Sec01-08-1\_東京都中小企業サイバーセキュリティ対策担当業務の位置づけ

1. 改版履歴
   1. **【2021年2月1日】てにおはの修正**
   2. 【2020年2月7日】長文折り返し設定
   3. 2019年9月19日　NISC会議対応についての考察

リレーションシップ:

エクスポート先 [NISC対応についての考察](#Njc0MTc4Mzg0MjEwNDIwNA==);

* 1. 2019年8月1日　IPAとの打合せ結果を反映
  2. 2019年7月25日　参考資料追加
  3. 2019年7月18日　2020年以降の考察
  4. 2018年1月29日　初版

1. 目的
   1. 専門員の具体的な職務の根拠となる方針・戦術等を認識する
2. 基本姿勢
   1. 公的機関である東京都としての役割を果たす
      1. 関係機関全体で効率的、 効果的に中小企業を支援
         * 中小企業に対して、 国、 東京都、 民間が連携し、 過不足なく支援することにより、 国全体のサイバーセキュリティ対策を実効性のあるものにする
   2. 業務の運営に当たっては、 公務員倫理に沿って行動する（公務員倫理＜東京都一般職、 非常勤職員版＞
      1. 便宜供与、 利益供与の禁止
         * 特定組織、 個人の利益、 自らの私的利益の追求者であってはいけない
      2. 法令の遵守そのものが目的でなく、 法の趣旨に従う
      3. 公務員の故意・過失の責任と同様に、 行政の不作為も賠償責任を負う
      4. 職業や仕事は、 単に「生活の糧をえるための手段」としてだけでなく、 能力の発揮や自己実現の場
3. 位置付け
   1. 国全体のサイバーセキュリティ対策の体制の中で役割を果たす
      1. 国全体の施策
         * 国としての施策・基本方針・ガイドライン等の体系に沿う
         * 推進体制
           + サイバーセキュリティ戦略本部

事務局

内閣官房　内閣サイバーセキュリティセンター（NISC）

* + - * + 関係省庁

警察庁

犯罪抑止

総務省

国民全体

外務省

経済産業省

全国の企業への支援

防衛省

* + 1. 全国の企業のセキュリティ対策支援
       - 国全体の情報セキュリティ対策
       - 中小企業の情報セキュリティ対策
    2. 東京都の中小企業はTCYSS
       - 国全体の中で、 東京都の中小企業に有益なサイバーセキュリティ対策情報を発信する。 具体的な対策を行うことを支援する担当窓口へ案内する
         * 国としての施策・基本方針・ガイドライン等の体系の認識
       - 東京都商工部
       - 警視庁
       - ベンダー企業
       - 中小企業団体
  1. 商工部の中小企業支援の一環としての役割を果たす
     1. 中小企業の情報化支援、 事業継続計画の一環
     2. 中小企業に対する総合的支援の１つ
     3. サイバーセキュリティ対策は、 中小企業における事業継続計画の１つ
        + ITを活用したビジネスの事業継続のリスクの１つとしてのサイバーセキュリティ対策の実施を支援する。
     4. サイバーセキュリティ対策は、 中小企業におけるIT利活用に必要な投資の１つ
        + 中小企業のビジネス展開のためのIT利活用投資の一環でサイバーセキュリティ対策を実施することを支援する

1. 相談窓口業務としての基本方針
   1. 投資戦略
      1. サイバーセキュリティ対策を、 IT活用の一環での投資と位置付けて、 実施できるようにする
   2. 費用対効果
      1. 中小企業は投入できる資金が少ないので、 特に、 費用対効果の高い対策に留意する
   3. 評価は、
      1. どれだけの中小企業がTCYSSの活動を通じて、 サイバーセキュリティ対策の必要性を認識し、 実施に向けて行動を取ったか？
      2. そのための費用対効果は適切であったか？
2. 戦術
   1. 相談窓口としての戦術
      1. 相談窓口は、 相談者が次にアクションを取るべきことを示唆する
         * FAQにある内容はその場で回答。 対応先が明確な内容は、 対応先へナビゲート
         * 相談・届出先クイックリスト
         * ※これは、 図書館等でのレファレンスサービスと似ている
           + 知識の蓄積

日々の情報収集

予測調査

* + - * + 知識をベースとして、 的確な情報のある文献名、 記載ページを案内
    1. その他、 相談者にとって今後のアクションに有用な情報の所在場所を案内
  1. 業務としての戦術
     1. 相談窓口として、 相談されたことに対して、 次にとるべきことを示唆する
        + 個人ではなく組織として蓄積した知識に基づいて、 答えられる範囲で回答
        + 的確な対応先にナビゲート
        + 相談回答内容の均質化
     2. 的確な回答のために
        + FAQの作成
          - FAQは、 本来過去に多い質問と回答を提示するものであるが、 Qが溜まらない段階では、 想定で準備する
        + 予測調査
          - 相談が来そうな内容をあらかじめ調べておくことが重要
          - レファレンス用情報の収集と、 情報提供のための整理

日々のサイバーセキュリティ関連情報の収集と整理

サイバーセキュリティ関連の情報の所在、 内容の確認とインデキシング

関連ガイドライン内容構成の整理

* + - * ナレッジデータ、 レファレンスデータの収集と整理
        + 相談窓口として、 次にとるべきことを、 的確に示唆するためには、 事前に有用と思われる情報源、 情報の内容を把握し、 それを参考に回答するデータベースが必要
        + 的確な情報へのナビゲーションのためのインデキシング
        + TCYSSとしての情報データベース

全文検索が可能なWebページ、 電子書籍形式

* + - * 緊急問合せ用のホットラインの確立
        + 警視庁CS本部
        + IPAセキュリティセンター
    1. サイバーセキュリティ対策が十分に行われていない多くの企業に向けて
       - 相談電話をかけてくる人はごく一部
       - Webページによる情報発信
         * 収集した情報を整理し信頼できる情報として公開

この情報を見て、 もっと知りたい人が相談にくる

相談者にはこの情報を元に回答する

* + - * + 信頼できる情報源の情報そのものへのナビゲーション
        + 有用な情報サイトと認識されれば、 サイトを見た人からの相談電話も増える

1. 国全体の方針・施策
   1. サイバーセキュリティ基本法
      1. 一部を改正する法律【2019年4月施行】
         * サイバーセキュリティ協議会の設置
   2. サイバーセキュリティ戦略2018(2018年7月)
      1. 今後3年間の基本的な計画として策定
   3. サイバーセキュリティ2019（2019年5月23日）
      1. （2018年度報告・2019年度計画）
   4. サイバーセキュリティ協議会
      1. 事務局：NISC, JPCERT/CC
         * 「一般社団法人JPCERT/ CC」が政令指定法人として、 協議会の連絡調整事務を担当
      2. サイバーセキュリティ基本法の一部を改正する法律の施行及び同法に基づくサイバーセキュリティ協議会の組織について【報道資料】

参照:

<https://www.nisc.go.jp/press/pdf/kyogikai.pdf>;

* 1. サイバーセキュリティ対処調整センター（政府オリパラCSIRT）
     1. 2020年東京大会に向けた対処態勢の整備
     2. ○取組状況
        + 情報共有・事案発生時の態勢について関係府省庁、 大会組織委員会、 東京都等と協議し、 運用方針等を決定した。 また、 サイバー脅威情報の提供について４社から協力を受けることを決定するとともに、 大会組織委員会、 東京都等を交えた机上演習を実施した。
        + 情報共有システムの構築が完了し、 2019年４月にサイバーセキュリティ対処調整センターを設置した。
     3. ○今後の取組
        + サイバーセキュリティ対処調整センターは、 大会関係組織と情報共有システムを介した情報共有の促進及びインシデント発生時の対処支援調整を実施。 また、 重要サービス事業者等も参加する情報共有及びインシデント発生時の対処支援調整等の訓練・演習を実施し、 大会関係組織間で緊密に連絡調整を図るための態勢を整備。 さらに、 大会までの大規模イベント（G20大阪サミット、 ラグビーワールドカップ等）において情報共有及びインシデント発生時の対処に係る試験運用を実施。
        + これらの取組を通じて、 大会に向けて万全の対処態勢の整備を目指す。
  2. サイバーセキュリティお助け隊
     1. 事務局：IPA

1. 東京都としての検討の論点
   1. サイバーセキュリティ協議会への参画の可否
      1. 参加する場合、 中小企業対応の商工部か？
      2. TCYSSとの関係は？
2. IPAとの連携の可能性
   1. 相談対応
      1. インシデント相談対応時のホットライン
         * IPA加賀谷氏と意見交換する？



* + 1. 相談対応のための情報交換
  1. サイバーセキュリティ関連の情報発信
     1. IPA作成普及啓発資料の配布
        + IPAにとってガイドラインはキーコンテンツ



* + 1. Webコンテンツのリンク及び引用
  1. サイバーセキュリティ対策要員、 企業、 製品の確保
     1. プレゼンターカンファレンス



* + - * 研修用資料、 ツール類の更新は？



* 1. サイバーセキュリティ対策の実施支援
     1. Security Action 1つ星、 2つ星、 取得支援
        + サイバーセキュリティ対策の助成金制度
        + 3 つ星は？



* 1. 国等の施策での連携
     1. 国等の網羅的な施策の一環での中小企業への支援策
     2. サイバーセキュリティ協議会
        + TCYSSとの関係
        + 中小のサイバーセキュリティ担当の所管ではない



* + 1. 中小企業サイバーセキュリティ対策支援促進事業
       - （30年度第2次補正予算）



* + - * サイバーセキュリティお助け隊
        + オーバースペックにならないように



* + - * + サイバー保険は？



* + - * 情報セキュリティマネジメント指導業務



* + - * + 登録シスオペが訪問指導



* + - * 中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォームの構築に向けた実現可能性調査



* 1. サイバーセキュリティ関連実態調査
     1. IT化が目的であり、 セキュリティ対策はIT化を円滑に進めるための必要要件の一つ
     2. 2019年3月28日「Security Action宣言事業者における情報セキュリティ対策の実態調査報告書」公開



* + 1. 事例集も



1. 想定される事業・業務
   1. 情報収集・蓄積
      1. 日々のニュースウォッチ
      2. 体系的情報整理
         * ハンドブックの維持・更新
      3. 中小企業経営者向け情報整理
         * 「極意」の追補版作成
         * プレゼンテーション資料作成
   2. 発信
      1. Webでの情報発信
         * 「極意」改訂版
           + HTML版
           + 電子書籍版
         * 体系的情報発信
      2. Twitterでの情報発信
         * 日々のセキュリティ関連ニュースから中小企業向けの厳選
      3. 出張相談、 外部機関でのプレゼンテーション
      4. 相談対応
         * 来庁者対応
         * メール対応
         * 電話対応
2. 対策の年次計画
   1. 2019年度
      1. Twitter
      2. Webページ
         * 「極意」テキスト版、 追補版発行
   2. 2020年度
      1. 東京オリンピック　サイバーセキュリティ対処調整センターとの連携
      2. サイバーセキュリティ協議会への参加
         * TCYSSの発展的解消？参加組織拡大？
      3. Webページ更新
         * 「極意」電子書籍版発行
         * 体系的情報発信
           + 随時更新
   3. 2021年度
      1. お助け隊（東京都）との連携
         * 相談窓口、 駆けつけ支援体制
      2. 「極意」冊子体版発行
      3. Webページ更新
   4. サブトピック 4
3. NISC対応についての考察

リレーションシップ:

開始点 [2019年9月19日　NISC会議対応についての考察](#NDkwMTczMTAxMzExOTM2Mw==);

* 1. 改版履歴
     1. （20190925）
     2. （20190919）
  2. 意見を述べる立場
     1. ⇒非常勤専門員の職務として
        + 学識・知識・経験等に基づき、 業務に補助的に従事し、 行政運営を補完する
  3. 現状認識
     1. 相談
        + 相談は、 件数、 相談内容ともに、 実績は評価されていない
     2. 「中小企業向けサイバーセキュリティ対策の極意」小冊子及びPDFファイル
        + 内容、 発行部数ともに評価されている
        + **TCYSSは、 これにより、 NISC、 IPAに一定の存在感を示せているのではないか？**
          - NISC, IPAのウェブページでの紹介
          - 活動状況の情報提供依頼
  4. 国の施策の体系の中での位置づけ
     1. **サイバーセキュリティ基本法の一部を改正（2019年4月1日施行）**
        + 基本法の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（個人・組織による平時からの対策）**

**平時・事象発生時の各々の努力だけでない、 情報共有、 個人と組織間の相互連携・協働を新たな「公衆衛生活動」ととらえる**

**国の行政機関、 地方公共団体、 重要インフラ事業者、 サイバー関連事業者、 教育研究機関、 有識者 等**

**東京都は、 地方公共団体の中核的団体**

****

* + - * １．サイバーセキュリティ協議会の創設
        + 官民の多様な主体が相互に連携して情報共有を図り、 必要な対策等について協議を行うための協議会を、 サイバーセキュリティ戦略本部長等が創設する。
        + 協議会の構成員（事務局：NISC、 専門機関）

国の行政機関、 地方公共団体、 重要インフラ事業者、 サイバー関連事業者、 教育研究機関、 有識者 等

* + - * ２．サイバーセキュリティ戦略本部による連絡調整の推進
        + サイバーセキュリティ戦略本部の所掌事務に、 サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整に関する事務を追加する。
    1. **サイバーセキュリティ戦略(2018年7月27日閣議決定）**
       - 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
    2. **サイバーセキュリティ2019(2018年7月27日閣議決定）**
       - サイバーセキュリティ戦略の目指す姿と対処方針
       - 年次報告（2018年度）と年次計画（2019年度）
       - 参考資料1-2(サイバーセキュリティ戦略本部第22回会合2019.5.23)
         * (2) 重点的な対象とその内容

・様々な対象に幅広く実施することを前提としつつ、 以下の対象について、 重点的に取組を実施

**①中小企業中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」の地域実証、 「SECURITY ACTION」活用の促進、 中小企業支援ネットワークによる啓発等**

・・・

* + 1. **サイバーセキュリティ意識・行動強化プログラム**
       - 「サイバーセキュリティ戦略」(2018年7月閣議決定)に基づき、 普及啓発について、 2020年東京オリンピック・パラリンピック競技大会を見据えつつ、 産学官民の関係者が円滑かつ効果的に活動し、 有機的に連携できるよう、 本プログラムを策定。
       - 「サイバーセキュリティ意識・行動強化プログラム（案）」に関する意見募集
         * 「サイバーセキュリティ戦略」（平成30年７月27日閣議決定）において、 『産学官民の関係者が円滑かつ効果的に活動し、 有機的に連携できるよう、 サイバーセキュリティの普及啓発に向けた総合的な戦略及びアクションプランを策定すること』とされています。 これに基づき、 サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会にて、 「サイバーセキュリティ意識・行動強化プログラム」の策定を目指して議論を行い、 この度、 案をまとめました。 　つきましては、 本件について以下の要領で広く国民の皆様からの意見を募集いたします。
       - サイバーセキュリティ戦略本部第21回会合（2019年1月24日）決定
         * ３ 今後の取組の基本的な考え方

・対策に関する情報が国民一人一人や中小企業に必ずしも行き届いていない、 いわば「サイバーセキュリティのラストワンマイル」の状況。

・「３つの視点」から取組を推進：①継続的な実施、 ②対象に合わせた適切なツール・コンテンツの提供、 ③関係者間の連携の促進

* + - * + ４ 具体的取組の推進

(2) 重点的な対象とその内容

・様々な対象に幅広く実施することを前提としつつ、 以下の対象について、 重点的に取組を実施

**①中小企業中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」の地域実証、 「SECURITY ACTION」活用の促進、 中小企業支援ネットワークによる啓発等**

②若年層無自覚なまま加害者になることを防ぐためのリテラシー向上の取組、 先端的人材育成施策の推進

③地域における取組の支援産学官連携型の取組の活性化、 高専学生によるボランティア活動等

* + - * TCYSSに関する言及
        + 官民の取組状況

タイムリーな情報発信・相談窓口

小規模・中小企業を対象として

* + - * + 具体的取組の推進

重点的な対象とその内容

中小企業

**自治体が警察組織や中小企業支援機関、サイバーセキュリティ支援機関な どと連携して設立した中小企業支援ネットワーク等において、 サイバーセキュリティの啓発、 情報共有、事案発生時の相互連携等に取り組むと共に、 サイバーセキュリティ相談窓口を設け、電子申請や電話、窓口による相談対応を行う。 （東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss）等）**

* 1. 姿勢
     1. 国として
        + 連携体制の強化
          - NISCをはじめとした関係機関が連携し、 各機関の役割や対象を位置付けて、 ラストワンマイルに情報が行き着くよう配慮しつつ取組を進めていくことが重要である。 このため、 互いに連携・補完しながら、 効果的・効率的に実施する体制づくりを目指す。
     2. 都として
        + 都は、 国全体の枠組みで、 地方公共団体の中心的な事業実施部隊としての役割を果たす姿勢があるか？
     3. 産業労働局として
        + 中小企業に支援策として、 関係機関と連携してセキュリティ対策を強化することが重要であるとの考えを持っているか？
     4. 経営支援課サイバーセキュリティ担当として
        + 都庁の施策が、 実施体制内の姿勢・能力の差で大きく変わることはあってはならない
        + 個人的な意見・見解でなく、 都、 局の姿勢を踏まえて、 大所高所からの判断が必要
  2. 私見
     1. 公務員倫理
        + 国民目線で考え、 サービス向上のため、 常に創意工夫に努める
        + 職務に権限を持つことは、 責任と義務が発生する。 また、 権限を行使しないことは不作為と見なされる可能性もある。
        + 本来果たすべき職務を遂行しない不作為の行為は、 公務員倫理違反であり、 またコンプライアンス（法令遵守）にも違反し、 訴訟のリスクを負う
     2. 国の施策の一環として実施できることは歓迎すべきことではないか
        + 「サイバーセキュリティ意識・行動強化プログラム」の本文、 「サイバーセキュリティ2019」の参考資料にTCYSS事業が記載されたことは歓迎すべきことではないか
          - 一般的に、 各府省は、 事業計画の承認、 予算要求をしやすくするために、 国の基本方針、 各種方針、 計画に、 固有名詞が記載されるよう努力する。
          - そういう努力もせず記載されたことは感謝すべきことではないか
     3. サイバーセキュリティ協議会は、 TCYSSの全国版
        + 地方公共団体として東京都は参加したほうが？
        + TCYSSはこの枠組みの一組織体として参加すべきでは？
     4. サイバーセキュリティお助け隊の実証実験は、 東京都の相談窓口の拡張版
        + 東京都の相談窓口はこの枠組みの一組織体として位置づけられるべきでは？
     5. 評価に関して
        + これらと連携した活動を行うことにより、 意義ある組織として評価されるのではないか
        + 監査対応では、 専門員の業務内容が指摘の対象になったが、
          - NISC等に評価されたのは、 小冊子の発行等による有用な情報発信機能であり、 その小冊子の章立て、 内容原案を作成したのは職員ではなく、 専門員である。
        + また、 今後の事業計画、 予算要求のためにも
          - 監査資料で提出した業務配分で示した１：４：５は、 今後のあるべき姿に近いものであり、 実際にそのように運用できる専門員体制を確立するとともに、 その業務の成果をエビデンスによって評価できるようにしていくことが重要ではないか

1. 【参考資料】
   1. サイバーセキュリティ戦略【2018戦略】
      1. 4.2.5 2020年東京大会とその後を見据えた取組
         * 2020年東京大会後も各種施策は適用範囲を拡大して引き続き推進し、 整備した仕組み、 その運用経験及びノウハウは、 レガシーとして、 以降の我が国の持続的なサイバーセキュリティの強化のために活用していく。
         * [1] 2020年東京大会に向けた態勢の整備
         * [2] 未来につながる成果の継承
           + 2020年東京大会の態勢整備のための各種施策を引き続き推進し、 整備した仕組み、 その運用経験及びノウハウは、 レガシーとして、 2020年東京大会以降の我が国の持続的なサイバーセキュリティの強化のために活用していく。
           + また、 構築した「サイバーセキュリティ対処調整センター」を、 サイバー攻撃等に対してオールジャパンで力を合わせて対処するための調整役・調整窓口（ナショナルCSIRT）として活用し、 サイバーセキュリティの基本的な在り方でも掲げた「リスクマネジメント」の手法については、 広く全国の事業者等に適用できるよう整備・普及を促進していく。
           + Subtopic
      2. 4.2.6 従来の枠を超えた情報共有・連携体制の構築
         * 他の組織との連携を重視する意識が官民ともに着実に広がっており、 行政機関や重要インフラ事業者に限らず、 幅広い主体が情報共有に取り組み始めている。
         * サイバー空間と実空間の一体化が進展し、 サイバー空間と密接に関連する分野が一層増加する中、 サイバーセキュリティに資する情報の共有に取り組むべき分野や関係者の範囲は、 更に広がり続けることが予想される。
         * そのため、 サイバーセキュリティの基本的な在り方で掲げた「参加・連携・協働」の観点から、 各主体との緊密な連携の下、 国はISAC※56を含む既存の情報共有における取組の推進を支援するとともに、 新たな役割を果たしていく必要がある。
         * (ISAC:Information Sharing and Analysis Centerの略。 サイバーセキュリティに関する情報収集や、 収集した情報の分析等を行う組織。 分析した情報はISACに参加する会員間で共有され、 各々のセキュリティ対策に役立てられる。 （出典：サイバーセキュリティ2017（平成29年8月25日））)
         * [1] 多様な主体の情報共有・連携の推進
           + 情報共有に十分な知見を有する専門機関を含む官民の多様な主体が、 安心して相互にサイバーセキュリティ対策に資する情報の共有を図るための新たな体制を構築する。
           + このような取組を進めることで、 官と民、 業界、 国内外といった枠を超えた情報の共有・連携を推進していく。
           + また、 官民で既に複数組織されている情報共有体制において、 関係者の更なる負担が生じることのないよう、 各々の特色や役割を踏まえて、 連携や統合について検討していく。
         * [2] 情報共有・連携の新たな段階へ
           + サイバーセキュリティを高めるためには双方向の情報共有が不可欠であるとの認識を社会に広く醸成していく。
           + さらに、 我が国の情報共有の仕組みを発展させつつ、 国際社会との戦略的な連携を視野に入れることも肝要である。
           + 官民や業界といった従来の枠を超えて、 各々の主体が共存・発展していくことのできる関係を構築できるよう、 国は各主体と緊密に連携し、 環境整備に積極的に取り組んでいくことで、 サイバーセキュリティに関する情報共有・連携が新たな段階へ移行していく。
      3. 4.4 横断的施策
         * 4.4.1 人材育成・確保
           + [1] 戦略マネジメント層の育成・定着

経営層が示す経営戦略や事業戦略の下、 組織がマネジメントすべき様々なリスクの一つとして、 業務やサービス等を実現するために必要なサイバーセキュリティに係るリスクを認識し、 事業継続と価値創出に係るリスクマネジメントを中心となって支える立場として、 社内外の実務者・専門家を活用・指揮しつつ、 対策や事案への対応を実践する役割を果たし得る人材が求められている

* + - * + [2] 実務者層・技術者層の育成

経営層の方針を理解しつつ、 他の専門人材と円滑にコミュニケーションをとりながらチームの一員として対処ができるようにすることが重要である。

戦略マネジメント層が示す概念的・抽象的な考えを理解し、 それを具体化するとともに、 様々な関係者と円滑なコミュニケーションができるような学び直しによるスキルの開発や実践的な演習が必要である。

* + - * 4.4.3 全員参加による協働
        + 実空間における防犯対策や交通安全対策と同様に、 サイバー空間で活動する主体としての国民一人一人がサイバーセキュリティに対する意識・理解を醸成し、 サイバー空間における様々なリスクに対して対処できることが不可欠になっている。
        + 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、 お互いの役割分担の下で、 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というかたちでリーダーシップを発揮していく必要がある。
        + 内閣サイバーセキュリティセンターが中心となって、 産学官民の関係者が円滑かつ効果的に活動し、 有機的に連携できるよう、 国は、 サイバーセキュリティの普及啓発に向けた総合的な戦略及び具体的なアクションプランを策定するとともに、 必要な情報発信や国民からの相談対応を行う。
        + また、 産学官民の様々なコミュニティの代表が参加する協議会の場を活用しながら、 関係者による実践を推進していく。
    1. ５．推進体制
       - サイバーセキュリティの確保を通じて、 情報通信技術及びデータの利活用を促進※64し、 経済・社会活動の基盤とする※65こと、 我が国の安全保障を万全のものとする※66ことは、 従来からの我が国政府の方針である。
         * ※64 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（平成29年5月30日閣議決定）は、 「データ利活用の促進に当たっては、 個人情報やプライバシーの保護、 サイバーセキュリティ対策、 知的財産権の在り方、 データの品質や信頼性・安全性の確保、 AI、 ロボット時代の倫理の在り方など、 同時並行的に対策を講じておくことは言うまでもない」としている。
         * ※65 未来投資戦略2017は、 「あらゆる場面で快適で豊かに生活できる超スマート社会、 Society 5.0では、 安全なサイバー空間の確保が経済・社会活動の重要な基盤」としている。
         * ※66 国家安全保障戦略（平成25年12月17日閣議決定・国家安全保障会議決定）は、 「情報の自由な流通による経済社会やイノベーションを推進するために必要な場であるサイバー空間の防護は、 我が国の安全保障を万全とするとの観点から、 不可欠」としている。
       - 本部は、 情報収集・分析機能の強化や、 サイバー攻撃の速やかな検知・分析・判断・対処を一体的サイクルとして行う機能を有する体制の整備に向けて、 官民連携を促進する。