参考資料１

「ICTサイバーセキュリティ総合対策2021」(案)の概要

令 和 ３ 年 ６ 月 ３ 日

事　　務　　局

「ICTサイバーセキュリティ総合対策2021」(案) の概要

～Ⅰ　改定に当たっての主要な政策課題①～

＜ 取りまとめに当たっての考え方 ＞

社会全体のデジタル改革・DX（デジタル・トランスフォーメーション）の推進

＜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）

デジタル改革が目指すデジタル社会のビジョンとして、「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せを実現できる社会」を掲げ、社会全体のデジタル改革・DXを強力に推進。

「自由、公正、かつ安全なサイバー空間」の確保

＜次期サイバーセキュリティ戦略（骨子）＞
（令和3年5月サイバーセキュリティ戦略本部）

サイバー空間の公共空間化が進展する中で、「誰一人取り残さない」サイバーセキュリティの確保(Cybersecurity for all)に取り組むことにより、「自由、公正、かつ安全なサイバー空間」を確保。

IoT、５Gを含むICTサービス・インフラは、デジタル改革・DX推進のための基盤であり、
国民一人ひとりが安心してICTを活用できるよう、サイバーセキュリティを確保することが不可欠の前提。

■　ICTサービス・インフラにおけるサイバーセキュリティを確保するための具体的な施策について、**「ICTサイバーセキュリティ総合対策2021」として取りまとめ**。

「ICTサイバーセキュリティ総合対策2021」(案) の概要

～Ⅰ　改定に当たっての主要な政策課題②～

<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　情報通信ｻｰﾋﾞｽ・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
- (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
- (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．ﾃﾞｼﾞﾀﾙ改革・DX推進の基盤となるｻｰﾋﾞ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．その他の具体的施策
- (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．ｻｲﾊﾞ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) 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．その他の横断的施策
- (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

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」(案) の概要
～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～

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

・電気通信事業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

・BGPやDNSに関して、効果的な脆弱性対の普及方策等の検討 等

（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

・電気通信事業者がサイバー攻撃元を検知できるよう、トラフィック（フロー情報）を把握・分析してC&Cサーバの検知を可能とするための制度的検討・分析手法の実証

（3）5Gの本格的な普及に向けたセキュリティ対策の強化

・制度、技術、情報共有、市場、振興及び国際等の既存の施策の着実な遂行

・Beyond5Gに向けた国際的なルール形成の議論への積極的な関与

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

・「テレワークセキュリティガイドライン」及び中小企業等向けのチェックリスト等を活用した周知

・テレワークセキュリティに関する実態調査と、チェックリスト等の理解度向上に向けた継続的な見直し

（2）トラストサービスの制度化と普及促進

・タイムスタンプ認定制度の適切な運用、eデリバリー等トラストサービスの普及方策の検討

「ICTサイバーセキュリティ総合対策2021」(案)の概要
～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②～

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

・NOTICE(*)調査の詳細化・高度化と、効果的な注意喚起（郵送等、SIerへの注意喚起等）の実施

・ソフトウェア脆弱性を有する機器(例：VPN機器)を特定し、注意喚起を行う手法について検討

(*)脆弱なIoT機器への注意喚起の取組

（２）クラウドサービスの利用の進展を踏まえた対応

・クラウドサービス利用者の設定ミスを防止・軽減するためのクラウドサービス事業者における取組の促進方策の検討

（３）スマートシティのセキュリティ対策

・「スマートシティセキュリティガイドライン(第2.0版)」の国内外への普及推進

4　その他の具体的施策

（１）無線LANのセキュリティ対策

・無線LAN利用者・提供者の双方に対するセキュリティ対策に関する周知啓発

（２）放送分野のセキュリティ対策

・放送設備のサイバーセキュリティ対策の確保に関する技術基準等の制度の着実な運用

（３）地域の情報通信サービスのセキュリティの確保

・地域のセキュリティ関係者のコミュニティ（「地域SECUNITY」）の構築の推進

「ICTサイバーセキュリティ総合対策2021」(案) の概要
～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

・NICTにおける「サイバーセキュリティ統合知的・人材育成基盤」(CYNEX)の早期の本格稼働を目標とした基盤構築 等

（２）サイバー攻撃被害情報の適切な共有及び公表の促進

・自組織に不都合が発生する状況を避けつつ情報共有できるかをまとめたガイダンスを作成、発信

・被害を公表した組織に対する適切な評価や支援の在り方等について検討

（３）その他の情報共有・情報開示の促進

・情報共有基盤の構築促進、民間企業におけるサイバーセキュリティ対策情報の開示促進

2　その他の横断的施策

（１）国際連携の推進

・ ASEAN各国はじめインド太平洋地域等との連携、国際的なISAC間連携、国際標準化の推進、サイバー空間における国際ルールをめぐる議論への積極的参画

（２）研究開発の推進

・基礎的・基盤的な研究、IoT機器のセキュリティ技術、脆弱性の検証手法の確立 等

（３）人材育成・普及啓発の推進

・NICT「ナショナルサイバートレーニングセンター」の取組、利用者への普及啓発の推進 等