スマートテレビの脆弱性検出に関するレポート

～ 情報家電の製品開発におけるファジング（Fuzzing）活用のアプローチ ～

IPA 独立行政法人情報処理推進機構
セキュリティセンター

スマートテレビの脆弱性検出に関するレポート

～ 情報家電の製品開発におけるファジング（Fuzzing）活用のアプローチ ～

目次

スマートテレビの脆弱性検出に関するレポート

～ 情報家電の製品開発におけるファジング（Fuzzing）活用のアプローチ ～

2013 年 3 月 18 日
IPA（独立行政法人 情報処理推進機構）
セキュリティセンター

本書の要旨

近年、テレビ放送を視聴できるだけではなく、インターネットや他の機器と接続することで、さまざまなことを実現できる多機能な「スマートテレビ」の普及が進んでいる。

2012 年に入り、スマートテレビに脆弱性[1]が発見された。この脆弱性が悪用されると、ネットワークから「スマートテレビを強制的に再起動されてしまう」可能性があり、最悪の場合「スマートテレビ上で任意のコードを実行されてしまう」恐れがある。このような被害が現実になる前に、スマートテレビの脆弱性対策を促進する必要がある。

IPA ではスマートテレビの脆弱性検出に、未知の脆弱性を検出できるファジングが有効であると考えた。そこで、日本国内、国外製品の計 4 機種のスマートテレビにファジングを実施し、ファジングの活用方法を調査・検討することとした。

調査の結果 4 機種で合計 10 件の脆弱性を検出した。ファジング対象のスマートテレビ 4 機種すべてで 1 件以上の脆弱性を検出していることから、ファジングがスマートテレビの脆弱性検出に有効であることを実証できた。また、製品開発者によるファジング活用が有効であることも実証できた。

本書では、スマートテレビに対するファジング結果とその分析に基づき、スマートテレビの製品開発におけるファジングの活用方法を提示する。

製品開発においてファジングを活用していただき、脆弱性の低減へつながることを期待します。本書がその一助となれば幸いである。

本書の想定読者

以下のような方々を対象読者として想定している

- （情報家電）製品開発メーカーの設計・開発および品質保証部門の部門長と担当者
- ファジングに興味のある方

本書の用語

用語	説明
バグ	本書では、製品が仕様通りに動作しなくなる等の問題を「バグ」と定義する。
脆弱性	本書では、製品を強制的に再起動させてしまう等のセキュリティ上の問題を「脆弱性」と定義する。この定義は、「情報セキュリティ早期警戒パートナーシップ[2]」におけるガイドラインに沿っている。

[1] 共通脆弱性識別子 CVE-2012-4329
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4329
[2] IPA：「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」
http://www.ipa.go.jp/security/ciadr/partnership_guide.html

1　背景

1.1 身近になる情報家電

我々が身近で使用している「情報家電」にはテレビや DVD レコーダー、ゲーム機などがある。一般的に「情報家電」とは、インターネットに接続できる機能を備えた家電製品を指し、情報家電の分野は市場が形成されつつある。総務省がまとめている「通信利用動向調査[3]」において、一般家庭での保有率をみると、家電製品のなかでもとくに、テレビはその傾向が顕著なことがわかる（図 1）。2013 年 2 月現在、日本国内のテレビの売れ筋ランキング上位 10 機種をみてみると、そのすべてがインターネットに接続できる機能を搭載している。このことから、日本国内で販売されているテレビの多くが「情報家電」に該当するといえる。

「情報家電」のテレビでも、最近では特に「スマートテレビ」が占める割合が高くなってきている。同テレビの売れ筋ランキング上位 10 機種をみてみると、そのうち 8 機種が「スマートテレビ」に該当する。このことから、現在国内で販売されているテレビの多くが「スマートテレビ」であるといってよいだろう。

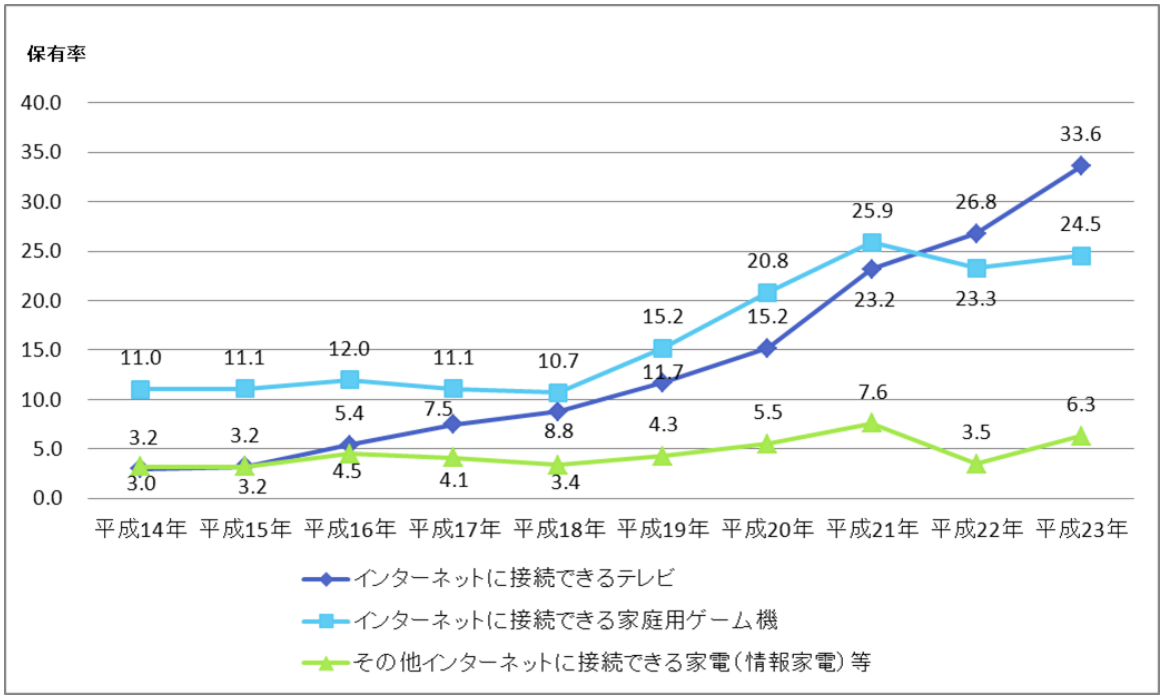


図 1　主な情報通信機器の保有状況の推移
（報告書及び統計表一覧(世帯編) 平成 23 年報告書を基に IPA が作成[4]）

[3] 統計調査データ：通信利用動向調査：報告書及び統計表一覧(世帯編) 平成 23 年報告書
http://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201100_001.pdf

[4] 報告書及び統計表一覧(世帯編) 平成 23 年報告書 1 ページ 図表 1-1「主な情報通信機器の保有状況の推移」を基に作成

1.2 スマートテレビとは

スマートテレビとは「テレビ放送を視聴できるだけではなく、インターネットや他の情報家電と接続することで、ウェブサイトや静止画などの閲覧や動画の再生などを実現できる多機能なテレビ」である。

スマートテレビは、テレビ本来の「テレビ放送を視聴すること」のほかにも、さまざまなことができる。例えば、次のようなことができる。

- Blu-ray/DVD レコーダーで録画した番組を、ネットワークを通じて視聴する

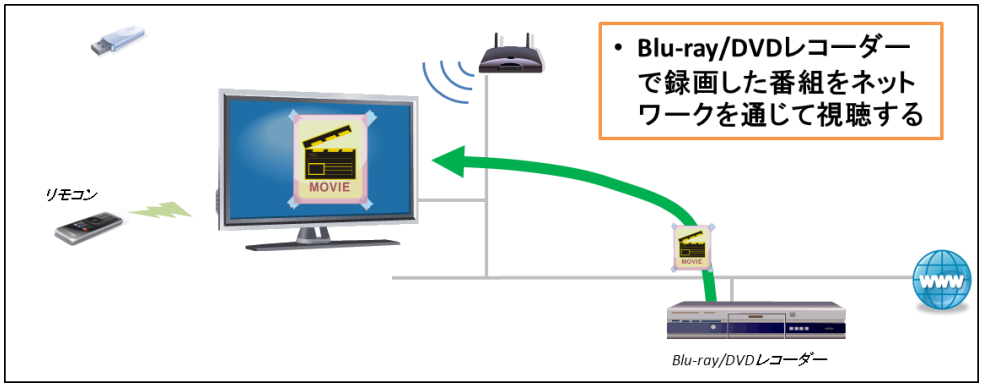


図 2　スマートテレビの利用例 1

- インターネット上のウェブサイトを閲覧する

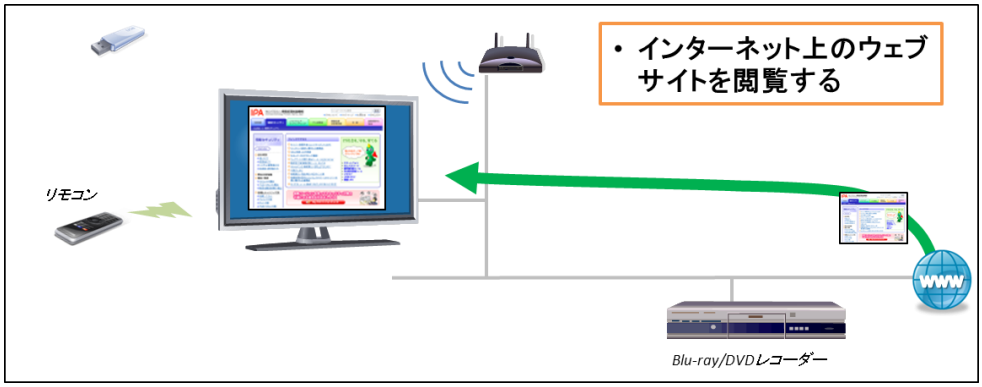


図 3　スマートテレビの利用例 2

- USB メモリや SD カードに入っている写真や動画を再生する

図 4　スマートテレビの利用例 3

1.3 高まるスマートテレビに対する脅威

2012 年になり、スマートテレビの脆弱性を悪用した脅威が示され、スマートテレビにおける脆弱性対策の必要性が急務となってきている。

スマートテレビがインターネットなどにつながることで、つながった分だけ「攻撃の入り口」ができてしまい、攻撃にさらされる可能性が高まる。このような状況を受け、2011 年 2 月、今後ますます市場が拡大していくと想定し、IPA および情報家電メーカー数社はスマートテレビにおけるセキュリティ上の問題および対策の検討を実施して「情報家電におけるセキュリティ対策 検討報告書[5]」にまとめた。この報告書では、脅威に対するセキュリティ対策のひとつとして、スマートテレビの脆弱性対策をあげている。

2012 年に入り、スマートテレビにおいて、他の機器と連携する部分に実際に脆弱性が発見された。この脆弱性を悪用されてしまうと、ネットワークから「スマートテレビが強制的に再起動されてしまう」可能性があり、最悪の場合「スマートテレビ上で任意のコードを実行されてしまう」恐れがある。

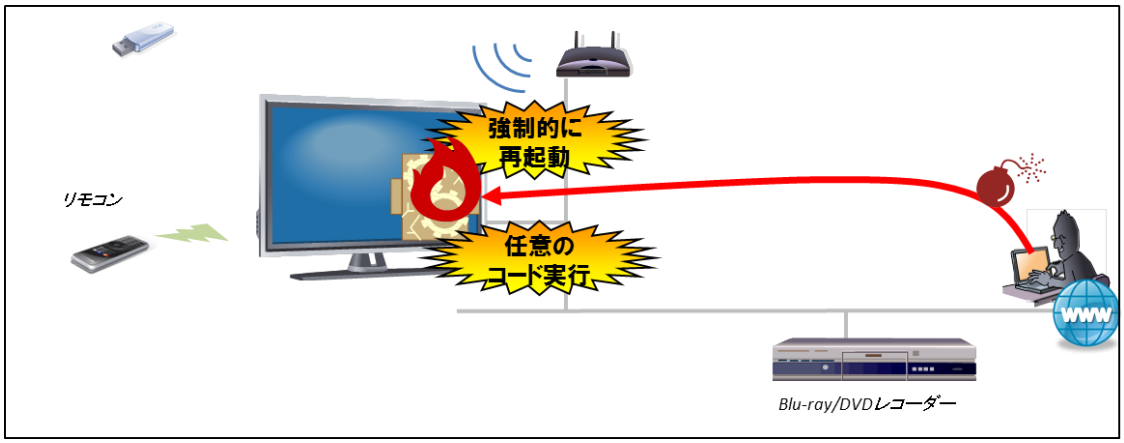


図 5 スマートテレビの脅威

報告書を公開した 2011 年 2 月に比べると、脅威が現実になっているものの、実際にまだ被害は報告されていない。しかしながら、日本国内で販売されているスマートテレビにも他の機器と連携する部分があることから、前述の脆弱性と同様のものが存在すれば被害につながってしまう可能性がある。このことから、被害が現実になる前に、スマートテレビの脆弱性対策を促進する必要があると考える。

[5] IPA：情報家電におけるセキュリティ対策 検討報告書
http://www.ipa.go.jp/security/fy22/reports/electronic/index.html

1.4 スマートテレビに対するファジングの活用方法の検討

これまでIPAでは「脆弱性検出の普及活動[6]」において、ブロードバンドルータなどへのファジングを実施し、その有効性を実証してきた。2012 年 7 月末までに、ブロードバンドルータを始めとする組込み機器 19 機種で、21 件の脆弱性を検出している。その活動のなかで、情報家電のひとつである「HDD レコーダー」に対してもファジングを実施して、脆弱性を検出した。このことから、同じ情報家電であるスマートテレビの脆弱性検出にもファジングを活用できないかと考えた。

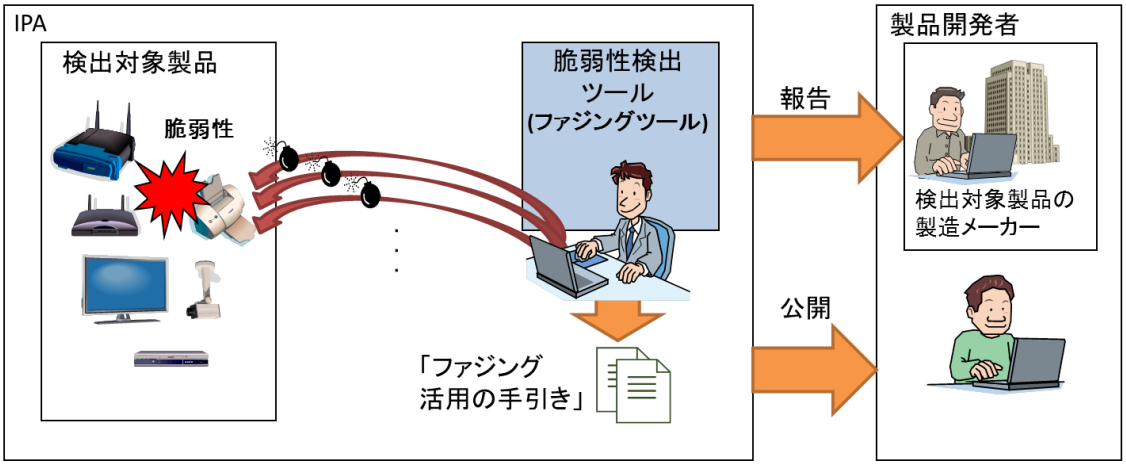


図 6　脆弱性検出の普及活動

そこで、これまでに得た知見をもとに、実際にスマートテレビに対してファジングを実施し、スマートテレビの製品開発におけるファジングの活用方法を調査・検討することとした。本書では、スマートテレビに対するファジング結果とその分析に基づき、スマートテレビの製品開発におけるファジングの活用方法を提示したい。

[6] IPA：「ソフトウェア製品における脆弱性の減少を目指す『脆弱性検出の普及活動』を開始」
http://www.ipa.go.jp/about/press/20110728.html

2　スマートテレビへのファジングの実践

本章では、ファジング対象とするスマートテレビについて述べ、それらに対するファジング実践の過程、そしてファジング結果を説明する。ファジング実践の過程では、スマートテレビの「どんな機能」に対して、「どんなファジングツール」でファジングを実践するか検討した過程に焦点を当てる。

2.1 ファジング対象のスマートテレビ

本書で調査したスマートテレビは、日本国内、国外製品の計 4 機種を選定[7]した。「スマートテレビそのもの」にどのような脆弱性の傾向があるか調査することを視野に入れ、4 機種は異なるメーカーを選定した。このうち 2 機種は日本企業が開発・販売したもので、日本国内の販売シェア上位 5 位以内のメーカーから選定した。残り 2 機種を全世界の販売シェア上位 5 位以内のメーカーが開発・販売したものを選定した。

2.2 スマートテレビに対するファジング検討

スマートテレビに対するファジングを実践するにあたり、スマートテレビの「どんな機能」に対して、「どんなファジングツール」でファジングを実践するか検討した。この検討過程を説明する前に、ファジングの特徴を図 7 でおさらいする。

ファジングでは、ファジング対象機器にテストデータ（入力値）を送信するため、ファジング対象機器がテストデータを受け取る「機能」を決める必要がある。また、ファジングを実施する場合、一般的にファジングツールを使用するが、ファジングツールごとにテストデータが異なるうえに、ファジングを実施できる機能も異なる。そのため、ファジング対象とする機能にあったファジングツールを選ぶ必要がある。

スマートテレビに対するファジングを実施するにあたり、次の 2 点を検討した。

① ファジング対象とするスマートテレビの「機能」
② 使用するファジングツール

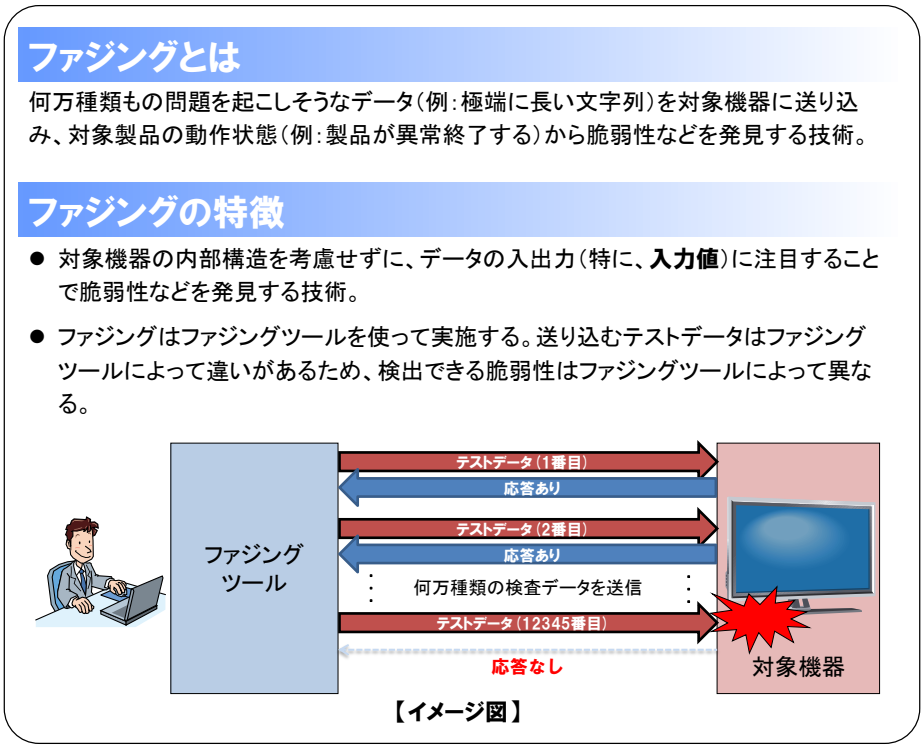
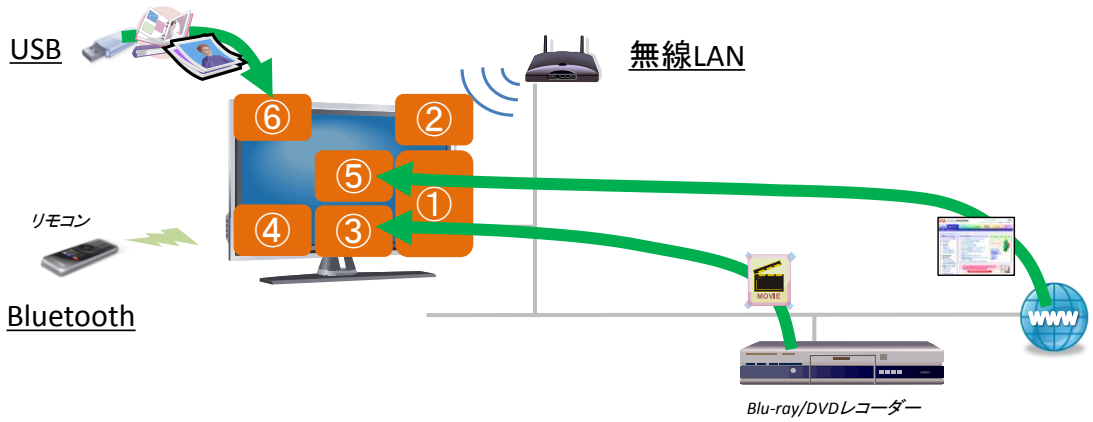


図 7　ファジング

[7] 2012 年 6 月時点の販売シェアを基準に選定した

① ファジング対象とするスマートテレビの機能

スマートテレビが「どんな機器」と「どんなデータ」のやり取りをしているかを調べた結果から、その機能の利用用途や入力値の特徴などにより、図 8 のようにスマートテレビの機能を大きく 6 つに分類した。スマートテレビへのファジングは、これらの 6 機能に対して実施することとした。



項番	機能	スマートテレビの機能
①	有線LAN機能(*1)	有線LANを通じてネットワークへ接続する機能
②	無線LAN機能(*1)	無線LANを通じてネットワークへ接続する機能
③	機器連携機能	他の機器と連携する機能
④	Bluetooth通信機能	Bluetooth通信を使ってリモコンなどを制御する機能
⑤	ウェブブラウザ機能	ウェブサイトを閲覧する機能
⑥	メディア再生機能	画像や動画を再生する機能

(*1):機能③や⑤は、有線LANや無線LANを介して実現されるが、有線LANや無線LANを実現することも一つの機能とみなすことができる。

図 8　スマートテレビのファジング対象機能

スマートテレビにはインターネット上のウェブサイトを閲覧する「⑤ウェブブラウザ機能」がある。また、ネットワーク利用した特徴的な機能として「③機器連携機能」がある。機器連携機能は UPnP[8]を使って機器同士が相互連携する機能である。たとえば「スマートテレビから DVD レコーダーで録画した番組を再生する」といった用途で利用するのはこの機能である。機器連携機能はスマートテレビをはじめとした多くの情報家電が搭載しており、機器同士の相互連携を実現している。

「⑤ウェブブラウザ機能」や「③機器連携機能」は有線 LAN や無線 LAN を介して実現されるが、有線 LAN や無線 LAN を実現することも一つの機能とみなすことができる。有線 LAN を実現する機能を「①有線 LAN 機能」、無線 LAN を実現する機能を「②無線 LAN 機能」と定義する。

その他にもデジタルカメラなどで撮影した画像や動画を USB メモリなどから再生する「⑥メディア再生機能」や、リモコン制御などに利用される「④Bluetooth 通信機能」がある。

[8] ネットワークに接続するだけで組込み機器やパソコンなどの機器同士が何の操作もなく相互に連携できる仕組み。

② 使用したファジングツール

スマートテレビのファジングは商用製品 2 種類を中心に、オープンソースソフトウェア 9 種類[9]（うち内製ツール 1 種類）の計 11 種類のファジングツールを使用することとした（図 9）。

機能＼ツール	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪
有線 LAN 機能	○	○									
無線 LAN 機能			○								
機器連携機能	○	○		○	○						
Bluetooth 通信機能	○										
ウェブブラウザ機能		○				○	○	○	○	○	
メディア再生機能	○										○

青：商用製品　赤：オープンソースソフトウェア　　○：ファジング可能な機能

図 9　スマートテレビにファジングを実施するファジングツール

スマートテレビが実装する機能と商用製品がファジングできる機能を比較すると、IPA が保有するライセンスではファジングできない機能があった。「無線 LAN 機能」がその機能にあたる。スマートテレビでより脆弱性を検出するためには、商用製品でファジングできない機能を他のファジングツールを使って補う必要がある。

そこで、さまざまなファジングツールを探したところ、オープンソースソフトウェアのファジングツールを利用すれば IPA が保有する商用製品がファジングできない機能を補えそうである、ということがわかった。また、商用製品でファジングできる機能においても、オープンソースソフトウェアのファジングツールでファジングできるものがあったため、このような機能にもオープンソースソフトウェアのファジングツールを使用することとした。

しかし、「メディア再生機能」においては調査したファジングツールでは限られた時間の中で、効率よくファジングできるようなツールが見当たらなかった。このため IPA では特定の機能に狙いを絞ってファジングできるツールを内製し、スマートテレビのファジングに使用した。このツールについては、将来的にオープンソースソフトウェアとして公開する予定である。

[9] 本書で使用したオープンソースソフトウェアのファジングツールは IPA が公開している「ファジング活用の手引き」の付録 A に掲載している。興味のある方はそちらを参照していただきたい。
http://www.ipa.go.jp/security/vuln/fuzzing.html

2.3 ファジングの結果

スマートテレビ 4 機種に対して 11 種類のファジングツールを使用して、2012 年 8 月から 2013 年 2 月末日までの期間に 1 台辺りおよそ 1-2 ヶ月程度の時間[10]をかけてファジングを実施した。このファジングの結果、4 機種で合計 10 件の脆弱性を検出した（表 1）。ファジング対象のスマートテレビ 4 機種すべてで 1 件以上の脆弱性を検出した。これらの脆弱性の中には、悪用されると「スマートテレビが強制的に再起動されてしまう」ものもあった。なお、検出した脆弱性については、製品開発企業へ報告している。

表 1 機種別の検出結果

	スマートテレビ A	スマートテレビ B	スマートテレビ C	スマートテレビ D
脆弱性検出件数	1	4	3	2

検出した脆弱性を機能別にまとめてみると、表 2 のようになる。無線 LAN 機能に 1 件、機器連携機能に 2 件、ウェブブラウザ機能に 4 件、メディア再生機能に 3 件の脆弱性を検出した。ファジング対象とした機能 6 機能のうち 4 機能に脆弱性が存在したことが分かる。

表 2 機能別の検出結果

	有線 LAN 機能	無線 LAN 機能	機器連携機能	Bluetooth 通信機能	ウェブブラウザ機能	メディア再生機能
脆弱性検出件数	0	1	2	0	4	3

また、商用製品やオープンソースソフトウェアというファジングツール種別に検出した脆弱性をまとめてみると、表 3 のようになる。商用製品のみで検出した脆弱性が 5 件、オープンソースソフトウェアのみで検出したものが 4 件、商用製品とオープンソースソフトウェア双方で検出したものが 1 件となる。商用製品、オープンソースソフトウェアともに 5 件以上の脆弱性を検出できたことが分かる。

表 3 ファジングツール種別の検出結果

	商用製品	オープンソースソフトウェア（OSS）	商用製品／OSS
脆弱性検出件数	5	4	1

次章では、機能別とファジングツール種別のファジング結果を細かく分析してみたい。

[10] この期間には「どういったファジングが実施できるか」等のファジングを検討する時間も含む。

3　ファジング結果の分析

3.1 ファジングツールからみた分析

ファジングツールに注目してファジング結果を分析してみると、商用製品だけではなくオープンソースソフトウェアもうまく使い、複数種のファジングツールを用いることで、より脆弱性を検出できたことが分かる。

機能別の脆弱性検出件数（表 2）をファジングツール種別にまとめると、図 10 のようになる。「機器連携機能」では商用製品で 1 件、オープンソースソフトウェアで 1 件検出している。「ウェブブラウザ機能」では商用製品で 2 件、オープンソースソフトウェアで 2 件、「メディア再生機能」では商用製品で 2 件、商用製品とオープンソースソフトウェア双方で 1 件検出している。このことから、商用製品と他のファジングツールを併用してファジングと実施した機能では、そのどちらでも脆弱性を検出していることがわかる。これら結果をみると、オープンソースソフトウェアのみを使用してファジングを実施していたとしても、ある程度（検出数の 50%）の脆弱性を検出できていたといえるだろう。

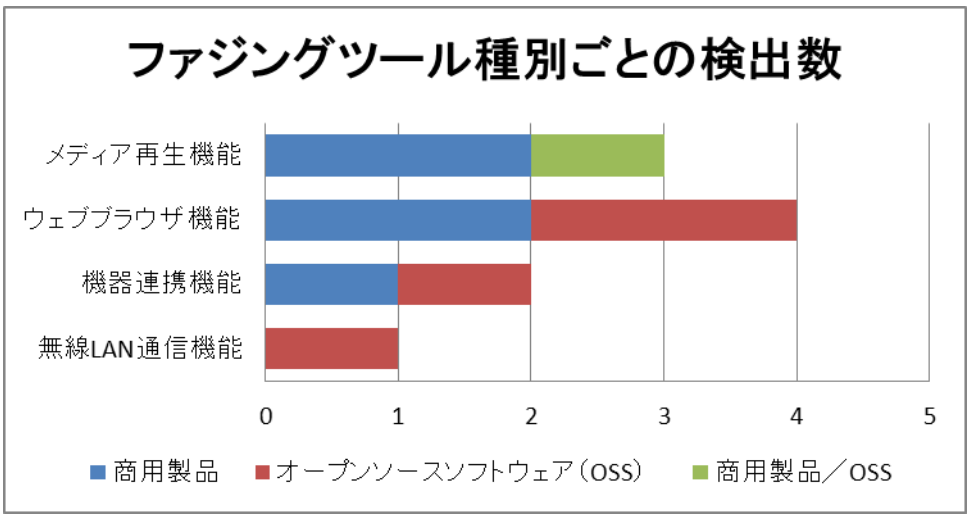


図 10　ファジングツール種別ごとの検出数

検出した機能のうち「機器連携機能」や「ウェブブラウザ機能」に注目してみると、特定のツールで脆弱性を検出できなくても、他のツールで検査すると検出していることがわかる。たとえば図 11 の「機器連携機能」をみると、ツール②、④では検出していないが、①、⑤のツールで脆弱性を検出している。また、「ウェブブラウザ機能」では、⑥、⑦、⑨では検出していないが、②、⑧、⑩のツールで脆弱性を検出している。特定のツールでは検出できない脆弱性も、多数のツール使うことで検出していることがわかる。

機能＼ツール	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪
有線 LAN 機能	ー	ー									
無線 LAN 機能			検								
機器連携機能	検	ー		ー	検						
Bluetooth 通信機能	ー										
ウェブブラウザ機能		検				ー	ー	検	ー	検	
メディア再生機能	検										検

青：商用製品　赤：オープンソースソフトウェア　　検：脆弱性を検出した機能

図 11　機能ごとにみたライセンス形態別検出数

3.2 機能別にみた検出結果の分析

脆弱性を検出した 4 機能を調べてみると、3 機能でオープンソースソフトウェアを利用していた。このことから、スマートテレビがオープンソースソフトウェアの脆弱性の影響を受けている可能性がある。

開発工数を抑えるためや、既にある技術を流用するために、オープンソースソフトウェアを利用してソフトウェアを開発することがある。スマートテレビにおいても同じように、スマートテレビが搭載する OS やソフトウェアにオープンソースソフトウェアが利用されていると推察した[11]。

[11] ソースコードを詳細まで確認していないため推察としている。

この推察をもとに、スマートテレビ 4 機種について次の 2 点を確認した。この確認において、6 機能それぞれが表 4 の判定条件に合致した場合、その機能でオープンソースソフトウェアを利用していると判断した。

(1). スマートテレビの取扱説明書などにおけるライセンス情報
(2). メーカーからダウンロードできるソースコード

表 4 機能別のオープンソースソフトウェア利用の判定条件

機能	利用を想定するソフトウェア	オープンソースソフトウェアの「利用あり」判定条件
有線 LAN 機能	ネットワークカードのデバイスドライバ[12]	ソースコードにデバイスドライバの存在を確認できる
無線 LAN 機能	無線 LAN ネットワークカードのデバイスドライバ	ソースコードにデバイスドライバの存在を確認できる
機器連携機能	UPnP のライブラリ[13]	マニュアルやソースコードからライブラリの利用を確認できる
Bluetooth 通信機能	Bluetooth 機器のデバイスドライバ	ソースコードにデバイスドライバの存在を確認できる
ウェブブラウザ機能	ウェブブラウザ	マニュアルやソースコードからウェブブラウザの利用を確認できる
メディア再生機能	画像を扱うライブラリ	マニュアルやソースコードからライブラリの利用を確認できる

確認の結果、6 機能それぞれのオープンソースソフトウェアの利用状況をまとめると表 5 のようになった。表 5 では 4 機種すべてにおいて利用を確認できた機能を「あり」としている。表 5 をみると 6 機能のうち 5 機能(83%)で、何らかのオープンソースソフトウェアを利用している可能性がある。今回ファジングで脆弱性を検出した 4 機能でも 3 機能が該当する。

ファジング結果から脆弱性が存在している箇所を特定することはできないが、検出した脆弱性がオープンソースソフトウェアのものであった可能性がある。

表 5 機能別のオープンソースソフトウェア利用状況

機能	オープンソースソフトウェアの利用 あり／なし
有線 LAN 機能	あり
無線 LAN 機能	あり
機器連携機能	なし
Bluetooth 通信機能	あり
ウェブブラウザ機能	あり
メディア再生機能	あり

12 デバイスドライバ：ネットワークカードなどのハードウェアを制御するソフトウェア
13 ライブラリ：特定の機能を再利用できるようにまとめたソフトウェアの部品

3.3 分析結果のまとめ

今回の実証の結果から以下のようなことがいえる。

- メディア再生機能やウェブブラウザ機能などの機能に脆弱性がある
- 複数種のファジングツールを使用して脆弱性を検出した
- 脆弱性を検出した多くの機能でオープンソースソフトウェアを活用しており、それらの脆弱性の影響を受けている可能性がある

次章からは、実証の得たスマートテレビに対するファジングの活用方法と、ファジングからみえたスマートテレビの製品開発における課題について説明する。

4　スマートテレビに対するファジングの活用方法

実証から得られたスマートテレビにおける、ファジングの活用ポイントを以下にまとめる。

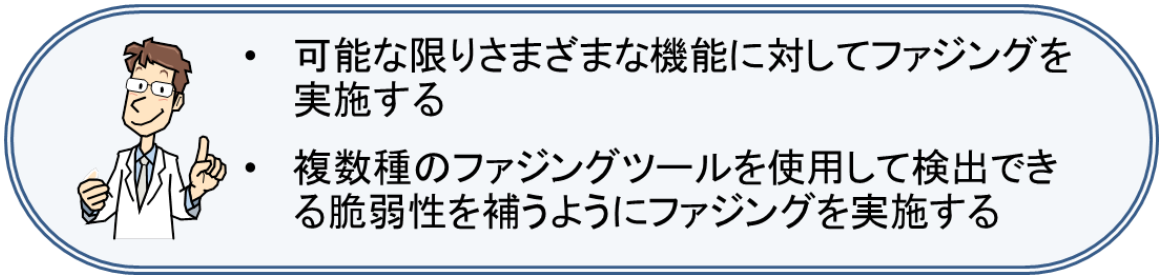


図 12　ファジング活用のポイント

ファジングを実施する場合には、複数のファジングツールを使用するのがよいだろう。複数のファジングツールで検出できる脆弱性を補うようにファジングを実施することで、脆弱性の検出を高めることができる。実証の結果をみると、オープンソースソフトウェアのファジングツールを組み合わせて使用するだけでも効果が期待できる。商用製品のファジングツールを導入していない場合、まずはオープンソースソフトウェアのファジングツールを使用し、ファジングを実施してほしい。

また、スマートテレビへのファジングは、できる限りさまざまな機能に対して実施するのが望ましい。スマートテレビは多くの機能を実装しているため、色々な所に脆弱性が潜んでいる可能性がある。これらの脆弱性を検出するためには、より多くの機能をファジングの対象とする必要がある。

しかし、今回 IPA が実施したファジング期間 1-2 ヶ月とは異なり、多機能なスマートテレビの限られた製品開発期間のテストの一つとしてファジングを実施するには、ある程度の機能に絞らなければならない場合もあるだろう。たとえば「リモートから攻撃される可能性がある機能（例：1.3 節で紹介した脆弱性があるような機能）を優先的にファジングする」などである。

このような可能性を考慮して、製品開発の現場でご活用いただける次の 2 つのコンテンツを公開する。スマートテレビに対するファジングに、ぜひこれらのコンテンツをご活用していただきたい。

(1). 「ファジング実践資料（UPnP 編）」
「機器連携機能」に対して、オープンソースソフトウェアだけでファジングを実現する手順をまとめた資料である。2013 年 1 月 29 日に US-CERT が「libupnp」にバッファオーバーフローの脆弱性[14]が複数存在すること公表したこともあり、多くの組込み機器において UPnP の実装に問題がある恐れがある。そのため、「機器連携機能」に対するファジングにご活用いただけると考え、本資料を公開する。

- ファジング実践資料（UPnP 編）
  http://www.ipa.go.jp/security/vuln/fuzzing.html

(2). IPA ファジングツール「Exif Fuzzer（仮称）」
IPA が作成した「メディア再生機能」に対するファジングツールである。本書を公開した後、公開にむけて情報を整理して、オープンソースソフトウェアとして公開する予定である。

14 http://www.kb.cert.org/vuls/id/922681

5　ファジングから見えた課題：「スマートテレビの脆弱性対策」

スマートテレビが利用するオープンソースソフトウェアに脆弱性が見つかった場合、悪用される前にできる限り早く脆弱性を改修する必要がある。しかし、脆弱性を改修するためには時間やコストがかかるため、すぐに対応するのは困難だといった課題がある。

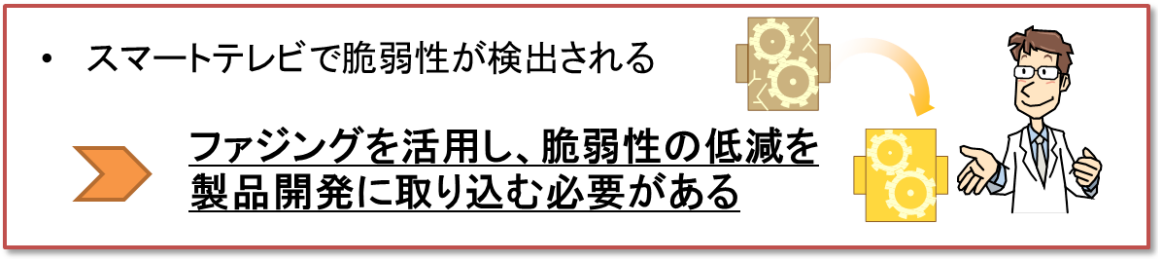
スマートテレビのオープンソースソフトウェアを利用している機能において、脆弱性を検出している。これらの脆弱性は、もともとオープンソースソフトウェアに含まれていた可能性がある。オープンソースソフトウェアの脆弱性が悪用されて「スマートテレビが再起動を繰り返す」といった被害があった場合、利用者からみると「スマートテレビの脆弱性」として捉えられてしまう可能性がある。メーカーからすればオープンソースソフトウェアに含まれる脆弱性だが、利用者からすればスマートテレビの一部に脆弱性があるようにみえるからである。また、他の機種でも同じオープンソースソフトウェアを利用していた場合、影響が他の機種にまで及んでしまうこともある。オープンソースソフトウェアを利用するうえでは、このような注意点があることを知っておく必要がある。

万一スマートテレビが利用しているオープンソースソフトウェアに脆弱性が見つかった場合には、悪用される前に脆弱性を改修し、放送波やインターネットを通じて対策したものを利用者のスマートテレビへ配信する必要がある。しかしながら、これらの対応には時間やコストがかかるため、すぐには実施できない場合もあるだろう。脆弱性を改修して配信できるようになるまでには、ソースコードの修正、テストによる動作確認、配信のためのもろもろの準備といった段階を踏まなければならない。これらの段階が全て完了してから、ようやく配信できるようになる。配信できるようになるまで時間がかかる分だけコストもかかってしまう。

スマートテレビへの攻撃コードを作るハードルは年々低くなってきており、脅威が増大している。脅威が増大するなか、脆弱性の改修に素早く対応するには、改修にかかる時間やコストをどのように削減していくかが重要となる。これらの課題は、スマートテレビの製品開発において業界全体で取り組んでいかなければならない課題であるといえるだろう。

6　まとめ

今回の実証から以下のようなことが明らかになった。



IPA は「ファジング」が開発ライフサイクルで活用されることを期待する。製品開発企業においては、さまざまなアプローチでのファジングをぜひ試してほしい。バグや脆弱性の早期発見・解決が品質向上への近道へのひとつであると考える。

本書がスマートテレビの製品開発におけるファジング活用の一助となれば幸いである。

付録１：情報家電や組込み機器の製品開発における脆弱性対策

スマートテレビの開発に限らず、情報家電や組込み機器の製品開発では、製品開発ライフサイクル[15]のそれぞれの工程において脆弱性対策を実施することが重要である（図 13）。本章では、図 13 の①から④に該当する各工程における脆弱性対策について、ファジングに限らず IPA の公開資料を交えながら紹介する。

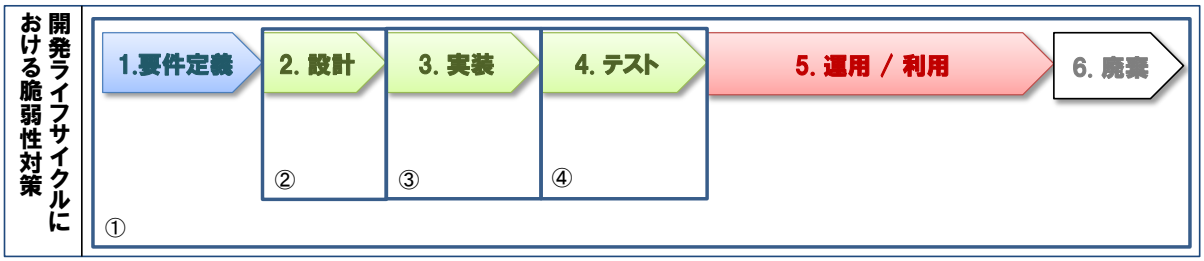


図 13 製品開発ライフサイクルにおける脆弱性対策

①開発ライフサイクル全体での脆弱性対策

IPA ではスマートテレビなどの組込みシステムの開発向けに「組込みシステムのセキュリティへの取組みガイド」を公開している。このガイドではオープンソースソフトウェアを利用した開発についての考慮点なども記載している。これらをスマートテレビの製品開発において活用していただきたい。

- 組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）
  http://www.ipa.go.jp/security/fy22/reports/emb_app2010/index.html

- 情報家電におけるセキュリティ対策 検討報告書
  http://www.ipa.go.jp/security/fy22/reports/electronic/index.html

②[設計]工程における脆弱性対策

OS やライブラリ、オープンソースソフトウェアを選定するうえで、最新の脆弱性情報を把握しておくことが重要である。脆弱性対策情報データベース「JVN iPedia」を検索することにより、今までに発見された脆弱性に関する情報を収集することができる。

- JVN iPedia
  http://jvndb.jvn.jp/

15 ソフトウェア製品における企画から開発、運用、廃棄（使用終了）までの一連の流れを、大きな作業のかたまり（プロセス）に分けて考える開発モデル。

③[実装]工程における脆弱性対策

製品開発における脆弱性対策には、セキュア・プログラミングやソースコードセキュリティ検査などがある。IPA ではソフトウェア開発の現場で働いている設計者およびプログラマ向けに、各種の脆弱性を紹介するとともに、これらを含まないようにプログラミングするテクニック「セキュア・プログラミング」を紹介している。また、C 言語で作成されたソースコードに脆弱性が存在しないかどうかを検査する「ソースコードセキュリティ検査ツール」なども公開している。

また、実装工程では単体テストの入力値として、ファジングツールのテストデータを使うこともできる。開発ライフサイクルの工程が進むにつれて、バグや脆弱性が検出された場合の修正コストは大きくなる。できるだけ早い段階でバグや脆弱性を潰しておくことで、修正や再テストといった手戻りにかかる期間や工数などを削減しコストを抑えることができる。

- セキュア・プログラミング講座
  http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html

- ソースコードセキュリティ検査ツール iCodeChecker
  http://www.ipa.go.jp/security/vuln/iCodeChecker/index.html

④[テスト]工程における脆弱性対策

テスト工程は脆弱性を検出して製品出荷前に対策できる最後の工程であり、製品の品質を保証するうえでもっとも重要な工程である。テスト工程では特にファジングを活用していただきたい。

製品全体の品質向上には特定箇所だけでなく、製品に実装されるすべての機能へ網羅的にファジングを実施することが望ましい。

とはいえ、企業において新たな機能にファジングを実施する場合、その分だけテスト工数が増えるといった課題が出てくるであろう。しかしファジングには同じような機能への流用が容易といった特徴や、ファジングツールによっては自動化できるといった特徴がある。いったんファジングできる環境を構築して、何種類もの製品に同じファジングを流用すれば、結果としてテスト工数の削減にもつながる。

製品開発企業においては、開発やテストにかけられる時間には限りがあるが、まずは可能な範囲でできるファジングや、結果としてテスト労力の削減につながるファジングから実施を検討していただきたい。

また、IPA では TCP/IP や SIP を実装する製品の開発者向けに、無償で脆弱性の検証ツールを貸し出している。これらのツールも合わせて活用していただきたい。

- ファジング活用の手引き
  http://www.ipa.go.jp/security/vuln/fuzzing.html

- TCP/IP に係る既知の脆弱性検証ツール
  https://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

- SIP に係る既知の脆弱性検証ツール
  https://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

著作・制作　独立行政法人情報処理推進機構（IPA）

編集責任　　小林 偉昭

執筆者　　澤田 迅

勝海 直人
岡崎 圭輔

協力者　　鵜飼 裕司（株式会社フォティーンフォティ技術研究所）
金野 千里
板橋 博之

伊藤 良孝　　相馬 基邦　　遠藤 基　　岡下 博子　　谷口 隼祐

※独立行政法人情報処理推進機構の職員については所属組織名を省略しました。

スマートテレビの脆弱性検出に関するレポート

― 情報家電の製品開発におけるファジング（Fuzzing）活用のアプローチ ―

［発　　行］２０１３年　３月１８日 第1版

［著作・制作］独立行政法人情報処理推進機構 セキュリティセンター