6-3　IoT 機器のセキュリティ確保への意識・課題・インセンティブを探る

6-3　Exploring Attitudes, Barriers, and Incentives Towards Securing IoT Devices: Insights from Internet Service Providers and Individuals

笠間 貴弘　藤田 彬　井上 大介
KASAMA Takahiro, FUJITA Akira, and INOUE Daisuke

IoT 機器のセキュリティ確保は、多様なステークホルダーが関係する複雑なオペレーションである。本稿では、特に主要なステークホルダーである ISP と IoT 機器利用者に対して、アンケート調査、ワークショップ、インタビュー調査を組み合わせた分析を行い、各ステークホルダーによる IoT 機器のセキュリティ確保に関する意識と課題認識を明らかにし、有効なインセンティブ設計について検討した結果を報告する。

Securing IoT devices is a complex operation involving a wide variety of stakeholders.This paper reports the results of an analysis combining questionnaire surveys, workshops, and interviews with ISPs and IoT device users to clarify each stakeholder's attitudes, barriers, and incentives for securing IoT devices.

1　はじめに

モノのインターネット（IoT：Internet of Things）の普及により、家庭や職場、街中、工場に至るまであらゆる場所において IoT 機器は我々の生活の一部として組み込まれている。我々が IoT 機器の利便性の恩恵を受ける一方で、IoT 機器は格好の攻撃対象として絶えずサイバー攻撃の脅威に晒されており、IoT 機器のセキュリティやプライバシー対策の遅れは機器利用者自身やネットワーク全体の被害に直結する。IoT 機器のセキュリティ確保においては IoT 機器ベンダ、機器利用者（ユーザ）、ISP（Internet Service Provider）といった多様なステークホルダーが存在する。IoT 機器ベンダはセキュアな機器を製造・供給する役割があり、脆弱性等の問題が生じた際にはセキュリティパッチの提供等の対処を実施する責任があるが、OEM（Original Equipment Manufacturing）のような複数の開発ベンダが関わるサプライチェーンの複雑さにより、適切な対処が困難な場合がある。ユーザは自らが保有する IoT 機器のセキュリティ確保において重要な役割を担っているが、一般的にサイバーセキュリティに関する十分な知識を持たないユーザが、セキュリティの重要性を正しく理解し適切な対処をすることは容易ではない。特に IoT 機器を踏み台にしたサイバー攻撃ではユーザへの直接的な被害が必ずしも発生しないため、IoT 機器のリスク状況をユーザが正確に認識できないという課題も存在する。また、IoT 機器を踏み台とした DDoS 攻撃（分散型サービス妨害攻撃）等は ISP のサービス提供にも影響を与えるため、ISP も IoT 機器のセキュリティ確保に対応する必要がある。ISP はサイバー攻撃発生時の事後的な対処だけではなくしばしば予防的な取組にも関わっており、NOTICE プロジェクト [1] ではパスワード設定不備の IoT 機器の所有者に対して注意喚起を実施する役割を担っている。効果的な IoT セキュリティ対策の実現においてはこれらステークホルダーの貢献と連携が必要不可欠であるものの、IoT 機器のセキュリティ確保の必要性に対する意識や課題認識、そして何より適切な行動を促すためのインセンティブ設計の在り方については明らかではなく、十分に理解されていない。そこで本稿では、日本国内の ISP 及びユーザへの調査を通じて彼らの意識、課題、そしてインセンティブの理解を試みた結果について概説する。

2　調査目的と手法

2.1　調査の目的

本調査では ISP とユーザへの調査を通じて、以下に示す 3 つの Research Questions を明らかにする。

- ISP 及びユーザは IoT 機器のセキュリティ確保に関してどのような意識を持っているか？
- ISP 及びユーザが IoT 機器のセキュリティ確保を

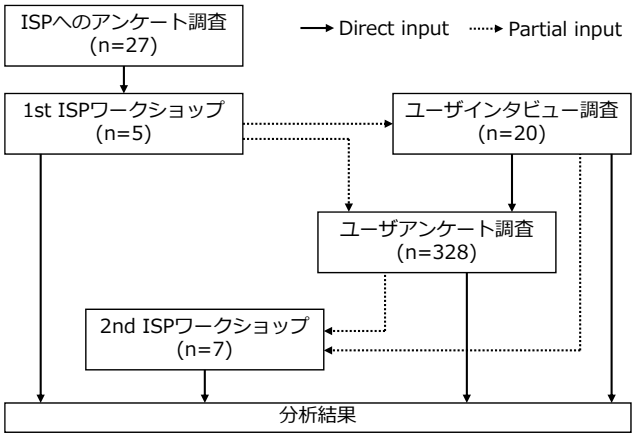

図 1　調査の全体像

実施する上での課題は何か？

- ISP 及びユーザが IoT 機器のセキュリティ確保を実施しようとするインセンティブは何か？

2.2　調査手法

本調査は図 1 に示す流れで実施した。ISP を対象とした調査としてアンケート調査と 2 回のワークショップを、ユーザを対象とした調査としてインタビュー調査とアンケート調査を実施し、ステークホルダー間の相互作用を反映するために各ステークホルダーの調査結果を基に調査内容を検討した。なお、ISP には自身の ISP ネットワーク内に存在するユーザが所有する IoT 機器のセキュリティ確保の視点での回答を依頼し、ユーザには自らの家庭で利用する IoT 機器のセキュリティ確保の視点での回答を依頼した。

2.2.1　ISP を対象とした調査

参加 ISP の募集：調査の参加 ISP は ICT-ISAC [2] の協力を受けて集めた。ICT-ISAC は ISP を含む通信事業者、放送事業者、ソフトウェアベンダー等が会員として参加する一般社団法人であり、サイバーセキュリティに関する情報収集や調査分析、会員間の情報共有や共同対処などを実施している。各 ISP へはインターネットのセキュリティ確保に対する ISP の役割や責任等を理解し新たなポリシーや戦略の策定に関わる立場の方の参加を依頼した。最終的にアンケート調査には 27 社、初回ワークショップには 5 社、2 回目のワークショップには 7 社（うち 4 社は初回ワークショップにも参加）からの協力が得られた。

ISP へのアンケート調査：ISP へのオンラインアンケートを実施した。アンケート項目は回答時間が 1 時間程度となるように設計し、IoT セキュリティへの意識や課題認識、インセンティブに関する考えを問う設問を用意した。具体的な設問については公表論文 [3] に記載してあるので参照されたい。アンケートは主に 3 つのパートに分かれており、パート 1 では ISP の規模等に関する基本的な情報を尋ね、パート 2 では IoT セキュリティに関する意識と課題について尋ねた。具体的には、ISP のネットワーク内に感染したもしくは脆弱な IoT 機器が存在することに対する懸念、ISP のネットワークが攻撃を受けるリスクの認識、IoT 機器のセキュリティ確保における ISP の役割と責任及び現在の貢献度等について尋ねている。また課題については、ISP が組織内で直面する課題に加え、法律や規制等の外的要因として直面する課題について尋ねた。パート 3 では ISP が IoT 機器のセキュリティ確保に取り組むためのインセンティブとなり得る要因について尋ねた。アンケート調査で収集した定量データについては調査結果の統計的有意性を確認するための各種統計検定を実施し、自由記述回答の定性データに関しては 2 名の研究者によって回答内容の分類を行った。

ISP とのワークショップ：ISP とのワークショップは 2 回開催し、COVID-19 の影響のためどちらもオンラインで開催した。初回のワークショップは ISP へのアンケート調査の後に実施され、アンケート調査結果の共有とそれに対する ISP からのフィードバックを得るために実施した。ここで得られた ISP からのフィードバックのうちユーザに関連した内容はユーザへのインタビュー調査やアンケート調査の設計に用いられた。2 回目のワークショップは一連のユーザに対する調査実施後に行われ、ユーザ調査から得られた知見を ISP に共有し、最終的なフィードバックを得るために実施した。

2.2.2　ユーザを対象とした調査

参加ユーザの募集：参加ユーザはモニター調査会社を通じて集め、日本国内に在住する 18 歳以上かつ家庭でスマートフォンや Wi-Fi ルータ等の IoT 機器を 1 つ以上利用している人を対象とした。最終的にインタビュー調査は 20 名、アンケート調査は 328 名のユーザを対象に実施した。

ユーザインタビュー：ユーザインタビューは IoT のセキュリティ確保に関するユーザの意識、課題、インセンティブについて予備的な理解を得るために実施した。ユーザインタビューはオンラインで実施され、各インタビュイーに対して約 1 時間の半構造化インタビューを実施した。インタビューは 3 つのパートから構成され、パート 1 では利用している IoT 機器とその用途、機器購入の意思決定に影響を与える要因等について尋ねた。パート 2 では IoT 機器のセキュリティ確保に関するユーザの懸念とその根拠、IoT 機器のセキュリ

ティ確保の優先度や IoT 機器が攻撃を受けるリスクの認識、IoT 機器のセキュリティ対処を行った経験などを尋ねた。パート 3 では、IoT 機器のセキュリティ確保のインセンティブとして有効だと考える要因について尋ねた。これらのインタビュー内容は全て録音・書き起こしを行った上で個人を特定できない ID を割当て、分析を行った。分析では、書き起こしデータを基に 2 名の研究者が独立して反復的主題分析を実施しコードを作成した。作成したコードについて議論し、再定義とコーディングプロセスを繰り返すことで最終的なコードブックを作成し回答を分類した。最終的なコードブックについては公表論文 [3] で記載しているためそちらを参照されたい。

ユーザへのアンケート調査：ユーザへのアンケート調査はオンラインで実施され約 20 分程度の回答時間を想定した構成となっている。設問のテーマとトピックはユーザインタビューと同様の構成となっており、インタビュー調査で得られた知見を基に回答の選択肢を作成した。アンケート調査で収集した定量データは ISP へのアンケート調査と同様に各種統計検定を行っている。

3　ISP を対象とした調査結果

ISP を対象とした調査結果を示す。今回は、各 ISP について契約顧客数が 1 万未満の ISP を小規模（Small）、1 万以上 100 万未満の ISP を中規模（Medium）、100 万以上の ISP を大規模（Large）に分類する。

3.1　IoT 機器を悪用したサイバー攻撃への ISP の懸念点

まず、IoT 機器を悪用したサイバー攻撃が発生した場合に、ISP が最も懸念していることの調査結果を表 1 に示す。全体として ISP が最も懸念していることは「顧客へのサービス停止」であり、その次に「発生した攻撃に対する社会的責任」、そして「評判の低下」という順番であった。これらの懸念事項の優先度は ISP の規模によって若干異なっており、大規模や中規模 ISP ではサービス停止が最も大きな懸念である一方、小規模 ISP では社会的責任を最も大きな懸念点として挙げていた。また小規模 ISP では金銭的コストが比較的上位に位置しており、小規模な ISP では財務リソースに制約があることを示唆している。

「顧客へのサービス停止」への懸念が最も大きいという結果は、サービス停止が発生することで評判の低下など他の問題が連鎖的に発生することからも理にかなっている。一方で、社会的責任への懸念がその他の金銭的コストや顧客の喪失への懸念よりも順位が高いという結果は、社会の調和を重要視する日本文化の特徴が反映されている可能性がある。この点に関して、初回 ISP ワークショップにおける小規模 ISP からのフィードバックとして、ユーザには脆弱な IoT 機器のリスクに関する情報が不足しているため、ISP はユーザ以上に IoT セキュリティに対して社会的責任を果たす必要があると述べていた。

表 1　IoT 機器を悪用したサイバー攻撃への ISP の懸念点

Concern	Overall	Large ISP	Medium ISP	Small ISP
Service disruption to customers	**1st**	**1st**	**1st**	2nd
Social responsibilities†	2nd	3rd	2nd	**1st**
Reputation damage	3rd	2nd	4th	4th
Loss of customer and market share	4th	4th	3rd	5th
Incurred financial costs	5th	5th	6th	3rd
Warning from relevant authorities	6th	6th	5th	6th
n	26‡	8	14‡	4
χ^2 (5)	45.01**	7.86	34.29**	11.00*

† The need to take responsibilities to society as a result of IoT attacks occurred in their network, ‡ Excluded 1 medium ISP whose ranking consensus can not be identified, *, ** denotes $p<0.05$ and $p<0.001$.

3.2　IoT 機器のセキュリティ確保の優先順位・責任・貢献

IoT 機器のセキュリティ確保に関する ISP の優先度を調査した結果、大多数の ISP は優先順位を「中」（実施することが望ましい課題）と考えていた。ただし、大規模及び中規模 ISP では「中」の回答が多かったが、小規模 ISP では「低」（余裕があれば行うべき課題）という回答が多かった。小規模 ISP において優先度が低いと考えられている要因として、小規模 ISP では IoT のセキュリティ確保のための投資について意思決定を行うための十分な知識や情報が不足していることが挙げられる。具体的なセキュリティ対策実施に関する認識を明らかにするために、各対策に対する ISP の責任と貢献度を調査した結果を図 2 に示す。図 2 を見ると、大半の ISP が予防（Prevention）、検知（Detection）、通知（Notification）、対処（Remediation）、復旧（Recovery）の 5 つの IoT 機器のセキュリティ確保に関する取組すべてにおいて、ISP が一定の責任を持つことに同意していることがわかる。各 ISP によるこれらの活動への自らの貢献度の認識については責任に対する回答と基本的に一致しており、全体としては多くの ISP が予防と復旧活動を除いて自らは一定以上の貢献をしていると考えていることが明らかとなった。

3.3　IoT 機器のセキュリティ確保への ISP の課題

内的な課題：表 2 に ISP が考える IoT 機器のセキュリティ確保への課題のうち内的要因に該当したものを示

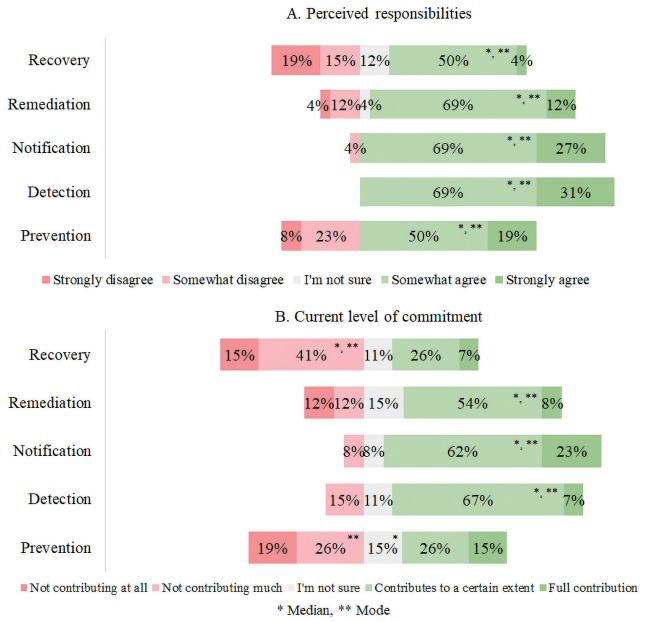

図 2　IoT 機器のセキュリティ確保への ISP の責任と貢献の認識

表 2　IoT 機器のセキュリティ確保への ISP の課題（内的要因）

No. of ISPs	Overall (27)		Large (8)		Medium (15)		Small (4)	
Barriers	*n*	%	*n*	%	*n*	%	*n*	%
Human resource	17	65	3	38	11	73	3	75
Executive buy-in	12	44	5	63	6	40	1	25
Financial	10	37	5	63	5	33	0	0
Technology	10	37	0	0	7	47	3	75
Others†	6	22	4	50	1	7	1	25
Not sure	1	4	0	0	1	7	0	0
$\chi^2(5)$	24.13**		14.66*		21.50**		10.50	

† Specified by ISPs as shortage of staff (internal but already part of the HR obstacle), law and regulation constraint (external), and the perception that it should be the responsibilities of device makers and users to keep IoT secured (external), *, ** $p<0.05$, and $p<0.001$, respectively.

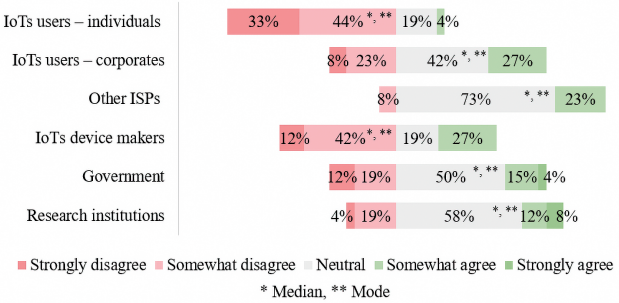

図 3　ISP 視点から見た各ステークホルダーの貢献度

す。全体として人的リソースの不足を課題として挙げた ISP が最も多く全体の 65 % に上った。また半数程度（44 %）の ISP は、IoT 機器のセキュリティ確保の必要性を幹部に納得してもらうことに課題を感じていた。内的要因による課題認識は ISP の規模によって有意に異なっており、大規模 ISP では財政的な課題を多く挙げる傾向にあるが、中規模や小規模 ISP では人的リソースの不足や技術的な課題を挙げる傾向にあった。実際に初回の ISP ワークショップにおけるフィードバックにおいて、ある小規模 ISP は財政的な課題よりも必要なコストを判断するための十分な知識や情報が無いことを課題点として挙げていた。また別の大規模 ISP からのフィードバックとして、IoT 機器のセキュリティ確保の重要性はスパムメール対策といったその他の取組と比べて意義や効果を幹部に説明することが難しいという意見があった。

外的な課題：他のステークホルダーによる IoT セキュリティ確保への貢献度について、ISP の認識を調査した結果を図 3 に示す。結果では ISP の規模による有意差は見られず、大半の ISP は IoT 機器の企業ユーザ、他の ISP、政府、研究機関の貢献度に関して中立的な認識を持っている一方で、IoT 機器の個人ユーザや IoT 機器ベンダについては十分な貢献をしていないという認識を持っていた。ISP ワークショップにおけるフィードバックでは、ISP 各社は個人ユーザが IoT 機器を適切に設定・管理できていないことで IoT 機器のセキュリティ上の問題が発生していると考えており、個人ユーザの必要な知識・スキルの不足が IoT 機器のセキュリティ確保が進まない大きな要因の一つであると考えていた。また、2019 年に技適にセキュリティ基準が追加される以前にベンダが販売しいまだ多数利用されている IoT 機器ではセキュリティ対策が不十分であり、それらの機器を製造・販売した機器ベンダに対して一定の責任があると半数程度の ISP が考えていた。その他の外的要因として、電気通信事業法の「通信の秘密」がセキュリティ確保の障壁となっていると考える ISP が存在した。彼らは「通信の秘密」によって ISP が原則として通常ユーザの通信の監視や阻止などの行為を行えないことが、ISP が取り得る手段の制限となっていると主張した。

ユーザへのセキュリティ通知の困難さ：ISP ワークショップの議論において、ISP が問題のある IoT 機器を発見もしくは外部から情報提供を受けた際に、ユーザへのセキュリティ通知を届けることの困難さがセキュリティ確保の課題点として挙げられた。この困難さはいくつかの要因によってもたらされており、一つは動的 IP アドレスの影響が挙げられる。特定の環境や状況では、通知を行おうとした際に ISP が動的 IP アドレスをユーザに割り当てた際のログが既に破棄されており、結果としてユーザを特定できないケースが存在していた。さらにユーザを特定できた場合には多くの ISP では ISP のキャリアメール宛にセキュリティ通知を行うが、近年のユーザは SNS 等の多様なコミュニ

表 3　ISP に対して有効なインセンティブ

Incentives	Overall		Large		Medium		Small	
	n	%	*n*	%	*n*	%	*n*	%
Internal								
Tech to detect infected IoT	13	50	4	50	7	50	2	50
Executive & staff buy-in	9	33	4	50	4	27	1	25
Offer IoT security service	3	12	2	25	1	7	0	0
Transfer cost to customer	0	0	0	0	0	0	0	0
External								
(M) Device makers secure IoT	19	70	7	88	8	57	4	100
(G) Amend law to restrict traffic	15	58	5	63	9	60	1	25
(G) Public recognition for ISPs	14	52	4	50	7	50	3	75
(G) Government subsidy	13	50	4	50	8	53	1	25
(U) Individuals keep IoT secure	9	33	1	13	6	40	2	50
(U) Corporate keep IoT secure	9	33	1	13	6	43	2	50
(G) Amend law to monitor traffic	8	31	1	13	7	50	0	0
(G) Public-private sector partnership	6	22	3	38	2	13	1	25
(G) Make net neutrality optional	3	11	1	13	1	7	1	25
(R) Input from research community	3	12	0	0	2	13	1	25
(I) Equal responsibilities for ISPs	1	4	0	0	1	7	0	0
(I) ISPs performance dashboard	1	4	0	0	1	7	0	0
Other	1	4	1	13	0	0	0	0
Not sure	0	0	0	0	0	0	0	0
$\chi^2(17)$	115.70**		48.76**		66.28**		29.53*	

(M) = device maker, (U) = end users, (G) = government, (I) = ISPs community, (R) = research community, *, ** $p<0.05$, and $p<0.001$, respectively.

ケーションツールの普及によってメールの利用が限定的になっており、セキュリティ通知のメールが正しくユーザに読まれていない可能性が指摘された。

3.4　ISP に対して有効なインセンティブ

IoT 機器のセキュリティ確保に ISP が取り組むうえで有効なインセンティブに関する回答結果を表 3 に示す。

内的なインセンティブ：ISP がインセンティブとなり得る内的要因して最も多く挙げたのは感染済み IoT 機器を検知する技術の習得であり、次点として幹部等の賛同であった。

これは表 2 で示した課題の順位において、技術不足よりも幹部の納得が上位に位置していたこととは対照的な結果となっている。一方で、サービス化による収益化を有効なインセンティブとして選択した ISP は数社に留まり、セキュリティ確保のコストをユーザに負担させようと考える ISP はなかった。この点に関してワークショップの議論では、IoT 機器の種類が多様であるためそれらの機器を網羅できるセキュリティサービスを設計することが難しいというコメントが得られた。また、そのようなセキュリティサービスとして ISP が提供できることとユーザが期待するサービスとの間にギャップが生じることで、ユーザからの過剰な期待を受けることを懸念する声も聞かれた。

外的なインセンティブ：ISP の大部分（70 %）はセキュリティ確保に取り組む前提として IoT 機器ベンダがセキュアな機器を製造することを望んでおり、これは図 3 で示した ISP が IoT 機器ベンダが十分な貢献を果たしていないと考えている状況と合致する。その一方で、ISP は IoT 機器の個人ユーザが IoT 機器のセキュリティ確保に対して十分な貢献を行っていないと考えているにも関わらず、個人ユーザによるセキュリティ確保を望む ISP は少なかった（33 %）。政府からのインセンティブとしては、顧客のトラフィックの制限を可能にするための法整備が最も多く回答された（58 %）。また、52 % の ISP は ISP の貢献に対する正当な社会的評価がインセンティブになり得ると回答し、50 % の ISP は政府からの補助金が有効だと回答した。

4　ユーザを対象とした調査結果

4.1　IoT 機器のセキュリティに関するユーザの懸念

全体として、ユーザの多く（約 70 %）は IoT 機器の種類に依らずセキュリティについて特に懸念を抱いていないと回答しており、年齢や性別による差異も見られなかった。IoT 機器のセキュリティに関して懸念を抱いていた一部のユーザでは、金銭的損失（IoT 機器に紐づけられたクレジットカードの情報漏えいなど）が最も大きな懸念点として挙げられ、次点として Web カメラ等からのデータ漏えいによるプライバシーの侵害が挙げられた。

4.2　自身の IoT 機器が侵害されている可能性への認識

ユーザの多数は自身の IoT 機器が侵害されている可能性について「わからない」と答えた。可能性が低いと回答したユーザの半数程度がその理由として「金銭的なサービス（クレジットカードなど）で不審な支払いなどが発生していない」を選んでおり、ユーザが IoT 機器のリスク状況を認識する手段として金銭的な被害の有無のみに頼っている状況が明らかになった。このような誤ったリスク判断を行うメンタルモデルはユーザインタビューでも観測されており、20 名中 9 名のユーザは IoT 機器のセキュリティ状況の判断の根拠としてパソコンのアンチウイルスソフトの結果を用いていた。つまり、パソコンに導入されているアンチウイルスソフトが何も脅威を検出していないことから、同じ環境に接続されている IoT 機器も安全だと考えていることが明らかとなった。このようなパソコン上のアンチウイルスソフトによる対策が IoT 機器にも適用されているという誤解は、オランダの ISP ユーザを対象とした研究報告 [4] でも同様の傾向が指摘されていた。

4.3　IoT セキュリティ対策実施への課題

自身の IoT 機器が侵害されている可能性について、「わからない」「もしかしたらあるかも」「おそらくあると思う」「確実にあると思う」を回答した参加者（169 名）に、当該 IoT 機器の修復を試みた経験を尋ねた結果、125 名（74 %）のユーザは何も行っていなかった。その理由について、56 名のユーザは「何から行えば良いのかわからない」と答え、36 名のユーザは「新しい機器に買い替えた方が簡単」と答えた。修復を試みたユーザのうち何も課題はなかったと回答した人は 21 % と少数であり、大半のユーザは何らかの困難に直面していた。特に多くのユーザにとって状況を理解し対策を実施するための技術的な知識やスキルが多すぎることが課題として挙げられ、また ISP や機器ベンダからの十分なサポートが無いと感じるユーザも多く存在した。

4.4　ユーザに対して有効なインセンティブ

IoT 機器のセキュリティ意識の向上やセキュリティ対策実施のインセンティブとなり得るものとして、最も多い 53 % のユーザが「IoT 機器に対する実際の攻撃事例に関するニュースや記事を見る」と回答し、その次に「自身の IoT 機器が攻撃を受ける経験」と答えたユーザが 47 %、「IoT 機器のリスクを啓蒙する広告を見る」と答えたユーザが 37 % であった。これらの回答結果から、ユーザが IoT 機器のセキュリティへ関心を持つきっかけとしてメディアからの影響が大きいことが明らかとなった。インタビュー調査においても、IoT 機器のセキュリティ・プライバシーを懸念するユーザの多くはニュースで攻撃事例を目にした影響で意識するようになったと答えていた。

4.5　ISP に対してユーザが期待する取組

IoT 機器のセキュリティ確保において、ユーザが ISP に期待する取組を表 4 に示す。最も多かった回答は「IoT 機器からの不審な通信を監視しユーザへ通知すること」で 55 % のユーザが回答した。更に 54 % のユーザはユーザへの通知無しに IoT 機器からの不審な通信を自動的にブロックすることを期待していた。すなわち、半数以上のユーザは ISP による積極的な介入を希望していたが、インタビュー調査においてあるユーザは「不審な通信をブロックしても良いか、と訊かれたら技術的なことに詳しくないので、危険ならばブロックしてください、と答える」と回答しており、ユーザにとって十分な知識がないことが ISP による積極的な介入を期待する要因の一つとなっていることが明らかになった。一方で、ISP 視点から見るとこのような積極的な介入は通信の秘密の侵害と見なされる恐れがあるため、ユーザの通信を自動でブロックするといった対策を ISP 判断で実施することは困難である。

表 4　ISP に対してユーザが期待する取組

Incentive	*n*	%
1. Monitor suspicious com. from IoT devices and *notify* customers.	180	55
2. Monitor suspicious com. from IoT devices and *automatically block* it.	177	54
3. Notify users about important software/firmware router updates.	140	43
4. Set appropriate security settings on devices before shipping.	119	36
5. Have a call center where users can easily consult about security.	114	35
6. Be transparent about how ISPs protect users' communication and personal data.	114	35
7. Provide online service to help users repair compromised devices.	103	32
8. Provide home visit service to repair compromised devices.	72	22
9. Educate users about the potential risks of using IoT.	71	22

328 participants total. The observed proportions among the incentives were statistically significant ($Jx^2 = 344.21, df = 9, p < 0.001$).

5　議論

5.1　IoT セキュリティ確保の優先度

第一に、今回の調査によって ISP 及びユーザは IoT 機器のセキュリティ確保に対して一定の懸念を抱いているにも関わらず、IoT 機器のセキュリティ確保の優先度を高いと考えていないという実態が明らかとなっており、セキュリティはあくまでも副次的な課題であると言える。すなわち、ISP 及び個人に対する適切なインセンティブの導入無しには、IoT 機器のセキュリティ確保は達成できないことを示している。

5.2　ステークホルダー間の連携の重要性

ISP 及びユーザへの調査を通じて、IoT エコシステムのセキュリティ確保の取組の複雑さを確認できた。特に各ステークホルダーは基本的にセキュリティ確保の責任を他のステークホルダーに求める傾向がある。例えば ISP は IoT 機器ベンダや個人ユーザが十分な貢献を果たしていないことが IoT 機器のセキュリティ問題の要因であると考えており、一方ユーザは ISP や機器ベンダによるセキュリティ確保の取組の強化を望んでいる。これらのステークホルダーが絡み合う状況では単独の取組のみで問題を解決することは困難であり、ステークホルダー間の連携が不可欠である。NOTICE の取組はその一つのアプローチであり、完璧ではないものの複数のステークホルダーを巻き込むことで協力的な取組を実現している。

5.3　ISP の貢献と更なるインセンティブ

ISP は IoT 機器のセキュリティ確保における様々な取組を行っている一方で、ユーザは ISP に更なる貢献を求めている。しかしながら、ISP が直面している内外の課題を考慮すると、ISP に更なる努力を求めることは困難である。特に ISP はセキュリティ確保の取組において金銭的なインセンティブがほとんど得られていないという課題がある。この点に関して、ユーザ調

査において一部のユーザは ISP によるセキュリティサービスにいくらかの金銭的な支払いをすることに同意したが、ISP との議論においてユーザが支払っても良いと考える金額は ISP が実際にサービス提供を行うためには十分ではないと判断された。これらの結果から、IoT 機器のセキュリティ確保においては政府から ISP に対する補助金などの金銭的な補助を提供することができれば有効なインセンティブとなり得ると考えられる。また、ISP は ISP 自身の貢献を世間に認められることを望んでいた。このような社会的な評価はインセンティブとして珍しいものではないが、今回の調査では 2 社中 1 社の割合の ISP が当該インセンティブを望んでいたことは特徴的であり、それだけ IoT 機器のセキュリティ確保の取組について組織内で賛同を得ることが容易ではないことを示している。この点に関しても政府などから取組に対する公的評価を与えることがインセンティブとなり得るが、具体的な評価方法については更なる議論が必要である。

6 おわりに

本稿では IoT 機器のセキュリティ確保に関係するステークホルダーのうち ISP 及び個人ユーザに焦点を当て、各種調査を通じて彼らの IoT 機器のセキュリティ意識や課題、そしてインセンティブを調査した。結果として、ISP と個人は IoT 機器のセキュリティについて一定の懸念を持っているものの、IoT 機器のセキュリティ確保を必ずしも優先しておらず、他の主要なステークホルダーからの支援がいまだ必要であることを本研究は示している。本稿では割愛した調査結果については公表論文 [3][5] を参照いただきたい。IoT エコシステムのセキュリティ確保に向けた取り組みは複雑であり、他のステークホルダーの認識や課題、効果的な介入方法など、まだ多くの疑問や課題が残っている。我々は引き続きこれらの課題の解決に向けた調査・研究を行っていく。

【参考文献】

1　“NOTICE”. https://notice.go.jp/
2　“一般社団法人 ICT-ISAC”, https://www.ict-isac.jp/
3　N. Sombatruang, T. Caulfield, I. Backer, A. Fujita, T. Kasama, K. Nakao, and D. Inoue, “Internet Service Providers’ and Individuals’ Attitudes, Barriers, and Incentives to Secure IoT,” https://arxiv.org/abs/2210.02137
4　O. Çetin, C. Ganán, L. Altena, T. Kasama, D. Inoue, K. Tamiya, Y. Tie, K. Yoshioka, and M. vanEeten, “Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai,” Proceedings of the Network and Distributed Systems Security Symposium 2019, pp.1–15, 2019.
5　N. Sombatruang, T. Caulfield, I. Becker, A. Fujita, T. Kasama, K. Nakao, and D. Inoue, “Internet Service Providers’ and Individuals’ Attitudes, Barriers, and Incentives to Secure IoT,” 32nd USENIX Security Symposium (USENIX Security 23), pp.1541–1558, 2023.

笠間 貴弘（かさま たかひろ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
室長
博士（工学）
サイバーセキュリティ
【受賞歴】
2022 年　電子情報通信学会 ICSS 2022 年度研究賞
2019 年　NDSS2019 Distinguished Paper Award
2011 年　情報処理学会 2011 年度山下記念研究賞

藤田 彬（ふじた あきら）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究員
博士（情報学）
ユーザブルセキュリティ、Web セキュリティ、IoT セキュリティ
【受賞歴】
2021 年　電子情報通信学会 第 16 回通信ソサイエティ論文賞（優秀論文賞）
2012 年　博報堂教育財団 第六回児童教育実践についての研究助成事業 優秀賞

井上 大介（いのうえ だいすけ）
サイバーセキュリティ研究所
研究所長
博士（工学）
サイバーセキュリティ、情報セキュリティ、セキュリティ可視化
【受賞歴】
2018 年　前島密賞
2016 年　産学官連携功労者表彰 総務大臣賞
2009 年　科学技術分野の文部科学大臣表彰（科学技術賞）