IoTとセキュリティ

株式会社セキュアサイクル
代表取締役　服部祐一

プロフィール

名前

服部 祐一

株式会社 セキュアサイクル
代表取締役

所属・役職

- OWASP Fukuoka チャプターリーダー
- SecHack365 研究駆動コーストレーナー
- 北九州情報セキュリティ勉強会「セキュ鉄」代表 等

経歴

九州工業大学卒。在学時はスマートフォンを使った行動認識の研究に携わり、
Microsoft Research AsiaにてResearch Internshipとして行動認識の研究に従事。
その後、ベンチャー企業でチーフエンジニアとして新規Webサービスの開発や脆弱性診断の経験後、
情報セキュリティ専門会社のCTOを経て現在に至る。
各地のセキュリティ関連イベントや、企業、大学等での講演・トレーニング多数。
現在も脆弱新診断や開発時のセキュリティ対策のコンサルなどの実務にも携わる。

会社概要

会社名	株式会社セキュアサイクル (Secure Cycle Inc.)
代表	服部 祐一
従業員	26名（役員・アルバイト含む）
所在地	**本社** 〒808-0138 福岡県北九州市若松区ひびきの北8-1 技術開発交流センター **仙台支社** 〒980-0803 宮城県仙台市青葉区国分町1-4-9 enspace内

設立	2017年06月19日
資本金	1000万円
事業内容	情報セキュリティの各種診断・対応 情報セキュリティのセミナー、コンサルティング 情報システムの設計・開発・研究・運営 システム開発のセミナー、コンサルティング
顧問弁護士	光雲法律事務所　吉井 和明
加盟団体	一般社団法人九州経済連合会 特定非営利活動法人日本ネットワークセキュリティ協会 IOT INNOVATION Base 公益社団法人 福岡貿易会

システム開発におけるセキュリティ対策を当たり前のものに

「システム開発におけるセキュリティ対策を当たり前のもの に」という理念のもとに、自社でのシステム開発、研究開発に おける製品に情報セキュリティ対策を行い安心安全な製品を提 供。情報セキュリティ部門においても開発を経験したエンジニ アが脆弱性診断等に従事しており、

開発者目線での助言などを行っています。また、契約内容に よってはコードレビューや新規機能作成時のセキュリティ面か らの助言といった開発段階での参画も可能です。

セキュリティサービス一覧

名称	概要
Webアプリケーション脆弱性診断	ECサイトや社内システム、コーポレートサイトなどの脆弱性診断
API脆弱性診断	シングルページアプリケーションやスマホアプリで用いるAPIなどの脆弱性診断
プラットフォーム診断	アプリケーションを設置するサーバや社内に設置してある ネットワーク機器などの脆弱性診断
スマホアプリ脆弱性診断	個人情報を取り扱うアプリやクーポン機能などの 悪用されると被害が発生する可能性があるアプリなどの脆弱性診断
セキュリティコンサルティング	ウイルス対策ソフトの選定や企業規模に応じた適切なセキュリティ対策のご提案や、自社開発のアプリケーションの扱うデータの内容等に応じたセキュリティ対策に対するご提案など
研修・講演	脆弱性診断に関する研修や各種セキュリティに関する講演、 情報セキュリティ競技の運営など

システム開発・研究開発

名称	概要
システム開発	工場向け在庫管理システムや営業所向け顧客管理システム、生産管理システム、ベンチャー企業様の独自サービスなどのシステム開発
研究開発	国の研究機関や大学などから委託を受けて行う調査や 研究用途のシステム開発、新規事業の検証用のシステム開発など

IoTとは

IoTとは、Internet Of Thingsの略で、日本語ではモノのインターネットと呼ばれています。

様々なものがインターネットにに接続されることにより、今までインターネットに接続されていなかった鍵や温度計、カメラ、スピーカーといったものがインターネットを介して相互に情報交換する仕組みです。

これらがインターネットに接続されることにより様々なセンサーのデータの分析や、機器との連携を実現することが可能になります。

代表的なIoT機器の種類としては下記の様なものがあります。

スマートロック、スマートスピーカー、ネットワークカメラ、
スマートリモコン、スマート照明、スマートプラグなど

IoT製品の
セキュリティ事例

IoT製品のセキュリティ事例

IoTに関するセキュリティの事例としていくつか紹介します。

- IoTボットネットによる大規模DDoS攻撃
- 脆弱なネットワークカメラの情報を集めたサイトの存在
- 水槽の温度計からカジノのデータベースがハッキングされる
- サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト「NOTICE」

IoTボットネットによる大規模DDoS攻撃

2016年10月に米国企業が大規模なDDoS攻撃を受ける被害が発生しました。その原因は、IoT機器等に感染し、ボットネットを構築する「Mirai」というマルウェアで、多くのIoT機器がそれらに感染し、DDoSの踏み台となってしまいました。主な原因は、IoT機器のログイン情報が初期設定のまま運用されていることによって、機器のマニュアルなどから集められた初期ID/PASSを使われ感染したと推察されます。

https://www.ipa.go.jp/security/anshin/mgdayori20161125.html

脆弱なネットワークカメラの情報を集めたサイトの存在

2009年にインターネットに接続しているデバイスを検索できる検索エンジンが登場し、様々な脆弱なデバイスが検索できることが知られていましたが、現在ではそのようなサイトも増えており、世界中のID/PASS等が初期設定で運用されているネットワークカメラを一覧で表示することができるサイトなども存在します。

今では、ネットワークカメラも安価になり、ホームセンターなどで容易に入手することができますが、IPで直接アクセスできるようなタイプのIoTデバイスは管理を怠ってる場合や、そもそも買って繋いだだけのような状態では、このようなサイトにリストアップされてしまい、外部から検索可能な状態になってしまいます。

※本講演では具体的なサイト名やURL、画面には触れません。また、検索結果や画面に他組織の機器が表示される可能性があり、それらに対してアクセスを行うと各種法律に抵触する可能性がありますので、絶対に行わないでください。

水槽の温度計からカジノのデータベースがハッキングされる

ロビーに設置されたスマート水槽経由でカジノの顧客データが漏洩しました。
この便利なスマート水槽は、温度、照明、水の状態を監視し、インターネット経由で報告する仕組みを持っていました。
VPNで通信するように設定されていたにもかかわらず、このスマート水槽がバックドアとなり、カジノ内のローカルネットワークを攻撃する足掛かりとなってしまい、10GBものデータを外部に送信され、その中身はカジノの上客に関する情報だったとのことです。

https://www.securityweek.com/hacked-smart-fish-tank-exfiltrated-data-rare-external-destination

サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト「NOTICE」

NOTICEは、総務省、国立研究開発法人情報通信研究機構（NICT）及びインターネットプロバイダが連携し、IoT機器へのアクセスによる、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組で平成31年2月20日より実施されています。毎月公式サイトにて実施状況が報告されており、2021/09の報告書では、参加手続きが完了しているISP66社の約1.12億IPアドレスに対して調査を実施しています。

https://notice.go.jp/

IoT機器調査及び利用者への注意喚起の実施状況（2021年９月度）

- 参加手続きが完了しているISP（インターネット・サービス・プロバイダ）は66社。
  当該ISPの約1.12億IPアドレスに対して調査を実施。
- NOTICEによる注意喚起は、１,７７４件の対象を検知しISPへ通知。
- NICTERによる注意喚起は、１日平均２４６件の対象を検知しISPへ通知。

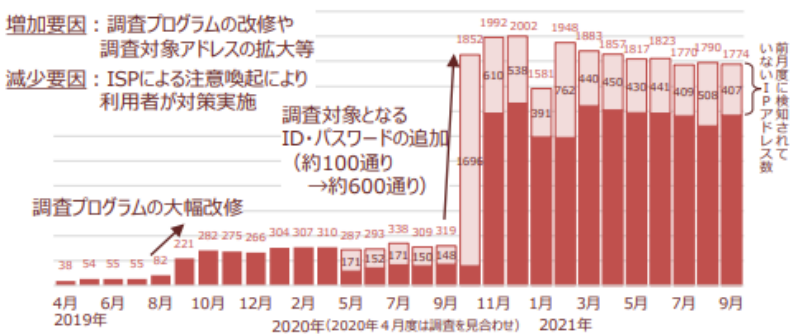
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

１,７７４件（８月度:1,790件）

（参考）2019年度からの累積件数：25,884件
ID･パスワードが入力可能だったもの：9.6万件

*) 特定のID･パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

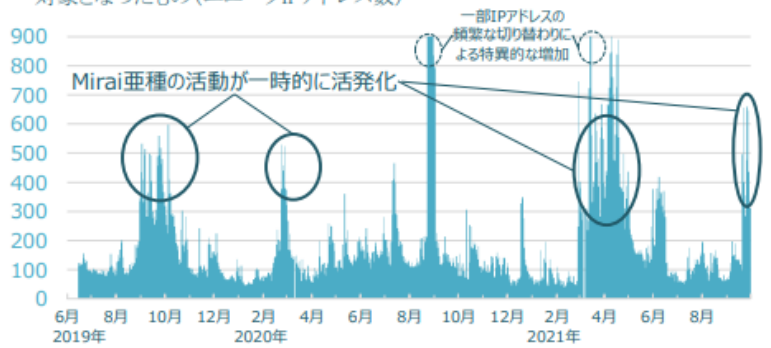
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均２４６件（８月度:107件）

（参考）期間全体での値：１日平均199件
最小：40件(2021/2/10)／最大：3,227件(2020/8/24)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



✓ NICTER注意喚起における９月下旬の主な増加要因は、海外でのMirai亜種の活動活発化を受け、脆弱性がありながら対処方法がない国内の機器が感染したことによるものと考えています。

https://notice.go.jp/docs/status202109.pdf

IoT製品における
セキュリティの問題点

IoT製品におけるセキュリティの問題点

IoT製品は下記の様なセキュリティの課題を抱えています。

- セキュリティ対策を後付けできない問題点
- 保守・サポート切れによる問題点
- 様々な機能や種類がある点

セキュリティ対策を後付けできない問題点

IoT機器は、機器のCPUやメモリといったリソースの面でセキュリティ対策を入れれない場合も多々ありますが、
そもそも、購入したIoT機器に対してユーザがエンドポイントのセキュリティ製品を導入することができる製品は、ほとんどありません。

セキュリティ対策を行う場合は、機器が接続しているネットワークの部分で、ポリシーを作成し対応していく必要があります。しかしながら、IoT機器の通信はほとんどブラックボックスであり、ポリシーを作成するにしても通信の内容を解析し、ポリシーを作成する必要があります。ポリシーを作成するためにはIoT機器の通信を可視化していく必要も出てくるでしょう。

保守・サポート切れによる問題点

IoT製品は、様々な製品が発売されており、大手ベンダーだけでなく小規模なベンダーからも多くのデバイスが販売されています。それらの製品の脆弱性や不具合対応としてアップデートが提供されることが普通であり、大手ベンダーが提供しているものに関しては、アップデートが定期的に提供される可能性が高いです。

しかし、小規模なベンダーが提供するIoT製品は、サポートの終了や倒産といった企業状況の変化により、アップデートが提供されなくなり、脆弱性や不具合を修正することができなくなることも多々あります。また、サービスの終了による影響は他にもあり、スマートロックのようなサービスであれば、鍵が開錠できなくなるような問題も発生しています。これは、IoT機器の管理インタフェースをクラウド上で提供しており、サービス終了と同時に使えなくなるためです。

様々な機能や種類がある点

IoT製品は、様々な製品が世の中に出回っています。それらには、マイク、照度計、温度計、カメラなどといった様々なセンサーが搭載されており、それらも攻撃に使われる恐れがあります。

例えば、マイクを入力として攻撃する場合は、人間が聞こえない周波数の音を発生させIoT機器に読み取らせることにより、誤動作させることや、聞こえる周波数帯でもスマートスピーカーの命令と同じ文言を聞かせることにより任意の動作をさせることができる恐れがあります。

また、IoT製品は通常のサーバやPCに使われている既存のWebの技術やOSが使われていることが多く、それらの脆弱性を元に攻撃を受ける場合が多々あります。通常のWebサーバ等であればマイクやカメラといったものがついていることは少ないですが、IoT機器にはそういった入力デバイスがついていることが多く、悪意のある攻撃者にIoT機器が乗っ取られた場合、室内のカメラの動画像を取得されたり、音声を取得される恐れがあります。また、温度計や照度計といった数値のデータでも家やオフィスに設置している場合は、エアコンや照明の状況から部屋に人がいるかどうかの判別を行うことが可能です。

IoTセキュリティの指標

IoTセキュリティの指標

IoTのセキュリティの指標として様々なドキュメントが公開されていますがそのうちのいくつかを簡単に紹介します。

- OWASP IoT Top 10 - OWASP
- OWASP IoT Security Verification Standard(Pre-release) – OWASP
- Baseline Security Recommendations for IoT - ENISA
- IoTセキュリティチェックリスト – JPCERT/CC
- IoT開発におけるセキュリティ設計の手引き - IPA

OWASP IoT Top 10とは、Webアプリケーションセキュリティの国際的な団体であるOWASPのプロジェクトの一つが出している開発者、製造業者、企業、消費者が IoT システムの作成や利用に関してより良い判断をするために、避けるべきセキュリティ上の注意点がTop 10形式で説明されたものです。最新版は2018です。

I1 Weak Guessable, or Hardcoded Passwords（弱い、推測可能もしくはハードコードされたパスワード)
I2 Insecure Network Services（安全でないネットワークサービス）
I3 Insecure Ecosystem Interfaces（安全でないエコシステムインターフェース）
I4 Lack of Secure Update Mechanism（セキュアなアップデートメカニズムの欠如）
I5 Use of Insecure or Outdated Components（安全でないか古いコンポーネントの使用）
I6 Insufficient Privacy Protection（不十分なプライバシー保護）
I7 Insecure Data Transfer and Storage（安全でないデータの転送と保存）
I8 Lack of Device Management（デバイス管理の欠如）
I9 Insecure Default Settings（安全でないデフォルト設定）
I10 Lack of Physical Hardening（物理的なハードニングの欠如）

https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

OWASPのプロジェクトの一つが出しているドキュメントの一つで、IoTア プリケーションとそれらが存在するIoTエコシステムのセキュリティ要件を定義したものです。ISVSが提供する要件は、IoTアプリケーションの設計、開発、テストを含む製品開発ライフサイクルの多くの段階で使用することができます。現時点では、Pre-release 1.0RC版です。

V1: IoT Ecosystem Requirements (IoTエコシステムの要件)
V2: User Space Application Requirements (ユーザスペースアプリケーションの要件)
V3: Software Platform Requirements (ソフトウェアプラットフォームの要件)
V4: Communication Requirements (通信の要件)
V5: Hardware Platform Requirements (ハードウェアプラットフォームの要件)

https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS

通信の要件の一般の部分はこのように記載されています。L1, L2, L3の3段階で要件が定義されています。

#	Description	L1	L2	L3
4.1.1	Verify that communication with other components in the IoT ecosystem (including sensors, gateway and supporting cloud) occurs over a secure channel in which the confidentiality and integrity of data is guaranteed and in which protection against replay attacks is built into the communication protocol.	✓	✓	✓
4.1.2	Verify that in case TLS is used, its configured to only use FIPS-compliant cipher suites (or equivalent).	✓	✓	✓
4.1.3	Verify that in case TLS is used, the device cryptographically verifies the X.509 certificate.	✓	✓	✓
4.1.4	Verify that either protection or detection of jamming is provided for availability-critical applications.		✓	✓
4.1.6	Verify that the device's TLS implementation uses its own certificate store, pins to the endpoint's certificate or public key, and disallows connections to endpoints with different certificates or keys, even if signed by a trusted CA.		✓	✓
4.1.7	Verify that inter-chip communication is encrypted (e.g. main board to daughter board communication).			✓

https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS

Baseline Security Recommendations for IoT - ENISA

欧州ネットワーク情報セキュリティ機関（ENISA）発行しているIoTのベースラインセキュリティに関する提言。
市民の健康、安全、経済的安定の確保の観点から、モノのインターネット（IoT）に必要とされるベースラインセキュリティを提言することを目的とした文書。セキュリティ上の課題や、攻撃シナリオ、セキュリティ対策／グッドプラクティスなどがまとめられている。

また、IPAから概要の日本語訳が出ています。(https://www.ipa.go.jp/files/000063605.pdf)

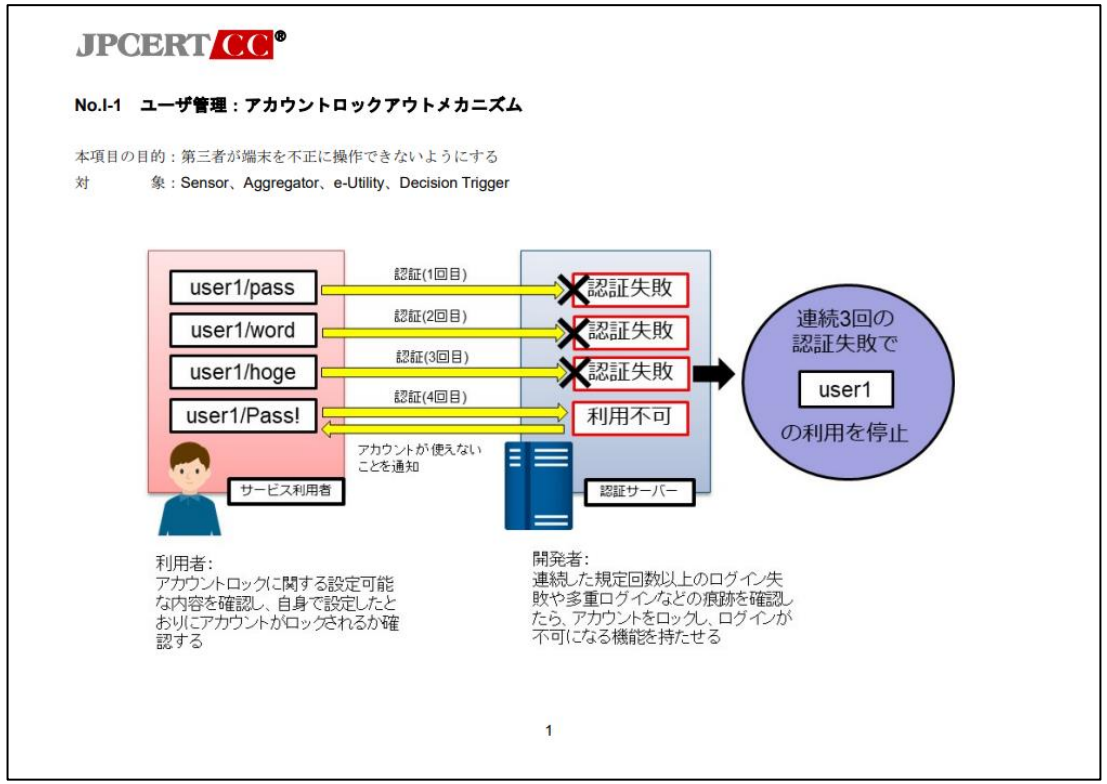
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

IoTセキュリティチェックリスト – JPCERT/CC

JPCERT/CC が出しているIoTセキュリティの課題を解決するためのIoT システム/IoT デバイスの開発者がチェックすべきことと、利用者がチェックすべきことをまとめた IoT セキュリティチェックリスト。PDFとExcelで公開されており、利用説明書や解説図も公開されている。

下記の分類で構成されており、計39項目。

- ユーザ管理
- ソフトウェア管理
- セキュリティ管理
- アクセス制御
- 不正な接続
- 暗号化
- システム設置
- 通知



https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

IoT開発におけるセキュリティ設計の手引き - IPA

2016年3月24日にIPAソフトウェア高信頼化センターが公開した IoT製品を安全に開発するための17の指針 に対し、具体的なセキュリティ設計と実装を実現するための手引き。

IoTのセキュリティ設計やIoT関連のセキュリティガイドの紹介、デジタルテレビやスマートハウス、コネクテッドカーに関するIoTシステムにおける脅威分析と対策検討の実施例等が記載されている。

https://www.ipa.go.jp/security/iot/iotguide.html

まとめ

- IoT機器が問題の原因となっている事例は多々ある。
- IoT製品は様々な問題点を抱えている。
  - セキュリティ対策を後付けできない問題点
  - 保守・サポート切れによる問題点
  - 様々な機能や種類がある点
- IoT機器の開発におけるセキュリティの指標としては様々なドキュメントが公開されており、日本語のチェックシートも存在する。

https://pr.fujitsu.com/jp/news/2021/08/11.html

SECURE CYCLE

システム開発におけるセキュリティ対策を当たり前に

〒808-0138 福岡県北九州市若松区ひびきの北8番1号
技術開発交流センター 314号室
TEL: 093-701-6735 / URL: https://secure-cycle.co.jp/