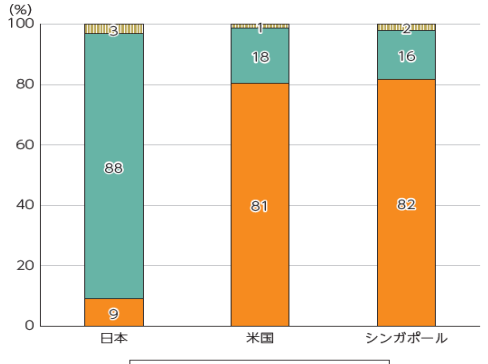
1. 新規事業の必要性 【中小企業のサイバーセキュリティ対策継続支援事業（仮称）】

（1）中小企業の現状（総論）

①日本企業は諸外国に比べ、セキュリティ人材が不足

・セキュリティ対策に従事する人材の充足状況については、米国及びシンガポールの8割以上の企業が充足していると回答したのに対し、約9割の日本企業は不足していると回答

図表 3-4-5-7 セキュリティ対策に従事する人材の充足状況



（出典）NRIセキュアテクノロジーズ（2019）「NRI Secure Insight 2019」を基に作成

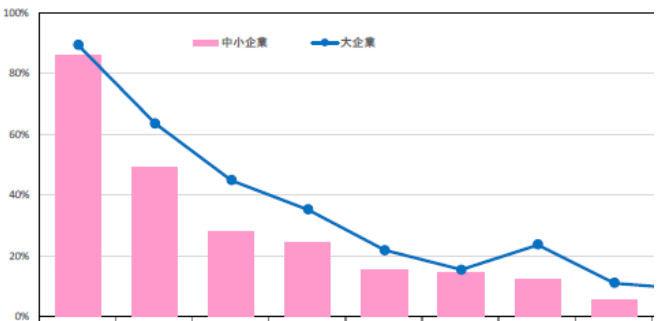
出典：総務省「令和２年版 情報通信白書」

②中小企業は大企業に比べ、特にサイバー人材の社内教育体制の実施状況が脆弱

・サイバー対策の社員教育実施率は、他のサイバーリスク対策と比べとりわけ大企業と中小企業の差が顕著な状況

・社員教育の実施率
大企業：44.8%
中小企業：27.7%
⇒17.1%ものポイント差があり、他の実施項目に比べてもとりわけ中小企業の体制が脆弱な箇所といえる。

【全国の1535企業が実施するサイバーリスク対策の分析】



出典：（一社）日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査2020」

		n=	ソフトウェア等の脆弱性管理・ウイルス対策ソフトの導入	アクセス権限・ログの管理および制御	社員教育（研修・訓練の実施）	データ保護（暗号化・DLPなど）	セキュリティ認証の取得	外部専門家からのアドバイス	セキュリティポリシーや事故対応マニュアルの策定	専門人材の雇用・育成
全体		(1535)	87.4%	54.1%	33.5%	28.1%	17.7%	14.7%	16.2%	7.1%
業種別	01 製造業	(428)	87.4%	56.1%	31.3%	24.3%	15.2%	12.9%	16.1%	7.9%
	02 非製造業	(1107)	87.4%	53.3%	34.3%	29.6%	18.6%	15.4%	16.2%	6.8%
企業規模別	01大企業	(520)	89.4%	63.7%	44.8%	35.2%	21.7%	15.4%	23.7%	11.0%
	02中小企業	(1015)	86.4%	49.2%	27.7%	24.5%	15.6%	14.4%	12.3%	5.1%

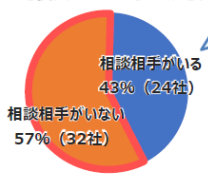
（2）中小企業の現状（R2年度向上支援事業参加中小企業の分析）

出典：東京都中小企業サイバーセキュリティ向上支援事業運営業務委託　実施報告書

①規模の小さな中小企業ほど、相談相手が不足

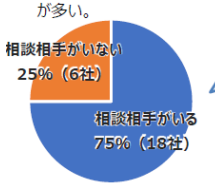
＜セキュリティ対策の相談相手※＞

企業規模が20名以下の企業はセキュリティ対策を相談できる専門家がいない場合が多い。社内システムが未整備で、システムを相談するきっかけがないことも要因の一つと考えられる。



【相談相手】
・システムベンダ 13社
・社外の有識者 10社
・その他 2社
（複数回答あり）

企業規模が21名～100名の会社では、システムベンダや専門家による支援を受けている企業が多い。

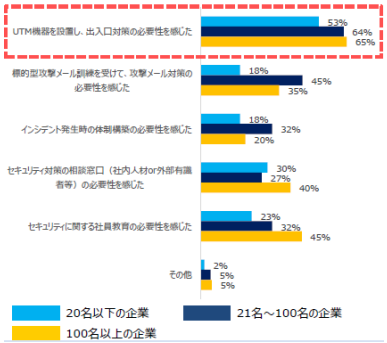


【相談相手】
・システムベンダ 11社
・社外の有識者 6社
・その他 2社
（複数回答あり）

②中小企業は大企業に比べ、特にサイバー人材の社内教育体制の実施状況が脆弱

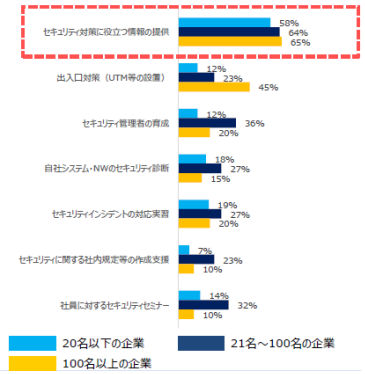
＜本事業に参加して感じたこと＞

企業規模の大小にかかわらず、本事業でサイバーセキュリティ対策の重要性を感じている。UTM機器の設置は、いずれの企業規模においても50%以上の企業が必要性を感じており、意識改革のきっかけとなった。人材育成や体制構築については、企業規模が大きいほど、意識が高まった傾向であるが、いずれも50%未満にとどまり、**インフラ整備に意識が偏重していることがうかがえる。**



＜今後支援事業において実施してほしいこと＞

どの企業規模においても、具体的な取り組みよりも、**セキュリティ対策に役立つ情報の提供を期待している傾向**となった。具体的な施策への落とし込みというよりは、**自社の状況を見極め、優先順位を決めて対策するための検討への支援を期待されていると想定**される。



・現状で、中小企業はその規模に関わらずセキュリティ人材の社員教育よりも、セキュリティ機器設置に優先意識を持つ。

⇒特に、小規模事業者にあればあるほどこの傾向は健著であるといえる。

・事業実施後、今後さらに期待する支援策については、中小企業の規模に関わらずセキュリティ対策に役立つ情報提供が強く要望されている。

⇒機器設置後も、今後何をすればいいか分からない状態に直面している可能性が高く、中小企業自身が不安を感じているといえる。

1．新規事業の必要性　【中小企業のサイバーセキュリティ対策継続支援事業（仮称）】

（3）国の事業実施状況（内閣府・経産省・IPAへのヒアリング結果）

①内閣サイバーセキュリティセンター（NISC）

・NISCが重視しているのは、普及啓発・意識向上

・中小企業は、サイバーセキュリティ対策にかかるランニングコストに慣れていない。
⇒このコストへの必要性の認識が進まない限り、機器などを設置しても継続性が担保できない。

・ＤＸをサイバーセキュリティは車の両輪であるが、現状ＤＸだけが突出していることが大きな問題

②経産省　商務情報政策局 サイバーセキュリティ課

・経産省は、サイバーセキュリティお助け隊事業の２年間の実証期間を経て、中小事業者向けの格安セキュリティサービスを民間事業者に作らせている（官から民へ事業を卸していくという発想）

・大企業・中堅企業向けの人材育成で、経営ガイドラインや人材の手引きなどを作成しているが、現状で、中小企業向けの人材育成は考えていない。
⇒経産省は人材育成よりも機器設置を優先

③IPA（独立行政法人 情報処理推進機構）

・IPAは、サイバーセキュリティお助け隊事業の実施主体として、同事業の普及啓発を最優先とする。

・サイバー対策のフェーズは、普及啓発→機器設置→人材育成と移行していくため、IPAも人材育成は非常に大きな関心事項という認識
⇒特に中小企業はリソースが少なく、今後人材育成がボトルネックになると危惧しているが、現状では機器設置の優先度から対策が進んでいない領域

（4）現行事業（国及び都）がカバーする領域の検討

		基　礎	中　級
ハード整備	機器設置	○ 向上支援事業（機器利用） → UTM設置・駆けつけサポート ※ UTM設置＋常時監視導入により、相当程度高度な対応が可能	○ サイバーお助け隊事業（経産省/IPA） → 中小企業向け低価格サービス ○ 危機管理対策促進助成金（公社） → IPAの２つ★宣言企業が要件
ソフト面の支援策	社内体制整備	○ 向上支援事業（マネジメント支援） → 個社支援（IPA２つ★宣言目標）	※ 国・都ともに未整備の領域
	人材育成支援	※ 国・都ともに未整備の領域	※ 国・都ともに未整備の領域
	普及啓発	○ 向上支援事業（普及促進）→ 一般普及啓発	

・サイバーセキュリティ対策のうちハード整備関係は、向上支援事業の取組により目途は立っている状況
⇒国のサイバーお助け隊事業の民間事業サービスも今後一層の充実が予想される。

・ソフト面の支援のうち、そもそもサイバー対策に関心を持ってもらう入口となる普及啓発事業は、今後も長く続けていく必要がある・

・人材育成は、国・都ともに現在は支援の空白地帯となっている状況

・社内体制の整備も、最も基礎的な部分は今年度から向上支援事業においてフォローを実施するが、そこから先の領域については、同じく支援の空白地帯となっている状況

（5）新規事業立案の必要性

・コロナ禍により社会にDXが急速に進行していく中で、サイバーセキュリティ対策の進行は劣後している状況にある。こうした中で、国と都は引き続き意識啓発を進めるとともに、セキュリティ機器の設置を迅速に進めてきた。
・しかしながら、急速な機器設置の後には、「これから何をすべきか分からない」という企業が多数発生する。こうした次のステップに至った中小企業に対し、進め方を知る方法を伝え、社内の体制を整えるための支援策が必ず必要となる。そこで、国に先駆けその支援を行い、モデルケースを創出する。

2. 支援の具体的な方向性

（1）支援の流れ

○ 新型コロナウイルス感染症の影響により、社会におけるDX化が急速に進行したが、本来、DX化と車輪の両輪であるべきサイバーセキュリティ対策は、特に中小企業において整備が追いついていない状況にある。
○ この現状を踏まえ、普及啓発に加え、機器設置等のハード面の整備を進めているが、中小企業のリソース不足（人材面・ノウハウ面）が、継続的なサイバー対策の実施を続ける上で大きな障害となっている。
○ そこで、サイバーセキュリティ人材の育成支援や実践的な課題解決を通じ、セキュリティ対策の継続性の担保を後押しし、サプライチェーンのセキュリティ対策などにもつながる中小企業の体制強化を目指す。

【対象】
○ サイバーセキュリティ向上支援事業等により、ある程度の機器を設置し次のステップを目指す中小企業

【支援機関】
○ 8カ月程度

【支援対象企業】
○ 20社程度

【事業スキーム】
○ セキュリティ人材育成と課題解決型ワークショップを並行して実施

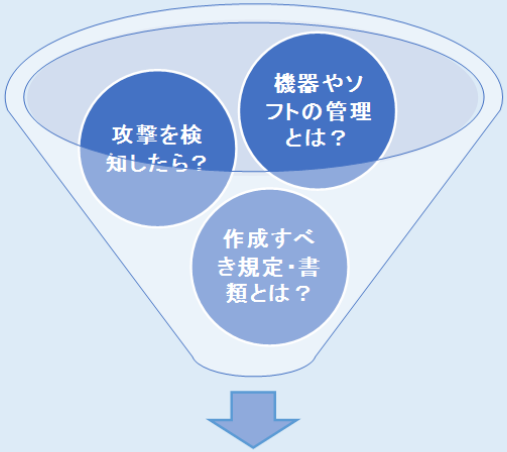
⇩

○ 個人の能力開発のみならず参加企業の課題解決にも資する取組を組み合わせ、企業自身の底上げを目指す

人材育成支援 【第一部】

■ 中小企業サイバー人材育成支援セミナー

セキュリティ対策の器となる機器やソフトを整備した中小企業に、運用ノウハウを提供



「次に何をしたらいいか分からない」状態を解消

※ 併せて、DXやサプライチェーン対策等のセキュリティ課題にも役立つ情報を提供

社内体制整備 【第二部】

■ 課題解決型実践ワークショップ

社内のサイバー体制構築上の課題検討

課題抽出 ⇩

⇧ フィードバック

■ 参加企業への専門家派遣 （1社4回程度）

ワークショップで抽出した課題に基づき、専門家と実地で検証、解決チャレンジ

⇩

解決できた課題について、ワークショップで他の参加企業と共有しフィードバック

2. 支援の具体的な方向性

(2)支援規模及び想定予算額

支援規模の考え方

【支援対象者とすべき中小企業の属性】

・サイバーセキュリティ対策の必要性を認識し、ある程度のセキュリティ機器の整備を終えている中小企業

⇒サイバーセキュリティ向上支援事業を終了し、支援期間終了後もN向上支援事業の受託事業者と契約し、機器設置を継続している中小企業をメインターゲットに想定

※ターゲット企業数（想定）：向上支援事業の単年度の支援企業数：250社×支援期間後のUTM継続社の割合（R2実績：40%）＝ターゲット企業の規模：100社（単年）

【事業の支援規模の考え方】

・本事業はセミナーだけでなく、ワークショップやハンズオン支援によるフィードバックなどを組み合わせ、人材育成と企業の社内体制整備の両立を目指すスキーム

⇒最終目標は、成果発信できるモデル事例の創出であることから、支援規模は向上支援事業のような大規模な数である必要はない。

双方向取組や、それによる参加企業間の交流を検討していることから、ある程度密な人間関係が形成できるスケールとして、20社程度の規模感を想定

想定予算額の考え方

【積算の前提として想定した項目及び事業者からの見積もりにより具体化された要素】

○ 支援企業数：２０社

○ 人材育成セミナー（第１部）＋課題解決ワークショップ（第２部）　あわせて１日×10回程度

○ ハンズオンによる社内課題解決実践：１社４回程度

○ 事例集の作成、アンケート調査の実施

○ その他プログラムの構築、講師の委嘱、参加者獲得に向けたアプローチ費用、オンライン対応に係る経費等

【事業者に対する見積結果】

（１）Ａ総研：121,000千円　　（２）Ｂ総研：84,000千円

⇒　２社の平均をとり、100,000千円で積算

※詳細については、積算資料を参照

2. 支援の具体的な方向性

【参考資料】

支援規模数に対する業種分布の推測

【参考：支援規模から想定される参加企業の業種バランスの試算】

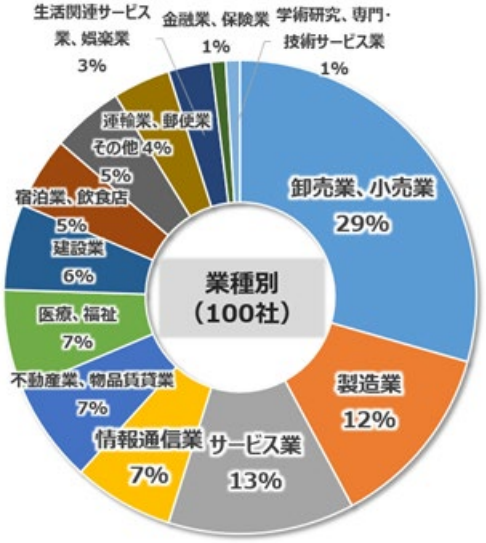
①R2年度の向上支援事業参加企業100社については、業種別の属性が判明している。【図１】

⇒全ての業種が一定の確率で向上事業終了後にUTM設置を継続すると仮定し、上述のターゲット企業100社の業種別比率も【図１】の割合を準用する。

また、本事業への参加表明をする確率も、全ての業種で一定の確立であると仮定する。

②100社の中から10、20、30社を選んだ場合の業種分布を試算する。①の前提の基で計算する場合には、総得票数=100票、各業種の分布比率=獲得票数に置き換え、この票数から定数10、20、30を比例配分することで、大まかな分布状況を推測【図２】（※小選挙区異例代表並立制を参考としたドント式による比例配分）

【図１：R2向上支援事業の参加企業分布】



【図２：ドント式による比例配分検討】

R2サイバーセキュリティ向上支援事業の参加企業の業種比率													
		卸売・小売	サービス	製造	情報通信	不動産	医療福祉	建設	宿泊飲食	運輸	娯楽	金融	学術
企業比率		29%	13%	12%	7%	7%	7%	6%	5%	4%	3%	1%	1%
向上支援事業の単年度の支援企業数：250社×支援期間後のUTM継続社の割合（R2実績：40%）＝ターゲット企業の規模：100社													
対象社数	100	29	13	12	7	7	7	6	5	4	3	1	1
ドント式による比例配分により、定数設定数に応じた事業者の分布を試算													
1で割る	1	29	13	12	7	7	7	6	5	4	3	1	1
2で割る	2	14.5	6.5	6	3.5	3.5	3.5	3	2.5	2	1.5	0.5	0.5
3で割る	3	9.6666667	4.3333333	4	2.3333333	2.3333333	2.3333333	2	1.6666667	1.3333333	1	0.3333333	0.3333333
4で割る	4	7.25	3.25	3	1.75	1.75	1.75	1.5	1.25	1	0.75	0.25	0.25
5で割る	5	5.8	2.6	2.4	1.4	1.4	1.4	1.2	1	0.8	0.6	0.2	0.2
6で割る	6	4.8333333	2.1666667	2	1.1666667	1.1666667	1.1666667	1	0.8333333	0.6666667	0.5	0.1666667	0.1666667
7で割る	7	4.1428571	1.8571429	1.7142857	1	1	1	0.8571429	0.7142857	0.5714286	0.4285714	0.1428571	0.1428571
8で割る	8	3.625	1.625	1.5	0.875	0.875	0.875	0.75	0.625	0.5	0.375	0.125	0.125
9で割る	9	3.2222222	1.4444444	1.3333333	0.7777778	0.7777778	0.7777778	0.6666667	0.5555556	0.4444444	0.3333333	0.1111111	0.1111111
10で割る	10	2.9	1.3	1.2	0.7	0.7	0.7	0.6	0.5	0.4	0.3	0.1	0.1
11で割る	11	2.6363636	1.1818182	1.0909091	0.6363636	0.6363636	0.6363636	0.5454545	0.4545455	0.3636364	0.2727273	0.0909091	0.0909091
12で割る	12	2.4166667	1.0833333	1	0.5833333	0.5833333	0.5833333	0.5	0.4166667	0.3333333	0.25	0.0833333	0.0833333

←R2向上支援事業の参加企業比率に対する、定数10の場合の業種分布（カットライン：6.0未満）
←R2向上支援事業の参加企業比率に対する、定数20の場合の業種分布（カットライン：3.5未満）
←R2向上支援事業の参加企業比率に対する、定数30の場合の業種分布（カットライン：2.5未満）

【図２の分布に関する検討】

・100社中の定数10（緑の網掛け）では、業種の数は全体の半数程度となり、100社中の定数30（緑・青・ピンクの網掛け）では、割合の高い業種の数が他と比べて相対的にかなり多くなる。傾向的には、全体の10%だと業種の多様性が取れず、全体の30%だと多数派の数が多くなりすぎると言える。

⇒総合的に見て、本事業の場合は、全体の20%となる定数20（青の網掛け）が、業種の多様性、多数派と少数派のバランスからみて妥当な数であると思料

3. 令和4年度以降の方向性

【参考】中小企業のサイバーセキュリティ対策関連事業の在り方に関する検討

○ 現在、サイバーセキュリティ向上支援事業により、中小企業に機器設置のトライアル等の機会を提供
○ 向上支援事業の参考とした経産省・IPAのサイバーセキュリティお助け隊事業は、実証期間を終え、令和3年度から、中小企業向けに低価格のメニューを造成した民間企業に事業が降ろされている状況
○ 民間サービスの充実度により、向上支援事業の機器設置の意義が問われる状況が将来発生することを想定