サイバーセキュリティ2019（案）（2018年度報告・2019年度計画） 全体概要

資料1-1

趣旨・背景

○ 1部を年次報告（2018年度）、2部を年次計画（2019年度）とし、記載の根拠となるデータを充実化しつつ、報告と計画の関連性を明確化するため冊子を一本化

○ 1部の１章を新設し、サイバー空間における動向と脅威の主なトピックとともに、新戦略(2018年7月決定）の目指す姿と対処方針等のポイントを改めて整理

○ 2部の１章を新設し、新戦略の対処方針について国内外の関係者の理解を図るため、対処方針（積極的サイバー防御等）に沿って、取組を抽出し、そのポイントを整理

1部 年次報告（2018年度）

新設（一般（経営層等）向け）

1章 サイバー空間と実空間の一体化の進展に伴う動向と対処方針

1 本章の位置づけ（一般（経営層等）への波及を期待、新戦略の理解と実践の参考）

2 変わりゆくサイバー空間とそれに伴う脅威の深刻化
- 2.1 新たなサイバーセキュリティ戦略の位置づけ（３年間の基本計画、我が国の基本的立場の明示）
- 2.2 新戦略で目指す姿とサイバー空間における脅威の状況
  - （1）サイバーセキュリティを通じたサイバー空間の持続的発展（自律的な取組による「Society 5.0」の実現への寄与）
  - （2）目指す企業経営とサイバーセキュリティの姿 ～DX with Cybersecurity～
    あらゆる企業が、自律的にサイバーセキュリティにも取り組む「デジタル企業」となり、新製品やサービス等を創出する姿
  - （3）身近にあるサイバー空間における脅威とその影響の拡大
    ①サイバー空間における脅威による影響（業務・サービス障害、情報漏えい、金銭被害）
    ②サイバー空間における攻撃者優位の状況（攻撃者（時間、場所の無制約等）、防御側（完全なリスク除去不可能等））
    ③サイバー空間における脅威の影響が広がる可能性（イベント、裾野拡大（人、供給網、IoT）、先端技術（AI等））
- 2.3 主なトピック
  - （1）業務・機能・サービス障害（平昌大会関係、奈良県病院のシステム障害等）
  - （2）情報の毀損及び漏えい（大学等におけるフィッシングによる情報漏えい事案、国家の関与が疑われるAPT10等）
  - （3）金銭の窃取・搾取等（フィッシング詐欺の増加、脅迫メール、暗号資産等）

3 新戦略に基づく対処方針
- 3.1 持続的な発展のためのサイバーセキュリティ ～サイバーセキュリティエコシステム～
- 3.2 積極的サイバー防御 ～事前の能動的な取組～
- 3.3 2020年東京大会とその後を見据えた対処態勢の強化

昨年度報告・計画に該当部分あり

2章 2018年度のサイバーセキュリティに関する情勢

1 サイバーセキュリティの基本的な枠組みに関する情勢（新戦略の策定経緯、基本法を一部改正する法律の経緯）
2 重要インフラ分野等におけるサイバーセキュリティに関する情勢
3 政府機関等におけるサイバーセキュリティに関する情勢
4 サイバー空間に係る国際的な動向

3章 2018年度のサイバーセキュリティ関連施策の取組実績と評価

1 経済社会の活力の向上及び持続的発展
2 国民が安全で安心して暮らせる社会の実現
3 国際社会の平和・安定及び我が国の安全保障への寄与
4 横断的施策
5 推進体制

2部 年次計画（2019年度）

1章 2019年度のトピックとなる取組

1 持続的な発展のためのサイバーセキュリティ ～サイバーセキュリティエコシステム～
- 1.1 サービス提供者関連
  - （1）企業 （戦略マネジメント層育成、企業におけるサプライチェーン・リスク対策、情報開示手引き等）
  - （2）重要インフラ事業者等（安全基準等策定指針の改定及び浸透等）
- 1.2 全ての主体関連
  - （1）意識・行動強化 （意識・行動強化プログラム等）
  - （2）IoT関連 （技術基準、国際標準化等）
- 1.3 国際協力・連携関連（法の支配の推進、能力構築支援等）
- 1.4 研究開発関連（研究・技術開発の取組方針等）

2 積極的サイバー防御 ～事前の能動的な取組～
- 2.1 政府関係者の取組
  - （1）改定された統一基準群に基づく取組（未知の不正プログラム対応、IT資産管理の自動化等）
  - （2）政府調達におけるサプライチェーン・リスク対策（IT調達に係る申合せに基づく取組等）
  - （3）ボットネット対策（パスワード設定に不備のあるIoT機器の調査等）
  - （4）先行的防御を可能にするための取組（脅威情報の共有・活用の促進、攻撃誘引技術の活用等）
- 2.2 従来の枠を超えた取組
  - （1）情報共有連携体制（サイバーセキュリティ協議会）
  - （2）暗号資産（仮想通貨）に関する取組
  - （3）自動運転に関する取組

3 2020年東京大会とその後を見据えた対処態勢の強化
- 3.1 2020年東京大会における対処態勢
- 3.2 大規模サイバー攻撃事態等への対処態勢

2章 2019年度の各種施策一覧表

1 経済社会の活力の向上及び持続的発展
1.1新たな価値創出を支えるサイバーセキュリティの推進 1.2多様なつながりから価値を生み出すサプライチェーンの実現
1.3安全なIoTシステムの構築

2 国民が安全で安心して暮らせる社会の実現
2.1 国民・社会を守るための取組 2.2 官民一体となった重要インフラの防護 2.3 政府機関等におけるセキュリティ強化・充実
2.4 大学等における安全・安心な教育・研究環境の確保 2.5 2020年東京大会とその後を見据えた取組
2.6 従来の枠を超えた情報共有・連携体制の構築 2.7 大規模サイバー攻撃事態等への対処態勢の強化

3 国際社会の平和・安定及び我が国の安全保障への寄与
3.1 自由、公正かつ安全なサイバー空間の堅持 3.2 我が国の防御力・抑止力・状況把握力の強化 3.3 国際協力・連携

4 横断的施策
4.1 人材育成・確保 4.2 研究開発の推進 4.3 全員参加による協働

5 推進体制

別添

別添１ 各府省庁における情報セキュリティ対策の総合評価・方針 別添２ 2018年度のサイバーセキュリティ関連施策の実施状況（一覧表）
別添３ 政府機関等における情報セキュリティ対策に関する統一的な取組 別添４ 重要インフラ事業者等における情報セキュリティ対策に関する取組等
別添５ サイバーセキュリティ関連データ集 別添６ 担当府省庁一覧（2019年度計画） 別添７ 用語解説

サイバーセキュリティ戦略（2018年）・サイバーセキュリティ2019の概要

資料1-2

◆ サイバーセキュリティ戦略(2018年７月)は、サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの

◆ サイバーセキュリティ2019は、同戦略に基づく初めての年次報告とそれを反映した年次計画を統合したもの。各府省庁はこれに基づき、施策を着実に実施

＜新戦略(2018年戦略)（平成30年7月27日閣議決定）の全体構成＞

1 策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2 サイバー空間に係る認識

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3 本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

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

～新たな価値創出を支えるサイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 多様なつながりから価値を生み出すサプライチェーンの実現
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現

～「積極的サイバー防御」の推進による任務保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 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

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

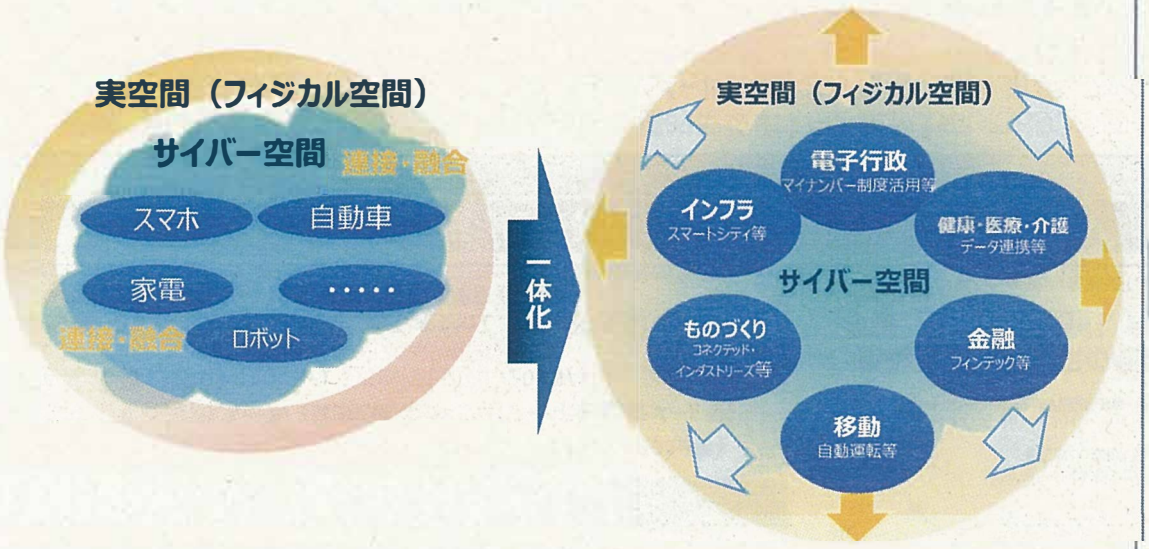
- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

5 推進体制

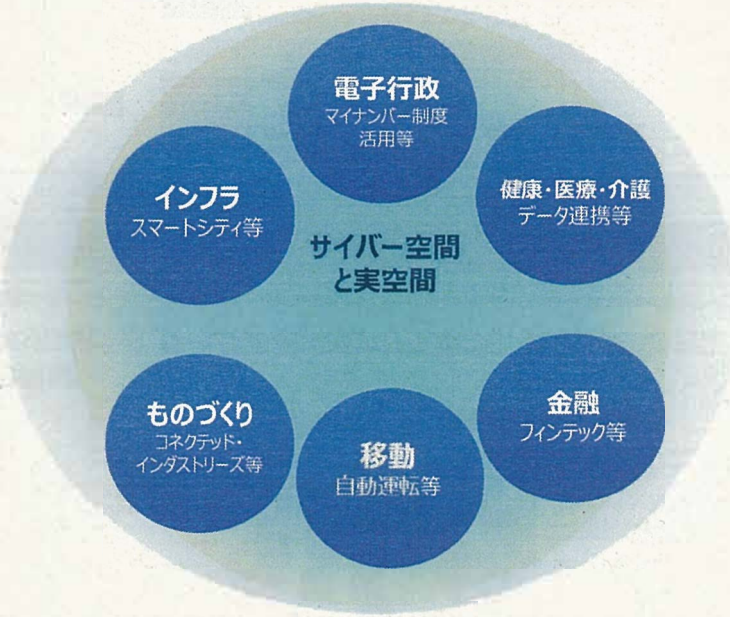
内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

（参考）サイバー空間と実空間の更なる一体化のイメージ

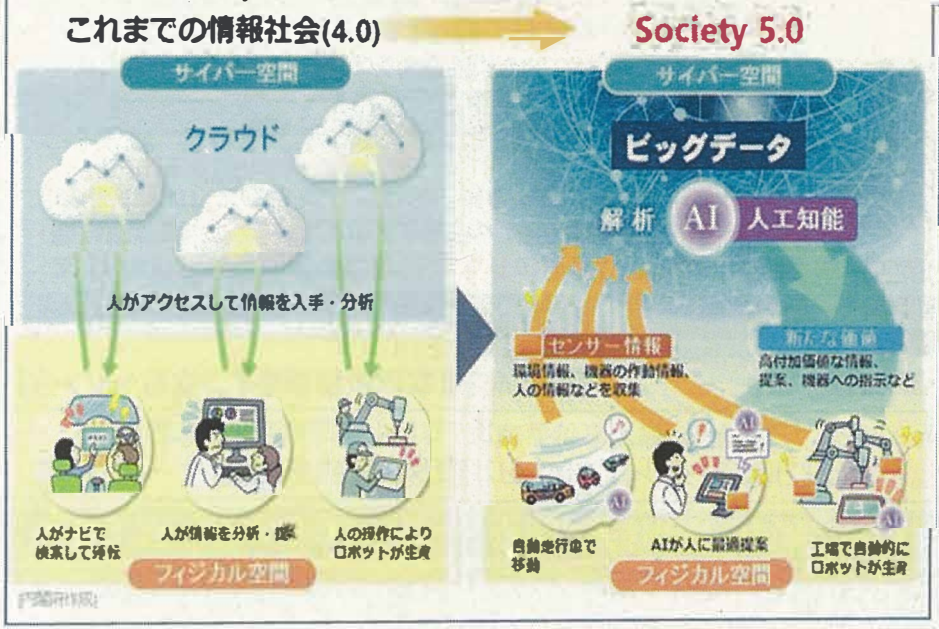
【サイバー空間と実空間の一体化・活動空間の拡張】(2018年戦略の概要資料)



一体化が更に進展すると、今まで関わりのない分野にも影響を与える可能性



参考：Society 5.0のしくみ（内閣府作成）



Society 5.0の実現に向けた政府の主な体制図

日本経済再生本部（2012年に設置）
〈戦略〉・未来投資戦略

その他の本部等
（総合科学技術・イノベーション会議、知的財産戦略本部等）

サイバーセキュリティ戦略本部
[2015年に設置]
〈戦略〉
・サイバーセキュリティ戦略
〈所管法令〉
・サイバーセキュリティ基本法

IT総合戦略本部（高度情報通信ネットワーク社会推進戦略本部）
[2001年に設置]
〈戦略〉・IT戦略(世界最先端デジタル国家創造宣言等)
・官民データ活用推進基本計画
〈所管法令〉
・高度情報通信ネットワーク社会形成基本法
・官民データ活用推進基本法

個人情報保護委員会
[2014年に設置]
〈所管法令〉
・個人情報の保護に関する法律

サイバーセキュリティ2019（１部（2018年度報告）　１章及び２章 ）の概要

１部１章（変わりゆくサイバー空間とそれに伴う脅威の深刻化）

➢ サイバー攻撃による被害が深刻化する中、サイバー空間における攻撃者優位の状況(攻撃者：時間・場所の無制約や低コストかつ豊富な手段、防御側：限られた資源、脆弱性の完全除去は不可能、攻撃者特定困難)も背景に、サイバー空間と実空間の一体化の進展により被害が拡大する可能性がある。

【サイバー攻撃による被害の主なトピック※1】

※1 2018年度を中心とした近年の事例をピックアップ

業務・機能・サービス障害

- **2018年平昌大会期間中に約550万件のサイバー攻撃との報道**
- **奈良県病院 約２日間にわたるカルテシステムの障害(2018/10)**

⇒今後ますます現場のデジタル化が進む中、通信障害、交通混乱や停電等の事態が発生する可能性

情報の毀損及び漏えい

- **大学におけるフィッシングによる情報漏えい(10大学での被害が報道)**
- **国家の関与が疑われるAPT10を非難(外務報道官談話　2018/12)**

⇒今後個人情報やリアルデータ等の情報の価値が高まっていくにつれて、金銭獲得や別の攻撃への悪用を目的に脅威が高まる可能性

金銭の窃取・詐取等

- **過去最大規模(前年比約2.5倍)のフィッシング詐欺(2018年)**
- **巧妙化する脅迫メール（実際に使用されたパスワードを記載したメール等）**
- **暗号資産の窃取（2018/1 約580億円相当、2018/8 約1500万円相当、2018/9 約70億円相当）**

⇒今後、低い労力で多くの利益を得ることを狙って、対策が不十分な分野や多額の金銭を得られる対象に関する脅威が高まる可能性

【サイバー空間における脅威の影響が広がる可能性】

○国際的なイベントの開催に伴う脅威

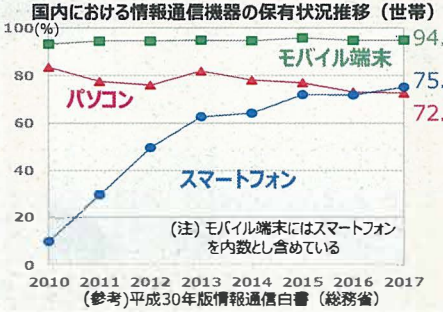
最高度の注目を集めるため攻撃のターゲットとなるおそれのある国際イベントが開催予定
(G20(2019/6)、ラグビーワールドカップ(2019/9)、2020年東京オリンピック・パラリンピック競技大会(2020/7))

○サイバー空間利用の裾野拡大に伴う脅威

スマートフォンやIoT等の生活への普及・浸透やDX※2の進展に伴い、人間の脆弱性、供給網（サプライチェーン）、IoT機器の問題に起因する脅威が広がるおそれ

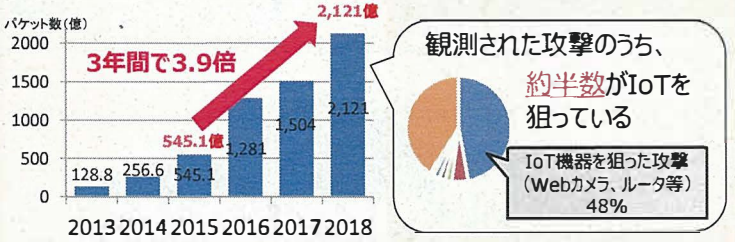
※2 将来の成長、競争力強化のために、新たなデジタル技術を活用して新たなビジネス・モデルを創出・柔軟に改変すること

国内における情報通信機器の保有状況推移（世帯）



(参考)平成30年版情報通信白書（総務省）

１年間で観測されたサイバー攻撃のパケット数



出典：国立研究開発法人 情報通信研究機構「NICTER」観測データ

○先端技術・サービスの利用拡大に伴う脅威

今後、AI、Fintech※3、自動運転車等の先端技術・サービスの利用拡大が予想され、新たな脅威が生じるおそれ

※3 Finance(金融)とTechnology(技術)を組み合わせた造語。ブロックチェーンやビッグデータといった新たな技術を活用した革新的な金融サービス

１部２章（サイバーセキュリティに係る情勢）

政府機関等に対する攻撃の高度化・巧妙化

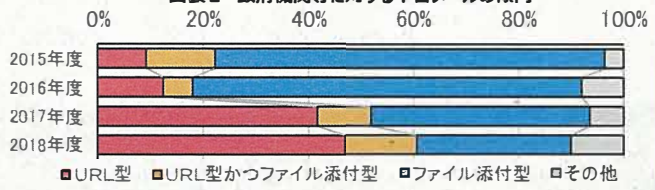
政府機関において、マルウェア感染の疑いがある通信や標的型攻撃を引き続き検知しており、標的型攻撃は増加（図表１）。標的型攻撃については、より巧妙化されたメールも確認されている。また、近年、ファイル添付型(不審なファイルを添付)に代わってURL型(不審なURLを記載)の不審メールの比率が増加（図表２）。

図表１　政府機関における引き続き警戒を要する攻撃等の検知件数※4

年度	2017年度	2018年度
マルウェア感染の疑い	169	111
標的型攻撃	57	66
タイポスクワッティング※5の疑い	0	5

(件)

図表２　政府機関等に対する不審メールの傾向



※4 既に攻撃手法に対応済みであるため攻撃としては失敗した通信、攻撃の前段階で行われる調査のための行為にとどまり明らかに対応不要と判断できる通信等を分析しノイズとして除去した上で、引き続き警戒を要するイベントについて集計

※5 URLやメールアドレスを入力する際に打ち間違うことを期待して、正規ドメインと紛らわしいドメインを所有しておく行為。

国外の動き（諸外国の戦略的取組）

米国
- 新たな国家サイバー戦略（2018/9）
- 連邦政府・重要インフラの保護、安全・信頼のインターネット維持等
- 国土安全保障省にサイバーセキュリティ・インフラストラクチャー・セキュリティ庁（CISA）を設置（2018/11）

EU
- 欧州NW・情報セキュリティ機関(ENISA)の権限拡大等を含むサイバーセキュリティ法成立（2018/12）
- 一般データ保護規則(GDPR)成立（2018/5 施行）

英国
- 国家サイバーセキュリティ戦略（2016）
- 「防御」、「抑止」、「開発」を目的

中国
- 国家サイバー空間セキュリティ戦略（2016）
- サイバー空間主権確保

サイバーセキュリティ2019（２部（2019年度計画））の概要

２部１章（2019年度のトピックとなる取組）

新戦略の対処方針に関する国内外の関係者の理解・浸透を図るため、その方針別に、「トピックとなる取組」を抽出し、その方向性と主な施策例を示したもの。その概要は以下のとおり。

１ 持続的な発展のためのサイバーセキュリティ ～サイバーセキュリティエコシステム～

１．１ サービス提供者関連

（１）企業（戦略マネジメント層育成、サプライチェーン・リスク対策、情報開示手引き等）
- －デジタルトランスフォーメーション(DX)とサイバーセキュリティを一体的に進める戦略マネジメント層の育成等の推進
- －サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装の推進、徹底した中小企業の現場支援

（２）重要インフラ事業者（安全基準等策定指針の改定及び浸透等）
- －自然災害に起因する重要インフラサービス障害の発生も可能な限り減らすための安全基準等を改善する取組の推進

１．２ 全ての主体関連

（１）意識・行動強化 （意識・行動強化プログラム等）
- －人材育成や普及啓発に関する官民の様々な取組みを集約するポータルサイトの構築等

（２）IoT関連 （技術基準、国際標準化等）
- －今後製品化されるIoT機器がパスワード設定の不備等により悪用されないようにする対策の推進等

１．３ 国際協力・連携関連

- －自由、公正かつ安全なサイバー空間を堅持するための理念の発信と途上国向け能力構築支援

１．４ 研究開発関連

- －サプライチェーン全体の信頼確保に向けたICT機器・サービスのセキュリティの技術検証を行うための推進体制の整備や、国内産業の育成・発展に向けた取組

２ 積極的サイバー防御 ～事前の能動的な取組～

２．１ 政府関係者の取組

（１）改定された統一基準群に基づく取組（未知の不正プログラム対応、IT資産管理の自動化等）
- －脅威が深刻化するサイバー攻撃への対応及びクラウドサービス利用時の適切な情報セキュリティ対策の推進

（２）政府調達におけるサプライチェーン・リスク対策（IT調達に係る申合せに基づく取組等）
- －サプライチェーン・リスク対応が必要な調達時の総合評価落札方式等、価格面だけでない総合的な評価を行う契約方式を採用する方針

（３）ボットネット対策（パスワード設定に不備のあるIoT機器の調査等）
- －サイバー攻撃を受けてから対応するのではなく、先手を打って悪用されるおそれのあるIoT機器の能動的な調査と利用者への注意喚起

（４）先行的防御を可能にするための取組（脅威情報の共有・活用の促進、攻撃誘引技術の活用等）
- －実証環境を用いた標的型攻撃の解析や、フィッシング詐欺の攻撃手法分析、なりすましメールを防止する送信ドメイン認証技術等の推進

２．２ 従来の枠を超えた取組

（１）情報共有連携体制（サイバーセキュリティ協議会）
- －官民・業界を問わず多様な主体が連携し、サイバーセキュリティの確保に資する情報の共有と、サイバー攻撃による被害とその被害拡大の阻止

（２）暗号資産（仮想通貨）に関する取組
- －自主規制機関と連携して暗号資産交換業者のサイバーセキュリティ対策の実施状況モニタリングし、利用者保護の確保を目指す

（３）自動運転に関する取組
- －自動運転システムへの新たなサイバー攻撃手法、インシデント情報、対策技術を調査した上での、脅威を想定した能動的な対策の推進

３ 2020年東京大会とその後を見据えた対処態勢の強化

３．１ 2020年東京大会における対処態勢

- －サイバーセキュリティ対処調整センター及び情報共有システムのG20大阪サミット等での運用による対処支援調整能力の向上と万全な対処態勢確立を目指す
- －対処態勢やリスクマネジメントの取組によって得られた経験・ノウハウを、大会後にもレガシーとして日本のサイバーセキュリティの確保に活用すべく、大会に向けた準備の推進

３．２ 大規模サイバー攻撃事態等への対処態勢

- －内閣官房を中心とした情報の集約・共有、初動対処に係る訓練・演習・見直しを通じて対処態勢の強化
- －各対処機関ではサイバー空間における情報収集・分析能力向上
- －サイバー攻撃の対象となり得る事業者での対処活動の支援強化

等

２部２章（2019年度の各種施策一覧）

新戦略の体系に沿って諸施策の目標や実施方針とともに、具体的な施策を網羅的に示したもの。