Confidential

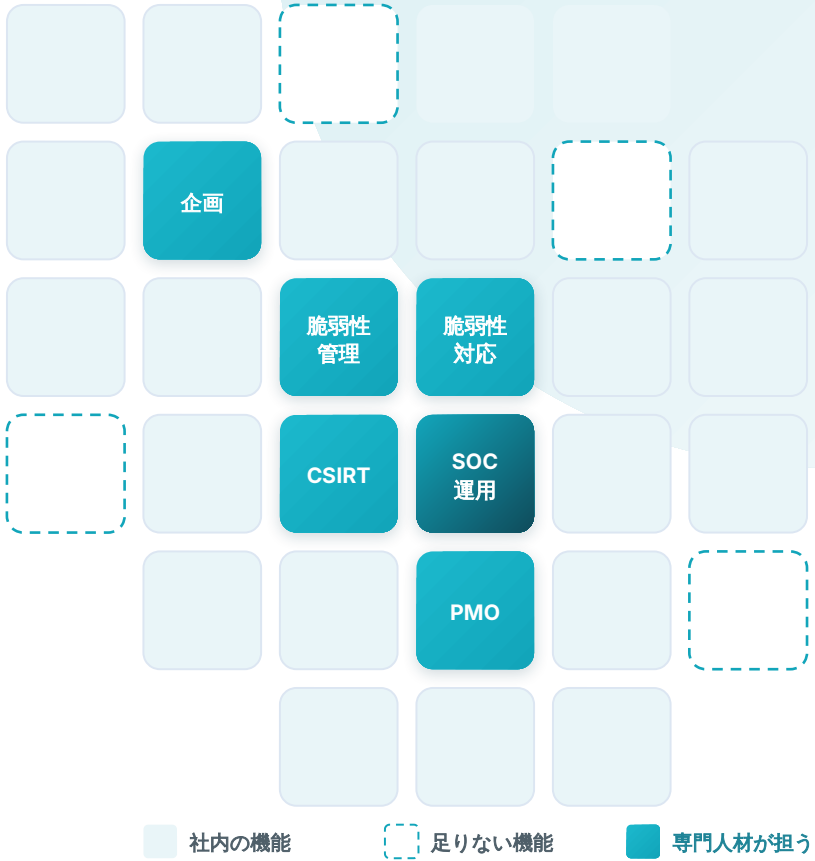
AI Security

SERVICE BROCHURE

セキュリティ社員代替サービス

社内のセキュリティ機能を、専門人材で「継続的に実行できる組織」へ。

企画・脆弱性対応・ CSIRT ／ SOC 運用・ PMO まで、
足りない機能だけを、月額の標準プランで。



AI セキュリティ株式会社

2026 年 10 月

Copyright(C)2026 AI セキュリティ株式会社

Confidential

WHAT IS ｜ セキュリティ社員代替サービスとは

セキュリティ担当者の業務を、専門人材が「社員と同じように」担うサービスです。

人材を紹介して終わりではなく、社内のセキュリティ機能そのものを提供します。
企画・脆弱性対応・ CSIRT 運用・ PMO まで、ご要件に応じた役割で稼働し、
月額の標準プランで、現状把握から 1〜2 か月で立ち上がります。

提供するもの

「人」ではなく「機能」

担当者の業務を代替・補完し、専門的な判断と施策の推進まで担う。社内の一員として機能を回す。

提供のかたち

月額の標準プラン

ライト／スタンダード／プレミアム。リモート常駐から常駐・複数名まで、派遣・業務委託で選べる。

人材紹介との違い

機能を止めない

当社の管理者が品質・引継ぎ・交代を担う。退職や異動があっても、セキュリティ機能は止まらない。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

Executive Summary

セキュリティ担当者の「機能」を、
月額の標準プランで、１〜２か月で立ち上げる。

専門人材が社内セキュリティ担当者の業務を代替・補完し、必要なセキュリティ機能を継続的に実行できる組織をつくります。
「人材提供」ではなく「組織機能の提供」として、立ち上がりの早さと継続性をお約束します。

01 何を提供するか

セキュリティ企画／ベンダー管理、脆弱性管理・対応、CSIRT ・ SOC 運用、セキュリティ PMO の各役割を、ご要件に応じて提供

12,000 名規模の人材データベースから、業務に合う専門家を選定

02 どう提供するか

ライト（0.5 人月＋管理者）／スタンダード（1.0 人月＋管理者）／プレミアム（常駐・複数名）の 3 プラン

派遣・業務委託から契約形態を選択。現状把握から標準 1〜2 か月で稼働

03 なぜ必要か

脅威の高度化と規制強化で業務は増え続ける一方、専門人材の採用は難しく、兼務・属人化が常態化

「対策の必要性は分かっているが、実行する人と時間がない」状態を解消

本資料では、サービスの内容・プラン・提供方法と実績を先にご紹介し、後半で背景となる環境変化と課題をご説明します。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

こんなお悩みはありませんか？

セキュリティ部門の現場では、「やるべきこと」は分かっていても、手が回らない状態が続いています。
多くのご相談は、次の 6 つのどれかに当てはまります。

01 **規程整備やベンダー調整に手が回らない**
企画業務が後回しになり年間計画も立てられない

02 **脆弱性が多く、優先順位が付けられない**
何から手を付けるべきか判断できない

03 **見つかった脆弱性が、解消されない**
現場・保守ベンダーとの調整が進まない



セキュリティ担当者

04 **アラートが多く、初動が遅れてしまう**
EDR ・ SIEM を入れたが、見る人がいない

05 **施策が多く、全体の進捗が見えない**
部門・ベンダーをまたぐ調整に追われている

06 **担当者が辞めたら業務が止まってしまう**
属人化していて、引継ぎ先がいない

そのお悩み、セキュリティ社員代替サービスで解決できます。
必要な役割の専門人材が社内に入り、止まっている業務を前に進めます。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

Service Overview

「人材」ではなく、「セキュリティ機能」を提供するサービスです

セキュリティ社員代替サービスの全体像

月額の標準プラン　派遣・業務委託　1〜2か月で立ち上げ

専門人材がお客様のセキュリティ部門に入り、担当者業務の代替・専門知識の提供・施策の推進を担います。

背後には当社の管理者・技術支援チーム・ナレッジがあり、個人の力量に依存しない形で機能を維持・高度化します。



Copyright(C)2026 AI セキュリティ株式会社

Confidential

標準パッケージプラン

まず始めやすいように、稼働量と管理体制を組み合わせた 3 つの標準プランをご用意しています。
業務の範囲や人数に応じて、プランの組み合わせや個別設計も可能です。

LIGHT

簡易トライアル Menu

150 万円／月（税別）

体制の構成

専門人材	0.5 人月	リモート常駐
管理者	0.1 人月	品質管理



■ 専門人材 ■ 管理者

こんなお客様に

- まず一部の業務から始めたい
- 週 2 〜 3 日相当の推進力がほしい
- 特定領域だけ代替したい

STANDARD

RECOMMEND

標準スターター Menu

380 万円／月（税別）

体制の構成

専門人材	1.0 人月	リモート常駐
管理者	0.5 人月	品質・継続性



■ 専門人材 ■ 管理者

こんなお客様に

- **担当者 1 名分を丸ごと代替したい**
- **品質と継続性を担保したい**
- **複数領域を 1 名で担いたい**

PREMIUM

戦略的拡張 Menu

個別お見積

体制の構成

専門人材	複数名	常駐も可
管理者	専任	体制に応じて



■ 専門人材 ■ 管理者

こんなお客様に

- オフィスへの常駐が必要
- 複数名のチームで提供したい
- ボリュームディスカウント

※「管理者」は当社の技術支援・品質管理担当（レビュー、エスカレーション対応、引継ぎ・交代の管理）。
※ 契約形態は派遣または業務委託（準委任）であり、価格は基本的には標準構成の目安で、業務範囲・スキル要件により個別にお見積します。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

Plan LIGHT

まずは週２〜３日分のセキュリティ実務を、専門人材に任せる

ライトプラン　専門人材 0.5 人月＋管理者 0.1 人月

150 万円／月（税別）　リモート常駐　業務範囲は個別に調整

週 2 〜 3 日相当の稼働で、規程整備や脆弱性管理など、特定の業務を代替します。管理者が品質を確認します。

向く場面は、まず一部の業務から始めたい場合や、特定の領域だけ手が足りない場合です。



Copyright(C)2026 AI セキュリティ株式会社

Confidential

Plan STANDARD

担当者１名分の セキュリティ機能を、 丸ごと任せる

スタンダードプラン　専門人材 1.0 人月＋管理者 0.5 人月

380 万円／月（税別）　リモート常駐　標準プラン

専門人材がフルタイムで担当者業務を代替し、管理者が業務管理・品質・引継ぎを担います。

向く場面は、担当者１名分の機能を確保したい場合や、退職・欠員の穴を埋めたい場合です。



Copyright(C)2026 AI セキュリティ株式会社

Confidential

AI Security

Plan PREMIUM

常駐・複数名のチームで、セキュリティ部門の運営そのものを支える

プレミアムプラン　常駐・複数名・専任管理者

個別お見積　常駐も可　ボリュームディスカウント可

お客様オフィスへの常駐や複数名のチームでの提供など、ご要件に合わせて体制を設計します。

向く場面は、複数の領域を同時に進めたい場合や、セキュリティ部門の立ち上げ・再編を行う場合です。



Copyright(C)2026 AI セキュリティ株式会社

Confidential

ご要件に応じた人材のご案内

「どの業務を任せたいか」に応じて、適した役割の人材をご案内します。
単独でも、複数の役割を組み合わせても構成できます。

こんなご要件なら	この役割の人材で	主な業務
01 企画・規程整備や、ベンダーとの調整を任せたい	セキュリティ企画／ベンダー管理	年間計画・規程整備、製品選定、ベンダー管理・契約調整、経営層への報告
02 脆弱性情報を継続的に把握し、優先順位を付けたい	脆弱性管理	脆弱性情報の収集、影響評価、対応優先度の決定、進捗管理と報告
03 見つかった脆弱性を、実際に解消したい	脆弱性対応	パッチ適用計画、設定変更、ベンダー・現場との調整、適用確認、例外管理
04 検知・初動・エスカレーションを回す体制をつくりたい	CSIRT ・自社 SOC 運用	アラート監視・トリアージ、初動対応、インシデント記録、手順の改善
05 複数の施策・ベンダー・部門をまとめて推進したい	セキュリティ PMO	施策の進捗・課題管理、会議体運営、部門横断の調整、経営報告

例：「脆弱性管理＋脆弱性対応」を 1 名で、「セキュリティ PMO ＋企画」を 2 名体制で、といった組み合わせも可能です。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

最近多いご相談

規制・取引先への対応や生成 AI の利用ルールなど、「新しい仕事」のご相談が増えています。
いずれも、専門人材が社内に入ることで前に進められるテーマです。

RECENT TOPICS

「やることは決まっているのに、回す人がいない」

ご相談の多くに共通するのは、
方針や必要性は明確でも、実務を
担う人と時間が足りないことです。

右のテーマは、次ページ以降の
提供領域 01 〜 05 で対応しています。

	よくいただくご相談	対応の例
金融・保険	「金融庁ガイドラインへの対応状況を整理し、説明できるようにしたい」	ギャップ分析と是正計画 → 領域 02
製造・取引先	「取引先から届くセキュリティ調査票への回答が追いつかない」	回答と証跡の整備 → 領域 02
生成 AI	「生成 AI の社内利用ルールとガバナンスを整えたい」	規程・ガイドラインの策定 → 領域 01
脆弱性	「診断結果が溜まり、対応が進まないまま残っている」	優先度付けと適用の調整 → 領域 03
SOC 運用	「EDR ・ SIEM を入れたが、アラートを見る人がいない」	監視・トリアージ・初動 → 領域 04
体制	「担当者の退職が決まり、引継ぎ先が見つからない」	引継ぎと業務の代替 → プラン

Copyright(C)2026 AI セキュリティ株式会社

提供領域　01

ガバナンス・企画

想定：企画担当が1〜2名の企業｜担い手：セキュリティ企画

方針・規程・計画を整え、経営に説明できる状態をつくります。

規程が古いまま年間計画も立てられず、ベンダーとの調整や経営報告に追われている状態です。企画の実務を担い、責任者が判断に集中できるようにします。

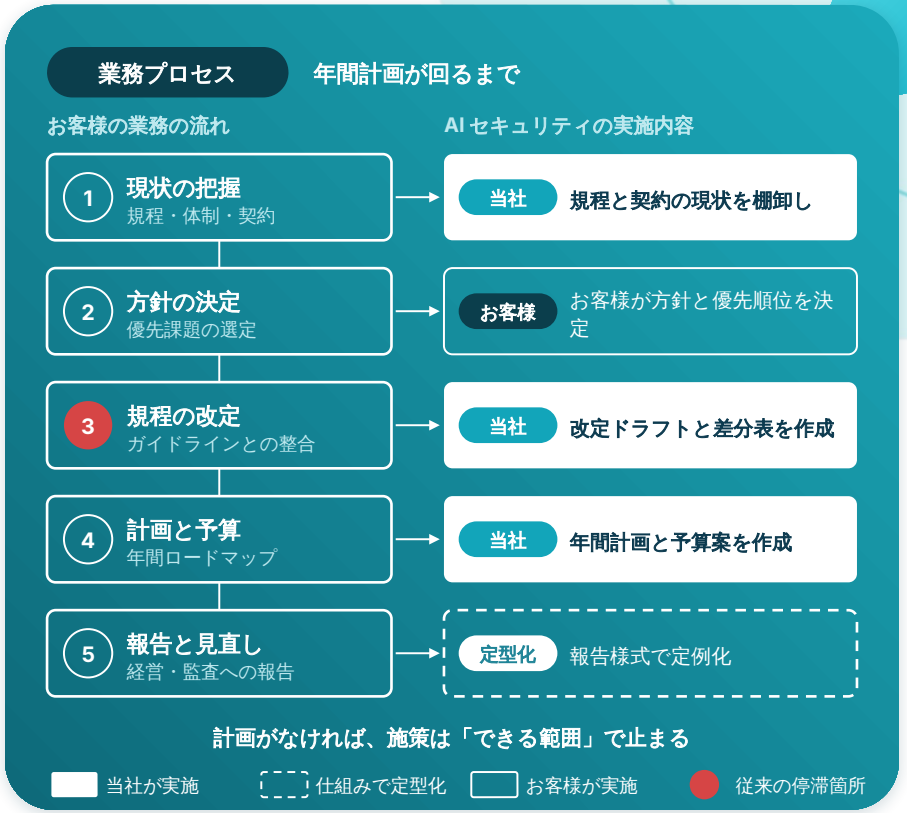
専門人材が担うこと

01　規程・ガイドラインの改定ドラフト

02　年間計画・ロードマップと予算案の作成

03　ベンダー管理（契約・ SLA ・評価）と経営報告

成果指標　規程の改定状況／計画に対する施策の実施率



Copyright(C)2026 AI セキュリティ株式会社

提供領域　02

リスク管理・規制対応

想定：規制業種・取引先調査が多い企業｜担い手：リスク管理

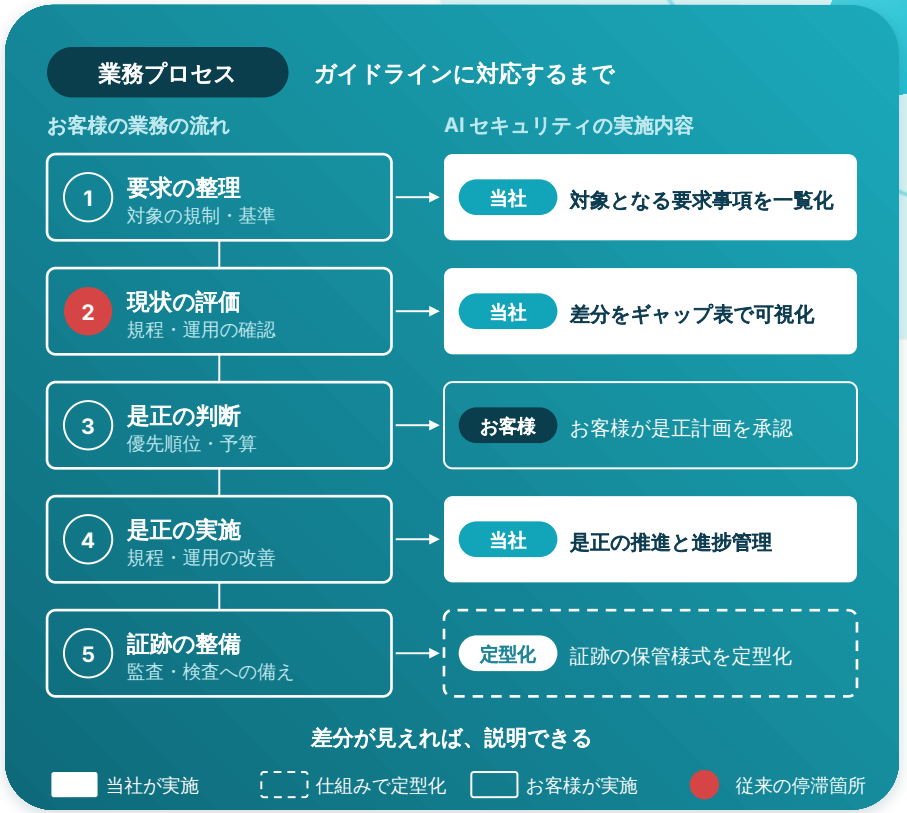
ガイドラインとの差を見える化し、当局・取引先に説明できる状態にします。

金融庁ガイドラインや取引先の調査票への対応が増える一方で、現状との差分が整理できていない状態です。差分の把握から是正までを担います。

専門人材が担うこと

- 01　ガイドライン・法規制とのギャップ分析
- 02　委託先・サードパーティのリスク評価
- 03　監査・検査・調査票への回答と証跡の整備

成果指標　ギャップの是正率／調査票の回答リードタイム



Copyright(C)2026 AI セキュリティ株式会社

提供領域　03

技術対策・運用

想定：診断結果が溜まっている企業｜担い手：脆弱性管理・対応

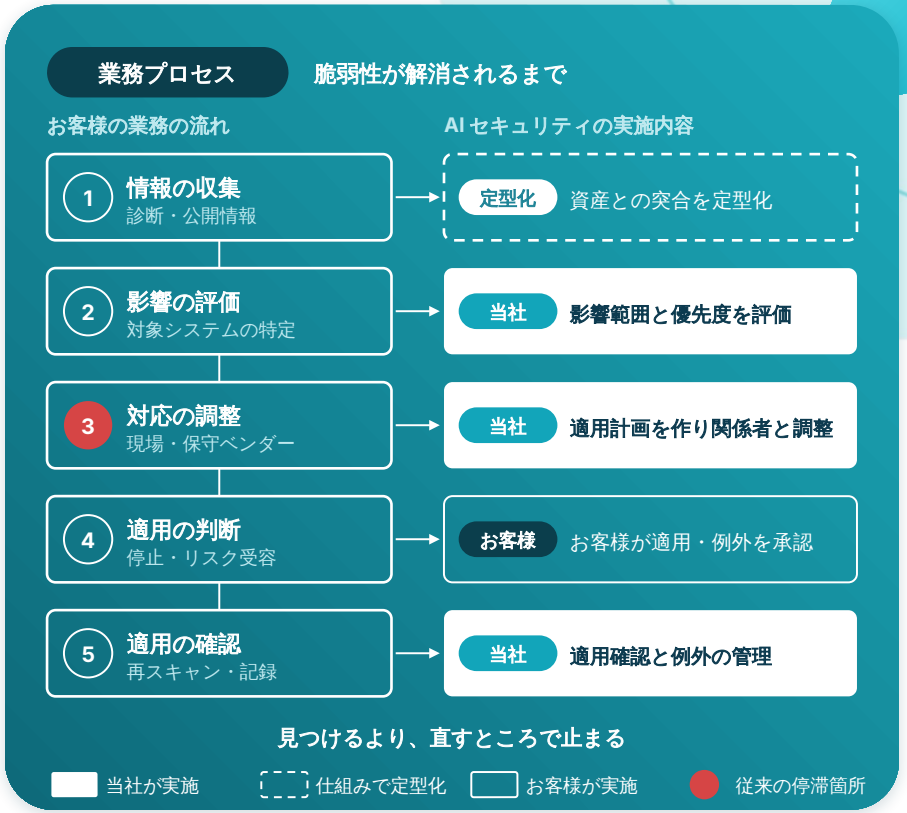
見つかった脆弱性を、優先順位を付けて確実に解消します。

診断やスキャンで脆弱性は見つかっても、影響評価と現場・ベンダーとの調整が進まず、対応が滞留している状態です。評価から適用確認までを担います。

専門人材が担うこと

- 01　脆弱性情報の収集と影響評価・優先度付け
- 02　パッチ適用計画と現場・保守ベンダーとの調整
- 03　EDR ／ SIEM 等の運用とチューニング

成果指標　高リスク脆弱性の対応日数／未対応件数の推移



Copyright(C)2026 AI セキュリティ株式会社

提供領域　04

インシデント対応

想定： EDR ・ SIEM 導入済みで人手不足｜担い手： CSIRT ・ SOC 運用

アラートから初動・報告までを、迷わず回せる体制にします。

ツールは導入したものの、アラートを見る人と
判断の基準がなく、初動が遅れがちな状態です。
監視・トリアージから手順の改善までを担います。

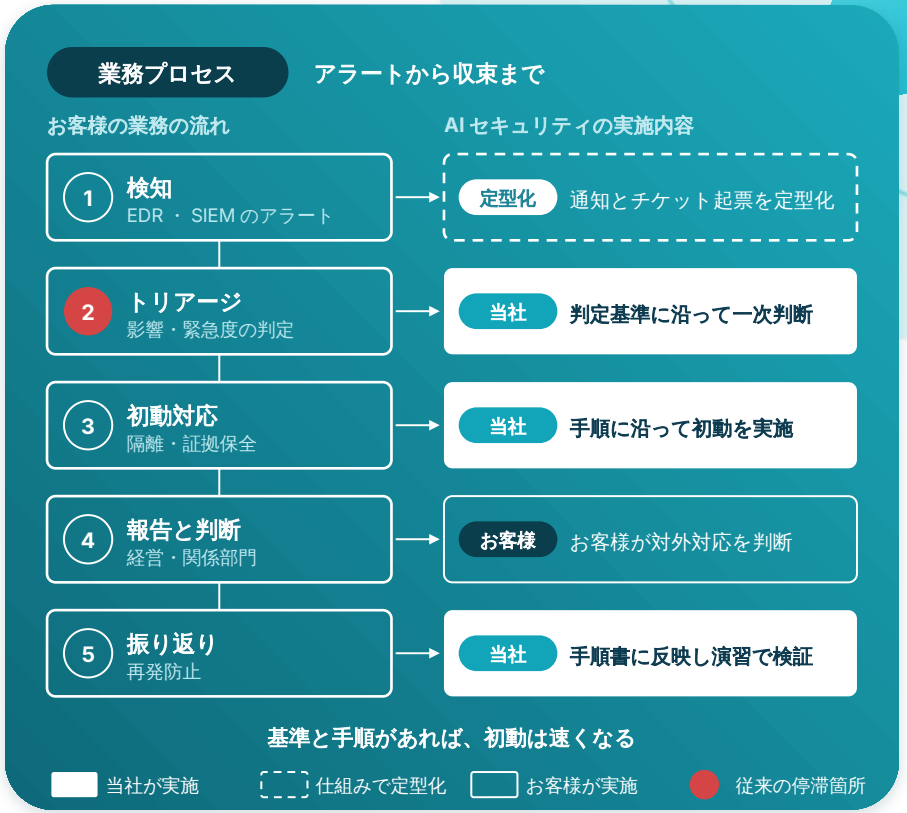
専門人材が担うこと

01　アラート監視とトリアージ・一次対応

02　インシデントの記録とエスカレーション

03　対応手順の整備と机上演習による改善

成果指標　初動までの時間／エスカレーションの適切率



Copyright(C)2026 AI セキュリティ株式会社

提供領域　05

教育・啓発／相談対応

想定：問い合わせが担当者に集中 | 担い手：セキュリティ企画

社員の意識を底上げし、担当者への問い合わせを減らします。

現場からの相談が担当者に集中し、教育や訓練は
毎年同じ内容の繰り返しになっている状態です。
相談窓口と教育の両方を担います。

専門人材が担うこと

- 01　全社教育コンテンツの作成と実施
- 02　標的型メール訓練の企画と結果の分析
- 03　相談窓口の一次対応と FAQ の整備

成果指標　訓練結果の推移／問い合わせ件数と対応時間



Copyright(C)2026 AI セキュリティ株式会社

Confidential

サービス提供モデル

常駐・リモート・ハイブリッドの３つの提供形態と、フルタイムから週数日までの稼働率を組み合わせます。
契約形態は、指揮命令の必要性に応じて派遣と業務委託（準委任）からお選びいただけます。

提供形態 × 稼働率

リモート型

稼働目安 週１日〜スポット

01

スポット・週１日

リモートで業務を担い、会議はオンライン参加
専門的なレビュー・助言、監査対応など専門性重視の業務に

ハイブリッド型

稼働目安 週２〜３日

02

稼働率

定例日に出社し、それ以外はリモートで推進
企画・規程整備・ベンダー対応など推進型の業務に

常駐型

稼働目安 週５日

03

週５日（フルタイム）

お客様オフィスに常駐し、社内担当者と同じ環境で業務
現場の相談対応・調整が多い業務、インシデント初動に

契約形態

派遣契約

指揮命令：お客様（派遣先）

- 社内担当者と同じ業務を、同じ指示系統で担ってほしい場合に
- 労働者派遣法に基づく契約（当社 許可番号：派 -13-317530 ）

業務委託（準委任）契約

指揮命令：当社が業務を管理

- 特定の業務領域・テーマを任せ、成果の報告を軸に進めたい場合に
- 想定成果物・報告頻度を事前に合意。成果物の完成保証は対象外

※ 稼働率と提供形態は、導入後も業務量の変化に合わせて見直せます。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

サービス提供体制

お客様が意思決定を担い、当社の専門人材が実務と専門的な判断を担います。
管理者・技術支援チームが後方から品質と継続性を支えるため、個人の力量に依存しません。

	意思決定・承認	実務の遂行	専門的な判断	品質・継続性
お客様 **責任者・担当者**	主担当 **方針・予算・施策の最終判断**	支援 社内手続き・関係部門との調整	支援 判断結果の確認と承認	支援 優先順位付けと評価
AI セキュリティ **専門人材（現場）**	支援 判断材料・選択肢・推奨案の提示	主担当 **担当者業務の代替・文書作成・ベンダー対応**	主担当 **リスク評価・技術的妥当性の評価**	支援 業務の標準化・文書化
AI セキュリティ **管理者・技術支援チーム**	支援 定例報告での論点整理	支援 繁忙期の増員・後方支援	支援 レビュー・インシデント時の助言	主担当 **品質管理・引継ぎ・交代の管理**

お客様が「決める」、当社が「実行し、専門的に支える」。この分担で、セキュリティ部門を一つのチームとして運営します。

※ 派遣契約の場合、業務上の指揮命令はお客様（派遣先）が行います。業務委託（準委任）契約の場合は当社が業務を管理し、成果の確認・報告を通じて連携します。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

導入プロセス

現状把握から運用開始までを標準で1〜2か月、その後は継続改善のサイクルを回します。
引継ぎを丁寧に行うことで、業務を止めずにスムーズに移行します。

約2週間	約2週間	約2〜4週間	稼働開始	継続
01	02	03	04	05
現状把握	業務設計	引継ぎ	運用開始	継続改善
• 現在のセキュリティ業務・体制・課題のヒアリング • 代替・補完する業務の候補と優先度の整理	• 対象業務・役割分担・提供形態・稼働率の設計 • 人材の選定・ご面談、契約形態の決定	• 既存担当者からの業務・ドキュメントの引継ぎ • 関係部門・ベンダーへの紹介、アクセス権の整備	• 定例報告・エスカレーションルールに沿って運用 • 技術支援チームによるレビュー	• 業務の標準化・文書化、プロセス改善の提案 • 稼働率・体制の見直し、クロストレーニング

導入後は「運用 → 改善」のサイクルを回し、セキュリティ機能を維持するだけでなく高度化していきます。
現状把握と業務設計の段階では、対象業務の範囲を一緒に決めるため、お客様側の工数も最小限で済みます。

Copyright(C)2026 AIセキュリティ株式会社

実績紹介　CASE 01

CSIRT 体制の構築

お客様：大手不動産デベロッパー｜体制：業務委託（体制構築支援）

インシデント時に「誰が何をするか」を、全社で動ける形にしました。

CSIRT の必要性は認識していても、役割と手順が
未整備で、専任の人材も限られている状態でした。
体制設計から演習・改善までを一体で進めました。

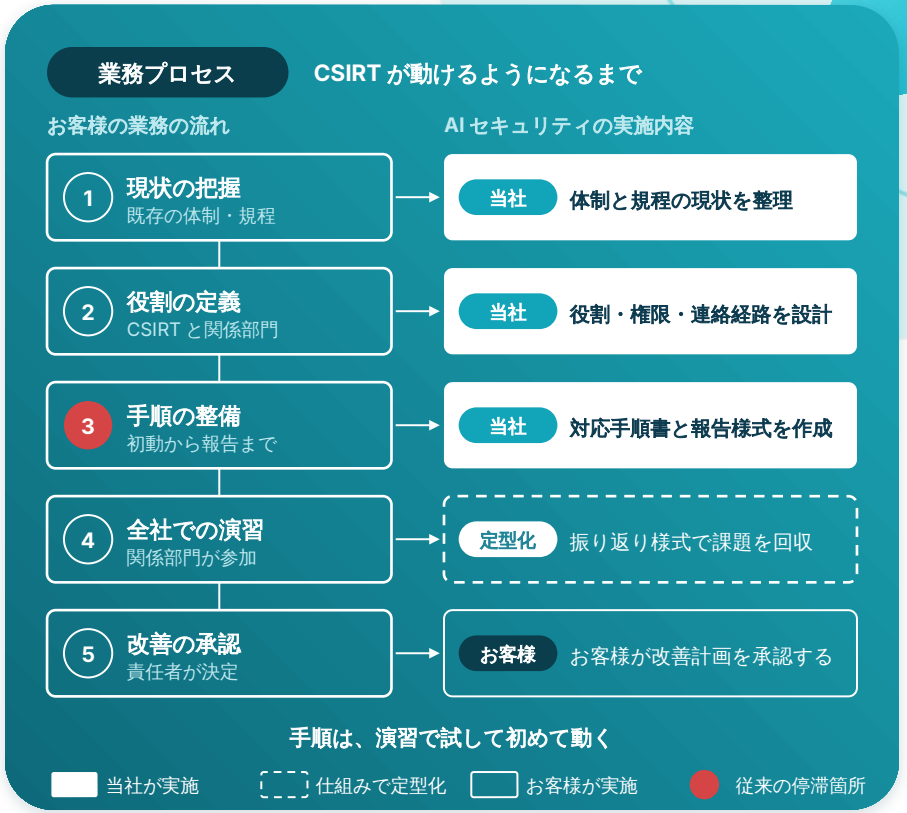
AI セキュリティが担ったこと

01　CSIRT の役割定義とエスカレーションルール

02　インシデント対応手順書と連絡体制の整備

03　全社机上演習の企画・実施と手順書への反映

成果　手順書の整備範囲／演習で見つかった課題の改善数



Copyright(C)2026 AI セキュリティ株式会社

実績紹介　CASE 02

提案〜デリバリーの代替

お客様：大手セキュリティ専門企業｜体制：派遣契約（社員代替）

社員と同じ指示系統で、提案からデリバリーまでを担います。

案件の増加に対して提案とデリバリーを担える人材が
不足し、採用では立ち上がりが間に合わない状態でした。
社員代替で稼働し、段階的にチームへ広げています。

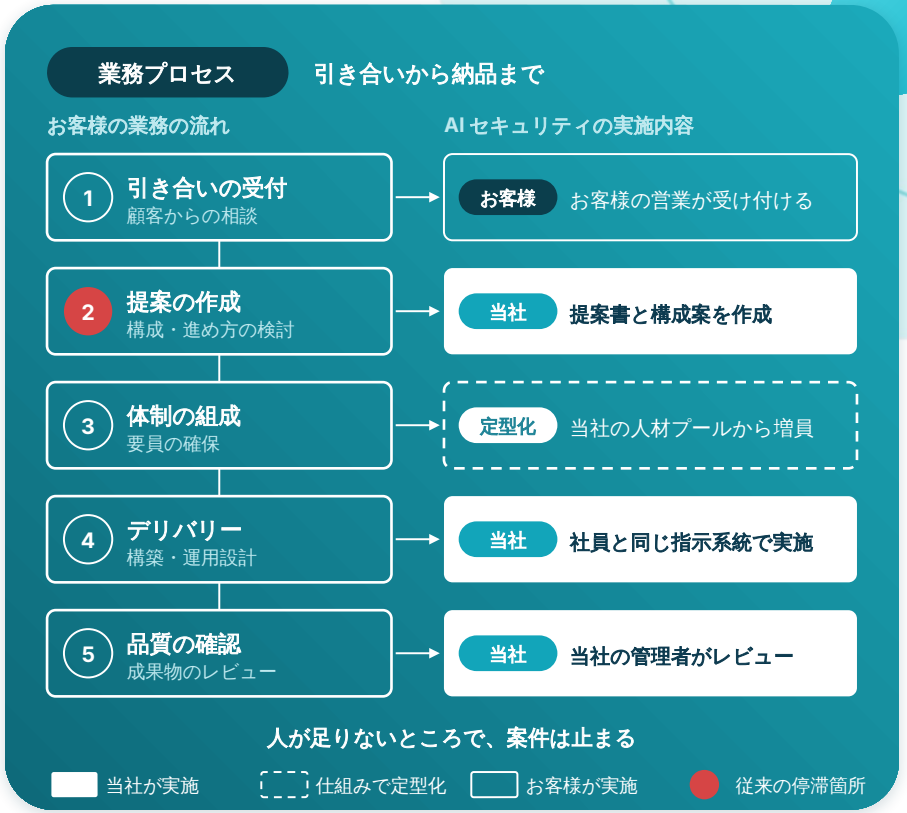
AI セキュリティが担ったこと

01　提案書の作成と顧客折衝の支援

02　プロジェクトのデリバリー（構築・運用設計）

03　当社管理者による品質管理と増員計画

成果　対応できる案件数／立ち上がりまでの期間



Copyright(C)2026 AI セキュリティ株式会社

実績紹介　CASE 03

人材プール型の体制支援

お客様：大手 SIer セキュリティ事業部門 | 体制：人材プール型

複数案件の人材依頼を、一つの窓口で回せるようにしました。

複数のエンド企業案件が同時に動き、 PM 人材が不足。
依頼ルートも複線化し、担当者の調整負荷が
増えていました。窓口を一本化し、差配を担います。

AI セキュリティが担ったこと

01　案件ごとの PM ・エンジニアのアサイン

02　依頼窓口の一本化と差配担当の配置

03　稼働状況と要員計画の定例報告

成果　依頼から参画までの日数／担当者の調整工数



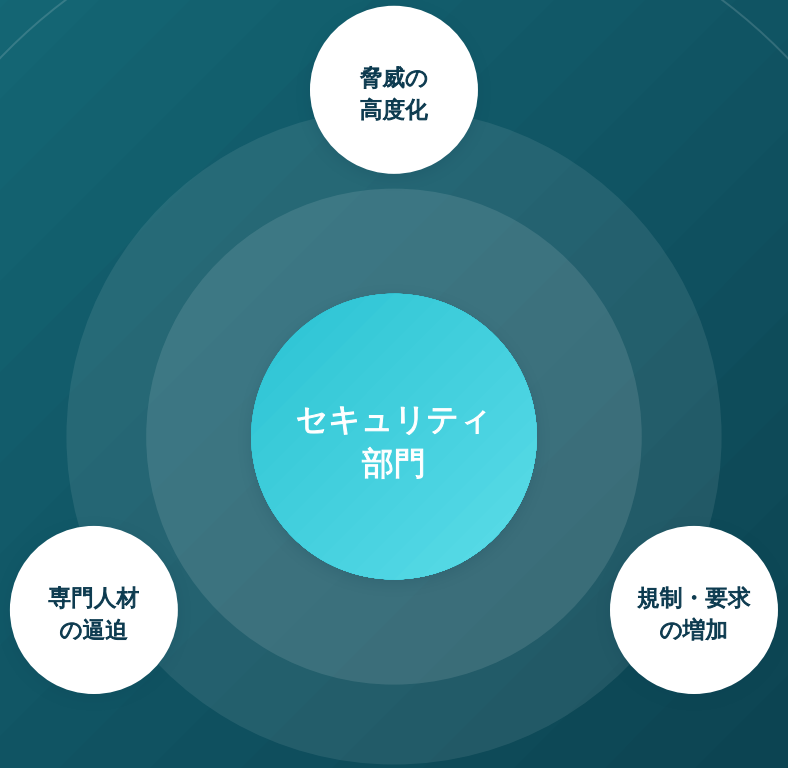
Copyright(C)2026 AI セキュリティ株式会社

Confidential

WHY NOW

なぜ今、「社員代替」なのか。

業務は増え続け、担う人は増えない。
その構造を、採用だけで解くのは難しくなっています。

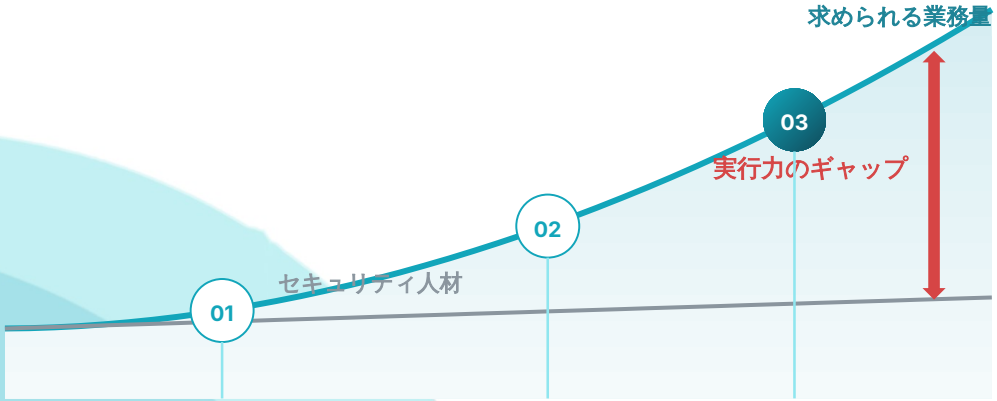


Copyright(C)2026 AI セキュリティ株式会社

Confidential

セキュリティ組織を取り巻く環境変化

サイバー脅威の高度化、規制・取引先からの要求増加、専門人材の逼迫が同時に進んでいます。
セキュリティ部門に求められる業務量は増え続ける一方で、担う人材は増えていません。



01 脅威の高度化

ランサムウェア被害は製造業が約 4 割、中小企業が約 6 割

02 規制・要求の増加

金融庁ガイドライン、サイバー対処能力強化法、取引先の調査票

03 守る範囲の拡大

クラウド・ SaaS ・ OT ・サプライチェーンへ対象が広がる

数字が示していること

01 攻撃は業種・規模を問わず「来る前提」に

2025 年のランサムウェア被害 226 件のうち製造業が約 4 割、中小企業が約 6 割。復旧費用 1,000 万円以上が 5 割超

02 「人がいない」より「スキルが足りない」が本質

セキュリティ組織の 95% が何らかのスキル不足を抱え、 59% は「重大・深刻」と回答（ ISC2 2025 ）

03 日本は人材確保の難しさが世界平均を上回る

「必要な人材を確保できない」は日本 42% 、世界 29% 。採用だけで埋めるのは現実的ではない

04 規制は「体制と人材の確保」を明示的に求める段階へ

金融庁ガイドライン（ 2024 年 10 月）、サイバー対処能力強化法（官民連携規定は 2026 年 10 月施行予定）

「対策が必要なこと」は分かっていても、「実行する人と時間」が足りない企業が増えています。

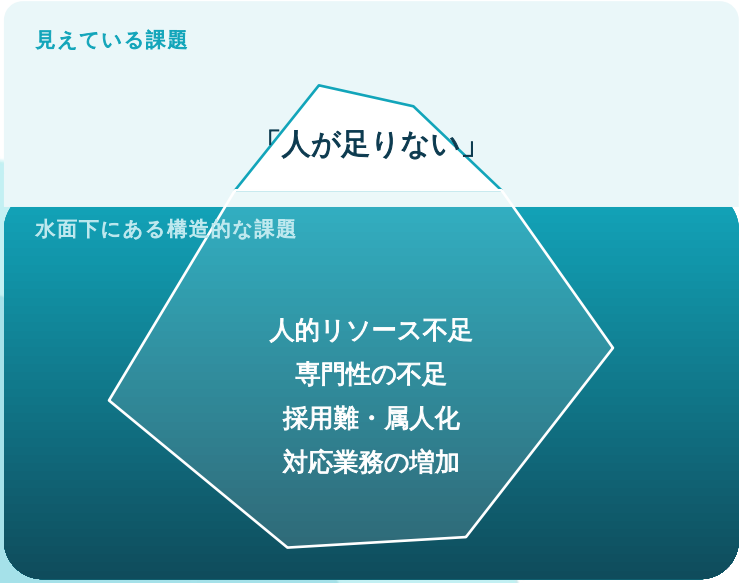
出典：警察庁「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」／ ISC2 「 Cybersecurity Workforce Study 2025 」／金融庁ガイドライン（ 2024 年 10 月）／サイバー対処能力強化法

Copyright(C)2026 AI セキュリティ株式会社

Confidential

企業が抱えるセキュリティ組織の課題

「セキュリティ人材が足りない」という一般論の水面下には、現場で起きている 4 つの構造的な課題があります。
いずれも、担当者個人の努力では解決しにくい問題です。



01 人的リソース不足

日常の運用・問い合わせ・監査対応に追われ、重要な施策を推進できない
IT 部門との兼務が多く、セキュリティに充てられる時間が限られる

02 専門性の不足

リスク評価・製品選定・インシデント時の判断など、高度な判断が難しい
ベンダー提案の妥当性を評価できず、意思決定が遅れる

03 採用難・属人化

採用に時間を要し、採用できても定着が課題
既存担当者の退職で業務が止まり、ノウハウが失われるリスクが高い

04 対応業務の増加

新たな脅威、規制改正、取引先の要求、経営層への報告が増え続ける
「やるべきこと」が「できること」を恒常的に上回る

結果として、セキュリティ施策の実行が停滞します。
対策の必要性を認識していても、実行する人材と時間が不足している――これが多くの企業の実態です。

Copyright(C)2026 AI セキュリティ株式会社

Confidential

業界別に見るセキュリティ組織の課題

課題の構造は共通ですが、業界ごとに「増え続ける業務」の中身は異なります。
保険・製造をはじめ、各業界の要求事項に精通した人材で対応します。

保険・金融

規制対応

当局・検査・ガイドラインへの対応が重い

ガイドライン

金融庁ガイドラインが、経営陣主導の態勢と人材・予算の確保を要求

当局・検査

保険会社向け監督指針も、サイバー対応強化へ改正案（2026 年）

第三者管理

代理店・委託先・共同利用システムまで管理範囲が広い

製造

OT ・供給網

工場・取引先まで守る範囲が広い

OT ・工場

工場の設備系は、 IT と OT の両方が分かる人材が少ない

被害の傾向

ランサムウェア被害は製造業が最多（2025 年 約 4 割）

取引先要求

取引先からの調査票・対策証明への対応が常態化

流通・サービス・その他

少人数兼務

1〜2 名が全領域を担っている

兼務

情報システム部門の 1〜2 名がセキュリティを兼務

認証・監査

ISMS ・ P マークの維持や取引先確認が担当者に集中

守る範囲

クラウド・ SaaS ・リモートワークで守る範囲が拡大

出典：金融庁（2024 年 10 月 4 日公表ガイドライン、 2026 年 3 月 30 日監督指針改正案）／経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」／警察庁（2026 年 3 月）

Copyright(C)2026 AI セキュリティ株式会社

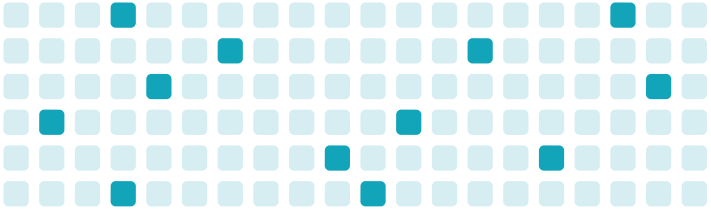
Confidential

目指すべきセキュリティ組織の姿

いまは「やるべき業務」の一部しか回っておらず、残りは担当者の手が空くのを待っている状態です。
専門人材を組み込み、機能として定義することで、業務の全体が継続的に回るようになります。

いま　一部しか回っていない

担当者の知識と頑張りで成り立ち、実行できているのは
やるべき業務の一部。退職・異動で止まってしまいます。



実行できているのは、やるべき業務の一部

これから　機能として全体が回る

社内担当者と専門人材で機能を定義し、欠員・繁忙期にも
止まらない体制に。人が替わっても業務は続きます。



やるべき業務が、継続的に実行される

3つの条件を備えることで、セキュリティ機能は「回り続ける」ようになります。
① 機能の定義（誰が・何を・どの頻度で）　② 体制の継続性（外部の専門人材を組み込む）　③ 専門性と高度化（標準化・改善を続ける）

※ タイル1マス＝1つのセキュリティ業務（イメージ）

Copyright(C)2026 AIセキュリティ株式会社

Confidential

導入効果・費用対効果

自社採用と比べ、立ち上がりの早さ・専門性・退職リスク・コスト構造の面で優位性があります。
採用を否定するものではなく、採用と並行して「今」機能を確保する選択肢になります。

自社採用との比較

比較軸	自社採用（正社員）	本サービス	補足
立ち上がりまでの期間	△	◎	採用活動に数か月〜1年以上を要することが多いのに対し、本サービスは1〜2か月で稼働
専門性の幅	○	◎	1人の採用では専門領域が限られる。本サービスは後方の技術支援チームで領域を補完
退職・異動による業務停止リスク	△	○	後任の引継ぎ・交代を当社が担い、業務を止めない
コスト構造	○	◎	固定費（給与・教育・採用費）に対し、稼働率に応じた変動費として最適化できる
業務の標準化・文書化	△	◎	属人化しやすい社内担当に対し、標準化と文書化を前提に業務を設計

◎ 優位　○ 標準　△ 課題になりやすい

期待できる 3 つの効果

01 セキュリティ施策の実行
停滞していた規程整備・脆弱性対応・演習などが、計画どおりに進む

02 監査・当局・取引先対応
ガイドライン・調査票・検査への対応を、専門人材が主導して負荷を下げる

03 担当者の本来業務への集中
社内担当者は意思決定・社内調整に集中でき、離職防止にもつながる

Copyright(C)2026 AI セキュリティ株式会社

Secure today, Design tomorrow

セキュリティを止めない組織を、専門人材とともに。

セキュリティ社員代替サービスは、「人」ではなく「機能」を提供します。
お客様のセキュリティ部門の一員として、必要な機能を継続的に実行し、高度化していきます。

AI セキュリティ株式会社

労働者派遣事業 許可番号：派 -13-317530

Copyright(C)2026 AI セキュリティ株式会社