取締役・監査等委員が執行側に聞く17の問い

聞く言葉／見せてもらう物／「分からない」の意味

使い方（役員向けの前書き）

この17の問いは、情報システムの知識がなくても**執行側**（社長・執行役員・情報システムの責任者と担当者。会社を実際に動かしている側）に聞ける言葉にしてあります。答えが「はい」でも「いいえ」でも、まず②の物を見せてもらってください。物が出てこない「はい」は、「分からない」と同じです。「分からない」は責める材料ではなく、次に確かめる場所です。

順	対策項目（点検表の ID）	①聞く言葉	②見せてもらう物	③「分からない」の意味
1	経営層が関与する（E-1・E-2）	今回の国の注意喚起に対して、何を・いつまでに・いくらでやるか、経営で決めましたか	経営会議や取締役会の議事録の該当箇所。有報の「事業等のリスク」の該当文。**指摘が経営に届いた日と、決めた日の記録。現場から経営への報告が定型（何が起きうるか／どこまで届くか／いま止めるか／直す期限／受容なら期限と代わりに置くもの、の5行）になっているか。直近3か月で、この形で上がった報告を1通。指摘した専門家に是正を命じる権限が無い場合は、取締役会へ直接届ける経路の文書**	現場任せで、順番も予算も決まっていない。以下の16項目の答えが揃っても、実行されない。**定型が無ければ、上がらなかったことの責任を後から分けられない**
2	脆弱性に対応する（A-13〜A-15）	社外から見える機器やソフト（VPN 装置・Web サーバーなど）の一覧があり、実際に攻撃に使われている弱点が残っていないことを、誰がいつ確かめましたか	一覧（製品名と版）と、確かめた日・人・結果の記録。**直した後、同じ観点で消えたことを確かめた記録（再診断の有無と日付）**	自社が外からどう見えているか把握できていない。最初の侵入口の多くがここ
3	権限の付与を見直す（B-3〜B-5）	管理者の権限を持つ人の一覧があり、全員について理由を言えますか。辞めた人・使っていないアカウントは残っていませんか	管理者の一覧と、最後に棚卸した日。退職者の停止記録	誰が何でもできる状態か把握できていない。内部不正と乗っ取りの両方の入口
4	委託先を含めて管理する（E-3・E-4）	当社のシステムやデータに触れる委託先の一覧があり、今回の注意喚起を受けて主な委託先に点検の状況を聞きましたか	委託先一覧と、聞いた記録（日付・相手・返答）。**直近で聞いたのはいつか。一覧のうち何社に聞いたか**	委託先経由の事故が起きても、どこから入られたか分からない
5	インシデント発生時の対応（C-9〜C-13）	被害が起きたとき誰が何をするかが文書になっていて、バックアップから実際に戻す試験をこの1年でやりましたか。管理者でも消せない場所に複製はありますか	対応手順書の最終更新日。復元試験の記録（日・対象・結果）。隔離した複製の説明	止まったとき戻れるかが分からない。ランサムウェアで最も差が出る項目
6	保存データを暗号化する（D-3）	データベース・バックアップ・ノートパソコンの中身は暗号化されていますか	暗号化の設定画面か、台帳の該当列	機器や媒体を失ったとき、中身がそのまま読まれる
7	自組織のシステムの認証を強化する（B-1・B-2）	管理者・VPN・クラウドの管理画面・メールに、パスワード以外の確認（スマホの確認など）がかかっていますか。管理者に1人でも未登録はいませんか	多要素認証の登録状況の一覧（管理者の行）	パスワードが漏れただけで入られる。不正ログインの型の大半がここ
8	ログを取得し一定期間保管する（C-4〜C-6）	ログイン・管理者の操作・外部との通信の記録を取り、決めた期間残していますか。消せる人	ログの保存先と保存期間の一覧。消せる権限を持つ人の一覧	何が起きたか後から調べられない。保険の免責や当局への報告にも響く

順	対策項目（点検表の ID）	①聞く言葉	②見せてもらう物	③「分からない」の意味
		は限られていますか		
9	不正アクセスを検知する仕組みを整える（C-7・C-8）	怪しいログインや大量のデータ持ち出しに気づいたとき、誰に知らせが届き、直近1か月で誰が見て判断しましたか	通知の届け先の設定と、直近の対応記録	侵入されても気づかない。被害が広がる時間が長くなる
10	外部への公開範囲を見直す（A-1〜A-4）	自社のドメインの下にあるサイトやサービスを全部把握し、誰でも見られる設定の置き場所や、外からつなげる管理画面・データベースが無いことを確かめましたか	把握した一覧と、確認した日	知らないうちに外に開いている物がある
11	漏えいした情報の悪用を防ぐ（C-14・C-15）	情報が漏れたとき、誰に何を知らせるかと、利用者にパスワード変更を呼びかける手順は文書になっていますか	通知の手順書と連絡先一覧	漏えいの後、二次被害を止める動きが遅れる
12	侵害の痕跡がないか調査、点検する（C-1〜C-3）	公開しているサーバーに身に覚えのないファイルや説明できない変更が無いことを、直近で誰が確かめましたか。すでに被害が疑われるなら、これを最初に	点検の記録（見た日・人・対象・結果）	すでに入られているかどうかを誰も見ていない。IPA が最初に行うよう示している項目
13	不要になったデータを残さない（D-1・D-2）	保存期間を過ぎた個人情報を消した記録はありますか。本番以外（検証環境・書き出したファイル）にある個人情報の置き場所を把握していますか	削除の記録と、置き場所の一覧	漏れたとき、本来持っていなくてよかった情報まで漏れる
14	通信を暗号化する（D-4・D-5）	公開しているサイトと API はすべて暗号化され、古い方式は受け付けず、証明書の期限は切れていませんか	証明書の一覧と期限。設定の確認結果	通信の途中で読まれる・改ざんされる。期限切れはサイト停止にも
15	API の管理状況やアクセス制御を見直す（A-5〜A-9）	自社で作ったサイトやアプリの裏の窓口（API）の一覧があり、ログインなしで呼べるものや他人のデータが見えるものが無いことを確かめましたか。辞めた人や終わった取引先に渡した鍵は止めましたか	API の一覧。鍵の台帳と失効の記録	自社開発の部分が、誰も見ていない入口になっている
16	被害や攻撃に関する情報を提供、共有する（E-5〜E-7）	同業や当局と情報を共有する先が決まっていて、出してよい情報の線引きは文書になっていますか	共有先の一覧と、線引きの文書	被害時に誰に言うべきか分からず、報告の期限を落とす
17	大量アクセスを制限する（A-10〜A-12）	同じ相手からの大量のアクセスに上限をかけ、超えたときに誰かが見ていますか。サイトが止まったとき、回線やクラウドの事業者に誰が何を頼むか決まっていますか	上限の設定と、超過の記録。事業者の連絡先	止められるまで気づかない。止まったとき頼る先が無い

＋1（当社の追加）社内で使う AI（点検表の F-1〜F-6）

聞く言葉＝社員が業務で使う AI の一覧と、入れてはいけない情報の決まりがありますか。権限を持って動く AI には、人とは別の鍵と、操作の記録がありますか

見せてもらう物＝AI の一覧（委託先一覧への記載）。利用規程。鍵と記録の説明

「分からない」の意味＝社員が何を AI に入れているか、AI が何をしたか、誰も追えない

国の注意喚起の17項目には入っていません。当社が足した1項目です。

役員の方への添え書き

- 17のうち、まず 2・7・12 の3つ（入口・アカウント・痕跡）だけ聞いてください。点検表の「今日の3問」と同じ3つです。
- ②の物が出てこない項目が、次の取締役会までの宿題です。
- 点検表（53問）は、会社を動かす側（情報システムの担当者）が答える表です。この17の問いは、それを外から見る立場（取締役・監査役）が聞く表です。同じ項目番号で対応しています。
