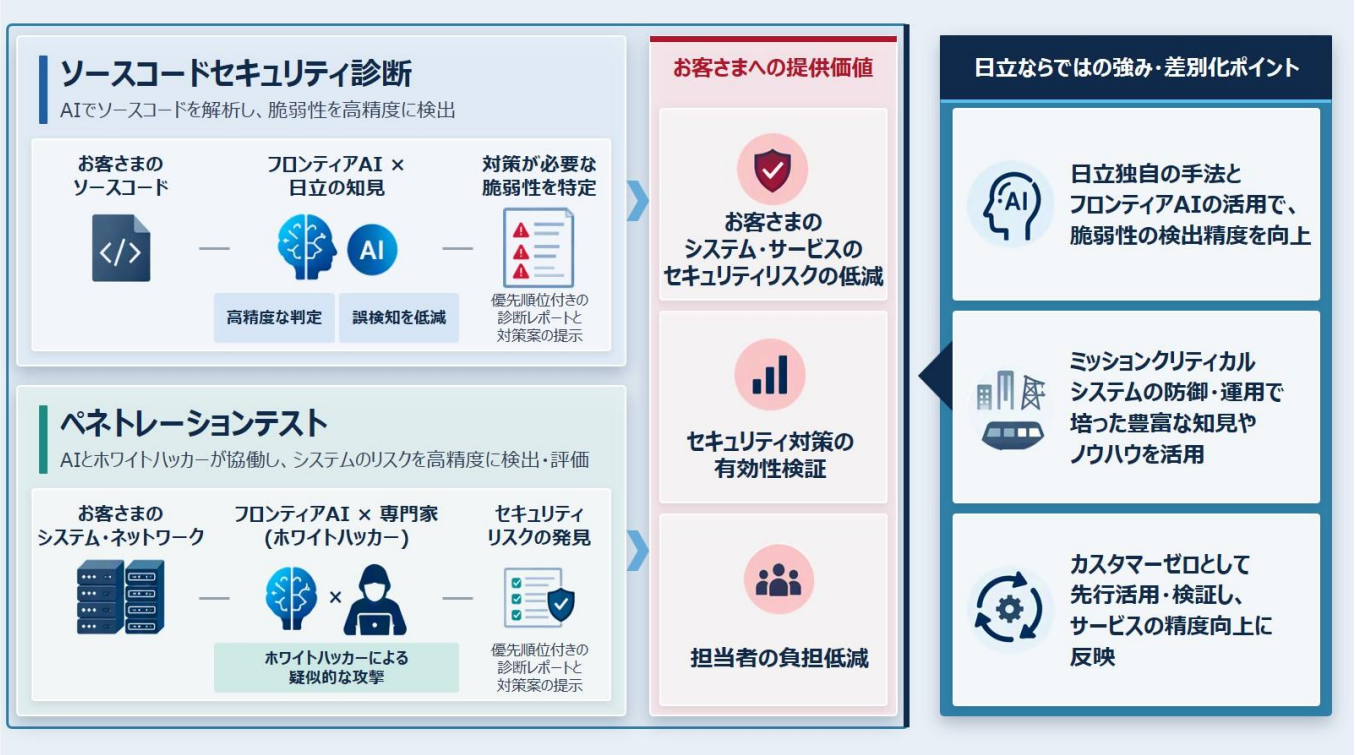
お知らせ

2026 年 11 月 12 日

日立の防御・運用の実践知とフロンティア AI を活用し、脆弱性やセキュリティリスクを高精度に検出する「ソースコードセキュリティ診断」と「ペネトレーションテスト」を提供開始

攻撃者に先んじたリスク対策で、サイバー攻撃の未然防止や被害の最小化に貢献



サービス概要図

生成 AI を活用して作成

株式会社日立製作所(以下、日立)は、社会インフラの現場で培ったミッションクリティカルシステムの防御・運用の実践知と Anthropic、OpenAI などのフロンティア AI モデルを活用し、脆弱性やセキュリティリスクを高精度に検出する「ソースコードセキュリティ診断」と「ペネトレーションテスト」を本日より提供開始します。両サービスは、脆弱性やセキュリティリスクの検出から優先順位付けされた対策立案までを支援します。これにより攻撃者に先んじてリスクを把握し、適切な対策につなげることで、サイバー攻撃の未然防止や被害の最小化に貢献します。これらは、AI 時代の事業継続を支援するオペレーショナルレジリエンスサービス「HMAX Cyber」に位置付けられるものです。

「ソースコードセキュリティ診断」は、お客さまが社内外に提供する IT サービスのソースコードを AI によって解析して脆弱性を高精度に検出し、優先して対処すべき脆弱性の診断レポートとその対策案を日立のセキュリティの専門家が提示します。また、「ペネトレーションテスト」は、日立のホワイトハッカーと AI が協働[*1]してお客さまのシステムを疑似的に攻撃します。これにより、セキュリティリスクの潜む箇所を見つけ出し、対応優先順位を付けた診断レポートと対策案を提示します。両サービスは、25 年以上にわたり脆弱性診断サービスを提供してきた株式会社日立ソリューションズ(以下、日立ソリューションズ)の知見とノウハウを生かし、日立グループ各社と連携し、お客さまのセキュリティ強化を支援します。また、カスタマーゼロとして金融・公共分野などのシステム開発環境において先行的に活用し、その有効性を検証するとともに、精度向上などのサービス改善に反映しています。

これら 2 つのサービスは、AI 時代の事業継続を支援するオペレーショナルレジリエンスサービス「HMAX Cyber」の Govern & Identify に位置付けられ、「HMAX Cyber」の各種サービスと連携することで、お客さまのシステム環境の 24 時間 365 日の継

続監視、サイバー攻撃を前提とした回復設計、被害発生後の迅速なデータ復旧[*2]、経営層を巻き込んだ BCP(事業継続計画)の実行までを一貫して支援します。

日立は今後も、AI の実装・活用やセキュリティの専門知見を有する Frontier AI Deployment Center(FADC)と、現場の課題解決を支援する FDE Team の連携を強化し、検出した脆弱性やリスクに対して、対策の具体化や実装を支援します。

さらに、お客さまの事業継続を支えていくためには、脆弱性が発生しにくく、継続的なセキュリティ対策を行いやすいシステム構成への見直しが重要です。日立は、お客さまの事業環境の変化に応じた既存システムの改善や刷新などのモダナイゼーションまで幅広く支援することで、最新のセキュリティ対策を迅速に取り入れやすい環境を実現し、セキュリティ強化と事業継続性、レジリエンスの向上に貢献していきます。

*1 ホワイトハッカーとの協働は、Professional プランが対象です。

*2 日立ヴァンタラのストレージによるデータ保護技術を活用したソリューション

背景

近年、AI の進化により、サイバー攻撃はこれまで以上に巧妙化かつ高速化しています。攻撃者は AI を利用して、多数の企業や広範なシステムを対象に同時多発的な攻撃を実行しており、企業や組織が把握できていない脆弱性やセキュリティリスクが狙われる危険性が高まっています。そのため、企業や組織は、攻撃者に先んじて自社システムや社内外に提供しているサービスに潜む脆弱性やリスクを把握し、優先順位の高い脆弱性から迅速に対策を講じることがこれまで以上に重要になっています。一方で、従来の脆弱性やセキュリティリスクの探索は専門家による人手作業が中心であり、調査できる範囲や頻度には限界がありました。また、従来のツールは誤検知が多く、検出結果の正誤判断に時間を要するうえに、対応すべき脆弱性の判断や優先順位付けにも専門的な知見、時間を要する状況がありました。このようなことから、広範なシステムを効率的に調査し、対応が必要な脆弱性やセキュリティリスクを的確に見極め迅速な対策をとることが求められています。

新サービスの特長

（1）ソースコードセキュリティ診断

お客さまからお預かりしたアプリケーションのソースコード[*3]をフロンティア AI で解析し、検出した脆弱性を日立のセキュリティの専門家が対応優先度を評価した上で、対策案とともにレポートとして提供します。AI が処理の流れや依存関係などの文脈を考慮してソースコードを詳細に解析することで、従来のツールで生じていた誤検知を低減するとともに、これまで検出が難しかった複数の機能が連携するような複雑な業務処理などのビジネスロジック起因の脆弱性についても、高度なセキュリティスキルを持つ人財と同等レベルで検出し、高精度に判定できます。また、AI が診断結果を整理し、対応の優先順位付けを支援します。これにより、検出結果の正誤判定にかかる工数を低減し、危険性の高い脆弱性の対策に注力できる環境を実現することで、セキュリティ担当者の負担軽減につながるとともに、お客さまが社内外に提供する IT サービスのセキュリティリスクの低減に貢献します。

*3 お客さまからお預かりしたソースコードは、安全な環境で管理・解析するとともに、診断完了後は速やかに削除するなど、厳格なセキュリティ管理のもとで取り扱います。

（2）ペネトレーションテスト

日立のホワイトハッカーとフロンティア AI が協働し、攻撃者の視点で目標や手法を検討した上で、お客さまのシステムの偵察から攻撃までを疑似的に実行します。その結果を基に、システムやネットワークに潜む脆弱性やリスクを、高度なセキュリティスキルを持つ人財と同等レベルで検出・評価し、優先順位と対策案をレポートとして提供します。AI の活用により、従来と比べてコストや工数を抑えながら、セキュリティ対策の有効性を検証できます。これにより、重大な脆弱性やシステムの設定不備など、サイバー攻撃につながるリスクを把握するとともに、危険性の高いものから優先的に対策することで、企業システムのセキュリティリスク低減に貢献します。

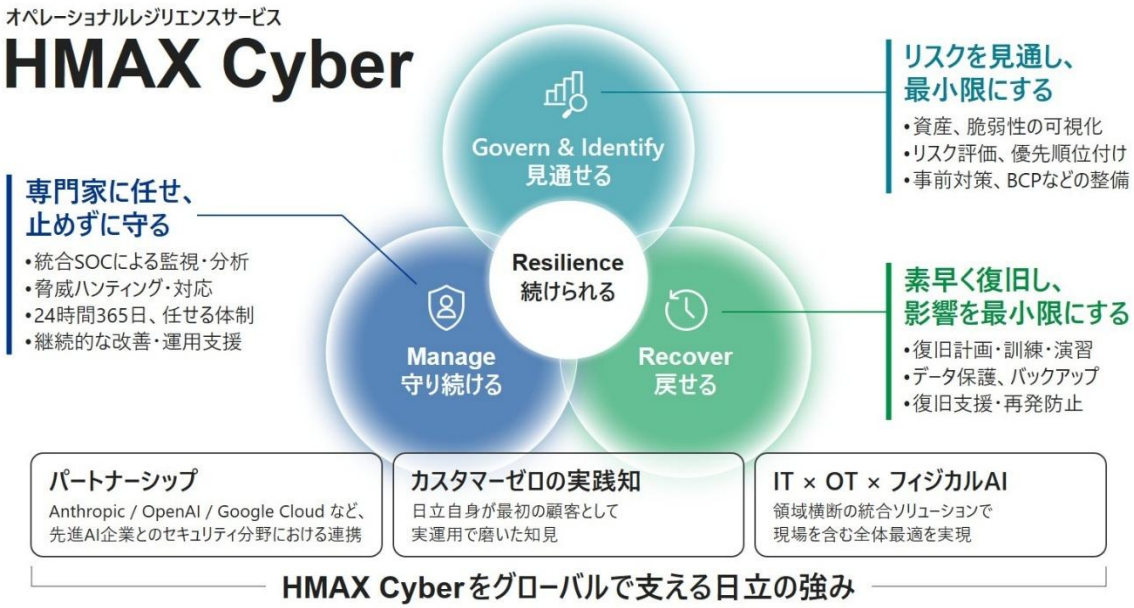
サービスの価格および提供開始時期

名称		概要	価格(税別)	提供開始時期
ソースコードセキュリティ診断[*4]	Liteプラン	フロンティア AI を活用して脆弱性を検出。検出結果に対して、日立の実践知を生かし、対応優先度と対策案を提示。	個別見積	2026 年 11 月 12 日
	Standardプラン	日立独自手法(ハーネス)[*5]とフロンティア AI を組み合わせて脆弱性を高精度に検出。検出結果に対して、日立の実践知を生かし、対応優先度と対策案を提示。		
ペネトレーションテスト[*6]	Standardプラン	フロンティア AI とペネトレーションテストを高精度に行うための独自手法(ハーネス) と長年にわたって培ってきたセキュリティに関するナレッジを組み合わせて疑似的な攻撃を実施。日立の実践知を生かし、対応優先度と対策案を提示。	個別見積	2026 年 11 月 12 日
	Professionalプラン	日立のホワイトハッカーと、フロンティア AI が協働し、独自の手法(ハーネス)や長年にわたって培ってきたセキュリティに関するナレッジも組み合わせて、より高度な疑似攻撃を実施。専門家の知見を生かした分析により、対応優先度と対策案を提示。		

*4 お客さまに応じて、日立または日立ソリューションズより提供します。（ソースコードセキュリティ診断）
*5 日立のカスタマーゼロのノウハウをもとに、AI への命令・指示を高度に設計することで、脆弱性の検出精度を向上させるための日立独自の手法。
*6 ペネトレーションテストの開発元は、日立ソリューションズです。（ペネトレーションテスト）

「HMAX Cyber」の概要

「HMAX Cyber」は、高度化するサイバー攻撃からお客さまのシステムを守り、事業継続を支援するオペレーショナルレジリエンスサービスです。潜在的なリスクを見通し、備える「Govern & Identify」、24 時間 365 日の監視・運用を支援する「Manage」、有事の早期復旧を行う「Recover」のサービスカテゴリーのもと、BCP(事業継続計画)の策定から脆弱性の可視化、サイバー攻撃の予防、迅速な復旧、BCP の実行までをトータルで支援し、お客さまのレジリエンス向上に貢献します。



関連ウェブサイト

HMAX Cyber：デジタル：日立

商標注記

記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

お問い合わせ先

株式会社日立製作所　AI＆ソフトウェアサービスビジネスユニット
お問い合わせフォーム：https://www.hitachi.co.jp/it-pf/inq/NR/?pr=261112

以上