資料情部44-2

国立研究開発法人情報通信研究機構の第５期中長期目標変更（案）の概要（１）

国立研究開発法人情報通信研究機構法の
一部を改正する等の法律について

令　和　５　年　１　２　月
総　　務　　省
サイバーセキュリティ統括官室

中長期目標変更（案）の概要

変更概要

➢ 改正ＮＩＣＴ法に基づき、法律上新たに業務として位置づけられた**サイバーセキュリティ対策を十分に講じていないと認められるＩｏＴ機器の管理者等に対する助言及び情報提供に関する業務**を対象とする目標を追加するとともに、同法に基づき、**信用基金を清算すること**を追記するもの。

＜国立研究開発法人情報通信研究機構法の一部を改正する等の法律（令和５年法律第87号）の概要＞

NICTが行うサイバー攻撃に悪用されるおそれのあるIoT機器の調査について、①令和５年度末に時限を迎えるID・パスワードに脆弱性があるIoT機器の調査を、令和６年度以降も継続的に実施を可能とするとともに、②調査の対象を拡充するための規定を整備する。あわせて、特定通信・放送開発事業実施円滑化法の廃止等を行う。

１．サイバーセキュリティ関連業務の規定の整備

① ID・パスワードに脆弱性があるIoT機器の調査の継続的な実施

○ NICTが令和５年度末までに限り行うこととされているID・パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）を、令和６年度以降も継続的に実施できることとする。

② 調査対象の拡充

○ NICTが行うIoT機器の調査等に係る業務について、その対象を拡充※するとともに、総務大臣が、サイバーセキュリティ戦略本部から意見を聴取した上で、NICTの中長期目標の策定等をする旨を規定する。

※ＩＤ・パスワードに脆弱性があるIoT機器に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とする。

２．信用基金の清算及び特定通信・放送開発事業実施円滑化法の廃止等

○ NICTの信用基金を清算し、これに伴い、NICTの関連業務及び当該基金に係る業務を規定する特定通信・放送開発事業実施円滑化法を廃止する。

サイバーセキュリティ関連業務の規定の整備（ＮＯＴＩＣＥ関係）

情報通信研究機構（NICT）法

総務大臣

中長期目標・計画に係る意見聴取 → **サイバーセキュリティ戦略本部**

特定アクセス行為等に係る実施計画認可

中長期目標策定・計画認可

情報通信研究機構（NICT）

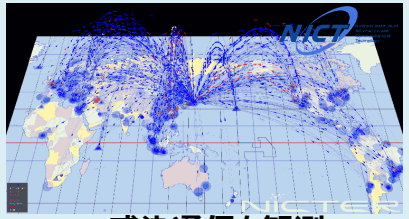
サイバーセキュリティ対策助言等業務

（サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、機器の管理者等に必要な助言及び情報を提供）

ID・パスワードの設定に脆弱性を有する機器

ファームウェアの脆弱性等のID・パスワード以外の脆弱性を有する機器

既にマルウェアに感染している機器



感染通信を観測

令和６年度以降も継続して実施（特定アクセス等実施業務）

NICTの業務として新たに法的に位置づけ

IoT機器メーカー

電気通信事業者（ISP）

SIer

その他セキュリティ関係者

注意喚起

機器の利用者

利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施するとともに、様々な関係者との連携により総合的なIoTセキュリティ対策を促進

信用基金の清算及び特定通信・放送開発事業実施円滑化法の廃止

1. 信用基金清算に係る経緯

- **NICTの信用基金**は、**特定通信・放送開発事業実施円滑化法**（以下「通信・放送開発法」）に規定する**債務保証業務を実施するための基金**として設置。
- **信用基金等に係る業務は、R3年度末までに既存案件を全て終了していることから、信用基金の維持は不要。**
- このため、信用基金の一部を構成する**民間出資金は**本年５月までに**その全額を出資者に払戻し済み。**

  ⇒ **これらを踏まえた所要の規定の整備を実施。**

2.信用基金清算に係る主な法改正事項

改正法第１条：NICT法の改正

- **信用基金に係る規定等の関連規定**※1**を削除**し、信用基金等の**残余財産の国庫納付規定**※2を設ける。

  ※1 通信・放送開発法に基づく特例業務（旧機構法第14条第２項第４号）、債務保証勘定（第16条第２号）、第18条（信用基金）等。

  ※2 債務保証勘定の残余財産を、政令の定めるところにより国庫に納付する規定を改正法附則第３条第４項に設ける。
- **民間からの出資を前提とした規定**※**を削除。**

  ※ NICTの資本金は、政府による出資及び政府以外の者からの出資金額の合計額と規定（旧機構法第６条等）。

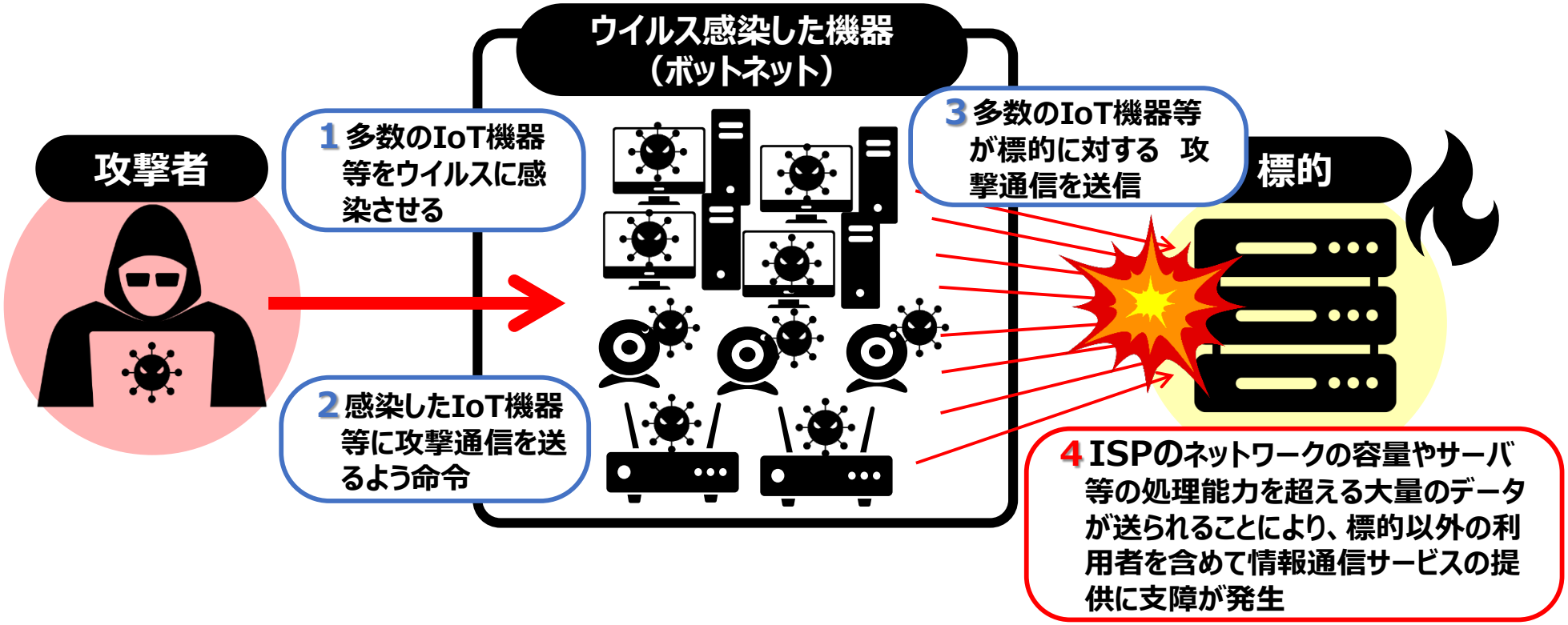
改正法第２条：通信・放送開発法の廃止

- これに伴い、信用基金に係る業務等の機構の業務の特則を定める**通信・放送開発法を廃止**※。

  ※残存する出資業務の継続のための経過措置規定を、改正法附則第３条第１項及び第２項に設ける。

（参考）脆弱なIoT機器が情報通信ネットワークに与える影響

【DDoS攻撃※のイメージ】※DDoS攻撃（分散型サービス不能攻撃：Distributed Denial of Service attack）



【最近の事例】

（IoT機器が不正アクセスされた事例）

- 2023年1月、国土交通省近畿地方整備局が管理する河川監視用のカメラ 199台において、大量の通信を確認。
- その後中国地方整備局、四国地方整備局が管理するカメラも合わせ、不正アクセスの疑いのある337台のカメラの運用を休止。

（ウェブサイト等への障害が発生した事例）

- 2022年９月以降、企業や中央省庁、地方自治体を狙ったDDoS攻撃が断続的に発生。
- ロシアを支持するハッカー集団「キルネット」の犯行が疑われるものなど攻撃は様々であり、e－GovやeLTAX等の政府サイトやJR西日本や東京電力等の民間企業のサイトにつながらない、奈良県では県下の自治体を含め役場からのインターネット接続ができない等の事例が発生。

（参考）現行のＮＯＴＩＣＥの概要

※NOTICE（National Operation Towards IoT Clean Environment）

➢ IoT機器（監視カメラ、ルータ等）を悪用するサイバー攻撃の深刻化への対応として、情報通信研究機構（NICT）が、参加通信事業者82社が管理するネットワーク下で、インターネットに直接接続している機器（約1.13億）を対象に、**ID・パスワードに脆弱性があるIoT機器及び感染通信を出しているIoT機器**を調査し、電気通信事業者（ISP）を通じて利用者への注意喚起を行う取組を2019年より実施。

【ID・パスワードに脆弱性があるIoT機器】

※NICT法を改正し、今年度末までの５年間の時限措置として実施

情報通信研究機構(NICT)

これまでサイバー攻撃に用いられたもの	Password admin1234
同一の文字等を用いたもの	aaaaaaa 12345678

機器調査

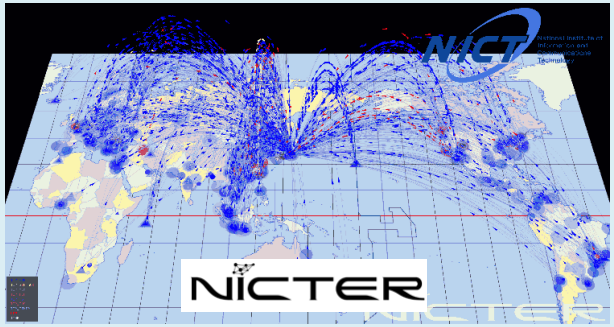
特定アクセス行為により、ID・パスワードに脆弱性がある機器（その機器に係るIPアドレス）を特定

攻撃者　インターネット上のIoT機器

【感染通信を出しているIoT機器】

情報通信研究機構(NICT)

感染通信の観測



ISPへの通知件数（2023年10月）

5,162件（９月度:5,162件）
（参考）2019年度からの累積件数：117,887件

通知

電気通信事業者（ISP）

注意喚起

ISPへの通知件数（2023年10月）

１日平均2,556件（９月度:808件）
（参考）2019年度からの値：１日平均510件

機器の利用者

利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施

（参考）明らかになった主な課題

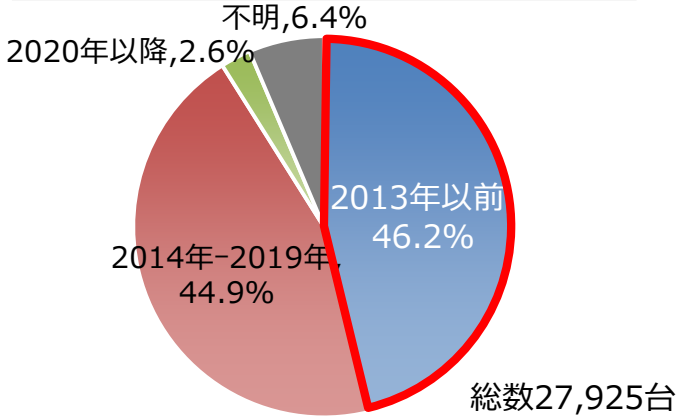
脆弱性等があるIoT機器やサイバー攻撃の脅威に関する課題

■ **ID・パスワードに脆弱性があるIoT機器**は、10年以上前の機種が４割強も存在するなど**古い機器を中心に残存。**

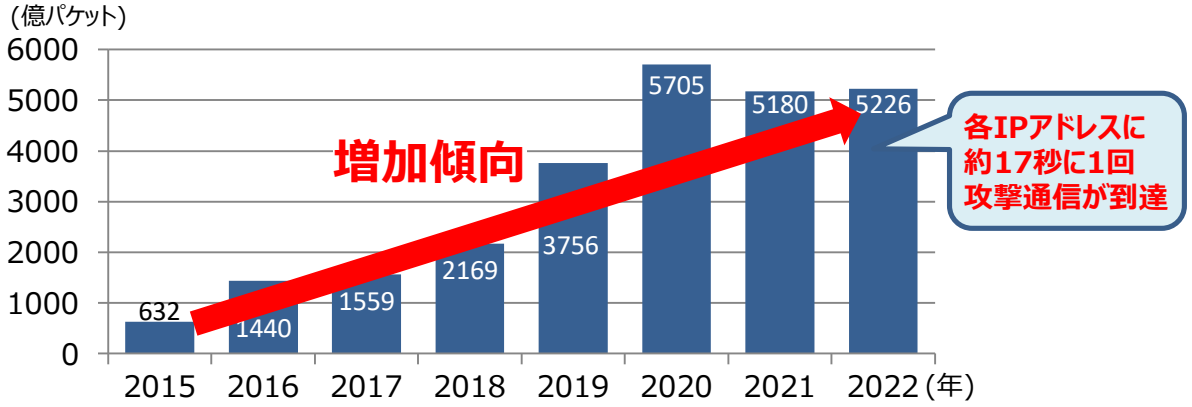
■ **サイバー攻撃の脅威は変化**しており、
①**新たなネットワーク経路**（通信プロトコル、ポート）を狙った攻撃
②**ID・パスワード以外の脆弱性**（ファームウェア等）を狙った攻撃
も発生。

■ **マルウェアの活動状況は依然として活発**であり、**サイバー攻撃関連の通信数**は、**５年前と比較して約3.4倍に増加。**

ID・パスワードに脆弱性がある機器の発売年別内訳
（2022年11月～2023年４月）



NICTERで１年間に観測されたサイバー攻撃関連の通信数



利用者の意識に関する課題

■ IoT機器のセキュリティ対策に対する**利用者の意識が十分ではなく、対策方法も利用者にとって難しい**ものとなっている。

Wi-Fiルータ利用者向けのアンケート結果によれば、
- **57.8%**の利用者がWi-Fiルータのセキュリティを意識したことがない
- **81.7%**の利用者が自宅のWi-Fiルータがサイバー攻撃されると考えたことがない
- 購入時のパスワードをそのまま利用している利用者が**42.7%**

（出典）デジタルライフ推進協会（DLPA）Wi-Fiルーターセキュリティ対策ポイントを基に作成

■ **法人利用者**については、管理責任の所在が曖昧など**適切な管理体制がない**ケースもある。

	所有者	設置者	管理者	使用者
一般利用者	購入者			（＋家族）
法人利用者	企業	設置委託業者	管理委託業者	社員、客

（出典）第３回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 ヤマハ発表資料を基に作成

（参考）今後のＮＯＴＩＣＥの方向性

サイバー攻撃の踏み台となり得るIoT機器に対する観測能力の維持・強化

■ **NICTによるIoT機器の調査の拡充**

下記の調査の実施を通じて、脆弱性等のあるIoT機器に対する観測能力の維持・強化を図る

①ID・パスワードに脆弱性があるIoT機器の調査

IoT機器のライフサイクルの長さを考慮し、
５年間の時限措置を延長

②脆弱性があるファームウェア等を搭載しているIoT機器の調査

③感染通信を出しているIoT機器の調査

幅広い関係者との連携や対処手段の多様化等による「プッシュ型支援」の強化

■ **個別の利用者への注意喚起の実効性向上**

注意喚起の効果のより詳細な把握や、ISP向けガイドラインの策定等を通じ、注意喚起の実効性向上を図る

■ **総合的な対処の推進**

対処を注意喚起のみに依存するのではなく、幅広い関係者と連携し、状況に応じて多様な手段を講じる

①ISPによる対処
（例）レンタルサービス等を通じてISPが管理している機器の場合、ISP側で一括して対処

②メーカーとの連携
（例）ファームウェアの改修や新製品の機能改善（ファームウェアの自動更新等）

③SIer ※との連携
（例）法人利用者等、機器の設置・管理にSIerが関与している場合、SIerを通じて対処を促す

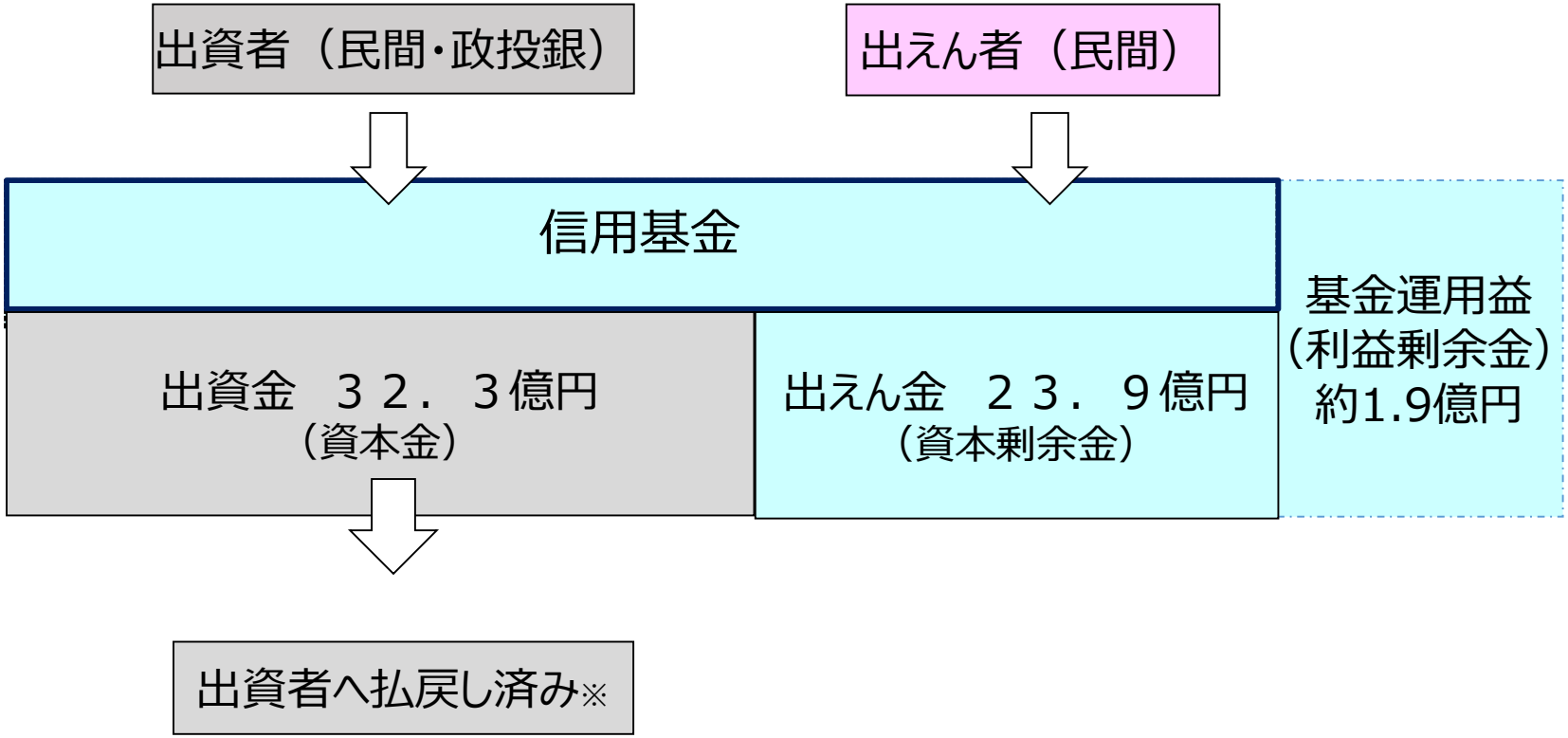
■ **IoT機器の適切な管理についての周知啓発の強化**

※SIer：システムの開発から保守・運用までを請け負う事業者

国民の日常生活・社会経済活動に必要不可欠な情報通信サービスの安定的な提供を図るため、IoT機器を悪用したサイバー攻撃の脅威に対する観測能力を強化し、攻撃の脅威に応じた効果的な対処を進める。

（参考）NICTの信用基金の概要

（令和４年度末時点）



※ 令和5年5月26日時点で全出資者へ全額払戻し実施済み。