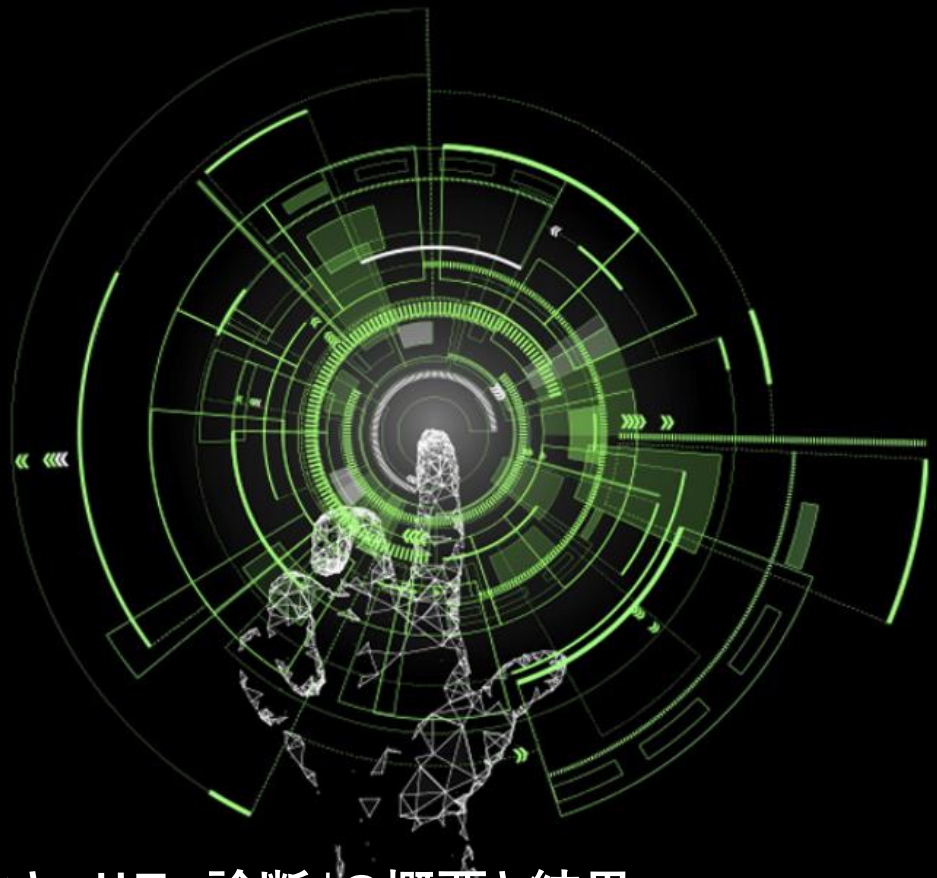


「中小企業等向け情報セキュリティ診断」の概要と結果

愛知県情報セキュリティ対策支援（診断）事業

目次

県内中小企業等を対象にした診断の結果、
多くの企業で情報セキュリティ対策が十分にできていない状況でした。

サマリ

診断内容

【一次診断】
チェックリストの回答による診断
（企業にメールで送付、88社）

【二次診断】
従業員ルールに着目して、企業を訪問して診断（10社）

一次診断結果要約

- 情報セキュリティ対策に対する意識が高い企業は多くあるものの、**43%の企業では情報セキュリティ対策が実施できていない**状態でした。
- 「経営層関与」、「組織対応」、「システム担当者ルール」、「従業員ルール」のカテゴリ別で見ると「経営層関与」のカテゴリについては意識が高い傾向がありましたが、**44%の企業が情報セキュリティ対策の基本方針を策定できていませんでした。**
- 情報セキュリティ対策の検討が進められていない項目において、多くの企業が規定等の必要性を感じているが策定していない状態でした。

二次診断結果要約

- **70%の企業が従業員ルールについての対応が十分に進んでいませんでした。**
- **70%の企業が情報セキュリティ対策の基本方針を策定できていませんでした。**
- 「基本方針・対策基準」、「ソフトウェア最新化」、「ウイルス対策ソフトウェア」等の質問項目別で見ても、**すべての質問項目で、半数以上の企業が十分に対応できていない状態でした。**

1. はじめに

はじめに

経緯

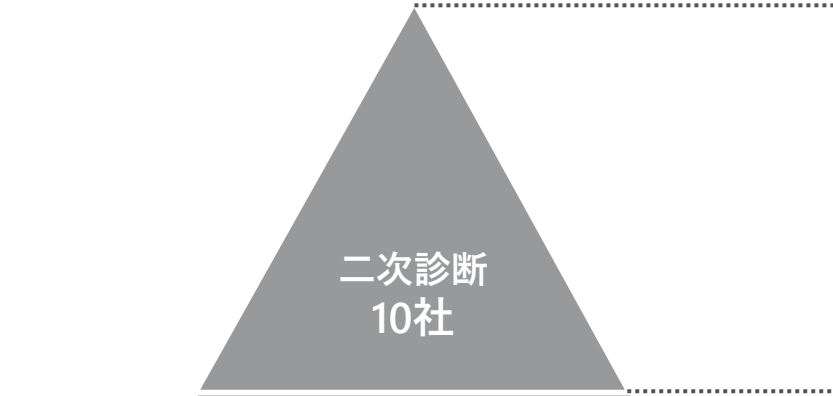
デジタル技術の普及とともに、情報セキュリティ対策の重要性が高まっています。しかし、多くの中小企業では、情報セキュリティ対策が十分に進んでいない状況にあります。
愛知県情報セキュリティ対策支援（診断）事業では中小企業が情報セキュリティ対策を始める足掛かりとして、「中小企業等向け情報セキュリティ診断」を実施しました。

中小企業等向け情報セキュリティ診断の目的

- 情報セキュリティ対策への意識を向上させる。
- 情報セキュリティ対策の必要性を理解する。
- 自社の強み、弱みを「見える化」する。
- 強化すべき箇所やその対策を提示することで、自社で情報セキュリティ対策を進めていけるようにする。

一次診断の参加企業と二次診断の参加企業を募集し、
両診断とも国や公的機関のガイドラインに準拠する項目を設定して診断しました。

診断のイメージ



二次診断

対象 **一次診断参加企業**
※二次診断のみの参加は不可。

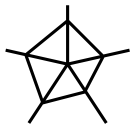
診断内容 **参加企業を訪問して診断**
- 一次診断結果を踏まえて従業員ルールを中心に診断。
  また、情報通信機器やソフトウェアの設定・管理状況等を診断

診断結果 **面談にて診断結果の説明と改善提案を実施**

一次診断

対象 **製造業を主とした県内中小企業等**
※同一サプライチェーンに属する企業等の企業グループで診断に参加する場合は大企業の参加も可能。

診断内容 **チェックリストの回答による診断（メールで送付）**
- 情報資産の管理状況
- 工場システムの情報セキュリティ対策状況 等



診断結果 **書面にて診断結果と改善案を提供**

参考ガイドライン

■ 独立行政法人情報処理推進機構（IPA）　中小企業の情報セキュリティ対策ガイドライン
■ 経済産業省　工場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　等

2. 一次診断の概要

情報セキュリティ対策診断は現在の情報セキュリティ対策の状況を把握するフェーズです。

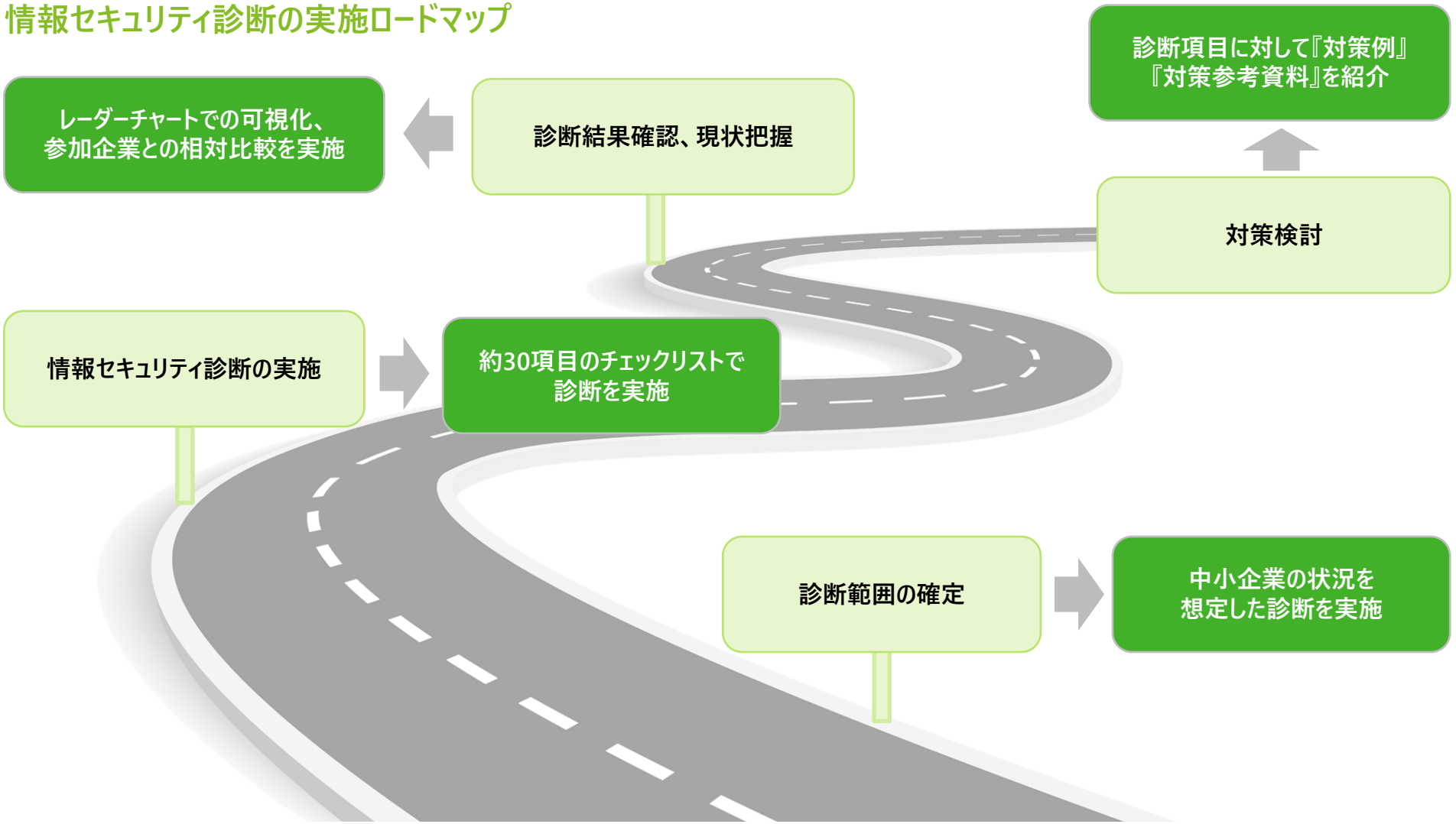
中小企業の情報セキュリティ対策ガイドライン
情報セキュリティ対策実施の４つのステップ

ステップ1	まず始めましょう	➢ 多くの中小企業にとっては、情報セキュリティ対策としていきなり高度な対策を開始するのは大変であるため、まずは、できるところから開始します。
ステップ2	現状を知り 改善しましょう	➢ 経営者を含めた情報セキュリティ対策に関する基本方針を策定します。 ➢ **現状の対策を把握し、**実施すべき対策を検討します。 ➢ 具体的な対策を定めて従業員に周知します。
ステップ3	本格的に 取り組みましょう	➢ 情報セキュリティ対策の管理体制を構築し、対策の費用を確保します。 ➢ 対応すべきリスクと対策を検討、規程を策定します。
ステップ4	改善を続けましょう	➢ 必要な対策を随時検討し、実施してください。

出典）中小企業の情報セキュリティ対策ガイドライン　P.2：独立行政法人情報処理推進機構（IPA）
（https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf）をもとに作成

一次診断では情報セキュリティ対策のチェックリストに記入いただいた内容をもとに、情報セキュリティ対策の状況の可視化及び対策例を示しました。

情報セキュリティ診断の実施ロードマップ



3. 一次診断の結果

個別質問については回答の点数化を行い、総合評価・カテゴリ別評価の平均点を評価しました。

個別質問の点数

質問	質問内容	カテゴリ	診断結果
1	経営層の意見を踏まえた情報セキュリティの基本方針を策定していますか	経営層関与	5.0
2	経営層は情報セキュリティ対策の重要性を認識し、自らリーダーシップをとって情報セキュリティ対応を実施していますか	経営層関与	5.0

点数	概要
5	対応している
4	対応を始めている
3	意識はあるものの対応できていない
2	対応していない
1	内容不明
0	対応不要と判断

総合評価、カテゴリ別の評価

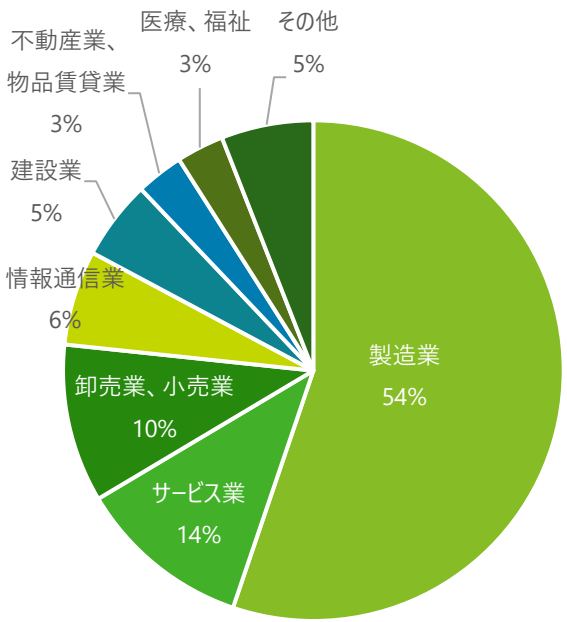
情報セキュリティ対策状況評価				
総合評価	カテゴリ別評価			
	経営層関与	組織対応	システム担当者ルール	従業員ルール
C	A	C	C	C

評価	平均スコア	概要
A	4.5~5.0	情報セキュリティ対策について多くが対応できている状態
B	3.5~4.4	情報セキュリティ対策について部分的に対応できている状態
C	2.5~3.4	情報セキュリティ対策について多くが意識はあるものの対応できていない状態
D	1.0~2.4	情報セキュリティ対策について多くが対応できていない状態

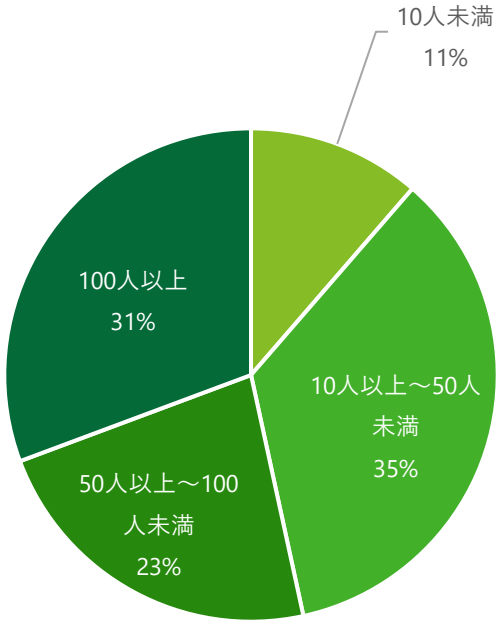
一次診断に参加した企業の業種別の割合、従業員規模別の割合、地域別の割合は以下のとおりです。

一次診断に回答した企業の各カテゴリ別の割合（申込社数：95社、調査回答数：88社）

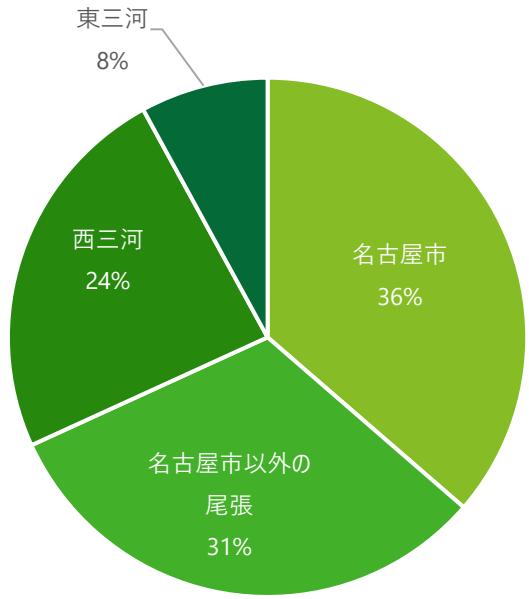
業種別の割合



従業員規模別の割合



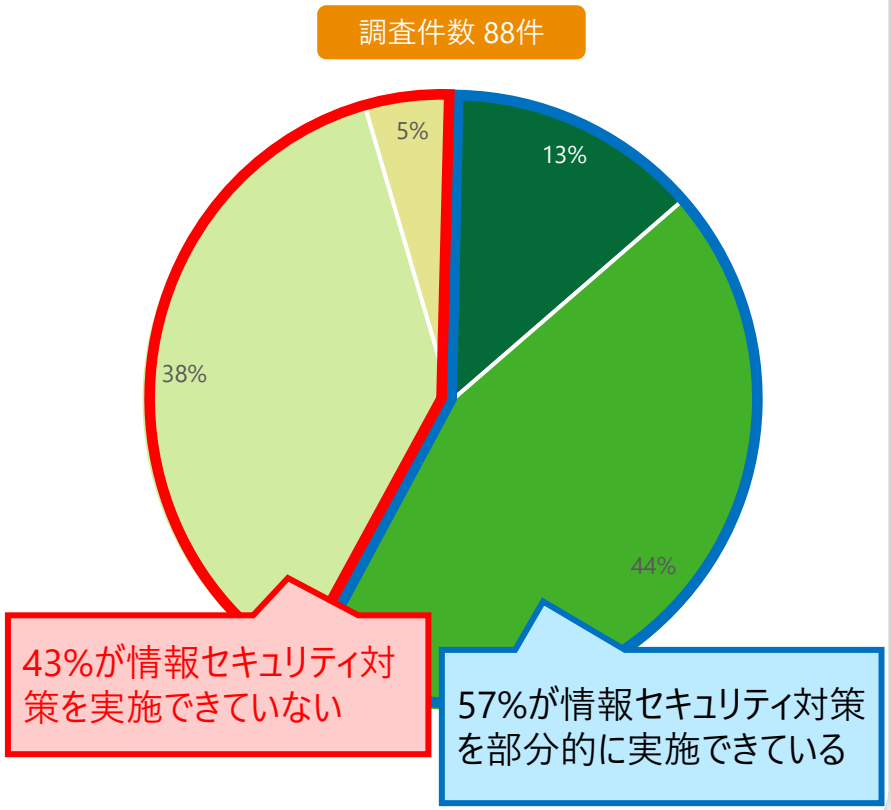
地域別の割合



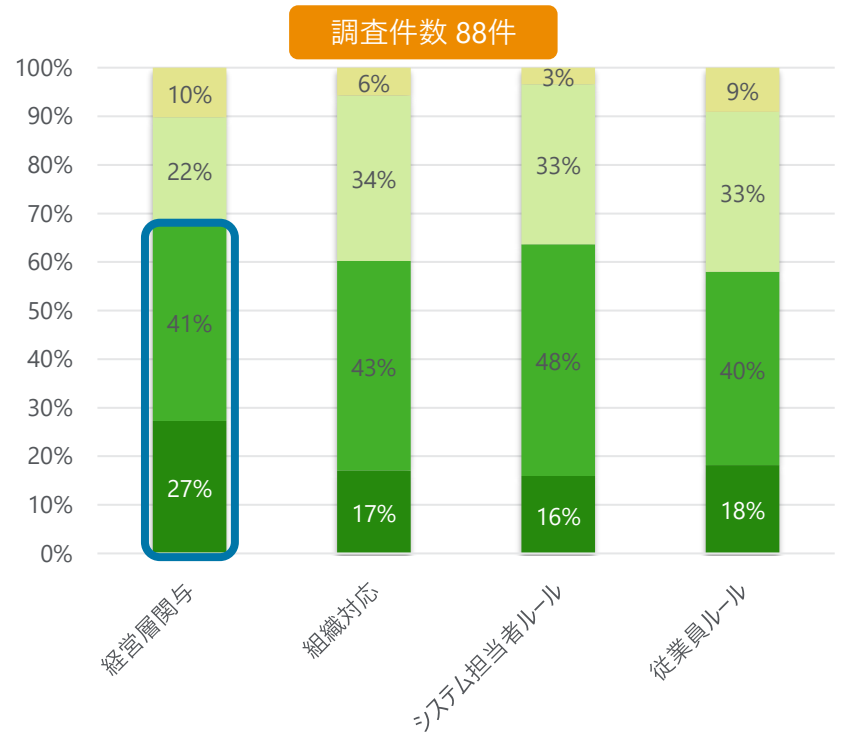
43%の企業では情報セキュリティ対策が実施できていない状態です。
一方で、経営層の情報セキュリティ対策に対する意識が高い企業は比較的多くあります。

診断に参加した企業全体の情報セキュリティ対策に関する傾向

総合評価別の割合



カテゴリ別の割合

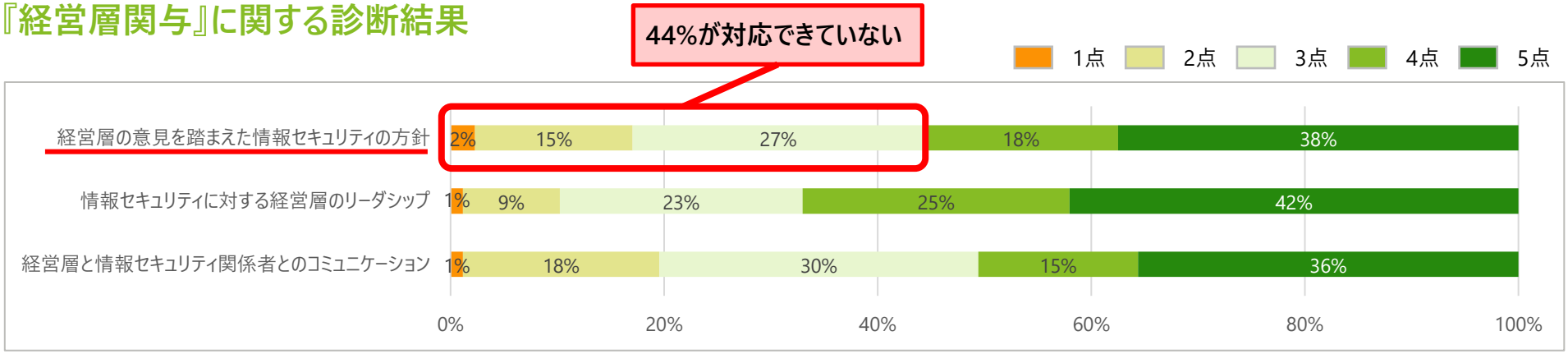


経営層の情報セキュリティ対策に対する意識は高い傾向にある

A評価	情報セキュリティ対策について多くが対応できている状態	C評価	情報セキュリティ対策について多くが意識はあるものの対応できていない状態
B評価	情報セキュリティ対策について部分的に対応できている状態	D評価	情報セキュリティ対策について多くが対応できていない状態

経営層の意見を踏まえた情報セキュリティ対策の基本方針の策定は優先して対応する必要があります。

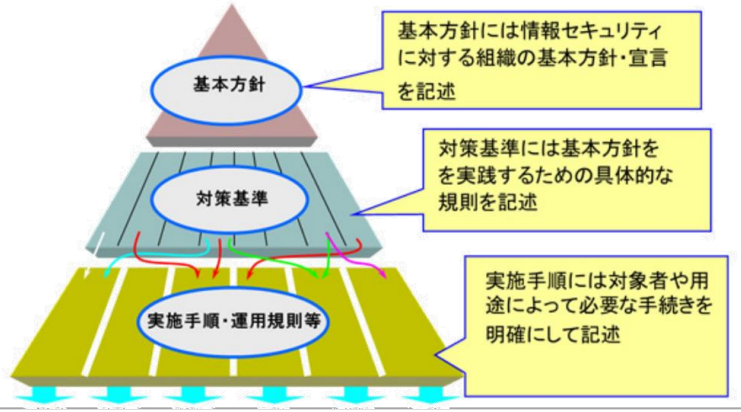
『経営層関与』に関する診断結果



- 「情報セキュリティに対する経営層のリーダーシップ」については、対策が実施できている企業が多くありました。
  一方で、「経営層の意見を踏まえた情報セキュリティの方針」と「経営層と情報セキュリティ関係者とのコミュニケーション」については十分な対策が実施できていない企業が多くありました。

「基本方針」は組織の情報セキュリティ対策のベースとなる方針です。

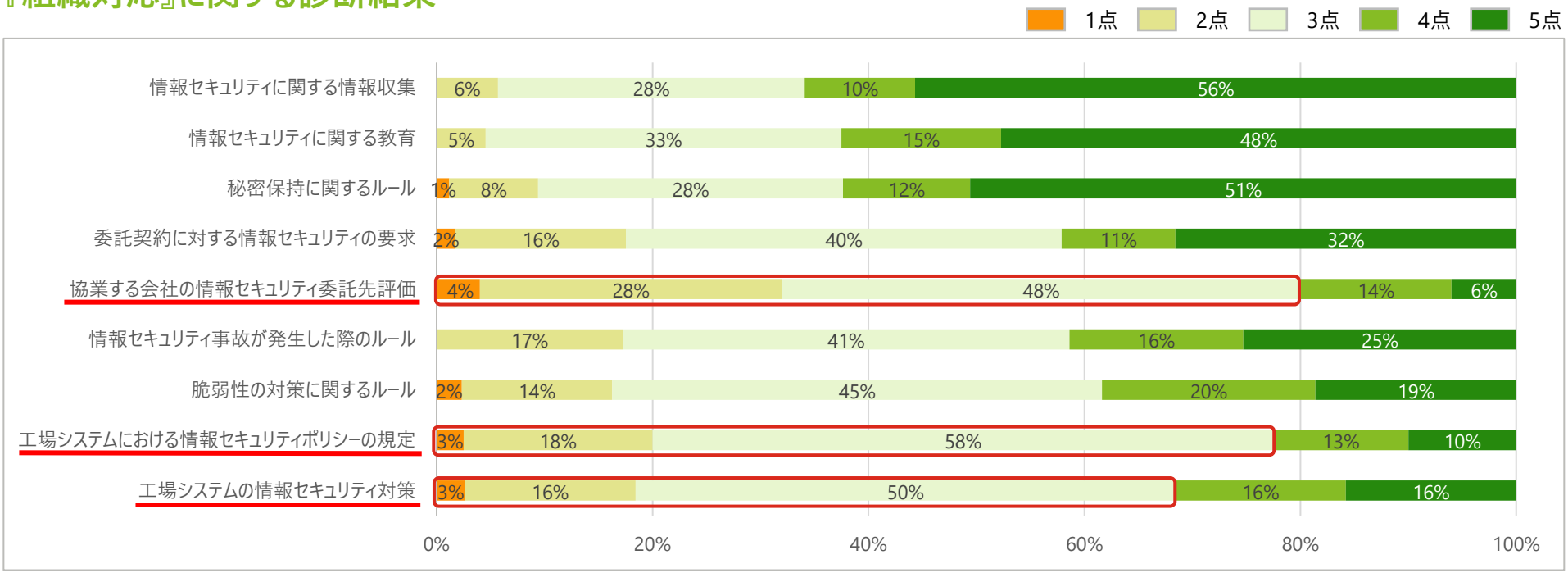
- 一般的に情報セキュリティポリシーの階層は
  「基本方針」、「対策基準」、「実施手順」で構成されます。
- 組織的に実施する意思を従業員や関係者に明確に示すために、
  自社に適した情報セキュリティ対策に関する基本方針を定め、
  宣言することが重要です。



出典）情報セキュリティポリシーの内容 | 国民のためのサイバーセキュリティサイト (soumu.go.jp)
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_04-3.html

組織対応に関する対策では、「委託先の評価」「工場システムの情報セキュリティポリシーの作成ならびに対策」を実施することが重要です。

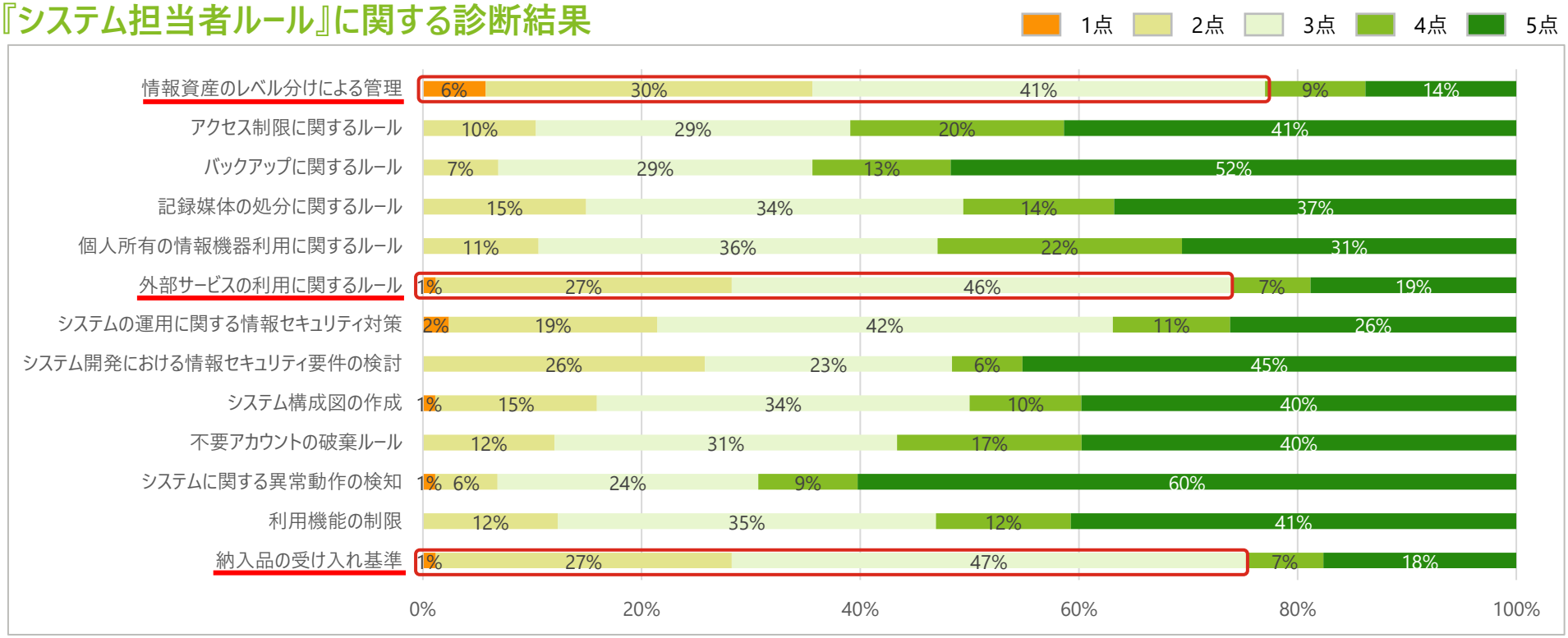
『組織対応』に関する診断結果



- 「情報セキュリティに関する情報収集」、「情報セキュリティに関する教育」、「秘密保持に関するルール」については対策が実施できている企業が多くありました。一方で、「協業する会社の情報セキュリティ委託先評価」、「工場システムにおける情報セキュリティポリシーの規定」、「工場システムの情報セキュリティ対策」については十分な対策が実施できていない企業が多くありました。
- 委託先に提供した情報の漏えい、改ざん等のインシデントが発生した場合、それが委託先の不備であったとしても、インシデントの影響を受けた者から**委託元としての管理責任を問われることがあります。**委託先について評価することが必要です。
- **工場システム**は内部ネットワークとして、インターネット等のネットワークにはさらされないことを前提に設計されるケースが多くあります。近年はデータ活用等で接続されることが増えており、**情報セキュリティ上のリスクも増加している**ため、情報セキュリティ対策を実施することが必要です。

システム担当者ルールに関する対策では、「情報資産のレベル分け」「外部サービスの評価」「納品する情報システムの確認」を実施することが重要です。

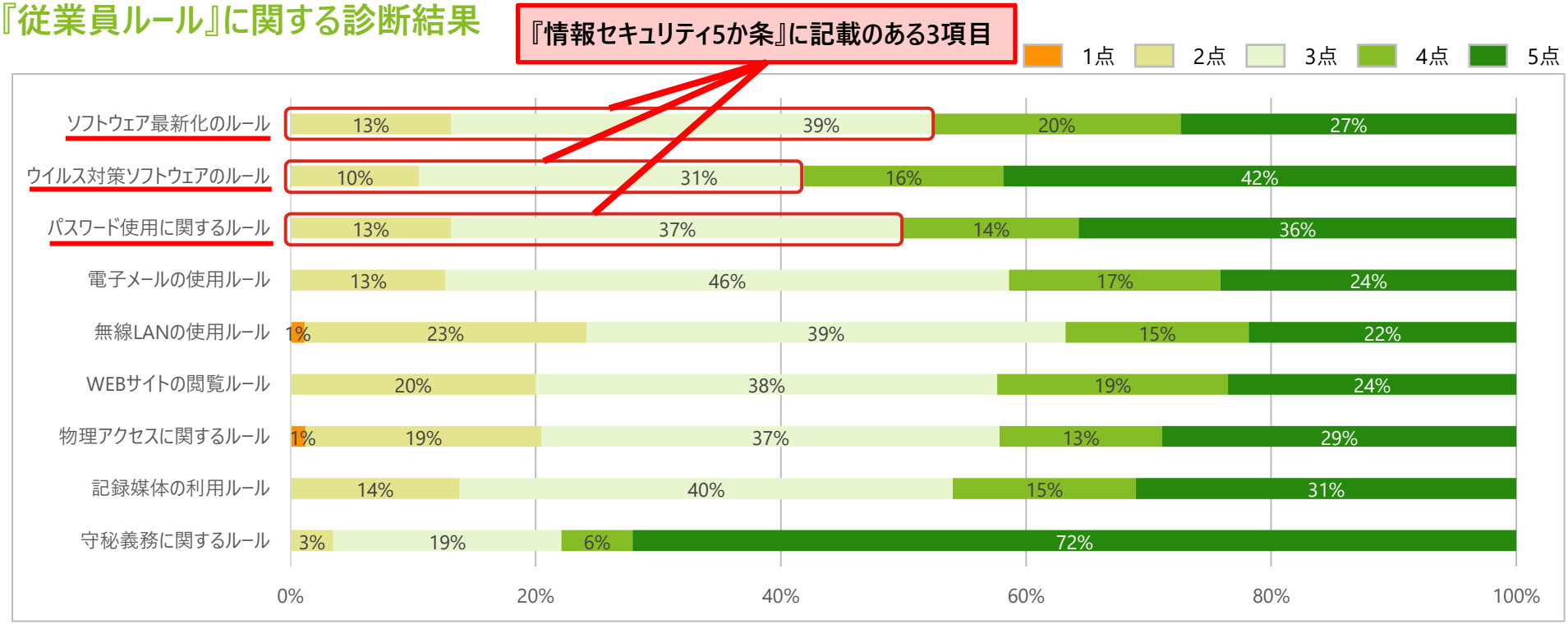
『システム担当者ルール』に関する診断結果



- 「システムに関する異常動作の検知」については対策が実施できている企業が多くありました。一方で、「情報資産のレベル分けによる管理」、「外部サービスの利用に関するルール」、「納入品の受け入れ基準」については十分な対策が実施できていない企業が多くありました。
- **情報資産の重要度が整理されていない場合、重要度に応じた対策の妥当性を判断できないことがあります。**情報資産をあらかじめ把握するとともに情報資産のレベル分けを行い、重要度に応じて管理することが必要です。
- 外部サービスが原因でシステムの停止等が発生した場合、影響を受けた者から**サービス提供者としての管理責任を問われることがあります。**使用する外部サービスについても情報セキュリティ対策の観点で精査することが必要です。
- 調達する機器等において、情報セキュリティ機能が装備されていない場合、**調達後に情報セキュリティ事故が発生する可能性があります。**調達する機器等について、導入基準を設けることが必要です。

従業員ルールに関する対策では、攻撃を防ぐための規定を策定し、周知徹底することが重要です。

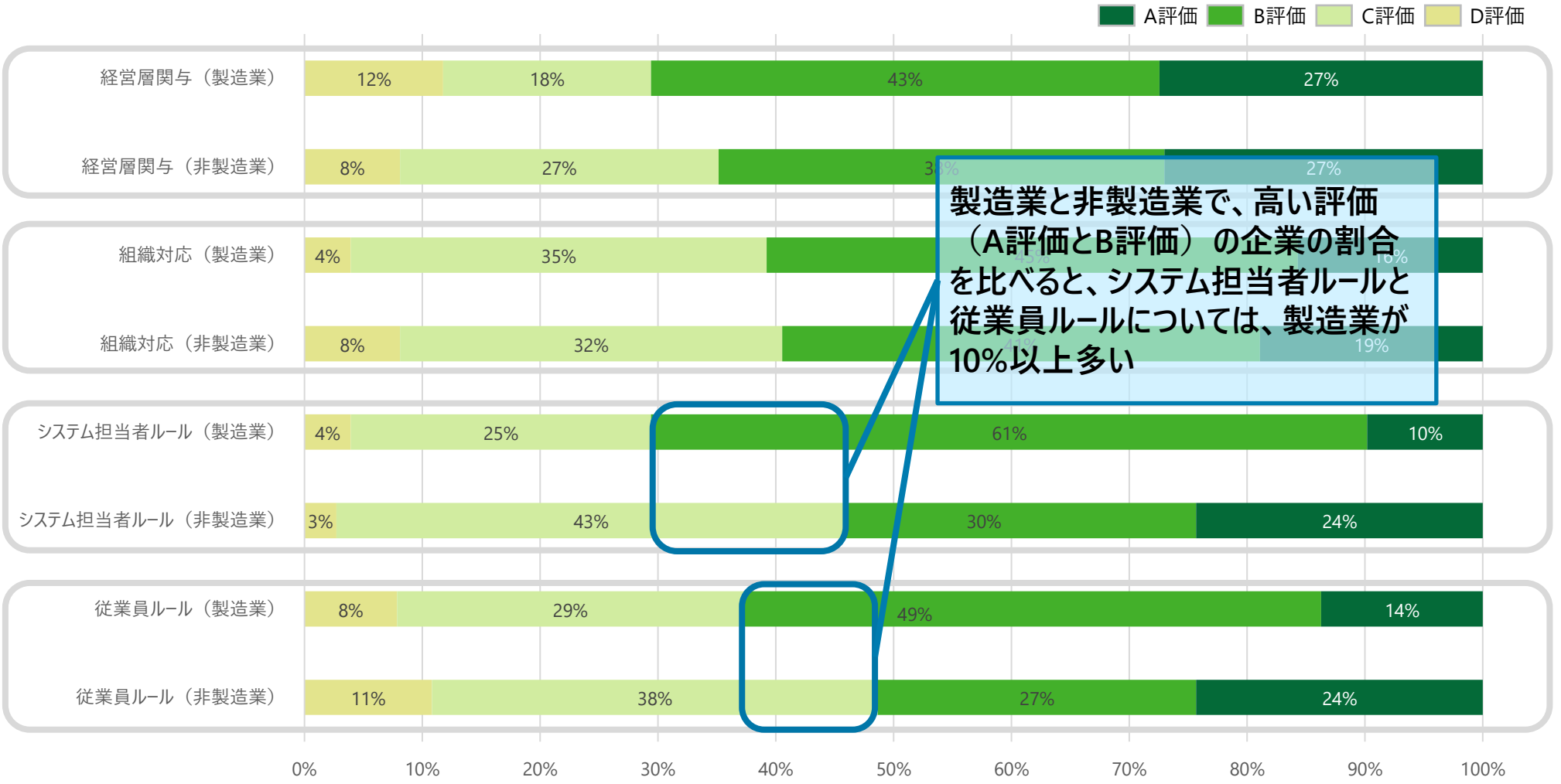
『従業員ルール』に関する診断結果



- 「守秘義務に関するルール」については対策が実施できている企業が多くありました。一方で、「ソフトウェア最新化のルール」、「ウイルス対策ソフトウェアのルール」、「パスワード使用に関するルール」については十分な対策が実施できていない企業が多くありました。
- 情報セキュリティ対策の最初に始める**『情報セキュリティ5か条』に記載のある「ソフトウェア最新化のルール」、「ウイルス対策ソフトウェアのルール」、「パスワード使用に関するルール」は特に優先して対応が必要です。**診断結果によると、約半数の企業が対応ができていない状態であるため、特に優先して対応する必要があります。

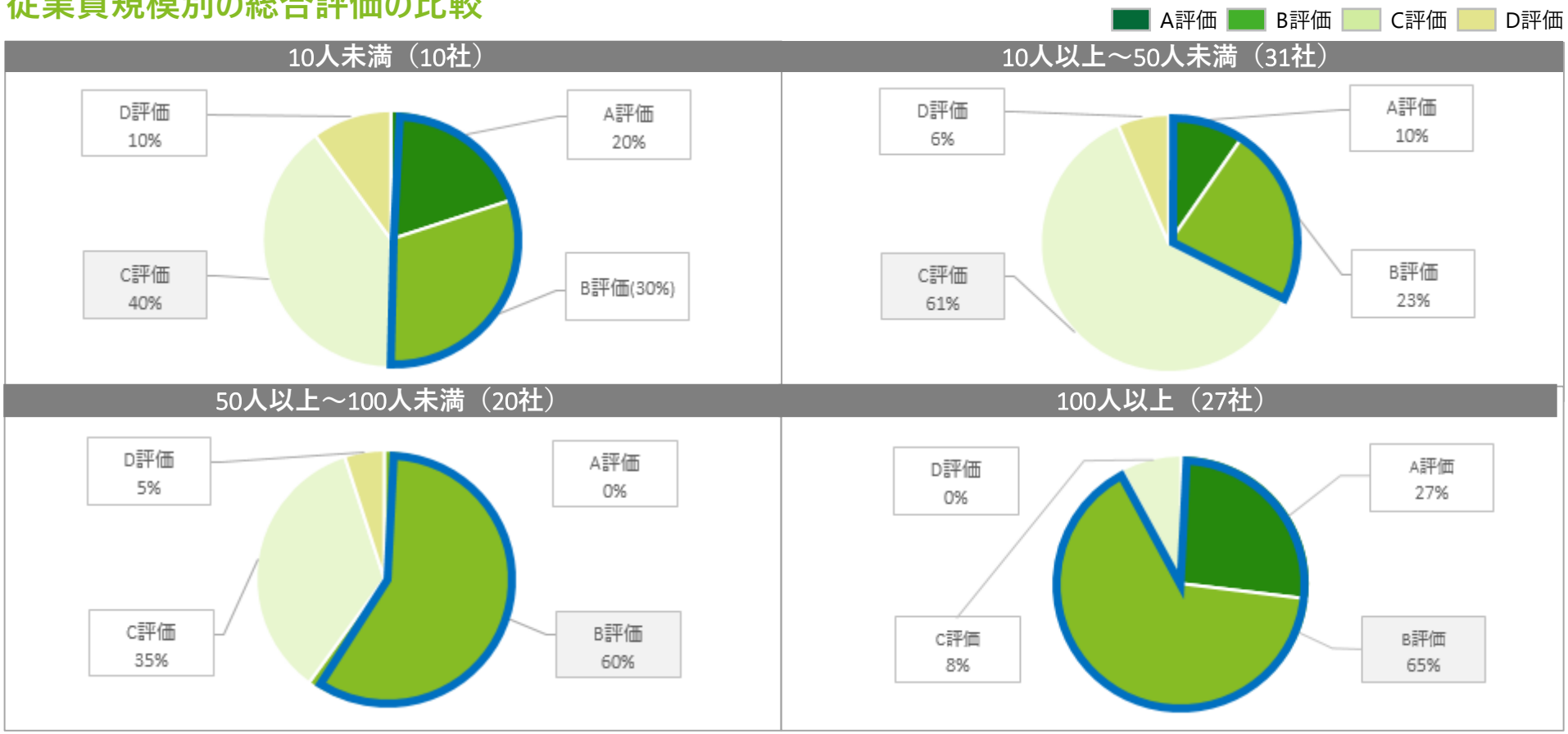
製造業と非製造業で、高い評価の企業の割合をカテゴリごとに比較すると、システム担当者ルールと従業員ルールについては製造業が10%以上多くなりました。

製造業（51社）と非製造業（37社）のカテゴリごとの割合の比較



10人以上の企業については、従業員数の増加に合わせて、総合評価が高くなる傾向があります。一方で、10人未満の企業については、10人以上～50人未満の企業よりも総合評価が高い企業が多く見られます。

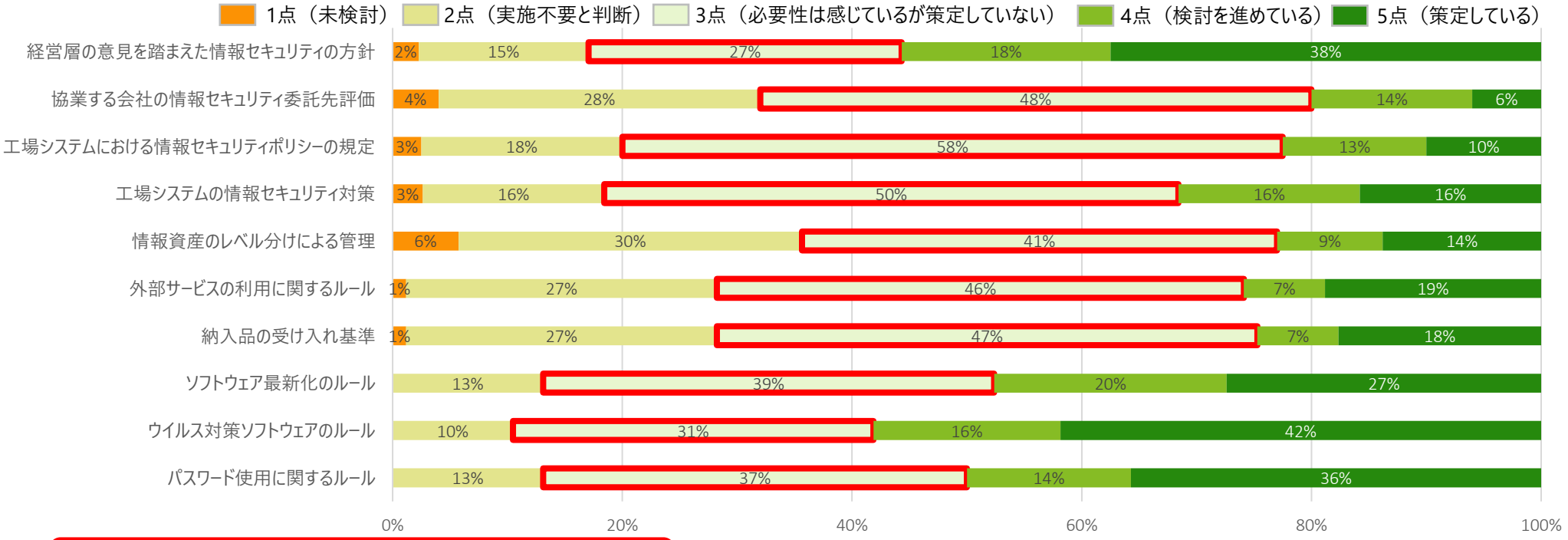
従業員規模別の総合評価の比較



- 従業員規模の増加に伴い情報セキュリティ対策に積極的に取り組む企業の割合が多くなるのは、**取り扱うデータ量が増加して情報セキュリティリスクやサイバー攻撃の被害額が増加するために、情報セキュリティ対策の優先度が高くなる**ことが理由である可能性がある。
- 10人未満の企業が情報セキュリティ対策に積極的に取り組む企業の割合が比較的多いのは、情報セキュリティ対策ツールが少額で導入可能な点や社内の関係者との調整がスムーズに実施できる点が理由である可能性がある。

各カテゴリで着目した情報セキュリティ対策の検討が進められていない項目において、多くの企業が規定等の必要性を感じているが策定していない状態でした。

情報セキュリティ対策の検討が進められていない項目



必要性は感じているが策定していない理由（想定）

人材の不足
情報セキュリティ対策にかける
人材を十分に確保できていない

→ 優先的に取り組むべき対策の考え方を紹介します。
また、人材を確保するための考え方について紹介します。

費用の不足
情報セキュリティ対策にかける
コストを十分に確保できていない

→ 優先的に取り組むべき対策の考え方を紹介します。
また、相談窓口や国の補助金等について紹介します。

人材や費用が少なくても対策が可能な『従業員ルール』について優先的に対策することを推奨します。

優先的に取り組む情報セキュリティ対策の考え方

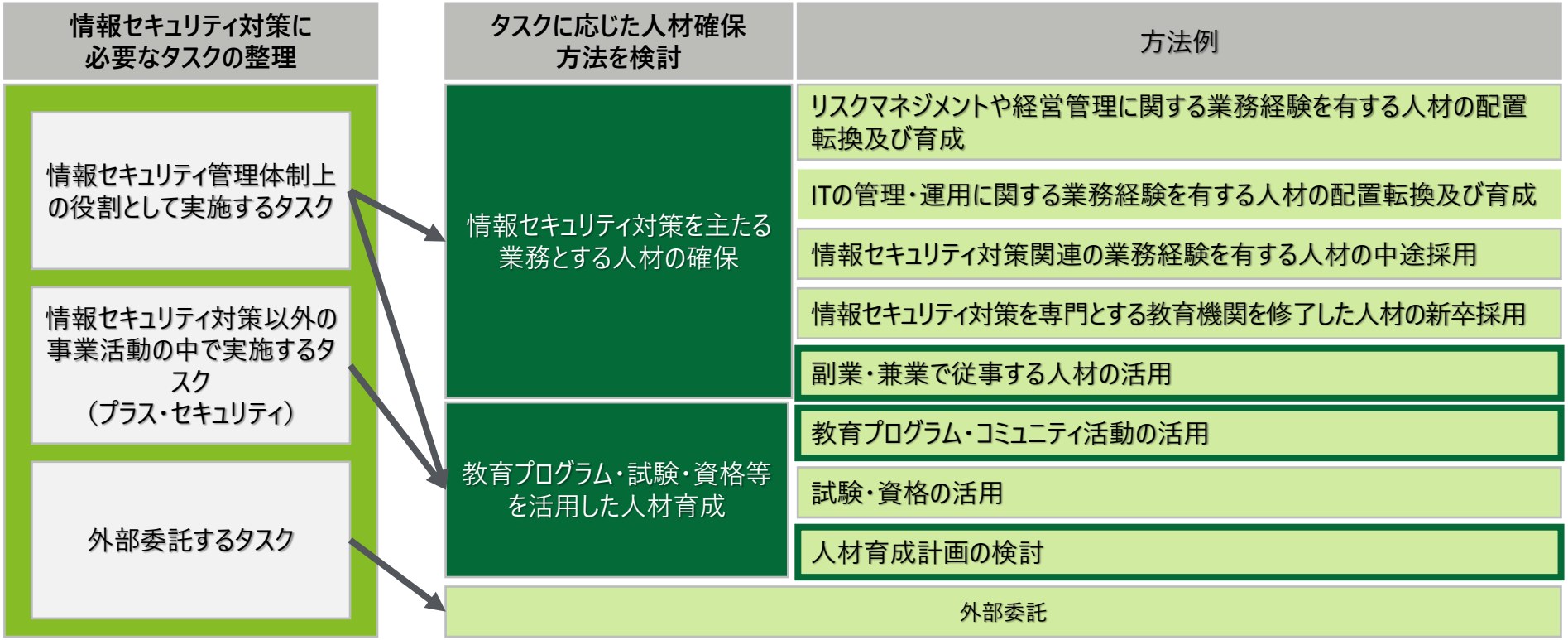
■今回実施した一次診断の各カテゴリを人材と費用を基準に評価。

	経営層関与	組織対応	システム担当者ルール	従業員ルール
専門的な知識を持った人材	適度に必要 (2点)	適度に必要 (2点)	必要 (1点)	**あまり必要ない (3点)**
想定される費用	低い (3点)	中程度 (2点)	高い (1点)	**低い (3点)**
優先度	**2 (5点)**	3 (4点)	4 (2点)	**1 (6点)**

必要なタスクを整理し、情報セキュリティ人材を育成していくことが重要です。

情報セキュリティ人材の確保

- 中小企業における情報セキュリティ対策の人材確保には、**社内の情報システム担当者等を育成する**ことが望まれます。また、育成費用を削減するためには**行政及び支援機関等の支援施策、教育プログラムやコミュニティ活動を活用する**ことが有用です。
- 専門人材を常勤で雇用する余裕がない場合は、**リモートワーク、特定の曜日のみの非常勤の勤務及び1人の人材が複数企業で勤務する副業・兼業といった新たな働き方・雇用形態を活用**し、柔軟な人材確保について検討することが望ましいです。



出典）サイバーセキュリティ体制構築・人材確保の手引き P5：独立行政法人情報処理推進機構（IPA） (https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf)
セキュリティ人材の活躍の促進に向けた流動性とマッチングの機会の促進 P.3：NISC (https://www.nisc.go.jp/pdf/council/cs/jinzai/dai14/14shiryou0106.pdf) もとに作成

4. 二次診断の概要

二次診断は、対象者数が多く攻撃経路となりやすい一方で、人材や費用が少なくても対策が可能な『従業員ルール』に着目して診断を実施しました。

一次診断カテゴリ

従業員ルール

基本方針・対策基準

ソフトウェア最新化のルール
業務で使用する情報端末（パソコン、スマホ等）について、ソフトウェアを常に最新の状態に保つためのルール

ウイルス対策ソフトウェアのルール
業務で使用する情報端末（パソコン、スマホ等）について、ウイルス対策ソフトウェアを導入し、常に最新の状態に保つためのルール

パスワード使用に関するルール
業務で使用する情報端末（パソコン、スマホ等）について、セキュリティ上安全なパスワードを設定するルール

電子メールの使用ルール
業務において電子メールを情報セキュリティ上安全に使用するためのルール

無線接続の使用ルール
業務において無線接続を情報セキュリティ上安全に使用するためのルール

WEBサイトの閲覧ルール
業務で使用する情報端末（パソコン、スマホ等）について、WEBサイトの閲覧を情報セキュリティ上安全に使用するためのルール

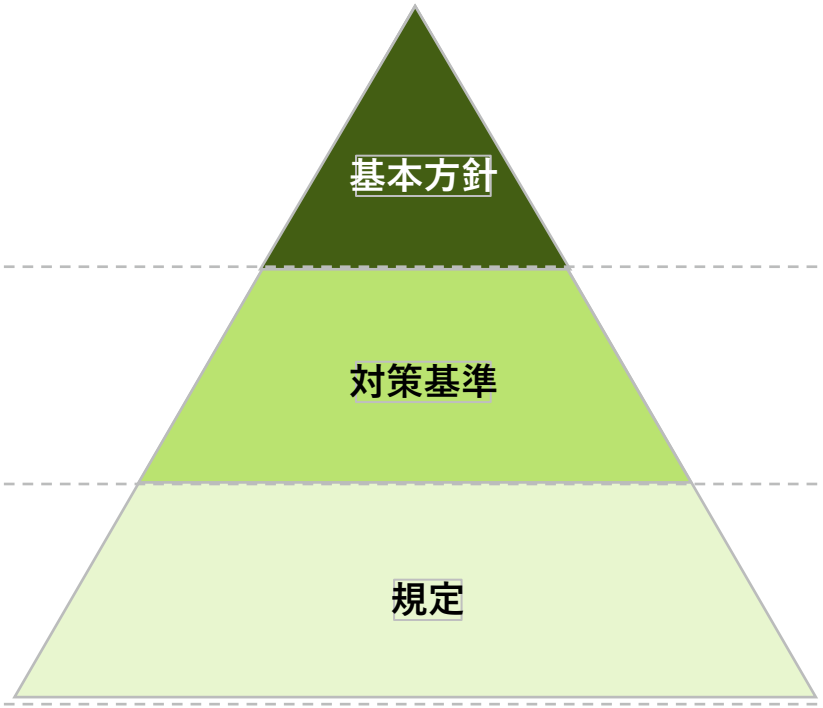
物理アクセスに関するルール
重要な情報資産が保管された場所へのアクセスに関して、施錠等を実施し、許可された人以外がアクセスできないルール

記録媒体の利用ルール
重要な情報資産が記録された書類や記録媒体の持ち出しに関するルール

守秘義務に関するルール
社内にて業務上知り得た情報の取り扱いを制限するルール

『従業員ルール』の各項目について情報セキュリティポリシーの階層をもとに、情報セキュリティ対策が実施できているかを診断しました。

情報セキュリティポリシーの階層と二次診断の採点項目



情報セキュリティポリシーの階層

採点項目
策定有無
策定有無
策定有無
浸透状況
管理方法
＋
技術的対策

二次診断では、実地診断から対策検討のフォローアップまで実施します。

二次診断の流れ

二次診断の実施

➢チェックリストの作成・送付・回収
- 「規定有無」、「浸透状況」、「管理状況」、「技術的対策」の観点を基に作成したチェックリストを作成し、送付した。また、チェックリストは実地診断前に回収した。

➢実地診断の実施
- 事前に回収したチェックリストの回答結果をもとに、チェックリストの項目に対して説明を加えながら、企業の実態を確認して診断を実施した。また、情報セキュリティに関する困りごとについての相談も併せて実施した。

診断結果の説明・改善提案

➢診断結果の送付
- 二次診断で実施した従業員ルールについての情報セキュリティ対策状況の評価と具体的な改善策の提案を記載し、送付した。

➢説明・改善提案
- 送付した診断結果をもとに、企業に説明を行い、二次診断の結果含めた情報セキュリティに関する困りごとについての相談も実施した。

二次診断のフォローアップ

➢対策の検討状況聞き取り
- 二次診断結果の説明・改善提案から１～２週間後を目途に受診企業に対策の検討について確認及び相談等がないか確認を行った。

➢フォローアップ
- 聞き取った相談事項をもとに、回答を行った。

5. 二次診断の結果

従業員ルールについての採点項目を10項目設け、採点項目ごとに４段階で評価しました。

二次診断対象企業の選定方針

- 業種ごとに申込数に応じて診断枠を設定
- 同一サプライチェーンに属する等、普段から業務上関わりがある２社以上の企業を１組選定
- 一次診断の「従業員ルール」の点数がばらつくように選定

採点方法

- 下記の二次診断チェックリストの回答をもとにA～Dの４段階で採点
- 採点時の観点は、「規定の有無」、「浸透状況」、「管理方法」、「技術的対策の有無」の４つ
- 「規定の有無」は、採点項目に該当する規定があるかどうかをもとに採点
- 「浸透状況」は、採点項目に該当する規定を浸透させているかどうかをもとに採点
- 「管理方法」は、採点項目に該当する規定の組織全体への浸透状況の管理をしているかどうかをもとに採点
- 「技術的対策」は、採点項目に該当する規定に対して、技術的対策の実施の有無を採点。実施している場合は、１ランクアップ

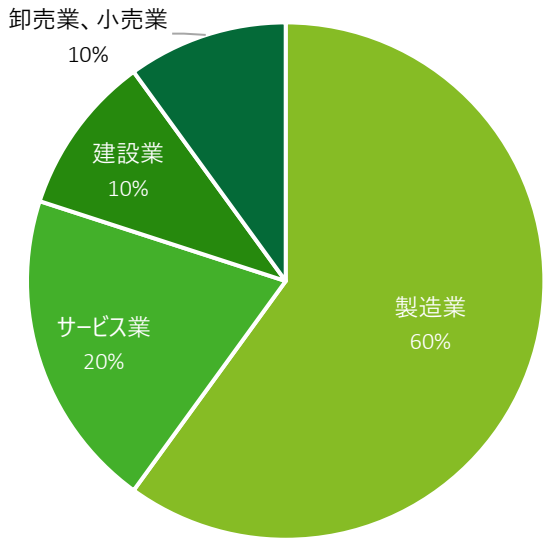
対策確認の対象	質問の分類	質問内容	回答
ソフトウェア 最新化のルール	規定有無	業務で利用する情報端末（パソコン、スマホ等）について、ソフトウェアを常に最新の状態に保つためのルール（規定、手順）を作成していますか	2. ルール（規定、手順）を作成していない
	浸透状況	上記ルールを組織全体に広く周知し、浸透させることができていますか	4. 浸透状況は不明
	管理方法	上記ルールについて、組織全体への浸透状況の管理を行っていますか （管理方法の例）ルールに対する定期的なテストの実施、従業員へのヒアリング	2. 管理されていない
	技術的対策	上記ルールを実施するために、技術的な対策を実施していますか （対策例）資産管理ソフトウェアを利用し、情報端末（パソコン、スマホ等）を管理する	1. 技術的対策を実施している

評価	概要
A	規定があり、浸透させており、浸透状況の管理がされている
B	規定があり、浸透させている
C	規定がある、もしくは規定は無いが浸透させている
D	規定なし

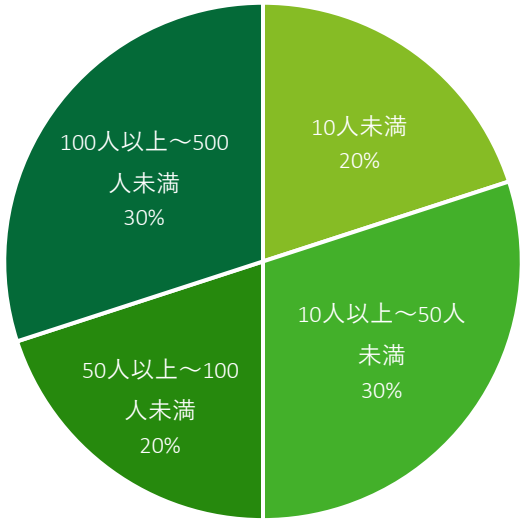
二次診断に参加した企業の業種別の割合、従業員規模別の割合、地域別の割合は以下のとおりです。

二次診断に参加した10社の各カテゴリ別の割合

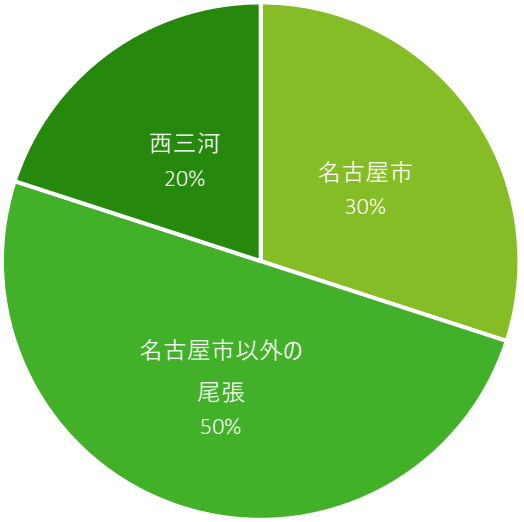
業種別の割合



従業員規模別の割合



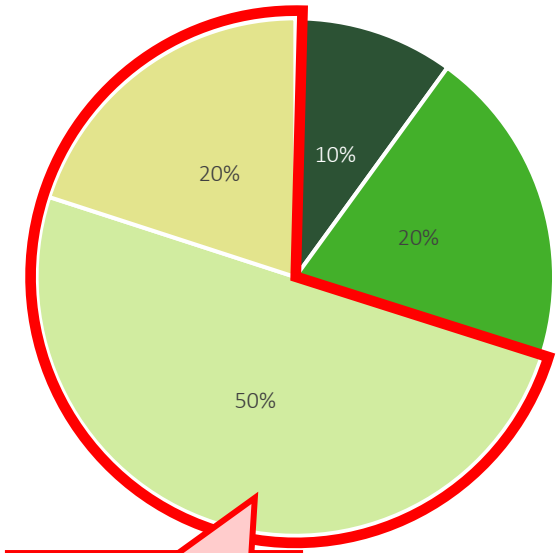
地域別の割合



70%の企業で基本方針の策定ができていない状態です。
また、多くの企業で従業員ルールが策定できていない状態です。

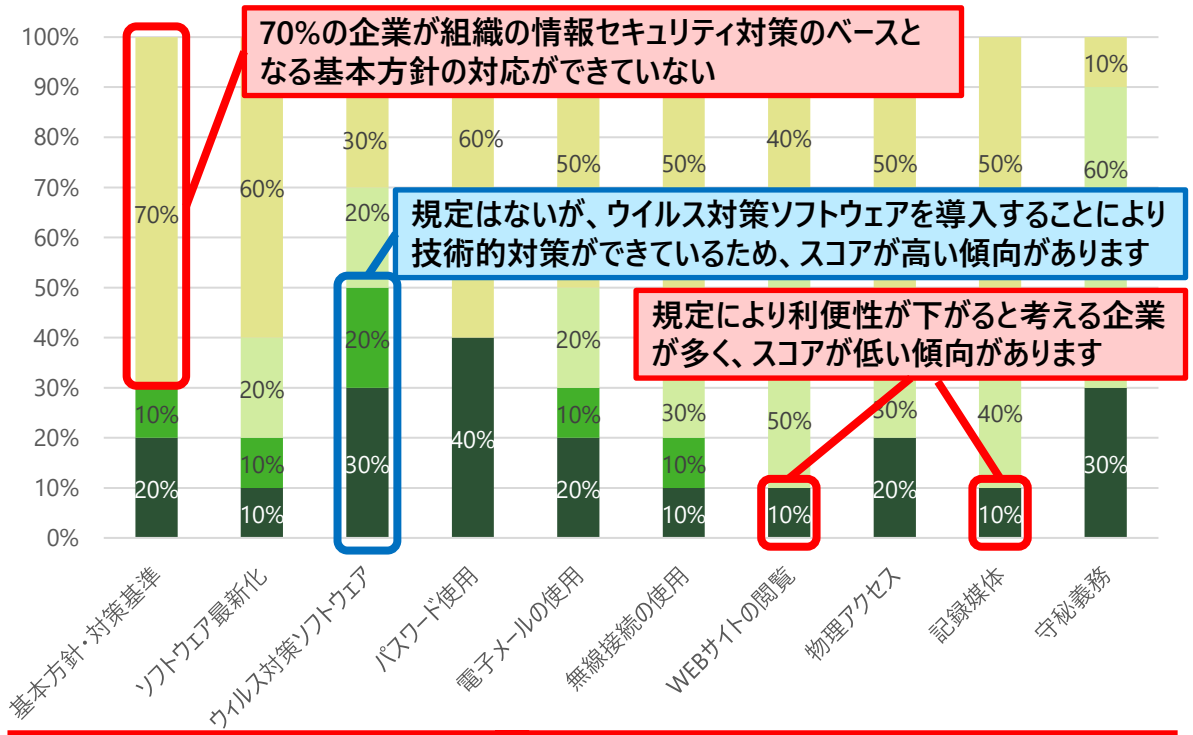
二次診断を実施した10社の情報セキュリティ対策に関する傾向

総合評価別の割合



70%が従業員ルールについての対応が進んでいない

質問項目別の割合



A評価とB評価の合計が50%を超える質問項目はないため、全般的に従業員ルールについての対応ができていない傾向にある

A評価	従業員ルールについて多くが対応できている状態	C評価	従業員ルールについて一部のみ対応できている状態
B評価	従業員ルールについて部分的に対応できている状態	D評価	従業員ルールについて多くが対応できていない状態

質問項目別の傾向と対策、注目すべき事柄は以下のとおりです。

質問項目別の傾向と対策、注目すべき事柄(1/4)

	傾向と対策、注目すべき事柄
基本方針・対策基準	➢ **70%の企業が組織の基本方針を策定できていませんでした。**一方で、**基本方針を策定している企業は、他の項目についてもスコアが高い**傾向があります。 ➢ 情報セキュリティ対策において**基本方針を策定することの重要さを理解していない**ため、基本方針の策定の優先度が下がっている可能性があります。**基本方針の重要性について理解する**ことが必要です。 ➢ 基本方針の策定が必要なことを理解しており、国のガイドライン等の存在を知っているものの、**ガイドラインの内容を理解することが難しい**という意見がありました。 ➢ **親会社、グループ会社及び取引先から基本方針のひな型が提供**され、そのひな型を元に策定中といういう企業がありました。 ➢ **ISO/IEC27001の取得**を目指している企業がありました。
ソフトウェア最新化のルール	➢ パソコンやソフトウェアの資産管理が適切に実施できていない企業においては、**「どのソフトウェアが使用されているのか」、「どのバージョンが最新なのか」といった情報を把握することが困難**なため、ソフトウェアの最新化が適切に実施できていない傾向があります。 ➢ ソフトウェアの最新化を適切に実施する前提として、情報端末を棚卸して、**情報端末リストを作成する**ことが必要です。 ➢ **資産管理ソフトウェアを使用して、情報端末を一覧化しソフトウェアの最新化を一元管理**している企業がありました。 ➢ **本社以外の拠点や工場については、情報端末やソフトウェアの状況を詳細に把握できていない**という意見がありました。

質問項目別の傾向と対策、注目すべき事柄は以下のとおりです。

質問項目別の傾向と対策、注目すべき事柄(2/4)

	傾向と対策、注目すべき事柄
ウイルス対策ソフトウェアのルール	➢ **ウイルス対策ソフトウェアはすべての企業で導入されていました。**一方で、**規定を策定していない企業が多くありました。** ➢ パターンファイルの更新を自動更新設定にしている企業がありました。**ウイルス対策ソフトウェアの性能を最大限に引き出すために、適切なタイミングで更新することが必要です。** ➢ **新規のパソコンを配布する前に、ウイルス対策ソフトウェアを導入する**という管理を実施している企業が複数ありました。 ➢ **ウイルス対策ソフトウェアの管理をITベンダーに任せておりソフトウェアのバージョンを把握していない**企業がありました。管理をITベンダーに任せる場合もバージョンを最新に保つことをITベンダーが保証しているかについて契約を確認することが望まれます。
パスワード使用に関するルール	➢ 従業員がパスワードを覚えることが難しくなる等の**ユーザビリティに影響を及ぼすことを懸念して、規定の策定を躊躇する企業が複数ありました**。 ➢ サイバー攻撃からアカウントを保護するためには**パスワードを複雑にすることやパスワードを使いまわさないことが重要です。** ➢ パスワードを定期的に変更する規定を定めたり運用をしている企業が多くありましたが、現在は一定の条件のもと**パスワードを定期的に変更することは推奨されていません**。 ➢ パスワードを設定しているが、設定した従業員本人しか知らないため、従業員が退職したりパスワードを忘れた場合は、そのアカウントに保存された情報にアクセスできなくなる状態の企業がありました。そのような状態は情報の損失や利便性の低下を引き起こす可能性があるため、パスワードのリセット機能の導入を検討していました。

質問項目別の傾向と対策、注目すべき事柄は以下のとおりです。

質問項目別の傾向と対策、注目すべき事柄(3/4)

	傾向と対策、注目すべき事柄
電子メールの使用ルール	➢ **情報セキュリティ対策ソフトウェアを導入して、不審メールを検知している**企業が複数ありました。 ➢ **不審メールを従業員が受信した際は、情報セキュリティ対策の担当者に連絡し、情報セキュリティ対策の担当者が社内に周知**する運用ができている企業が複数ありました。 ➢ **標的型攻撃メールの訓練**を実施したいと考えている企業はありましたが、実際に**実施している企業は少なかったです。**
無線接続の使用ルール	➢ 無線接続を使用していない企業は、ありませんでした。 ➢ 自社で使用している暗号方式を把握している企業は少なかったですが、すべての企業で**WPA2以上の強固な暗号方式を用いた無線接続を使用**していました。一方で、ほとんどの企業で、**社外における無線接続についての規定を策定できていません**でした。 ➢ 出張時等の社外で自社の情報端末を使用する時は、公衆Wi-Fiの使用を禁止にし、自社貸与のモバイルWi-Fiやスマートフォンのテザリング機能を使用するよう規定している企業がありました。
WEBサイトの閲覧ルール	➢ 従業員が業務で使用するWEBサイトを使用できなくなってしまう等の**ユーザビリティに影響を及ぼすことを懸念して、規定の策定を躊躇する企業が多くありました。** ➢ 規定はないものの、WEBフィルタリング機能のある機器を導入し、対策を実施している企業が複数ありました。 ➢ **フィッシングサイトにアクセス**してしまった事例がある企業がありました。フィッシングサイトや偽のWEBサイトにアクセスすることで、個人情報の盗難や詐欺の被害に遭う可能性があります。信頼できるソースから提供される公式WEBサイトを使用することが推奨されます。

質問項目別の傾向と対策、注目すべき事柄は以下のとおりです。

質問項目別の傾向と対策、注目すべき事柄(4/4)

	傾向と対策、注目すべき事柄
物理アクセスに関するルール	➢ **部屋ごとにセキュリティレベルを設けて、入退室管理を実施している企業がありました**。一方で、**重要な情報資産が保管されている部屋でも施錠管理を実施していない**企業も複数ありました。 ➢ 入退室管理の方法としては、**張り紙を使用して制限したり、社員証をカードキーとして使用**したりしている企業がありました。 ➢ 一部の企業は、**サーバの管理においてラックを用意して、施錠管理**を行っていました。一方で、サーバをそのまま設置している企業がありました。
記録媒体の利用ルール	➢ **記録媒体の利用を制限することで業務の効率性や生産性が低下する等の影響を懸念して、規定の策定を躊躇する企業が多くありました。** ➢ **資産管理ソフトウェア等を使用して、記録媒体の利用を管理**している企業が複数ありました。
守秘義務に関するルール	➢ 守秘義務に関する規定はあるものの、**従業員へ説明する場や署名を求める**等の守秘義務の運用に関する規定を策定していない企業が多くありました。 ➢ １年に１回の**従業員教育の際に守秘義務に関する項目を取り上げ**、署名を求め保管している企業がありました。 ➢ 守秘義務の内容を説明している企業の場合、**入社時に説明している企業が多く**ありました。

VPN装置やリモートデスクトップを使用している企業が多くありました。VPN装置やリモートデスクトップは、適切に管理していないとサイバー攻撃の起点となる可能性があります。

近年のトレンドに沿った確認の傾向と対策、注目すべき事柄

	傾向と対策、注目すべき事柄
VPN	➢ **VPN装置の管理をITベンダーに任せておりソフトウェアのバージョンを把握していない**企業がありました。管理をITベンダーに任せる場合もバージョンを最新に保つことをITベンダーが保証しているかについて契約を確認することが望まれます。 ➢ VPN装置は定期的にアップデートする必要があります。アップデートにはセキュリティパッチや脆弱性の修正が含まれており、最新のバージョンを使用することでセキュリティを強化できます。 ➢ 自社だけではなく、グループ会社も含めてVPN装置を使用したネットワークを構築している企業がありました。
リモートデスクトップ	➢ コロナ禍で在宅勤務の環境を用意したが、現在は出社を求めているため、**基本的には使用していない**という企業が多くありました。 ➢ パスワードを設定しているものの規定が無いため、簡易なパスワードを使用している企業が複数ありました。**強固なパスワードの設定をすることが必要です。** ➢ **接続元IPアドレスの制限やログインの試行回数制限**を実施していない企業が多くありました。
バックアップ	➢ **定期的にバックアップを取得している企業が多く**ありました。また、自動的にバックアップを取得するように設定している企業がありました。 ➢ **複数のサーバを用意したり、NASやHDDを使用してバックアップを保管している**企業が多くありました。ただし、近年では、ランサムウェア対策としてバックアップの１つはオフラインでの保管が推奨されています。 ➢ **バックアップからの復元を定期的にテストしている企業はほとんどありませんでした。**

グループ会社内では情報セキュリティ対策を連携して推進している企業がありましたが、差異がある状況でした。また、サプライチェーン内の連携はあまり進んでいない状況でした。

グループ会社やサプライチェーンの情報セキュリティ対策の傾向と対策、注目すべき事柄

	傾向と対策、注目すべき事柄
グループ会社	➢ **基本方針を策定済みの企業と未策定の企業が混在**しているグループ会社がありました。 ➢ **親会社の情報セキュリティ対策の規定を子会社が部分的に準用**している企業がありました。人材や費用に限りがある子会社においては、親会社の規定を参考にすることが有効です。 ➢ 規定を準用していても、浸透状況に差異があるグループ会社がありました。一方で、**グループ会社全体を対象に社員向けの教育を実施**しているグループ会社がありました。グループ会社全体の情報セキュリティ対策を向上させるためには、グループ会社全体で教育を実施することが有効です。 ➢ 親会社が子会社に対して、情報セキュリティ対策についてのガイドラインを提供し、**ガイドラインに基づいたチェックリストの回答を提出**することを求めているグループ会社がありました。 ➢ UTM等の情報セキュリティ対策機器を使用した**共通のネットワークを構築**しているグループ会社がありました。親会社がリーダーシップを発揮して、グループ会社全体の技術的な情報セキュリティ対策を支援することが有効です。
サプライチェーン	➢ この数年で**納入先からの情報セキュリティ対策についての情報提供や要求が増えた**という企業が多くありました。 ➢ **納入先から提供された情報セキュリティ対策のガイドラインや基本方針のひな型を活用**し、基本方針等の策定を検討中の企業がありました。 ➢ 納入先の企業から情報セキュリティ対策についての要求を受けている企業はありましたが、**納入元の企業へ情報セキュリティ対策について要求している企業はありませんでした。**情報セキュリティ対策について情報を共有することや契約書等に情報セキュリティ対策についての条項を盛り込むことが有効です。

診断で得られた気づきは以下のとおりです。

診断で得られた気づき(1/3)

1　情報セキュリティ対策ツールの運用

➢技術的対策として**情報セキュリティ対策ツール**（ウイルス対策ソフトウェア、UTM等）を導入していても、**適切に運用できていない**企業が多くありました。
（例）・ウイルス対策ソフトウェアのアップデートが、情報端末を使用する従業員任せになっている。
・UTMのアップデート状況や運用保守契約状況を把握できていない。

➢このような状況は、**情報セキュリティ上のリスク**となります。
➢情報セキュリティ対策ツールの**性能を最大限に引き出す**ためには、**規定を定めて適切に運用すること**が大切です。

導入した後の運用が大切なのは、他の業務機器や工作機械と同じではないでしょうか？

2　情報資産の把握

➢自社の**情報資産や情報端末を把握できていない**企業が多くありました。
（例）・どの情報が重要な情報資産なのか把握できていない。
・どの情報端末にどの情報資産があるのか、どのソフトウェアが使用されているのかを把握できていない。

➢このような状況は、**情報セキュリティ上のリスク**となります。
➢ソフトウェアの最新化、ウイルス対策ソフトウェアの導入等の**情報セキュリティ対策の前提**として、**情報端末を抜け漏れなく把握すること**が必要です。

抜け漏れなく把握することが大切なのは、情報資産ではない「資産」と同じではないでしょうか？

診断で得られた気づきは以下のとおりです。

診断で得られた気づき(2/3)

3　情報セキュリティ対策に伴う業務上の不便への懸念

➢**規定を策定することで、業務上の不便が生じる**ことを懸念する企業が多くありました。
（例）・パスワードを複雑にすると、従業員がパスワードを覚えにくくなる
・WEBサイトの閲覧を制限すると、業務で自由にWEBサイトを閲覧できなくなる

➢規定は業務を実施しにくくするものではなく、**規定を策定するからこそ安心して業務を実施できる**ようになります。
［（例）不正なアクセスを防ぐ。不審なWEBサイトを閲覧するリスクを低下する。］

規定を策定することが大切なのは、職場の安全管理と同じではないでしょうか？

4　情報セキュリティ対策を実施する体制

➢情報セキュリティ対策を**総務部門等の特定の担当者に任せている**企業が多くありました。
➢また、情報セキュリティ対策の担当者からは「**他部門を巻き込むことが難しい**」、「**本社以外の拠点や工場については詳細に状況を把握できていない**」という意見がありました。
➢一方で、以下の体制で情報セキュリティ対策を実施している企業は、**本診断の結果が高い評価**となりました。
・総務部門ではなく、**各業務部門に情報システム・情報セキュリティ対策の担当者を置いている。**
・**担当者が協力して規定の策定・運用、技術的対策を実施している。**

➢企業の状況にもよりますが、総務部門だけでなく**業務部門も情報セキュリティ対策に関わることが大切**です。また、本社だけでなく、**本社以外の拠点や工場が関わることも大切**です。

業務部門が関わることが大切なのは、職場の他のルールと同じではないでしょうか？

診断で得られた気づきは以下のとおりです。

診断で得られた気づき(3/3)

5　ガイドラインを参考に基本方針等を策定すること

➢基本方針の策定が必要なことを理解しており、ガイドラインの存在を知っているが、**ガイドラインの内容を理解して自社に合った基本方針や規定を策定することが難しい**という意見がありました。

➢情報セキュリティ対策担当者のみでなく、実務に詳しい**他部門（業務部門、法務部門、人事部門等）**が協力することが必要です。
➢複数部門を巻き込むためにも、**経営者のリーダーシップが必要**です。

➢国のガイドライン以外では、以下が参考となります。
・自社の属する業界や近い業界の**業界団体のガイドライン**を活用する。
・自社に近い業種・規模の**他社の基本方針**を参考にする。
（企業によっては、基本方針をWEBサイトで公開しています）
・**親会社やグループ会社の規定**をもとに策定する。

➢自社だけでは規定の策定が難しい場合、**専門家**に協力を求めることも有効です。
・必要に応じて、**外部委託**する。
・**親会社やグループ会社に協力**を求める。

情報セキュリティ対策には、自社内の協力が必要です。
また、自社だけでは難しい場合、他社・他団体に協力を求めることも有効です。

診断結果の説明・改善提案及びフォローアップ時の気づきは、以下のとおりです。

診断結果の説明・改善提案及びフォローアップ時の気づき

1　相談対応に対する需要

➢**他社の情報セキュリティ対策についての状況や動向**を気にしている企業が多くありました。
➢情報セキュリティ対策に関してITベンダーと契約を結んでいるものの、**第三者的な意見や相談窓口を求めている**企業がありました。
（例）・ITベンダーの推奨するシステムを導入しているが、自社に適しているかどうか判断できない。
・情報セキュリティ対策について相談できる相手がいない。

➢**自社と近い業種や規模の企業の情報セキュリティ対策状況**は参考になりますが、公開されているものは少なく、**詳細な内容を知ることは難しい**です。
➢情報セキュリティ対策は、**費用**と**情報セキュリティ事故が発生する可能性や発生した場合の損失額のバランス**を考慮して実施することが大切です。
➢このような場合には、情報提供や相談対応が可能な**公的機関・支援機関に協力を求める**ことが有効です。

2　社内の教育や意識向上

➢情報セキュリティに関する**社内の教育や従業員の意識向上に課題**を感じている企業がありました。
（例）・社内教育を実施するために必要な教材がない。
・専門知識が不足しているので、教えることが難しい。

➢専門知識が少ない人が一から教材を作成することはハードルが高いため、**公的機関が無料で公開している教材を活用**することを推奨します。また、説明動画やオンライン研修の活用も有効です。

相談対応や教育には、公的機関・支援機関の施策を活用することが有効です。

6. 総評

情報セキュリティ対策に課題を抱えている企業が多くありました。
経営者がリーダーシップを発揮して、まずは以下の項目に着手することを推奨します。

総評

基本方針、対策基準、規定の策定

- 「基本方針」は組織の情報セキュリティ対策のベースとなる方針です。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、自社に適した**基本方針を定め宣言することが重要であり、優先して対応**することが必要です。
- 人材や費用が少なくても対策が可能な**「従業員ルール」について優先的に規定を策定**することを推奨します。また、**情報セキュリティ対策ツールの性能を最大限に引き出すため**には、**ツールの導入に併せて規定を策定すること**が必要です。

情報資産管理

- 重要な情報資産を特定し、適切な情報セキュリティ対策を講じるために、**情報資産の管理簿を作成して、組織内の情報資産を抜け漏れなく把握して適切に分類する**ことが必要です。

社内の組織体制

- 総務部門等の特定の担当者のみでなく、複数部門を巻き込み、**組織的に情報セキュリティ対策を進める**ことを推奨します。
- **社内教育**を実施して、**従業員全体の意識を向上**させることが大切です。その際は、**公的機関が公開する教材**の活用が有効です。
- 近年、工場において情報端末が利用されることが増え、工場の情報セキュリティ対策が必要とされています。そのためには、**工場関係者も情報セキュリティ対策に関わる組織体制作り**が必要です。

社外との関係構築

- 規定の策定や情報セキュリティ対策の実施においては、国や業界団体のガイドラインが参考になりますが、自社だけでは実施が難しい場合は、**グループ会社、支援機関及びITベンダーに協力を求めることも有効**です。
- **サプライチェーン内で規定の準用や合同教育の実施等**、具体的な**情報セキュリティ対策**を進めることが望まれます。

7. 参考情報

情報セキュリティ対策に関する相談窓口や補助金の例として、以下のものがあります。

相談窓口や補助金等についての情報

相談無料　愛知県デジタル技術活用相談窓口

デジタル技術活用・情報セキュリティ対策の専門家であるアドバイザーが、相談内容に応じて、課題の解決につながるアドバイスをします。

- **事業詳細**

https://www.pref.aichi.jp/press-release/aichi-pref-iot/digital-adviser2023.html

- **相談申込**

https://forms.office.com/e/N7vAWxseBP

TEL： 052-565-5955
（受付時間 平日 10:00~17:00　※11:45~12:45は除く）

相談無料　公益財団法人　あいち産業振興機構

ITやDXの専門家が、あらゆるご相談に無料でお応えします。
中小企業等向け情報セキュリティ診断のチェックリストに基づく助言が可能です。
出張相談も行います。現場を拝見した上で、アドバイスさせていただきます。

- **事業詳細**

https://www.aibsc.jp/support/257/

- **相談申込**

https://www.aibsc.jp/inquiry?pid=257

Pit-Nagoyaセキュリティ

「名古屋中小企業IT化推進コンソーシアム」（略称： Pit-Nagoya、主催：名古屋商工会議所）では、情報セキュリティ対策サービス「Pit-Nagoyaセキュリティ」を提供しています。

- **事業詳細**

https://pit-n.nagoya-cci.or.jp/core/wp-content/themes/pit-nagoya-theme/common/doc/pit-n-security.pdf

- **相談申込**

https://answer.cci.nagoya/sogyo/?code=c118eda9

IT導入補助金（セキュリティ対策推進枠）

- **事業詳細：** https://it-shien.smrj.go.jp/applicant/subsidy/security/
- **補助対象者：** 中小企業・小規模事業者等
- **補助額：** 5万円以上100万円以内
- **補助率：** 1 / 2 以内
- **補助対象：** ITツールの導入費用及び、サービス使用料*（最大2年分）
  (※)独立行政法人情報処理推進機構（IPA）が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されているサービスをメインのITツールとした申請（「サイバーセキュリティお助け隊サービス」単品での申請）を実施することができます。

参考情報

参考情報

資料名	発行元	URL
中小企業の情報セキュリティ対策ガイドライン	独立行政法人　情報処理推進機構	https://www.ipa.go.jp/security/guide/sme/about.html
サイバーセキュリティ体制構築・人材確保の手引き	独立行政法人　情報処理推進機構	https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf
情報セキュリティ教材	独立行政法人　情報処理推進機構	https://www.ipa.go.jp/security/net-anzen/security_materials.html
工場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	経済産業省	https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html
国民のためのサイバーセキュリティサイト	総務省	https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html
一般利用者が安心して無線LANを使用するために	総務省	https://www.soumu.go.jp/main_sosiki/joho_tsusin/security.html
セキュリティ人材の活躍の促進に向けた流動性とマッチングの機会の促進	内閣サイバーセキュリティセンター	https://www.nisc.go.jp/pdf/council/cs/jinzai/dai14/14shiryou0106.pdf
メール訓練手引書	日本シーサート協議会	https://www.ipa.go.jp/security/guide/sme/about.html

用語集

用語集(1/2)

用語	説明
インシデント	情報セキュリティの分野において、情報セキュリティリスクが発現・現実化した事象のことです。
ウイルス対策ソフトウェア	ウイルスからパソコンやスマホの防御するためのソフトウェアを指します。アンチウイルスソフトやワクチンソフトとも呼ばれています。 パソコンやスマホに侵入したウイルスを駆除したり、電子メール等で送信するファイルにウイルスが含まれていないか等をチェックしたりすることができます。
ウイルス定義ファイル	ウイルス対策ソフトウェアがマルウェア等のウイルスを検出するための定義情報が入ったファイルを指します。
記録媒体	パソコンやスマホ等で作成したデータを保存しておくものです。 記憶メディアや記録メディア、または単にメディアと呼ばれることもあります。 現在利用されている記憶媒体には、ハードディスク、フラッシュメモリ、CD/DVD-ROM、SDカード等があります。
脅威	システム又は組織に損害を与える可能性があるインシデントの潜在的な原因を指します。 不正行為、操作ミス等の人為的な脅威、自然災害やアクシデント等の組織がコントロールできない脅威等があります。 脅威は、脆弱性とともに情報セキュリティリスクを構成する要素の一つです。
情報資産	企業や組織等で保有している情報全般のことを指します。 顧客情報や販売情報等の情報自体に加えて、ファイルやデータベースといったデータ、CD/DVD-ROM、SDカード等のメディア、そして紙の資料も情報資産に含まれます。
情報セキュリティ対策	情報資産を安全に管理し、適切に利用できるように運営する経営管理を指します。 適切な管理・運営のためには、情報の機密性・安全性・可用性が保たれていることが必要です。
情報漏えい	障害、事故、人為的ミス、不正行為、不正プログラム等により、パソコンやサーバで管理していた情報がユーザの意図に反して外部に流出すること等を指します。
脆弱性	パソコンやネットワークにおいて、情報セキュリティ上の問題となる可能性がある弱点のことを指します。 多くの場合は、OSやソフトウェアのセキュリティホールが脆弱性と表現されます。また、設定ミスや管理体制の不備等も脆弱性となることがあります。 脆弱性が具体的な脅威と結び付くと、情報セキュリティのインシデントが発生します。

用語集

用語集(2/2)

用語	説明
セキュリティパッチ	パソコンやスマホのシステム上に開いた情報セキュリティの「穴」を塞ぐために、メーカー等から提供される修正プログラムです。 ソフトウェアアップデートに含まれる場合もあります。
セキュリティホール	パソコンやスマホのソフトウェア等において、攻撃者が不正な侵入等を行える状態になっているプログラム上の「穴」のことです。
ソフトウェアアップデート	ソフトウェアやアプリの更新を実施することを指します。情報セキュリティ対策の向上を含む場合もありますが、単に機能向上のみ場合も存在します。 情報セキュリティ対策の向上のみを実施する場合は、情報セキュリティパッチと呼ばれることもあります。
バックアップ	パソコンやスマホの情報を別途保存しておき、機器が故障したり紛失や盗難したりした場合に復元するためのものです。
フィッシング	メールやWEBサイト等を使用し、攻撃者がターゲットから、お金につながる情報や個人情報を盗み取る行為です。 フィッシング（phishing）は洗練された（sophisticated） ＋ 釣る（fishing）に由来していて、嘘の情報を餌にして釣り上げるというイメージです。
リモートデスクトップ	遠隔地の情報端末（パソコン、スマホ等）にネットワークを介してアクセスし、手元の端末で操作する技術のことです。
MDM	MDMとは「Mobile Device Management 」の略称であり、企業や組織等で、スマートフォンやタブレット端末等の携帯端末を安全に管理する仕組みのことです。
VPN	「Virtual Private Network」の略で、インターネット上に仮想的なプライベートネットワーク（専用線）を設けて、情報セキュリティ上の安全な経路を使ってデータをやり取りする技術のことです。