国の2つの文書と、監査役協会の調査を、当社の公開資料に置き換える対応表

2026年11月5日の注意喚起と、11月6日に関係閣僚会議で策定された緊急対策パッケージと、監査役協会の調査。この3本を、当社が公開している資料のどこで聞けるか・どの工程で満たすかに置き換えた1枚です。

新しい紙は作っていません。**どれも公開済みの資料への地図です。**

読み手は3層です。**経営は対応表C から、情報システムは対応表A から、開発と運用は対応表B から**開いてください。

使う順（最初に開くシートから）

5シートありますが、自分の立場の1枚だけで足ります。

#	立場	開くシート	そこで分かること
1	経営・取締役・監査役等	**対応表C**	監査役協会の着眼点6区分ごとに、執行側へ聞く言葉と、調査で分かっている割合
2	情報システム	**対応表A**	11月5日の注意喚起の3章8項目ごとに、点検表61問のどれで確かめるか・どの工程か・別の方法で確かめる所
3	開発・運用	**対応表B**	緊急対策パッケージのうち企業に関わる施策と、今週できること
4	全員	**出典**	3本の原本の名前・日付・どの語を採ったか

経営の方は、対応表C の「着眼点」と「執行側へ聞く言葉」の2列・6行だけで足ります。 残りの2列（問いの番号・調査の割合）は、**担当者に渡すときの手がかりです。** 5分で読み終わります。

この表は、当社の資料を売るための物ではありません。 資料はすべて公開しています。**読み手が自分の組織で使えればそれで足ります。**

この表でできることと、人が決めること

この表は、どこで確かめるかを立場ごとに最短で示します。 確かめた結果をどう判定するかは、**その組織の人が決めます。**

「準拠」「適合」「対応済み」の語を使わないのは、国の文書が企業に義務を課すものではないからです。

対応表C（経営・取締役・監査役等）

日本監査役協会の報告書にある着眼点6区分に、当社の「17の問い」を当てました。

#	着眼点（報告書の語）	当社の17の問いの番号	執行側へ聞く言葉（要旨）	調査で分かっていること
1	サイバーセキュリティが経営課題となっているか	問1	何を・いつまでに・いくらでやるか、経営で決めたか	取締役会等で定期報告がされていない会社が**43.7%**（Q1・回答1,527社）

#	着眼点（報告書の語）	当社の17の問いの番号	執行側へ聞く言葉（要旨）	調査で分かっていること
2	サイバーセキュリティリスク管理体制の整備・運用状況	問3・問7・問8	管理者権限の一覧はあるか。多要素認証に未登録の管理者はいないか。ログは決めた期間残っているか	独立した専門組織が設置されていない会社が**53.7%**（Q6・回答1,525社）
3	「侵入後」を想定した緊急対応体制の整備	問5・問9・問12	バックアップから戻す試験を1年でやったか。侵入の痕跡を誰がいつ調べたか	サイバー攻撃を想定した BCP を策定していない会社が**56.7%**（Q12・回答1,513社）
4	グループ会社・サプライチェーンでの対策	問4	委託先の一覧はあるか。注意喚起を受けて何社に聞いたか	監査役等が確認していない・報告を受けていない会社が**38.4%**（Q16-1・回答1,497社）
5	監査計画へのサイバーセキュリティの反映と監査活動	問2・問10・問14・問15	外から見える機器の一覧はあるか。公開範囲を誰がいつ確かめたか	以前から特に監査対象にはしていない会社が**26.6%**（Q17・回答1,498社）
6	インシデント発生時の監査役等の対応	問11・問16	漏えい時に誰へ何を知らせるかは文書になっているか	監査役等への第一報が発生当日〜1日後だった会社が**47.8%**（Q25・回答270社＝攻撃を受けた会社のみ。**この数だけ、できている側の割合です**）

数の読み方（3つ）

(1) 母数は設問ごとに違います。 調査全体の回答は1,528社ですが、設問ごとに答えた会社数が異なります。6区分の母数は 1,527／1,525／1,513／1,497／1,498／270 で、**同じ数字はひとつもありません。** だからこの表では、**数のたびに設問番号と回答社数を併記しています**（調査全体の1,528社との違いは、出典のシートに書いています）。

(2) 区分6の 47.8% だけ、向きが逆です。 他の5つは「できていない会社の割合」ですが、47.8% は「監査役等への第一報が当日〜1日後だった会社」＝**できている側の割合**です。報告書は「裏を返せば、半数近くの会社では監査役等への第一報が2日後以降にずれ込んでいる」と書いています。**5つと並べて「悪い数が6つ」と読まないでください。**

(3) 区分6の母数270社は、全社ではありません。 サイバー攻撃を受けた会社だけが答えた設問です。**他の5区分（1,497〜1,527社）とは比べられません。**

使い方

6区分を順に聞く必要はありません。 自社で弱いと感じる区分から1つ選び、**「執行側へ聞く言葉」の列をそのまま聞いて、物が出てくるかだけを見てください。**

物が出てこない「はい」は、「分からない」と同じです。 これは17の問いの前書きに書いた線で、この表でも変えていません。

対応表A（情報システム）

11月5日の注意喚起の3章8項目に、当社の点検表61問と、判定の5工程を当てました。

項目の見出しは、注意喚起の原文のままです。 当社が言い換えていません。

「工程」の列は、判定の工程を番号で書いています。 工程0＝資産の把握／工程1＝検知／工程2＝判定／工程3＝修正／工程4＝確認。**第10弾「判定の台帳と組む手順」の5工程と同じ番号です。**

章の名前だけは、当社が短くしています。 原文は「1．運用・管理段階におけるセキュリティ対策の徹底」「2．設計・開発段階におけるセキュリティ対策の徹底」「3．サプライチェーンを通じた侵害への対策」で、**表の列に収まらないためです。** 原文は出典のシートに書いています。

章	項目（原文）	当社の点検表で確かめる問い	工程	別の方法で確かめる所
1 運用・管理	（1）デジタル資産の適切な把握及び脆弱性の解消	A-13（社外に面した機器・ソフトの一覧）／A-14（悪用されている脆弱性が残っていない）／A-15（直す期限を決めて守る）／A-16（設定ファイルやバックアップが外から取り出せない）	工程0・1	**ライブラリの深さ（何段目まで追うか）は、依存を管理するツールの側で決める所。** 点検表は「一覧があるか」までを問います
1 運用・管理	（2）アタックサーフェスの継続的な棚卸し及び最小化	A-1（サブドメインの把握）／A-2（社外から接続できる窓口）／A-3（クラウドの保存場所の公開設定）／A-4（部署ごとのクラウドサービス）	工程0	**「業務上不要な機能」を外す判断は、その業務を担当する部門が決める所。** 点検表は「一覧と公開設定」までを問います
1 運用・管理	（3）AI の活用等による継続的な脆弱性診断及び不審な挙動の監視	C-1（身に覚えのないファイル）／C-3（直近1か月のログを見た記録）／C-7（知らせの届け先）／C-8（見て判断した記録）	工程1・4	**AI に診断させる所は、当社の別の資料「判定の台帳と組む手順」の「AI に渡す指示」シートで扱っています**
2 設計・開発	（1）セキュリティ・バイ・デザインの適用	A-17（他社スクリプトの一覧と変化の検知）／A-8（アプリの中の鍵で管理者操作ができない）	工程0	**設計段階のレビューの進め方は、開発の工程の中で決める所です**
2 設計・開発	（2）利用する API のセキュリティ対策の強化	A-5（公開 API の一覧）／A-6（ログイン不要の API が無い）／A-7（他人のデータが見えない）／A-9（止めた鍵の記録）／A-10〜A-12（大量アクセスの上限と検知）	工程0・1	—
2 設計・開発	（3）公開前の脆弱性診断の実施	A-14（悪用されている脆弱性が残っていない）／A-15（直す期限）	工程1・4	**公開前の外部診断は、診断の事業者に頼む所です**
3 サプライチェーン	（1）委託先のセキュリティ統制及び委託先からの接続経路の厳格化	E-3・E-4（委託先の一覧と点検）／B-6（委託先アカウントの多要素認証と接続元の限定）／B-7（他社アカウント連携の一覧）	工程0・2	—
3 サプライチェーン	（2）オープンソースソフトウェア（OSS）や外部ライブラリ等の適切な管理	A-13（製品名とバージョンの一覧）／A-14・A-15	工程1	**構成の一覧（SBOM）の出力は、ツールで出す所。** 当社もまだ手作業で、自動にしていません

使い方

8項目を順にやる必要はありません。 自社で薄いと感じる章から1つ選び、右の2列（工程と、別の方法で確かめる所）を先に読んでください。

「別の方法で確かめる所」を先に読むのは、点検表で済む所と、別の担当や外部に回す所を、最初から分けて動けるようにするためです。

この表の次に、点検表で確かめる

8項目を満たしているかは、この表が示す点検表の問いに答えると分かります。

注意喚起は企業に義務を課すものではなく、 原文も「改めて基本的な対策の徹底をお願いいたします」という書き方です。

対応表B（開発・運用）

緊急対策パッケージのうち、企業に関わる施策だけを抜きました。

パッケージは4つの柱でできていて、施策の多くは府省がやることです。 企業に義務を課すものではありません。 ここに挙げたのは、企業の側に影響するか、使える窓口が増えるものだけです。

#	柱	施策（原文の見出し）	担当	時期	今週できること（当社の考え）
1	1	最近の情勢を踏まえた注意喚起の実施	国家サイバー統括室	2026年11月5日に発出済み	注意喚起の3章8項目を、対応表A で自社に当てる
2	1	保有する個人データの最小化と安全管理の強化	個人情報保護委員会	ガイドラインは**令和9年1月中の施行を目指す**	使わなくなった個人データが残っていないかを数える。本人確認で取った画像の保存期間を決める
3	1	不正アクセスに関する個人情報保護法の厳格な執行	個人情報保護委員会	随時	漏えい時の報告の窓口と手順を、文書で持っているか確かめる
4	1	トップガン人材チームの立上げ	経済産業省	**11月中**	自社の診断を頼む先を1つ決めておく
5	1	AI の実装を前提としたサイバーセキュリティ対策の強化	関係省庁	継続	AI に渡す物と、やらせない操作を決める（「判定の台帳と組む手順」の「AI に渡す指示」シートが使えます）
6	2	SCS 評価制度における企業等からの情報収集	国家サイバー統括室・経済産業省	評価制度は**令和9年3月頃に運用開始**。その後に仕組みを導入	SCS を取得済み・取得予定なら、情報提供の求めが来たとき誰が答えるかを決めておく
7	4	警察の相談対応の充実・強化	警察庁	都道府県警察本部に専用窓口	被害時の連絡先を、相談窓口まで含めて1枚にする
8	4	無料相談窓口の設置	経済産業省	IPA に**2026年10月16日**に特別相談窓口	同上
9	4	二次被害の防止・お困りの方のための情報発信の強化	関係省庁	継続	漏えい時に利用者へ何を知らせるかの文面を、先に作っておく

この表で確かめていないこと

施策の総数を書いていません。 当社が原本のテキストから数えようとしたところ、**式を変えるたびに違う数になりました**（4通り）。**原文は改行の都合で見出しが2行に分かれ、入れ子の番号も行頭に来るためです。 数えられなかったので、「4つの柱」までにしています。**

時期が書かれていない施策があります。 「随時」「継続」と書いたものは、**原文に時期の記載が無いという意味**です。当社が推測した日付ではありません。

この表で対象にしていない施策

量子暗号・医療・学校・通信事業者向けの施策は、この表の対象から外しています。 当社が出しているのが、**一般的なクラウド基盤の上で動くウェブアプリ・API・データベースを持つ企業**向けの資料だからです。

出典

#	資料	発行	日付	この表で使った所
1	個人情報の漏えい等につながる不正アクセスへの対策について〜ウェブサイトやモバイルアプリに関する基本的な対策の徹底〜	内閣官房国家サイバー統括室	2026年11月5日	対応表A の3章8項目

#	資料	発行	日付	この表で使った所
2	サイバーセキュリティ緊急対策パッケージ（概要および本体）	サイバーセキュリティに関する関係閣僚会議	2026年11月6日に**策定**	対応表B の柱と施策
3	経営リスクとしてのサイバーセキュリティ ―アンケート調査から読み解く企業の現状と監査役等の着眼点―	公益社団法人日本監査役協会（月刊監査役 No.795）	2026年10月29日	対応表C の着眼点6区分と6つの割合

調査の母数について（1,528社と、設問ごとの回答社数）

調査の総回答社数は1,528社です。 法人会員7,775社に対して回答率19.7%、調査期間は2026年5月下旬から6月上旬です。**設問ごとの回答社数はこれより少なく、設問によって違います。**

だから対応表C では、割合のたびに設問番号と回答社数を書いています。 1,528社は調査全体の数で、個々の割合の母数ではありません。**この2つを混ぜて「1,528社のうち56.7%」と書くと、原本と合わなくなります。**

どの語を採ったか

着眼点の6区分は、報告書の概要ページの語を使いました。 本文（51ページ以降）では (2)(3)(4) の言い回しが少し違います（「〜の確認」「〜が整備されているか」「〜がなされているか」）。**概要ページの語の方が短く、表に収まるためです。**

パッケージは「策定された」と書いています。 本体の PDF の表紙は「サイバーセキュリティに関する関係閣僚会議決定／令和８年11月６日」ですが、**同じ日の会議資料の PDF は表題が「(案)」で、日付欄が空欄です。** 版によって表記が違うため、**どちらでも正しい「策定された」を使いました。**

SCS 評価制度の運用開始は「令和9年3月頃」です。 原文に3か所あります（本体 2.(2) と、別紙の施策一覧に2か所）。**IPA が告知している「2027年3月の登録申請受付開始予定」とは別の語なので、混ぜていません。**

注意喚起の項目の見出しは、原文のままです。 当社が言い換えていません。

章の名前だけ短くしました。 原文と、表に書いた名前の対応は次のとおりです。

原文の章	表に書いた名前
1．運用・管理段階におけるセキュリティ対策の徹底	1 運用・管理
2．設計・開発段階におけるセキュリティ対策の徹底	2 設計・開発
3．サプライチェーンを通じた侵害への対策	3 サプライチェーン

短くした理由は、表の列に収まらないためです。 意味を変えた言い換えはしていません。