beyond

# セキュリティ診断サービス
# RayAegis
## サービス紹介資料

# RayAegis（レイ・イージス） とは？

beyond

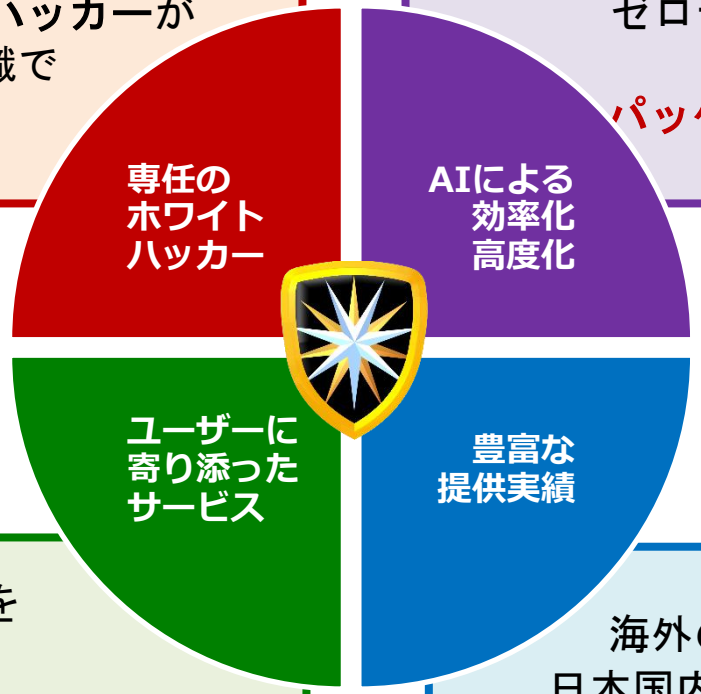
RayAegis


- RayAegis（レイ・イージス）は、政府機関 や 金融機関・大手製造業・交通システム などのシステムのセキュリティコンサルティングとして活躍する、全世界で250名を超える技術力の高いホワイトハッカー・セキュリティエンジニア集団です。
- RayAegis（レイ・イージス）の技術チームはアメリカ・カーネギーメロン大学、パデュー大学、国立台湾大学の電気情報学科のコンピュータ及び情報セキュリティの修士・博士の学位取得者や、CISSP / CISM / CEH などの情報セキュリティの各種資格を取得している専門家といった優秀なセキュリティエンジニアで構成されています。
- 世界最先端のセキュリティとAIの技術を組み合わせ、RayAegis（レイ・イージス）が開発した「RayScanner」と「RayInvader」は、米国政府と同期した独自情報を含むデータベースを使用して、Webサイトやアプリケーションがハッキングされているかどうか、また、ゼロデイなどの未知の脆弱性をも効率的に確認し、最も厳しい国際基準を満たしたセキュリティサービスを提供します。

# RayAegis セキュリティ診断の特徴

各種セキュリティ防護システムを熟知した**全世界で250名を超える**CISSPやCEHなどの**有資格ホワイトハッカー**がリアルな攻撃者の技術と知識でサービスを提供。

自動化や高度な疑似攻撃用のAIツールを独自開発し、論理チェックや権限奪取、ゼロデイ攻撃など効率的に実施。
**診断期間の短縮**だけでなく
**パッケージ型定額価格体系**を実現




対策が正しく適用できたかを確認する再診断を全サービス標準で提供。
特に、**ペネトレーションテストでは**納得するまで**初回診断後1年間何度でも再診断にご対応。**

海外の金融・政府系機関のほか、日本国内でも金融・SaaS事業者など大規模環境向けにサービスを提供中。
台湾政府の**セキュリティベンダー格付け**でも**例年トップクラスにランキング。**

# RayAegis セキュリティ診断の強み

beyond

## 安　パッケージ型定額サービスなので「安価」

- リクエスト数が多いECサイトやSaaSプラットフォームなど、大規模システムになるほどお得に診断いただけます。

## 楽　事前の診断対象絞り込みの「手間が不要」

- 診断規模にかかわらず定額なので、「どこを診断してもらうか」という優先順位付け作業は不要です。

## 短　診断作業の期間が「短い」

- 独自AIツールによる高品質な自動化で、ページ数の多いECサイトなどでも1～5営業日の短期間で診断できます。

## 援　発見項目の再診断などの「アフターサポート」

- 特にペネトレーションテストでは**1年間**にわたって、分割再診断や再々診断対応で修正完了までご対応いたします。

# RayAegis 価格体系の仕組み

beyond

■高度なセキュリティエンジニアを **必要な部分に注力させられる仕組み**

・ 一般的なツールへの独自開発プラグインや、
独自AIツール（RayScanner・RayInvader）による検出・疑似攻撃の高度化・自動化を実現。

・ エンジニアはコンピュータが代替できない「ビジネスロジック」や
「完全な新規の脅威」に注力して調査・検査を実施。

■シンプルな **サブドメイン / FQDN単位 の価格体系**

・リクエスト数ベースではなく、サブドメイン / FQDNあたりの簡単・一律な課金体系を実現。

# 情報セキュリティ 10大脅威

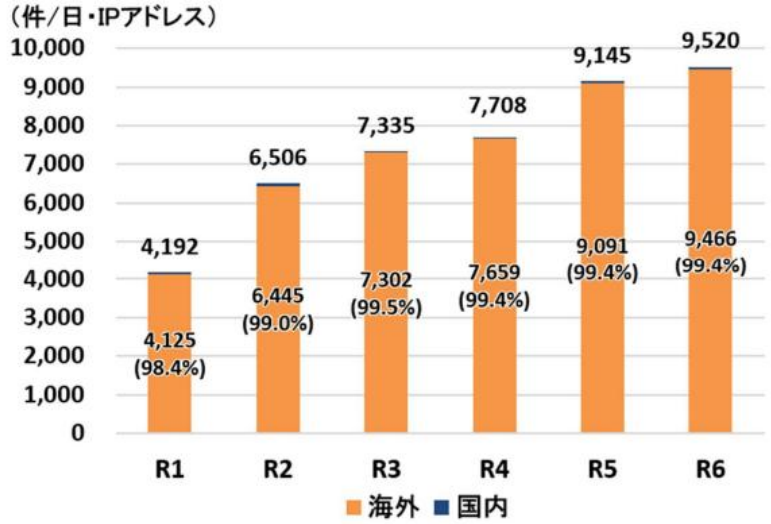
| 個人 | 順位 | 組織 |
|---|---|---|
| インターネット上のサービスからの<br>個人情報の窃取 | 1位 | ランサム攻撃による被害 |
| インターネット上のサービスへの不正ログイン | 2位 | サプライチェーンや委託先を狙った攻撃 |
| クレジットカード情報の不正利用 | 3位 | システムの脆弱性を突いた攻撃 |
| スマホ決済の不正利用 | 4位 | 内部不正による情報漏えい等 |
| 偽警告によるインターネット詐欺 | 5位 | 機密情報等を狙った標的型攻撃 |
| ネット上の誹謗・中傷・デマ | 6位 | リモートワーク等の環境や仕組みを狙った攻撃 |
| フィッシングによる個人情報等の詐取 | 7位 | 地政学的リスクに起因するサイバー攻撃 |
| 不正アプリによるスマートフォン利用者への被害 | 8位 | 分散型サービス妨害攻撃（DDoS攻撃） |
| メールやSMS等を使った脅迫・詐欺の<br>手口による金銭要求 | 9位 | ビジネスメール詐欺 |
| ワンクリック請求等の不当請求による金銭被害 | 10位 | 不注意による情報漏えい等 |

脆弱性を利用した
攻撃が、自動化・
高度化により
改めて再燃しています

出典： 独立行政法人 情報処理推進機構 (IPA) 「情報セキュリティ10大脅威 2025」
2025/1/30 公開

# サイバー攻撃の拡大

【図表１：警察庁が検知した不審なアクセス件数（１日・１IPアドレス当たり)】




■内訳
・不審アクセスの送信元の大部分が海外

・令和６年におけるランサムウェアの被害報告件数は 222 件であり、高水準で推移

出典： 警察庁サイバー警察局 サイバー企画課 「令和６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」（2025/3/13）

## リスクの急激な増加

- サイバー攻撃の高度化やAIを活用した**攻撃数の増大**
- RaaS（Ransomware as a Service）の登場により技術的スキルが無い場合でも攻撃可能になり**犯罪者層の拡大**

## 求められる対策

- 最新の脆弱性情報や攻撃手法に基づいたセキュリティ診断による**網羅性の確保**
- サイト公開前と公開後の定期的なペネトレーションテストの実施による**早期発見**

# 複雑化するセキュリティインシデント

beyond

## ■セキュリティインシデントの傾向

・フィッシングによる攻撃は前年比約3倍に増加。
コロナ以後に Emotet などが高度化し再燃。
ECサイトだけでなく、一般企業を騙るフィッシングサイトも
500件以上報告されており、増加傾向にある。

・ランサムウェアは減少傾向だが、攻撃が実現した場合の影響は引き続き甚大。

・企業のシステムとしては、自社システムの脆弱性が他社への攻撃に悪用され、
サプライチェーン攻撃の事例が増大。

・Webシステムについては脆弱性の即時利用や不正ログインが容易化しており、
従来以上に対応の重要性が増している。

・単一の脆弱性をつく攻撃から、効果や状況に応じて複数の脆弱性を
組み合わせるなど変遷・進化しながら攻撃するマルチベクトル型攻撃が主流化。

・重大な脆弱性に絞っての対策では防止できないケースが増加中。

# ニューノーマルでのビジネス形態の変化

beyond

## COVID-19 緊急事態宣言以前

**オフィスに出社して業務に従事**

- リモートアクセスは限定的であり、対策も容易

**営業活動は対面が基本**

- 重要情報は対面でのやり取りが大半で、
  ECサイト等のeコマースは対面を補完する位置づけ

**サイバー攻撃は大手企業がメインターゲット**

- 特に中小企業ではセキュリティの知識に乏しく、
  投資の優先度も低い

## ニューノーマル以降

**大手を中心にリモートワーク化**

- VPNやクラウドアクセスなど対策が必要な箇所が増大

**営業活動はリモート・ECサイト中心**

- B2B / B2CともにECサイトの売上比率が増加し、
  これまで以上に企業活動の生命線として重要システム化

**サプライチェーンリスク攻撃の急増**

- フィッシングやビジネスメール詐欺などによる
  サイバー攻撃は、中小企業が踏み台としてターゲットに
- 大企業は取引先のセキュリティ対策状況の把握がほぼ必須に

# AIを利用した高度化する サイバー攻撃への対処

beyond

攻撃側

**ハッカーによるサイバー攻撃の AI による**
**自動化 / 高速化 / 高度化**

- AIなどの採用による探索・攻撃の自動化。
- 動的な亜種・難読化攻撃の自動生成。
- 大量の攻撃を多数のターゲットに短期間で手配・実行。

**検知・診断技術の AI による診断、**
**防護の自動化 / 高速化 / 高度化**

- AIを採用した防護策（WAF/IPS/NDR）による 防護の高度化。
- 脆弱性検出や亜種・難読化攻撃耐性検知も
  AIを採用して高度な自動化。
- 増加する保護・診断対象システムには、
  AIによる自動化・高速化が必須技術に。

防御側

# 各種お問い合わせ

お気軽にお問い合わせください。

| 電話でのお問い合わせ | メールでのお問い合わせ |
| --- | --- |
| **06-6536-8422**<br>平日10:00～19:00 | **sales@beyondjapan.com**<br>会社名・氏名・メールアドレス・電話番号を<br>ご記入の上、お問い合わせください。 |

https://beyondjapan.com/contact
当社のホームページからでもお問い合わせいただけます。