

サイバーセキュリティ政策会議報告書（概要）

～生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進～

I-1 生活様式の変化等に伴うサイバー空間の新たな脅威

1. コロナ禍が顕在化させるサイバー空間の新たな脅威

- キャッシュレス決済サービスの不正利用をめぐる被害の急増
- テレワークの脆弱性等を狙ったサイバー攻撃

2. 犯行手口の悪質化と被害の深刻化

- フィッシング被害の急増と手口の巧妙化
- 悪質化するマルウェア攻撃

3. 国家の関与が疑われるサイバー攻撃被害の深刻化

I-2 今後のサイバーセキュリティに求められる新たな基本理念

公共空間としての安全性確保

～誰もが安心して参画できるサイバー空間の実現～

II-1 犯行主体の特定を通じた 犯罪対策・安全保障

1. 事後追跡可能性の向上

- 犯罪インフラを提供する悪質事業者の摘発強化
- 捜査の合理化・効率化

2. アトリビューションの強化と 戦略的な活用

- アトリビューション体制の充実強化、新たな捜査手法の研究、関係省庁・機関との連携強化、情報発信への活用

II-2 健全なサイバー空間の実現に 向けた各主体による取組

1. 事業者や個人における取組の促進

- キャッシュレス決済サービスの不正振替事案を踏まえた対応
- リスクベース・アプローチに基づく民間事業者の自主的な取組の促進
- 基本的なリテラシーの普及
- 専門家によるボランティア活動の支援

2. 公的機関としての関与・支援

- 情報発信の強化
- 子供や高齢者への安全教育拡充
- 地方の中小企業に対する支援
- 産学官における情報共有促進

II-3 安全性確保に向けた取組の 実効性を担保する基盤・観点

1. サイバー空間を構成する プラットフォームの信頼性確保

- SMS機能付きデータSIM契約時の本人確認の徹底

2. 見落としがちな要素・観点への対応

- 通信インフラ等のセキュリティ強化
- サプライチェーンリスクへの対応

3. ソーシャルエンジニアリングに 対応するための技術的措置

- フィッシングサイトに誘導するSMSの遮断