世界のサイバーセキュリティ政策から見る
これからのサイバーセキュリティの流れ

2025年01月24日

PwCコンサルティング合同会社パートナー
丸山満彦

自己紹介

丸山満彦

パートナー PwCコンサルティング合同会社

JPCERTコーディネーションセンター監事

日本シーサート協議会監事

情報セキュリティ大学院大学客員教授

略歴

- 25年にわたり製造業、サービス業、金融機関、政府などの幅広い業種に対するサイバーセキュリティ、ITリスク分野のコンサルティング、監査に携わる。内閣官房に出向し、内閣官房サイバーセキュリティセンターの立ち上げ、政府統一基準の策定、改訂に関与。ISMS制度の立ち上げ、普及にも関わる。内閣官房、総務省、経済産業省などの有識者委員に多数就任しているほか、複数のセキュリティ関連団体の理事、監事も務める。
- 情報セキュリティ文化賞（2021年）受賞

資格

- 公認会計士(CPA)
- 公認情報システム監査人(CISA)

本日の概要

世界のサイバーセキュリティ政策から見るこれからのサイバーセキュリティの流れ

インターネットにより作り出されるデジタル空間が、**社会の重要なインフラの一部**となってきています。デジタル空間の安全を確保することが社会の発展と安全につながります。この**デジタル空間の安全を守る**ために各国、地域はそれぞれ**国民、国家の利益**となるような政策を作り、実行しています。そこで、これら世界の**主要国のサイバーセキュリティ政策を概観**し、私たちが**進むべき方向**を考えてみたいと思います。それは、皆様のこれからのビジネスのヒントにつながるかもしれません。

Agenda

1.世界のサイバーセキュリティ政策概観

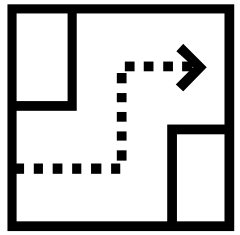
(1) サイバーセキュリティ政策の歴史
(2) サイバーセキュリティ政策の位置付け

2.各国のサイバーセキュリティ政策

(1) 米国のサイバーセキュリティ政策
(2) 英国のサイバーセキュリティ政策
(3) 欧州のサイバーセキュリティ政策
(4) 中国のサイバーセキュリティ政策
(5) 日本のサイバーセキュリティ政策

3.各国のサイバーセキュリティ政策を眺めてみて…

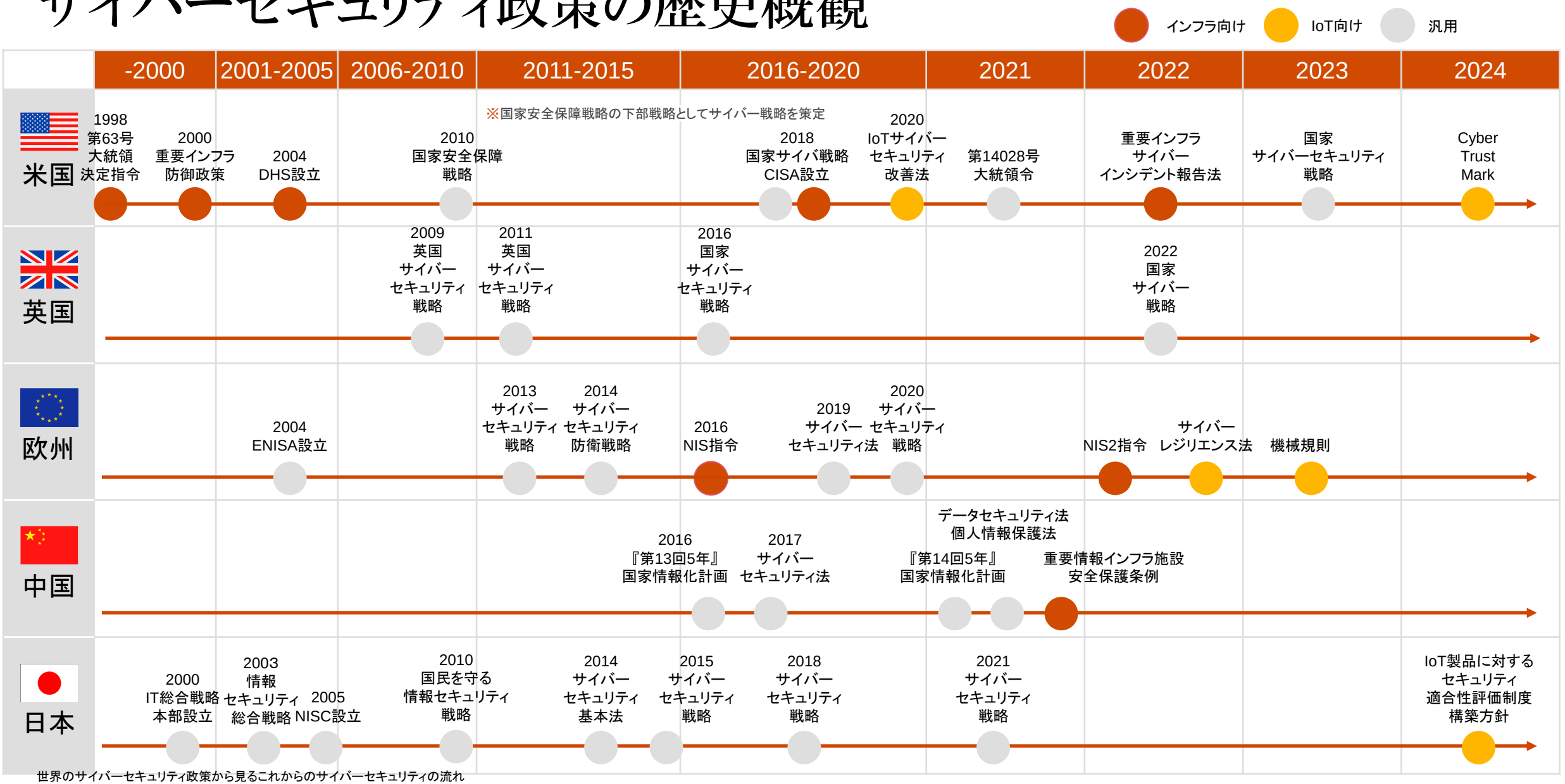
4.まとめ



1

世界の
サイバーセキュリティ
政策概観

サイバーセキュリティ政策の歴史概観



世界のサイバーセキュリティ政策から見るこれからのサイバーセキュリティの流れ

※**重要インフラ事業者**向けの計画、ガイド等もNISC設立時から策定している。

サイバー（セキュリティ）政策の位置付け

国家安全保障（National Security）政策の一環

国家安全保障

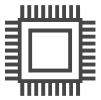
国民の生命、自由、繁栄を外部および国内の脅威から守るための戦略および政策の集合体

国家の主権と国民の安全を守る


外交


軍事


経済


技術


情報

サイバー空間の安全を維持することがサイバーセキュリティ政策の目的に含まれるのであれば、サイバーセキュリティ政策は国家安全保障政策の一部となる。

国家安全保障戦略

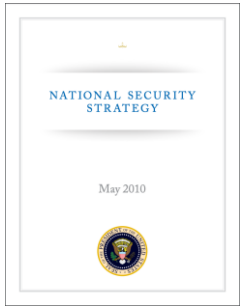
サイバーセキュリティ戦略

2

各国の
サイバーセキュリティ
政策

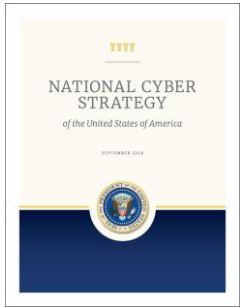
(1)米国のサイバーセキュリティに関連した戦略の歴史

米国の国家サイバーセキュリティ戦略は、政府、重要インフラから製品セキュリティへ



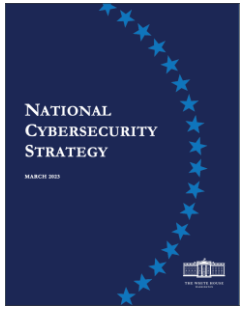
国家安全保障戦略 2010

- 国家安全保障を強化するためのビジョンを提示
- 国際協力、国内経済力・競争力強化、軍事・防衛改革、グローバル脅威への対応
- サイバー空間の安全性のために、特に**政府機関・重要インフラ**の人材・テクノロジー投資、法規制・データ保護・ネットワーク防御などでの国際協力



国家サイバー戦略 2018

- 4つの柱：①国家サイバー防衛強化、②米国の繁栄促進、③平和維持とサイバー犯罪防止、④国際協力
- **重要インフラ防御**、人材育成、インシデント報告、デジタル経済レジリエンス強化など



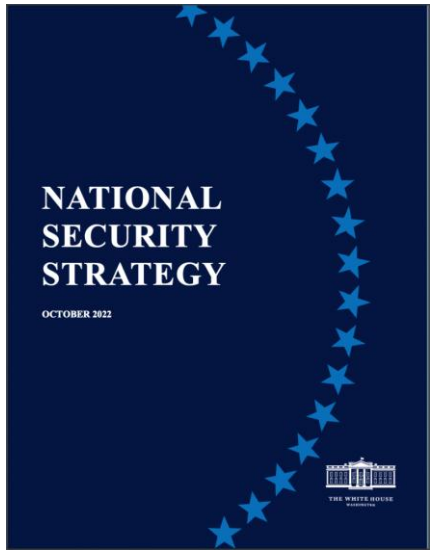
国家サイバーセキュリティ戦略 2023

- 5つの柱とその柱にそった戦略：①重要インフラの防護、②脅威アクターの妨害・解体、③市場におけるセキュリティ・レジリエンス推進、④レジリエントな将来への投資、⑤国際パートナーシップ
- **ZTA推進、ランサムウェア対策、サプライチェーンセキュリティ（OT含む）**

世界のサイバーセキュリティ政策から見るこれからのサイバーセキュリティの流れ
PwC

(1)米国の国家安全保障戦略2022

米国の力の源泉に投資（先端産業の育成など）、同志国との協力関係を通じた影響力の強化、軍の近代化と強化などがうたわれている。



次に来るもののための競争

国際秩序を形成するために独裁的な大国と競争すべき

米国人は普遍的な人権を支持し、自由と尊厳を求める国外からの人々と連帯する。

強さへの投資

開かれた市場により、近代的な産業・イノベーション戦略を推進

半導体、先進コンピュータ、次世代通信、グリーンエネルギー技術、バイオテクノロジーへの投資

サイバー空間を含めた産業基盤の保護

外交による連合体の構築

軍の近代化と強化

国家防衛戦略2022

グローバルな優先課題

競合相手（中国、ロシア）による国際秩序への挑戦に対応する。

共通課題への協力

気候変動・エネルギー安全保障、パンデミック、食料安全保障、軍拡、テロ、国際犯罪など

将来に向けて

技術への投資、サイバー空間の確保、貿易・経済

地域別戦略

陸の優先順位は、

インド太平洋

欧州

中南米

中東

アフリカ

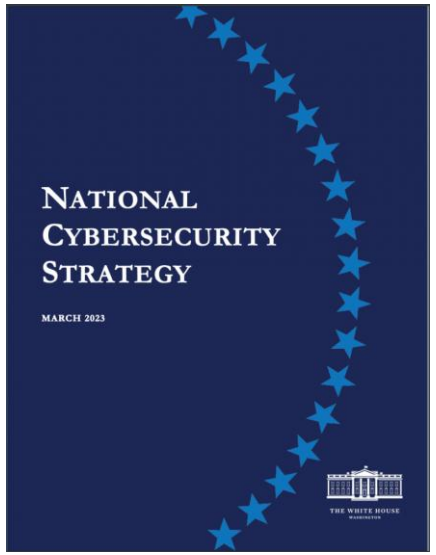
北極圏

海・空・宇宙

出所；米国ホワイトハウス ‘NATIONALSECURITYSTRATEGY（国家安全保障戦略）
https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

(1)米国の国家サイバーセキュリティ戦略2023

- インターネットが人権と基本的自由を尊重する普遍的価値に支えられ、オープン、自由、信頼性、安全性などを維持することを保証
- サイバースペースでの行動に関するルールや規範を策定
- 官民間の強固な協力がサイバースペースの安全確保に不可欠

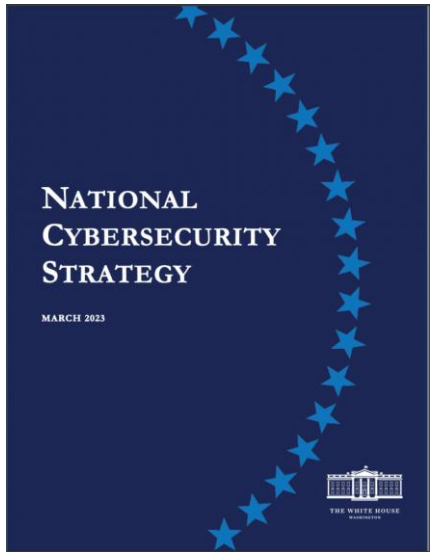


重要インフラ保護	脅威アクターの破壊・解体	市場の力の形成	未来への投資	国際的なパートナーシップの構築
1. 国家安全保障と公共安全を支援するためのサイバーセキュリティ要件の確立	1. 連邦政府による破壊活動の統合	1. データの管理者に説明責任を持たせる	1. インターネットの技術的基盤の確保	1. デジタル・エコシステムへの脅威に対抗するための連合を構築する
2. 官民協力の拡大	2. 敵対者をかく乱するための官民の作戦協力の強化	2. 安全なIoTデバイスの開発の促進	2. サイバーセキュリティのための連邦政府研究開発の活性化	2. 国際的なパートナーの能力の強化
3. 連邦政府のサイバーセキュリティセンターの統合	3. 情報共有と被害者通知の速度と規模の拡大	3. 安全でないソフトウェア製品とサービスに対する責任の転換	3. 量子時代後の未来への備え	3. 同盟国やパートナーを支援する米国の能力の拡大
4. 連邦政府の事故対応計画及びプロセスの更新	4. 米国拠点のインフラ悪用の防止	4. 連邦政府の補助金やその他のインセンティブを利用したセキュリティの構築	4. クリーンエネルギーの未来の確保	4. 責任ある国家行動の世界的規範を強化するための連合体構築
5. 連邦防衛の近代化	5. サイバー犯罪への対抗とランサムウェアの撲滅	5. 連邦調達の活用によるアカウンタビリティの向上	5. デジタルIDエコシステムの開発支援	5. 情報・通信・OT製品およびサービスのためのグローバル・サプライ・チェーンの安全確保
		6. 連邦政府によるサイバー保険のバックアップの検討	6. サイバー人材強化のための国家戦略の策定	

出所；米国ホワイトハウス‘NATIONAL CYBERSECURITY YSTRATEGY（国家サイバーセキュリティ戦略）
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdff

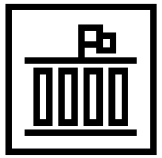
(1)米国の国家サイバーセキュリティ戦略2023

ファクトシートで強調されている2点



1. サイバーセキュリティの負担を個人、中小企業、地方自治体から、最も能力があり、我々全員のリスクを軽減できる立場にある組織に移すことで、サイバー空間を防衛する責任を再分配しなければならない。

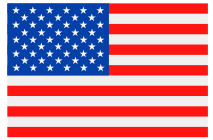
2. 今日の緊急の脅威から身を守ると同時に、レジリエンスの高い将来に向けて戦略的に計画を立て、投資することの間で慎重にバランスを取ることにより、長期的な投資を促進するようインセンティブを再編成しなければならない。



中小規模の組織に多くを求めても実現できない....

出所；米国ホワイトハウスFACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy
https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

(1)参考：米国の主要なサイバーセキュリティ関連組織



ホワイトハウス
国家情報セキュリティ長官室
（ONCD）

2021年度国防主権法に基づき、大統領府内に設置されている。
大統領にサイバーセキュリティに関連する事項を助言する。
政府のセキュリティ政策の取りまとめを行い、各省庁間の政策等の調整を行う。

国防省
（DoD）

国家安全保障局
（NSA）

防衛産業基盤（DefenseIndustrialBase;DIB）にかかる
・サイバーセキュリティ
・SIGINT
・暗号
を所管

司法省
（DoJ）

連邦捜査局
（FBI）

サイバー攻撃、サイバー脅威、スパイ行為を含む、
サイバー犯罪の捜査・起訴などの
サイバーセキュリティの法執行

国土安全保障省
（DHS）

サイバーセキュリティ・重要インフラセキュリティ庁
（CISA）

連邦機関システムの
・サイバーセキュリティ、
・インシデントレスポンス
を所管

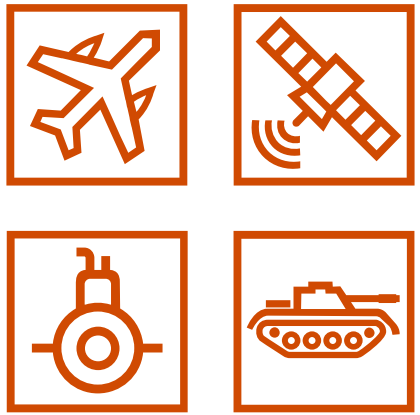
商務省
（DoC)

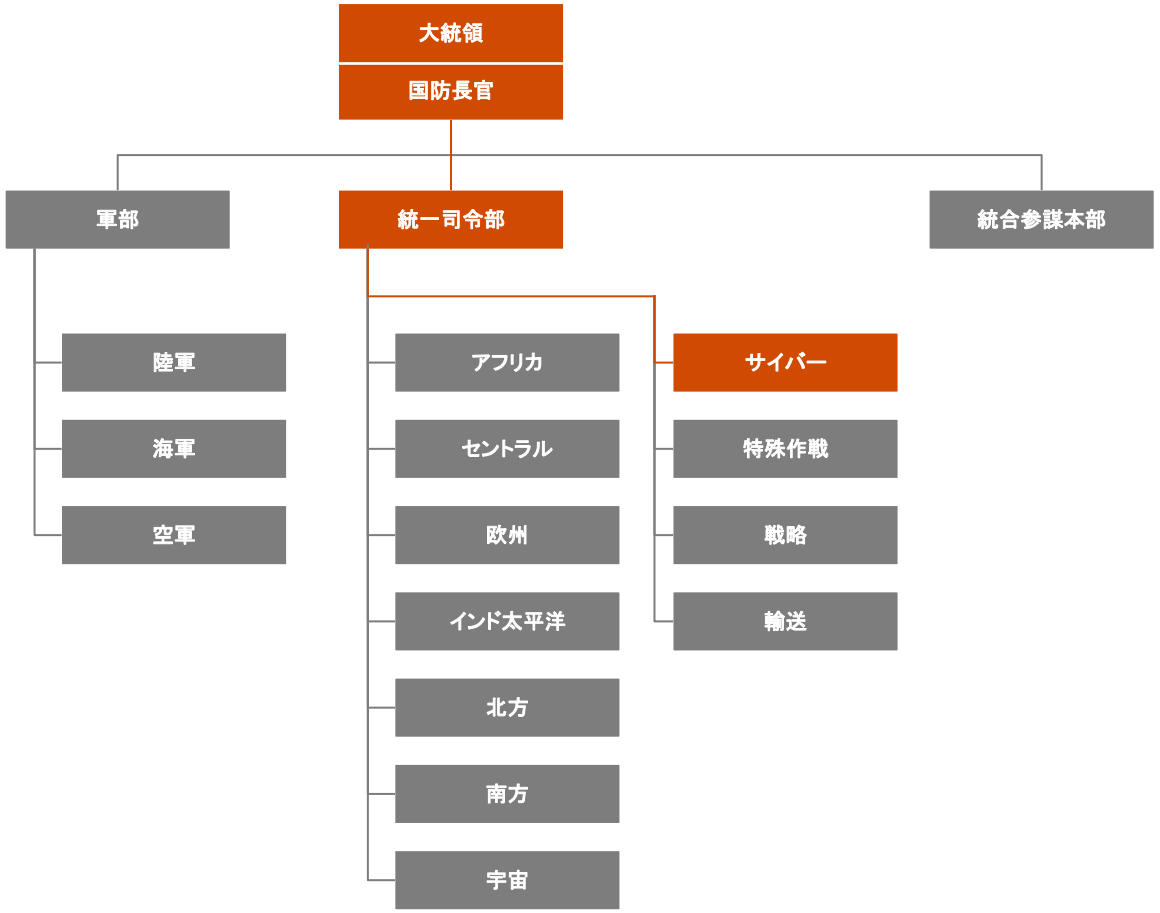
国立標準技術研究所
（NIST）

サイバーセキュリティ分野に関し、
・標準
・基準
・ガイドライン
・ベストプラクティス等
作成

(1)参考：米国のサイバー軍　(Cyber Command)

11ある統一戦闘司令部（7地理的基盤＋4機能的基盤）の1つ（機能的基盤）としてサイバー軍がある。

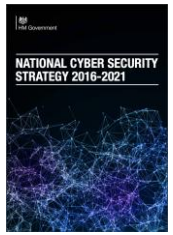


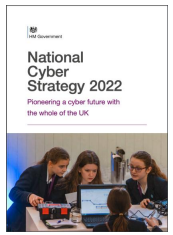


サイバー軍が守るのは

1. 軍のシステム
2. 政府のシステム
3. 重要インフラのシステム

(2)英国のサイバーセキュリティに関連した戦略の歴史





2009 英国サイバーセキュリティ戦略

- 19世紀は海、20世紀は空、21世紀はサイバー空間を制するものが世界を制する。
- サイバー空間の安全性、セキュリティ、レジリエンスを確保し、そこから生まれる機会を最大限に活用するための政府の取り組み
- 政府横断プロジェクトを組成する。政府にサイバーオペレーションセンターを設置し、インシデント対応を調整する

2011 英国サイバーセキュリティ戦略

- **民間セクターとのパートナーシップ強化**
  - GCHQの専門知識の商業的応用
  - 中小企業支援
  - サイバーセキュリティ産業の海外展開
- **サイバー犯罪に取り組む**
  - サイバー特殊部隊の活動強化
  - 国家犯罪庁にサイバー犯罪部門の設置
  - 民間への単一報告システムの設置
- **重要インフラ保護**
- **研究、教育、訓練の強化**

2016 国家サイバーセキュリティ戦略

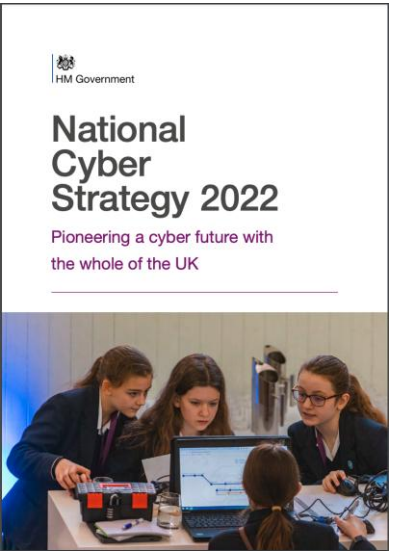
- 防御（サイバー脅威から防御）、抑止（攻撃者から難攻な存在となる）、発展（世界をリードする研究開発をする）に力を入れる。
- 政府は投資を通じて積極的に介入しつつ、標準を利用した市場原理を活用する。
- 軍を強化し、軍との連携を強め、必要に応じて軍が支援する。

2022 国家サイバー戦略

- 2016年の戦略を引き継ぐ。
- サイバーに不可欠な技術分野で英国の能力を強化し、価値観が異なる体制で開発された技術への依存を減らす。
- 5つの柱(1)サイバーエコシステムの強化、(2)レジリエンスなデジタル国家の構築、(3)技術優位性の維持、(4)グローバルリーダーシップ、(5)安全保障の強化のための敵対者の検知、撹乱、抑止

(2)英国の国家サイバー戦略2022のポイント

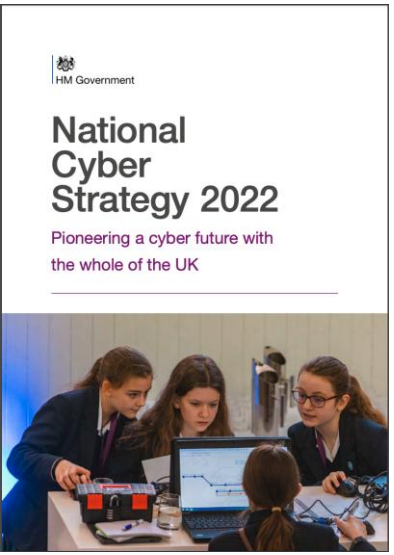
- 2016年の戦略を引き継ぐ。
- サイバーに不可欠な技術分野で英国の能力を強化し、価値観が異なる体制で開発された技術への依存を減らす。



サイバーエコシステム	レジリエンスな国家	技術優位性の維持	グローバルリーダーシップ	敵対者を攪乱し、抑止する
1.サイバーへの全社会的アプローチを支援するのに必要な**構造、パートナーシップ、ネットワークの強化** 2.国家の**サイバースキル**を強化・拡充する。(含む、人材育成) 3.**情報セキュリティセクターの成長を促進**(高品質の製品・サービスの提供)	1.サイバーセキュリティおよびと**レジリエンスに関する効果的な行動**をの促進。 2.組織内の**サイバーリスク管理を改善** 3.国と組織の**レジリエンスの強化**	**1.科学技術**の発展の予測、評価と、それに基づく行動。 2.サイバー空間に必要不可欠な技術の育成と維持 **3.次世代のコネクテッドテクノロジーおよびインフラを確保**。 4.グローバルな**デジタル技術標準の開発**	**1.パートナー諸**国のサイバーセキュリティとレジリエンスを強化 2.自由でオープンで平和で安全なサイバー空間を推進するための**グローバルガバナンス**の形成 3.英国のサイバー能力および専門知識の**輸出**	1.サイバー行為者と活動の**検知、調査、情報共有** 2.サイバー行為者と**活動の抑止し、攪乱** **3.サイバー空間の内部およびサイバー空間を通じた対策**の実行

出所:英国政府
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

(2) 参考：英国の国家サイバー戦略2022



英国のサイバーエコシステムを強化する	レジリエントで豊かなデジタル国家を構築する	サイバーパワーに死活的重要性をもつ技術を先導する	英国のグローバルなリーダーシップと影響力を増進する	敵対者を検知し、攪乱し、抑止する
1. サイバーへの全社会的アプローチを支援するのに必要な**構造、パートナーシップ、ネットワークを強化**する。 2. あらゆるレベルで国家のサイバースキルを強化・拡充する。ここには、世界トップレベルの多様なサイバー専門職へと将来世代の**人材**を育成することも含まれる。 3. 持続可能で革新的、かつ国際競争力を持つサイバーおよび**情報セキュリティセクターの成長を促進**しつつ、政府や経済全体のニーズに応える高品質の製品・サービスを提供する。	1. サイバーリスクへの理解を深め、サイバーセキュリティおよびと**レジリエンスに関する効果的な行動**を促進する。 2. サイバー攻撃をより効果的に防止しこれに抵抗するために、英国の組織内の**サイバーリスク管理を改善**し、国民の保護を強化する。 3. サイバー攻撃に備え、対応し、そこから回復するために、国と組織レベルで**レジリエンスを強化**する。	1. サイバーパワーにとって死活的**重要性をもつ科学技術**の発展を予測、評価し、それに基づいて行動する能力を高める。 2. サイバー空間に必要不可欠な技術の安全保障に関して、主権国家および他国の同盟国としての優位を育成し維持する。 堅牢でレジリエントな**国家的暗号キー**（Crypt-Key)事業を継続していく。この事業は、英国政府の顧客、パートナー諸国、同盟国のニーズを満たすとともに、最強の敵対者からの脅威をも含めて最も重大なリスクを適切に軽減する実績をあげている。 **3. 次世代のコネクテッドテクノロジーおよびインフラを確保**しつつ、グローバル市場への依存で生じるサイバーセキュリティリスクを軽減し、英国のユーザーに信頼性の高い多様な供給へのアクセスを確保する。 4. マルチステークホルダーコミュニティと協力して、グローバルな**デジタル技術標準の開発**に寄与する。特に、民主主義的価値の擁護、サイバーセキュリティの確保、英国の科学技術を通じた戦略的優位の推進に関わる分野を優先する。	**1. パートナー諸**国のサイバーセキュリティとレジリエンスを強化し、敵対者を混乱させ抑止するための集団的活動を増強する。 2. 自由でオープンで平和で安全なサイバー空間を推進するために、**グローバルガバナンス**を形成する。 3. 英国のサイバー能力および専門知識を活用して**輸出**し、戦略的優位を高め、より広範な外交政策と繁栄のための利益を促進する。	1. 英国とその利益および国民を守るために、国家、犯罪者、その他悪意のあるサイバー行為者と活動を**検知し、調査し、情報共有**する。 2. 英国とその利益および国民を狙った、国家、犯罪者、その他悪意のあるサイバー行為者と**活動を抑止し、攪乱**する。 3. 国家安全保障と重大犯罪の防止・検知を支援するため、**サイバー空間の内部およびサイバー空間を通じた対策**を実行する。

出所：英国政府
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

(3)欧州サイバーセキュリティに関連した戦略の歴史

EUは欧州におけるサイバーセキュリティの最重要の要素として、EU市民の個人データ保護の確保、EU・加盟国の安全保障、EU経済の保護、EUにおける民主的プロセスの保護を掲げる


P7_TA(2017)0076
EU cybersecurity strategy: an open, safe and secure cyberspace
European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))
The European Parliament,

サイバーセキュリティ戦略 2013

- 自由と民主主義という欧州の価値観を推進し、デジタル経済の安全な成長を確保することを目的
- 優先事項：①**サイバーレジリエンス**の達成、②サイバー犯罪の激減、③サイバー防衛政策と能力の開発、④サイバーセキュリティのための産業・技術資源の開発、⑤国際サイバー政策の確立を通じたEUの中核的価値を促進
- **重要インフラ向け**のセキュリティ法規制NIS指令策定
- サイバー脅威への対応、EU加盟国の協力強化、**サイバー犯罪防止**、重要インフラ保護、セキュリティ技術強化、国際的安全基準確立、官民連携


EUROPEAN COMMISSION
HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY
Brussels, 16.12.2020
JOIN(2020) 18 final
JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL
The EU's Cybersecurity Strategy for the Digital Decade
EN
EN

サイバーセキュリティ戦略 2020

- 欧州の安全保障と人々の基本的権利にリスクがある場合に、強力なセーフガードを備えたグローバルでオープンなインターネットを確保することが目的
- 構成要素：①**レジリエンス**、技術主権、リーダーシップ、②**防止・抑止・対応**のための活動能力、③**グローバル**で開かれたサイバー空間を推進するための協力
- 手段：規制、投資、政策イニシアティブ

(3)欧州サイバーセキュリティ戦略2020

欧州の安全保障と人々の基本的権利にリスクがある場合に、強力なセーフガードを備えたグローバルでオープンなインターネットを確保することが目的


EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 16.12.2020
JOIN(2020) 18 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The EU's Cybersecurity Strategy for the Digital Decade

EN EN

1. レジリエンス、技術主権、リーダーシップ

1. レジリエントなインフラと重要なサービス
2. 欧州サイバーシールドの構築
3. 極めて安全なコミュニケーションインフラ
4. 次世代のブロードバンドモバイルネットワークのセキュリティ確保
5. 安全なIoT
6. グローバルなインターネットセキュリティの強化
7. テクノロジー・サプライチェーンにおける存在感の強化
8. EUのサイバー技術に精通した労働力

2. 防止・抑止・対応のための運用能力

1. 共同サイバーユニット
2. EUのサイバー外交ツールボックス
3. サイバー防衛能力の強化

3. グローバルで開かれたサイバー空間を推進するための協力

1. サイバー空間における標準、規範、枠組みに関するEUのリーダーシップ
2. パートナーおよびマルチステークホルダー・コミュニティとの協力
3. グローバルなレジリエンスを高めるためのグローバルな能力強化

手段：(1) 規制、(2) 投資、(3) 政策

世界のサイバーセキュリティ政策から見るこれからのサイバーセキュリティの流れ
PwC　出所；https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018

(2)参考:EUサイバーセキュリティ関連組織

サイバーセキュリティに関連する主なEU組織

サイバーセキュリティ庁（ENISA）

EUでサイバーセキュリティ基準高度化を推進する専門機関。効果的なサイバーセキュリティの実践に関するガイダンスと推奨事項を提供する。

CERT-EU

EU機関のITセキュリティ専門家のチームで構成。ICTインフラに関連する脅威、脆弱性、インシデントに関する情報をEUの機関、団体等と収集、管理、分析、共有する。インシデント対応の調整、専門的な運用支援等も行う。

欧州危機対応リエゾン（EU-CyCLONe）

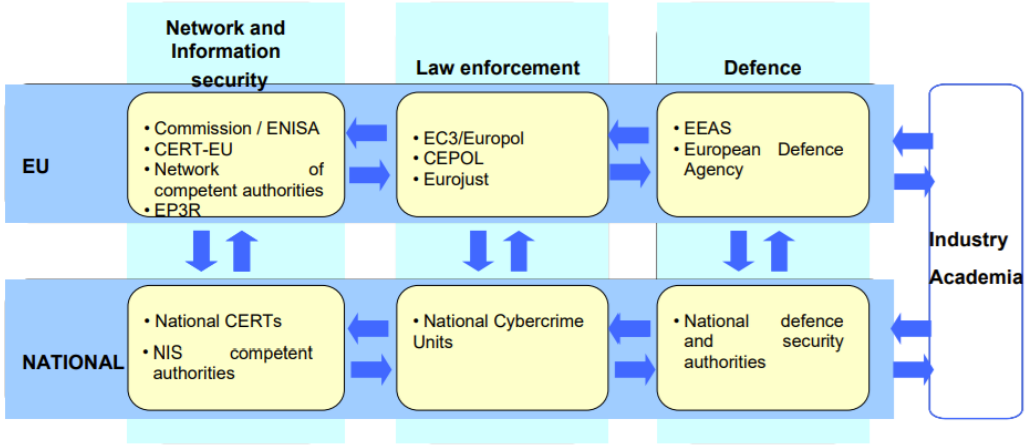
NIS2第16条の発効に伴い2023年1月に正式に組織化。ENISAが提供するツールとサポートに基づいて、タイムリーな情報共有と状況認識を協力して開発する組織。

Europo IEC3 サイバー犯罪センター

EUにおけるサイバー犯罪への法執行対応を強化し、欧州市民、企業、政府をオンライン犯罪から保護することを目的として、欧州警察機構（Europol）によって設立された。

欧州防衛省（EDA）Cyber

加盟国に対し、任務を継続しながらサイバー攻撃を検知し、それに耐え、回復する能力として定義されるサイバーレジリエンスを向上させるための能力開発の支援をする。



出所:欧州サイバーネット
https://www.eucybernet.eu/wp-content/uploads/2020/08/2013-cybersecurity-strategy-of-the-european-union.pdf

(4)中国サイバーセキュリティに関連した戦略の歴史

国家情報化発展戦略綱要および『第13回5年』国家情報化計画 2016

- 向こう10年間の情報化分野の計画・政策立案の根拠指針.
- デジタル化組織体制を定義。サイバーセキュリティは中央指導グループが審査と承認を
- **データ資源管理**の強化、データセキュリティ強化、越境データ移転の管理システム構築、応用の推進、データプラットフォーム建設

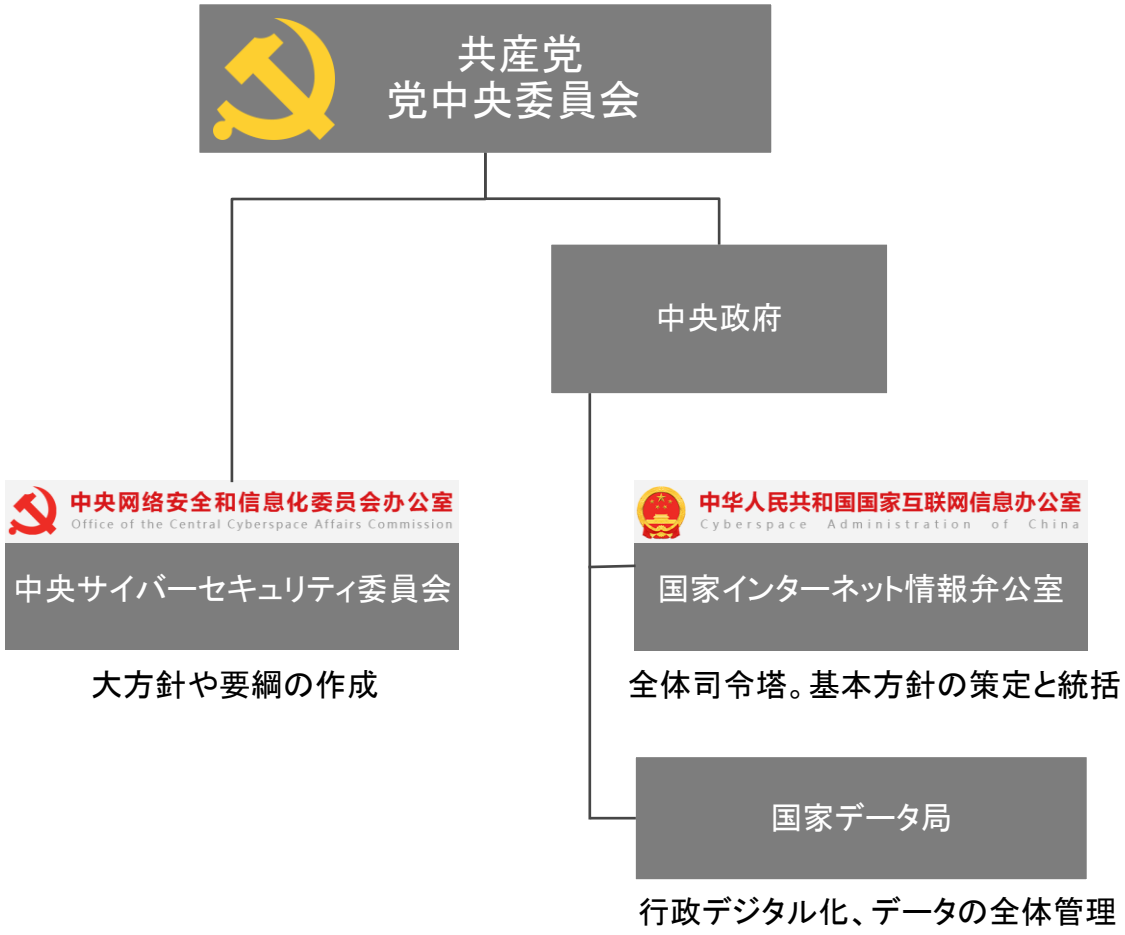
『第14回5年』国家情報化計画 2021

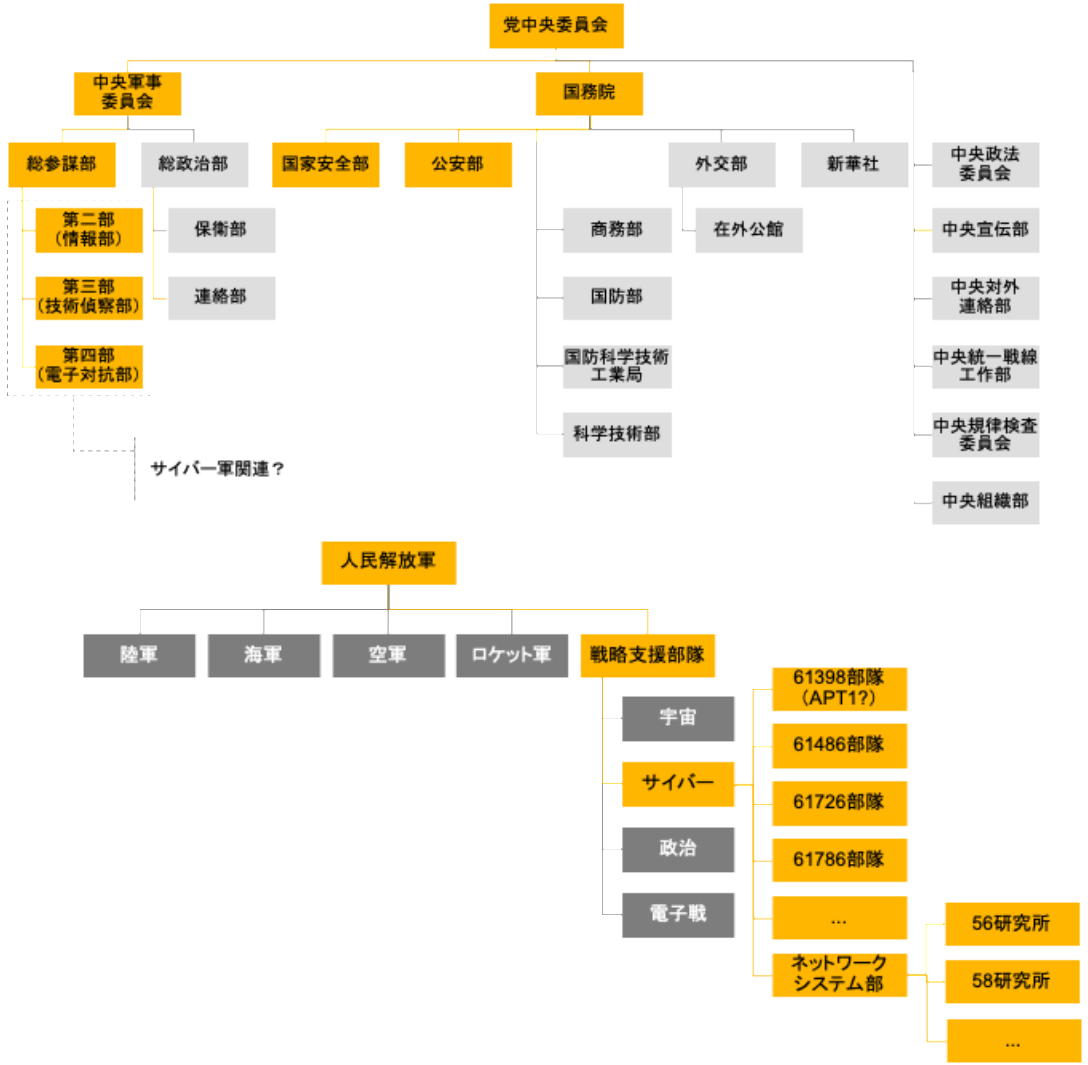
- 「国民経済及び社会発展の第14回5年計画及び2035年の目標綱要」
- 科学技術全般の発展、イノベーション促進、デジタル化推進などハイレベルな戦略が柱であるが、セキュリティも含まれる
- **公共データセキュリティ**、**ネットワーク（クラウド）セキュリティ**、**製品セキュリティ**、国際的産業（**サプライチェーン**）**セキュリティ**推進

基本的な政策として、社会主義革命体制の維持、つまり共産党独裁体制の維持がある。

(4)参考:中国サイキュリティ関連組織

中国におけるサイバーセキュリティに関して頻出する組織。一本化された組織は存在しないものの、中央サイバーセキュリティ弁公室・国家インターネット情報弁公室が全体を指導する立場





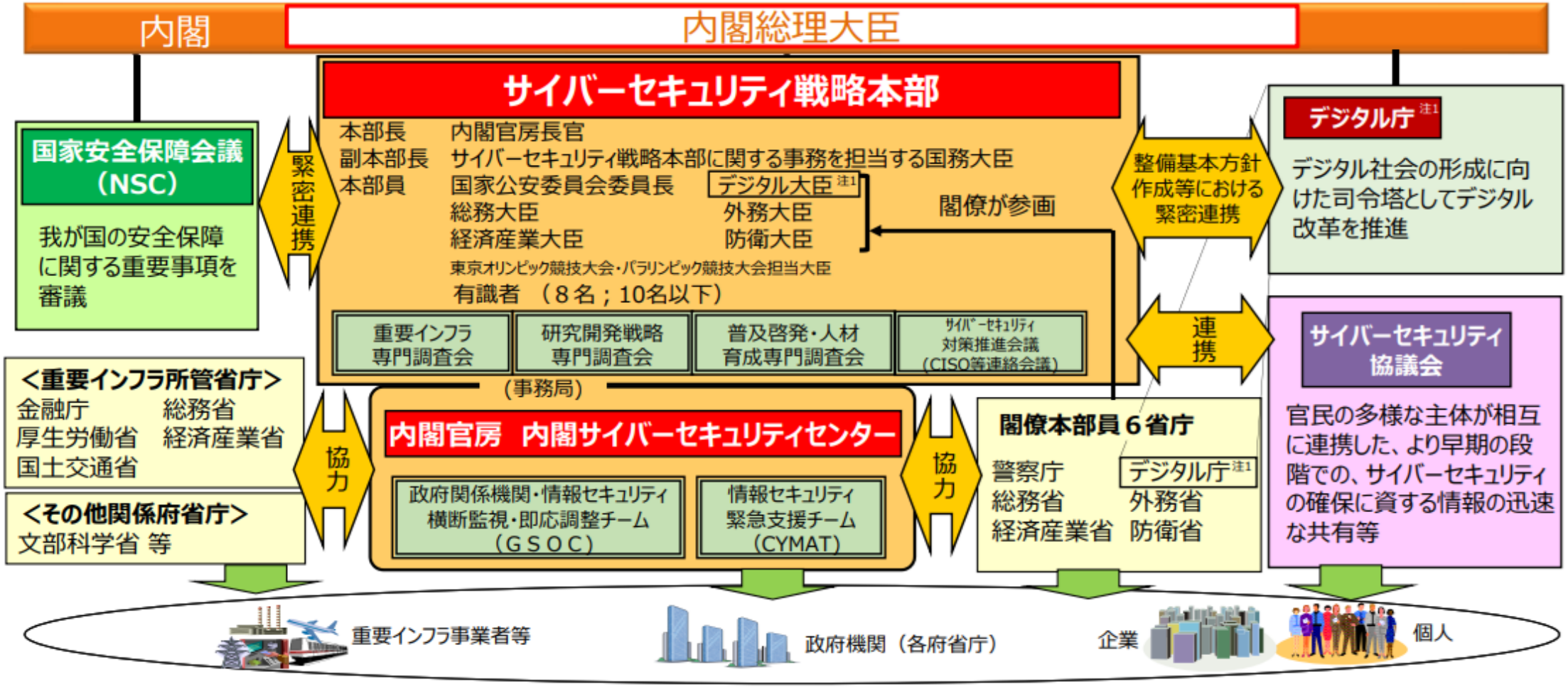
(5)日本サイバーセキュリティに関連した戦略の歴史

経済の持続的発展、安心・安全な国民生活、安全保障の目的の中で、時間と伴にキーワードに変化

2003	情報セキュリティ総合戦略	•世界最高水準の「高信頼性社会」実現による 経済･文化国家日本の競争力強化と総合的な安全保障向上
2006	1次情報セキュリティ基本計画	•「セキュア・ジャパン」の実現に向けて」。新しい官民連携モデルの構築を目指す。
2009	2次情報セキュリティ基本計画	•IT時代の力強い「個」と「社会」の確立に向けて
2010	国民を守る情報セキュリティ戦略	•（米国・韓国への大規模なDDoS攻撃を受けて、2次情報セキュリティ基本計画に追加する形で発表） •重要インフラ防護の強化等、安全保障・危機管理の観点から速やかに 実施すべき取組を推進
2013	サイバーセキュリティ戦略	•世界を率先する強靭で活力あるサイバー空間を目指して •サイバーセキュリティ立国を実現。①情報の自由な流通の確保 ②深刻化するリスクへの新たな対応③リスクベースによる対応の強化④社会的責務を踏まえた行動と共助
2014	サイバーセキュリティ基本法	•情報の自由な流通を確保しつつ、サイバーセキュリティを確保する。 •国民が安全で安心して暮らせる社会の実現や経済社会の活力の向上、国際社会の平和および安全の確保、日本の安全保障に寄与する。
2015	サイバーセキュリティ戦略	•基本原則：①情報の自由な流通の確保、②法の支配、③開放性、④自律性、⑤多様な主体の連携 •目的：①経済社会の活力向上及び持続的発展（安全なIoT、経営層意識変革、社内体制整備、セキュリティ産業振興）、②国民が安全で安心して暮らせる社会の実現（サイバー犯罪対策、情報共有、監査）、③国際社会の平和・安定及び我が国の安全保障（国際的法の支配確立、各国連携）、その他（研究開発、人材育成）
2018	サイバーセキュリティ戦略	•2015年版と目的は変わらず。 •新しいキーワードとして、「サプライチェーン」「積極的サイバー防御」「リアルタイム管理」「教育・研究環境のセキュリティ」「オリンピック」「国家の強靭化」「セキュリティバイデザイン」などが登場
2021	サイバーセキュリティ戦略	•2015年版と目的は変わらず。 •新しいキーワードとして、「クラウドサービスへの対応」「DX with Cybersecurity」「AI for Security」「データ流通」など登場

(5)参考：日本サイバーセキュリティ関連組織

内閣サイバーセキュリティ本部と事務局のNISCを中心に関係組織との連携体制



出所：内閣官房
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf

3

各国の
サイバーセキュリティ
政策を眺めてみて...

サイバー空間は、国民生活、国家の存続、経済発展に不可欠

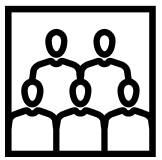
実空間とサイバー空間を一体として人類の活動を支える空間と考える

レジリエンス向上	犯罪対策 （抑止と対応）	システムの保護 データの保護	連携（協働）	研究開発 人材育成
				
国民生活に不可欠な重要インフラが提供するサービスが（サイバー起点で）途切れないようにする。	国民の財産、生命が、（サイバー起点）で脅かされないようにする。	レジリエンスの向上、知財、個人の人権の保護を図る。	政府、企業等がもっている情報を持ち寄り、効果的な対応ができるようにする。	サイバー対応能力を強化、維持できるようにする。

どの国も課題認識、解決手法に大きな違いはない。

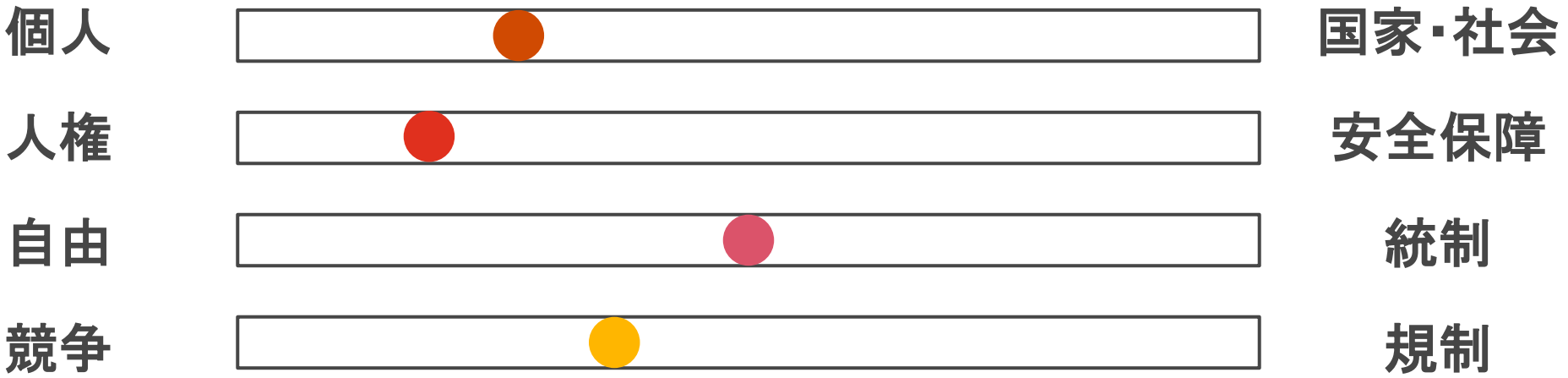
政策内容に大きな違いはないのであれば、違うのは

意志	実行力	実現したい状態
リソースの割り当て： 予算、人材	政策の継続性 政策管理	国民の意図

私たちはどのような社会を目指しているのか？

正義幸福



4

まとめ

ふりかえり

1.世界のサイバーセキュリティ政策概観

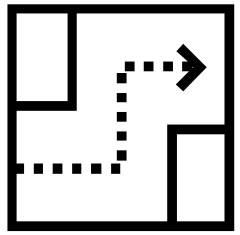
(1) サイバーセキュリティ政策の歴史
(2) サイバーセキュリティ政策の位置付け

2.各国のサイバーセキュリティ政策

(1) 米国のサイバーセキュリティ政策
(2) 英国のサイバーセキュリティ政策
(3) 欧州のサイバーセキュリティ政策
(4) 中国のサイバーセキュリティ政策
(5) 日本のサイバーセキュリティ政策

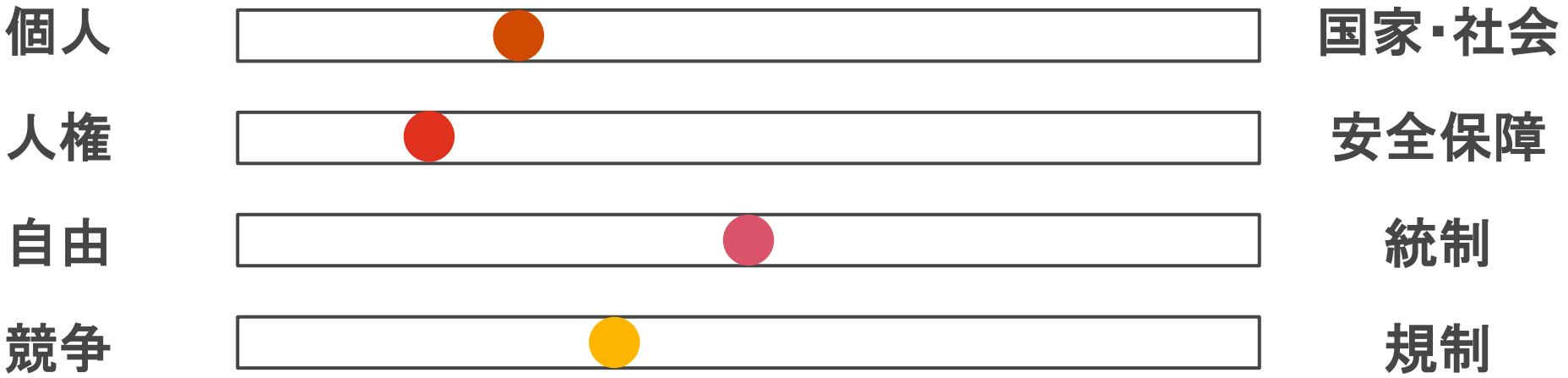
3.各国のサイバーセキュリティ政策を眺めてみて…

4.まとめ



私たちはどのような社会を目指しているのか？

正義幸福



Thank you

www.pwc.com/jp