IoT eラーニング

IoTとセキュリティ

（IoTに関するセキュリティ技術の概要）

国立大学法人　琉球大学

目次

IoTにおけるセキュリティの重要性

- **IoTのセキュリティ**

IoTが広く認知されるようになり、活用される場所も広がり続けている。

家電やオフィス機器・自動車・工場の制御用システム・医療機器等、あらゆる分野であらゆるモノがインターネットにつながるようになってきた。

IoTは、これらの機器から集められた情報をもとに、業務の効率化から新しいビジネスモデルの創造まで可能性を広げている。

しかし、セキュリティ面での懸念が増してきている。

IoT機器の数は、2020年に全世界で数百億に達すると言われており、セキュリティを考慮しなければならない数も大幅に範囲が広がる。また、IoTデバイスが抱える課題もありセキュリティ対策に影響を与えている。

IoTにおけるセキュリティの重要性

- **市場調査で見えた課題**

IoT機器に対して、ある市場調査が行われた。この調査で次のような結果が示された。

- パスワードの脆弱性
  80%のIoT機器が、パスワードの複雑さや文字列長を十分満たしていない
  70%のIoT機器が、パスワードを見破られる可能性がある

- 暗号化対策の不備
  70%のIoT機器が、暗号化対策の行われていないネットワーク上でデータを送受信している

- 個人情報の所持
  90%のIoT機器が、IoTサービスにより他の機器やアプリケーションにつながることで１つ以上の個人情報を所持している

- Webインタフェース
  60%のIoT機器が、外部からの攻撃や認証方法などで、脆弱なWebインタフェースを持っている

IoTにおけるセキュリティの重要性

- **IoTのセキュリティリスクポイント**

  - IoT機器の入手のしやすさによる影響

    IoT機器は、家庭やオフィスにも広く浸透し、個人でもその機器を入手しやすい状態になっている。
    誰もがIoTに触れられることが成長につながる一方、機器を入手し様々な攻撃手法を実際に試すことができる環境が作りやすい状況にある。

  - IoT機器を構成するソフトウェア

    IoT機器を開発する際に、機器にOSを搭載し機能を実装する場合がある。
    このOSに脆弱性が潜んでおり、対策を施さないままネットワークに繋がれてしまうと攻撃の侵入口として狙われる可能性がある。
    また、新たに脆弱性が発見された場合の対策をどうするのか等、機器の使われる状況によって影響してくる。

IoTにおけるセキュリティの重要性

● セキュリティの分類

IoTのセキュリティを考える上で、一般的なセキュリティの考え方を適用することができる。

一般的にセキュリティは、物理セキュリティと論理セキュリティに分けられる。

- 物理セキュリティ
  建物や設備の防犯や防災など。
  データが安全に保存されるためのバックアップ。安定稼働するための電源供給や通信環境。これらをセキュリティの対象としている。

- 論理セキュリティ
  論理セキュリティはシステムセキュリティと人的セキュリティとに分けられる。
  システムセキュリティは、認証や暗号化、アクセス制御などシステムを対象とする。
  人的セキュリティは、セキュリティ対策に取り組む体制作りや人材の育成などを対象とする。

IoTにおけるセキュリティの重要性

● セキュリティの要件

セキュリティには、機密性、完全性、可用性の三大要件がある。

企業で活用されている情報システムでは一般的に機密性が重視されるが、IoTは利用状況によっては可用性が最優先される場合がある。
電力等のエネルギー、鉄道等のインフラといった制御システムは、稼働率が下がると生産性やサービスの低下につながり収益や人命などに影響する危険がある。

- 機密性
  情報に対して許可されたもの以外アクセスできなくすること。
  またアクセスできる範囲も制限すること。外部への情報漏洩を防止する。
  技術的には認証や暗号化、アクセス権の設定が利用される。

- 完全性
  情報が改ざんや破壊されないこと。情報の正確性を保証すること。
  技術的にはハッシュ関数やデジタル署名などで、改ざんの検知に利用される。

- 可用性
  情報やシステムなどが、必要とするときに中断することなくアクセスできること。
  技術的には電源対策や機器またはシステムの二重化が利用される。

IoTの脆弱性

- **IoTに対する攻撃**

IoT機器はセンサーなどから得た情報を、インターネットを経由してクラウドなどのホストに送っている。

そのため、機器を構成するハードウェアなどの制御のためOSを実装している場合がある。このOSに脆弱性があるとサイバー攻撃に利用されてしまう。
また、OSなどは、違う構成のIoT機器でも共通して利用される場合もあるため、脆弱性が見つかると影響範囲は膨大な量に広がると考えられる。

IoTでは機器を設置している場所がIoTのサービスの種類により、ネットワーク的にも物理的にもアクセスしずらい場所に設置されていることがある。そのため、脆弱性が見つかりかりアップデートなど対策を施そうとしてもパソコンのように手早く済ませることができないことが考えられる。

IoTが普及する前からサイバー攻撃は行われている。IoTもその攻撃にさらされ攻撃を受ける可能性があり、実際に被害を受けた事例も発生している。

サイバー攻撃の手法

● ネットワークスキャン

サイバー攻撃を行う上で、攻撃対象のネットワーク情報の収集が最初に行われる。

ネットワークに接続している機器の製品名、IPアドレス、使用または提供されているサービスなどを特定することをネットワークスキャンという。

また、ポートスキャンという攻撃があり、攻撃対象となるホストの通信可能なポートを探り出し、システムの内容を確認する攻撃である。ポートに対するセキュリティが十分に施されていないと、不正アクセスに利用されシステムへ攻撃が行われる。

組み込みLinuxなどが利用されたIoT機器（ルーターやWebカメラ等）でネットワークスキャンによって、セキュリティホールを見破られ不正アクセスの攻撃を受けた事例がある。

対策としては、
◆ ファイアーウォールのフィルタリングによる特定のサービスのみ許可する
◆ 脆弱性が発見された場合にセキュリティパッチを施す
などがある。

サイバー攻撃の手法

- **パスワードクラック**

ネットワークスキャンなどにより攻撃対象となるホストを特定すると、次の攻撃としてOSやアプリケーションのパスワードを特定しホストへの侵入を試みる。

このパスワードを特定する行為をパスワードクラックという。

代表的な手法にブルートフォースアタックがある。
この攻撃は総当たり攻撃とも呼ばれ、使われる文字の組み合わせを全て試す方法である。
パスワードの文字列長が短く文字の種類も少ないと特定される危険性がある。

この攻撃の他に登録しがちなパスワードを予め辞書として用意しそれを利用する攻撃もある。

インターネットに接続されたWebカメラなどが、この攻撃によりシステムへの侵入を許し第三者に映像が流出してしまうという事例が発生している。
IoT機器に施すパスワードを含め、パスワードの使い回しや管理・運用などの対策が必要となってくる。

サイバー攻撃の手法

- **バッファオーバーフロー**

IoT機器を開発する際に、組み込みソフトウェアとしてC／C++が利用されているケースが多い。

C／C++ではプログラム実行中のデータを保存するために、メモリ上にまとまった領域を確保し利用している。この領域をバッファと呼んでいる。バッファのサイズを超えるデータが入力されるとバッファオーバーフローという事象が発生する。

入力値チェックなどで十分に対策が施されていないと最悪の場合、システムがフリーズしてしまう恐れがある。

IoT機器についても、入力値をネットワークなどの外部から取り込む際に対策が施されていないと悪意あるデータの入力によりフリーズさせる攻撃を受ける可能性がある。
開発時の注意はもちろん、不具合が見つかった場合のセキュリティパッチの適用などの対策が必要となる。

サイバー攻撃の手法

● マルウェア

マルウェアとは、ワーム、トロイの木馬、ボットなどを総称する呼び方で、コンピュータがこれに感染すると、利用者の意図とは違う動作やデータの改ざんや破壊、外部からの遠隔操作といった攻撃を受け、深刻な被害を受ける。

典型的な手法としては、メールへのマルウェアの添付や取引先などを装って不正URLへ誘導するなどで感染させる手法がある。一旦感染すると、情報の漏洩など重大な被害を受けることになる。

- ワーム
  自己増殖し、潜入／潜伏機能と遠隔操作や改ざん／破壊攻撃を行う発病機能をもつ。

- トロイの木馬
  一見正常なプログラムに見せるよう装いながら、密かに攻撃を行う。

- ボット
  感染した機器をネットワーク越しに遠隔操作されたり、他の機器への攻撃に利用されたりするなど被害者だけではなく加害者にもなる攻撃を行う。

サイバー攻撃の手法

- **DoS**

システムの可用性に対する攻撃を行う。

ウェブサービスなどに対して処理しきれないほどの量のリクエストや巨大なデータを送り付けるなどしてサービスの利用を不能にする攻撃である。

この攻撃を受けると、
◆ ネットワークトラフィックの増大による遅延
◆ サーバやウェブサイトへなどへのアクセスが行えなくなる
などの障害が発生する。

大量のマシンから１つのサービスに対して一斉にDoS攻撃を仕掛けることをDDoS攻撃と呼ぶ。

この攻撃はボットに感染した機器を踏み台として利用し、それらから一斉に攻撃対象を攻撃する手法と、何らかの方法で攻撃対象を装い、大量のマシンにリクエストを要求し応答を一斉に返答させることにより攻撃対象を攻撃する手法がある。

IoT機器なども攻撃対象となると機器の停止による影響を受けることとなる。

セキュリティ対策手法

- **セキュリティ対策**

IoTでは、提供するサービスを充実するために、多様で膨大な量の機器の接続を行う。

そのため、特定の機器に脆弱性があるだけで、実際に攻撃を受けるだけでなく不具合対策などでシステム全体への影響を与えることになる。

IoTサービスの提供者は、外部からの侵入を防ぐだけでなく、脆弱性の発見／侵入による攻撃があった場合に被害や影響を最小限に抑えるための対策をしておくことも重要である。

対策としては、認証などによる技術的なものと合わせ、IoT開発時からセキュリティ対策設計を行うことが必要である。

セキュリティ対策手法

- **パスワード認証**

IDとパスワードによる認証は実装が簡単なため、多くのシステムで利用されている。

パスワードは
◆ 第三者に特定されないよう、単純なパスワードは使用しない
◆ 定期的にパスワードを変更する
などの対策が必要である。

IoT機器ではOSが実装されている場合など、パスワード認証を運用する際に注意が必要である。

最低でも、デフォルトのパスワードを変更しておく、不要となったログインID は削除しておくなどの対策が必要である。

セキュリティ対策手法

- **生体認証**

生体認証は、指紋や虹彩、静脈パターンなどの身体的な特徴を鍵とする認証方法である。偽造が難しく紛失しないなどの特徴がある。

利用方法として、オンラインサービスを受ける際に、生体認証機器を使うことでパスワードを必要としない運用などがある。

しかし、鍵として使用した部位に加齢や怪我などにより変化があると、たとえ本人であっても認証されない場合がある。その場合、鍵の変更はできないので、2度と利用できなくなる可能性がある。

虹彩など加齢の影響を受けない部位を使うなどの対策を考慮しておく必要がある。

セキュリティ対策手法

● 暗号化

暗号化とは、データを任意の方法で変換し、容易に内容を解析できないようにすることである。

暗号化はデータを暗号化する際と元に戻す復号の際に鍵を利用している。
この鍵を第三者から守ることにより、暗号化したデータを入手されたとしても、復号できないようにする。
鍵を利用した暗号化には、共通鍵方式と公開鍵方式がある。

- 共通鍵
  共通鍵方式は、暗号化と復号化を同じ鍵で行う方式である。この方式は簡単な原理なため実装しやすく広く使われているが、この鍵をどのように受信者へ安全に届けるかが問題となる。

- 公開鍵
  公開鍵方式は、暗号化と復号化でそれぞれ鍵を用意し、暗号化用の鍵を公開し復号化用の鍵は秘密にしておく方式である。利用方法としては、データを送信したい人が、送信先（受信者）の公開鍵を使い暗号化し送信する。受信者は自身の復号化用の鍵を使い復号する。
  共通鍵のように暗号化の際に使用した鍵を伝える必要もなく、受け取った鍵も厳重に保管しておく必要もない。

セキュリティ対策手法

- **デジタル署名**

デジタル署名は、公開鍵暗号方式とハッシュ関数を使い、改ざんされていないかを確認する方式である。

- ハッシュ関数
  「改ざんされていないか」の確認に使用する。
  送信者は送付したいデータをハッシュ関数を使用しハッシュ値を求める。このハッシュ値を公開鍵暗号方式で送信する。受信者は送られてきたデータのハッシュ値を求め、送られてきたハッシュ値と比較し一致するかを照合する。

- 公開鍵暗号方式
  「誰から送られてきたのか」の確認に使用する。
  送信者は自身の秘密鍵で暗号化したハッシュ値を送付する。受信者は送信者の公開鍵で復号しハッシュ値を取り出す。送られてきたデータのハッシュ値と照合し一致すれば、改ざんされることなく送信者から送信されてきたと判断できる。

セキュリティ対策手法

- **セキュリティプロトコル**

  WebサーバとWebブラウザ間での通信に、HTTPプロトコルとHTTPSプロトコルがある。

  それぞれ、
  ◆ HTTPプロトコルではデータを平文で送信する
  ◆ HTTPSプロトコルではSSL認証を用いた暗号化を行って送信する。
  という違いがある。

  このように、セキュリティプロトコルを使用することでネットワーク上の安全性を確保する方式である。

セキュリティ対策手法

- **セキュリティ設計**

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解説した「IoT開発におけるセキュリティ設計の手引き」を公開している。

これにはIoTを構成する要素の分類分けと、課題の抽出と整理が行われており、脅威の分析と対策検討の実施例を解説している。

この手引きを活用するなどし、IoTを設計する段階から脅威に対する分析と対策を検討・実装しておくことで安全性の高いシステムを構築する必要がある。