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

中小企業向け情報セキュリティ対策ガイドラインの作成と運用において考慮すべき要件についての考察と提案

本資料では、中小企業の情報セキュリティ対策導入に活用できる対策基準のガイドラインを扱います。以下、特に断りの無い限り、「ガイドライン」はこの意味で用いています。

2022年3月31日　（2022年10月11日 修正）

特定非営利活動法人日本ネットワークセキュリティ協会

目次

1. 検討の経緯と現状の課題

本文書の位置付けとねらい

- 現状の課題認識
  - 中小企業の情報セキュリティ対策導入、あるいは、それを支援する際に利用可能なガイドラインは複数存在するが、企業個社の実状に合わない、対策実施に結びつかない、対策の有効性の評価が定まらないなど、それらが十分に機能していないとの指摘がある。
  - 一方で新たに、業界ごとのガイドラインの作成や、それに基づく調達の仕組みや認証の仕組みの議論も為されつつある。
  - 上記のような状況に鑑みると、ガイドラインの作成と運用において作成者が考慮すべき要件というべきものを正しく踏まえずに、新たなガイドラインの作成、若しくは、既存のガイドラインの改定を行うと、その効果を十分に得られないことが懸念される。
- 検討のねらい
  - JNSA 社会活動部会 中小企業支援施策WGでは、中小企業を対象とした情報セキュリティ対策のガイドラインが備えるべき要件、すなわち、ガイドラインの作成と運用において作成者が考慮すべき要件と、そのガイドラインを活用した簡易な認証などの相互信頼を得るための仕組みについて検討を行ったので、その結果を本文書として整理した。
  - このような要件を踏まえて開発されたガイドラインが利用可能となることで、中小企業の情報セキュリティ対策実施の費用対効果の向上や、取引に関わる総合的なコストが低減されることを期待する。

検討内容

1. 既存のガイドラインと現状の課題
   - 現在参照できるガイドラインとしては、どのようなものがあるか
   - 「現状の課題の抽出」 → なぜ「中小企業のガイドラインの要件」を定める必要があるのか
2. ガイドラインの要件を作ることの目的
   - ガイドラインの定義と機能
   - ガイドラインの要件定義を行うことの目的
   - ガイドラインのライフサイクルモデルと課題
3. 要件の検討対象とするガイドラインのスコープ（論ずべきガイドラインの範囲）
   - ガイドラインによるリスク分析の手法とアセスメントの対象
4. 目的を達成するためのガイドラインの特性 ⇒ 要件
   - ライフサイクルモデル上の課題をどのようにして解決するのか
   - 要件（Should）、Shouldn‘t（やってはいけないこと）
   - 構造（参照関係、包含関係、共通部分（汎業界、汎業態）／固有部分（業界、業態に固有の特性））
5. 相互信頼（安心）のための認証のしくみ
   - 認証のしくみの要件
   - 認証のしくみの構成要素
   - 認証のしくみの展開

1. 既存のガイドラインと現状の課題

- 現在参照できるガイドラインとしては、どのようなものがあるか。
  - IPA 中小企業の情報セキュリティ対策ガイドライン（5か条、自社診断）
  - NISC青本＊1、東京都黒本＊2、自工会/部工会＊3、 IPA 情報セキュリティ対策ベンチマーク …

    ＊1：NISC 小さな中小企業とNPO向け情報セキュリティハンドブック
    ＊2：東京都労働産業局 中小企業向けサイバーセキュリティ対策の極意
    ＊3：自動車産業サイバーセキュリティガイドライン
  - CIS Controls、DoD CMMC、enisa Cybersecurity for SMEs、FFIEC Cybersecurity Assessment Tool （CAT） …
- 「現状の課題」の抽出 → なぜ「中小企業のガイドラインの要件」を定める必要があるのかの根拠となる。
  - 基準としての妥当性はあるか。
  - 中小企業の担当者や支援者にとっての使いやすさはどうか。
  - 他の基準や業務との適合性は保たれるか。
  - ガイドラインの適切な保守運用が為されているか。

1. 既存のガイドライン、現状の課題（課題抽出の観点）

- 基準としての妥当性
  - リスクの低減が出来るか。相互信頼（コンセンサス）に寄与するか。
- 使いやすさ
  - 分かり易さ、具体性、客観性、検証容易性。使うためのコスト（時間、前提知識、専門人材）。
  - どこまでやればいいのか？対策例とされているが全部やるのか？ 必要最低限、「ここまでやれば十分」があるか？
- 適合性
  - 情報セキュリティ以外の基準との親和性。事業、業務全体の中での受け容れ易さ。個社の事情との適合性（カスタマイズ、テーラーリングの要否、可否）
- （ガイドラインの）保守運用
  - 作り易さ。作るためのコスト。メンテナンスのし易さ。普及、流通のコスト。

課題の検討結果一覧については、巻末「【参考】現状の課題の抽出結果」を参照

2. ガイドラインの要件を作ることの目的
3. 要件の検討対象とするガイドラインのスコープ

2. ガイドラインの定義と機能

- 本活動でのガイドラインの定義
  - 「ガイドライン」とは、中小企業が情報セキュリティ対策の要否を検討し、自社に合った対策を導入する、あるいは、その導入を支援する際に活用するもの。
    - 拠って、単に、情報セキュリティ対策の必要性を説くもの（啓蒙目的）や、総花的な脅威と対策や対策プロセスの解説書などは除く。
- 想定すべきガイドラインの利用シーン （備えるべき機能）
  - アセスメント（評価）
    - 自社の対策状況を評価する。（絶対評価）
    - 自社の対策状況を他社と比較（ベンチマーク）する。（相対評価）
  - 対策強化
    - 対策実施計画を策定する。（目標や優先順位付けなど）
    - 具体的な対策内容を理解する。（何をどこまで、どうやって）
  - 相互信頼（BtoB、BtoC、BtoP） を醸成
    - 評価結果を認証*1する事によって、対策の実効性を客観的に担保する。
    - 認証された評価結果を公開することにより、相互に信頼を確認（安心）する。

＊1：第1者認証、第2者認証を含む、簡易な認証の仕組みを想定する。

ガイドラインの利用シーン

（ガイドラインの機能）

アセスメント

↓

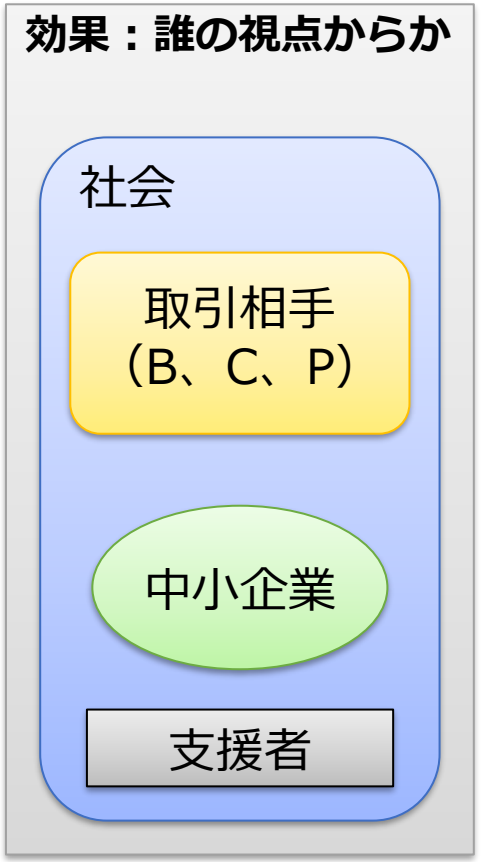
対策強化

↓

相互信頼

2. ガイドラインの要件定義を行うことの目的

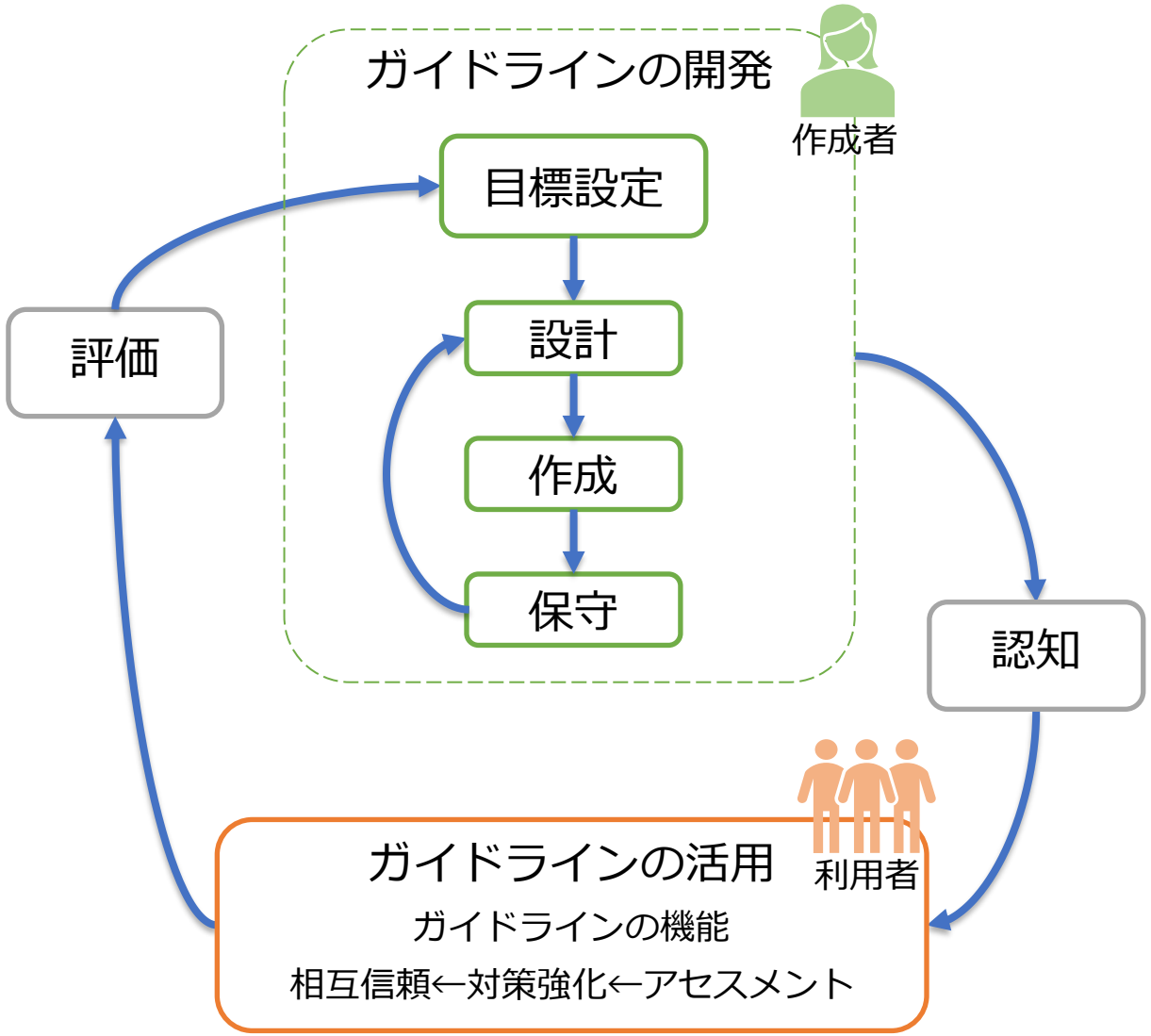
- ガイドラインを作る目的（得られる効果）
  - ガイドラインが活用されることによって、以下の効果が得られる。
    - 情報セキュリティ対策実施の費用対効果（ROSI*1）を向上できる。
    - 取引に関わるコストを低減できる。*2
    - 本来の業務を保護し（任務保証）、攻めの施策（IT導入、DX対応等）に経営資源を集中できる。
- ガイドラインの要件定義を行うことの目的（期待される効果）
  - ガイドラインの要件の目的は、それに即したガイドラインが作られ活用されることで上記のガイドラインの活用による効果を最大化すること。



＊1：ROSI（Return on Security Investment）

＊2：情報セキュリティリスクを低減するための活動や、リスクによりインシデントが発生した際の対応など、それらの何れも、取引に関わる双方の何れか、又は、両者のコストの増加につながる。

2. ガイドラインのライフサイクルモデルと課題



ガイドラインの作成者は、全ライフサイクルを考慮して、各プロセスで発生する下記のような課題を認識し、それらをガイドラインの開発時に解決する。

リテラシーギャップ

- 中小企業の経営者や担当者が、ガイドラインについてどこまで知る必要があるのか？ベンダーや専門家がガイドラインを利用して適切にアドバイスができて、対策強化につながれば良いのではないか？「ガイドラインの利用者は誰」問題。

作成するガイドラインの定義（例）

- 対象：中小企業、数百万事業者、BtoB/BtoC/BtoP。
- ガイドラインの活用における機能（アセスメント、対策強化、相互信頼）を備える。
- 最も重視すること：What（対策基準。カタログ、チェックリスト。）。WhyやHowは副次的。

開発指針

- ベースラインアプローチの限界：どこまでリスクベースアプローチを加味するか。
- 一律性問題：A社とB社は同じガイドラインの対策で良いのか？
- 対策強化のレベル：どこまでやれば良いのか？

実行可能性

- 実行可能性：具体的な対策強化のアクションにつながるか？（Whatが曖昧、Howが不足などが原因？）
- リソースが足りない。ROSIに基づく、実行可能性（妥当性）。

3. 要件の検討対象とするガイドラインのスコープ

- ガイドラインをアセスメントの観点で整理し*1、且つ、中小企業を意識したガイドラインを取り巻く環境の想定を考慮し、以降の要件の検討で対象とするガイドラインを以下のように定める。

  *1：巻末「【参考】ガイドラインについての基本的な整理」を参照

- リスク分析手法
  - レベル付きのベースラインとする。
    - レベルとは、対策項目に関連付けるLow、Mid、Highなどの指標である。
    - ベースラインとリスクベースとの中間的位置付け、折衷案である。
    - ベースラインだけだと、一律性問題に陥る。（様々な企業、ステークホルダに対して、単一、一律な対策基準が有用なのか。）
    - リスクベースのリスク分析はコスト高となる。
    - レベルのバリエーションは継続検討が必要。
      - 何によって自社の目標とするレベルを決めるのか。業態、情報資源、リスクプロファイル 、成熟度、リソースなど。
      - レベルによって対策項目の何を変えるか。選択する対策、個々の対策の強度など。

- 対策基準に対するアセスメントの対象
  - 対策実施の達成度（どこまで実施できているか）を評価する。
    - 本来は、対策の実施結果としての残存リスク（対策による効果・有効性）を評価したいが、これは容易ではない。
    - 対策の実施と、その結果としてのリスク値の低減との関係は、線形ではなく、また、組織によって異なるが、負の相関があることを前提に対策の達成度を評価する。但し、そのような相関を持つように、ガイドラインの対策項目が設計されていなければならない。

4. ガイドラインの要件

4.1 開発 – 目標設定

4.2 開発 – ガイドラインの構成

4.3 認知

4.4 活用 – アセスメント

4.5 活用 – 対策強化

4.6 活用 – 相互信頼

4.1 開発 – 目標設定

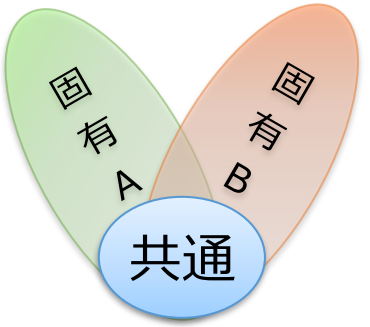
- 目的・役割の明確化
  - ガイドラインの開発に当たっては、企画書、計画書、設計書等を作成する。
    - 公的機関がガイドラインを開発する際は、企画書等も公開し、説明責任を果たすことが望ましい。
    - 企画に際しては読み手は誰（経営者、社内実務担当者、支援者等）であるのか、また、その読み手の目的、役割を明確にする。
      - 対策の実装は支援者（専門家やベンダー）に委託されることを前提として、それらを対象とするガイドラインと位置づけることも可能。
    - ライフサイクルにおける評価は、当初の企画、計画に照らして評価する。さらに、その評価の結果を、企画書等の改訂に反映させる。
- リテラシーギャップへの配慮
  - 明確化した読み手のIT、及び、ITセキュリティに関するリテラシーを設定する。
  - リテラシーのギャップが想定される場合には、それを補う情報（用語集や外部参照資料等）を提供する。
  - リテラシーギャップを補うために、適宜、社内の識者や社外支援者を活用することも推奨する。
  - ガイドラインを活用する際の最低限の前提条件（例：要保護情報、IT機器、ネットワー構成等が判ること。）を示す。
  - 企画、作成段階に、異なるリテラシーレベルの利用者からのヒアリング、テストマーケティングを行う。

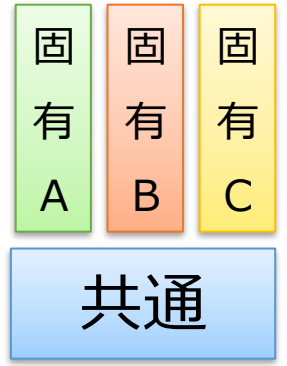
4.2 開発 – ガイドラインの構成（1）

- ガイドラインの位置付け
  - ガイドラインの位置付け、スコープ（利用者、及び、その環境や制約条件、対応する脅威など）を明確に示す。
  - 既に普及している他のガイドラインとの関係を明確にし、これらの他のガイドラインと（部分的にでも）対策内容が重複することを避ける、若しくは、他のガイドラインの当該箇所を明示した上で引用、又は、参照する。
  - 既に普及している他のガイドラインと同様な対策内容になるようであれば、新たな開発を控えることも検討する。
  - 既に普及している他のガイドラインが、中小企業には適さないような場合、あるいは、特定の業界、業態などに限っては適さないような場合は、必要な箇所だけを追加、改変する、あるいは、不要な箇所を省略する。

4.2 開発 – ガイドラインの構成（2）

- 一律性問題*1を解消するための工夫
  - 業種、業態などによらない必須の順守項目（共通項目）と、業種、業態などに固有となる対策項目（差分項目）とを分離させる。
    - 分離した範囲毎に、開発者、開発時期が異なることあり得る。
  - 業種、業態などがリスクレベルと関係づけられる場合は、それに応じた対策レベルによって、実施すべき対策項目を選択できるようにする。
  - 企業の異なる拠点や部署によって、必要となる対策項目も異なる場合があることを考慮し、それらの特定、対策項目の選択、対策実施の優先順序づけが出来るようにする。（適用条件付きの対策項目など）
  - 外部の支援者に委託（アウトソース）できる対策項目を明示し、各企業に固有な制約条件を軽減できるようにする。





＊1： 一律性問題：個々の業界や企業によって、様々な状況が異なるのに、一律に定めたガイドラインが役に立つのかという懸念。

4.2 開発 – ガイドラインの構成（3）

- 各企業が目標とするレベル
  - 各企業がどのように自社の目標レベルを決定するのかの方法、手順、指標を示す。
    - 各企業が自ら自社の目標レベルを決定する場合もあれば、サプライチェーン上の調達者など、他のステークホルダが所定の目標レベルを要求する場合もあり得る。
    - 読み手のIT、及び、ITセキュリティに関するリテラシーの想定（例えば、成熟度）を多段階に設定し、これを自社の目標レベルと対応付けることも検討する。
  - 各企業が、手順に沿って自社、若しくは、事業の目標レベルを決定することを推奨する。
  - 各企業がどのような状態となったら自社の目標レベルを見直し、変更するのかを示す。
- 対策項目のレベル付け
  - 各対策項目のレベルに応じて、何に差異を設けるのかを検討する。（実施すべき対策項目自体を変える、対策の強度を変える、アセスメントの指標を変えるなど。）
  - 各レベル毎の求める対策について、その前提や根拠を示し、各企業に対する妥当性を企業、若しくは、支援者が評価できるようにする。

4.3 認知

- ガイドラインを開発する際は、そのガイドラインが広く認知され、かつ、採用されるようにするための要件、目標、計画を定め、その目標を達成できるように活動を行う。
  - このような認知のための活動としては、ガイドラインの内容と併せて、以下のような情報も中小企業の経営者、社内実務担当者、支援者に周知する。
    - 脅威情報や事故被害事例、社会的要請
    - 開発したガイドラインの活用事例、効果、ガイドラインを活用した対策実施の有効性（ROSI）評価など
- 開発したガイドラインを活用した対策実施を促すために、中小企業、又は、支援者のモチベーションにつながる施策を実施する。若しくは、既存のモチベーションにつながる施策と、ガイドラインを活用した対策実施や認証とを関連付ける。
- 公的な支援機関が、中小企業の情報セキュリティ対策実施につながる各種ガイドラインの特徴や、利用方法などを網羅的に整理し、中小企業や支援者が最適なものを見つけ出せるような、一元的な情報提供の場を設けることが望ましい。

4.4 活用 – アセスメント

- ガイドラインの対策基準は、客観的な評価、及び、検証と再現が可能な基準となるように定める。
- 評価結果に点数付けを行う場合は、以下について考慮する。
  - 点数付けの目的や、結果の利用の仕方を定める。
    - 目的の例としては、例えば、合計点の時間的推移を捉えるとか、対策項目をグループ化しそのグループ毎の点数により、対策の偏りの分析をするなど。
  - 目的や利用の仕方に基づき、個々の点数の尺度、点数の基準、配点等の設計を行う。
    - 例えば、点数の値は対策の強度を示しているのか、点数は客観的に一意に決定できるのか、異なる対策に対する点数は比較可能なのかなど。
  - 点数付けの目的、点数の持つ意味（尺度）、結果の解釈や利用の仕方を利用者に明確に示す。
  - 点数付けが不要な場合、若しくは、上記の要件を満たしていない場合は、点数付けを行わない。

4.5 活用 – 対策強化（1）

- 対策項目の選定
  - ガイドラインに記載する対策項目は、設定したガイドラインの位置付けの範囲で、出来るだけ網羅性を持たせる。
  - ガイドラインを活用する際の最低限の前提条件（例：要保護情報、IT機器、ネットワーク構成等が判ることなど）を示し、これらの情報の整備に取り組むことも、対策項目とすることを検討する。
  - 一時点の対策実施に留まることなく、対策の運用、モニタリング、改善等、対策の有効性が継続することを促すような対策項目とする。
- 対策の判り易さ
  - 個々の対策項目の記述では、対策の目的や必要性の理解を促すために、例えば、その対策によって保護される資産を例示し、対処できる脅威、脆弱性、被害事例等を示す。
  - リスクや対策内容などの記述内容の理解を促進するために、例えば、図表、イラスト、マンガ、動画等との連携を活用する。

4.5 活用 – 対策強化（2）

- 対策の実施に対する考慮
  - 個々の対策項目で何を対策するかを示すことに加え、その対策をどのように実装するのかを示す解説を付加するか、若しくは、ヒントとなるような他の参照先を例示する。
  - 対策の具体的な実装方法としては、手作業で行う、ツールを利用する、サービスとして調達するなど、複数の手段があることを示す。
  - その対策を導入し、さらに、運用していく際に必要となる資源（人材、手間、コスト）、及び、効果（ROSI）を、各企業、若しくは、支援者が想定できる様に配慮する。
  - 具体的な実装方法を検討する際には、自動化やサービス調達も含め、その実施に必要となる資源（人材、手間、コスト）を各社の実情に即して考慮し、自社にとってROSIが優れているものを採用することを推奨する。
  - 可能、かつ、妥当である場合は、サンプル、テンプレート、事例等も併せて提供し、中小企業の対策導入の負担を、極力、軽減するように配慮する。
  - 自社のリソースで実施する対策項目に加え、外部の支援者に委託する場合の対策の実施方法、留意点についても記載することを検討する。

4.6 活用 – 相互信頼

- ガイドラインに基づいた対策実施が、取引先などのステークホルダとの相互信頼に役立つためには、そのガイドラインが継続的に保守、更新され、さらに、中小企業もそれに合わせて実施した対策の評価、見直しを続けることが必要となる。
  - ガイドラインを開発する際は、予め、保守や更新の要件、計画も定め、それらの保守、更新が将来に渡り持続的に実施されることが確実になるような措置を取る。
  - ガイドラインの保守、更新に際しては、IT技術とその利活用、攻撃の手口や脆弱性、新たな他のガイドライン、対策ツールやサービスの流通など、それらの最新の動向を踏まえて見直しを実施する。
  - ガイドラインの保守、更新に際しては、公的機関や外部団体が定期的に公表しているレポートなどを参考にし、それらとの整合性が取れているようにする。
  - ガイドラインの開発に当たっては、広くセキュリティ専門家や中小企業への支援者、市場のステークホルダーからのフィードバックを取り入れ、開発するガイドラインの内容が広くコンセンサスを得られ、よって、ガイドラインに基づく対策の実施が相互の信頼の確保に寄与するものとなるように配慮する。

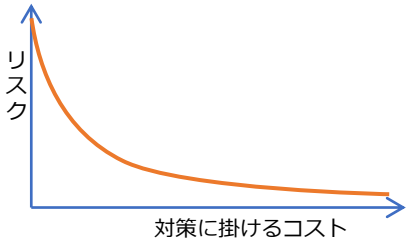
5. 相互信頼（安心）のための認証の仕組み

1. 要件
 1.1 簡易な認証の仕組みを作る目的
 1.2 簡易な認証の仕組みの制約条件
2. 構成要素
 2.1 評価方法の選択肢
 2.2 評価者の候補
 2.3 評価基準を定める
 2.4 認証の仕組みの設計
3. 展開
 3.1 認証の結果の公開と他社による確認の仕方
 3.2 認証の仕組みに関するその他の要検討事項、課題

5. 認証の仕組み ～ 1. 要件（1）

1.1 簡易な認証の仕組みを作る目的は以下の通り

- 中小企業の情報セキュリティ対策の状態が、他者にとって「安心できるものであること」が判ること。
  - 「情報セキュリティ対策の状態」とは：コンセンサスが得られたガイドラインの対策基準に対する達成度。
  - 「他者」とは：BtoBの取引相手、BtoCの消費者、業界や社会。
  - 「安心できるもの」の概念：対策コストと残存リスクとの曲線がなだらかになる辺り。



- （ガイドラインに期待される効果である）「取引に関わるコストを低減できる」につながること。
- 情報セキュリティ対策の導入が促進されること。
  - 認証取得状況が広く公開されることにより、自社の現状を他社と比較ができるようになる。
  - 認証の取得、維持を目標とする事で、社内への啓蒙･啓発（社員の意識向上、対策レベル維持、対策目標）が期待できる。

5. 認証の仕組み ～ 1. 要件（2）

1.2 簡易な認証の仕組みの制約条件は以下となる

- コスト、手間（人手）が掛からないこと。
  - 年1回の更新で、無償、若しくは、数万円（多くの中小企業の場合）から数十万円（中規模企業、調達条件などにより必要性が高い場合）が目安となる。
    - できれば、初回の認証取得費用だけでも無償に出来ると望ましい。⇒ 公的補助金の検討が必要。

	補助する取得費用	年間100万社	年間1.6万社
参考試算額	30万円（法人による第3者認証を想定）	3,000億円	48億円
	10万円（個人事業主等よる第3者認証を想定）	1,000億円	16億円

    - 企業規模で変動とするかは要検討。その場合でも根拠が必要となる。（従業員数 ≈ 審査コスト、売上高 ≈ 支払い能力、等）
- スケールが効くこと。
  - 対象とする事業者（中小企業）数（例えば、「年間100万社の認証が可能であること」など）は、広くステークホルダによる合意が必要である。
    - 合意の際の論拠の例
      - » BtoBビジネスの中小企業（サプライチェーン・セキュリティの観点）
      - » 秘密情報、個人情報、機微情報等を扱う中小企業
      - » 被害の影響範囲（例えば、利用者数、取引者数等）が 5,000人以上の中小企業
      - » ITやデータを事業に利用している中小企業数に対する割合（サイバーハイジーンの視点）

5. 認証の仕組み ～ 2. 構成要素（1）

2.1 評価方法の選択肢

- 経営者、担当者へのヒアリング
  - 口頭によるインタビュー形式の他に、事前記入する調査票（ヒアリングシート）を用いることも可能。
- 文書、記録の閲覧、対策状況の観察による実態の検査
- ツールを使った自動評価
  - ツールの機能として、証跡を収集する、収集した証跡を取りまとめて可視化する、取りまとめた証跡を基に結果を判定する等がある。
  - ツールにより証跡を収集できる対象は、技術的な対策などに限定される。

2.2 評価者の候補

- 第1者：社内の評価担当者（例：経理責任者（経営者を除く）、監査役等）
- 第2者：取引先による評価、及び、その評価結果の他社公開、再利用。
- 第3者：セキュリティ支援者（例：RISS、情報セキュリティ監査業務従事者等）、中小企業支援者（例：士業等）
  - 評価者が一定の資格を持つか、基準を満たす者であることは必要。
  - 評価者が、個人事業主の様な立場で良いか、一定の基準を満たす法人に所属する者であるべきかは要検討。（後者の場合は、その法人が認証の主体（認証機関）となることが可能。）
  - 中小企業と評価者のマッチングの仕組み、報酬の考え方を整備する必要がある。

5. 認証の仕組み ～ 2. 構成要素（2）

2.3 評価基準を定める

- ガイドラインの対策基準に対する客観的な評価の手法、指標（監査における標準監査手続きのようなもの）の開発が必要となる。
  - 対策基準項目ごとに、評価対象となる証跡やその収集方法、評価方法、判定の基準等を定める。
  - ガイドラインの基準をレベル付きとする場合、評価の指標、手法もレベルごとに定める。
- ガイドラインの基準をレベル付きとする場合、評価の結果、及び、認証は、どのレベルに対する評価結果（認証）であるかが判るようにする。

2.4 認証の仕組みの設計

- 認証の仕組みの設計に際しては、認証の仕組みの目的と制約条件とを勘案して、評価方法と評価者の組み合わせ、及び、評価基準を定める。
  - 目的の「他者にとって「安心できるものであること」が判る」を満たすには、評価が十分な客観性、正確性を持つことが必要である。
  - 加えて、制約条件である、手間、コストが掛からない、かつ、スケーラブルであることも必要。
- 組み合わせの検討例
  - 文書や記録などを、評価者である第3者に送付して、ツールを用いて検査する。
  - 技術的な対策の実施状況は、ツールを用いて第1者評価を行う。
  - 第1者評価の結果を、第3者の評価者、又は、機関がサンプリングして、客観性、正確性を検証する。（この場合、検証した結果、第1者評価の内容に不備があれば、是正勧告、認証の取り消し、ペナルティを科すなども検討する。）

5. 認証の仕組み ～ 3. 展開

3.1 認証の結果の公開と他者による確認の仕方（例）

- 認証を取得した中小企業が自社で公開（Webサイトなどで）する。
- 確認を必要とする利害関係者に、都度、オンデマンドで開示する。
- 第3者組織（複数でも良い）が登録を受付け、公開する。

3.2 認証の仕組みに関するその他の要検討事項、課題

- 認証の有効期間と更新の仕組み
- 認証の仕組みの普及、定着を図る施策
  - 調達基準、委託先選定基準として認証の取得を要求するよう働きかける。
  - 中小企業が、IT/DX推進や情報セキュリティ対策導入の支援施策を受ける際の要件とする。
- 認証の仕組みの評価と見直し
  - 評価と見直しは必要であるが、ガイドラインの対策基準や評価の基準が変更された際の、認証結果の互換性、有効性に対する措置が必要となる。
- 完全認証に対する部分認証＊1の導入の是非
  - 部分認証は、あくまでも、例外的、あるいは、暫定的、猶予的な位置付けであり、認証の仕組みの目的を阻害しない範囲とする。
  - 部分認証を認める場合は、ガイドラインのどの対策基準が未達成なのかが分かる資料、あるいは、完全認証を得るための改善計画書などの付帯を義務づけることを検討する。

＊1：対策基準の全てを完全に達成していなくても、概ねその基準の目的が達成されいると判断できる場合に認証を与える考え方。

【参考】

- 現状の課題の抽出結果
- ガイドラインについての基本的な整理

【参考】現状の課題の抽出結果

#	Org	課題	観点	課題の分類
1	16	誰が使うガイドラインなのか（読み手が誰なのか）が定まっていない。（中小企業の経営者や担当者を対象として作っても、リテラシーとレベル格差の問題で有効に使われない。）	保守運用	目標設定
2	28	サイバーセキュリティに関する用語やシステムに関する知識がない。（ガイドラインやメーカー提案についていけない）	その他	リテラシーギャップ
3	29	情報セキュリティに関する情報共有の場や機会がないので、情報収集手段がなく知識が得ることができない。	その他	リテラシーギャップ
4	5	使う相手のセキュリティリテラシに依存するので、基準の内容、意図が理解されない。よって、 自分で正しく評価が出来ない。答えのレベル（1,2,3）なども解釈が定まらない。	使いやすさ	リテラシーギャップ
5	6	ISGL4SMB 25項目ですら、中小企業には理解できる人がいない。現状が判らない、判断できない、必要性（脅威、被害）が理解できない。	使いやすさ	リテラシーギャップ
6	7	利用者のリテラシーが考慮されていない。	使いやすさ	リテラシーギャップ
7	31	多くの広義のガイドライン（セキュリティフォーカスではない、IT利活用や働き方のガイドラインなども含めて）がある中で、そのガイドライン位置づけや、他との関連性を明確ではない（元から考慮されていない。）。複数ガイドラインを利用する場合に、MECEにならない。全体最適とならない。	適合性	構造
8	14	ガイドラインが複数有って、どれを使ってよいのか判らない。業界によってはドミナント（唯一性、デファクト）が存在しているケースもある（FISCやPCI-DSSなど）が、SMBに特化した、あるいは、考慮したものではない。	適合性	構造
9	18	業種、業態、その他のリスク要素が異なる企業に対して、一律のガイドラインを適用することが適切なのか。	基準としての妥当性	一律性問題
10	8	中小企業には、リスクやリテラシー、リソースに格差があるので、一律に同じ重要性としている基準では使えない。	使いやすさ	一律性問題
11	13	全社とか工場とか、評価や実装のスコープ決めをして使えるようになっていないと、全社を対象にせざるを得ないため、評価が軒並み三角（一部で実施できている）になる。	適合性	一律性問題
12	2	対策項目に「基本」や「最重要」などを定めているガイドラインがあるが、これらが選択された根拠が判らない。誰にとっても本当に正しいのか。	基準としての妥当性	対策強化-レベル
13	4	どこまで満たせば良いのか、対策実施のゴール、目標値が判らない。	基準としての妥当性	対策強化-レベル
14	15	カスタマイズ（テーラリング）をして使うことを前提としていないので、100%やらなくてはいけないと思われて 普及しない。	適合性	対策強化-レベル
15	1	数値化（対策達成度の点数付け）は出来た方が良いが、分布（平均してそこそこ、一部だけだが高得点）等を考慮しないと達成度や効果の解釈ができない。	基準としての妥当性	アセスメント
16	9	外部攻撃とか内部脅威などの「何から守る」だけでは、「何を守るか」（情報資産、業務、コンプライアンスなど）が判らない。	使いやすさ	Actionability
17	26	人材不足で、インシデントが発生時の対策が分からない。また、相談ができない。	使いやすさ	Actionability
18	27	自社の状況が理解できていないので、何をどこまですればよいか判断がつかない。（システム導入時にメーカやネットワーク業者任せ）	保守運用	Actionability
19	32	保守・運用（PDCA）が回すために考慮すべき事項（場合によっては委託先）の説明がない。	保守運用	Actionability
20	10	ISGL4SMBの「本格的に取組む」の実装の流れ（実装プロセス）が判りにくい。（Howの部分が足りない。）	使いやすさ	Actionability
21	11	対策の評価までは出来るが、対策のためのツール、サービスが探せない、又は、コストが判らないため、実装に繋がらない。	使いやすさ	Actionability
22	19	対策を継続的に実施するには、コストや手間が掛かりすぎるものがある。	使いやすさ	Actionability
23	23	具体的な実装方法やどのようなルールを作ったらよいか判らない。（Howの部分が足りない。）	使いやすさ	Actionability
24	30	対策を実施するステップと費用、それを実現することで低減できるリスクを想像できるようにする。	使いやすさ	Actionability
25	17	IT技術とその利活用、攻撃の手口や脆弱性など、それらの最新の動向をキャッチアップできていない。	基準としての妥当性	相互信頼
26	3	誰もが納得できる基準ではない。「誰」は、主にセキュリティ専門家。	基準としての妥当性	相互信頼
27	25	サイバーセキュリティに対する脅威・リスクが、認識できていない（ウィルスソフトだけで十分との認識）	使いやすさ	認知
28	22	市場にはどんなガイドラインがあるのか分からない。	その他	認知
29	24	ガイドラインの存在を知らない	その他	認知
30	12	そもそも、ガイドラインに沿ってセキュリティ対策をすることの重要性が理解されていない。（Whyの部分）	適合性	認知
31	20	コストを掛けて対策を実施することによって得られる、対策レベル向上以外のメリット、投資効果、モチベーションなどが認められない。	適合性	認知
32	21	市場に展開されている多くのガイドラインの中から、(進行中の)取組で参考にできるガイドラインを見つけられない。	適合性	認知

【参考】ガイドラインについての基本的な整理

- 情報セキュリティ対策のためのガイドライン（アセスメントの観点から）
  - リスク分析手法のバリエーション
    - ベースラインコントロール
      - ベースラインコントロールは実施すべき情報セキュリティ対策。
      - ガイドラインはその集まり、カタログ、チェックリスト。
    - リスクベース
      - リスクベースの場合、資産価値（ミッションへの影響）、脅威、脆弱性等の考慮が必要で、分析が複雑になる。また、これらは、業界、業態毎、さらに個社によって異なる。
  - 対策基準に対するアセスメント対象のバリエーション
    - コントロール（対策）の達成度（どこまで実施できているか）を評価するもの。
    - コントロールの実施結果としての残存リスク（インシデント発生頻度やそれによるビジネス影響）＝ コントロールの効果・有効性を評価するもの。
    - 成熟度（組織能力、マネジメントシステム）を評価するもの。
      - 成熟度の指標の例：PDCAを回す、対策リソースを最適化する。

Thank you