資料34－１

「ICTサイバーセキュリティ総合対策2021」に基づく取組

令和3年10月

サイバーセキュリティタスクフォース事務局

サイバーセキュリティ戦略（令和3年9月28日閣議決定）について

サイバーセキュリティ戦略(2021年９月28日閣議決定)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**に向けて行ってきた取組

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～

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

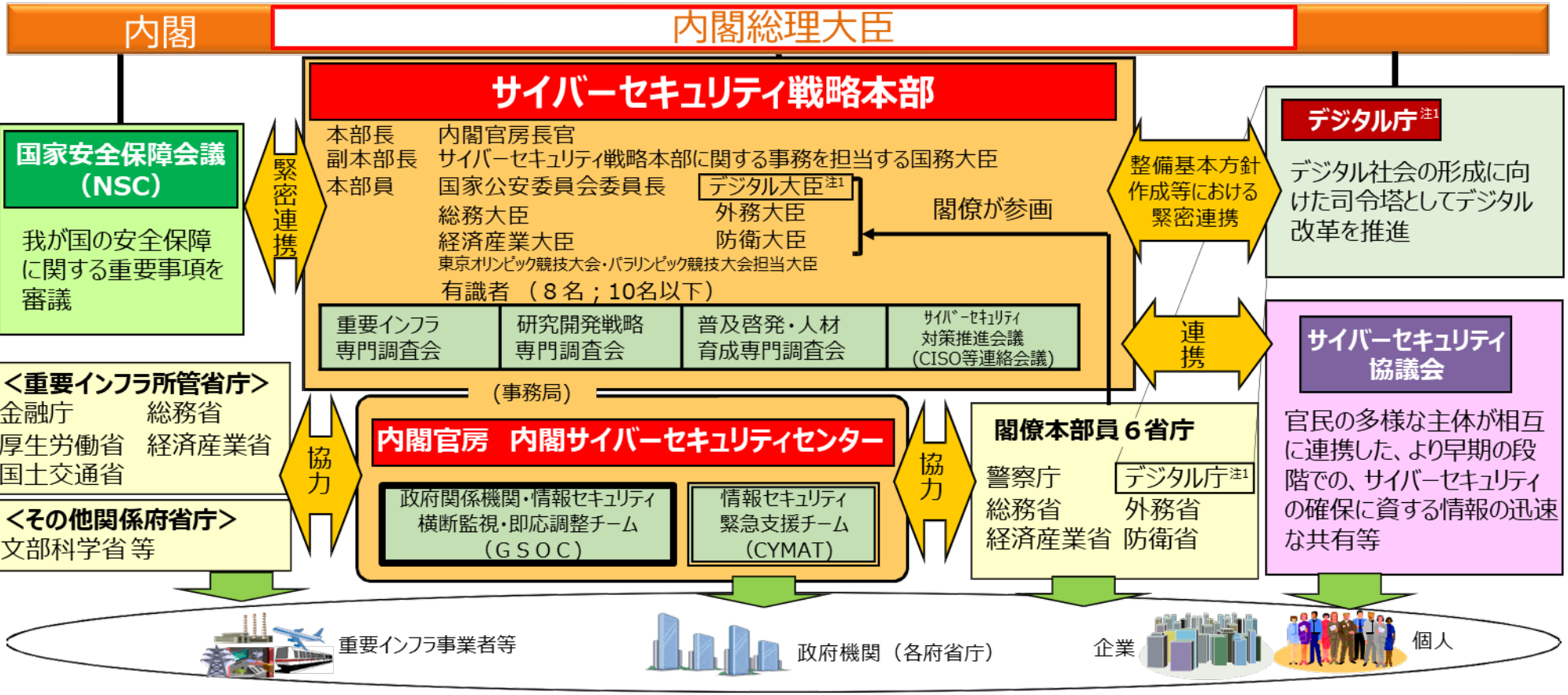
公共空間化と相互連関・連鎖が進展する サイバー空間全体を俯瞰した 安全・安心の確保

「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

サイバーセキュリティ戦略（推進体制）

- **我が国の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。
- 各主体に期待される具体的な対策につながるよう、また、国際協調の重要性を認識し、攻撃者に対する抑止の効果や各国政府に対する我が国の立場への理解を訴求するよう、NISCと関係府省庁が連携して、本戦略を国内外の関係者に積極的に発信。
- 本部は、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備を行う。
- 年次報告・年次計画は、一体的に検討を行い、前年度の取組実績、評価及び次年度の取組を、戦略の事項に沿って、一連の流れを示すように整理。



（注1）デジタル社会形成基本法（令和３年法律第35号）、デジタル庁設置法（令和３年法律第36号）。（令和３年９月１日施行）

サイバーセキュリティ戦略の構成

中長期的

1　2020年代を迎えた日本をとりまく時代認識

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、東京大会に向けた取組の活用

2　本戦略における基本的な理念

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

環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策

＜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 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
（３）安全保障の観点からの取組強化

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．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

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

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」の確保

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

「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

「ICTサイバーセキュリティ総合対策2021」に基づく取組

（１）「電気通信事業ガバナンス検討会」における検討の状況

（２）「電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会」における検討の状況

（３） 人材育成・普及啓発の進捗状況

「ICTサイバーセキュリティ総合対策2021」（令和3年7月）の概要

＜政策課題に対処するための主な施策＞

＜電気通信事業者における安全かつ信頼性の高いネットワークの確保＞

5Gを含めて、電気通信事業者のネットワークや電気通信サービスにおけるリスクの高まりに応じた適切なセキュリティ対策を講じる必要

＜COVID-19への対応を受けたセキュリティ対策の推進＞

COVID-19感染拡大が続く中、中小企業等におけるテレワーク推進のためセキュリティ対策が急務。コロナ後も視野に、トラストサービスの推進も重要。

＜デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策＞

IoT、クラウド、スマートシティについて、それぞれの課題に応じた適切な対策を推進していくことが必要。

＜サイバーセキュリティ情報に関する産学官での連携・共有等の促進＞

有効な技術や知見の共有による社会全体での対策の底上げ等が重要。

「ICTサイバーセキュリティ総合対策2021」の構成

Ⅰ　改定に当たっての主要な政策課題

Ⅱ　情報通信サービス・ネットワークの個別分野に関する具体的施策

1. 電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進

（1）安全かつ信頼性の高いネットワークの確保　…取組（1）

（2）サイバー攻撃に対する電気通信事業者の積極的な対策の実現　…取組（2）

（3）5Gの本格的な普及に向けたセキュリティ対策の強化

2. COVID-19への対応を受けたセキュリティ対策の推進

（1）テレワークセキュリティの確保

（2）トラストサービスの制度化と普及促進

3. デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策の推進

（1）IoTのセキュリティ対策

（2）クラウドサービスの利用の進展を踏まえた対応

（3）スマートシティのセキュリティ対策

4. 分野別の具体的施策

（1）無線LANのセキュリティ対策

（2）放送分野のセキュリティ対策

（3）地域の情報通信サービスのセキュリティの確保

Ⅲ　横断的施策

1. サイバーセキュリティ情報に関する産学官での連携・共有等の促進

（1）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（2）サイバー攻撃被害情報の適切な共有及び公表の促進

（3）その他の情報共有・情報開示の促進

2. ICTサイバーセキュリティに係る横断的施策

（1）国際連携の推進

（2）研究開発の推進

（3）人材育成・普及啓発の推進　…取組（3）

別添：プログレスレポート2021（総合対策2020の各施策の進捗状況）

＜施策の推進・実施に当たっての基本的考え方・主な留意点＞

①サイバーセキュリティ戦略に定める５原則を踏まえた施策展開

情報の自由な流通、法の支配、開放性、自律性、多様な主体の連携の５原則を確保。

②サービス・製品の提供側と利用側の双方の観点からの施策展開

③各施策の粒度やタイムスパン等の違いに応じた施策展開

具体的・政策的施策の双方、短期的・中長期的施策の双方を総合的・有機的に推進。

「ICTサイバーセキュリティ総合対策2021」に基づく取組

（１）「電気通信事業ガバナンス検討会」における検討の状況

（２）「電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会」における検討の状況

（３） 人材育成・普及啓発の進捗状況

電気通信事業ガバナンス検討会について

1．背景・目的

- 「デジタル社会」の実現のためには、その中枢基盤として、サイバー空間とフィジカル空間を繋ぐ神経網である通信サービス・ネットワークが安心・安全で信頼され、継続的・安定的かつ確実に提供されることが不可欠。
- 最近、通信サービス・ネットワークを司る電気通信事業者において、利用者の個人情報や通信の秘密の漏えい事案が発生し、海外の委託先等を通じ、これらのデータにアクセス可能な状態にあることに関するリスク等が顕在化。
- 更に、電気通信事業者に対するサイバー攻撃により、通信サービスの提供の停止に至る事案や、通信設備に関するデータが外部に漏えいした恐れのある事案など、サイバー攻撃のリスク等が深刻化。
- デジタル時代における安心・安全で信頼できる通信サービス・ネットワークの確保を図るため、電気通信事業者におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の在り方を検証し、今後の対策を検討。

2．主な検討事項

① 電気通信事業者におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の今後の在り方

② 上記①を踏まえた、政策的な対応の在り方

③ その他

3．体制

- データ、サイバーセキュリティ及びガバナンスに関する有識者から構成される検討会（座長：大橋教授）を設置。構成員は右図のとおり。
- オブザーバとして、IT総合戦略室、内閣サイバーセキュリティセンター（NISC）、個人情報保護委員会事務局及び内閣官房国家安全保障局（NSS）が参加。

相田　仁	東京大学大学院工学系研究科教授
石井　夏生利	中央大学国際情報学部教授
上沼　紫野	虎ノ門南法律事務所弁護士
大橋　弘	東京大学公共政策大学院院長
後藤　厚宏	情報セキュリティ大学院大学学長
中尾　康二	（一社）ICT-ISAC顧問 （国研）NICTサイバーセキュリティ研究所主管研究員
中村　修	慶應義塾大学環境情報学部教授
古谷　由紀子	（公社）日本消費生活アドバイザー・コンサルタント・相談員協会監事
森　亮二	英知法律事務所弁護士
山本　龍彦	慶應義塾大学大学院法務研究科教授

電気通信事業ガバナンス検討会における主な論点

①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策

利用者の利益の保護を確保する観点から、大量の情報を所有する者による電気通信事業に係る情報の漏えい・不適正な取扱い等を原因として、利用者やサービス提供に影響を及ぼすおそれがあることを踏まえ、新たに利用者情報の適正管理等を促進するための規律を検討。

政府による規制・ガイドライン等の新たな枠組みを構築し、情報の適正管理等に関する事業者自らの取組を促進する方策を検討。

- 対象となる情報・者の整理
- 利用者情報の管理方法等
- 設備関連情報に係る対策

②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策

電気通信役務の円滑な提供を確保する観点から、ネットワークを構成する設備の多様化を踏まえ、クラウド事業者等の設備やサービスを使用して提供される多様な通信サービスを前提とした設備規律を検討。

また、単独の事業者では対応が困難なリスクに対応するため、事業者間連携によるサイバー攻撃対策等を検討。あわせて、情報の不適正な取扱いや事故による多様な法益侵害を最小化する観点から、それらの未然防止や被害軽減を図るため、兆候段階における事態の速やかな報告や対策を検討。

- 設備のクラウド化・多様化への対応
- 事業者間連携によるサイバー攻撃対策等
- 事故の兆候段階からの報告義務

③情報の適正な取扱いや通信サービスの提供等に関する利用者等への情報提供

利用者に対しては、平常時から、情報の適正な取扱いや通信サービスの提供に関する情報、情報の漏えい・不適正な取扱い等や事故が生じた際の対処方策等について利用者に理解しやすい形での周知広報に努め、非常時においても、電気通信事業者等は、適時に適切な方法で情報提供を行い、利用者が適切な対応ができるような方策を検討。

※第9回電気通信事業ガバナンス検討会資料9－1より抜粋

「ICTサイバーセキュリティ総合対策2021」に基づく取組

（１）「電気通信事業ガバナンス検討会」における検討の状況

（２）「電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会」における検討の状況

（３） 人材育成・普及啓発の進捗状況

電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会

- サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行うことを目的として、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」（総合通信基盤局長及びサイバーセキュリティ統括官による原則非公開の研究会）を開催している。
- 平成26年４月には「第一次とりまとめ」、平成27年９月には「第二次とりまとめ」をそれぞれ公表したところ。
- 平成30年２月より研究会を再開し、電気通信事業法及び国立研究開発法人情報通信研究機構法の改正も踏まえ、近年新たに整理が必要となった課題等について検討し、同年９月に「第三次とりまとめ」を公表。
- 第一次～第三次とりまとめについては、関係団体が作成する「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」に反映されている。
- 今般、サイバー攻撃に予防的に対処するため、①ISPが、平時から自らのネットワーク内の通信トラフィックデータを把握・分析し、C&Cサーバである可能性が高い機器の検知等を行うこと、②検知したC&Cサーバである可能性が高い機器に関する情報を他の電気通信事業者と共有することについて、通信の秘密との関係性を整理し、「第四次とりまとめ」として公表するべく、本年６月29日に第10回WGを、８月31日に第11回WG、10月１日に第７回親会を開催し、現在は、第四次とりまとめ案の意見募集中。

構成員

＜本会合＞	（座長）	鎮目　征樹	学習院大学法学部 教授
	（座長代理）	宍戸　常寿	東京大学大学院法学政治学研究科 教授
		木村　孝	一般社団法人日本インターネットプロバイダー協会 事務局長
		木村　たま代	主婦連合会 事務局長
		小山　覚	一般社団法人ICT-ISAC ステアリング・コミッティ 運営委員長
		中尾　康二	国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 主管研究員
		藤本　正代	情報セキュリティ大学院大学 教授
		森　亮二	英知法律事務所 弁護士
		吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院 准教授
＜WG＞	（主査）	宍戸　常寿	東京大学大学院法学政治学研究科 教授
	（主査代理）	森　亮二	英知法律事務所 弁護士
		井上　大介	国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティネクサス ネクサス長
		木村　孝	一般社団法人日本インターネットプロバイダー協会 事務局長
		小山　覚	一般社団法人ICT-ISAC ステアリング・コミッティ 運営委員長
		齋藤　衛	株式会社インターネットイニシアティブ セキュリティ本部長
		鎮目　征樹	学習院大学法学部 教授
		丸橋　透	明治大学法学部 教授
		吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院 准教授

第四次とりまとめ（案）のポイント

ポイント

（1） 平時におけるフロー情報の収集・蓄積・分析によるC&Cサーバである可能性が高い機器の検知について

→ 正当業務行為として許容される

〈考え方〉

ISP※が平時において、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IP アドレス等のフロー情報を収集・蓄積・分析して未知のC&Cサーバを検知することは、必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報をC&Cサーバ検知以外の用途で利用しない場合に限り、正当業務行為として許容される。

（2） フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有について

→ 通信の秘密の保護規定に抵触しない

〈考え方〉

一のISPが、（1）の取組により得られたC&Cサーバに関する情報（IPアドレス、ポート番号）を取りまとめてリスト化したものを、サイバーセキュリティ対策を行うために適切な事業者団体等に提供することは、通信の秘密の保護規定に抵触しない。

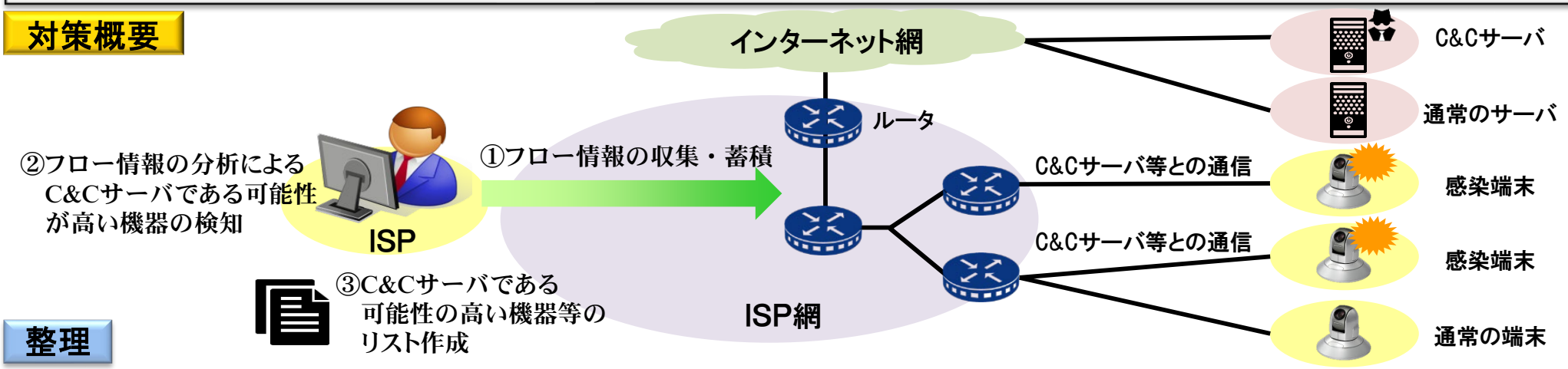
※ Internet Service Provider の略であり、インターネット接続サービスを提供している事業者のこと

検討課題（１） 平時におけるフロー情報の収集・蓄積・分析によるC&Cサーバである可能性が高い機器の検知

論点

ISPがサイバー攻撃に予防的に対処するため、平時から、ISPが、自らのネットワーク内の通信トラフィックに係るデータを収集・蓄積・分析し、C&Cサーバである可能性が高い機器の検知を行うことが考えられる。具体的には、現状多くのISPにおいて、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IPアドレス及びポート番号等の情報（フロー情報）を、通信の傾向把握のために収集・活用しているところであるが、これを分析して未知のC&Cサーバの検知を行うことが考えられる。このような取組は、通信の秘密との関係上どのように整理が可能か。

対策概要



整理

以下のことから、本件対策は、正当業務行為として違法性が阻却される。

「目的の正当性」：本件対策は、DDoS攻撃等のC&Cサーバを起点とするサイバー攻撃が発生する前から未知のC&Cサーバ等を検知し、その検知した情報をもとに、各ISPにおいて適切な対処ができるようにすることにより、自己の電気通信役務の提供への重篤な支障の発生を未然に防止し、または、その被害の拡大を最小限に抑え、電気通信役務の円滑な提供を確保するための措置であり、目的の正当性を認めることができる。

「行為の必要性」：サイバー攻撃の複雑化・巧妙化が進んで攻撃の頻度は高まり、ISPの提供する電気通信ネットワークに対するC&Cサーバを起点としたサイバー攻撃がいつ行われてもおかしくない状態にさらされている等、現在の電気通信ネットワークを取り巻く状況においては、行為の必要性が認められる。

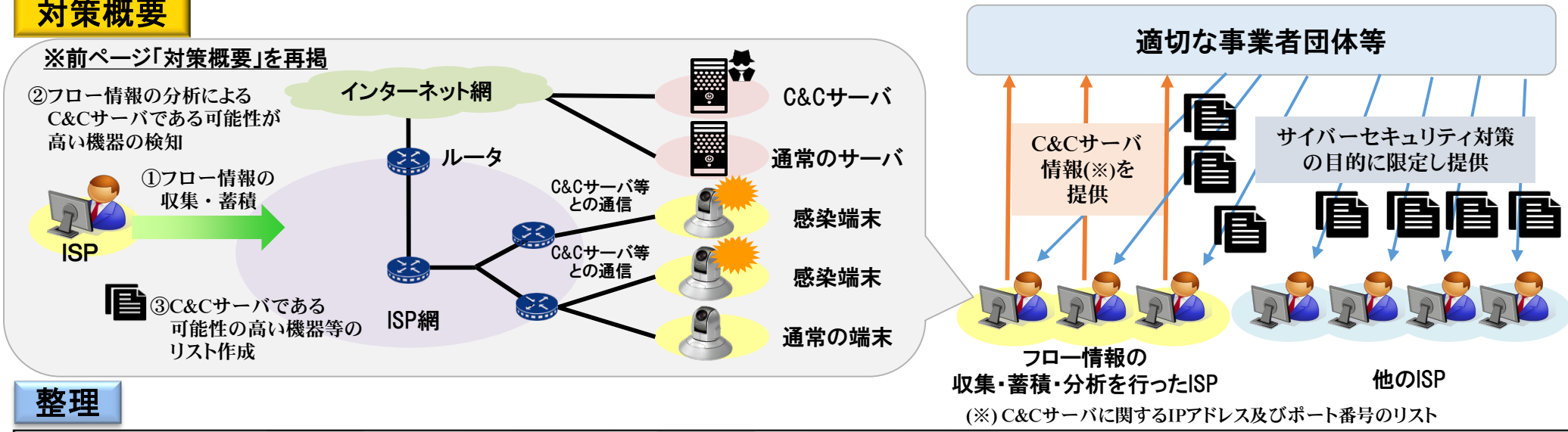
「手段の相当性」：必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報をC&Cサーバ検知以外の用途で利用しない場合には、手段の相当性が認められる。

検討課題（２）フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有

論点

各ISPがサイバー攻撃に対処できるようにする観点から、一のISPが自らの電気通信ネットワーク内のフロー情報の収集・蓄積・分析によって検知したC&Cサーバに関する情報（IPアドレス、ポート番号）を、適切な事業者団体等に提供することが考えられる。このような取組は、通信の秘密との関係上どのように整理が可能か。

対策概要



整理

本件において対象とされるC&Cサーバに関する情報は、必要最小限のフロー情報について、C&Cサーバを検知する目的のみのために集合的に分析した結果として得られたC&Cサーバに関するIPアドレス及びポート番号を取りまとめてリスト化したものである。すなわち、個別の通信と切り離され、個々の通信がいつ誰に対して行われたかといった個々の通信の構成要素を明らかにすることにつながらないものである。

したがって、このように、C&Cサーバに関するIPアドレス及びポート番号のリストの情報のみを、サイバーセキュリティ対策を行うために必要最小限の情報として、適切な事業者団体等に提供することは、通信の秘密の保護規定に直ちに抵触するとまではいえないと考えられる 。

「ICTサイバーセキュリティ総合対策2021」に基づく取組

（１）「電気通信事業ガバナンス検討会」における検討の状況

（２）「電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会」における検討の状況

（３）人材育成・普及啓発の進捗状況

実践的サイバー防御演習（CYDER）

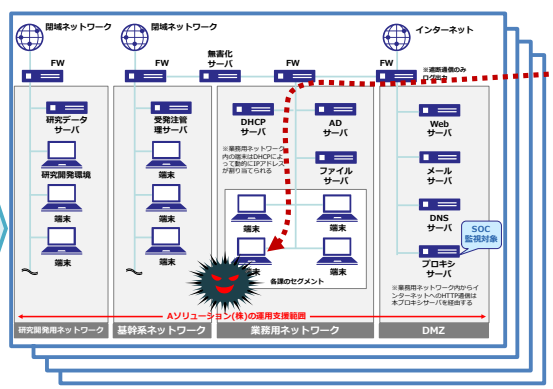
CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習(CYDER)**を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。 参加申込 → https://cyder.nict.go.jp
  ※2017年度：3,009名／2018年度：2,666名／2019年度：3,090名／2020年度：2,648名、2021年度：1,973名申込済（10/12時点）

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント対処能力の向上

令和３年度の実施計画

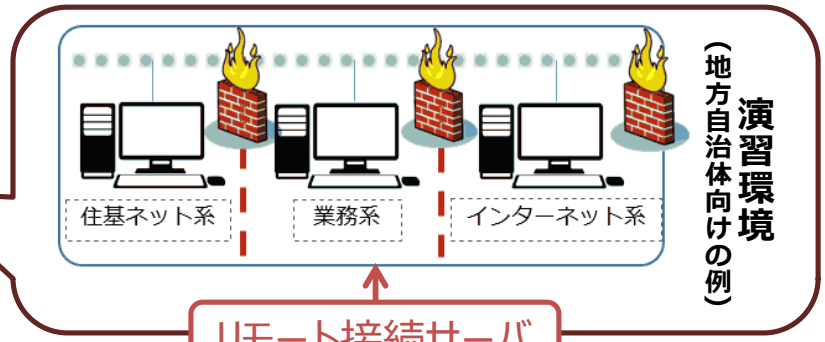
コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	６５回	７月～翌年２月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国１１地域	２１回	10月～翌年２月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	翌年１月～２月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	２回	翌年１月～２月
オンラインA	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	（受講者職場等）	随時	11月～翌年２月

令和３年度から**新規**開設

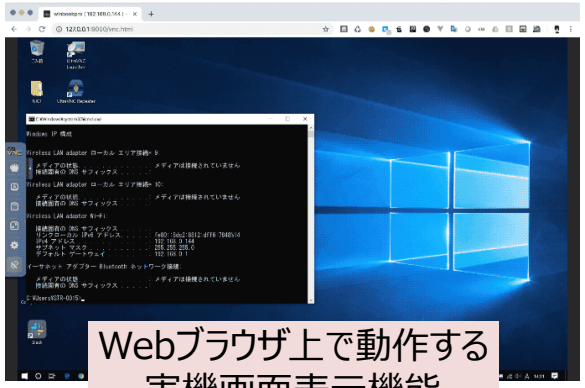
CYDERのオンライン受講

- **感染症拡大防止対策**として、また、**地理的・時間的要因**等によりCYDERが受講できない方への対応として、**オンライン受講環境**を**現在整備中**。
- 自組織のパソコンの**Webブラウザから演習環境に接続**し、**ｅラーニング方式**により演習を**受講**。
- 令和３年８月まで試験提供を実施し、改修を加えた上で、**令和３年１１月中に正式提供予定**。

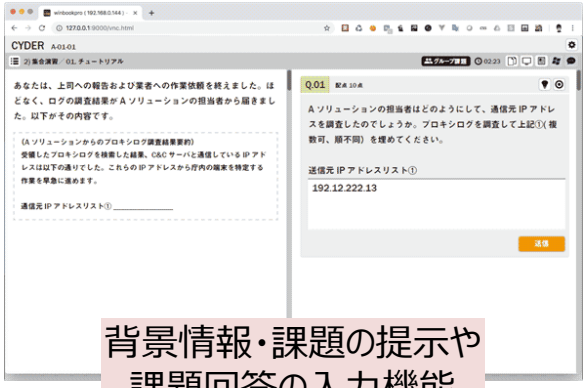
NICT内の大規模計算環境



自身のPC上の**Webブラウザ**において**遠隔受講機能**を利用可能



Webブラウザ上で動作する
実機画面表示機能



背景情報・課題の提示や
課題回答の入力機能

解説表示機能や
チュートリアル表示機能

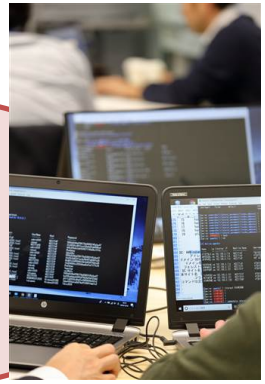
東京大会に向けた実践的サイバー演習（サイバーコロッセオ）

- 高度化・多様化するサイバー攻撃に備え、東京オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象**とした、**高度な攻撃に対処可能な人材の育成**を行う実践的サイバー演習**「サイバーコロッセオ」**を平成30年２月から本格的に実施。
- 大会運営システム等のネットワーク環境を模擬し、**実機演習**により攻撃対処手法を学ぶ**「コロッセオ演習」**に加え、平成30年度からは、**講義演習形式**によりセキュリティ関係の知識や技能を学ぶ**「コロッセオカレッジ」**を実施。
- 令和２年度の事業終了までに、コロッセオ演習で延べ**571名**、コロッセオカレッジで延べ**1,717名**の人材を育成。

サイバーコロッセオ概要

コロッセオ演習

実機演習を伴っての演習
（攻防型演習を含む）



コロッセオカレッジ

講義演習形式により
セキュリティ関係の
知識や技能を学習
（20種の講義科目を開講）

コロッセオ演習の特徴

- 大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を模擬した、演習舞台（仮想ネットワーク環境）を構築。
- 東京大会時に想定されるサイバー攻撃を擬似的に発生させることができるようにし、本格的な攻防型演習等を繰り返し実施。

コロッセオ演習の当日以外でも
学習可能なコンテンツも提供

「**攻防型演習**」とは・・・
受講者が複数チームに分かれ、自組織のネットワークの守備と他チームのネットワークへの攻撃を両方体験することで、攻撃者側の視点をも踏まえたハイレベルな防御手法の検証及び訓練を行う演習

サイバーコロッセオの実施実績

- 実機演習を伴う**コロッセオ演習**において、**2020年度までに延べ571名**が受講。
- 講義演習形式によりセキュリティの知識等を学ぶ**コロッセオカレッジ**は、**2020年度までに延べ1,717名**が受講。

サイバーコロッセオ受講人数（括弧内は実施回数）

※受講人数は延べ人数

	2017年度	2018年度	2019年度	2020年度	合計
初級コース		３８名（２回）	７２名（４回）	４２名（２回）	**１５２名**（８回）
中級コース	３４名（１回）	５１名（２回）	６７名（５回）	４６名（２回）	**１９８名**（10回）
準上級コース	４０名（１回）	４８名（２回）	５３名（６回）	８０名（４回）	**２２１名**（13回）
コロッセオ演習　計	**７４名**（２回）	**１３７名**（６回）	**１９２名**（15回）	**１６８名**（８回）	**５７１名**（31回）
初級コース	－	５９名（５回）	２５６名（15回）	８７名（５回）	**４０２名**（25回）
中級コース	－	１１１名（４回）	３７２名（21回）	１５１名（７回）	**６３４名**（32回）
準上級コース	－	１７７名（７回）	３６４名（23回）	１４０名（８回）	**６８１名**（38回）
コロッセオカレッジ　計	**－**	**３４７名**（16回）	**９９２名**（59回）	**３７８名**（20回）	**1,７１７名**（95回）

サイバーカレッジ カリキュラム

初級コース
- ◇ ☆ セキュリティ基礎
- ◇ ☆ セキュリティツールE
- ◇ ☆ インシデントレスポンス概論
- ◇ ☆ 個人情報保護関係法令
- ◇ システムアーキテクチャ
- ☆ GDPR

中級コース
- ☆ システムアーキテクチャ
- ◇ ☆ 実践インシデントレスポンス
- ◇ ☆ セキュリティツールM
- ☆ 脆弱性診断実務
- ☆ ペネトレーションテスト実務
- ◇ ☆ 最新セキュリティトレンド
- ◇ ☆ セキュア開発

準上級コース
- ☆ セキュリティツールP
- ◇ ログ・パケット解析実務
- ☆ ログ解析実務
- ◇ ☆ マイクロハードニング
- ◇ ☆ サイバーインテリジェンス
- ◇ ☆ フォレンジック実務
- ◇ ☆ マルウェア解析実務
- ◇ 脆弱性診断実務１
- ◇ 脆弱性診断実務２
- ☆ トラフィック解析実務
- ☆ IRノンテクニカルスキル演習

<凡例>
◇ 2018年度開講
☆ 2019･2020年度開講

サイバーコロッセオの知見を活用したCYDER　Cコースの実施内容

- 2020年度まで実施した「サイバーコロッセオ」のレガシー(遺産)のうち中級A, Bを、CYDERのCコース(準上級)として、2022年1月、2月に各1回ずつ開催
- コロッセオでは1日間で提供していたコースを2日間に延長し、演習スケジュールに余裕を持たせることで、受講者がしっかりと技術を習熟できるように工夫

コースの具体的内容

1回目(案): Web系を主とした攻撃と対処【2022年1月】

脆弱性のあるWebサイトへの攻撃や攻撃ツールを利用した攻撃体験と攻撃解析を通じて防御方法の検討を行う。

- Web系への攻撃を学ぶ
- 自チームから他チームを攻撃
- 各種攻撃ログの調査や分析を行う
  - ✓ 他チームの受講者が行った攻撃を解析
  - ✓ 受講者の攻撃以前に用意しておいた攻撃痕跡を解析

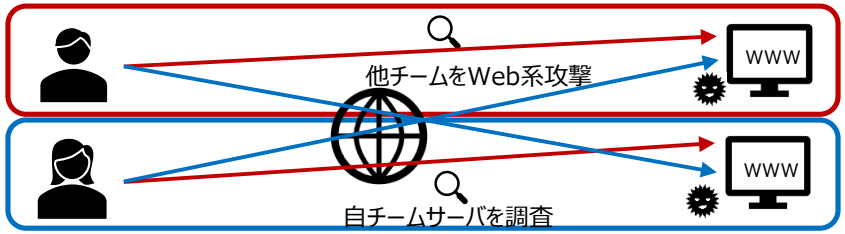
2回目(案): パケット解析を主とした攻撃と対処【2022年2月】

外部公開サーバ経由での侵害を発端とする1つの大規模なインシデントを解き明かす。

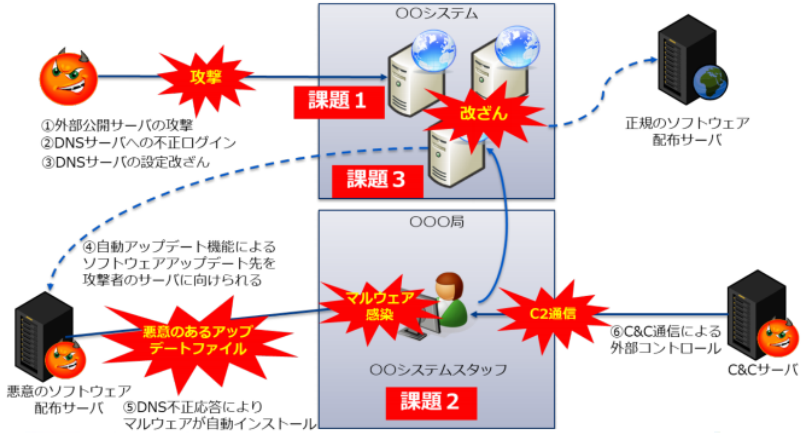
- 外部公開サーバへの侵害(サーバログ調査)
- クライアント端末のマルウェア感染
  - ✓ Proxyログ解析
  - ✓ ネットワークパケット解析
- 被疑サーバの調査

コース内容のイメージ

1回目(案)



2回目(案)



国民のための情報セキュリティサイトの改修

- 総務省は、国民のための情報セキュリティサイトを運用し、情報セキュリティに関する周知啓発を実施。
- 2020年度においても**約130万件のアクセス**があり、多くの国民が閲覧。
  （ https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/ ）
- 内容の最終更新が2013年4月のため、情報が老朽化しており、最新のセキュリティ動向に対応した内容に刷新するべく、2021年度に改修を行う。

改修の進め方

●コンテンツの現行化

・サイバーセキュリティに関する知見（技術を含む）を有する者、サイバーセキュリティ事業者の意見を代表する者（業界団体等）、消費者団体関係者等へのヒアリングを実施。
・内容が老朽化している点、新たに追加すべき点（テレワーク時のセキュリティ等）をとりまとめ。

●レビューの実施

・改定案の全頁を対象として、テクニカルレビューおよび消費者目線レビューを実施。

●公開中WEBサイトの刷新

・CMS対応化、あわせてスマートフォン・タブレットからの閲覧用ページの作成検討。

反映

改修・公開

スケジュール

- **2022年春頃公開予定**