見つけた後に、誰がどう決めるか（判定の台帳）

検知を増やすと、詰まる場所が検知から判定へ移ります。決めた人と決めた日を残す1枚。

機械は見つけるところまでです。どうするかは人が決めます。この台帳は、その決めたことを置く場所です。**判定に使える時間を増やすものではありません。**

台帳の列

#	列	書くこと	誰が埋めるか
1	識別子	CVE 番号など。無ければ自社の連番	機械
2	見つけた日	検知の日付	機械
3	どこで見つけたか	依存関係の検査／静的な検査／外からの受け身の検査／脅威情報の取り込み／外部からの連絡	機械
4	外から届くか	インターネットから直接届く／社内からだけ／届かない	人（機械の下書きを確かめる）
5	悪用されているか	公的な一覧に載っている／報告がある／無い	機械
6	攻撃を自動化できるか	できる／できない／分からない	人（機械の下書きを確かめる）
7	乗っ取りの程度	全部取られる／一部だけ／限定的	人
8	段	下の「段の4つ」から1つ	人
9	期限	日付。数え始めの日も書く	人（機械が候補を出す）
10	対応の種類	直す／つなぐ／受け入れる	人
11	決めた人	役割名。個人名でなくてよい	人
12	決めた日	日付	人
13	閉じた日・見直す日	直したら閉じた日。受け入れたなら次に見直す日と、その理由	人

列は13です。4から7の4つが、段を決める材料です。10から12の3つが、この台帳の芯です。

11と12を空欄のまま運用すると、**半年後に「なぜこれを受け入れたのか」が誰にも分からなくなります。** 直した件は記録が無くても困りませんが、**受け入れた件は記録が無いと困ります。**

段の4つ

段	意味	次にすること
すぐ動く	外から届き、悪用されていて、自動化もできる	その日のうちに、直すか、届かない状態にする
順番に入れる	外から届くが、悪用の報告が無い。または悪用されているが外から届かない	期限を決めて、通常の作業の列に入れる
記録して見直す	いまは当たらないが、構成が変われば当たる	台帳に残し、構成を変える前にもう一度見る
記録だけ	当たらない。使っていない機能	台帳に残す。作業は起こさない

この4つは、米国の CISA が公開している SSVC（2022年11月10日）の結論の4つと同じ並びにしています。訳と言い換えは当社のものです。

判定の4つの要素

要素	問い	なぜこれを見るか
外から届くか	インターネットから直接たどり着けるか	届かない物は、同じ深刻度でも急がない
悪用されているか	実際に使われた報告があるか	深刻度の数字より、使われている事実が先に来る

要素	問い	なぜこれを見るか
攻撃を自動化できるか	手作業が要るか、まとめて撃てるか	自動化できる物は、広く・速く来る
乗っ取りの程度	全部取られるか、一部で止まるか	一部で止まる物は、つなぎの策が効く

深刻度の数字（CVSS の基本値）だけで順番を決めません。基本値は、自社の事情を含んでいません。CVSS を作っている FIRST 自身が、基本値を脅威と環境の値で補うべき（should enrich）と書いています（CVSS v4.0 仕様書・2023年11月1日）。

米国 CISA の BOD 26-04（2026年6月10日）も、この4つの要素で段を決めています。**ただしこの指令は米連邦の文民行政機関だけを拘束するもので、日本の企業の義務ではありません。**

期限の物差しの比較表

物差しを6つ並べます。どれも、その対象のために作られた物差しです。日本の企業一般の義務ではありません。自社の期限は、この表を見ながら自社で決めてください。

物差し	対象	期限	延長・例外	出典の日付
CISA BOD 26-04	米連邦の文民行政機関（契約で定めれば委託先も）	4つの要素で段を決める。最短3日（修正か緩和に加えて、侵害の有無の調査も）。最も低い段は「次の大きな更新のとき」	CISA は免除や例外を出さないと明記。外から届かない状態にすれば段が下がる	2026-06-10（手引 2026-08-25）
CISA BOD 22-01	同上	公的な一覧に載った物は2週間（古い物は6か月）	廃止済み。BOD 26-04 に置き換わった	2021-11-03
SCS 評価基準 4-4-4-2（★3・★4）	任意の評価制度を申請する事業者	**アップデートプログラムがリリースされてから14日以内。**対象は、ベンダーが「重大」または「高リスク」と説明する脆弱性を直す物、深刻度の基本値が7.0以上の物、レベルの詳細がベンダーから提供されていない物	期限内に当てられない場合は、機能の無効化・ベンダー推奨の回避策・ネットワークからの分離・不正な通信の遮断のいずれかで リスクを下げる。基本値7.0以上でも、情報公開の時点で攻撃が観測されていない（蓋然性が低い）物は、対応計画と代替策を前提に期限の延長を認める。**公的機関等の一覧に載っていて攻撃が観測されている物は、引き続き14日**	IPA・要求事項・評価基準 Ver.1.1（2026-10-28）
重要インフラ統一基準 3.3.6③	重要インフラ事業者が安全基準に盛り込む事項	日数は決めない。修正を当てる作業方針を確立すること	リスクに応じた措置	2026-07-31 決定・2026-10-01 施行
NIST SP 800-40 Rev.4	一般向けの手引	日数を決めない。資産のまとまりごとに自分で期限を決める	例外は追跡し、定期的に見直す	2022-04
国の注意喚起	重要インフラ事業者等	「速やかに」（日数は無い）	事業継続を含む総合的な判断。手順を事前に作ること	2026-05-18

共通しているのは、**期限が1つの数字ではない**ことです。どれも「外にどれだけ出ているか」と「実際に悪用されているか」で変え、状況が変わったら見直す形になっています。

数え始めの日も決めておいてください。BOD 26-04 は、公的な一覧に追加された日か、自分で検知して管理の仕組みに載せた日の、**早い方**から数えると書いています。

この表で確かめていないこと

BOD 26-04 の中間の段の日数は、確かめられていません。 CISA のページでは該当の表が画像で埋め込まれていて、本文に日数が載っていません。確かめられたのは、最短が3日であることと、最も低い段が「次の大きな更新のとき」であることの2つだけです。**中間の段に何日と書いてある表は、当社は見ていません。**

この表から、1つ落としました。 民間の脅威報告が「外に面した物と認証の仕組みは72時間以内」を推奨している、という記述を見かけることがあります。当社も当初この表に入れていましたが、**原本に辿り着けなかったので落としました。** 公式のページは前の年の版のままで、二次の記事のうち1本は「報告の本文で確かめられなかった」と自ら書いています。

数字を載せるかどうかは、その数字が正しそうかではなく、原本に辿れたかで決めています。 72時間という数字が間違っているという話ではありません。当社が確かめられなかった、という話です。

回す頻度（当社の案）

どの文書の要求でもありません。人が1人か2人の会社で回る形として置いています。

何を	どのくらい
検知	毎日（公的な一覧と依存関係は機械で）
判定	週に1回15分。それと、急ぐ物が出たとき
振り返り	月に1回
経営への報告	四半期に1回
外部の診断	年に1回から数回。役割は「仕組みが回っているかの確かめ」

外部の診断を減らす提案ではありません。役割を変える提案です。毎日の検知で見るのは「出てきた物を捌けているか」、年に数回の診断で見るのは「捌く仕組みそのものが働いているか」です。

30日・90日・それ以降

やることは、30日が5つ、90日までが5つ、それ以降が4つです。合わせて14です。

最初の30日：一覧と期限を作る

#	やること
1	外に面した物の一覧を作る（製品名・版・持ち主・組み込まれた部品まで）
2	脆弱性の情報をどこから受け取るかを決める
3	期限の物差しを自社で1枚に決める（例＝「悪用あり×外から届く」「悪用あり×内部だけ」「悪用なし」の3段）
4	止めるか続けるかを決める人と、つなぎの策の候補を先に書く
5	自動で更新できる所は、自動更新を有効にする

90日まで：突き合わせを機械にして、記録を残す

#	やること
1	一覧と公的な一覧の突き合わせを機械にして、当たったら通知する
2	開発の流れに、依存関係の検査と静的な検査を入れる。危ない物が出たら止める
3	外からの受け身の検査を、月1回と変更の後に。能動的な検査は検証用の環境だけ
4	この台帳を作り、期限の超過が見える形にする
5	外に出ている資産の発見を、一覧の漏れの点検に使う

それ以降：AI の下書きと振り返り

#	やること
1	AI の修正案と影響の要約は、下書きまで。承認と取り込みは人が行い、試験を通す。新しい依存先は、人が実在と版を確かめる
2	AI の道具そのものも、委託先として確かめる（渡すコードやデータの範囲・保存期間・権限・止められるか）
3	月に1回振り返る。期限を守れた割合は「資産の重要度×深刻度」で見る。例外を見直す
4	AI の道具を起動する場所を決める。外から届いたファイルが混ざる場所で起動しない

4つ目は、2026年10月に海外のセキュリティ会社の報告として報じられた手口に対応するものです。悪意のあるページがダウンロードのフォルダに指示のファイルを置き、そのフォルダで起動した開発支援の AI が、それを「この案件の指示」として読んでしまう、という形です。修正版が出る種類の問題ではなく、起動する場所を分ける運用で防ぎます。

AI に任せる範囲と、任せない範囲

段	機械に任せる	人が決める
資産の把握	外に面した物の発見。製品名と版の一覧の更新	持ち主。業務上の重要度。止めてよい時間帯
検知	公的な一覧との突き合わせ。依存関係の検査	検知の対象に入れる範囲
判定	期限の候補の計算。情報の要約	自社への影響。期限の確定。例外を認めるか
修正	修正案の下書き。影響範囲の説明	本番に当てる承認。止めるか続けるか。受け入れる理由と期限
確認	修正後の再検査。期限の超過の通知	「閉じる」の判定。例外の見直し。経営への報告

英国の NCSC は2026年4月の文書で、AI の道具は問題を見つける方が、対応を確実に実行するより得意な場合がある（can be better at）と書いています。あわせて、**防御する側は AI の道具の出力をどう捌くかを考える必要がある**とも書いています。この台帳は、その「どう捌くか」を置く場所です。

AI が自動で直すようになる、とは書きません。この分野の一次の文書は、どれも人の確認を前提にしています。

記入の例

この値を推すものではありません。書き方の例です。固有名（サーバ名・委託先名・鍵の置き場所）は書かず、記号で書きます。

#	列	例
1	識別子	CVE-20XX-XXXXX
2	見つけた日	11月4日
3	どこで見つけたか	脅威情報の取り込み（公的な一覧の更新）
4	外から届くか	インターネットから直接届く
5	悪用されているか	公的な一覧に載っている
6	攻撃を自動化できるか	できる
7	乗っ取りの程度	全部取られる
8	段	すぐ動く
9	期限	11月7日（数え始め＝11月4日。公的な一覧に載った日）
10	対応の種類	つなぐ（修正版が出ていないため、対象Aへの経路を閉じる）
11	決めた人	情報システムの責任者
12	決めた日	11月4日
13	閉じた日・見直す日	未。11月11日に見直す（修正版が出たら直してから閉じる）

受け入れる場合の例も1つ置きます。

#	列	例
1	識別子	CVE-20XX-YYYYY
4	外から届くか	届かない（検証用の環境だけ）
5	悪用されているか	報告が無い
8	段	記録して見直す
10	対応の種類	受け入れる
11	決めた人	情報システムの責任者
13	閉じた日・見直す日	2月4日に見直す。理由＝検証用の環境だけで使っており、本番に出す計画が無い。本番に出すことが決まった時点で、見直しを前に倒す

受け入れた件に**見直す日を書かないと、受け入れが永久になります。** 受け入れは判断で、放置は判断ではありません。この2つが台帳の上で同じ見た目になると、見分けられなくなります。

この台帳の限界

この台帳は、判定する人の時間を増やしません。

検知を毎日に増やすなら、判定に使える時間も増やす必要があります。台帳は、増えた件数を捌く道具ではなく、**捌いた結果を残す場所**です。残す場所が無いと、同じ判断を何度もやり直すことになります。

決める人が1人しかいない組織では、この台帳は「その1人が決めた記録」にしかなりません。それでも、半年後に理由を思い出せる価値はあります。

この資料について

合同会社SecuROI が無料で配っています。登録は要りません。出典（合同会社SecuROI・www.securoi.com）を残し、趣旨を変えなければ、複製・転送・書き換えは自由です。

当社は検知の道具を売っていません。この台帳は、検知の後ろに置く物です。
