ZETA Alliance　TOPPAN

狙われる「IoTデバイス」へのセキュリティ対策
～ セキュアアクティベートサービス®～

IoTにおけるトレンド
国家的・組織的サイバー攻撃も増大~IoTデバイスが主要ターゲットに

- 近年のサイバー攻撃の約半数がIoTデバイスを狙ったもので、2019年の攻撃対象ではIoTデバイスが第一位に
  （出展：情報通信研究機構 NICTER 観測レポート2019）
- 多くのIoTデバイスはセキュリティ対策が不十分で脆弱 ~ IoTデバイスへの攻撃や管理不徹底による事故が増加
- 閉域ネットワークであれば安全とされてきた領域でも、IoTデバイスの接続により完全なクローズ環境ではなくなってきている

求められる対策の方向性
IoTデバイスの強固な認証と、確実なライフサイクル管理が重要

❶ 接続先との認証面の強化	⇒ 電子証明書を活用した認証（PKI） ID・PW等による認証等に比べ強固な認証
❷ ハードウェア面の強化	⇒ デバイスへの組込みセキュアエレメント（SE） PKIにおいて重要な認証情報をセキュアに格納・保持
❸ 管理面での安全性・効率性確保	⇒ 電子証明書の有効性によるデバイスの適切なライフサイクル管理 散在するデバイスに対し、リモートでセキュアかつ効率的に

ZETAのセキュリティ
PKIやSEによる、さらなる国際標準にも準拠するIoTデバイスセキュリティ

ZETAでは、独自のアルゴリズム・方式を採用したエンドポイントのIoTデバイス認証や、データ暗号化、
ホワイトリストによる不正デバイスの介入防止などの、IoTデバイスへのセキュリティ対策がなされています。

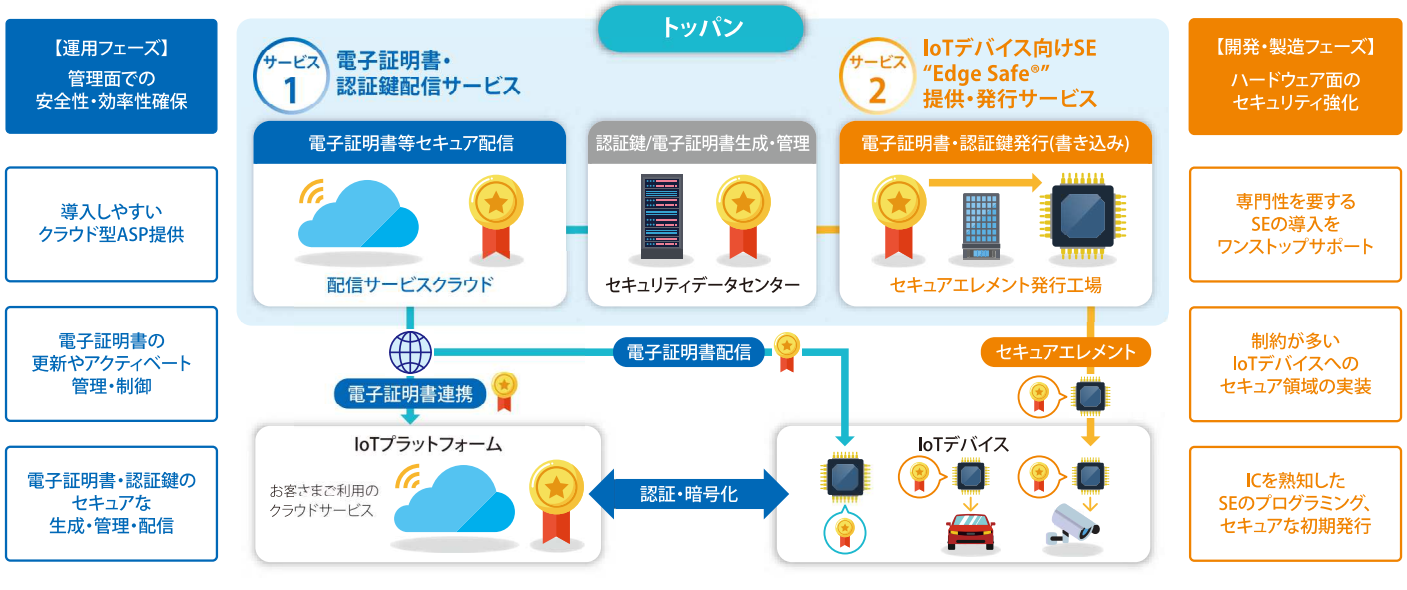
＋

国際標準である楕円曲線暗号を使った「PKI認証」にも対応（FIPS（米国連邦情報処理標準）への準拠）すること、
IoTデバイスへのハードウェアとしてのセキュア領域を保持することで、さらなるセキュリティ対策の充実が図れます。

提供ソリューション
IoTデバイスの認証強化と運用効率化 「セキュアアクティベートサービス®」

- IoTデバイスの認証に、電子証明書を用いたセキュアな認証を採用
- IoTならではのハードウェアセキュリティと、その運用業務の安全性確保と効率化を支援

サービス①　電子証明書・認証鍵配信サービス：IoTデバイスの、電子証明書によるライフサイクルのリモート管理ASP
サービス②　IoTデバイス向けSE(Edge Safe®)提供・発行サービス：IoTデバイスの認証情報保護に向けた、SEのプログラム開発・発行・提供



凸版印刷株式会社