NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

資料10－1

次期重要インフラ行動計画の検討の方向性について

令和３年５月31日

内閣サイバーセキュリティセンター
重要インフラグループ

サイバーセキュリティ政策のこれまでの経緯

○今後の重要な環境変化
- 2020年東京オリンピック・パラリンピック競技大会

省庁ＨＰ連続改ざん 2000.1
Webサーバの脆弱性への攻撃
米国同時多発テロ 2001.9
偽サイト誘導詐欺スパイウェア
エストニアへの大規模サイバー攻撃
Winny
誘導型攻撃の出現
米韓への大規模攻撃
イランの核施設への攻撃
9.18攻撃
韓国大規模障害
遠隔操作ウィルス
水飲み場型攻撃
標的型攻撃組織的高度化
米国での中国軍関係者起訴・指名手配
感染PCによる不正送金
米国ソニー年金機構ピクチャーズ情報流出への攻撃
世界規模の身代金要求型攻撃
世界規模の重要産業等からの情報窃取攻撃

年度 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

試行錯誤 | DoS攻撃、コンピュータウイルス対策 | リスクゼロ社会 | 「事故前提社会」でのリスクベース対策 | 国家安全保障・危機管理としてのサイバーセキュリティ | 高度なサイバー脅威に対し、積極的な対処が求められる時代に

e-Japan 戦略 (2001.1.22)
e-Japan 戦略Ⅱ (2003.7.2)
IT新改革戦略 (2006.1.19 IT戦略本部決定)
i-Japan 戦略2015 (2009.7.6)
新たな情報通信技術戦略 (2010.5.11 IT戦略本部決定)
世界最先端ＩＴ国家創造宣言 (2013.6.14 閣議決定, 2014.6.24 改定, 2015.6.30 改定, 2016.5.20 改定)
世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画 (2017.5.30 閣議決定)
世界最先端デジタル国家創造宣言・官民データ活用推進基本計画 (2018.6.15閣議決定, 2019.6.14改定, 2020.7.17改定)

参考：IT利活用

基本戦略
- 第１次情報セキュリティ基本計画 (2006.2.2 政策会議決定)
- 第２次情報セキュリティ基本計画 (2009.2.3 政策会議決定)
- 国民を守る情報セキュリティ戦略 (2010.5.11 政策会議決定)
- サイバーセキュリティ基本法公布 (2014.11.12)
- ＣＳ戦略 (2015.9.4 閣議決定)
- サイバーセキュリティ戦略 (2018.7.27閣議決定)
- ＣＳ戦略 (2013.6.10 政策会議決定)
- サイバーセキュリティ基本法改正公布 (2016.4.22)
- サイバーセキュリティ基本法改正公布 (2018.12.12)

年次計画
SJ：セキュアジャパン　JS：情報セキュリティ　CS：サイバーセキュリティ
SJ2006 SJ2007 SJ2008 SJ2009 JS2010 JS2011 JS2012 CS2013 CS2014 CS2015 CS2016 CS2017 CS2018 CS2019 CS2020

政府機関対策
- 情報セキュリティポリシーに関するガイドライン (2000.7 情報セキュリティ対策推進会議決定)
- 政府機関の情報セキュリティ対策のための統一基準
  - 第1版 (2005.12.13 政策会議決定) 第2版 (2007.6.14 政策会議決定) 第3版 (2008.2.4 政策会議決定)
  - 第4版 (2009.2.3 政策会議決定) 平成23年度版 (2011.5.11 政策会議決定) 平成24年度版 (2012.4.21 政策会議決定)
  - 平成26年度版 (2014.5.19 政策会議決定)
  - 平成28年度版 (2016.8.31 戦略本部決定)
  - 平成30年度版 (2018.7.25 戦略本部決定)

重要インフラ対策
- 重要インフラのサイバーテロ対策に係る特別行動計画 (2000.12 情報セキュリティ対策推進会議決定)
- 重要インフラの情報セキュリティ対策に係る行動計画 (2005.12.13 政策会議決定)
- 重要インフラの情報セキュリティ対策に係る第2次行動計画 (2009.2.3 政策会議決定)
- 重要インフラの情報セキュリティ対策に係る第3次行動計画 (2014.5.19 政策会議決定, 2015.5.25 戦略本部改定)
- 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 (2017.4.18 戦略本部決定, 2018.7.25,2020.1.30 戦略本部改定)

組織体制
- 内閣官房 情報セキュリティ対策推進室 (2000.2設置)
- 内閣官房情報セキュリティセンター (2005.4 設置)
- 情報セキュリティ政策会議 (2005.5 設置)
- GSOC (2008.4 運用開始)
- CYMAT (2012.6 設置)
- 内閣官房内閣サイバーセキュリティセンター (2015.1設置)
- サイバーセキュリティ戦略本部 (2015.1設置)

次期サイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験
テレワーク、オンライン教育等の進展
- 厳しさを増す
安全保障環境
- **SDGｓ**への
デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**
に向けた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映
国家間競争の場に
安全保障上の課題にも
- 不適切な利用は
国家分断、人権の阻害へ
- 官民の取組の
活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

DXとサイバーセキュリティの同時推進

安全保障の観点からの取組強化

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

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

「次期サイバーセキュリティ戦略」（骨子）の概要

中長期的

戦略期間

1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、オリンピック・パラリンピックの取組の活用

2　基本的な考え

2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」

2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3　サイバー空間をとりまく課題認識

3－1　サイバー空間におけるリスクの増大

・新たな技術革新の浸透と依存度の高まり、クラウドサービス利用拡大と境界型セキュリティの限界、サイバー空間を構成するシステムのサプライチェーンの複雑化、リテラシー差異や人材不足・偏在など攻撃者から狙われ得る弱点の顕在化、サイバー空間を巡る国際情勢

3－2　突き付けられている課題と方向性　～Cybersecurity for All～

・デジタル改革を踏まえた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

4　目的達成のための施策

経済社会の活力の向上及び持続的発展

1．経営層の意識改革

2．地域・中小企業におけるDX with Cybersecurityの推進

3．サプライチェーン等の信頼性確保に向けた基盤づくり

4．インクルーシブなデジタル／セキュリティ・リテラシーの定着

国民が安全で安心して暮らせるデジタル社会の実現

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

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

3・4・5．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)
②(重要インフラ)
③(大学・教育研究機関等)

6．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

7．大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

1．「自由、公正かつ安全なサイバー空間」の堅持

2．我が国の防御力・抑止力・状況把握力の強化

3．国際協力・連携

横断的施策

研究開発の推進　人材の確保・育成・活躍促進　全員参加による協働・普及啓発

5　推進体制

サイバーセキュリティ政策により、自由、公正かつ安全なサイバー空間を確保するためには、政府一体となった推進体制が必要。
デジタル庁が司令塔として推進するデジタル改革に寄与するとともに、公的機関が限られたリソースを活用しその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。

（参考）次期サイバーセキュリティ戦略の骨子［重要インフラ関係抜粋］

サイバーセキュリティ戦略本部（第28回）[2021年5月13日]　資料１

４.２.４ 経済社会基盤を支える各主体における取組②（重要インフラ）

- 我が国の経済や社会は、様々な重要インフラサービスの継続的な提供に依存しているが、重要インフラ間の相互依存性の高まりやサプライチェーンの複雑化・グローバル化を踏まえると、安全で安心な社会の実現には、**脅威が年々高まっている重要インフラのサイバーセキュリティを確保し、強靭性を高めることが不可欠**である。
- 平成26年に公布・施行されたサイバーセキュリティ基本法では、重要インフラ事業者の責務を明確に定めるとともに、国は、重要インフラ事業者等のサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他自主的な取組の促進その他必要な施策を講ずるよう規定されている。
- こうしたことを踏まえ、**重要インフラに関わる各主体がそれぞれの責務を認識し、官民が一体となって堅牢な重要インフラの実現に向けた取組を推進**する。

（１）官民連携に基づく重要インフラ防護の推進

- 国民生活及び社会経済活動の基盤である重要インフラサービスの安全かつ持続的な提供のため、**重要インフラ防護に責任を有する国と自主的な取組を進める事業者等との共通の行動計画を官民で共有し、これを重要インフラ防護に係る基本的な枠組みとして引き続き推進**する。
- 重要インフラを取り巻く脅威は年々高度化・巧妙化しているが、その一方で、重要インフラ分野ごとにシステムの利用形態が異なることから、各組織における脅威の差異が拡大してきている。このことを踏まえ、重要インフラ防護のよりどころとなる現行の「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」を基本としつつ、**重要インフラ分野が全体として今後の脅威の動向、システム、資産を取り巻く環境変化に柔軟に対応できるようにするため、行動計画を積極的に改定**し、**官民連携に基づく重要インフラ防護の一層の強化**を図る。
- 重要インフラサービスの安全かつ持続的な提供において、デジタル技術は大きな役割を果たすものであり、サイバーセキュリティの確保は経営の根幹に関わるものである。この認識の下、ビジネスとセキュリティのバランスが取れ、先進的でセキュリティ対策が適切に講じられた重要インフラサービスの実現を確実なものとするため、各組織が先行事例で得られた教訓を有効に生かせるよう、重要インフラ事業者等による情報収集を円滑にするための横断的な情報共有体制の一層の充実を図るとともに、セキュリティ対策は組織一丸となって取り組むことが重要であることから、**経営層のリーダシップが遺憾なく発揮できる体制の構築**を図っていく。

（２）地方公共団体に対する支援

- 地方公共団体は、個人情報等の多数の機微な情報を保有し、**国民生活に密接に関係する基礎的なサービスを提供していることに鑑み、国は、地方公共団体において適切にセキュリティが確保されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施**する。
- 「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」という。）に基づくセキュリティ対策が着実に実施されるよう、人材の確保・育成及び体制の充実並びに必要な予算を確保するための取組を支援する。
- 地方公共団体情報システムの標準化、行政手続のオンライン化、「クラウド・バイ・デフォルト原則」等を受けたクラウド化、働き方改革や業務継続のためのテレワークの導入等、新たな時代の要請に柔軟に対応できるよう、ガイドラインの継続的な見直し等、必要な諸制度の整備を推進する。
- 地方におけるデジタル改革（デジタル・ガバメントの実現）を促進するため、国は、「デジタル社会の実現に向けた改革の基本方針」（令和２年12月閣議決定）を踏まえ、整備方針において、地方公共団体のセキュリティについての方針を規定する。
- 国民生活・国民の個人情報に密接にかかわるマイナンバーについて、利便性とセキュリティの調和を考慮して対策を強化し、安全・安心な利用を促進する。

次期重要インフラ行動計画の検討について

重要インフラ専門調査会 (第24回) [2021年1月26日]　資料５
サイバーセキュリティ戦略本部 (第26回) [2021年2月9日]　資料６

○ 次期重要インフラ行動計画策定に向けた検討スケジュール

◆「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」（平成29年４月18日サイバーセキュリティ戦略本部決定）は、重要インフラ防護に係る基本的な枠組みとして、重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画として策定・推進してきた。

◆ 第４次行動計画策定後３年を経過したところであるが、東京2020大会終了後改定を行うこととしている。

◆「サイバーセキュリティ戦略」（平成30年７月27日閣議決定）についても、東京2020大会終了後に新たな戦略の策定が予定されていることから、同戦略の検討内容を踏まえながら、次期重要インフラ行動計画の検討を令和３年度内を目途に行っていく。

○ 検討の視点（例）

➢ 事業の特質及び現状を踏まえた最適な重要インフラ防護の枠組みの在り方

- 重要インフラ防護の目的は、「重要サービスの継続的提供の強靭性の確保」である。サイバー依存度の高まりとともに、日々脅威が巧妙、複雑化している現状を踏まえ、その強靭性確保のための方法論は分野、事業者によって異なってきている現状をどのように反映すべきか。
- 「重要インフラのサイバーテロ対策に係る特別行動計画」(平成12年12月決定)が重要インフラ防護の端緒。同計画策定当初は、重要インフラに使用される情報システムの横断的かつ具体的なセキュリティ対策の導入が目標。過去20年間に得られた知見、今般の環境変化等を踏まえ、重要インフラ防護に当たり、今後どのような視点の切替えが必要なのか。

➢ 行動計画の位置づけの再確認

- 平成26年に公布、施行されたサイバーセキュリティ基本法において、重要インフラ事業者及び地方公共団体の責務、当該事業者等におけるサイバーセキュリティ確保の促進のために国が必要な施策を講ずる旨規定されていることを踏まえ、行動計画の位置づけを再確認するとともに、事業者等の自主的な取組をどのように支援することが適切であるか。

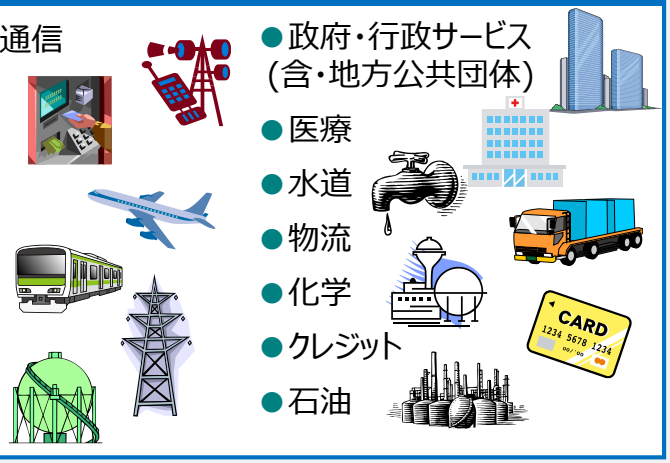
「重要インフラの情報セキュリティ対策に係る第４次行動計画」の概要

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

重要インフラ(全14分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



NISCによる調整・連携

重要インフラ所管省庁

- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省　［医療、水道］
- 経済産業省　［電力、ガス、化学、クレジット、石油］
- 国土交通省　［航空、空港、鉄道、物流］

関係機関等

- 情報セキュリティ関係省庁　［総務省、経済産業省等］
- 事案対処省庁　［警察庁、防衛省等］
- 防災関係府省庁　［内閣府、各省庁等］
- 情報セキュリティ関係機関　［NICT、IPA、JPCERT等］
- サイバー空間関連事業者　［各種ベンダー等］

「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」

安全基準等の整備・浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

現行動計画の取組を踏まえた次期行動計画に向けた課題

重要インフラに対するサイバーセキュリティ上の脅威の増大

- 重要インフラに対するサイバーセキュリティ上の脅威が増大
- 国民生活や経済社会活動は重要インフラの強靭性・信頼性に依存

脅威動向の変化

- サイバーセキュリティが政策課題となった2000年頃はWebページ改ざん等が主たる脅威であり、分野共通的に必要とされる現場レベルでの対策に関する基準・指針等が求められていたところ
- しかしながら、 20年が経過し、サイバー攻撃の高度化等に伴うリスクの複雑化によって、共通脅威が高まりつつあると同時に、組織ごとの脅威の違いが増大しており、求められるセキュリティの水準や対策は分野や事業者ごとに異なりつつある状況
- また、DX等により重要インフラを取り巻く環境やリスクは今後も大きく変化していくと考えられることから、重要インフラ事業者等は変化に柔軟に対応できる能力の向上を図る必要（リスクインフォームドアプローチ）
- 加えて、重要システムだけでなく関連するシステムも含めた組合せによる新たなリスク（システミックリスク）への対応、ハードウェアの脆弱性管理、サプライチェーンマネジメント対応の必要

重要インフラサービスの停止に関する傾向

- 重要インフラサービス停止は、自然災害、管理ミス等を原因とするものが多数を占め、管理を適切に行うことで防止できた事案が繰り返し発生していることから、上層部、CISO、戦略マネジメント層、担当者の責務の明確化を図る必要

ビジネスとセキュリティのバランスの確保

- 組織におけるセキュリティ・バイ・デザインの明確化
- セキュリティが組織内のセキュリティ担当だけで閉じている現実を改善し、組織内全体の課題とする必要
- 組織における情報収集、知見の活用

官民の責務・連携の在り方の明確化

- 国、重要インフラ事業者等の責務の明確化
- 自助ありきの共助、自助と共助（互助）を促進させるための公助
- 事業者における情報収集の活性化、業界主導での業界横連携の促進

次期重要インフラ行動計画において特に明確にすべき事項（案）

論点１ 重要インフラに対する脅威の変化とその対応

- 重要インフラを取り巻く脅威の変化(2000年から現在まで)
- 分野や事業者に共通する脅威の増大
- 組織固有の脅威の増大
- 重要システムを支える外部システムが重要システムに大規模な障害を引き起こすリスク(システミック・リスク)の顕在化
- サプライチェーンリスクマネジメントの必要性
- ハードウェアに関する脆弱性管理の必要性

論点２ 重要インフラと我が国の経済・社会との関係

- 重要インフラサービスの途絶が国民生活や経済社会活動に与える影響
- 重要インフラ事業者等の社会的責任

論点３ サイバーセキュリティ基本法と行動計画の関係

- 内閣官房、重要インフラ所管省庁、重要インフラ事業者等の責務の明確化
- サイバーセキュリティ基本法(以下「基本法」という。)等の関係法令における行動計画の位置付けの明確化
- 基本法第５条事業者(地方公共団体)と基本法第６条事業者(重要社会基盤事業者)の特性に応じた役割の検討
- 重要インフラと基本法第７条事業者(サイバー関連事業者その他の事業者)との関係の明確化

論点４ 重要インフラ防護の範囲について

- 各分野における重要インフラ事業者の明確化
- 重要システムや防護対象の妥当性の検討(例：海外拠点等)
- 新たな重要インフラ分野の検討

論点５ デジタル庁設置に伴う対応

- 政府のデジタル改革への対応(例：地方公共団体との関係)

論点６ 関係主体の責任及び権限並びに実施事項の明確化

- 内閣官房、重要インフラ所管省庁、重要インフラ事業者等の責任及び権限並びにそれらに基づく各関係主体の実施事項の明確化

論点７ 重要インフラ事業者等におけるコミットメントの確保

- 上層部(経営層)、CISO、戦略マネジメント層、担当の責務の明確化
- ビジネスとセキュリティのバランスの在り方

論点８ 重要インフラ事業者等が自らの組織に最適な防護対策

- 組織の特性を踏まえた経営層による組織のリスクの明確化
- CSIRT概念の明確化(経営におけるサイバーとCISOの役割の明確化)
- 既存の基準類をどのように当てはめればよいかを示すガイダンスの整備
  - ✓ サイバーセキュリティ確保のための組織に根差した枠組みモデル

論点９ 情報共有の強化

- 情報共有における共助の推進(自助ありきの共助、自助と共助(互助)を促進させるための公助)
- 重要インフラ事業者等の情報収集の活性化
- NISCの情報提供の在り方
- サイバーセキュリティ協議会との連携
- ISAC連携等による民主導での分野間連携の枠組みの整備

論点10 環境変化に対する柔軟な対応

- DX、コロナウイルス感染症の拡大等の様々な社会的・技術的な環境変化に応じたサイバーセキュリティの実現

論点11 東京2020大会のレガシーの活用

論点12 これまでの施策の検証・評価

次期重要インフラ行動計画の基本的な方針（案）

環境の変化

- **サイバー依存度の高まり**
- **共通脅威の劇的な高まり**
- **リスク・脅威の多様化・複雑化**
  - ✓ サプライチェーン・リスクの顕在化
  - ✓ 分野間による脅威の差異の拡大
  - ✓ 重要システムや関連系のリスクの組み合わせによって生じるシステミック・リスクへの配慮
- **防護対象の拡大**
  - ✓ 海外拠点の増加
  - ✓ クラウドサービスの利用拡大
  - ✓ IoT機器の増加
  - ✓ テレワークの普及
  - ✓ サイバー攻撃の増加
- **制御系システムの脆弱性の増加**
  - ✓ ハードウェア固有の脆弱性の顕在化

等

現行動計画の評価・課題

- **対策の効果を客観的に測定するための指標・手法(KPI)の整備**
  - ✓ 関係省庁等、重要インフラ事業者等の取組の効果を適切に測定できる指標の整備
- **責任・権限や役割分担の明確化**
  - ✓ 内閣官房、重要インフラ所管省庁、重要インフラ事業者等の一層の明確化
- **防護対象となる範囲の一層の明確化**
  - ✓ 事業者、システム等の明確化
- **同じ失敗が繰り返されることへの対策**
  - ✓ 重要インフラ全体としてのPDCAサイクルの構築
- **事業者ガイダンスの策定**
  - ✓ どのようなセキュリティ対策をどこまで実施すればよいのかをガイドする、事業者に向けた指針の策定

等

行動計画の位置付け等

- **行動計画の**サイバーセキュリティ基本法やその他の関係法令における**位置づけを明確にすることが必要**
- **関係者間の責任と権限の明確化が必要**(内閣官房、重要インフラ所管省庁、重要インフラ事業者等)
- **政府のデジタル改革への対応**(デジタル庁の設置等)
- **東京2020大会のレガシーの活用**

等

重要インフラサービスの安全かつ持続的な提供を確保するため、重要インフラの強靭性を高めていく

① 重要インフラを取り巻く環境の変化を認識
② サイバーセキュリティ基本法等の関係法令との関連の明確化
③ 内閣官房、重要インフラ所管省庁、重要インフラ事業者等の官民の関係主体の役割の明確化
④ 関係主体の実施状況を評価可能なものとし、重要インフラのサイバーセキュリティ対策の継続的な改善を図る