NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

中小企業の情報セキュリティ対策導入を促進する官民による支援施策について（概要版）

社会活動部会
中小企業対策支援施策検討会

検討のきっかけ

- 中小企業層でのセキュリティ対策が進まない（バラツキが出る）**原因**は何か。
- それを打破する支援施策はどのようなものがあるか。（国や自治体の機関、商工団体、支援者など）
- それらの支援施策は**有効か**？ 効率良く**成果**に繋がっているか？
- 対策導入支援施策のあるべき姿を考察する。
- **セキュリティベンダーが出来ることは何か**。
- **他の支援機関/支援者と何をどの様に協働できるのか**。

検討の観点

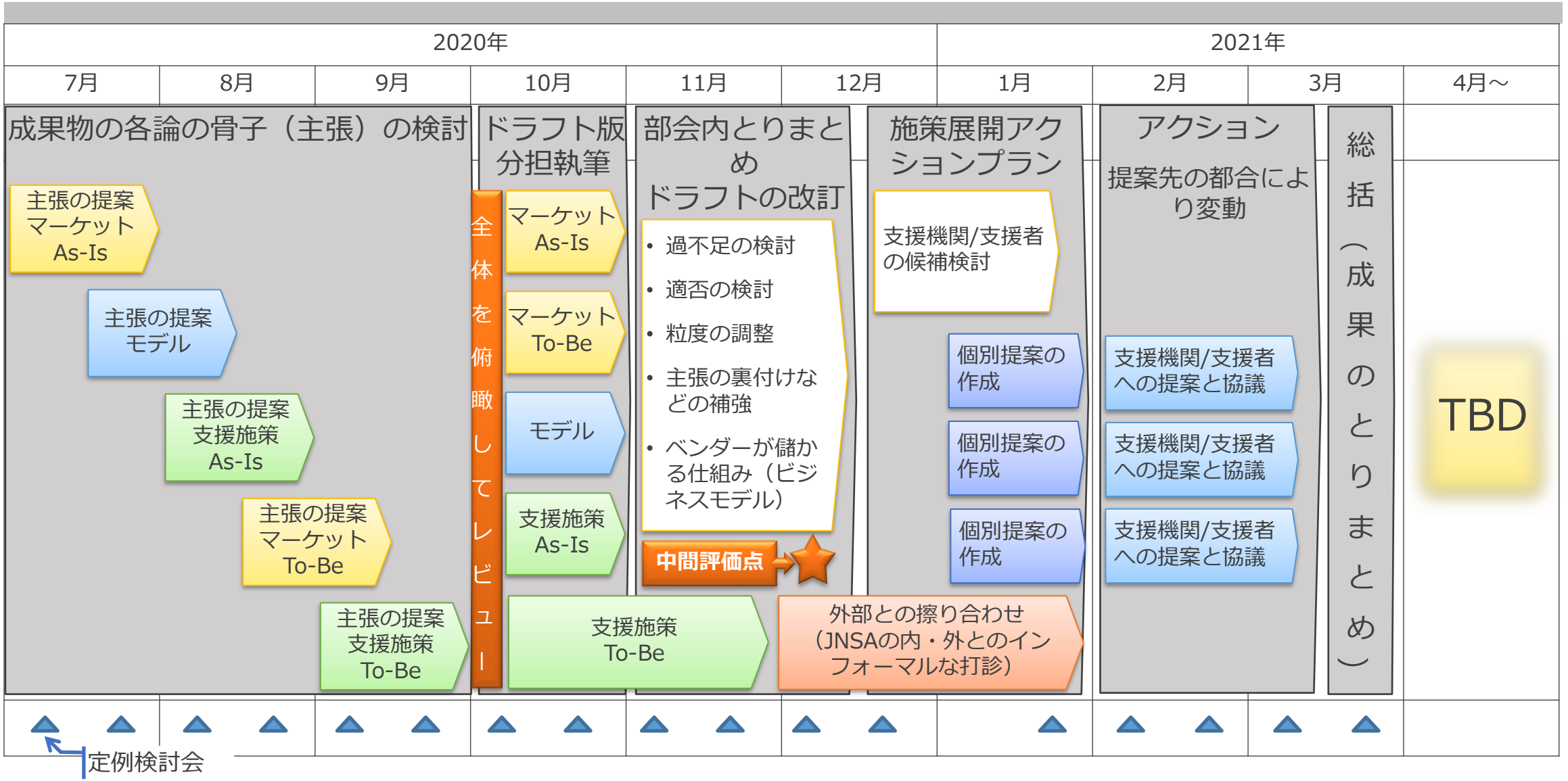
- 現状と課題
  - 中小企業の**IT導入の現状**や、この先、**向かっていく/流れていく方向（変化）**、課せられた課題。
  - 中小企業の**情報セキュリティ対策導入の現状と課題**。
  - 情報セキュリティとして何を求められているのか。
    - **サプライチェーン**からの要求など、何が社会全体としてみた最適解なのか。
    - ある意味、**目標の設定**。支援施策検討の前提。
  - 適切な対策導入に至る**プロセス**と、その**阻害要因、促進要因**。
- 支援施策と施策展開
  - 現状の対策支援施策による**効果**は得られているのか。効率良く**成果**に繋がっているか。
  - **個々の支援施策**の立案。（アイディア出し。阻害要因の除去を目的として。）
  - 「支援者としてのベンダー」の関わり方。
    - 中小企業（その経営者）、ベンダー、そして、公的組織･機関や支援者の**それぞれにとって魅力のある建付（Win³モデル）**は何か。
    - どのような仕組みがあれば、**市場規模**が広がり、かつ、我々、**ベンダーの役割**が増えるか。
    - 支援施策の提案を持っていく協業先はどこか。どう巻き込むか。

検討の枠組み

	マーケット （中小企業の情報セキュリティ）	対策導入モデル	支援施策と施策展開
	• 中小企業の業務、IT利活用 • セキュリティリスクとその対策 • 求められる情報セキュリティのあり方、外的要請 • お金の流れ（コスト負担者）	• 対策導入のインセンティブ、モチベーション • 対策へ至る行動のメカニズム、プロセス、意思決定のしくみ、プロセスの促進要因、阻害要因 • 対策導入に必要なリソース	• 対策導入モデルの実装を促進するための触媒 • 対策導入モデルに即して、促進要因を強化する、または、阻害要因を除去する手立て（支援施策） • 施策展開の枠組み（支援機関/支援者間の協業）
As-Is： 現状、課題	• IT導入と情報セキュリティの現状 • 向かっていく/流れていく方向（変化） • リスク、課題、潜在的ニーズ	• 現状の対策導入モデル（プロセス）の評価、課題	• 現状の支援施策の評価、課題（主に考え方）
To-Be： あるべき姿	• 求められる情報セキュリティのあり方（個社として、社会全体として、ある意味ゴール設定） • お金の流れ（コスト負担者）	• 対策導入の戦略モデル • 除去されるべき阻害要因と、強化されるべき促進要因の特定	• **支援施策案（考え方/個別、新規/改善）** • **何を（支援施策）、誰が（フォーメーション）** • **中小企業、支援機関/支援者、ベンダーのそれぞれにとって魅力のある建付** • **提案を持っていく協業先**

最終目標は、支援施策と施策展開のTo-Be（あるべき姿）

工程表



本文書の構成

2. 中小企業の情報セキュリティの現状と課題

2.1 中小企業の業務、IT利活用の現状

- 中小企業にとって守るべき資産は、営業秘密、知的財産、個人情報などがあるが、現実的には、企業の経営、業務、ステークホルダの利益・権利などが優先される。
- 中小企業の**ITの導入と利活用は十分には進んでいない**。
  - 中小企業のIT利活用は約55%

  （経理などのパッケージソフトでは全体の40%、調達、販売、受注管理では約20%）[2016年全国中小企業取引振興協会調べ]
- 中小企業の**ITの導入と利活用に関するガイドライン的なものが特にない**。

2.2 中小企業を取り巻く情報セキュリティの環境とその変化

- 中小企業のITの導入と利活用は、先ずは、業務の効率化、生産性向上から始まり、次第にDX、デジタル・ネイティブへと移行していく。
- 中小企業における**情報セキュリティの脅威とインシデントは増加傾向**にある。ITの導入・利活用が進むことで、より顕著となる。
- 中小企業のステークホルダからの**情報セキュリティに対する要請は高まっている**。特に、発注元、委託元、親会社などからサプライチェーンリスクとしての情報セキュリティ対策導入の要請が強まりつつある。

2. 中小企業の情報セキュリティの現状と課題

2.3 中小企業の情報セキュリティ対策の現状と課題

– 中小企業の情報セキュリティ対策の現状

- 中小企業の情報セキュリティ対策は、**意識、投資、対策状況とも大企業に較べると低い**、又はバラツキがある。
  - 経営者の情報セキュリティに対する意識が低い。
  - 費用対効果を適切に認識できず情報セキュリティ対策への投資が出来ない。（対策にかけられる費用の不足。）
  - セキュリティベンダは、中小企業の費用感に合った安価な製品、サービスを提供できていない。
  - 対策の検討、導入に必要な人材が不足している。

– 中小企業の情報セキュリティ対策の課題

- ITの利活用と並行して情報セキュリティ対策導入を進めなければならないのに、**セキュリティが疎かになっている**。
- 中小企業が自社の状況を考慮した**リスク分析や評価を行うようなリスクベースのアプローチを自ら行うことは難しい**。
- 情報セキュリティ対策のガイドラインとして、「中小企業の情報セキュリティ対策ガイドライン」はあるが、このような**ガイドラインの不足が中小企業において情報セキュリティ対策が進まない一因**となっている。

3. 中小企業の情報セキュリティのあるべき姿

- 情報セキュリティ対策の目的は、**企業の経営、事業を継続させ、ステークホルダの利益や権利を守る**こと。
- 情報セキュリティ対策のためのコストは、企業活動の価値（製品、サービス、ブランドなど）としてその**対価に転嫁**できることが望ましい。但し、コストと対価のギャップについては、公的支援を行う（社会が負担する）。
- 中小企業が情報セキュリティ対策を実施するにあたり、**経営者が積極的に取り組む姿勢**が不可欠であり、そのためには、以下の何れかの存在が必要となる。
  - 情報セキュリティ対策投資の費用対効果（ROSI：Return on Security Investment）が顕在化する外的要因（**インセンティブ**）
  - 短期的な費用対効果とは異なるモチベーション（**ミッション**。社会的使命、企業責任など。）を与える社会的合意。
- 求められる対策レベル
  - **ステークホルダが合意できるガイドライン（対策基準）**を示すベースラインでのアプローチが妥当であり、このような基準の存在が必要。
  - 先ずは、このガイドラインが満たすべき、要件（仕様）や普及、利活用に関する議論が必要。

3. 中小企業の情報セキュリティのあるべき姿

- **企業の特性**＊1に応じて、求められる対策基準の内容（重要視される対策項目やその達成レベル）が異なることがあり、ガイドラインの作成はこれを考慮する。

  ＊1： 企業の業種、業態や規模、IT依存度、保有する情報資産などに基づくセグメンテーションを想定している。

- ステークホルダに対して対策状況を明示できるよう、ガイドラインに基づく**簡便な認証の仕組み**が必要となる。
  - この認証がステークホルダが**相互に合意できる信頼**を得ることを担保する。
  - 認証は、第1者、第2者、第3者が想定されるが、これらの組合せにより必要かつ十分でコスト的にも実施可能な方法を模索する必要がある。
  - 認証を目的として、ガイドラインに評価基準を加えたり、改善計画書（PoA）やセキュリティ記述書（SSP）を併用することも検討する。

3. 中小企業の情報セキュリティのあるべき姿

- 企業においてITの利活用が進むと、機会と同時に情報セキュリティリスクも高まる。そのリスクを受容基準内に納めるために、**情報セキュリティ対策のレベルもリスクに合わせて向上させていく**べき。
  - 但し、リスクベースの対策導入は容易ではないため、既に**セキュリティ機能が組み込まれているIT**（Embedded Security）の導入や、**外部の専門家**を活用するなどの方策により対策レベルを向上させていく必要がある。
- 情報セキュリティ対策レベルの維持に不可欠な運用については以下とする。
  - 中小企業が自ら運用するツールは、運用者に高いスキルや負荷を求めない。
  - もしくは、ツール導入（主に、技術的対策）より、**サービス利用**（MSS、Sec.aaS（Security as a Service））を優先する。
- ベンダによる中小企業向けのセキュリティ対策製品やサービスの商用化を促すには、製品、サービスの**品質特性、及び、その水準**を定めていくことが必要である。（品質のガイドライン化）
  - このようなガイドライン化は、ベンダにとって、仕様決定の参考や目標とすることで、投資リスクの低減に資するべきものであり、製品認定やブランディング化、それによるコストの増大や寡占化など、投資や参入の障壁になるようであってはならない。
  - ガイドライン化は、ベンダによる業界団体などが主導するか、もしくは、ベンダの意見を十分に取り入れる仕組みが必要。
  - ガイドライン化に際しては、 IPA 「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査」や、既存の品質基準（ISO/IEC 25000など）を参照する。

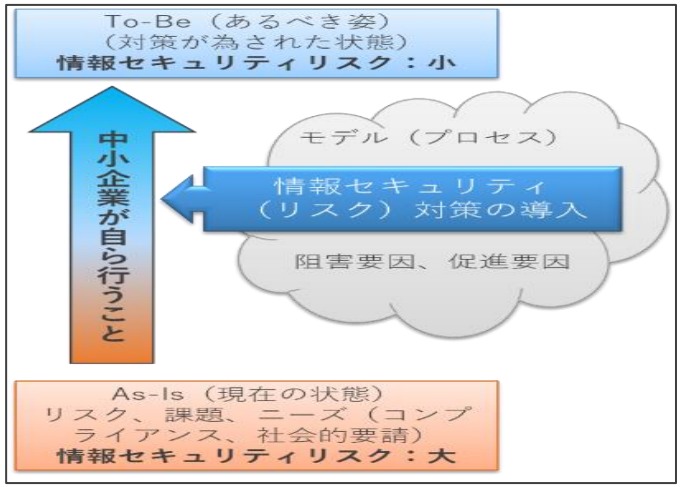
4. 対策導入モデル

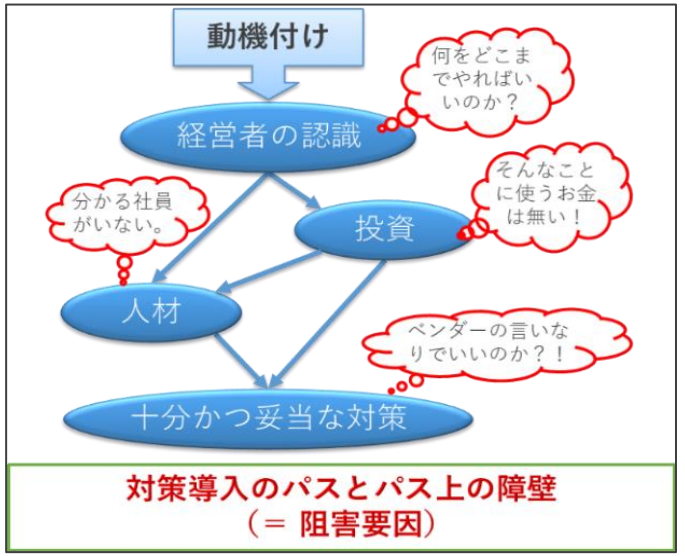
4.1 対策導入モデルとは

- 中小企業が情報セキュリティ対策の導入実施へ至る**行動のメカニズム、プロセス、意思決定のしくみ**
- その過程で情報セキュリティ対策の導入実施（対策実施）に至らない要因（**阻害要因、促進要因の欠如**）

4.2 対策実施までのパス

- 経営者に対する動機付け
- 経営者の認識
- 投資（予算化）
- 人材
- 十分かつ妥当な対策
- **対策導入が進まない要因 ⇒ パス上に存在する障壁（阻害要因）**





4. 対策導入モデル

4.3 対策導入の動機

- インセンティブ：比較的短期に経営上の損得として現れる動機
  - 正のインセンティブ：セキュリティ対策をすることで得られる便益
  - 負のインセンティブ：セキュリティ対策をしない場合にリスクとして負う費用
- ミッション：社会的責任として損得抜きでやるべき事と捉えるもの

インセンティブ		ミッション
やると得する	やらないと損する	損得抜きでやりたい、やるべき
● 取引の差別化要因になる。 ● 参入機会につながる。 ● 優遇税制、低利融資、調達補助金、資金獲得支援 ● 人材獲得	● 入札条件になる。（排除される。） ● 課税される。 ● サイバー攻撃の被害者でも、第3者に迷惑を掛けると罰せられる。	● 社会的責任（迷惑を掛けない） ● 顧客と従業員の保護 ● 経営者の責任（コーポレートガバナンス）として明示、開示

4. 対策導入モデル

4.4 プロセスの阻害要因

- 経営者の認識に関する阻害要因
  - リスク認識：世の中で起きているインシデントなどを、自社へのダメージとして投影できない。
  - 他責バイアス：攻撃者が悪いのであって、被害に合う自分の責任とは考えない。
  - ROSI感覚の欠如：リスク対応による損失低減額と、それに対する適正な費用の感覚が掴めない。
  - 結果として、「取組 2 情報セキュリティ対策のための予算や人材などを確保する」が行われない。
- 投資（予算化）に関する阻害要因
  - セキュリティ対策導入に対する投資額が少ない。（起こりにくくする投資）
  - インシデントが起こっても対応費用が取れない。（ダメージを抑える投資）
- 人材に関する阻害要因
  - 人材のスペックが分からない。
  - ソーシング戦略（社員を充てるか、外部専門家を調達するか）が分からない。
  - 妥当な人材コストが分からない。
- 十分かつ妥当な対策に関する阻害要因
  - 必要十分な効果が見込め、安価で導入しやすいソリューションが少ない。
  - もしくは、これらが知られていない、流通していない。
  - ソリューションベンダーによるIT利活用の提案において、情報セキュリティ対策が担保されていない。

4.5 望ましい対策導入モデル

- 対策実施までのパスにおけるこれらの**阻害要因が除去され、動機付けから適切な対策導入までが流れていく**状態。

5. 支援施策と施策展開の現状と課題

5.1 現状のセキュリティ対策に対する支援策

- **セキュリティ対策導入だけを直接支援する財務的支援は未だ少ない。**
- **現状の各種補助金、税制優遇等は有効性の評価がし難い。**
- 各種補助金、税制優遇等を申請した企業がセキュリティ対策への活用に至った動機や背景は、**受動的なものが多い。**
- 各種支援機関が行っている**セキュリティの専門家派遣制度は、十分なPRができていない可能性がある。**
- 「IT導入補金」は、申請する企業に対して要求するセキュリティ対策が「SECURITY ACTION 一つ星」とされているが、本来、**考慮すべきリスクに見合ったセキュリティの対策ができていない可能性がある。**

5. 支援施策と施策展開の現状と課題

5.2 支援施策と支援展開の課題

- 現状の支援施策の課題
  - 中小企業のセキュリティ対策の底上げを目的とした支援施策はあるが、**狙い（目標設定）、目標に即した施策立案、施策実施の成果の評価といったプロセスが公表されていないものが多く、その効果を把握しづらい**現状にある。
- 普及啓発・コンサルティング支援策の課題
  - 様々な支援機関（経済産業省、中小企業庁、IPAや各種団体、ITベンダー、地域団体、警察等）において中小企業向けの各種支援施策（普及啓発、専門家派遣、補助金等）が実施されているが、**それぞれ独立した動きで、非効率**に見えてしまっている。（例えば、IPAと警視庁とで類似した啓発映像を制作しているなど）
  - 規模の小さな**中小企業（100人以下）、小規模企業には、普及啓発活動が届いていない**と思われる。

5. 支援施策と施策展開の現状と課題

– 補助金・税制優遇等の課題

- 補助金・税制優遇等は、セキュリティ対策を行う**効果や、メリットが十分に考慮されていない**ことが考えられ、その結果、**施策の利用が少なく効果も出ない**。
- 支援施策の立案と展開に当たっては、その支援施策を利用してセキュリティ対策導入を行うことによって得られる**具体的な効果やメリット（インセンティブ）と、その施策を得るための労力との対比にも考慮する必要**がある。

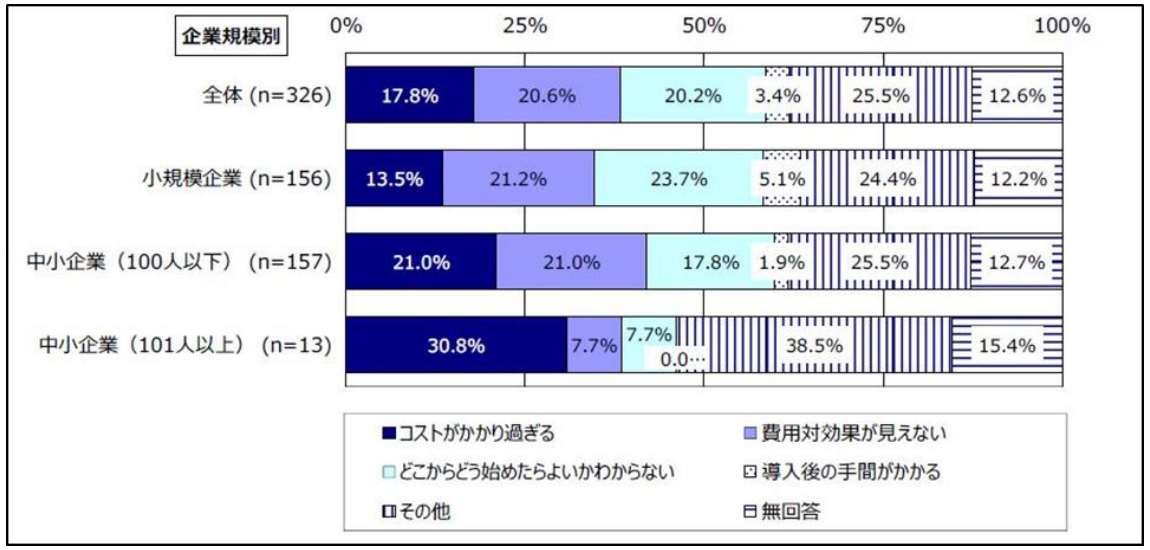


表 IT投資にセキュリティ対策が含まれない理由（企業規模別）

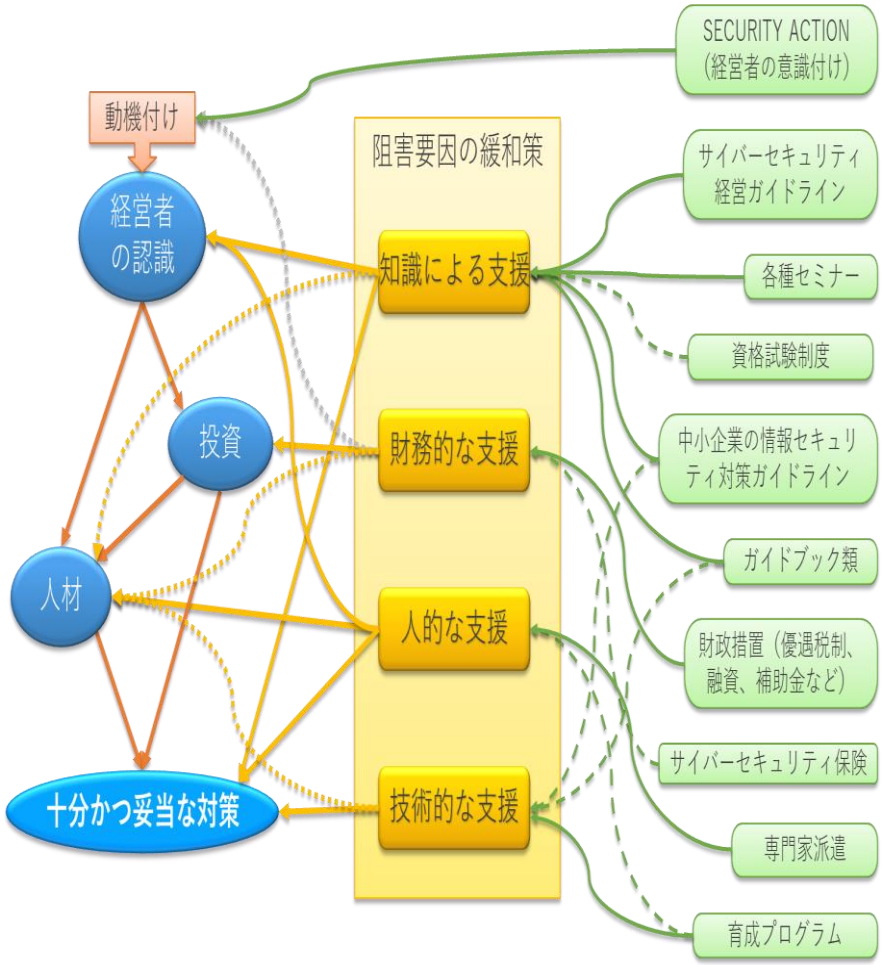
– 補助金を利用したセキュリティ対策導入のインセンティブの具体例

- セキュリティ対策の底上げが図れる。（やりたかった対策が実現できる）
- 就業規則や社内規定など技術的対策以外の面でも外部のアドバイスを受けることができる場合がある。
- 効果報告により対策の結果を可視化できる。

6. 支援施策のあるべき姿

6.1　中小企業に適した支援施策

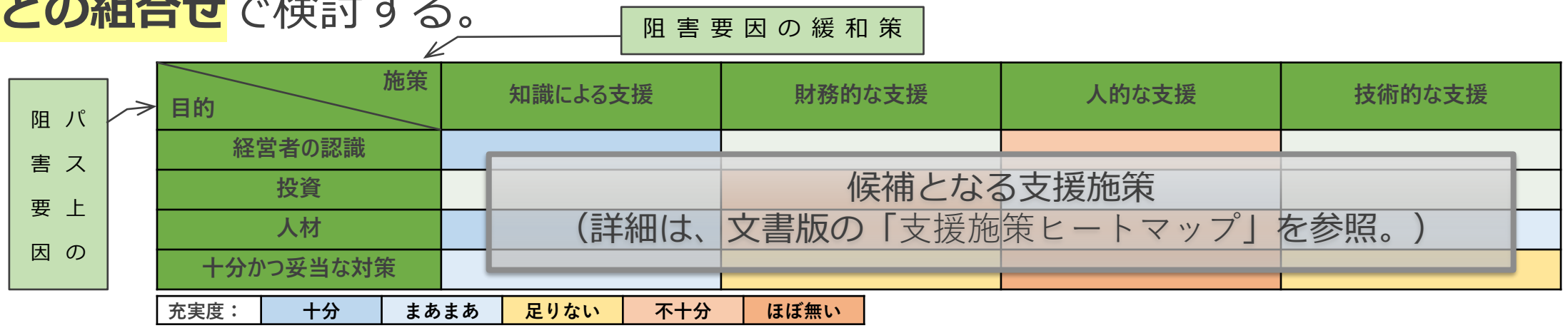
- **対策導入支援施策（=パス上の阻害要因を除去する施策）**の、**目的と手段との関係が明確な総合的なフレームワーク（支援施策のセット）**が必要。
- 素となる資源による施策の分類（「知識」,「財務的」,「人的」,「技術的」）
- 施策展開に関わる支援機関/支援者が、目的、目標、手段などについて共通の理解を持つことが必要。
- 施策の目的、目標の設定においては、中小企業全体の情報セキュリティ対策レベルの向上の、**具体的な効果と関連させる。(SMARTを意識する。)**
- 目的、目標に対する結果の評価は、ステークホルダと共有する。
- **民間の支援機関/支援者（ベンダーを含む）による投資を得るには、市場の形成が必要。**
- 市場が形成されるまでは、公的機関による支援、または、民間による支援のバックアップが必要。



6. 支援施策のあるべき姿

6.2 求められる具体的な支援施策

- インセンティブは、初めは正のインセンティブを多くし、徐々に負のインセンティブへ移行する。
- ミッションとしての動機付けは、経営者が主な対象であるが、加えて、社会全体に対して発信できるメディアも使う。
- 支援施策のセットは、**目的としての除去すべき阻害要因と、手段としての阻害要因を除去できる施策（「知識」,「財務的」,「人的」,「技術的」で分類 ）との組合せ**で検討する。



6. 支援施策のあるべき姿

6.2.3 知識による支援
- セミナー、ガイドブック類は充実しており、阻害要因としての「経営者の認識」、「人材」、「十分かつ妥当な対策」をカバーしている。
- これらの情報、支援施策の整理、統合と、対象者へのリーチの仕組みに改善が必要。
- 対策ガイドラインは、利用の目的、方法を踏まえた整備と、さらなる普及策が必要。

6.2.4 財務的な支援
- 経営者の認識：第3者によるアセスメント実施の公的補助
- 投資：セキュリティ対策投資を直接支援する補助金制度等を強化する
- 人材：セキュリティ人材の育成、雇用や、外部委託に対する補助金、奨励金
- 十分かつ妥当な対策：プロダクト、サービスの開発、販売のための補助金、融資制度、税制優遇や、支援機関による買い取り提供など

6.2.5 人的な支援
- 経営者の認識：経営を主とする支援機関（商工団体、金融機関）/支援者（士業など）への情報セキュリティ教育、専門家派遣
- 人材：トレーナー派遣、外部メンター、コミュニティ形成
- 十分かつ妥当な対策：実務を幅広く支援する情報セキュリティ人材派遣ビジネスの推進
- その他：情報セキュリティ人材の流動性やレバレッジを高めるための施策や、需要サイド（中小企業）と供給サイド（専門家、支援者）をマッチングさせる仕組みも必要

6.2.6 技術的な支援
- 経営者の認識：知識による支援や人的な支援を柔軟に提供するプラットフォームの構築
- 十分かつ妥当な対策：中小企業が利用できるツールやサービスの整備・調達、及びポータルサイトでの公開･周知
  - 例：ポリシー文書類のテンプレート、OS、アプリケーション、アプライアンスなどの設定テンプレート、無償のセキュリティツールの開発・普及支援、SaaS型セキュリティツール、MSS（低価格に限る）の支援

7. 支援機関/支援者の役割と連携

7.1　支援機関/支援者の協働

- **幅広い支援機関/支援者による協業体制、分業体制**が必要。
- 各施策の位置付け、関連性、あるべき姿に向けた相乗効果などを明確にし、共有する。
- **支援機関（組織）、支援者（専門家）への動機付け（インセンティブ、ミッション）も考慮**し支援が継続的に行われるようにする。

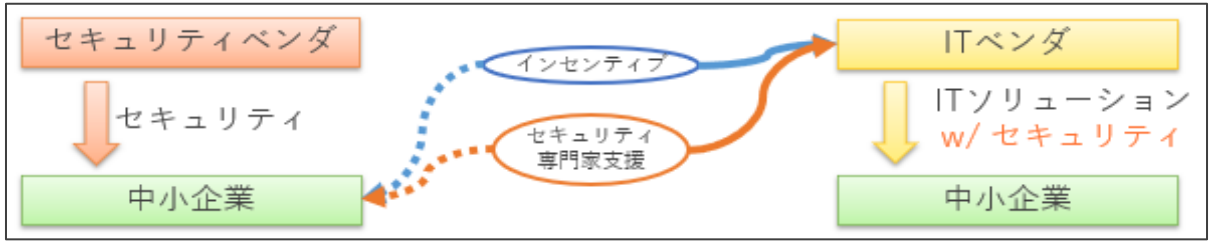
7.2　IT導入支援施策へのセキュリティ導入のバンドル

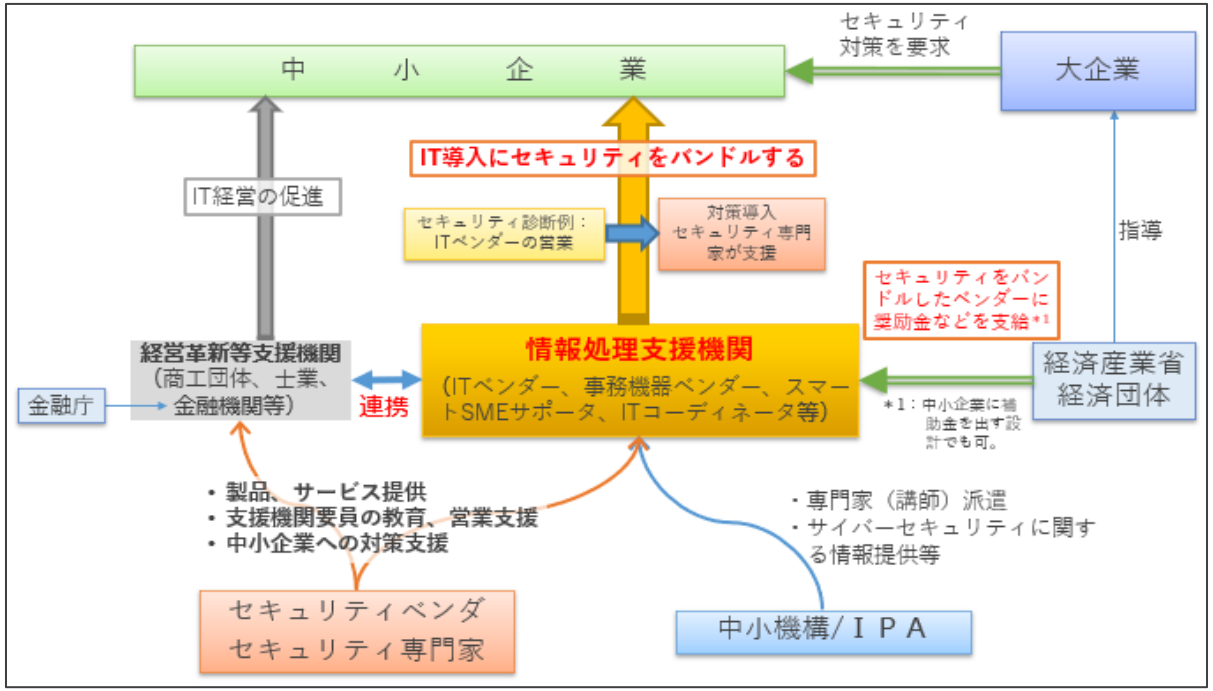
- 支援施策により情報セキュリティを単独でインセンティブ誘導することが難しい企業も存在する。
- 多くの中小企業は、未だ、IT導入を進めていく段階であり、その為の支援施策が多くある。
- 実態として、中小企業のIT導入において、相応の情報セキュリティ対策が伴っていないケースもある。
- IT導入と情報セキュリティ対策の不可分性を考えた場合、**IT導入支援施策に情報セキュリティ対策を組み込む、または、バンドルする**ことも有用である。
- ただし、このバンドルが適さない領域もある。（例：ガバナンス強化、ISMS系（ポリシー作成、監査、認証、教育）、SOC/CSIRTなど）

7. 支援機関/支援者の役割と連携

7.3 支援機関/支援者に対する支援施策の整備

- **IT導入支援施策の担い手であるベンダーや支援者に、情報セキュリティ対策を組み込む、または、バンドルさせる**には、そこへの**インセンティブを与える**必要がある。
- この場合、**情報セキュリティに関する知識・費用・人的等の支援**は、中小企業に直接アプローチするよりも、**IT導入支援機関やベンダー、支援者に対して提供する**のが効率的である。





まとめ

- 対策導入のモデルを考える（4章）
  - パス：　動機付け ～ 経営者の認識 ～ 投資（予算化） ～ 人材 ～ 十分かつ妥当な対策
  - 対策導入が進まない要因 ⇒ パス上に存在する障壁（阻害要因）
- 支援施策（主に6章）
  - 中小企業における情報セキュリティ対策の導入を支援する（促進する）官民による施策
  - 対策導入支援施策 = パス上の阻害要因を除去する（もしくは、促進要因を補強する）施策
  - 目的（効果、状態、To-Be）と手段*1との関係*2が明確な総合的なフレームワーク（支援施策のセット）
  - 目的、目標に対する結果（状態の変化）の評価（差異とその原因の考察）、および、その共有
- 支援機関/支援者（7章）
  - 幅広い支援機関/支援者（ベンダーも含む）による協業体制、分業体制
    - 民間の支援機関/支援者（ベンダーを含む）による投資を得るには、市場の形成が必要。
    - 支援機関（組織）、支援者（専門家）への動機付け（インセンティブ、ミッション）が必要。
  - IT導入支援施策に情報セキュリティ対策を組み込む、または、バンドルする
    - ITベンダーやIT導入の支援者に、情報セキュリティ対策を組み込む、または、バンドルすることのインセンティブを与える。
    - 情報セキュリティに関する支援は、IT導入支援機関やベンダー、支援者に対して提供する。

＊1：「知識」,「財務的」,「人的」,「技術的」
＊2：マトリックス、連関図

社会活動部会
中小企業対策支援施策検討会