公表にあたり
一部編集

資料２

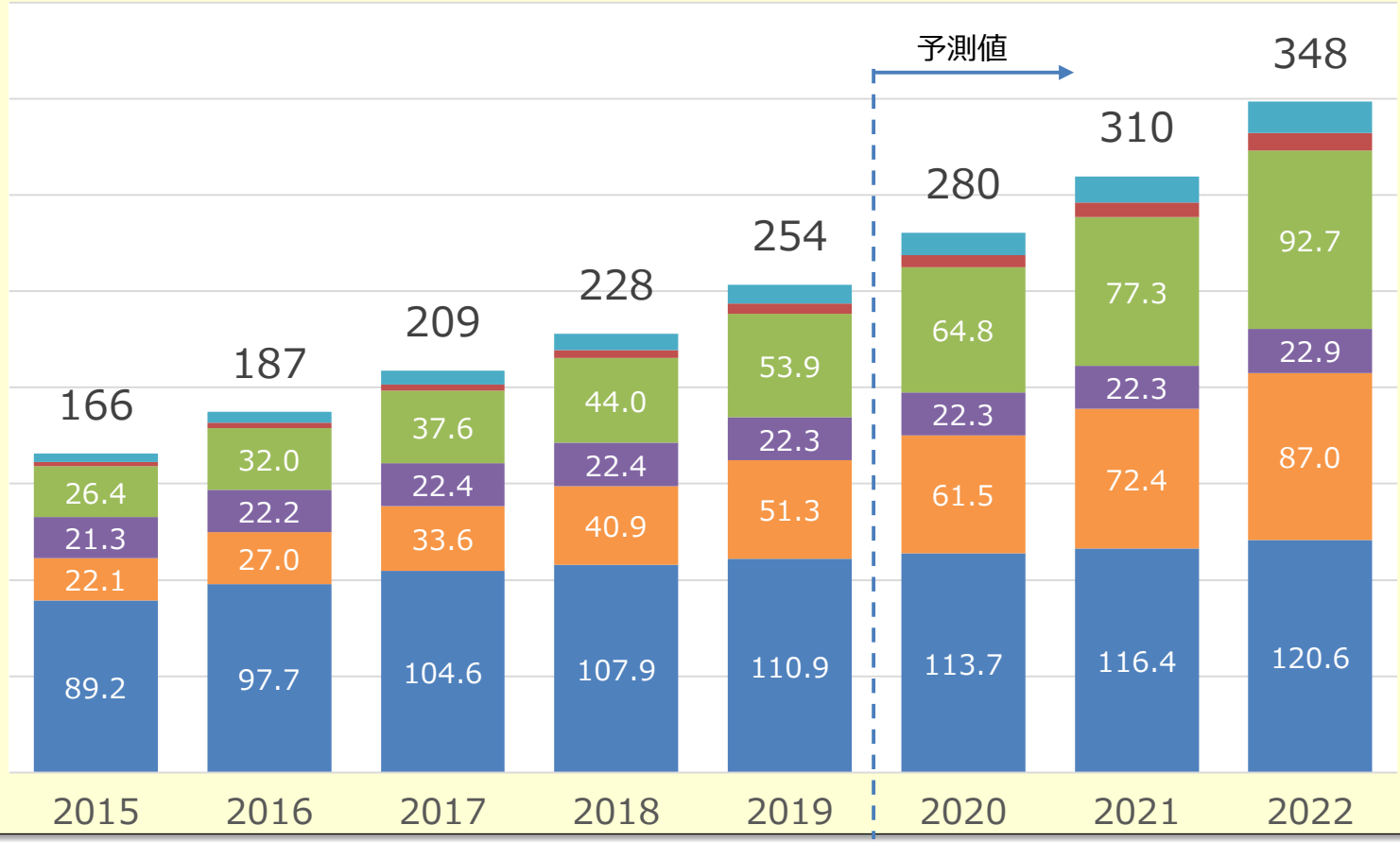
サイバー攻撃に関する最近の動向

令和３年６月２９日

IoTデバイス数の増加

- インターネットにつながるモノ（IoT機器）の数は300億個程度と推定されている。
- 今後も、スマート工場・スマートシティ等の「産業用途」や、スマート家電等の「コンシューマ」の増加が想定。

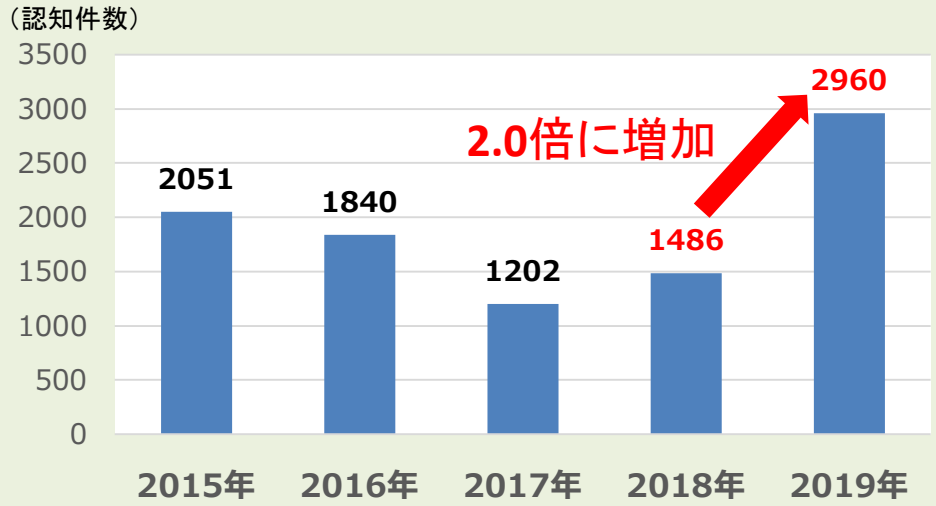
世界のIoTデバイス数の推移及び予測（単位：億台）



（出典）令和2年度情報通信白書

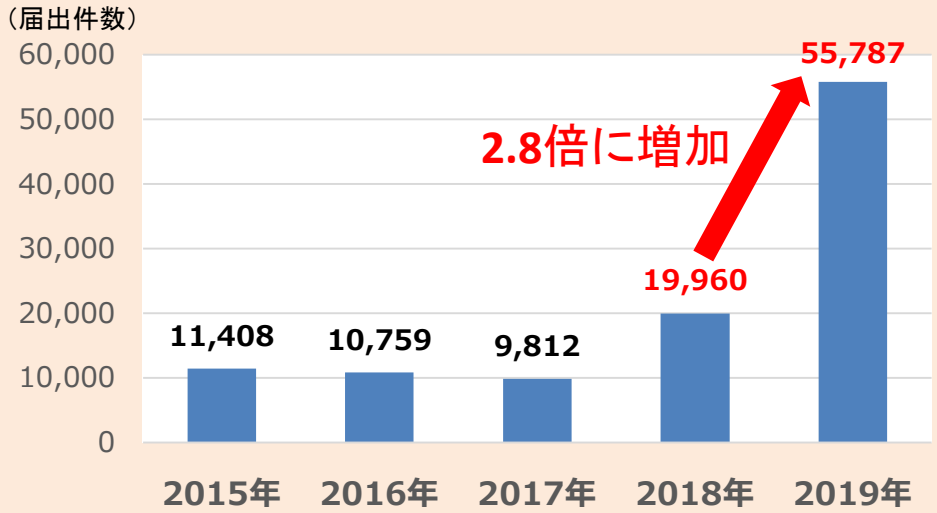
サイバーセキュリティ上の脅威の増大

不正アクセスの増加



出典：「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（令和2年3月警察庁・総務省・経済産業省）

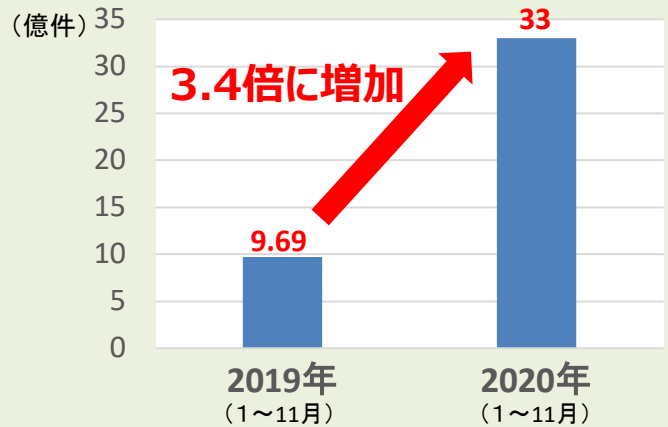
フィッシングの増加



出典：「フィッシングレポート2016」~「フィッシングレポート2020」（フィッシング対策協議会技術・制度検討WG）

テレワーク環境を狙った攻撃*の増加

＊リモートデスクトップ（RDP）を狙ったブルートフォース攻撃数（kaspersky社による検出数（世界））



出典：Kaspersky The story of the year: remote work(10 Dec. 2020)より作成

※フィッシング対策協議会に寄せられたフィッシング報告件数（海外含む）

出典：フィッシング対策協議会　2021/01 フィッシング報告状況（2021.0203）

昨今発生したサイバー攻撃事例

【2020年】

（piyolog、各社公表資料、各種報道等より総務省作成）

1月　三菱電機のネットワークが**不正アクセス**を受け、**機密情報**(防衛省の「注意情報」を含む。)**等が外部流出した可能性**が判明。

4月　国内高校の半数が利用するClassi社が**不正アクセス**を受け、**IDや暗号化パスワード等が流出**した可能性が判明。

5月　NTTコミュニケーションズ従業員の**テレワーク環境(仮想デスクトップ)に係るアカウント及びパスワードが窃取**され、**顧客情報（政府機関を含む）が流出**した可能性が判明。

6月　ホンダが**サイバー攻撃**を受け、**世界の９工場で生産を一時停止**。

8月　国内数十社において、**VPN機器の脆弱性を悪用した不正アクセス**が行われVPN接続用のパスワードなどが流出した可能性が判明。

10月　原子力規制委員会が、**不正アクセス**を受け、メール等のやりとりを含む**外部とのアクセスを遮断**。

11月　カプコンが、**オーダーメイド型ランサムウェアによる標的型攻撃**を受け、**個人情報・人事情報・開発資料等が流出**した可能性が判明。

12月　楽天が、**クラウド型**営業管理システムの**設定不備**を突かれ、**個人情報等にアクセス**された可能性が判明。

12月　米SolarWinds社のIT管理ソフトウェア（orion platform）の脆弱性とソフトウェア更新を悪用した、**複数の米政府機関への大規模サイバー攻撃**が判明。

【2021年】

3月　東京都等の複数の自治体から住宅政策関連の調査を委託していたランドブレイン社が**不正アクセスを受けランサムウェアに感染**、社内のファイルサーバ内情報が暗号化された上、個人情報が流出した可能性も判明。

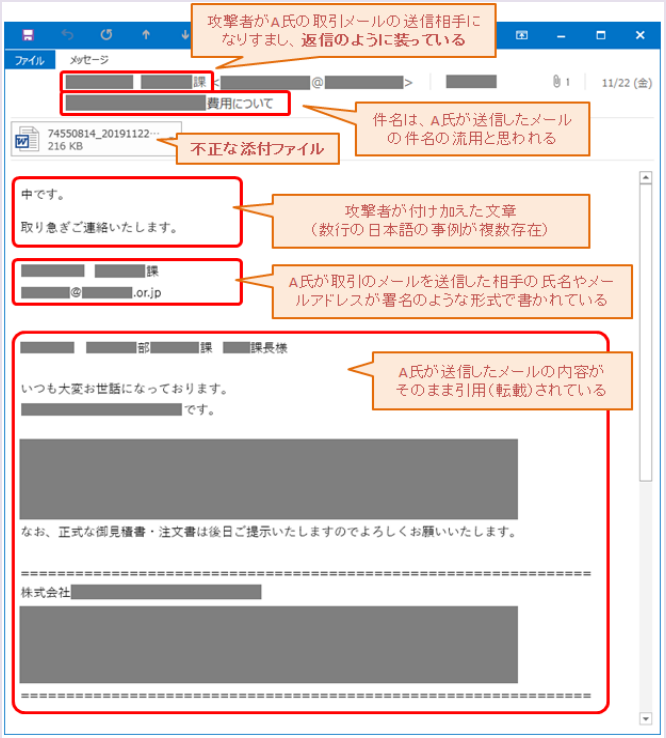
4月　HOYAの米子会社が**ランサムウェアによる標的型攻撃**を受け、盗まれた情報とみられる**顧客の個人情報等が、闇サイトに公開**されたことが判明。

マルウェア「Emotet」の感染拡大

○ 取引相手になりすまして、過去に実際にやり取りしたメールの本文の一部をそのまま引用し、不正なプログラムが仕組まれたファイルを添付するなどしたメールを送り付ける手法によるサイバー攻撃（攻撃型メール）

○ 一昨年夏頃から、世界規模で観測。特に昨年夏から秋にかけて攻撃が急増し、被害も拡大。

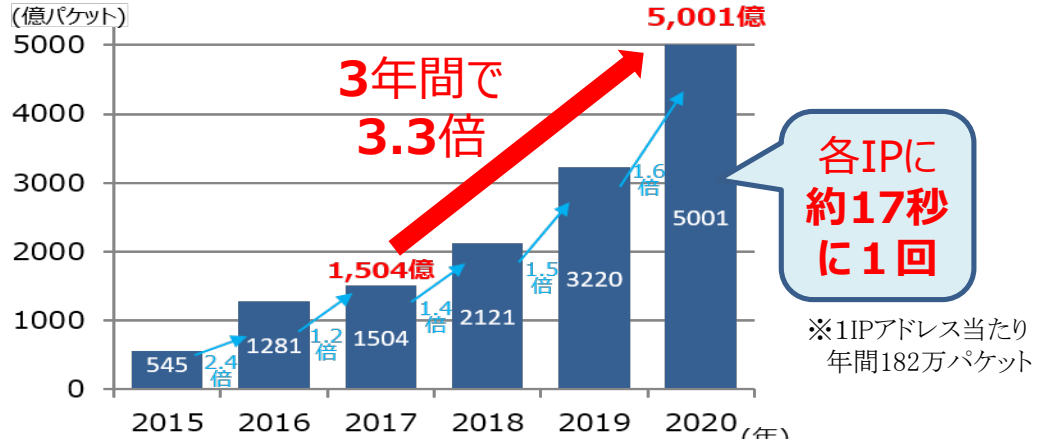
○ 添付ファイルを開くことで、パソコン内に不正なプログラム（マルウェア）を感染させ、当該マルウェアに感染したパソコン内の情報を窃取したり、当該パソコンを踏み台にして情報システム内の他の機器に侵入し、当該他の機器内の情報を窃取するなどの攻撃を行う。
また、感染したパソコンに他のマルウェアを秘密裏にダウンロードすることで被害を拡大させるおそれがある。



NICT(NICTER）によるサイバー攻撃観測

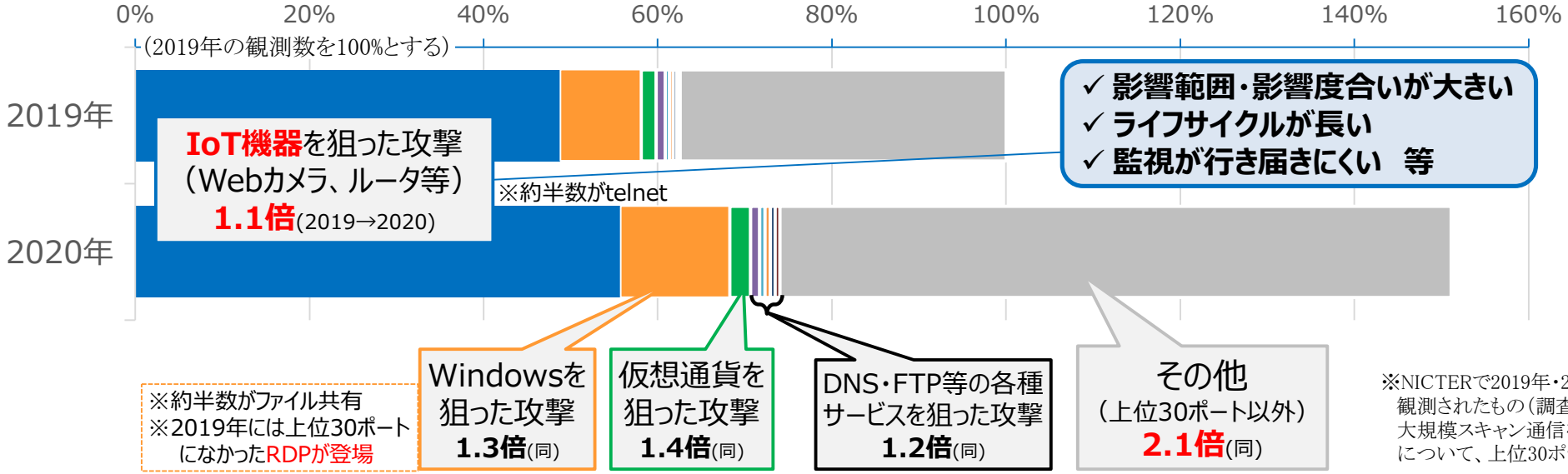
➢ 国立研究開発法人情報通信研究機構(**NICT**)では、大規模サイバー攻撃観測網である**NICTERにおいて、未使用のIPアドレス30万個(ダークネット)を活用**し、グローバルに**サイバー攻撃の状況を観測。**

NICTERで１年間に観測された国内外からのサイバー攻撃関連の通信数



NICTERにより観測された国内外からの通信の内容（上位30ポートの分析）

✓ **IoT機器を狙った攻撃が依然としてトップ**
✓ **攻撃(対象ポート)が年々多様化**



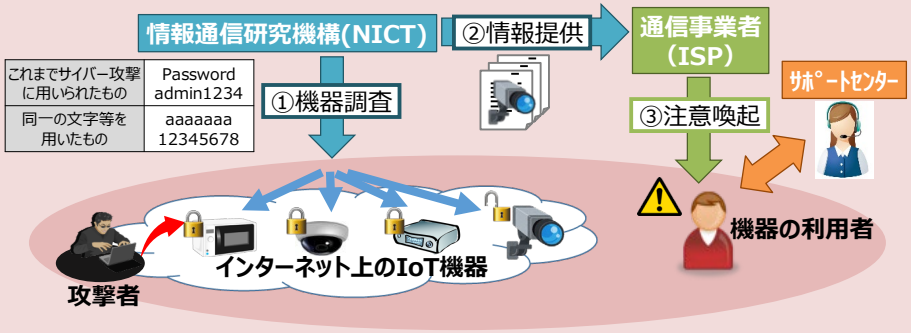
※NICTERで2019年・2020年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析。

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】

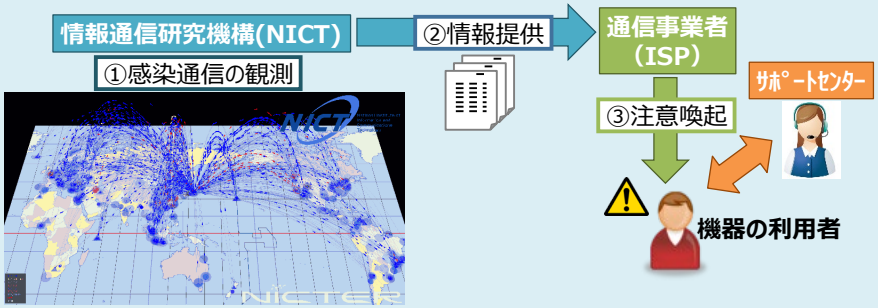


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

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

NOTICEの取組強化（実施計画の変更認可）

- 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。
  ※2019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。
- NOTICEの**実施計画**に記載された事項のうち、特定アクセス行為において**入力する識別符号**、及び特定アクセス行為の**送信元のIPアドレス**について、NICTから**変更**したい旨の申請。

  →2020年９月11日付けで**総務大臣認可**　（10月度の調査から適用）

実施計画に記載が必要な事項

総務省令※において規定。

※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）第2条第2項各号

- ✓ 業務従事者の氏名・所属部署・連絡先
- ✓ 特定アクセス行為の**送信元のIPアドレス**
- ✓ 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**
- ✓ 特定アクセス行為の送信先のIPアドレス範囲
- ✓ 特定アクセス行為に関する情報の適正な取扱い
- ✓ ISP等への通知先に求める情報の適正な取扱い
- ✓ その他必要な事項

変更内容

(1) 特定アクセス行為において（ID・パスワード）入力する識別符号の追加

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

IoT機器調査及び利用者への注意喚起の実施状況（2021年３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**66社**。
  当該ISPの**約1.12億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**１,８８３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**４６９件**の**対象を検知**しISPへ通知。

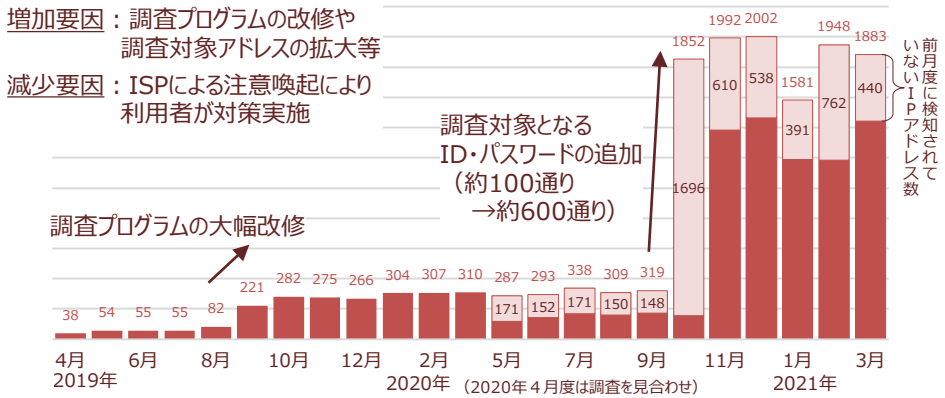
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

１,８８３件（２月度:1,948件）

（参考） 2020年度の累積件数：12,804件（2019年度：2,249件）
ID・パスワードが入力可能だったもの：9.6万件

*) 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

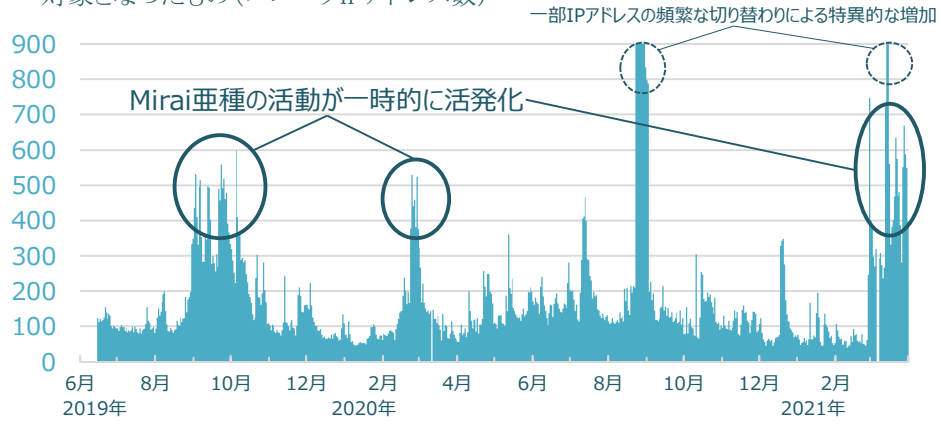
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均４６９件（２月度:94件）

（参考） 期間全体での値： １日平均190件
最小：40件(2021/2/10)／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）



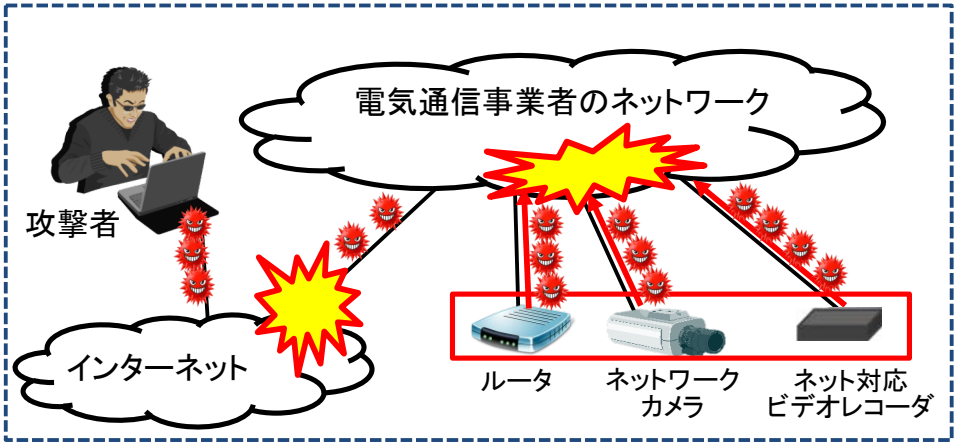
IoT機器のセキュリティ対策に関する技術基準の改正

【背景・課題】

- 近年、インターネットにつながるWebカメラやルータ等のIoT機器を悪用したサイバー攻撃により、通信網に深刻な障害を及ぼす事案が発生。
- その原因としては、**パスワード設定の不備などによりIoT機器を悪用されるケースが多く**、その対策が重要な課題。

※1　2016年10月、「Mirai」というマルウェアに感染した10万台を超えるIoT機器が、米国のDyn(ダイン)社のシステムを攻撃し、Dyn社のサーバーを利用していた数多くの大手インターネットサービスやニュースサイトに障害が発生。

＜IoT機器が乗っ取られてサイバー攻撃に悪用される事案のイメージ＞



【端末設備等規則（省令）の改正概要】

- インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準（端末設備等規則）に追加する。

  ①アクセス制御機能※1（例えばアクセス制限をかけてパスワード入力を求め、正しいパスワードの入力時のみ制限を解除する機能のこと）

  ②初期設定のパスワードの変更を促す等の機能

  ③ソフトウェアの更新機能※1

  又は①～③と同等以上の機能※2

  ※1 ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。
  ※2 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

- PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

【その他】

- 2020年４月１日に改正省令を施行。
- 改正省令の運用方法や解釈等を定めるガイドラインも策定し、公表した。

ネットワーク側での機動的な対処の実現に向けた検討①

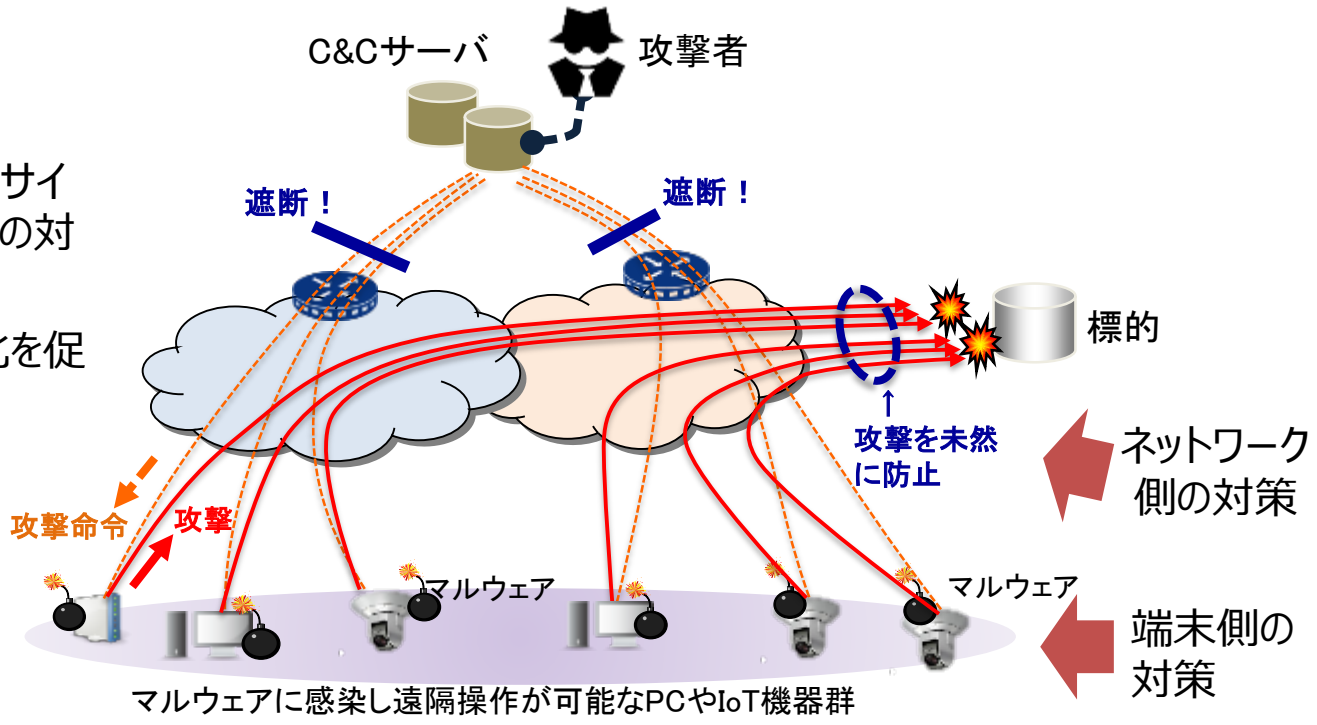
- IoTの進展に伴い、脆弱でセキュリティ対策が困難な端末機器も増加する中、**端末側とネットワーク側の双方から、総合的なセキュリティ対策を実施**することが求められている。
- 端末側の対策としては、電気通信事業法における端末設備等規則へのセキュリティ要件の追加や、脆弱な状態にある機器の利用者への注意喚起等の取組みを実施。
- **ネットワーク側の対策**として、**電気通信事業者が個々の感染端末に指示を出すC&Cサーバに直接対処**するなど、**より効率的・機動的にセキュリティ対策を実施**することが重要。

  ⇒ サイバー攻撃が通過する**ネットワーク側で機動的な対処を行う環境整備**が必要。

■ 端末側の対策とも連携しつつ、ISPが管理するネットワーク側においても高度かつ機動的な対処を実現するための方策の検討が必要。

- ISPが自らC&Cサーバを検知し、サイバー攻撃の指令通信の遮断などの対策を実施するための方策
- 新技術を活用した対策の高度化を促進するための方策　等

⇒ **制度的・技術的な観点から検討**を推進



ネットワーク側での機動的な対処の実現に向けた検討②（参考）

（以下、「サイバーセキュリティタスクフォース第31回会合（令和3年5月13日）資料31-3より抜粋）

- IoTのセキュリティ対策としては、**端末側の対策として、これまで電気通信事業法**（昭和59年法律第86号）における端末設備等規則（昭和60年郵政省令第31号）**へのセキュリティ要件の導入や、パスワード設定に不備のあるIoT機器やマルウェアに感染している機器の利用者への注意喚起といった取組を実施**してきた。
- しかしながら、IoTを狙った攻撃は依然として多く、また、今後、5Gの進展により様々な産業でIoT機器の利用が更に拡大することが予想される中、**これまでの対策だけでは必ずしも十分ではないおそれ**がある。
- そのような中、**IoTのセキュリティ対策をより実効的なものにするためには、サイバー攻撃が通過するネットワーク側でより機動的な対処を行う環境整備が必要**と考えられる。
- このため、ユーザ側で運用している情報通信機器や情報システムのセキュリティ対策と連動する形で、**インターネット上でISPが管理する情報通信ネットワークにおいても高度かつ機動的な対処を実現するための方策の検討が必要**ではないか。
- 具体的には、**電気通信事業者が自らトラフィックの流れ**（フロー情報）**を把握・分析してC&Cサーバ**（マルウェアに感染した端末に対して指令を与えるサーバ）**を検知し、検知したC&Cサーバに関する情報を電気通信事業者間で共有し、サイバー攻撃の予兆を捉えて早期に対処できるよう**にするため、通信の秘密に配慮した適切な対応を電気通信事業者が円滑に行うことが求められるところ、**制度的な観点から対策の検討を行うことが重要ではないか**。なお、中長期的な課題として、通信の秘密の保護を図りつつ、より迅速なセキュリティ対策を実現するために、必要に応じ新たな視点からも検討を行うことが適当ではないか。
- また、**フロー情報分析によるC&Cサーバ検知の手法について、現場での実証を行い、技術面・運用面での課題を検証するとともに、**AIを活用して検知の高度化を図るなど、**新技術を活用した対策の高度化を促進することとしてはどうか**。

（参考）過去の会合における構成員からの御意見

- ✓ フロー情報分析を行って、本当にC&Cサーバを検知することができるのか、通信業界でもトライアルをさせていただけるのであればありがたい。いきなり通信を遮断するのではなく、C&Cサーバの検知が本当にできるのかということを、通信の秘密との関係や法的な課題や技術的な課題を整理するという所から始めさせていただけるのであれば、非常にありがたい。
- ✓ NICTとしては、電気通信事業者のフロー情報だけではなくて、例えばNICTでの色々な知的基盤が集まっているデータとのコリレーションなどを行うことによって、精度の高いC&Cサーバの検知などへの活用ができると良い。

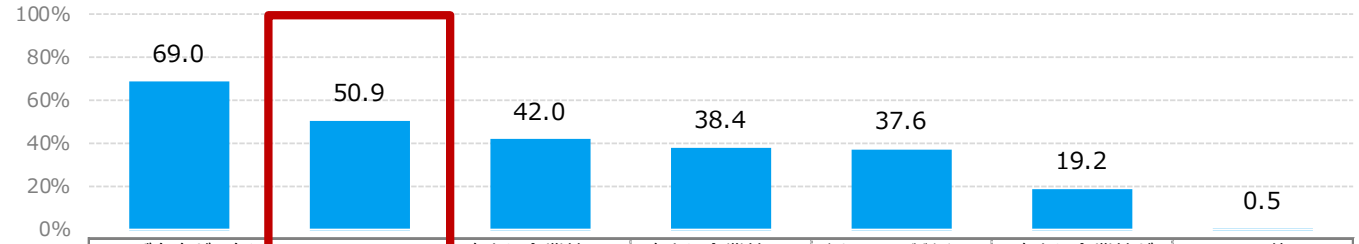
サイバーセキュリティに関するインターネット利用者の意識調査結果

本年３月に、学業や仕事の利用以外にインターネットサービスを利用する18歳から69歳の男女を対象としたウェブアンケートを行った結果、コンピュータウイルス感染防止の有効な対策として、ISP等の事業者が十分なセキュリティ水準を確保するよう努めるべきとの回答が過半数であった。

（以下、「サイバーセキュリティタスクフォース第30回会合（令和3年4月7日）資料30-1-1より抜粋、一部編集）

（対象者）全数

Q13.あなたは、パソコンやルータ等、また、家庭内でネットにつないだ監視カメラ等のIoT機器がコンピュータウイルスに感染するなどの被害を防ぐための対策として、どのようなことが有効だと思いますか。（いくつでも）



※数表内の網掛け
- 全体値より10%以上高いもの
- 全体値より5%以上高いもの
- 全体値より5%以上低いもの
- 全体値より10%以上低いもの

		n	ユーザ自身が、自らの保有する機器がコンピュータウイルスに感染しないように、もっと心掛けるべきである	インターネット接続サービスを提供するISPや携帯電話事業者、また、WiFi設置者等は、ユーザが安心してネットを利用できるよう、十分なセキュリティ水準を確保するよう努めるべきである	政府や企業等は、ユーザに対して、特に基本的なセキュリティ対策について、わかりやすい周知啓発に努めるべきである	政府や企業等は、ユーザに対して、高度なセキュリティ対策も含めて、周知啓発に努めるべきである	政府は、ユーザが安心してネットを利用できるよう、インターネット接続サービスを提供するISPや携帯電話事業者、また、WiFi設置者等に対して、わかりやすい指針等を示すなどにより、十分なセキュリティ水準が確保されるように努めるべきである	政府や企業等がユーザに対して周知啓発を行っても感染防止の効果には限界があり、周知啓発の必要性はあまり高くない	その他
全体		(2,000)	69.0	50.9	42.0	38.4	37.6	19.2	0.5
ネット１日当たり平均使用時間	30分未満	(105)	49.6	37.1	36.5	29.5	39.7	18.2	0.5
	30分～2時間未満	(802)	65.1	50.6	38.9	33.9	38.4	17.0	0.4
	2時間以上	(1,032)	74.5	53.2	45.7	43.9	36.3	21.6	0.5
ネット最利用機器	パソコン	(635)	70.8	49.9	41.1	38.4	35.7	18.7	0.6
	スマホ	(1,268)	68.5	51.7	42.6	38.6	38.5	19.8	0.3
マルウェア感染認知度	知っている	(1,475)	75.7	56.2	44.6	42.0	39.0	19.7	0.3
	聞いたことはある	(390)	55.0	41.3	39.9	32.5	29.5	18.9	0.9
	知らない	(136)	37.0	19.9	19.7	16.3	45.9	14.1	0.2
サイバー攻撃踏み台認知度	知っている	(954)	80.8	54.6	45.5	43.4	36.0	20.1	0.4
	聞いたことはある	(624)	60.3	47.9	40.3	35.0	34.5	17.8	0.6
	知らない	(422)	55.1	46.7	36.3	32.0	46.0	19.1	0.4

※全体で降順ソート

(%)