Ksisnet
Kyoto Small and Medium Enterprises Information Security Support Network
京都中小企業情報セキュリティ支援ネットワーク

Ksisnetだより

平成２８年
６月２０日
Vol. １４

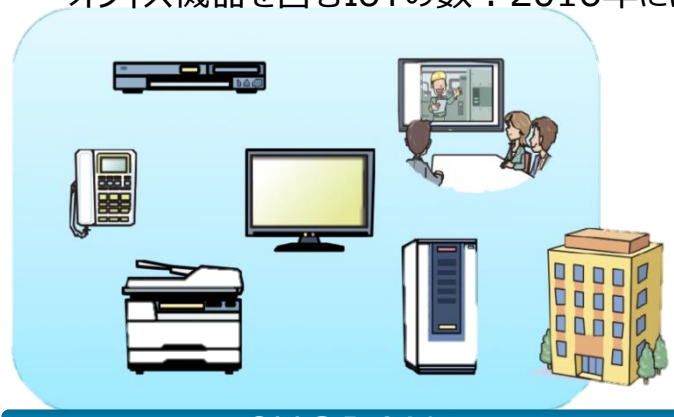
発行：京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）事務局

注意するのはPCやスマートフォンだけではありません

IoT(モノのインターネット)※1のセキュリティ対策

※1 :Internet of Thingsの略

～オフィス機器を含むIoTの数：2016年には64億・2020年には208億に達すると予想～



IoT機器の中にはサーバー機能を有しているものも多く、ネットワークに接続することでＰＣやスマートフォンなどからの利用が可能となりますが、不適切にインターネットに接続されているIoT機器は、攻撃者にとって格好のターゲットになっています。

この背景の一つとして、インターネットに接続されているIoT機器を検索できる「SHODAN」「Censys」のサービスが開発され、ターゲットとなる機器の発見が容易になったことが挙げられます。

SHODAN

2009年に開発された検索エンジン。ウェブサーバだけではなく、オフィス機器、情報家電など、インターネットに接続されている様々な機器の情報がデータベースに格納されており、利用者はその機器の情報をウェブで検索できる。

Censys

2015年に開発された検索エンジン。利用者がインターネットに接続されているシステムの脆弱性を見つける支援をする機能を有している。データベースに格納されている情報はSHODANとほぼ同様。

◎危険性を認識しましょう

機器を初期設定のままインターネットに接続することで
●不正アクセスや機密情報の漏えい●設定情報が変更される●攻撃の踏み台にされる
といった可能性があります。

◎自社のIoT機器を確認して対策を取りましょう

攻撃者による外部からのアクセスを意識したうえで３つの対策が必要です。

①管理の明確化

- ネットワーク接続のルールを定め、内部に周知する
- 管理者を明確にする
- SHODANやCensysならびにペネトレーションツール(※2) の活用などによって、定期的にネットワークを外部から検査し、意図して公開している以外のIoT機器の接続を確認する

※2 システムなどの脆弱性を見つけるツール

②ネットワークによる保護

- 必要性がない場合、インターネットに接続しない
- 原則ファイアウォールやブロードバンドルーターを経由させ許可した通信だけに限定する
- ネットワークセグメントを適切に分離又はアクセス元のIPアドレスを限定して管理機能へのアクセスを制限する

③IoT機器の適切な設定

- 使用しない機能はオフにする
- 管理者用アカウント／パスワードを工場出荷時から変更する
- ソフトウェアのアップデート

出典(独)情報処理推進機構(IPA)：IPAテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」～あなたのシステムや機器が見られているかもしれない～
詳しくはIPAホームページからご欄下さい。【https://www.ipa.go.jp/security/technicalwatch/20160531.html】

※注意事項：検索エンジンを利用した調査により、他組織の機器情報が表示される可能性がありますが、他組織の機器にはアクセスしないでください。

お困りのときは!!
京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）
ＩＴ相談窓口（公益財団法人京都産業２１ お客様相談室）
相談内容：情報セキュリティ対策、情報漏えい・流出事案等
※毎週月曜日～金曜日の９：００～１７：００（祝日を除く）
TEL 075-315-8660 メールアドレス okyaku@ki21.jp
公益財団法人京都産業２１ お客様相談室（〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内）