IoTサービスの必要条件：『IoT管理システム』の継続性

影響を限定するUI分離

UI

UI ライブラリ

障害検知、対応時間を短縮する『ビッグデータ分析システム』

ログ
モニタリング

ログ
分析

ログ収集

IoT管理システム
（MDMエンジン）

負荷テスト

※100万台以上可能

デバイス
シュミレータ

同期

ログ分析結果に基づく、シュミレーション

確実に処理を実行する、新『同期』メカニズム

99.999%の稼働率を確保するアーキテクチャー

IoTサービス最大の課題：安心安全な IoTシステムの維持

安心安全なIoTシステムは、設計時ではなく、運用・保守時に最大のリスクを抱える。
ローカルログイン、リモートログインによる個別アップデートは、コストや運用面で問題。

大項目	指針	要点
方針	指針1 IoT の性質を考慮した基本方針を定める	要点 1. 経営者が IoT セキュリティにコミットする
		要点 2. 内部不正やミスに備える
分析	指針2 IoT のリスクを認識する	要点 3. 守るべきものを特定する
		要点 4. つながることによるリスクを想定する
		要点 5. つながりで波及するリスクを想定する
		要点 6. 物理的なリスクを認識する
		要点 7. 過去の事例に学ぶ
設計	指針3 守るべきものを守る設計を考える	要点 8. 個々でも全体でも守れる設計をする
		要点 9. つながる相手に迷惑をかけない設計をする
		要点 10. 安全安心を実現する設計の整合性をとる
		要点 11. 不特定の相手とつなげられても安全安心を確保できる設計をする
		要点 12. 安全安心を実現する設計の検証・評価を行う
構築・接続	指針4 ネットワーク上での対策を考える	要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける
		要点 14. 機能及び用途に応じて適切にネットワーク接続する
		要点 15. 初期設定に留意する
		要点 16. 認証機能を導入する
運用・保守	指針5 安全安心な状態を維持し、情報発信・共有を行う	要点 17. 出荷・リリース後も安全安心な状態を維持する
		要点 18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える
		要点 19. つながることによるリスクを一般利用者に知ってもらう
		要点 20. IoT システム・サービスにおける関係者の役割を認識する
		要点 21. 脆弱な機器を把握し、適切に注意喚起を行う

出展：IoT セキュリティガイドライン ver 1.0（総務省）表３　セキュリティ対策指針一覧

IoTの最大の課題は、セキュリティを維持する安価で、汎用的な手段がないこと

IoTは比較的長く使われることが想定されています。そのため、設計時に安全であっても、 5年10年使う間に、脆弱性が発見されたり、新たな攻撃手法が開発されたりすることが考えられます。

セキュリティ対策としては、脆弱性に対応したOSやアプリにアップデートしてもらう以外に利用者には選択肢はありません。

IoT機器は、画面やキーボードが無いことも考えられるが、大量のデバイスのアプリやOSを、どうすれば効率良く（安く、早く、安全に）アップデートできるかが鍵になります。

安心安全なIoTサービスを実現する『IoT管理システム』

MDMのAPIを拡張し、大量のIoTデバイスの脆弱性を、遠隔からリモートログインせず、全自動で、サイレントに、アプリを配布・更新・削除し、OSのアップデートを行う事で解決。