# 重要生活機器の脅威事例集

## 2016年度 調査事例

2016年11月1日

一般社団法人
重要生活機器連携セキュリティ協議会(CCDS)事務局

# Samsung 製ネットワークビデオレコーダーに複数の脆弱性（2016）

| 分　類 | 脆弱性 | 分野 | 家電 | 時期 | 2016/1/13 | 地域 | 韓国 |
|---|---|---|---|---|---|---|---|
| 情報源 | Japan Vulnerability Notes<br>https://jvn.jp/vu/JVNVU97593732/index.html | | | | | | |
| 脅威 | Samsung 製ネットワークビデオレコーダーに複数の脆弱性 | | | | | | |
| 概要 | | | | | | | |

Samsung が提供するネットワークビデオレコーダー SRN-1670D には、複数の脆弱性が存在
(詳細情報)
認可・権限・アクセス制御の問題
　説明書に記載されていない URL にアクセスすることで、システム内の任意のファイルを取得することが可能です。
情報漏えい
　エラーメッセージに必要以上の情報が含まれているため、攻撃者はエラーメッセージから有効なユーザ名などを特定することが可能です。
不完全またはリスキーなアルゴリズムの使用
　ファームウェアのファイルシステムは、単純な XOR をもとにした独自の暗号化スキームを使用しており、容易に解読可能です。
(想定される影響)
　遠隔の攻撃者によって、機器内の任意のファイルを取得されたり、有効なユーザ名を特定されたりする可能性があります。

# Auction Camera におけるアクセス制限不備の脆弱性（2015）

| 分　類 | 脆弱性 | 分野 | 家電 | 時期 | 2015/9/16 | 地域 | 日本 |
|---|---|---|---|---|---|---|---|
| 情報源 | Japan Vulnerability Notes<br>https://jvn.jp/vu/JVNVU97593732/index.html | | | | | | |
| 脅威 | Auction Camera におけるアクセス制限不備の脆弱性 | | | | | | |
| 概要 | | | | | | | |

株式会社ニューフォリアが提供する Auction Camera には、アクセス制限不備の脆弱性が存在

(詳細情報)
株式会社ニューフォリアが提供する Auction Camera は、ハイブリッドアプリ開発支援プラットフォーム「アプリカン」で作成されたスマートフォン向けアプリです。Auction Camera には、URL スキームを使って起動することで、任意のページを表示させることが可能になる問題が存在します。

(想定される影響)
Andorid アプリケーションでは、アプリケーションの権限で使用可能な任意の API を実行される可能性があります。
iOS アプリケーションでは、iOS で使用可能な任意の API を実行される可能性があります。

# デジタルビデオレコーダがパスワード認証をしていない問題（2015）

| 分　類 | 脆弱性 | 分野 | 家電 | 時期 | 2015/8/21 | 地域 | シンガポール |
|---|---|---|---|---|---|---|---|
| 情報源 | Japan Vulnerability Notes<br>https://jvn.jp/vu/JVNVU97593732/index.html | | | | | | |
| 脅威 | Dedicated Micros のデジタルビデオレコーダが、平文で通信し、パスワード認証をしていない問題 | | | | | | |

## 概要

Dedicated Micros のデジタルビデオレコーダ製品は、デフォルト設定では、暗号化されていない平文で通信し、また、パスワードによるユーザ認証を行いません。
(詳細情報)

**センシティブなデータを暗号化しない**

Dedicated Micros のデジタルビデオレコーダ製品は、デフォルト設定では、通信内容を暗号化しないプロトコルである HTTP、Telnet、FTP を用いており、よりセキュアなプロトコルを使用するよう設定するのはエンドユーザの責任としています。そのためデフォルト設定では、第三者によって通信が閲覧されたり改ざんされたりする可能性があります。

**不適切なアクセス制御**

Dedicated Micros のデジタルビデオレコーダ製品は、デフォルト設定ではユーザ認証を要求しません。エンドユーザはデバイスにパスワードを設定することができますが、必須ではありません。デフォルト設定では、第三者によって自由にデバイスにアクセスされたりデータを改ざんされたりする可能性があります。

(想定される影響)
遠隔の攻撃者によって、センシティブなデータを閲覧されたり操作されたりする可能性があります。また、セキュアな設定を行っていないデバイスは完全に制御を奪われる可能性があります。

# オムロン製 PLC および CX-Programmer に複数の脆弱性（2015）

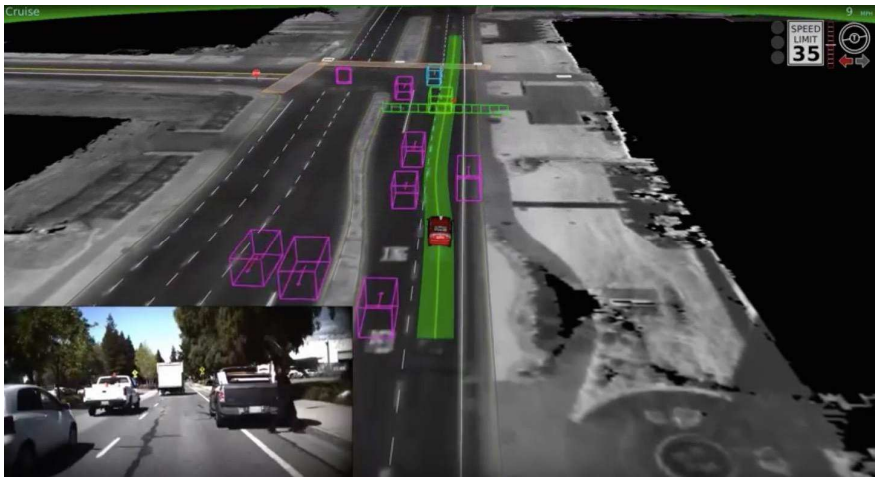
| 分　類 | 脆弱性 | 分野 | 工場制御 | 時期 | 2015/10/1 | 地域 | 日本 |
|---|---|---|---|---|---|---|---|
| 情報源 | Japan Vulnerability Notes<br>https://jvn.jp/vu/JVNVU97593732/index.html | | | | | | |
| 脅威 | オムロン製 PLC および CX-Programmer に複数の脆弱性 | | | | | | |
| 概要 | | | | | | | |

オムロン製プログラマブルロジックコントローラ (以降 PLC) および　CX-Programmer には、複数の脆弱性が存在します。
(詳細情報)
オムロンが提供する PLC 製品 CJ2 シリーズおよび、PLC や HMI の設定やプログラムを行うためのソフトウェア CX-Programmer には、次に挙げる脆弱性が存在します。
　パスワードが平文で送信される脆弱性
　CX-Programmer 用プロジェクトファイルからパスワードを取り出せる脆弱性
　コンパクトフラッシュカードに保存されるオブジェクトファイルからパスワードを取り出せる脆弱性
(想定される影響)
遠隔の第三者によってパケットを盗聴された場合、平文で送信されるパスワードを取得される可能性があります。また、システムのファイルシステムにアクセスできる攻撃者にパスワードを取得される可能性があります。

# レーザーで人や障害物の偽信号を発生し、強制的に車を減速・停止（2015）

| 分　類 | 研究 | 分野 | 自動車 | 時期 | 2015/9/10 | 地域 | 米国 |
|---|---|---|---|---|---|---|---|
| 情報源 | Japan Vulnerability Notes<br>https://jvn.jp/vu/JVNVU97593732/index.html | | | | | | |
| 脅威 | レーザーで人や障害物の偽信号を発生し、強制的に車を減速・停止 | | | | | | |
| 概要 | | | | | | | |

ネットワーク経由ではなく、自動運転車の屋根の上で周囲の状況をスキャニングするレーザースキャナー（ライダー＝LIDAR）にレーザーでハッキングされる脆弱性があることがわかった。
ハッキングされた自動運転車は減速したり、停止したまま動けなくなってしまうという。




自動運転車がライダーを使って周囲の状況を確認している様子

# 自作での自動運転技術を開発（2015）

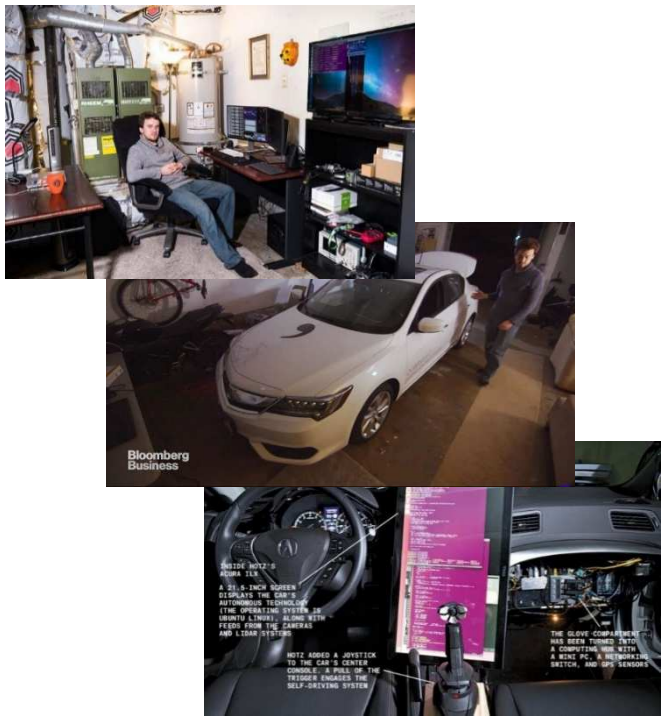
| 分　類 | 研究 | 分野 | 自動車 | 時期 | 2015/12/16 | 地域 | 米国 |
|---|---|---|---|---|---|---|---|
| 情報源 | Bloomberg Business<br>http://www.bloomberg.com/features/2015-george-hotz-self-driving-car/<br>https://www.youtube.com/watch?v=KTrgRYa2wbI | | | | | | |
| 脅威 | 自作での自動運転技術を開発 | | | | | | |

**概要**

Geohot氏が、経済誌bloombergにて紹介。その内容として、自作で自動運転技術を開発し、実際に車に搭載させ走行していると報じられている。
開発は2015年10月下旬からスタートし、ベース車はホンダ「2016年型 アキュラ ILX」。車の改造を自身で行ったようで、Hondaサービスセンターの認可（オンラインで申し込める簡易な物）を受けアキュラ ILXのマニュアルや構成図を入手。それを参考に改造を行った。

内部は「Linux」を搭載した「Intel NUC ミニコンピュータ」がメイン。カメラは車の周囲を捉えるために6台、スマホなどにも使われる13ドル程度の安価なカメラを使用。また、前方を捉えるために魚眼カメラを含む2台が使用されている。

2015年12月上旬に撮影された動画が公開されている。
開発したガレージの様子やGeohot氏へのインタビュー、また実際にハイウェイ上での自動運転を行う様子などをみることができる。



# テレビなどの映像・音声処理ソフトに脆弱性　乗っ取りの恐れ（2015）

| 分　類 | 研究 | 分野 | 家電 | 時期 | 2015/8/9 | 地域 | 米国 |
|---|---|---|---|---|---|---|---|
| 情報源 | DEFCON<br>日経新聞(http://www.nikkei.com/article/DGXLASDZ09H0B_Z00C15A8TJC000/) | | | | | | |
| 脅威 | テレビなどの映像・音声処理ソフトに脆弱性　乗っ取りの恐れ | | | | | | |
| 概要 | | | | | | | |

テレビなどに使われている映像と音声処理のソフトの一部にセキュリティー上の欠陥（脆弱性）が見つかったとの発表があった。
インターネットとつながっている機器の場合、攻撃者がテレビ操作を乗っ取る恐れがある。テレビやブルーレイ・ディスクプレーヤーなど世界で７億５千万台に影響する可能性が出てきた。
　米ヒューレット・パッカードの分析官、ジョシュア・スミス氏が発表した。問題のソフトは「ＨＤＭＩ―ＣＥＣ」と呼ばれ、地上デジタル放送のデータ処理をしたり、録画予約などの操作ができるようにテレビと録画機器で情報をやりとりしたりする。
　インターネットでつながっている機器の場合、攻撃者は脆弱性を悪用してネット経由でコンピューターウイルスを送り込め、感染させることができる。スミス氏はパナソニックのテレビや韓国サムスン電子のブルーレイ・ディスクプレーヤーでソフトの脆弱性を確認したと話した。


ヒューレット・パッカードのスミス氏はソフトの脆弱性を指摘した（米ラスベガス）

# ATMのイーサネット回線をジャック（2016）

| 分　類 | 実例 | 分野 | 金融 | 時期 | 2016/2/10 | 地域 | 不明 |
|---|---|---|---|---|---|---|---|

**情報源**

GIZMODO JAPAN : http://www.gizmodo.jp/2016/02/_atm_skimmer.html
Gizmodo US : http://gizmodo.com/crooks-dont-need-a-fancy-skimmer-they-can-just-tap-an-1758228948
Krebs on Security reports : http://krebsonsecurity.com/2016/02/skimmers-hijack-atm-network-cables/

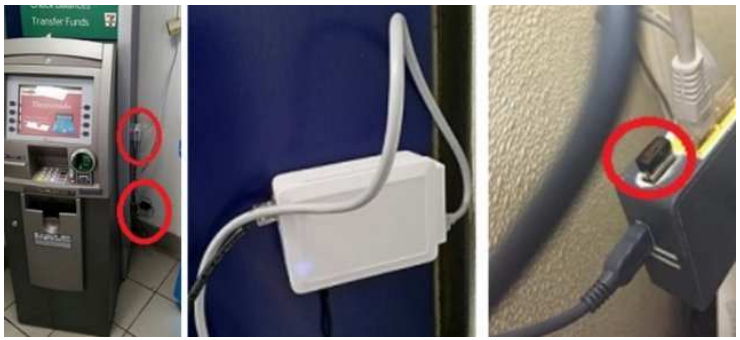
**脅威**

ATMのイーサネット回線をジャック

**概要**

ATMを狙った犯罪のすべてが、必ずしも複雑な読み取り装置を使用するわけではなく、最近になって登場したパターンの攻撃では、ATMのイーサネット回線をジャックすることでカード情報を不正に取得するという方法もあることがわかった。
セキュリティ・ジャーナリストのブライアン・クレブス氏が自身のサイトKrebs on Securityで語っている内容によれば、NCRという私たちがそれこそ毎日のように使っているATMなどのキャッシングマシンを数多く製造している会社が、この新種の攻撃に関して警告を発したとのこと。

これはあるデバイスを使った手法で、そのデバイスを機械のネットワーク回線に接続することでカードの詳細情報を入手するというもの。
その一方でセパレート型のカメラやキーパッドのカバー部分を使って暗証番号も同時に入手するのです。クレブ氏によれば、こういったハードウェアを使用した犯行はすでにNCRやDieboldのATMで行なわれている。
右の画像からもわかるとおり、このタイプの犯行はネットワークケーブルへの細工が簡単にできる独立型のATMを狙って行なわれている。



ネットワークケーブルに取り付けられたスキミング装置

# 電動スケートボードやトスライダーのコントロールを奪取（2015）

| 分　類 | 実例 | 分野 | 家電 | 時期 | 2015/4/8 | 地域 | オーストラリア |
|---|---|---|---|---|---|---|---|
| 情報源 | DEFCON 23 : Hacking Electric Skateboards: Vehicle Research For Mortals<br>wired : http://www.wired.com/2015/08/hackers-can-seize-control-of-electric-skateboards-and-toss-riders-boosted-revo/ | | | | | | |
| 脅威 | 電動スケートボードやトスライダーのコントロールを奪取 | | | | | | |

**概要**

メルボルン、オーストラリアの交差点に向かって電動スケートボードに乗っていたところ、突然ボードが停止。そして乗っていた人は投げ出されてしまった。そして、ボードを制御することも、何が間違っているかも解らなかった。そのことから、自然とハッキングされているのではないかという考えに行きついた。

原因がBluetoothのノイズであるということが判明するまでにあまり時間はかからなかった。スケートボードは携帯型リモコンからBluetooth経由で駆動コマンドを送信するなどして制御されていた。フェデレーション・スクエア近くの交差点では、無線周波数のノイズで飽和していることで有名で、その状況から、自分のリモートの接続を妨害していた、と結論付けました。

さらに、研究を重ね他社の電動スケートボードの制御を完全に奪取するFacePlantを開発した。この内容は、DEFCON 23にて発表された。

＊DEFCONでは、電動で動くスケートボードのBluetoothをハッキングを実演

# 玩具からの情報漏洩（2015）

| 分　類 | 脅威 | 分野 | 家電(玩具) | 時期 | 2015/11/2 | 地域 | 米国 |
|---|---|---|---|---|---|---|---|
| 情報源 | Forbes JAPAN：http://forbesjapan.com/articles/detail/11208 | | | | | | |
| 脅威 | ネット接続可能なテディベアに不具合があり、コマンドを送って操ったり子供の個人情報を盗んだりすることができる状態に | | | | | | |
| 概要 | 問題のぬいぐるみはモバイルアプリを使用して機能を拡張できるもので、Rapid7によると、いくつかのAPIがメッセージの送信元を正しく判別していなかった。つまり、ハッカーがユーザー名を予想できた場合、子供たちの名前や誕生日、性別、使用言語、使用したおもちゃの履歴などの個人情報を閲覧することができる状態だった。<br>また、ハッカーらが「おもちゃの通常の動作を妨害し、子供が意図していないような動作をさせることもできた」とフィッシャープライス（親会社は米大手玩具メーカーのマテル）はブログで説明した。同社はRapid7のリサーチャーMark Stanislavから2015年11月23日に不具合の指摘を受け、1月19日に修正した。<br>　また、ハッカーらが「おもちゃの通常の動作を妨害し、子供が意図していないような動作をさせることもできた」とフィッシャープライス（親会社は米大手玩具メーカーのマテル）はブログで説明した。同社はRapid7のリサーチャーMark Stanislavから2015年11月23日に不具合の指摘を受け、1月19日に修正した。<br>  <br>(画像はイメージです) | | | | | | |