

サプライチェーン強化に向けたセキュリティ対策評価制度 に関する実証報告書

2025/12/23

エグゼクティブサマリ (1/3)

【1.実証の実施概況】

- 近年、サプライチェーンに起因するサイバー・インシデントを背景に、企業の取引においてもサイバーセキュリティ対策の担保が求められる中、受注企業が異なる取引先から様々な対策水準を要求される一方、発注企業は外部から各企業等の対策状況を判断することが難しいといったサプライチェーン上の課題が存在している。このような課題に対応するため、経済産業省ではサプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組み(「サプライチェーン強化に向けたセキュリティ対策評価制度」)の検討をこれまで推進してきた。2025年4月には当該制度の概要を整理した『サプライチェーン強化に向けたセキュリティ対策評価制度 構築に向けた中間取りまとめ』(以下「中間取りまとめ」という。)を公表。
- 中間取りまとめで提示された制度の基礎的な骨格に基づき、対策項目・評価基準の実施可能性や評価スキームの妥当性等を確認することを目的として、2025年4月から11月までにかけて、以下の3つの実証事業等を推進した。
 - ①★3実証事業 ②★4実証事業 ③発注元企業に対するヒアリング
 - ①においては19社、②においては16社、③においては10社にそれぞれ参画いただいた。

【2.実証の実施結果】

- 実証に当たっては、中間取りまとめで提示した評価スキーム案に基づき★3・★4で想定される一連の流れを試行するとともに、本制度のユーザーとなり得る発注元企業に対してヒアリングを実施することで、運用上生じ得る具体的な課題を特定することとした。
- ①★3実証事業、②★4実証事業、③発注元企業に対するヒアリングそれぞれにおける実施結果等は以下のとおりである。

<★3実証>

- ★3実証では、以下の流れに沿って実証事業を実施した。
 - ①適用範囲の決定 → ②自己評価 → ③専門家による評価 → ④ヒアリング等による調査
- ①適用範囲の決定では、全社を適用範囲とする企業の割合が高い傾向が見られたが、適用範囲外を設ける場合であっても、ファイアウォール又はVLANによる通信制御の実施等によりネットワークを分離を行っていた。
- ②自己評価では、技術的対策の実装が求められる事項について、遵守率が低い傾向が見られた。
- ③専門家による評価においては、従業員数100名以下の小規模な会社(計6社)において、評価の前提として実施が必要な①適用範囲の決定及び②自己評価について、専門家によるサポート(伴走)が必要となった。
- ④ヒアリング等による調査において、★3実証参画企業からは、主に(1)★3取得のためのコスト、(2)要求事項・評価基準の内容理解、(3)他制度との連携の3点についてそれぞれ意見を頂戴した。

エグゼクティブサマリ (2/3)

【2.実証の実施結果】(続き)

<★4実証>

- ★4実証では、以下の流れに沿って実証事業を実施した。
 - ①適用範囲の決定 → ②自己評価 → ③第三者評価 (→ ④技術検証) →⑤ヒアリング等による調査 ※④は一部企業のみ実施
- ①適用範囲の決定では、★3同様、実証参画企業の中では、全社を適用範囲とする企業の割合が高い傾向が見られ、適用範囲外を設ける場合、一部の企業を除きファイアウォール又はVLANによる通信制御の実施等によりネットワークを分離を行っていた。
- ②自己評価の実施では、各企業とも概ね高い水準で要求事項を達成できていたが、特にサイバーセキュリティサプライチェーンリスクマネジメントに関連する要求事項・評価基準については、遵守率が相対的に低い傾向が見られた。
- ③第三者評価では、文書審査及び実地審査の2通りの審査を実施し、どの企業においても概ね問題なく実施することができた。
- ④技術検証については、外部診断及び内部診断の2通りの検証を実施した。課題として、外部診断と比較して、内部診断においては、事前調整工数が大きいほか、現地訪問等による実施期間等の制約も受けやすいという課題が上がった。また、外部診断では相対的に困難は少なかったが、対象IPが多数に渡る場合にツールによる解析に大きな時間を要する等の指摘があった。
- ⑤ヒアリング等による調査においては、★4実証に参画いただいた企業からは主に、(1)要求事項及び技術検証実施の内容、(2)ガイダンス資料の充実、(3)他制度との連携等についてそれぞれ意見を頂戴した。

<発注元企業へのヒアリング>

- 発注元企業へのヒアリングにおいては、電気業、ガス業、製造業、各種商品卸売業の分野から10社に協力いただいた。
- 結果として、各社とも取引先へのセキュリティ対策については関心が高く、主に以下のような本制度における活用に期待する意見が多く上がった。
 - 本制度の要求事項・評価基準の粒度が比較的高く、★3・★4の判断理由も特段抜け漏れ等はないように見受けられるため、取引先を含めたセキュリティ管理高度化に活用できる。
 - 本制度により取引先のセキュリティ対策レベルがより可視化される点に期待がある。

エグゼクティブサマリ (3/3)

【3.実証を通じて得た課題と対応の方向性】

- 実証を通じて、主に以下のような課題が上がった。
 - ★3・★4実証参画企業において、多くの企業において共通して達成できていない要求事項・評価基準が存在している。
 - 実証時点で全要求事項・評価基準を達成していた参画企業はいなかった。
 - 実証での技術検証を通じて、外部診断と比較して、内部診断の事前調整工数が大きいほか、現地訪問等による実施期間等の制約も受けやすく、非現実的との指摘があった。他方、外部診断では相対的に困難は少なかったが、対象IPが多数に渡る場合にツールによる解析に大きな時間を要する等の指摘があった。また、内部機器の脆弱性に対しては、資産管理ツールによる確認等の代替手段を設けられないかとの意見があった。
 - 参画企業へのヒアリングの結果、中小企業等において★取得に必要な対策を実装できるよう、制度運営側からの支援の拡充を求める意見が多く上がった。
- 上記のような課題に対しては、以下のような検討を進める。
 - 実証の結果を踏まえ、過大であることが考えられる要求事項の内容について見直し。
 - ★3・★4の取得条件(評価基準全件への適合が必要か等)について精査。
 - ★4における技術検証における実施内容について精査。
 - 各業界・企業からの意見等を踏まえ、制度導入促進に向けた取組の具体化。

目次

1 実証の実施概況

- 1.1 背景
- 1.2 実証等の目的
- 1.3 実証等の類型
- 1.4 参画団体の概要
- 1.5 スケジュール

2 実証の詳細内容

- 2.1 事前準備
- 2.2 ★3実証
- 2.3 ★4実証
- 2.4 発注元企業へのヒアリング

3 実証を通じて得た課題と対応の方向性

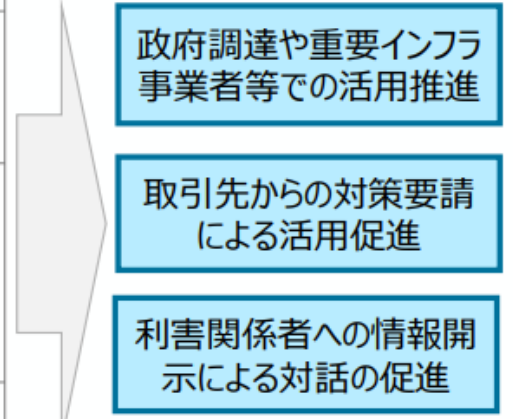
1. 実証の実施概況

1.1 背景

- サプライチェーンに係るセキュリティの課題に対応するため、本年4月に制度の概要を整理した中間とりまとめを公表。
- 本年度においても引き続き、実証事業等を通じた評価スキームの具体化や制度の利用促進のための施策の検討等を進め、2026年度中の制度開始を目指している。

構築する評価制度（現時点案）

成熟度の定義	三つ星（★3）	四つ星（★4）	五つ星（★5）※
想定される脅威	<ul style="list-style-type: none"> • 広く認知された脆弱性等を悪用する一般的なサイバー攻撃 	<ul style="list-style-type: none"> • 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃 	<ul style="list-style-type: none"> • 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策： <ul style="list-style-type: none"> • 基礎的な組織的対策とシステム防御策を中心に実施 	サプライチェーン企業等が標準的に目指すべきセキュリティ対策： <ul style="list-style-type: none"> • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施 	サプライチェーン企業等が到達点として目指すべき対策： <ul style="list-style-type: none"> • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
評価スキーム	自己評価	第三者評価	第三者評価



制度実現に向けた検討課題（例）

- 国内外の関連制度・評価制度との整合性確保、相互認証
- 対策推進のための企業への支援の在り方（専門家の活用促進、中小企業支援策との連動、評価機関の支援）
- 下請法や価格転嫁に関する課題の整理
- 実効性の強化に向けた取組（政府機関や重要インフラ事業者等における活用推進、サプライチェーン上の取引先や投資家等のステークホルダとの対話での活用等の促進）

※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

※サプライチェーン間の結び付きが強固・複雑な自動車、半導体、主要製造業等において、優先的に本制度の利用を促進。

1.2 実証等の目的

- 中間とりまとめで提示された制度の基礎的な骨格に基づき、対策項目・評価基準の実施可能性や評価スキームの妥当性等を確認することを目的として、実証等を推進した。(※)

※ 本実証は、サプライチェーン構成企業における現状の対策状況を把握しつつ制度案の具体化及び改善に活用するために行うものであり、★3又は★4の付与又はその支援等を目的としたものではない。

実証で確認を行う事項(例)

<p>1</p> <p>要求事項・評価基準案の実施可能性</p>	<ul style="list-style-type: none"> ★3・★4で要求される対策と、対象企業で実際に講じられている対策との差分 社内外の資格者による協力のもと行う★3 自己評価の正確性 社内外の資格者による協力のもと行う★3 自己評価の実施難易度 ★4 評価機関及び検証事業者に必要な知見・スキルと情報セキュリティサービス基準等の既存ルールで要求される水準との差分
<p>2</p> <p>対策、評価の実施等に係る工数及びコスト等</p>	<ul style="list-style-type: none"> ★3・★4 評価の結果、追加で対応が必要とされた事項の実装にかかる工数及びコスト 対象企業における売上規模やIT関連予算の規模に鑑みた、追加で対応が必要とされた事項の実装にかかるコストの金額的な妥当性 ★3 自己評価にかかる工数及びコストの許容可否 第三者による★4 評価・検証等にかかる工数及びコストの許容可否
<p>3</p> <p>制度に関する規定等のわかりやすさ</p>	<ul style="list-style-type: none"> 対策実装又は評価を行う上での★3・★4 要求事項・評価基準案における不明点・誤解を招き得る点 ★3 自己評価プロセス及び関連ドキュメントにおける不明点・誤解を招き得る点 ★4 第三者評価プロセス及び関連ドキュメントにおける不明点・誤解を招き得る点

1.3 実証等の類型

- 前頁に示す目的のため、サプライチェーン構成企業における実証(★3・★4 評価スキームの試行)に加え、サプライチェーン構成企業に一定のセキュリティ対策を要請する側である発注元企業に対しても現状の取組み及び本制度の活用等に係るヒアリングを行った。

サプライチェーン構成企業における実証		発注元企業に対するヒアリング
★3実証	★4実証	
参画者 <ul style="list-style-type: none"> ■ サプライチェーン構成企業 主にサプライチェーンを構成する中堅・中小企業のうち、上位の★の条件に該当しないものを想定 ■ セキュリティに係る専門家(※) ※社内に専門家(有資格者)がない場合は外部の資格者に依頼することも可 	<ul style="list-style-type: none"> ■ サプライチェーン構成企業 <ul style="list-style-type: none"> ①発注元事業者から機密情報の提供を受けている、 ②発注元事業者の事業継続上重要な位置づけを占めている、 ③取引先環境から発注者の内部システムへのアクセスが可能等の条件に合致するサプライチェーン構成企業 ■ 評価機関 ■ 技術検証事業者(※) ※評価機関が検証実施不可の場合 	<ul style="list-style-type: none"> ■ 発注元企業 自社のサプライチェーンを構成する企業に対して、一定のセキュリティ対策を要請することでリスクの緩和を図る企業
主な実施内容 <ul style="list-style-type: none"> ■ 適用範囲の検討 ■ ★3 要求事項・評価基準に基づく、現状の対策状況の自己評価 ■ 社内外の専門家による自己評価結果のレビュー ■ 対策実装に必要なコストや自己評価の正確性に関する検証 ■ 制度対応の難易度や必要な支援策等に関するヒアリング 等 	<ul style="list-style-type: none"> ■ 適用範囲の検討 ■ ★4 要求事項・評価基準に基づく、現状の対策状況の自己評価 ■ 評価機関等による第三者評価の実施 ■ 対策実装に必要なコストや第三者評価の費用、必要スキル等に関する検証 ■ 制度対応の難易度や必要な支援策等に関するヒアリング 等 	<ul style="list-style-type: none"> ■ 発注元企業に対するヒアリングの実施

1.4 参画団体の概要

- 製造業及びサービス業を中心に、計35社(★3：19社、★4：16社)のサプライチェーン構成企業からの参画を得た。

★3実証 参画企業 (計19社)

主な事業内容 (日本標準産業分類 中分類)	本文書内の呼称	従業員数
生産用機械器具製造業	★3A社	11~50名
	★3B社	11~50名
	★3C社	51~100名
	★3D社	51~100名
	★3E社	51~100名
	★3F社	51~100名
	★3G社	101~300名
	★3H社	101~300名
鉄鋼業	★3I社	51~100名
機械器具卸売業	★3J社	51~100名
化学工業	★3K社	1001~3000名
	★3L社	1001~3000名
	★3M社	10001名~
保険媒介代理業	★3N社	~10名
専門サービス業	★3O社	~10名
情報サービス業	★3P社	1001~3000名
	★3Q社	101~300名
技術サービス業	★3R社	51~100名
ガス業	★3S社	5001~10000名

★4実証 参画企業 (計16社)

主な事業内容 (日本標準産業分類 中分類)	本文書内の呼称	従業員数
輸送用機械器具製造業	★4A社	10001名~
	★4B社	10001名~
	★4C社	10001名~
	★4D社	5001~10000名
	★4E社	1001~3000名
	★4F社	1001~3000名
	★4G社	501~1000名
	★4H社	10001名~
電子部品・デバイス・電子回路製造業	★4I社	10001名~
生産用機械器具製造業	★4J社	5001~10000名
	★4K社	1001名~3000名
非鉄金属製造業	★4L社	3001~5000名
化学工業	★4M社	5001~10000名
情報サービス業	★4N社	1001~3000名
	★4O社	3001~5000名
倉庫業	★4P社	1~500名
印刷・同関連業	★4Q社	501~1000名

1.4 参画団体の概要

- ★4実証における第三者評価を行う機関として6社、その他発注元企業ヒアリングに関しては10社にご協力いただいた。

★4実証 評価機関 (計6社)

主な事業内容	本文書における呼称	従業員数	技術検証実施可否
各種マネジメントシステム認証に係る審査業務等	評価機関A	101~300名	×
	評価機関B	301~500名	○
	評価機関C	1001~3000名	×
セキュリティコンサルティング、その他のサービス提供	評価機関D	51~100名	×
	評価機関E	101~300名	○
	評価機関F	10001名~	○

発注元企業ヒアリングご協力企業 (計10社)

主な事業内容 (日本標準産業分類 中分類)	本文書における呼称	従業員数
電気業	ヒアA社	10001名~
	ヒアB社	10001名~
	ヒアC社	10001名~
	ヒアD社	10001名~
ガス業	ヒアE社	5001~10000名
電子部品・デバイス・電子回路製造業	ヒアF社	10001名~
輸送用機械器具製造業	ヒアG社	10001名~
	ヒアH社	10001名~
化学工業	ヒアI社	5001~10000名
各種商品卸売業	ヒアJ社	10001名~

1.5 スケジュール

- ★事前の調整・準備を行ったうえで、7月以降に順次実証及びヒアリングを推進した。

	4月	5月	6月	7月	8月	9月	10月	
事前準備等	実証で用いる資料等の作成		業界団体、個社との参画等調整					
★3実証				実証に係る作業の推進(順次)		ヒアリング等	とりまとめ	
★4実証				実証に係る作業の推進(順次)			ヒアリング等	とりまとめ
ヒアリング等					ヒアリング調査の推進(順次)		とりまとめ	

2. 実証の詳細内容

2.1 事前準備

2.2 ★3

2.3 ★4

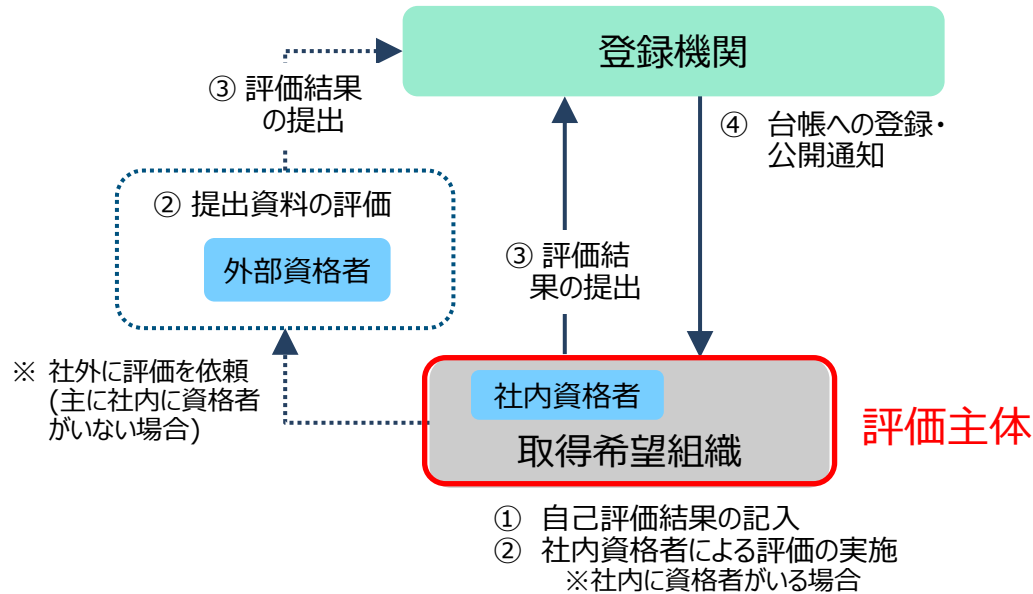
2.4 発注元企業へのヒアリング

2.1 事前準備 — ★3・★4 評価スキーム(案)の確認

- 本年4月に公表した中間とりまとめで提示した評価スキーム案に基づき、本実証では★3・★4で想定される一連の流れを試行し、運用上生じ得る具体的な課題を特定することとした。

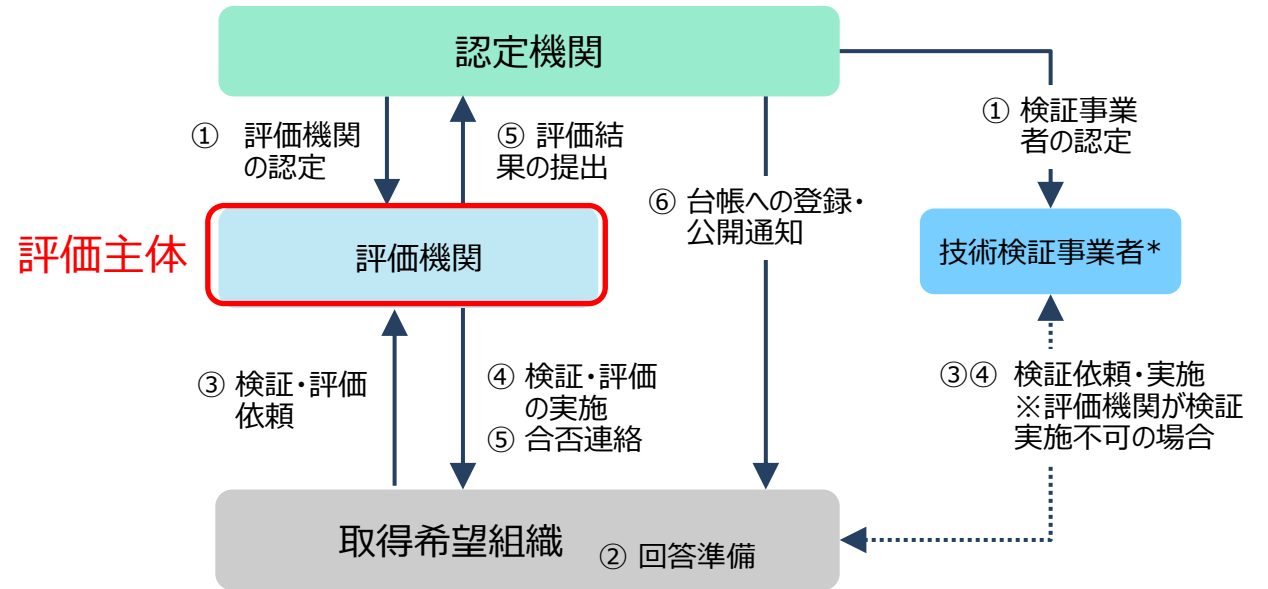
自己評価：★3

- ① 取得希望組織は、★3要求事項に基づき自己評価を記入（必要に応じ、社内外の資格者の助言を得る）
- ② 社内外の資格者は、記入内容を評価、要求事項に対する合否を判断
- ③ 取得希望組織または社内外の資格者は、登録機関に評価結果を提出
- ④ 登録機関は、申請内容に問題が認められない場合には台帳に登録・公開



第三者評価：★4

- ① 認定機関は、評価機関・技術検証事業者を認定
- ② 取得希望組織は、★4要求事項に基づき回答を準備
- ③ 取得希望組織は、評価機関または技術検証事業者に、検証・評価を依頼
- ④ 評価機関または技術検証事業者は、検証・評価を実施
- ⑤ 評価結果を取得希望組織に通知し、認定機関に提出
- ⑥ 認定機関は、「合格」とされた組織を台帳に登録し、公開



* ★4で求められる技術的対策の一部について、脆弱性診断等の実機検証を行う事業者

2.1 事前準備 — 実証で用いる資料等の作成

- 前頁に示した評価スキームの試行を行うにあたって、実証の各工程で作業に必要と考えられる資料等を作成した。

分類	想定利用者	作成資料	前頁における対応タスク
★3・★4実証共通	全体	✓ 守秘義務に関する誓約書	-
★3実証	取得希望組織	✓ 適用範囲に関する質問事項 ✓ ★3取得希望組織向けアセスメントシート	①自己評価結果の記入
	専門家	✓ ★3専門家向けアセスメントシート	②社内外資格者による評価の実施
★4実証	取得希望組織	✓ 適用範囲に関する質問事項 ✓ ★4取得希望組織向けアセスメントシート	②回答準備
	評価機関等	✓ ★4評価機関向けアセスメントシート ✓ 第三者評価及び技術検証に関するガイダンス ✓ 第三者評価報告書テンプレート	④検証・評価の実施 ⑤合否連絡
ヒアリング	発注元企業	✓ ヒアリングシート	-

2.1 事前準備 — 実証等で確認する項目の整理

- 制度のさらなる具体化に向けて実証において確認すべき事項の整理を行った。

分類	実証等で行う確認の観点	確認項目	
★3実証	要求事項・評価基準案の実施可能性	<ul style="list-style-type: none"> ✓ 要求事項・評価基準案ごとの遵守/不遵守比率 ✓ 不遵守とされた評価基準案の追加実装等におけるハードル等 	
	対策、評価の実施等に係る工数及びコスト等	参画企業による自己評価等 参画企業による自己評価等 ★3専門家による確認	<ul style="list-style-type: none"> ✓ 適用範囲の検討、アセスメントシートの記入に要した工数 ✓ 作業実施にあたり直面した困難 ✓ 参画企業又は当該企業と取引のあるITベンダー等における専門家(本実証においては情報処理安全確保支援士等)の在籍状況 ✓ アセスメントシートの確認に要した工数 ✓ アセスメントシートの改善事項(確認時に判断が困難だった点等)
	制度に関する規定等のわかりやすさ	<ul style="list-style-type: none"> ✓ 適用範囲の検討、アセスメントシートの記入における不明点・疑問点 	
	要求事項・評価基準案の実施可能性	<ul style="list-style-type: none"> ✓ 要求事項・評価基準案ごとの遵守/不遵守比率 ✓ 不遵守とされた評価基準案の追加実装等におけるハードル等 	
★4実証	要求事項・評価基準案の実施可能性	<ul style="list-style-type: none"> ✓ 要求事項・評価基準案ごとの遵守/不遵守比率 ✓ 不遵守とされた評価基準案の追加実装等におけるハードル等 	
	対策、評価の実施等に係る工数及びコスト等	参画企業による自己評価等 参画企業による自己評価等 ★4評価機関による第三者評価等	<ul style="list-style-type: none"> ✓ 適用範囲の検討、アセスメントシートの記入に要した工数 ✓ 作業実施にあたり直面した困難 ✓ アセスメントシート確認、实地審査及び技術検証に要した工数(実施に際して要した社内調整等の工数を含む) ✓ 所定工数内で第三者評価又は技術検証として実施可能であった範囲 ✓ アセスメントシートの改善事項(確認時に判断が困難だった点等)
	制度に関する規定等のわかりやすさ	<ul style="list-style-type: none"> ✓ 適用範囲の検討、アセスメントシートの記入における不明点・疑問点 	
	要求事項・評価基準案の実施可能性	<ul style="list-style-type: none"> ✓ 要求事項・評価基準案ごとの遵守/不遵守比率 ✓ 不遵守とされた評価基準案の追加実装等におけるハードル等 	
発注元 ヒアリング	現行の取引先等に向けたセキュリティ施策との整合性	<ul style="list-style-type: none"> ✓ 同左 	
	本制度の利用拡大に向けて官民で講ずべき施策の方向性	<ul style="list-style-type: none"> ✓ 同左 	

2. 実証の詳細内容

2.1 事前準備

2.2 ★3実証

2.2.1 実施概要

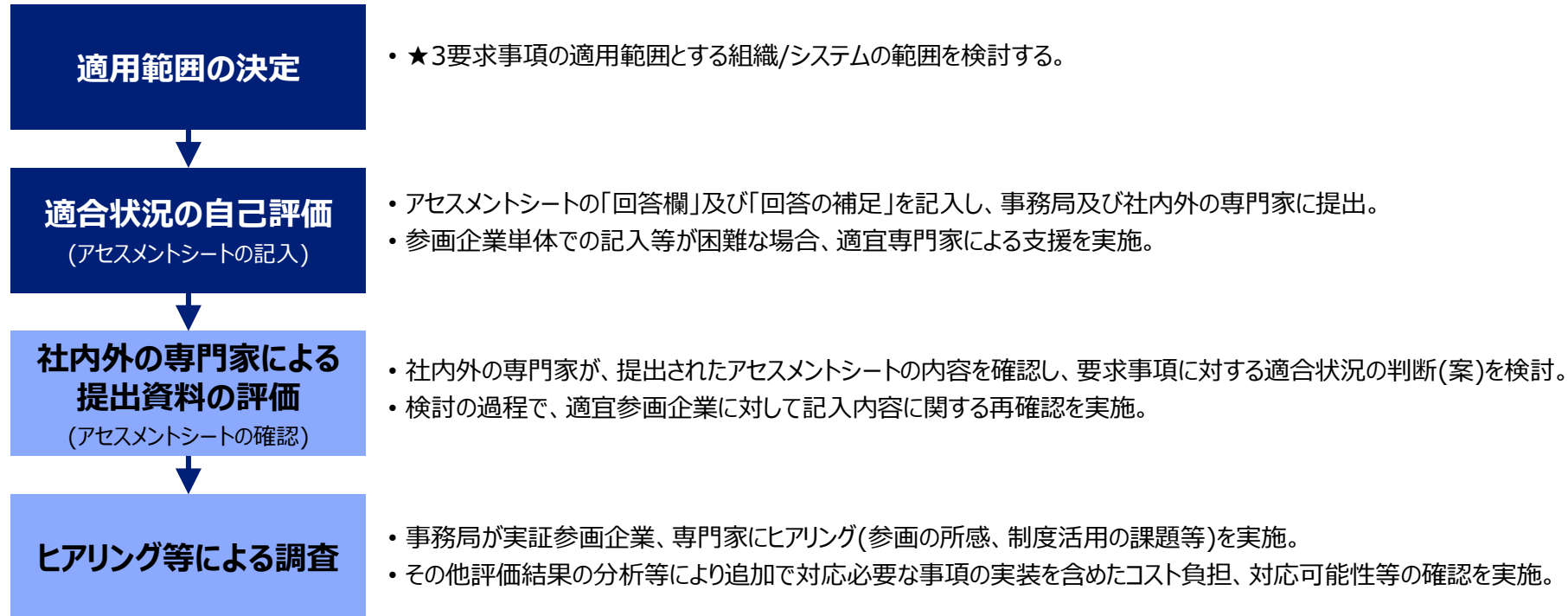
2.2.2 実施結果

2.3 ★4実証

2.4 発注元企業へのヒアリング

2.2.1 ★3実証の実施概要 — 全体像

- 自己評価の実施及び専門家による確認等、★3取得に必要とされるプロセスを一通り試行しつつヒアリング等を行うことで、前項で述べた制度のさらなる具体化に向けて必要な情報を収集した。



*1 本頁で「専門家」とされている者は、基本的に同一人物を指す。

[凡例] ■ : 主に実証参画企業に実施いただいた事項 ■ : 実証参画企業にご協力いただいた事項(主たる検討は事務局又は専門家にて実施)

2.2.1 実証の実施概要 — 適用範囲の決定

- 「適用範囲の決定」にあたっては、実証参画団体に対して適用範囲について質問を行うとともに、記入者や質問への回答に要した時間や困難に直面した事項、直面した概要についても回答いただいた。

適用範囲に係る質問事項

No.	質問事項
1	適用範囲は、貴社又は貴社が属する企業グループ等の全体をカバーしていますか？[YES/NO]
2	貴社又は貴社が属する企業グループ等の全体を適用範囲としない場合、適用範囲はどのように提示されますか？[記述式]
3	適用範囲から除外する範囲について、適用範囲との間でどのような保護措置を講じていますか？[記述式]
4	適用範囲には、貴社からグループ企業その他の取引先等の内部システムへ接続する際の境界となるネットワーク機器は含まれていますか？[YES/NO]
4-1	4.がYESの場合、それらにはどのような保護措置を講じていますか？[記述式]
5	IT基盤を構成し得る以下の構成要素を、適用範囲に含んでいますか？ - クラウドサービス - BYOD(業務利用される個人所有の端末) - 在宅勤務に用いられるIT機器
6	本評価の対象となる貴社の事業拠点の地理的所在地を記載してください。 [記述式]

その他質問事項

No.	項目	確認項目
1	会社情報について	<ul style="list-style-type: none"> 会社名
2	記入者について	<ul style="list-style-type: none"> 氏名 所属 サイバーセキュリティ関連業務の経験年数 保有資格
3	質問への回答作業について	<ul style="list-style-type: none"> 回答作成の所要時間 回答作成にあたって困難に直面した事項 直面した困難の概要
4	その他	<ul style="list-style-type: none"> 本実施内容に関わるご要望等

2.2.1 実証の実施概要 — 適合状況の自己評価

- 「適合状況の自己評価」にあたっては、★3における25件の要求事項、78件の評価基準に関して、「対策実施のためのガイダンス」も参考にさせていただきつつ、実証参画企業にアセスメントシートの所定欄に記入いただく形で自己評価いただいた。

参画企業向けアセスメントシートの抜粋

実証参画企業記入欄

大分類	中分類	★ 3 N O.	要求事項(案)	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答 タイプ	回答欄 ・回答を記載 - 回答のタイプがYes/Noの場合、「はい」か「いいえ」を記載した上で、回答の補足欄に補足事項を記載（必須） - 回答のタイプが選択の場合、選択結果を記載。補足事項があれば回答の補足欄に記載（任意） - 回答のタイプが記述式の場合、対策の実施内容を記載。補足事項があれば回答の補足欄に記載（任意）	回答の補足 質問のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
	役割/責任/権限	1	セキュリティ推進活動を担当する部署及び役員、従業員を決定し、責任及び権限を割り当てること。	セキュリティを統括する役員(CISO等)やセキュリティ担当部署を決めて、その役割・責任を明確にしていますか。	Yes/No			・情報セキュリティ関連規程に記載することが考えられる。 ・情報セキュリティ体制図を作成することも考えられる。
				平時のセキュリティ推進活動に必要な連絡先リストを作成していますか。	Yes/No			・連絡先リストは以下の観点で作成することが考えられる。 - 社内からの情報セキュリティに関するルールなどについての問い合わせを受ける窓口を明確にする - 情報セキュリティ担当部署からの社内向け周知事項、依頼事項を連絡する際のルートが目的・対象範囲別に整理する - 情報セキュリティ責任者や、システム管理者の連絡先を明確にする

2.2.1 実証の実施概要 — 専門家による提出資料の評価

- 自団体に在籍している場合には、その情報処理安全確保支援士が文書審査を行った。
- 自団体に情報処理安全確保支援士がない場合には、事務局や実証にいただいた情報処理安全確保支援士が文書審査を行った。

★3専門家向けアセスメントシートの抜粋

大分類	中分類	★3 N O	要求事項(案)	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答タイプ	実証参画企業記入欄		★3専門家記入欄		評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例(回答タイプ:記述式のもの)
						回答欄 ・回答を記載 - 回答のタイプがYes/Noの場合、「はい」か「いいえ」を記載した上で、回答の補足欄に補足事項を記載(必須) - 回答のタイプが選択の場合、選択結果を記載。補足事項があれば回答の補足欄に記載 - 回答のタイプが記述式の場合、対策の実施内容を記載。補足事項があれば回答の補足欄に記載(任意)	回答の補足 質問のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称(: 最新の更新日) ・記録の名称 ・その他	評価結果 -適合 -再確認 -不適合から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載(任意) - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載(必須) - [不適合]の場合、評価結果の補足欄にその理由を記載(必須)		
	役割/責任/権限	1	セキュリティ推進活動を担当する部署及び役員、従業員を決定し、責任及び権限を割り当てること。	・セキュリティを統括する役員(CISO等)やセキュリティ担当部署を決めて、その役割・責任を明確にしていますか。	Yes/No						
				・平時のセキュリティ推進活動に必要な連絡先リストを作成していますか。	Yes/No						

2.2.1 実証の実施概要 — ヒアリング等による調査の実施

- ここまでの実証での実施事項を踏まえたうえで、以下のような事項を含むヒアリング等を実施した。

参画企業に対するヒアリング等での確認事項

分類		質問事項(案)
要求事項・評価基準案の実施可能性	要求事項・評価基準	<p>アセスメントシートに記載の要求事項・評価基準のうち、①貴社において費用、その他の観点から導入又は運用が困難と考えられる対策、②導入又は運用は可能だが導入に複数年がかかるような対策がある場合、そのように判断した理由とともにご記載ください。</p> <p>「中小企業の情報セキュリティ対策ガイドライン」や「サイバーセキュリティお助け隊サービス」等の支援策が実施されたとしても中小企業による対応が難しいと考えられる要求事項・評価基準はありますか。それはどの要求事項、評価基準ですか。</p>
	アセスメント記入に必要な知見、スキル	<p>自社内の担当でアセスメントシートを記入することは可能ですか。難しい場合、お取引のあるベンダ等から協力をいただいた上でアセスメントシートを記入することは現実的に可能ですか。</p> <p>支援士のアクティブリスト等が公開された場合、情報処理安全確保支援士に対する相談が行いやすくなると考えられますが、本番運用後に活用することは考えられますか。</p>
対策、評価の実施等に係る工数及びコスト	工数	アセスメントシートを記入する際、アセスメントシートの記入に時間がかかると考えられる要因は何ですか。
	コスト	今回不遵守となった項目について、新たに対応するために想定される対策内容とコスト感(工数と支援期間)を可能な範囲でご教示ください。
制度に関する規定等のわかりやすさ	質問事項・回答欄	評価のためのガイダンスにおいて修正すべき点はありますか。ある場合には理由と修正方針を併せてご教示ください。
制度普及における課題、要望	課題	各企業が★3を取得するにあたり、課題がいくつか想定されますが、制度側が特に解決すべき課題と講じるべき施策にはどのようなものがあるでしょうか。

専門家に対するヒアリング等での確認事項

分類		質問事項(案)
要求事項・評価基準案の実施可能性	要求事項・評価基準	評価を行いにくいと感じた要求事項、評価基準はありますか。また、それはどの要求事項、評価基準ですか。
		アセスメントシートに記載の要求事項・評価基準のうち、①貴社において費用、その他の観点から導入又は運用が困難と考えられる対策、②導入又は運用は可能だが導入に複数年がかかるような対策がある場合、そのように判断した理由とともにご記載ください。
		「中小企業の情報セキュリティ対策ガイドライン」や「サイバーセキュリティお助け隊サービス」の拡充等の支援策が実施されたとしても中小企業による対応が難しいと考えられる要求事項・評価基準はありますか。
対策、評価の実施等に係る工数及びコスト	工数	アセスメントシートの確認は想定工数内で対応は可能でしょうか。対応が難しい場合は、特にどここの部分で工数がかかりますでしょうか。
	コスト	<p>今回は謝金にて対応いただきましたが、実際に評価支援を行う際にどの程度の費用がかかりますか。</p> <p>未遵守の項目について、新たに対応するために情報処理安全確保支援士側で想定される支援内容とコスト(支援工数と支援期間)をご教示ください。</p>
制度に関する規定等のわかりやすさ	質問事項・回答欄	質問事項・回答欄(回答欄の補足)において修正すべき点はありますか。ある場合には理由と併せてご教示ください。
	評価のためのガイダンス	<p>評価のためのガイダンスにおいて修正すべき点はありますか。ある場合には理由と修正方針を併せてご教示ください。</p> <p>上記の点について、どのように修正すべきですか。</p>
制度普及	課題	各企業が★3を取得するにあたり、課題がいくつか想定されますが、制度側が特に解決すべき課題と講じるべき施策にはどのようなものがあるでしょうか。

2. 実証の詳細内容

2.1 事前準備

2.2 ★3実証

2.2.1 実施概要

2.2.2 実施結果

2.3 ★4実証

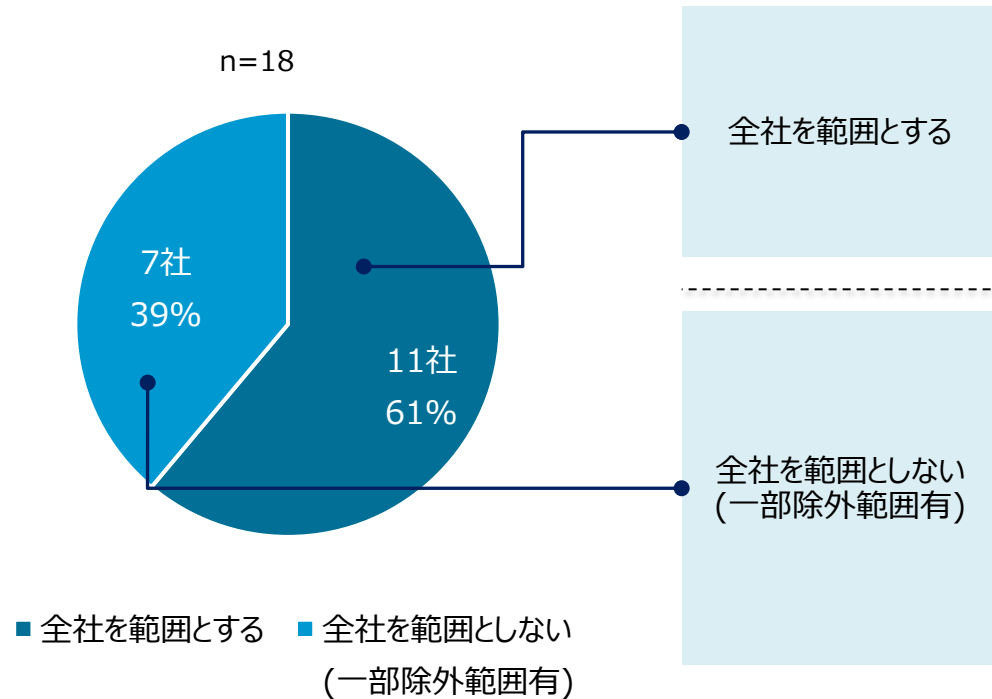
2.4 発注元企業へのヒアリング

2.2.2 実施結果 — 適用範囲の決定

- 実証参画企業の中では、全社を適用範囲とする企業の割合が高い傾向が見られた。
- 適用範囲外を設ける場合、ファイアウォール又はVLANによる通信制御の実施等によりネットワークを分離を行っていた。

各社回答の集計結果

適用範囲の事例



- 参画企業法人全体を適用範囲とする。

- 適用範囲を除外した主な事例は、以下のとおりである。
 - 一部工場を適用範囲外とする
 - グループ会社は適用範囲外とする
 - オフラインで運用しているシステムやグループ別法人の端末は適用範囲外とする
- 上記のような適用範囲の対象外を設けた企業については、以下の2通りの方法により、ネットワークの分離等を実施していた。
 - ファイアウォールやVLANにより、適用範囲内外の通信を制御する
 - ネットワーク基盤そのものを別々のものとする

2.2.2 実施結果 — 適合状況の自己評価

- 実証参画企業の中では、全社を適用範囲とする企業の割合が高い傾向が見られた。
- 適用範囲外を設ける場合、ファイアウォール又はVLANによる通信制御の実施等によりネットワークを分離を行っていた。

分類		企業全体の 遵守率	企業規模(従業員数)別の評価基準における平均遵守率 (単位:名)			
			1~50	51~100	101~1000	1001~
ガバナンスの整備	役割/責任/権限	94%	90%	90%	100%	96%
	ポリシー	88%	83%	67%	100%	100%
	監督	72%	75%	33%	100%	80%
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	68%	75%	42%	75%	80%
リスクの特定	資産管理	70%	70%	45%	90%	74%
攻撃等の防御	アイデンティティ管理とアクセス制御	65%	67%	43%	69%	81%
	意識向上及びトレーニング	80%	63%	58%	100%	100%
	データセキュリティ	61%	62%	56%	43%	85%
	プラットフォームセキュリティ	63%	72%	50%	44%	85%
	技術インフラのレジリエンス	61%	62%	56%	43%	85%
攻撃等の検知	継続的モニタリング	70%	56%	63%	75%	85%
インシデントへの対応	インシデントマネジメント	72%	67%	44%	75%	100%
全体の平均		70%	68%	52%	73%	85%

[傾向1]

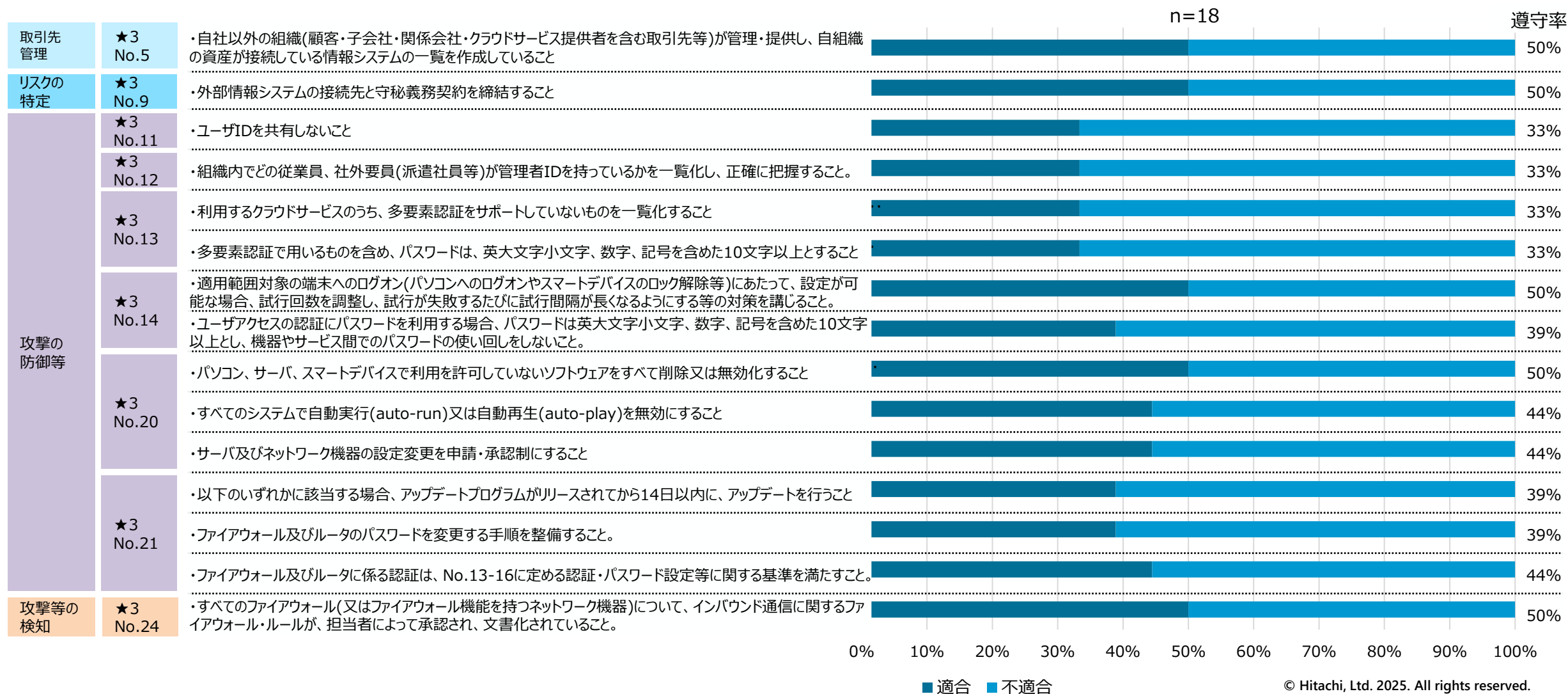
- 技術的対策の実装が求められる事項については、相対的に遵守率が低くなっている。

[傾向2]

- 概ね企業規模が大きくなるほど全体平均の遵守率も増加している。

2.2.2 実施結果 — 適合状況の自己評価

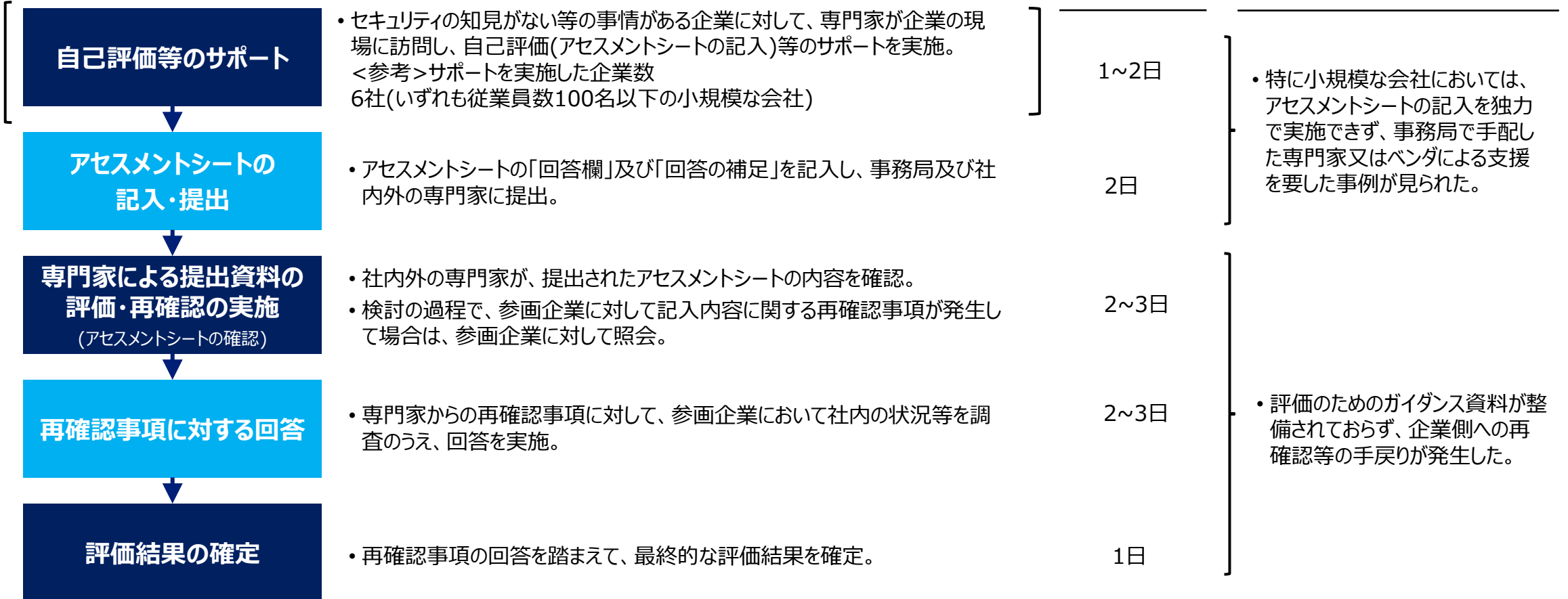
- 参画企業において遵守率が相対的に低いと考えられる(遵守率50%以下)評価基準は以下のとおりであった。



2.2.2 実施結果 — 社内外の専門家による提出資料の評価

- 各専門家において、概ね以下の流れで評価を実施いただいた。
- 特に★3企業では、セキュリティに関する知見不足等の事情により、専門家による自己評価のサポートが必要な事例が存在した。

※ 一部企業に限る。



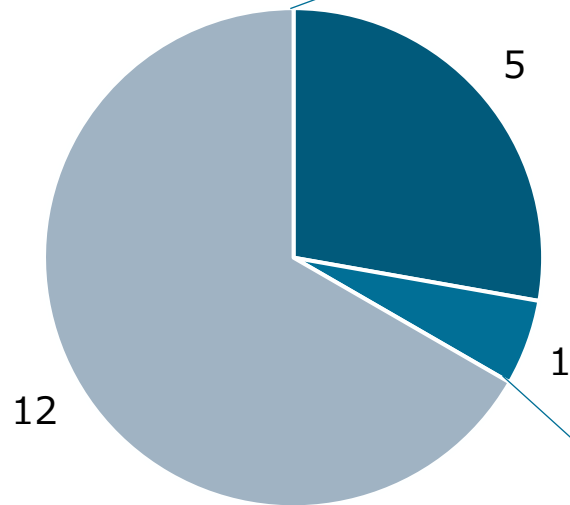
- セキュリティの知見がない等の事情がある企業に対して、専門家が企業の現場に訪問し、自己評価(アセスメントシートの記入)等のサポートを実施。
<参考>サポートを実施した企業数
6社(いずれも従業員数100名以下の小規模な会社)
- アセスメントシートの「回答欄」及び「回答の補足」を記入し、事務局及び社内外の専門家に提出。
- 社内外の専門家が、提出されたアセスメントシートの内容を確認。
検討の過程で、参画企業に対して記入内容に関する再確認事項が発生して場合は、参画企業に対して照会。
- 専門家からの再確認事項に対して、参画企業において社内の状況等を調査のうえ、回答を実施。
- 再確認事項の回答を踏まえて、最終的な評価結果を確定。

2.2.2 実施結果 — [参考]社内外の専門家による提出資料の評価

- ★3実証参画団体内だけでなく、取引のあるベンダにおいても情報処理安全確保支援士は在籍していない団体が多い。
- また、自社または取引のあるベンダに情報処理安全確保支援士が在籍したとしても、実証に参画いただけなかったケースがみられた。

情報処理安全確保支援士の在籍状況

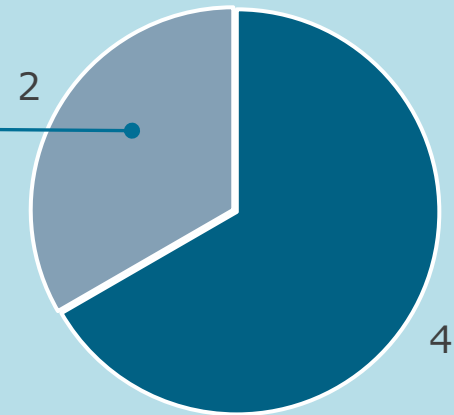
[単位：社]



- 自社に在籍
- 自社には在籍していないが、取引のあるベンダには在籍
- 自社及び取引のあるベンダのどちらにも在籍していない

情報処理安全確保支援士の実証へ参加有無

[単位：社]



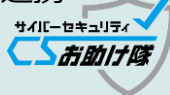



■ 実証に参加 ■ 実証に不参加

不参加の理由

- 取引先のベンダに在籍しているが、営業支援の範疇を越えていることを理由に参加を断られた。(★3I社)
- 資格を保有しているものの、実績面で不安がある(★3Q社)

2.2.2 実施結果 — ヒアリング等による調査の実施

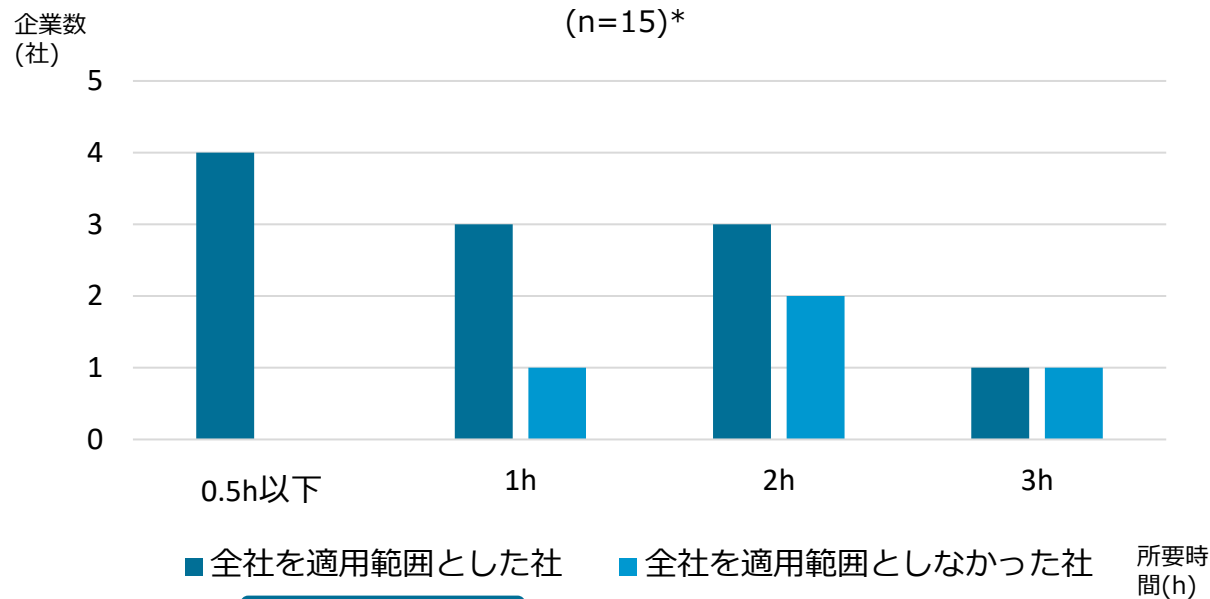
- ヒアリングを通じて、★3実証に参画いただいた企業からは主に、①★3取得のためのコスト、②要求事項・評価基準の内容理解、③他制度との連携についてそれぞれ意見を頂戴した。

		参画企業からの主な意見	想定される今後の対応
要求事項・ 評価基準の 実施可能性	実施の難しい要求 事項・評価基準	<ul style="list-style-type: none"> パッチ・アップデート適用に係る要求事項について、評価基準ごとの対応期限内の対応が困難である。 どのようなツールを導入すれば★3を達成できるかについて、必要な製品・ツールを整理してほしい。 	<p>お助け隊サービス等の中小企業支援施策との連携</p>  <p>要求事項の内容について妥当性の精査</p>  <p>各種資料の整備</p>  <p>他制度との連携促進</p> 
	お助け隊サービス 等への期待	<ul style="list-style-type: none"> お助け隊サービスにおいて、★3達成のための相談窓口を設置してほしい ★3に対応した規程類のひな形を整備してほしい。 	
	自己評価の実施 可能性	<ul style="list-style-type: none"> アセスメントシートの内容について不明点があり、専門家やベンダ等のの補助が必要な場合があった。 	
工数及びコ スト	工数	<ul style="list-style-type: none"> アセスメントシートの内容を理解するのに工数を要した。 他部署も含め、社内の状況を調査するのに工数を要した。 	各種資料の整備
	コスト	<ul style="list-style-type: none"> IT資産管理ツールの導入について、費用を要することが懸念 遠隔地バックアップについては、現行のストレージを統合する必要がある、コストが懸念である。 	
規定等の わかりやすさ		<ul style="list-style-type: none"> アセスメントシートについて各質問の回答例があるとよい。 自工会ガイドラインとの対応関係について明確にしてほしい。 	他制度との連携促進
課題、要望		<ul style="list-style-type: none"> ★3取得に必要な対策コストについて、経営層への理解を深めていってほしい。 自工会ガイドラインとの統一を図ってほしい。 	他制度との連携促進

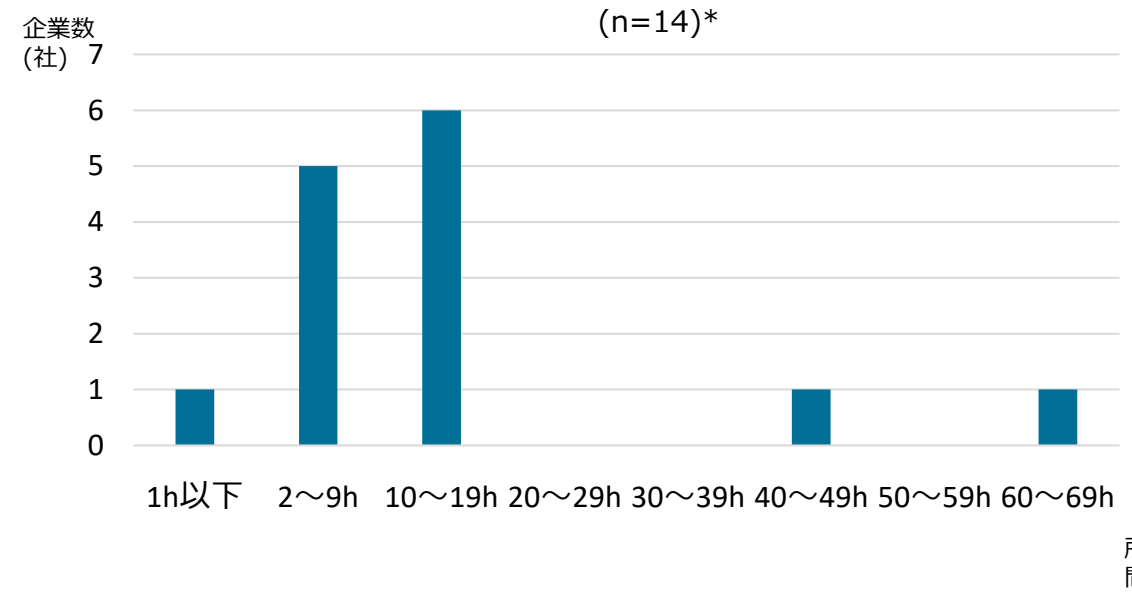
2.2.2 実施結果 — 実施工数

- 適用範囲の決定については、★3企業では全社が3時間以内に実施
(※適用範囲の除外設定有無による大きな工数の差は見られなかった)
- アセスメントシートの記入については、★3では2社を除いて19時間以内に実施

適用範囲の決定



自己評価(アセスメントシートの作成)



工数を要した要因

ヒアリング等による参画企業への調査の結果、工数を要した要因として主に以下の2点が考えられる。

- ✓ サイバーセキュリティ及び制度に関する知見不足により、アセスメントシート等の関連資料の読み込みに時間を要した。
- ✓ セキュリティ担当部門に社内の情報が集約されておらず、人事部門や総務部門等の社内関連部門に対して調査を実施する必要があった。

*工数のデータを収集することができた企業のみ集計

2. 実証の詳細内容

2.1 事前準備

2.2 ★3実証

2.3 ★4実証

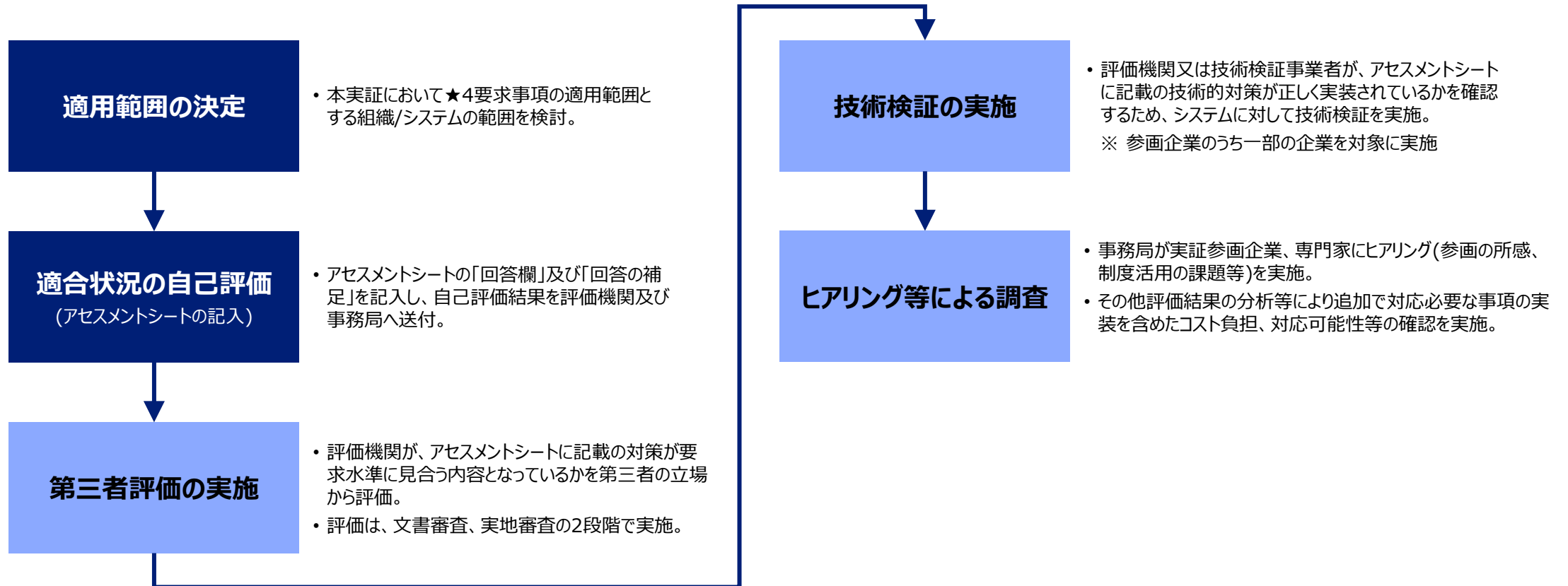
2.3.1 実施概要

2.3.2 実施結果

2.4 発注元企業へのヒアリング

2.3.1 ★4実証の実施概要 — 全体像

- 自己評価の実施及び専門家による確認等、★4取得に必要とされるプロセスを一通り試行しつつヒアリング等を行うことで、述べた制度のさらなる具体化に向けて必要な情報を収集した。



2.3.1 実証の実施概要 — 適用範囲の決定 [再掲]

- 「適用範囲の決定」にあたっては、実証参画団体に対して適用範囲について質問を行うとともに、記入者や質問への回答に要した時間や困難に直面した事項、直面した概要についても回答いただいた。

適用範囲に係る質問事項

No.	質問事項
1	適用範囲は、貴社又は貴社が属する企業グループ等の全体をカバーしていますか？ [YES/NO]
2	貴社又は貴社が属する企業グループ等の全体を適用範囲としない場合、適用範囲はどのように提示されますか？ [記述式]
3	適用範囲から除外する範囲について、適用範囲との間でどのような保護措置を講じていますか？ [記述式]
4	適用範囲には、貴社からグループ企業その他の取引先等の内部システムへ接続する際の境界となるネットワーク機器は含まれていますか？ [YES/NO]
4-1	4.がYESの場合、それらにはどのような保護措置を講じていますか？ [記述式]
5	IT基盤を構成し得る以下の構成要素を、適用範囲に含んでいますか？ - クラウドサービス - BYOD(業務利用される個人所有の端末) - 在宅勤務に用いられるIT機器
6	本評価の対象となる貴社の事業拠点の地理的所在地を記載してください。 [記述式]

その他質問事項

No.	項目	確認項目
1	会社情報について	<ul style="list-style-type: none"> 会社名
2	記入者について	<ul style="list-style-type: none"> 氏名 所属 サイバーセキュリティ関連業務の経験年数 保有資格
3	質問への回答作業について	<ul style="list-style-type: none"> 回答作成の所要時間 回答作成にあたって困難に直面した事項 直面した困難の概要
4	その他	<ul style="list-style-type: none"> 本実施内容に関わるご要望等

2.3.1 実証の実施概要 — 適合状況の自己評価 [再掲]

- 「適合状況の自己評価」にあたっては、★4における44件の要求事項、150件の評価基準に関して、「対策実施のためのガイダンス」も参考にさせていただきつつ、実証参画企業にアセスメントシートの所定欄に記入いただく形で自己評価いただいた。

参画企業向けアセスメントシートの抜粋

大分類	中分類	★ 3 N.O.	要求事項(案)	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答 タイプ	実証参画企業記入欄		
						回答欄 ・回答を記載 - 回答のタイプがYes/Noの場合、「はい」か「いいえ」を記載した上で、回答の補足欄に補足事項を記載（必須） - 回答のタイプが選択の場合、選択結果を記載。補足事項があれば回答の補足欄に記載（任意） - 回答のタイプが記述式の場合、対策の実施内容を記載。補足事項があれば回答の補足欄に記載（任意）	回答の補足 質問のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	
	役割/責任/権限	1	セキュリティ推進活動を担当する部署及び役員、従業員を決定し、責任及び権限を割り当てること。	セキュリティを統括する役員(CISO等)やセキュリティ担当部署を決めて、その役割・責任を明確にしていますか。	Yes/No			<ul style="list-style-type: none"> 情報セキュリティ関連規程に記載することが考えられる。 情報セキュリティ体制図を作成することも考えられる。
				平時のセキュリティ推進活動に必要な連絡先リストを作成していますか。	Yes/No			<ul style="list-style-type: none"> 連絡先リストは以下の観点で作成することが考えられる。 <ul style="list-style-type: none"> 社内からの情報セキュリティに関するルールなどについての問い合わせを受ける窓口を明確にする 情報セキュリティ担当部署からの社内向け周知事項、依頼事項を連絡する際のルートが目的・対象範囲別に整理する 情報セキュリティ責任者や、システム管理者の連絡先を明確にする

2.3.1 実証の実施概要 — 第三者評価の実施

- 実証に参画いただいた各第三者評価機関が実証参画団体に対して、文書審査、実地審査等を行った。

★4第三者評価における実施事項

項目		実施事項	想定所要時間
第三者評価	文書審査	<ul style="list-style-type: none"> • 質問事項への回答の確認(アセスメントシートのみを参照) 	<ul style="list-style-type: none"> • 1人日程度
	実地審査 (リモートも可)	<ul style="list-style-type: none"> • 重要性が認められるが、技術検証の範囲にないものについて証跡の確認を含めた評価を実施。 [現地審査で確認すべき事項(例)] <ul style="list-style-type: none"> ✓ セキュリティ担当部署・従業員の決定 ✓ 定期的な経営層への対策実態報告 ✓ 脆弱性の管理体制、管理プロセス ✓ セキュリティインシデント対応手順 ✓ 事業継続要件に沿った復旧準備 	<ul style="list-style-type: none"> • 1人日程度
技術検証		<ul style="list-style-type: none"> • セキュリティアップデート管理等に係る要求事項について実機検証(次頁に示す脆弱性診断等)を実施 	<ul style="list-style-type: none"> • 1~2人日程度

2.3.1 実証の実施概要 — 技術検証の実施

- 実証に参画いただいた各第三者評価機関が実証参画団体に対して、文書審査、実地審査等を行った。

No.	名称	検証対象	実施内容の概要(現時点の想定)
1	リモート診断 (外部診断)	<ul style="list-style-type: none"> • 対象企業が利用する全ての外部公開IPアドレス(グローバルIPアドレス) • 上記を推奨されるTCP及びUDPポートでスキャンした結果発見されたインターネット経由でアクセス可能なサービス 	インターネットを介した攻撃者が一般的かつ高度なスキルを要しない方法で企業の内部システムに侵入できるかを検証する。
2	サーバ、端末における パッチ適用の確認 (内部診断)	<ul style="list-style-type: none"> • サンプルされたエンドユーザ端末、サーバ、IaaSインスタンス 	適用範囲内に残存した悪用可能性のある、未修正の脆弱性を特定する。

2.3.1 実証の実施概要 — ヒアリング等による調査の実施

- ここまでの実証での実施事項を踏まえたうえで、以下のような事項を含むヒアリング等を実施した。

参画企業に対するヒアリング等での確認事項

分類		質問事項(案)
適用範囲の決定		柔軟に適用範囲を設定可能な仕組みは貴社が今後本制度に基づく対応を進める場合に有効でしょうか。 適用範囲を決定する際、今回実証用に提示した資料以外で、制度側から提示すべき情報としてどのようなものが挙げられるでしょうか。
要求事項・評価基準案の実施可能性	要求事項・評価基準	現状の要求事項・評価基準のうち、①費用、その他の観点から導入等が困難と考えられる対策、②導入に複数年がかかるような対策はあるか。 現状の要求事項・評価基準以外で、★4取得に際して対応すべき対策事項(標準的なセキュリティ対策)として追加すべきものがあるでしょうか。
	アセスメントシート記入	アセスメントシートへの記入をより円滑に行うために、どのような情報をさらに充実させるべきか、実証にて対応に苦慮されたポイントとともにご記載ください。
実地審査	工数	実地審査について、今後制度化までに解決すべき懸念、関連して制度にて規定すべき事項等あればご教示いただけないでしょうか。
	コスト	制度では実証で実施したものと同様、1~2日程度での実地審査を予定していますが、コスト負担や制度の信頼性等の観点から見て妥当でしょうか。
技術検証		今回実施した2件のテストを今後★4取得時に求める点について、被評価側によるコストその他の負担等に鑑みて妥当と言えるでしょうか。 技術検証を実施する際、今回実証用に提示した資料以外で、制度側からどのような情報を提示すべきでしょうか。
その他	制度側へのご要望等	普及支援策として制度側から最低限対応してほしい事項、可能であれば対応してほしい事項をご教示いただけないでしょうか。
	★5に係るご要望等	★5にて踏まえるべき基準(例：自工会ガイドライン LV3)及び具体的に盛り込むべき対策、評価の実施内容や実施方法などについてご意見があればご記載ください。

評価機関に対するヒアリング等での確認事項

分類		質問事項(案)
要求事項・評価基準案の実施可能性	要求事項・評価基準	評価を行っていくと感じた要求事項、評価基準はありますか。また、それはどの要求事項、評価基準ですか。
	技術検証	今回実施した2件のテストを今後★4取得時に求める点について、被評価側によるコストその他の負担等に鑑みて妥当と言えるでしょうか。妥当とは言えない点がある場合、具体的にどの点に改善が必要かをご教示ください。 技術検証を実施する際、今回実証用に提示した資料以外で、制度側からどのような情報を提示すべきでしょうか。
	評価に必要な知見、スキル	今回第三者評価を行ったところ、以下の知見、スキルで十分と考えられますか。(以下略) 今回技術検証を行ったところ、以下の知見、スキルで十分と考えられますか。(以下略)
対策、評価の実施等に係る工数及びコスト	工数	今回の実証では、★4に係る評価として、所定工数の範囲内で文書審査、実地審査及び技術検証(※)の実施をお願いいたしましたが、同様の内容を制度の本番運用でも実施すると仮定した場合に、実施内容ごとに想定される工数(対応に必要な人数及び時間数)を改めてご教示いただけないでしょうか。
制度に関する規定等のわかりやすさ	質問事項・回答欄	質問事項・回答欄(回答欄の補足)において修正すべき点はありますか。ある場合には理由と併せてご教示ください。
	評価のためのガイダンス	評価のためのガイダンスにおいて修正すべき点はありますか。ある場合には理由と修正方針を併せてご教示ください。
制度普及	課題	各企業が★3を取得するにあたり、課題がいくつか想定されますが、制度側が特に解決すべき課題と講じるべき施策にはどのようなものがあるでしょうか。

2. 実証の詳細内容

2.1 事前準備

2.2 ★3実証

2.3 ★4実証

2.2.1 実施概要

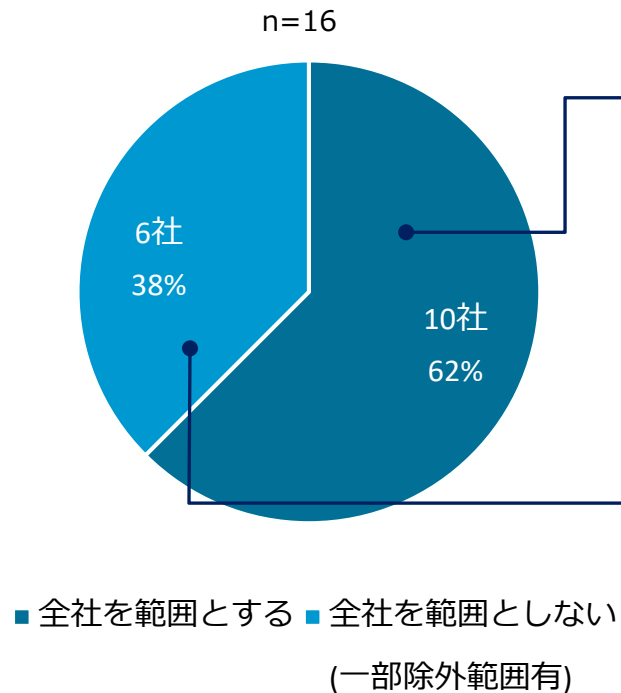
2.2.2 実施結果

2.4 発注元企業へのヒアリング

2.3.2 実施結果 — 適用範囲の決定

- ★3同様、実証参画企業の中では、全社を適用範囲とする企業の割合が高い傾向が見られた。
- 適用範囲外を設ける場合、多くの企業ではファイアウォール又はVLANによる通信制御の実施等によりネットワークを分離を行っていた。

各社回答の集計結果



適用範囲の事例

- 参画企業法人全体を適用範囲とする。
- 共通のネットワーク基盤を利用するグループ全体を適用範囲とする。

- 適用範囲を除外した主な事例は、以下のとおりである。
 - 海外子会社は適用範囲外とする。
 - 国内外グループ会社は適用範囲外とする。
 - 出資率50%未満の国内外グループ会社は適用範囲外とする。
- 上記の企業については、以下の2通りの方法により、ネットワークの分離等を実施
 - ファイアウォールやVLANにより、適用範囲内外の通信を制御する
 - ネットワーク基盤そのものを別々のものとする
- ただし、除外範囲を設けた6社中2社について、上記のようなネットワーク分離を実施できていない事例があった。
(今回の実証の趣旨や今後の評価取得範囲を考慮して適用範囲を決定したことによる。)

2.3.2 実施結果 — 適合状況の自己評価

- ★4企業における全体的な遵守率の状況は以下のとおり。
- 特にサイバーセキュリティサプライチェーンリスクマネジメントに関連する要求事項・評価基準については、遵守率が低い傾向が見られた。

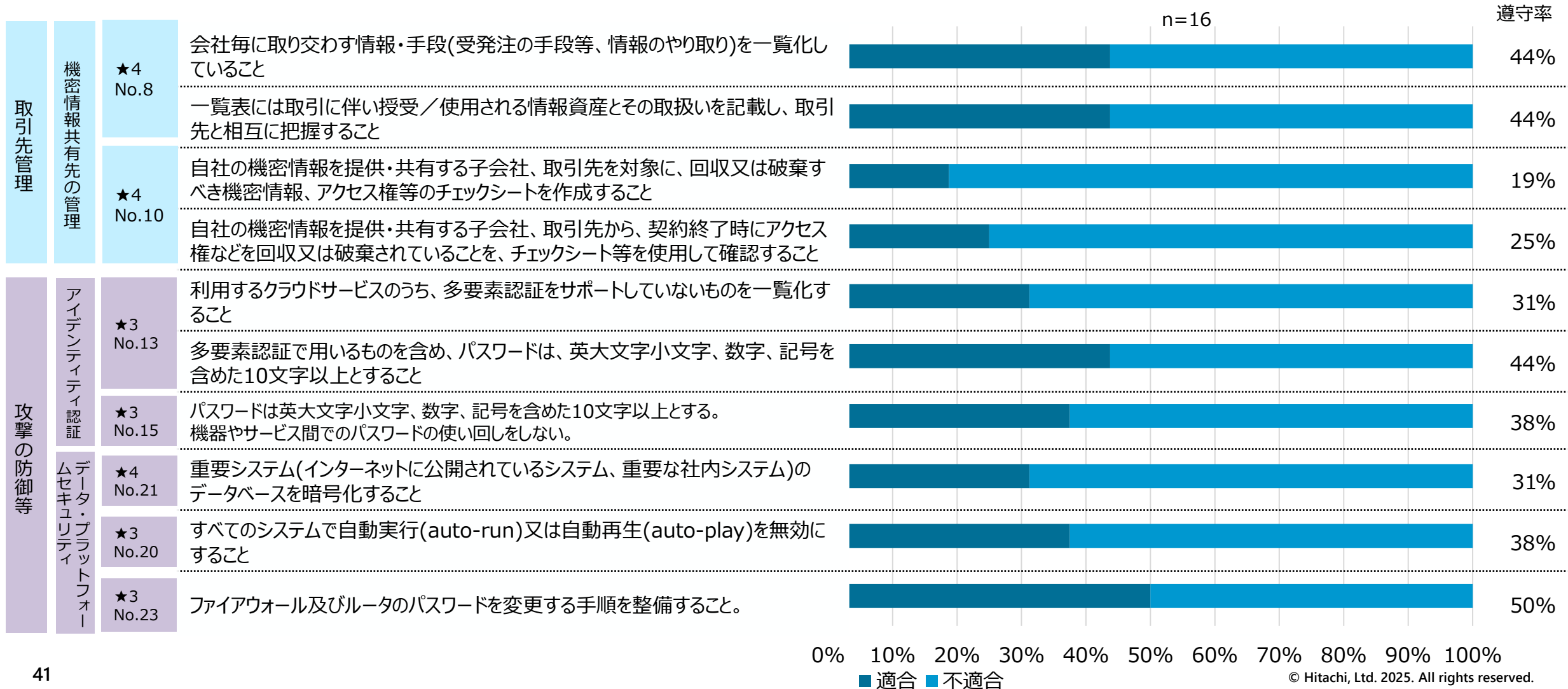
分類		企業全体の遵守率	企業規模(従業員数)別の評価基準における平均遵守率 (単位:名)					
			1~500	501~1000	1001~3000	3001~5000	5001~10000	10001~
ガバナンスの整備	組織的文脈	98%	100%	83%	100%	100%	100%	100%
	役割/責任/権限	99%	100%	100%	100%	95%	100%	100%
	ポリシー	94%	100%	100%	100%	100%	67%	100%
	監督	94%	100%	75%	100%	100%	83%	100%
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	47%	50%	13%	42%	25%	33%	81%
リスク特定	資産管理	91%	100%	84%	90%	94%	88%	94%
	リスクアセスメント	83%	100%	70%	67%	70%	93%	95%
防御	アイデンティティ管理とアクセス制御	82%	82%	60%	84%	77%	87%	86%
	意識向上及びトレーニング	82%	82%	60%	84%	77%	87%	86%
	データセキュリティ	84%	80%	75%	97%	70%	73%	93%
	プラットフォームセキュリティ	78%	88%	65%	80%	74%	86%	75%
	技術インフラのレジリエンス	81%	70%	65%	80%	90%	90%	78%
検知	継続的モニタリング	81%	70%	65%	80%	90%	90%	78%
	有害イベントの分析	91%	50%	50%	100%	100%	100%	100%
対応	インシデントマネジメント	98%	100%	92%	94%	100%	100%	100%
復旧	インシデント復旧計画の実行	100%	100%	100%	100%	100%	100%	100%
全体の平均		85%	88%	70%	87%	82%	87%	90%

[固有で見られた傾向]

- 全体を通じて遵守率が低い
- 従業員数3,000~10,000名の企業で特に遵守率が低く、企業規模が大きいほど取引先が増え、達成を困難にしていることが伺える。

2.3.2 実施結果 — 適合状況の自己評価

- 遵守率が相対的に低いと考えられる評価基準として、各参画企業における自己評価の遵守率が50%以下のものを以下に示す。



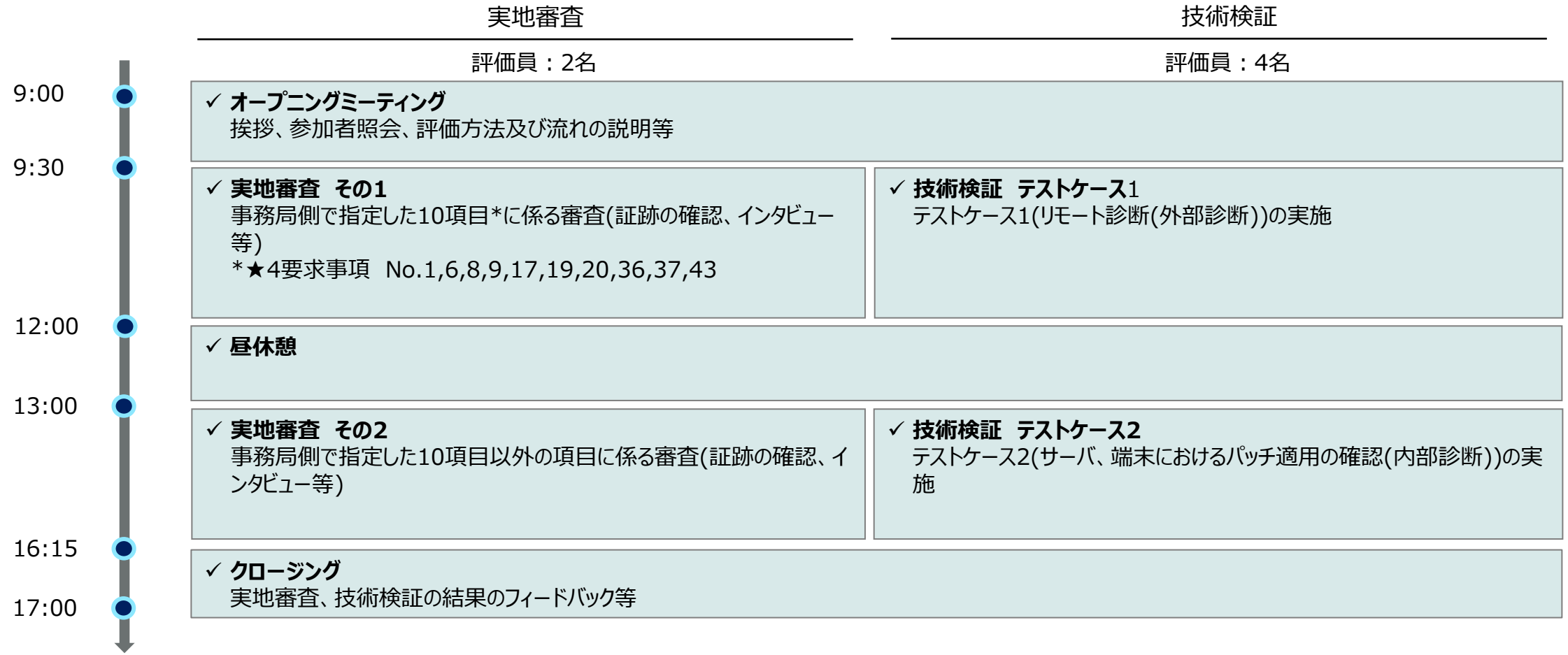
2.3.2 実施結果 — 第三者評価の実施

- 各評価機関において、概ね以下の流れで評価を実施いただいた。

		平均的な工数	各プロセスにおける課題等
審査に係る事前調整	<ul style="list-style-type: none"> 参画企業及び評価機関との間において、今後の審査の進め方等について調整を実施。 必要に応じて審査計画を策定する。 	1~2日	—
文書審査	<ul style="list-style-type: none"> アセスメントシートの記入内容のみを対象とした審査を実施。 検討の過程で、適宜参画企業に対して記入内容に関する再確認を実施。 	1~2日	<ul style="list-style-type: none"> 評価のためのガイダンス資料が整備されておらず、企業側への再確認等の手戻りが発生した。
実地審査	<ul style="list-style-type: none"> 重要性が認められるが、技術検証の範囲にないものについて証跡の確認を実施。 6社中5社は現地に訪問の上、実施。残る1社については、一部遠方の企業においてオンラインによる審査を実施 	1日	<ul style="list-style-type: none"> 概ね問題なく実施
技術検証	<ul style="list-style-type: none"> リモート診断及びパッチ適用の2項目について実機検証等により技術的な確認を実施 	1日	<ul style="list-style-type: none"> P44参照
		※一部参画企業のみ実施	
評価結果の確定	<ul style="list-style-type: none"> 文書審査、実地審査(、技術検証)の結果を踏まえて、最終的な評価結果を確定。 	1日	—

2.3.2 実施結果 — 標準的な実地審査/技術検証の流れ

- 1日で実地審査及び技術検証を実施する場合の標準的な流れは以下のとおりである。






[註]

- 標準的な流れを示したものであり、担当評価機関や被評価企業の状況によって異なることが想定される。
- 実地審査及び技術検証は必ずしも同日に実施する必要はない。

2.3.2 実施結果 — 技術検証の実施

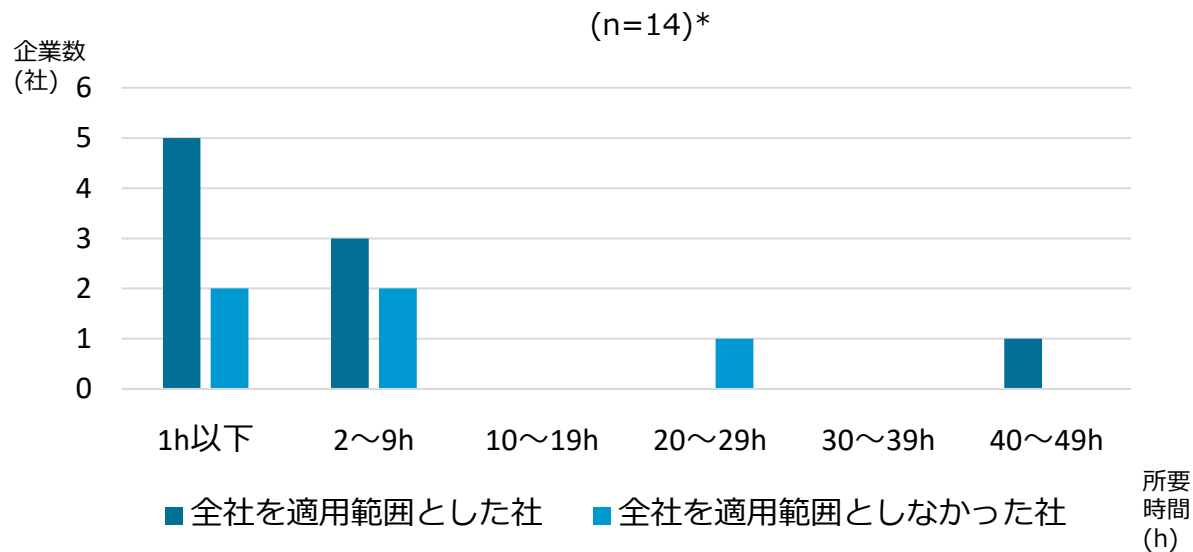
- 実証における技術検証については、以下のような方法により実施した。
- 外部診断と比較して内部診断については、事前調整工数や参画企業への理解を得る点など、多くの課題があった。

検証実施評価機関	技術検証の実施方法		実施に当たって直面した課題等
評価機関B	テストケース1 (外部診断)		<ul style="list-style-type: none"> ✓ 他方、外部診断では相対的に困難は少なかったが、対象IPが多数に渡る場合にツールによる解析に大きな時間を要した。
	テストケース2 (内部診断)	<p>参画企業側から提示された外部公開アドレス及び内部サーバ・端末等から解析対象を抽出(当日現地にて協議)</p> <p>診断ツールを使用し、対象となる外部公開アドレスに対して脆弱性診断を実施</p>	<ul style="list-style-type: none"> ✓ 実証での技術検証を通じて、外部診断と比較して、内部診断の事前調整工数が大いはいほか、現地訪問等による実施期間等の制約も受けやすい。 ✓ 内部機器の脆弱性に対しては、資産管理ツールによる確認等の代替手段を設けられないかとの意見もあった。
評価機関F	テストケース1 (外部診断)	 <p>資産情報一覧及びヒアリングを通じて、診断対象を決定</p> <p>診断ツールを使用し、対象外部公開アドレス脆弱性診断を実施</p> <p>認証に関する設定状況の確認</p>	<ul style="list-style-type: none"> ✓ 対象IPが多数に渡る場合に対象の絞り込みに苦慮した。 ✓ ファイアウォールよりも内部側の機器等について、診断を実施することができなかった。
	テストケース2 (内部診断)	 <p>資産情報一覧及びヒアリングを通じて、診断対象を決定</p> <p>診断対象となるサーバ等に対して診断用ソフトウェアをインストールし診断を実施</p>	<ul style="list-style-type: none"> ✓ サーバ等への診断用ソフトウェアについて、参画企業側の理解を得る点に課題があった。

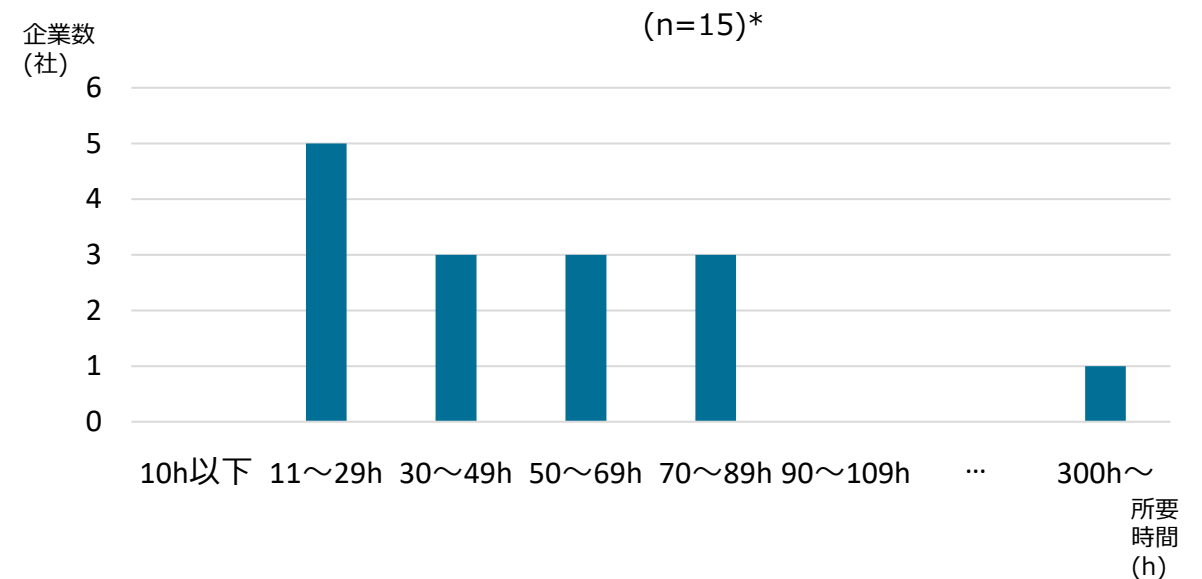
2.3.2 実施結果 — 実施工数

- 適用範囲の決定については、★4企業では2社を除き9時間以内に実施
(※適用範囲の除外設定有無による大きな工数の差は見られなかった)
- アセスメントシートの記入については、★4企業では1社を除き89時間以内に実施。

適用範囲の決定



自己評価(アセスメントシートの作成)



工数を要した要因

ヒアリング等による参画企業への調査の結果、工数を要した要因として主に以下の2点が考えられる。

- ✓ サイバーセキュリティ又は制度に関する知見不足により、アセスメントシート等の関連資料の読み込みに時間を要した。
- ✓ セキュリティ担当部門に社内の情報が集約されておらず、人事部門や総務部門等の社内関連部門に対して調査を実施する必要がある。

*工数のデータを収集することができた企業のみ集計

2.3.2 実施結果 — ヒアリング等による調査の実施

- ヒアリングを通じて、★4実証に参加いただいた企業からは主に、①要求事項及び技術検証実施の内容、②ガイダンス資料の充実、③他制度との連携等についてそれぞれ意見を頂戴した。

参加企業からの主な意見、コメント等

適用範囲の決定		<ul style="list-style-type: none"> 各企業によりネットワーク環境等が異なる場合も想定されることから、企業側で適用範囲を柔軟に選択できる制度としてほしい。 適用範囲決定に当たっての指針や具体例を示してほしい。
自己評価	要求事項・評価基準の内容	<ul style="list-style-type: none"> 主に以下の要求事項・評価基準について、達成が困難である旨の意見が上がった。 <ul style="list-style-type: none"> ✓ 多要素認証の実装 ✓ パスワード桁数の要件 ✓ 全システムでの自動実行・自動再生の無効化 ✓ 重要システムにおけるデータベース暗号化
実地審査		<ul style="list-style-type: none"> 実地審査についてはおおむねスムーズに実施することができた。 実地審査に当たり事前に準備すべき資料等について、予め提示していただきたい。 評価機関向けのガイダンス資料の整備も必要ではないか。
技術検証		<ul style="list-style-type: none"> 技術検証について、自社で実施している脆弱性診断の結果等の証跡を提出することにより代替できないか。
課題、要望	制度への要望	<ul style="list-style-type: none"> 既存の評価制度との統一を図ってほしい。 政府調達要件に組み込むなど、★取得のインセンティブを付与する仕組みを作ってほしい。
	★5への要望	<ul style="list-style-type: none"> 内部不正対策、特権ID管理システムの導入、SOARの導入について追加が望ましい。 ★4で除外された項目(自工会ガイドラインの一部項目、物理的対策等)について追加が望ましい 経営層への意識等、ガバナンス面の強化を図ってほしい。

想定される今後の対応

要求事項の内容について妥当性の精査

大分類	中分類	A3 No.	A4 No.	要求事項(種)
多要素認証	認証方式	1	1	セキュリティに關する事項を考慮し、対応すること。

各種資料の拡充



他制度との連携促進



★5のスキーム等の検討



2. 実証の詳細内容

2.1 事前準備

2.2 ★3

2.3 ★4

2.4 発注元企業へのヒアリング

2.4.1 ヒアリングの実施概要

- 発注元企業に対して、以下の要領でヒアリング調査を行った。

実施目的等

- ✓ 発注元企業における取引先等(グループ会社等を含む)に対するセキュリティ対策の取組み及び本制度との関係性について把握しつつ、発注元企業にとって利用しやすい形で本制度の構築を進めるための示唆を得ること。

[再掲]発注元企業ヒアリングご協力企業 (計10社)

主な事業内容 (日本標準産業分類 中分類)	本文書における呼称	従業員数
電気業	ヒアA社	10001名～
	ヒアB社	10001名～
	ヒアC社	10001名～
	ヒアD社	10001名～
ガス業	ヒアE社	5001～10000名
電子部品・デバイス・電子回路製造業	ヒアF社	10001名～
輸送用機械器具製造業	ヒアG社	10001名～
	ヒアH社	10001名～
化学工業	ヒアI社	5001～10000名
各種商品卸売業	ヒアJ社	10001名～

主なヒアリング項目

分類	質問事項(案)
取組みの背景等	貴社では、取引先等に一定のセキュリティ対策を求める、又は対策状況の確認を行う等のサプライチェーンのサイバーセキュリティ確保に向けた取組みを行っているでしょうか。 (取組みを行っている場合)具体的にどのように取組まれているでしょうか。
取引先等の分類	取引先等に一定のセキュリティ対策を求める、又は対策状況の確認を行う等の取組みを行う際、貴社では、当該取引先の事業上の重要性等に鑑みて、取引先等の分類を行っていますか。 上記では、どのような条件を踏まえ、分類を行っているでしょうか。 本制度で想定している条件(機密情報の提供有無、事業上の重要度、ネットワーク接続の有無)について、貴社による取組みの観点等を踏まえた場合に大きな抜け漏れはないでしょうか。
取引先に対する評価の実施	取引先等に提示している対策事項は具体的にどのようなものでしょうか。特定のガイドライン等を参照されている場合は文書名を含めてご回答ください。 貴社で既に運用されている対策基準等と本制度にて提示している要求事項・評価基準(案)との関係はどのようなものとなっているでしょうか。 貴社では取引先等の対策状況を誰が、いつ、どのように確認されているでしょうか。
遵守状況等のモニタリング	貴社による取引先等の対策状況確認はどのような頻度、方法で実施されているでしょうか。 貴社は取引先のセキュリティ対策状況に関する情報としてどのようなものを取得しているでしょうか。 本制度に関連して、★取得事業者に関する情報として、どのようなものが取得できれば貴社のセキュリティ管理上有用でしょうか。
制度への期待・普及のための施策	貴社及び貴社の属する業界において本制度の活用・普及に当たり、どのような障壁がありますか。また、官民でどのような協力や役割分担をすることを期待しますか。 上記でお伺いしている観点以外で、サプライチェーンのサイバーセキュリティに係る取組みを今後進めようとする際に、発注側として直面し得る課題や政府等に期待する支援等としてどのようなものがあるでしょうか。 本制度が想定する★3、★4の評価実施方法や評価取得後の効果について、貴社の取組との比較の中で、現時点で期待事項や懸念事項はあるでしょうか。

2.4.2 ヒアリングの実施結果

- ・ ヒアリングに参加いただいた発注元企業からは、以下のような意見が上がった。
- ・ とりわけ取引先へのセキュリティ対策については関心が高く、自社の取組への本制度の活用に期待する意見が多く上がった。

参画企業からの主な意見、コメント等

既存の取組	<ul style="list-style-type: none"> ・ 取引先に対して既に★3・★4と同じような、セキュリティ対策を認定するスキームを実施している。 ・ 各契約の中でセキュリティ対策事項の取決めを実施している。 ・ 自社独自の基準を策定し、連結子会社や関連会社等に遵守を依頼している。 ・ 重要性は理解しているものの、現状取引先に対するセキュリティ対策確保の取組は実施できていない。 	
取引先の部類	分類の実施方法	<ul style="list-style-type: none"> ・ 取引先の分類は特段実施していない ・ 株式保有率に応じた関連会社の分類を実施 ・ 個人情報の取り扱いを委託するか否かという観点で分類
	本制度の分類	<ul style="list-style-type: none"> ・ 本制度における取引先の分類について、抜け漏れている観点等は特段ない。
取引先への評価	参照しているガイドライン等	<ul style="list-style-type: none"> ・ 中小企業の情報セキュリティ対策ガイドライン等を参照した対策準を作成 ・ 「個人情報の保護に関する法律についてのガイドライン」を参照した対策準を作成
	評価の実施方法	<ul style="list-style-type: none"> ・ アンケート等を取引先に配布することにより実施している。
制度への期待等	<ul style="list-style-type: none"> ・ 既に実施している取引先への評価の取り組みについては、今後本制度と統合させていきたい ・ 各種制度等と連携を図り、中小企業の負担を軽減してほしい。 ・ ★取得企業については、ホームページ等で一覧化してほしい。 ・ 中小企業が★を取得できるよう、支援施策を推進してほしい。 	

3.実証を通じて得た課題と対応の方向性

3. 実証を通じて得た課題と対応の方向性

- 実証結果として以下のような課題が浮上しており、これらも踏まえて制度に対して必要な見直し及び制度普及に向けた施策を進めていく予定。

	実証を通じて得た課題	今後必要となる対応
制度で用いる要求事項・評価基準	<ul style="list-style-type: none"> ■ ★3・★4実証参画企業において、多くの企業で達成できていない要求事項・評価基準が存在 [実証参画企業において遵守率が低い評価基準の例] <ul style="list-style-type: none"> ✓ 機密情報を共有する取引先一覧の作成 ✓ パスワードの要件 ✓ データベースの暗号化 	<p>1. 要求事項・評価基準の見直し</p> <p>実証の結果を踏まえ、過大であることが考えられる要求事項の内容について見直しを行う。</p>
制度における評価スキーム	<ul style="list-style-type: none"> ■ 実証時点で全要求事項・評価基準を達成していた参画企業はいなかった。 ■ ヒアリングでは、要求事項の一部に、企業が実装するにあたり、多大なコストを要するものが含まれるとの指摘があった。 	<p>2. ★3・★4の取得要件の検討</p> <p>★3・★4の取得条件(評価基準全件への適合が必要か等)について精査を行う。</p>
制度における評価スキーム	<ul style="list-style-type: none"> ■ 実証での技術検証を通じて、外部診断と比較して、内部診断の事前調整工数が大きいほか、現地訪問等による実施期間等の制約も受けやすく、非現実的との指摘あり。 ■ 他方、外部診断では相対的に困難は少なかったが、対象IPが多数に渡る場合にツールによる解析に大きな時間を要する等の指摘があった。 ■ 内部機器の脆弱性に対しては、資産管理ツールによる確認等の代替手段を設けられないかとの意見あり。 	<p>3. 技術検証の実施内容の検討</p> <p>★4における技術検証における実施内容について精査を行う。</p>
制度普及に向けた要望	<ul style="list-style-type: none"> ■ 実証参画企業から、主に以下の観点で制度普及のための支援を求める意見 [支援の要望があった項目の例] <ul style="list-style-type: none"> ✓ 中小企業に対するセキュリティ専門家の派遣支援 ✓ 要求事項・評価基準において策定が求められる各種規程のひな形の整備 ✓ 他制度との連携 	<p>4. 制度普及のための施策推進</p> <p>各業界・企業からの意見等を踏まえ、制度導入促進に向けた取組の具体化を進めていく。</p>

[参考]実証結果を踏まえた要求事項・評価基準の見直し

- 実証を通じて収集した参画企業からの意見等を踏まえ、要求事項・評価基準の改定について以下のとおり見直すことを想定。

対象となる要求事項(例)*1 *2		実証を通じて収集した意見等	見直しの方向性
★3 No.13 ★4 No.20	システムや情報の重要度に応じて認証の強度や実装方法を決定すること。	課題となった評価基準 多要素認証の実装 実証参画企業からの意見(例) ・ 全社員にスマートフォンを配布しておらず、求められる追加要素を利用できない。	評価基準を修正 ・ 多要素認証の追加要素を一定程度拡大(一部の多段階認証を含む)
★3 No.15 ★4 No.22 ★3 No.16 ★4 No.23	パスワード設定に関するルールを定め、周知すること。 パスワードの管理に関するルールを定め、周知すること。	課題となった評価基準 パスワードの設定要件 実証参画企業からの意見(例) ・ パスワードの設定要件を要求事項・評価基準に対応させるためにシステムの改修を要する場合もあり、その場合相当な時間・費用がかかるが見込まれる。	評価基準を修正 ・ 多要素認証等の実装有無に応じてパスワードの設定要件を修正
★4 No.30	情報機器、情報システムの保管データを適切に暗号化するようルールを定め、周知すること。	課題となった評価基準 重要システムのデータベースの暗号化 実証参画企業からの意見(例) ・ 対象システム全てについて暗号化を実施するために相当な費用を要する。 ・ 機密度に応じて暗号化の必要性を判断すべきではないか。	評価基準を修正 ・ 要求事項の目的に鑑み、暗号化の実施を求める対象を機密性の高い保管データに限定
★3 No.20 ★4 No.33	ハードウェア・ソフトウェア等の安全な構成を確立し、維持すること。	課題となった評価基準 全システムでの自動実行・自動再生の無効化 実証参画企業からの意見(例) ・ 全ての端末で一律に設定すると、システム等の動作不良のリスクがある。	評価基準を修正 ・ 各文献等を参照の上、自動実行又は自動再生の無効化を求める対象システム等を限定
★3 No.21 ★4 No.36	ハードウェア・ソフトウェア等へのセキュリティパッチやアップデートの適用に係る手続等を策定し、実行すること。	課題となった評価基準 一定の脆弱性について14日以内のアップデート実施 実証参画企業からの意見(例) ・ 検証期間等を踏まえ、対応期限内にアップデートできない場合が想定される。	代替策の追加 ・ やむを得ず評価基準どおりにアップデートを適用できない場合の代替策を追加
★4 No.44	事業上重要なシステムについて、事業継続の要件に沿った復旧に必要な準備を行うこと。	課題となった評価基準 システム停止時における業務を回復するための対策 実証参画企業からの意見(例) ・ 過去にサイバー攻撃を受けた経験から、セキュリティインシデント発生を念頭に置き業務を継続するための対策(業務代替手段等)を整備することが重要である。	評価基準の追加 ・ サイバー攻撃を念頭にシステム停止時における業務を回復するための対策の整備に係る評価基準を追加

【備考】 *1 要求事項・評価基準案の詳細は別添参照。なお、本ページにおける要求事項No.は、中間とりまとめ公表時点のものを指す。 *2 本ページで記載する要求事項についてはあくまで例示であり、見直しの対象とする要求事項の全てを網羅するものではない。

HITACHI