

政府の「革新的 AI サイバー防御」の取組に呼応し、OGC 参画企業による民間主導の対策・検討状況を毎月公開へ

～2026 年 9 月末時点の各社最新取組を公表～

一般社団法人オープンガバメント・コンソーシアム（以下、OGC）は、政府が推進する AI を活用したサイバー防御体制の構築に向けた動きに呼応する形で、参画企業による民間主導のサイバーセキュリティ対策および検討を積極的に推進しております。

昨今、革新的 AI 技術の急速な進展に伴い、サイバー脅威が高度化・複雑化する一方、AI を駆使した防御陣形の構築やリスク管理の重要性はかつてないほど高まっています。こうした背景のもと、OGC では民間企業の主体的なアクションとして、参画各社が進める最先端の技術検証、国際的なイニシアチブへの参画、具体的なソリューション展開などの取組状況を整理し、広く社会へ発信していくこといたしました。

本取組の一環として、参画各社の最新の対策状況を、毎月継続的に公開してまいります。今回は、2026 年 9 月末時点における各社の革新的 AI サイバー防御への検討・対策状況を取りまとめました。

OGC は今後も、政府の施策と緊密に足並みを揃えながら、民間主導の強力なサイバー防御体制の具現化と、安全・安心なデジタル社会の実現に向けて、積極的な情報発信と対策の推進をリードしてまいります。

OGC 各社の革新的 AI サイバー防御への検討や対策状況をご紹介します。| 2026 年 9 月度
(会社名：五十音順)

会社名：株式会社チェンジホールディングス

取り組み：

2026 年 10 月 8 日より、「サイバー攻撃対応ナビ」の提供を開始します。（10 月 1 日より申し込み受付開始）

「サイバー攻撃対応ナビ」は、サイリーグ HD と SMBC サイバーフロントが共同開発した AI セキュリティ判断支援サービスです。SMBC グループ、株式会社ラック（JLIST®）、株式会社ピーエスシー、株式会社クエスト等、国内企業・組織のセキュリティ運用現場で蓄積された知見・データを活用し、汎用的な回答ではなく、実務に即した判断支援を目指します。

セキュリティアラートや SOC 通知、サイバー攻撃の可能性のある事象について入力することで、AI が内容を整理し、危険度、確認すべき項目、推奨される対応手順等を提示します

「これはサイバー攻撃の兆候なのか」「今すぐ対応すべきなのか」「次に何を確認すべきなのか」。セキュリティ担当者は「危険かどうか分からない」「何から確認すべきか分からない」という状態から脱し、根拠を持って初動対応に移ることができます。

参考情報：

<https://www.cyleague.jp/service/cyber-navi/>
<https://www.changeholdings.co.jp/news/334/>
<https://www.changeholdings.co.jp/news/333/>

会社名：TISI 株式会社

取り組み：

■ AI を活用した脆弱性対応の迅速化

TISI は、金融分野の脆弱性対応を支援するセキュリティ運用基盤モデル「AI Security Control Plane」の取り組みを開始しました。

脆弱性情報やシステム構成、診断結果、攻撃状況などを統合し、AI による継続的なリスク評価と対応の優先順位付けを通じて、防御側の対応を迅速化します。

■ 自動化と人による統制の両立

AI エージェントが対応方針を提示し、人の承認を経て修復・検証・適用を進める「Human in the Loop」を採用しています。

金融機関に求められる承認プロセスや監査証跡を考慮し、迅速な対応と運用の統制を両立します。

■ 各社の技術と運用知見を結集

TISI の基幹システム構築・運用の知見に、協力関係にある企業の先進技術を組み合わせて提供します。

(詳細はプレスリリースをご覧ください)

参考情報：

TISI、フロンティア AI を悪用したサイバー攻撃に対応するセキュリティ運用基盤「AI Security Control Plane」の取り組みを開始（2026 年 9 月 15 日）

https://www.tisi.jp/news/2026/tisi_news/20260915_1.html

会社名：トレンドマイクロ株式会社

取り組み：

1. 基本的な対策の、全般的かつ確実な実施をサポート

-- クライアント PC、メール、クラウドなど、組織全体で多層防御を、AI セキュリティプラットフォーム「TrendAI VIsion One」で提供

-- 個々のセキュリティ対策製品のアラートの集中管理、相関分析により、見つけづらい脅威を組織全体早期に把握、対応する XDR

-- セキュリティイベントの収集、分類、調査に AI を活用し、検知と対応を加速、自動化する Agentic SIEM を提供

2. 脆弱性を含む組織のサイバーリスクを可視化、優先度づけ、軽減するサイバーリスク管理ソリューション「Cyber Risk Exposure Management」の提供。

-- 加えて、サイバーリスクと想定被害を定量化・スコアリングし、経済的損失（金額）として可視化することで、経営層の理解、把握、管理、戦略立案を促進（Cyber Risk Quantification）

3. 仮想パッチの提供

-- 世界各地の研究者が参加する脆弱性発見コミュニティ「TrendAI Zero Day Initiative（ZDI）」で発見した脆弱性に対して、正規パッチに先行して最大 115 日早く仮想パッチによる保護を提供。AI による脆弱性探索の効率化が進む中、正規パッチ前の「空白期間」を埋める手段を提供。

4. AI を管理下に置くためのソリューションを提供

-- AI 利用状況と関連リスクの可視化（Visibility）

Cyber Risk Exposure Management（CREM）、Data Security／DSPM により、公認・シャド―AI を含む AI の利用状況、AI 関連アセット、攻撃経路、機密データの流入を可視化

-- AI アプリケーションの挙動と脅威の監視（Observability）

AI Application Security（AI Scanner＋AI Guard）により、AI アプリケーションの出荷前スキャンと運用時のプロンプト・出力・ツールコールの検査を実施。XDR により、AI テレメトリとエンドポイント、ネットワーク、ID のシグナルを相関分析し、異常検知と調査を支援

-- AI に関わるコード、権限、ID の管理（Ownership）

Cloud Security（Code Security／Container Security、Cloud Risk Management）と AI Secure Access により、漏えいシークレット、コンテナ、過剰権限、非人間 ID、AI ツールへのアクセスを管理・制御

-- AI が管理下にあることを証明するガバナンス（Governance）

上記 3 つの取り組みを通じて、AI 資産、利用状況、リスク、アクセス、対応状況を一元的に把握し、経営層や監査人に AI が管理下にあることを説明・証明できる状態を支援

5. AI を活用した脆弱性研究と予防型サイバー防御を高度化

-- 脆弱性・脅威研究の高度化

セキュリティサーチ基盤 AESIR（AI-Enhanced Security Intelligence & Research）により、世界中の脆弱性・脅威動向を継続的に監視。AI を活用したゼロデイ脆弱性の発見、分析、トリアージにより、脅威への対応力を強化

-- 脆弱性対応と早期保護の迅速化

Claude Opus などの先端 AI を活用して脆弱性の影響度、悪用可能性、緊急度を分析し、対応優先度の判断を支援。正式パッチが提供されるまでの期間には、仮想パッチによる早期保護につなげる

-- TrendAI Cybertron による予防型サイバー防御

TrendAI Vision One に組み込まれたサイバーセキュリティ AI により、脅威の検知・分析・防止を高度化し、顧客環境に応じたセキュリティ推奨と対応を支援

-- 先端 AI 技術・セキュリティエコシステムとの協業

OpenAI、Anthropic、NVIDIA などの AI 企業、研究機関、技術コミュニティとの連携を通じて、AI を活用した脆弱性研究、脅威分析、サイバー防御技術の実装を推進

参考情報：

"脆弱性研究 AI を活用したセキュリティサーチ基盤「AESIR」：

https://www.trendmicro.com/ja_jp/research/26/a/aesir.html

エージェント型エクスプロイト修復エンジン「AESIR」を拡張：

https://www.trendmicro.com/ja_jp/research/26/h/trendai-advances-threat-hunting-to-dynamic-real-world-exploitation-of-ai-infrastructure.html

自動で脆弱性を発見する「TrendAI™ Autonomous Vulnerability Discovery」を提供開始：

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20261001-01.html

脆弱性対応・早期保護 Claude Opus 5 で脆弱性の優先順位付けと仮想パッチを強化：

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260731-01.html

CISA KEV を活用した脆弱性管理を強化：

https://www.trendmicro.com/ja_jp/research/26/h/cisa-kev-commitment-ai-vulnerability-management.html

OpenAI の GPT サイバーモデルで、エクスポージャー時間の短縮を推進 :

https://www.trendmicro.com/ja_jp/research/26/i/trendai-brings-openai-daybreak-models-into-the-race-to-shrink-exposure-time-to-zero.html

AI セキュリティの研究・実証・連携 CyberGym の AI セキュリティベンチマークで首位を獲得 :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260903-01.html

OpenAI DayBreak Cyber Partner Program に参画 :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260623-01.html

Anthropic との AI セキュリティ連携を強化 :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260414-01.html

Anthropic の Glasswing に参加 :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260604-01.html

Nvidia の Open Secure AI Alliance に参画 :

https://www.trendmicro.com/ja_jp/research/26/g/open-secure-ai-alliance.html

NVIDIA Agent Safety Platform を拡張 :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260930-01.html

AI セキュリティ製品・基盤への実装 組織横断でサイバーリスクを可視化・優先順位付けし、対応を支援するプラットフォーム :

<https://www.trendaisecurity.com/ja/platform>

Claude Compliance API を TrendAI Vision One に統合 :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260625-01.html

Claude Compliance API の連携対象を Claude Code と Cowork に拡張 :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20261002-01.html

AWS 上の AI ワークロードを保護するアーキテクチャ :

https://www.trendmicro.com/ja_jp/research/26/h/the-architecture-behind-a-billion-dollars-how-customers-run-trendai-vision-one-on-aws-and-secure-their-ai-workloads.html

AI セキュリティに関する研究・知見 AI エージェントの構造的なサイバーリスクを実証 (PwC コンサルティングとの共同レポート) :

https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260717-01.html

会社名：パロアルトネットワークス株式会社

取り組み：

■パロアルトネットワークス、Unit 42 の Continuous Frontier AI Defense を通じて Anthropic の Mythos (ミトス) および OpenAI の GPT-5.6 を顧客に提供

<https://www.paloaltonetworks.jp/company/press/2026/palo-alto-networks-delivers-anthropic-s-mythos-and-openai-s-gpt-5-6-to-customers-with-unit-42-continuous-frontier-ai-defense>

主な機能は以下のとおりです。

Continuous Testing Engine（継続的テストエンジン）

企業全体のベースラインスキャンを実施した後、環境変化に応じて継続的なセキュリティテストを実行します。

Multi-Model AI Harness（マルチモデル AI 基盤）

タスクごとに最適な AI モデルへ処理を振り分ける独自アーキテクチャを採用し、精度とカバレッジを向上させながら、最先端 AI の運用コストを管理します。

Leading Cyber Models（先進的サイバーセキュリティ向け AI モデル）

Anthropic Claude Mythos 5 や OpenAI GPT-5.6-Cyber をはじめとする高度な能力を備えた AI モデルに加え、オープンウェイトモデルを活用して構築されています。

Advanced Adversary Simulation（高度な攻撃者シミュレーション）

自社およびサードパーティの Web アプリケーション、API、クラウドインフラ、ソースコードリポジトリ、ネットワーク資産に対するエンドツーエンドの攻撃経路を検証し実際の悪用可能性を実証します。

Accelerated Remediation（修復の迅速化）

優先順位付けされた実行可能な修正策、コードレベルのガイダンス、仮想パッチの推奨を提供します。脆弱性が公表される前や正式なパッチが存在しない段階でも、Frontier Virtual Patching と組み合わせることで仮想パッチの適用が可能です。

■ OpenAI のサイバー モデルをセキュリティ業務に活用

<https://www.paloaltonetworks.com/blog/2026/09/putting-openai-cyber-models-to-work-for-defenders/?lang=ja>

本日発表するのは、OpenAI とのパートナーシップを通じた Unit 42 Frontier AI Exposure Analysis の拡張です。この拡張により、顧客環境での業務に先進的なフロンティア サイバー モデルを直接活用できます。Unit 42 の指示により、これらのモデルがエクスポーチャの発見、エクスプロイト可否のテスト、攻撃経路の検証、最優先で修正すべき問題の優先順位付けの支援を行います。

■ フロンティア AI 時代のネットワーク セキュリティの再定義

<https://www.paloaltonetworks.com/blog/2026/09/redefining-network-security-for-the-frontier-ai-era/?lang=ja>

本日、パロアルトネットワークスはフロンティア仮想パッチの提供を開始し、防御側に究極の優位性を提供しています。フロンティア AI を活用して未知の脆弱性を発見し、保護機能を数時間で導入することで、従来のパッチを展開するのにかかる業界平均の 55 日、リスクにさらされる期間をほぼゼロに短縮しています。これは、パッチの適用を迅速化することだけではありません。攻撃者がネットワークに到達する前にエクスプロイトを無効化することで、攻撃者の可能性を排除することでもあります。

※公開日：2026年10月8日

■ 一般社団法人オープンガバメント・コンソーシアムについて

オープンガバメント・コンソーシアム（OGC）は2009年4月の設立以来、オープンなクラウド技術による世界最高水準のデジタル政府・自治体の実現を目指してきました。2013年4月の一般社団法人化を機に、活動領域を従来の提言中心から、デジタルの視点による政策提言の深化、および社会実装に向けたモデル創出へと拡大させています。現在、私たちは民間サイドから政府方針を支援・促進するため、以下の4つの柱を軸に活動しています。

- ① サービス・アーキテクチャデザイン分科会
- ② サイバーセキュリティ分科会
- ③ デジタル人材分科会
- ④ 行政DX分科会

政策提言に留まらず、システムの標準化や実証、普及活動に積極的に関わることで、市民・利用者に寄り添ったサービスの実現を強力に推進し、社会の発展に貢献し続けてまいります。

活動目的や詳細については、こちらをご覧ください。<https://ogc.or.jp/about>

※ 記載されている会社名、製品名は、各社の登録商標または商標です。

※ 記載されている情報は、発表日現在のものです。最新の情報とは異なる場合がありますのでご了承ください。

【当発表に関するお問い合わせ先】

一般社団法人オープンガバメント・コンソーシアム（OGC）事務局

Mail： info@ogc.or.jp