

イベント概要

日程：2026 年 9 月 29 日（火）

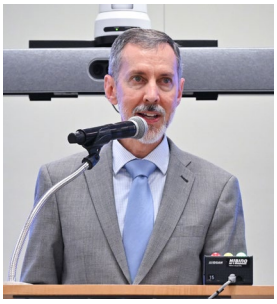
会場：シスコシステムズ社 東京本社

主催：Business Software Alliance （ビジネス・ソフトウェア・アライアンス、BSA）

協賛・後援：一般社団法人 AI ガバナンス協会（AIGA）、一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）、一般社団法人日本経済団体連合会（経団連）、一般社団法人電子情報技術産業協会（JEITA）、在日米国商工会議所（ACCJ）、日本マイクロソフト株式会社、シスコシステムズ合同会社、トレンドマイクロ株式会社

AI がサイバー攻撃の速度と規模を変える一方、防御側にとっても、脆弱性の発見や脅威の分析を支える有力な手段となっています。2026 年 9 月 29 日に開催された BSA カンファレンスでは、政府、公的機関、国内外のテクノロジー企業、重要インフラ事業者、大使館関係者が一堂に会し、AI 時代のサイバー防御を支える政策、取組、ガバナンス、国際協調について議論しました。本レポートでは、基調講演とラウンドテーブルの主な論点を紹介します。

開会挨拶



アーロン・クーパー
(Business Software Alliance グローバルポリシー担当シニア・バイス・プレジデント)

開会にあたり、BSA およびシスコシステムズ社から、参加した政策立案者、政府関係者、産業界のリーダー、協力団体に謝意が示されました。AI の急速な進展によりサイバーセキュリティの重要性がこれまで以上に高まる中、政府と産業界の専門家が一堂に会し、今後の政策や標準、技術のあり方について知見を共有することの意義を強調。本カンファレンスで得られる議論や知見を、AI 時代のサイバーセキュリティ強化に向けた具体的な取組につなげていくことへの期待が示されました。



ティマヤ・スバイヤ 氏
(シスコシステムズ　エグゼクティブ バイス プレジデント、オペレーションズ)

第一部：AI 時代の国家サイバー防御：制度・体制・技術の現在地

1）基調講演：平 将明 氏

衆議院議員、自由民主党・国家サイバーセキュリティ戦略本部長



平議員は、自身がサイバー安全保障担当大臣を務めていた際に、サイバー対処能力強化法の成立と国家サイバー統括室（NCO）の新設を進め、能動的サイバー防御を可能とする体制整備に取り組んだことを紹介しました。また、金融庁、NCO、AI セーフティ・インスティテュート（AISI）の連携に加え、重要インフラや国内事業者の技術基盤を守る取組として Project YATA-Shield に言及。その上で、AI エージェントによる自律的な攻撃など、AI の進展によってサイバー脅威が急速に変化しているとして、政府機関のみならず、同盟国・同志国や民間テクノロジー企業との連携を一層強化する必要性を強調しました。

さらに、AI をサイバーセキュリティに活用する上では、高性能な AI と小規模なオープンウェイト・モデルの使い分け、機微なデータの保護、秘密計算技術など AI 同士の対抗以外の手法も含めたソリューションの組み合わせに加え、コスト、安全性、経済合理性のバランスも重要だと指摘しました。今後の課題として、AI のミスアライメント、再帰的自己改善（RSI: recursive self-improvement）、認知戦などにも言及し、信頼できる AI を民間企業が利用しやすい環境の整備と、官民・国際連携を通じた AI・サイバーセキュリティ政策の強化を進めていく考えを示しました。

2）基調講演：アーロン・クーパー

Business Software Alliance グローバルポリシー担当シニア・バイス・プレジデント



続く基調講演で、BSA のクーパーは、フロンティア AI や AI エージェントの急速な発展により、サイバーセキュリティが技術的課題にとどまらず、経済、競争力、国家安全保障に関わる重要課題になっていると指摘し、AI 時代に重視すべき 5 つのポイントを提示しました。第一に「官民連携」として、政府と産業界それぞれの強みを組み合わせる必要性、第二に「AI 時代におけるサイバーセキュリティ原則の重要性」として、AI の登場によって従来の原則が時代遅れになるのではなく、「共通の責任」、リスクベース、成果重視といった考え方が一層重要になることを強調しました。第三に「AI の二つの役割」として、AI がサイバー攻撃を高度化する一方、防御側にとっても脅威の検知・分析や脆弱性への対応を強化する重要なツールになるとして、サイバー防御への AI 活用を促進する必要性を指摘しました。

第四に「フロンティア AI のセキュリティモデル」について、BSA の提言「サイバーセキュリティ専門人材を最優先に」を紹介しました。本提言では、フロンティア AI モデルを戦略的かつ段階的に展開するための自主的な官民パートナーシップ発足を呼びかけ、一般公開に先立ち、信頼できる防御側にモデルへの先行アクセスを提供することで、防御側が重大な脆弱性を早期に発見・修正できる時間を確保することを目的としています。第五に「国際協力」として、国境を越えるサイバー脅威への対応には信頼できるパートナーとの連携が不可欠であり、デジタル主権についても、企業の本社所在地による制限ではなく、「レジリエンス、信頼、選択」を重視し、信頼できるテクノロジーへのアクセスや相互運用性を確保することが重要だと述べました。



BSA 提言
「サイバーセキュリティ専門人材を最優先に」

3）表彰式：デジタル外交チャンピオン

受賞者：平 将明 氏　衆議院議員、自由民主党・国家サイバーセキュリティ戦略本部長



BSA は、世界的に整合性のあるデジタル政策の推進や、政府・産業界・市民社会との連携を通じてデジタル分野の国際協力に貢献した世界の政府・政策リーダー8 名を「デジタル外交チャンピオン（Digital Diplomacy Champion）」に選出し、日本から平将明衆議院議員を表彰しました。平議員は、デジタル大臣および初代サイバー安全保障担当大臣として、政府 IT システムの刷新、サイバーセキュリティ体制の強化、AI の導入促進などを推進するとともに、国際協力を通じて日本のデジタル政策を前進させてきました。

今回の表彰では、こうしたデジタル政策におけるリーダーシップと国際協力への貢献が称えられました。受賞にあたり、平議員は、デジタル、AI、サイバーセキュリティに加え、認知戦など、今後対応すべき課題が数多くあることに言及しました。その上で、今回の「デジタル外交チャンピオン」の受賞を励みに、これまで以上にこれらの課題にしっかり取り組んでいきたいとの意欲を示しました。







第二部：ラウンドテーブル・ディスカッション「官民連携と AI サイバー防御」

第 2 部のラウンドテーブル・ディスカッションでは、「官民連携と AI サイバー防御」をテーマに、国家サイバー統括室、AI セーフティ・インスティテュート、国内外のテクノロジー企業、重要インフラ事業者が、AI によって変化するサイバー脅威と防御のあり方について議論しました。



モデレーター：佐久間 弘明 氏
(AI ガバナンス協会 業務執行理事 兼 事務局長)

モデレーターを務めた AI ガバナンス協会の佐久間弘明氏は、AI の高度化によってサイバー攻撃と防御の双方が変化する中、AI を活用してシステムを守る「AI for Security」と、AI そのものを攻撃から守る「Security for AI」の双方が重要になっていると指摘。特に、最先端 AI をサイバー防御にどのように生かすかという観点から、官民それぞれの取組や課題について議論を促しました。



飯田 陽一 氏
(内閣サイバー官（併）
国家安全保障局次長)

AI 時代におけるサイバー防御と官民連携の強化

飯田氏は、サイバー対処能力強化法の運用開始に向け、官民連携の強化、通信情報の利用、悪質なサーバーへのアクセス・無害化という新たな枠組みの準備を進める一方、AI の進展や地政学的環境の変化によって、サイバー空間を取り巻く状況が急速に変化していると指摘しました。AI によってサイバー攻撃のスピードと規模が飛躍的に高まる中でも、多要素認証、ゼロトラスト、迅速なパッチ適用、事業継続など、サイバー防御の基本は変わらないとし、こうした対策を日常のサイバー防御に着実に取り込むことの重要性を強調しました。同時に、防御側も AI を積極的に活用する必要があるとして、フロンティア AI モデルなどの先端技術に早期にアクセスし、新たな脅威への備えに必要な時間を確保するとともに、それらの技術を政府機関や重要インフラ・基幹産業が継続的かつ安定的に利用できる環境を確保することが重要だと述べました。先端技術への「早期アクセス」と「持続的なアクセス」の双方が、日本のサイバー対処能力の強化に不可欠であるとの考えを示しました。

また、YATA-Shield や新たな協議会の枠組みを活用し、政府がよりプロアクティブに情報を共有するとともに、民間企業や同盟国・同志国との連携を通じて「集合知（collective intelligence)」を形成し、それを「共同の行動（collective action)」へとつなげていく考えを示しました。

AI モデルの第三者評価と国際連携の強化

続いて、西村氏は、AISI が AI の安全性に関する幅広いリスクを分析し、安全な社会実装に向けた方向性や指針を示す公的機関であると説明しました。AI セキュリティについても、YATA-Shield を技術面から支援するとともに、AI モデルを開発者とは異なる第三者の視点から評価するための能力・環境整備を進めており、海外のさまざまなモデルやオープンウェイトモデルを含め、特にセキュリティ面からの評価に取り組んでいると紹介しました。



西村 卓 氏
(AI セーフティ・インスティテュート　副所長・事務局長)

また、一企業だけで AI リスクに対応することには限界があるとして、AISI が企業や政府機関の知見を集約・分析し、その成果をガイドやアプローチとして社会に還元していく必要性を強調。英国をはじめ各国の AISI との国際的な連携も活用し、AI の安全な社会実装に貢献していく考えを示しました。



ティマヤ・スバイヤ 氏
(シスコシステムズ　エグゼクティブ バイス プレジデント、オペレーションズ)

「AI for Security」と「Security for AI」の両輪

シスコシステムズ社のスバイヤ氏は、AI がもたらした最も大きな変化の一つとしてイノベーションの圧倒的なスピードを挙げました。テクノロジーの進化と AI による複雑なタスクの実行の双方において、これまでにないほど時間が短縮されていることは、業務上の 大きなメリットをもたらす一方、新たなリスクに対応するための高度なガバナンスがかつてないほど求められている、と指摘しました。

また、AI を活用する際にも人間が確実に主導権を持つことが重要であり、 例えば、人間が仮説を立てて結論を検証し、AI が調査や分析を加速するといったことが不可欠だと述べました。サイバーセキュリティの領域においては、AI を防御に活用する「AI for Security」と AI 自体を保護する「Security for AI」の双方が必要だと強調しました。特に後者については、AI の基盤となるデータの保護に加え、適切なガバナンスが不可欠であり、ガバナンスは個々の AI モデルごとに異なるのではなく、政府や BSA などとも連携しながら、共通の標準やアプローチ、データセキュリティ フレームワーク を構築していくことが重要だと述べました。

AI によるサイバー防御を支える三つの優先事項

マイクロソフト社のジョーンズ氏は、AI によるサイバー防御を強化するための三つの優先事項として、1．データとインテリジェンス、2．目的に最も適した AI ツールの活用、3．パートナーシップを挙げました。第一に、政府・企業がそれぞれ把握する脅威情報を共有し、より包括的な脅威像を構築することで、AI を活用した迅速な検知・対応につなげることが重要だと説明。第二に、一つの AI モデルに依存せず、複数のモデルや AI エージェントを目的に応じて組み合わせることで、より強靭な防御能力を構築できると述べました。

その例として、多数の異なる AI モデルと数百の AI エージェントを組み合わせ、脆弱性を特定するスピードを飛躍的に向上させた、同社のプロジェクト「MDASH」を紹介しました。第三に、グローバルなテクノロジー企業と日本企業との連携を挙げ、マイクロソフトと NTT の取組などを例に、世界の優れた技術や知見を組み合わせ、日本のサイバーセキュリティ・エコシステム全体を強化していくことの重要性を強調しました。



マーカス・バートリー・ジョーンズ 氏（マイクロソフト グローバル アフェアズ シニアディレクター、ヘッド・オブ・ノースアジア）



生田目 雅史 氏
(明治安田生命保険相互会社 執行役専務 グループデジタル責任者、グループ AI 責任者 / AI ガバナンス協会 代表理事)

AI リスクへのアカウンタビリティと「集合知」の形成

生田目氏は、明治安田生命の執行役専務、また、AI ガバナンス協会の代表理事としての観点から発言しました。まず、企業経営者には AI のリスクから自社とステークホルダーの利益を守り、AI 利用に関するアカウンタビリティを確立する責任があると指摘しました。そのために重要な要素として、迅速に対応する「プロンプトネス（promptness）」、幅広く対策を講じる「エクステンシブネス（extensiveness）」、将来の変化を先取りする「プロアクティブネス（proactiveness）」の三点を提示。
また、AI の便益を最大化するためにはセキュリティを高め、社会的受容性を確保することが不可欠だと述べました。一企業から得られる知見には限界があるため、AI ガバナンス協会は 180 社の加盟企業の知見の集約を意識し活動している。この知見をもとに AISI や NCO とも連携して国内外の「集合知」を形成していくことが重要だと強調しました。

重要インフラの強靭化と業界横断の協調

自社のセキュリティ向上やインシデント対応に取り組む儀間氏は、基幹インフラ事業者としてサイバー対処能力強化法への対応を進めるとともに、フロンティア AI を含む新たな脅威への備えを強化していると説明しました。

AI が加わってもサイバー脅威への基本的な対応そのものは変わらないとの認識から、パッチの優先順位付けや適用方法など、従来からの基本的な対策を改めて検証し、インフラの強靭性向上に取り組んでいると述べました。

一方、AI によって攻撃速度が高まる中、通信事業者が危険な脆弱性に直面した際にサービスを能動的に停止する場合の考え方など、新たに検討すべき課題もあると指摘。こうした分野は競争領域ではなく協調領域であるとして、ICT-ISAC などを通じた事業者間の連携に加え、政府も交えたルール形成を進める必要性を強調しました。



儀間 哲仁 氏
(株式会社 NTT ドコモ
セキュリティイノベーション
統括部 CISO 室、室長)

大使館からのコメント



サム・ホール 氏
在日英国大使館
政治部一等書記官



ミッシェル・ウォーレン 氏
在日米国大使館
経済科学部 科学技術担当官



エロイーザ・ジャイ 氏
在日オーストラリア大使館
政治部 二等書記官

オブザーバーとして参加していた英国、米国、豪州の各大使館からは、AI の急速な進展によってサイバー脅威の不確実性が高まる中でも、基本的なサイバーセキュリティ対策を着実に進めるとともに、官民および国際的な連携を一層強化することが重要との認識が共有されました。特に、AI によって高度化するサイバー脅威は国境を越える課題であり、一国や一組織だけで対応することはできないとして、政府間の協力に加え、官民の情報・脅威共有、AI の安全性に関する機関同士の連携、国際的な標準形成などを通じ、信頼できるパートナーがそれぞれの知見や強みを持ち寄って対応していく必要性が強調されました。また、日本のサイバー対処能力強化に向けた取組への支持が示されるとともに、日本と英国、米国、豪州との既存の協力をさらに発展させ、同志国や地域のパートナーも含め、AI とサイバーセキュリティに関する国際協力を一層深めていくことへの期待が示されました。

デジタル競争力を支える強固なセキュリティと AI の選択肢 - ラウンドテーブル総括

BSA のクーパーは、経済競争力の向上にはデジタルトランスフォーメーションが不可欠であり、その基盤となるのが強固なサイバーセキュリティであると総括しました。その上で、AI 時代のサイバーセキュリティを強化するためには、最も高性能な AI モデルを活用できる環境を確保すると同時に、特定のモデルに依存せず、目的に応じて多様なモデルから選択できることが重要であり、こうした「選択肢」の確保そのものが、全体としてのセキュリティ強化につながると強調しました。








【BSA カンファレンス 参加者一覧】（敬称略）

司会進行：直江 智子（Business Software Alliance カントリー・マネージャー＆ディレクター、ポリシー担当（日本））

基調講演：

• 平 将明（衆議院議員、自由民主党・国家サイバーセキュリティ戦略本部長）

• アーロン・クーパー（Business Software Alliance グローバルポリシー担当シニア・バイス・プレジデント）

ラウンドテーブル・ディスカッション：

• モデレーター: 佐久間 弘明 （AI ガバナンス協会　業務執行理事 兼 事務局長）

ディスカッション参加者

• 飯田 陽一（内閣サイバー官（併）国家安全保障局次長）

• 西村 卓（AI セーフティ・インスティテュート　副所長・事務局長）

• ティマヤ・スバイヤ（シスコシステムズ　エグゼクティブ バイス プレジデント、オペレーションズ）

• マーカス・バートリー・ジョーンズ（マイクロソフト グローバル アフェアズ　シニアディレクター、ヘッド・オブ・ノースアジア）

• 生田目 雅史 （明治安田生命保険相互会社　執行役専務　グループデジタル責任者、グループ AI 責任者 / AI ガバナンス協会代表理事）

• 儀間 哲仁（株式会社 NTT ドコモ セキュリティイノベーション統括部 CISO 室、室長）

• アーロン・クーパー（Business Software Alliance グローバルポリシー担当シニア・バイス・プレジデント）

ラウンドテーブル・ゲスト

• サム・ホール（在日英国大使館 政治部 一等書記官）

• ミッシェル・ウォーレン（在日米国大使館 経済科学部 科学技術担当官）

• エロイーザ・ジャイ（在日オーストラリア大使館 政治部 二等書記官）