# IoT（Internet of Things）セキュリティについて

IoT とは「Internet of Things（モノのインターネット）」の略であり、世の中に存在するさまざまなモノをインターネットにつなげることで、モノの状態を把握できたり、モノをリモート操作したり、といったことが可能になる技術のことです。わかりやすい例では、防犯カメラ、テレビやエアコンや洗濯機など、スマートフォンで操作や管理できるスマート家電も IoT 機器ですし、店舗にあるトイレの空き状況を確認できるサービスも IoT 技術を活用したものです。

建設業界においても、国内建設業が抱える課題として①複雑な施工体制、②人手不足、③労働災害、④国内需要の減少、といった課題の解決に向け、国交省が 2025 年時点で 2015 年から 20%の生産性向上を目指す「i-Construction」を提唱し、取り組みが進められおり、IoT 技術を活用した事例が多く発表されています。

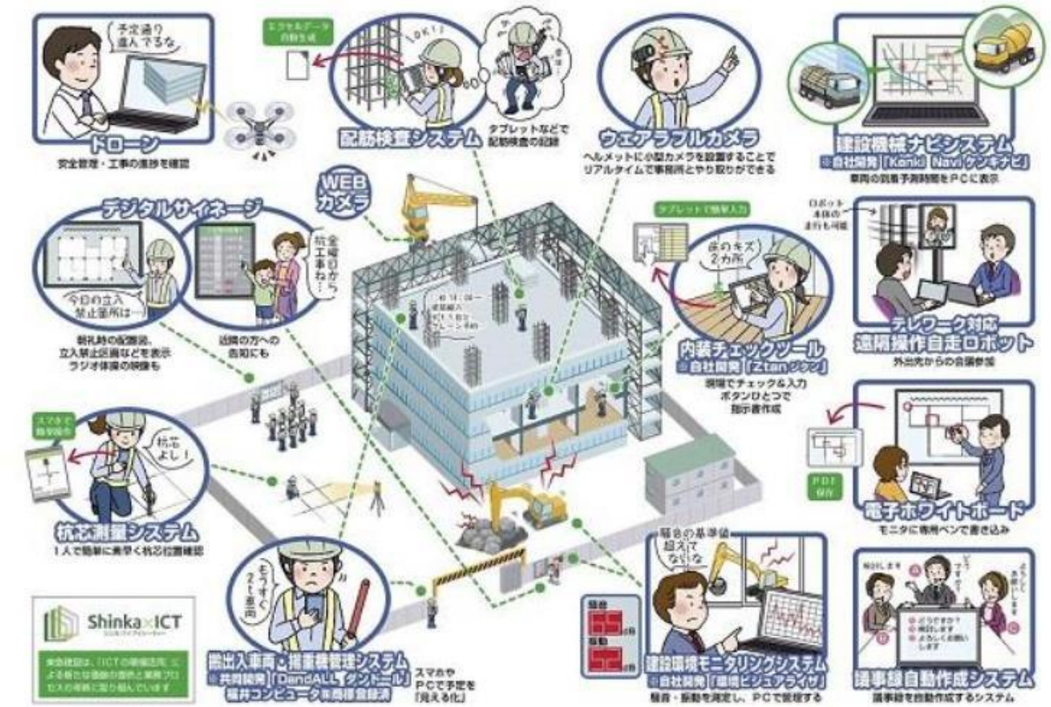
ただし、さまざまなモノがインターネットにつながると、省力化や生産性向上に繋がる利便性がたくさんある反面、非常に危険なことでもあります。

インターネットにつながるモノは、常に世界中からセキュリティの穴がないか、調べられています。セキュリティの設定が甘い機器をインターネットに接続すると、数時間で乗っ取られることがわかっており、十分なセキュリティ対策を行わずに活用していると、サイバー攻撃によって多大な損害を受ける危険性があるばかりでなく、攻撃者の踏み台として利用され加害者になることもあります。

IoT 機器が抱えるリスクの説明と、最低限のセキュリティ対策を挙げますので、参考にして確認・対策を行ってください。

・建設業における IoT 活用例としては以下のようなものが挙げられます。
ウェアラブルデバイスを活用した作業員の管理
ネットワークカメラによる遠隔臨場やモニタリング
ドローンを使った現場の把握
IoT を使った建機の自動制御

・建設業における IoT 活用例のイメージ図




ICT モデル現場　イメージ図　出典：東急建設

## （１）IoT もセキュリティをきちんと対策しないと危険…>>>

**・チェックしてみよう（詳細は（5)サンプル　確認のこと）**

- **SHODAN**
  - デフォルトパスワードのままのネットワーク機器やデバイス、外部から見えるソフトウェアの脆弱性などを確認することができる。
- **サイバー版 PCR 検査　横浜国大「IoT の感染検査サービス “am I infected?”」**
  https://amii.ynu.codes/
  - 家庭用ルーターやスマート家電などの IoT 機器がマルウェアに感染していないか、脆弱な状態で利用していないかを利用者自身で検査・対策できる無料のサービス。

・**IoT 機器はセキュリティに関して脆弱性が生じやすい**

➢ **脆弱性が生じる理由**

- ハードウェアが持つ処理能力の限界

  限られた処理能力しか持たないため、セキュリティの仕組みとデータ保護を搭載するための十分な性能がない場合がある。

- 通信保護の機能を持たない伝送技術

  軽く、早く通信することを優先した伝送技術によりセキュリティ保護機能と両立しない場合がある。

- ソフトウェアが脆弱

  IoT 機器のソフトウェアの脆弱性は発見されにくく、発見されたとしても対処が困難な場合がある。

- 機器提供側のベンダー、利用者ともにセキュリティに対する意識不足

- 「IoT 機器もコンピュータでありセキュリティ対策が必要」であることの意識が低く、セキュリティを考慮していない製品や、継続的なセキュリティ対策を含めたサービスを提供しないような製品を販売するベンダーも存在する。利用者側も IoT 機器を不用意にインターネット上に露出させたり、脆弱性を放置したまま使用したりする可能性がある。

**・世界の IoT 機器を対象としたサイバー攻撃事例や公開された脆弱性**

➢ **2016 年 Mirai**

50 万台の IoT 機器（ルーターや Web カメラ）が乗っ取られ、Twitter、Amazon、PayPal などの著名なサービスを利用困難な状態に陥れた。

➢ **2018 年 NASA 情報漏洩**

攻撃者は NASA ジェット推進研究所（JPL）のネットワークに侵入し、火星プロジェクトに関する機密データが盗み出した。原因は無許可接続された IoT 機器 Rapsberry Pi だった。

➢ **2020 年 Ripple20**

悪用された実例はまだ公表されていないものの、米国企業 Treck 社製のソフトウェアに任意のコードが実行できる脆弱性があり、数百万個の IoT 機器に深刻な影響を与える、と報道された。

➢ **2022 年 ドローンの脆弱性公開**

ドローンへのサイバー攻撃リスクは「データ漏えい」と「不正操作」が考えられる。「Japan Drone 2022」で、GMO インターネットはドローンへのサイバー攻撃の手法デモを公開した。

## （2）最低限の対処…＞＞＞

➢ **サイバー版 PCR 検査　横浜国大 「IoT の感染検査サービス “am I infected?”」**

感染が疑われる場合は対処法まで結果で返してくれる。

➢ **NICT（国立研究開発法人情報通信研究機構）「すぐできる IoT 機器セキュリティ対策 6」**

（「サイバー攻撃の動向とセキュリティ研究 2021」セミナー）

1．IoT 再起動
　（IoT 機器は記憶装置を持たないのでマルウェア感染に対しては再起動で駆除できる）
2．ファームウェアアップデート
3．ID/パスワード変更
4．インターネット側からのアクセス拒否設定
5．ゲートウェイ機器の内側に設置
6．古い機器は買い替え（自動アップデート機能がない機器は NG）

➢ **NICT「NOTICE」活動**

NOTICE とは、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ーが連携し、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り組み。

➢ **IoT 機器から情報を集めて保存する先のセキュリティも要確認**

IoT 機器から収集した情報をクラウド上に保存する場合がある。クラウド側のセキュリティにも注意が必要。

## （3）IoT に関するセキュリティ対策全体の詳細…>>>

➢ **IoT に関するセキュリティチェックを網羅的に実施するには**

各機関から IoT に関してセキュリティ上のチェックすべき項目が公開されている。
しかし、導入を検討するすべての IoT 機器に、これらの項目をすべてチェックするのは大きな負担であり、IoT 機器のリスクの大きさに応じて、チェック項目を取捨選択することが肝要である。

・JSSEC「IoT セキュリティチェックシート」（https://www.jssec.org/iot）
・JPCERT/CC「IoT セキュリティチェックリスト」
（https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html）

➢ **IoT セキュリティに対する理解を深めるためには**

IoT セキュリティに関して参考になる文献を以下に挙げる。

・NISC「安全な IoT システムのためのセキュリティに関する一般的枠組」
（https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai05/05sankou02.pdf）
・IoT 推進コンソーシアム「IoT セキュリティガイドライン」
（http://www.iotac.jp/wg/security/）
・IPA「IoT のセキュリティ」（https://www.ipa.go.jp/security/iot/）
・経済産業省「IoT セキュリティ・セーフティ・フレームワーク」
（https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html）
・NOTICE「IoT 機器とサイバーセキュリティ」（https://notice.go.jp/）

## （4）実際に被害が発生してしまったら…>>>

➢ **通報・相談・アドバイス**

警察（#9110 , https://www.npa.go.jp/cyber/soudan.html）
IPA 情報処理推進機構 （https://www.ipa.go.jp/security/anshin/#4-1）
JPCert **J**ap**C**omputer **E**mergency **R**esponse **T**eam Coordination Center
（info@jpcert.or.jp , https://www.jpcert.or.jp/incidentcall/）

➢ **調査・対処の依頼（例）**

LAC （0120-362-119 , 119@lac.co.jp 緊急事故対応サービス「サイバー119」）

GSX（03-3578-9055、119@gsx.co.jp、https://www.gsx.co.jp/emergency/index.html）

サイバーディフェンス研究所（03-5843-9015 https://www.cyberdefense.jp/services/ir/）

イエラエセキュリティ（https://ierae.co.jp/service/forensics/）

➢ **被害に遭った場合の対応と再発防止対策（例）**

1.侵入の疑いのある機器の完全初期化、または機器の入れ替え。

2.機器のファームウェアを最新にアップデート。

3.ID/パスワードを変更する。

4.インターネット側からのアクセスを制限する。

## （5）「サンプル」 チェック サイト で確認 >>>

➢ **SHODAN**

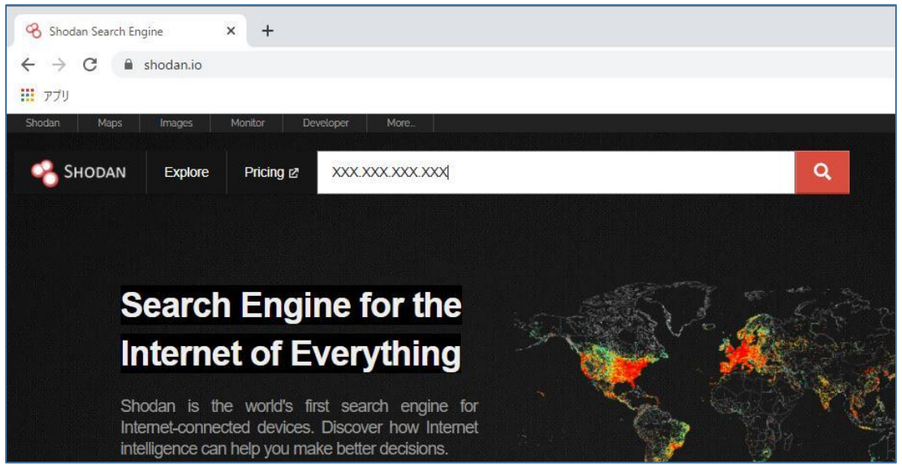
SHODAN の利用にあたっては、IPA（情報処理推進機構）発行の「増加するインターネット機器の不適切な情報公開とその対策」を必ず参照してから実施してください。

https://www.ipa.go.jp/about/technicalwatch/20140227.html

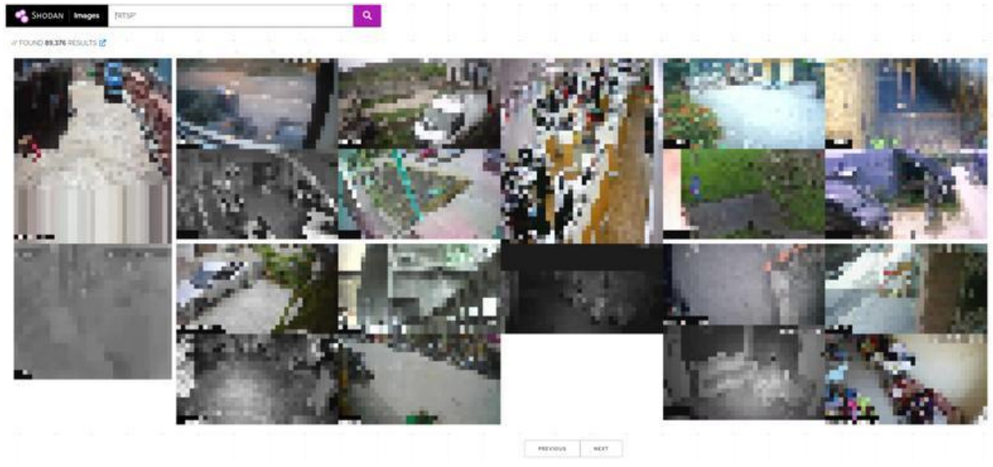
・SHODAN って知っている？悪用されることでどのような危険があるのか？
https://eset-info.canon-its.jp/malware_info/special/detail/201015.html

・【闇】最高に危険なサーチエンジン「SHODAN」とは
https://softantenna.com/blog/dangerous-search-engine-shodan/

・SHODAN： https://www.shodan.io




・SHODAN 結果サンプル：https://note.com/hiro_shi_note/n/ndea5027cdcd9




➢ **サイバー版 PCR 検査　横浜国大「IoT の感染検査サービス “am I infected?”」**

https://amii.ynu.codes/

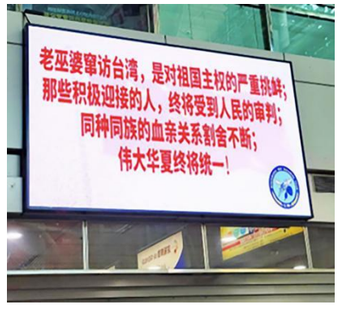
- 家庭用ルーターやスマート家電などの IoT 機器がマルウェアに感染していないか、脆弱な状態で利用していないかを利用者自身で検査・対策できる無料のサービス


**※参考（IoT に関する最新サイバー攻撃事例）**

2022 年 8 月初旬、ペロシ米下院議長の台湾訪問にあわせて、台湾各地で「サイバー攻撃」の報告が相次いだ。（出典：プレジデントオンライン https://president.jp/articles/-/60711?page=1）

セブン-イレブン店内モニターに「戦争屋ペロシ」の文字が

朝の混在する時間帯で、多くの人がセブン-イレブンで朝食やコーヒーを買っていた。突然店内の照明が切れ、真っ暗になった中に、電光掲示板に浮かび上がったメッセージを見て、恐怖心を覚えた人も多かったようだ。




ハッキングされた高雄新左営駅の大型デジタルサイネージ


セブン-イレブン店内モニターに「戦争屋ペロシ」の文字が

今回の攻撃では、APT27 は、台湾国内の 6 万台ものインターネット接続デバイスをシャットダウンさせたと主張している。（APT27 は、10 年以上前からサイバースパイ活動などを行っている中国のハッカー集団）