ANDGATE METHODS

セキュリティ対応スキル 活用ガイド

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」の思想を、暫定対応→恒久計画→恒久対応の3フェーズで完全再現するためのClaude専用スキルセットの活用ガイドです。

■ 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 4.6 / Sonnet 4.6
  - Claude Code (開発者・CLI利用者向け): Opus 4.6
  - 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。

セキュリティ対応スキル

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」に基づき、暫定対応→恒久計画→恒久対応の3フェーズで、セキュリティ対応の「判断と段取り」を再現可能にするAIスキルです。

「正しい指摘（コンサル・経営・ベストプラクティス）」と現場の間を埋めることが目的です。技術構成やツール選定は扱わず、制約だらけの現場でも前に進められる計画の立て方に集中します。

成果物	効果
暫定対応の記録	初動レポート・申し送り一覧 「やったこと」と「触らなかった理由」を時系列で記録。次フェーズへの引き継ぎ資料になります
恒久計画の成果物	突き合わせ一覧・優先順位一覧・マスタスケジュール コンサル指摘と対応実績を照合し、「もうやった」を可視化。経営・監査への報告根拠になります
恒久対応の成果物	手順書・経営報告 対応の全記録と残存リスクを経営が判断できる粒度で可視化します

こんなときに使えます

- セキュリティ対応を任されたが、どこから手をつけるかわからない
- コンサル指摘・経営要求は揃っているが、現場への落とし込みができない
- 監査指摘やSCS評価制度対応で、「全部やる」を回避した計画を作りたい
- 時間・予算・人員・権限の制約がある中で、動ける計画が必要

想定しないユースケース

- 技術構成・ツール選定の推奨が欲しい場合 → 別途ベストプラクティス文書を参照してください
- インシデント発生中のリアルタイム対応手順書化 → CSIRT用の別フレームワークが必要です
- 脆弱性個別の調査・通知 → vuln-check スキルを利用してください
- リスク登録簿の作成 → risk-register スキルを利用してください
- EoL対応の計画策定 → eol-planning スキルを利用してください

ファイル構成

```
None
security-response-pattern/
  SKILL.md                      # スキル本体
  README.pdf                    # 本ファイル
  templates/                    # 各フェーズの出力テンプレート
    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         # 経営報告書
  references/                   # 判断基準の参考資料
    triage-criteria.md          # 「対応する／触らない」仕分け判定フロー
    scenario-catalog.md         # 積み残しシナリオDB
    priority-matrix.md          # 優先順位マトリクス基準
    notification-protocol.md    # 影響確認・通告の作法
    benchmark-mapping.md        # CIS/NIST等ベンチマーク照合手順
    handoff-criteria.md         # フェーズ間ハンドオフ判断基準
```

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: セキュリティ対応スキル）

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、以下のファイルをアップロードします 。

#	ファイル	説明
1	`SKILL.md`	スキル本体。 Claudeへの指示が記述されています
2〜9	`templates/ 配下（8ファイル）`	各フェーズの出力テンプレート。 Claudeが生成した内容の清書用として使用します
10〜15	`references/ 配下（6ファイル）`	判断基準・シナリオDB等の参考資料。 スキルが内部で参照します

> ポイント：templates/ 配下のファイルは、Claudeが生成した成果物の「清書・共有用」テンプレートです。Claudeに「テンプレートの項目に合わせて出力して」と指示することで、内容をそのままコピー＆ペーストして資料を完成させることができます。

Step 3：カスタム指示を設定する（任意）

プロジェクト画面の「カスタム指示を設定」に、以下のように追記するとより効果的です。

```
None
あなたはプロジェクトナレッジに登録された「セキュリティ対応スキル」を活用して回答してください。
セキュリティ対応の立ち上げや計画策定に関する相談があった場合は、SKILL.md に記載された3フェーズの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言語で依頼するだけでOKです 。

スキルを起動すると、最初に以下3点の確認を行います。事前に整理しておくとスムーズです。

- 現在フェーズ：Phase 1（暫定対応）から始める／暫定対応済みでPhase 2から／ロードマップがありPhase 3から
- トリガー：監査指摘／インシデント発生／経営号令／退職者発生／自発的な対応
- 制約（3行で）：使える時間／動ける人数／持っている権限

```
# 例：立ち上げを依頼する
セキュリティ対応の立ち上げを手伝って

# 例：暫定対応から始める
暫定対応の計画を作って。トリガーは監査指摘で、対応期間は1週間、担当者は私1人です

# 例：恒久計画の策定を依頼する
セキュリティロードマップを作って。暫定対応は完了済みです
```

フェーズ別の成果物レビュー

各フェーズで生成される主な成果物は以下のとおりです。

フェーズ	成果物	**Excel**出力対応
Phase 1 暫定対応	• 初動レポート • 申し送り一覧	• 初動レポート（Excel）
Phase 2 恒久計画	• 突き合わせ一覧 • 調査結果 • 優先順位一覧 • 全体ロードマップ • マスタスケジュール	• 突き合わせ一覧 • 優先順位一覧 • マスタスケジュール（Excel）
Phase 3 恒久対応	• 手順書 • 経営報告	—

補足：スキルはフェーズごとに確認ポイントがあり、承認が取れるまで次のフェーズに進みません。Phase 1の段階で「全部やる」ではなく「致命傷の回避だけ」に絞るのがコアの考え方です。

チェックポイント

- Checkpoint①（Phase 1）：「対応する／触らない」仕分け結果を承認

- Checkpoint②（Phase 2）: 優先順位一覧を承認

出力形式

- md形式（デフォルト）: 各成果物を独立した .md ファイルで出力します
- Excel形式（オプション）: 主要成果物のみ対応。Python（openpyxl）でランタイム生成します
    - ファイル名形式: [案件名]_[成果物名]_[YYYYMMDD].xlsx
    - 書式: ヘッダー青（#4472C4）、オートフィルター、列幅自動調整、優先度セル色分け

参考資料（references/）

ファイル	内容
scenario-catalog.md	積み残しシナリオDB （記事6ケース＋AWS/Azure/オンプレ拡充）
triage-criteria.md	「対応する／触らない」仕分け判定フロー
notification-protocol.md	影響確認・通告の作法（通告先・タイミング・5要素）
priority-matrix.md	影響度×発生確率マトリクス基準
benchmark-mapping.md	CIS/NIST/AWS Well-Architected等との照合手順
handoff-criteria.md	フェーズ間ハンドオフ判断基準

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。

配布ZIPファイル（methods_0005_security.zip）をそのまま使用します。ZIPを展開する必要はありません。

Step 1: スキルをアップロードする

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. methods_0005_security.zip を選択してアップロード

Step 2: 使ってみる

アップロード後はチャット画面から自然言語で話しかけるだけでOKです。
操作方法は Claude Desktop と同様です。

```
None

# 例：立ち上げを依頼する
セキュリティ対応の立ち上げを手伝って
```

使い方3：Claude Code（CLI版）で使う

開発者の方や、ターミナルから利用される場合は、以下のパスに配置してご利用ください。
まずZIPを展開し、フォルダをコピーします。

```
None

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

またはシンボリックリンクで登録する場合：

```
None
ln -s "$(pwd)/security-response-pattern"
~/.claude/skills/security-response-pattern
```

補足：Claude Code をお使いの場合

スキルの起動はスラッシュコマンドまたは自然言語で行えます。

```
None
/security-response-pattern
```

または、以下のように自然言語で話しかけてください。

- セキュリティ対応の立ち上げを手伝って
- 暫定対応の計画を作って
- セキュリティロードマップを作って
- 監査指摘への対応計画を作って

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.**