ホワイトハウス『サイバー戦略白書』

President Trump’s Cyber Strategy for America

―サイバー空間における米国の攻撃的抑止と同盟ネットワーク戦略

政策分析レポート
Policy Analysis Report

Issue No. 001
2026 年 3 月 9 日

発行元: 一般財団法人 日本危機管理研究所
執筆：舩山 美保

Note
An English version of this report is included in the latter half.

1　はじめに

本稿は、2026 年 3 月 6 日ホワイトハウスが正式公開した『米国サイバー戦略白書』の概要と分析である。
今回の白書は「President Trump’s Cyber Strategy for America」というタイトルで約 7 ページにまとめられており、トランプ政権 2 期目における最初の“包括的サイバー戦略”とされている。実際の米国『サイバー戦略』は非常に長く、例えば

・National Cyber Strategy（約 40 ページ）
・National Cybersecurity Strategy（約 35 ページ）

などは「政策」、「法制度」、「官民連携」、「実行計画」まで細かく書かれている。
しかし今回の文書はそのような“政策文書”ではなく、“戦略宣言”に近い構造となっている。
実際の作戦は、

・NSC（国家安全保障会議）
・United States Cyber Command

・National Security Agency

などの内部文書で定められている可能性が高い。

米国は“軍事戦略の転換期”に、短い文書で方針だけを示すことがあり、今回の文書もその可能性が高い。

2　今回の戦略の基本構造

今回発表された戦略は、以下の 6 つの柱で構成されている。

1　敵対勢力の行動を抑止（offensive cyber 含む）
2　サイバー規制の合理化
3　連邦政府ネットワークの近代化
4　重要インフラ防護
5　AI・量子など新技術での優位維持
6　サイバー人材の育成

白書自体は短いが、いくつか非常に重要な「暗示」が含まれている。

特に注目されるのは以下である。

・AI サイバー戦争
・私企業の攻撃参加
・国家を超えたサイバー作戦

3　最大のポイント

「サイバーは防御ではなく戦争手段」

従来の米国サイバー政策（2010 年代〜2023 頃）は主に

・インフラ防御
・民間防御
・サイバー犯罪対策

つまり**守り中心**だった。

しかし今回の戦略では以下のキーワードが頻出する。

・proactive disruption
・pre-emptive cyber action
・persistent engagement

これは簡単に言えば

「敵の攻撃前にこちらが先に潰す」

という考え方であり、軍事でいう**先制攻撃ドクトリン**に近い。

4　AI 戦争の正式認識

白書のもう一つの重要な点は、AI を「サイバー戦争の中核技術」と明言したことである。

現在のサイバー戦争は

・数百万の脆弱性
・数百万の端末
・数百万の通信パケット

をリアルタイム処理する必要がある。これは人間では不可能であり、**AI が攻撃し AI が防御する戦争**へ移行している。

5　民間テック企業の軍事化　―“協力”から“統合”への転換

米国のサイバー戦略では、政府と民間企業の協力は従来から重要視されてきたが、今回の戦略では、民間企業をサイバー戦力として統合する方針が明確に示されている。
米国では既に以下の企業が実質的に軍事サイバー能力の一部となっている。

・Microsoft
・Palantir
・Amazon

・Google
・SpaceX
・CrowdStrike

ウクライナ戦争でも

・Starlink
・Microsoft threat intelligence

などが実際に使用された。

つまり現代の戦争は

****国家＋テック企業連合****

という構造になっている。

6　サイバー同盟ネットワーク

白書では具体的な同盟国名は明記されていない。これはサイバー戦争では、

・政府
・軍
・情報機関
・民間企業
・外国政府

など複数の主体がネットワークとして作戦に参加するため、参加国が流動的だからと考えられる。

実際のサイバー同盟としては

・Five Eyes
・米国
・英国
・カナダ

・オーストラリア
・ニュージーランド

さらに拡張ネットワークとして

・イスラエル
・日本
・オランダ
・韓国
・ポーランド

などが存在するとされる。

特にイスラエルは AI サイバー領域で極めて重要な役割を持つ。

7　Epic Fury 作戦との関係

今回の白書が出たタイミングも重要である。
Epic Fury 作戦（米国・イスラエル対イラン）では、すでに新しい戦争形態が使われていたと考えられているのでそれを明言したことになる。

新しい戦争構造は

サイバー攻撃
↓
AI 分析
↓
ドローン攻撃
↓
ミサイル攻撃

つまり

****デジタル → 物理攻撃****

の連動である。

8　AI サイバー冷戦の構図

現在のサイバー戦争は、二つの陣営の競争になりつつある。

西側

・米国
・NATO
・日本
・イスラエル
・Five Eyes

対

非西側

・中国
・ロシア
・イラン
・北朝鮮

本白書が公開されたタイミングも注目される。
ロシアがイランに米軍の位置情報を共有したとの報道の直後であったためである。米国が敵対勢力に対し、サイバー領域での抑止意思を示す“戦略的シグナル”としての意味を持つ可能性が指摘されている。

9　日本にとっての意味

今回の白書は日本にとっても重要である。
米国はサイバー戦争の前線を同盟国に広げる方針を示している。

日本は

・米軍基地
・データセンター

・通信インフラ

などを通じて、**サイバー戦争の前線になりうる。**

10　結論

今回のホワイトハウスの『サイバー戦略』は、米国の安全保障政策の重要な転換を示している。

特にこの三点は、今後の戦争の形を大きく変える可能性がある。

・サイバーを攻撃的戦争手段として位置付けたこと
・AI を戦争の中核技術として認識したこと
・テック企業を含む同盟ネットワーク戦略

最終的に本白書の目的は、米国が AI やサイバー分野で、同盟国と協力した「信頼できる技術圏（技術同盟）」を形成し、**米国を中心とした新たな国際デジタル秩序の形成を主導しようとする戦略的意図がうかがえる。**

以上

・主要資料

The White House
President Trump’s Cyber Strategy for America
（ホワイトハウス「米国サイバー戦略」）
https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf
（2026 年 3 月 6 日公開 / 2026 年 3 月 9 日確認）

（注）
本レポートの内容は執筆者個人の見解であり、必ずしも一般財団法人日本危機管理研究所の公式見解を示すものではない。

English Version

White House “Cyber Strategy White Paper”

President Trump’s Cyber Strategy for America

— Offensive Cyber Deterrence and Alliance Network Strategy in Cyberspace —

Policy Analysis Report

Issue No. 001
March 9, 2026

Issued by: Japan Institute for Crisis Management
Author: Miho Funayama

1. Introduction

This report provides an overview and analysis of the U.S. Cyber Strategy White Paper officially released by the White House on March 6, 2026.

The document, titled “President Trump’s Cyber Strategy for America,” is summarized in approximately seven pages and is regarded as the first comprehensive cyber strategy of the second Trump administration.

In practice, official U.S. cyber strategy documents are usually much longer. Examples include:

- National Cyber Strategy (approx. 40 pages)
- National Cybersecurity Strategy (approx. 35 pages)

These documents typically detail policy frameworks, legal structures, public–private partnerships, and implementation plans.
However, the current document differs in nature. Rather than a detailed policy paper, it resembles a strategic declaration.

Actual operational frameworks are likely defined in internal documents of:

- the National Security Council (NSC)
- United States Cyber Command
- the National Security Agency (NSA)

The United States has historically issued short documents outlining strategic direction during periods of military transition, and this document may represent such a case.

2. Structure of the Strategy

The newly announced strategy consists of six major pillars:

① Deterrence of adversarial activities (including offensive cyber operations)
② Rationalization of cyber regulations
③ Modernization of federal government networks
④ Protection of critical infrastructure
⑤ Maintaining technological superiority in AI and quantum technologies
⑥ Development of cyber workforce

Although the white paper itself is short, it contains several important implicit signals.
Particularly noteworthy are the implications regarding:

- AI-driven cyber warfare
- Participation of private companies in cyber operations
- Cyber operations extending beyond national borders

3. The Most Significant Point

“Cyber is no longer merely defensive—it is a tool of warfare.”

Previous U.S. cyber policies (from the 2010s to around 2023) primarily focused on:

- infrastructure defense
- private-sector protection
- countermeasures against cybercrime

In other words, they emphasized defensive strategies. However, the new strategy repeatedly uses the following terms:

- proactive disruption
- pre-emptive cyber action
- persistent engagement

Simply put, this reflects the concept of:

“Neutralizing the adversary before their attack occurs.”

This approach closely resembles a pre-emptive strike doctrine in traditional military strategy.

4. Formal Recognition of AI Warfare

Another significant aspect of the white paper is the explicit identification of AI as a core technology of cyber warfare.

Modern cyber warfare requires real-time processing of:

- millions of vulnerabilities
- millions of devices
- millions of communication packets

Such tasks exceed human capacity.

As a result, warfare is evolving into a domain where AI conducts both attacks and defenses.

5. Militarization of Private Tech Companies

From “Cooperation” to “Integration”

Public–private cooperation has long been an important element of U.S. cyber strategy. However, the new strategy clearly signals a shift toward integrating private companies as components of national cyber power.

In the United States, the following companies already function, in practice, as part of the country's cyber capabilities:

- Microsoft
- Palantir
- Amazon
- Google
- SpaceX
- CrowdStrike

During the war in Ukraine, technologies such as:

- Starlink
- Microsoft threat intelligence

were actively used in real operations.

Modern warfare is therefore increasingly structured as:

- a coalition of states and technology companies.

6. Cyber Alliance Network

The white paper does not explicitly name allied countries.
In cyber warfare, however, operations typically involve multiple actors, including:

- governments
- militaries
- intelligence agencies
- private companies
- foreign governments

Because these participants form dynamic operational networks, specific participants may change depending on circumstances.

Existing cyber alliances include:

- Five Eyes
- United States
- United Kingdom
- Canada
- Australia
- New Zealand

Additionally, an expanded network is believed to include:

- Israel
- Japan
- Netherlands
- South Korea
- Poland

Among these, Israel plays an especially important role in AI-driven cyber capabilities.

7. Relation to “Operation Epic Fury”

The timing of the white paper’s release is also significant.
In “Operation Epic Fury” (a U.S.–Israel operation against Iran), a new form of warfare is believed to have already been employed.
The strategy may therefore represent an explicit acknowledgment of this emerging warfare model.

The new operational structure can be summarized as:

Cyber attack
↓
AI analysis
↓
Drone strike
↓
Missile strike

In other words:

“Digital operations” → “physical attacks”

8. The Emerging AI Cyber Cold War

Cyber warfare today is increasingly evolving into a competition between two major blocs.

【Western bloc】

United States
NATO
Japan
Israel
Five Eyes

【Non-Western bloc】

China
Russia
Iran
North Korea

The timing of the white paper’s release is also notable because it came shortly after reports that Russia had shared U.S. military location data with Iran.
This suggests the possibility that the document serves as a strategic signal, demonstrating U.S. deterrence intentions in cyberspace toward adversarial powers.

9. Implications for Japan

The strategy also carries important implications for Japan.
The United States appears to be expanding the frontline of cyber warfare to include allied nations.

Japan could become a frontline cyber theater due to:

- U.S. military bases
- data centers
- communication infrastructure

10. Conclusion

The White House Cyber Strategy represents a significant shift in U.S. national security policy. In particular, the following three elements could fundamentally reshape the future of warfare:

- positioning cyber operations as an offensive instrument of warfare
- recognizing AI as a core military technology building
- an alliance network strategy including technology companies

Ultimately, the white paper suggests that the United States seeks to establish a “trusted technology sphere” (technology alliance) with its allies in the fields of AI and cybersecurity.

Through this framework, **the U.S. appears to aim to lead the formation of a new international digital order centered on American technological leadership.**

Key Source:
The White House
President Trump’s Cyber Strategy for America
(https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf)
Published March 6, 2026 / Accessed March 9, 2026

Note:
The contents of this report represent the views of the author and do not necessarily reflect the official position of the Japan Institute for Crisis Management.