IoT eラーニング

IoTとセキュリティリスク

（ロボット、ビッグデータ等に関連するセキュリティリスクとその対応）

国立大学法人　琉球大学

目次

IoTデバイスにおけるセキュリティの課題

IoTデバイスにはセキュリティの観点から次の課題がある。

- **コストによるセキュリティ実装への影響**

  IoTデバイスはPCの様な汎用コンピュータではなく、特定の機能を実現した専用コンピュータと捉えることができる。コスト効率を考えるとハードウェアへの制約が課せられることが多くなる。

  ハードウェアに制約が課せられることにより、そのスペックに影響し、結果的にソフトウェアの実装レベルへも影響する。これにより、高度なセキュリティレベルを実装する上で障害となってくる場合がある。

  デバイスで取得したデータを暗号化することなくインターネットへ通信する仕様のIoTデバイスが作られてしまう、といったことがその一例である。

IoTデバイスにおけるセキュリティの課題

- **入手のしやすさが攻撃手段を生む**

  ルーターやインターネットカメラといったIoTデバイスは広く市場に出回っており、簡単に入手することができる。悪意ある利用者がこれらのデバイスを入手し、実物を使って攻撃手法を検討することが可能となる。

  - デバイスを構成するシステムの環境（出荷時のアカウント情報、利用プロトコル等）が分かれば、これらの脆弱性を探し出しハードウェアへの侵入に悪用することができてしまう。

  - また、IoTデバイスは多くのデータをクラウドへ送信・保管する設計となるため、デバイスのなりすましによるクラウドへの不正アクセスのリスクが高まる恐れもある。

IoTデバイスにおけるセキュリティの課題

- **利用するOSの脆弱性の影響**

IoTのデバイスを開発する際に、高度な機能を実現するためにOSを実装して開発する場合がある。

- ルーター等はLinuxを搭載しているものが多くあるが、汎用的な操作を行うPCと比べ、設置した後は利用者が操作することがほとんどない場合が多い。

- このような汎用的な操作を想定していないデバイスの場合、OS関連の脆弱性が狙われる場合が予想される。

次のように大きな被害が発生したLinux OS周りの脆弱性があげられる。

IoTデバイスにおけるセキュリティの課題

- **広くIoT機器に影響するLinuxの脆弱性**

2014年にLinuxのシェルの１つであるBashに存在する脆弱性が公表された（俗にシェルショックと呼ばれている）。Bashは、ほとんどのLinuxディストリビューションで利用されているシェルのため、影響範囲が広く、悪用することが容易であり、また悪用されると被害が大きく深刻な問題である。

IoTデバイスとの関連性の場合、資源が限られる組み込み機器では利用されていないものと考えられていたが、インターネットに接続されたNASが攻撃された事例が確認されている。

公開サーバからIoTデバイスまで幅広く使用されるLinuxに注目が集まることにより、脆弱性の報告も増加してきている。

- 攻撃を行う立場からすると、今後爆発的に増加することが見込まれているIoTデバイスで利用が想定されるLinuxは、脆弱性を突き攻撃に利用できるといえる。

- 逆にセキュリティを守る側の立場からは、Linuxの脆弱性を先に確認・修正することで攻撃の芽をつぶすことが出来るといえる。

IoTデバイスにおけるセキュリティの課題

- **IoTにおける典型的な攻撃**

  - 脆弱な認証
    パスワード認証で保護されていたとしても、パスワードが設定されていなかったりデフォルトのパスワード設定のままであったりと、問題点を突かれる場合がある。
    IoTデバイスに組み込まれたOSやソフトウェアでセキュリティの配慮が欠けていると、これらの点を攻撃され悪用される危険性がある。

  - 暗号鍵の窃盗
    脆弱な認証を突破されてしまうと、セキュリティ対策と利用している暗号化の鍵や電子認証等の情報が盗まれてしまう。
    これらの情報が盗まれてしまうと、侵入されたIoTデバイスだけではなくクラウドなど他への影響を与えてしまう。

  - なりすまし
    脆弱性の対処など問題が発生した場合、ファームウェアなどの更新が必要となってくる。これも攻撃者の標的とされる場合がある。
    インターネットとデバイスの間で暗号化を行わずに通信を行う仕様の場合、本来の接続先とは違う場所を適正な更新サイトと誤認させ悪意あるプログラムをダウンロードさせることが可能である。

IoTデバイスにおけるセキュリティの課題

- **データの流出や悪意ある操作**

ひとたび侵入を許しデバイスの制御を奪われてしまうと、乗っ取ったデバイスを踏み台としてクラウド側への攻撃に利用されてしまう。

- 攻撃が成功してしまうと、クラウド上に収集された貴重なデータの持ち出しや消去などの被害が発生する可能性がある。
- インターネットカメラなどの場合、カメラに映った画像を持ち出される被害も報告されている。
- 人命への被害は報告されていないが、点滴を投与するデバイスも侵入を許し投薬量を変更できてしまうことが報告されている。

IoTデバイスにおけるセキュリティの課題

- **IoTデバイスのセキュリティ対策**

前述のような典型的な攻撃の手段を考慮し、IoTデバイスのセキュリティ対策を考えることが必要となる。

IoTデバイスでは、PCなどの汎用的なコンピュータと異なり、

- 製品のライフサイクルを踏まえたうえでIoTデバイスの機密性や安全性を担保する機能を整える
- 出荷後もセキュリティ対策されたソフトウェアの更新が行える仕組を用意する

などの対策を設計時に吟味し実装する努力が必要である。

IoTを狙った攻撃事例

- **IoTを狙った攻撃の増加**

  IoTが登場してから数多くの製品が発売され、家庭や企業などへの利用が増えてきた。

  利用者がその利便性に気付き利用が増え、IoTメーカーも様々な機能に対応した製品の出荷を増やしており、これらIoTで使用されているデバイスをターゲットとしてセキュリティ侵害が発生するようになった。

  この数年間で、IoTをターゲットとした攻撃が数多く発生しているが、攻撃の頻度が増加傾向を示しているにもかかわらず、IoTの利用や市場の拡大が進んでいる。

  IoTデバイスを狙った攻撃を紹介し、どうすれば対応できるのかを考える材料としたい。

IoTを狙った攻撃事例

- **Stuxnet**

スタックスネット（Stuxnet）は、2010年6月に発見されたWindowsで動作するコンピュータワームである。

- 標的とされたのは、ドイツのシーメンス社が開発した遠隔監視制御・情報取得システムで利用されているプログラマブルロジックコントローラ（PLC）に対するWindows側のインターフェイスソフトウェアである。現在の標準からすれば典型的なIoTデバイスとは言えないがスマートコントローラと考えることが出来る。

- 2010年9月には、イランのナタンズにある核燃料施設のウラン濃縮用遠心分離機が標的とされ、スタックスネットを使ったサイバー攻撃が実施された。この攻撃により遠心分離機のすべてが稼働不能状態に陥ったと言われている。

スタックスネットはWindowsマインにPLCが接続されていることを前提としているので、IoTに対する典型的な攻撃とは言えないが、デバイスがセキュリティ侵害を受ける可能性があることを示している。

この攻撃は、標準的なPCプラットフォームを必要とするデバイスの場合は、必要でない限りWANに接続してはならないことを示している。
また、USBストレージを介して感染が広がった事例が合わせて報告されており、不要な人員は排する等、デバイスへのアクセスの安全性を確保する必要があることを示している。

IoTを狙った攻撃事例

- **Mirai**

Miraiは、Linuxで動作するコンピュータを、ネットワーク攻撃のために遠隔操作できるボットにするマルウェアある。

- 2016年に発見され、ネットワークカメラや家庭用ルーターなど家庭内のIoTデバイスを主要ターゲットとしている。
- その攻撃方法は、乗っ取ったデバイスから攻撃対象に対してDDoS攻撃を仕掛けるもので、感染したデバイスの数が多く、攻撃の対応が出来ずに大規模な被害が発生した。
- Linuxを使用しているデバイスが標的とされ、デフォルトユーザー名とパスワードを変更していない点を悪用した攻撃である。

この攻撃から、IoTデバイスにパスワード設定が行われている場合、すぐにデフォルトのパスワードを変える必要があることが分かる。
ただし、パスワードによっては破られる可能性があるため、Linuxのアップデート等による対応が必要となってくる。

しかし、製造コストを抑えるためにデバイスのストレージ容量を最低限に抑えていることなどにより、アップデートが行えず脆弱なままで使用されている状態が多くある。メーカー側は定期的にアップデートできることを考慮した対応が必要となってくる。

IoTを狙った攻撃事例

- **フィンランドの暖房停止事件**

フィンランドのラッペーンランタの街に２棟のビルがある。このビルはオートメーション化が進んでおり、暖房や水温の管理などをシステムが行っていた。

- 2016年11月、このシステムがDDoSによるサイバー攻撃を受けた。
- この攻撃によりシステムがダウンし、暖房が使えない状態になった。
- フィンランドの冬で暖房が使えないことは重大な問題となった。

この攻撃から、DDoSなどの攻撃を受けていないか定期的にネットワークを監視し、疑わしき兆候が現れたら対応を直ちに行うことが必要であることを示している。

IoTを狙った攻撃事例

- **Brickerbot**

  この攻撃は、Miraiとほぼ同じ方法でIoTデバイスへ感染する。

  - Brickerbotは、感染後にデバイスのストレージを破壊するなどのIoTデバイスそのものへの破壊行為を行う。この点がMiraiとの違いである。

  - もし大量に導入したIoTデバイスがこの攻撃を受けた場合、攻撃を受けたIoTデバイスは使用不能となってしまうため、企業の業績に重大な結果を引き起こす可能性がある。

  Miraiと同様に、デバイスのデフォルトのユーザー名／パスワードは直ちに変更しておく必要があることを示している。

IoTを狙った攻撃事例

- **攻撃への最低限の対策**

これらの事例から、IoTデバイス開発メーカーは、

- 出荷するIoTデバイスに対して最新のOSとファームウェアを搭載する
- 新たに脆弱性が発見されることを想定し定期的にアップデートできる仕組みを整える

などの対応が必要である。

利用者は、

- ネットワークを監視し、疑わしい兆候が現れたら対応できる運用体制を整えておく
- デバイスを導入した際にデフォルトパスワードを必ず変更する

などの対処も必要である。

IoTデバイスのセキュリティ対策

IoTデバイスに対する攻撃は増加し手法も様々な方法となってきている。
そのため、IoTデバイスのセキュリティ対策でも様々な方法を考慮しておく必要がある。

そこで、IoTデバイスの動きを段階的に分けてセキュリティ設計を行い、対応を進めていくことが必要であると考える。

１．デバイスの起動

デバイスは起動するとファームウェアをロードし定義されたとおりに動き始める。
そのため、この段階ではファームウェアが改ざんされていないかの確認が必要である。

- 改ざんの確認
  ファームウェアが改ざんされていないか確認する仕組みを整え（セキュアなパスワードを設定しておく等）問題がないかチェックを行う。

2．デバイスの初期化

起動処理が完了すると、接続機器との接続を行いデータの同期などの初期化処理が行われる。この段階で、運用時に使用する情報の安全性を確保しておく必要がある。

- セキュアなパスワードの保証
  IoTデバイスの認証に使用するアカウントのパスワードが初期設定のままであることは避けるべきである。デバイス導入段階で行われる初期設定時にパスワードの変更を利用者に求めるなどの仕組みを整え、パスワードがデフォルトのまま使用されていないことを保証する。

- 暗号／認証で使用する鍵の保護
  データ送信時などに暗号化で使用する鍵が、安全な方法で保管されており第三者による窃盗などが行えない仕組みを整えておく。

- 通信の保護
  IoTデバイスから各接続先（他のデバイス、インターネット等）との通信で使用するプロトコルを用途に合わせて選択（SSL等）し、保護された通信環境を整えておく。

3．デバイスの運用

初期化が終了すると、センサーで計測したデータをクラウドへ送信する等の企画された目的に合わせた動作を継続的に実行せれる。
この段階では、IoTデバイスの動作が安全に実施されることを配慮する必要がある。

- アカウントの保護
  運用に不要なアカウントを削除し、不正な侵入の芽を摘んでおく必要がある。
  また、運用中に他のシステムとの連携で新たに作成されるアカウントについても認証による保護などが図られるよう仕組みを整えておく。

- デバイスの異常監視
  デバイスが異常動作していないか状態を監視し、異常が見つかった場合は利用者に警告を通知する仕組みを整えておく。

- アップデート
  デバイスの脆弱性が見つかった場合、攻撃を阻止するためにもファームウェアの更新が必要となってくる。ただし、この行為も攻撃の対象となってくるため、侵入防止システムやホワイトリスト等のセキュリティ対策を合わせて実装できる仕組みを整えておく。

現在の対策動向

- **SDN/NFV技術による対策**

インターネットイニシアティブは2017年10月30日、SDN（Software Defined Networking）とNFV（Network Function Virtualization）技術を利用し、脅威を早期に検知し隔離することでオフィスネットワークへの拡散を防止する実証実験を実施すると発表した。

実証実験の流れは、

- ユーザーが利用するPCやIoTデバイスなどからオフィスネットワーク内にセキュリティ脅威が侵入すると、クラウド上の侵入検知システムがそれを発見する。
- その動きを監視し、不正と判断された場合にSDNの機能で動きを遮断し脅威を隔離する。

※不正アクセスの侵入検知などのセキュリティ機能はトレンドマイクロのNFV向けネットワークセキュリティ技術「Trend Micro Security VNF」を使用する。

現在の対策動向

● 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）は、IoTシステムに関する脅威分析と対策検討の実施例を開設した「IoT開発におけるセキュリティ設計の手引き」を公開した。

IPAではIoTの定義を次の５つの構成要素に分類し、IPAのIoTモデルを設定している。
- ◆ サービス提供サーバ・クラウド
- ◆ 中継機器
- ◆ システム
- ◆ デバイス
- ◆ 直接相互通信するデバイス

そのうえで、それぞれの構成要素における課題の抽出と整理を行った。

また、次の４分野を具体的なIoTシステム事例として、脅威の分析と対策検討の実施例を図解を交えて解説している。
- ◆ デジタルテレビ
- ◆ ヘルスケア機器とクラウドサービス
- ◆ スマートハウス
- ◆ コネクテッドカー

暗号技術に関して、実装した際の安全性を客観的に確認するためのチェックリストを付録として作成し、合わせて公開している。開発者は、これを利用することで暗号技術の利用・運用方針の明確化と、安全性の評価が容易に行えるとしている。