セキュリティ対応の型スキル 活用ガイド

本ダウンロードコンテンツについて

本ドキュメントは、ANDGATE METHODS『セキュリティ対応の型――制約だらけの現場で前に進める判断と段取り』（https://andgate.co.jp/methods/security-response-method/）で紹介している、セキュリティ対応の進め方を支援する、Claude専用のスキルの活用ガイドです。1つのスキルと、連動するExcelで構成されています。

■ 最短で試す3ステップ（Claude Cowork の場合）

1. 配布ZIPを展開し、`security-response-pattern` フォルダを、Claude Cowork の「Customize」→「Skills」→「Upload a skill」からアップロードする。
2. チャットで「セキュリティ対応」と送る。聞かれたら、今の状況をA〜Dの記号で答える。
3. 指摘を大量に抱えているときは、Bを選んで仕分けのモードに進み、出てきた入力案を、展開したフォルダの `templates/` 内のExcelに貼り付ける。

Claude Desktop・Claude Code の場合は「使い方1」「使い方3」をご覧ください。

■ 動作確認済み環境

本コンテンツは、以下の環境において正常な動作を確認しております。

- **OS**：macOS / Windows
- 推奨ツールおよびモデル：
  - **Claude Desktop**（一般利用者向け）：Opus 推奨（Sonnet でも簡易的な利用は可能）
  - **Claude Code**（開発者・CLI利用者向け）：Opus 推奨
  - **Claude Cowork**（チーム並行作業向け）
- 配布形式：ZIP形式

■ ご利用の際の注意点

- **PC環境を推奨**：ZIPファイルの展開やプロンプトのコピー＆ペースト操作が必要なため、WindowsまたはMacのPC環境での操作を強く推奨します。スマートフォン、タブレット、Chromebook等での動作確認は行っておりません。
- **他環境での動作**：上記以外のOSや、旧バージョンのAIモデル、他社生成AI（ChatGPT等）では、設計通りの動作にならない、あるいは十分なパフォーマンスを発揮できない場合があります。
- **仕様変更**：AIモデルのアップデート等により、予告なく動作や出力結果が変化する場合があります。あらかじめご了承ください。

セキュリティ対応の型スキル

ANDGATE METHODS『セキュリティ対応の型』に基づき、**暫定対応（致命傷の回避）→ 恒久計画 → 恒久対応**の3フェーズを、現場が動ける形で進めるための、Claude専用のスキルです。「セキュリティ対応」の一言で、今の状況をヒアリングし、必要なモードへ進みます。技術構成やツールの選定は扱いません。判断と段取りに絞っています。

モード	作るもの	効果
仕分け	指摘の仕分け／Excelへの入力案。	監査・コンサル・診断ツールの指摘を、「いま触る」「触らない（恒久計画送り）」「他部門・ベンダーへ依頼」に分けます。迷ったら触らない。連動Excelに貼る入力案も出します。
Phase 1 暫定対応	初動レポート／恒久計画への申し送り一覧	数分〜数時間で止められるものだけを、通告 → 手順書 → 1件ずつ実行 → 観測の順で進めます。通告は承認ではなく、異議を言える猶予を渡す手続きです。
Phase 2 恒久計画	突き合わせ一覧／優先順位一覧／全体ロードマップ／マスタスケジュール	指摘・要求と暫定対応の実績を突き合わせ、影響度×発生確率で優先順位をつけ、8つの制約への回答を入れた計画にします。
Phase 3 恒久対応	手順書／経営報告	対象・前提条件・操作手順・切り戻し・確認方法の5項目で手順書を作り、やったこと・残っていること・残りの費用を報告します。

連携のポイント：基準（CIS・NISTなど）の版や項目番号は、変わります。スキルは、公式情報での確認をユーザーに任せ、確認できていない項目は「未確認」と書きます。担当者・期限・費用は、推測で埋めません。暫定対応で「触らない」とした項目を、Claudeの判断で「対応する」に格上げすることもありません。

こんなときに使えます

- コンサルや監査から指摘が100項目も来て、どこから手をつけてよいか分からない。
- 指摘は正しいが、時間・予算・人・権限の制約で、すべてには手が回らない。
- 止めてよいのか、止めたら何が壊れるのか分からない設定や権限が残っている。
- 暫定対応をやったあと、恒久計画をどう作ればよいか迷っている。
- 経営や監査元に、「何をやったか・何が残っているか・残りにいくらかかるか」を報告したい。

想定しないユースケース

- 本番環境への直接の操作・設定の変更 → スキルは、文書の作成と確認のみです。設定の変更や現物の確認は、担当者が行います。
- インシデントの最中の、リアルタイムの対応手順の作成 → このスキルは、計画を作る型です。
- 技術構成・ツールの選定 → 扱いません
- 出力を、そのまま関係者に提出・送信すること → 必ず人がレビューしてください。通告文や報告文は、下書きです。
- Excelへの自動書き込み → 入力案を出力するだけです。貼り付けとプルダウンの選択は手作業で行います

入力時の注意

セキュリティの話は、それ自体が機密になります。以下の情報は入力しないでください。

- 認証情報（パスワード・APIキー・アクセスキー・トークン・秘密鍵・接続文字列）
- アカウントID・ユーザー名・IPアドレス・内部ホスト名・内部URL・リソースの完全なARN
- 顧客名・個人の氏名・メールアドレス・電話番号
- 診断レポート・監査報告書の全文や、脆弱性の再現手順（貼るのは、指摘を1行にした要約まで）。

`[サーバA]`、`[ユーザーX]` のように、伏せ字にして渡してください。現物は、担当者が自分で確認し、結果を伏せ字にして貼ります。含まれていそうなときは、スキルが処理を止めて、「これ、マスクしていますか？」と確認を返します。見つけた種類と場所だけを伝え、値は書き写しません。伏せ字に置き換えて貼り直すか、マスク済み・ダミーの値であることを伝えれば、そのまま続きます。

この確認でできないこと：確認が動くのは、文字を送信したあとです。送る前に止めることはできません。また、見た目でわかるものしか見つけられず、見逃すこともあります。「確認が出なかった＝安全」ではありません。貼り付ける前に、ご自身で伏せ字にしておくのがいちばん確実です。送ってしまったときは、会社の決まりに沿って、履歴の扱いを担当窓口に確かめてください。キーを送ってしまったときは、そのキーの失効も、担当者が行ってください。

ファイル構成

```
methods_MI-015_security.zip
  README.pdf                                  # 本ファイル
  templates/
    セキュリティ指摘の仕分け判定ツール.xlsx     # 連動Excel（5つのシート）
  docs/
    セキュリティ指摘の仕分け判定ツール.pdf      # 印刷用のPDF
  security-response-pattern/                  # セキュリティ対応の型スキル
    SKILL.md                                  # スキル本体
    templates/                                # 成果物のひな形（8ファイル）
      initial-report.md                       # 初動レポート
      carryover-list.md                       # 申し送り一覧
      alignment-table.md                      # 突き合わせ一覧
      priority-list.md                        # 優先順位一覧
      roadmap.md                              # 全体ロードマップ
      master-schedule.md                      # マスタスケジュール
      procedure.md                            # 手順書
      executive-report.md                     # 経営報告
    references/                               # 判断基準（6ファイル）
      triage-criteria.md                      # 触る／触らないの判定
      notification-protocol.md                # 通告の作法
      priority-matrix.md                      # 優先度マトリクス
      benchmark-mapping.md                    # ベンチマークとの照合
      handoff-criteria.md                     # フェーズ間の移行条件
      scenario-catalog.md                     # 積み残しシナリオ集
```

連動Excel「セキュリティ指摘の仕分け判定ツール」

指摘を1行ずつ入れてプルダウンを選ぶと、「いま触ってよいか、触らないほうがよいか」が自動で出るExcelです。判断の基準を先に固定して、機械的に流すためのものです（100件まで）。Claudeを使わずに、直接書き込んでも使えます。印刷用のPDF（`docs/セキュリティ指摘の仕分け判定ツール.pdf`）も同梱しています。

シート	内容
1_使い方	進め方、判定の考え方、貼り付け範囲。
2_判定シート	C列に指摘を貼り、G〜J列（切り戻せるか／影響範囲が言えるか／所管／作業量）をプルダウンで選びます。判定と理由が自動で出ます。「不明」を選んでも構いません（調査要になります）。
3_着手順	判定を、着手すべき順に自動で並べます。入力はできません。
4_サマリー	区分ごとの件数と、指摘元・上長に返せる報告文が自動で出ます。
5_判定ルール	判定のルールと、その理由。自社の事情に合わなければ、ここを見ながら数式を直せます。

ポイント：黄色いセルが記入欄、青いセルは自動計算です。数式を消してしまわないよう、シートは保護しています（パスワードなし）。変更したいときは、「校閲」→「シート保護の解除」を選んでください。2_判定シートの1〜5行目は記入例です。消してから使ってください。

判定のルール

上から順に当てはめ、先に当てはまったものが採用されます。暫定対応になるのは、**切り戻せて、影響範囲が言えて、自部門で、数時間以内に終わる**ものだけです。

条件	判定	理由
所管が他部門・ベンダー	他部門・ベンダーへ依頼	自分で変更できません。依頼先と回答期限を決めます。
切り戻せない・影響範囲が言えない・作業量が不明（「不明」を含む）	恒久計画送り（調査要）	迷ったら触らない。先に調べます。
作業量が「数時間以内」	暫定対応	通告して、1件ずつ実行します。影響度・発生確率は使いません。
上記以外。スコア6以上／3〜5／1〜2	恒久計画送り（計画化）／（そのまま）／（優先度低）	影響度×発生確率のスコアで、恒久計画の中の優先度を決めます。

注意：「触らない」は「対応不要」ではありません。恒久計画の調査項目として管理します。判定と違う扱いにするときは、備考欄に理由を残してください。

貼り付け範囲

入力案は、タブ区切りのテキストで出力されます。貼り付ける範囲の左上のセルを1つだけ選んで貼り付けてください。値のみ貼り付けを使うと、黄色のセルの書式が崩れません。

シート	形	入力のしかた
2_判定シート	N行 × 2列（見出し行なし）。指摘内容・出どころ。1回に20件まで	C7 を選択して貼り付け。21件目からは C27、C47 のように、20行ずつずらします。

注意：切り戻せるか・影響範囲・所管・作業量は、Claudeは推測しません。現場の方が、G〜J列で選んでください。Claudeは、1件ずつ確かめることを一覧にして返します。列の区切りにはタブ文字を使っています。コピーの過程でタブがスペースに変わり、全部が1つのセルに入ってしまうときは、「セルごとの入力案で出して」と依頼してください。

使い方1：Claude Desktop で使う（推奨）

Claude Desktop の「プロジェクト」機能を使ってスキルを登録します。

Step 1: プロジェクトを作成する

1. Claude Desktop を開く
2. 左サイドバーの検索欄の下にある プロジェクト をクリック
3. 「新しいプロジェクトを作成」 をクリック
4. プロジェクト名を入力（例: セキュリティ対応）

Step 2: プロジェクトナレッジにファイルを追加する

プロジェクト画面の右側にある 「プロジェクトナレッジにコンテンツを追加する」 から、`security-response-pattern/` 配下の次のファイルをアップロードします。

- `SKILL.md`（必須）
- `templates/` 配下（8ファイル）
- `references/` 配下（6ファイル）

> **ポイント：**Excel と PDF は、プロジェクトナレッジには登録しません。手元のPCで開いて使います。templates/ 配下のファイルは、Claudeが作った成果物の「清書・共有用」です。「テンプレートの項目に合わせて出力して」と指示すると、そのまま資料にできます。

Step 3：カスタム指示を設定する（任意）

```
あなたはプロジェクトナレッジに登録された「セキュリティ対応の型スキル」を活用して回答してください。
セキュリティ対応や指摘の仕分けに関する相談があった場合は、SKILL.md に記載されたワークフローに従って支援を行ってください。
```

Step 4：使ってみる

プロジェクト内のチャットで、自然な言葉で依頼するだけです。

```
# 起動する（今の状況を聞いて、必要なモードへ進む）
セキュリティ対応

# 指摘を仕分ける（マスクした指摘を貼り付ける）
監査の指摘を、いま触るものと触らないものに仕分けたい

# 暫定対応のあとに、恒久計画を作る
暫定対応は済んだ。恒久計画を作りたい

# 通告文を作る
この対応の通告文を作って
```

使い方2：Claude Cowork で使う

非エンジニアの方には、デスクトップアプリ「Claude Cowork」からのご利用を推奨します。
スキルのインストールはGUI操作のみで完結します。

Step 1: ZIPを展開する

配布ZIPを展開します。展開後に `security-response-pattern/` のスキルフォルダと、Excelを入れた `templates/`、PDFを入れた `docs/` が作成されます。

Step 2: スキルをインストールする

1. Claude Cowork を開く
2. 右上の「Customize」をクリック
3. 「Skills」タブを選択
4. 「＋」ボタンをクリックし、「Upload a skill」を選択。
5. `security-response-pattern` フォルダを選択してアップロード

使い方3：Claude Code（CLI版）で使う

ZIPを展開し、スキルフォルダをコピーします。

```
cp -r security-response-pattern ~/.claude/skills/security-response-pattern
```

スラッシュコマンドで起動します。

```
/security-response-pattern
```

状況ごとの使いどころ

状況	スキルのモード	主な成果物／使うExcelのシート
指摘が大量に来た	仕分け	Excelの 2_判定シート に貼り、プルダウンを選ぶと、3_着手順 に着手順が出ます。4_サマリー の報告文で、指摘元に一次回答を返せます。
インシデント・経営号令・退職などが起点	Phase 1 暫定対応	初動レポート／恒久計画への申し送り一覧。通告文の下書きも作れます
暫定対応が済んだ	Phase 2 恒久計画	突き合わせ一覧／優先順位一覧／全体ロードマップ／マスタスケジュール
ロードマップが決まった	Phase 3 恒久対応	手順書／経営報告

出力形式

- まずチャットに出力します。ファイルを作れる環境（Claude Code・Cowork）では、md形式で `output/` に保存することもできます。
- 日付は `YYYY/MM/DD` の形です
- Excelのファイルは、Claudeは作りません。「Excelに出力して」と頼むと、貼り付け用の入力案が出ます。表を自分の表計算に貼りたいときは、見出し行つきのタブ区切りで出せます。

免責事項

【重要】本スキルの動作環境および免責事項

本資料は、Anthropic社が提供するAIモデル「Claude」専用のスキルセットです。他社AI環境での動作は意図しておりません。

本資料は、スキルの動作を補助するものであり、生成される回答の正確性、完全性、または特定の目的への適合性を保証するものではありません。

免責事項

当社は、本コンテンツおよびそれを利用した成果物について、その完全性、正確性、有用性を保証しません。利用者は自己の責任において本コンテンツを利用するものとし、利用の結果、利用者または第三者に生じた不利益、不具合、損害（法的責任、データの損失、業務中断を含む）について、当社は理由の如何を問わず、また予見可能性の有無に関わらず一切の責任を負わないものとします。

Provided by ANDGATE, Inc.