Vol.2020-DPS-182 No.36
Vol.2020-CSEC-88 No.36
2020/3/13

テレビ視聴ロボット用外部クラウドインターフェースにおけるセキュリティ対策

村﨑康博[†1]　星祐太[†1]　萩尾勇太[†1]　上村真利奈[†1]　金子豊[†1]　山本正男[†1]

概要：人と一緒にテレビを視聴するコミュニケーションロボットを開発するにあたり，ロボットシステムの企画・設計段階からセキュリティ機能を組み込むことを検討している．こうした中，ロボット利用者向けにセキュリティ意識調査をしたところ，特に個人情報やプライバシー保護を求めていることが分かった．本稿では，視聴実験を進めていくに必要と考える，セキュリティ対策の取組みについて，主に開発時でのセキュリティ要件をまとめ，その一部を実装したことについて述べる．

キーワード：コミュニケーションロボット，テレビ視聴，情報セキュリティ，クラウドサービス，IoT，AI，セキュリティガイドライン

Security Measures in External Cloud Interface for Companion Robots Watching TV with People

YASUHIRO MURASAKI[†1]　YUTA HOSHI[†1]　YUTA HAGIO[†1]
MARINA KAMIMURA[†1]　YUTAKA KANEKO[†1]　MASAO YAMAMOTO[†1]

Abstract: In developing a companion robot watching TV with people, we are considering incorporating security functions from the planning and design of a robot system. Under these circumstances, we conducted a security awareness survey for robot users, and found that they were particularly seeking protection of personal information and privacy. This paper describes security measures that we consider necessary for conducting viewing experiments, mainly summarizes security requirements at the time of development, and describes the implementation.

Keywords: communication robot, social robot, TV viewing, information security, cloud service, IoT(Internet of Things), AI(Artificial Intelligence), security guidelines

1. はじめに

少子高齢化や単独世帯の増加，スマートフォンの普及等に伴い，日本人のライフスタイルが変化してきている．テレビ視聴の傾向も例外ではない．NHK 放送文化研究所の調査では，若年層を中心にテレビを見る時間が減ってきており，いわゆる「テレビ離れ」が進んでいる[1]．これを受けて NHK 放送技術研究所（以下，技研）では公共メディアとしてより多くの人に豊かなテレビ番組を楽しんで頂くための研究開発を進めている．

本稿の「人と一緒にテレビを視聴するコミュニケーションロボット（以下，テレビ視聴ロボット）」はテレビ番組の映像音声や字幕情報から番組内容を認識し，認識結果から発話文を生成して視聴者と対話することを目指している[2]．これによって普段一人で番組視聴している人々に家族や友人らと一緒に見るような環境を提供し，かつての一家団らんでテレビを楽しんでもらえるものと期待する．

本稿では，今後安全安心なテレビ視聴ロボットの開発・実験を進めていくに必要なセキュリティ対策について，主に開発時のセキュリティ要件をまとめた．さらにセキュリティ要件に従って，その一部を 2 章で紹介する外部クラウドインターフェースに実装した取り組みについて述べる．

2. 外部クラウドインターフェース

テレビ視聴ロボットでは，映像音声認識処理の一部[a]に外部クラウドベンダーが提供する商用サービス認識 API を利用している．そのため当該 API を利用するにあたり，ロボットと外部クラウドとを接続するための外部クラウドインターフェース（以下，クラウド IF）を開発してきた．

図 1 はクラウド IF の概要図である．クラウド IF の仕組みは次の通りである．まずテレビ視聴ロボットが自身のカメラ・マイクで収集した映像音声をクラウド IF に送信する．クラウド IF では，映像は一定時間間隔にサ

†1 日本放送協会放送技術研究所
NHK STRL

a) テレビ視聴ロボットには商用クラウドによる映像音声認識処理のほか，オンプレミスで処理する機能も実装しており，複合的な処理機能を有する．

Vol.2020-DPS-182 No.36
Vol.2020-CSEC-88 No.36
2020/3/13

ンプリングした画像を，音声はストリーミング方式で連続的に，外部クラウドへ送信する．外部クラウドでは，送られた映像音声をそれぞれ画像認識用・音声認識用の AP によって認識処理を行い，それぞれで得られたキーワードをクラウド IF に返信する．クラウド IF では受信したキーワードを指定時間間隔で集計し，テレビ視聴ロボット側が実装している発話生成部と動作生成部に送信する．

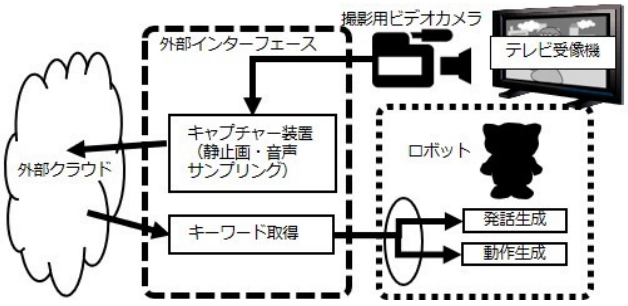

図 1　外部クラウドインターフェース概要図

次に認識処理過程の流れを図 2 に示す．認識処理は次の Step1 から Step5 に従って実行される．

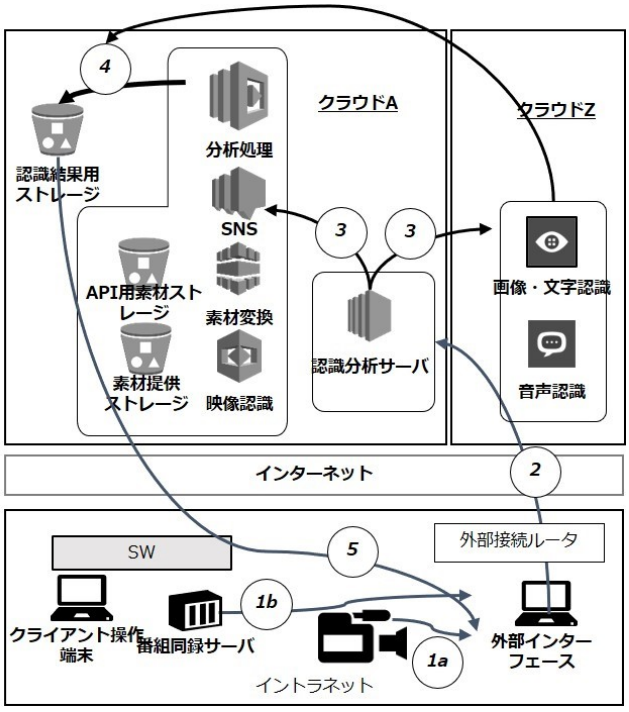

図 2　クラウド IF・外部クラウドでの
認識処理フローの概要

Step1a : 民生用カメラからの映像信号をクラウド IF に送信

Step1b : (もしくは) 番組同録サーバから映像コンテンツをクラウド IF に送信

Step2. : クラウド IF からサンプリングされた画像および音声データを外部クラウドの認識分析サーバに送信

Step3 : 外部クラウドの画像・音声認識 API を利用し画像・音声解析を実施

Step4 : 画像・音声データそれぞれの解析結果を外部クラウド上の認識結果用ストレージに格納

Step5 : 外部クラウド上の認識結果用ストレージから解析結果をクラウド IF に送信

なお現状のクラウド IF は，テレビ視聴ロボットと外部クラウドとの中間に位置するオンプレミス装置（PC）で実装している[b].

3. クラウド IF でのセキュリティ対策へ課題

テレビ視聴ロボットはこれまで技研公開やデモ展示を通じて設計方針を紹介してきた[3]. また実際に視聴実験に向けてシステム設計やロボットの試作[4], 被験者との対話に関わる研究成果[5]を発表してきた．

視聴実験用に試作したテレビ視聴ロボットは，2 章で紹介したクラウド IF 以外，実験室内のオンプレミス装置で構築している．またテレビ視聴ロボットは，現在実験室内での視聴実験を実施している．そのため，仮に情報セキュリティインシデントが発生したとしても，回線を即座に遮断するなど迅速な対応が可能である[c].

我々は実験室内での視聴実験を経て，さらに一般個人宅や外部施設など実験室外での長期間の視聴実験を検討している．これはテレビ視聴ロボットを普段の生活と変わらない状態で触れてもらうことで，使い勝手の検証や必要となる機能，解決すべき課題の確認などを正確に把握することを目的としている．

このような実験室外での視聴実験を実現するために，テレビ視聴ロボットと軽量な可搬型端末のみを持ち込む程度で実験を行えるシステム構成を検討している．具体的には現在のテレビ視聴ロボットを稼働させている複数のオンプレミス装置（PC 端末・サーバと周辺機材）のほぼ全てを外部クラウドで再構築する．これにより，受け入れ施設・家庭への物理的設置にかかる負担を軽減することができる．さらに外部クラウドにアクセスすることで技研からリモート監視・操作が可能となり，実験管理者の負荷も抑えることが期待できる．

しかしながら，テレビ視聴ロボットが施設・家庭内で撮影・収録する映像音声を，クラウド内で画像音声認識処理を実施するためには，個人情報・プライバシーの保護への対策が必要となる．これは実験室内という閉じた領域でのデータのやりとりと異なり，外部とネットワーク接続していることによる，第三者からの侵入・攻撃の

b) 今後所外実験に向けてシステムの携帯化を図る事から，外部クラウドの 1 エレメントとするか，それともロボットに内蔵するか，あるいはロボットに付随するホームゲートウェイのようなものにするか，様々な態様が考えられる．

c) この場合，外部クラウドによる映像音声認識処理ができなくなるが，オンプレミスのみ使用することで認識処理を継続することは可能である．

リスクが増えるためである．

3.1 ソーシャルロボットへのセキュリティ対策の先行研究

そこで個人情報・プライバシーの保護を中心としたセキュリティ対策を検討するにあたり，ソーシャルロボット[d]へのセキュリティ対策に関する先行研究を調べた．本稿ではその事例として以下の 3 つを取り上げる．

3.1.1 Kaspersky and Ghent University (Belgium)

情報セキュリティソリューションの開発・販売企業であるカスペルスキー（Kaspersky）とベルギーのゲント大学（Ghent University）は，ソーシャルロボットが人間を説得したり操ったりできる可能性に関する検証を実施した．具体的には立ち入り禁止エリアへのロボットの侵入，パスワードリセットに使われる個人情報の聞き出しなどの成功の可否を分析している．

その結果，ロボットが関係者以外立ち入り禁止区域に侵入する目的で当該関係者を巧みに説得し，随行することに成功したり，本人のプライバシーに関わる情報を対話しながら入手できたりすることが明らかになったと報告している[6].

実験の結果を受けて，この調査ではロボットが人間らしくなるにつれ，人への説得力や信ぴょう性が高まることが，セキュリティ上のリスクを高めているとしている．一方，人はこのようなリスクを深く考えず，ロボットは親切で信頼できると考える傾向にあり，これが悪意ある攻撃を受ける可能性があると説明している．したがって，起こりうるリスクや脆弱性を理解し、それらに対応することが重要としている．

3.1.2 Oklahoma State University (US), and Guizhou University (China).

米国オクラホマ州立大学（Oklahoma State University）と中国貴州大学（Guizhou University）らは，ソーシャルロボットが家庭で利用されると，装備されているカメラで入浴中などの生活シーンを撮影されることで，プライバシーに関する懸念が生じると指摘した．そこで日常生活で裸の映像を検出するために，畳み込みニューラルネットワーク（CNN）に基づく方法を提案した[7]．具体的にはロボットの制御には ROS を利用し，ディープラーニングフレームワーク TensorFlow を用いて裸の映像レベルを検出する CNN モデルを構築した，としている．

このシステムにより，人の様々なポーズを学習し，ロボットが裸等プライバシーに敏感な状況を検出した場合には向きを変え，人にその所作を伝えるように工夫した．ロボットが人に背を向けることで，人はロボットに監視されていないことが確認できる．この研究ではさらにこのロボットの所作について被験者に調査したところ，好意的に受け入れる結果が得られたとしている．すなわちこの先行研究から，ロボットが利用者のプライバシー保護のために，直接見るのを避ける動作などの機能が求められていると考える．

3.1.3 中南経済法学院 (China) **ほか**, King Saud University(Saudi Arabia), Menoufia University(Egypt)

中南経済法学院らの研究では，個人に特化するサービスの需要が増す中で，個々の感情や精神をケアするためのソーシャルロボット（感情認識ロボット）を開発する上でのセキュリティ対策を紹介している[8].

感情認識ロボットは装着された様々なセンサーによって，利用者の感情データ，ソーシャルデータ，およびその他のデータを収集する．このデータを，深層学習をはじめとする機械学習によって分析し，パーソナライズされた感情ケアを利用者に提供している．

しかし感情認識ロボットは利用者とのやり取りによって多くの個人データを保存する．そのためデータのアクセス制御はプライバシー保護にとって重要であるとしている．

そこでこの研究では，感情認識ロボットに対して考慮した ID 認証およびアクセス制御ポリシーを提案し，そのアーキテクチャを分析することでセキュリティの問題を解決するとしている．具体的にはロボットで使用するエッジクラウドでの協調認証処理をサポートするために，小さな演算処理で個人情報・プライバシー保護対策できるよう設計した．その上でセキュリティ要件を満たすエッジクラウドノードと，一人の利用者が複数のデバイス使用をサポートするユニバーサルアクセス制御スキームを実現している．この装置を試行実験で実際に評価したところ，複数要素 ID 認証のパフォーマンスが従来方法より優れていると結論づけている．

3.1.4 先行研究とテレビ視聴ロボットでのセキュリティ対策における関連性

以上，個人情報・プライバシー保護に関するセキュリティ対策への先行研究を紹介した．テレビ視聴ロボットにおいても，利用者（被験者）との対話や撮影した映像音声から個人情報やプライバシーに関わる情報を入手しやすい点，またこれらの情報を保護するために，外部クラウド側で処理するデータとオンプレミス側で処理するデータとを切り分ける必要がある点，さらには外部からの侵入・攻撃を検知・防止する対策が必要である点などに関連性があると考える．

なお先行研究を 3.3 節で後述する「IoT セキュリティ対策」と「AI 対策」で分けると，AI は全ての先行研究に，IoT については 3.1.3 項に関わると考える[e].

d) 本稿では，テレビ視聴ロボットが人と一緒にテレビを見て楽しむコミュニケーションロボット・ソーシャルロボットとして分類する．

e) 4 章で述べるとおり本稿では IoT セキュリティ対策を先行して実装を試みている．

Vol.2020-DPS-182 No.36
Vol.2020-CSEC-88 No.36
2020/3/13

3.2 ロボット利用者のセキュリティへの意識調査

人はコミュニケーションロボットと対話することで親和性を持つことを 3.1.1 項で紹介したが，さらに日本人は欧米人と比べて一般にロボットへの親和性があり，家族やペットとして扱う傾向にあるといわれている[9][10]．そのため日本のロボット利用者はコミュニケーションロボットに撮影・録音されているにも関わらず，気兼ねなく近づいて話しかけたりするものと考える．

したがってロボット利用者がコミュニケーションロボットと一緒に暮らすにあたり，個人情報やプライバシーが侵害される可能性があることを，実際に危惧しているのかどうか疑問に思った．それはロボット利用者が普段からコミュニケーションロボットを家族やペットのように身近に利用していると仮定すれば，ロボットに対する警戒感が少ないと想定したからである．

そこで我々は実際に家庭でコミュニケーションロボットを利活用している 1,000 人を対象に，ロボットへの印象や扱い方など Web アンケートによる実態調査を行った．図 3 にロボット利用者が抱えるロボットへの不安要素について尋ねた結果を示す．

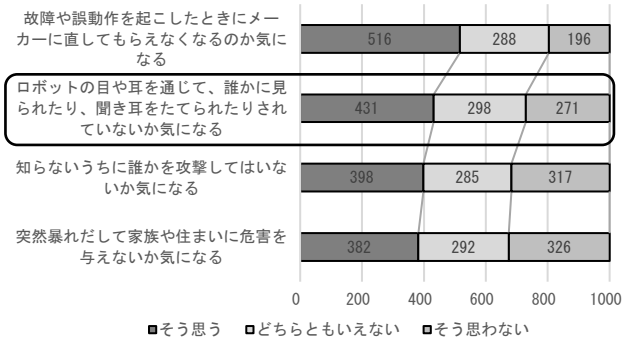

図 3　ロボット利用者が抱えるロボットへの不安要素
（択一，単位：人）

図 3 の Web アンケートの結果から，ロボット利用者であっても「ロボットの目や耳を通じて、誰かに見られたり、聞き耳をたてられたりされていなか気になる」設問に対して，「そう思う」と回答した者が全体の 43.1%（431 人）と，「そう思わない」の 27.1%（271 人）よりも 16 ポイント多いことがわかった．

また Web アンケートでは，ロボットの安全安心面への期待について自由記述形式で尋ねた．回答文字数（30 文字以上）の多かった 13 人の回答結果を表 1 に示す[f]．

表 1 より「ロボットにウイルスが仕掛けられて機能不全にならないようにしてほしい」「サイバー攻撃を受け、誤動作しないようセキュリティ対策を希望する」「ロボット三原則を遵守したプログラム開発が望ましい」などの意見も寄せられた．このことから，テレビ視聴ロボットを開発していく上では，個人情報・プライバシー保護を重点としたセキュリティ対策が必要であり，それを担うクラウド IF への対策が求められると考えた．

表 1　ロボットの安全安心面への期待

高齢者や独身者にとって生活の一部となり命の尊さを学ぶ事が出来る（と安心）。
自宅で倒れたりした時に、異常を察知して病院に連絡が入る機能などがあれば安心できる。
防犯カメラや、会話記録をデータとして利用の権限をもたせずに記録として保管できるようになると安心。
自分に不利益になるようなことはしないのであれば、いいと思います。
熱を持って壊れたりしないよう、異常の前に何か信号を発する機能を付けるとより安心である。
ロボットにウイルスなどが仕掛けられて制御不能になったりしないで欲しい。
一人暮らしの人の場合、会話ができなくなったら他の人に知らせてくれる機能がある良い。
セキュリティ（対策）をしてくれたり、身体的な不調を感知してくれたら良い。
停電、災害時などにトラブルを起こしてしまい混乱にならないような対策をしっかり対処してもらいたい。
売った製品に対してのサポートは最後まで見て頂きたい。
サイバー攻撃を受け、誤作動を起こすのではないかと心配になるので、しっかりとしたセキュリティを期待する。
製作者が安全に関しディープラーニングを強化し、ロボット3原則（を遵守した）プログラミングをしておけば別に問題はないのでは。
電気で動くものだから、誤作動が起きないように最新の安全対策をしてほしい。

3.3 ロボット開発ガイドライン策定の動向

次にテレビ視聴ロボットにセキュリティ対策を講じていくにあたり，設計への参考となる開発ガイドラインの動向を把握していく必要がある．そこで我々は，コミュニケーションロボットに関わると考える国内外の主なガイドラインを「IoT セキュリティ関連」と「AI 開発・利用関連」の 2 つに分けてまとめた[11]．これはコミュニケーションロボットがネットワーク（インターネット）につながるデバイス（すなわち IoT デバイス）としての要素と，学習機能を搭載した AI デバイスとしての要素を兼ね備えていると考えるからである．表 2 に主なガイドラインを示す．

表 2 をもとに内容を精査し，我々はテレビ視聴ロボットにおいて IoT，AI それぞれ特に中核となるガイドラインを，IoT では「IoT セキュリティガイドライン」，AI では「AI 開発ガイドライン」と位置付けた．

IoT セキュリティガイドラインは，経済産業省や総務省が 2016 年 7 月に発行したものである[12]．IoT 機器やシステム・サービスについて求められる基本的な取組を Security by Design として基本原則としつつ，明確化することによって，産業界による積極的な開発等の取組を促すことなどを目的にしている．一方で，一律に具体的なセキュリティ対策の実施を求めるものではなく，守るべきものやリスクの大きさを踏まえ，役割・立場に応じて適切なセキュリティ対策の検討を行うことを期待している．

一方，AI 利活用ガイドライン案は，総務省情報通信政策研究所が 2016 年 10 月に「AI ネットワーク社会推進会議」を立ち上げ，2017 年 7 月に公開した AI 開発ガイドライン案をもとに拡張したもので，2018 年 7 月に公

f) なお回答文字数については，アンケートに対して積極的な意見や感想を提供されているものと本稿では判断した．

開している．ガイドライン案では 6 つの基本理念と 8 つの AI 利活用原則を提唱し，開発者のみならず，AI をビジネスに活用する利用企業や，企業の製品やサービスを通じて AI に触れる一般消費者も対象としている．しかしながら現状は案として推奨しており，強制力がない「ソフトロー」と位置づけ，AI 開発を制約するものでないと解釈される．

IoT セキュリティガイドラインは，実際に利活用している開発ベンダーも多く，実装に近いものである一方，AI 開発ガイドラインにおいては，個別具体的な手引きがそろっていないのが現状と考える．そのため我々は，まず IoT セキュリティ対策への実装を優先し，テレビ視聴ロボットに実装することを検討した．

表 2　コミュニケーションロボットに関わる開発ガイドライン

		ガイドライン名	策定元
IoTセキュリティ関連	1	IoT セキュリティガイドライン ver1.0	IoT 推進コンソーシアム、総務省、経済産業省
	2	IoT 開発におけるセキュリティ設計の手引き	独立行政法人情報処理推進機構(IPA)
	3	GSMA IoT セキュリティ・ガイドライン	GSM Association (GSMA)
	4	CCDS 製品分野別セキュリティガイドライン v2.0	重要生活構器連携セキュリティ協議会
	5	IoT Security Guidance	Open Web Application Security Project (OWASP)
AI開発・利用関連	6	AI 利活用ガイドライン案／AI 利活用原則案	総務省
	7	国際的な議論のための AI開発ガイドライン案	AI ネットワーク社会推進会議（総務省）
	8	「人間中心のAI社会原則」	統合イノベーション戦略推進会議（人間中心の AI 社会原則会議）
	9	人工知能学会「倫理指針」	人工知能学会
	10	AI・データの利用に関する契約ガイドライン 1.1 版	経済産業省
	11	Ethics Guideline for Trustworthy AI	European Commission (High Level Expert Group on AI(HLEG))
	12	Ethically Aligned Design	IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems
	13	Asilomar AI Principles	Future of Life Institute (FLI)
	14	Tenets	Partnership on AI

4. クラウド IF のセキュリティ検知機能

4.1 クラウド IF の IoT セキュリティ設計要件

3 章を受けて我々はセキュリティ対策の最初の取り組みとして，テレビ視聴ロボットにおいて直接外部クラウドやカメラ・マイク接続するクラウド IF への対策に絞った．その上で現時点でのクラウド IF および外部クラウドへのセキュリティ脆弱性を調べるために，外部調査機関を利用して脆弱性検査を実施した．この診断項目にあたって外部調査機関では，表 2 に挙げた「IoT セキュリティガイドライン」のうち，IPA が公開している「安全なウェブサイトの作り方」および 5. OWASP が公開している「OWASP IoT Top 10 2018」を採用した．

IPA の「安全なウェブサイトの作り方」は，「ウェブアプリケーションのセキュリティ実装」として，11 種類の脆弱性を取り上げている．そしてそれぞれの脆弱性で発生しうる脅威や特に注意が必要なウェブサイトの特徴等を解説し，脆弱性の原因そのものをなくす根本的な解決策，攻撃による影響の低減を期待できる対策を示したものである．

OWASP の「OWASP IoT Top 10 2018」は，開発者，製造業者，企業，消費者が IoT システムの作成や利用に関してより良い判断をするために，避けるべきセキュリティ上の注意点が Top10 形式で説明されているものである．

以上この 2 つの検査基準は多くの脆弱性検査機関で一般的に採用されており，デファクトスタンダードとなっている．今回外部調査機関によるクラウド IF の脆弱性検査では，クラウド IF に構築したプログラムのソースコードの診断項目に採用した[g]. またソースコード診断といった静的診断に加え，攻撃フレームワーク（Pacu）を利用したペネトレーションテスト（動的診断）も合わせて実施した．

脆弱性検査の主な結果として，クラウド IF におけるデータの入出力部分，コード上の設定ファイルの秘匿性および入出力データ（映像・音声）・処理データ（キーワード）への秘匿性に関する脆弱性が指摘された．さらにはアラート情報管理の見える化にも不具合が見られた．

なお 3 章で述べたように，現在のテレビ視聴ロボットでは，上記の脆弱性が認められたとしても，障害時には回線を即座に遮断するなど，実験室内での迅速な対応が可能である．そのため早急なセキュリティ対策が必ずしも求められるとは限らない．

一方で実験室外での視聴実験を行うことを想定した場合，実験を行う施設や一般家庭と実験実施者との間をネットワーク接続する設計を考えるため，個人情報・プライバシー情報が，第三者からの侵入・攻撃によって搾取されるリスクが高くなる．そのため現段階から今後を見据えたセキュリティ対策が求められ，現在使用しているクラウド IF にて実装し検証を重ねる必要がある．

そこで現状のクラウド IF において求められる IoT セキュリティ設計要件として，7 つの要件をまず設定した[h]．表 3 にリストを示し，それぞれの要件について説明

g) なお詳細な検査項目と手順については外部調査機関に帰属するため省略する．

h) 7 つの要件の策定に至っては，IoT セキュリティガイドラインに基づく脆弱性検査結果を前提に，過去の情報システム管理部門での実務

Vol.2020-DPS-182 No.36
Vol.2020-CSEC-88 No.36
2020/3/13

を付加した．

表 3　所外実験に向けて必要と考えるクラウド IF の IoT セキュリティ設計要件

	要件	説明
1	IoT 機器（ロボット・カメラ・マイク・エッジ PC 等）の特定・検出	IoT 機器が持つ識別符号等をクラウド IF 側で予め登録し，照合することにより，映像音声の受信の判断を行えるようにする．
2	映像音声データの特定識別化	映像・音声データに識別信号などを付加し，クラウド IF もしくは外部クラウド側で予め登録していた信号と照合することで，データ処理を実施するかの判断ができるようにする．
3	映像音声データ・処理データの秘匿化（暗号化・匿名加工化）	映像音声データおよび処理結果データ（キーワード）が第三者に閲覧されないように，暗号化や匿名加工化などの秘匿性を維持する．
4	入出力部（クラウド IF・クラウド）の強化	映像音声データおよび処理結果データ（キーワード）が第三者に搾取されたり，攻撃されたりしないように入出力部の制限をかける．
5	セキュリティログの収集と分析	不具合を迅速に判断するために必要なセキュリティログを収集し分析できるようにする．
6	侵入・攻撃検知	外部クラウドおよびクラウド IF への不正アクセスなどを自動検知し，第三者による侵入・攻撃を人的判断できるようにする．
7	侵入・攻撃の（自動）防御	侵入・攻撃に対する防御を自動もしくは手動で実施できるようにする．

4.2 セキュリティ検知機能の設計

我々は表 3 に示したセキュリティ設計要件のうち，まずは映像データ収集時や外部クラウド接続時でのセキュリティ対策として，6.の「侵入・攻撃検知」機能をクラウド IF に実装した．このセキュリティ検知機能を作動させるために，2.「映像音声データの特定識別化」と 5.「セキュリティログの収集と分析」の実装も合わせて試みた．図 4 にクラウド IF の構成図を示す．

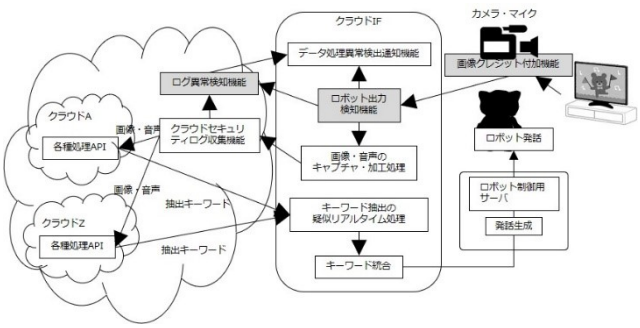

図 4　クラウド IF 概要図
（灰色箇所がセキュリティ検知機能）

具体的には図 4 中の灰色箇所に示す「画像クレジット付加機能」，「ロボット出力検知機能」及び「ログ異常検知機能」を実装した．以下これら 3 つの機能について述べる．

4.2.1 画像クレジット付加機能

画像クレジット付加機能は，映像データが指定のカメラから撮影されたものかどうかを検証するために，カメラ側で画像にインデックスキャプションを合成し，クラウド IF に送信する機能である．図 5 はインデックスキャプションの一例である．

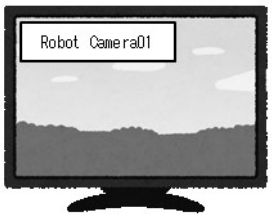

図 5　インデックスキャプションのイメージ
（画像の左上に付加した例）

これによりクラウド IF 側で指定のカメラからの画像データであるかどうか判別できるようにした．

4.2.2 ロボット出力検知機能

ロボット出力検知機能は，指定されたロボットによる映像音声データであるかどうかをクラウド IF 側で検知する機能である．インデックスキャプションを文字認識によって識別することで，カメラ（即ちロボット）からの入力データかどうか判別できる．インデックスキャプションがないなど異常が発生した場合は警告を出し，ログ異常検知機能にログを送信する．これによりカメラを遮断するかどうか人的判断できるようにした．

4.2.3 ログ異常検知機能

ログ異常検知機能は，実験管理者が第三者からのクラウドへの攻撃や侵入を判断できるように，クラウド IF 以外からのアクセスを検知する機能である．ロボット出力検知機能のログも受信し，セキュリティ関連のログを収集して一元管理できるようにした．これにより不具合時にアラート表示によってクラウド内処理を継続・停止するなど，人的判断を速やかに実施できるようにした．

5. セキュリティ検知機能の実装と課題

5.1 セキュリティ検知機能の実装

4.2 節で述べた 3 つの機能をもとにセキュリティ検知機能の実装を試みた．図 6 はログ監視画面の一例である．画面では次のアラートの原因箇所が把握できるようにしている．

1. カメラのインデックスキャプションの有無
2. 指定時間帯以外でのアクセスの有無
3. 指定 IP アドレス以外からのアクセスの有無

による知見と，情報処理安全確保支援士・情報セキュリティ監査人補による監修に基づいた．

これらセキュリティ関連のログを一元管理でき，障害が発生した際に，原因箇所を明確に把握できるようにした．その結果，第三者からの侵入を識別するなど，不具合時での警告表示をもとに手動での対策措置が可能となり，ネットワーク管理部門への報告も迅速に行えるようになった．

図 6　ログ監視画面の例

なお本研究では自己検証として，JPCERT/CC が公開しているチェックリストを試行的に採用した[13][i]．JPCERT/CC（JPCERT コーディネーションセンター)は，技術的な立場における日本の窓口 CSIRT であり，IPA や OWASP 同様，情報セキュリティに関わる脆弱性情報を提供している．特に JPCERT/CC と IPA は脆弱性情報の取り扱いに関する「情報セキュリティ早期警戒パートナーシップガイドライン」の 2019 年版を公開し，連携強化を図っている[14].

JPCSERT/CC のチェックリストをもとにクラウド IF 用の IoT セキュリティチェックリストを作成し，開発時・利用時でのセキュリティ機能を自己検証した．表 4 はそのうちの開発時での検証結果の一部を示す．自己検証の結果については概ね確認できているものの，クライアントデータへの閲覧権限やログ閲覧など実験運用時での動作確認を要する項目も見られた[j].

以上により，クラウド IF にセキュリティ検知機能を実装したことで，実験室内外を問わず視聴実験時での IoT セキュリティ対策への実装する基盤を得ることができた．これは今後テレビ視聴ロボットへの付加機能を拡張していくにあたり，安全安心な環境で開発を継続できる目処ができたと考える．

5.2 セキュリティ検知機能への課題

一方で，今回実装したセキュリティ検知機能には，十分な対策を取るために課題が残されている．これは今回見送った設計要件 1,3,4,7 への取り組みが必要であることと，実装した検知機能自体においても改良していく必要があると考えるからである．

表 4 IoT セキュリティチェックリスト確認一覧
（開発時，一部）

大項目	小項目	開発する際に確認する項目	確認	回答の補足
セキュリティ管理	ログ管理機能	ログ情報が見られることを確認	○	クラウド API 利用時のログを保存
	セッション管理 (Cookie 設定)	Cookie の適切な値に secure 属性、HttpOnly 属性が設定されていることを確認	※	機能未使用
	セッション管理 (URL リライティング)	URL にセッション ID が埋め込まれていないか確認	※	機能未使用
	セッション管理 (ログイン時や重要な確定処理の前後でセッション ID の払い出し)	ログイン時や重要な確定処理の前後でセッション ID が変わっていることを確認	※	機能未使用
	クライアントデータの操作のセキュリティ対策	他のアカウントのデータが操作・閲覧できないことを確認	※	閲覧権限の分離を確認
	システムデータの操作のセキュリティ対策	特定のシステム管理者以外でシステムデータが操作・閲覧できないことを確認	○	ログインには各クラウドのアカウントが必要
	クラウドインターフェースやネットワークの脆弱性（API インターフェースやクラウドベースの Web インターフェース等）	公開情報を元に脆弱性情報を確認	※	利用している外部ソフトウェアをドキュメントに明示する
	XSS、SQLi、および CSRF の脆弱性	公開情報を元に脆弱性情報を確認	※	要確認
	Web アプリケーションの SSL 証明書	利用している証明書を確認	※	証明書を利用していない
アクセス制御	管理されていない物理手段によるアクセス	管理されていない物理的手段によるアクセスに対して制限ができているか確認	※	ローカル PC はアカウント、パスワードによる認証
	リモートアクセス用ポートのデフォルトポート	デフォルトポートの変更を行えるか確認	※	基本的に標準ポートから変更できない
	無線通信におけるセキュリティ(暗号化方式)	接続時にセキュアな暗号化方式が選択されていることを確認	○	ログの保存、閲覧には TLS を使用
	無線通信におけるセキュリティ(WPS)	WPS が動作するか確認	○	未使用
不正な接続	ネットワークポートの制限	ポートの制御が設定したとおりに開閉されていることを確認	※	Web 側の仕様を確認する
	UPnP	デバイスを接続したときに、設定した通りの挙動になっていることを確認	○	未使用
暗号化	データの暗号化機能	データを暗号化する機能があることを確認	○	SSL/TLS 利用
	通信の暗号化機能	暗号化通信が利用できるようことを確認	○	SSL/TLS 利用
	暗号化方式	利用している暗号化方式を確認	○	ログの閲覧には SSL/TLS を利用 クラウド側 REST API 呼び出し時は SSL/TLS 接続を利用
	証明書更新機能	証明書が有効であることを確認	○	証明書未使用
システム設定	センサーの動作状況確認機能	センサーの動作状況を確認	○	カメラ側から機器識別文字の通知機能がある
	ログのセキュリティ管理	閲覧権限のないユーザーでログが見えないことを確認、閲覧可能なユーザーでログが書き換えられないか確認	※	ログの閲覧と作成とで権限を変更していることを運用時に確認する
通知	セキュリティイベントのアラートと通知機能(状態異常等)	仕様通りに動作するか確認	○	メール、クライアントソフトに通知する
	セキュリティイベントのアラートと通知機能(認証失敗、証明書の期限切れ等)	仕様通りに動作するか確認	○	メール、クライアントソフトに通知する
セキュリティ管理	ログ管理機能	ログ情報が見られることを確認		クラウド API 利用時のログを保存
	セッション管理 (Cookie 設定)	Cookie の適切な値に secure 属性、HttpOnly 属性が設定されていることを確認	※	機能未使用

確認欄の「○」は達成，「※」は要検討を示すものと判断する．

i) 4.1 節で採用した IPA・OWASP の診断項目は調査機関にて非公開のため採用できなかった．
j) この結果を受けて，今後 JPCSERT/CC のチェックリストも有用であ

5.2.1 実装した機能での課題

5.1 節で検知する項目について，1 項目目のカメラのインデックスキャプションについては，現状はクラウド側でカメラ映像にスーパーインポーズされた文字列（図 5 参照）を認識している．固定された文字列では，クラウド IF が第三者に侵入されれば特定されるおそれがある．したがってカメラ映像の認証においては，文字列のランダム化や，他の認証情報の付加によってさらに補強しなくてはならない．また不必要な映像送信の除去や必要領域の切り出しによる精度の向上も求められる．

2 項目目の指定時間帯でのアクセスや 3 項目目の指定 IP アドレスでのアクセスについても，それぞれ改ざんされた場合に，なりすましでアラートを回避される可能性がある．この場合は，他の認証方法との組み合わせや暗号化への対応等を検討することが求められる．

5.2.2 未実装機能への対応

また個人情報・プライバシー保護への対策についても，今回は実験室外での視聴実験で用いるカメラ映像を特定することで実装した．しかし現状では映像コンテンツはそのままクラウド API の認識処理を施している．すなわちクラウド IF を経由して外部クラウドに送ってしまっている．

そのため番組解析に直接不要な利用者の顔画像や部屋の映像は，クラウド IF もしくはロボット本体でのローカル処理で識別処理されるのが望ましい．たとえば，部屋を撮影した場合，テレビ受像機のエリア（テレビ番組画面）とそれ以外のエリア（人や家具などの家庭内を映した映像）とを切り分け，それぞれ別系統で認識処理を施すことが求められると考える．さらには今回実装しなかった音声認識においても同様の施策が必要である．

さらにセキュリティ検知機能については，クラウド IF に限定して外部クラウドの異常検知に特化した．将来実験室外での視聴実験を想定するならば，セキュリティ検知機能をクラウド IF からテレビ視聴ロボット全体に拡張し，包括的な異常検知機能を検討する必要がある．

6. まとめと今後に向けて

本稿では，テレビ視聴ロボットの視聴実験を進めていくに必要と考える，セキュリティ対策の取組みについて，主に開発時でのセキュリティ要件をまとめた．このセキュリティ要件は利用者の個人情報やプライバシーの保護を基本とする．そして要件の一部をクラウド IF へのセキュリティ検知機能として設計し実装した．具体的には，画像クレジット付加機能，ロボット出力検知機能およびログ異常検知機能を実装し，動作確認・自己検証したうえで今後の課題について述べた．

5.1 節で述べたように，視聴実験時での IoT セキュリティ対策への実装する基盤を得ることができたことは，今後実験室外での視聴実験を検討するにあたり，個人情報・プライバシーの保護対策への取り組みに役立つものと期待できる．

今後はこの検知機能の動作検証を継続し，さらにセキュリティ防止機能への構築に取り組み，人的判断への負担軽減もしくは自動化に取り組んでいく．また IoT セキュリティ対策と同等に，個人情報・プライバシー保護，倫理面での考慮していくうえで，学習機能も取り入れた AI 開発・利用面での機能追加に取組んでいく．

参考文献

[1] NHK 放送文化研究所, “メディア多様化時代の 20 代とテレビ”,放送研究と調査,2020 年 2 月号
[2] 金子豊, 星祐太, 上原道宏．人と一緒にテレビを視聴するロボットの機能検討と試作．RSJ2017 (2017)
[3] NHK 放送技術研究所,“テレビ視聴ロボット”,NHK 技研ホームページ, https://www.nhk.or.jp/strl/open2018/tenji/9.html
[4] 萩尾 勇太, 金子 豊, 星 祐太, 村崎 康博, 上原 道宏, “人とロボットの共時視聴実験に向けたコミュニケーションロボットの設計と試作”, 映像情報メディア学会年次大会, 33B-31,(2019)
[5] 星 祐太, 金子 豊, 萩尾 勇太, 村崎 康博, 上原 道宏, "ロボット発話に向けたテレビ視聴時の人同士の対話解析," 信学技報, CNR2019-1, pp.1-6 (2019)
[6] Kaspersky, Ghent University,“A glimpse into the present state of security in robotics” (2019)
[7] F.E.Fernandes, G, Yang, H. M. Do, W. Sheng, “Detection of privacy-sensitive situations for social robots in smart homes”, 2016 IEEE International Conference on Automation Science and Engineering (CASE),pp. 727-732, (2016)
[6] ZHANG et al.,” Emotion-Aware Multimedia Systems Security”, IEEE Transactions on Multimedia, Vol.21, pp.617-624(2019)
[9] “海外から見た日本のロボット産業・技術”,三菱 UFJ リサーチ&コンサルティング, https://www.murc.jp/wp-content/uploads/2016/08/global_1607_1.pdf, (2016)
[10] “ロボット・AI 技術の導入をめぐる生活者の受容性と課題”, 野村総合研究所,知的資産創造 2016 年 5 月号,pp108-125, https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/publication/chitekishisan/2016/05/cs20160509.pdf, (2016)
[11] 村﨑康博，金子豊，星祐太，上原道宏．テレビを一緒に視聴するロボットの開発ガイドライン策定に向けての一考察．情報処理学会研究報告．Vol.2017-EIP-78,No.14（2017）
[12] IoT セキュリティガイドライン ver1.0 概要，2016 年 7 月，IoT 推進コンソーシアムほか, http://www.meti.go.jp/press/2016/07/20160705002/20160705002-2.pdf, (2016)
[13] JPCERT/CC, IoT セキュリティチェックリスト, https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html
[14] IPA,LPCERT/CC“情報セキュリティ早期警戒パートナーシップガイドライン”, 2019 年 5 月 30 日年,https://www.ipa.go.jp/security/ciadr/partnership_guide.html,(2019)