2－1　モニタリング機器の追加でIoTセキュリティ監視を提供

IoT向け対策技術

多様なIoT機器に自動適応して動作を監視・解析し、セキュリティ異常を検知します。

特長

① **未知なものを含む多様なIoT機器に対応したIoTシステムの動作監視・解析**
新たなIoT機器や、用途が多様化したとしても、自動的に適応して動作を監視・解析します（IoT機器特徴学習技術）。
IoT機器自体に特別な機能を備える必要がありません（IoT機器挙動監視技術）。

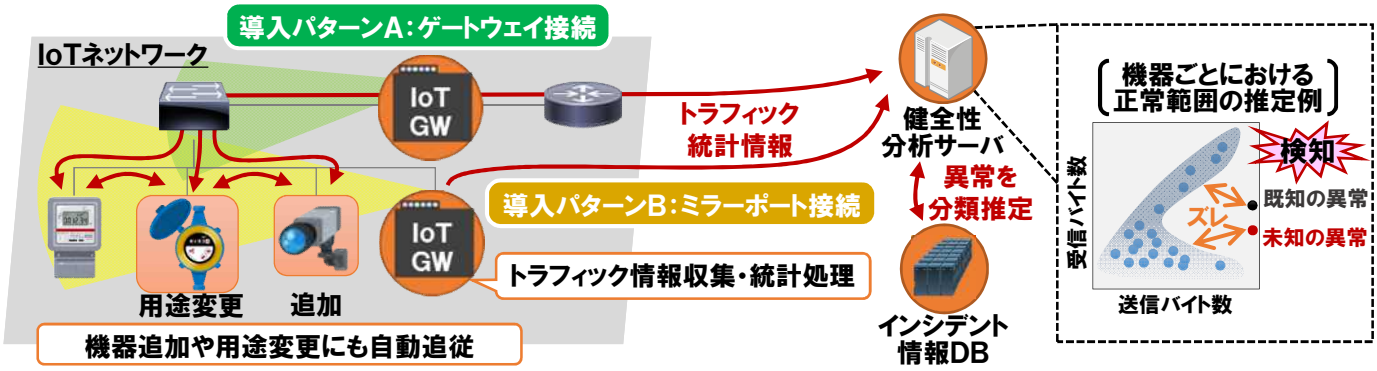
② **膨大なIoT機器により構成されたIoTシステムの動作監視・解析**
膨大なIoT機器を接続方法によらず自動検出し、効率的に導入できます（監視対象自動設定技術）。
複数IoTシステムからの結果を安全に集約・解析して異常を分類推定します（IoTシステム統合解析技術）。

③ **重要インフラ事業者向けセキュリティ監視サービスの導入・運用**
事業者毎の利用形態や既存管理システムに合わせ、2020時代に適した柔軟なIoTセキュリティ監視サービスを提供します（IoTセキュリティ監視サービス）。

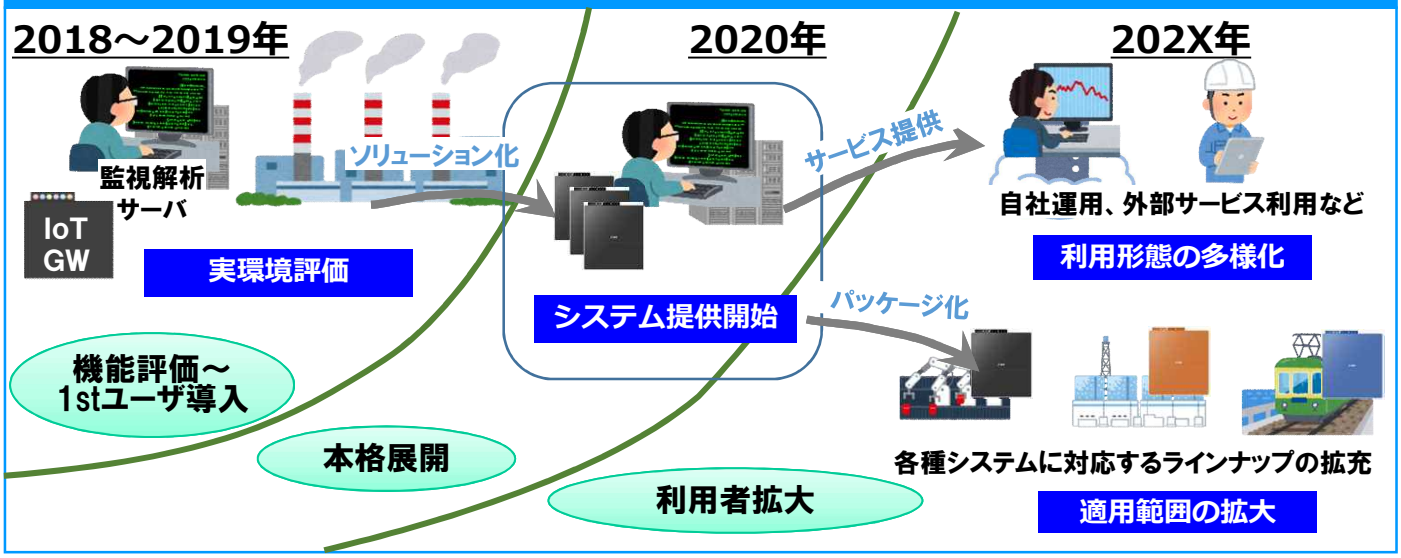
急速なIoT化に伴い脅威が拡大しているため、IoTが招くセキュリティ事故に備える必要があります。

IoT機器改造やシステム構成変更を伴わず導入可能で、多様なIoT機器の新たな脅威にも即時対応可能です。

お客様環境に応じて、健全性分析サーバおよびインシデント情報DBはMSSとしても提供可能です。
IoT GWをお客様環境に設置して頂くことは必須となります。



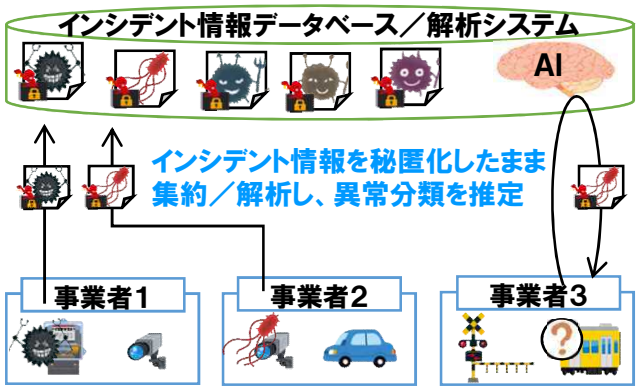
IoT GWを用いたセキュリティ技術の社会実装、ビジネス展開



戦略的イノベーション創造プログラム（SIP）　【三菱電機、日本電信電話】

2－1　モニタリング機器の追加でIoTセキュリティ監視を提供

インシデント情報を安全に集約して分類を推定します



大量なIoT機器からリアルタイムに情報を収集します

攻撃検知には、大量のIoT機器から行われる通信の
一つ一つを、漏れなく統計情報化する必要があります。

対象システム例：　映像監視の場合
カメラ256台 x 4種類の通信フロー ＝ 1024通信フロー

		要件	本技術
統計情報収集	①フロー数 ②項目数	①1024フロー以上 ②9項目以上 （5tuples+通信量）	①5000 ②17項目 （+フラグ情報）
通信転送性能		1Gbpsワイヤレート	

異常検知と異常分類の推定を併せもつ技術を開発（既存技術との比較）

AIを活用したホワイトリスト方式の拡張によって、ホワイトリストの自動生成と異常分類の推定を実現

	ブラックリスト方式	ホワイトリスト方式	本技術（ホワイトリスト方式拡張）
既知の攻撃による異常検知	○	○	○（自動）
未知の攻撃による異常検知	×	○	○（自動）
異常分類の推定	○	×	○

［ブラックリスト方式］

- 既知の異常を定義
  ⇒ 異常分類の推定が可能
- 定義されていない未知の
  攻撃は対処不可

［ホワイトリスト方式］

- 正常動作を定義
- 異常検知は可能だが
  異常分類の推定は不可

［本技術］

- 正常動作を自動定義
- 異常分類の推定も可
- IoT機器の追加および
  変更に自動追従

導入構成

① SI提供（オンプレミス）

- 自社にてセキュリティ運用が可能な
  事業者様向けにオンプレミスで
  フルセットを提供

② パッケージ提供＋サービス提供

- IoT GW設置のみでユーザは特別な
  知識を必要としない遠隔セキュリティ
  監視サービスとして提供
- 高精度な異常分類推定が可能な
  インシデント情報DBサービスを
  付加価値として提供