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 10 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。

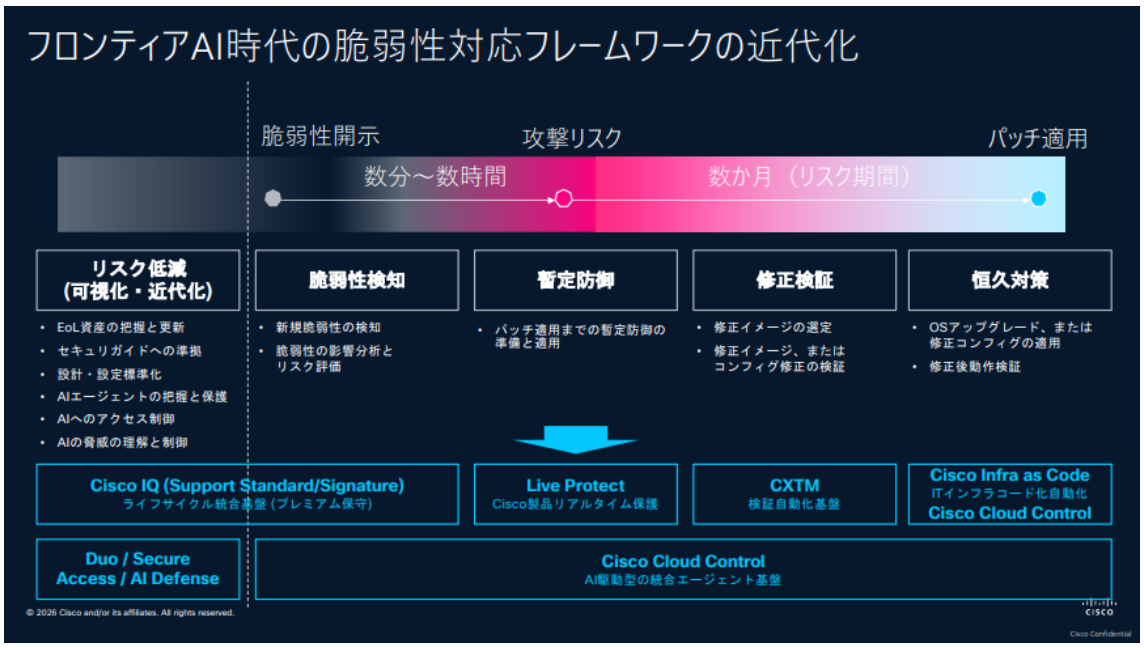
本取組の一環として、2026 年 10 月末時点における各社の革新的 AI サイバー防御への検討・対策状況を取りまとめました。なお、参画各社の最新の対策状況について、2026 年 6 月より継続的に公開してまいりましたが、今回をもちまして、定期的な公開を終了することといたします。

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 10 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：フロンティア AI の進展により、攻撃側は脆弱性の公開から数分～数時間で攻撃を成立させる一方、防御側は影響調査と検証を経た恒久対策（パッチ適用）までに数か月を要します。当社はこの差を人手中心の運用では埋められないと考え、「可視化 → 検証 → 実行」を一体化した脆弱性対応フレームワークの近代化を推進しています。
AI 運用プラットフォーム「Cisco IQ」は、ネットワーク機器の自動検出とサポート終了（EoL／LDOS）時期の可視化により技術負債の解消を支援するとともに、PSIRT が公開するセキュリティアドバイザリをお客様が保有する機器とソフトウェアバージョンに自動照合し、脆弱性公開の直後に影響範囲を絞り込みます。あわせて、CISA および当社のベストプラクティスに基づく機器設定アセスメントや PQC（耐量子計算機暗号）対応状況の評価により、攻撃対象領域の縮小を支援します。
検証自動化基盤「Cisco CXTM」は、修正版ソフトウェアの適用前検証を自動化し、お客様環境に即した検証シナリオを資産として蓄積・再利用可能にすることで、脆弱性対応で最大のボトルネックとなる検証の長期化を解消します。さらに、パッチ適用までの期間を無停止で防御する仕組みと、IT インフラのコード化（Infrastructure as Code）による適用の自動化を組み合わせ、恒久対策までの時間を短縮します。加えて、AI エージェントの把握・アクセス制御・脅威制御により「AI を守る」取り組みも進めています。



会社名：ソフォス株式会社

取り組み：
■ AI ネイティブなサイバー防御システム「Sophos Fusion」
ソフォスは、管理プラットフォーム「Sophos Central」を進化させ、「Sophos Fusion」として提供を始めました。
Sophos Fusion は単独の製品ではありません。
ソフォスの製品、サービス、AI 機能を一つにまとめたサイバー防御システムで、追加購入なしで利用できます。
Sophos Fusion の一部として、次の機能を順次提供しています。

・拡張版「Sophos MDR」
・Secureworks の技術を活かして強化した「Sophos XDR」
・MDR・XDR 向けのアドオン「Sophos Next-Gen SIEM」
・経営層によるサイバーリスク管理を支援する「Sophos CISO Advantage」
・Sophos Fusion に組み込まれたエージェント型 AI「Fusion AI」

個別の製品を別々に運用するのではなく、一つの防御システムとして連携して動かします。
これにより、AI で高度化・高速化するサイバー攻撃に対し、組織全体で一貫した防御を行えるようにします。

■ AI 利用の可視化と統制を実現する「Sophos AI Defense」
2026 年 10 月から、Sophos Fusion のソリューションとして「Sophos AI Defense」の一般提供を始めました。
生成 AI の業務利用が急速に広がる中、組織内の AI の使われ方を可視化し、統制するためのソリューションです。
Sophos EDR、XDR、MDR のアドオンとして利用でき、早期アクセスプログラムには約 300 社が参加しました。

・AI の可視化（See AI）：組織内で使われている AI ツール、エージェント、ワークフローを検出しま

す。IT 部門が把握していない「シャドーAI」も対象です。
・リスクの把握（Understand risk）：AI アプリケーションだけでなく、その裏にある AI プロバイダーの単位でリスクを評価し、根拠となる情報を示します。この結果は、経営層、取締役会、内部監査、サイバー保険の審査への説明にも使えます。
・AI の統制（Control AI）：「許可・警告・ブロック」のポリシーを設定し、Sophos Endpoint や Sophos Firewall など既存のセンサーで適用します。新しいエージェントを導入する必要はありません。
　医療、金融・法務、教育・公共向けのポリシーテンプレートも用意しています。
・AI の保護（Secure AI）：AI ツールに入力される機密情報を保護し、安全な AI 活用を支援します。

■ AI と専門家の組み合わせで 24 時間 365 日守る「Sophos MDR」
「Sophos MDR」では、セキュリティの専門家が 24 時間 365 日体制で脅威を監視し、対応します。Sophos Fusion への移行に合わせて、次の点を強化しました。

・脅威ハンティングにエージェント型 AI を取り入れ、検知と調査を高度化・効率化
・他社製品との双方向連携と、自動で実行できる対応アクションを拡充
・Sophos AI Defense が検知した AI 関連の脅威を MDR の調査・対応につなげ、AI 利用にかかわるリスクも専門家が監視・対応する仕組みを提供
・上位プランの「Sophos MDR Plus」で、根本原因分析、本格的なインシデントレスポンス、専任のインシデントレスポンスリード、侵害時の補償（Breach Protection Warranty）を提供

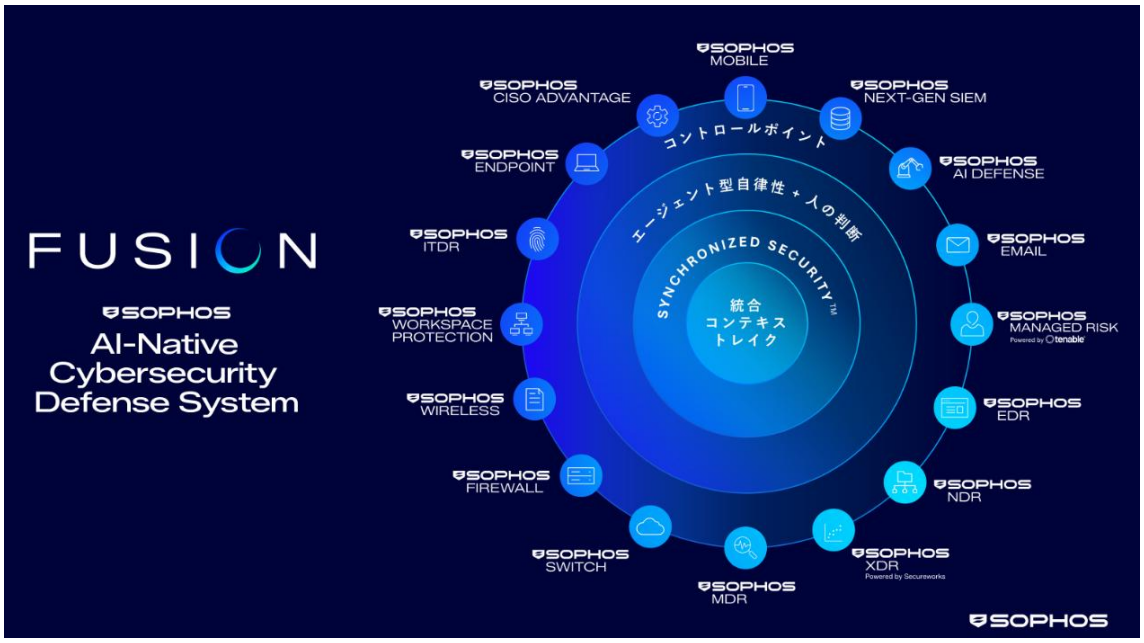
AI による高速な分析と専門家の判断を組み合わせることで、専任のセキュリティ担当者がいない組織でも、AI 時代の高度な攻撃に迅速かつ確実に対応できる体制を支えます。

参考情報：
■ Sophos Fusion
・製品ページ
　https://www.sophos.com/ja-jp/products/sophos-fusion

■ Sophos AI Defense
・製品ページ
　https://www.sophos.com/en-us/products/ai-defense
・一般提供開始の発表ブログ（Sophos AI Defense now available）
　https://www.sophos.com/en-us/blog/sophos-ai-defense-now-available
・製品ドキュメント
　https://docs.sophos.com/fusion/customer/help/en-us/ManageYourProducts/AIDefense/index.html

■ Sophos MDR
・製品ページ
　https://www.sophos.com/en-us/services/managed-detection-and-response
・サービス内容の説明（MDR Service Description）
　https://www.sophos.com/en-us/legal/mdr-description

参考情報：
https://www.sophos.com/ja-jp



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・シャドー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
セキュリティリサーチ基盤 ÆSIR（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 A 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リサーチ基盤「ÆSIR」：
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

TrendAI™ Zero Day Initiative™、Pwn2Own での脆弱性発見に総額 120 万米ドル超を授与：
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20261015-01.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

NVIDIA Nemotron™ オープンモデルとの連携により、顧客の管理下で運用可能な AI 駆動型セキュリティをソブリンクラウドおよびプライベートクラウド向けに提供：
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20261026-01.html

---

会社名：パロアルトネットワークス株式会社

取り組み：
■「証明書切れでシステムダウン」はもう許されない：2027 年 100 日化・PQC 時代を乗り切る金融 IT の「暗号アジリティ」戦略
https://www.paloaltonetworks.com/blog/2026/10/crypto-agility-pqc/?lang=ja

■Palo Alto Networks の PA シリーズが「JC-STAR Level 1」を取得：日本市場における IoT・ネットワークセキュリティ要件への準拠
https://www.paloaltonetworks.com/blog/2026/10/pa-network-security-jc-star-level-1/?lang=ja

■上場企業の適時開示にみる、2026 年下半期のセキュリティインシデントのキートレンド
https://www.paloaltonetworks.com/blog/2026/10/key-trends-2nd-half-2026/?lang=ja

■危険にさらされる無数の PHP インスタンス - 今求められる対策
https://www.paloaltonetworks.com/blog/2026/10/millions-of-php-instances-exposed-what-organizations-need-to-do-right-now/?lang=ja■脅威の概要: PHP における重大な脆弱性: CVE-2026-109618、CVE-2026-109619 (10 月 29 日更新)
https://unit42.paloaltonetworks.com/ja/cve-2026-109618-cve-2026-109619/

※公開日：2026 年 11 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