RayAegis Japan

レイ・イージス・ジャパンのご紹介

株式会社レイ・イージス・ジャパン

2023年6月

株式会社レイ・イージス・ジャパン　会社概要

会社名　：株式会社レイ・イージス・ジャパン

住所　　：〒160-0023　東京都新宿区西新宿７丁目22番33号
Polar西新宿4階

設立　　：2019年10月10日

親会社　：　Ray Aegis Information Security　（台湾）
設立：2011年11月　従業員：約300名
株式会社アリス
設立：2001年6月　　従業員：約200名

主要業務：各種セキュリティ診断サービス
AI クイック・ツール診断 / AI リモート脆弱性診断
ペネトレーションテスト　/ モバイルアプリ診断/プラットフォーム診断
WAF、IDS, Sandboxなどのクラウドサービス、SOCサービスなど

加入団体：日本カード情報セキュリティ協議会 (JCDSC)
日本サイバー犯罪対策センター（JC3）

021-0012-20

株式会社レイ・イージス・ジャパン「情報セキュリティサービス基準審査登録制度」に登録したサービスを提供する企業です。

創業者Ray Chiangがカーネギーメロン大学在学中にAI技術や最新セキュリティ技術を学び、米国大手銀行でのレッドチーム業務などに従事して知識と技術を確立し、台湾に帰国後にRay Aegis Information Security社を設立。金融機関向けのペネトレーションテストやレッドチームコンサルティングで多数の実績を持ち、金融機関以外でも政府系機関、大手航空会社、大手製造業を中心に高度なセキュリティサービスを提供しています。

レイ・イージス・ジャパンのサービスメニュー

ペネトレーションテスト	ファスト ペネトレーションテスト	ネットワーク内不正通信 攻撃検知サービス	マルウェア検知サービス （クラウド型Sandbox）	マネジドサービス （クラウド型 WAF）
				
脆弱性診断	プラットフォーム診断	モバイルアプリ診断	フォレンジックサービス	マネジドサービス （SOC）
				

＊マネージドサービスのCloud WAF と SOC については、2023年夏からの提供開始予定です。

RayAegis Japan

レイ・イージスの強み

専任のホワイトハッカー

各種セキュリティ防護システムを熟知した**全世界で300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。

AIによる効率化・高度化

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。

ユーザーに寄り添ったサービス

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。**

豊富な提供実績

海外金融・政府系機関を中心に豊富なサービス提供実績を持ち、長期にわたってサービス提供中。
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 Japan

脆弱性とは

脆弱性とは

- 脆弱性＝安全上の欠陥です。サイバー攻撃の攻撃者は、脆弱性を利用して、攻撃をします。
- その攻撃者は、**高度な技術力を持つブラックハッカーだけではありません。**
- 平易にツールを購入、ダウンロードして、個人情報やクレジットカード情報、医療情報を扱うような一部の大企業、病院、政府機関だけでなく、
- **中小企業も含めて無差別**に攻撃が行われています。
- **2021年　世界で届け出のあったインシデント件数：847,376件　被害額69億ドル　出典元：2022　情報セキュリティ白書**

RayAegis Japan

Webセキュリティと社内セキュリティ

一般向けに公開

WebサイトやWebサーバーなど

一般向けには非公開

社内ネットワークやPC本体など

レイ・イージス・ジャパンでは「Webセキュリティ」と「社内セキュリティ」いずれも、ネットワークにつながるあらゆるものに対して、攻撃者の視点から診断（テスト）を行い、そこに脆弱性がないか確認することが可能です。

RayAegis Japan

公開されたWebサイトへの脆弱性診断

弊社コーポレートサイト
https://www.rayaegis.co.jp/

□提供可能サービス

・脆弱性診断

AIリモート脆弱性診断　　費用：980,000

AIクイックツール診断　　費用：450,000

（OWASP Web Security Testing Guide等各種基準に沿った脆弱性診断を実施します。）

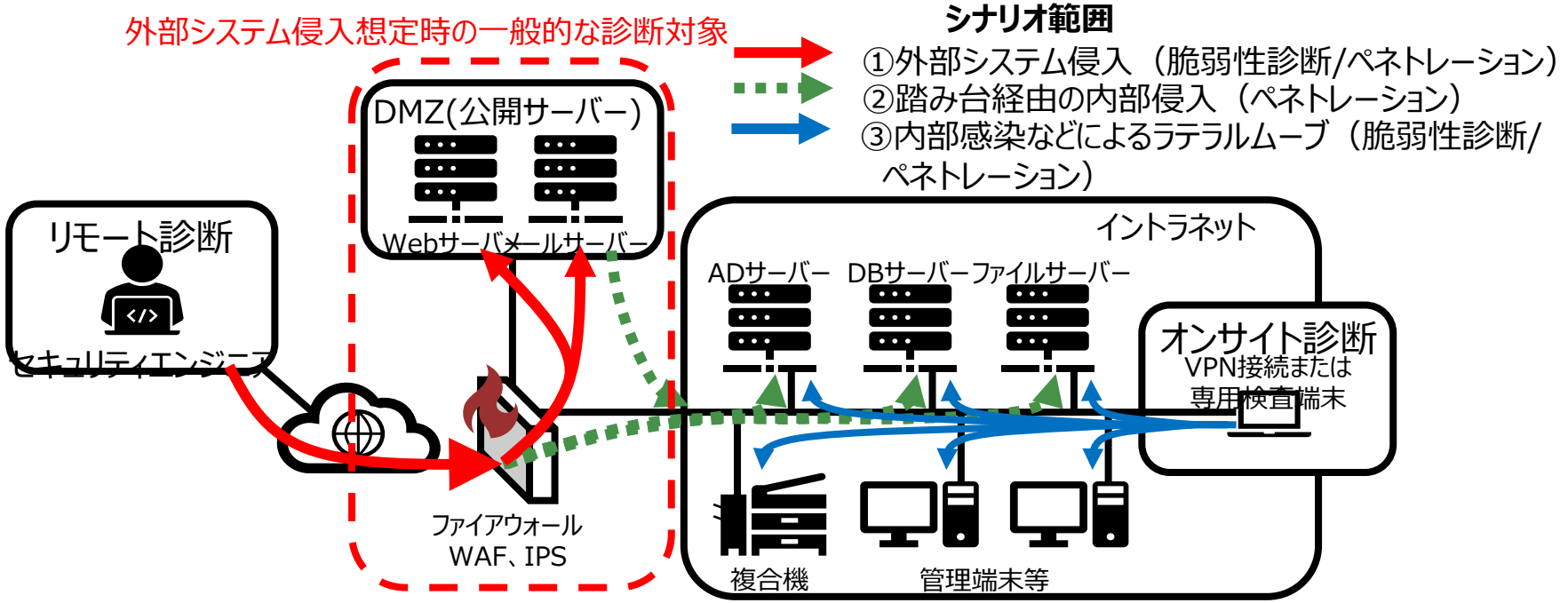
□対策できるもの

悪意ある攻撃者による、サイトの改ざんや、
個人情報の漏洩につながる悪意ある攻撃に対して、
脆弱な箇所がないかの確認が可能

上記のようなサイトではAIクイックツール診断でも通常十分です。
reCAPCHAで守られている部分についても追加で手動診断をしたい場合にはAIリモート脆弱性診断がお勧めです。
その他、会員様限定サイトや非公開のWebアプリケーションなどがある場合は、AIリモート脆弱性診断やペネトレーションテストをお勧めします。

RayAegis Japan

各種ペネトレーションテストのイメージ



RayAegis Japan

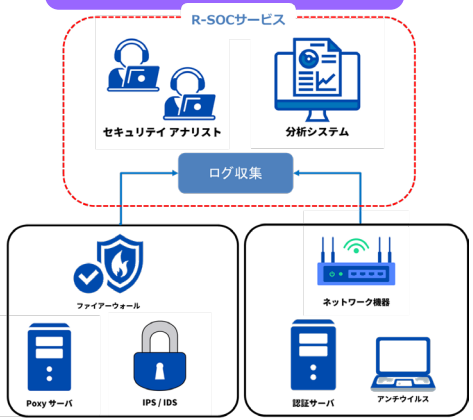
モバイルアプリケーション診断の範囲

モバイルアプリ診断単体では、サーバー側のM4とM6を除く、アプリケーション単体のセキュリティリスクを診断します。
M4とM6については、API診断オプションにてサーバー側の診断とともに提供いたします。

OWASP Top 10 Mobile Risks		モバイルアプリ診断	API診断オプション
M1 - Improper Platform Usage	プラットフォームの不適切な利用	✓	
M2 - Insecure Data Storage	安全でないデータストレージ	✓	
M3 - Insecure Communication	安全でない通信	✓	✓
M4 - Insecure Authentication	安全でない認証		✓
M5 - Insufficient Cryptography	不十分な暗号化	✓	✓
M6 - Insecure Authorization	安全でない認可		✓
M7 - Client Code Quality	クライアントコードの品質	✓	
M8 - Code Tampering	コードの改ざん	✓	
M9 - Reverse Engineering	リバースエンジニアリング	✓	
M10 - Extraneous Functionality	無関係な機能	✓	

特殊なサービス

マネジドサービス（SOC）



①セキュリティデバイスから出力されるログ・アラートをリアルタイムで監視・分析

•ログ・アラートから顧客への影響の有無を判断

•分析結果で顧客に影響がありそうなら顧客に通知

②顧客からの問い合わせの窓口

③前月の対応実績をまとめた成果物を月次レポートしてお客様に報告

フォレンジックサービス

サイバー攻撃によるマルウェア感染や不正アクセス、情報漏洩や 内部犯による不正操作の痕跡を調査・解析し、被害状況の把握や 必要な対策の立案をサポートします。

実環境のリモート調査のほか、システムイメージの静的・動的やファイル提供など、 提供いただける情報の中で可能な限りのサービスを提供します。

高度なホワイトハッカー集団による最新攻撃手法に対応した調査

● 世界中でのペネトレーションテストやフォレンジック調査などから得られた知見を持つレイ・イージスのホワイトハッカーが、実際に悪用されている最新の攻撃手法やマルウェアの情報をダークウェブなどから継続的に調査収集し、攻撃者の視点から調査を実施します。

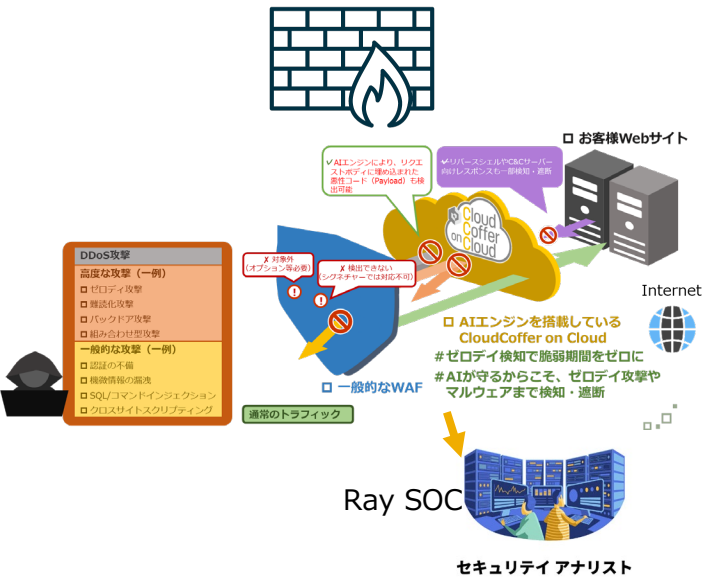
AIを活用したより網羅的・効果的な調査の実現

● AIマルウェア検査ツールにより、提供いただいたファイルやシステムイメージから従来のアンチウィルスやEDRで検知できないマルウェアや悪意のあるコードを発見します。
ゼロデイ攻撃を含む、新種や亜種など、特に標的型攻撃でみられるカスタマイズ型の攻撃痕跡を解析・発見します。

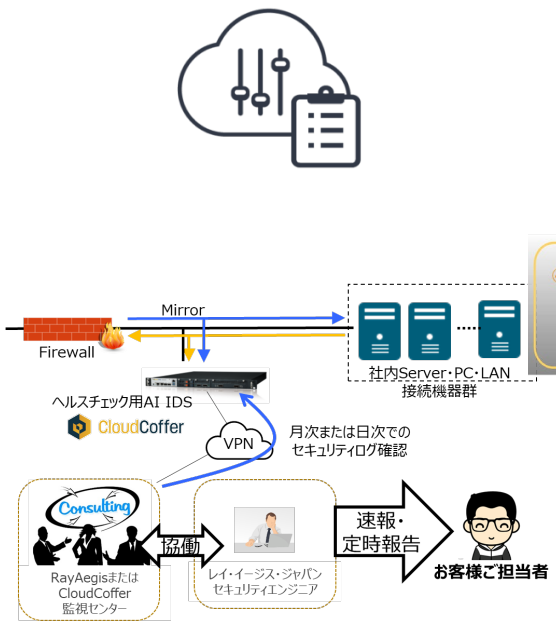
RayAegis Japan

保護検知サービス

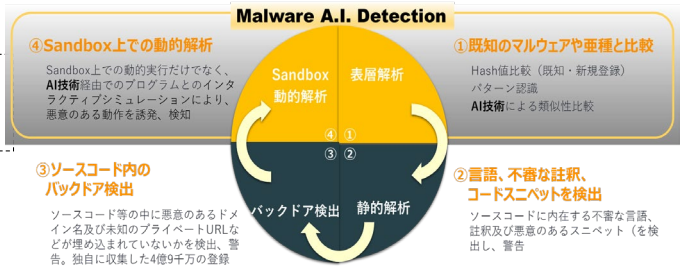
マネジドサービス（クラウド型 WAF）



ネットワーク内不正通信攻撃検知サービス



不正コード マルウェア検知サービス



RayAegis Japan

RayAegis Japan

より安全な環境の実現に、
より現実的なセキュリティ対策を

株式会社レイ・イージス・ジャパン

〒160-0023　東京都新宿区西新宿７丁目22番33号
Polar西新宿4階

☎ 03-6703-6619　https://www.rayaegis.co.jp/