資料43－４

「ICTサイバーセキュリティ総合対策2023（仮）」の骨子（案）

令和５年４月

サイバーセキュリティタスクフォース事務局

これまでのサイバーセキュリティタスクフォースにおける検討状況

➢ 過去３回のサイバーセキュリティタスクフォースにおいて、2022年８月の「ICTサイバーセキュリティ総合対策2022」の策定・公表以降のサイバー攻撃を巡る最近の動向や総務省のサイバーセキュリティ政策に係る取組等について御議論いただいてきたところ。

	議 事 内 容
第41回 （R4.12.13）	✓ 「ICTサイバーセキュリティ総合対策2022」等に基づく取組 ✓ 最近の無差別型サイバー攻撃の動向と対策（NICT） ✓ 国際的なサイバーセキュリティ・ボットネット対策（日本マイクロソフト） ✓ サイバーセキュリティタスクフォースの今後の進め方
第42回 （R5.2.1）	✓ 国際連携に関する取組状況と課題について （事務局、NTT、JPCERT/CC） ✓ 普及啓発・人材育成に関する取組状況と課題について （総務省近畿総合通信局、園田構成員）
第43回 （R5.4.28）	✓ 情報通信ネットワークの安全性・信頼性の確保に関する取組状況と課題について （事務局、MRI、NTTコミュニケーションズ） ✓ サイバー攻撃への自律的な対処能力の向上に関する取組状況と課題について （事務局、NICT） ✓ 情報通信ネットワークにおけるサイバーセキュリティ対策分科会の検討状況について

今後のスケジュール（予定）

（第６回分科会（６月中旬）　とりまとめ（案））

第44回TF（ ６月下旬）　総合対策（案）

→パブコメを経て夏頃策定

「ICTサイバーセキュリティ総合対策2023（仮）」の骨子（案）

Ⅰ サイバーセキュリティを巡る最近の動向

新たな国家安全保障戦略の策定等をはじめとする政府のサイバーセキュリティ政策や、サイバー攻撃の脅威の増大等、2022年８月の「ICT サイバーセキュリティ総合対策2022」の策定以降のサイバーセキュリティ全般を巡る最近の動向　等

Ⅱ 情報通信ネットワークの安全性・信頼性の確保

1　総合的なIoTボットネット対策の推進（「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」報告）

NOTICEの今後の在り方、C2サーバの検知に関する実証　等

2　その他の情報通信ネットワークにおけるサイバーセキュリティ対策の推進

情報通信分野におけるサプライチェーンリスク対策（5Gセキュリティ、SBOM等）、電気通信事業者による積極的対策、クラウドサービスやスマートシティにおけるセキュリティ対策　等

3 トラストサービスの普及

Ⅲ サイバー攻撃への自律的な対処能力の向上

1　CYNEX等の推進

CYNEXやCYXROSSの推進　等

2 研究開発の推進

CRYPTRECの推進　等

3 人材育成の推進

実践的サイバー防御演習（CYDER）、大規模イベント向け演習（CIDLE）、SecHack365の推進　等

Ⅳ 国際連携の推進

途上国向けの能力構築支援（AJCCBC、太平洋島しょ国への展開）や二国間・多国間連携の推進　等

Ⅴ 普及啓発の推進

1　事業者向けの普及啓発

テレワークセキュリティの確保、地域SECUNITYの強化、サイバー攻撃被害情報の共有・公表やサイバーセキュリティ対策に係る情報開示の推進　等

2　個人向けの普及啓発

無線LANセキュリティの確保、「国民のためのサイバーセキュリティサイト」を通じた普及啓発　等