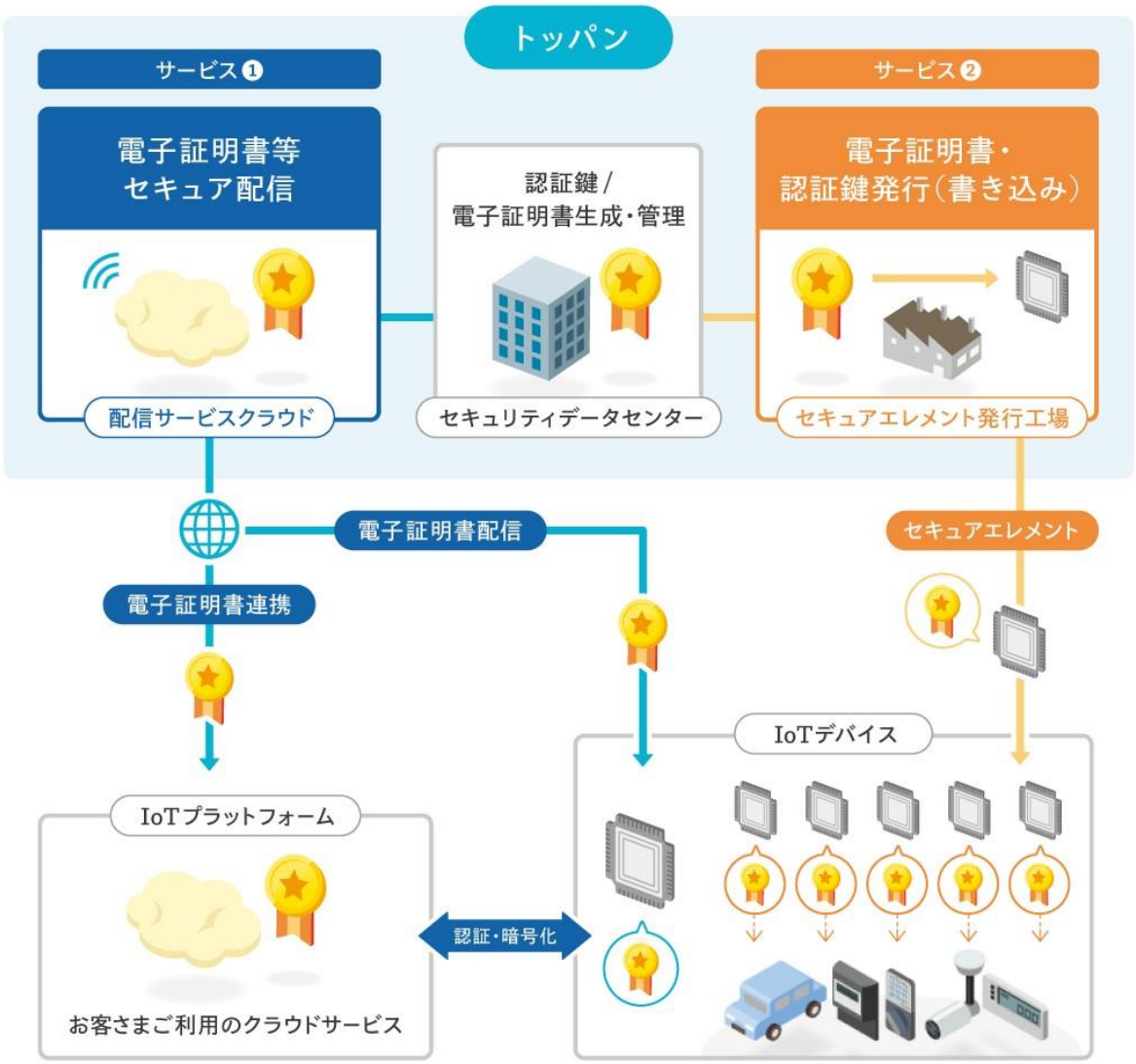
セキュアアクティベートサービス™

近年、増えるハッキングや不正アクセスをはじめとしたIoTデバイスのサイバー攻撃リスクに、高度なセキュリティを備える**「電子証明書・認証鍵配信サービス」**と**「IoTデバイス向けセキュアエレメント（SE）提供・発行サービス」**の2つのサービスで備えます。これらのサービスには、トッパンが長年に渡るICカード（ICチップ）の取り組みで培ったセキュリティへの技術開発・ファシリティなどの実績・ノウハウ・が活かされています。



→ サービス❶ **電子証明書・認証鍵配信サービス**　→ サービス❷ **IoTデバイス向けセキュアエレメント(SE)提供・発行サービス**

IoTデバイスのサプライチェーンを含むライフサイクル管理が可能

●厳重な管理・運用が求められる電子証明書・認証鍵などの認証情報を、トッパンのセキュアな環境で生成・発行・管理の上、IoTデバイスへ配信。IoTデバイスの認証情報の更新・無効化・消去など、適切なライフサイクル管理をリモートで実現。

提供機能

- ID管理
- 認証鍵配信
- デバイス認証
- 認証鍵更新
- セキュア接続
- 認証鍵消去

トッパンの高セキュリティな環境でIoTデバイス向けSEを発行

●金融系ICカード業務も取り扱うセキュリティ性の高い工場で、SEにファームウエアや認証鍵、電子証明書等の重要情報を発行
●このSEをIoTデバイスへ搭載することで、限られたリソースでも電子証明書・認証鍵などの厳重に守るべきデータを分離して格納・保持することが可能に。

提供機能

- 重要データ保護
- Root of Trust
- セキュアプログラミング
- セキュアアップデート

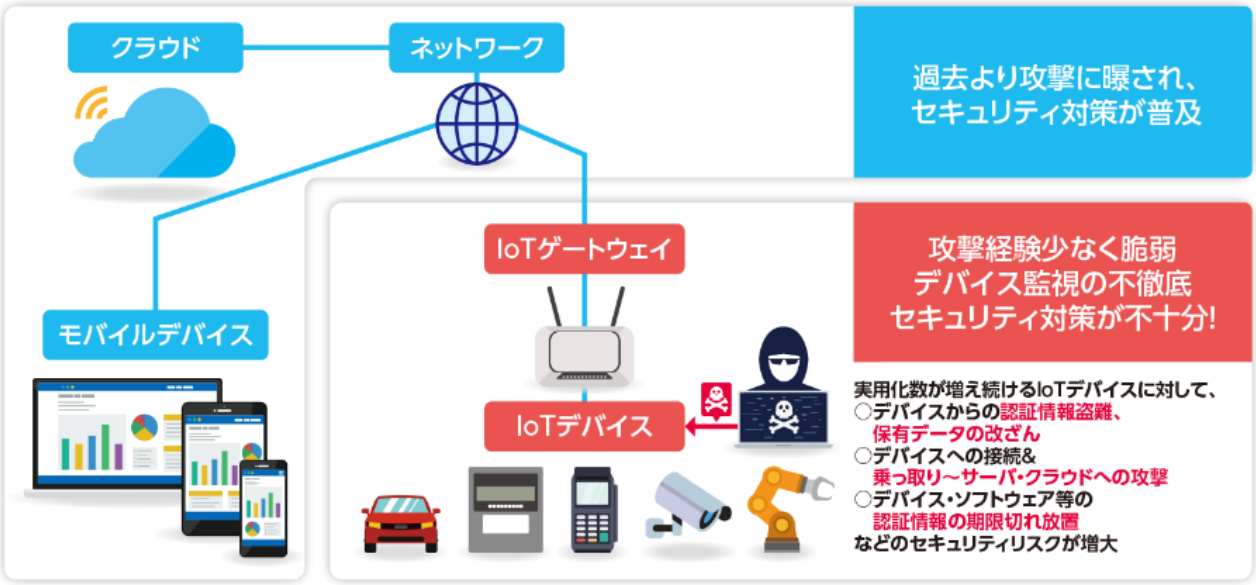
※本情報は2021年9月現在のものとなります。サービス情報は変更となる場合がございます。

© TOPPAN INC.

背景　なぜセキュアアクティベートサービスが必要か？ IoTデバイスのリスクと、セキュリティ対策の必要性の高まり

IoT活用時、ITインフラ（クラウド・ネットワーク・IoTゲートウェイ）やスマホ等のモバイルデバイスは、これまでにサイバー攻撃を受けた歴史からセキュリティ対策が普及している一方、多数のIoTデバイスはセキュリティ対策が不十分で無防備な状態にあります。近年、IoTデバイスへの攻撃や管理不徹底によるセキュリティ事故が増加しており、早急な対策が求められています。

※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1位となっています。（出典：情報通信研究機構 NICTER 観測レポート 2019）



事例　IoTデバイスが原因のセキュリティ事故例

IoTデバイスの「脆弱性」や「管理の不徹底」により発生したセキュリティ事故をご紹介します。

IoTデバイスへの不正アクセス・ハッキング

事例①｜監視カメラへのハッキング～石油パイプラインの爆発
海外石油工場に設置された防犯カメラへのハッキングにより、一定期間の映像記録が消失。
その間に不審者が侵入したものと見られ、その後石油パイプラインが爆発した。

事例②｜自動車へのハッキング～認証情報の盗難
ネットワーク接続された自動車へのハッキングを通じて認証情報が盗難され、
自動車メーカーのクラウドサーバへ不正アクセスされた

各種電子証明書の有効期限切れ

事例③｜ウェブ会議サービス～一時アクセス不能に
ウェブ会議サービスにおいて、サーバ証明書が期限切れになり、一定時間ユーザーがアクセスできなくなった。

事例④｜ヘルスケアデバイス～商品回収の事態に
ヘルスケアデバイスのサーバ証明書が期限切れになり、デバイスが動作しなくなったため
メーカーにて商品回収となった。

事例⑤｜ヘッドマウントディスプレイ～ソフトウェアが稼働不能に
ヘッドマウントディスプレイのソフトウェア証明書が期限切れになり、認証エラーが発生し利用不可となった。

<お問合せ先>
https://solution.toppan.co.jp/secure/service/secureactivate.html

より詳細な資料もございますので、お気軽にお問合せください！

※本情報は2021年9月現在のものとなります。サービス情報は変更となる場合がございます。
© TOPPAN INC.