CRA報告対応における実務課題

CVSSスコアのみに頼らない高度な要否判断と、
極めて厳格なタイムラインへの追従が企業に
求められています。

CRA報告対応における「2つの壁」

要否判定の曖昧さと過剰不可

- CRA上の報告対象は「高CVSS値の脆弱性」全般ではありません。「積極的に悪用されているか」や「製品・利用者への実質的影響」を踏まえたリスク評価が要求されます。判断基準が曖昧な場合、報告漏れによる罰則リスクや過剰報告によるコスト肥大化が発生します。

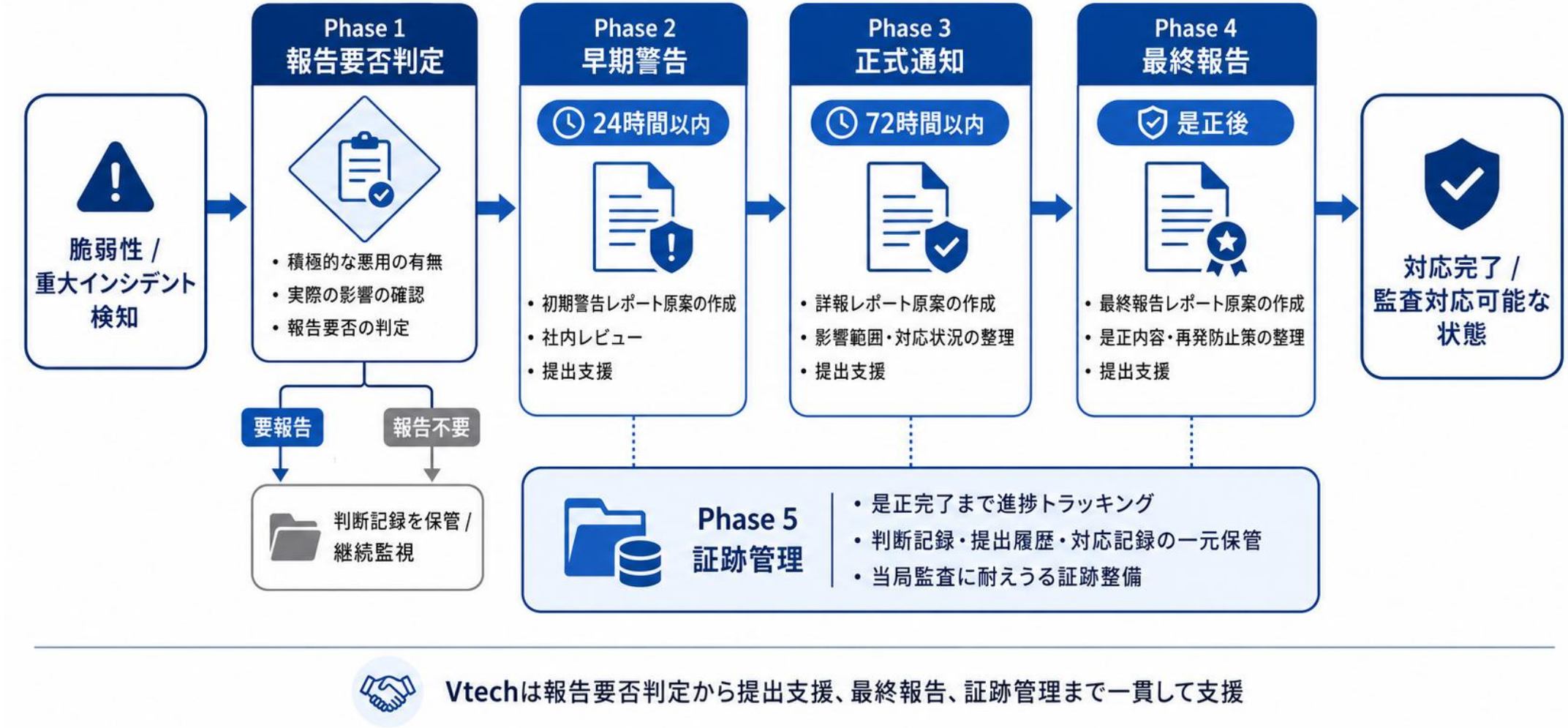
24時間以内の厳格なタイムライン

- 認知から24時間以内の「早期警告」を筆頭に、72時間以内の詳細報告、是正完了までの進捗管理と多段階の報告手順が存在します。既存の社内プロセスのみで速やかにCSIRT/ENISA指定の報告書を作成するのは困難です。

Vtechの解決アプローチ

発見から是正・最終報告までを一貫してカバーする「CRA脆弱性・インシデント報告対応支援サービス」を提供します。

CRA脆弱性・インシデント報告対応支援フロー



Vtechは報告要否判定から提出支援、最終報告、証跡管理まで一貫して支援

支援Phase

【Phase 1】報告要否判定
積極的な悪用の有無や、実際の影響を踏まえて報告の要否判定を実施

【Phase 2】早期警告支援
認識から24時間以内に提出が求められる初期警告レポート原案の
作成・提出支援

【Phase 3】正式通知支援
認識から72時間以内に提出が求められる詳報のレポート原案の
作成・提出支援

【Phase 4】最終報告支援
是正後の最終報告のレポート原案の作成・提出支援

【Phase 5】証跡管理
是正完了までの進捗トラッキングおよび当局監査にたえうる全対応の
一元保管

【Phase 1】報告要否判定

- 検出された脆弱性またはセキュリティインシデントについて、以下の観点からCRAに基づく報告要否を判定します。

- 積極的な悪用を示す信頼できる証拠の有無
- 製品および利用者への実際の影響
- 影響範囲
- 重大なセキュリティインシデントへの該当性

- 判定結果、判断根拠および関係者間の合意内容を記録し、報告または非報告の判断証跡を整備します。

【Phase 2, 3, 4】多段階報告の支援

- 多段階の報告書の原案を作成し、貴社の正式報告を支援

  - 早期警告： 24時間以内
    報告対象と判断された脆弱性または重大なセキュリティインシデントについて、認識後24時間以内に提出する早期警告を支援します。

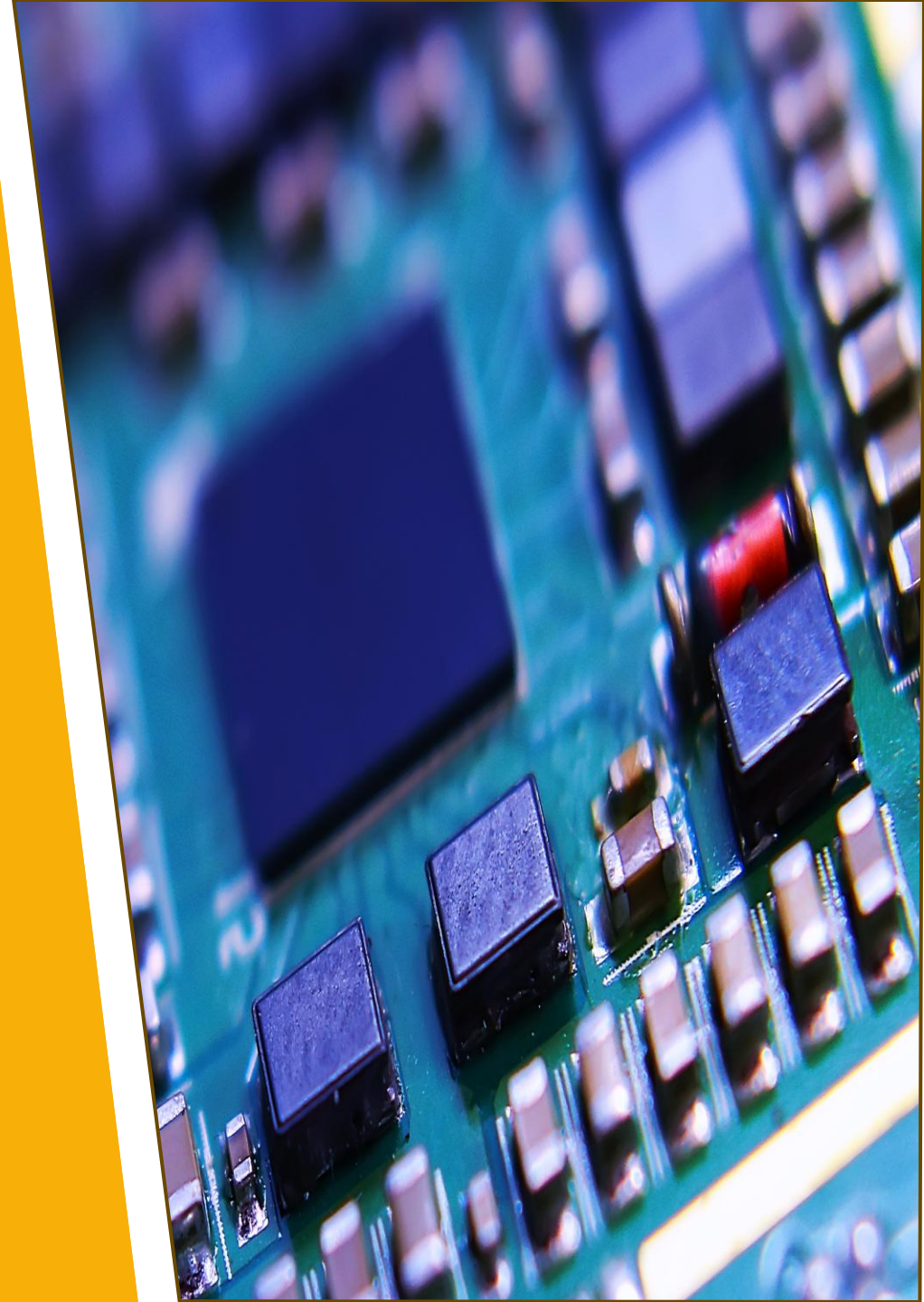
  - 正式通知：72時間以内
    脆弱性またはインシデントを認識してから72時間以内に提出する正式通知について、詳細情報の整理およびレポート原案の作成を支援します。

  - 最終報告：14日以内(脆弱性)/1ヶ月以内(インシデント)
    原因調査および是正対応の結果を整理し、CRAで求められる最終報告書の原案作成および提出を支援します。

【Phase 5】証跡管理

- 脆弱性またはインシデントの認識から是正完了まで、すべての対応状況を一元的に管理します。
  - 対応タスク、担当者および進捗状況の管理
  - 報告要否の判断記録
  - 脆弱性評価および影響分析結果の保管
  - 当局への提出資料および提出履歴の管理
  - 社内会議、承認および意思決定記録の保管
  - 修正版ファームウェアおよびソフトウェアの履歴管理
  - 利用者および顧客への通知記録の管理
  - 是正完了確認およびクローズ判定
  - 当局確認や監査に対応可能な証跡パッケージの整備
- これにより、対応漏れや報告期限の超過を防止するとともに、当局から説明を求められた際に、判断および対応の妥当性を迅速に提示できる状態を整備します。

費用のご案内



1．事前準備・初回導入

項目	主な作業	概算工数
対象製品・体制確認	製品、F/W、販売地域、関係部門、連絡体制の整理	5人日
報告要否判定基準の整備	判定基準、エスカレーション条件、承認者の明確化	6人日
24時間・72時間報告フロー	検知から承認・提出までの業務フロー作成	6人日
報告書テンプレート作成	早期警告、正式通知、最終報告のひな型作成	8人日
証跡管理台帳の整備	案件台帳、期限管理、判断記録、提出履歴の様式作成	5人日
説明・模擬演習	関係者説明、机上演習、改善事項の反映	5人日
合計		35人日

既存のPSIRT、脆弱性管理台帳、インシデント対応フローが整備されている場合は工数を縮小できる可能性があります。

2．インシデント1件当たりの対応工数

Phase	主な作業	概算工数
Phase 1 報告要否判定	情報収集、悪用状況確認、影響評価、判定会議、判断記録	4人日
Phase 2 早期警告	初期情報整理、24時間報告原案、レビュー、提出支援	4人日
Phase 3 正式通知	技術情報・影響範囲整理、72時間報告原案、関係部門調整	8人日
Phase 4 最終報告	原因、是正措置、影響範囲、再発防止策、最終報告原案	10人日
Phase 5 証跡管理	期限管理、進捗管理、会議・判断・提出証跡の整理	6人日
PM・全体調整	会議運営、課題管理、顧客窓口、成果物レビュー	5人日
合計		37人日／件

CRA上、最終報告は、積極的に悪用されている脆弱性では是正・緩和措置が利用可能になってから原則14日以内、重大なセキュリティインシデントでは72時間通知後1か月以内に求められます。

案件難易度別の目安

案件区分	想定ケース	工数
軽微・限定的	対象製品と原因が明確、影響範囲が限定的	18人日
標準	複数部門との調整、影響製品・顧客の確認が必要	30人日
複雑・重大	複数製品、海外顧客、原因調査長期化、重大インシデント	60人日

3．平時の継続支援

支援レベル	内容	月額工数
ライト	定例会、台帳レビュー、相談対応	2人日／月
スタンダード	脆弱性情報確認、判定支援、台帳更新、月次報告	5人日／月
フルサポート	継続監視、トリアージ、報告準備、関係部門調整	10人日／月

推奨する見積のご案内

見積区分	推奨工数
初期導入・報告体制整備	35人日
平時運用支援	5人日／月
インシデント発生時対応	30人日／件
重大・複雑案件	別途見積

Thank you!