

スマートホームにおける SDN を用いたトラフィック監視による不正アクセス防御手法の検討

A Study on Unauthorized Access Protection Method by Traffic Monitoring Using SDN in Smart Home

塚崎 拓真 / Takuma Tsukasaki

1 はじめに

近年, IoT(Internet of Things) が注目を集めるようになり, 今後あらゆるものがネットワークに接続され, 利用されることが予想される. 現在, IoT 機器が様々なところに置かれるようになり, 以前のパソコンやスマートフォンに限らず, 現在ではテレビやゲーム機, Web カメラ, 冷蔵庫などの家電などがインターネットに繋がり, 情報を通信するようになっている. それに伴い, ネットワーク内には様々な端末や機器が混在することになる. ホームネットワークは情報家電などの普及も加わり, その形態が多様化していくと考えられる.

しかし, IoT の登場で利便性が高まる一方で, これまでのネットワークに接続されていないモノが接続されることにより, セキュリティ上のリスクが高まっている [1]. IoT はセキュリティを考慮せずに開発されたものが多く, 悪意のある攻撃者によるサイバー攻撃の標的になりやすく, 特に不正アクセスが多発している. これらが各種端末やネットワークごとに顕在した場合, 個別に対処するとコストや時間がかかってしまうため, 脅威に対し一括に対処する必要がある. ホームネットワーク内には異なる規格のハードウェアやそれらに搭載される様々なアプリケーションが混在しているため, それら全てに対応したシステムの構築や更新を続けるのは困難である. ホームネットワーク内には異なる規格のハードウェアやそれに対応したソフトウェアとして構築するのではなく, ホームネットワーク内で通信するのであれば, どの端末も必ず利用するネットワークを利用したシステムを構築することが望ましい.

2 関連研究

村上らは, OpenFlow を用いてホームネットワーク内に, 動的な認証システムを構築し, 不正アクセスによる被害を軽減する手法を提案した. 本提案方式では, 認証時に頻繁に利用される情報を用いることで, ネットワークに接続する端末を制限すると共に, 万が一認証が突破された場合でも不正アクセスが検出できるシステムを構築した. しかし, 1 度入られてしまったら, 攻撃されてしまう. 現在のスマートホームデバイスは, クラウド上のシステムと連携す

ることで, デバイス間の連携を可能にしているが, 今後はホームネットワーク内で閉じたデバイス間の通信によって連携を行う形になることが想定される [2]. また, 同じホームネットワークに他の多くの機器が何の制限もなく接続されているという事実を利用して, マルウェアをインストールする. カメラに搭載されたマルウェアは, ローカルネットワーク上で他の潜在的に脆弱なデバイスをスキャンし, 例えばよく知られたセキュリティ上の欠陥を利用してそれらのデバイスにアクセスし, 同じまたは異なるマルウェアのコピーをさらにインストールしようとする. 感染した機器がマルウェアの支配下に置かれると, 個人情報の漏洩など, スマートホームネットワーク自体に被害を及ぼすだけでなく, DDoS 攻撃への加担やサービスの操作など, 他の悪意ある活動を行う可能性がある [3].

2.1 図

図を挿入する場合は, 図 1 や図 2 のように引用することができる. 図の横幅が大きい場合は, 図 2 のようにすることもできる.

ちなみに, L^AT_EX ではベクターファイルとして EPS ファイルを推奨していた頃もあったようだが, 現在は PDF ファイルを使用することが推奨されている. PDF ファイルに出力するのが前提なら, dvipdfmx では PDF, PNG, JPEG がそのまま使用できる. dvipdfmx は EPS ファイルそのものを自分で扱えないので, Ghostscript を内部で呼び出して変換する. PDF ファイルで問題がなければ EPS にこだわる必要はないと思われる. ただし, ジャーナルによっては図として PDF を使うのがダメだったりするので慎重に.

2.2 表

表は表 1 のように引用することができ, 表を作成する場合は罫線を少なくすることと, 横線のみを使用を心がけることが推奨される.

3 研究者にとっての論文十箇条

論文を書くことは大切だ必要だ, と周囲から言われる. それは自分でも分かっているつもりだけれど, その理由をはっきりと伝えてもらえる機会は少ない. 研究者にとっての論文十箇条 [?] は, とてもシンプルでわかりやすく, 非常に心にきた. 一度目を通して見るべきであろう.



図 1 悩む男の子

表 1 代表的なデータの型

データの型	宣言	ビット幅
短整数型	short	16
整数型	int	32
単精度浮動小数点型	float	32
倍精度浮動小数店型	double	64

1. 書かれた論文は書いた人の研究者としての人格を表す
2. データのみ出して論文を書かない者は，テクニシャンである
3. データも出さず，論文（原著論文）を書かない者は，評論家である
4. 研究者は論文を書くことによって成長する．また，成長の糧にしなければならない
5. 論文は研究者の飯のタネである
6. 論文は後世の研究に影響を与えなければならない
7. 研究者は書いた論文に責任を問われる
8. 忙しくて論文が書けないというのは，言い訳にはならず，能力がないといっているのと同じである
9. 博士論文以上の論文を書けない者は，その博士論文は指導教官のものといわれても仕方がない
10. 研究において最も重要なのはアイデアであり，それが試されるのが論文である

参考文献

[1] IoT 推進コンソーシアム, 総務省, 経済産業省, "IoT セキュリティガイドライン ver 1.0", 2016.

[2] C. Vallati, A. Virdis, E. Mingozzi and G. Stea, "Mobile-Edge Computing Come Home Connecting things in future smart homes using LTE device-to-device communications," IEEE Consumer Electronics Magazine, Vol.5, No.4, pp. 77-83, 2016.

[3] M. Serror, M. Henze, S. Hack, M. Schuba, and K. Wehrle, "Towards



図2 ドライブする家族