

サイバーセキュリティにおける戦略的関与
国家サイバーセキュリティ戦略策定ガイド
第三版 2025 年

一部の権利を留保する

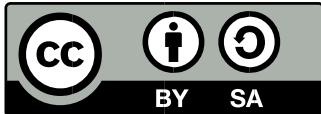
ISBN 978-92-61-42081-9 (PDF 英語版)

© 2025 国際電気通信連合 (ITU) 及び世界銀行 (WB)。

本ガイドは、政府間組織、国際機関、民間セクター、学術界、市民社会からなる 37 名の寄稿者によって作成された。参加組織は以下の通りである：

アクセンチュア、アフリカ連合 (AU)、アラブ連盟、アクソソ・パートナーズ・グループ、英連邦電気通信機構 (CTO)、欧州評議会 (CoE)、サイバー犯罪研究所 (CRI)、南部アフリカサイバーセキュリティ能力センター (C3SA)、デロイト、ディプロ財団 (Diplo)、欧州復興開発銀行 (EBRD)、e ガバナンス・アカデミー (eGA)、欧州連合サイバーネット (EU CyberNet)、エクスペリレ戦略・アドバイザー、インシデント対応・セキュリティチームフォーラム (FIRST)、ジュネーブ安全保障分野ガバナンスセンター (DCAF)、グローバルサイバーセキュリティ能力センター (GCSCC)、グローバルサイバー専門知識フォーラム (GFCE)、グローバル・パートナーズ・デジタル (GPD)、Hathaway Global Strategies LLC、米州開発銀行 (IADB)、国際刑事警察機構 (INTERPOL)、国際通貨基金 (IMF)、国際電気通信連合 (ITU)、KPMG、マイクロソフト、NATO サイバー防衛協力センター (CCDCOE)、NRD サイバーセキュリティ、米州機構 (OAS)、国連開発計画 (UNDP)、国連地域間犯罪司法研究所 (UNICRI)、国連軍縮研究所 (UNIDIR)、国連テロ対策室 (UNOCT)、国連軍縮局 (UNODA)、国連薬物犯罪事務所 (UNODC)、国連大学 (UNU)、世界銀行 (WB)、世界経済フォーラム (WEF)、欧州連合サイバーセキュリティ機関 (ENISA) は、オブザーバーとして本ガイドの作成に貢献した。上記のすべての事業体は、以下「貢献者」と総称する。

権利と許可



本著作物は、特に明記されていない限り、クリエイティブ・コモンズ表示-非営利 3.0 IGO ライセンス (<https://creativecommons.org/licenses/by-nc/3.0/igo/deed.en>) の下で利用可能である。本ライセンスに含まれない本著作物の利用については、ITU (cybersecurity@itu.int) に許可を求めること。

本ライセンスの範囲および条件において、非営利目的で著作物を複製、再配布、改変することができる。ただし、下記に示す通り適切に引用することが条件である。本著作物のいかなる利用においても、国際電気通信連合、世界銀行、または寄稿者のいずれかが特定の組織、製品、サービスを推奨していることを示唆してはならない。国際電気通信連合、世界銀行、または寄稿者の名称やロゴを無断で使用することは認められない。本作品の翻訳を作成する場合、推奨される引用方法に加え、以下の免責事項を追加すること：「本翻訳は国際電気通信連合、世界銀行、または寄稿者によって作成されたものではなく、翻訳の内容や正確性について責任を負わない。英語版原本が拘束力のある真正な版である」。本著作物の翻案を作成する場合、帰属表示とともに以下の免責事項を追加すること：「これは国際電気通信連合、世界銀行及び寄稿者による原著作物の翻案である。翻案に表明された見解及び意見は、翻案の作成者（複数可）の単独の責任によるものであり、国際電気通信連合、世界銀行及びいかなる寄稿者もこれを支持するものではない。」本ライセンスに基づく紛争に関する調停は、世界知的所有権機関 (<http://www.wipo.int/amc/en/mediation/rules>) の調停規則に従って行われる。

サードパーティの資料。本著作物に含まれるサードパーティに帰属する資料（表、図、画像など）を再利用する場合、その再利用に許可が必要か否かの判断及び著作権者からの許可取得は利用者の責任である。著作物内のサードパーティが所有する構成要素の権利侵害に起因する請求リスクは、利用者自身が単独で負う。

出典明記 - 本著作物は以下の通り引用すること：国際電気通信連合 (ITU)、世界銀行、他、2025 年。『国家サイバーセキュリティ戦略策定ガイド 第 3 版 - サイバーセキュリティにおける戦略的関与』。クリエイティブ・コモンズ表示-非営利 3.0 IGO ライセンス (CC BY-NC 3.0 IGO)。

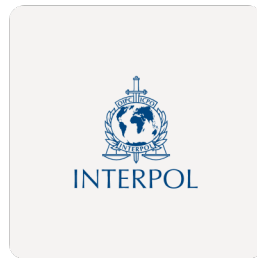
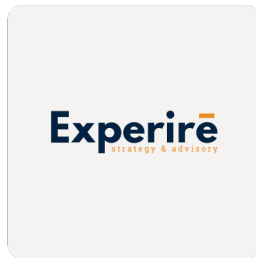
免責事項

本出版物における名称の使用及び資料の提示は、国際電気通信連合、世界銀行、または寄稿者のいずれかが、いかなる国、地域、都市、区域、またはその当局の法的地位、あるいはその国境や境界線の画定に関して、いかなる見解も表明するものではない。

本出版物に記載された見解や意見は著者のものであり、国際電気通信連合、世界銀行、その理事会、またはそれらが代表する政府、あるいは寄稿者の見解を必ずしも反映するものではない。特定の企業、製品、サービスに言及しても、それらが言及されていない類似の性質を持つ他のものより推奨または支持されていることを意味しない。誤りや脱落を除き、専有製品の名称は頭文字を大文字で区別する。

国際電気通信連合、世界銀行及び寄稿者は、本出版物に含まれる情報の検証に合理的な注意を払った。しかしながら、掲載資料は明示的・黙示的を問わず、いかなる保証もなく配布される。資料の解釈及び使用に関する責任は読者にある。国際電気通信連合、世界銀行及び寄稿者は、いかなる場合においても、本資料の使用に起因する損害について責任を負わない。

寄稿者





World
Economic
Forum

監視者



共同まえがき

技術と接続性は、包括的かつ持続可能な開発を実現する強力な推進力である。しかし技術の発展は、持続的かつ進化するサイバーセキュリティ上の課題をもたらす。経験が示すように、基盤となるインフラとサービスが安全でレジリエンスがあり信頼性のあるものでない限り、デジタル化の潜在能力を十分に引き出すことはできない。

政府がサイバーセキュリティリスクに対処しつつデジタル変革を推進する上で最も重要な措置の一つは、資源配分の指針となり、優先順位を設定し、能力構築を促す長期的な戦略計画への投資である。サイバーセキュリティは、各国のより広範なビジョンに統合され、実施、監視、評価の反復サイクルを通じて、戦略的かつ体系的に取り組みられるべきである。この目的のために、多くの国々は、国家サイバーセキュリティ戦略の策定と継続的な改訂を通じて貴重な経験を蓄積してきた。この蓄積された知見は、経験や資源が限られている国々が、この絶えず進化する領域をナビゲートするための指針となる結論を導き出し、提言を策定するための強固な基盤を提供する。

2018 年、国家指導者や政策立案者が国家サイバーセキュリティ戦略を策定するために必要な分析的・概念的ツールを提供するため、寄稿者グループが『国家サイバーセキュリティ戦略策定ガイド』（以下「ガイド」）を共同執筆した。初版が好評を得たことを受け、より広範な連合が結成され、ガイドを更新して 2021 年に第 2 版を出版した。

ガイドの両版は、世界的に国家サイバーセキュリティ戦略の採用が大幅に増加した時期と一致している。2018 年には 76 カ国しか正式な戦略を採用していなかったが、2021 年までにその数は約 127 カ国に増加した。現在では 136 カ国が国家サイバーセキュリティ戦略を策定しており、多くの国が第二版、あるいは第三版の策定段階にある。この過程を通じて、本ガイドは広く認知されたリソース、権威ある参考資料、そして国家指導者や政策立案者向けの青写真となった。

この第 3 版は、国家のサイバーセキュリティ態勢を保護するための実践的措置に焦点を絞り、新興技術、接続デバイスの普及、複雑なサプライチェーンや脅威に起因する最新のリスクに対処しつつ、ますます動的な環境下でレジリエンスを強化する実行可能な保護策を提供する。実施ロードマップ、測定、継続的改善、そして国境を越えた協力に一層重点を置いている。本ガイドの目的は、適切な法的・運用枠組みに基づく国家サイバーセキュリティ戦略・政策の策定、実施、改訂において、戦略的思考を促し国家指導者や政策立案者を支援することにある。この新版が、サイバーセキュリティ責任を有する全ての関係者にとって有用なツールとなることを確信している。

前版と同様に、本ガイドは国家サイバーセキュリティ戦略・政策・サイバー能力構築分野で活動する組織を結集した、協力的かつ包括的なマルチステークホルダーによる独自の取り組みの成果である。2021 年の第 2 版には 20 団体が寄与したが、今回の第 3 版では参加団体がほぼ倍増し、官民セクター、学術界、市民社会から 38 団体が知見と経験を共有した。本版は彼らの集積的専門知識を基に、補完的な出版物や追加リソースを参照している。

本プロジェクトを効果的なマルチステークホルダー協働の具体例とした、関係する貢献者たちの貴重な支援と献身に心からの感謝を表明する。継続的な連携を奨励するとともに、政府、地域・国際団体、法執行機関、学術界、民間セクター、市民社会、国連事業体との関与を深め、実施を加速し、サイバーセキュリティ、サイバー能力構築、サイバーレジリエンスに関する戦略的対話を促進することを期待する。

共同署名者：

ホルガー・ツヴィングマン

セキュリティ変革担当副部長

テクノロジー戦略・アドバイザリー部門 サイバー責任者

アクセンチュア IX EMEA

アルバロ・ネイラ氏

アクソン・パートナーズ・グループ パートナー

バーナデット・ルイス氏

コモンウェルス事務局長

電気通信機関

ヴァージル・スピドン氏

欧州評議会サイバー犯罪対策プログラム運営責任者

ウオレス・チゴナ教授

南アフリカ・アフリカサイバーセキュリティ能力センター所長

アフリカサイバーセキュリティ能力センター所長、南アフリカ共和国ケープタウン大学

ヨヴァン・クルバリヤ博士

ディプロ財団 事務局長

ハネス・アストク氏

e ガバナンス・アカデミー管理委員会委員長

リーナ・アレンク氏

EU サイバーネット プロジェクトディレクター

ロイ・ヤロム氏

副部長、サイバーセキュリティ政策専門家、
欧州復興開発銀行（EBRD）デジタルハブ

アレックス・オルタルダ氏

エクスペリエンス創業者兼代表取締役

戦略・アドバイザー

クリス・ギブソン氏

エグゼクティブディレクター、FIRST

ナタリー・シュアール大使

ジュネーブ安全保障分野ガバナンスセンター（DCAF）所長

サディ・クリス教授

グローバル・サイバーセキュリティ能力センター所長

デイビッド・ヴァン・デュレン氏

グローバル・サイバー専門知識フォーラム（GFCE）事務局長
（GFCE）事務局

リー・カスパー氏

グローバル・パートナーズ・デジタル事務局長

メリッサ・ハサウェイ氏

ハサウェイ・グローバル・ストラテジーズ社 社長

ポーラ・アコスタ氏

州機構能力ディビジョン長

IADB

トビアス・エイドリアン氏

IMF 金融・資本市場局長兼金融顧問

コスマス・ラキソン・ザヴァザヴァ博士

通信開発局（BDT）局長

開発局（BDT）局長、国際電気通信連合

サイリル・グート氏

シリル・グート氏

警察サービス担当代理事務局長、インターポール

カレド・ワリ氏

全権公使、情報通信技術部長、

アラブ連盟

カジャ・チグリッチ氏

シニアディレクター、サイバーセキュリティ政策・外交担当、
顧客セキュリティと信頼部門、マイクロソフト

トニス・サー氏

NATO サイバー防衛協力センター所長

ヴィリウス・ベネティス博士

NRD サイバーセキュリティ担当ディレクター

ギジェルモ・モンカヨ氏

米州機構（OAS）米州テロ対策委員会（CICTE）担当副
事務局長。

マウロ・ミエディコ氏

国連テロ対策センター所長

テロ対策センター所長

ロバート・オップ氏

国連開発計画（UNDP）最高デジタル責任者

ロビン・ガイ博士

国連軍縮研究所所長

レイフ・ヴィラドセン氏

国連地域間犯罪・司法研究所 代理所長

犯罪・司法研究所

黄景波博士

マカオ国連大学研究所所長

中満泉氏

国連軍縮局次長兼軍縮担当上級代表者

ブリジット・シュトロベール＝ショー氏

国連薬物犯罪事務所（UNODC）条約ディビジョン部長代理

クリスティン・ジェンウェイ・チャン氏

世界銀行 デジタル変革グローバルディレクター

タル・ゴールドスタイン氏

戦略・成長部門責任者、サイバーセキュリティセンター

サイバーセキュリティセンター

目次

1 文書の概要	11
1.1 目的	11
1.2 適用範囲	11
1.3 本ガイドの全体構成と活用方法	11
1.4 対象読者	12
2 序論	13
2.1 サイバーセキュリティとは何か	13
2.2 国家サイバーセキュリティ戦略とその策定プロセスの利点	13
3 国家サイバーセキュリティ戦略のライフサイクル	15
3.1 フェーズ I - 開始	15
3.2 フェーズ II - 現状把握と分析	19
3.3 フェーズ III - 持続可能な資金調達と資源計画	20
3.4 フェーズ IV - 国家サイバーセキュリティ戦略の策定	22
3.5 フェーズ V - 実施	23
3.6 フェーズ VI - モニタリングと評価	24
4 包括的原則	27
4.1 ビジョン	27
4.2 包括的アプローチと国別優先事項	27
4.3 包括性	28
4.4 経済的・社会的繁栄	28
4.5 基本的人権	28
4.6 リスクマネジメントとレジリエンス	28
4.7 適切な政策手段の組み合わせ	29
4.8 明確なリーダーシップ、役割分担、資源配分	29
4.9 信頼環境	29
4.10 技術的先見性と適応性	29
5 国家サイバーセキュリティ戦略の優良実践	30
5.1 重点分野 1 - ガバナンス	31
5.2 重点分野 2 - 重要インフラ、重要情報インフラ、および重要サービス	32
5.3 重点分野 3 - 国家サイバーセキュリティにおけるリスクマネジメント	35
5.4 重点分野 4 - インシデント対応	36
5.5 重点分野 5 - 能力・体制構築と意識向上	38
5.6 重点分野 6 - 立法と規制	41
5.7 重点分野 7 - 国際協力	43
6 参考資料	45
7 略語一覧	46

序文

国家サイバーセキュリティ戦略策定ガイドは、成功するサイバーセキュリティ戦略の構成要素について最も包括的な概要の一つである。これは、ユニークで協力的かつ公平なマルチステークホルダーの取り組みの結果である。

寄稿者たちは、サイバー能力構築に関する国際社会全体の協力と調整を強化する必要性を認識して集まった。この取り組みの目的は、国家指導者や政策立案者が、国家サイバーセキュリティ戦略（NCS）という形でサイバーセキュリティリスクに対する防御的かつ積極的な対応策を策定し、サイバーセキュリティ、サイバー準備態勢、対応、レジリエンスについて戦略的に考えることを支援すると同時に、デジタル技術の利用における信頼と安全を構築することにある。

本ガイドは合意形成を通じた合意達成を目指す反復的アプローチにより作成された。既存の権威ある資料に基づき、各国の関係者がそれらを活用することを促進することを目的とする。可能な限り、本ガイドの各章作成に用いた関連資料及びツールは参考資料セクション（www.ncsguide.org で閲覧可能）に記載し、それらの広範な利用を促す。

サイバーセキュリティは、現代経済における社会経済目標の達成を支える基盤的要素である。この『国家サイバーセキュリティ戦略策定ガイド』第 3 版が、国家指導者、政策立案者、立法者、サイバーセキュリティ責任を有する規制当局など、この種の公式文書の策定、実施、改訂に関わる全ての関係者にとって有用なツールであり続けることを期待する。さらに、ここで紹介される概念は地域レベルや自治体レベルでも適用可能であり、産業向けに適応させたり学術研究に活用したりすることもできるため、より広範な適用性が期待される。

読者への更新に関する注記

『国家サイバーセキュリティ戦略（NCS）策定ガイド』第 3 版は、2021 年に発行された第 2 版を更新・改良・拡充したものである。その後もサイバーセキュリティのリスク環境、技術、政策実践は進化を続け、複雑さを増している。本版では、政府が国家戦略計画において考慮すべきサイバーセキュリティの主要な進展や新興・破壊的技術を取り込みつつ、旧版との互換性および本ガイドのプロセスと内容の両立というアプローチを維持している。

この新版は実践的な提言と使いやすさに重点を置き、実践が進んだ分野では新たな内容を追加している。ただし、バージョン 3 はバージョン 2 との完全な互換性を維持し、プロセス（ライフサイクル）と内容（包括的原則と重点分野）のバランスをガイドとして保っている。以前の版を採用した国々は、第 3 版を用いて国家サイバーセキュリティ戦略の見直し・更新、あるいは特に資金調達、ガバナンス、重要インフラ・重要情報インフラ・重要サービス（CI/CII/ES）の要件、リスクマネジメント、インシデント対応、立法、国際的関与といった分野における段階的な改善を行うことができる。

主な更新と追加内容は以下の通りである：

- **ライフサイクル資金調達と長期維持**：より詳細な記述により、国家サイバーセキュリティ戦略（NCS）の全ライフサイクル（策定、実施、監視、見直し、更新）にわたる戦略的資源計画と持続可能な資金調達を強調している。これには、国家予算および公共投資サイクルとの整合性、専用資金ラインの活用、既存政府資源の最適化、外部資金調達（例：多国間開発銀行（MDB）、国際金融機関（IFI）、ドナー、技術支援）が含まれる。複数年にわたる維持、将来年度のコストへの配慮、先を見据えた予算予測、そして完全に資金が確保された取り組みが強調されている。資源は、資金、人材、物資の観点から定義されるべきだ。
- **モニタリング、評価、定期的な見直し**：政府は、戦略と行動計画に SMART KPI（具体的、測定可能、達成可能、関連性、期限付き）を組み込み、モニタリングと評価の明確なガバナンスを確立し、定期的な見直し（例：中間チェック、3～5 年ごとの更新）を伴うベースライン指標を定義し、戦略が脅威、技術、国家の優先事項に即した最新性を維持するよう求められる。
- **技術的先見性と適応性（新たな原則）**：この原則は、進化するデジタルリスクを予測し、新興技術（人工知能（AI）、自動化、量子コンピューティング、モノのインターネット（IoT）、5G/6G、分散型台帳技術）に適応するための地平線スキャンニングと政策の機敏性を強調する。先見性を戦略と規制に転換する仕組みも含まれる。
- **ガバナンスと説明責任**：主管機関の役割、政府全体・社会全体の調整、ステークホルダーの関与、諮問メカニズムに関する指針を強化する。政府内部およびセクター横断的な調整、責任と権限の明確な割り当て、行動計画へのガバナンス統合を強調する。

- 重要インフラ、重要情報インフラ、および重要サービス（CI/CII/ES）**：拡大されたガイダンスは、識別、指定、ガバナンス、および事業者に対するリスクベースの要件に対処する。成果重視の基準、段階的な期待値、監視メカニズム、国境を越えた相互依存性やシステム的なサイバーセキュリティリスク（例：広く利用されるソフトウェアプロバイダのインシデントが数千の顧客に混乱をもたらすケース、重要金融機関の障害が金融システム全体を混乱させ広範な経済的影響を及ぼすケース）への配慮が導入されている。
- リスクマネジメント・フレームワーク**：改訂版ガイドは、サイバーセキュリティリスクの評価・管理における国家的なアプローチの重要性を強調する。これには、動的な国家・セクター別アセスメント、重要セクター・サービス・機能・事業者・資産を網羅する継続的に更新される国家リスク登録簿、国際標準に沿った共通手法の採用、リスク知見を政策・投資・危機管理に結びつけるフィードバックループが含まれる。
- インシデント対応とレジリエンス**：今回の改訂版では、国家サイバーセキュリティアーキテクチャにおける国家対応チーム（コンピュータ緊急対応チーム（CERT）、コンピュータセキュリティ・インシデント対応チーム（CSIRT）、コンピュータインシデント対応チーム（CIRT））と、セクター別対応チーム、セキュリティ・オペレーションセンター（SOC）、製品セキュリティインシデントレスポンスチーム（PSIRT）の役割に関するガイダンスを拡充している。また、緊急時対応計画、情報共有メカニズム（ISAC/ISAOを含む）、国内外の演習、深刻度・影響度アセスメントの重要性を強調している。
- 能力・体制・意識**：国家サイバーセキュリティ人材枠組み、教育から職場への移行経路（初等教育から高度プログラム・見習い制度まで）、女性や少数派を含む人材の確保・定着に向けた包括的戦略について、より詳細な指針を示す。本ガイドは、幹部・実務者向け訓練、資格認定、専門キャリアパス、多様な対象層に合わせた全国的な啓発キャンペーンの重要性も強調する。
- 立法と規制**：改訂版ガイドは政策目標を法的・規制的手段に結びつける包括的アプローチを提示する。権限と監督を明確化し、サイバー犯罪及び電子証拠規定に保護措置を組み込み、比例性、人権、適正手続き、データ保護を強調する。法的調和と越境協力も支援する。
- 国際協力**：本版は国内優先事項と外交政策の連携を強化する。国際法・規範策定プロセス、信頼醸成措置（CBM）、標準団体への参加を促進し、公式・非公式ネットワーク（CERT/CSIRT/CIRT コミュニティ、法執行機関ルート、マルチステークホルダープラットフォームを含む）を通じた実務協力を推進する。サイバー外交と国際関与のための能力構築を拡充する。
- 参考資料セクション（www.ncsguide.org で閲覧可能）**：本ガイドのウェブサイトには動的な参考資料セクションを設置し、参照情報の最新化に向けた簡便なアクセスと保守を可能とする。

この改訂版ガイドは、国家指導者、政策立案者、規制当局、業界代表者、市民社会、その他 NCS 構築に関わる関係者向けの実践的参考資料として作成された。マルチステークホルダーの関与の重要性を認識しつつ、本ガイドの一部で政府事業体に重点を置くのは、プロセスの持続可能性において政府事業体のリーダーシップが極めて重要となる点を強調するためである。本ガイドは、各国が進化するリスク、新興技術、国際的な優良実践に沿って、効果的な国家サイバーセキュリティ戦略（NCS）を策定、実施、維持することを支援することを目的とする。

1 文書の概要

1.1 目的

本文書の目的は、国家指導者や政策立案者が国家サイバーセキュリティ戦略（NCS）を策定・実施・改訂する際の指針となり、サイバーセキュリティ、サイバー準備態勢、レジリエンスについて戦略的に考えることを支援することである。

本ガイドは、各国の社会経済的ビジョンと現在の国家サイバーセキュリティ態勢の文脈を設定し、各国の特定の状況、文化的規範、社会的価値観を考慮した戦略の策定または改訂を支援するとともに、安全でレジリエントで、デジタル技術によって力を得て、つながった社会の追求を促す、有用で柔軟かつ使いやすい枠組みを提供することを目的とする。

本ガイドは、この分野で実証された多様な経験を持つ組織によって開発・承認された枠組みを提供し、それらの組織の先行研究を基盤としている点で独自のリソースである。したがって、成功する国家サイバーセキュリティ戦略を構成する要素について、現時点で最も包括的な概要を提供するものだ。

1.2 適用範囲

サイバーセキュリティは、ガバナンス、政策、運用、技術、法的な側面を包含する複雑な課題である。本ガイドは、既存の確立されたモデル、枠組み、参考資料に基づき、これらの領域の多くを扱い、整理し、優先順位を付ける。ガイドはサイバー空間の民間分野の防御に焦点を当て、国家サイバーセキュリティ戦略の策定、開発、実施、改訂において考慮すべき包括的な原則と優良実践を強調する。

この目的のため、本ガイドは国家サイバーセキュリティ戦略のライフサイクル（策定開始、現状把握・分析、策定、実施、見直し）において各国が採用する「プロセス」と、「内容」（すなわち国家サイバーセキュリティ戦略文書に実際に記載される本文）を明確に区別する。本ガイドは、多くの国々が開発を進めているものの、国家の軍隊、防衛機関、情報機関による防御的または攻撃的なサイバーセキュリティ能力の開発といった側面は扱わない。

本ガイドは、(i) 国家サイバーセキュリティ戦略に「何を」含めるべきか、(ii) それを「どのように」構築・実施・見直すかについて論じる。また、国家がサイバー対応態勢を整えるために必要な中核的要素の概要を提供し、政府が国家戦略や行動計画を策定する際に考慮すべき重要な側面を強調する。最後に、本ガイドは国家指導者や政策立案者に対し、既存のアプローチや応用事例に関する包括的かつ高水準な概要を提供するとともに、各国の具体的なサイバーセキュリティ取り組みに資する追加・補完的リソースを掲載したオンライン参照セクションを設けている。

1.3 本ガイドの全体構成と活用方法

本ガイドは主に、国家指導者や政策立案者が国家サイバーセキュリティ戦略を準備・ドラフト・管理するための支援リソースとして構成されている。内容は戦略策定のプロセスと順序に沿って整理されている：

- [第2章 - 序論](#)：本ガイドの主題の概要と関連定義を提供する。
- [第3章 - 戦略策定ライフサイクル](#)：戦略策定の各段階と、その全ライフサイクルにおける管理方法を詳細に説明する。
- [第4章 - 戦略の包括的原則](#)：戦略策定時に考慮すべき横断的かつ基本的な事項を概説する。
- [第5章 - 重点分野と優良実践](#)：戦略策定時に考慮すべき主要要素とテーマを識別する。
- [補足参考資料](#) (www.ncsguide.org でオンライン公開中)：関係者がドラフト作成やレビュー作業の一環として参照できる関連文献を提供するプロバイダ。

特に、[セクション3](#) は国家サイバーセキュリティ戦略の策定プロセス及び関連側面（準備、起草、実施、長期的な持続可能性など）を扱う一方、[セクション4](#) 及び[セクション5](#) は国家サイバーセキュリティ戦略の内容に焦点を当て、文書に盛り込むべき概念や要素を強調している。

1.4 対象読者

本ガイドは、何よりもまず国家サイバーセキュリティ戦略の策定を担当する国家指導者および政策立案者（1）を対象としている。二次的な対象読者には、戦略の策定と実施に関与するその他の官民の利害関係者、例えば責任ある政府職員、規制当局、法執行機関、デジタルサービスプロバイダ、重要インフラの所有者・運営者、市民社会、学术界、研究機構などが含まれる。本ガイドは、サイバーセキュリティ分野で支援を提供する国際開発コミュニティの利害関係者にも有用である可能性がある。

¹ 本ガイドでは「政策立案者」を、NCSの開発、実施、改訂に関わる全ての政府事業体や機能を指す広義の用語として用いる。

2 序論

情報通信技術（ICT）とデジタルサービスは、登場以来、現代のビジネス、重要サービス・インフラ、ソーシャルネットワーク、そして世界経済全体の基盤へと進化してきた。

その結果、各国指導者はデジタル戦略を策定し、インターネット接続性の向上やデジタル技術の利点を活用した経済成長の促進、生産性・効率性の向上、サービス提供能力の強化、ビジネス・情報へのアクセス提供、e ラーニングの実現、労働力スキルの強化、良きガバナンスの推進を目的としたプロジェクトに資金を投入している。各国は、接続性の向上とデジタル経済への参加に伴う機会を無視することはできない。

デジタルインフラへの依存が高まる一方で、技術そのものは本質的に脆弱性を持っている。データ、情報システム、デジタルインフラの機密性、完全性、可用性は、電子詐欺、知的財産や個人を特定できる情報の窃取、サービス妨害、物理的・デジタル資産の損傷や破壊など、急速に進化するサイバーセキュリティリスクによって脅かされている。デジタル技術とインターネットが経済成長と社会開発の触媒として持つ変革力は、重大な岐路に立っている。なぜなら、サイバーセキュリティの脆弱性と弱点の悪用により、市民や国家がこれらの技術の利用に抱く信頼と確信が次第に損なわれているからだ。

技術の潜在能力を完全に実現するためには、各国は国家経済ビジョンと国家安全保障上の優先事項を整合させねばならない。デジタル化インフラとインターネットアプリケーションの普及に伴うセキュリティリスクが、包括的な国家サイバーセキュリティ戦略とレジリエンス計画によって適切に均衡化されない場合、各国は目指す経済成長と国家安全保障目標を達成できなくなる。これに対応し、各国政府はサイバー空間における不正・違法活動から自らを守るため、また被害が発生する前に事前の対応を取るため、攻撃的・防衛的双方の能力を開発している。本稿では特に防衛的かつ予防的な対応、とりわけ国家サイバーセキュリティ戦略の形態に焦点を当てる。

2.1 サイバーセキュリティとは何か

「サイバーセキュリティ」という用語には、国内外でいくつかの定義が存在する。本稿における「サイバーセキュリティ」とは、政府・民間組織・市民の接続インフラ内における資産の可用性、完全性、機密性を防御するために活用可能な、ツール・政策・ガイドライン・リスクマネジメント手法・行動・訓練・ベストプラクティス・保証措置・技術の総体を指す。これらの資産には、接続されたコンピューティングデバイス、要員、インフラ、アプリケーション、デジタルサービス、通信システム、デジタル環境内のデータが含まれる。

2.2 国家サイバーセキュリティ戦略とその策定プロセスの利点

国家サイバーセキュリティ戦略は、各国の目標やサイバーセキュリティの成熟度に応じて、様々な形態をとり、詳細度も異なる。したがって、国家サイバーセキュリティ戦略を構成する要素について、確立された普遍的な定義は存在しない。

この分野の既存研究に基づき、本文書は関係者が国家サイバーセキュリティ戦略を以下のように捉えることを推奨する：

- サイバーセキュリティへの取り組みを導く、国家のビジョン、高次目標、原則、優先事項の表明であること。
- 国家のサイバーセキュリティ強化を担う関係者と、それぞれの役割・責任の概要を示すもの。
- 国家のデジタルインフラの防御を行い、その過程でセキュリティとレジリエンスを高めるために国が実施する手順、プログラム、イニシアチブの説明。

ビジョン、目標、優先事項を事前に設定することで、政府は特定のリスクへの対応や個別インシデントへの対応に終始せず、自国のデジタルエコシステム全体を包括的に捉えたサイバーセキュリティ戦略を構築できる。つまり戦略的な対応が可能となるのだ。国家サイバーセキュリティ戦略の優先事項は国によって異なる。重要インフラの保護に重点を置く国もあれば、知的財産保護、デジタル環境への信頼促進、一般市民のサイバーセキュリティ意識向上、あるいはこれらの目標の組み合わせを優先する国もある。

サイバーセキュリティのように包括的な分野においてリスクを効果的に管理するには、戦略の策定・実施および関連プログラム・イニシアチブに向けた投資と資源の識別・優先順位付けが不可欠である。

国家サイバーセキュリティ戦略は、サイバーセキュリティの優先事項をより広範な ICT 関連目標と整合させる機会も提供する。サイバーセキュリティは現代経済の社会経済的目標達成の中核であり、戦略はそれらをいかに支援するかを反映すべきだ。これは、国のデジタル化や開発アジェンダを実施する既存政策を参照するか、それらにサイバーセキュリティを組み込むことで達成できる。

最後に、国家サイバーセキュリティ戦略の策定プロセスは、政府のビジョンを、その目標達成に資する首尾一貫した実行可能な政策へと転換すべきである。これには、実施すべき手順、プログラム、取り組みだけでなく、それらの取り組みに割り当てられる資源とその活用方法も含まれる。同様に、このプロセスでは、設定された予算とスケジュール内で望ましい成果が達成されることを保証するための測定基準と業績評価指標を識別すべきである。

3 国家サイバーセキュリティ戦略のライフサイクル

本セクションでは、国家サイバーセキュリティ戦略策定の段階について概説する。これには以下が含まれる：

- フェーズ I – 開始
- フェーズ II – 現状把握と分析
- フェーズ III – 持続可能な資金調達と資源計画
- フェーズ IV – 生産
- フェーズ V – 実施
- フェーズ VI – モニタリングと評価

また、戦略策定に関与すべき主要な事業体を紹介し、プロセスに貢献できるその他の関連ステークホルダーを強調する。

最終的に、このセクションは、読者が国家サイバーセキュリティ戦略のドラフトまたは更新のために取るべき手順、およびその実施のための可能なメカニズムを理解することを目的としている。これらは、各国の特定のニーズと要件に合わせて調整され、包括的な原則（[セクション 4](#)）と優良実践の要素（[セクション 5](#)）を統合したものである。

図 1 に示すこのライフサイクルは、本文書の利用者が国家レベルでのサイバーセキュリティとサイバーレジリエンスに関する戦略的思考に焦点を当てるための指針となる。[セクション 2](#) で説明したように、この戦略的思考は、サイバーセキュリティを効果的な国家ガバナンスと持続可能な開発の基盤と認識し、国家安全保障、経済的繁栄、デジタルレジリエンスにわたる国の優先事項を考慮し、それらと整合させるべきである。

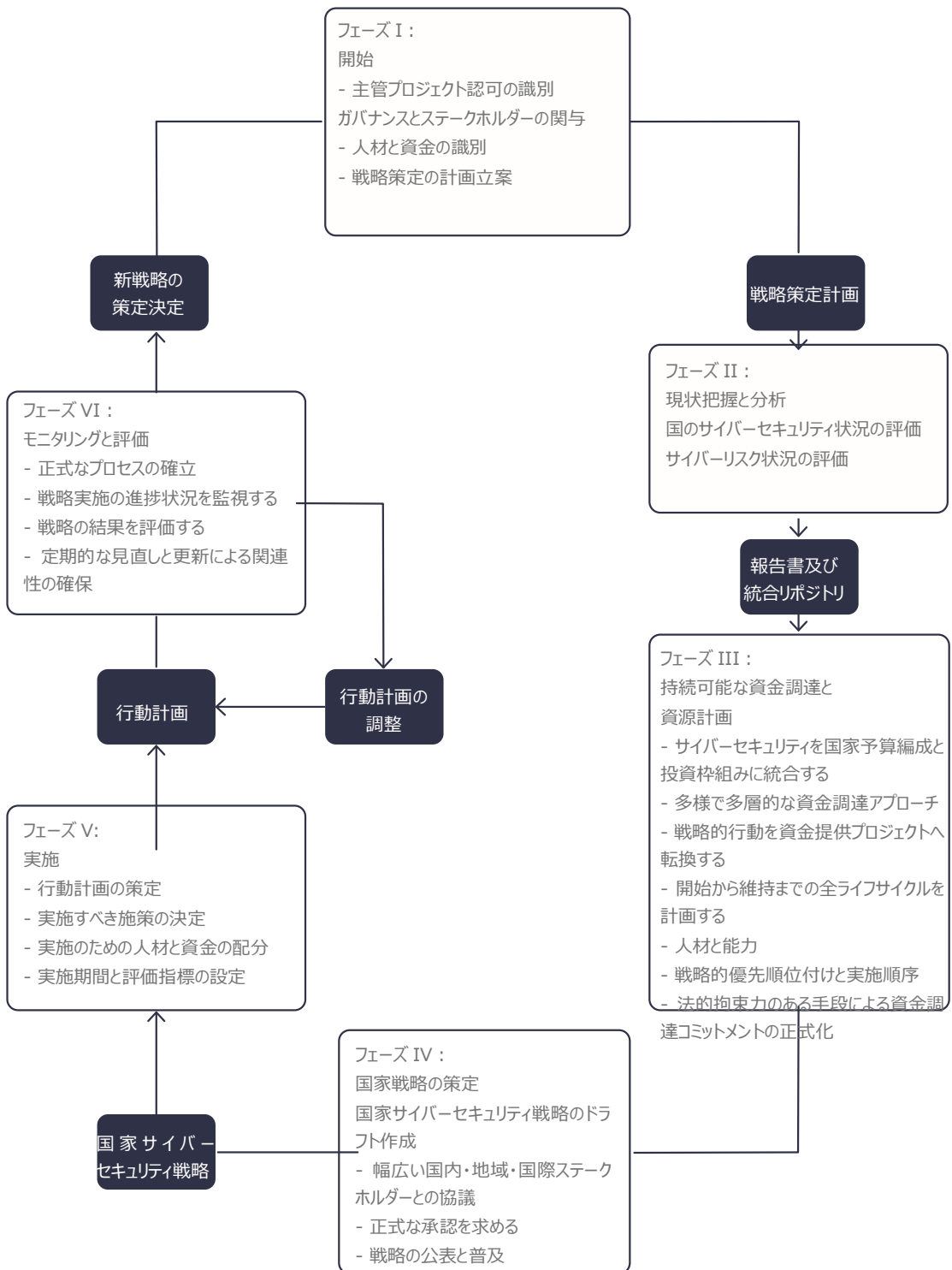
3.1 フェーズ I – 開始

開始フェーズは効果的な戦略策定の基盤を提供する。このフェーズでは、主要政府事業体の関係ステークホルダーが明確な役割と責任を確立し、プロジェクト管理プロセスとタイムラインを定義し、戦略策定に関与すべき追加ステークホルダーを特定すべきである。また、文書が国家全体の戦略となるか、主に政府事業体と国家重要資産に焦点を当てるかを決定すべきである。この段階の成果は戦略策定計画であり、国家ガバナンスプロセスで必要とされる場合には、国の行政機関による承認が必要となる場合がある。

3.1.1 主管プロジェクト機関の識別

明確なリーダーシップ、役割分担、資源配分（[セクション 4.8](#)）の原則に沿い、戦略策定は単一の有能な機関が調整すべきである。行政機関は、省庁、庁、局など既存または新設の公的事业体を戦略策定の主導機関として任命すべきである。本セクションで主導プロジェクト機関と呼ぶこの事業体は、策定プロセスの主導・調整に責任と説明責任を負う個人またはチームを任命すべきである。主導プロジェクト機関の指定は、当該事業体が新たな特定プロジェクトを監督しなければならないことを意味しない。既存の取り組みを有する省庁・機関・団体であっても、あるいは単に政治的権限を有するものであっても、戦略策定の調整を正式に委任されていれば同等に適任である。

図 1 - 国家サイバーセキュリティ戦略のライフサイクル



フェーズ I :
開始

- 主管プロジェクト認可の識別
ガバナンスとステークホルダーの関与
- 人材と資金の識別
- 戦略策定の計画立案

**新戦略の
策定決定**

戦略策定計画

フェーズ VI :
モニタリングと評価

- 正式なプロセスの確立
- 戦略実施の進捗状況を監視する
- 戦略の結果を評価する
- 定期的な見直しと更新による関連性の確保

フェーズ II :
現状把握と分析

- 国のサイバーセキュリティ状況の評価
- サイバーリスク状況の評価

**報告書及び
統合リポジトリ**

行動計画

**行動計画の
調整**

フェーズ V :
実施

- 行動計画の策定
- 実施すべき施策の決定
- 実施のための人材と資金の配分
- 実施期間と評価指標の設定

フェーズ III :
持続可能な資金調達と
資源計画

- サイバーセキュリティを国家予算編成と投資枠組みに統合する
- 多様で多層的な資金調達アプローチ
- 戦略的行動を資金提供プロジェクトへ転換する
- 開始から維持までの全ライフサイクルを計画する
- 人材と能力
- 戦略的優先順位付けと実施順序
- 法的拘束力のある手段による資金調達コミットメントの正式化

**国家サイバー
セキュリティ戦略**

フェーズ IV :
国家戦略の策定
国家サイバーセキュリティ戦略のドラフト作成

- 幅広い国内・地域・国際ステークホルダーとの協議
- 正式な承認を求める
- 戦略の公表と普及

可能な限り、主導プロジェクト機関は実施責任事業体とは別個に設置され、全てのステークホルダーと公平に連携する権限を持つべきだ。その任務遂行に必要なツール、資源、権限（例：省庁間会議の招集権限、政府全体への情報要求権限）と、それらを効果的に活用する能力が与えられるべきだ。

3.1.2 ガバナンスとステークホルダーの関与

戦略策定における主導プロジェクト機関を支援するため、執行部は戦略的方向性と品質保証のための運営委員会、官民・市民社会から構成される専門家諮問グループ、正式な協議チャネルなど、一つ以上のガバナンス機構を確立すべきである。これにより戦略ライフサイクル全体を通じた透明性と包括性を確保する。

これらのメカニズムの権限、構成、運営手順は、機密情報を扱う可能性のある参加者に対する適切な認可とともに、当初から明確に定義されるべきである。また、メンバー構成は、割り当てられた責任と、必要に応じて上級性を反映したものであるべきである。

並行して、主導プロジェクト当局は初期の利害関係者を識別し、その役割を明確化し、協力に関する期待を設定すべきである。優先的に考慮すべきは、(1) 正式な政策決定権限を持つ事業体（例：省庁、部門、機関）、(2) 戦略的に重要な主体（例：重要インフラの所有者・運営者）、(3) プロセスに知見を提供できる実証済みの専門性を持つ組織・個人（例：技術・デジタルサービスプロバイダ、専門アドバイザー、学術専門家）である。

作業が進むにつれ、主導プロジェクト当局は包括性の原則（[セクション 4.3](#)）に沿って、政府、民間セクター、市民社会から生じる新たなニーズや知見を取り込むため、関連するステークホルダーのリストを見直し、拡大することができる。

ステークホルダー間の効果的な協力を可能にするため、主導プロジェクト当局は、定期的な省庁間会議（対面またはオンライン）、学術界や市民社会との構造化された関与、NCS ライフサイクル全体にわたるマイルストーンレビュー、定期的な進捗報告などを検討すべきである。

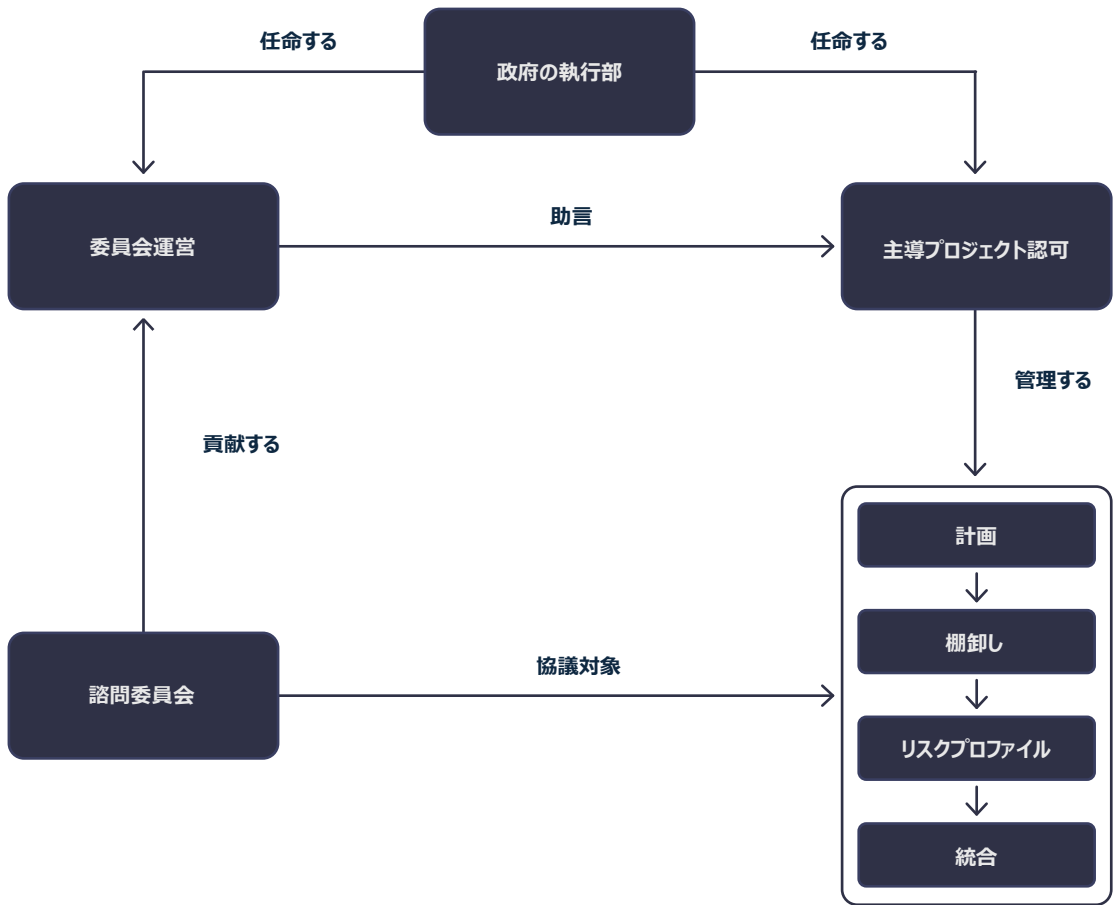
必要に応じて、国際機関、開発機関、地域団体、民間事業体などの国際パートナーを、専門家交流や集中作業会合を通じて関与させ、NCS に関する追加支援や専門的知見を提供させることができる。

3.1.3 人材及び財政資源の識別

主導プロジェクト当局は、戦略策定に必要な人的・財政的資源を識別し、その調達源を決定し、調達・配分方法を概説すべきである。例えば、必要な専門知識は政府機関、政府間組織、民間セクター、市民社会、学術界などから求めることができる。

資金調達には、特定の NCS 目標に紐づく専用の国家予算枠、既存政府資源の再配分または最適化、新たな予算認可、外部投資（例：国際機関、多国間開発銀行（MDB）、国際機関）など、複数の財源を組み合わせるべきである。

図 2 - ステークホルダーの役割と責任



金融機関（IFIs）、二国間ドナー、慈善活動や技術支援プログラム）。外部関係者は、特にサイバー能力構築、インフラ開発、法制度改革、サイバーセキュリティ人材育成において、NCS 目標に沿った対象を絞った投資を提供することがある。

各国の慣行に応じて、このステップは戦略策定のための資源確保のみに焦点を当てる場合（実施予算は後述のセクション 3.3 で扱う）もあれば、両者を統合する場合もある。いずれにせよ、戦略的計画と持続可能な資源確保は、NCS が計画された期間内にドラフトされ、短期的には実行可能であり、長期的には持続可能であることを保証するのに役立つ。

3.1.4 戦略策定の計画立案

開始段階の最終ステップとして、主導プロジェクト機関は戦略策定計画を準備すべきだ。ドラフト作成後、国内のガバナンスプロセスに従い、関連ステークホルダー（例：運営委員会）に審査を依頼し、執行機関に承認を求めべきだ。

策定計画を作成する際、主導プロジェクト機関は、NCS が法律か政策のいずれの形態をとるかを検討すべきである。これは、必要な正式なプロセスや採択までの期間に影響を与える可能性があるからである。

戦略策定計画では、主要な手順と活動、主要な利害関係者、タイムライン、必要なリソース（人的・財政的）を明確に識別すべきである。また、関連する利害関係者がいつ、どのように参加し、意見やフィードバックを提供することが期待されているかを明記すべきである。

図 2 は、ステークホルダーと委員会間の相互作用と役割分担の例を示している。

3.2 フェーズ II – 現状把握と分析

本フェーズの目的は、国家サイバーセキュリティの現状と既存・新興リスクの評価に必要な情報を収集し、戦略のドラフト・策定に資することである。成果物として、国家サイバーセキュリティの現状、リスク状況、喫緊の課題に関する概要をまとめた報告書を作成し、主要な意思決定者に提出する。

戦略の作成（または更新）を開始する前に、主導プロジェクト機関は現状把握の結果を慎重に分析・評価し、サイバーセキュリティ能力のギャップを識別するとともに、それらに対処するための選択肢を提示すべきである。分析では、既存の政策・規制・運用環境が国家のニーズをどの程度満たしているかを評価し、不足点を明らかにすべきである。また、具体的な課題（例：教育・人材の不足）を識別し、戦略で達成すべき成果と、その達成のために利用可能かつ必要な手段を定義すべきである。

3.2.1 国家サイバーセキュリティ状況の評価

戦略が効果を発揮するためには、国のサイバーセキュリティ態勢を反映していなければならない。したがって、政府、民間部門、市民社会のステークホルダーと連携し、既存の強みと弱みの分析を実施すべきである。このステップは、包括的アプローチと個別対応型優先事項の原則（[セクション 4.2](#)）に従うものである。

主導プロジェクト機関は、優れた実践を活用し重複を削減するため、国家サイバーセキュリティにおける関係者の役割と責任を明確にすべきである。

この取り組みの一環として、主導プロジェクト機関は、社会と経済の適切な機能に不可欠な資産とサービスを識別し、サイバーセキュリティに関連する既存の国内法、規制、政策、プログラム、能力をマッピングし、官民パートナーシップなどのソフト規制メカニズムをカタログ化し、サイバーセキュリティ課題に対応する既存の能力（例：国家およびセクター別の CERT/CSIRT/CIRT および SOC）を把握すべきである。規制当局やデータ保護機関など、サイバーセキュリティの責任を有する関連団体の役割と責任もマッピングすべきである。

マッピングすべき主要要素

- **ステークホルダー**
- **役割と責任**
- **重要資産・重要サービス**
- **既存の法令・規制・政策等**
- **ソフト規制メカニズムインシデント対応能力**
- **国内及び国際サイバーセキュリティイニシアチブ**
- **多国間及び二国間協定**
- **民間セクタープロジェクト**
- **教育及び研究開発プログラム**
- **国家デジタル発展指標**
- **脅威情報**
- **実施中または計画中の技術支援と投資**

さらに、国家のサイバーセキュリティ態勢を把握するためのデータも収集すべきである。具体的には、既存の国家サイバーセキュリティプログラムや国際的取り組み、多国間・二国間協定、民間セクタープロジェクト、デジタル・サイバーセキュリティ教育および技能開発プログラム、サイバー研究開発イニシアチブ、インターネット普及率・接続性・デジタル化に関する指標、新興脅威や広範なサイバーセキュリティ動向に関する知見などである。民間セクター、研究機構、その他のステークホルダーグループからの関連情報もこの分析に含めるべきである。

開発途上国においては、技術支援と投資を調整するため、開発パートナーとの協力イニシアチブのマッピングが極めて重要である。主導プロジェクト当局は、地域・国際レベルでの関連情報、ならびにセクター固有の戦略やイニシアチブについても検討すべきである。

3.2.2 サイバーリスク環境の評価

現状把握の結果を踏まえ、主導プロジェクト機関は国家のデジタル依存に関連するリスクを評価すべきである。これは、重複や偏った配分を避けつつ、最大のリスク低減機会に向けて活動を優先順位付けし、資源を配分するための基礎となる。

このアセスメントは、まず国内のデジタル資産（公的・民間）を識別し、それらの相互依存関係、脆弱性、脅威を明らかにするとともに、サイバーインシデントや混乱の発生確率と潜在的な影響を推定することから始めるべきである。

この取り組みは、リスクマネジメントとレジリエンスの原則（[セクション 4.6](#)）に沿うものであり、リスクマネジメントが社会経済開発におけるデジタル環境の利点を十分に実現するために重要であることを認識している。

この初期リスクアセスメントは、将来のより具体的なリスクアセスメントの基礎として活用できる（リスクマネジメントとレジリエンスの原則、およびリスクアセスメントの実施方法に関する詳細は、[セクション 4.6](#)、[5.2](#)、[5.3](#)を参照）。

3.3 フェーズ III – 持続可能な資金調達と資源計画

効果的なサイバーセキュリティには、政策や政治的意志だけでなく、資金調達においても持続的な取り組みが必要である。策定から実施、評価、更新に至る戦略ライフサイクルの各段階では、専用で予測可能かつ長期的な資金が求められる。適切かつ継続的な財政支援がなければ、よく設計された戦略でさえ実現されないリスクがある。本セクションでは、戦略の全ライフサイクルを支援するための持続可能な資金の識別、確保、管理に関する主要な考慮事項を概説する。全てのステップは行動計画に盛り込むべきである。

3.3.1 サイバーセキュリティを国家予算・投資枠組みに統合する

戦略の策定と実施は、確立された国家予算編成および公共投資計画プロセスを通じて資源を調達するのが理想的である。サイバーセキュリティは、孤立した一時的な取り組みとして扱うべきではなく、インフラ開発、デジタル接続性、公共サービスの近代化、国家安全保障などの他の戦略的投資と統合・連携された、横断的な国家優先課題として位置付ける必要がある。

サイバーセキュリティ専用の資金枠は、年次予算サイクル、中期支出枠組み、国家開発計画などに適切に反映されるべきだ。効果と費用対効果を最大化するため、政府は戦略と他の優先分野との相乗効果を積極的に追求すべきである。保健、教育、交通、重要インフラ近代化などの主要な国家プログラムには、しばしばデジタル化やサイバーセキュリティの要素が組み込まれている。これらのプログラムに後付けで対応するのではなく、設計段階でサイバーセキュリティ対策を組み込むことで、コスト削減、運用上の整合性強化、国民の信頼と任務のレジリエンス向上を図ることができる。

3.3.2 多様で多層的な資金調達アプローチ

戦略の資金調達には、以下の多様な財源を組み合わせることで活用することが可能であり、またそうすべきである：

- 特定の目標、所管省庁の活動、あるいは国家サイバーセキュリティの役割と責任を担うその他の主要事業体に紐づく、専用の国家予算配分。
- 既存資源の再配分または最適化。特に、サイバーセキュリティの改善によって現行プログラムを強化できる分野において。
- 単一の予算サイクルや政権期間を超える長期計画を必要とする戦略的イニシアチブへの資金提供を可能にする、複数年にわたるコミットメントを認める新たな予算認可や立法措置。
- 外部資金（例：国際機関、MDB/IFI、二国間ドナー、慈善・技術支援プログラム）。これらの主体は、特に能力構築、インフラ開発、法制度改革、機構改革において、戦略目標に沿った対象を絞った資金調達手段を提供し得る。

開発パートナーとの連携及び国家開発協力戦略への本戦略の組み込みにより、対外援助ポートフォリオ内でサイバーセキュリティが適切な注目を受けることが保証される。国家サイバーセキュリティ優先事項と連動した、ドナー及びパートナー関与のための中央調整メカニズムの確立は、重複の回避、吸収能力の向上、資金と戦略的ニーズの整合化に寄与する。

3.3.3 戦略的行動の資金付きプロジェクトへの転換

追加的な考慮事項として、戦略的行動計画を、国内で認められた計画・予算編成手法を用いて正式な公共投資プロジェクトへ転換することが挙げられる。戦略的行動を国の公共投資管理システムと整合させることで、サイバーセキュリティイニシアチブを、明確な目標、指標、タイムライン、責任機関、資源要件を備えた正式なプロジェクトとして構築できる。

政府は、論理的枠組みアプローチ（LFA）、費用便益分析（CBA）、変化の理論（ToC）などの手法を適用し、実現可能性、有効性、国家優先事項との整合性を評価することが推奨される。こうした取り組みを中期支出枠組みなどの国家計画・予算編成サイクルに組み込むことで、サイバーセキュリティ活動が臨時的活動として扱われることなく、持続的かつ説明責任を果たし、より広範な公共政策アジェンダに統合されることが保証される。

3.3.4 開始から維持までの全ライフサイクルにわたる計画

持続可能な資金調達では、新規イニシアチブの立ち上げだけでなく、継続的な運用、保守、更新も考慮しなければならない。戦略的イニシアチブは複数年にわたる場合が多く、特定の政権の任期を超えて継続することもある。したがって予算編成では、ライセンス更新、研修、インフラ維持、人員配置といった継続的支出を含むライフサイクル全体のコストを考慮する必要がある。維持管理計画の不備は深刻な悪影響を及ぼす。例えばセキュリティツールを展開してもライセンス更新や継続的研修を怠れば、脆弱性が生じたりデジタル公共サービスへの信頼が損なわれたりする。同様に、外部資金による一時的な資金で開始されたサイバーセキュリティ施策は、並行する国内の取り組みがなければ持続不可能となる。したがって戦略では以下の点を重視すべきだ：

- 多くの資金不足の取り組みよりも、少数の完全資金調達された取り組みを優先すること；
- 将来を見据えた予算計画に翌年度以降の費用を組み込むこと；
- 開発パートナー、民間セクター、地域イニシアチブとの費用分担や共同資金調達の機会を識別すること；
- 予期せぬ費用や新たなニーズに対応できるよう予算の柔軟性を維持すること。

3.3.5 人材と能力

戦略において重要でありながら、しばしば資金不足に陥りがちな要素が人的資源である。有能で十分な資源を与えられ、定着したサイバーセキュリティ人材なしに戦略の成功はありえない。戦略は人的資源のニーズを一時的な費用ではなく、基本的かつ継続的な経費項目として考慮すべきだ。

政府は省庁やセクターを横断した共通スキルニーズを識別し、効率性を最大化するため、共有の研修パイプライン、キャリアパス、専門能力開発プログラムを構築すべきだ。人材育成への投資は戦略的投資として扱われ、ほぼ全ての他の取り組みの基盤となる推進力である。教育、研修、資格認定における地域・国際パートナーとの共同投資は、規模拡大、持続可能性、成果向上に寄与し得る（スキル開発に関する詳細は[セクション 5.5](#)を参照）。

3.3.6 戦略的優先順位付けと順序付け

資源計画は戦略的な優先順位付けに基づいて策定すべきである。一部の NCS 活動は高コストかつ長期にわたるが、それに見合わないほどの利益をもたらす場合がある。こうした活動は「戦略的投資」と位置付け、それに応じた資金を投入すべきだ。取り組みが成熟するまでに要する期間が長く、支援する目標が多いほど、当初から十分な資金を確保することが重要となる。

利用可能な国家資源やパートナー資源の範囲内で実現可能な取り組みは限られている。したがって政府は、利用可能な資金、政治的勢い、機構の準備状況に基づいて実施順序を慎重に決定し、初期段階で成果を上げ、その後の段階に向けた勢いを構築すべきである。

3.3.7 拘束力のある手段による資金調達コミットメントの正式化

サイバーセキュリティ投資の継続性と持続可能性を確保するため、戦略実施のための資金と責任は、拘束力のある手段（例：行政命令、省庁間協定、閣議決定、法的に制定された予算規定）を通じて正式に定めるべきである。こうした手段は、資源配分の正式な基盤を確立し、機構の責任を明確化し、サイバーセキュリティ資金を裁量的予算配分の変動から防御する。こうした約束を法的に

明文化することは、政治的意志を強化し、省庁間の連携を強化し、長期的な能力開発と戦略的優先事項の実施のための持続可能な基盤を提供する。

結局のところ、持続的かつ予測可能な資金調達、NCS ライフサイクル全体の基盤である。これがなければ、戦略は国家レジリエンスの運用上の推進力ではなく、単なる理想を掲げた文書に終わるリスクがある。サイバーセキュリティを長期的な資源計画に組み込むことで、実施から監視、見直し、更新に至るまでの各段階が、具体的かつ持続的な効果をもたらすことが保証される。

3.4 フェーズ IV – 国家サイバーセキュリティ戦略の策定

この段階の目的は、一連の公開協議や作業部会を通じて、公共部門、民間部門、学術界、市民社会の主要な利害関係者を巻き込み、戦略の文書を作成することである。主導プロジェクト機関が調整するこの広範なステークホルダーグループは、戦略の全体的なビジョンと範囲の定義、高次元の目標設定、現状把握（フェーズ II で詳述）、社会・市民・経済への影響と利用可能な資源（フェーズ III で詳述）に基づく目標の優先順位付けを担当する。この段階では、本ガイドで詳述されているすべての横断的原則（[セクション 4](#)）および優良実践要素（[セクション 5](#)）を考慮すべきである。

3.4.1 国家サイバーセキュリティ戦略（NCS）のドラフト

持続可能な資金調達と資源計画のフェーズが完了したら、主導プロジェクト機関は運営委員会と連携し、国家サイバーセキュリティ戦略（NCS）のドラフトを開始すべきである。このプロセスは主導プロジェクト機関が直接推進することも可能だが、多様な重要な視点を確実に反映させるため、関連する利害関係者を巻き込むことが望ましい。可能であれば、利用可能な資源の範囲内で、特定のトピックに焦点を当てたり戦略の異なるセクションをドラフトしたりするための専門作業部会を設置することができる。これらのグループは開始段階で確立されたプロセスに従い、必要に応じて調整すべきである。

戦略は、国家全体のサイバーセキュリティの方向性を示すべきである。明確なビジョンと範囲を提示し、特定の期間内に達成すべき目標を設定し、社会・経済・インフラへの影響度に基づいて優先順位を付ける必要がある。さらに、可能な行動方針を識別し、実施努力を促進し、これら活動を支えるための必要な資源配分を導くべきである。戦略には、現状把握・分析段階で得られた知見を含めることも可能である。

戦略策定計画の段階と同様に、最終文書では主要関係者の役割と責任を定義する明確なガバナンス枠組み（[セクション 5.1](#)）を提示すべきである。これには、戦略の管理・評価を担当し説明責任を負う事業体、ならびに中央機関や国家サイバーセキュリティ評議会など、戦略の全体的な管理・実施を担当する団体の識別が含まれる。

戦略はまた、国家サイバーセキュリティアーキテクチャを構成する様々な事業体を識別すべきである。これには、サイバーセキュリティ政策・規制の策定、脅威・脆弱性情報の収集、サイバーインシデント対応（例：国家 CERT/CSIRT/CIRT）、準備態勢強化・危機管理を担当する事業体が含まれる。これらの事業体が相互に、また中央機関とどのように連携するかを明確に記述すべきである。

3.4.2 幅広い国内・地域・国際ステークホルダーとの協議

前述の通り、戦略の成功にはステークホルダーの関与が不可欠である。最終文書が共通のビジョンに基づき、他国の戦略との要求事項の不整合や矛盾リスクを最小限に抑えるため、ドラフトは戦略策定プロセスに直接関与しないステークホルダーも含め広く周知すべきである。オンライン協議、妥当性確認ワークショップ、追加作業部会など多様な関与手段を通じて実施可能である。国際機関や地域機関、その他の外部ステークホルダーも、助言や専門知識の提供を通じて役割を果たすことができる。このプロセスから得られたフィードバックやコメントは、最終的な戦略に反映させるべきである。

3.4.3 正式な承認の取得

最終段階として、主導プロジェクト当局は戦略が行政機関によって正式に採択されることを確保すべきだ。この採択プロセスは国によって異なり、立法枠組みに依存する。例えば、議会手続きや政府の高レベル行政文書（政令や決議など）を通じて採択が行われる可能性がある。

さらに、戦略が政府の最高レベルで承認されるだけでなく、このコミットメントが実施段階まで継続されることが不可欠である。関連する事業体や担当者は、政治的資本と資源の両方で支援され、説明責任を果たすべきである。これにより、戦略の公表後も、サイバーセキュリティへの取り組みが長期にわたり強力かつ持続可能なものとなる。

3.4.4 戦略の公表と普及

戦略は公開文書として容易に入手可能であるべきだ。戦略の発表には、理想的には内部・外部向けの普及活動が伴うべきである。戦略の広範な普及は、国民が政府のサイバーセキュリティにおける優先事項と目標を認識することを保証し、国家的な啓発活動を支援する。

戦略に附属書として添付されるか別途公表されるかを問わず、付随する行動計画も、全ての関連ステークホルダーとのさらなる関与と協力の機会を強調すべきである。

3.5 フェーズ V – 実施

戦略の成功には、適切な人的・財政的資源（[セクション 3.3 も参照](#)）に支えられた体系的な実施アプローチが不可欠であり、戦略策定の一環として考慮すべきである。この文脈における適切な人的資源とは、ガバナンス、政策、サイバーセキュリティ、技術、規制問題に関する専門知識を持つ十分なスタッフと専門家の確保を指す。実施段階は、構想された活動を導く行動計画を中心に展開されることが多い。

3.5.1 行動計画の策定

戦略の策定と同様に、その実施も単一の団体や当局の単独責任では成り立たない。むしろ、政府全体の多様な関係者の関与と調整が必要であり、重要インフラの所有者・運営者、市民社会、民間セクターからの追加的な支援も求められる。明確なリーダーシップ、役割分担、資源配分（[セクション 4.8](#)）の原則に沿って策定される行動計画は、効果的な実施のための枠組みを提供する。

行動計画策定のプロセスは、文書そのものとはほぼ同等に重要である。主導プロジェクト機関が調整役となり、関連するステークホルダーを集めて目標と成果について合意し、取り組みを調整し、資源を共有する仕組みとして機能すべきである。

3.5.2 実施すべき取り組みの決定

戦略は政府の目標と、各重点分野で求める成果を定義する。行動計画では、主導プロジェクト機関が関連ステークホルダーと連携し、これらの目標を達成する具体的な施策を特定すべきだ。例としては、サイバーセキュリティ演習の実施、重要インフラ分野のセキュリティ基準設定、インシデント報告枠組みの構築などが挙げられる。

これらの施策の実施に必要なスケジュールと労力は、重要度に応じて優先順位を付け、限られた資源を効果的に活用できるようにすべきだ。このため、フェーズ II（現状把握と分析）の結果、特にサイバーセキュリティリスク状況の評価（[セクション 3.2.2](#)）を優先順位付けの根拠とすべきだ。

3.5.3 実施のための人材・資金資源の配分

取り組みの優先順位付けが完了したら、それらを戦略および／または行動計画に正式に盛り込むべきである。この計画では、各取り組みの責任事業体および説明責任事業体を識別する必要がある。これらの事業体は、割り当てられた各具体的取り組みの実施について説明責任を負い、実施プロセスの一環として他の関連ステークホルダーとの調整を行うことが求められる。

主導プロジェクト機関は、これらの事業体が任務を遂行するための適切な法的または機構的権限を有していることを確認すべきである。また、作業達成に必要な人的・技術的・財政的資源（専門知識、人員配置、資金需要など）を決定するため、これら事業体と連携すべきである。主導プロジェクト機関は、フェーズ III（[セクション 3.3](#)）に沿って必要な資源を特定し確保する支援を行うべきである。

3.5.4 期間設定と指標

行動計画の重要な要素は、行動計画に定められた各施策の実施状況を追跡し進捗を評価するための具体的な指標と主要業績評価指標（KPI）を策定することである（[セクション 3.6 も参照](#)）。これには、完了した施策の割合、これまでの予算執行状況、実施が遅れている事業体の特定などが含まれる。各施策の実施に関する具体的なタイムラインも明確に設定すべきである。

主導プロジェクト認可は、実施事業体と連携してこれらの指標と KPI を開発すべきである。実施事業体はまた、完了時および完了後の効率性と有効性の評価を支援するため、より詳細な指標セットを維持すべきである。

3.6 フェーズ VI – モニタリングと評価






戦略の策定と実施は継続的なプロセスである。管轄当局は戦略を監視・評価する正式なプロセスを策定すべきだ。監視段階では、政府は戦略が行動計画に沿って実施されていることを確認する。評価段階では、政府と国家管轄当局は、変化するリスク環境を踏まえて戦略が依然として適切か、政府目標を反映し続けているか、必要な調整事項を評価すべきだ。

3.6.1 正式なプロセスの確立

戦略実施の効果的な監視・評価を確保するため、政府は進捗の監視と有効性の評価を担当する独立した事業体を識別すべきである。この事業体は、策定・開始段階において、戦略とその行動計画に対する適切な監視・評価指標の定義に理想的には関与すべきである。

行動計画のパフォーマンスと実行状況の監視・測定は、国が戦略のために確立するガバナンス機構に組み込まれるべきである。実施進捗（すなわち、何が機能し、何が機能していないか）の継続的なアセスメントは、調整の参考となる。優れたガバナンス機構は、の成功的な実行に対する説明責任と責任を明確に区分すべきである。短期、中期、長期の目標ごとに指標や KPI を設定することは、ガバナンスと管理構造の強化に役立つ。

主要業績評価指標（KPI）や測定基準は SMART であるべきだ。

	具体的である：	改善すべき明確な領域をターゲットとし、期待される変化に焦点を当てる。
	測定可能である：	進捗を数値化するか、明確な指標を提示する。
	達成可能である：	利用可能な資源で現実的に達成可能な結果を明示せよ。
	関連性があること：	進捗の重要な指標に焦点を当て、責任者を明確にすること。
	時間的制約をおくこと：	結果がいつまでに期待されるかを明記せよ。

KPI は常に特定の目標に合わせて調整し、具体的な取り組みと結びつけることで是正措置を容易にする。KPI が詳細になればなるほど、信頼性のある測定は困難になるため、バランスが求められる。効果的なモニタリングと改善領域の特定には、ベースライン指標が不可欠である。予算配分も、意図する影響の野心度と複雑性を反映すべきだ。

3.6.2 戦略実施の進捗状況のモニタリング

戦略の実施進捗を監視する事業体は、戦略の全ライフサイクルにわたって合意されたタイムラインに従ってこれを行うべきだ。監視成果物（例：報告書）は、合意された評価パラメータ（例：期限、品質標準、支出など）からの逸脱を強調し、優先順位の変更、人員や資源の不足など遅延の理由を説明すべきだ。

これは、イニシアチブ所有者からリードプロジェクト機関への定期的な更新を補完するものである。すべての関連する利害関係者は、戦略の実施と進捗状況の監視に積極的に関与すべきである。このアプローチは、約束に対する説明責任を確保し、課題の早期発見を促進し、政府が実施プロセスで得られた教訓に基づいて是正措置を講じたり、行動計画を適応させたりすることを可能にする。

3.6.3 戦略の成果評価

進捗状況の追跡に加え、当初設定した目標に対する成果を定期的に評価することも不可欠である。この評価により、戦略の目標が達成されているか、あるいは調整が必要か判断される。

このプロセスの一環として、より広範なデジタル・サイバーセキュリティリスク環境も定期的に再評価し、外部環境の変化が戦略の成果に影響を与えていないかを判断する必要がある。実質的に、このプロセスは国のリスクアセスメントプロファイルに対する軽微な見直しとして機能する。

アセスメント結果と関連する提言は、主導プロジェクト機関向けの報告書にまとめられるべきだ。この報告書には、行動計画を更新し、進化する政策、国家サイバーセキュリティアーキテクチャ、リスク環境に対応し続けるための提案を含める必要がある。

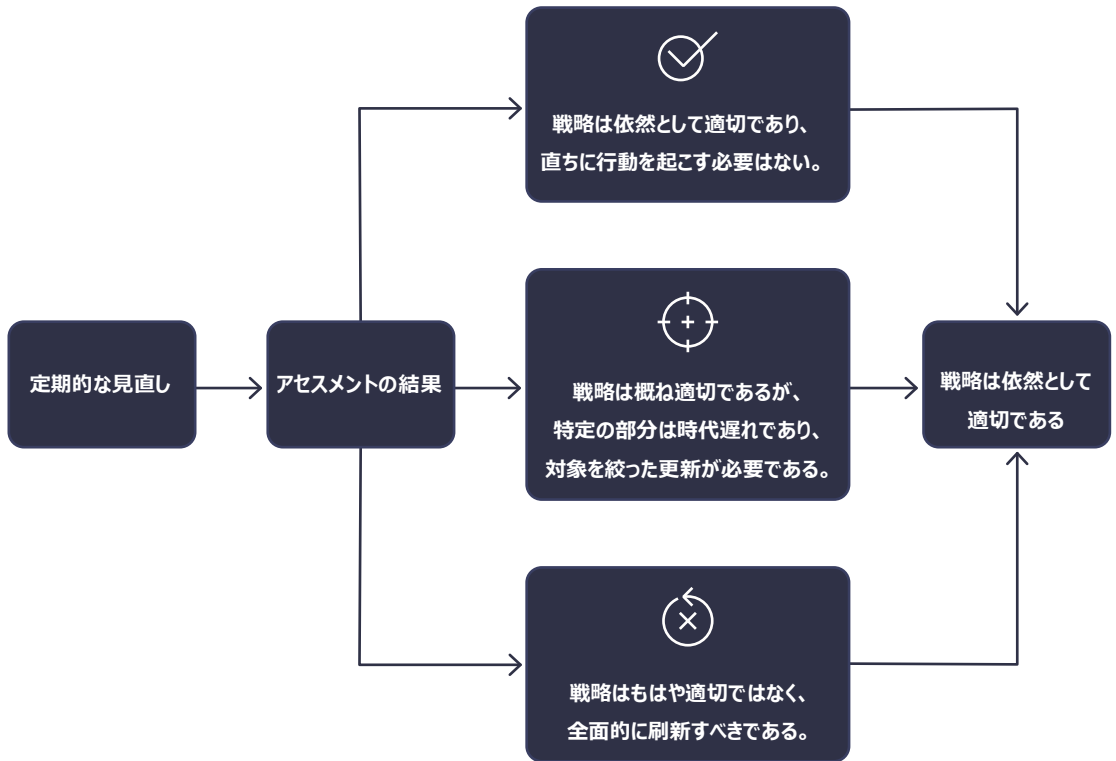
最終的に、NCS ライフサイクルを通じて作成される報告書は、開始段階で設定されたタイムラインに沿って、戦略全体のレビューの基礎となるべきだ。この包括的なレビューでは、進捗状況や外部環境の変化だけでなく、政府の優先事項や目標の変化も評価すべきである。

3.6.4 定期的な見直しと更新による関連性の確保

戦略は、進化する脅威、技術的变化、国家の優先事項の変化に対応し続けるため、定期的な見直しを受けるべきである。レビューはガバナンス枠組みに制度化され、可能な限り代替的視点を提供できる外部関係者の参加を含め、定期的な間隔（例：3～5年ごと）で実施されるべきである。また、戦略の想定寿命の中間点で少なくとも1回の中間レビューを実施する。加えて、重大なサイバーインシデント、法規制の変更、地政学的状況の変化といった重大な事象が発生した場合にもレビューをトリガーすべきである。

見直しプロセスでは、戦略の継続的な妥当性を評価し、今後の進め方に関する提言をまとめるべきだ。例えば、以下のような内容が含まれる可能性がある：

図 3 - 戦略の定期的な見直し



結局のところ、定期的かつ中期的な見直しによって、戦略は変化する状況に対応できる生きた文書であり続ける。これらの見直しは、開始と現状把握から再び始まる次の NCS 策定サイクルに直接反映されるべきだ。

4 包括的原則

本セクションでは、10 の横断的原則を提示する。これらを総合的に考慮することで、先見性のある包括的な国家サイバーセキュリティ戦略の策定に資する。

これらの原則は、本文書で識別された全ての重点分野に適用される。戦略文書の起草から実施に至るまでの戦略策定プロセスの全段階で考慮すべきである。

これらの原則の順序は、重要度の順序ではなく、論理的な流れを反映したものである。

図 4 - 包括的な原則



4.1 ビジョン

戦略は、政府全体および社会全体の明確なビジョンを設定すべきである。

戦略は、すべての関係者が、何が危機に瀕しているのか、なぜ戦略が必要なのか（背景）、何を達成すべきか（目標）、誰に影響を与えるのか（範囲）を理解するのに役立つビジョンを設定することで、成功する可能性が高まる。

ビジョンが明確であればあるほど、指導者や主要な利害関係者が包括的、一貫性、整合性のあるアプローチを確保しやすくなる。明確なビジョンは、関連する利害関係者間の調整、協力、支援、実施も促進する。ビジョンは十分に高いレベルで策定され、デジタル環境の動的な性質を考慮すべきである。戦略の目標と実施スケジュールは、このビジョンと整合させる必要がある。

4.2 包括的アプローチと国別優先事項

戦略は、デジタル環境全体を包括的に理解・分析した結果として策定されるべきだが、各国の状況や優先事項に合わせて調整される必要がある。

サイバーセキュリティは技術的課題であるだけでなく、経済的・社会的繁栄を超え、法執行、国家・国際安全保障、国際関係、貿易交渉、持続可能な開発などの領域にまで及ぶ多面的な問題である。

優先事項は、国の具体的な状況に基づき、国家目標や戦略の実施スケジュールと整合させ、適切な資源で支えられるべきである。一部のサイバーセキュリティ課題は、別の戦略文書（例：国家安全保障戦略や防衛戦略における国家安全保障・防衛のデジタル側面）で扱われる場合もある。

戦略は、政策の一貫性と機構のレジリエンスを確保するため、データガバナンス、AI、デジタルトラストなどの広範なデジタルガバナンス枠組みとも明確に整合させるべきである。このような統合は戦略の包括的アプローチを強化し、サイバーセキュリティをデータや新興技術の安全かつ責任ある利用に組み込むことで、信頼性が高く持続可能なデジタル環境の構築に寄与する。

4.3 包括性

戦略は、全ての関連する利害関係者の積極的な参加を得て策定されるべきであり、プロセス全体を通じて彼らのニーズと責任に対応すべきである。

デジタル環境は政府、組織、個人にとって極めて重要である。これらの主体はサイバーセキュリティリスクに直面し、それぞれの役割に応じてその管理責任を共有する。政府は、NCS の開発と実施において全ての関連する利害関係者を包含するパートナーシップと協カメカニズムを確立すべきである。

困難ではあるが、戦略が多様なニーズと専門性を反映し、成功裏に実施されるためには、関係者を識別し、有意義に関与させることが不可欠である。包括性と透明性を促進するため、戦略は公開文書とすべきである。

4.4 経済的・社会的繁栄

本戦略は、経済的・社会的繁栄を促進し、デジタル技術が持続可能な開発と包摂性に最大限貢献するよう努めるべきである。

接続性の向上、デジタル化、デジタル経済への参加は、成長と社会的進歩を加速し、重要な社会的価値を推進し、公共サービスの提供と能力を改善し、国際貿易を促進し、良きガバナンスを促進する。

社会の機能におけるデジタルインフラへの依存度が高まるにつれ、サイバーセキュリティへの注目も増す必要がある。ただし、サイバーセキュリティはそれ自体が目的ではない。本戦略は、対象国のより広範な社会経済目標と整合し、信頼と確信を構築することで、社会がサイバーセキュリティリスクから自らを防御しながらこれらの目標を実現できるようにすべきである。

4.5 基本的人権

本戦略は基本的人権を尊重し、これと整合性を保つべきである。

人々がオフラインで有する権利は、オンライン上でも防御されなければならないという事実を認識すべきである。本戦略は、国連世界人権宣言や市民的及び政治的権利に関する国際規約に規定される権利、ならびに関連する多国間・地域的法的枠組みに定められた権利を含む（ただしこれらに限定されない）普遍的に認められた人権を尊重すべきである。特に表現の自由、プライバシー、個人データ保護に留意すべきである。特に、本戦略は恣意的・不当・違法な監視、通信傍受、個人データ収集を助長することを避けるべきである。

国家が正当な利益を満たすための行動を取れるようにしつつ、個人の人権を尊重することを確保するため、本戦略は、適用可能な場合、監視、傍受、データ収集が、特定の調査または法的事件の文脈においてのみ、合法的な権限の下で、公的、明確、包括的かつ非差別的な法的枠組みに基づき、国際的義務に沿った効果的な監督、手続き上の保障、救済措置を伴って行われることを保証すべきである。

4.6 リスクマネジメントとレジリエンス

本戦略は、サイバーセキュリティリスクの効率的な管理を可能にし、経済・社会活動のレジリエンスを強化すべきである。

他の種類のリスクと同様に、サイバーセキュリティリスクを完全に排除することはできないが、管理および緩和は可能である。本戦略は、事業者がサイバーセキュリティ投資を優先し、リスクと機会を均衡させ、継続的なリスクマネジメントを採用し、相互依存する事業者やセクター間で一貫したアプローチを促進するよう奨励すべきである。

レジリエンスには、インシデントへの備え、危機管理、復旧が必要である。本戦略は、事業継続および災害復旧対策の導入を促進し、デジタルインフラへの混乱に耐え、そこから回復できる重要なサービスと機能を確保すべきである。

4.7 適切な政策手段の組み合わせ

戦略は、各国の具体的な状況を考慮し、その目的達成に最も適切な政策手段を活用すべきである。

政府は、成果を達成するために様々な手段や政策手段を自由に使える。これには、立法、規制、標準、認証、インセンティブ、情報共有メカニズム、教育、優良実践の共有、行動規範、信頼のコミュニティ構築などが含まれる。これらの手段はそれぞれ長所と短所があり、コストも異なり、異なる結果をもたらす。

意図した目的に応じてこれらの政策手段とツールを選択し、バランスを取ることによって、最も効果的な成果が達成される。

4.8 明確なリーダーシップ、役割分担、資源配分

戦略は政府の最高レベルで策定され、その実行に対する明確なリーダーシップと説明責任が求められる。関連する役割と責任を割り当て、十分な人的・財政的資源を配分しなければならない。

サイバーセキュリティは政府の最高レベルで推進・維持されるべきだ。さらに、説明責任と進捗を確保するため、各作業分野の責任者を明確にし、全ての関係者がそれぞれの役割と責任を明確に理解する必要がある。

戦略はまた、その実施に必要な適切な人的・財政的・物的資源を配分すべきである。この原則は、戦略策定プロセスと行動計画及び関連イニシアチブの詳細化の両方を導く必要がある。

4.9 信頼環境

本戦略は、市民や組織が信頼できるデジタル環境の構築に寄与すべきである。

ユーザーの権利と利益が防御され、データと情報システムの安全性が確保される国家デジタルエコシステムへの信頼構築は、デジタル変革をもたらす社会的・政治的・経済的機会の可能性を最大限に実現するために不可欠である。本戦略は、電子政府、電子商取引、デジタル金融、遠隔医療などの重要サービスを確保するための政策、プロセス、行動を可能にしなければならない。権利を防御し、システムの安全性を保証することで、本戦略は一般市民とデジタルサービスを提供する官民組織の双方の間で信頼を育む。

4.10 技術的先見性と適応性

サイバーセキュリティの優先事項、目標、行動は、進化するデジタル環境とリスク環境に適応しなければならない。

新興技術や破壊的技術（例：AI、自動化、IoT、量子コンピューティング、5G/6G、分散型台帳技術）は、国家戦略的思考を再構築する可能性を秘めた機会とリスクの両方をもたらす。

政府は、破壊的トレンドを予測し、その影響を評価し、それに従って政策を適応させるため、技術的先見性、地平線スキャンニング、定期的な見直しを制度化すべきである。これには、政府、産業界、学界、研究機関との構造化された連携が必要であり、イノベーションの知見と国際的な優良実践を統合することが求められる。

戦略は、技術変化と共に進化しつつ、レジリエンス、セキュリティ、デジタルイノベーションを支える「生きている枠組み」として扱わなければならない。見直しと中間更新（[セクション 3「ライフサイクル」](#)参照）は、NCS ライフサイクルに適応性を組み込むために極めて重要である。

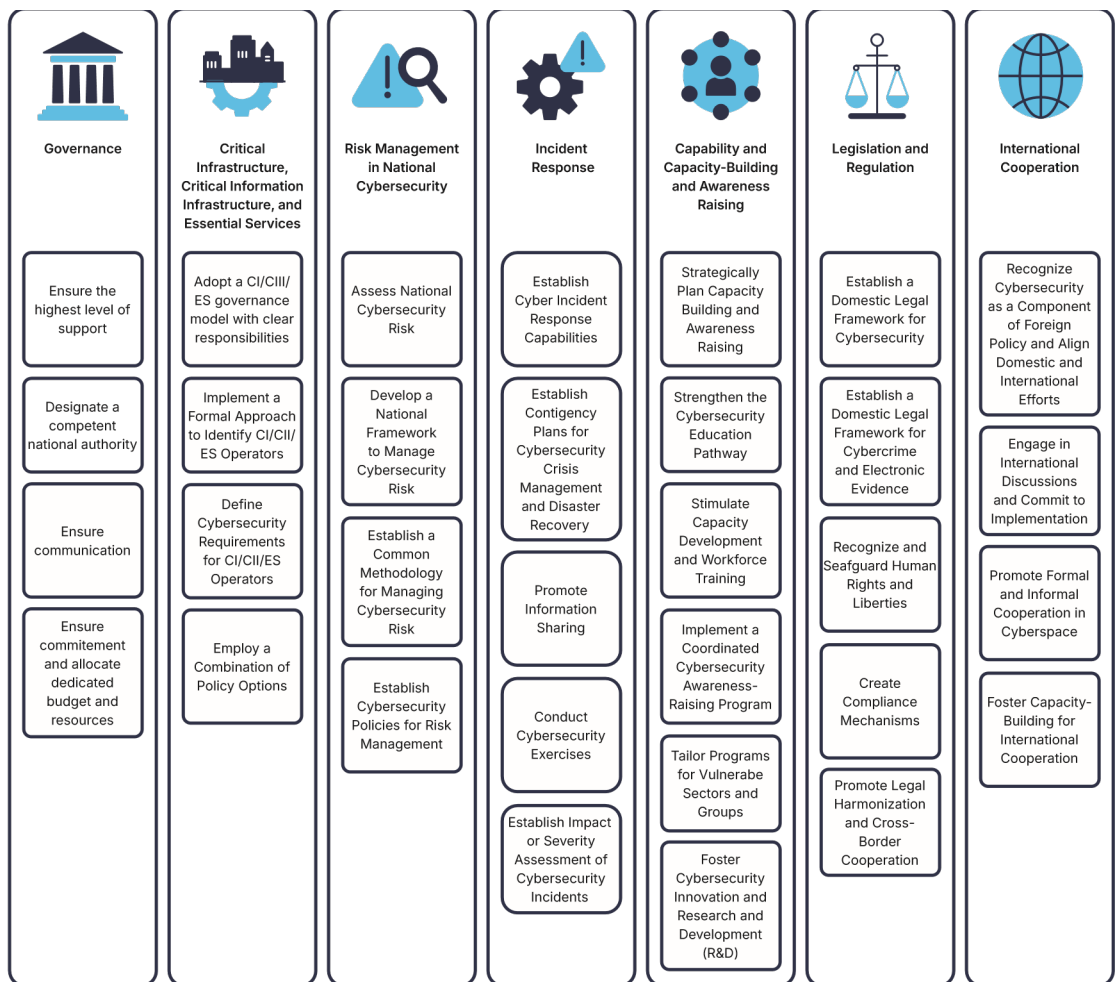
5 国家サイバーセキュリティ戦略の優良実践

サイバーセキュリティは社会経済発展の多くの分野に影響を与え、国家の文脈における複数の要因の影響を受ける。

したがって、本セクションでは、国家の文脈に合わせた調整を可能にしつつ、戦略を包括的かつ効果的にする一連の優良実践要素を紹介する。

これらの優良実践要素は、包括的な NCS のための包括的テーマである、明確な重点分野に分類されている。重点分野と優良実践要素の双方が優良実践の例として提示されているが、後者は国家の文脈で捉えることが特に重要である。なぜなら、一部は特定の国の状況に関連しない可能性があるからである。各国は、自国の戦略（[セクション 4.1](#)）で定義されたビジョンに沿って、自国の目標と優先事項を支援する優良実践要素を識別し、それに従うべきである。以下の個々の要素や重点分野の順序は、重要度や優先順位を示すものではない。

図 5 - 重点分野



5.1 重点分野 1 – ガバナンス

この重点分野では、国家サイバーセキュリティのためのガバナンス構造、モデル、枠組みに関する優良実践要素を紹介する。これには、国家のレジリエンスを高め、国民、企業、重要インフラ、サービス、資産に対するリスクを低減するために、政府が政治的、運用的、技術的レベルで追求する戦略的目標と成果を明確に表明することが含まれる。戦略では、戦略の実施を担当する関係者（該当する場合、管轄国家機関など）の役割、責任、権限、権能、説明責任の仕組みも識別すべきである。

5.1.1 最高レベルの支援を確保する

本戦略は政府最高レベルによる正式な承認を得るべきである。この承認には二つの重要な目的がある。第一に、十分な資源が配分され、調整努力が成功する可能性を高めることである。第二に、国内の広範なエコシステムに対し、国のサイバーセキュリティがデジタル経済やデジタルシステムに依存するその他の社会的・政治的側面と密接に結びついており、したがって国家の優先課題として扱わなければならないことを示すことである。

戦略は国内法体系に明文化される必要もあり、それによって国家的な重要性和優先順位が得られる。

5.1.2 管轄権限を有する国家機関の指定

効果的な国家サイバーセキュリティガバナンスには、国の規模や憲法上の構造に応じて、一つ以上の有能な国家サイバーセキュリティ当局の指定が必要である。連邦制や非中央集権化システムでは、複数の機関が必要となる場合がある。これらの機関は、サイバーセキュリティガバナンスの主導・調整、実施に向けた指導・支援を担う責任主体として、戦略において明示的に特定されるべきである。権限と実効性を確保するため、最高レベルの政府機関または国家指導部と密接に連携し、戦略的方向性の提示、行動の調整、実施状況の監視を可能とする体制を構築すべきである。

管轄当局の任務には、サイバーセキュリティガバナンスに関する法案・政策のドラフト作成、役割・責任・プロセス・意思決定権限の定義と明確化、戦略の効果的な実施の確保が含まれる。サイバーセキュリティは横断的領域であるため、管轄国家機関が関連ステークホルダーを巻き込み指導できることが重要だ。これには、運用上の任務やイニシアチブを担当するステークホルダーの特定と監督、関連する業績目標の設定が含まれる。

管轄当局はまた、サイバーセキュリティ活動の進捗状況と成果に関する報告責任を負うべきである。報告を円滑化するため、責任あるステークホルダー及び政府事業体は、測定可能な形で管轄国家機関に報告する義務を負うべきである。主要業績評価指標（KPI）の使用は、進捗を評価し、監視を可能にすることで説明責任を促進する効果的な方法である（SMART KPIの説明については[第7セクション 3.6](#)を参照）。

管轄当局がその任務を遂行できるようにするためには、関連するすべてのステークホルダーに対して明確な権限を付与すべきである。この権限は、当局がその機能を遂行できるようにするために、政策や法律で正式に定める必要があるかもしれない。

5.1.3 コミュニケーション、調整、協働の確保

サイバーセキュリティには、社会全体の取り組みを基盤とした国家全体のアプローチが必要であり、官民を含む様々なステークホルダー間の協力が不可欠である。国家サイバーセキュリティガバナンスシステムは、効果的・効率的かつ説明責任のあるサイバーセキュリティ対策の実施を確保するため、各ステークホルダーの役割、責任、プロセス、相互関係を定義すべきである。

役割と責任の配分は、各ステークホルダーが国内の憲法・法的枠組み内で担う使命に沿うべきである。例えば、政府団体は公共サービスを提供し、市民社会は監視・助言支援を行い、立法府は法制定を担う可能性がある。

したがって、ガバナンスは、法律や政策、戦略、運用、技術など、複数の側面における主体に対応し、組織、地方、国家、地域、国際レベルにわたって機能しなければならない。

5.1.3.1 政府内の連携の確保

戦略は、その実施に影響を受ける、あるいはその実施に責任を持つ政府機関を識別し、含めるべきである。政府機関内のコミットメント、調整、協力は、政府機構の中核的な機能であり、ガバナンスの仕組み（標準、規制、市場インセンティブなど）と資源が戦略の

望ましい成果をもたらすために不可欠である。確立された高レベルの国家サイバーセキュリティ担当当局の存在も、政府機関内の調整と協力の強化に役立つ。

効果的なコミュニケーション、調整、連携により、すべての省庁および政府機関が、相互の権限、使命、任務を認識することができる。例としては、関連する利害関係者を招いた定期的な会合や、特定の課題に対処するための政府内部タスクフォースの設置などが挙げられる。

政府内の調整メカニズムは、サイバーセキュリティ政策と行動が省庁間で一貫性を保ち、重複を避け、国のより広範なデジタル変革アジェンダとの整合性を促進することも保証すべきである。

5.1.3.2 セクター間の連携の確保

国家サイバーセキュリティガバナンス構造は、政府が民間部門やその他の非政府ステークホルダーに依存している（またその逆も同様である）という理解を反映し、包括性の原則（[セクション 4.3](#)）に沿って、より安全で、よりレジリエントなエコシステムの実現に向けて協力できるようにすべきである。この目的のために、戦略は、政府がこれらの非政府ステークホルダーをどのように関与させるかを明確にし、ガバナンスの枠組みにおけるそれらの役割と責任を明確に定義すべきである。

戦略では、重要なサービスやインフラの運用と復旧に不可欠な産業について、権威ある国内連絡窓口のネットワークを特定するよう求めることが良い慣行である。各ステークホルダーに割り当てられる役割は、国内の法的・機構の枠組みにおけるその全体的な任務と整合性があるべきである。

戦略は、接続性の手頃な価格・利用可能性・包括性の確保、イノベーション促進と並行したデータ保護・プライバシーの推進、災害・気候変動・パンデミックに直面したインフラレジリエンスとサービス可用性の強化、AI・ブロックチェーン・量子コンピューティング・分散型台帳技術などの新興技術の責任ある探求・採用といった、他の国家優先事項とも整合させるべきである。こうした整合性により、サイバーセキュリティに関するセクター間の協力が孤立化せず、デジタル変革、レジリエンス、持続可能な開発というより広範な国家目標に組み込まれることが保証される。

5.1.4 コミットメントの確保と専用予算・資源の配分

国家のサイバーセキュリティ対策の成功には、信頼できるパートナーシップに裏打ちされた政治的コミットメントとリーダーシップが必要である。この文脈におけるコミットメントとは、国家のサイバーセキュリティ優先事項が確実に達成されるよう、長期にわたる一貫した政策を支援することを意味する。良い実践例として、国内政策と外交政策の目標間に整合性を確保する安全策を設けることが挙げられる。これにより、同一の政策課題（例：貿易の流れとデュアルユース技術の輸出管理）に関して、ある省庁が別の省庁の立場と矛盾する主張を行い、相互に足を引っ張り合う事態を防げる。

この長期的視点は、新興技術に関するサイバーセキュリティガバナンスにも適用されるべきだ。技術的に中立性を保ちつつ、状況の変化に応じて技術革新を予測・管理するレジリエントな仕組みを構築する必要がある。

国家サイバーセキュリティにおいてコミットメントを要するもう一つの重要要素は資源配分である。効果的な国家サイバーセキュリティ態勢の基盤は、十分かつ一貫性のある継続的な資金調達にある。ガバナンス構造は、関係者が任務を遂行するために必要な資源を提供する専用予算を前提に設計されねばならない。資源は金銭（専用予算）、人材、物資の観点から定義されるべきである。

戦略内の目標と任務は、資源の一時的な配分として捉えるべきではない。資源要件は、戦略内の任務や目標の実施における進捗状況や不足に基づき、定期的に見直されるべきである。政府は、国家ガバナンス機構が管理する中央サイバーセキュリティ予算の設置も検討できる。異なる資金源を統合した一貫性のあるプログラムへの統合であれ、政府内部の統一予算の創設であれ、プログラム全体は、成功裏な実施を確保するため、マイルストーンを通じて管理・追跡されるべきである。

詳細は www.ncsguide.org を参照のこと。

5.2 重点分野 2 – 重要インフラ、重要情報インフラ、および重要サービス

この重点分野では、重要インフラ（CI）、重要情報インフラ（CII）、および重要サービス（ES）を識別・防御し、その信頼性とレジリエンスを強化するための優れた実践例を検討する。

CI/CII/ES に影響を与えるインシデントの潜在的な影響は深刻であり、社会秩序の混乱、サービス提供の中断、国家の経済的繁栄の損なわれを引き起こす可能性がある。したがって、戦略では、こうした破壊的・妨害的インシデントの発生確率と影響を低減するためのリスクマネジメントとレジリエンス強化の取り組みの重要性を強調すべきである。

CI/CII/ES には普遍的に認められた定義は存在せず、最終的には各国の地政学的、社会経済的、文化的特性に依存する可能性がある。したがって政府は、自国のサイバーセキュリティリスクアセスメント、状況、優先事項に基づいてこれらの用語を定義すべきである。

本ガイドは共通用語の欠如を認識し、CI/CII/ES および関連事業者の概念について異なる解釈を許容する柔軟なアプローチを採用する。これらのインフラと サービスは相互依存性が高く、一方が機能するには他方の依存が常にある。ある領域の混乱は複数のシステムに波及する可能性がある。例としては：

- **重要インフラ (CI)**：社会と経済の機能及び安全保障に不可欠な資産（例：発電所、水処理施設、鉄道網）。
- **重要情報インフラ (CII)**：重要インフラの主要機能を支える情報通信技術 (ICT) および運用技術 (OT) システム（例：インターネットエクスチェンジポイント (IXP)、海底ケーブル、監視制御とデータ収集 (SCADA) システム、国家データセンター）。
- **重要サービス (ES)**：重要社会活動や経済活動を維持するために必要なサービス（例：電力供給、デジタル・モバイルコミュニケーション、公共交通機関、医療サービス）。
- **CI/CII/ES 事業者**：重要インフラ (CI) および/または重要情報インフラ (CII) を所有・運営し、必須サービス (ES) を提供する公的・民間事業者（例：インターネットサービスプロバイダ (ISP)、ドメインネームサービスプロバイダ (DNS)、通信事業者、主要病院、中央銀行、水道・エネルギー公益事業者など）。
- **サービスレベル契約 (SLA)**：相互依存システム全体で業務継続性とレジリエンスを維持するために必要な、期待されるサービスレベル、パフォーマンス指標、責任、対応メカニズムを定義する、CI/CII/ES 事業者間の正式な契約または合意。

5.2.1 明確な責任分担を備えた CI/CII/ES ガバナンスモデルの採用

戦略は、明確なリーダーシップ、役割、資源配分という原則（[セクション 4.8](#)）に従い、CI/CII 防御に関わる様々なステークホルダーのガバナンス構造、役割、責任、調整メカニズムを大まかに定義すべきである。

CI/CII/ES の保護は単一の政府機関の能力を超える場合が多いため、省庁間委員会などの CI/CII/ES サイバーセキュリティ全体の調整役を任命することで、調整と保護の取り組みを大幅に強化できる。

CI/CII/ES 防御のガバナンスモデルには以下を含めるべきである：特定セクターを担当する政府事業者の特定、事業者の責任と説明責任、重要サービスの継続性と復旧を確保するための官民間のコミュニケーション経路及び協力メカニズムの確立；権限が重複する政府事業者間での調整と整合性を促進する仕組み；そして、セクター規制当局が明確で一貫性のあるセキュリティ要件を策定し、重複を避け、資源の浪費を防ぎ、官民双方のコンプライアンス努力を合理化する方法を確保する手段。

CI/CII/ES の越境的性質を考慮すると、ガバナンスモデルには地域的・国際的な調整と協力の仕組みも含めるべきである。

5.2.2 CI/CII/ES を識別するための正式なアプローチの実施

本戦略は、正式かつ反復可能で規準に基づくアプローチによる CI/CII/ES の特定を促進すべきである。このプロセスは中央で調整され、定期的に見直され、国家リスクマネジメント、資源配分、対応計画の策定に活用されるべきである。成果物としては、重要度レベルとリスクプロファイルを付した、重要セクター、サービス、機能、事業者、資産の国家登録簿が典型的に含まれる。

CI/CII/ES を識別する手法は様々だが、各国は以下のような部門別・機能別・影響規準の適用を検討すべきである：他のインフラとの依存関係・相互依存関係、最低限のサービス水準維持におけるインフラの重要性（）、冗長性、市場シェア、地理的位置。

登録簿の正確性と妥当性を維持するため、定期的な見直し（例：2年ごと）または重大なインシデント・技術的変化発生後に行うべきである。公的機関、規制当局、民間インフラ事業者を含む関連ステークホルダーの早期かつ継続的な関与が不可欠である。本戦略は、民間事業者が定期的な事業影響度分析 (BIA) およびリスクアセスメントを実施するよう奨励またはインセンティブを与えるべきである。これらのアセスメントでは、重要資産・業務・機能に対する障害の潜在的影響を評価し、その結果を関連当局と共有して、

国家レベルの特定、事業継続計画、災害復旧計画に反映させる必要がある（[セクション 3.2.2](#)、[セクション 5.3.1](#)、[セクション 5.4.2 参照](#)）。

本戦略は、インシデント、演習、監査から得られた教訓を将来の特定サイクルに統合するためのフィードバックループを確立し、国境を越えた整合性を支援するため、地域および国際的な枠組みとの収斂を促進すべきである。

5.2.3 CI/CII/ES 事業者に対するサイバーセキュリティ要件の定義

本戦略は、重要インフラ（CI/CII/ES）事業者及びその他の関連ステークホルダーに対するサイバーセキュリティ要件を規定する既存の法的・規制的枠組みを強調するか、新たな枠組みの構築を促進すべきである（[セクション 5.6.1](#)「立法と規制」に準拠）。これらの要件は、対象事業者がサイバーセキュリティ実践の最低基準を満たしつつ、自社のリスクマネジメント優先事項との整合性を保つ柔軟性を維持できるよう構成されるべきである。

基準は国際的に認められた標準や優良実践を活用し、グローバルサプライチェーンへの統合を促進するとともに、国境を越えた相互運用性の問題を回避すべきである。要件は、リスク指向アプローチの採用（[セクション 4.6](#)「リスクマネジメントとレジリエンス」[及びセクション 5.3.2](#)「国家リスク評価」に準拠）、データとシステムの防御、調達プロセスとサプライチェーンのセキュリティ確保、デジタル環境の監視と潜在的な異常とイベントの検知、明確に定義されたインシデント・危機管理プロセス、事業継続措置、災害復旧計画に支えられたインシデント対応と復旧など、幅広いサイバーセキュリティ実践を網羅すべきである。

事業者には、リアルタイム監視とインシデント対応のためのセキュリティ・オペレーションセンター（SOC）の維持が求められる場合もある。サイバーセキュリティの基準は、関係する事業体のリスクプロファイルと重要性に比例したものであるべきだ。階層的アプローチを適用し、影響度の高い事業体と低い事業体を区別することで、中核的な保護を損なうことなく、コンプライアンス努力の効率的な配分を確保できる。

まずセクター横断的な基準を策定し、セクター固有の実践の相互運用性と一貫性を高め、セクター横断的機能やサブセクターにおけるコンプライアンスを効率化すべきである。これらを補完する形で、セクター固有の「実践方法」ガイダンスを提供し、エンタープライズの実践を啓発・統合するための選択肢を示すことができる。これらのガイドラインは、監視メカニズム（例：実績ベースの監査、自己評価、義務的報告）によって支えられるべきであり、これにより基準要件が採用されるだけでなく、積極的に維持されることが保証される。

サイバーセキュリティのベースラインは、リスク環境と技術が進化し続ける中で、時間の経過とともに高い適応性を確保するため、成果重視であるべきだ。運用者が達成すべき目標（例：「重要なリソースへの論理アクセスを制御する」）を明確にすること、セキュリティの実装方法（例：「二要素認証を使用する」）を規定することよりも、政府と産業が継続的なセキュリティ改善の恩恵を受けられるようにする。

成果ベースで要件を定義することは、実装の柔軟性を可能にし、イノベーションを促進し、絶え間ない更新に伴う規制負担を軽減する。このアプローチは、運用者を特定の技術的解決策に早期に縛り付けることを回避するため、新興技術や変化する脅威環境への適応において特に価値がある。

5.2.4 政策オプションの組み合わせを採用する

本戦略は、包括的アプローチと個別優先事項の原則（[セクション 4.2](#)）に基づき、サイバーセキュリティ責任が実行可能かつ達成可能となるよう、幅広い政策手段の展開を想定すべきである。

CI/CII/ES 分野の事業者に対し、直面するリスクに見合ったサイバーセキュリティ対策を採用させるため、政府はインセンティブとディスインセンティブをバランスよく展開するべきだ。政策オプションには以下が含まれる：監査やその他のコンプライアンス監視の実施、責任と説明責任の定義、認証・認可スキームの開発、財政的インセンティブや補助金の提供、サイバー能力構築イニシアチブの実施、およびセクター別情報共有分析センター（ISAC）や情報共有分析組織（ISAQ）といった構造化された官民連携（PPP）の促進。これにより、セクター横断的な情報共有と集団防衛が促進される（適切な政策手段の活用に関する[セクション 4.7](#)、情報共有の促進に関する[セクション 5.4.3 参照](#)）。

事業者はサイバーセキュリティインシデントの広範な社会的影響を十分に内部化しない可能性があるため、企業利益だけでなく広範な公共の利益のために安全対策が採用されるよう、政策介入がしばしば必要となる。したがって政策手段は、市場が推進できる範囲と推進すべき範囲、そして進化するリスク環境が要求する範囲とのギャップに対処できるよう慎重に調整されるべきである。

自主的または市場ベースの解決策が不十分である場合、本戦略は特に高リスクまたは競争の少ない分野において、対象を絞った規制や直接的な公的介入の役割を認識すべきである。同時に、効果的な政策枠組みは、イノベーションを阻害したり既存の取り組みを重複させたりする過剰な規制を避け、公的・民間事業体を横断して要件を合理化すべきである。

最後に、本戦略はこれらの政策手段を定期的に評価し、行動変容、レジリエンス成果、市場応答性を測定すべきである。新たなリスク、技術発展、実施経験に基づく教訓を踏まえ、随時調整を加える必要がある。この見直しサイクルを組み込むことで、説明責任が強化され、国家優先事項との持続的な整合性が確保され、重要インフラ／重要情報インフラ／エネルギーシステム（[ライフサイクルセクション](#)）の長期的なレジリエンスが支援される。

5.3 重点分野 3 – 国家サイバーセキュリティにおけるリスクマネジメント

本重点領域では、リスクマネジメントを通じたサイバーセキュリティ対応の優良実践を紹介する。リスクマネジメントとレジリエンスの原則（[セクション 4.6](#)）で規定される通り、サイバーセキュリティリスクを完全に排除することは不可能であるため、リスクマネジメントアプローチを採用すべきである。自国が直面するリスクを明確に理解することで、資源配分の優先順位付け、脆弱性の低減、総合的な準備態勢の強化が可能となる。さらに、包括的アプローチと個別対応の原則（[セクション 4.2](#)）に従い、リスクマネジメントは国家の優先事項と整合し、デジタル環境全体を考慮すべきである。セクター内およびセクター間の相互依存関係、ならびに国境を越えた依存関係から生じるリスクの識別に焦点を当てる必要がある。

戦略は、リスクマネジメントを単発的な取り組みではなく、戦略的先見性、セクター別情報、進化する脅威状況を統合した継続的かつデータ駆動型のプロセスとして位置付けるべきである。サイバーセキュリティ脅威とデジタル環境は極めて動的で予測不可能なため、あらゆるリスクマネジメントアプローチは定期的に見直され、未知のリスクに対処できるよう設計されるべきである。したがって、本戦略はレジリエンス強化と継続的改善を確保するため、リスクマネジメント活動のモニタリングと評価を計画すべきである。これには、国家・セクター・組織レベルにおけるリスクマネジメント・フレームワークの監督、評価、改善に関する機構の責任を確立することが含まれる。

5.3.1 国家サイバーセキュリティリスクの評価

戦略は、正式かつ反復可能な手法に基づき、国家レベルでのサイバーセキュリティリスクの定期的な特定、分析、アセスメントを促進すべきである。これには通常、脅威、脆弱性、社会機能の相互依存性に基づいて、サイバーセキュリティインシデントの発生確率と潜在的影響を推定することが含まれる。アセスメントは動的であるべきであり、脅威インテリジェンス、国境を越えた要素や地政学的考慮事項、AI や量子コンピューティングの進歩がもたらすような新興技術リスクを組み込む必要がある。

アセスメントには、社会と経済にとって最も重要とみなされるセクターのセクター別リスクプロファイルを含めることができる。セクター別リスクプロファイルは、より具体的なリスクアセスメントの基礎を提供し、国内の全セクター内およびセクター間の整合性を導入するのに役立つ。さらに、このアセスメントでは重要インフラ／重要情報インフラ／エネルギーシステム（[セクション 5.2.2](#)）と、セクター内およびセクター間（例：エネルギー、通信、水道、医療間）の相互依存性を考慮すべきである。相互接続されたシステム全体に波及し、重要サービスの継続性を阻害する可能性のある、体系的なサイバーセキュリティリスクを識別する必要がある。

本戦略は、国家およびセクター別リスクアセスメントの実施・更新のためのガバナンスメカニズムを定義し、国家サイバーセキュリティ当局、セクター規制機関、情報機関、主要民間関係者がアセスメントへの貢献と妥当性確認において担う役割を明示すべきである。こうした取り組みは、サイバーリスクマネジメント戦略を国家危機管理計画と整合させると同時に、国家全体のサイバーセキュリティ態勢強化に必要な能力、キャパシティ、専門知識、資金、政策を動員する基盤となる。

5.3.2 サイバーセキュリティリスク管理のための国家枠組みの構築

本戦略は、相互依存するセクターや資産全体にわたるサイバーセキュリティリスクの一貫性ある調整された管理のための国家枠組みの開発と実施を促進すべきである。この枠組みは、政府がリスクとその管理手法を可視化し監督できるように、安全に保管・伝達される国家リスク登録簿を確立すべきである。枠組みは発生確率と潜在的影響に基づきリスクを優先順位付けすべきである。リスク登録簿は、異なるセクターや機能にわたる国家のリスク許容度と耐容レベルを考慮し、それに応じてリスク分類を導くべきである。国家リスク登録簿は動的なものであり、進化する脅威や技術に基づき、定期的な間隔（例：毎年、または重大なインシデント発生後）で更新されるべきである。

また、機密性やデータ保護要件を尊重しつつ、部門別・組織別のリスクデータを集約する仕組みを含めるべきである。これにより、機密性の高い運用詳細を暴露することなく、戦略レベルでの可視性を確保する。各部門における主要事業体の責任を明確化し、国家レベルのサイバーセキュリティリスクの評価、受容、対応を規定すべきである。これにより説明責任と明確な報告ラインを確保し、システム的なサイバーセキュリティリスクに関連するエスカレーション手順や意思決定経路など、調整された意思決定を支援する。

さらに、本戦略はサイバーセキュリティ対策の効果を評価するための国家レベルのリスク指標の定義を促進するとともに、継続的な政策改善を支援し、将来の戦略的・運用上の意思決定に情報を提供するフィードバックメカニズムを確立すべきである。

5.3.3 サイバーセキュリティリスクマネジメントのための共通手法の確立

本戦略は、サイバーセキュリティリスク管理のための共通手法の確立を推進すべきである。これにより組織間の効率性と一貫性が確保され、相互依存システム間での脅威・リスク情報の交換が促進される。国際標準に基づく手法が望ましい。これによりコスト削減が可能となり、民間セクターとの連携が改善されるためである。この共通手法は、セクター固有のニーズに適応可能であり、将来の技術変化や脅威アクターを柔軟に取り込める柔軟性を備えるべきである。

この手法は、脅威の評価から資産の評価、リスク許容度と耐容レベルの定義、緩和措置の実施と維持、残存リスクの受容に至るリスクマネジメントライフサイクル全体に関する指針を提供すべきである。また、コンプライアンスを評価・改善するための認証プログラムも含めるべきだ。この認証は拡張性と階層性を備え、規模や重要度が異なる組織向けに異なるレベルの管理策を提供し、国内のコンプライアンス枠組みや関連する国際的義務と整合性が取れている必要がある。

重要な点として、デジタルインフラやサービスの調達においては、リスクマネジメントがサプライチェーンの信頼性を高める仕組みに関する指針を提供すべきである。また、設計段階からのセキュリティ確保（secure-by-design）とデフォルトでのセキュリティ確保（secure-by-default）の原則を推進すべきである。

5.3.4 リスクマネジメントのためのサイバーセキュリティ政策の確立

本戦略は、適切な政策手段の組み合わせ（[セクション 4.7](#)）及び包括的アプローチと個別優先事項の設定（[セクション 4.2](#)）の原則に基づき採択される国家サイバーセキュリティ政策の策定を促進すべきである。これらの政策は、ガバナンス、運用、技術要件を網羅し、関係者の役割と責任を明確化し、これらの課題に対する具体的なアプローチを義務付けるべきである。一貫性を確保するため、戦略は、セクター間の取り組みを調整し、重複を排除し、重要セクター全体で最低限の期待値を定義する国家サイバーセキュリティ政策枠組みの構築を促進すべきである。

こうした政策の例としては、安全な調達におけるサイバーセキュリティ要件、情報共有プログラム、調整された脆弱性開示、最低限のセキュリティ基準と注意義務基準、コンプライアンス認証プログラム、管轄当局への義務的報告などが挙げられる。これらの政策はまた、タイムリーで安全かつ標準的なインシデント通知の手順を定義し、セクター固有および越境的な報告義務との互換性を確保すべきである。

調整された国家政策枠組みは、慣行の調和、重複の削減、セクター間の一貫性と相互運用性の確保を通じて、より効率的かつ効果的なサイバーセキュリティ管理につながる。この目的のため、戦略は規制当局、政府機関、民間セクターの利害関係者間の政策調整メカニズムを確立すべきである。具体的には、国家作業部会、省庁間タスクフォース、諮問委員会など、明確に定義された権限と報告責任を有する組織を設け、サイバーセキュリティ政策が一貫して適用され、目的に適合し続けることを保証する。

5.4 重点分野 4 – インシデント対応

この重点分野は、サイバーセキュリティインシデントへの準備、予防、検知、緩和、対応、復旧のための国家能力の確立と持続可能性を支援する優良実践の概要を示す。同時に、国の全体的なサイバーレジリエンスの向上を図るものである。

5.4.1 サイバーインシデント対応能力の確立

戦略では、国内のインシデント対応能力を促進・調整する中央窓口として機能する国家機関の設置を求めるべきである。多くの場合、これは国家レベルの責任を担うコンピュータ緊急対応チーム（CERT）、コンピュータセキュリティ・インシデント対応チーム（CSIRT）、またはコンピュータインシデント対応チーム（CIRT）²の設置を伴う。

国家レベルの CERT/CSIRT/CIRT は、業界別または組織別チーム（例：金融、医療、エネルギー、運輸）によって補完される場合がある。これらのチームは業界固有のサービスを提供し、組織と国家レベルの CERT/CSIRT/CIRT との間の仲介役を務める。

CERT/CSIRT/CIRT の具体的な組織モデルは多様である（例：国家レベル、政府機関、セクター別）。全ての国が同一のニーズや資源を有しているわけではないが、こうした専門的かつ専任のチームは、予防的・教育的サービスに加え、積極的・消極的機能の両方を提供すべきである。これらの事業者は、インシデントへの迅速な対応能力と復旧能力を高めると同時に、悪影響を軽減し、レジリエンスを強化する。

CERT/CSIRT/CIRT が通常提供する中核サービス領域には、サイバーインシデント対応・調整、脆弱性管理、状況認識（脅威インテリジェンス・情報共有を含む）、知識移転が含まれる。国家レベルの CERT/CSIRT/CIRT は政府セキュリティ・オペレーションセンター（SOC）を運営し、公共機関向けに情報セキュリティ事象の監視・検知・管理などのサービスを提供することもある。

本戦略は、民間事業者によるセキュリティ・オペレーションセンター（SOC）や製品セキュリティインシデントレスポンスチーム（PSIRT）の設置を促進し、脅威の検知、事象の管理、ICT 製品の脆弱性対応能力を強化する可能性がある。最終的にこれらの事業者は、インシデントの管理と封じ込めにおける最初の防衛ラインとして機能し、国家対応システムに情報を提供する。

本戦略は、国家レベル、セクター別、民間レベルのインシデント対応チーム間、ならびに地域・国際的な対応機関との協力メカニズムと連絡手順を定義し、正式に定めるべきである。

5.4.2 サイバーセキュリティ危機管理と災害復旧のための緊急時対応計画の策定

本戦略は、サイバーセキュリティ緊急事態・危機対応のための国家緊急時対応計画の策定を求めるべきである。計画は、より広範な国家緊急時対応枠組みに統合されるか、整合性が図られるべきである。重要情報インフラ及び重要サービスに関するセクター別計画も検討すべきである。

この国家サイバーセキュリティ緊急時対応計画は、全ての関係者からの意見（包括性に関する原則 4.3）に加え、国家リスクアセスメントの結果や、重要情報インフラ（CI）、重要情報インフラ（CII）、重要サービス（ES）の業務継続に影響を及ぼす可能性のある部門横断的な依存関係の分析結果を統合すべきである。また、インシデントの優先順位付け、伝達、管理の方法について明確化を図りつつ、エスカレーション手順、インシデント分類規準、災害復旧メカニズムを定義すべきである。

5.4.3 情報共有の促進

戦略は、官民セクター間およびセクター内で実用的な情報および脅威情報の交換を促進するための情報共有メカニズムの確立を求めるべきである。

公式・非公式の情報共有プログラムは、調整の改善、インシデント対応・復旧時の迅速かつ正確なコミュニケーションの促進、影響を受ける当事者やその他の関係者間での脅威情報の迅速な拡散を可能にする。これらの仕組みは、どのセクターがどのように標的とされたかの理解を深め、影響を受けた資産への損害の緩和のための対策の識別、そして最終的には脆弱性と連鎖的影響の低減に寄与する。

本戦略では、公的・民間アクターを含む国内ステークホルダー間で正確かつ実行可能な情報を伝達する責任を担う、一つ以上の機構（例：CERT/CSIRT/CIRT）を指定すべきである。また、情報共有分析センター（ISAC）、情報共有分析組織（ISAO）、その他の官民連携（PPP）や協力体制といった構造化された情報共有メカニズムへの参加を促進することも考えられる。

² CERT、CSIRT、CIRT という用語は、起源や使用法に微妙な違いはあるものの、インシデント対応コミュニティ内では広く互換的に使用されている。本ガイドでは、対応チームが提供する典型的なサービス範囲を説明するために、インシデント対応・セキュリティチームフォーラム（FIRST）が開発した CSIRT サービス枠組みを参照している。 https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1。

重要なのは、情報共有は双方向のプロセスであるべきだということだ。政府事業体は、パートナーシップを示し信頼を構築するために、関連情報を提供しなければならない。それによって民間セクターの事業体も、自らの知見を共有するよう促される。この相互交換により、インシデント対応者は優先度の高い脅威に集中し続け、効果的な対応をよりよく準備できるようになる。

5.4.4 サイバーセキュリティ演習の実施

本戦略は、戦略的・運用レベルにおける国内外のサイバーセキュリティ及びインシデント対応演習の組織化と調整を促進すべきである。これらの演習はシミュレーション、机上演習、実動訓練の形態をとり、技術的・非技術的双方の関係者を巻き込むべきである。

サイバーセキュリティ演習及び関連する危機対応計画メカニズムは、各国が対応手順を検証し、コミュニケーション経路の妥当性確認を行い、必要なスキルを開発し（能力構築に関する[セクション 5.5](#) 参照）、CERT/CSIRT/CIRT がプレッシャー下でサイバーセキュリティインシデントやサービス障害に対応する運用準備態勢を評価するのに役立つ。また、セクター間の依存関係に対する理解を深め、インシデント対応のための機構的能力を育成する。

同様に、地域的・国際的なサイバーセキュリティ演習は、国境を越えたサイバーインシデント対応能力の強化、相互依存関係の理解促進、政府間の信頼構築、捜査・司法協力のための情報共有と協働の促進、集団的レジリエンスと準備態勢の強化に寄与する。

5.4.5 サイバーセキュリティインシデントの影響度・深刻度アセスメントの確立

本戦略は、サイバーセキュリティインシデントの深刻度と影響度に基づく評価・分類のための標準メカニズムの確立を促進すべきである。これらのアセスメントは、重要分野・インフラ・サービス・人口集団への潜在的・実際的影響、相互依存システム間での連鎖的影響など、サイバー関連インシデントの広範な文脈を評価することを目的とする。

アセスメントは透明性を持って協働的に実施され、幅広い関係者を巻き込むべきである。アセスメント結果は国家災害復旧計画や緊急時対応計画に統合され、国家サイバーインシデント対応枠組みに直接反映されるとともに、将来の政策改善に資するものであるべきだ。

5.5 重点分野 5 – 能力・体制構築と意識向上

技術や政策枠組みがサイバーセキュリティ議論を支配しがちだが、最終的に国のサイバーレジリエンスの有効性を決定づけるのは人的要素、スキル、意識、そして機構的能力である。この重点分野は、サイバー安全の推進、行動・意識・デジタル環境におけるサイバー衛生への対応を通じて、社会のあらゆるレベルにおけるサイバーセキュリティ能力の向上に関連する課題に取り組む。政府事業体、市民、学術界、民間セクターなど、国のデジタル経済を可能にする上で重要な主要な利害関係者の意識向上を目指し、人的・機構的開発の両方に焦点を当てる。

本セクションで検討する優良実践には、能力構築活動の戦略的計画と調整、人材育成プログラム、サイバーセキュリティ教育課程の正式な教育への統合、対象を絞った啓発キャンペーンの実施が含まれる。さらに、政府、民間部門、学術界間の研究、イノベーション、セクター横断的連携を促進することが、国家能力を強化し、サイバーセキュリティ対策の長期的な持続可能性を支える方法を本セクションは強調する。

5.5.1 能力構築と啓発活動の戦略的計画

戦略的計画は、効果的なサイバー能力構築と啓発活動の基盤である。このプロセスでは、戦略のライフサイクルを通じて国家の専門知識と人材パイプラインを強化する長期的な人的資本開発と、対象を絞った訓練や公共キャンペーンなどの短期的な能力構築活動を区別すべきだ。明確に策定された計画は、異なる主体や政府レベル間の調整、資源の最適化、説明責任を可能にする。

長期的な人的資本計画には、教育、外務、法務、労働、経済、デジタル政策などの関連省庁と国家サイバーセキュリティ機関を招集した政府全体のアプローチが必要だ。この計画策定プロセスは、将来のサイバースキル需要を識別し、国家サイバーセキュリティ人材枠組みを構築し、早期教育から大学、大学院プログラム、先端研究に至る明確な実施経路と連動した測定可能な KPI を定義する、エビデンスに基づくものであるべきだ。また、タイムライン、資金調達モデル、定期的な見直しと調整の仕組みも含める必要がある。

重要なのは、サイバーセキュリティ人材の拡充計画が、過小評価されているコミュニティ、地方や経済的に不利な立場にある人々、女性などにおける専門性の育成を通じて、包摂性とジェンダー平等を促進する機会となる点だ。これにより、能力開発機会への公平なアクセスを通じて、国家レベルのスキルギャップに対処できる。

計画策定プロセスは、短期的な能力構築イニシアチブ（幹部・実務者向け訓練、演習、シミュレーション、啓発活動、サイバーセキュリティ啓発月間関連イベントへの参加などの広報活動）の指針ともなるべきだ。これらの活動は資源集約度は低いものの、関連性を維持し、包括性を保ち、変化する脅威環境、コミュニケーション経路、公衆の行動に対応するためには戦略的な監督が必要である。これらの活動は、管轄する国家サイバーセキュリティ機関によって調整・監督され、戦略の実施期間を通じて組み込まれるべきである。

政府、学術界、民間セクターの三者連携は、人材供給と国家サイバー技能需要の均衡を図る上で不可欠である。この連携において、政府は方向性とインセンティブを提供し、学術機構と訓練プロバイダは教育と技能を供給し、民間セクターは実践的経験、イノベーション、資金支援を貢献する。この連携はまた、イノベーションと起業家精神の育成、国家エコシステムの強化、持続可能で先見性のあるサイバーセキュリティ人材の育成支援において戦略的役割を果たす。

最後に、各国の優先事項、成熟度、資源レベルには差異があるため、サイバー能力構築に万能なアプローチは存在しない。したがって収集した情報は、各国の政治的、経済的、社会的状況に適合したアプローチを設計するために活用すべきである。

5.5.2 サイバーセキュリティ教育の道筋を強化する

本戦略は、幼児教育から高等教育・職業訓練に至る全正式教育システムにおいて、サイバーセキュリティ技能開発と意識向上を加速させるための専門教育課程の整備・拡充を促進すべきである。カリキュラムは学際的かつ多分野にわたり、技術的スキルだけでなく非技術的サイバーセキュリティ技能、ならびにデジタルリテラシー、公共政策、法、ガバナンス、経済学、リスクマネジメント、倫理、社会科学、国際関係などの分野を網羅すべきである。

初等・中等教育段階では、基礎的なデジタルリテラシーの構築と安全なオンライン行動の促進に重点を置くべきである。高等教育では、より専門的で高度なプログラムを開発すべきであり、これには全てのコンピュータサイエンス及び IT プログラムへのサイバーセキュリティ科目の統合、ならびに専門的なサイバーセキュリティ学位及び見習い制度の創設が含まれる。政府、産業界、教育機構の連携による実習プログラムを開発し、正式な教育で習得した知識・技能が実務に直接適用可能で業界ニーズと整合するよう確保すべきだ。これにより、労働力の即戦力化と長期的なキャリア開発を両立させる継続的な学習サイクルを構築する。成人学習者や専門家には、変化する労働力需要に対応するための再スキル化・スキルアップに焦点を当てた柔軟な短期プログラムが必要となる場合がある。

サイバーセキュリティ教育は学際的性質を持つため、大学、短期大学、研修センターその他の教育機構は、プログラムの開発・更新にあたり、学内各部門や学術・民間セクターのステークホルダーと連携し、資源と取り組みを最適化するよう奨励されるべきである。これらの機構は、サイバーセキュリティの独自原理を労働者に教育する上で重要な役割を果たし、理論・方法論・ツール・実装を統合し、学内資源を活用して知識と実践的スキルを融合させることで、将来の労働力の育成拠点となり得る。

戦略にはサイバーセキュリティ人材フレームワークの構築も含まれる。この枠組みは、セクター横断的なサイバーセキュリティの役割・能力・研修機会の識別・開発・調整を体系化する。戦略的人材計画を支援し、教育施策を業界の現状および新興ニーズに整合させる。例えば既存の SOC や PSIRT を、運用・製品セキュリティ職を目指す学生向けの実践的研修環境やインターンシップ機会として活用できる。

さらに、カリキュラムはサイバーセキュリティ分野のキャリア機会に対する認識を高め、関心を喚起すべきである。取り組みを推進するため、政府と民間セクターは、奨学金、助成金、官民連携など様々なインセンティブ制度の創設を検討し、特に代表性の低いコミュニティを含むあらゆるレベルの学習者・研修生を支援すべきである。

5.5.3 能力開発と人材育成の促進

本戦略は、官民双方の専門家・非専門家を対象としたサイバーセキュリティ研修・技能開発スキームの構築を促進すべきである。この取り組みには、産業界と政府が識別したニーズに基づき、経営幹部・運用担当者向け研修、正式なインターンシップ・研修制度、メンター制度、セキュリティ専門家向け国内・国際認証の提供が含まれる。本戦略はまた、規制当局や立法機関を含む国内外政策に関わる国家レベルの主体に対する対象を絞った訓練を促進すべきである。訓練は、サイバーリスクマネジメントに焦点を当てた取り組みや、政府事業体内および政府事業体間、その他の利害関係者との実践的な演習（訓練やシミュレーションなど）によって補完されるべきである。

これらの取り組みは、サイバーセキュリティ分野への参入やキャリアアップを目指す専門家、公務員、業務がサイバーセキュリティと交差する非専門家など、幅広い受益者を対象とすべきである。政府、学界、民間セクター、市民社会は、主要な実施主体 および推進役として、サイバーセキュリティエコシステムの変化するニーズに応える研修の設計・提供に協力すべきである。

本戦略はまた、特に公共部門向けに、専門的なサイバーセキュリティのキャリアパスと将来の従業員の効率的な供給経路を開発する取り組みを促進し、有資格のサイバーセキュリティ専門家の供給を増やし、人材の定着を支援するインセンティブを推進すべきである。これらは学界、民間セクター、市民社会との連携で構築されるべきだ。

サイバーセキュリティ分野における継続的なジェンダー格差に対処するため、スキル開発と訓練を目的としたあらゆる取り組みにおいて、女性のより積極的な関与を動機付け、奨励し、促進するジェンダーバランスの取れたアプローチを検討すべきである。本戦略はまた、地理的に遠隔地や経済的に不利な地域に住む個人、少数派コミュニティ、障害や神経多様性を持つ人々など、他の過小評価されているグループにも届く包括的なアプローチを推進すべきである。こうした人々の多くは、未開拓の大きな潜在能力を秘めている。多様な人材を惹きつけ維持するためには、戦略は人材パイプラインのあらゆる段階におけるアクセシビリティとインクルージョンに取り組むべきである。

5.5.4 サイバーセキュリティ啓発プログラムの調整実施

国家レベルでサイバーセキュリティキャンペーンや活動を担当する事業者は、関連するステークホルダーと連携し、サイバーセキュリティリスクや脅威に関する情報、およびそれらに対抗するためのベストプラクティスの普及に焦点を当てた、データ駆動型の調整されたプログラムを開発・実施すべきである。

こうした取り組みには、銀行、通信プロバイダ、デジタル・ソーシャルメディアプラットフォームなどの民間セクターとの連携も含まれる。これらの民間セクターは、金融詐欺、フィッシング、データ・プライバシーの脅威など、自社のユーザーベースに関連する特定のサイバーセキュリティリスクについて、ターゲットを絞った啓発キャンペーンを実施するのに最適な立場にあることが多い。

5.5.5 脆弱性のある分野やグループ向けのプログラムを調整する

戦略は、サイバー能力構築と意識向上に関して特に注意を要する社会集団を識別すべきである。サイバーセキュリティ啓発プログラムは、一般市民、子供、高齢者、障害者、デジタル技術に不慣れな層、学校教員、社会福祉士、官民セクターの経営幹部など、異なる対象層に合わせた多様な取り組みを含めるべきだ。これらのプログラムは、ネットいじめ、セクハラ、オンライン安全といった問題を明確に扱う必要がある。サイバー衛生の文化、技術の責任ある利用、批判的思考力を促進し、個人がオンライン上のリスクを識別し対応する力を養うべきだ。

中小企業（エンタープライズ）、地域コミュニティ組織（CBO）、サービスが行き届いていないコミュニティや低所得コミュニティなど、特にリスクが高い、あるいは防御能力の強化が必要な分野に対しては、個別に対応したプログラムを開発すべきである。

5.5.6 サイバーセキュリティのイノベーションと研究開発（R&D）の促進

本戦略は、セクターやステークホルダーグループを横断したサイバーセキュリティ分野における基礎研究・応用研究を促進する環境を醸成すべきである。具体的には、国家 研究活動が本戦略の目標を支援するよう確保すること、公的研究機関におけるサイバーセキュリティ特化型 R&D プログラムの開発、新たな知見・基盤技術・手法・プロセス・ツールの効果的な開発・普及などが含まれる。また、効率的で競争力があり持続可能なサイバーセキュリティサービス国内市場の育成も目指すべきである。

さらに、本戦略は、若者、高齢者、中小企業、農村地域など多様な人口層に影響を与える進化するサイバーリスクに関する継続的な研究を促進し、関連性と効果を兼ね備えた対象を絞った研修プログラムやキャンペーンの設計に資すべきである。

この目的のため、政府は学界や民間セクターとの緊密な連携を促進し、ダイナミックなサイバーセキュリティエコシステムを支援すべきである。スタートアップや中小企業に対する資金調達やインキュベーションプログラムへのアクセスを含む的を絞った支援は、競争力のある国内市場の構築と、サイバーセキュリティ製品・サービスの広範な普及を確保するのに役立つ。

こうしたソリューションの開発を促進するため、戦略では助成金、調達プログラム、税額控除、コンテスト、その他革新的なサイバーセキュリティソリューション・製品・サービスの開発を促す施策を含むインセンティブメカニズムを検討すべきだ。

さらに各国は、サイバーセキュリティに関連する科学分野（コンピュータサイエンス、電気工学、応用数学、暗号学など）や、非技術分野（社会科学・政治学、経営学、犯罪学、法学、心理学など）において、国際的な研究コミュニティとの連携を構築すべきである。

5.6 重点分野 6 – 立法と規制

この重点分野は、国家サイバーセキュリティ戦略の一環として取り組むべき法的・規制の側面を扱う。戦略は、サイバーセキュリティの義務と責任を確立し、サイバー犯罪や技術の悪用から社会を防御し、包括性、基本的人権、信頼環境の原則に沿ったデジタル環境を促進する法的枠組みを求めるべきである（それぞれ[セクション 4.3](#)、[セクション 4.5](#)、[セクション 4.9](#) 参照）。法的枠組みは、少なくとも国際的・地域的・国内の人権法に基づく国の義務と整合し、以下を含むべきである：

- 国家サイバーセキュリティ当局、分野別規制機関、調整メカニズムの役割と責任を確立または明確化する。
- 重要情報インフラを指定する法的権限の付与、リスクマネジメント義務、セキュリティ管理措置、インシデント報告義務、国家インシデント報告プラットフォームの設置。
- 刑事法における実質的なサイバー犯罪の定義、及び捜査、起訴、国際協力のための手続き上の権限と保護措置の提供。
- 監査権限、是正措置、制裁、審査手続きを含む、遵守、執行、監督メカニズムを提供するプロバイダであること。
- 国境を越えた情報共有、司法共助、多国間サイバーセキュリティ調整枠組みへの参加を通じた国際協力の実現。
- 持続的な法的能力開発、規制の制度化、国際的な動向に沿った枠組みの適応に関する規定を組み込むこと。

本戦略は、政策目標と法的・規制の枠組み（運用面を含む）との関係性を明確化し、ギャップを識別するとともに、立法または規制の調整が必要な分野を示すべきである。また、基本法、二次的法規制、技術標準、業界行動規範、ガイドラインを網羅する法的枠組みの広範性を認識し、比例性、権利保護、技術的対応力、国内外の基準との整合性を確保するための定期的な見直しプロセスを定義すべきである。

5.6.1 サイバーセキュリティに関する国内法制度の枠組みの確立

本戦略は、政府、セクター規制当局、その他の関連ステークホルダーの役割分担を明確に定め、規制上の責務を定義し、責任を調整するための明確な法的権限を付与する国内法制度の構築を促進すべきである。

この法的枠組みは、重要インフラ（CI）、重要情報インフラ（CII）、重要エネルギーインフラ（ES）を指定する明確な権限を定め、事業者に対してサイバーセキュリティ義務を課すべきである。法定指定メカニズムは、こうした義務の割り当てにおいて正確性、予測可能性、比例性を確保すべきである（例：影響規準に基づく段階的義務構造。[セクション 5.2.2](#) および [セクション 5.2.3](#) 参照）。透明性のある指定規準は規則の一貫した適用を保証し、行政・司法審査手続きは事業者が明確に定義された法的経路を通じて指定への異議申し立て、規制当局の決定への異議、制裁への異議申し立てを可能にするべきである。

明確に定義された法的基盤は、限られた規制資源が国家レベルの影響を及ぼす可能性のある事業体を優先することを保証する。また、技術的先見性と適応性の原則（[セクション 4.10](#)）に沿って技術発展に対応可能であり、包括的なサイバーセキュリティ法と分野別規制制度の関係性を明確に定義し、整合性を確保するとともに、重複と規制の空白を回避すべきである。

5.6.2 サイバー犯罪と電子証拠に関する国内の枠組みの確立

本戦略は、サイバー犯罪及び関連する刑事犯罪を明確に定義し、許容される電子証拠に基づく効果的な捜査、起訴、裁判のための適切な手続き上の権限を提供する国内法制度の枠組みの整備を促進すべきである。

この枠組みは、実質的な刑事犯罪、電子証拠収集のための手続き上の権限、収集・認証・完全性・保管の連鎖・証拠採用に関する証拠規則などの側面を定義すべきである。管轄規定は、国内で犯された犯罪、国内システムに対する犯罪、国外にいる自国民による犯罪、または域外効果を伴う犯罪に対して国内法を適用することを明記し、適切に応じて属地主義、属人主義、または効果主義の原則を適用すべきである。

また、国際協力（[セクション 5.7.2](#)）の法的認可を確立すべきであり、これには司法共助、合同捜査チーム、引渡し、国際協力メカニズムへの参加が含まれる。効果的な越境執行を確保するため、国際的・地域的枠組みとの整合性を図るべきである。

さらに、サイバー犯罪の捜査・起訴に関する運用面については、専門部署の設置、デジタルフォレンジック能力の構築、標準業務手順（SOP）の策定、体系的な犯罪報告メカニズムの構築など、二次的な手段で対処することが考えられる。

5.6.3 人権と自由の認識と保護

本戦略は、サイバーセキュリティの水準に影響を与え、人権に波及効果をもたらす可能性のある技術関連の法的課題（暗号化、匿名性、責任ある脆弱性開示、倫理的ハッキングなど）に特に注意を払うべきである。その際、技術的安全対策と刑事司法対応の双方が、憲法上の原則及び適用される国際人権義務（[セクション 4.5](#)）と整合性を保つことを確保すべきである。サイバーセキュリティ（技術的・予防的措置）とサイバー犯罪（刑事司法対応）の違いを認識し、セキュリティと権利保護の適切なバランスを維持する形で対処すべきである。

NCS の一環として法的枠組みの設計において検討すべき点の一つは、正当なサイバーセキュリティ及びサイバー犯罪対策の目的でパーソナルデータの処理の方法の定義である。同時に、データ保護原則を遵守する安全措施を組み込む必要がある。データ保護規則は、調査やインシデント対応時の個人データに対する不法なアクセス・利用からの保護、及び適切な取り扱いを確保するため、サイバーセキュリティ及び法執行の枠組みに統合されるべきである。

捜査権限に対する保護措置は、司法または独立した機関による認可を必要とし、必要性和比例性の原則に基づくべきである。また、国家による監視や捜査措置の影響を受けた個人に対して、効果的な法的救済手段を提供しなければならない。サイバー犯罪立法に関する戦略的検討では、当局が重大な犯罪を捜査・起訴するための合法的な手段を確立すると同時に、過度に広範な監視、政治的動機による起訴、またはプライバシー権の侵害を防ぐための手続き上の保護を組み込むべきである。本戦略の法的考察では、倫理的ハッキング、侵入テスト、調整された脆弱性開示、セキュリティ研究など、より安全なデジタル環境の構築に寄与する正当なサイバーセキュリティ活動の犯罪化を防ぐ方法も検討すべきである。

5.6.4 コンプライアンス体制の構築

本戦略は、サイバーセキュリティ及びサイバー犯罪に関する法的枠組みが効果的に実施・執行されるよう、コンプライアンス、執行、監督メカニズムの確立を促進すべきである。立法は、法定義務を明確かつ監査可能な要件に変換し、規制対象事業体に対する法的確実性を維持し、機構の責任を保持し、執行措置に異議を申し立てるための明確な法的手段を提供すべきである。

枠組みは、監査、検査、コンプライアンス監視、インシデント対応のレビューを実施し、是正期限付きの是正命令を発出し、比例した行政的、財政的、または運営上の制裁を課すための監督権限を管轄当局に付与すべきである。

監督権限は、重複、分断、または矛盾する要件を防止するため、国家サイバーセキュリティ当局、セクター別規制機関、調整団体の間で明確に配分されるべきである。

執行決定が法的・経済的に及ぼす潜在的影響を考慮し、手続き上の保障措置により透明性、比例性、公平性を確保すべきである。これには、明確な行政不服審査手続（）、司法審査の選択肢、制裁の正当性・合理性を評価する法的標準が含まれる。

執行は、自主的な報告やセクター間の情報共有を促進するインセンティブとバランスを取るべきである。タイムリーかつ誠実なインシデント開示のためのセーフハーバー規定、共有された脅威インテリジェンスの機密性保護、執行機能と協力的な情報共有機能（CERT/CIRT/CSIRT、SOC、ISAC/ISAO、PSIRT など）の明確な分離は、説明責任を確保しながら、信頼の維持と協力の促進に役立つ。

5.6.5 法の調和と国境を越えた協力の促進

この戦略は、サイバーセキュリティの越境的側面を認識し、国際協力協定の批准を検討し、各国の法的枠組みを国際協力標準に整合させることを奨励すべきである。共有標準は、複数の管轄区域にまたがる越境データ共有やサイバーセキュリティの取り組みにおいて、法的確実性および国益と優先事項の保護を支援する。

法的枠組みは、国内の権限と国家安全保障上の優先事項を守りつつ、構造化された国際協力に従事するための明確な権限を国家当局に付与すべきである。これらの規定は、タイムリーな情報共有を可能にし、守秘義務およびデータ保護規則の下で共有データの一貫した取り扱いを確保すべきである。また、司法共助や国境を越えた捜査を促進し、サイバーセキュリティインシデントへの協力的対応を支援し、管轄権の紛争を解決するためのメカニズムを提供すべきである。

さらに、本戦略は、欧州評議会サイバー犯罪条約（ブダペスト条約）、国連サイバー犯罪防止条約（2024年）、OECD 勧告、司法共助条約（MLAT）、その他の関連枠組みなど、地域的・国際的な手段との国内法の調和を促進すべきである。こうした統合は、法的・運用上の整合性を確保し、断片的な立法、規制間の義務の重複、あるいは機構や規制対象事業体の行政・技術的能力を超える権限付与を避けるため、慎重な制度的調整を経て行われるべきである。

5.7 重点分野 7 – 国際協力

この重点分野では、二国間、地域、国際レベルにおける国の対外的なサイバーセキュリティ関与に関して、本戦略がカバーすべき要素を強調する。二国間レベルでは、例えば情報共有、インシデント対応、サイバー能力構築などに関して、主要パートナー国とのサイバー協力協定の締結が考えられる。地域レベルでは、サイバーセキュリティ関連の問題に取り組む関連地域組織や枠組みへの積極的な参加を検討すべきである。国際レベルでは、国連、標準団体、政府間またはマルチステークホルダーのプラットフォームなどの国際機関との関わりが不可欠である。こうした取り組みには、官民パートナーシップも含まれる。民間セクターの関係者（ウイルス対策会社、SOC、PSIRT、ISAC/ISAO、脅威情報コミュニティ、ソーシャルメディアプロバイダ、グローバルデジタルプラットフォームなど）との協力は、国際協力の重要な要素として認識されるべきである。

デジタル化は、人権、経済社会開発、貿易交渉、商業関係、新興および破壊的技術の開発と利用、サプライチェーンのセキュリティ、安定、平和、紛争解決といったより広範な問題など、国際関係のあらゆる分野に影響を与えているため、サイバーセキュリティは、各国の外交政策に欠かせない要素となっている。したがって、本戦略はサイバーセキュリティの境界を越えた性質と国際的側面を認識し、国際的な議論への参加や、国家・地域・国際的なステークホルダー、市民社会、産業界、非政府組織、学術界との協力の必要性を強調すべきである。

その際、戦略は既存の地域的・国際的枠組みを考慮し、分断を防止し、優良実践を活用し、国境を越えた協力を促進すべきである。国際的な官民ステークホルダーとの関与は、建設的な対話の促進、信頼と協力メカニズムの構築、相互に受け入れ可能な解決策の模索、共通課題への対応、そしてサイバーセキュリティとレジリエンスの重要性に関する世界的な理解の醸成において鍵となる。地域および国際協力は、包括的アプローチと個別対応の優先事項という原則に沿い（[セクション 4.2](#)）、国の政治的、社会的、文化的、経済的優先事項と調和して促進されるべきである。

5.7.1 サイバーセキュリティを外交政策の一要素と認識し、国内と国際的な取り組みを整合させる

戦略は、政府の優先分野を明確に述べ、国際協力に関する長期目標を示すべきである。これには、どのステークホルダー（例：公共、民間、地域、グローバル）が関与すべきかも含まれる。

戦略は、サイバーセキュリティに関する国際協力へのコミットメントを表明し、サイバーセキュリティ問題を、国際平和と安全保障、貿易交渉、サイバー犯罪、サイバー能力構築（CCB）を含む関連するすべての分野における国家の外交政策の不可欠な構成要素として認識すべきである。

さらに、戦略は国内政策と外交政策の整合性を確保し、国家のサイバーセキュリティアプローチを国際的取り組みと整合させるべきである。これには、国際法上の義務と約束を反映した政策の採用や国内法体系の調和が含まれる。具体的には、国際的なサイバーセキュリティ規範と信頼醸成措置（CBM）への支援、CCB への取り組み、国際サイバーセキュリティ標準策定への参加、既存の地域・国際プロセスへの参加などが挙げられる。

これには、国家元首や内閣、外務省、デジタル化（またはデジタル変革）省、産業貿易省、法務省、防衛省、国家 CERT/CSIRT/CIRT、その他国家安全保障・サイバー・デジタル分野を担当する機構など、異なる政府事業体間の調和（政府全体アプローチ）も必要となる場合がある。これにより、国際的な交渉の場で、事業体が表明する立場が、政府全体で適切に調整され、整合性が保たれる。

5.7.2 国際的な議論への参加と実施へのコミットメント

本戦略は、サイバー関連課題に効果的に関与するため、二国間・地域・国際レベルで参加または協力する具体的な国際フォーラム及び協力メカニズムを識別すべきである。国連憲章、国際人道法、国際人権法を含む、サイバー空間への国際法の適用に対する国のコミットメントを再確認し、国際法がこの領域にどのように適用されるかに関する国家見解を概説してもよい。

本戦略は、サイバー犯罪対策やその他のサイバー脅威への対応を目的とした既存の地域的・国際的枠組み（欧州評議会サイバー犯罪条約（ブダペスト条約）、国連サイバー犯罪条約、関連する地域条約など）への参加及び実施を約束すべきである（[セクション 5.6.5](#)）。また、多くの国際貿易協定がデジタル/サイバー関連条項（例：越境データ流通、デュアルユース技術）を含んでいることを認識すべきである。

約束事項には、国連総会が承認した ICT 利用における責任ある国家行動に関する国連枠組みの実施が含まれる可能性がある。この枠組みは規範、信頼醸成措置（CBM）、共通行動基準（CCB）を包含する。また本戦略は、国際安全保障における ICT に関する国連グローバル・メカニズムなど、他の関連する地域的・国際的プロセスへの参加を強調する可能性がある。グローバル・メカニズムは、国家主導の恒久的な仕組みであり、開放的で安全かつ安定し、アクセス可能で平和的な ICT 環境の促進を目的とする。

信頼性を確保するため、戦略は測定可能な目標を強調し、十分な資源（人的・財政的）を割り当て、国際的関与の任務を定義し、結果を評価するための説明責任メカニズムを確立すべきである。

5.7.3 サイバー空間における公式および非公式の協力を促進する

この戦略は、国が関与しようとする、公共部門と民間部門にわたる公式および非公式の国際協力メカニズムの両方を強調すべきである。公式の協力とは、政策、立法、法執行に関する協力を促進する、条約、協定、制度的パートナーシップなど、構造化された、多くの場合法的拘束力のある取り決めを指す（例：INTERPOL、WIPO）。非公式の協力とは、より柔軟で信頼に基づくネットワークであり、法的拘束力のない、自発的な情報や専門知識の交換を可能にするものである。例えば、マルチステークホルダー・フォーラム（GFCE、IGF など）、インシデント対応及び脅威共有メカニズム（例：FIRST、ISAC、ISAO、SOC-CSIRT ネットワーク、国際安全保障における ICT 利用に関する政府間連絡窓口グローバルディレクトリ）、並びに地域的な信頼構築イニシアチブである。これらの取り組みへの参加は、関連当局間の調整強化、情報交換の迅速化、脅威や脆弱性への協調的対応を促進する。また、この戦略は、国際協力を促進するための法的枠組みの強化も支援すべきである（[セクション 5.6.5](#)）。

5.7.4 国際協力のための能力構築の促進

国がサイバー空間に関連する国際的な取り組みを行うにつれて、サイバー外交、国際法、データ保護とプライバシー、貿易、新興および破壊的技術、サプライチェーンのセキュリティ、その他のデジタル問題に関する専門知識を含め、関連するすべての政府団体にわたって能力とスキルを開発または拡大する必要がある。

国際的な議論や協力を効果的に関与するためには、政府内にサイバー外交の専門能力を開発することを奨励すべきである。例えば、専門事務所を設立し、サイバー外交官を任命し、あるいは既存の政府機関や省庁内に訓練を受けた担当者を指定するなどの方法がある。これらの担当者は、国際フォーラムに参加し、サイバー関連の問題について交渉し、国境を越えたサイバーセキュリティの協力を調整する能力を備えているべきである。

その他の能力構築の優先事項としては、国家 CERT/CSIRT/CIRT の国際協力能力強化、法執行・司法協力の強化、サイバー空間における国際法・規範適用スキルの構築、国際サイバー演習への参加などが挙げられる。各国政府は、既存の国際能力構築プログラム（GLACY+、グローバル・サイバー専門知識フォーラム（GFCE）、インターポール等）を活用してこれらの能力を開発すべきである。例えば、法執行能力構築の取り組みは、地方及び国家の法執行機関が、国境を越えたサイバー犯罪の防止、検知、捜査、起訴のためにハイテクツールやシステムを活用するスキル、知識、技術的能力を向上させるのに役立つ。また、法執行機関がサイバー犯罪の動向や絶えず進化する脅威の状況を把握し、犯罪に先んじることを可能にする。

本戦略はまた、国際的なパートナーとの相互学習、知識・技能移転を促進し、国際的なサイバーセキュリティ演習や越境インシデント対応訓練への参加を、能力構築と信頼醸成の両面での措置として重視すべきである。

6 参考資料

本ガイド作成にあたり、我々は世界各国の既存ガイド、枠組み、優良実践を精査した。このプロセスにより、各国が国家サイバーセキュリティ戦略の設計、実施、維持を支援できる多様なリソースを識別できた。

本セクションではこれらの参考資料を包括的なカタログとしてまとめ、読者が本ガイドで議論された原則、概念、アプローチをより深く探求し、自国の状況に応用できるようにする。網羅的ではないものの、このコレクションは政策立案者、実務者、研究者が基盤として活用できる強固な土台を提供し、新たに利用可能なリソースの継続的な探求を促すものである。

本ガイドの最新版では、参考資料セクションがウェブサイト (www.ncsguide.org) で公開されており、簡便なアクセスと保守により参考資料を最新の状態に保つことが可能である。

参考資料セクションは www.ncsguide.org で閲覧可能。

7 略語一覧

略語	Definition	定義
AI	Artificial Intelligence	人工知能
AU	African Union	アフリカ連合
BIAs	Business Impact Analyses	事業影響分析
C3SA	Cybersecurity Capacity Centre for Southern Africa	南部アフリカサイバーセキュリティ能力センター
CBA	Cost-Benefit Analysis	費用便益分析
CBMs	Confidence-Building Measures	信頼醸成措置
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	NATO サイバー防衛協力センター
CCB	Cyber Capacity-Building	サイバー能力構築
CBOs	Community-Based Organizations	コミュニティベースの組織
CERTs	Computer Emergency Response Teams	コンピュータ緊急対応チーム
CII	Critical Information Infrastructure	重要情報インフラ
CIRTs	Computer Incident Response Teams	コンピュータインシデント対応チーム
CISRTs	Computer Security Incident Response Teams	コンピュータセキュリティ・インシデント対応チーム
CI	Critical Infrastructure	重要インフラ
CoE	Council of Europe	欧州評議会
CRI	Cybercrime Research Institute	サイバー犯罪研究所
CTO	Commonwealth Telecommunications Organisation	英連邦電気通信機構
DCAF	Geneva Centre for Security Sector Governance	ジュネーブ安全保障分野ガバナンスセンター
Diplo	DiploFoundation	ディプロ財団
EBRD	European Bank for Reconstruction and Development	欧州復興開発銀行
eGA	e-Governance Academy	e ガバナンスアカデミー
ENISA	European Union Agency for Cybersecurity	欧州連合サイバーセキュリティ機関
ES	Essential Services	重要サービス
EU CyberNet	European Union CyberNet	欧州連合サイバーネット
FIRST	Forum of Incident Response and Security Teams	インシデント対応・セキュリティチームフォーラム

GCSCC	Global Cyber Security Capacity Centre	グローバルサイバーセキュリティ能力センター
GFCE	Global Forum on Cyber Expertise	グローバル・サイバー専門知識フォーラム
GLACY+	Global Action on Cybercrime Extended	サイバー犯罪対策グローバル行動（拡張版）
GPD	Global Partners Digital	グローバル・パートナーズ・デジタル
ICCs	International Coordinating Committees	国際調整委員会
ICT	Information and Communication Technology	情報とコミュニケーション技術
IADB	Inter-American Development Bank	米州開発銀行
IFIs	International Financial Institutions	国際金融機関機構
IGO	Intergovernmental Organization	政府間組織
IGF	Internet Governance Forum	インターネットガバナンスフォーラム
IMF	International Monetary Fund	国際通貨基金
INTERPOL	International Criminal Police Organization	国際刑事警察機構
IoT	Internet of Things	モノのインターネット
ISACs	Information Sharing and Analysis Centers	情報共有・分析センター
ISAOs	Information Sharing and Analysis Organizations	情報共有・分析組織
IT	Information Technology	情報技術
ITU	International Telecommunication Union	国際電気通信連合
IXPs	Internet Exchange Points	インターネットエクスチェンジポイント
KPIs	Key Performance Indicators	主要業績評価指標
LFA	Logical Framework Approach	論理的枠組みアプローチ
MDBs	Multilateral Development Banks	多国間開発銀行
MLATs	Mutual Legal Assistance Treaties	相互司法共助条約
NCS	National Cybersecurity Strategy	国家サイバーセキュリティ戦略
OAS	Organization of American States	米州機構
OECD	Organisation for Economic Co-operation and Development	経済協力開発機構
PPP	Public-Private Partnerships	官民連携
PSIRTs	Product Security Incident Response Teams	製品セキュリティインシデントレスポンスチーム
R&D	Research & Development	研究開発
SCADA	Supervisory Control and Data Acquisition	監視制御とデータ収集
SLA	Service Level Agreement	サービスレベル契約

SMART	Specific, Measurable, Achievable, Relevant, Time-related	具体的、測定可能、達成可能、関連性、時間的制約
SMEs	Small- and Medium-Sized Enterprises	小・中規模エンタープライズ
SOCs	Security Operations Centers	セキュリティ・オペレーションセンター
ToC	Theory of Change	変化の理論
UNDP	United Nations Development Programme	国連開発計画
UNICRI	United Nations Interregional Crime and Justice Research Institute	国連地域間犯罪司法研究所
UNIDIR	United Nations Institute for Disarmament Research	国連軍縮研究所
UNOCT	United Nations Office of Counter-Terrorism	国連テロ対策室
UNODA	United Nations Office for Disarmament Affairs	国連軍縮局
UNODC	United Nations Office on Drugs and Crime	国連薬物犯罪事務所
UNU	United Nations University	国連大学
WB	World Bank	世界銀行
WEF	World Economic Forum	世界経済フォーラム
WIPO	World Intellectual Property Organization	世界知的所有権機関