Code Red — サイバーインシデント対応

サイバー攻撃を受けた組織の、封じ込め・フォレンジック立ち上げ・復旧計画策定。対象は病院・学校・企業。緊急時は lv3.biz/help-hacked-system/ からご連絡ください。

対応は4段階 — 救急救命の現場と同じ進め方で

STEP 1
被害の拡大を止める
封じ込めの初動指示。外部連絡の停止判断。

STEP 2
何が起きたかを突き止める
フォレンジックの立ち上げ。事実関係・影響範囲・根本原因。

STEP 3
業務を立て直す
復旧計画の策定と、優先順位づけ。

STEP 4
弱点をふさぐ
再発防止策を新アーキテクチャに落とし込む。

契約開始後のタイムライン（標準）

最初の72時間	状況の聞き取り、封じ込めの初動指示、外部連絡停止の判断
その後の1週間	フォレンジック立ち上げ、経営層ブリーフ作成、規制当局への通報判断
1ヶ月以内	復旧計画ドラフト納品、優先順位リスト、外部開示の草案
1年目以降	復旧支援の継続、または SOC ベンダーへのハンドオフ

エンゲージメント概要（契約形態: リカバリ）

体制	シニアITデザイナーを中心に、Research（フォレンジック）・Data・Support チームが関与
期間	通常1年程度
納品物	課題・進捗の共通報告書 + 被害調査報告書（事実関係・影響範囲・根本原因）・復旧報告書（復旧後の構成図・再発防止策・引き継ぎ事項）
含まれないもの	攻撃元の追跡（法執行機関の領分） / 長期の SOC 運用
対応形態	リモート基本。大規模対応が必要な場合はオンサイトも可

復旧手順の考え方は書籍『WAH — 会社の非常事態時に読む本』（2027年初旬刊行予定）にまとめています。

お取引の流れ（全サービス共通）

契約形態・進め方・契約条件の標準形です。個別の契約で定めた内容が優先されます。最新版は lv3.biz/ja/how-we-work/ を参照してください。

3つの契約形態（すべて準委任契約）

	プロジェクト	アドバイザリー	リカバリ（CODE RED）
範囲	単発のIT設計（ロードマップ・新規システム設計・移行計画）	進行中のDX / ITプログラムへの月次関与（設計レイヤー）	インシデント後の封じ込め・フォレンジック立ち上げ・復旧計画
期間	通常数年程度〜	通常数ヶ月〜数年	通常1年程度
固有の納品物	ロードマップ文書・データモデル	月次設計レビュー記録・ベンダー会議同席議事	被害調査報告書・復旧報告書（新アーキテクチャ）
含まれないもの	運用代行 / 24×7監視	開発リソース提供（人月貸し）	攻撃元追跡 / 長期SOC運用

どの契約形態でも、課題報告書・進捗報告書を継続的に提出します（標準セット・案件に応じて変更可能）。

問い合わせからキックオフまで（最短 約2週間）

WEEK 0
お問い合わせ
フォーム送信 → スコープ概要のヒアリング。必要に応じて30〜60分のオンライン打ち合わせ。

WEEK 1
NDA + スコープ書
NDA締結。スコープ書のドラフトはLV3が起案。

WEEK 2
キックオフ
MSA + SOW締結。チームをアサインし、始動。

WEEK 3〜N
実行
週次レビュー + 月次の経営層向けブリーフ。

CLOSEOUT
引き継ぎ
最終ドキュメント納品。追加支援は別契約で。

サイバーインシデント（Code Red）はこのフローを待たず、緊急経路（lv3.biz/help-hacked-system/）で即応します。

契約の標準条件（個別契約が優先）

契約形態	準委任契約（業務遂行に対する報酬。請負＝成果物完成責任の形式ではありません）
契約書式	標準 MSA + SOW。クライアント法務のレビューに対応。発注書ベースも可
秘密保持（NDA）	標準の2者間NDA。初回相談の前に締結可。クライアント側テンプレートも受付
価格・請求	個別見積（Pricing on request）。初月1ヶ月、以降3ヶ月ごとの更新。海外通貨建て可
データ取扱	案件終了後の保管・破棄ルールを契約書に明記
対応形態	リモート支援が基本。リカバリで大規模対応が必要な場合はオンサイトも可