OUCH! | 2018 年 08 月

SANS SECURITY AWARENESS

OUCH!

コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

スマート家電

スマート家電とは何か

これまではノートパソコンやスマートフォン、ゲーム用コンソールといった限られた種類の家庭用機器でしか、インターネットに接続することはできませんでした。ところが現在では、電球やスピーカーからテレビ、ドアの鍵、さらには車に至るまで多くの機器がインターネットに接続されています。近い将来、家庭にあるほぼすべての機器がインターネットにつながるようになるかもしれません。こうしたインターネットに接続された機器は、よくINTERNET OF THINGS (IoT) やスマート家電の名で呼ばれています。これらの接続された機器は、生活の利便性を大きく向上させてくれる一方、特有の危険をはらんでいます。

何が問題なのか

自宅のネットワークに接続された機器が増えれば増えるほど、より多くの問題に直面するようになります。ハッカーらはあなたの機器を踏み台にして他人を攻撃するプログラムを組み込み、膨大な活動記録を収集することが可能です。あるいは機器がマルウェアに感染し、制御できなくなる可能性もあります。スマート家電を開発している企業の多くは、サイバーセキュリティに関する経験が無く、セキュリティをコストと捉えています。結果、あなたが購入する機器の多くは、セキュリティ機能を全く備えていないか、少ししか備えていないかのどちらかでしょう。例えば、いくつかのスマート家電は、広く一般に知られたパスワードをデフォルトで使用していたり、アップデートや設定変更ができないようになっていたりします。

自分の身を守るにはどうすれば良いか

あなたにできることは何でしょうか。まずは今インターネットに接続されている機器を、安全かつセキュアに使用してください。これらのスマート家電は、あなたの生活の無駄を省いてくれる、素晴らしい機能をもっています。さらに、技術の進歩にともない、スマート家電を使うことが当たり前になる日が来るかもしれません。あなたの身を守るためのステップは、次のとおりです。

必要なものだけを接続する：機器をセキュアな状態に保つ最も簡単な方法は、その機器をインターネットに接続しないことです。使用している機器をオンラインにしておく必要が無いのであれば、無線ネットワークへの接続は控えましょう。トースターからの通知をあなたのスマートフォンで受信する必要が本当にありますかを考えれば自明なはずです。

何を接続したのか覚えておく：どの機器を自宅のネットワークに接続しましたか。記憶があいまい、もしくは覚えていないのではないでしょうか。無線ネットワークを切断し、どの機器が稼働しなくなったか見てみましょう。全てを見分けることはできないかもしれませんが、きっと考えていたよりも多くの機器の存在を忘れていたことに驚くでしょう。

常にアップデートする：パソコンやモバイル端末のように、どのようなものであれ全ての機器を最新の状態にしておくことは大切です。使用している機器に自動アップデート機能がある場合は、有効化しましょう。

パスワード：使用している機器のパスワードを、あなたしか知りえないユニークで強力なパスフレーズに変更しましょう。おそらく入力が必要なのは一度きりです。全てのパスフレーズを覚えきれないと思われるかもしれませんが、そんなこと私たちにもできないので安心してください。そこで、全てのパスフレーズを安全に管理するため、パスワードマネージャの使用を検討することをお勧めします。

プライバシー設定：あなたの機器においてプライバシー設定が可能であれば、その機器が収集、共有する情報の量を制限しましょう。一つの設定例としては、単純にあらゆる情報を共有する機能を無効化することです。

ベンダー：機器を購入する際は、あなたが知っていて信頼できる企業のものを選びましょう。そしてセキュリティ機能をサポートしている製品を探しましょう。例えば、自動アップデートやデフォルトパスワードの変更、プライバシー設定の変更が可能なものです。

常に聞かれている：声で命令を与えることができる機器の場合、その機器は常に聞き耳を立てています。例えば、AlexaやGoogle Homeといった機器は、機微な会話を録音してしまう可能性があります。自宅で機器を設置する場所を決める際、このことに留意しましょう。そしてプライバシー設定を確認しましょう。

ゲストネットワーク：スマート家電を、普段パソコンやモバイル端末で使用しているメインの無線ネットワークではなく、別に用意した「ゲスト用」無線ネットワークに接続することを検討しましょう。そうすることで、スマート家電のどれかがマルウェアに感染した場合、メインのネットワークに接続されているあなたのパソコンやモバイル端末を、安全な状態に保つことができます。

新しい技術を恐れる理由は何一つありませんが、そうした技術が抱えるリスクを理解しましょう。上に挙げた簡単なステップを踏むことで、これまでよりはるかにセキュアなスマートホームを構築できます。

ゲストエディタ

ロバート・M・リー氏 (@RobertMLee) は、SANS認定インストラクターであり、FOR578 – Cyber Threat IntelligenceおよびICS515 – ICS Active Defense and Incident Responseの著者であり、産業サイバーセキュリティ企業であるDragos社のCEOおよび創設者です。

リソース

パスフレーズについて:	https://www.sans.org/u/GEB
パスワードマネージャ:	https://www.sans.org/u/GEG
自宅のネットワークは安全にするには:	https://www.sans.org/u/GEL

 Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | **Translated by:** 小山 裕之, 時田　剛