

【臨時公開資料】

自社の状況を把握し、必要な対策を検討するために — 今できることを整理した実践ガイド —

情報システム・IT管理者・Webサイト運営者向け

株式会社セキュアスカイ・テクノロジー

公開日:2026年10月13日

本資料を公開する目的

情報漏えいに関する報道が相次ぐなか、自社への影響に不安を感じている方も多いと思います。

「自社で何をすればよいかわからない」

「すでに攻撃を受けているのか、判断がつかない」

本資料は、こうした不安や悩みを少しでも解消し、自社のWebサイトの状況を把握するとともに、被害の防止・拡大防止に向けた行動につなげていただくことを目的としています。

該当する対象の方

- ・報道を見ても「自社は大丈夫だろう」と感じている方
- ・何から確認すればよいかわからない優先順位がわからない方
- ・社内や経営層を動かす材料がほしい方

本資料の位置づけ

- ・「これだけやれば大丈夫」ではありません
- ・「今できること」を整理し、行動のきっかけにするものです

1. Webサイトへの不正アクセスとその対策に特化した資料であること

報道されている不正アクセス事案では、公開されているWebサイトへの攻撃だけでなく、VPNや仮想化基盤が攻撃されたと思われるものやメール経由でマルウェアに感染したものなどが含まれています。本資料ではそれらのうちのWebサイトへの攻撃に焦点を当てています。

2. 基本的な指針であること

記載した対策を実施すれば安全性が保証されるものではありません。サイトの構成や運用状況に応じた継続的な確認・改善が必要です。

3. 単一のセキュリティ対策の限界

WAFは重要な防御手段ですが、すべての攻撃や情報漏えいを防げるわけではありません。また、ログ分析ツールでは、不審なアクセスが確認されても攻撃の成功や情報漏えいの発生を断定できず、異常が確認されなくても被害がないとは断定できません。サイトの構成や運用状況に応じた継続的な確認・改善および総合的な対策が必要です。

アジェンダ

1. 実践ガイド | 【最優先】被害の有無を確認する
2. 実践ガイド | 【次に行う】Webサイトの堅牢化
3. 参考資料 | クラウド型WAF「Scutum」の防御ログから見た直近の攻撃傾向

| 実践ガイド | 【最優先】被害の有無を確認する

まずは「すでに攻撃を受けていないか」を確認する

不正アクセスによる被害が頻発している現状では、まずは自分たちの保有しているWebサイトにおいて、すでに攻撃が行われていないかを確認してください。現時点では被害が発生していないと判断できれば、今後の被害を防ぐため、Webサイトの堅牢化を進めます。

【最優先】被害の有無を確認する

Webサーバーログを中心に、攻撃が行われた痕跡がないかを確認することが重要です。すでに被害を受けている可能性を優先し、最初に行うべき確認です。



【次に行う】Webサイトの堅牢化

被害が発生していないと判断した場合でも、これから攻撃が発生する可能性を考慮し、Webサイトの堅牢化を検討します。公開資産の把握、脆弱性・設定の確認、WAFの導入・見直しなど

■ 今すぐ確認しておきたい5つのポイント

不正アクセスによる被害が頻発している現状では、まずは自社が運営するWebサイトに攻撃の痕跡がないか、ログを確認してください。

1. 直近のWebサーバーログ・WAFログに不審なアクセスがないか ☐
2. 管理画面やAPIへの想定外のアクセスが発生していないか ☐
3. エラー(404・500など)やログイン失敗の急増がないか ☐
4. 公開している資産(サブドメイン・検証環境含む)を把握できているか ☐
5. 既知の脆弱性や設定不備が残っていないか ☐

該当する項目が見つかった場合と、被害が発生していないと判断した場合のそれぞれについて、次に行うことを整理します。



該当するものが見つかった／ 判断がつかない場合

被害が発生している可能性がある場合や、被害の有無を判断できない場合は、インシデント対応を専門とするセキュリティ事業者にご相談し、協力を得ながら詳細な調査を行います。



被害が発生していないと判断した場合

これから攻撃が発生する可能性があるため、次のステップとして Web サイトの堅牢化(公開資産の把握、脆弱性・設定の確認、 WAF の導入・見直しなど)を検討します。

参考資料: [JNSAソリューションガイド](#)を活用し、適切なセキュリティ事業者を探すことも有効です。

ログの確認が難しい・判断がつかない場合

ログの確認には、セキュリティ観点での分析や知識が必要になることがあります。自社で十分に確認できない場合や、判断に自信がない場合は、株式会社ビットフォレストが提供するWeb攻撃ログ分析ツール『Loggol(ログgol)』の無償提供枠をご活用ください。ログ分析を通じて、自社のWebサイトの状況把握に役立てることができます。

【緊急点検の支援】Web攻撃ログ分析ツール「Loggol(ログgol)」無償提供

Web攻撃ログ分析ツール「Loggol」(ベーシックプラン)を1ヶ月間無償で提供

対象: 自社が管理するWebサイトの脆弱性を狙った攻撃の状況を

確認したい日本国内の法人・組

利用期間: 利用開始から1ヶ月間

詳細・お申し込み: <https://www.loggol.jp/trial.html>



※ログ分析のみでは被害の有無や安全性を保証するものではありません。

ログ分析は現状把握の有効な手段ですが、次の点を理解した上で結果を活用してください。

攻撃成功を断定できない

不審なアクセスがあっても、攻撃が成功した・情報漏えいが起きたと断定できるものではありません。



該当する痕跡が見つかった場合は、専門のインシデント対応サービスを提供しているセキュリティ事業者への相談を検討してください。

被害がないとも断定できない

ログに異常が見つからなくても、被害が発生していないと断定できるものではありません。



安心材料の一つとして受け止めつつ、あわせて公開資産の把握や脆弱性確認など、堅牢化の取り組みを進めてください。

ログの取得状況に依存する

ログの内容や取得状況によって、確認できる範囲には限界があります。必要なログが保存されていない場合もあります。



インシデント発生時の調査や影響範囲の特定が難しくなる可能性があります。公開資産の把握や脆弱性対応など、他の対策の状況とあわせて確認し、不足がある場合は優先的に整備・専門事業者への相談を検討してください。

| 実践ガイド | 【次に行う】Webサイトの堅牢化

Webサイトの堅牢化で確認したいポイント

被害が発生していないと判断した場合の次のステップとして、Webサイトの堅牢化を進めます。

自社が運営するWebサイトは今後も攻撃を受ける可能性があるため、セキュリティ対策を強化する必要があります。具体的には、次のような施策を実施します。

- ・ OS、ライブラリ、フレームワーク等、自社サイトで使用されているソフトウェアの更新プログラムを適用する ☐
- ・ OSやネットワーク、クラウド環境の設定不備が存在しないかを確認する ☐
- ・ 自社独自のWebアプリケーション部分に脆弱性が存在しないかを確認する ☐
- ・ 発行したAPIキーの管理が適切かを確認する ☐
- ・ 不要な個人情報や機密情報を保有し続けていないか確認する ☐
- ・ WAFの導入により速やかにWebサイト全体のセキュリティを向上する ☐

ソフトウェアを最新の状態に保つ

- OS、ライブラリ、フレームワーク等、自社サイトで使用されているソフトウェアの更新プログラムを適用する

インフラ・環境の設定を確認する

- OSやネットワーク、クラウド環境の設定不備が存在しないかを確認する

Webアプリケーションの脆弱性の確認と改修

- 自社独自のWebアプリケーションに、以下のような脆弱性が存在しないか確認する
 - SQLインジェクションやOSコマンドインジェクションのような、どこか1か所にでも存在すれば致命的な被害につながる危険な脆弱性が存在している
 - ゲストユーザーが高権限の処理やデータにアクセスできる、一般ユーザーが管理者の機能呼び出せる
 - 管理画面や管理機能に一般ユーザーやゲストユーザーがアクセスできてしまう、管理画面に弱いパスワードがつけられている
 - JavaScript内やスマホアプリ内に秘匿すべき認証情報やAPIキー、機密情報が埋めこまれている
- Webアプリケーション部分に脆弱性が存在する場合には、開発元の協力を得てソフトウェアを修正する

APIキーの管理を見直す

- 過去に発行したAPIキーが現在どのように使用されているか不明な場合やAPIキーの漏えいが疑われる場合には、APIキーを無効化し必要に応じて再発行する
- サービス提供が終了している場合、サーバーの停止やスマホアプリの配信停止に加えてそのサービス運用のために使われていたAPIキーの破棄も忘れずに行う

不要な個人情報や機密情報を保有し続けていないか確認する

- 保有し続ける必要のない個人情報や機密情報は、適切に削除する
- 法律や業界ガイドラインなどにより保有が必要な情報は、Webアプリケーションから直接アクセスできる場所を避けるなど、万が一Webサイトが侵害されても容易に漏えいしない場所で保管する

WAFの導入により速やかにWebサイト全体のセキュリティを向上する

- ソフトウェアの更新、脆弱性診断、発見された脆弱性の修正は、Webサイトのセキュリティを高めるうえで重要だが、実施には時間とコストがかかるため、まずWAFで保護しながら、根本的な対策を進める

本質的な対策と、WAFによる速やかな保護

Webサイトのセキュリティ向上のための本質的な対応という意味では、更新プログラムの適用や脆弱性診断の実施、発見された脆弱性の修正が必要です。

一方で、以下のような一連の対応は、今日からすぐに実施できるものではなく、体制を構築するために時間もコストもかかります。

- 使用しているソフトウェアの更新プログラムをすべて適用することは動作確認やソフトウェアの組み合わせの互換性などから現実的には難しいこともよくある
- 提供されている更新プログラムのうち、重要性・緊急性の高いものから優先的に適用する判断が求められる
- 更新プログラムの適用は、Webサイトを公開している間、継続的に実施し続ける必要がある
- 自社Webアプリケーション部分に対する脆弱性診断で発見された脆弱性を修正するためには、プログラムコードの修正も必要になる

まずはWAFを導入することで、プラットフォームやWebアプリケーションに対して広く実効性のある保護を速やかに適用し、その間にセキュリティ施策を継続的に実施する体制の構築や脆弱性診断、ソフトウェアの修正などを行うという方針が効果的です。

WAFはWebサイトへの攻撃を防ぐ重要な手段ですが、製品によって防御性能や対応範囲はまちまちです。攻撃が自動化・大量化し、防御の状態を見ながら手口を変える中、「導入しているか」ではなく「どこまで守れているか」を確認します。

01 防御できる範囲(仕様)

既知の攻撃パターンだけでなく未知の攻撃に対応できるか、APIのリクエスト(JSONなど)を検査できるか、サイズ制限など仕様により守れていない箇所はないか



自社のサイト・APIに対して、何が守れて何が守れないかを把握

02 新たな脆弱性への対応

自社で使っているOS・ミドルウェア・フレームワークに新たな脆弱性が公表されたとき、WAF側がいつ・どのように対応し、それをどう知らせるか



パッチ適用までの間、攻撃を防ぐ手段として機能するかを確認

03 設定・運用の状態

誤検知対応などで、除外設定が増えている、保護対象から漏れたホストやAPIがある



設定と定期的に見直し、実際に遮断できているかを確認

WAFだけでは防げないものもある

認可制御の不備のような仕様上の欠陥や、正規の操作と見分けにくいアクセスは、WAFでの判別が難しい。

→ 脆弱性診断による根本的な修正と組み合わせる

自動化された攻撃を踏まえた見直しの観点

総当たりや大量アクセスには、WAFだけに限らず、**アカウントロック・多要素認証・アクセス頻度の制限など、アプリケーション側の対策と組み合わせ**て備える。誤検知時に調整しやすいか、検知・遮断の状況を確認しやすいかもあわせて確認する。

脆弱性・設定を確認する

一連の不正アクセスでは、攻撃者がWebサイトを個別に調査し、サイトごとの特性に合わせて攻撃している様子が伝えられています。Webサイト・スマホアプリ・動作環境への脆弱性診断は、対策として大きな意味を持ちます。

01 プラットフォーム／クラウド設定診断

サーバーのソフトウェアに残る脆弱性 (CVE) やネットワーク設定の不備を確認。クラウド環境ではクラウド設定診断で固有の設定不備を確認。EC2・Azure VM など IaaS は利用者の責任範囲

設定不備や残存脆弱性が狙われた例も。
パッチ適用漏れに備え定期的に実施

02 Webアプリケーション診断

各システム固有のアプリケーション部分も調査・攻撃されている。管理用APIの呼び出しなど、本来の権限を超える操作 (認可制御の不備) を狙った試行も確認

動作環境の診断とあわせて実施を強く推奨

03 スマホアプリ診断

公開アプリは攻撃者も入手・解析できる。設定ファイル、端末内データ、通信先一覧、ハードコードされた認証情報やAPIキーが攻撃の糸口に

解析で管理用APIやAPIキーが特定された例も。バックエンドの診断とあわせて実施

過去に診断したから安心、とは限らない

管理者向け画面やAPIは対象外にされやすく、権限ごとの機能差が診断側に伝わらず確認から漏れることも。

→ 管理画面や重要な機能が実際に診断対象だったかを再確認

「何をどこまで診断するか」を決める

費用対効果を考えると、すべての機能の診断は現実的ではない。

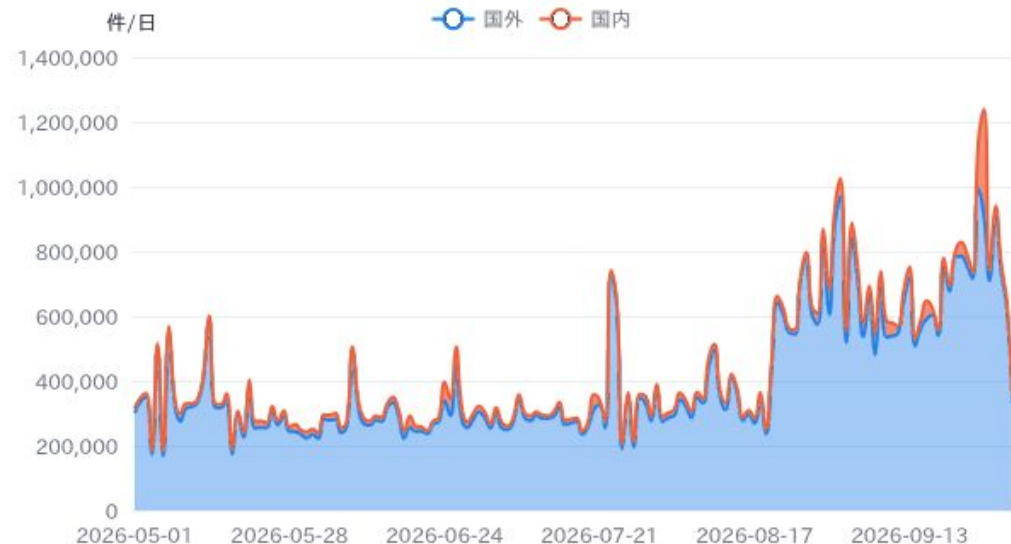
対象範囲の選定に迷う場合は、**診断を行うセキュリティ事業者**に**範囲の絞り込みから相談**するとよい。

参考資料 |

| クラウド型WAF「Scutum」の防御ログから見た 直近の攻撃傾向

7月から9月にかけて、攻撃件数は増加している

① 日別アラート総数(国内 / 国外 内訳)



グラフから読み取れること

5～7月

1日あたり20～40万件前後で推移

8月中旬～

60～80万件前後へ水準が上昇し、高止まり

9月

100万件を超える日も発生

※Scutumで検知した日別アラート数(国内／国外)
(本調査対象サイトでの実績)

攻撃の特徴:3種類の攻撃を確認

分析の対象

株式会社マクニカ「相次ぐWEBシステムからの情報漏えい事案について」に記載された、攻撃を行っていたIPアドレス(210.149.87[.]120、69.10.51[.]162)がどのような攻撃を行っていたかを、Scutumの防御ログから分析しました。

参考URL:<https://security.macnica.co.jp/blog/2026/10/web-incidents2026.html>

以下の3種類の攻撃が行われていました。

1 複数ツールによる攻撃

curlやsqlmapなど、複数の攻撃ツールを使い分けて攻撃

2 APIの組み合わせ総当たり

隠れたAPIを探すため、エンドポイント名の組み合わせを大量に送信

3 認証キーの総当たり

データを取得するため、認証キーを利用者IDごとに総当たり

攻撃① 自動SQLインジェクション

単一のツールではなく、複数の攻撃ツールを使い分けて攻撃を行っていました。

ログ上で確認されたツール(例)

curl

任意のリクエストを送れるコマンドラインツール

sqlmap 1.10.9

SQLインジェクションを自動で検出・悪用するツール

ツールを組み合わせることで、手作業では難しい規模・速さで、サイトに対するさまざまな攻撃を試すことができます。

ポイント 複数のツールを使い分けて攻撃している

攻撃② APIの組み合わせ総当たり

サイトの隠されたAPIを総当たりで探し、情報を取得しようとする攻撃を行っていました。

1

正規のAPIフローを実行

サイトの正規の手順どおりにAPIを呼び出す

2

既知のAPIにSQLインジェクション

判明しているAPIに対して攻撃を試行

3

エンドポイント名を総当たり

名前の組み合わせを大量に送り、実在するAPIを確認

4

検知されたら減速して継続

WAF側に検知され拒否される挙動を観察しながら攻撃の速度を調整

観測された規模

5万 リクエスト以上

エンドポイント名の総当たり

約1万 リクエスト／分

総当たり時の送信ペース

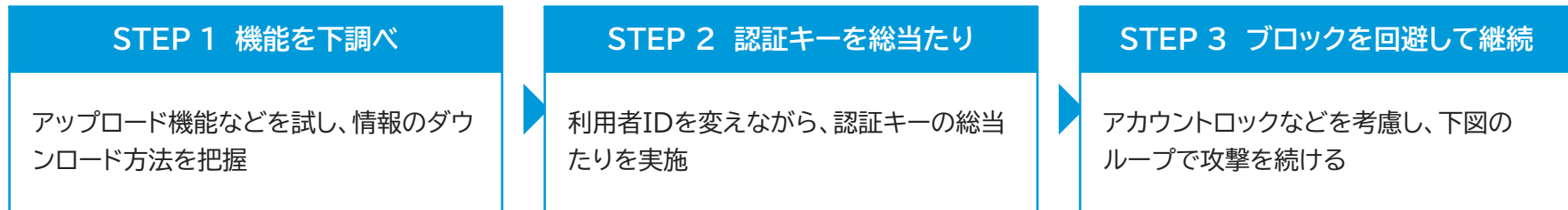
毎分1～6回

検知後に落としたリクエスト頻度

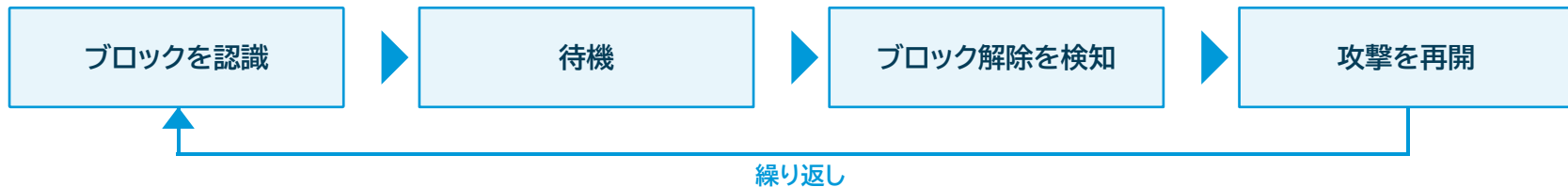
ポイント サイトの内容と防御機能を確認しながら、検知を避けるように攻撃を続けている

攻撃③ データ取得を目的とした認証キーの総当たり

情報をダウンロードするサイトにおいて、認証キーを総当たりし、情報を取得しようとする攻撃を行っています。



ブロックを回避するループ



ポイント サイトの内容と防御機能を確認しながら、ブロックをかわして攻撃を続けている

被害事例が増えている要因はAIエージェントなのか

観測された攻撃に、「LLM型エージェント」の実行パターンと整合する要素があるかを確認しました。

LLM型エージェントと整合する要素

- ✓ 複数のツールを使い分けている
- ✓ 人間らしくないダミー値を利用している
- ✓ 下調べの成果を大量に保持したまま、複数サイトへ展開している
- ✓ URIを辞書ではなく、規則に基づいて網羅的に生成している
- ✓ 防御状態を把握し、機械的にループしている

判断

人間の攻撃者でも説明できるため、AIエージェントによる攻撃とは断定できない



ただし

これまでWAFで観測してきた攻撃に比べ、サイトの内容把握や防御機能への対応など、攻撃が進化している様子は確認できる

直近の観測を踏まえて、これまでと「変わらないこと / 変わること」

必要な対策の多くは、今回の事案によって初めて必要になったものではありません。一方で、攻撃の手法や量、狙われやすいポイントには変化が見られます。従来から求められるWebサイトの基本的な対策を確実に実施し、変化する脅威に応じて見直すことが重要です。

変わらないこと

- ・ 基本的なセキュリティ対策(公開資産の把握、脆弱性対応、認証・アクセス制御)の重要性
- ・ ログの取得と確認体制の必要性
- ・ インシデント発生時の初動手順の重要性

変わること

- ・ 攻撃の自動化・量的増加
- ・ APIや管理機能を狙う動きの活発化
- ・ 設定不備や管理漏れを突く事例の増加
- ・ 「まず何を確認すればよいか」を明確にしたいというニーズの高まり

| さいごに

情報漏えいに関する報道が相次ぐなか、不安を感じている方も多いと思います。大切なのは、慌てず、できることから確実に確認を行い、自社のWebサイトの安全を優先して行動することです。

1. 被害の有無を確認する | Webサーバーログを中心に、不審なアクセスや異常がないかを確認する
2. 確認が難しい場合は支援を活用 | Webサーバーログ分析ツールなどを活用し、現状把握を行う
3. 被害懸念があれば専門事業者へ相談 | インシデント対応を行っているセキュリティ事業者にご相談する
4. 被害なしと判断したらWebサイトの堅牢化 | 公開資産の把握、脆弱性確認、WAF・監視の強化を進める
5. 優先順位を決めて継続する | すべてを一度に完了できなくても、担当者と期限を決めて継続的に進める

本資料は、現時点で考えられる対応についてまとめたものであり、「これだけやれば大丈夫」ということではありません。今できることを整理し、行動につなげていただくことを目的としています。

状況は現在進行形で変化しています。JPCERT/CCなど信頼できる情報源の最新情報を随時確認してください。

- 直近で相次いでいる国内組織における不正アクセスに関する注意喚起

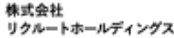
<https://www.jpccert.or.jp/at/2026/at260030.html>

- 【注意喚起】相次ぐ情報漏えい、その原因の一つは「アプリ解析からのサーバ攻撃」— AIで高度化する脆弱性探索、Androidアプリを手がかりにしたA2B攻撃に注意 — | ライブラリー | サイバーセキュリティネクスス | NICT

<https://cynex.nict.go.jp/library/261013-01.html>

本資料が、被害拡大防止と影響緩和の一助となりますようご活用ください。

会社名	株式会社セキュアスカイ・テクノロジー
所在地	本社： 〒101-0032 東京都千代田区岩本町2-2-4 PMO神田岩本町II 10F 福岡ラボ： 〒810-0001 福岡県福岡市中央区天神1-9-17 福岡天神フコク生命ビル 14F
設立	2006年3月
代表者	代表取締役 大木 元
事業内容	Webアプリケーションに特化したセキュリティサービス ・脆弱性診断サービス ・セキュリティ教育・支援サービス ・クラウド型WAFサービス ・EASM（ASM）サービス ・その他、セキュリティコンサルティング
URL	https://www.securesky-tech.com/

主な取引先		
	 アイティーエム	 Internet Initiative Japan
		
 株式会社NTTデータ先端技術		 CyberAgent
 GMOグローバルサイン・HD GlobalSign		 TIS INTEC Group
		 HEARTBEATS
	 パナソニック ソリューションテクノロジー株式会社	 株式会社 リクルートホールディングス
 CTC Cyber Technology Company	 株式会社電通総研	

Webアプリケーションセキュリティの観点から、Webサーバーに対する攻撃からの保護、脆弱性の診断、公開資産の把握やセキュリティ推進に関する支援を提供しています。

- クラウド型WAF「Scutum」: Webアプリケーションに対する攻撃への防御を支援
- 脆弱性診断サービス: Webアプリケーション、OS、ミドルウェアなどの脆弱性の把握と改善に向けた支援
- ASMサービス「Dredger」: インターネットに公開された資産の把握や管理の支援
- セキュリティ教育・支援、コンサルティング: セキュアな設計・開発や運用のための支援

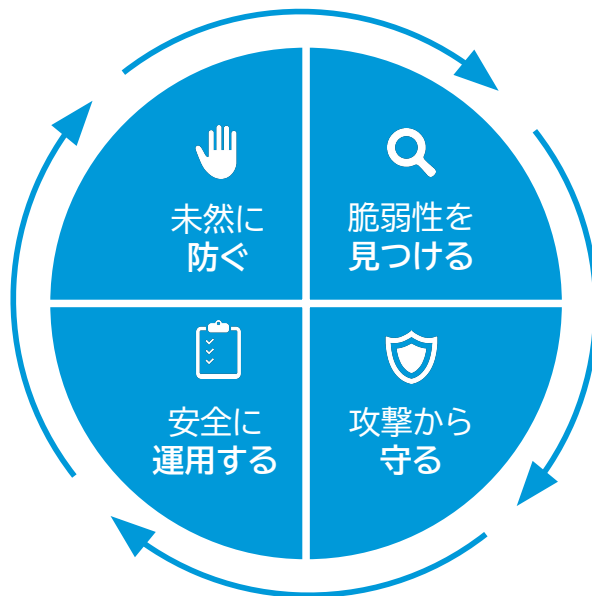
一方、侵害発生後のフォレンジック調査やシステム復旧、ネットワーク・端末を含む広範な調査など、当社の専門領域だけでは対応が難しいケースもあります。そのような場合には、必要に応じて、適切な専門性を持つパートナーとの連携や紹介を通じた対応が必要となります。

潜在的な脅威を未然に防ぐ 準備とサポート

- ・セキュアな構築・運用のための脅威分析
- ・対策支援
- ・開発者・サイト運営者向けセミナー

安全なWebサイトを維持する ための継続的な運用と改善

- ・EASM(ASM)サービス
- ・セキュリティアドバイザリー
- ・従業員向けセキュリティセミナー



脆弱性やリスクを 迅速かつ的確に発見

- ・脆弱性診断
 - └ Webアプリケーション診断
 - └ プラットフォーム診断
- ・ペネトレーションテスト
- ・アタックサーフェス調査サービス

Webサイトを狙った 攻撃から防御

- ・クラウド型WAF
- ・クラウド型DDoS対策
- ・不正検知
- ・Web改ざん対策

Webアプリケーションの開発から運用までを支える包括的なセキュリティサービス

本件に関するお問い合わせ

本ガイドの内容やWebサイトのセキュリティ対策に関するご相談がございましたら、
以下のお問い合わせフォームよりご連絡ください。

お問い合わせフォームはこちら



03-3525-8045

月～金 10:00 - 18:00



info@securesky-tech.com

会社名・氏名・メールアドレス・電話番号を
ご記入の上、お問い合わせください。

株式会社セキヤスカイ・テクノロジー