◎ **ソースコード診断（令和8年11月12日時点）**

提供事業者	サービス名	サービス概要	価格	備考	連絡先
アマゾンウェブサービスジャパン合同会社	AWS Continuum（AWS Security Agent） ソースコード診断等（プレビュー版）※未発売	https://aws.amazon.com/jp/blogs/news/aws-security-agent-full-repository-code-scanning-feature-now-available-in-preview/	未定 （現在はプレビュー版（無償）で提供中。正式提供時期、提供金額ともに現時点では未定のため、問合せ時点での状況をお伝えいたします）	（１）概要 検出結果の修正（ソースコードの自動修復）を除く推論等をすべて日本国内で完結するAIを活用して、システム等のソースコードの診断を実施し、セキュリティの脆弱性を自動的に発見及び検証して修正を提案する機能。再現手順、検証コード、推奨コード修正案等を記載した詳細なレポートが出力可能であり、全体状況の把握や修復及び対策工程において活用可能。 （参考資料） https://docs.aws.amazon.com/securityagent/latest/userguide/security-best-practices.html#_cross_region_inference:~:text=Japan%20%E2%80%94%20Asia%20Pacific%20(Tokyo)%20%E2%80%93%20ap%2Dnortheast%2D1 （２）実行可能な対象 地方公共団体のウェブシステム等（※その他実行可能な対象等については参考資料参照）。オンプレミスのシステムやAWS以外のクラウドサービス上に構築されているシステムに対しても実行可能。 （参考資料） https://docs.aws.amazon.com/ja_jp/securityagent/latest/userguide/connect-agent-vpc.html （３）必要な事前準備等 AWSアカウント（コンソールアクセスのためにインターネットが必要） （４）補足 ソースコード診断は現在「プレビュー版」であり、本番提供前の試行段階として一部機能を先行提供し、改善要望等を受け付けている段階。現時点で「GA（General Availability／一般提供）には至っておらず、正式な提供の時期、および提供金額は未定。	aws-jp-pubsec-lg-security-scan@amazon.com
SB OAI Japan合同会社 / ソフトバンク株式会社	Patching as a Service（PaaS）ソースコード診断	https://www.softbank.jp/business/service/security/paas/	コード1行あたり1.5円～ ※2026年11月1日時点	【提供企業】 ソフトバンクグループとOpenAIの合弁会社「SB OAI Japan」が提供 「最新モデルのフロンティアAIのサイバーモデル」を活用した脆弱性診断と対策案を提供するサービス。 【サービス概要】 最新モデルのフロンティアAIサイバーモデルを活用し、コードの脆弱性を見つけるだけでなく、攻撃の成立可否を確認し、具体的な修正案まで提示します。ソースコードに潜む脆弱性の検出から、攻撃の成立可否の確認、修正案の提示までを一貫して支援する。 【特徴】 コードの処理フローや周辺ロジックまで多面的に分析し、脆弱性の候補を検出。さらに、実際の環境で攻撃が成立するかを確認し、影響範囲を評価することで、優先的に対処すべきリスクを明確にする。	ソフトバンク株式会社 公共本部 自治体向けPaaS事務局 電話番号：080-4372-0649（担当：寺島） メールアドレス：GRP-LG-PaaS@g.softbank.co.jp
株式会社NTTデータ	AI駆動型ソースコード診断	サービスの詳細をご希望の場合は、メールにてお問い合わせください。サービス概要資料をお送りいたします。	個別見積/要相談		frontier-ai-security@hml.nttdata.co.jp

提供事業者	サービス名	サービス概要	価格	備考	連絡先
グーグルクラウドジャパン	CodeMender（診断結果のトリアージまで行う場合は+Wiz）※未発売	https://cloud.google.com/security/codemender?hl=ja&e=48754805 （Wiz： https://www.wiz.io/ja-jp）	価格はこちらの前提で積算となります Code Mender（ソースコード解析） ・プログラミング言語 ・ステップ数 ・ファイル数 ・ファイルサイズ（最大のもの） Wiz（脆弱性の優先順位付け） ・稼働しているシステムがオンプレミス環境か、クラウド環境か（クラウド環境の場合ベンダー名） ・仮想マシン台数（クラウド上のサーバー数／Amazon EC2） ・バケット数（クラウド上のデータ／Amazon S3） ・データベース（データベース数／Amazon RDS等） 役務 ・期間や診断回数、既存事業者との責任分界点により異なります	CodeMenderは現在プレビュー中で12月頃正式リリース予定です データ保持ポリシーhttps://docs.cloud.google.com/gemini-enterprise-agent-platform/codemender#what-is-the-retention-policy ・最長7日間保持：セッション再開用途のみ。7日後に自動完全削除（Zero Data Retention）。 ・即時削除対応：DeleteInteraction API呼出により作業直後に即時データ破棄が可能。 ・オンメモリ保持：脆弱性検出結果やパッチは実行中メモリ上のみ保持し長期DB不保持。 現時点ではグローバルリージョンのみ。今後の需要に応じて日本国内へ処理を閉じる機能を計画中。 ISMAPは現時点で未登録で、申請に向けて社内手続き中	Google Cloud 自治体様向け セキュリティ脆弱性診断 相談窓口 googlecloud-jp-lg-security@google.com
トレンドマイクロ株式会社	TrendAI™ Autonomous Vulnerability Discovery ※未発売	AIを活用した発見技術と専門家による検証を組み合わせ、信頼性が高く、実行可能な検出結果を提供します。お客様のソースコード全体を広範囲に分析し、脆弱性、悪用される可能性のある脆弱性、新たな脅威、ゼロデイ脆弱性を自律的に特定します。 TrendAI™、自動で脆弱性を発見する「TrendAI™ Autonomous Vulnerability Discovery」を提供開始：AI速度で実現する次世代の脅威対応 | トレンドマイクロ https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20261001-01.html	お問い合わせください	リリース日： 2027年第1四半期（変更の可能性あり） 一部の詳細はまだ確定していません。記載のリリース時期および価格は確約されたものではなく、変更される可能性があります。	トレンドマイクロ羽田、藤原 cybersecurity_for_localgovernments@trendmicro.com
日本電気株式会社	Threat-Driven Security Assessment※未発売	https://jpn.nec.com/press/202609/20260902_02.html （紹介ページは12月末に整備予定です、詳しくはお問い合わせください）	500,000LOC：11,500,000円 LOC:lines of Code（行数）	・正式見積にあたっては、見積ヒアリングシートへの回答が必要となります。 ・ソースコード情報の受け渡し方法については、弊社ファイル転送・共有クラウドサービス（Box等）を利用する想定です。 ・提供いただいたソースコードは脆弱性診断の実施にのみ利用し、AIモデルの学習データとして利用することはありません。 ・クラウド上で診断が行われますが、現状、診断時のリージョン指定ができないため、海外リージョンで診断を行われる可能性があります。 （海外へソースコード持ち出しをすることに対して、ご了承をいただく必要があります） ※国内リージョン指定バージョンについては、FY26年度内にリリース予定です。 ・当社ＡＩソースコード診断用の標準契約約款に基づくご契約となります。 （ＡＩによる診断への同意等が必要となります。）	導入前のご相談・お問い合せフォーム（企業・官公庁・通信事業者のお客さま） https://inquiry.nec.com/webapp/form/26880_wtnb_3/index.do?inqid=1208cybersec
株式会社日立システムズ	SHIELD 脆弱性診断サービス※未発売	SHIELD 脆弱性診断サービスについて： https://www.hitachi-systems.com/solution/s003/shindan/ ※資料入手については、相談窓口に問い合わせください	個別見積	SHIELD 脆弱性診断サービスにおいて、2026年11月中に高性能AIを使ったサービスを提供開始予定。 2026年11月中旬頃からご相談対応可能。	HISYS_ssp_kk@hitachi-systems.com

◎ **フロンティアAIテスト（令和8年11月12日時点）**

提供事業者	サービス名	サービス概要	価格	備考	連絡先
アマゾンウェブサービスジャパン合同会社	AWS Continuum（AWS Security Agent） ペネトレーションテスト	https://aws.amazon.com/jp/security-agent/	1タスク時間あたり 50 USD （参考資料） https://aws.amazon.com/jp/blogs/news/aws-security-agent-on-demand-penetration-testing-now-generally-available/	（１）概要 検出結果の修正（ソースコードの自動修復）を除く推論等をすべて日本国内で完結するAIを活用して侵入テスト等を実施し、セキュリティの脆弱性を自動的に発見及び検証して修正を提案する機能。数時間程度で実行可能であり、再現手順、検証コード、推奨コード修正案等を記載した詳細なレポートが出力されるとともに、全体状況の把握や修復及び対策工程において活用可能。 （参考資料） https://docs.aws.amazon.com/securityagent/latest/userguide/security-best-practices.html#_cross_region_inference:~:text=Japan%20%E2%80%94%20Asia%20Pacific%20(Tokyo)%20%E2%80%93%20ap%2Dnortheast%2D1 （２）実行可能な対象 インターネットに公開されている地方公共団体のウェブシステム等（※その他実行可能な対象等については参考資料参照）。オンプレミスのシステムやAWS以外のクラウドサービス上に構築されているシステムに対しても実行可能。 （参考資料） https://docs.aws.amazon.com/ja_jp/securityagent/latest/userguide/connect-agent-vpc.html （３）必要な事前準備等 AWSアカウント（コンソールアクセスのためにインターネットが必要）	aws-jp-pubsec-lg-security-scan@amazon.com
SB OAI Japan合同会社 / ソフトバンク株式会社	Patching as a Service（PaaS）ブラックボックス診断	https://www.softbank.jp/business/service/security/paas/	1,000,000円～ / 1システムあたり ※2026年11月1日時点	【提供企業】 ソフトバンクグループとOpenAIの合弁会社「SB OAI Japan」が提供 「最新モデルのフロンティアAIのサイバーモデル」を活用した脆弱性診断と対策案を提供するサービス。 【サービス概要】 最新モデルのフロンティアAIサイバーモデルを活用し、攻撃者の視点からWebシステムの侵害リスクを診断するサービスです。 対象URLを起点にWeb・API・認証を調査し、攻撃シナリオの生成から攻撃成立性の評価までを行います。 【特徴】 AIによる攻撃経路の探索と攻撃成立性の評価。 「脆弱性があるかどうか」だけでなく、「攻撃が成立する」ことから、対策の優先順位を判断しやすく実効性のあるセキュリティ対策を支援する。 パートナー経由で提供もできるので既存業者経由でもサービス提供可能。※侵入可否診断を早期に実施することも可能	ソフトバンク株式会社 公共本部 自治体向けPaaS事務局 電話番号：080-4372-0649（担当：寺島） メールアドレス：GRP-LG-PaaS@g.softbank.co.jp
グーグルクラウドジャパン	Mandiant コンサルティングペネトレーションテスト	https://cloud.google.com/security/consulting/mandiant-penetration-testing?e=48754805&hl=ja	1.対象アプリケーションの概要とシステム数 2. アプリケーションの規模（アタックサーフェス） ・動的ページ数やソースコード行数など 3. ユーザーロール（権限種別）と管理画面・テナント構成 4. 診断方式（ソースコード・仕様書の提供可否） 5. 実施時期・体制等の特別な制約事項 ・ご希望の実施時期・完了期限：（例：202X年○月頃までに実施・報告完了希望） ・テスト実施時間帯の制限：（平日日中で問題なし / 夜間・休日のみ等の制限あり） ・特別な制限事項：（国籍要件、現地オンサイト作業の必須有無、その他特記事項）		Google Cloud 自治体様向け セキュリティ脆弱性診断 相談窓口 googlecloud-jp-lg-security@google.com

提供事業者	サービス名	サービス概要	価格	備考	連絡先
トレンドマイクロ株式会社	TrendAI Vision One™ Adversarial Exposure Validation（Cyber Risk Exposure Management の機能）※未発売	AIエージェントが実際の攻撃手法に基づいて仮想的な攻撃を自律的に行ない、 その攻撃実現性の度合いに応じてリスクを評価し、改善を促す（推奨対策を示す）ものです。 具体的には、AIエージェントが、特定されたCVE脆弱性や設定不備等が実際に攻撃に悪用できるか、 それを繰り返すことで攻撃者が重要資産まで到達することができるかを検証し、その結果に基づいて優先度に基づいた改善策を提示します。 TrendAI Vision One Cyber Risk Exposure Management : Cyber Risk Exposure Management (CREM) | TrendAI (JP)https://www.trendaisecurity.com/ja/platform/cyber-risk-exposure-management 本機能の紹介資料は、上記連絡先にご依頼いただければご提供します。	お問い合わせください	2027年（変更の可能性あり）現在パブリックプレビューの準備中 一部の詳細はまだ確定していません。上記のリリース時期および価格は確約されたものではなく、変更される可能性があります。	トレンドマイクロ羽田、藤原 cybersecurity_for_localgovernments@trendmicro.com