資料21－４

# 今後重点的に取り組むべき研究開発の推進方策について

サイバーセキュリティタスクフォース事務局

令和２年２月20日

# 重点的に取り組むべき研究開発の推進方策案



- 今後、インターネットをはじめとするネットワークに接続される機器の更なる増加に伴い、サイバー攻撃の対象が拡大するとともに、AIの進展やサプライチェーンの複雑化等により、攻撃手法・能力が巧妙化・大規模化していくことが想定される。

- こうした状況を踏まえ、有識者ヒアリング及びサイバーセキュリティタスクフォースでのご議論を受けて、今後５年間程度で重点的に取り組むべきと考えられるサイバーセキュリティ分野の研究開発について

  - データ駆動型サイバーセキュリティ技術
  - エマージング技術に対応したネットワークセキュリティ技術
  - 暗号基盤技術

  の３つの柱の下に整理し、それぞれについて研究開発課題案及び工程表案をまとめたものを次ページ以降に示す。

- なお、サイバーセキュリティが社会経済活動のインフラとなりつつある現状を踏まえ、研究開発を進めるに際しては、サイバーセキュリティ技術の研究者だけでなく、法制度やAI等の専門家も取り込む形で、社会システム全体の中での位置づけを踏まえた実証等の取組を進めていく必要がある。
  また、ガラパゴス化しないよう、国際標準化や国際連携についても積極的に進めることが求められる。

# 今後重点的に取り組むべき研究開発課題及び工程表（案）　1/3



| 年度 | 2021年度 | 2022年度 | 2023年度 | 2024年度 | 2025年度 | 2026年度 | アウトカムと社会的メリット |
|---|---|---|---|---|---|---|---|
| ① データ駆動型サイバーセキュリティ技術 | グローバルサイバー攻撃観測網の運用・拡充・高度化<br>・無差別型攻撃、DDoS攻撃等の大規模リアルタイム観測技術の確立<br>・サイバー攻撃の世界的傾向の分析、新たな脅威の把握 | | | | | | サイバー攻撃観測技術、可視化技術、分析技術を高度化するとともに、多種多様なサイバーセキュリティ関連情報を大規模集約し、セキュリティ検証、実証、人材育成等に寄与するデータ駆動型サイバーセキュリティ統合研究基盤を構築 |
| | アクティブ・ディフェンス基盤の運用・拡充・高度化<br>・標的型攻撃、Web媒介型攻撃等の能動的観測・分析技術の確立<br>・新たなサイバー攻撃に対する能動的対応技術の開発・実証 | | | | | | |
| | セキュリティ情報融合基盤の実装・運用・高度化<br>・脅威情報等のセキュリティ関連情報の大規模集約<br>・研究開発と運用を融合したセキュリティオペレーションの高度化 | | | | | | |
| | | データ駆動型サイバーセキュリティ統合研究基盤の構築・運用<br>・攻撃の観測情報、脅威情報など多種多様なサイバーセキュリティ関連情報を大規模集約<br>・AI/IA（Intelligent Assistance）技術等を活用した各種分析・オペレーション等の自動化・可視化技術を統合<br>・国産セキュリティ技術の検証・実証、SOC（Security Operation Center）人材育成 | | | | | 本研究基盤を国産セキュリティ技術の実証・検証、SOC人材育成等に活用することで、我が国のサイバー攻撃対処能力の向上に貢献 |
| | AI/IA技術等を活用したセキュリティ・オートメーション技術の研究開発<br>・インシデントの優先順位判定<br>・マルウェア機能分析自動化<br>・攻撃の検知・脅威予測<br>・IoTマルウェアの無害化・無機能化<br>・AIの信頼性の確保 | | | | | | |

# 今後重点的に取り組むべき研究開発課題及び工程表（案）　2/3



| 年度 | 2021年度 | 2022年度 | 2023年度 | 2024年度 | 2025年度 | 2026年度 | アウトカムと社会的メリット |
|---|---|---|---|---|---|---|---|
| ② エマージング技術に対応したネットワークセキュリティ技術 | 5Gネットワークセキュリティテストベッドの構築・高度化<br>・エミュレーション環境等の構築・高度化 | | | | | | |
| | 5Gネットワークセキュリティの検証・分析<br>・テストベッドを活用した5Gネットワークセキュリティ検証・分析技術の確立<br>・エッジ、コアネットワーク、クラウド等のセキュリティ検証と課題の抽出<br>・安全な5Gネットワーク構築のためのセキュリティガイドラインの作成 | | | | | | 5G/beyond 5G等の今後世の中に出てくる新たなネットワーク環境におけるセキュリティ課題を抽出し、対策するための検証環境や検証技術を確立 |
| | Beyond 5Gネットワークセキュリティ技術の調査<br>・Beyond 5G等の新技術に対応したセキュリティ技術の検討・調査<br>・研究機関の国際連携推進 | | | | Beyond 5Gネットワークセキュリティ技術の開発<br>・Beyond 5Gのセキュリティ課題の抽出<br>・サービス指向ネットワーク・分散クラウド環境等におけるセキュリティ技術要素の検討と開発 | | |
| | コネクテッドデバイスのセキュリティ検証環境の構築及び攻撃時の動作検証・分析<br>・通信機器、IoT機器、コネクテッドカー等を対象とした検証環境の構築・高度化<br>・検証環境を用いた脅威分析、影響分析、及び攻撃シナリオの評価 | | | | | | 本検証環境や検証技術を活用することで、新たな脅威に対抗し、安心して新技術を享受できる社会の形成に貢献 |
| | ハードウェアチップの脆弱性検知手法の開発<br>・回路情報から不正回路を検知する技術の確立<br>・電子機器の外部情報から不正動作を検知する技術の確立 | | ハードウェアチップの脆弱性検知手法の高度化・運用<br>・チップの脆弱性検知手法の実用化に向けた開発 | | | | |
| | 新技術・新たな攻撃に機動的に対応するための研究開発 | | | | | | |

# 今後重点的に取り組むべき研究開発課題及び工程表（案）　3/3



| 年度 | 2021年度 | 2022年度 | 2023年度 | 2024年度 | 2025年度 | 2026年度 | アウトカムと社会的メリット |
|---|---|---|---|---|---|---|---|
| ③ 暗号基盤技術 | データを秘匿した状態で安全に解析する技術の研究開発<br>・秘密計算等のための暗号化技術、統計処理によるデータの秘匿技術の確立<br>・秘匿されたデータに対する機械学習等のAIを用いた解析技術の確立 | | | | | | 安全にデータを提供・収集・保管・解析・展開等を行うことで業界内でのデータ共有・業界横断的な連携を促進するデータ統合利活用技術を構築する |
| | データを秘匿した状態で安全に収集・保管する技術の研究開発<br>・データ提供者のプライバシー保護のための匿名認証の確立<br>・秘匿されたデータに対する検索・アクセス制御・改ざん防止技術の確立<br>・データ利活用促進のためのセキュリティ技術のユーザビリティ向上 | | | | | | |
| | データを秘匿した状態で安全に収集・保管・解析技術の検証・分析<br>・秘匿されたデータに対する収集・保管・解析技術の連携技術の確立<br>・社会展開を見据えた実証実験の実施 | | | | | | |
| | 新たな脅威に対抗できる暗号技術の確立<br>・量子計算機時代における脅威に対抗できる暗号技術等、新たな暗号技術の研究開発<br>・電子政府システムをはじめ国民生活を支える様々なシステムで利用される暗号技術の高速・小型化実装 | | | | | | 量子計算機時代においても、安全な暗号技術の利用にに関する指針を継続的に提示し、暗号技術の安全な利用に貢献 |
| | 量子計算機・IoT・AI時代に対応した暗号安全性評価技術の確立 | | 量子計算機・IoT・AI時代に対応した暗号安全性評価技術の高度化 | | | | |
| | ・CRYPTRECの運営を通じた電子政府推奨暗号（現行の暗号技術）の安全性評価への貢献<br>・耐量子計算機暗号、軽量暗号、高機能暗号等の次世代暗号技術の信頼性向上・普及・標準化への貢献（ガイドライン作成を含む） | | | | | | |