

「侵入は防げない」時代の新たなサイバーセキュリティ対策。 侵入後の被害拡大を AI が防ぐ 「ランサムウェア対策サービス」の提供を開始。

インクレイブ株式会社（本社：宮城県仙台市、取締役社長：丸山 秀行）は、AI がサーバの自動監視・攻撃検知・攻撃遮断を行う「ランサムウェア対策サービス」を本日より提供開始いたします。

本サービスは、AI が 24 時間 365 日サーバを監視し、サイバー攻撃を自動で検知・遮断するセキュリティサービスです。従来のルールベースでは対応が難しかった未知の攻撃にも対応し、近年深刻化・巧妙化するランサムウェア被害の拡大を低減します。

また、導入から運用・保守までを専任チームが支援することで、専門人材を確保することが難しい企業でも、安心して高度なサイバーセキュリティ対策を導入いただけます。

初期費用 165,000 円（税込）、月額 16,500 円（税込）という導入しやすい価格体系で、対象の専有サーバをご契約のお客様向けに提供いたします。

INCRAVE
ランサムウェア対策サービス
SentinelOneサーバ向け EDR

- AI監視** 24時間365日
- 自動隔離** 被害拡大を抑制
- ゼロデイ攻撃対応** 0+

サーバ運用・データ管理で、こんな不安はありませんか？

- ランサムウェアの被害が自社で起きた場合、大きな損害が予想される
- 万が一のサイバー攻撃に的確に対応できる体制が整っていない
- 従来のセキュリティ対策だけで、最新の脅威に対応できるのか疑問
- セキュリティ対策は必要だと思うが費用はかけられない

ランサムウェアなどの脅威から、大切なデータ資産を守ります

EDR (エンドポイント監視・制御)

従来の防御だけでは防げられない侵入後の不審な動きを検知・記録・対応するEDR対策です。挙動監視により兆候を捉えて即時対応し、データ保護と業務停止リスクの軽減を実現します。導入から保守まで、貴社の環境に合わせてサポートします。

図の制御が前提となる状態に侵入

侵害者が生ずる「Ransomware」により、侵害者によりデータの保護が実現されています。侵害者によるデータの保護が実現されるため、サービスなどの導入が重要となります。

— EDRのしくみ —

脅威 ランサムウェア、不正アクセスなど

EPP (侵入前対策) デバイス内への脅威の侵入を防ぐための対策

EDR (侵入後対策)

検知 → 隔離 → 調査 → 復旧 → CLEAN

ランサムウェアなど侵入を検知し、管理を自動化

感染端末をネットワークから隔離し、被害を抑制

検知したログ情報を基に、侵害者や被害を調査・分析

ランサムウェアの検知・復旧

脅威の侵入後の被害を最小限に抑えるための対策

サーバ内部の監視と復旧までカバーし、被害拡大を防止します

— ランサムウェア対策サービスで実現できること —

従来のアンチウイルスでは防げない「未知の脅威」に検知・遮断を自動対応、復元も組み合わせて実現します。

- AIが挙動を監視し未知の脅威も検知**
サーバ内のプロセスやネットワークの挙動を監視し、異常な挙動を検知。未知の脅威にも検知が可能です。
- 不審プロセスを自動遮断し被害拡大を抑制**
不審プロセスを検知したら、自動でそのプロセスを遮断し、被害拡大を抑制します。
- スナップショットで安全性を強化**
サーバの状態を定期的にバックアップし、万一の被害発生時も、スナップショットから復元して正常な状態に戻すことができます。
- 侵入後の兆候を見逃さない内部監視**
サーバ内の活動で検知プロセスを継続的に監視し、不審な挙動や侵害兆候の発生を早期に検知・対応します。
- 侵入後の横展開・暗号化の拡大を抑制**
検知した脅威の挙動を、他のシステムやネットワークに広げないよう、自動的に検知・遮断します。
- 独自開発のログ蓄積、レポート機能**
アラートの通知やレポートを一覧化し、発生時の調査・分析・復旧の効率化を実現します。

サポート体制

サーバセキュリティの専任チームが管理・運用をサポートします。運用上のご不明点などは、お気軽にご相談ください。

カスタマーサポート
カスタマーサクセス
テクニカルサポート

料金について

図解を参照し、詳細な料金体系をご確認ください。

初期費用	運用費用
165,000円	16,500円/月

その他、高いセキュリティのサーバと環境をご提供しています

仮想化環境 (HVC) ソリューション
NUTANIX

クラウド型WAFサービス
攻撃遮断くん

No.1

INCRAVE インクレイブ株式会社
〒980-0004 宮城県仙台市青葉区大森1-14 TAKAYUKIビル
0570-086190

■社会的背景・課題

1. ランサムウェア被害の深刻化

ランサムウェアとは、企業や組織のシステムやデータを暗号化して使用不能にし、その復旧と引き換えに金銭を要求するサイバー攻撃です。

近年では攻撃手法が高度化・巧妙化しており、事業停止と復旧に数か月を有する被害事例が多数公表されています。

実際に、ランサムウェア攻撃の被害報告件数は2022年7月～2024年6月で174件、被害額は平均で6,019万円にのぼります（※1）。企業規模に関わらず、中小企業から、国内の大手飲料グループ会社、大手通信販売会社まで被害を受けています。

年々ランサムウェア攻撃のリスクが高まっており、安全に企業活動を行う上で、サイバーセキュリティ対策は必須ともいえます。

2. サイバーセキュリティ対策を取り巻く考え方の変化

今までのサイバーセキュリティ対策は、「いかに脅威の侵入を防ぐか」という観点が重視されてきました。しかし、サイバー攻撃の手口はますます巧妙化しており、脅威の侵入を防ぎきれなくなってきました。

そのため、ここ数年では、「脅威の侵入は必ずしも防げない」という前提に立ち、「侵入された場合、いかに早く検知して被害の拡大を防ぐか」というアプローチも重視するようになってきています。

IPAの「SECURITY ACTION」（※2）と、2026年度中に運用開始を予定している、経済産業省の「サプライチェーン強化に向けたセキュリティ対策評価制度」（※3）の中にも、「侵入を前提とした対策」の考え方が含まれており、社会全体でもこの考え方が浸透しつつあります。

こうした社会的背景とサイバーセキュリティ対策の変化を受け、当社では本サービスの提供を開始しました。

※1：NPO 法人日本ネットワークセキュリティ協会 インシデント損害額調査レポート 別紙 2025年版
<https://www.jnsa.org/result/incidentdamage/202507.html>

※2：独立行政法人 情報処理推進機構（IPA） SECURITY ACTION とは？
<https://www.ipa.go.jp/security/security-action/sa/>

※3：経済産業省 「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」（SCS 評価制度の構築方針）を公表しました
<https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html>

■「ランサムウェア対策サービス」とは

ランサムウェアだけでなく、マルウェア、不正アクセスなどの脅威を検知し、サーバ本体を守る堅牢なサイバーセキュリティ対策です。挙動監視で兆候を捉え、即時対処することで、情報漏洩や業務停止などのリスクを低減します。

また、導入から運用・保守まで、専任チームが安全な運用をサポートいたします。

[概要]

- ・導入対象：弊社クラウドホスティング上の専有サーバおよび、お客様にてご契約中の専有 VPS サーバ
※お客様にてご契約中の専有 VPS サーバにつきましては、インストール作業はお客様にてご対応いただきます。
- ・提供方法：初期費用 165,000 円（税込） + 月額 16,500 円（税込）
- ・提供開始日：2026 年 5 月 21 日（木）

■サービスの特長

1. AI による監視で未知の脅威、侵入の兆候も見逃さない

24 時間 365 日、サーバ内部のプロセスや通信の動きを監視します。

人手による監視では難しい常時監視体制を AI で実現し、不審な挙動を即座に検知・自動隔離します。

また、AI が検知・分析するため、刻一刻と進化する未知の攻撃に対しても早期に対処することができます。

2. 不審プロセスの遮断で被害拡大を防止

不審なプロセスを検知すると、自動で脅威を遮断します。

人手を介さない即時対応により、侵入後の被害拡大を最小限に食い止めます。これにより、業務停止の長期化や復旧コストの増大といった二次的なリスクを低減します。

3. バックアップ機能によるファイル復元

暗号化されたファイルは、バックアップ機能により復元することが可能です。万が一ファイルを暗号化された場合に備えることができます。

※弊社指定の対象サーバをご契約の方が対象です

4. 専任チームによる安心のサポート体制

サーバ・セキュリティの専任チームが管理・運用をサポートします。運用上のご不明点などは、お気軽にご相談ください。

■今後の展開

検知した脅威やサーバの状況をより分かりやすく確認いただけるレポート機能の提供を、今後予定しています。

なお、本機能の内容および提供時期は変更となる場合があります。

■初年度導入目標

提供開始初年度の導入目標を30件に設定し、販売活動を行います。本サービスの普及と提供体制の強化を進め、ランサムウェアを始めとするサイバー攻撃のリスクが高まる中、より多くの企業が安心して事業活動を継続できる環境づくりと、社会全体のセキュリティ向上に貢献してまいります。

■各種資料について

サービスサイト：<https://cloud.incrave.co.jp/>

本記事ダウンロード：https://incrave.co.jp/pressrelease/20260521/inc_pressrelease.pdf

画像ダウンロード：<https://incrave.co.jp/pressrelease/20260521/flyer1.jpg>

<https://incrave.co.jp/pressrelease/20260521/flyer2.jpg>

■会社概要

会社名：インクレイブ株式会社（拠点：仙台・東京・新潟・青森）

取締役社長：丸山 秀行

資本金：5,000万円

営業所：宮城（仙台本社）・東京・新潟・青森

所在地：〒980-0804 宮城県仙台市青葉区大町2-10-14 TAKAYU パークサイドビル5F

電話番号：022-796-6101(代表)

Webサイト：<https://incrave.co.jp/>

公認資格：プライバシーマーク（登録番号：23820036号）

取引銀行：七十七銀行・三井住友銀行・仙南信用金庫

■本件に関する問い合わせ

インクレイブ株式会社 カスタマーセンター

- ・お電話でのお問い合わせ

TEL：022-796-6101（受付時間 9:00～17:30 土・日・祝日を除く）

- ・インターネットからのお問い合わせ

<https://incrave.co.jp/customer/contact>