

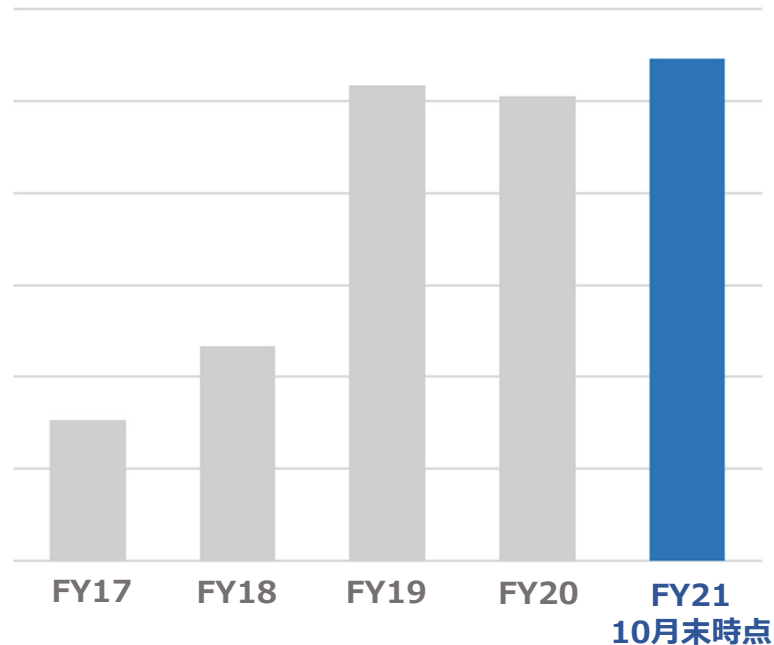
ご挨拶

IIJのIoTビジネスについて

株式会社インターネットイニシアティブ
IoTビジネス事業部長 岡田晋介

IIJのIoT案件概況

IoT関連案件数



- FY20はコロナ影響により事業部門需要が一時減少もFY21に入り大きく回復基調に
- IoT用途モバイルサービスは引き続き好調、産業分野など顧客検討の具体化が進む



産業系を中心にIoTセキュリティに係る意識の変化

工場ネットワーク

設備リモート監視

エネルギー管理

etc...

IIJのIoT全体像



※ WISE-PaaS IIJ Japan-Eastは台湾Advantech社とIIJの協業により実現されたAdvantech社によるサービスです
 ※ 独居ケアアシスタントは中部電力とIIJの協業により設立されたネコリコ合同会社によるサービスです

凡例

IIJ活動領域

IoTデバイス向け新セキュリティサービス - 「IoTトラストサービス™」 記者発表会資料 -

株式会社IIJグローバルソリューションズ
営業本部 営業開発部 部長 稲田 憲二

IoTデバイス向けセキュリティサービス開発の背景

IoT領域を取り巻く世の中の動き①

■IoTデバイス(※)数の急速な増加

- ・2023年IoTデバイス数**340億台**
- ・分野別では、スマート工場やスマートシティが拡大する「**産業用途**」（工場、インフラ、物流）、コネクテッドカーの普及によりIoT化の進展が見込まれる「**自動車・宇宙航空**」が顕著である

総務省「令和3年版 情報通信白書」より

<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105220.html>

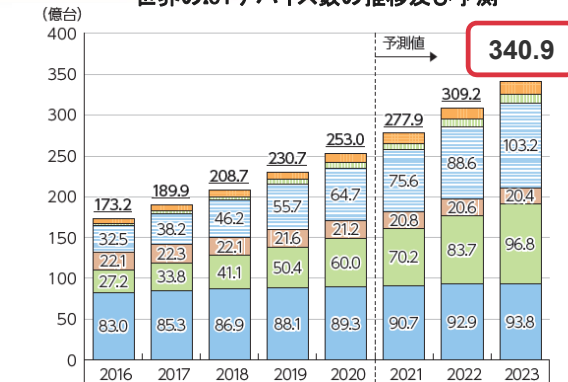
(※) IoTデバイス：固有のIPアドレスを持ちインターネットに接続が可能な機器及びセンサーネットワークの末端として使われる端末等

■IoTデバイスを狙ったサイバー攻撃が半数（約50%）に上る

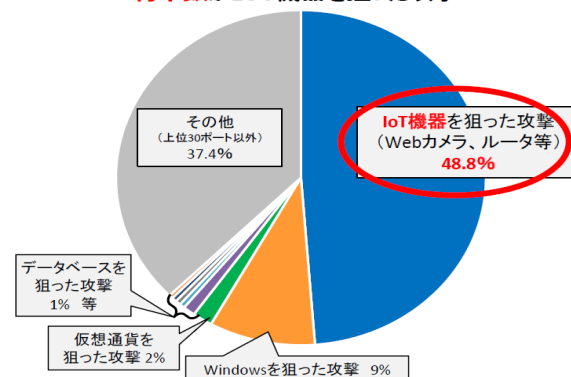
「情報通信研究機構(NICT)レポート」令和2年総務省

「サイバーセキュリティタスクフォース事務局レポート」より

世界のIoTデバイス数の推移及び予測



約半数がIoT機器を狙った攻撃



！ IoTデバイスのセキュリティ脅威が増加

IoT領域を取り巻く世の中の動き②

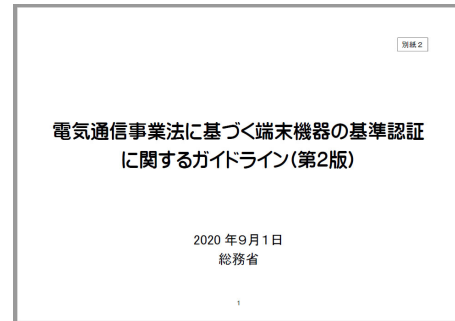
■ 国際：産業機器の汎用制御システムのセキュリティ基準「IEC62443」の制定

- ・産業用オートメーション及び制御機器及び開発プロセスを対象とした規格
- ・IEC62443-4-1,4-2が機器類に対する標準規格として定義されている

■ 国内：総務省/経済産業省：「IoTセキュリティガイドライン」の制定

(※) 総務省「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第2版）」
(※) 総務省、経済産業省、IoT推進コンソーシアム「IoTセキュリティガイドライン Ver1.0」

- ①不特定多数からのアクセスを遮断できる機能
- ②IDやパスワードを初期値から変更を促す機能
- ③ソフトウェアを常に更新できる機能
- ④認証機能の導入
- ⑤出荷・リリース後も安全安心な状態を維持する



！ 国際基準、ガイドラインに沿った製造・運用が必要

企業活動におけるセキュリティの脅威



IoT機器や工場
制御システムを
踏み台にした被
害が増加
脅威はあらゆる
場所に存在

！ ゼロトラストを前提とした対応策が必要

IoTセキュリティの課題

■ IoTデバイスの主な特性

- 演算処理能力が**低い**、**省電力**
- 通信プロトコルが**ユニーク**（様々なプロトコル）
- 何らかの**ネットワークに繋がっている**
- ライフサイクルが**長い**
- **設置場所変更**、**使い回し**（移転）がある
- **数が多い**
- セキュリティ**対応策が多岐**（チップ？ファーム？証明書？）
- **管理されていない**（管理ツール/画面が無い）
- ファームウェア、証明書が**更新されない**



従来型セキュリティの適用
や運用が困難



IoTデバイスの特性に応じたトラストの実現が必要

「IoTトラストサービス™」とは

IoTトラストサービス™とは

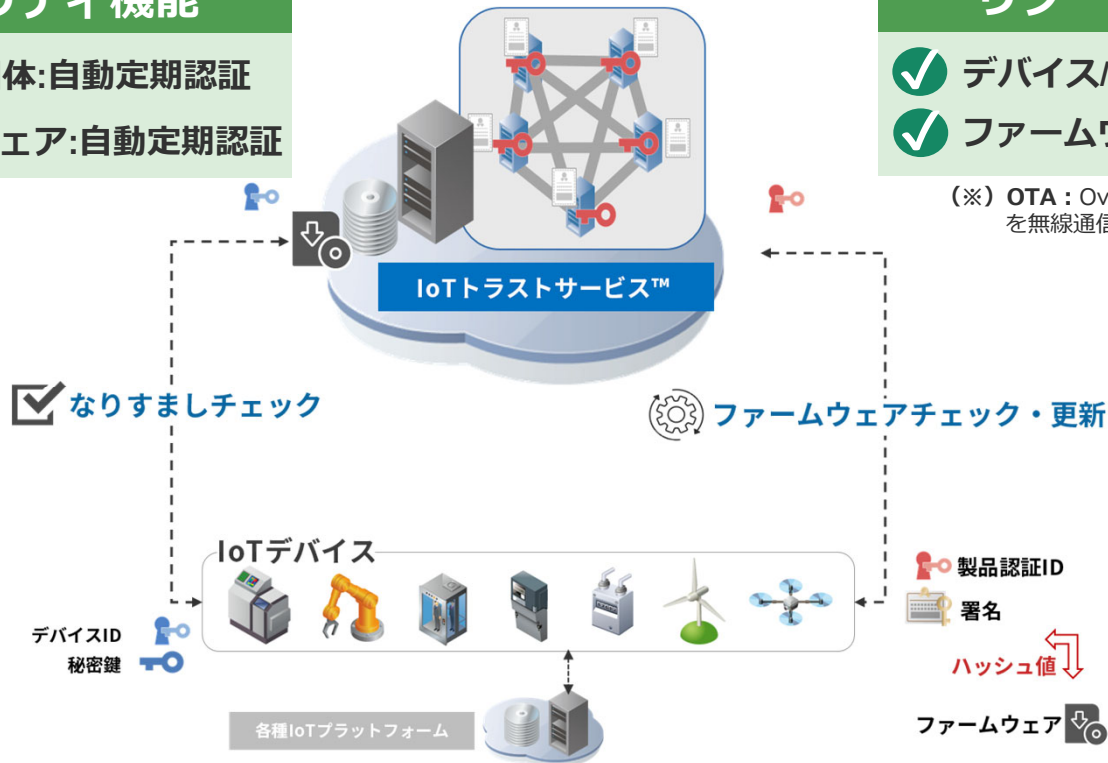
セキュリティ機能

- ✓ デバイス個体:自動定期認証
- ✓ ファームウェア:自動定期認証

リソース管理機能

- ✓ デバイス/ファームウェア管理
- ✓ ファームウェアOTA(※)機能

(※) OTA : Over The Air (データの送受信を無線通信で行うための技術)



✓ デバイスの信頼性を高める認証プラットフォームサービス

Kusabi特許(※)技術採用による安全性・信頼性の担保

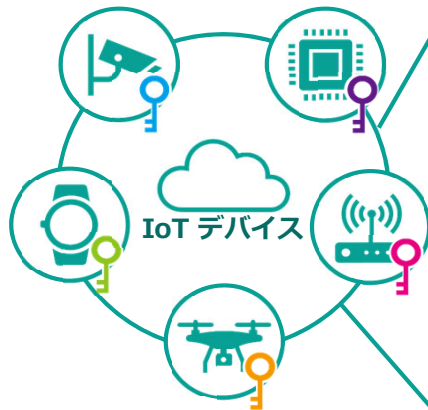
■ 電子証明システム

(※) 2018 年 5 月 18 日国内特許取得 (特許 第 6340107 / 6480528 号)

(※) 2021 年 9 月 21 日米国特許取得 (米国 PATENT NO. 11128477)

ブロックチェーンが論理的に持つ技術特性 (耐改ざん性) を活用し、公開鍵を保証。大量のデバイスに対しても即時発行を可能とするとともに、様々なデバイスへの適用を実現。

ブロックチェーン



■ デバイスプロビジョニングシステム

(※) 2018 年 5 月 18 日国内特許取得 (特許 第 6340120 号)

プロビジョニングサーバー主導で、デバイスの登録、公開鍵の格納、電子認証に紐づく秘密鍵を配布し、デバイスの適用から運用フェーズの自動化を実現。

🔑 : 秘密鍵

🔑 : 公開鍵



ブロックチェーン技術を活用した新たなPKIシステム

PKI : Public Key Infrastructure (公開鍵暗号の技術を利用して暗号化や電子署名の機能を提供するセキュリティ基盤)

IoTトラストサービス™の特徴/メリット

特徴 1 : 全自動

デバイス/ファームウェア認証の為の鍵取得、プロビジョニング(※)、認証、更新を自動で実施

特徴 2 : 独自ID

認証用/証明書として独自IDを採用。秘密鍵+公開鍵+独自IDにより専用チップ不要でデバイス認証が可能

特徴 3 : ブロックチェーン

認証用公開鍵をセキュリティ強固なブロックチェーン上に格納
プライベートCAとしての信頼性を向上

(※) プロビジョニング:リソースの割り当てや設定などを行い、利用や運用が可能な状態にすること

証明書機能を 安価に提供

- ・パブリックCA証明書と比較し安価に証明書機能を提供
- ・証明書期限も自動更新
- ・公開鍵はブロックチェーン上で安全に保管

鍵・証明書発行の 面倒な手続き軽減

- ・製造者リクエストにより自動で鍵交換、証明書発行
- ・公開鍵認証の運営軽減が可能
- ・大量デバイスの証明書運営が可能

二段階プロビジョニングによる 強固なセキュリティ

- ・デバイス製造時と出荷時の鍵証明書による二段階プロビジョニング機能
- ・デバイスのライフサイクルに合わせたセキュリティ強化が可能



CA認証局不要で運用の手間とコストを削減

CA認証局 : CA=Certification Authority (デジタル証明書を発行する機関で、電子証明書の登録、発行、失効をおこなう第三者機関)

IoTトラストサービス™ サービス提供機能

セキュリティ認証

- ✓ デバイス個体:自動定期認証
- ✓ ファームウェア:自動定期認証

デバイス管理

- ✓ デバイス管理/ファームウェア管理
- ✓ 自動ファームウェア更新OTA

自動鍵交換／自動証明書発行／自動プロビジョニング

- ✓ ユーザーリクエストにより自動で鍵交換/証明書発行
- ✓ 鍵、証明書の自動プロビジョニング環境提供



API (※)連携

- ✓ API連携による他サービスとの連携、機能の拡張



(※) API : Application Programming Interface (ソフトウェアやプログラム、Webサービスの間をつなぐインターフェース)

オプション : OT環境構築ツール/コンサルテーション



本番サービスご利用前にPoCプランをご利用ください

PoC : Proof of Concept (実現可能性や実際の効果などを検証する目的で実施される検証プロセス)

IoTトラストサービス™ ターゲット市場/活用シーン

デバイス製造メーカー

- ✓ 自社製品の付加価値向上
- ✓ セキュリティガイドライン対応
- ✓ IoT家電向け認証、ファームウェア更新



社会インフラ

- ✓ インフラ制御機器の安全性担保
- ✓ 交通・電力・公共設備等
- ✓ ドローン運用管理、認証
- ✓ 医療関連機器



車載向けデバイス

- ✓ 車載デバイスのファームウェア更新・管理
- ✓ WP29(※)レギュレーション対応



(※) WP29 : 自動車基準調和世界フォーラム作業部会29番目
(自動運転車のサイバーセキュリティとソフトウェアアップデート
法規基準の検討を行う組織)

IoT関連サービス

- ✓ IoTプラットフォームサービス
- ✓ IoTゲートウェイ製造メーカー



✓ サイバー攻撃が社会的影響を及ぼす市場を中心に適用

今後の展開：パートナー共創によるサービス拡充

- ✓ **組み込み用ハードウェア/ソフトウェア製造開発企業様**
 - ・ OT（※）サイドの組込サポート、コンサルティング

（※）OT：Operational Technology（運用制御技術の総称）

- ✓ **商用OS提供企業様**
 - ・ Linuxサポート、コンサルティング

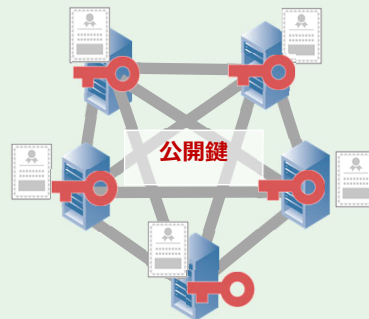
- ✓ **チップ/マイコン製造企業様**
 - ・ チップ標準機能としての組み入れ

- ✓ **車載向けOTAサービス提供企業様**
 - ・ WP29レギュレーションに対応したOTAの実現

- ✓ **IoTプラットフォームサービス提供企業様**
 - ・ DXに向けたIoT収集データの利活用推進

- ✓ **IoT-SOC（※）サービス機能提供**
 - ・ 異常検知時のアラート、通知、可視化

（※）SOC：Security Operation Center
（ログ監視や分析を行いサイバー攻撃の検出・通知を行う組織）



- ✓ **業界/機能に特化したパートナー企業様と順次協業予定**

IIJ-IoTサービス全体像



IoTサービスの拡充によりIT／OT両面から支援します

人を、クラウドを、世界をつなぐ
ビジネスの未来に**新しい価値**を

【IoTトラストサービス™に関するお問い合わせ】

E-mail: info@iijglobal.co.jp

URL: <https://www.iijglobal.co.jp/>

株式会社IIJグローバルソリューションズ

営業本部 営業開発部 ソリューション推進グループ

IoT推進チーム



株式会社IIJグローバルソリューションズ

 info@iijglobal.co.jp

 www.iijglobal.co.jp

本書には、株式会社IIJグローバルソリューションズに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。文中では™、®マークは表示していません。本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。

IoTトラストサービスを支援する
アイビーシー株式会社の特許技術

セキュリティ電子証明基盤「kusabi」

2021 年 11 月 30 日



アイビーシー株式会社
サービス事業部
DX・コンサルティング部
部長 鈴木 大和

アイビーシー株式会社 会社概要



MISSION

IT 障害をゼロにする

VISION

IT 活用で永続的に成長し、
事業・社会へ貢献する

社 名	アイビーシー株式会社 IBC : Internetworking & Broadband Consulting Co.,Ltd.
所在地	【本社】 東京都中央区新川1-8-8 アクロス新川ビル8F 【西日本事業所】 大阪府大阪市淀川区西宮原2-7-38 新大阪西浦ビル3F
上場区分	東京証券取引所 市場第一部（証券コード：3920）
設 立	2002 年 10 月 16 日
資本金	442,930 千円 (2021 年 9 月 30 日現在)
代表者	代表取締役 加藤 裕之
事業内容	1) IT システム性能監視ツールの開発 / 販売 / サポート 2) IT システムの性能評価サービス 3) IT システムの設計・構築、コンサルティング 4) IoT 電子証明セキュリティ基盤の開発 / 提供 5) 各種機器、ソフト販売



インテグレーション

システムインテグレーションサービス

IBC-Integration



モニタリング・可視化

システム情報管理ソフトウェア



System Answer G3



性能アセスメントサービス

IBC-PAS

セキュリティアセスメントサービス

IBC-SAS



レポート自動作成オプション

Stats Option

powered by Yellowfin

分析サービス

予防保守レポート

次世代 MSP サービス

SAMS

「将来的に障害をゼロにする」 安定した IT インフラをご提供

アイビーシーが考える IoT セキュリティへのアプローチ

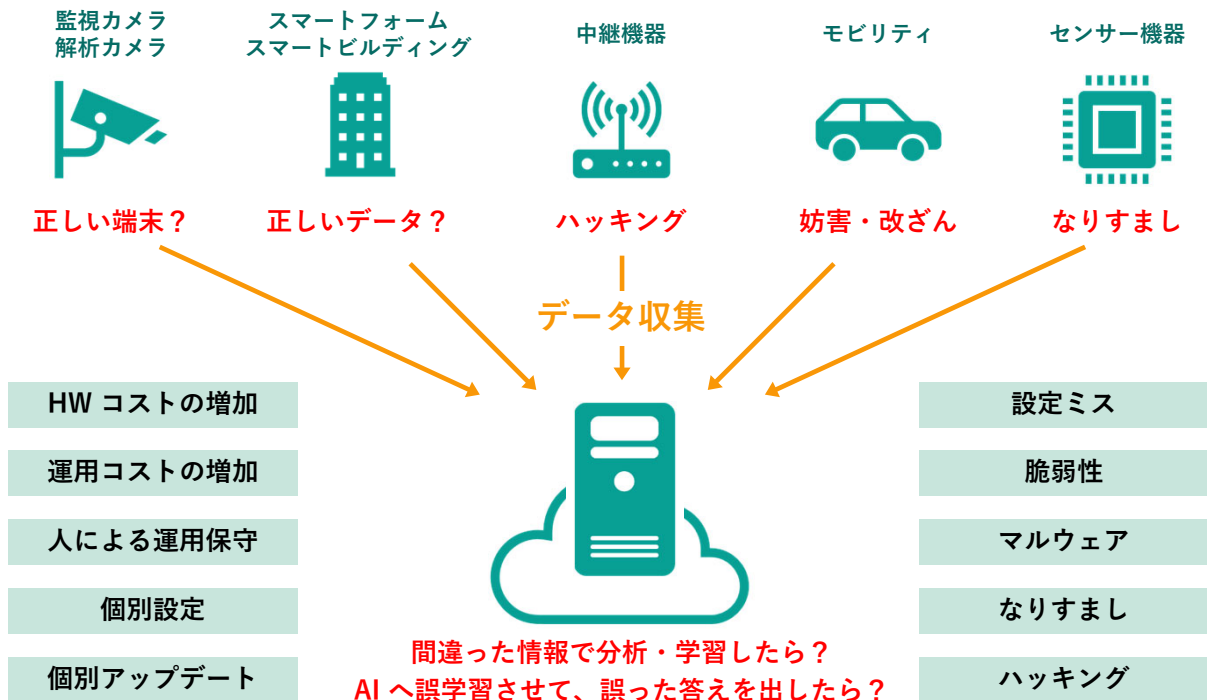


IoT 化で実現できること

DX によるデータ活用で 社会の問題を解決する

- ・ 多種多様なデバイスから目的に合った情報を収集
- ・ 取得した情報を分析・学習し、新たなサービスにつなげる

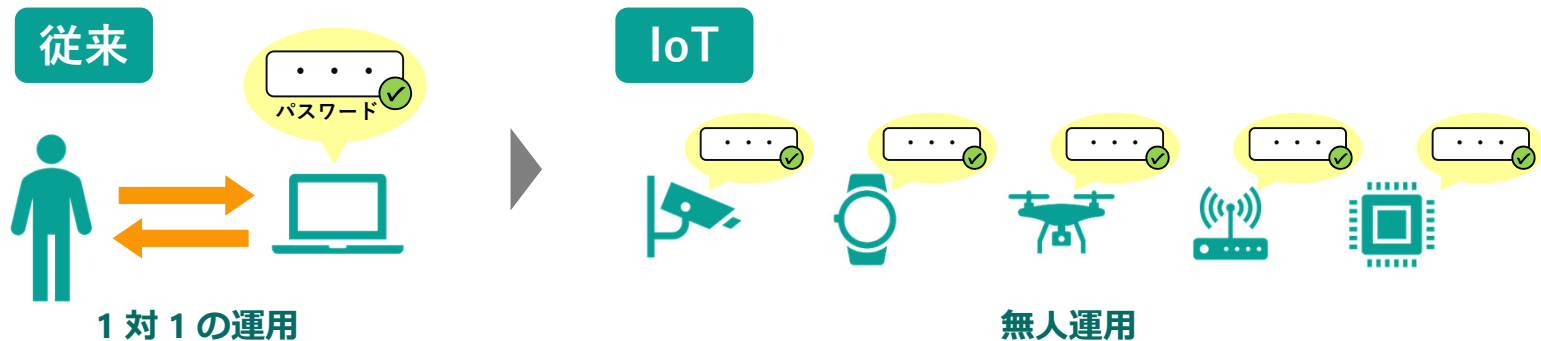
▶ それにともなうリスクや課題も



新たなサービスを提供するには **データの価値・信用性** が重要

IoT デバイスは従来型 PC セキュリティの適用が難しい

- ・多面的で高度な技術が必要
- ・コストや性能による制限がある
- ・無人で運用する
- ・大量のデバイスを多様な環境で運用する
- ・GUI がないデバイスや状態を通知しないデバイスもある
- ・遠隔運用での侵入経路は攻撃者に狙われやすい



PKI によるパスワード型運用からの脱却

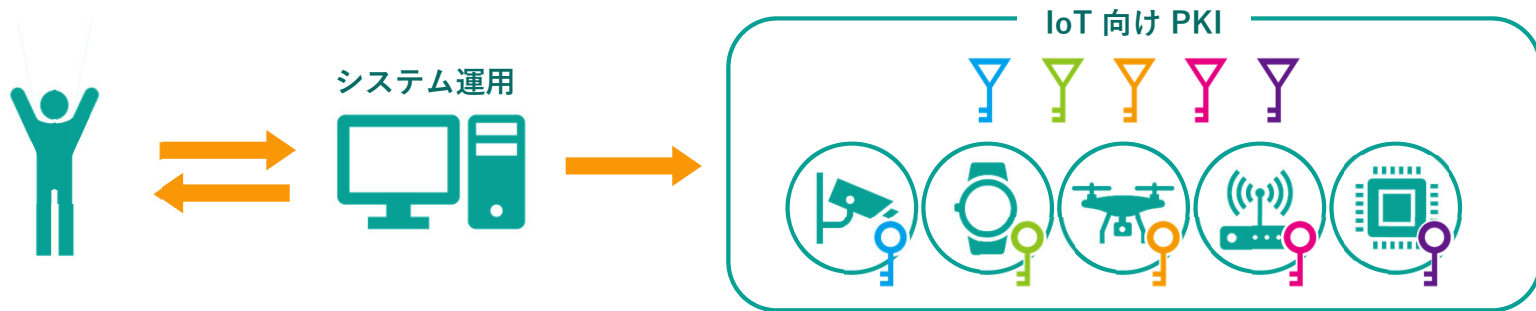
PKI (Public Key Infrastructure / 公開鍵暗号基盤)

公開鍵と秘密鍵のキーペアからなる「公開鍵暗号方式」技術を利用し、インターネット上で安全に情報のやりとりを行うセキュリティのインフラ（基盤）のこと

非パスワード運用を実現

暗号化処理ができる

コードサイニングができる



大量の証明書を配布するため、
レベルの低い認証（ドメイン認証程度）や
プライベート認証局の証明書を使用する

コスト的課題

大量の証明書更新の運用コストを
下げるため、有効期限が長い証明書
を使用し、更新頻度が低下する

セキュリティ的課題

新 PKI 技術 により IoT デバイスの運用・コスト・セキュリティ課題を解決する



セキュリティ電子証明基盤





電子証明システム

*2018 年 5 月 18 日国内特許取得（特許 第 6340107 / 6480528 号）

*2021 年 9 月 21 日米国特許取得（米国 PATENT NO. 11128477）

ブロックチェーンが論理的に持つ技術特性（耐改ざん性）を活用し、公開鍵を保証。大量のデバイスに対しても即時発行を可能とするとともに、様々なデバイスへの適用を実現。

ブロックチェーン



デバイスプロビジョニングシステム

*2018 年 5 月 18 日国内特許取得（特許 第 6340120 号）

プロビジョニングサーバー主導で、デバイスの登録、公開鍵の格納、電子認証に紐づく秘密鍵を配布し、デバイスの適用から運用フェーズの自動化を実現。

 : 秘密鍵

 : 公開鍵



IoT の設計から開発、量産、運用まで一貫性のあるセキュリティ対策のための電子認証を提供

① 安全性 Safety

電子証明の発行・適用・運用を自動化し、人的ミスを抑制するとともに運用工数を大幅に削減

② 機密性 Confidentiality

デバイスの管理画面、ID / パスワードを不要にし、攻撃ポイントとなるポート解放不要

③ 追跡性 Traceability

デバイスごとに固有のデジタル ID を付与することで情報の真正性も実現

④ 適用性 Adaptability

システムはファンデーションソフトウェアで構成しているため、様々なシステムとの API 連携が可能

お問い合わせ窓口

アイビーシー株式会社

【本社】

〒104-0033

東京都中央区新川1-8-8 アクロス新川ビル 8F

TEL : 03-5117-2780 FAX : 03-5117-2781

【西日本事業所】

〒532-0004

大阪府大阪市淀川区西宮原2-7-38 新大阪西浦ビル 3F

TEL : 06-7653-1014 FAX : 050-3473-4160

〈URL〉

コーポレートサイト → <https://www.ibc21.co.jp/>

ソリューションサイト → <https://system-answer.com/>

