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
～初回として 2026 年 5 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といたしました。

本取組の一環として、今後は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。初回となる今回は、2026 年 5 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いたします。｜2026 年 5 月度
（会社名：五十音順）

会社名：シスコシステムズ合同会社

取り組み：
Project Glasswing 初期パートナー

参考情報：
https://gblogs.cisco.com/jp/2026/05/rising-to-the-era-of-ai-powered-cyber-defense/

会社名：TIS 株式会社

取り組み：
重要インフラに関連する技術支援サービスを提供中
革新的 AI サイバー防御に関連するオファリングサービスを企画中

会社名：トレンドマイクロ株式会社

取り組み：
1.　基本的なサイバーセキュリティ対策の、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 を活用した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で早期に把握、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、想定される被害を定量的にスコア化、コスト換算するとすることで、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
-- 全世界にリサーチャーを要する脆弱性発見コミュニテイ「 TrendAI Zero Day Initiative (ZDI」で発見した脆弱性に対して、公式パッチより最大 96 日早く仮想パッチを提供。AI による脆弱性発見が加速する中、正規パッチ前の「空白期間」を埋める手段を提供。

4. AI アプリケーションの保護
- AI システム自体への攻撃（プロンプトインジェクション、モデル汚染など）への防御機能。日本企業が AI を利用・開発する際の安全な環境を整備

5. 高性能 AI を活用した自組織、製品の安全性向上、脆弱性の発見、対応体制の強化
-- Anthropic 社の Glasswing プロジェクトへの参加
--セキュリティリサーチ基盤 ÆSIR（AI-Enhanced Security Intelligence & Research）の運用を開始。世界中の脆弱性の動向継続的監視、ゼロデイ脆弱性の発見とエージェント型のトリアージに高機能 AI を採用
--Anthropic 社と戦略的パートナーシップ：同社の高性能 AI を利用して TrendAI Vision One や TrendAI Zero Day Initiative (ZDI)、Pwn2Own などのイニシアチブを推進

参考情報：
組織横断でのサイバーリスクの可視化・優先度づけ・対応のためのプラットフォーム：
https://www.trendmicro.com/ja_jp/business/products/one-platform.html

セキュリティリサーチ基盤 ÆSIR（AI-Enhanced Security Intelligence & Research）：
https://www.trendmicro.com/ja_jp/research/26/a/aesir.html

Anthropic 社との連携：
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260414-01.html

Anthropic Glasswing への参加の発表：
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260604-01.html

---

会社名：株式会社ディー・ディー・エス

取り組み：
多要素認証ソリューションでの脆弱性診断（外部の評価機関）を計画中
企業やそのサプライチェーンのサイバーリスクを客観的に評価するサービスの取り扱いを企画中

会社名：パロアルトネットワークス株式会社

取り組み：
1. 情報提供として下記 2 つのブログを公開。

サイバー防御ガイド: フロンティア AI がサイバーセキュリティに与える影響
https://www.paloaltonetworks.com/blog/2026/04/defenders-guide-frontier-ai-impact-cybersecurity/?lang=ja
Anthropic 社の Project Glasswing と OpenAI 社の Trusted Access for Cyber に参画し、フロンティア AI がサイバーセキュリティにもたらす影響について解説。

フロンティア AI のサイバーセキュリティへの影響についての防御担当者向けガイド: 2026 年 5 月更新
https://www.paloaltonetworks.com/blog/2026/05/defenders-guide-frontier-ai-impact-cybersecurity-may-2026-update/?lang=ja
フロンティア AI を活用したシステム診断の検証結果と、そこから浮き彫りになった実践的な教訓を公開。企業が今すぐ着手すべき具体的な「4 つの対策ステップ」を提示。

2. フロンティア AI がもたらす脅威対策を支援するため、「Unit 42 Frontier AI Defense」を提供。

Unit 42 Frontier AI Defense の概要
https://www.paloaltonetworks.com/blog/2026/04/introducing-unit-42-frontier-ai-defense/?lang=ja

---

会社名：株式会社マクニカ

取り組み：
セキュリティ研究センターにて、フロンティア AI とサイバーセキュリティについての調査と研究、今後の展開について取りまとめ予定

参考情報：https://sd-stream.macnica.co.jp/home/

※公開日：2026 年 6 月 15 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