
Sec20-01_ サイバーセキュリティ戦略および
サイバーセキュリティ2021
1. 概要
改版履歴
2021年12月17日 改訂 4.4
横断的施策の追加
2021年10月7日 初版
2. サイバーセキュリティ戦略
資料要約の趣旨
中小企業におけるサイバーセキュリテ
ィ対策の取組のため、特に中小企業に
関連する記述部分を抜粋した。
次期サイバーセキュリティ戦略の課題と方向性
課題認識と方向性
－デジタルトランスフォーメーション
とサイバーセキュリティの同時推進－
→デジタル経営に向けた行動指針の実
践を通じ、サイバーセキュリティ経営
のガイドラインに基づく取組の可視化
・インセンティブ付けを行い、更なる
取組を促進
① 経営層の意識改革
→地域のコミュニティの推進・発展、
中小企業向けサービスの審査登録制度
を通じ、デジタル化に当たって直面す
る知見や人材等の不足に対応
②地域・中小企業におけるDX with
Cybersecurityの推進
→Society5.0に対応したフレームワー
ク等も踏まえ、各種取組を推進。
－サプライチェーン：
産業界主導のコンソーシアム
経済社会の活力の向上及び持続的発展
主な具体的施策

エーン等の信頼性確保に向けた基盤づくり

データマネジメントの定義、「トラストサービス」によるデータ信頼性確保

－セキュリティ製品・サービス：第三者検証サービスの普及

－先端技術 ：情報収集・蓄積・分析・提供等の共通基盤構築

④誰も取り残さないデジタル／セキュリティ・リテラシーの向上

→情報教育推進の中、「デジタル活用支援」と連携して、各種取組を推進

課題認識と方向性 －
公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心確保 －

●サイバー空間の公共空間化、相互連関・連鎖の深化、サイバー攻撃の組織化・洗練化。

国は、様々な主体と連携しつつ、①自助・共助による自律的なリスクマネジメントが講じられる環境づくりと、②持ち得る手段の全てを活用した包括的なサイバー防御の展開等を通じて、サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築し、国全体のリスク低減、レジリエンス向上を図る。

主な具体的施策（１）国民・社会を守るためのサイバーセキュリティ環境の提供

①安全・安心なサイバー空間の利用環境の構築

●サプライチェーン管理のためのガイドライン策定や産業界主導の取組、IoT、5G等の新技術実装に伴う安全確保

●利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討

②新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）

●政府機関・重要インフラ事業者等向けにクラウド利用の際に考慮すべきセキュリティルール策定

●ISMAPの取組等の民間展開による一定のセキュリティが確保されたクラウド利用の促進

●信頼性が高く、オープンかつ使いやすい高品質クラウドの整備の推進

③ サイバー犯罪への対策

●サイバー空間を悪用する犯罪者やトレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等の摘発を推進し、実空間と変わらぬ安全・安心を確保

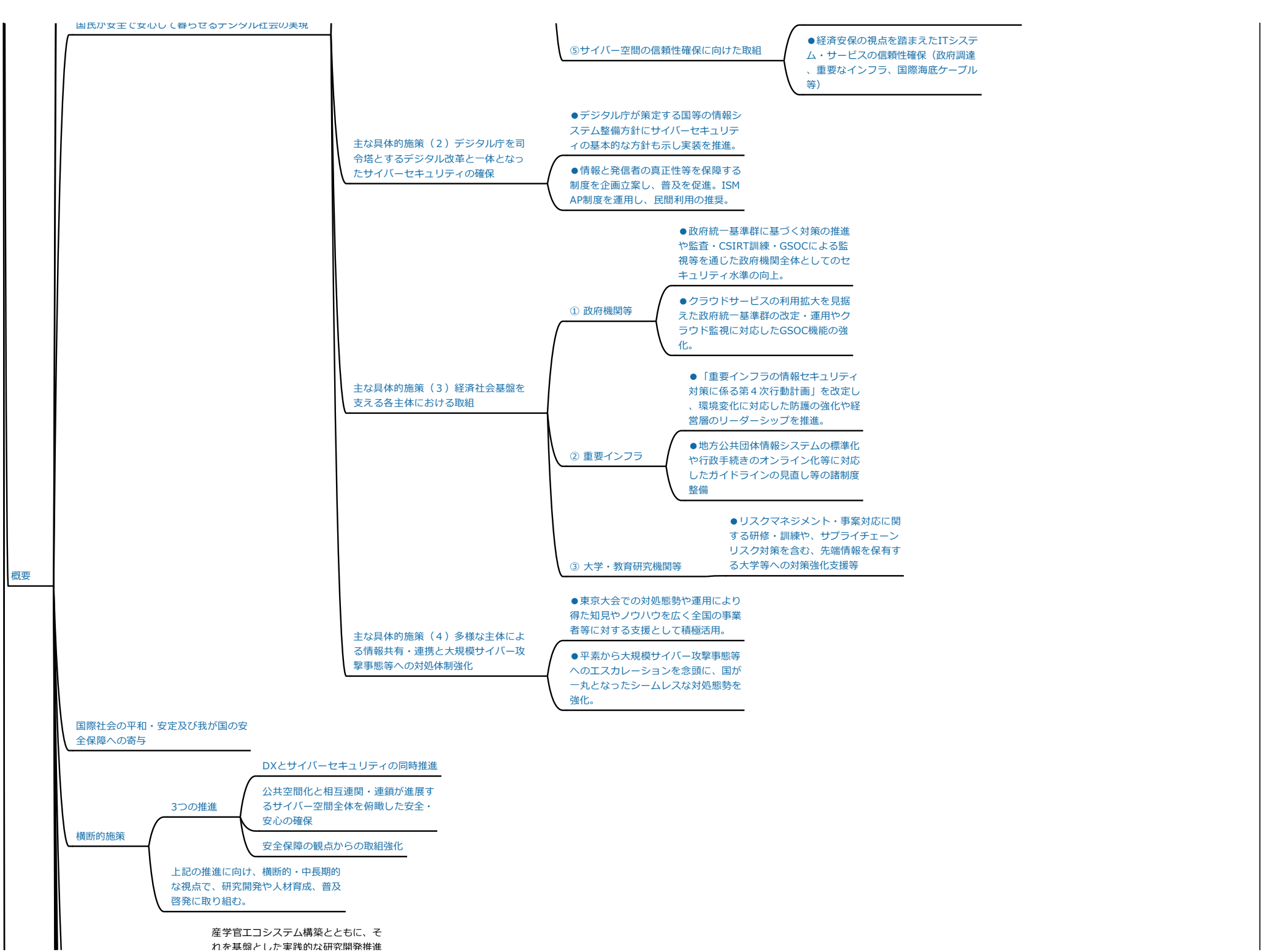
●警察におけるサイバー事案対処体制の強化

④ 包括的なサイバー防御の展開

●サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化（対処官庁のリソース結集と連携強化、サイバーセキュリティ協議会等の関係機関との連携による官民連携・国際連携強化）

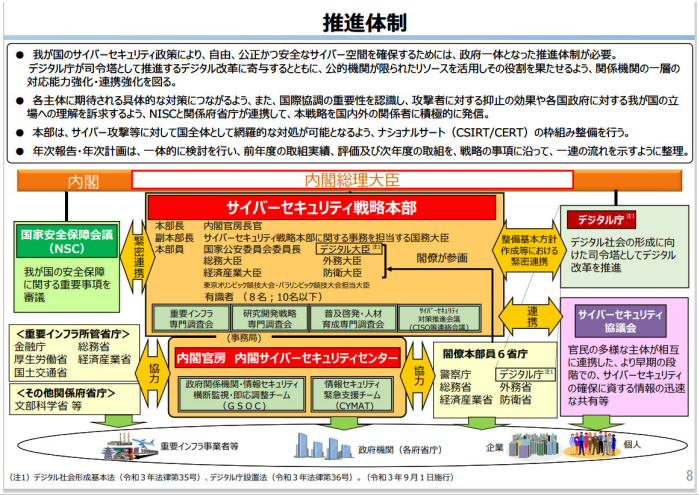
●包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）

●個人情報や知的財産を保有する主体への支援


概要
国民が安全で安心して暮らせるデジタル社会の実現
主な具体的施策（２）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保
●デジタル庁が策定する国等の情報システム整備方針にサイバーセキュリティの基本的な方針も示し実装を推進。
●情報と発信者の真正性等を保障する制度を企画立案し、普及を促進。ISMAP制度を運用し、民間利用の推奨。
主な具体的施策（３）経済社会基盤を支える各主体における取組
① 政府機関等
●政府統一基準群に基づく対策の推進や監査・CSIRT訓練・GSOCによる監視等を通じた政府機関全体としてのセキュリティ水準の向上。
●クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能の強化。
② 重要インフラ
●「重要インフラの情報セキュリティ対策に係る第４次行動計画」を改定し、環境変化に対応した防護の強化や経営層のリーダーシップを推進。
●地方公共団体情報システムの標準化や行政手続きのオンライン化等に対応したガイドラインの見直し等の諸制度整備
③ 大学・教育研究機関等
●リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策を含む、先端情報を保有する大学等への対策強化支援等
⑤サイバー空間の信頼性確保に向けた取組
●経済安保の視点を踏まえたITシステム・サービスの信頼性確保（政府調達、重要なインフラ、国際海底ケーブル等）
主な具体的施策（４）多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化
●東京大会での対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用。
●平素から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化。
国際社会の平和・安定及び我が国の安全保障への寄与
横断的施策
3つの推進
DXとサイバーセキュリティの同時推進
公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
安全保障の観点からの取組強化
上記の推進に向け、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組む。
産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進

。中長期的な技術トレンドも視野に対応。

- 1．研究開発の推進
  - (1)国際競争力の強化－産学官エコシステムの構築
  - (2)実践的な研究開発の推進
  - (3)中長期的な技術トレンドを視野に入れた対応
- 2．人材の確保、育成、活躍促進
  - 「質」・「量」両面での官民の取組を一層継続・深化させつつ、環境変化に対応した取組の重点化。官民を行き来しキャリアを積める環境整備も。
  - (1)DX with Cybersecurityの推進
    - ・「プラス・セキュリティ」知識を補充できる環境整備
    - ・機能構築・人材流動に関するプラクティス普及等(xSIRT、副業・兼業等)
  - (2)巧妙化・複雑化する脅威への対処
    - ・人材育成プログラムの強化
      - SecHack365 / CYDER / enPiT
      - ICSCoE中核人材育成プログラム 等
    - ・人材育成共通基盤の構築・産学への開放
    - ・資格制度活用に向けた取組
  - (3)政府機関における取組－外部高度人材活用の仕組み強化
    - 「デジタル区分」合格者の積極採用、研修の充実・強化
- 3．全員参加による協働、普及啓発
  - デジタル化推進を踏まえ、アクションプランの推進・改善、高齢者への対応を含め見直しの検討
- 推進体制



「次期サイバーセキュリティ戦略」（案）の構成

「Cybersecurity for All」を踏まえた対応の強化

特筆すべき用語
- Cybersecurity for All
- DX with Cybersecurity
- セキュリティ・バイ・デザイン

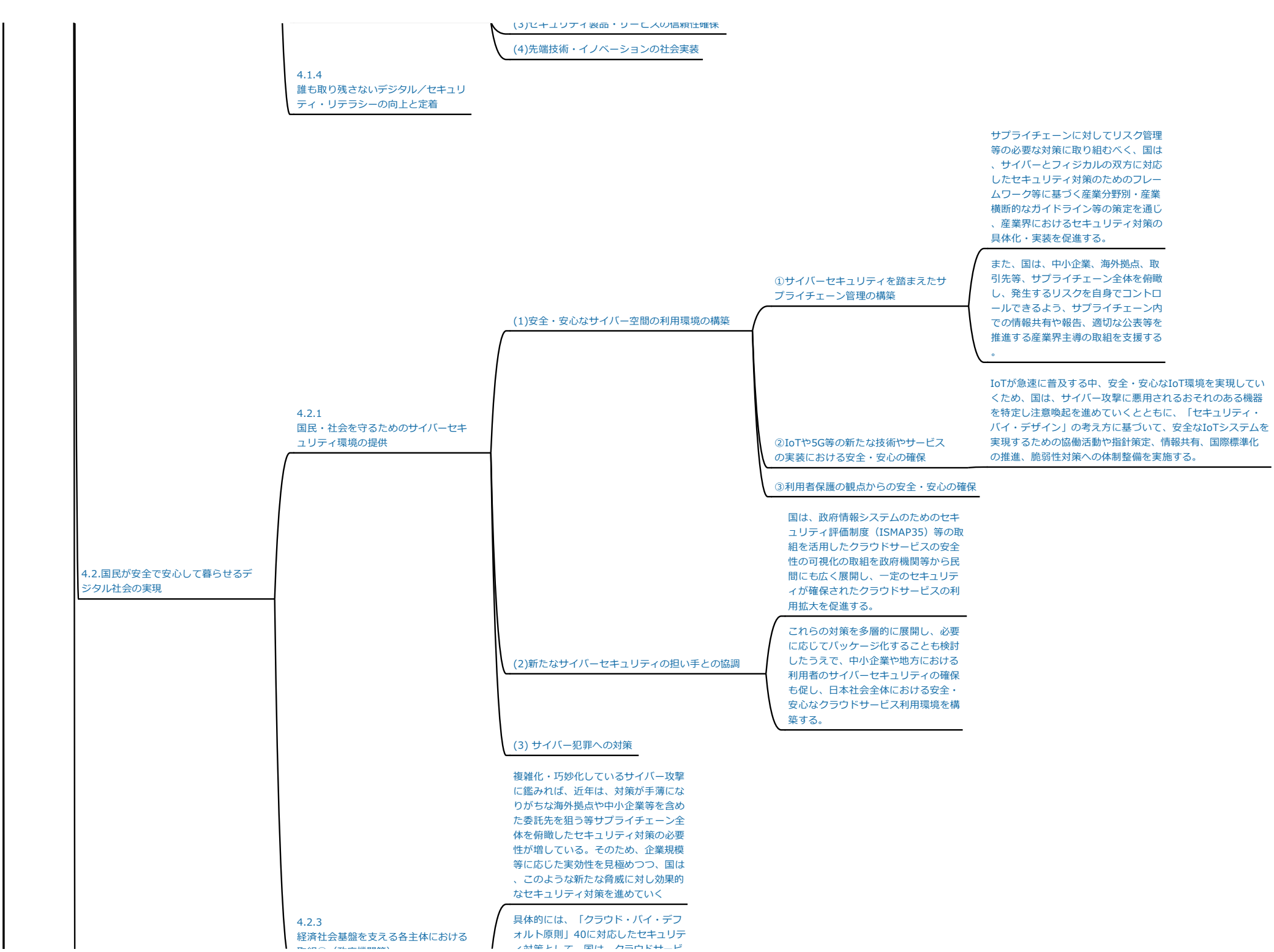
本文抜粋（要約）

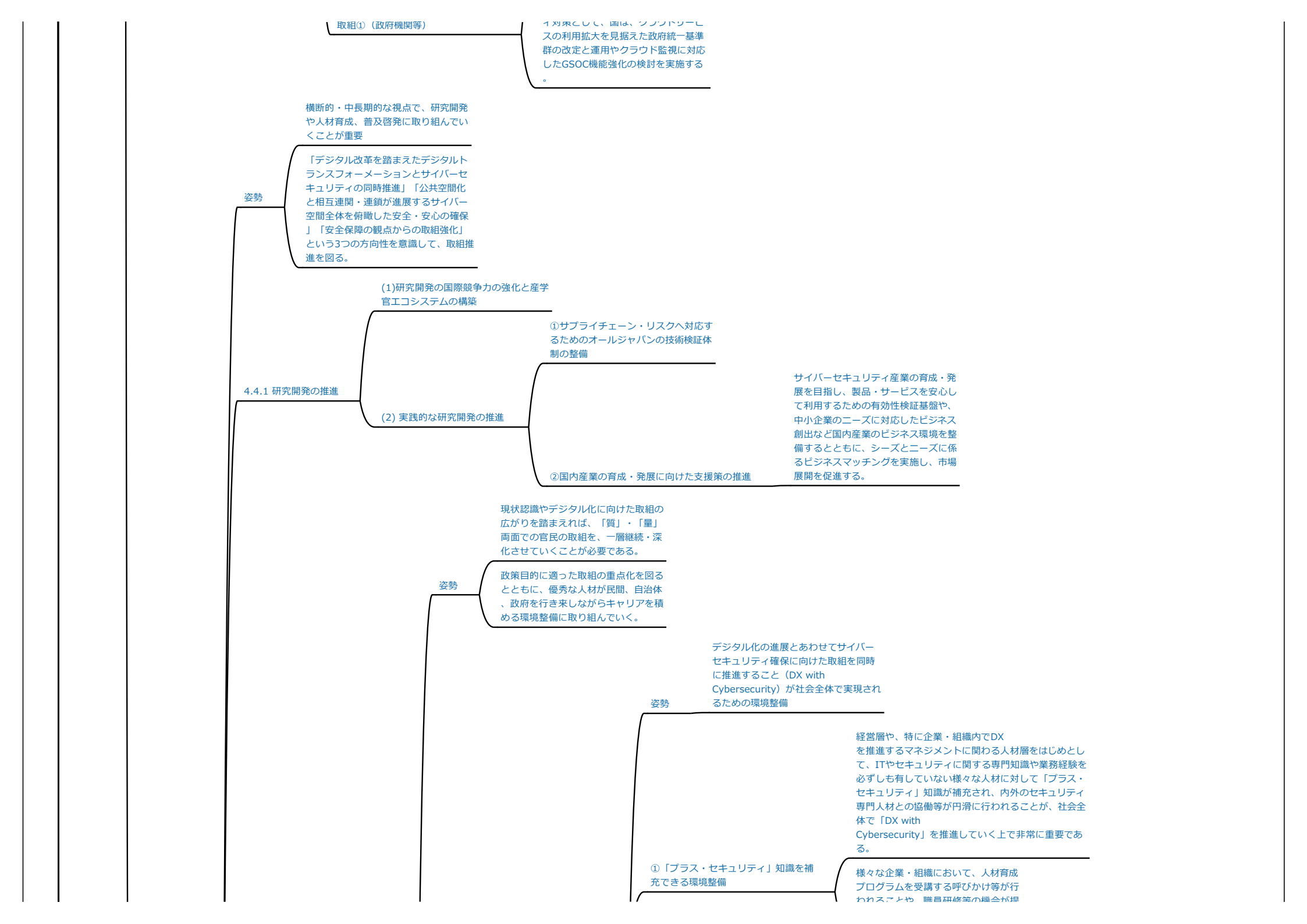
4. 目的達成のための施策
～Cybersecurity for All～

<3 つの方向性>
- (1)デジタル改革を踏まえたデジタルトランスフォーメーション24とサイバーセキュリティの同時推進
- (2)公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
  - ①「任務保証」の深化（エンドユーザへのサービスの確実な提供を意識したサプライチェーン全体の信頼性確保）
  - ②「リスクマネジメント」に係る取組強化
- (3) 安全保障の観点からの取組強化

社内外のセキュリティ専門家と協働するに当たって必要な知識として、時宜に応じてプラスして習

- 4.1.経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity の推進～
  - 4.1.1 経営層の意識改革
    - 得すべき知識（以下「『プラス・セキュリティ』知識」という。）を補充できる環境整備を推進する。
    - コロナ禍への対応を余儀なくされること等を通じ、ビジネスモデルの変革や働き方・雇用形態のあり方にも変化が及ぶ中で、デジタル化の機会は、地域・中小企業、そしてサイバー空間とは繋がりのなかった業種・業態の企業にも例外なく広がっていくと想定される。
  - 4.1.2 地域・中小企業における DX with Cybersecurity の推進
    - 一方で、中小企業がデジタル化と同時にサイバーセキュリティ対策に取り組むに当たっては、セキュリティ専任の人材を配置できないなど、知見や人材等のリソース不足に直面しており、これらの課題への対処が必要である。
    - また、中小企業においては、セキュリティに多額の予算を割くことが難しいという課題もあるところ、中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策の推進に取り組む。
    - 具体的には、中小企業を含むサプライチェーン全体のサイバーセキュリティ強化を目的として設立された産業界主導のコンソーシアムとも連携しつつ、一定の基準を満たすサービスに商標使用権を付与するための審査・登録、セキュリティ対策の自己宣言等の取組を推進するとともに、中小企業向け補助金における自己宣言等の要件化等を通じたインセンティブ付けに取り組む。これらの取組を通じ、サイバーセキュリティ強化に向けた取組状況が取引先等に対して可視化されることで、地域・中小企業に取組を広げる契機となることが期待される。
    - 加えて、今後は、中小企業に広くクラウドサービスの利用が普及することも一つの重要な選択肢となると想定される。その利用に当たっては、情報資産が企業外に置かれることに加え、設定の不備等により意図せず流出するリスクも一定程度伴うことから、クラウドサービス利用者が留意すべき事項に関する手引き等の周知に取り組むとともに、クラウドサービス利用時の設定ミスの防止・軽減のため、クラウドサービス事業者に、利用者に対する情報提供やツールの提供等の必要なサポートの提供を促す方策等を検討する。
  - 4.1.3 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり
    - (1) サプライチェーンの信頼性確保
    - (2) データ流通の信頼性確保
    - (3)セキュリティ製品・サービスの信頼性確保


(3)セキュリティ製品・サービスの信頼性確保
(4)先端技術・イノベーションの社会実装
4.1.4
誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着
サプライチェーンに対してリスク管理等の必要な対策に取り組むべく、国は、サイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等に基づく産業分野別・産業横断的なガイドライン等の策定を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。
また、国は、中小企業、海外拠点、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、サプライチェーン内での情報共有や報告、適切な公表等を推進する産業界主導の取組を支援する。
①サイバーセキュリティを踏まえたサプライチェーン管理の構築
IoTが急速に普及する中、安全・安心なIoT環境を実現していくため、国は、サイバー攻撃に悪用されるおそれのある機器を特定し注意喚起を進めていくとともに、「セキュリティ・バイ・デザイン」の考え方に基づいて、安全なIoTシステムを実現するための協働活動や指針策定、情報共有、国際標準化の推進、脆弱性対策への体制整備を実施する。
②IoTや5G等の新たな技術やサービスの実装における安全・安心の確保
③利用者保護の観点からの安全・安心の確保
(1)安全・安心なサイバー空間の利用環境の構築
国は、政府情報システムのためのセキュリティ評価制度（ISMAP35）等の取組を活用したクラウドサービスの安全性の可視化の取組を政府機関等から民間にも広く展開し、一定のセキュリティが確保されたクラウドサービスの利用拡大を促進する。
これらの対策を多層的に展開し、必要に応じてパッケージ化することも検討したうえで、中小企業や地方における利用者のサイバーセキュリティの確保も促し、日本社会全体における安全・安心なクラウドサービス利用環境を構築する。
(2)新たなサイバーセキュリティの担い手との協調
(3) サイバー犯罪への対策
4.2.1
国民・社会を守るためのサイバーセキュリティ環境の提供
4.2.国民が安全で安心して暮らせるデジタル社会の実現
複雑化・巧妙化しているサイバー攻撃に鑑みれば、近年は、対策が手薄になりがちな海外拠点や中小企業等を含めた委託先を狙う等サプライチェーン全体を俯瞰したセキュリティ対策の必要性が増している。そのため、企業規模等に応じた実効性を見極めつつ、国は、このような新たな脅威に対し効果的なセキュリティ対策を進めていく
具体的には、「クラウド・バイ・デフォルト原則」40に対応したセキュリティ
4.2.3
経済社会基盤を支える各主体における


取組①（政府機関等）
イ対策として、国は、クラウドサービスの利用拡大を見据えた政府統一基準群の改定と運用やクラウド監視に対応したGSOC機能強化の検討を実施する。
横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組んでいくことが重要
姿勢
「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」「安全保障の観点からの取組強化」という3つの方向性を意識して、取組推進を図る。
4.4.1 研究開発の推進
(1)研究開発の国際競争力の強化と産学官エコシステムの構築
①サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備
(2) 実践的な研究開発の推進
サイバーセキュリティ産業の育成・発展を目指し、製品・サービスを安心して利用するための有効性検証基盤や、中小企業のニーズに対応したビジネス創出など国内産業のビジネス環境を整備するとともに、シーズとニーズに係るビジネスマッチングを実施し、市場展開を促進する。
②国内産業の育成・発展に向けた支援策の推進
現状認識やデジタル化に向けた取組の広がりを踏まえれば、「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要である。
姿勢
政策目的に適った取組の重点化を図るとともに、優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境整備に取り組んでいく。
デジタル化の進展とあわせてサイバーセキュリティ確保に向けた取組を同時に推進すること（DX with Cybersecurity）が社会全体で実現されるための環境整備
姿勢
経営層や、特に企業・組織内でDXを推進するマネジメントに関わる人材層をはじめとして、ITやセキュリティに関する専門知識や業務経験を必ずしも有していない様々な人材に対して「プラス・セキュリティ」知識が補充され、内外のセキュリティ専門人材との協働等が円滑に行われることが、社会全体で「DX with Cybersecurity」を推進していく上で非常に重要である。
①「プラス・セキュリティ」知識を補充できる環境整備
様々な企業・組織において、人材育成プログラムを受講する呼びかけ等が行

- 4.4. 横断的施策
  - 4.4.2 人材の確保、育成、活躍促進
    - (1)「DX with Cybersecurity」に必要な人材に係る環境整備
      - ②企業・組織内での機能構築、人材の流動性・マッチングに関する取組
        - 供されることが重要である
        - 迅速で柔軟な開発・対処、新たなリスクに対応した監視・対処のプラクティスが必要となる。特に、前者の実践に当たっては「セキュリティ・バイ・デザイン」の考え方の重要性も一層増し、企画部門や開発運用部門と企業・組織内のセキュリティ機能との連携・協働が一層重要となると考えられる。
        - 働き方や雇用形態の多様化、デジタル改革の推進を機会としてIT・セキュリティ人材の流動性・マッチング機会の促進が図られるための環境整備が必要である。
        - 特に地域・中小企業においてセキュリティ人材の不足が顕著であるところ、地域における「共助」の取組や、産業界と教育機関との連携促進・エコシステム構築を通じ、プラクティスの実践に当たって参考となるノウハウやネットワークの提供を行う。
    - （2）巧妙化・複雑化する脅威への対処
      - 近年の脅威動向に対応するとともに、男女や学歴等によらない多様な視点や優れた発想を取り入れつつ、これら実践的な対処能力を持つ人材の育成に向けた取組を一層強化し、コンテンツの開発・改善を図っていく。
      - 人材の活躍促進やマッチング促進の観点から、多様な人材の活躍等の先進事例の発信、プログラムに参加した修了生同士のコミュニティ形成や交流の促進、資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進にもあわせて取り組む。
    - （3）政府機関における取組
      - 、外部の高度専門人材を活用する仕組みの強化や、新たに創設される国家公務員採用試験「デジタル区分」合格者の積極的な採用、デジタル化の進展を踏まえた研修の充実・強化等に向けた方針に基づき、政府機関全体で取組を強化していく。
      - 特に、高度なサイバー犯罪や安全保障への対応等を行うため、外部の高度専門人材を活用するだけでなく、政府機関等内部においても独自に高度専門人材を育成・確保する。
    - 国民一人ひとりがサイバーセキュリティに対する意識・理解を醸成し、基本的な取組を平時から行い、様々なリスクに対処できることが不可欠である。
    - リテラシーを身に付け、自らの判断で脅威から身を守れるよう、官民が一体となって行動強化につなげるための普

- 4.4.3 全員参加による協働、普及啓発
  - 及啓発・情報発信に取り組むことか重要である。
  - 国は、地域、企業、学校など様々なコミュニティの自主的な活動を尊重しつつ、各々の関係者が、連携・協働をできるような仕組みを構築し、その仕組みを下支えしていく役割を担う。
  - 「全員参加による協働」に向けた具体的なアクションプランを策定し、地域・中小・若年層を重点対象として、取組推進を行ってきた。
  - 本戦略では「Cybersecurity for All」という考え方を示しているが、これは「全員」が自らの役割を主体的に自覚しサイバーセキュリティに取り組む、という考え方を含んでいる。
  - また、高齢者への対応を含め、当該アクションプランの見直しを検討する。
  - 加えて、特に、テレワークの増加やクラウドサービスの普及等の近年の人々の行動や企業活動の変化に応じて、ガイドラインや様々な解説資料等の整備が進められている。
  - これらも含め、情報発信・普及啓発のあり方（コンテンツ）についても、必要な対応を実施する。
- 3. サイバーセキュリティ2021
- 4.
- 5.
- 6.
- 7.
- 8.