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 6 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、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 6 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 6 月度
（会社名：五十音順）

会社名：株式会社アズム

取り組み：
当社としては AI を用いたサイバー攻撃の高度化・自動化は、顧客へサービスを提供する上での最重要課題と認識している。

単なる技術（製品）の導入にとどまらず、デジタル社会の「標準化」や「ガバナンス策定」のフェーズから深くコミットしていく方針。

自治体特有の環境に対し、自律型インシデント対応（未知の脅威検知とインフラ・ネットワークの自動連携防御）製品やネットワーク分離に対応したファイル検疫ソリューションを展開し、重要行政データの安全な交換と保護を推進する。

「地方の存続」と「安全な DX 推進」は表裏一体であると考え、地域に深く根ざした活動を継続する。

AI 技術に係る知見を継続的に収集し、AI を活用した脆弱性対策の自動化など、脅威への即応体制を準備する。

会社名：株式会社チェンジホールディングス

取り組み：
革新的 AI のサイバー攻撃への転用を含め、攻撃がより容易かつ安価となり、より攻撃者に優位な状

況となっている。しかしながら、中堅・中小企業にとっては、要員・技術、また費用の観点で、サイバー攻撃対策は不十分なままである。ツール等により「検知」はできるものの、その検知結果を適切に判断し対応に結び付けることが困難な組織が特に多くみられる。このために、AI を活用して企業・組織のサイバー攻撃対応を支援する新サービス「サイバー攻撃対応ナビ」を 2026 年 10 月より提供開始する予定である。本サービスは、SMBC グループをはじめとする国内企業・組織のセキュリティ運用現場で蓄積された知見・データを活用した AI が、サイバー攻撃の可能性がある事象の危険度判断や対応手順を提示するものである。専任のセキュリティ人材を確保しにくい企業・組織の迅速な初動対応をサポートし、サイバー攻撃対応力の向上に貢献する。

参考情報：
https://www.changeholdings.co.jp/news/247/

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：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 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
--OpenAI Daybreak Cyber Partner Program に参画
-- Claude Compliance API を TrendAI Vision One™に統合
-- 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

TrendAI、OpenAI DayBreak Cyber Partner Program に参画：
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260623-01.html

TrendAI™、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

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

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

会社名：パロアルトネットワークス株式会社

取り組み：
革新的 AI サイバー防御に関連して、新しくブログを公開
「AI vs AI」の時代へ：最先端 AI が金融インフラにもたらす脅威と次世代のレジリエンス
https://www.paloaltonetworks.com/blog/2026/06/ai-against-ai-financial-services-japan/?lang=ja

参考情報：
https://www.paloaltonetworks.com/blog/2026/04/introducing-unit-42-frontier-ai-defense/?lang=ja

---

会社名：HENNGE 株式会社

取り組み：
当社では、対策パッケージ「Project YATA-Shield」の方針を踏まえ、クラウドセキュリティベンダーとして以下の対策および検討を進めている。

■高度化する脅威（AI を用いたフィッシング等）に対する多層防御の提供

生成 AI の悪用により、認証情報を狙う標的型攻撃やフィッシングメールが巧妙化・高速化している。これに対抗し、政府機関等に求められる「基本的な対策」の徹底を支援するため、クラウドセキュリティサービスを通じた厳格なアクセス制御や多要素認証（MFA）による多層防御の構築を支援している。

■実践的なインシデント対応力強化の支援
AI によって生成される巧妙な不審メール等に対する組織的な対応力を高めるため、標的型攻撃対策ソリューションを通じ、政府機関や自治体職員様向けの実践的な訓練やインシデントの早期発見・被害防止に向けた取り組みを支援している。

■AI サイバー攻撃を見据えた自社サービスの防御力強化・検証の検討
ソフトウェアベンダーとして、攻撃の高度化や早期化、高頻度化等に対応するため、当社が提供する認証基盤やセキュリティソリューションに対する脆弱性診断の高度化や、防御機能の継続的な検証を AI の活用も含めて計画・推進している。

※公開日：2026 年 7 月 10 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