3分でわかる Securiy

AIのサイバー攻撃には、AIで守る。

攻撃する側がAIを使う今、年1回の点検では間に合いません。Securiyは、AIによる毎月の脆弱性診断・ペネトレーションテストと、毎朝の社員アカウントの点検で、情報漏洩の入り口の抜けを見つけて直します。

いま対策が必要な理由

攻撃する側もAIを使い、守る入り口は増えている。

入り口が増えるほど、一度の抜けが取引先にも広がります。

78%

日本でAIを使う人のうち、会社が用意していない自前のAIツールを仕事に持ち込んでいる割合

出典：Microsoft・LinkedIn「2024 Work Trend Index」日本の結果（2024年5月）

98.6%

パスワードが漏れていても、2段階認証で減らせる乗っ取りのリスク

出典：Meyerほか（Microsoft）2023年、arXiv:2305.00945。漏えいしたアカウントでのリスク低減率

約7割

被害にあった中小企業のうち、取引先にも影響が出た割合

出典：IPA「2024年度 中小企業における情報セキュリティ対策の実態調査」（2025年5月、4,191社が回答）

どれも公的機関や調査会社の公表値です。Securiyの実績の数字ではありません。

困りごと

こんな困りごとはありませんか

退職した人のアカウントが残っていないか不安

人事名簿と照合して、有効なままの退職者アカウントを見つけます

Securiy ID　7ページへ

社員のパスワードが漏れていないか知りたい

社員のメールアドレスを、公開されている漏えいデータと毎朝照合します。2段階認証の未設定も見つかります

Securiy ID　7ページへ

年1〜2回の脆弱性診断・ペネトレーションテストで足りているか不安

AIが毎月攻撃を試し、新しく見つかった弱点にも早く気づけます

脆弱性診断・ペネトレーションテスト　5ページへ

取引先のセキュリティチェックシートに答える材料がほしい

2段階認証の実施率や毎月の診断結果を、チェックシートに書ける形で毎月残します

月次レポート　8ページへ

Securiy とは

入り口の抜けを、AIで見つけて、直して、確かめる。

01 自社のサービスと社内ネットワーク

脆弱性診断・ペネトレーションテスト

AIが毎月、攻撃を試す。直し方と、直ったかの再テストまで届けます。

5ページへ

02 社員のアカウント

Securiy ID

7ページへ

03 攻撃の見張り

自動防御AIエージェント

権限は段階的に設定

あわせて AIの使い方

AI利用の安全設計

11ページへ

サービス1 · 脆弱性診断・ペネトレーションテスト

その対策で、本当に攻撃を止められるかを試す。

整えた対策で攻撃を防げるかを、合意したシナリオで実際に攻撃して確かめます。

AIの利用環境

プロンプトインジェクション・情報の持ち出し

文書やメールに埋め込んだ指示、許可していないMCP、AI経由で人より広く読める状態。

社員のアカウント

乗っ取り・権限昇格

漏えいしたパスワード、弱い2段階認証、権限の強い外部アプリを使った侵入。

社内ネットワーク

入口から重要な情報までの経路

社内ネットワークを別の環境に再現し、入口から重要な情報までの経路を試します。

自社サービス

業務に沿った攻撃

顧客データの持ち出し、権限の乗っ取り。直すところまでは開発チーム向けで。

テスト報告

表示は例です

共有ファイルに埋め込んだ指示で、AIに社外へ送信させる AI環境・一般データ	止まった
一般社員の権限で、社外秘フォルダをAIに要約させる AI環境・社外秘	通った
漏えいしたパスワードで、2段階認証なしのIDに入る アカウント	止まった
他人の注文IDで注文情報を取得する 自社サービス	範囲外

止まった・通った・範囲外を分け、確かめられなかったことも書きます。

サービス1 · 脆弱性診断・ペネトレーションテスト

相談から再テストまで、5つの段階で進める。

01

範囲を決める

30分の相談で、期間・対象・やらないことを先に決めてから見積ります。

02

書面で合意する

対象・期間・方法を書面で合意します。本番は個別に合意した場合だけです。

03

攻撃して試す

合意したシナリオで攻撃します。見つけた認証情報でログインはしません。

04

分けて報告する

止まった・通った・範囲外を分け、確かめられなかったことも書きます。

05

直したら再テスト

直したあとに、同じ方法でもう一度試します。

- 単発でも毎月でも選べます。年1回の診断の間の月を埋める使い方もできます
- 標準ではテスト環境で行います。本番環境には予告なしに攻撃しません
- 今の診断会社はそのままで、併用できます
- 自社サービスの脆弱性を直す修正PRと再テストは、開発チーム向けで承ります

サービス2 · Securiy ID · 提供中

つなぐだけで、乗っ取りの入り口が毎朝そろう。

Google Workspace か Microsoft 365 の管理者が、読み取りの権限を許可するだけ。2段階認証の未設定、パスワードの漏えい、休眠・退職者のアカウントを毎朝8:30に見つけます。

- ID・パスワードは預かりません。端末には何も入れません
- 漏えい監視も基本料金に込みです
- 共有・社外・システムの ID は数えません



サービス2 · Securiy ID · 直すのは本人

本人に直してもらい、結果は毎月の記録に残る。

no-reply@securiy.ai → 佐藤さん

【対応のお願い】2段階認証の設定をお願いします（5分）

あなたのアカウントで2段階認証が設定されていません。パスワードが漏れると、そのままログインされてしまいます。

表示は例です。このメールにはログイン用のリンクは含まれていません。

- 返事がなければ3日後・7日後に再送します。直ったものは一覧から消えます
- 退職者の残ったアカウントは、管理者に知らせます
- 2段階認証の実施率などを、取引先のチェックシートに書ける形で毎月残します

提供時期

提供中
毎朝のチェック、2段階認証、休眠・未ログイン、漏えいの照合、本人への依頼と再送、人事名簿との照合、操作の記録

2026年11月
Slack通知、月次レポートの自動送付

2026年12月
止める操作、外部アプリとAIに渡した権限の一覧

2027年1〜3月
Microsoft Teams通知ほか

提供状況は2026年10月30日時点です。

Securiy ID · 導入の流れ

許可したその日に、件数が分かる。

01 · 許可した日

管理者が許可する

「Google Workspaceで試す」か「Microsoft 365で試す」からログインし、読み取りの権限をOAuthで許可します。

02 · その日のうち

件数が分かる

2段階認証の未設定と、パスワードの漏えいの件数が分かります。

03 · 翌朝8:30から

毎朝確かめる

翌朝からは毎朝8:30に、アカウントの状態を確かめます。

04 · 見つかったとき

本人に直してもらう

見つかった社員に、手順つきの依頼を送ります。

使い始める前に確かめること

必要な管理者	Google Workspaceは特権管理者、Microsoft 365はグローバル管理者が最初の許可をします。許可したあとは、ふだんの確認は一般の管理者でもできます。
いまの設定	SSOと2段階認証はそのままです。連携のために外す必要はありません。
Microsoft 365	最終サインイン日時など一部の情報の取得には、Entra ID P1が必要です。P1がない場合はその項目を「取得できません」と表示し、ほかの確認は続けます。
社員への連絡	導入すること、確認する情報の種類と目的を、利用企業から社員へ事前に伝えていただきます（利用規約）。

Securiy ID · 使う権限の一覧

機能ごとに、必要な権限だけを使う。

使わない機能の権限は求めません。書き込みの権限は、停止などの操作を使う場合にだけ、別途同意をいただきます。

機能	Google Workspace	Microsoft 365	種類
社員の一覧・管理者・2段階認証・最終ログイン	admin.directory.user.readonly	User.Read.All・UserAuthenticationMethod.Read.All・AuditLog.Read.All・RoleManagement.Read.Directory	読み取り
組織で2段階認証を強制しているか	上と同じ	Policy.Read.All	読み取り
パスワードの最終変更日	admin.reports.audit.readonly	User.Read.All	読み取り
休眠アカウントの判定（Entra ID P1がない場合の利用状況レポート）	なし	Reports.Read.All・ReportSettings.Read.All	読み取り
外部アプリへの許可	admin.directory.user.security Googleには読み取り専用の権限がないため、取り消しもできる権限を使います。当社は一覧の取得にだけ使います	Directory.Read.All・Application.Read.All	読み取りに限定して使用
セッション取り消し・停止（使う場合のみ）	別途同意	別途同意（User.RevokeSessions.All など）	書き込み

ログインには、ほかにopenid・email（Microsoft 365はoffline_access・User.Readも）を使います。2026年11月1日時点の実装と照合済みです。最新の一覧は **securiy.ai/trust/** で公開しています。

見ないもの：パスワード、メール本文、ファイルの中身、チャット、端末の中。やめるときは、Googleは「セキュリティ ＞ アクセスとデータ管理 ＞ APIの制御」、MicrosoftはEntra管理センターの「エンタープライズ アプリケーション」でSecuriyを削除します。

あわせて・AI利用の安全設計

AIを止めずに、データの置き場所を決める。

一律に禁止すると、社員が個人のアカウントで使い始め、会社から見えなくなることがあります。データを3段階に分け、使ってよいAIと設定を決めて組み、最後に疑似攻撃で確かめます。

最重要

外部のAIに入れない。使うなら社内で動くAIだけ

社外秘

会社契約で、学習に使われない設定のAIだけ

一般

会社が許可したAIなら使ってよい

4週間で一周

1週目
洗い出す

2週目
重要度を決める

3週目
組む

4週目
攻めて確かめる

料金（税抜）

Securiy IDは月¥10,000から。14日間、無料で試せる。

Securiy ID

スターター
月¥10,000
30 IDまで・31 ID目から1 IDにつき¥300

ビジネス
月¥20,000
30 IDまで・31 ID目から1 IDにつき¥600

ビジネスは、SSO・複数の管理者・監査ログが加わります。社員50人ならスターターで月¥16,000です。

1年契約（自動更新）・年払いが基本です。月払い・請求書払いはご相談ください。

脆弱性診断・ペネトレーションテスト

お見積り

範囲を決めて行うテストと、30日間予告せずに試す抜き打ちテスト。単発でも毎月でも、対象の数と規模に合わせて

開発チーム向け

お見積り

自社のサービスに攻撃して見つけ、修正PRを出し、直ったことまで確かめる。アプリ1つ・主な操作2つから

AI利用の安全設計

お見積り

初期の構築（データの分類、使うAIの選定、環境づくり、ルールのたたき台）と月次の見直し

1 ID＝有効な社員のアカウント1つ（停止中、共有・社外・システム用は数えません）。会社のドメインは1つまで込み、2〜3つは月 +¥6,000、4つ目から1つごとに月 +¥3,000。トライアル中に自動更新を止めれば料金はかかりません。

信頼とデータの扱い

約束することと、しないことを分けて伝える。

契約終了から
30 日以内に削除

貴社が取り扱う情報を AI モデルの学習に
学習に使わない

操作ログ
1年保存

第三者認証（SOC 2・ISO 27001）
未取得

約束すること

- 合意した範囲を、合意した方法で確かめます
- 見つけたことと、確かめられなかったことを分けて報告します
- 止める操作は、管理者の承認を得てから実行します
- 当社が管理するデータの漏えいに気づいたら、すぐにお知らせします

約束しないこと

- すべての攻撃を防げる、すべての問題を検知できるとは言いません
- 確かめた範囲の外まで安全だとは言いません
- 漏えいデータベースの網羅性は保証しません

契約の書類
利用規約、秘密保持契約（NDA）、データ処理契約（DPA）、テストの対象範囲合意書のひな形をお渡しできます。

サポート
平日10:00〜18:00、メールで1営業日以内に返信。緊急の漏えいは24時間以内に連絡します。

まずは、つないで
件数を見てください。

Securiy IDは14日間、無料で試せます。脆弱性診断・ペネトレーションテストとAIの使い方は、試す範囲を30分の相談で一緒に決めます。

14日間 無料で試す

30分無料相談