CSA Japan Summit 2026　プログラム

11:00～11:05	**本日のプログラムのご紹介　CSAジャパン事務局**
11:05～11:35	 **開会挨拶・CSAジャパン講演　江崎 浩　CSAジャパン会長　東京大学大学院情報工学系研究科教授** **「AI前提のデジタルインフラにおけるセキュリティ」** AIは「学習生成」の集中から「推論と自律分散連携（Agentic）」への 移行が進行しており、システムアーキテクチャとそのセキュリティー対策 の劇的な変化が要求されている。コンピュータシステム(IT)だけではなく、 ITを支えるOTのオープン化が進行しており、ＩＴ＋ＯＴのサイバーを含む 総合的なセキュリティーが、デジタル地政学として議論されなければ ならない段階を迎えている。 本講演では、CSAジャパン会長としてSummitの 開会を宣言するとともに、AIがもたらすパラダイムシフトと、私たちが 構築すべきデジタルインフラセキュリティーあり方について議論する。
11:35～12:20	 **CSA本部講演　Daniele Catteddu　Chief Technology Officer, CSA** **「Governing the Autonomous Future: CSA's Mission to Secure the Agentic Control Plane（自律的な未来のガバナンス：エージェンティック・コントロールプレーンの保護に向けたCSAのミッション）」** The rapid proliferation of autonomous AI agents is reshaping how organizations operate, exposing a fundamental gap in how security, governance, and trust have traditionally been designed. This keynote traces the evolution of the Cloud Security Alliance's AI Safety Initiative, from its foundational work producing the AI Controls Matrix (AICM), the TAISE certification, and STAR for AI, through to the launch of CSAI and its defining mission of Securing the Agentic Control Plane: governing the identity, authorization, orchestration, runtime behavior, and trust assurance layers that underpin autonomous AI ecosystems. As agents initiate workflows, delegate tasks, and interact with other agents at machine speed, they become a new class of digital participants demanding identity, permissions, and accountability at a scale traditional frameworks were never built to handle. The session will also update attendees on STAR for AI Level 2 which offers organizations with a verifiable path to AI trustworthiness. Additionally, it will introduce the Catastrophic Risk Annex, CSA's forward-looking research frontier into existential risks posed by highly transformational AI systems. 自律型AIエージェントの急速な普及は、従来のセキュリティやガバナンスの設計に新たな課題を突きつけています。本講演では、CSAのAIセーフティ・イニシアチブ（AICMやSTAR for AI等）の進化を辿り、自律型AIエコシステムを統制する「エージェンティック・コントロールプレーンの保護」という中核ミッションを解説します。 機械の速度で自律的に連携するAIエージェントは、新たな「デジタル参加者」として次世代のアイデンティティ管理や権限付与を必要としています。これらへの実践的アプローチに加え、AIの信頼性を検証する「STAR for AI Level 2」や、高度なAIがもたらす重大リスク（Catastrophic Risk Annex）に関するCSAの最新研究動向をご紹介します。
12:20～13:20	**昼食休憩：主催者側で、軽食、ランチマップを用意します**
13:20~13:50	 **招待講演１　河野省二　日本マイクロソフト株式会社　Chief Security Officer** **「自律型AI活用の現場を見据えた、セキュリティとガバナンスの考え方」** 自律型AIに関するセキュリティについては多くのところで語られていますが、それらを利用する現場についてはまだまだ議論が必要なようです。自律型AIを活用したスクリプトなどを簡単に使えるようになれば、マクロによるアプリケーション拡張と同様の市民開発環境におけるガバナンスの欠如も懸念されます。セキュリティとガバナンス、そして生産性向上のバランスをとるためのベースとなる考え方について解説します。
13:50～14:20	 **スポンサー協賛講演　蓮井雅弘氏　ファイルフォース株式会社 プロダクトマーケティング部** **「ランサムウェアが猛威を振るう今、クラウドストレージに求めるべき要件とは？」** 23,000社を超える法人企業導入実績を誇るクラウドファイルサーバーを提供するファイルフォース株式会社が、ランサムウェア感染時の対応における課題や有効な対策機能について、実際の事例をもとにご紹介します。
14:20～14:35	**休憩：主催者側でコーヒーを用意します**
14:35～15:05	 **招待講演２　山寺 純　株式会社 Eyes, JAPAN　代表取締役 チーフ･カオス･オフィサー** **「攻撃者の思考を先読みする自律型AIの衝撃 ～フェイク医療データとPhysical AIが変えるセキュリティの境界～」** 生成AIから自律型AI（Agentic AI）へと進化が進む中、サイバー攻撃はデータ領域に留まらず、現実世界へと直接影響を及ぼす段階に入りつつあります。医療分野では、AIによるフェイク画像・動画の生成やディスインフォメーションにより診断や意思決定が攻撃対象となる一方、Physical AI（ロボット・ドローン・自律システム）の進展により、クラウドを起点とした攻撃が現実の動作として実行されるリスクが現実化しています。 また、連合学習（Federated Learning）など分散型AIの普及は、新たな攻撃面を生み出しています。 本講演では、OWASPにおけるAIセキュリティの知見と、Physical AIの実装現場の視点を統合し、攻撃者の思考から見た脅威モデルを再定義します。その上で、「何を守るべきか」「どこまで守れるのか」という現実的な境界を提示し、クラウドと現実世界を横断する実践的なセキュリティアプローチについて論じます。
15:05～15:35	 **招待講演３　森永　聡　日本電気株式会社 研究開発部門 上席主席研究員、 自律調整SCMコンソーシアム 理事長** **「エージェント経済圏の健全な勃興にむけて」** AIエージェントが経済主体となってビジネスを行う「エージェント経済圏」が近いうちに勃興することは、多くの有識者から予想されているが、その健全な勃興のためには適切なリスクの認識と対応が必要である。講演では、エージェント経済圏のコンセプト、およびキー技術の一つである自動交渉AIについて紹介したうえで、自律型エージェントが経済活動を行う社会において、認識すべきリスクやその対応方針に関する議論と提言を行う。
15:35～15:50	**休憩：主催者側でコーヒーを用意します**
15:50～16:20	 **招待講演４　西村 卓 AISI（AIセーフティ・インスティテュート）副所長・事務局長** **「AIセーフティの最前線と日本の戦略：自律型AI時代に向けたAISIの取り組み」** 生成AIから自律型AIへと技術が急速に進化する中、AIの安全性（セーフティ）とセキュリティの確保は、社会インフラや経済活動において喫緊の課題となっています。本講演では、AIセーフティ・インスティテュート（AISI）の最新の活動や、先般発表されたガイドライン・評価手法の動向を踏まえ、AIセキュリティに関する日本の政策と今後の戦略について解説します。国際連携の枠組みや、企業に求められる実践的ガバナンスのあり方について展望します。
16:20～16:50	 **招待講演５　福田俊介氏 トレンドマイクロ株式会社 執行役員 TrendAIマーケティング本部 本部長 エバンジェリスト** **「自律型AI時代のクラウドセキュリティ実践論：AI駆動型CNAPPがもたらす次世代の防御戦略」** AIの進化に伴い、クラウド環境を狙うサイバー攻撃はかつてないスピードと複雑さで高度化しています。この自律型AI（Agentic AI）時代において、企業がクラウドネイティブ環境を安全に保つためには、防御側もAIの力を最大限に活用することが不可欠です。本講演では、トレンドマイクロの最前線の知見をもとに、クラウドセキュリティにおけるAI活用の実践論を解説します。自組織に対する脅威をいかに「プロアクティブに予測して侵害を防ぐ」か、そして仮に侵入された場合には「迅速に検知し、対応・復旧を自動化・効率化する」か―― トレンドマイクロの新しい法人向けビジネスユニット“TrendAI”が提供する、AIテクノロジーを活用したCNAPPを基に、AIを活用した次世代のクラウドセキュリティのあり方を提示します。
16:50～17:00	**閉会挨拶・懇親会ご案内　CSAジャパン事務局**
17:30～	**懇親会（準備でき次第）　　会場：弥生講堂会議室**