Confidential

# インシデント対応
# 机上演習パック

**侵入される前提で、組織が動けるかを半日で確かめる。**
**5つの標準シナリオ × 参加部門で選ぶ3つの定額パック（300万円／500万円／950万円）**

こんなご担当者に

- ✓ マニュアルはあるが、一度も動かして確かめていない
- ✓ 有事に誰が何を判断するか、まだ固まっていない
- ✓ ガイドラインや上長から、演習の実施を求められている

**サービス説明資料**

2026年10月

**AIセキュリティ株式会社**

Copyright(C)2026 AIセキュリティ株式会社

# こんなお悩みはありませんか

**体制やマニュアルは整えたものの、「本当に動けるのか」に自信が持てないというご相談が増えています。**
**部門ごとに、よくいただくお悩みを整理しました。**

## セキュリティ部門（CSIRT）

- マニュアルは作ったが、一度も「動かした」ことがない
- ガイドラインや取引先から「演習の実施」を求められている
- シナリオ作成や部門調整に手が回らず、訓練が後回しになる

## IT部門（情シス・インフラ・運用）

- 遮断・停止・復旧の判断を、誰がいつ下すのか決まっていない
- 障害対応の手順はあるが、サイバー攻撃を想定した切り分けがない
- 委託先・クラウド事業者との連絡経路が実態と合っているか不安

## 業務部門（広報・法務・事業部門）

- 有事に自部門が何をすべきか、誰も説明してくれない
- 本社と支店・グループ会社の報告ラインが曖昧
- 顧客・取引先への説明責任を、誰がどう果たすのか分からない

**共通するのは「整備はした。でも、動くかどうかを確かめていない」こと。**
机上演習は、この不安を半日で「具体的な課題」に変えます。

Copyright(C)2026 AIセキュリティ株式会社

Confidential

# 机上演習で、
# 手に入るもの。

**侵入を完全に防ぐことは、もうできません。**
**問われるのは、侵入されたときに組織が「動けるか」。**
**机上演習は、それを全員で体験して確かめる方法です。**

### こんな状況の方へ

- ✓ **ガイドラインや上長から、演習の実施を求められている**
- ✓ **マニュアルはあるが、一度も動かしたことがない**
- ✓ **有事に誰が何を判断するか、決まっていない**

01

### CSIRTの運用を動かして確かめる

アセスメントにとどまらず、検知→報告→判断→封じ込めの運用が実際に回るかを検証

02

### 関係各所を巻き込み危機意識を醸成する

IT部門・広報・法務・事業部門が同じ部屋で判断し、「自分ごと」になる

03

### 文書を「動くもの」に変える

マニュアル・行動手順書と実態の乖離が、半日で具体的な課題として見える

04

### 投資と対応を説明できる

ガイドラインが求める演習実績と、社内・取引先への説明材料が同時に手に入る

Copyright(C)2026 AIセキュリティ株式会社

Confidential

# 「防ぐ」から「侵入前提で動ける組織」へ

**攻撃の高度化により、侵入を完全に防ぐ前提は成り立たなくなりました。**
**侵入されても事業を止めないために、組織に備わっていてほしい7つの要件を整理しました。**

01 **検知して報告する**
異常をCSIRTに即時に上げる

02 **影響範囲を把握する**
被害と持ち出しの痕跡を整理する

03 **判断者が決める**

04 **封じ込めを指示する**
技術と事業の判断を分けて動く

05 **代替手段で連絡する**
ツール停止時の連絡経路を持つ

06 **社外に説明する**
顧客・取引先への説明責任を果たす

07 **復旧し教訓を残す**
課題を整理し手順書を改訂する

前提 | **侵入は防ぎ切れない**

**7つの要件は、文書に書いてあるかではなく「動けるか」で確かめるものです。**

**机上演習は、この7つを半日で順に試し、組織の「動けなさ」を安全に可視化する最短の手段です。**

Copyright(C)2026 AIセキュリティ株式会社

Confidential

# 本資料の構成

**本資料は5章で構成しています。**
**市場動向から「なぜ今、机上演習か」を示し、サービスの中身と3つのパックをご説明します。**

01
WHY NOW
## 市場動向
直近の事案、AIによる攻撃の自動化、発生後の対応の差、ガイドラインが求める「演習」
P.8〜11

02
ISSUE
## お悩み
セキュリティ・IT・業務部門それぞれの不安と、演習で見えるもの
P.2 / 12〜13

03
SERVICE
## サービス概要
演習の流れ、選べる5つの標準シナリオ、当日の風景、当社の特徴
P.14〜18

04
PACKAGE
## パック・価格
2／3／5ヶ月、参加部門で選ぶ300／500／950万円の3パックと提供内容
P.19〜23

05
DELIVERY
## 進め方・実績
パック別スケジュール、想定成果物、ご支援実績、前提条件
P.24〜29

Copyright(C)2026 AIセキュリティ株式会社

Confidential

# AI時代のセキュリティ対策を担う会社

**AI時代を代表する”AI推進とSecurity強化の総合型ファーム”として、皆さまの持続的な企業価値向上を支援いたします。**



CEO MESSAGE

**Secure today, Design tomorrow**

**堀居 隆生** 代表取締役 CEO

AI活用と安全性を両立させる
新たなセキュリティの基盤づくりに挑んでいます

COMPANY

## AIセキュリティ株式会社 AI Security Inc.

**代表者** 代表取締役 CEO 堀居 隆生
代表取締役 COO 市川 貴大

**本 社** 東京都新宿区四谷1-9-16 三宅ビル4F
**許認可** 有料職業紹介 13-ユ-314622 ／ 労働者派遣 派-13-317530

**200社**
累計支援企業数

**120名**
従業員数
※パート・業務委託込

**6期目**
2021年9月設立
※4期目に決算期変更

### 当社の特徴

1. **Glasswing採択ベンダーと提携**
   CrowdStrike・AWS・Cisco（Splunk）等
2. **国内最大手SIerと強連携**
   AI×Security領域で独占的に推進中
3. **プライム上場から急成長企業まで**
   業種を問わず累計200社を支援
4. **社内にAI Security研究組織**
   大手ファーム・SIer出身者が在籍

### 出身企業

Deloitte. デロイト トーマツ / accenture / pwc / NRI SECURE / IBM / EY / NEC Orchestrating a brighter world / HITACHI Inspire the Next / CTC / baycurrent / Simplex Inc. / IIJ / GMO CYBER SECURITY IERAE / BANK OF AMERICA

### 所属団体

JNSA 特定非営利活動法人 日本ネットワークセキュリティ協会 / 一般社団法人 AIガバナンス協会 AI Governance Association

### 取得認証

ISO27001（ISMS）
JISQ15001（Pマーク）

Copyright(C)2026 AIセキュリティ株式会社

中核メンバー

# 大手ファーム・グローバルセキュリティベンダー出身の中核メンバーが在籍

大手ConsultingファームにてPMDを務めたメンバーや、グローバルセキュリティベンダーにて責任者を務めたメンバー、官公庁対応・事業会社としてのセキュリティ戦略・管理に従事した布陣にて、お客様への価値提供を推進しております。



コンサルティング&ソリューション事業統括本部 事業統括本部長

## 和田Benjamin真治

Apple Inc.、NRIセキュアテクノロジーズ株式会社に従事し、セキュリティ戦略策定とDigital Identityに強みを有する



Account Sales本部
本部長

## 前田 和則

Symantec社にて営業本部長・執行役員を歴任した後に、AccentureではManaging DirectorとしてSecurity Consulting部門を立ち上げ



Partner
兼 Security Evangelist

## 河北 将弥

KPMGアソシエイトパートナーとして東京大学の松尾研究室に出向し、AI×Security領域にて市場動向調査・政府機関との推進を実施



コンサルティング&ソリューション事業統括本部 ゼロトラスト推進事業部長

## 江口 真

NTT研究所、Zscaler IncのTACマネージャー、Illumio社のプリンシパルを歴任し、ゼロトラスト領域とマイクロセグメンテーション領域に強みを有する



コンサルティング&ソリューション事業統括本部 プリンシパル

## 渡辺 英治

EMC/RSAの後にシスコシステムズ（Splunk Inc）では、Professional Service部門を責任者として立ち上げ、SIEMやログ監視に強みを有する



コンサルティング&ソリューション事業統括本部 Sec for AI推進事業部長

## 河太 優治

中央省庁に約20年間従事し、楽天㈱ではAIガバナンス部門長に就任し、AIガバナンス及びIncident対応に強みを有する

Copyright(C)2026 AIセキュリティ株式会社

Confidential

# 直近3週間で実際に起きたこと

**2026年9月末からの3週間で、委託先・クラウド基盤・会員向けAPIを入口とする漏えいと事業停止が相次ぎました。**
**共通点は「入口が自社の外側にある」こと。侵入を前提に、組織が動けるかが問われています。**

起きたこと（9/28〜10/19）

| | | |
|---|---|---|
| 10/7 | クラウド基盤への攻撃 | IDCフロンティアのクラウドへの攻撃が495の企業・自治体に波及。復元は顧客自身のバックアップからのみ |
| 10月 | 委託先端末の感染 | 第一興商：委託先端末の感染で約872万件のおそれ。大和証券：委託先FAQシステムへの不正ログインで約11万人分 |
| 10月 | 会員アプリ・APIの不備 | 焼肉きんぐ約1,078万件、バーガーキング約1,118万件、ソースネクスト最大約2,252万件の漏えいが相次ぐ |
| 10月 | 事業停止まで波及 | 日水物流は入出荷が停止、丸木医科器械は基幹システムが全面停止、大阪公立大学は全授業休講 |
| 9/25→10/2 | 市場の反応 | パーク24は不正アクセス公表後、株価が−12.0%。集団訴訟の参加表明は2,000人超と報道 |

机上演習で備える3つの状況

**入口は委託先・クラウド基盤**
自社が直接管理しないシステムが入口。委託先との連携と復旧の優先順位を、演習で確かめる

**大量の会員情報が流出**
本人通知・広報初動・問い合わせ対応が同時に発生。広報・法務・事業部門の動きを検証する

**事業が止まる**
出荷停止・授業休講など事業影響が先に出る。業務停止と復旧の判断を迫られる場面を付与する

出典：IDCフロンティア公表（2026/10/9）、各社公表の集計「セキュリティ対策Lab」「テリアブログ」（2026/10/16時点）。件数は公表時点の最大値・漏えいのおそれを含みます。

Copyright(C)2026 AIセキュリティ株式会社

# AIツールによる攻撃の自動化と同時多発化

**2026年秋、AIで侵入テストを自動化するツール「ARTEX」の悪用が疑われる攻撃が、韓国・日本で報告されました。**
**「少人数が、多数の組織を同時に狙う」段階に入っています。**

ARTEX とは

## AIと連携して侵入テストを自動化する

**開発元**

中国で開発されたと報道

**仕組み**

大規模言語モデル（LLM）と連携し、偵察～侵入の一部を自動化

**現状**

開発者は公開を停止。配布済みのコードは回収が難しいとされる




**韓国**

### 16社・約10万件

2026年9月下旬以降、金融機関の周辺業務システムに不正アクセス（10/14 当局発表）

**日本**

### 約20社が標的

GMOサイバーセキュリティ by イエラエが攻撃基盤で確認。うち8社が9～10月に漏えいを公表

### 当社の見立て

**01 攻撃の「量」が変わる**

偵察から侵入までが自動化され、少人数でも多数の組織を同時に狙える

**02 狙われるのは周辺システム**

基幹ではなく、外部とつながる業務支援システムの認証・権限の不備が突かれる

**03 差がつくのは初動**

防御を完全にはできない以上、検知から遮断・報告・公表判断までの速さが被害を左右する

出典：ビジネス+IT（2026/10）、GMOサイバーセキュリティ by イエラエ報告（2026/10/19・報道経由）。調査は継続中。「当社の見立て」は当社の整理です。

Copyright(C)2026 AIセキュリティ株式会社

# インシデント発生後の対応比較

**事業や顧客に大きな影響が出た2つの事案を、公表情報に基づき時系列で並べました。**

**初動・業務継続・情報開示の進め方は企業によって異なり、公表後の株価の動きにも違いが見られます。**

| | アサヒグループHD<br>2025年9月・ランサムウェア | | パーク24「タイムズカー」<br>2026年9月・不正アクセス |
|---|---|---|---|
| 検知と遮断 | 9/29 7時ごろ暗号化を確認、11時にネットワークを遮断 | | 9/25〜9/26 不正アクセスを検知し調査開始、翌日に侵入経路を閉鎖 |
| 公表 | 9/29〜10/8 第1報〜第3報。ランサムウェアと流出の疑いを公表 | | 9/28〜9/29 第2報で約660万アカウント、第3報で本人確認書類画像 約160万件 |
| 事業継続・復旧 | 10/1〜10/2 紙・FAXで手作業の出荷再開、ビール全6工場で製造再開 | | 10/16 免許証画像の保有方針を変更。SNSでは「証拠隠滅」との声も（報道） |
| その後の説明 | 11/27 社長会見。身代金は支払っていないと説明 | | 10/23 第4報で漏えい項目の個別案内時期を延期。集団訴訟の参加表明は2,000人超と報道 |
| | 公表後の株価<br>**約−3% → 約−8%**<br>9/26終値1,839円 → 一時1,782.5円（9/29）→ 1,696円（10/16） | | 公表後の株価<br>**−12.0%**<br>9/25 → 10/2。10/2は約4か月ぶりの安値 |

出典：アサヒグループHD 公表資料・会見、パーク24 公表（第2〜4報）、ITmedia @IT。株価は報道・分析記事。株価は地合い等の要因も含み、対応との因果を示すものではありません。

Copyright(C)2026 AIセキュリティ株式会社

# ガイドラインが求める「実践的な演習」

**経済産業省・金融庁・IPAの文書は、体制の整備にとどまらず「演習の実施」と「結果を踏まえた改善」を求めています。**
**机上演習は、その要請に最も低コストで応えられる手段です。**

経済産業省・IPA

**サイバーセキュリティ経営ガイドライン Ver3.0**

指示7

**「演習を実施せよ」**

インシデント発生時の緊急対応体制を整備し、適宜実践的な演習を実施する。「演習を行っていない」ことが想定課題として明示

金融庁

**金融分野におけるサイバーセキュリティに関するガイドライン**

2.2.5

**「定期的に訓練し、結果を把握せよ」**

定期的な演習・訓練を実施し、業務部門の責任者も関与して結果を把握する。顧客に深刻な影響を与える現実的なシナリオを含める

IPA

**セキュリティインシデント対応 机上演習教材（2025年4月）**

公開教材

**「机上演習を標準の取り組みに」**

中小企業・医療機関向けの演習教材と実施マニュアルを無償公開。座学＋グループ討議の2部構成を推奨

**体制図とマニュアルを「整備した」だけでは、ガイドラインの要請にも、実際のインシデントにも応えられません。**
演習で検証し、課題を改善に回すサイクルまでが求められています。

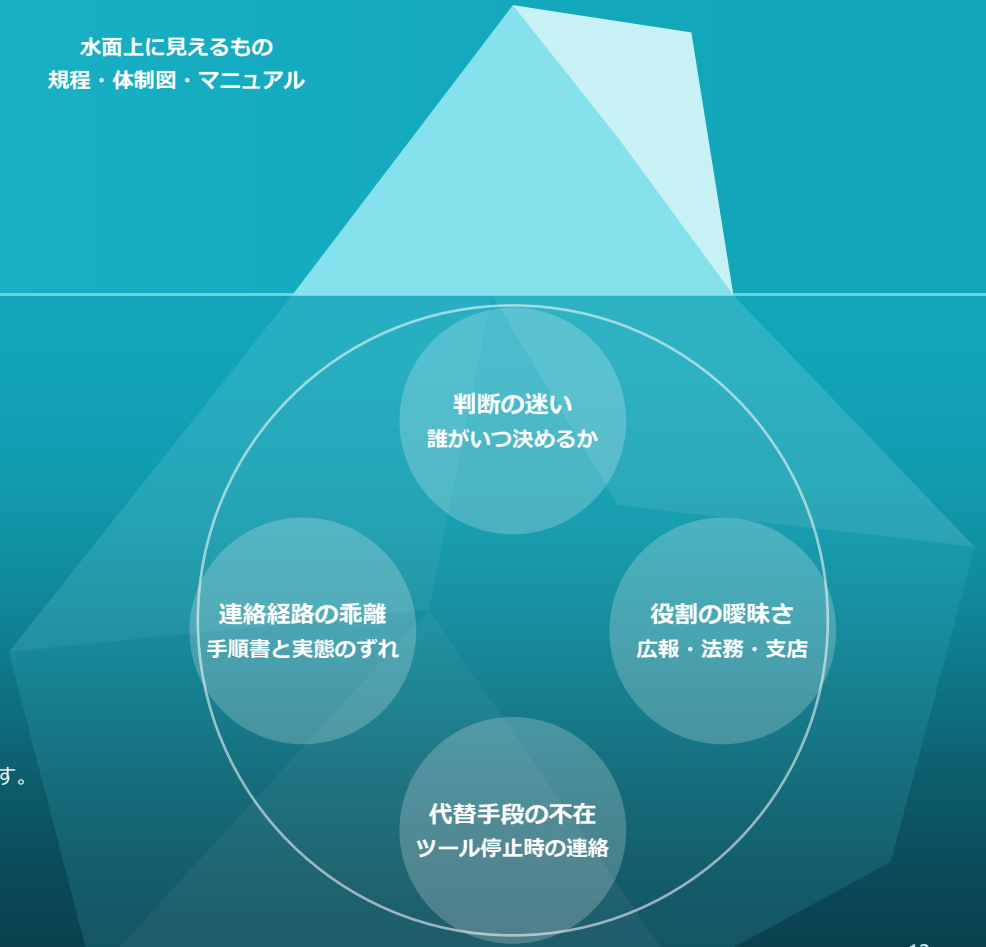
出典：経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver3.0」／金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」（2024年10月）／IPA 机上演習教材（2025年4月）

Copyright(C)2026 AIセキュリティ株式会社

# 文書は整っていても、「動けない理由」は水面下に隠れています

規程・体制図・マニュアルは外から見える成果です。
しかし有事に組織を止めるのは、
文書に書かれていない水面下の要因です。

机上演習は、水面下の要因を
安全に・半日で表に出し、
改善の優先順位を決める手段です。




Copyright(C)2026 AIセキュリティ株式会社

# 机上演習は、整備した手順書を「動くもの」に変える最短の方法です。

**ランサムウェア感染などのシナリオを時系列で付与し、
各部門が「そのとき何をするか」を議論しながら進めます。
システムを止めず、半日で組織の対応力を検証できます。**

### 01 手順の理解と習熟

インシデント対応マニュアル・行動手順書に沿って動けるかを確認し、記載の粒度不足や実態との乖離を洗い出します。

### 02 組織間連携の検証

CSIRT・情シス・広報・法務・総務の情報連携と意思決定（遮断判断、公表判断など）の流れを検証します。

### 03 意識向上と役割理解

参加者が自部門の役割を実感し、「有事に誰が何をするか」が組織に浸透します。

Copyright(C)2026 AIセキュリティ株式会社

SERVICE OVERVIEW —— 全体像

# 準備から改善まで、当社が一気通貫で担います。

APPROACH ／ SCOPE

## 『シナリオ開示型 机上演習』

### 部門横断の判断を付与し、改善まで伴走する。

Test today, Improve tomorrow

MENU —— 提供する8つの支援

- 標準5シナリオからの選択・調整
- 事前説明会・事務局支援
- 演習当日のファシリテーション
- アンケート分析・訓練結果報告書
- 課題整理（5カテゴリ）・改善方針
- マニュアル・行動手順書の改訂
- 翌年度の訓練計画・ロードマップ
- 最終報告会・フォローアップ




外周＝演習に参加する部門 ／ 内周＝当社が担う4工程

Copyright(C)2026 AIセキュリティ株式会社

# シナリオ開示型ウォークスルー演習の流れ

**検知から事後対応までの一連のプロセスを、7つのフェーズで時系列に付与します。**
**各フェーズで「自部門は何をするか」を議論し、行動記録表に残していきます。**




## 参加する部門と演習で問われること ―― 当社ファシリテーターが状況を付与して進行します。システムには一切触れません

**IT部門**
システム停止・復旧手順の判断

**CSIRT**
技術的封じ込めと復旧の指揮

**広報**
対外発信の要否・タイミング

**法務・総務**
外部弁護士・警察との連携

**事業部門**
顧客対応と代替運用の判断

Copyright(C)2026 AIセキュリティ株式会社

# 選べる5つの標準シナリオ × 業界別の想定

**当社が用意した5つの脅威シナリオから1つを選び、9つの変数の範囲で貴社の環境に合わせて調整します。**

**業界ごとに「何が止まり、何が漏れるか」をあらかじめ想定しているため、短期間・定額で「貴社の演習」になります。**

| 脅威シナリオ | 金融 | 製造 | 小売・サービス | 医療・公共 | IT・SaaS |
|---|---|---|---|---|---|
| 01 **ランサムウェア感染**<br>保守用VPNの脆弱性から侵入、基幹が暗号化 | 事務・周辺システムの停止 | **工場停止・出荷遅延** | POS・ECの停止 | **電子カルテ・窓口業務の停止** | 提供サービスの停止 |
| 02 **委託先・クラウド基盤経由の侵害**<br>委託先端末・共用クラウドへの攻撃で自社データが流出 | **委託先からの顧客情報流出** | **設計データ・図面の流出** | 会員基盤の流出 | 委託業者経由の住民・患者情報流出 | 他テナントへの波及 |
| 03 **会員アプリ・APIからの大量漏えい**<br>アプリの仕様不備を突かれ会員情報が流出 | **口座・本人確認書類の流出** | 取引先ポータルの流出 | **会員・決済情報の流出** | 予約・申請システムの流出 | API悪用による大量取得 |
| 04 **標的型メール・アカウント乗っ取り**<br>従業員アカウントが乗っ取られ業務システムに不正ログイン | **送金指示の詐取** | **取引先なりすましの請求** | 本部アカウントの乗っ取り | 職員アカウントの悪用 | 管理者権限の奪取 |
| 05 **公開サーバーの侵害・改ざん**<br>AIで自動探索された脆弱性から公開システムに侵入 | ネットバンキング周辺の侵入 | リモート保守口からの侵入 | **ECサイトの改ざん** | Webサイトの改ざん・停止 | **公開APIサーバーからの侵入** |

**色付き＝想定の多い組み合わせ**

※ 調整できる変数：侵害方法／侵入経路／被害内容／部門名／サービス名／システム名／連絡経路・方法／判断者／委託先（ご契約前に確定）。これ以外のご要望は個別にお見積りします。

Copyright(C)2026 AIセキュリティ株式会社

Confidential

# 演習当日の風景

**貴社オフィスの会議室に各部門が集まり、画面に付与される状況に対して議論し、記録しながら進めます。**
**ファシリテーターが各席の判断を全体に共有し、論点を整理していきます。**



### 部門をまたいで、その場で判断する

遮断・業務停止・公表といった判断を、その場で参加部門に求めます。
報告を待つのではなく、限られた情報で決める難しさを各部門が体験します。

### 部門席ごとに議論し、記録する

CSIRT・情シス・広報・法務・総務・事業部門が席に分かれ、自部門の動きを議論します。各フェーズの判断は行動記録表に残し、手順書との差分を洗い出す素材にします。

### ファシリテーターが全体を進める

当社が画面に状況を付与し、各席の判断を全体に共有しながら進行します。
部門間で判断が食い違った点は、その場で論点として整理し課題に変えます。

※ 写真はイメージです。演習は貴社の関係者を招集するため、貴社オフィスの会議室での対面実施をお願いしています（オンライン実施は対象外）。

Copyright(C)2026 AIセキュリティ株式会社

Confidential

AI Security

# 訓練手法の中での位置づけ

**座学研修と実機演習の間にある「机上演習」は、全社の判断と連携を検証できる唯一の手法です。**
**当社は、構築支援の実績をもとに準備から改善までを一気通貫で担います。**

| 観点 | 座学研修・eラーニング | 公開教材での自主演習 | 机上演習（当社） | 実機演習・レッドチーム |
|---|---|---|---|---|
| **検証できる範囲** | 知識の習得 | 基本的な対応の流れ | **全社の判断・連携・手順書** | 技術的な検知・対処 |
| **部門横断の参加** | △ | △ | ◎ **IT・業務部門まで参加** | — |
| **貴社シナリオへの適合** | — | ○ 教材の範囲で調整 | ◎ 標準5シナリオを貴社環境に調整 | ◎ |
| **準備の負荷（貴社側）** | 小 | 大（自前で運営） | **小（当社が運営）** | 大 |
| **システムへの影響** | なし | なし | **なし** | あり（本番影響の考慮） |
| **改善への接続** | — | △ | ◎ 課題整理・手順書改訂 | ○ 技術面のみ |

### 構築支援の実績

CSIRT構築～全社演習～改善まで支援した進め方を、5つの標準シナリオとして標準化

### 部門をまたぐ判断まで踏み込む

遮断・公表・支払いの判断をシナリオに組み込み、各部門が自ら決める場面をつくる

### 改善の「実装」まで担える

手順書改訂や翌年度計画に加え、必要に応じてセキュリティ人材の供給で実行を支援

Copyright(C)2026 AIセキュリティ株式会社

# 参加する部門で選ぶ、3つの定額パック

**価格は「どの部門まで演習に参加するか」で決まります。机上演習はいずれも1回（半日・貴社オフィス）。**
**上位パックほど参加部門が広がり、演習後の課題整理・改善の成果物も増えます。**

## LIGHT　2ヶ月

演習実施パック

**300万円** 税別・期間定額

**セキュリティ部門で、まず1回**

参加部門

- セキュリティ部門（CSIRT）

主な成果物

シナリオ／行動記録表／訓練結果報告書（簡易版）

## STANDARD　3ヶ月

演習＋課題整理パック

**500万円** 税別・期間定額

**IT部門と連携して動けるかを確かめる**

参加部門

- セキュリティ部門（CSIRT）
- ＋ IT部門（情シス・インフラ・運用）

主な成果物

＋ 課題一覧（5カテゴリ）／改善方針／報告会

## PREMIUM　5ヶ月

演習＋改善定着パック

**950万円** 税別・期間定額

**業務部門まで含めて検証し、定着させる**

参加部門

- セキュリティ部門（CSIRT）
- ＋ IT部門（情シス・インフラ・運用）
- ＋ 業務部門（広報・法務・総務・事業部門）

主な成果物

＋ 改訂版マニュアル・手順書／翌年度の訓練計画

**価格は参加部門の範囲で決まります。上位パックほど、演習後の課題整理・改善の範囲が広がります。**
個別要件（複数拠点での開催、追加シナリオ、英語対応など）は個別にお見積りします。

Copyright(C)2026 AIセキュリティ株式会社

Confidential

AI Security

# パック別の提供内容

**提供内容の違いを一覧にしました。**

**◎は標準提供、○は範囲を限定して提供、△はオプション、ーは対象外です。**

| | LIGHT 300万円 | STANDARD 500万円 | PREMIUM 950万円 |
|---|---|---|---|
| **期間** | 2ヶ月 | 3ヶ月 | 5ヶ月 |
| **シナリオ** | 標準5シナリオから選択・調整 | 選択＋貴社環境に合わせ作り込み | 選択＋貴社環境に合わせ作り込み |
| **机上演習の実施** | 1回（半日・貴社オフィス） | 1回（半日・貴社オフィス） | 1回（半日・貴社オフィス） |
| **参加部門** | セキュリティ部門（CSIRT） | ＋IT部門（情シス・インフラ・運用） | ＋業務部門（広報・法務・事業） |
| **事前説明会・判断場面の付与** | ー | ◎ | ◎ |
| **アンケート・訓練結果報告書** | ○ 簡易版 | ◎ | ◎ |
| **課題整理（5カテゴリ）・改善方針** | ー | ◎ | ◎ |
| **全社マニュアル・行動手順書の改訂** | ー | ー | ◎ CSIRT所管の全社版が対象 |
| **改善策の実装支援** | ー | ー | ◎ 連絡経路・判断基準・報告様式 |
| **翌年度の訓練計画・ロードマップ** | ー | △ | ◎ |
| **最終報告会** | ○ 報告書の送付・説明 | ◎ **参加部門向け報告会** | ◎ **報告会＋フォローアップ会** |

※ 価格は参加部門の範囲で決まります。各事業部が個別に保有するマニュアル・行動手順書は改訂の対象外です。参加部門・拠点数は協議のうえ調整します。

Copyright(C)2026 AIセキュリティ株式会社

# LIGHT 演習実施パック 2ヶ月

## まずセキュリティ部門で、
## 机上演習を確実に実施する。

**標準5シナリオから1つを選び、貴社の構成に合わせて調整。**
**半日の演習と簡易報告書までを2ヶ月・定額でご提供します。**

### 想定するお客様

- 初めて机上演習を実施する
- セキュリティ部門（CSIRT）で実施したい
- マニュアル・手順書の「初動」を確かめたい
- まずは年度内に実績をつくりたい

### 標準提供内容

- 標準5シナリオから1つを選択し、貴社の構成に合わせて調整
- 半日（約3時間）の机上演習を1回実施（貴社オフィス）
- 参加はセキュリティ部門（CSIRT）を想定
- 演習当日のファシリテーション
- アンケート集計と訓練結果報告書（簡易版）

### 2ヶ月の進め方

**1ヶ月目：準備**
シナリオ選択・ヒアリング・調整・参加者確定

↓

**2ヶ月目：机上演習（半日・1回）**
貴社オフィスで当社ファシリテーターが進行

↓

**2ヶ月目：報告**
アンケート集計・訓練結果報告書（簡易版）

**想定成果物**
シナリオ／行動記録表／訓練結果報告書

Copyright(C)2026 AIセキュリティ株式会社

STANDARD **演習＋課題整理パック** 3ヶ月

# IT部門と連携して動き、課題を5つの観点で可視化する。

**セキュリティ部門とIT部門が参加する7フェーズのシナリオで遮断・復旧の連携と判断を検証し、課題と改善方針を提示します。**

### 想定するお客様

- 部門横断の連携を検証したい
- IT部門（情シス・インフラ・運用）にも参加してほしい
- 遮断・復旧の判断を部門をまたいで確かめたい
- 検出した課題を翌年度の計画に反映したい

### 標準提供内容

- 標準5シナリオから選択し、貴社の事業・システム構成に合わせて作り込み
- 事前説明会＋半日の机上演習1回（貴社オフィス）
- セキュリティ部門・IT部門が参加し、遮断・復旧の判断場面を付与
- アンケート分析と課題の5カテゴリ整理・改善方針
- 最終報告会（参加部門向け）

### 3ヶ月の進め方

**1ヶ月目：準備**
シナリオ選択・貴社向け作り込み・事前説明会

↓

**2ヶ月目：机上演習（半日・1回）**
遮断・復旧の判断場面を付与

↓

**3ヶ月目：課題整理・報告会**
5カテゴリ整理・改善方針・報告会

**想定成果物**
シナリオ／報告書／課題一覧・改善方針

Copyright(C)2026 AIセキュリティ株式会社

# PREMIUM 演習＋改善定着パック 5ヶ月

## 演習で終わらせず、
## 改善を定着させる。

**業務部門まで参加する演習と課題整理に加え、全社マニュアル・行動手順書の改訂、翌年度の訓練計画までを5ヶ月でご支援します。**

### 想定するお客様

- 検出した課題を確実に手順書へ反映したい
- 連絡経路・判断基準・報告様式を整備し切りたい
- 広報・法務・事業部門まで巻き込みたい
- 翌年度の訓練を継続運用に乗せたい

### 標準提供内容

- STANDARDの全内容＋業務部門（広報・法務・総務・事業部門）の参加
- 全社マニュアル・行動手順書の改訂（CSIRT所管）
- 改善策の実装支援（連絡経路・判断基準・報告様式）
- 翌年度の訓練計画・改善ロードマップ
- 改善後のフォローアップ会
- グループ会社・拠点の参加対応

### 5ヶ月の進め方

**1〜3ヶ月目：演習と課題整理**
業務部門まで参加し、年度内に課題整理まで完了

↓

**4ヶ月目：改訂・実装支援**
全社マニュアル・手順書改訂、連絡経路・報告様式

↓

**5ヶ月目：定着・翌年度計画**
翌年度訓練計画・ロードマップ・フォローアップ会

**想定成果物**
改訂版マニュアル・手順書／訓練計画

Copyright(C)2026 AIセキュリティ株式会社

# パック別の実施スケジュール

**準備・演習・報告の骨格は共通で、LIGHTとSTANDARDは年度内（3月末）に完結します。**
**PREMIUMは年度内に演習と課題整理を終え、4〜5月で改善の定着までを行います。**




※ LIGHTは2月開始の例です。開始月は1月上旬〜2月上旬の範囲で協議して確定します。PREMIUMは年度をまたぐため、年度内の検収範囲は協議して確定します。

Copyright(C)2026 AIセキュリティ株式会社

# パック別の想定成果物

**演習の記録だけでなく、翌年度の改善につながる文書を残します。**
**STANDARDは課題整理まで、PREMIUMは改善の実装まで成果物に含まれます。**

LIGHT以上

### インシデントシナリオ

選択した標準シナリオを貴社向けに調整したファシリテート資料。各フェーズの各部門のセリフまで明記

LIGHT以上

### 行動記録表

各部門が各フェーズで取った行動・判断を記録。手順書との差分の素材になる

LIGHT以上

### 訓練結果報告書

アンケート結果（有意義度・理解度・難易度等）と総評、気づきの一覧

STANDARD以上

### 課題一覧・改善方針

検出課題を「役割／権限・プロセス／手順・情報共有・ステークホルダー対応・訓練／教育」の5カテゴリで整理

PREMIUM

### 改訂版 全社マニュアル・行動手順書

CSIRT所管の全社インシデント対応マニュアル・行動手順書を、実態に合わせて改訂

PREMIUM

### 翌年度 訓練計画・改善ロードマップ

検出課題の主管部門・時期を定め、次年度の訓練テーマまで計画

※ 成果物は準委任契約における想定成果物です。様式・粒度は協議して確定します。各事業部固有のマニュアル・行動手順書は対象外です。

Copyright(C)2026 AIセキュリティ株式会社

# 机上演習のご支援実績

**不動産・金融・製造・小売・公共など、9社で机上演習をご支援してきました。**

**業務部門まで参加する全社規模から、CSIRT中心の少人数まで、同じ骨格で実施しています。**

**01 不動産デベロッパー** ランサムウェア感染
各事業部の責任者を含む全社規模。課題を5カテゴリに整理し改善方針を提示

**02 地方銀行** 委託先経由の侵害
委託先FAQシステム経由の不正アクセスを想定。当局報告と顧客説明の判断を検証

**03 生命保険** 標的型メール・乗っ取り
人事システムへの不正ログインを想定。公表判断と広報初動を演習

**04 自動車部品メーカー** ランサムウェア感染
基幹システム停止による出荷停止を想定。事業部門の代替運用判断を検証

**05 食品物流** 委託先経由の侵害
委託先データセンターへの攻撃を想定。入出荷停止時の取引先連絡を演習

**06 小売チェーン** 会員アプリ・API漏えい
会員情報の大量漏えいを想定。本人通知・問い合わせ対応・SNS対応を検証

**07 ECサービス** 会員アプリ・API漏えい
仕様不備による漏えいを想定。サービス停止判断と広報・法務の連携を演習

**08 大学法人** ランサムウェア感染
全授業休講となる事態を想定。学生・保護者への説明と復旧優先順位を検証

**09 医療機器商社** 情報持ち出し（個別）
退職予定者による持ち出しを想定。証拠保全・法務対応・警察連携を演習

**いずれも「演習の実施」で終わらせず、検出した課題を5カテゴリに整理し、主管部門と改善方針を定めるところまでご支援しています。**

※ 業種・内容は守秘のため一部を抽象化しています。

Copyright(C)2026 AIセキュリティ株式会社

# ご契約前の確認事項

**演習を確実に実施し、効果を出すために、ご契約前に以下の6点を確認させていただきます。**
**パッケージの範囲で実現できないご要望は、個別にお見積りします。**

### 01 既存マニュアル・手順書の確認

演習は、既存の手順書の実効性を確かめるものです。手順書がなければ検証できないため、ご契約前に内容を拝見し、整備状況を確認します。

### 02 シナリオの調整範囲

標準5シナリオから選択します。調整は侵害方法・侵入経路・被害内容・部門名・サービス名・システム名・連絡経路・判断者・委託先の9変数に限り、事前に確定します。

### 03 会場の確保

大人数が入れる貴社オフィスの会議室での実施が前提です。確保が難しく外部会場を借りる場合、会場費は実費でご請求します。

### 04 複数拠点の接続

拠点はTeams等のWeb会議で接続できます。音声が聞き取りにくい等の品質は会場設備に依存するため、機材は貴社でご準備ください。

### 05 参加者の日程調整

各部門のご担当者の日程確保には時間がかかります。ご契約手続きと並行して、早めに調整を始めてください。

### 06 パッケージ外のご要望

特別対応は原則お受けしていません。パッケージで実現できないご要望は、内容を伺ったうえで個別にお見積りします。

Copyright(C)2026 AIセキュリティ株式会社

# ご提供の前提条件

**価格・期間・提供範囲を定額で固定するための前提条件です。**
**条件に合わない場合も、内容を調整したうえでお見積りします。**

| | |
|---|---|
| **期間** | LIGHT 2ヶ月／STANDARD 3ヶ月／PREMIUM 5ヶ月（キックオフは1月上旬～2月上旬を想定） |
| **お申込み期限** | 2026年12月中旬まで（準備期間を確保するため） |
| **契約形態** | 準委任契約。成果物は想定成果物として提示。PREMIUMの年度内検収範囲は協議して確定 |
| **価格** | 各パックの定額（税別）。交通費、外部会場を利用する場合の会場費は実費でご請求します |
| **実施形式** | 対面のみ。貴社オフィスの会議室で実施。複数拠点はWeb会議で接続可（音声品質は会場設備に依存） |
| **シナリオ** | 当社の標準5シナリオから1つを選択。調整は9つの変数の範囲に限り、ご契約前に確定します |
| **前提資料** | 全社インシデント対応マニュアル・行動手順書が整備されていること（ご契約前に内容を確認） |
| **対象外** | 各事業部固有のマニュアル・行動手順書の改訂、実機操作を伴う技術演習、セキュリティ製品の導入・設定 |

**パッケージで実現できないご要望（特別対応）は原則お受けせず、個別にお見積りします。**

Copyright(C)2026 AIセキュリティ株式会社

Confidential

# 年度内の実施に向けて、
# 12月中のパック・シナリオ選定をおすすめします。

**まずは30分のオンライン打合せで、体制と文書の整備状況を**
**お聞かせください。最適なパックとシナリオをご提案します。**

### 01 ヒアリング（30分）

体制・文書の整備状況、参加を想定する部門、ご予算感を確認

### 02 パック・シナリオ選定

3パックと5つの標準シナリオから選定し、正式お見積りを提示

### 03 12月中のご発注

ご契約手続きと並行して、各部門の日程と会議室の確保を開始

Copyright(C)2026 AIセキュリティ株式会社