別紙１

国立研究開発法人情報通信研究機構法（平成11年法律第162号）
附則第８条第２項に規定する業務の実施に関する計画の認可申請の概要

平成31年１月
総務省　サイバーセキュリティ統括官室

国立研究開発法人情報通信研究機構法の一部改正について

● IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、**パスワード設定等に不備のあるIoT機器の調査**等を追加（**5年間の時限措置**）する等を内容とする**国立研究開発法人情報通信研究機構法の改正**を行い、平成30年11月1日に施行された。

サイバー脅威の深刻化

•IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。

※IoT機器を狙った攻撃は全体の3分の2（2016年）

対策の必要性

•パスワード設定等に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

•NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進（下図）。

情報通信研究機構法の改正

中長期目標・計画

CS戦略本部 ← 意見聴取 ― 総務大臣

実施計画認可

中長期目標変更・計画認可

これまで送信型対電気通信設備サイバー攻撃のために用いられたもの	password admin1234 supervisorsm cadmin
同一の文字のみ又は連続した文字のみを用いたもの	888888 00000000 123456 54321

情報通信研究機構

・ 特定アクセス行為により、パスワード設定等に不備のある機器を（その機器に係るIPアドレス）特定

①機器調査

・ パスワード設定等に不備のある機器に係るIPアドレス等を提供

②情報提供

第三者機関

※ 改正後の電気通信事業法に規定する第三者機関に委託

電気通信事業者

③注意喚起

・ パスワード設定等に不備のある機器に係る利用者を特定し、設定変更の注意喚起

※ 平成30年度予算を活用しつつ、サポート体制整備等を実施

インターネット上のIoT機器

攻撃者

機器の利用者

IoT機器調査の業務概要①

情報通信研究機構

①　特定アクセス行為等による調査

(1)　ポートスキャン調査

- 日本国内の約2億のグローバルIPアドレス(IPv4)を対象として、それぞれのIPアドレスに係る機器への接続要求を行い、セッションを確立できるか確認。

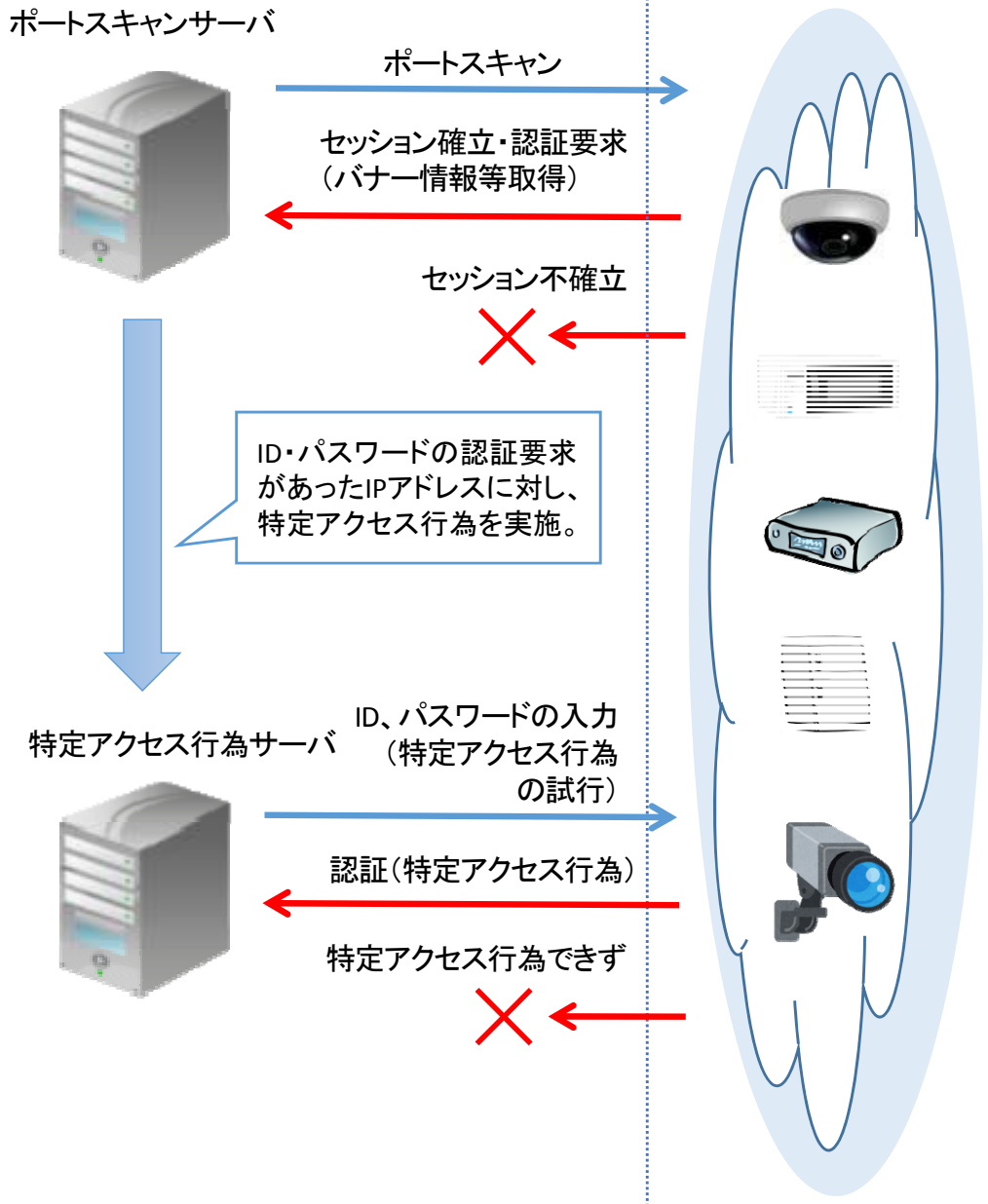
(2)　特定アクセス行為による調査

- ID、パスワードによる認証要求があったものについて、ID、パスワードを入力し、特定アクセス行為を行うことができるか確認。

- 過去に大規模なサイバー攻撃に用いられたID、パスワードの組合せ約100通りを入力。

②　通信履歴等の電磁的記録の作成

- ①による調査において、特定アクセス行為を行うことができた機器について、当該機器への通信の送信元IPアドレス、送信先IPアドレス、通信日時(タイムスタンプ等)の情報を内容とする通信履歴等の電磁的記録を作成。



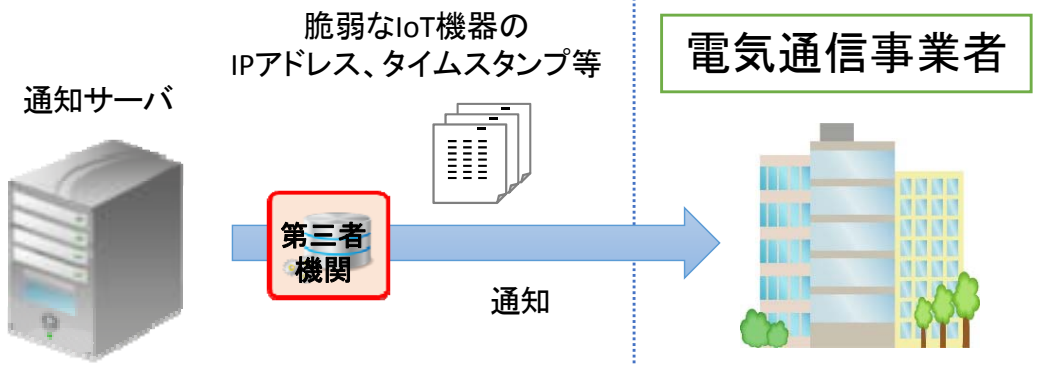
IoT機器調査の業務概要②

情報通信研究機構

③　電気通信事業者への通知※

- 特定アクセス行為を行うことができた送信先IPアドレスに係る電気通信事業者に対して、②を証拠に送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行う。

※　「認定送信型対電気通信設備サイバー攻撃対処協会」に委託を行う。



④　その他業務

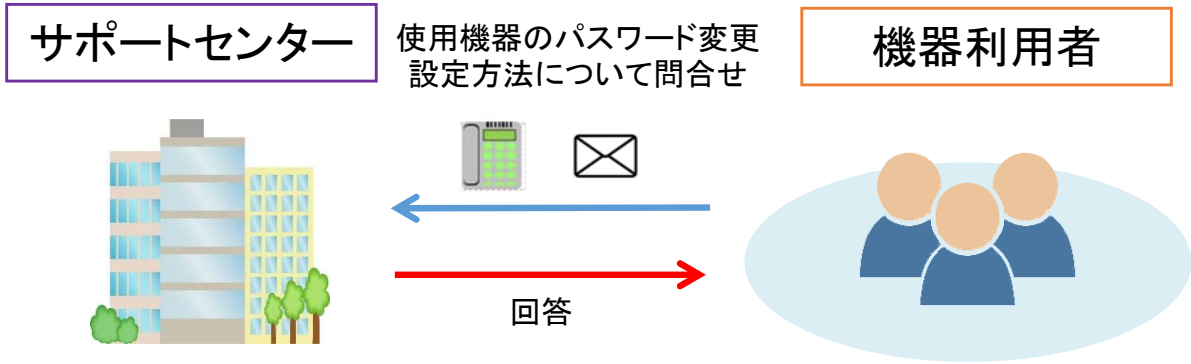
- パスワード設定以外の脆弱性を有する機器（アクセス制御機能を有しない、ソフトウェアの脆弱性を有する等）に関する情報ついても、①(1)のポートスキャンで判別可能な場合には、送信先IPアドレスに係る電気通信事業者に対して、当該情報の提供を行う。

⑤　電気通信事業者による注意喚起

- 対処を求める通知を受けた電気通信事業者は、脆弱な機器の利用者を特定し、当該利用者に対して、設定変更等の注意喚起を行う。

⑥　サポートセンターによる支援

- 平成30年度の総務省予算を活用し、電気通信事業者から注意喚起を受けた機器の利用者が、パスワード設定の変更等を円滑に行えるよう、サポートセンターを設置。



実施計画に関する省令の規定について

NICT法の概要

○ NICTにおいて特定アクセス行為等の業務が適切に行われることを確保する観点から、「総務省令で定めるところにより、当該業務の実施に関する計画を作成し、総務大臣の認可を受けなければならない」とされている。（NICT法附則第９条）

○ 総務大臣は、実施計画の認可をする際、「審議会等で政令で定めるもの※１に諮問しなければならない」とされている。（NICT法附則第11条第２号）

※１　国立研究開発法人情報通信研究機構法施行令附則第２項にて、「情報通信行政・郵政行政審議会」を規定。

省令※２の概要

※２国立研究開発法人情報通信研究機構法附則第八条第四項第一号に規定する総務省令で定める基準及び第九条に規定する業務の実施に関する計画に関する省令（平成30年総務省令第61号）

○　実施計画の認可に係る申請・変更手続、実施計画の記載事項を規定。（省令第２条）

【実施計画の記載事項】

①　特定アクセス行為に係る業務に従事する者の氏名、所属部署及び連絡先

②　特定アクセス行為の送信元の端末設備又は自営電気通信設備に割り当てられるアイ・ピー・アドレスその他のこれらの設備に関する事項

③　特定アクセス行為に係る識別符号の方針及び当該方針に基づき入力する識別符号

④　特定アクセス行為の送信先のアクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備に割り当てられるアイ・ピー・アドレスの範囲その他のこれらの設備に関する事項

⑤　特定アクセス行為により取得する通信履歴等の情報の安全管理措置その他の当該情報の適正な取扱いを確保するために必要な措置に関する事項

⑥　送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知先に求める特定アクセス行為により取得する通信履歴等の電磁的記録に記録された情報の適正な取扱いを確保するための措置に関する事項

⑦　その他必要な事項

実施計画の記載内容①

本頁は委員限り

実施計画の記載内容

① 特定アクセス行為に係る業務に従事する者の氏名、所属部署及び連絡先

[redacted]

② 特定アクセス行為の送信元の電気通信設備に割り当てられるアイ・ピー・アドレス

153.231.215.11～14	153.231.216.179～182	153.231.216.187～190	153.231.216.219～222	153.231.226.163～166
153.231.226.171～174	153.231.227.195～198	153.231.227.211～214	153.231.227.219～222	153.231.227.226～230

（合計:41個のIPアドレス）

③ 特定アクセス行為で入力する識別符号の方針・方針に基づき入力する識別符号

(1) 特定アクセス行為に係る識別符号の方針

- 送信型対電気通信設備サイバー攻撃の実績のあるマルウェア（亜種含む）で利用されている識別符号
- 同一の文字のみの暗証符号を用いているもの（1111、aaaa等）
- 連続した文字のみの暗証符号を用いているもの（1234、abcd等）
- 連続した文字のみを繰り返した暗証符号を用いているもの（12341234、abcdabcd等）
- 機器の初期設定の識別符号（機器固有に識別符号が付与されていると確認されたものを除く。）

(2) (1)の方針に基づき入力する識別符号

[redacted]

④ 特定アクセス行為の送信先の電気通信設備に割り当てられるアイ・ピー・アドレスの範囲

- サイバー攻撃を禁止する旨の技術的条件を設定した電気通信事業者の利用者等の電気通信設備に割り当てられるIPアドレス

実施計画の記載内容②

実施計画の記載内容

⑤　特定アクセス行為により取得する情報の安全管理措置

(1)　組織的安全管理措置

- 情報取扱者の明確化や、情報の漏えい等発生時における事務処理体制の整備等

(2)　人的安全管理措置

- 情報取扱者に対する内部規程等の周知、教育・訓練の実施等

(3)　物理的安全管理措置

- 情報取扱区域の明確化・区分化や、ICカード及び生体認証による情報取扱区域への入室管理システムの設置等

(4)　技術的安全管理措置

- 情報取扱サーバへのアクセス制御機能の導入や、認定送信型対電気通信設備サイバー攻撃対処協会への情報送信の際に電気通信回線として、VPN接続又はhttps接続を行う等

(5)　その他の措置

- 情報の保持期間を1年間にする等

⑥　通知先の電気通信事業者に求める情報の安全管理措置

通知対象となる情報に関して、以下の法令等を遵守する旨が記載された覚書を電気通信事業者とNICT間で取り交わす。

- 個人情報の保護に関する法律（平成15年法律第57号）
- 電気通信事業における個人情報の保護に関するガイドライン（平成29年総務省告示第152号）

⑦　その他必要な事項

- 電気通信事業者への通知に関する業務を、認定送信型対電気通信設備サイバー攻撃対処協会に委託する等