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 7 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 7 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 7 月度
（会社名：五十音順）

会社名：TISI 株式会社

取り組み：
TISI は、フロンティア AI 時代に求められる「システム構造改革（モダナイズ）」「AI for Security」「自動化運用」の 3 つの変革が重要であると考えている。

■ システム構造改革（モダナイズ）
SaaS 活用、クラウドネイティブ化、ゼロトラスト、レガシー刷新を通じて、攻撃対象そのものを削減し、変化に迅速に対応できるシステム基盤を実現する。

■ AI for Security
AI 脆弱性診断、AI コードレビュー、AI ペネトレーションテスト、継続的脆弱性管理により、従来の定期診断型から常時診断・常時評価型のセキュリティへ転換する。

■ 自動化運用（Autonomous Security Operations）
DevSecOps、自動検知、自動修正、自動封じ込めを組み合わせ、人手に依存しない継続的なリスク低減を実現する。

参考情報：
フロンティア AI 時代のサイバー防御～問われるのは防御力ではなく変化対応力～
https://www.tisi.jp/special/frontierai-security_column_01/

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擁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、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
-- Claude Opus 5 を採用し脆弱性の優先順位付けと仮想パッチを強化
-- Nvidia の Open Secure AI Alliance に参画

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

AI エージェントの構造的なサイバーリスクを実証：
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260717-01.html

Nvidia の Open Secure AI Alliance に参画：
https://www.trendmicro.com/ja_jp/research/26/g/open-secure-ai-alliance.html

Claude Opus 5 を採用し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

---

会社名：パロアルトネットワークス株式会社

取り組み：
■プレスリリース
「IBM、Red Hat、パロアルトネットワークス、Project Lightwell を拡張し、ソフトウェアの脆弱性への対応強化を支援」

IBM、Red Hat、パロアルトネットワークスの 3 社が協力し、システムの不具合（脆弱性）を悪用したサイバー攻撃から企業を迅速に守る仕組みを発表しました。

近年は AI の悪用により、不具合が見つかってから攻撃されるまでの時間が劇的に短くなっています。そこで、システム全体の根本的な修正（プログラムのパッチ適用）が完了するまでの間、まずはネットワーク側で攻撃を遮断する「仮想パッチ」を即座に適用する技術を導入しました。

「攻撃を防ぐガード」と「システムの根本的な修復」をセットで迅速に行うことで、企業の業務を止めずに安全を確保できるよう支援します。

https://www.paloaltonetworks.jp/company/press/2026/ibm-red-hat-and-palo-alto-networks-expand-project-lightwell-to-help-organizations-respond-to-software-vulnerabilities

■プレスリリース
「パロアルトネットワークス、業界をリードするオブザーバビリティプラットフォームを革新的なデジタルエクスペリエンスモニタリング機能で拡張」

パロアルトネットワークスが Embrace 社の買収方針と新機能「Synthetics」を発表しました。これにより、システム監視（オブザーバビリティ）の性能が大きく強化されます。

従来のツールでは見落としがちだった「ユーザーがアプリを操作した瞬間の反応」から「システムの裏側の動き」までを、単一の画面で一括監視できるようになります。

ユーザーがトラブルに気づく前に、アプリの不具合や速度低下を自動で早期発見・修復できるようになり、システムの停止による売上減少や信頼低下を未然に防ぐことが可能になります。

https://www.paloaltonetworks.jp/company/press/2026/palo-alto-networks-to-extend-leading-observability-platform-with-innovative-digital-experience-monitoring

■ブログ記事
「フロンティア AI の脅威に備える金融機関の TLPT：実効性のあるサイバーレジリエンス評価とは」

AI の悪用によりサイバー攻撃が超高速化する現代では、年に数回行う従来の静的なセキュリティテストだけでは防御が追いつかなくなっています。

そこで注目されているのが、実際の攻撃手法を再現して防御力を確かめる「TLPT（脅威ベースのペネトレーションテスト）」です。実戦に近い演習や AI を使った疑似攻撃を「継続的」に行うことで、手作業では見落とす設定ミスや対応の遅れといった弱点を素早く特定できます。

手遅れになる前にテストで弱点を把握し、検知から対処までを AI で自動化する体制を整えることが、攻撃スピードに対抗するための鍵となります。

https://www.paloaltonetworks.com/blog/2026/07/tlpt-financial-institutions/?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おります。

■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・高速化しています。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おります。

■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おります。

■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・推進しております。

参考情報：
クラウドセキュリティサービス「HENNGE One」
https://hennge.com/jp/

※公開日：2026 年 8 月 7 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