるセキュリティログをチェックし、Anti Bot 検知を認識、メールで発報・ボット感染を検知し、遮断・インターネットの接続障害をリアルタイム通知	? (C&Cのみ)
キヤノンマーケティングジャパン	UTM	HOME-UNIT4L	・キヤノンからの月１回のレポート（どんな攻撃があったか等）を提供 ・悪意ある C＆C サーバーからの攻撃があった際には、キヤノンより直接電話にて連絡	? (C&Cのみ)
S&J	EDR	KeepEye	・端末上の振る舞いからマルウェアを検知する機能、端末上の振る舞いからマルウェアを防御・隔離する機能※オプション、AIを用いてマルウェアを検知する機能、AIを用いてマルウェアを防御・隔離する機能※オプション、	△ (検知のみ)
ウェブルート	EDR	Edge Xperience セキュリティ対策パック	・マルウェア対策、Web脅威対策、ファイアウォール、個人情報保護	○
セキュアイノベーション	簡易EDR	EISS	・ウイルス感染の可能性を早期 発見に特化し、悪意的に行うアクションや挙動を検知。 ・検知したウイルスの駆除はリモート操作や駆け付け駆除。	△ (検知のみ)
CyCraft	EDR	AI型EDRサービス	・ランサムソフトウェアをリアルタイムで遮断、解析、通報	○
NTT西日本	EDR	セキュリティおまかせプラン	・ウイルス対策、スパイウェア対策、ファイアウォール、URLフィルタリング、USB禁止設定	○
Blue Planet-works	EDR	AppGuard	・マルウェア対策、レガシーOS保護、閉域環境内の端末保護、特定端末の保護	○
ウィズセキュア	EDR	WithSecure Elements EDR／Elements EPP	・ランサムウェアや未知のマルウェアによるゼロデイ脆弱性の侵害の自律的な保護、未知の脅威やエクスプロイトに対抗、パッチ管理を完全自動化し、セキュリティパッチがリリースされた際にすぐに適用。	○
三井物産セキュアディレクション	EDR		・PC毎のネットワーク通信を監視し、標的型攻撃等により感染したPCが情報漏えいや、悪意あるサイトへの誘導、不正なファイルのダウンロードをブロックします。尚且つブロックのもとになったPCを特定し隔離。（マルウェア感染が要因と考えられるサイトへの接続PCを自動隔離し、マルウェア感染源の封じこめ及び横展開防止）	△ (不正サイトへの接続防止)
FFRIセキュリティ	EDR	FFRI yarai Cloud	・マルウェア対策	○