IoT eラーニング

IoTとネットワークセキュリティ

（IoTで活用されるネットワークセキュリティ技術）

国立大学法人　琉球大学

目次

ネットワークセキュリティ対策

● IoTセキュリティへの懸念

IoTによる可能性が様々な人達に認識されるようになるにつれ、家電やオフィス機器、自動車、工場の制御システム等、あらゆるものがインターネットに繋がり多くのサービスが提供されるようになった。

IoTから得られたデータやサービスの活用により業務の効率化や新規ビジネスの創造などの可能性がある一方、セキュリティの面で懸念が広がり始めている。

IoTを構成するデバイスは2020年に世界で数百億個に達するといわれており、セキュリティを考慮しなければならない範囲が大幅な広がりを示している。

ある市場調査では
- 約８割のデバイスで使用されているパスワード長が不十分
- 約７割のデバイスで使用されているパスワードが脆弱（見破られる可能性）
- 約９割のデバイスが何らかの個人情報を保有
- 約７割のデバイスが非暗号化ネットワークを使用

という結果が出ている。

IoTデータとリスク

IoTで扱われている情報の中には、
- 監視カメラの映像
- 電気・ガスの使用量
- 車両のプローブ情報

など利用者の行動を類推することが可能な情報が多数あり、IoTサービス提供者が情報漏洩などの問題を起こしてしまうと、サービス提供の廃止などの信用を大きく損なう事態が考えられる。

また、工場の制御システムや病院の医療機器などと連携したIoTデバイスに対してサイバー攻撃を受け正常な稼働が出来なくなると重大な事態を引き起こされる可能性も考えられる。

そのため、IoTに対するセキュリティ対応は必須の課題である。

ネットワークセキュリティ対策

- **モノと情報のセキュリティ**

  従来から、家電製品や車などのモノ（デバイス）を開発する際に、誤動作や事故による人や環境への被害を与えないようなセキュリティ対策が配慮されている。

  一方、銀行システムやSNSなどの情報システムを開発する際には、安定的に継続してサービスが提供できることを保証する品質やデータ漏洩などのセキュリティ対策が配慮されている。

  IoTではモノ（デバイス）と情報システムが連携してサービスを提供するため、セキュリティ対策において両分野における開発者の協力関係が必要になってくる。

ネットワークセキュリティ対策

- **被害の実例**

2010年にStuxnetというコンピュータワームによる被害が発生した。

標的にされたのはドイツのシーメンス社製のシステムで、イランの核燃料施設を制御不能に陥れた。ネットワークを経由し感染後も、人の脆弱性を突きUSBメモリでさらに感染を広げていった。

また、2016年にMiriaというボットネットによる被害が発生した。

標的にされたのはインターネットに接続されたLinuxを搭載したIoTデバイス（ルーターやネットワークカメラ等）で、侵入されてしまうとDDoS攻撃の端末として利用されてしまった。IoTデバイスのOSとして利用されていたLinuxのユーザーIDやパスワードがデフォルトのまま使用されていたことを突いた攻撃だった。
DDoS攻撃の対象とされたしまったシステムは膨大な数のIoTデバイスからの攻撃に耐えられず、システム障害を起こし深刻な影響を受けた。

ネットワークセキュリティ対策

● ネットワークセキュリティ対策の必要性

Stuxnet／Miraiのように、既にIoTを狙ったサイバー攻撃は始まっており、IoTのセキュリティ対策は喫緊の課題である。

Stuxnet／Miraiでは
- 人の脆弱性（USBメモリ）
- デバイスの脆弱性（ユーザーID・パスワードがデフォルトのまま）

で被害を拡大させていたが、侵入経路の中にはネットワークによるものがあり、ネットワークに対するセキュリティも重要な対策の一つであると言える。

ネットワークを「監視」し、確認できた動向の中から不正な動きを「検知」し、知りえた情報から「対応」をとることにより、ネットワーク経由のサイバー攻撃に対する被害の防止や被害範囲の縮小が図れると言える。

ネットワーク攻撃に関する実例

- **Reaper**

2017年10月19日、IoT機器を狙う「Reaper」が確認された。

100万に及ぶ法人ネットワークに感染し、感染の拡大は続いている。
Reaperを確認したセキュリティ企業によると、Reaperで構成されるIoTボットネットは、2016年末に確認されたIoT機器（Linux搭載）を狙う「Mirai」よりも巧妙で潜在的な危険度も高い。
ReaperはMiraiのソースの一部を利用しているが、感染する手法は異なる。

Mirai は開放されているポートスキャンするか、初期設定または弱いパスワードを使用するセキュリティ上の脆弱な機器を利用して拡散する。
一方Reaperは、特定のIoT機器を狙うのではなく、広く利用されている多くのルータを対象としている。既に数百万台のIoT機器がReaperに感染している。

MiraiはDDoSを実行することが既に周知されている。
一方、Reaperによる DDoS 攻撃は、まだ確認されていない。しかし、Reaperは、より複雑な攻撃を実行する能力を備えている。今後Miraiよりも大規模な被害が及ぼされる可能性がある。

ネットワーク攻撃に関する実例

- **「Mirai」の新しい亜種**

「Mirai」の新しい亜種が急速に拡散している。

2017年11月22日に確認された2323番および23番ポートへのトラフィックが急増したのは、Miraiの亜種による攻撃と確認された。

既に南米や北アフリカに拡散しており、アルゼンチンに加え、コロンビア、エクアドル、パナマ、エジプト、チュニジアで Mirai による攻撃活動の急増が確認されている。

利用された認証情報から、ネットワークカメラ、デジタル・ビデオ・レコーダー、ネットワーク・ビデオ・レコーダー、モデムなどのさまざまな機器が攻撃対象となっている。
機器の製造業者にはZyXELやDahuaなどが含まれる。

ネットワーク攻撃に関する実例

- **BrickerBot**

IoT機器を攻撃する新しいマルウェア「BrickerBot」が確認された。

報告によると、その攻撃経路はMiraiに類似している。
Miraiは感染IoT機器をボット化するが、BrickerBotはIoT機器を完全に使用不能とするのが特徴である。

Miraiと同様に、BrickerBotは初期設定のアカウントとパスワードを利用した総当り攻撃によって機器に接続する。

他のIoT機器を狙うマルウェアとは違い、BrickerBot の場合は
◆ IoT機器の動作速度を低下させる
◆ ファイルを削除する
などの不正なLinuxコマンドを実行することにより機器に致命的な改変を加え、最終的には使用不能にする。

脅威への対応

- **脅威の可視化**

セキュリティ対策を考える上で必要となるのは、対象となるシステムがどのような環境に構築され利用されているのかを把握することである。

- どのようなデバイスやコンピュータが存在し配置されているのか
- それぞれはどのように接続されてネットワークを構成しているのか
- データ通信の頻度や内容やプロトコルには何を使っているのか

が見えてくることにより、脅威の影響はどのように始まり広がっていくのかも見えてくる。

これらをもとに、様々な情報の中から何を収集し蓄積しておく必要があるのかを検討・実装することにより脅威を検知するための情報を得られるようにしておく必要がある。

脅威への対応

- **脅威の検知**

  脅威の可視化で集められた情報を監視することにより、異常な動向を示しているポイントを見つけ出し対応を行う事が可能となる。

  この作業がいかに早く行えるかが影響の広がる範囲を抑えるポイントとなる。

  しかし、IoTの広がりとともに、使用されるデバイスとそこから出力されるデータは膨大な量となってきており人が判断できる限界を超えることが考えられる。

  AI技術を活用し脅威と捉えるべき動向を学習させ、AIで一次検知を行い人はその中から対応を必要とする脅威を検知する、等の対策を検討する必要があると思われる。

● 脅威への対応

ネットワーク上で異常なふるまいを検知したならば、迅速に対応し被害の影響を少しでも抑える必要がある。

ただし、システムが提供しているサービスに影響をできるだけ与えないことも必要である。

そこで、どこでネットワークを遮断し、どこまでをその範囲とすれば影響が少ないのかを事前に検討しておく必要がある。

また、利用者への影響が考えられる場合は、どのように通知し対処してもらうのかも事前に検討しておく必要がなる。

システムの運用を進めていく中でシステムに脆弱なポイントが見つかったならば、迅速に対応しサイバー攻撃の回避を図る必要がある。そのためには、迅速に対応が行える体制を整えておくことと、改修したモジュールを配布・更新できる仕組みを考えておく必要がある。
但し、IoTデバイスが改修の対象となった場合、設置されている数や場所により配布・更新が難しい場合が考えられる。
その場合、配布・更新が難しいデバイスについてはライフサイクル期間を短縮し、デバイスの更新時に改修が反映されたデバイスを設置するなどの検討も考えておく必要があるだろう。

企業による対策サービスの提供

- **大日本印刷株式会社（DNP）**

大日本印刷株式会社（DNP）では、IoT機器との接続に簡単な設定でセキュアで多彩なネットワークの構築を可能としている「DNP Multi-Peer VPN」を提供している。

「DNP Multi-Peer VPN」は、DNP独自の技術で中継サーバを経由せずにスマートフォンやタブレット端末などの多数の機器の間で同時にインターネットVPNを構築することができる。

一般的なインターネットVPNと DNP Multi-Peer VPN の特徴は次のようになる。

- 一般的なインターネットVPN
  - インターネットにVPN機器を接続して構築する
  - VPN装置の購入と複雑な設定を必要とする
  - ネットワークの構成変更や拠点増加の度に設定作業が発生する

- DNP Multi-Peer VPN
  - インターネット上で通信機器同士によるVPN通信が可能
  - 通信経路の機器に設定は不要
  - 導入時のハード購入は不要
  - VPN通信機能を搭載したアプリケーションや機器向けにSDKを提供

企業による対策サービスの提供

- **BBソフトサービス株式会社**

BBソフトサービス株式会社では「Bitdefender BOX」を提供している。
家庭に浸透しているIoT機器を想定し、家庭内のネットワーク全体を保護することを目的としている。

提供される形態はルーターに接続する箱型のハードウェア（BOX）とセキュリティソフトで提供される。接続するとネットワーク上のデバイスを検知し保護の対象とする。BOXのコントロールはiOS／Android端末のモバイルアプリで行われる。

Bitdefender BOXの特徴は、
◆ 家庭内ネットワークに接続されている機器の「見える化」
◆ セキュリティ機能を搭載していない無防備な機器も保護できる
◆ PC／モバイル用セキュリティソフトが付属し台数無制限

ホームネットワークの入り口であるルーターでセキュリティ対策を施し、ネットワークセキュリティの安全性を確保している。

企業による対策サービスの提供

- **アラクサラネットワークス株式会社**

アラクサラネットワークス株式会社（AlaxalA）はルータ、スイッチを開発・製造・販売している。IoT機器に対するセキュリティ課題に対応するための対策を提案している。

- ホワイトリスト機能
  ネットワークを構成するスイッチに、通過を許可する通信フローをホワイトリストにして事前に登録する。運用中はそれ以外の通信をすべてスイッチの段階で遮断する。登録された通信フロー以外は通さないので、工場やビル、病院の監視カメラなど、特定用途のネットワークのセキュリティ対策に最適である。

- ポリシーベースミラーリング機能
  脅威の挙動を “見える化”するためには、ネットワーク内の通信を監視するセキュリティ機器の導入を必要とするが、その際ネックとなるのがコスト面である。
  ポリシーベースミラーリング機能は、各通信フローの中から必要な部分を抽出、ミラーリングすることを可能としている。通信フローすべてを検査する必要がないため、無理に高性能なセキュリティ機器を導入する必要がなく、コストを抑えることができる。

企業による対策サービスの提供

- **Rapid7**

  アメリカRapid7の日本法人であるラピッドセブン・ジャパンは2017年5月16日に、車載デバイスなどのIoTシステムを対象としたセキュリティサービスを開始すると発表した。脅威のモデル化と各開発・テスト段階でのセキュリティ面から見た支援を包括的に提供する。

  Rapid7が開発しているオープンソースソフトウエアで、サイバー攻撃者の視点から見たシステムの脆弱性を調査する侵入テストツール「Metasploit Framework」を使う。
  もともとはWebアプリケーションなど、一般的な情報システムを対象にしたテストツールであるが、IoT機器をテストするための機能を2017年2月に追加した。

  Metasploit Frameworkの機能強化では、車載ネットワークや無線通信など、これまでセキュリティが考慮されてこなかった領域を対象に、ソフトウェア組み込み機器の脆弱性をテストできるようにした。

  Metasploit Frameworkがインストールされたパソコンから、ゲートウェイなどを介して機器を直接テストする。

情報セキュリティマネジメント試験

- **概要**

情報セキュリティをいかに確保するかは大きな課題であるが、多種多様な攻撃方法による脅威は、技術的な対策だけでなく、組織の在り方や利用者の意識向上など人による対策も重要となってくる。そのための情報セキュリティマネジメントを担う人材をいかに育成し進めて行くかが、社会全体の課題ともいえる。

このような社会のニーズの高まりにより、国家試験「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が創設された。

「情報セキュリティマネジメント試験」とは次のような組織作りに欠かせない情報セキュリティマネジメントの人材を認定する試験である。

◆ 部門全体の情報セキュリティ意識の向上、組織における情報漏えいリスクを抑える
◆ 万が一問題が発生しても、適切な事後対応により最小限の被害にとどめる
◆ 情報セキュリティ確保を推進し、安全で積極的なIT利活用の環境を実現する

情報セキュリティマネジメント試験

- **試験内容**

「情報セキュリティマネジメント試験」の試験実施日や試験内容などは次のようになる。

- 試験実施日
  春季：4月第3日曜日／秋季：10月第3日曜日

- 試験内容
  午前と午後の90分間で多肢選択式の出題形式

- 問われる知識
  - ◆ 情報セキュリティ全般
    機密性・完全性・可用性、脅威、脆弱性、攻撃手法、暗号、認証 など
  - ◆ 情報セキュリティ管理
    情報資産、リスク、インシデント管理などの各種管理策 など
  - ◆ 情報セキュリティ対策
    マルウェア対策、不正アクセス対策、情報漏えい対策、情報セキュリティ啓発 など
  - ◆ 情報セキュリティ関連法規
    サイバーセキュリティ基本法、個人情報保護法、不正アクセス禁止法 など