重大な脆弱性が公表された日の判断表

止めるか、続けるか、誰が決めるかを、その日が来る前に決めておく1枚

この表の頭に置く数字

止める人が決まっている割合　　／　　（一次責任者と代理の両方が書いてあるサービス数 ÷ サービス数）

前書き

広く使われるソフトの部品に重大な脆弱性が公表されたとき、現場が困るのは直し方より、止めるか続けるかを誰がどの基準で決めるかです。

この1枚は、その判断を平時に書き出しておくためのものです。埋まらない欄があっても構いません。決まっていないと分かることが、最初の成果です。

値の3つ（表の「値」の欄は、この3つから1つを丸で囲みます）

値	意味	次にやること
○	決まっている。人も基準も言葉になっていて、記録がある	そのまま。年1回見直す
△	決まっていない。または決まっているが記録が無い	欄7に「誰が・いつ決めるか」を書く
→	いまは決められない。決める人と日付だけ決めた（欄7に書いてある）	その日付が来たら ○ か △ に変える

合否も点数もありません。△ が多いことは失敗ではなく、次に決めることが見えた状態です。

記入の約束

値を1つ丸で囲み、右の欄に1行か2行で書きます。固有名（サーバ名・委託先名・鍵の置き場所）は書かず、「対象A」「委託先B」のような記号で書きます。

第1報とは（欄3で出てきます）

第1報は、止めるか続けるかを決めた直後に、外へ最初に出す知らせです。顧客・取引先・社内に向けて出します。

原因と影響の全体が分かる前に出すものなので、分かっていないことを「まだ分かっていない」と書くのが要点です。全部分かってから出すと遅くなります。

第1報に書く4つ	中身
調査の責任者	誰が調べているか（役職で書く）
これから検証する事項	まだ分かっていないことを、分かっていないと書く
進捗の公表の方法	どこで続きを知らせるか
次回報告の日時	いつ次を出すか

この表で決めておくのは、第1報の文そのものではありません。**平時に決めるのは「この4つを書く」と「何時間以内に出す」の2つだけ**です。文は、起きた日に書きます。

表

欄	問い	値（○△→）	書く中身
1 どこで動いているかが、すぐ分かるか	その部品が自社のどのシステムで動いているか、組み込まれた部品も含めて、半日以内に一覧にできるか	○ △ →	一覧の有無、持っている人（役職）、委託先の分も分かるか

欄	問い	値（○△→）	書く中身
2 止めるか続けるかを、誰がどの基準で決めるか	止める判断を下す人は誰か。止める条件と続ける条件は言葉になっているか	○ △ →	決める人（役職）、止める条件、続ける条件
2-b 続けると決めたときの記録	期限付きで続けると決めた場合、誰が決め、いつまでで、代わりに何を置いたか。次に見直す日はいつか	○ △ →	決めた人（役職）、期限、代わりに置くもの、次に見直す日
3 止めるなら、何が止まり、誰に何を知らせるか	止めたときに止まる業務、顧客への影響、契約上の通知先は分かっているか。第1報に何を書くかは決まっているか	○ △ →	止まる業務、影響を受ける相手の種類、知らせる人と手段。第1報の4つ＝調査の責任者、これから検証する事項、進捗の公表の方法、次回報告の日時
4 止めずに直す手順があるか	本番に当てる前に試す場所、失敗したときの戻し方、修正までのつなぎは決まっているか。直した後、消えたことを誰が確かめるか	○ △ →	試す場所の有無、戻し方の有無、つなぎの手段と入れる人、直した後の再確認の有無と日付（同じ観点での再診断か）
5 委託先の連絡先と、修正の期限	委託している部分について、連絡先といつまでに直すかが契約か合意で決まっているか	○ △ →	連絡先の役割（記号で）、期限の定め方、守られないときの手
6 直すまでの間、誰が見ているか	修正を当てるまで、不審な動きを誰がどの頻度で見るか。見つけたら誰に伝えるか	○ △ →	見る人（役職）、見る頻度、伝える先。見られないなら「見られない」と書く
7 決めていないことを、誰が、いつ決めるか	上の欄で三角が付いたものについて、決める人と日付を書く	→	欄番号、決める人（役職）、日付。1つでよい

2-b が埋まっていない「続ける」は、続ける判断ではなく放置です。

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）

欄	値	書く中身の例
1 どこで動いているか	△	外から見える資産の一覧はある（最終更新 4か月前）。組み込まれた部品までは追えていない
2 止めるか続けるか	○	決める人＝情報システム部長、不在時は経営企画室長。止める条件＝外から到達でき、認証を越えられるとき。続ける条件＝通信を遮断でき、監視を付けられるとき
2-b 続けると決めたとき	○	決めた人＝情報システム部長。期限＝30日。代わりに置くもの＝該当機能の遮断と、1日1回のログ確認。次に見直す日＝12月5日
3 止めるなら	△	止まる業務＝受注の受付。知らせる相手＝顧客、取引先、社内。第1報は2時間以内に、調査の責任者（情報システム部長）・これから検証すること・次回報告の日時（24時間以内）を書く
4 止めずに直す	△	試す場所＝検証環境あり。戻し方＝手順書あり。つなぎ＝通信の遮断。直した後の再確認＝指摘した側に同じ観点で見てもらう（未実施）
5 委託先	△	連絡先＝委託先A の窓口。期限＝契約に記載なし。次の更新で「重大なものは14日以内」を入れる
6 誰が見ているか	○	見る人＝情報システム担当（2名）。頻度＝1日1回。伝える先＝情報システム部長
7 決めていないこと	→	欄5。決める人＝法務担当。日付＝11月28日

期限の数字（2時間・24時間・14日・30日）は、書き方を示すための例です。自社の値は自社で決めてください。決めない、測らない、記録しない、の3つだけを避けてください。

脚注

この1枚は、米国の当局が公開している対処の手順（どこで動いているかを洗い出す、修正を当てる、当てられないものは止める、つなぎ、監視）の5つの段をすべて欄に持っています。欄の順は、経営が決める順に並べています。

合否や点数はありません。埋まらない欄があることが、次に決めるべきことを示します。

国の注意喚起の対応点検表（無料）の「修正の手順」の問いと同じ考え方で作っています。点検表で「不明」「いいえ」だった項目を、この1枚で誰が決めるかに落とせます。

使い方

情報システムの担当者と、止める判断をする人が同席して、上から順に埋めます。所要は約30分。1人で埋めず、2人以上で。

三角と矢印が3つ以上残ったら、それがその日までに決めておくことです。欄7に、1つだけ日付を入れます。

年に1回、または大きな注意喚起が出た日に見直します。前の版は捨てずに、日付を付けて残します。

合同会社SecuROI　2026-11-05 版。この紙に合否や点数はありません。固有名（サーバ名・委託先名・鍵の置き場所）は書かずに、記号で記入してください。