AI 時代の国家サイバーセキュリティに対する提言書

第 3 回 GMO 大会議 春 サイバーセキュリティ 2026

開催：2026 年 3 月 5 日（木）

発行日：2026 年 3 月 18 日（水）

本提言書は、2026 年 3 月 5 日（木）に開催された「第 3 回 GMO 大会議🌸春 サイバーセキュリティ 2026」における産官学の議論を集約し、我が国のサイバーセキュリティ強化に向けた 5 つの政策提言としてとりまとめたものである。

本会議の開催にあたり、「産官学で守り抜く！AI 時代のサイバーセキュリティ」をテーマに、GMO インターネットグループ グループ代表の熊谷 正寿は、戦国時代の長篠の戦いになぞらえ、「武田軍も織田軍も共に鉄砲を持っていたが、勝敗を分けたのはその使い方であった。AI 時代のサイバーセキュリティも同様であり、ブラックハッカーもホワイトハッカーも AI という同じ武器を手にしているが、その使い方こそが勝敗を分ける。」と述べた。本会議は、技術・制度・人材・産官学連携のあるべき姿を議論し、以下の政策的示唆を導き出したものである。

【提言の骨子】

1. 災害から安全保障まで情報を統合・可視化する 米国 Palantir Technologies（パランティア）の日本版構想

産官学の脅威情報を統合分析するデータ基盤を構築し、
国内 AI 技術と既存の国際連携を活かした自律的なサイバー防衛を実現

2. 能動的サイバー防御の運用基準の明確化

偵察活動段階での介入要件・法的免責範囲を早期に明確化し、
攻撃者側にコストを強いる国家戦略を確立

3. 「国産 AI 基盤」構築と人材育成への国家支援

システムソフトウェア領域の海外依存を脱し、
設計から運用まで自国内で制御可能な AI 基盤とホワイトハッカー人材を育成

4. 社会的セーフティネットの創設

AI 攻撃の完全防御は不可能という前提に立ち、互助的保険制度・公的支援枠組みで
社会全体のリスクを吸収

5. シームレスな脅威情報共有体制の確立

組織の壁を越えた「顔の見える信頼関係」を基盤に、産官学間で双方向の脅威情報
共有体制を構築

各提言の背景と具体的な政策的示唆については、「2. 政府に対する政策的示唆」に詳述する。

Copyright (c) 2026 GMO Internet Group, Inc. All Rights Reserved.

1. 開催の目的と背景

1.1. 開催概要

2026 年 3 月 5 日、内閣官房国家サイバー統括室が推進する「サイバーセキュリティ月間」に合わせ、GMO インターネットグループの主催により、国内最大級のセキュリティカンファレンスである「第 3 回 GMO 大会議🌸春 サイバーセキュリティ 2026」が開催された。本会議には、政府閣僚、官庁審議官、学術経験者、および民間企業の経営層から成る産官学のトップ層、ならびに約 5,000 名[1]の関係者が集結した。主催の GMO インターネットグループは、グループ約 8,200 人のうち約 1,200 人がセキュリティ業務に従事し、国内ホワイトハッカーの約半数が所属するインターネットインフラ企業である。

1.2. 登壇者一覧

高市 早苗 氏（内閣総理大臣）※メッセージ
小泉 進次郎 氏（防衛大臣）※ビデオメッセージ
飯田 陽一 氏（内閣サイバー官）
村井 純 氏（慶應義塾大学 特別招聘教授・名誉教授）
江崎 浩 氏（東京大学大学院 情報理工学系研究科 教授）
岡野原 大輔 氏（株式会社 Preferred Networks 代表取締役社長）
中島 聡 氏（一般社団法人シンギュラリティ・ソサエティ 代表理事）
奥家 敏和 氏（経済産業省 大臣官房審議官）
夏野 剛 氏（KADOKAWA 取締役・代表執行役社長 CEO）
伊東 寛 氏（国立研究開発法人情報通信研究機構 主席研究員）
川邊 健太郎 氏（LINE ヤフー株式会社 代表取締役会長）
小山 直伸 氏（陸上自衛隊教育訓練研究本部 研究部長・陸将補）
小澤 隆生 氏（Boost Capital 株式会社 代表取締役）
増田 幸美 氏（日本プルーフポイント株式会社 チーフエバンジェリスト）
鵜飼 裕司 氏（株式会社 FFRI セキュリティ 代表取締役社長）
登 大遊 氏（IPA 産業サイバーセキュリティセンター シニアエキスパート）
熊谷 正寿（GMO インターネットグループ グループ代表）
西山 裕之（GMO インターネットグループ 取締役・グループ副社長執行役員・COO）
廣恵 次郎（GMO インターネットグループ グループサイバー防衛事業推進本部「6」本部長）
小池 悠生（GMO サイバーセキュリティ by イエラエ株式会社 執行役員 CTO）
米内 貴志（GMO Flatt Security 株式会社 取締役 Co-CTO）

---

[1] Youtube 同時配信の視聴数を含む

Copyright (c) 2026 GMO Internet Group, Inc. All Rights Reserved.

福森 大喜（GMO サイバーセキュリティ by イエラエ株式会社 GMO サイバー犯罪対策センター局長）
平野 賢一（MUFG GMO セキュリティ株式会社 代表取締役副社長）

1.3. 社会的背景

デジタル化の進展に伴い、サイバー空間は国民生活、企業活動、そして国家運営を支える不可欠な社会基盤となった。一方で、どこからでも低コストでアクセスできるという特性が悪用され、国家が関与する高度なサイバー攻撃や重要インフラへの侵害が相次いでいる。ひとたびインシデントが発生すれば国家安全保障にまで深刻な影響が及び、サイバー空間はもはや平時とは言えず、現実の安全保障と直結する領域である。

こうした中、生成 AI の登場により、サイバー攻撃は「スピード」「自動化」「もっともらしさ」の面でかつてない次元に進化した。攻撃の入り口はシステムコードにとどまらず、文書・音声・画像といった人間の「信頼」そのものへと広がっている。この攻撃側が圧倒的に有利な構造に対抗するには、技術的対策だけでなく、制度・組織・オペレーション・人材育成を社会全体で刷新する必要がある。

本会議は、AI を防御側の力へと転換し、政府の政策、民間の技術力、学術機関の知見を結集する「産官学連携」によって、我が国のサイバーセキュリティ対策を根本から強化することを目的として開催された。

2. 政府に対する政策的示唆

2.1. 「日本版パランティア」構想による統合データ基盤の構築

本会議の議論を通じて、産官学が保有する脅威情報を統合的に分析するデータ基盤の不在が、我が国のサイバー防衛における構造的な課題として浮き彫りとなった。加えて、国家サイバー統括室がサイバー情報のハブとして機能し、地政学的情勢や現実空間の事象を含む関連情報を統合的に分析し、抑止・防御の具体的なアクションにつなげていく必要性が、本会議において明確に示された。

政府は、こうした統合データ基盤の「日本版」を構築することを検討すべきである。その際、内閣官房国家サイバー統括室を中心に、経済産業省、総務省、防衛省、警察庁その他の関係機関が連携し、重要インフラ事業者、行政機関、官民協議会参加企業等から得られる脅威情報、インシデント情報、関連する外部情報を横断的に統合分析し得る枠組みを整備することが重要である。とりわけ初年度においては、重要インフラ分野の複数業種を対象とした実証を開始し、接続機関数、共有インシデント件数、分析結果に基づく対応指示件数等を成果指標として設定したうえで、双方向の情報共有体制を早期に立ち上げるべきである。

Copyright (c) 2026 GMO Internet Group, Inc. All Rights Reserved.

2.2. 能動的サイバー防御の運用基準の明確化と実効性確保

2025 年 5 月に成立したサイバー対処能力強化法により、能動的サイバー防御の法的基盤は整備された。本会議においても、防衛省・自衛隊がアクセス無害化措置という新たな任務を担うこと、また政府として脅威ハンティング、技術的注意喚起、パブリックアトリビューション等を組み合わせ、平時から攻撃者側にコストを付加する考え方が共有された。

しかしながら、これを真に社会実装するためには、有事と平時の境界が曖昧な現代戦における具体的な運用基準の確立が急務である。現場の懸念として、ID やパスワードの窃取といった偵察段階においてどの時点で国家として介入できるのか、またボットネット停止や重大なランサム被害のような事案をどの範囲で対象とするのかについて、実務上の判断基準がなお十分に明文化されていない。

政府は、内閣官房国家サイバー統括室を司令塔とし、防衛省、警察庁その他の関係省庁が連携して、偵察段階、侵入準備段階、被害発生段階のそれぞれに応じた介入要件、対象類型、判断主体、法的手続を体系的に整理し、公表すべきである。あわせて、重要インフラ事業者を含む官民合同演習を定期的に実施し、演習回数、参加機関数、初動判断時間等を指標として、制度の実効性を継続的に高めていく必要がある。

2.3. 「国産 AI 基盤」構築への国家支援と高度専門人材育成の拡充

我が国のデジタル基盤における最大の脆弱性は、クラウド基盤やそれを根底で制御する中核システムといった「システムソフトウェア領域」において自国技術の厚みが不足している点にある。本会議でも、GPU 等の計算資源を確保するだけでは不十分であり、クラウド基盤、ハイパーバイザー、セキュリティ層その他のシステムソフトウェア領域を含め、設計から運用まで自国で理解し制御できる基盤を持つことの重要性が繰り返し指摘された。

政府は、経済産業省を中心に、文部科学省、デジタル庁、内閣官房等と連携し、半導体、クラウド基盤、推論実行環境、AI セキュリティ検証の各層を対象とする支援策を講じるべきである。同時に、ホワイトハッカー、システムソフトウェア技術者、AI 安全性評価人材を重点育成対象として位置づけ、大学、高専、専門機関、民間事業者と連携した人材育成枠組みを拡充すべきである。支援プロジェクト数、育成人材数、国内実証環境数、重要インフラ向け実装案件数等を成果指標として設定し、国家支援の実効性を可視化していくことが求められる。

Copyright (c) 2026 GMO Internet Group, Inc. All Rights Reserved.

2.4. サイバー被害に対する社会的セーフティネットの創設検討

生成 AI の普及により、攻撃者は極めて低いコストで無限に近いパターンの攻撃手法を生成できるようになり、もはや個別の企業や個人の自助努力には限界が生じている。本会議でも、AI 詐欺やフィッシングのようなランダム被害については、被害者の自己責任として処理するだけでは救済が行き届かず、社会全体でリスクを吸収する仕組みが必要であるとの問題意識が共有された。

サイバー攻撃を 100%防ぎ得ないという現実に鑑み、ランダムかつ大規模に発生する被害を救済するための互助的な保険制度や、公的な支援枠組みの創設を本格的に検討すべきである。その際には、金融庁、総務省、経済産業省、警察庁その他の関係機関が連携し、個人向けの相談・被害回復支援と、中小企業向けの初動復旧支援を組み合わせた試行的制度の創設を進めることが望ましい。支援件数、平均復旧日数、相談窓口到達率、再発防止策の実施率等を成果指標として設定し、制度の実効性を継続的に検証すべきである。

2.5. シームレスな脅威情報共有体制の確立に向けた制度設計

サイバー脅威に対抗するためには、技術やシステム以上に、組織の壁を越えた「顔の見える信頼関係（ヒューマンネットワーク）」の構築が極めて重要である。本会議では、官民協議会の立ち上げ、民間事業者との双方向コミュニケーション、外国政府との情報共有拡大の必要性が示されるとともに、最終的には人と人との信頼が実効的な連携を支えるとの認識が共有された。

政府は、内閣官房国家サイバー統括室を中心に、重要インフラ事業者、IT 事業者、セキュリティ企業、研究機関等を含む常設の官民協議会を早期に整備すべきである。共有対象については、インシデント情報にとどまらず、攻撃兆候、脆弱性情報、地政学リスク、偽情報や心理戦に関する兆候等も含め、より実践的なものへと拡張していく必要がある。さらに、官民人材の出向、共同演習、分野横断のワーキンググループの設置等を通じて、平時から顔の見える関係を構築し、参加組織数、共有情報件数、共同演習数、人材交流人数等を指標として体制の成熟度を評価すべきである。

Copyright (c) 2026 GMO Internet Group, Inc. All Rights Reserved.

3. おわりに

本提言書は、「第 3 回 GMO 大会議🌸春 サイバーセキュリティ 2026」における産官学の議論を集約し、5 つの政策提言として整理したものである。ご登壇いただいた有識者の皆様、ならびにご参加いただいた約 5,000 名の皆様に、心より感謝申し上げる。

AI 技術の急速な進展とサイバー脅威の高度化により、サイバーセキュリティは個々の組織の課題を超え、わが国の経済安全保障に直結する喫緊の課題となった。本会議の議論が示すように、産官学の垣根を越えた連携と対話が、かつてないほど求められている。

GMO インターネットグループは、インターネットインフラを支える企業として、引き続き産官学の対話の場を提供し、わが国のサイバーセキュリティの強化に貢献していく所存である。本提言が、今後の政策立案における一助となれば幸いである。

以上

2026 年 3 月 18 日（水）
GMO インターネットグループ株式会社
第 3 回 GMO 大会議🌸春 サイバーセキュリティ 2026 事務局

Copyright (c) 2026 GMO Internet Group, Inc. All Rights Reserved.