資料３－２

総務省におけるサイバーセキュリティ施策の取組状況について

2024年10月

総務省サイバーセキュリティ統括官室

「ICTサイバーセキュリティ政策の中期重点方針」の概要

➢ 総務省では、本年２月から「ICTサイバーセキュリティ政策分科会」（主査：後藤厚宏　情報セキュリティ大学院大学学長）を開催し、総務省が取り組むべきサイバーセキュリティ政策について、2030年頃も見据えた中長期的な方向性について検討し本年７月末に公表。

【政府の主な動き】

- **国家安全保障戦略**
- **経済安全保障推進法の施行（特定社会基盤事業者の指定等）　等**

【サイバーセキュリティを巡る主な課題】

- **厳しさを増す国際情勢とサイバー攻撃リスクの高まり**
- **多様化・複雑化するサプライチェーンとアタックサーフェス（攻撃対象領域）の増加**
- **セキュリティ人材の確保**
- **生成AI等の新たな技術への対応**

１．重要インフラ等におけるサイバーセキュリティの確保

- 通信分野（総合的なIoTボットネット対策（新NOTICEの推進やC&Cサーバの検知・対処能力の向上）、スマートフォンアプリのセキュリティ対策やサプライチェーン対策の推進等）
- 放送分野（安全・信頼性に関する新たな技術基準に基づくセキュリティ対策の着実な推進等）
- 自治体分野（クラウド化・標準化等の環境変化を見据えた人材育成やCSIRT能力向上の取組等）
- クラウドセキュリティの確保やトラストサービス（eシールの認定制度を2024年度中に創設等）の推進

２．サイバー攻撃対処能力の向上と新技術への対応

- CYNEX・**CYXROSS**を強力に推進し、国産のサイバーセキュリティ情報・技術による自律的なサイバーセキュリティ対処能力を抜本的に強化
- CYXROSSとGSOCとの連携により政府システムの一元的な監視体制の構築に貢献
- CYDER等を通じた国や地方公共団体等におけるCSIRT対処能力の抜本的強化
- サイバーセキュリティ研究分野の国際競争力向上を図るため、NICT内に米国との連携を強化するための結節点を形成
- 生成AI等の新技術への対応（**AIを起因とするセキュリティリスクの回避・低減に向けた取組、AIを活用したサイバーセキュリティ対策の促進**、耐量子計算機暗号技術（PQC）等の研究開発等の推進）

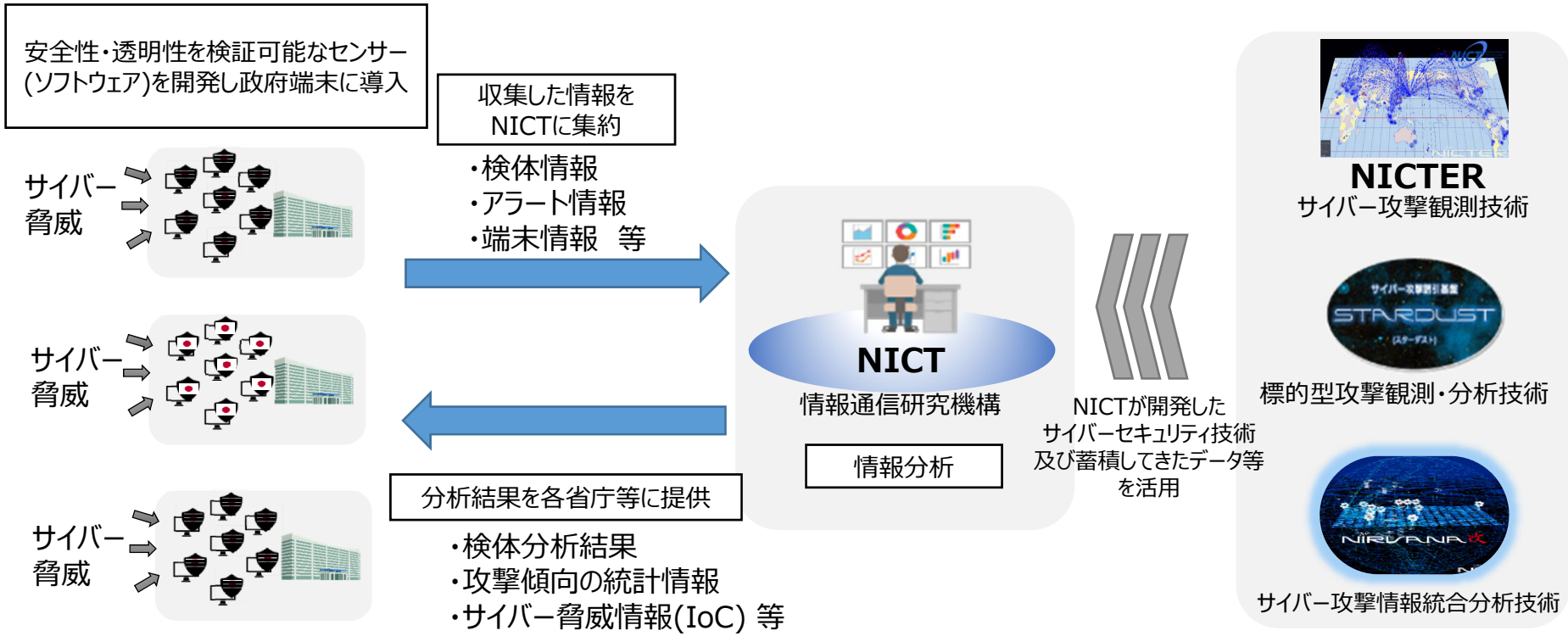
３．地域をはじめとするサイバーセキュリティの底上げに向けた取組

- 地域SECUNITYの活動強化（他機関との更なる連携、持続的な推進体制の整備等）
- 各種ガイドラインの周知啓発等

４．国際連携の更なる推進（国際連携全般、人材育成支援）

- 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）の活動強化（プログラムの拡充、有志国との連携強化等）
- 大洋州島しょ国向け人材育成支援プロジェクトの2025年度以降の本格的な実施

- **安全性や透明性の検証が可能なセンサーを開発し端末に導入することで、海外製品に頼らずに端末情報**（悪意のあるソフトウェアに感染した端末の動作状況等の実データ）**を収集し、分析**する取組みを試行的に実施。
- サイバーセキュリティ対策の優先度の高い政府機関の端末を対象とし、有意な分析結果を得るために必要な数千台規模の政府端末から情報を収集、得られた情報をNICTに集約して分析。
- 国産技術により端末情報を収集・分析する仕組みの実現性・有効性を検証し、海外セキュリティ製品に依存しない、**政府端末に係るサイバーセキュリティ情報の収集・分析環境を実証する**。



生成AI等を活用したサイバーセキュリティ対策強化

- あらゆる分野において生成AIの実装が急速に進んでいる一方で、生成AIを巡るリスクとして、偽誤情報の拡散、プライバシーの侵害、知的財産権の侵害等に加えて、サイバー攻撃への悪用等によるサイバーセキュリティのリスクが新たに指摘されている。
- 他方、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、サイバーセキュリティ対策の業務負荷が課題となっている中、サイバー攻撃対策への生成AI等の利活用が期待されている。
- こうした背景を踏まえ、生成AI等のAI技術を巡る最新動向を把握しつつ、AIに起因するセキュリティリスクを可能な限り回避・低減するための「Security for AI」に取り組むとともに、AIをセキュリティ対策に効果的に活用するための「AI for Security」に取り組むことが必要。

生成AIの負の影響

サイバー攻撃に悪用される可能性

（例）
- 生成AI利用によるフィッシングメールの巧妙化
- マルウェアの生成、亜種の大量生産

生成AIへのサイバー攻撃・脆弱性内包

（例）
- リスクにつながる悪意のある入力
- LLMの学習データの汚染
- 事業者設定ミスによる安全ではない出力処理

生成AIの正の影響

サイバー攻撃対策への活用の可能性

（例）
- サイバー防御の自動化
- セキュリティレポート作成の自動化
- 脅威インテリジェンスの精度向上
- 脆弱性のない安全なコード開発の支援
- サイバー攻撃の予見
- インシデント対応の支援

Security for AI

安心安全な利用の促進

① 生成AIの進展によるサイバーセキュリティへの影響に係る調査・検証
- 生成AI等がサイバーセキュリティに与える負の影響の検証・評価
- AIの安心・安全な開発・提供に向けたセキュリティのガイドラインの策定

＜実例検証＞

② 米国専門機関とのAI安全性に関する共同研究事業
- AIの安全性に係る分野の研究開発を推進するため、北米にNICTの研究拠点を構築し、米国MITRE等の様々な専門機関との共同研究事業を実施

＜理論研究＞

AI for Security

サイバーセキュリティ対策への活用

③ AIを用いたサイバー脅威情報収集・分析の高度化
- 世界中の様々な機関等から発信されるサイバー脅威情報をAIを活用して収集・分析するための技術を開発及び展開

＜平時の分析活動＞

④ 生成AIを活用した重要インフラ分野におけるサイバーセキュリティ対策強化
- 生成AIを活用した攻撃インフラ分析の精緻化・迅速化の検証
- 当該情報等を用いた対処オペレーション業務の効率化・迅速化の検証とノウハウの展開

＜攻撃インフラ特定＞