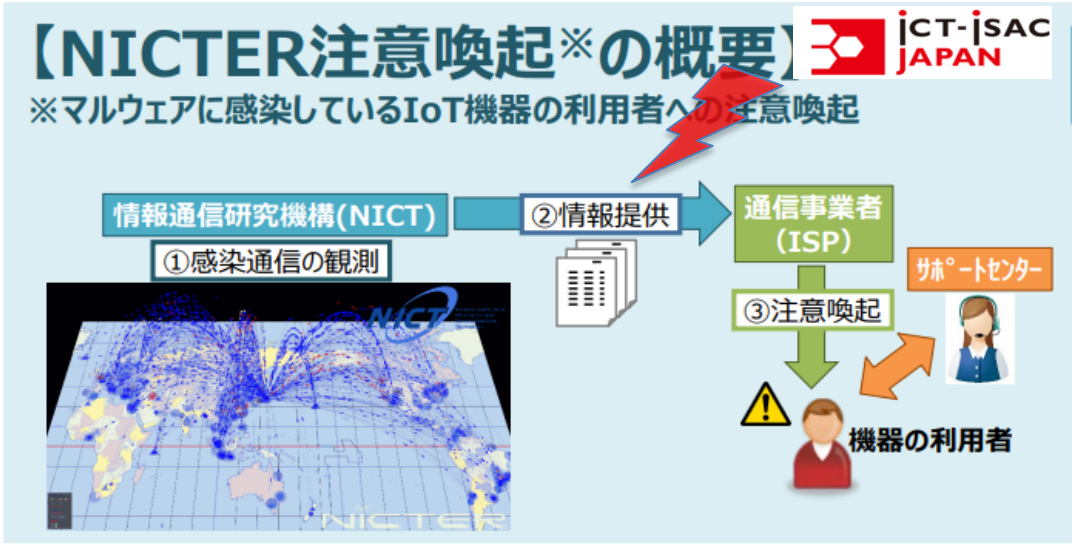
資料１－４－３

NOTICEにおけるICT-ISACの役割と課題認識

2023．1．18

ICT-ISAC

NOTICEにおけるICT-ISACの役割



【NOTICEにおけるICT-ISACの役割】

1. NOTICEのハブとして、参加ISP連絡窓口とセキュアネットワークを管理し、注意喚起対象情報をISPに配信。
   - 専用セキュアネットワークKIZUNAの提供
   - 毎月月初に、各ISPから検査対象のIPアドレスを収集
   - NOTICEでは第4週に注意喚起対象となるIPアドレスとタイムスタンプをNICTから受け取り、各ISPに受渡し
   - NICTERでは、NICTが観測した感染通信ログを、各ISPに受渡し
   - ISPは受信した情報でユーザ特定し、注意喚起を実施
   - 卸先事業者には、卸元事業者経由で送信
2. 各ISPが注意喚起した状況(月次報告)を集計・分析し、NOTICE注意喚起方法の改善を支援
3. NOTICE説明会等を定期的に開催し、NOTICEに参加するISPの拡大を支援
   - NOTICEに参加する手続きの説明(技術的条件の認可申請・約款の改訂・NICT覚書・ICT-ISACとの守秘義務契約)
   - 特に卸元・卸先に役割がわかれる場合の考え方の説明
   - YouTubeを活用して、いつでもNOTICEを理解できる周知・広報

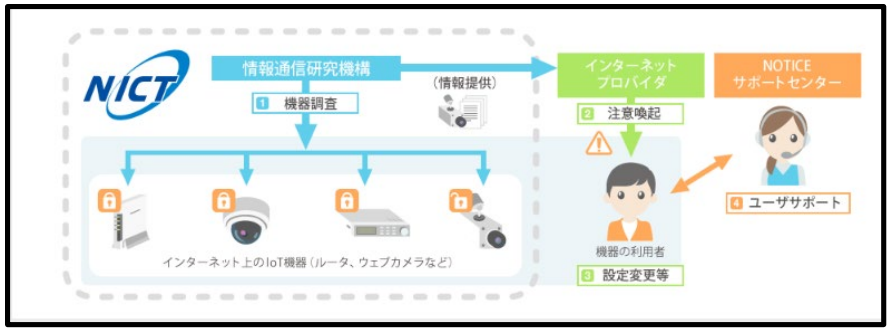
NOTICEで伝えたい注意喚起のポイント

- NOTICEを通じて、脆弱なIoT機器の利用者が、機器の利用を通じて意図せずサイバー攻撃に悪用されることがないように、注意喚起を実施。

NOTICEの仕組みがない場合の利用者の声

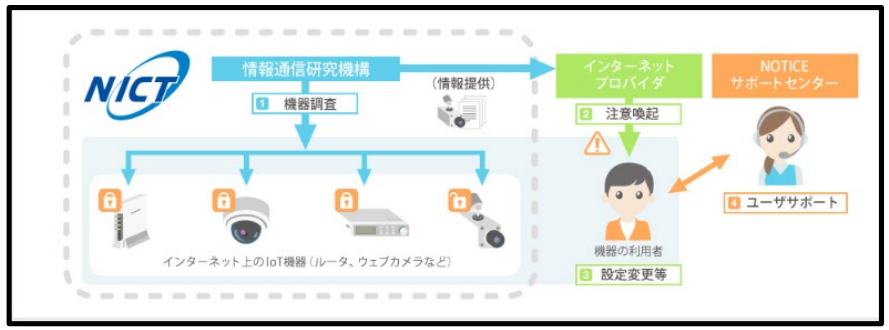
- 利用者はサイバー攻撃に備えて何をすればいいの？
- サイバー攻撃なんかわからないから、私たちは関係ないよね？
- 本当に危ないときだけ、教えてくれればいいのに？
- IoT機器って、使わない方がいいの？
- ルータ等機器メーカからは、危険な場合に教えてくれないの？

NOTICEで伝える利用者へのメッセージ

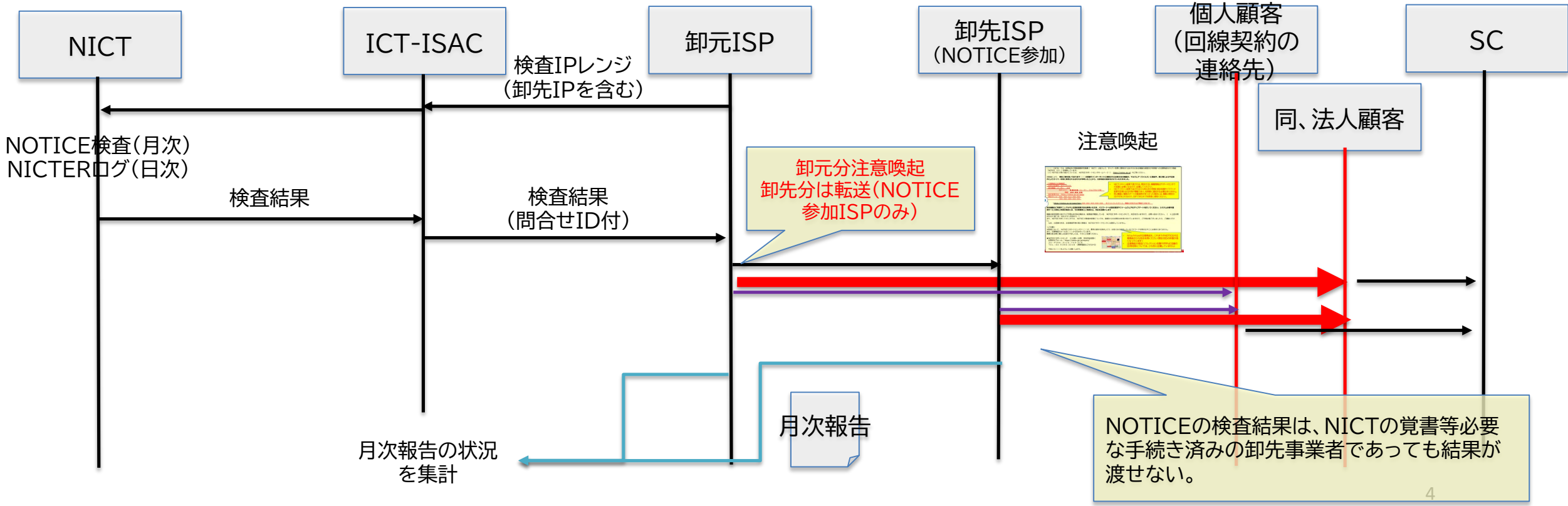


- インターネットの使い方によっては、意図せずあなた（の会社）の機器がサイバー攻撃の原因を作ることもある。
- あなたの回線に、サイバー攻撃を行う蓋然性の高いIoT機器（またはすでに感染通信を出しているIoT機器）が接続されていることを観測している
- 必要な対処（パスワード変更等）をお願い

【参考】NOTICE/NICTERの注意喚起業務の流れ



1. ISPから検査のIPレンジを集める
2. NOTICEは月次、NICTERは日次で情報を提供する
3. ISPは利用者を特定し、ISP名で利用者に注意喚起するか、卸先に転送する。但し、卸先がNOTICEに入っていない場合には、情報は渡せない
4. ISPでユーザ特定し注意喚起する。（この段階で、ISPで個人か法人かを分類）
5. 注意喚起した情報をISPは月次報告として報告する。ICT-ISACで注意喚起の状況を集計する



NOTICEの注意喚起対処依頼の内容

NOTICEでは、IoT機器の利用者への対処依頼を、注意喚起として以下の情報を提供

○○○（ISP名）では、総務省及び情報通信研究機構（NICT）と協力して、サイバー攻撃に悪用されるおそれのある機器の調査及び利用者への注意喚起を行う取組「NOTICE（※）」を実施しています。（※）NOTICEの取り組みについては、NOTICEサポートセンターホームページ（ ください。
当取組により、現在ご契約頂いております○○○の回線でインターネットに接続されたお客さまの機器が、マルウェア（ウィ 不正操作によりサイバー攻撃に悪用されるおそれが判明したことから、注意喚起の連絡をさせていただきました。

【注意喚起の対象機器】
お客さま番号：N********
該当機器：メーカー　A社
カテゴリー　●●●●●（ルーター、ウェブカメラ等）
機器　●●-●●-●●
設定変更方法：https://notice.go.jp/cases
問合せＩＤ：XXX-XXX-XXX-XXX

（https://notice.go.jp/cases?isp=XXX-XXX-XXX-XXX　をクリックいただくと、機器の対処方法が確認できます）

該当機器のご利用マニュアルや上記設定変更方法を参照いただき、パスワードへの設定変更やファームウェアのアップデートを 守運用サービス等をご利用の場合には、その事業者とご相談の上、対応をお願いします。

機器の設定変更にあたりご不明な点がある場合は、総務省が開設しているNOTICEサポートセンターにて、対応を行い 記の問合せIDに基づき、対応させて頂きます。）
また、NOTICEサポートセンターでは、NOTICEの取組内容等についても、皆様からのお問合せを受け付けていますので、ご不明点 たら、ご連絡 ください。
なお、お客様の氏名、お客様番号等の個人情報はNOTICEサポートセンターには提供していません。

<ご注意>
本取組において、NOTICEサポートセンターや○○○が、費用の請求を請求したり、お客さまの設定しているパスワードを聞き
また、注意喚起のメールは○○○からのみ行っています。
悪意のある第三者による成りすましには、十分にご注意ください。

■NOTICEサポートセンター　※10時～18時　年末年始を除く
お問合せフォーム：https://notice.go.jp/inquiry/
フリーダイヤル：０１２０-７６９-３１８
ＴＥＬ：０３-４３４６-３３１８　（携帯電話はこちらから）
今後とも○○○をよろしくお願いします。

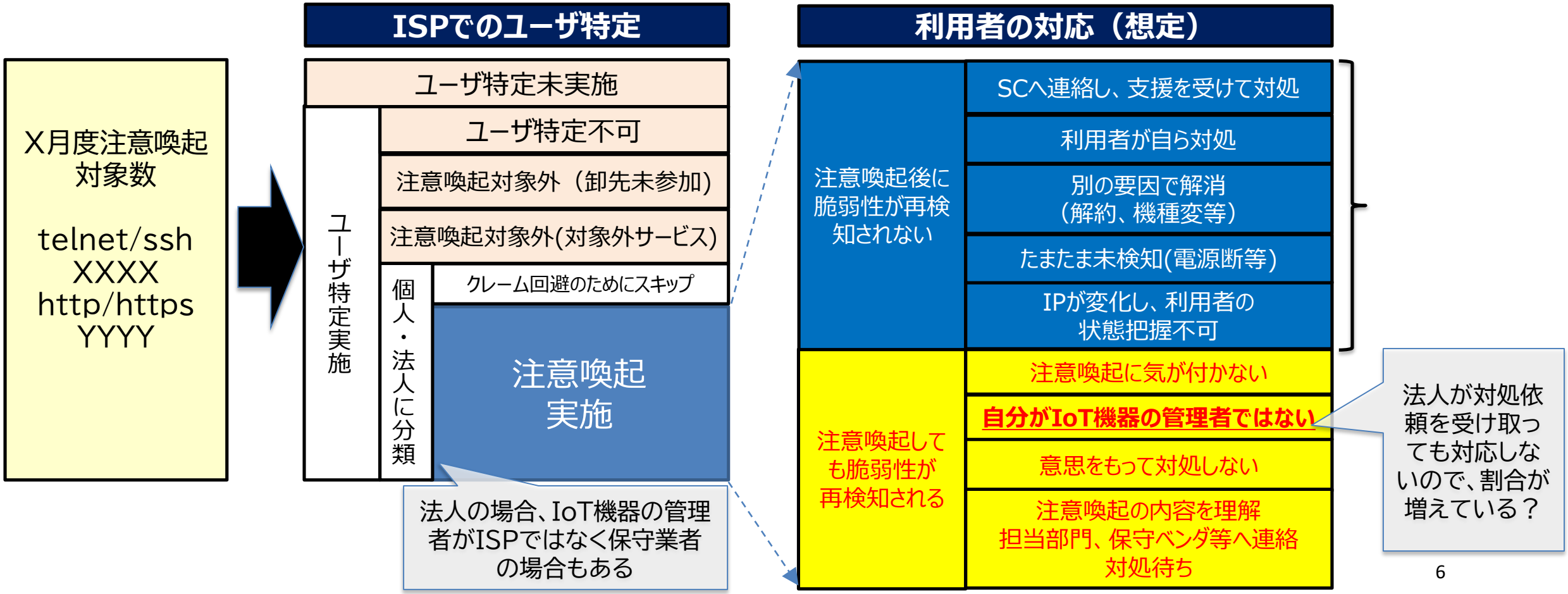
【NOTICEでの注意喚起であることとその危険性】
ISP名で、NOTICEの取り組みによる注意喚起であること、回線で接続された機器がマルウェア感染や第3者の不正操作によりサイバー攻撃に悪用されている恐れ、を説明している

【NICT検査で判明した機種情報と、問合せID】
（NOTICE検査で脆弱性が見つかった）脆弱な機器の機種情報をなどを示して、注意喚起している。
その際、NOTICEの取り組みであることを示す、問合せIDを付与している。
（※設定パスワードは、安全上記載しないし、ISP側ではパスワードはわからない）

【対処方法】
当該機器のマニュアルへのリンク情報など、対処方法は示すので、基本は自身でパスワード再設定やファーム更新などを対処すること。
不明な点がある場合に、NOTICE SCへの問合せを案内している

ISPでのユーザ特定と利用者の対応

- 注意喚起対象の情報を、各ISPに配信（NOTICEでは月次、NICTERは日次）
- ISPでは注意喚起のために、ユーザを特定。この際、ユーザを特定する際に、併せてISPで、注意喚起対象が個人契約か法人契約かの分類も依頼
- 法人契約の場合には、注意喚起を受ける当人が、IoT機器の設置や保守に関わっていない可能性も考えられる。

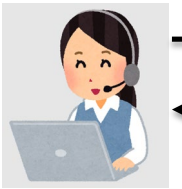


NOTICE注意喚起での課題と、改善推進の取り組み

1. 利用者に直接調査し、脆弱性対処状況を把握
   - 専用部隊で架電調査すると、メール等の注意喚起ではパスワード変更しない利用者？
2. NOTICEがリスクを、利用者に伝わるように啓発・広報の強化
   - 毎月数百件注意喚起しても、利用者の反応は少ない（NOTICE-SCへの入電は月十数件）
   - Emotetでの注意喚起の際には、「あのニュースでやっているEmotetがわが社でも感染しているのか？」と、利用者の反応が大きい
   - NOTICEの注意喚起には、パスワードが緩いだけなら人には迷惑かけないとの誤解？
3. ISPのサイバー対処の強化へ。調査情報の効果的な活用
   - 3年半で5百種類以上の機器。注意喚起対象の大半は、2016年以前に発売されたルータ
   - ISPには関係する機種以外は、NOTICEで検知した情報はISPにも情報公開していない
4. IoT機器管理者に危険性と対処を促すことを容易にするエコシステムが必要？
   - 回線契約者は必ずしもIoT機器管理者でないため、注意喚起を確実にIoT機器管理者に伝えるため利用者側の体制が必要。
5. ISP側の負担軽減の推進
   - コロナ禍、情報管理のために、NOTICEのために出勤を強いられる

架電による注意喚起対象者への直接調査（2021年度実施）

2021年に、架電調査を実施（NOTICEの注意喚起を行った社に対して、架電調査専門体制から架電して、「注意喚起に気が付かなかったのか」など、**法人24社29件に対して直接状況をヒアリング）→1社を除き、注意喚起にはPositiveな対応**



「注意喚起、気が付いた？」

「担当者は、誰ですか？

【架電調査での利用者の反応】

- **キーマンが誰か※を教えて**・・・（注意喚起対象となる法人内で、IoT機器の設置やサイバー対処の担当者）
- 「（3割程度で）**パスワード変更やっておきます」と回答をいただいても、実際に対応されることはない。**
- 「IoT機器のサイバー攻撃と言っても実感がわかない」「何か今支障があるわけではない」「実際にサイバー攻撃が起きても自社に影響がない」と考えているのではないか→ **サイバー攻撃に加担するイメージがわかない。**
- **個人情報の取り扱いにより、そもそも架電調査をISPから専門体制への委託が困難**

架電調査の流れ

■架電ステータス別件数

大項目	ステータス	リスト別件数 件数 29	割合	件数	割合	ユーザ別件数 件数 24	割合	件数	割合
未着手	未着手	0	0%	0	0%	0	0%	0	0%
	現アナ	0	0%			0	0%		
	連絡先不明	0	0%			0	0%		
キーマン調査中	不出	1	3%	19	66%	1	4%	14	58%
	キーマン調査中	17	59%			12	50%		
	干渉拒否	1	3%			1	4%		
	対応不可	0	0%			0	0%		
	架電先相違、認識なし	0	0%			0	0%		
キーマン把握済み	キーマン把握済み	0	0%	2	7%	0	0%	2	8%
	キーマン折衝、注意喚起中	2	7%			2	8%		
注意喚起済み	注意喚起済み	0	0%	0	0%	0	0%	0	0%
	利用状況ヒアリング予定	0	0%			0	0%		
	利用状況ヒアリング中	0	0%			0	0%		
	利用状況ヒアリング済み	0	0%			0	0%		
パスワード変更	パスワード変更依頼	8	28%	8	28%	8	33%	8	33%
	パスワード変更済み	0	0%			0	0%		

もともと根雪となっている法人顧客について、個人情報を除いて架電委託

注意喚起相手の情報がない架電調査のため、キーマンを探せるかどうかは一つのハードル

キーマン通じて注意喚起とパスワード変更出来たが、実際の変更は業者が実施。翌月以降ISPで実際に変更されたかを調査？

キーマン情報がなくても、3割程度でパスワード変更に了解いただくが、実際には変更されない

機器メーカ（ルータ等）のヒアリングを通じた知見

NOTICEの注意喚起対象となるIoT機器の多くは、ルータ等機器メーカの初期パスワードが脆弱であることが大きい。
→ 個人の場合と、法人の場合で、今後のリスクが異なると想定

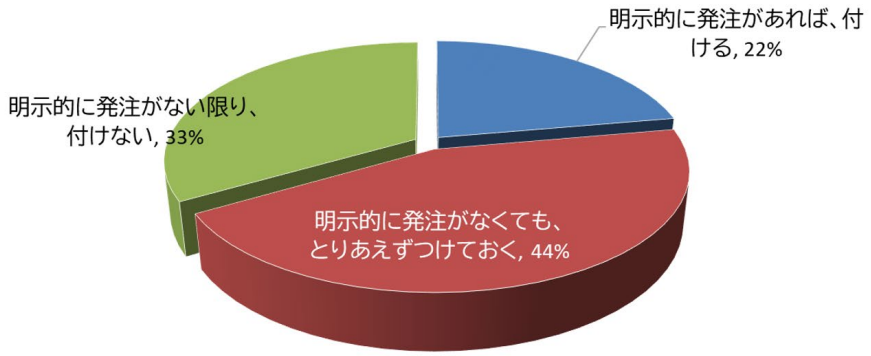
個人

→ 一部機器メーカでは、2019年頃から、初期パスワードが脆弱でない機種を販売している。個人向けのルータは順次買い替えが進むことで、注意喚起対象は減っていくものと思われる（WANからのアクセスは基本開かない）
→ 端末施行規則の見直しで、2020年4月以降に発売される機器には、初期パスワードに対策が取られている（注意喚起対象は少ない）

法人（今後実地調査で確認予定）

→ コストを抑えるために、意図的に中古のルータが継続して使われることがある
→ 法人の社内のガバナンス外でネット利用のアクセス口を付ける場合、必要な保守や注意喚起が行き届ず、抜け穴になることもある。
→ 将来的な遠隔保守のために、発注がなくてもWAN側からtelnetなどが使えるように設定されることがある
→ 法人向けのIoT機器が、今後サイバー攻撃の悪用に使われやすいのではないか？

遠隔保守のための仕組みは、どのような場合に付けますか？



Sier向けのアンケート調査では、将来的な遠隔保守のために、明示的な発注がなくても遠隔保守の仕組みは付けられる

※NOTICE外の講演でのアンケート調査による

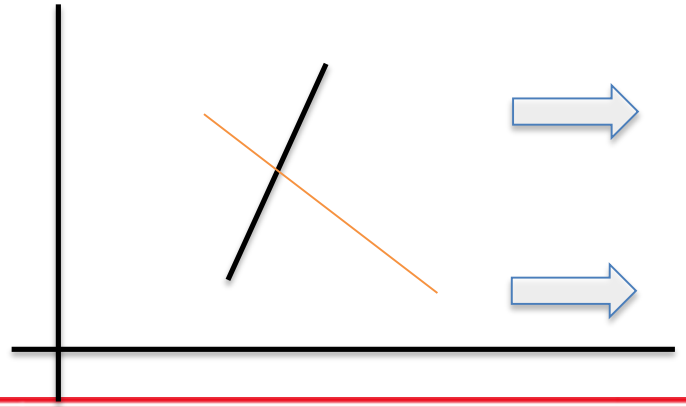
参考：NOTICEを通じて得られた知見

毎月の注意喚起ではそれほど効果がすぐに表れないが、乱高下を示す機種はあり、深堀のきっかけとなる
（例：　脆弱なポートを通じてマルウェアが感染が発生したのか（マルウェアに感染するとポートを閉じるマルウェアがある）、特定の法人やISPが大量に設置したのか、など）

例：2022年11月検査を通じて判明した差異（※　ONとは、注意喚起対象となった対象機種のIP数

ISP（検査種別）	前月ON※	今月ON※（前月比）	主な増減理由	ISPヒアリングを通じた対処
A社（http/https）	183	355（+172）	●●製作所「XXXXX」がA社で0→171件（他、B社でも0件→9件）	A社に、ICT-ISACから調査依頼中（→　以下の製品の、初期パスワードの問題？であれば、当該機器メーカにコンタクトするなどを想定
B社（http/https）	4	54（+50）	▲▲システム「YYYYY-YYYY」で、7, 8月が54件、9, 10月が4件、11月54件	B社より、ISPとしての動きは把握していないため、詳細わからない（但し、右下表のような検出の増減が出ているため、継続モニタ予定）
C社（http/https）	658	607（−51）	51件減少のうち、■■「ZZZZ-ZZ」が125件→79件と46件も減少	C社より回答。ISP側では特に作業なし。感染が広がってポートを閉じたのかもしれない→継続監視、必要に応じてNICTERも注視

定期的観測での注意喚起対象数の増加が、サイバー攻撃の予知につながるのではないだろうか？



- （大きく増えた場合）
  脆弱な機器の大型設置で注意喚起対象が増加
- （大きく減った場合）
  第3者アクセスが原因で注意喚起対象数が減少？
  （マルウェア感染でポートを閉じた？）

まとめ

NOTICEのメリット

1. 70以上の事業者、ipV4の半数以上を定期的に検査することで、様々な情報が取得でき、その中にはサイバー攻撃の前兆となりうる情報が含まれる。（特定機種の脆弱な機器が短期間に増減する）
2. 特に法人IoT機器については、継続して注意が必要
   注意喚起対象となる回線契約の連絡先と、IoT機器の関係者の関係が遠いことを踏まえた対応が必要だとわかってきた
   （法人の場合の注意喚起対象者の特定が適切かどうか。社会的にIoT機器のサイバー攻撃の危険度とNOTICEの関係を広報周知徹底を）
3. ルータ等の初期パスワードや、Sierの初期設定のパスワードが脆弱性につながることがわかってきており、一部機器メーカとの連携で、新しい機器に関しては危険な機種が確実に減っている
4. NICTERについては、ルータのファイアフォールの先からの感染通信も検出できることから、機種特定も含めて高度化できるとISPのサイバー対処能力向上につながるのかもしれない

NOTICEの改善

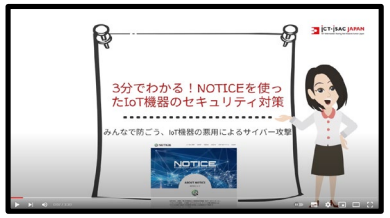
1. ISPにのみ依存した、繰り返し単調な注意喚起から、多様的な啓発活動の推進へ
   → 専門部隊による架電調査や実地調査など、実際の機器がどうなっているのかの調査がないと、サイバー攻撃の危険な実態を調査を保管。
2. ISPでの注意喚起での業務負荷軽減と、実効性を高める。NOTICEに参加していない、一定以上規模のISPの参加を義務化？
   → 脆弱性が見つかっても、NOTICEに参加していないISPには情報が渡せない
3. IoT機器のパスワードの再設定という作業は、利用者にとっては非常に難易度が高い。
   → 利用者の要望により、駆けつける体制で対策を行うことが重要
4. 手間がかかるNOTICE参加手続きを引き続きわかりやすく広報
   → 攻撃者がNOTICE検査をやらないISPに逃げ込み得にならない仕組みづくり

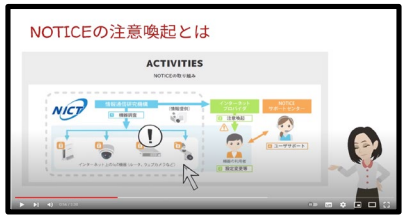
【参考】動画によるIoTセキュリティの活動紹介

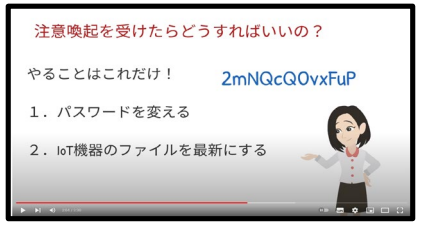
知りたい時に、HPや動画を使っていつでも啓発

ICT-ISACでは、YouTube等を活用して、利用者にも、NOTICE未参加のISPにも、情報発信を実施

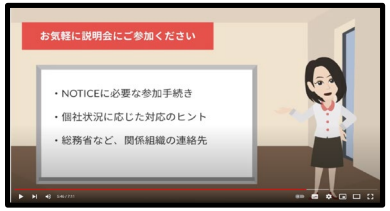
（一般向け）NOTICEを知ってください。　https://youtu.be/0ASZd9qvdGs







（ISP向け）NOTICEに参加してください。　https://youtu.be/0ASZd9qvdGs



法人IoT機器とセキュリティ　https://youtu.be/cY5dBYSlrdg

法人向けIoT機器の悪用によるサイバー攻撃防止ページ
https://www.ict-isac.jp/iot_security/