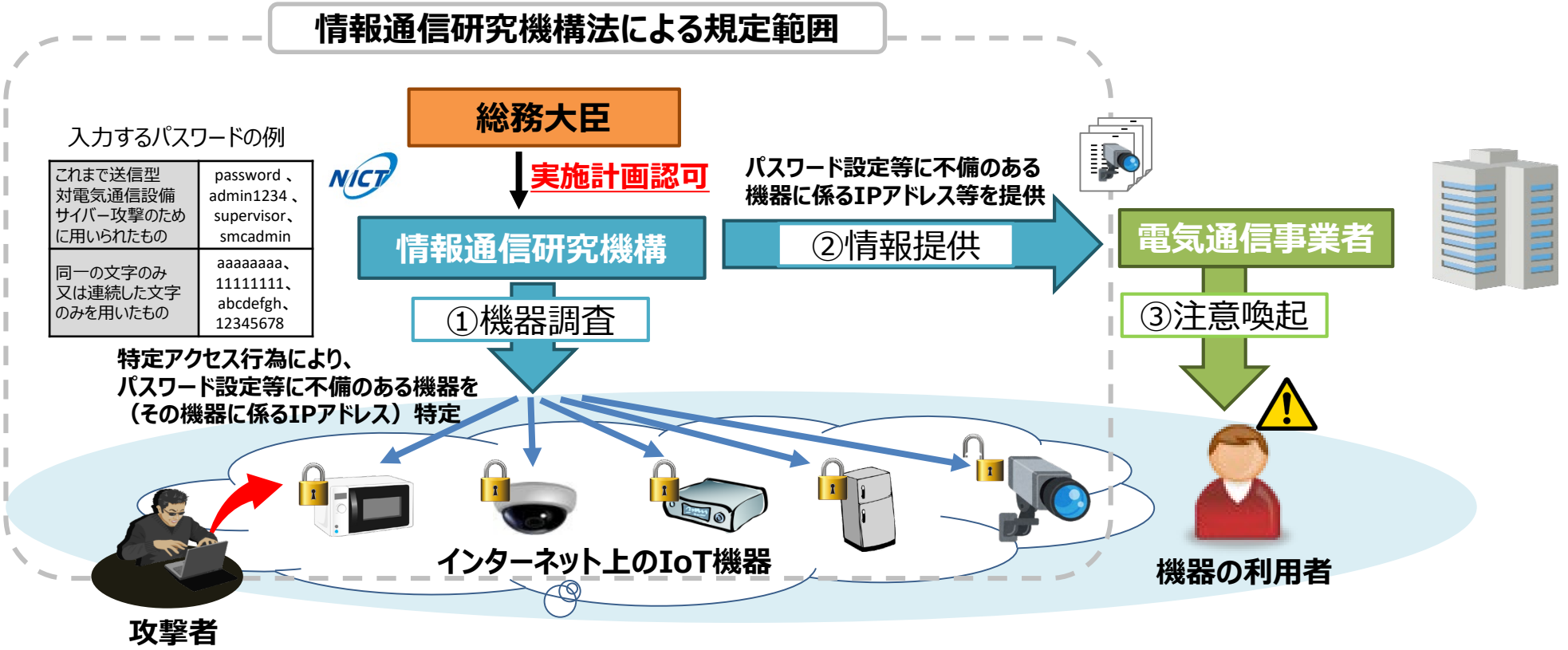
資料26－３

NOTICEの実施状況
及び実施計画の変更について

令和2年10月12日

IoT機器調査及び利用者への注意喚起（NOTICE）

- 情報通信研究機構(NICT)が**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、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「**NOTICE**」を平成31年２月より実施。
  ※平成30年改正の国立研究開発法人情報通信研究機構法（NICT法）に基づくNICT業務（令和5年度末までの時限措置）
- NOTICEの業務の実施に当たっては、実際に**IoT機器にID・パスワードを入力する特定アクセス行為**を行う必要があるため、NICTは**実施計画**を作成し、**総務大臣の認可**を受ける必要がある。
  ※平成31年2月からの実施に先立って同年1月25日に実施計画を認可。

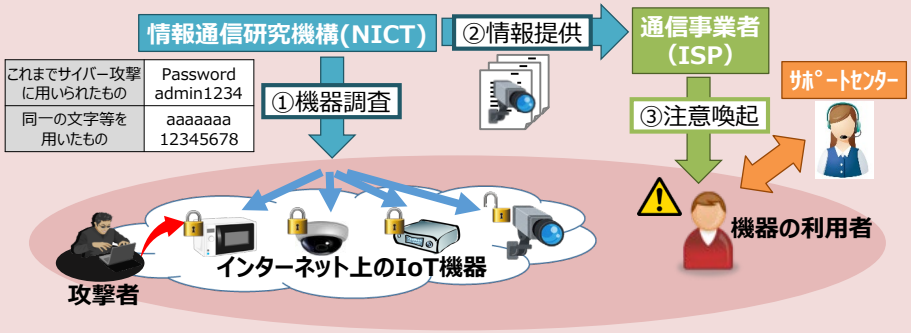


IoT機器調査及び利用者への注意喚起

- 情報通信研究機構(NICT)が**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、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「**NOTICE**」を2019年２月より実施。
- NOTICEの取組に加え、**マルウェアに感染しているIoT機器**をNICTの「**NICTER**」プロジェクト※で得られた情報を基に特定し、ISPから利用者へ注意喚起を行う取組を2019年６月より開始。

※NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

【NOTICE注意喚起の概要】

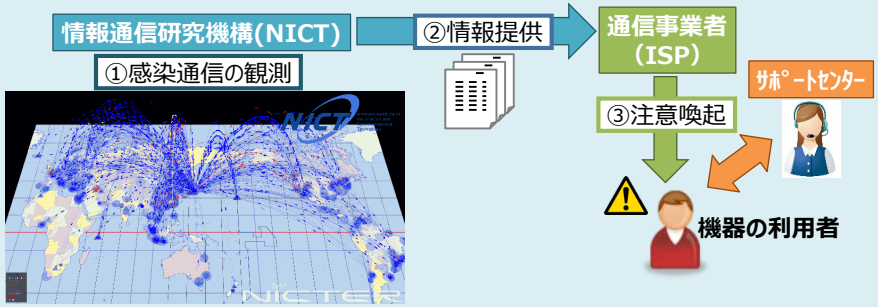


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力するなどして、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報をISPに通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施。

【NICTER注意喚起※の概要】

※マルウェアに感染しているIoT機器の利用者への注意喚起



調査対象：既にMirai等の**マルウェアに感染している**IoT機器

① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群
② 当該機器の情報をISPに通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施

IoT機器調査及び利用者への注意喚起の実施状況（2020年９月度）

- 参加手続きが完了しているISP（インターネット・サービス・プロバイダ）は**63社**。
  当該ISPの**約1.1億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**３１９件の対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**１８６件の対象を検知**しISPへ通知。

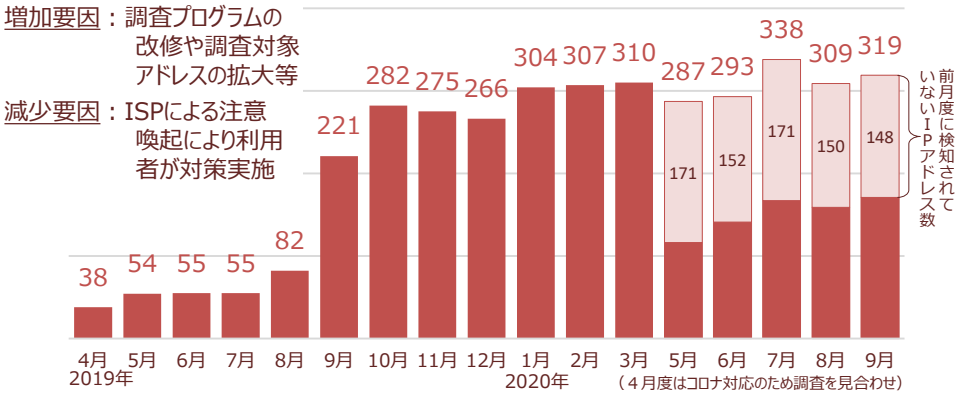
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

３１９件（８月度:309件）

（参考）2020年度の累積件数：1,546件（2019年度：2,249件）
ID・パスワードが入力可能だったもの：8.2万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

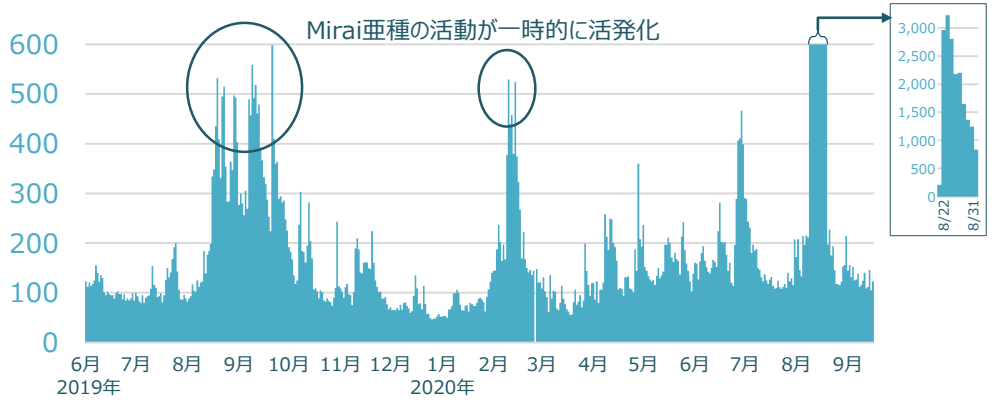
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均１８６件（８月度:700件）

（参考）期間全体での値：１日平均200件
最小：46件(2020/1/9)／最大：3,227件(2020/8/24)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



※８月末の増加は、一部の利用者でIPアドレスが頻繁に切り替わったためで、全体的なマルウェア活動活発化を直接示すものではないと推定しています。

2020年９月度分については、全体として大きな変化はありません。
なお、2020年10月度から、2020年９月11日付けの総務省報道発表のとおり、識別符号を追加して調査を実施する予定です。

実施計画の記載内容

- 総務省令の規定に従いNICTにおいて実施計画を策定。
- 情報通信行政・郵政行政審議会（電気通信事業部会）の諮問・答申を経て、平成31年１月25日に認可。

① 業務従事者の氏名・所属部署・連絡先

非公表

② 特定アクセス行為の送信元のIPアドレス

153.231.215.11～14
153.231.216.187～190
153.231.226.163～166
153.231.227.195～198
153.231.227.219～222
153.231.216.179～182
153.231.216.219～222
153.231.226.171～174
153.231.227.211～214
153.231.227.226～230
（合計：41個のIPアドレス）

③-1 特定アクセス行為に係る識別符号の方針

① 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
② 同一の文字のみの暗証符号を用いているもの（1111、aaaa等）
③ 連続した文字のみの暗証符号を用いているもの（1234、abcd等）
④ 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）
⑤ 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。）

③-2 方針に基づき入力する識別符号

非公表（約100通りのID・パスワードの組み合わせ）

④ 特定アクセス行為の送信先のIPアドレス範囲

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

⑤ 特定アクセス行為に関する情報の適正な取扱い

(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 ISP等への通知先に求める情報の適正な取扱い

通知対象となる情報に関して、個人情報保護法や関係ガイドライン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。

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、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

実施計画の変更の認可

➢ 今般、NOTICEの取組強化のため、NICTから実施計画の変更の認可申請があり、総務省が認可。

申請年月日　令和２年９月２日

申請概要　実施計画については、総務省令の規定により、特定アクセス行為の送信元のIPアドレス及び特定アクセス行為において入力する識別符号が記載されているところ、当該記載内容を変更するためNICT法附則第９条の規定に基づき、実施計画の変更認可申請が行われたもの。

変更内容

(1) 特定アクセス行為において入力する識別符号（ID･パスワード）の追加

変更前	変更後
約１００通り	約６００通り

（追加理由）
継続して新たなIoT機器向けのマルウェア(Mirai等)が登場していることを踏まえ、当該マルウェアで利用されている識別符号や、機器の初期設定の識別符号等を新たに調査対象とするため。

(2) 特定アクセス行為の送信元のIPアドレスの追加

変更前	変更後
４１アドレス	５４アドレス

（追加理由）
(1)により入力する識別符号が増加することから、特定アクセス行為に係る通信量も増加し通信回線を増設するため

➢ 上記変更は、**審議会への諮問を要さない軽微な事項※に該当**することから、総務省において、令和２年９月11日付けで**実施計画の変更を認可**。
※諮問を要しない軽微な事項について（情報通信行政･郵政行政審議会電気通信事業部会決定）附則第１項

➢ 変更後の実施計画は、**10月度**のNOTICE**調査から実施**予定。

NOTICEの実施状況等に関する情報公開

➢ NOTICEのWebサイト（https://notice.go.jp/）を活用した情報公開

- 月ごとに調査実施状況を公表
- 特定アクセス行為の送信元IPアドレスの範囲を公表
- 特定アクセスに用いるID・パスワードについては、おおよその数と、いくつかの例のみ公表

［入力するID・パスワードの例］

これまでサイバー攻撃のために用いられたもの	
ID	パスワード
admin	admin
admin1	password
root	user
root	default
supervisor	supervisor

同一の文字、連続した番号など	
ID	パスワード
admin	111111
root	123456
root	666666
root	54321
888888	888888