Orchestrating a brighter world NEC

ID・鍵管理ソフトウェア

SecureWare/Credential Lifecycle Manager ご紹介資料

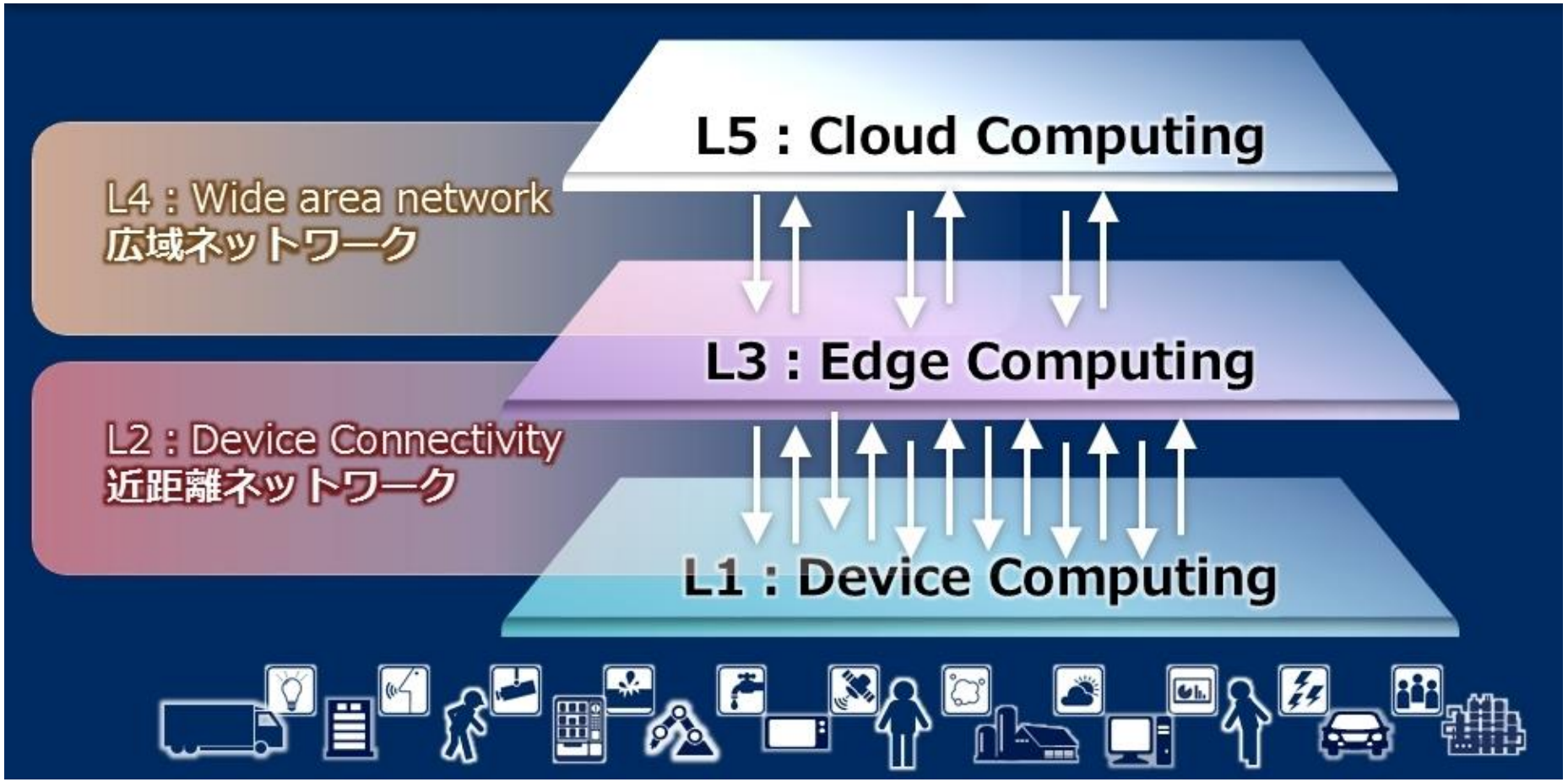
日本電気株式会社

サイバーセキュリティ事業統括部

IoTデバイス利用における課題
（セキュリティの観点から）

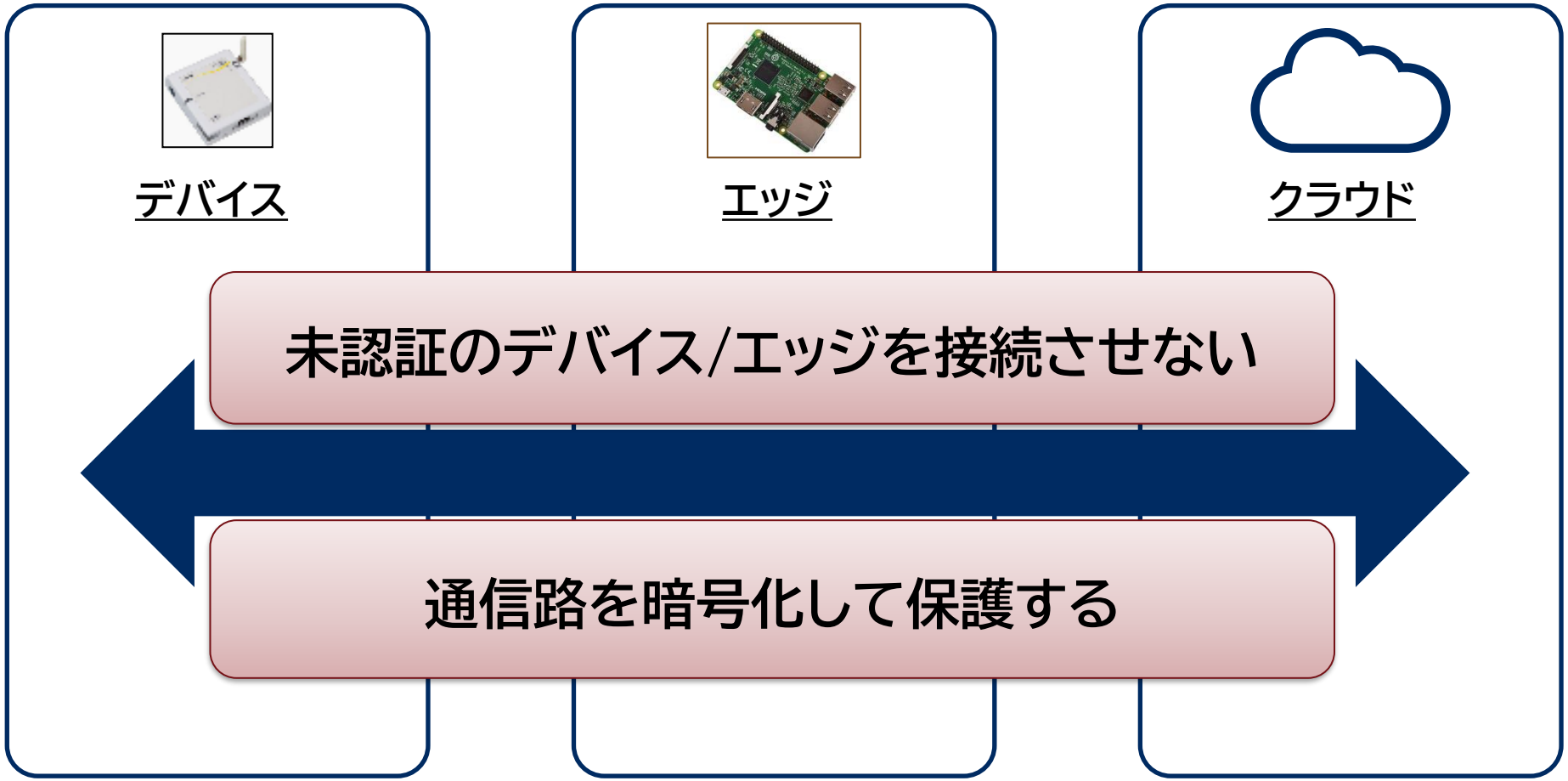
NECが考えるIoTアーキテクチャモデル

NECはIoT領域における共通のアーキテクチャモデルとして下図の5層で表すモデルが最適と考えます。



IoTシステムを安全に利用するため最初に実施したいこと

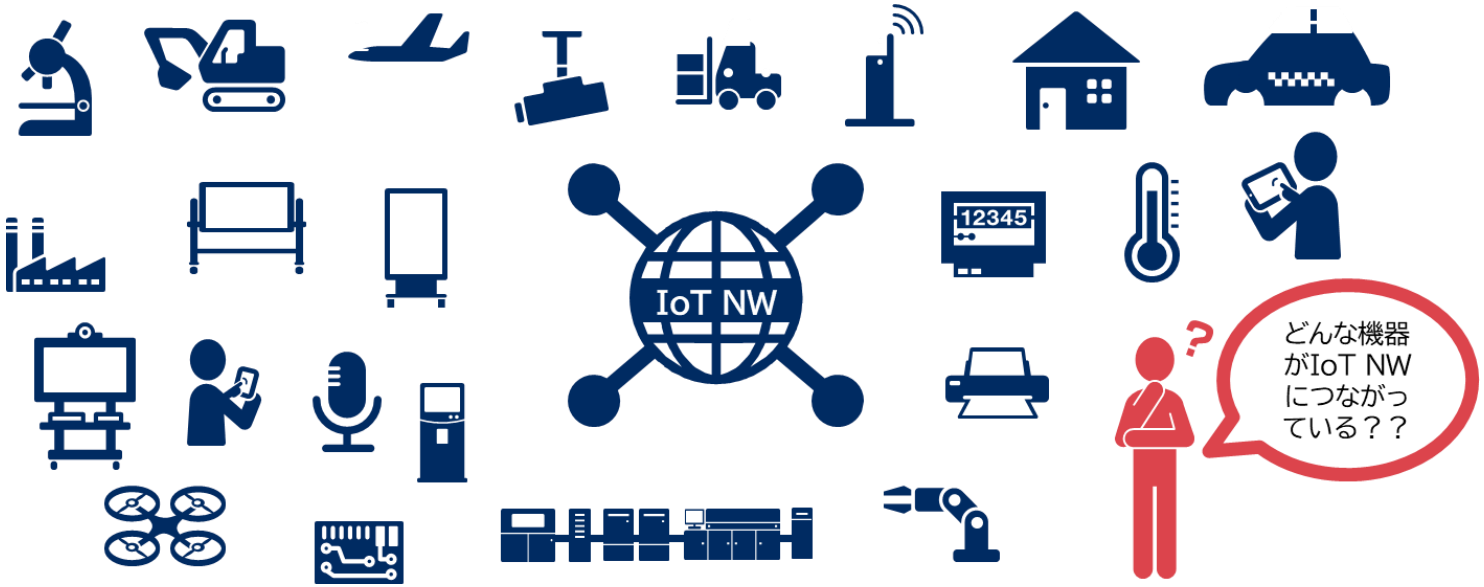
「認証(特定)」と「暗号化」がすべてのセキュリティの基礎です。



[課題1] 大量のデバイスを個体管理できていない

デバイスが特定できなければ安全なIoTネットワークとは言えない。

- 事業者にとって危険な通信が発生している可能性がありますが、それがどのデバイスなのか分からないと対処できません。
- 従業員が持ち込んだデバイスがネットワークにつながると、セキュリティ設定の不備などにより、そこから情報漏えいが起こる可能性があります。



[課題2] クラウドサーバとの相互認証/通信暗号化に苦労する

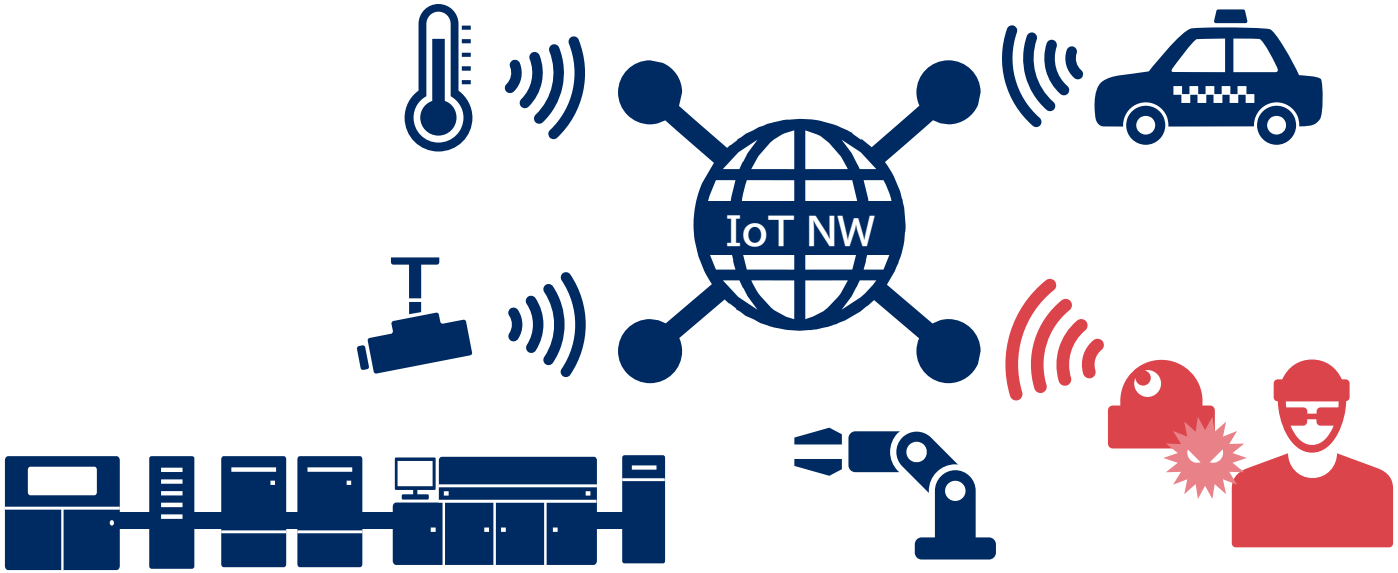
相互認証と暗号化通信に必要な電子証明書の発行は煩雑で大変。

- IoTプラットフォームを提供する各社ともにエッジとクラウド間の通信は相互認証と暗号化が必須です。
  - インターネットを経由するので、平文での通信では情報漏えいにつながります。
- 相互認証と暗号化通信をするためには、例えば電子証明書を取得しなければなりませんが、必要な知識や作業が膨大であり、担当者は苦労します。
  - デバイスの数も膨大であるので、大変さはさらに増します。

[課題3] エッジ－デバイス間の通信暗号化も必要

近距離ネットワークの通信も狙われる可能性がある。

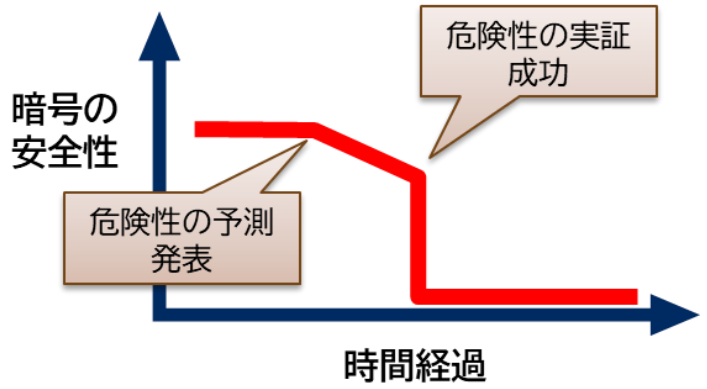
- エッジ-デバイス間の通信も暗号化しないと、業務に思わぬ悪影響をもたらす可能性があります。
  - 業務秘密が詰まったセンサーから送信される情報を盗聴されることで、ノウハウが盗まれる可能性
  - 通信内容から脆弱性を推定され、サイバー攻撃（DDoS攻撃など）にデバイスが悪用されてしまい、加害者側に立ってしまう可能性



[課題4] 脆弱性が発見された場合、鍵の更新に苦労する

次の場合に「鍵の無効化」と「鍵の再発行」が必要となる。

- アプリケーションの脆弱性により秘密鍵が流出し、重要情報が第三者に漏えいすることがあります。
  - 例）2014年、OSSの暗号化ライブラリ「OpenSSL」に “Heartbleed” と呼ばれる致命的なバグが見つかり、秘密鍵の流出や暗号化通信の傍受が発生した。
  - 例）セキュリティ設定の誤りにより、一定期間、サーバのパスワードファイルや秘密鍵がインターネットに公開されていた。
- デバイスは長期にわたり利用されますが、その間に鍵（暗号）の安全性が破られることがあります。
  - 例）SHA-1は1995年に発明されたが、2005年に理論上の危険性が予測され、2017年にGoogleが危険性の実証に成功。
  - コンピュータ技術向上や性能向上、数学研究の発展により、このようなことが起こります。



［課題5］高度なスキルを持った人材の確保が困難

ここまでの課題を人手で解決するには、担当者の負担が大きい。

- ◆ 求められるスキルセット
  - ■ IoTデバイスの管理と運用スキル（設置から撤去まで）
  - ■ 電子証明書・暗号鍵運用のスキル
  - ■ 暗号に関わる脆弱性が事業に与えるリスクを理解し、対応できるスキル
- ◆ セキュリティ人材は世界的に不足
  - ■ ITセキュリティで人材不足が顕著
  - ■ IoTセキュリティはこれから発展する領域であるため、現時点で不足

SecureWare/Credential Lifecycle Manager がこれらの課題を解決します

- ID発行・デバイス認証
- 電子証明書・共通鍵の発行
- ID・鍵発行/無効化の自動化

課題の整理

前掲の課題の内、SecureWare/Credential Lifecycle Manager が解決可能な課題は以下の通りです。

前掲の課題	本製品が解決可能な課題	対応機能
[課題1] 大量のデバイスを個体管理できていない	デバイスへのID発行と認証を行う必要がある	• ID発行・デバイス認証
[課題2] クラウドサーバとの相互認証/通信暗号化に苦労する	相互認証と暗号化通信に必要な電子証明書や共通鍵の発行、および運用が大変	• 電子証明書・共通鍵の発行 • ID・鍵発行/無効化の自動化
[課題3] エッジ－デバイス間の通信暗号化も必要		
[課題4] 脆弱性が発見された場合、鍵の更新に苦労する		
[課題5] 高度なスキルを持った人材の確保が困難	人的負担の軽減が必要	• ID発行・デバイス認証 • 電子証明書・共通鍵の発行 • ID・鍵発行/無効化の自動化

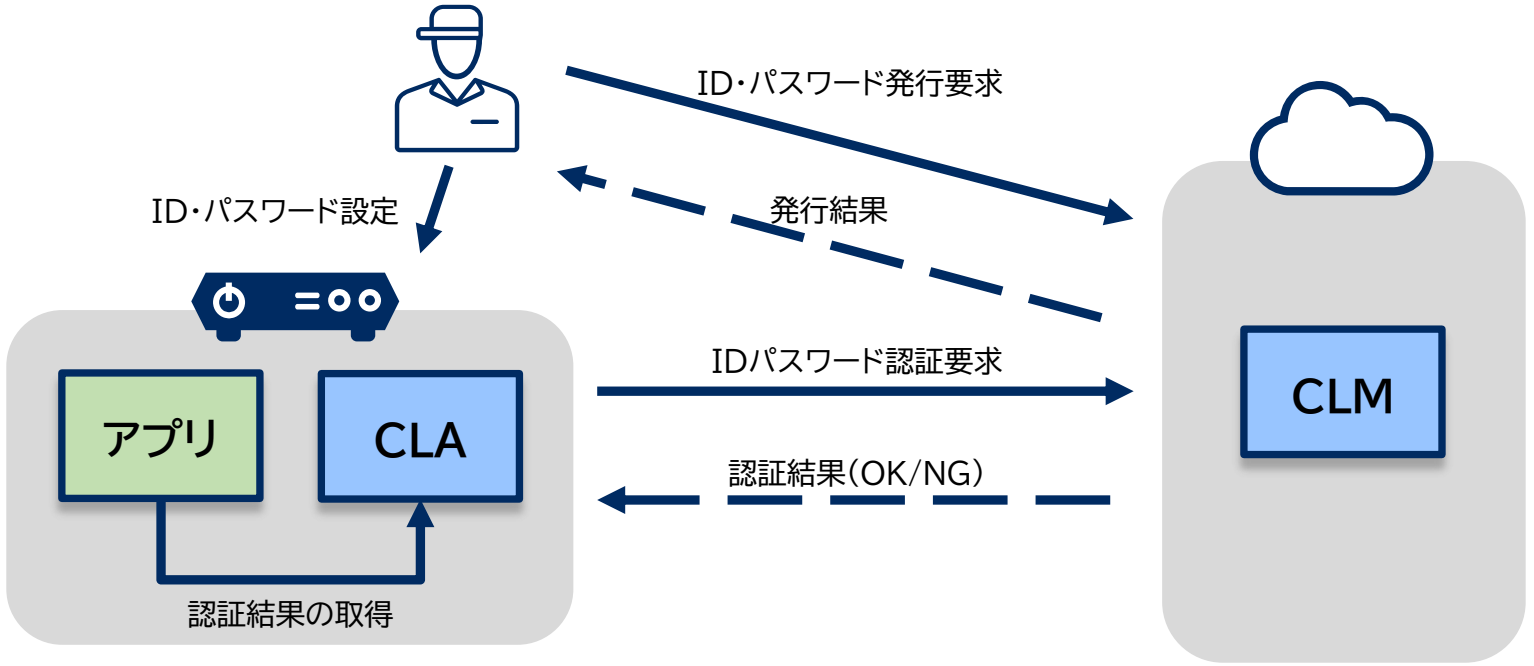
SecureWare/Credential Lifecycle Manager がこれらの課題を解決します

- ID発行・デバイス認証
- 電子証明書・共通鍵の発行
- ID・鍵発行/無効化の自動化

IDを発行し、デバイス認証が可能

IDとパスワード（事前認証キー）を発行し、簡易な認証が可能。

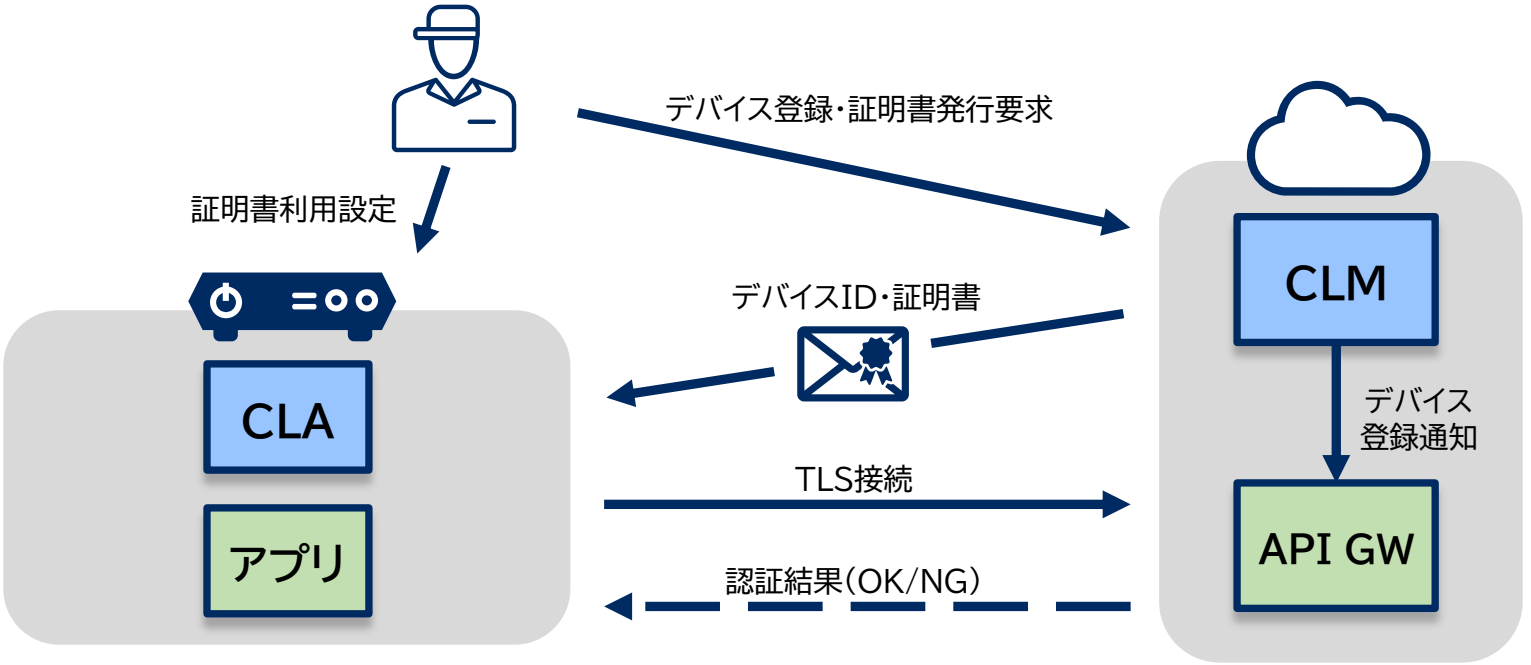
- SecureWare/Credential Lifecycle Manager がIDとパスワード（事前認証キー）を発行することで、ID・パスワードによるデバイス認証が可能です。
- デバイス認証の結果を利用して、IoTアプリケーションの利用制御が可能です。



証明書認証によるデバイス認証

デバイス登録時に証明書を発行し、相互認証を実現

- 証明書認証方式では、エッジ本体やアプリケーションがクラウド上のデバイス管理基盤と相互認証を実現でき、IoTシステム全体の安全性向上が望めます。



※ **API GW:**NECモバイルバックエンド基盤 API Gateway

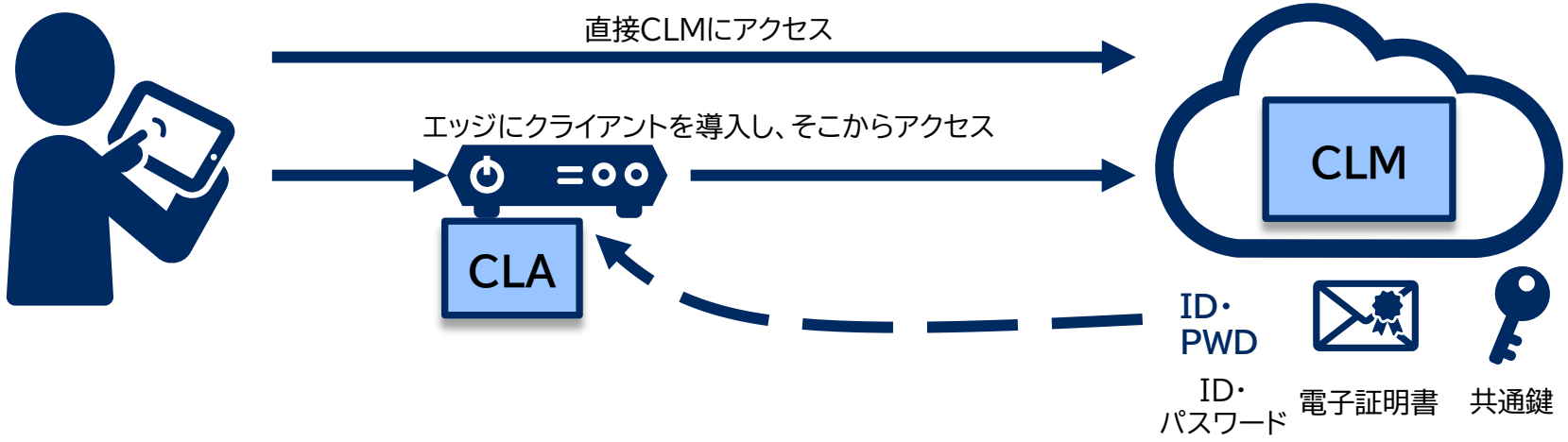
SecureWare/Credential Lifecycle Manager がこれらの課題を解決します

- ID発行・デバイス認証
- 電子証明書・共通鍵の発行
- ID・鍵発行/無効化の自動化

ID・鍵の発行作業を統一手順化し、どこからでも発行可能

簡単な手順で誰でも作業可能

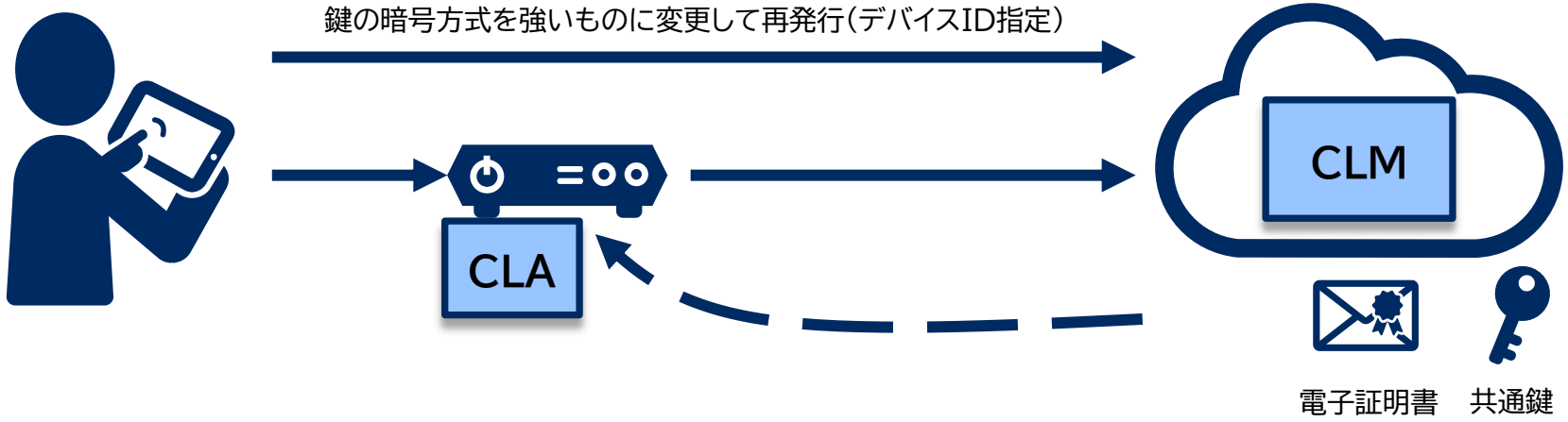
- SecureWare/Credential Lifecycle Manager の管理画面にログインしてデバイス情報を入力するだけで、IDと電子証明書を取得可能です。
- 共通鍵も同様の作業で取得可能です。
- デバイス管理システムと連携することでこれらの作業を自動化可能です。



鍵の更新が容易

鍵(暗号)に関する脆弱性が発表されても直ちに対応可能

- 電子証明書の初回発行時と同じ手順で更新ができます。
  - 暗号方式をより強いものに変更し、統一手順で再発行
  - 証明書や共通鍵の提供にかかるリードタイムを短縮可能
- 再発行のリードタイムを短縮し、従来より短期間・安価にセキュリティリスクへの対応が完了します。



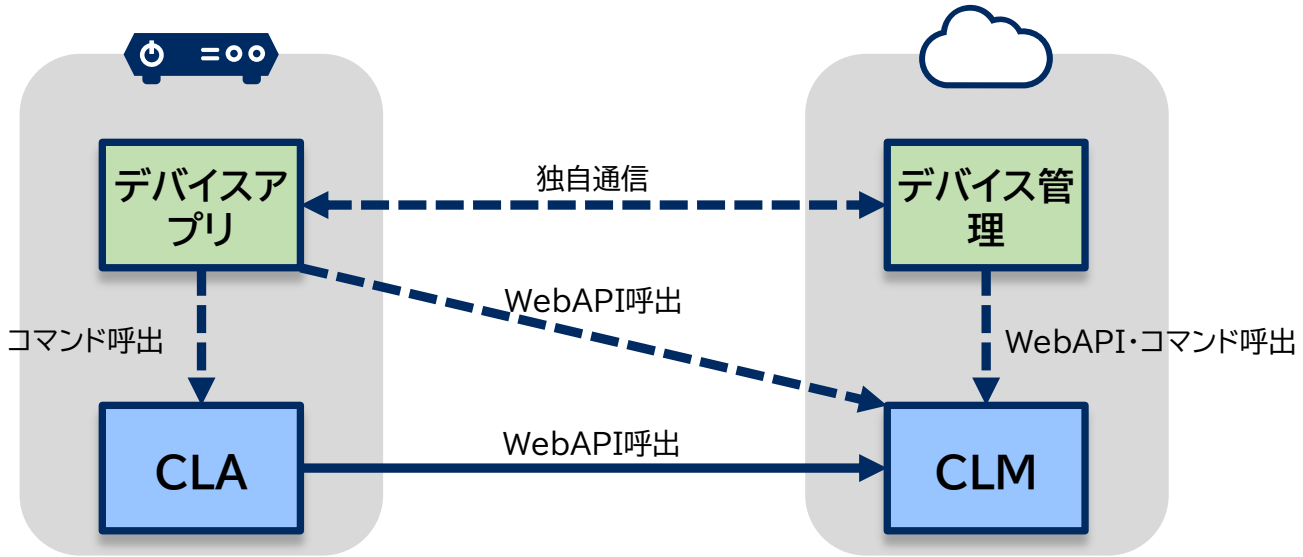
SecureWare/Credential Lifecycle Manager がこれらの課題を解決します

- ID発行・デバイス認証
- 電子証明書・共通鍵の発行
- ID・鍵発行/無効化の自動化

ID・鍵情報の自動発行/自動無効化が可能

デバイス管理システムから利用可能なAPI・コマンドを提供

- SecureWare/Credential Lifecycle Manager の機能を外部から利用可能なWebAPI・コマンドを提供します。
- これをデバイス管理システムから利用することにより、デバイスのライフサイクルに合わせて、ID・鍵情報の自動発行および自動無効化が可能となります。
- デバイスの追加時に人為的作業なしに、IoTネットワークの安全性を高めることができます。



SecureWare/Credential Lifecycle Manager
製品紹介

SecureWare/Credential Lifecycle Manager 概要

IoTに必要な認証情報(ID・鍵)をリモートで安全に発行・管理でき、エッジ/デバイスのライフサイクルに合わせた認証制御が可能

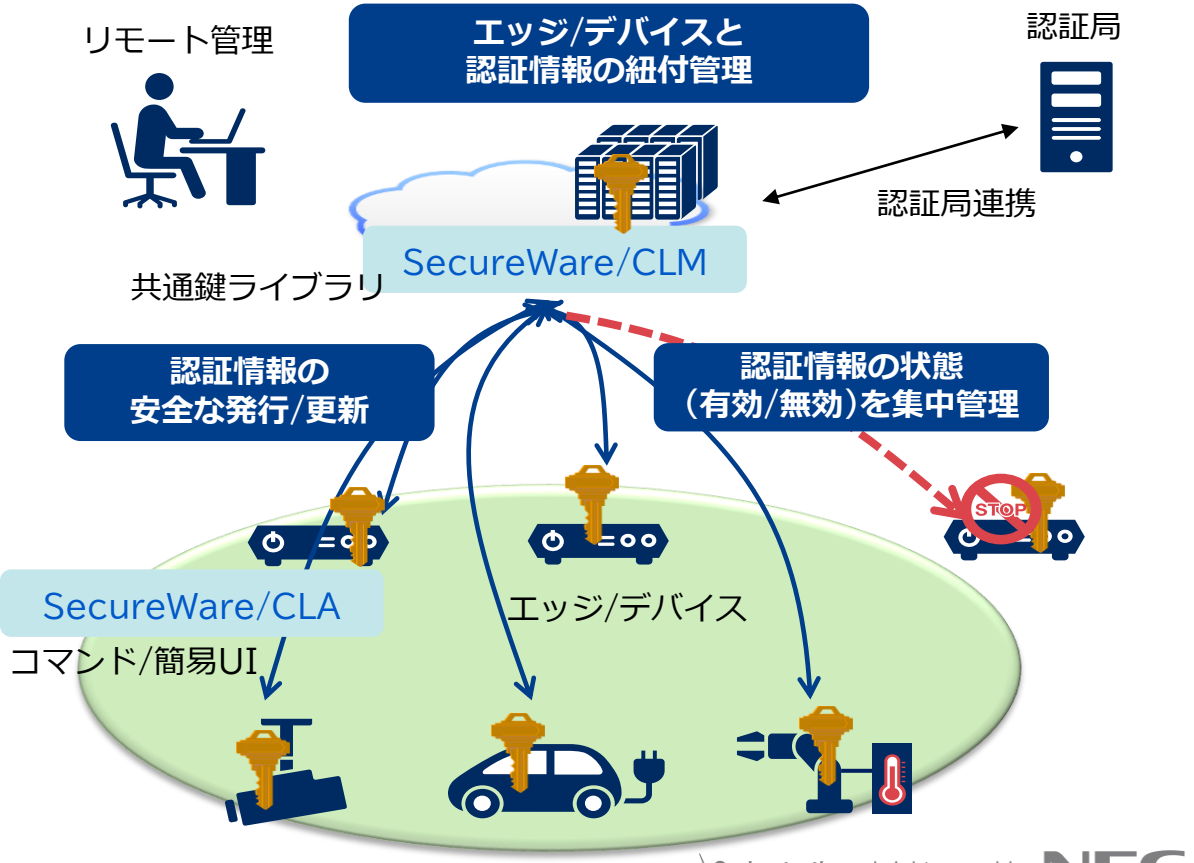
導入によるメリット

- **どこからでも安全に認証情報を発行**
  大量のエッジ/デバイスの認証情報(ID・鍵)をリモートで安全に人手を掛けず管理可能
- **統一的な発行手順**
  デバイス用のID/パスワードに加え、公開鍵や共通鍵などが同じ手順で容易に生成可能
- **セキュリティ強度の高い認証情報を提供**
  認証局(CA局)と連携した公開鍵証明書発行に加え、JCMVP認定レベルの共通鍵生成など強度の高い認証情報を生成

商品情報

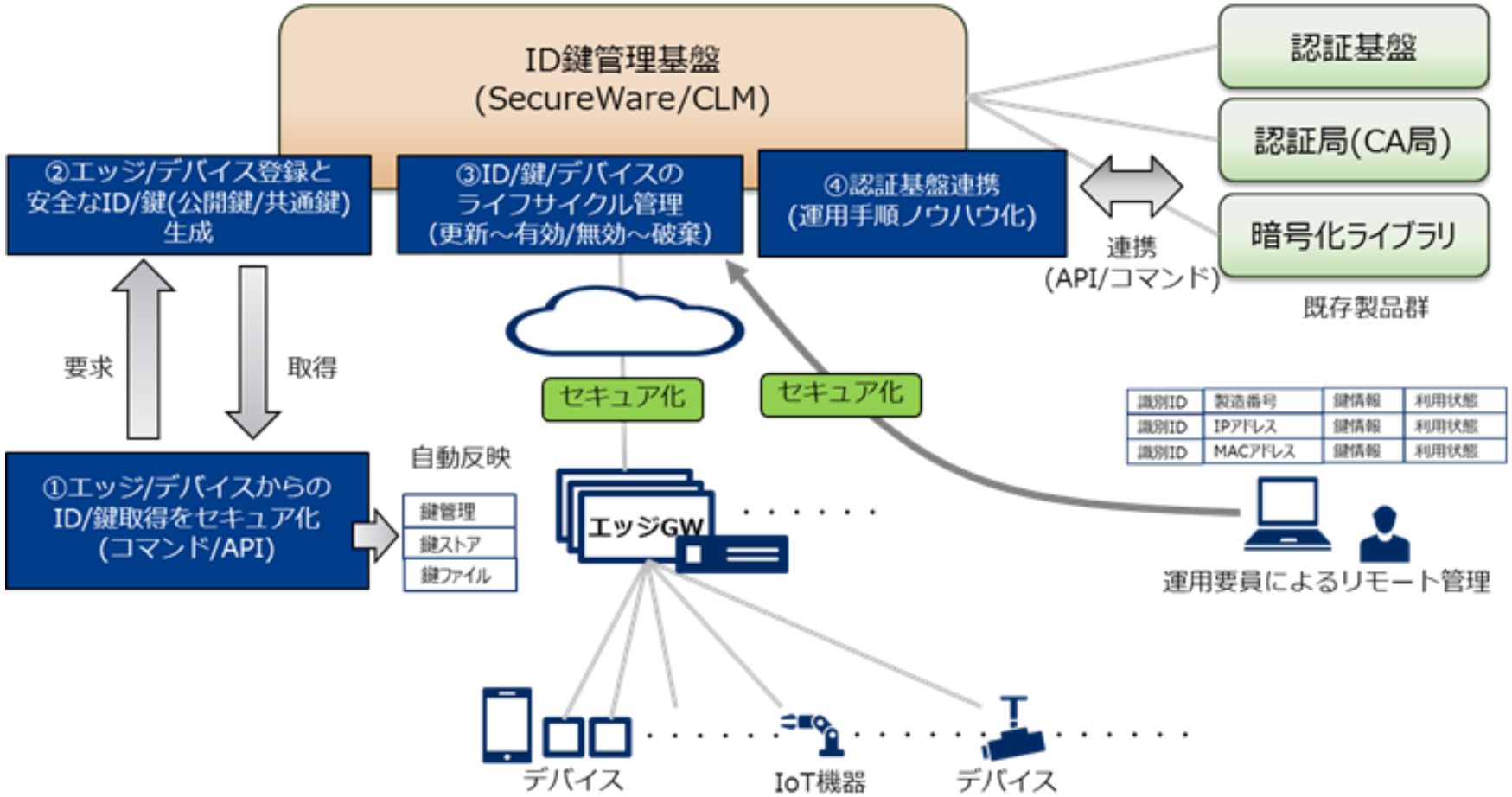
- エッジ/デバイスの認証情報を一元管理可能なID鍵管理システムを実現できるソフトウェア製品
  - SecureWare/CLM(サーバ製品)
  - SecureWare/CLA(クライアント製品)

活用イメージ



SecureWare/Credential Lifecycle Managerの提供機能概要

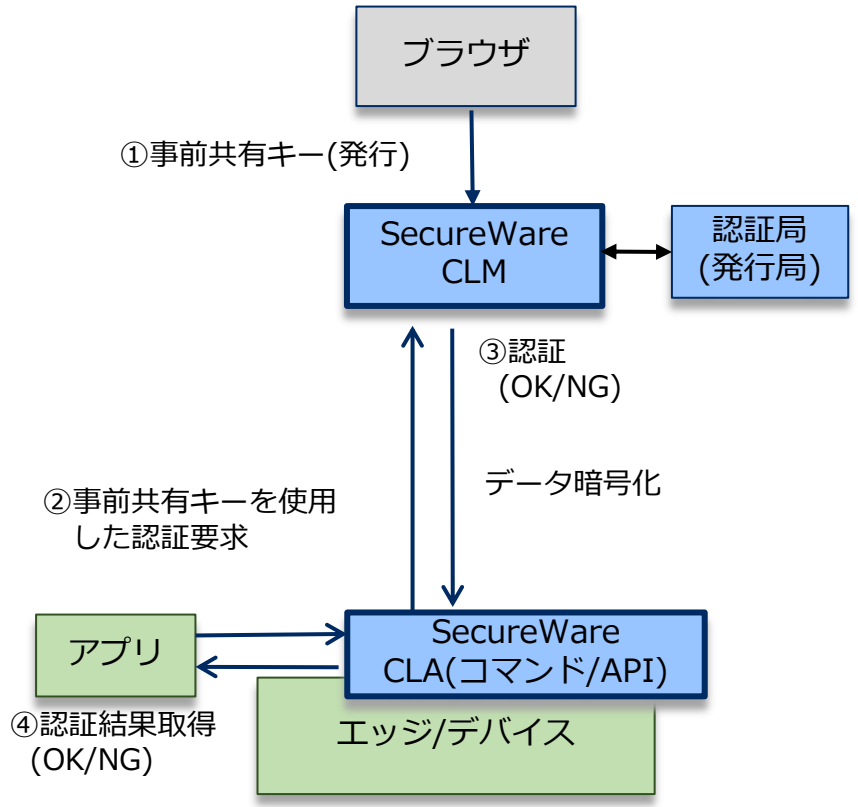
大量のエッジ/デバイスをリモートから人手を掛けずに相互認証/暗号化通信を確立するために必要となるIDと鍵を共通基盤で提供



①②エッジ/デバイスへのセキュアな鍵発行と管理

エッジ/デバイスからのID/鍵取得をセキュアに実行できます

- CLMで事前共有キーを発行し、エッジ/デバイス側に設定すると、正しいエッジ/デバイスであることを特定して認証します。この後、エッジ・デバイスから暗号化通信により、安全にID/鍵取得ができるようになります。



エッジ/デバイス登録と安全なID/鍵(公開鍵/共通鍵)生成します

- CLMでは、どのエッジ/デバイスにいつ鍵を発行したかの情報を管理できます。
- IPAのJCMVP認定レベル(組込み利用している共通鍵生成ライブラリSecureWare開発キットV5.1)の安全な共通鍵生成や認証局(発行局)と連携した公開鍵証明書の発行を統一したAPIで行うことができます。

暗号モジュール試験及び認証制度(JCMVP)

独立行政法人情報処理推進機構（IPA）

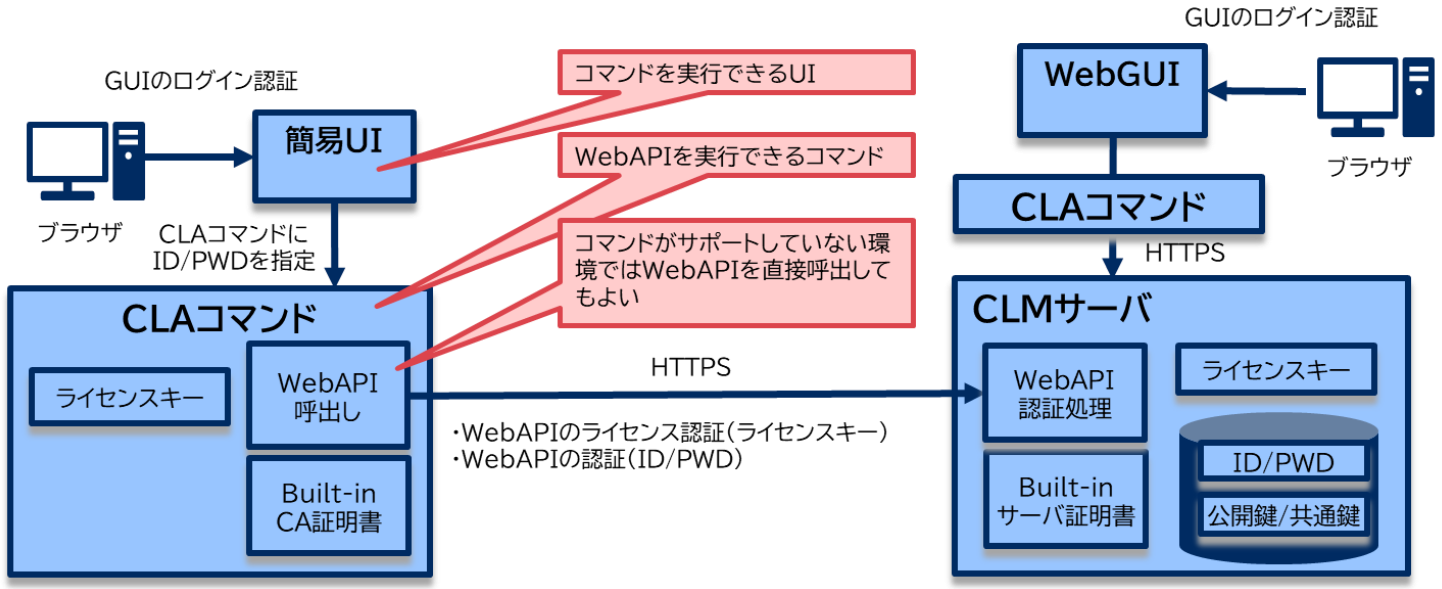
暗号モジュール認証製品リスト

認証番号:J0008
SecureWare開発キットV5.1

③ID/鍵/デバイス情報のライフサイクル管理

ID/鍵/デバイスのライフサイクル管理(更新～有効/無効～破棄)を行い、常に最新で安全な状態を維持します。

- SecureWare/Credential Lifecycle Managerは、IoT環境での相互認証/暗号化通信に必要となる認証情報(ID・鍵)を生成・管理できます。
- 生成した認証情報(ID・鍵)は、暗号化通信と多段階の認証機構により安全に配布します。
  - CLM/CLA間の通信路は、ビルトイン証明書によるHTTPS通信を使用して暗号化
  - CLMのWebAPIは、ライセンス認証とID/Pwd認証の2段階の認証が必要



④認証基盤連携(運用手順ノウハウ化)

IoT環境特有の手動運用に頼ることができない環境でもスムーズに運用できます

鍵状態をリモートで把握

デバイスの鍵状態を収集しグラフ化
ドリルダウンでデバイスの有効化/無効化
鍵更新のリモート実行が可能

定期自動鍵更新により手作業が不要

TWINE(軽量暗号)/AES共通鍵の定期自動更新
公開鍵証明書の定期自動更新も可能

エッジの自動検出

InfoCage NAと連携し、NWに接続したエッジを自動検出

AWS IoTへの接続容易化

AWS IoTへの接続に必要な認証情報を自動設定
※Azure IoTへの接続は手順書を用意

プライベート認証局が簡単に使える

電子政府認証局でも採用されている商用認証局製品(Carassuit)との連携ができ、発行/更新用の証明書テンプレートや証明書発行状況確認手順などを用意。プライベート認証局の運用が容易

どこでも動く

CLMは、Windows Server 2016/Windows10を動作サポート
CLAは、ARM版Debian/Ubuntu/AutomotiveGradeLinuxを動作サポート
(対応エッジ:RaspberryPi3 Model B/R-Car H3/Armadillo-IoT)

鍵状態をリモートで把握

デバイス鍵情報統計情報収集画面イメージ

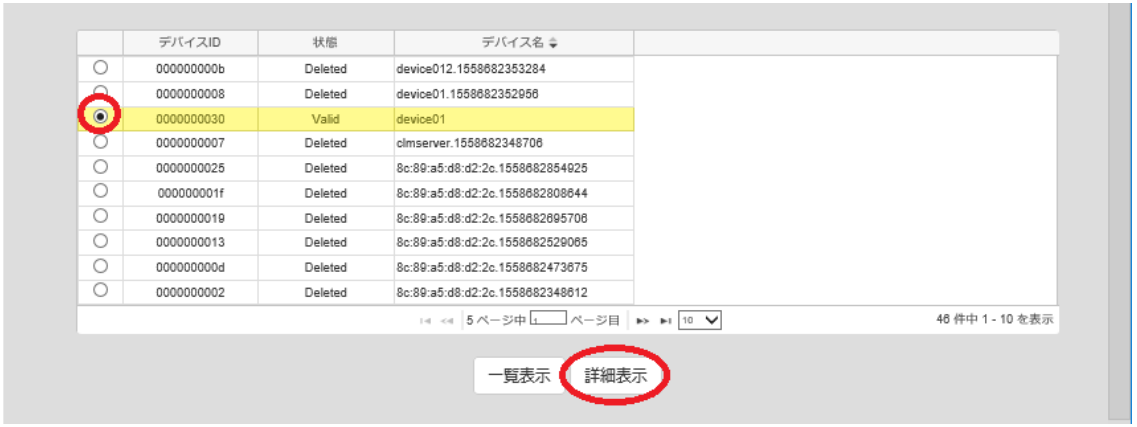
鍵証明書ダッシュボード

鍵証明書リモート実行

エッジの自動検出/デバイス一覧機能(デバイス管理オプション)

◆ エッジ/デバイスの管理画面イメージ

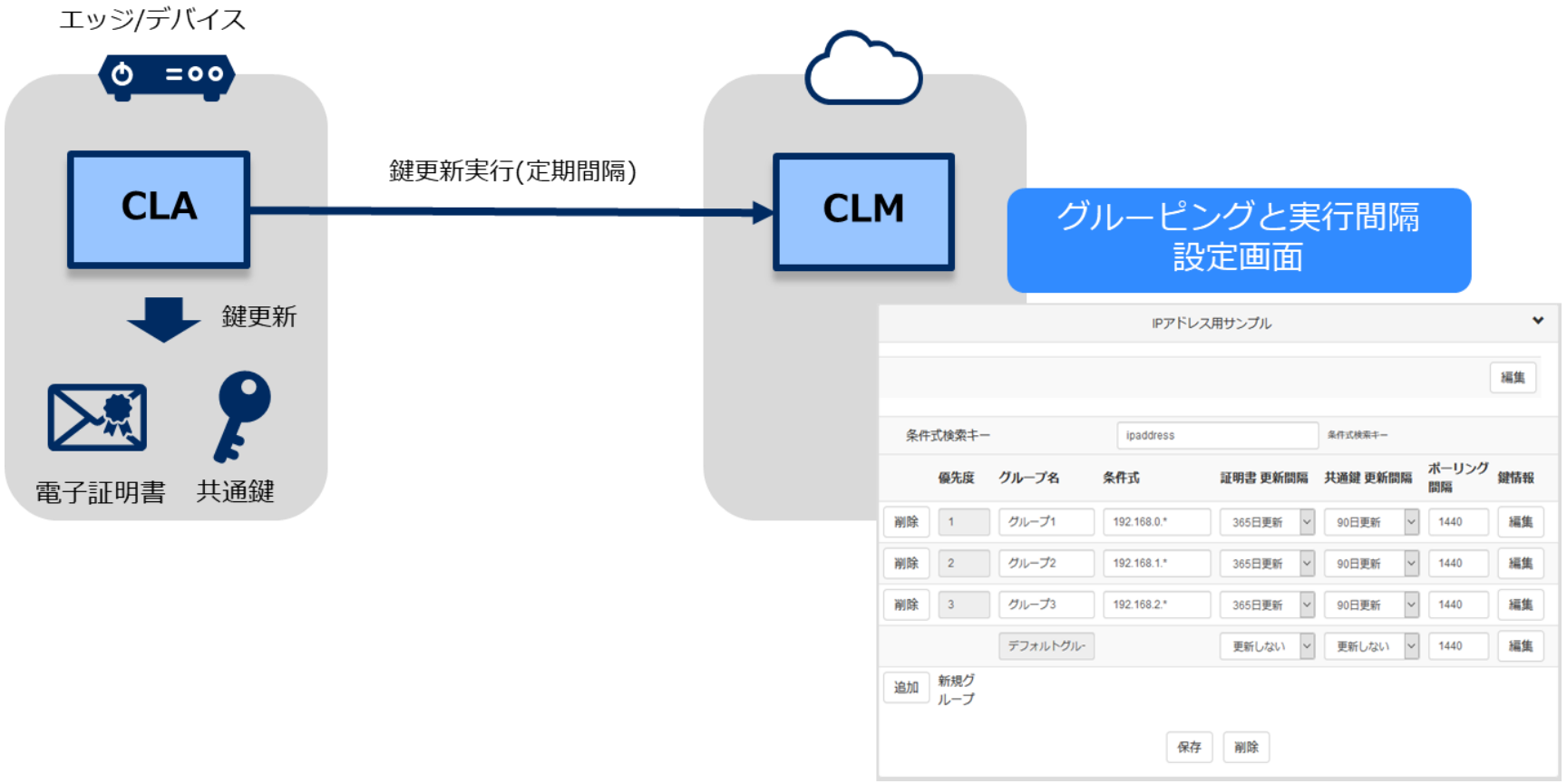
■ ネットワークに接続したエッジを自動的に検出する機能を有します。



定期自動鍵更新により手作業が不要

◆ 定期自動鍵更新のイメージ

- エッジ/デバイスにクライアント製品のCLAをインストールすることで、エッジ/デバイス上の鍵(公開鍵証明書・共通鍵)を定期的に自動更新できます。エッジ/デバイスをグルーピングする機能を有し、グループ単位で鍵の更新間隔(日数)等の設定が可能です。

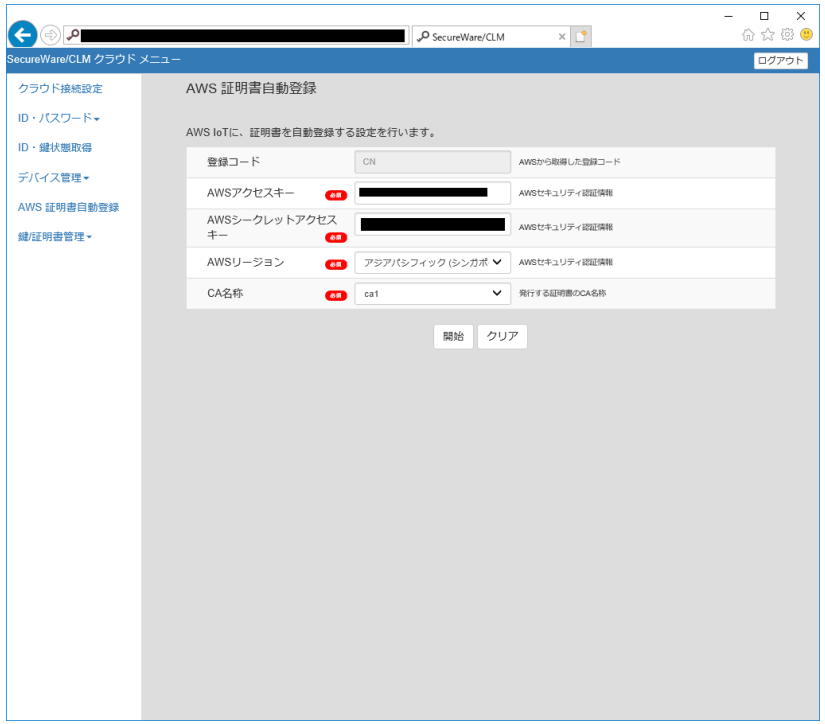


AWS IoTへの接続容易化機能(外部鍵管理連携オプション)

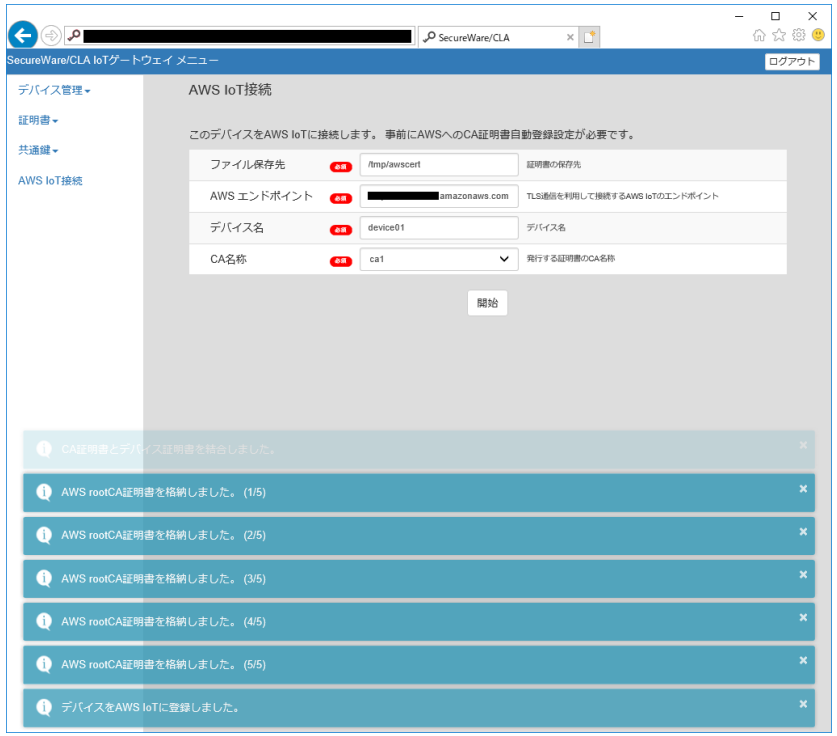
◆ AWS IoTへの接続容易化機能

- エッジがAWS IoTに接続できるようにするためには、AWS IoT Hub側へのデバイス登録やSSL用証明書の発行/登録、関連する設定作業を事前に行う必要があります。また、エッジ側にも証明書の設定を行う必要があります。
- SecureWare/CLMでは、エッジにCLAのWebUIを配備してワンクリックするだけで、AWS IoTへ接続設定を行うことができます。

AWS証明書自動登録機能



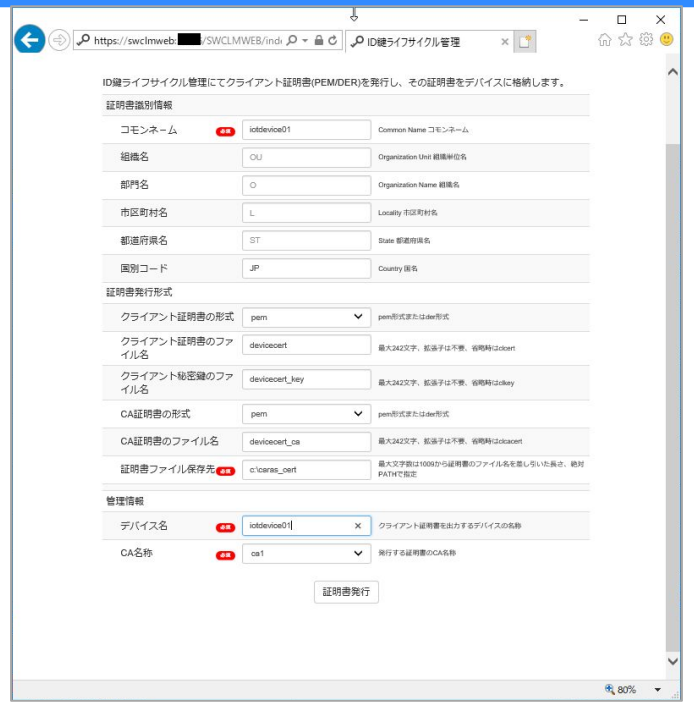
AWS IoT接続確認機能



プライベート認証局が簡単に使える

- プライベート認証局と連携する手順書とテンプレートを提供
  - SecureWare/CLMでは、OSSベースのプライベート認証局機能を同梱していますが、よりセキュアなシステムを実現するために電子政府認証局でも採用されているNEC製の商用プライベート認証局製品（Carassuit）との連携も可能。
  - 認証局を用いた証明書発行手順は専門的な知識を必要としますが、SecureWare/CLMでは、専門家が作成した手順書や証明書発行テンプレートを提供しており、認証局側の難しい操作を行うことなく証明書発行等が行えます。

証明書発行テンプレートにより難解な設計不要



認証局を直接操作せず証明書発行

API・メンテ用簡易GUI

提供機能一覧(WebAPI①)

CLMは統一的なWebAPIを提供します。

機能	説明
ID･パスワード発行	デバイスID･パスワード(事前共有キー)を生成する。パスワードの複雑さはCLMサーバで設定可能。
ID･パスワード取得	発行済みのID･パスワード(事前共有キー)を取得する。
ID･パスワード照合	デバイスID･パスワード(事前共有キー)を照合(認証)する。
ID･パスワード削除	発行済みのID･パスワード(事前共有キー)を削除する。
証明書発行	公開鍵証明書を発行する。署名アルゴリズムは sha256withRSA など(OpenSSLで発行可能な署名アルゴリズムに準拠)
証明書取得	発行済みのCA証明書、公開鍵証明書を取得する。
証明書更新	発行済みの公開鍵証明書を更新する。
証明書失効	発行済みの公開鍵証明書を失効する。
共通鍵発行	共通鍵を発行する。AES鍵 と TWINE鍵を選択可能。(AES:128ビット、256ビット)(TWINE:80ビット、128ビット)
共通鍵取得	発行済みの共通鍵を取得する。
共通鍵更新	発行済みの共通鍵を更新する。
共通鍵削除	発行済みの共通鍵を削除する。
共通鍵照合	Webブラウザから利用するCLMの管理画面。
共通鍵一括取得	共通鍵を一括取得する。

提供機能一覧(WebAPI②)

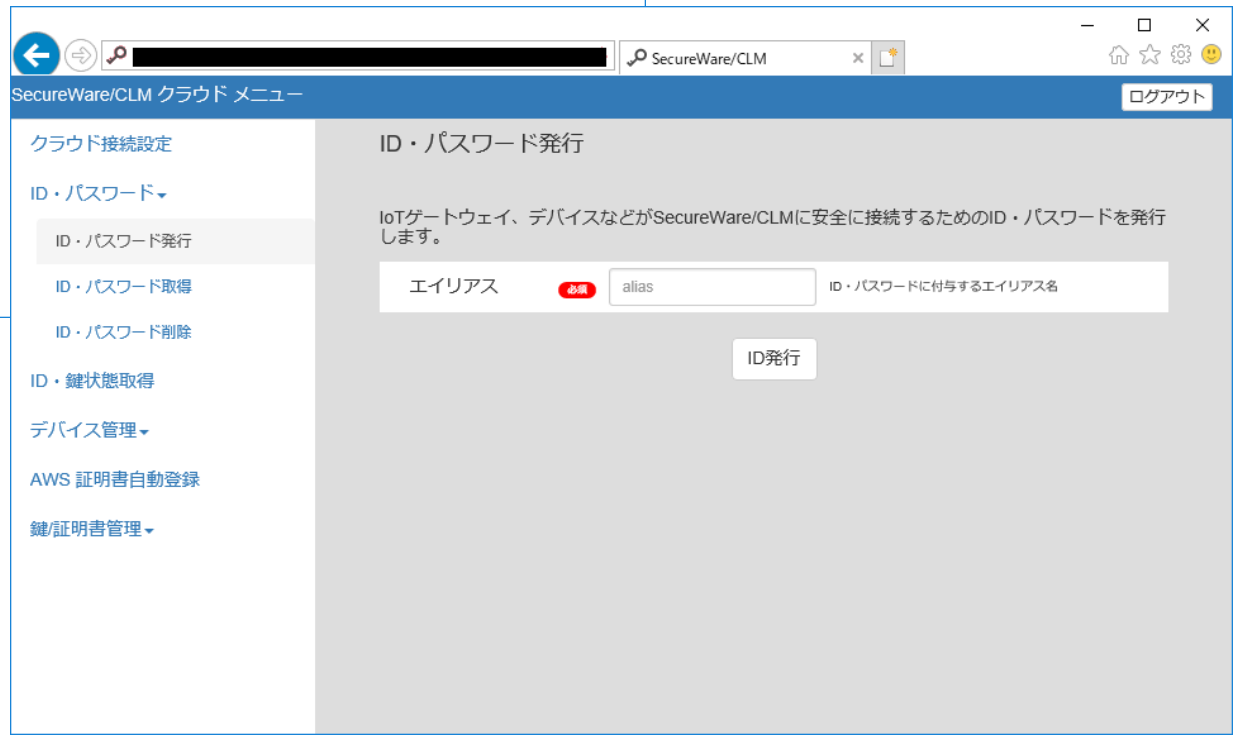
CLMは統一的なWebAPIを提供します。

機能	説明
デバイスID登録	デバイス情報を登録し、デバイスIDとデバイス用パスワードを発行する。
デバイスID認証	デバイスIDとデバイス用パスワードで認証する。
デバイスID無効化	デバイスIDを無効化する。
デバイスID有効化	デバイスIDを有効化する。
デバイスID情報更新	デバイスIDの情報を更新する。
デバイスID削除	デバイスIDを削除する。 デバイスIDに紐づいた電子証明書は失効する。
デバイスID一括登録	デバイス情報を一括登録し、デバイスIDとデバイス用パスワードを一括で払い出す。
デバイスID一括無効化	デバイスIDの状態を一括で無効化する。
デバイスID一括有効化	デバイスIDの状態を一括で有効化する。
デバイスID一括削除	デバイスIDを一括削除する。 デバイスIDに紐づいた電子証明書は失効する。
デバイスID一括情報更新	デバイスIDの情報を一括で更新する。
デバイスID情報取得	デバイスIDの情報を取得する。
デバイスID情報検索	デバイスIDの情報を検索・取得する。
デバイスID鍵情報取得	デバイスIDに紐づく鍵の情報情報を検索・取得する。

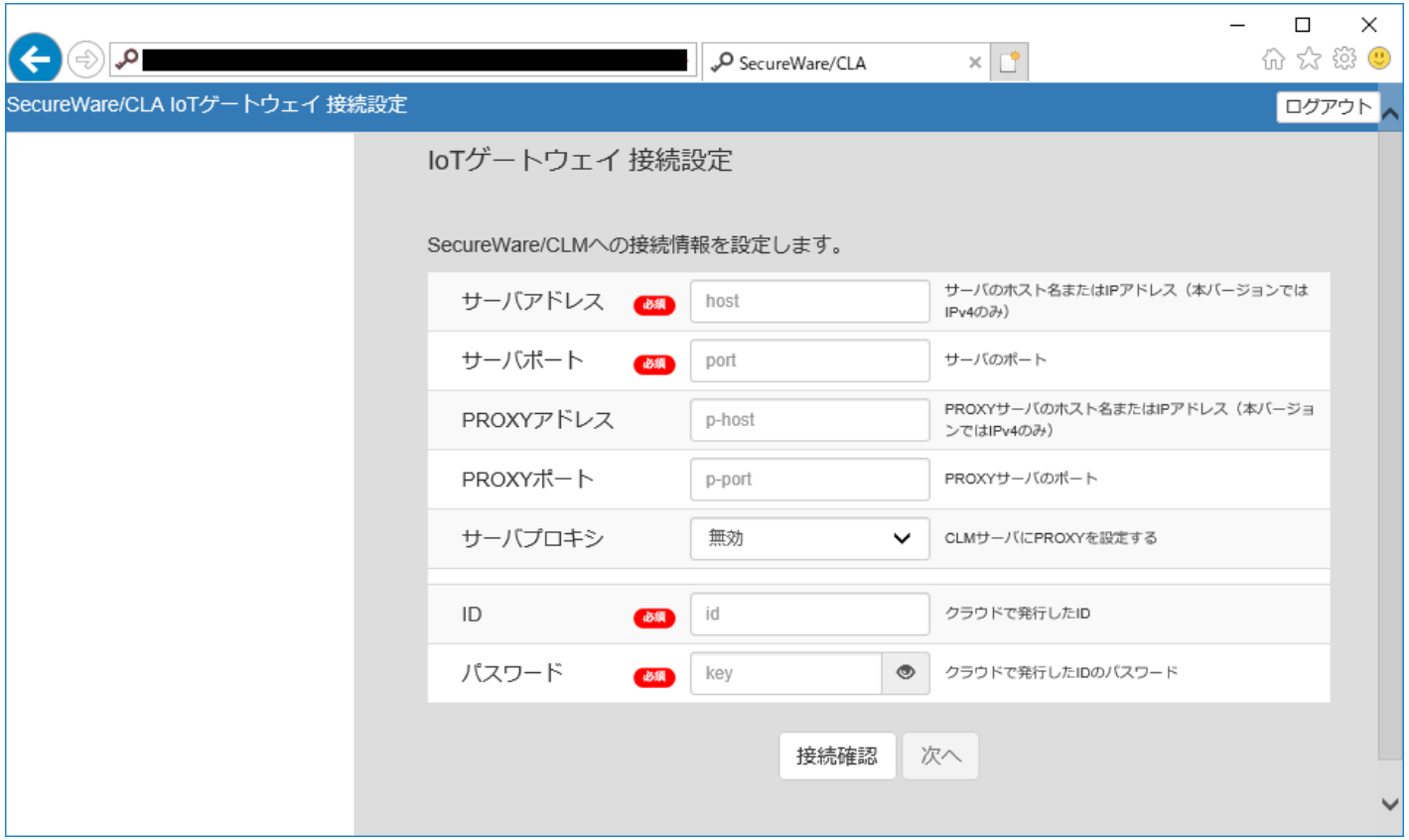
参考)メンテ用簡易WebUIイメージ(事前共有キー発行)

ログイン画面

事前共有キー(ID・パスワード)
発行画面

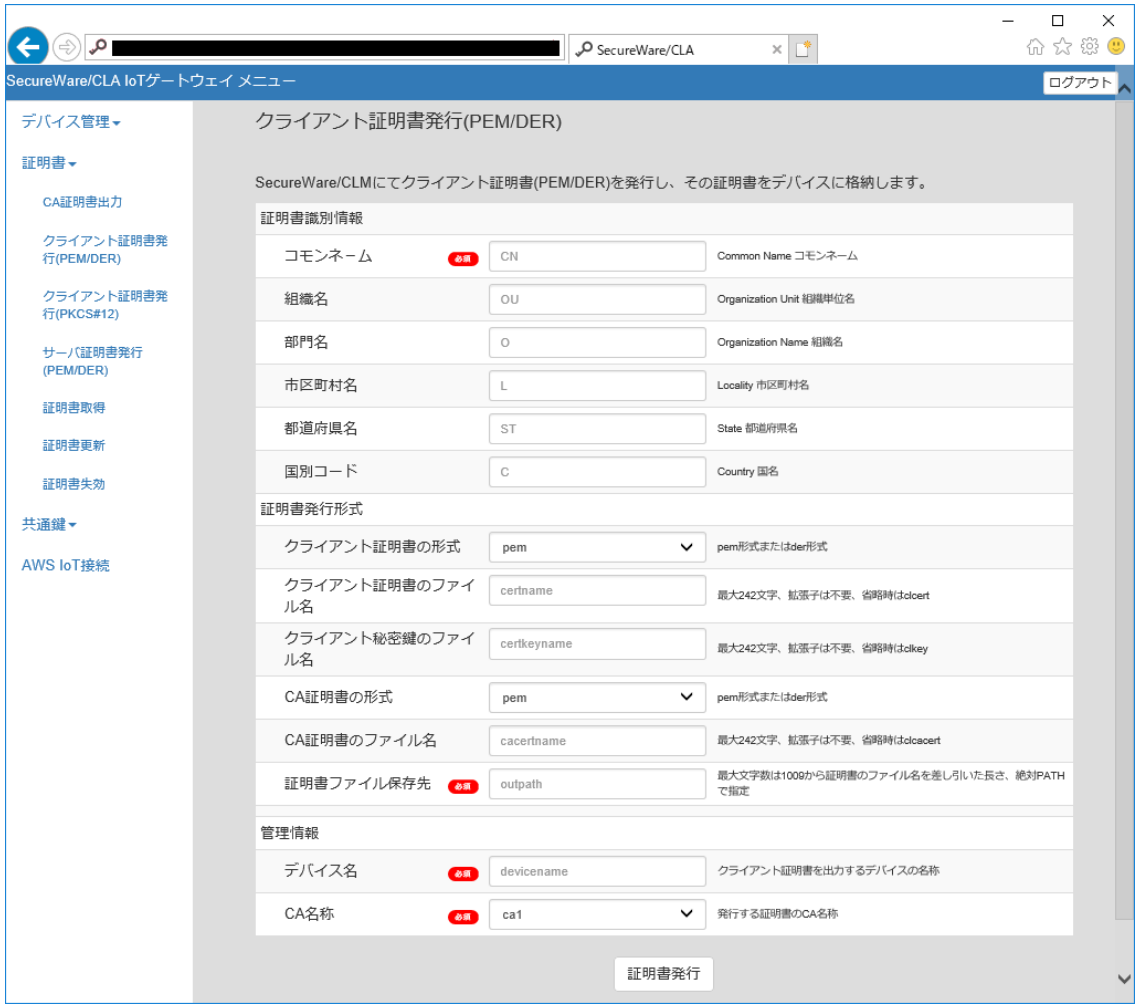


参考)メンテ用簡易WebUIイメージ(事前共有キー設定)



接続先設定画面

参考)メンテ用簡易WebUIイメージ(証明書発行)



証明書発行画面

動作環境

SecureWare/Credential Lifecycle Manager 動作環境①

No.	サーバ	プラットフォーム	必要 メモリ	必要 HDD	搭載コンポーネント	必須SW
1	ID鍵管理基盤サーバ 【CLM】	RedHat Enterprise Linux 6.8 RedHat Enterprise Linux 7.x RedHat Enterprise Linux 8.x CentOS 6.8 CentOS 7.x CentOS 8.x	4GB	2GB以上 (ログ別)	・CLM(WebAPIサーバ)	・OpenJDK 1.8.0 u282 以降 ・Apache Tomcat 8.5.64 以降 ・PostgreSQL 9.6.21 以降 ・OpenSSL 1.1.1k
					・CLM(コマンド)	・boost(同梱) ・OpenSSL(同梱)
					・CLM(WebUI)	・OpenJDK 1.8.0 u282 以降 ・Apache Tomcat 8.5.64 以降 ・perl-JSON ・sudo 1.8.19p2 以降(7.x～)
		Windows 10 IoT Enterprise Windows 2012 R2 Windows 2016	4GB	2GB以上 (ログ別)	・CLM(WebAPIサーバ)	・Oracle Java SE(JRE) 8u202 以降 ・Apache Tomcat 8.5.37 以降 ・PostgreSQL 9.6.11 以降 ・OpenSSL 1.1.1k
					・CLM(コマンド)	・boost(製品同梱) ・OpenSSL(製品同梱)
					・CLM(WebUI)	・Oracle Java SE(JRE) 8u202 以降 ・Apache Tomcat 8.5.37 以降 ・Strawberry Perl

※ CLMサーバ1台で管理可能なエッジ/デバイスは、最大10万台程度です。

※ 今後のバージョンアップにて管理可能台数を増強する予定です。

※ 上記「必要HDD」の値は、『実行環境の必要容量』に『管理機器10万台それぞれにID・公開鍵・共通鍵を1つずつ発行したときのデータ容量』を加算したものです。

SecureWare/Credential Lifecycle Manager 動作環境②

No.	サーバ	台数	プラットフォーム	必要メモリ	必要HDD	搭載コンポーネント	必須SW
2	エッジ リッチデバイス 仮想VM 【CLA】	1台	Debian GNU/Linux 8.6 Debian GNU/Linux 8.8 Debian GNU/Linux 9.11	10MB	15MB (ログ別)	・CLA(コマンド)	・boost(同梱) ・OpenSSL(同梱)
				4MB	1MB (ログ別)	・node-red用ライブラリ	・node.js ・node-red
				3MB	10MB (ログ別)	・CLA(簡易WebUI)	・lighttpd ・libjson-perl ・sudo
		1台	RedHat Enterprise Linux 6.8 RedHat Enterprise Linux 7.x CentOS 6.8 CentOS 7.x	10MB	15MB (ログ別)	・CLA(コマンド)	・boost(同梱) ・OpenSSL(同梱)
				4MB	1MB (ログ別)	・node-red用ライブラリ	・node.js ・node-red
				3MB	500MB (ログ別)	・CLA(簡易WebUI)	・OpenJDK 1.8.0 u181 以降 ・Apache Tomcat 8.5.51 以降 ・perl-JSON ・sudo 1.8.19p2 以降(7.x～)
		1台	Windows 10 IoT Windows 2012 R2 Windows 2016	10MB	15MB (ログ別)	・CLA(コマンド)	・boost(同梱) ・OpenSSL(同梱)
				3MB	500MB (ログ別)	・CLA(簡易WebUI)	・Oracle Java SE(JRE) 8u202 以降 ・Apache Tomcat 8.5.37 以降 ・Strawberry Perl

※　上記「必要HDD」の値は、『実行環境の必要容量』です。

※　必要なコンポーネントを選択してインストール可能です。

- 「node-red用ライブラリ」の実行には「CLA(コマンド)」が必要です。
- 「CLA(簡易WebUI)」の実行には「CLA(コマンド)」が必要です。

製品ライセンス体系

製品ライセンス体系

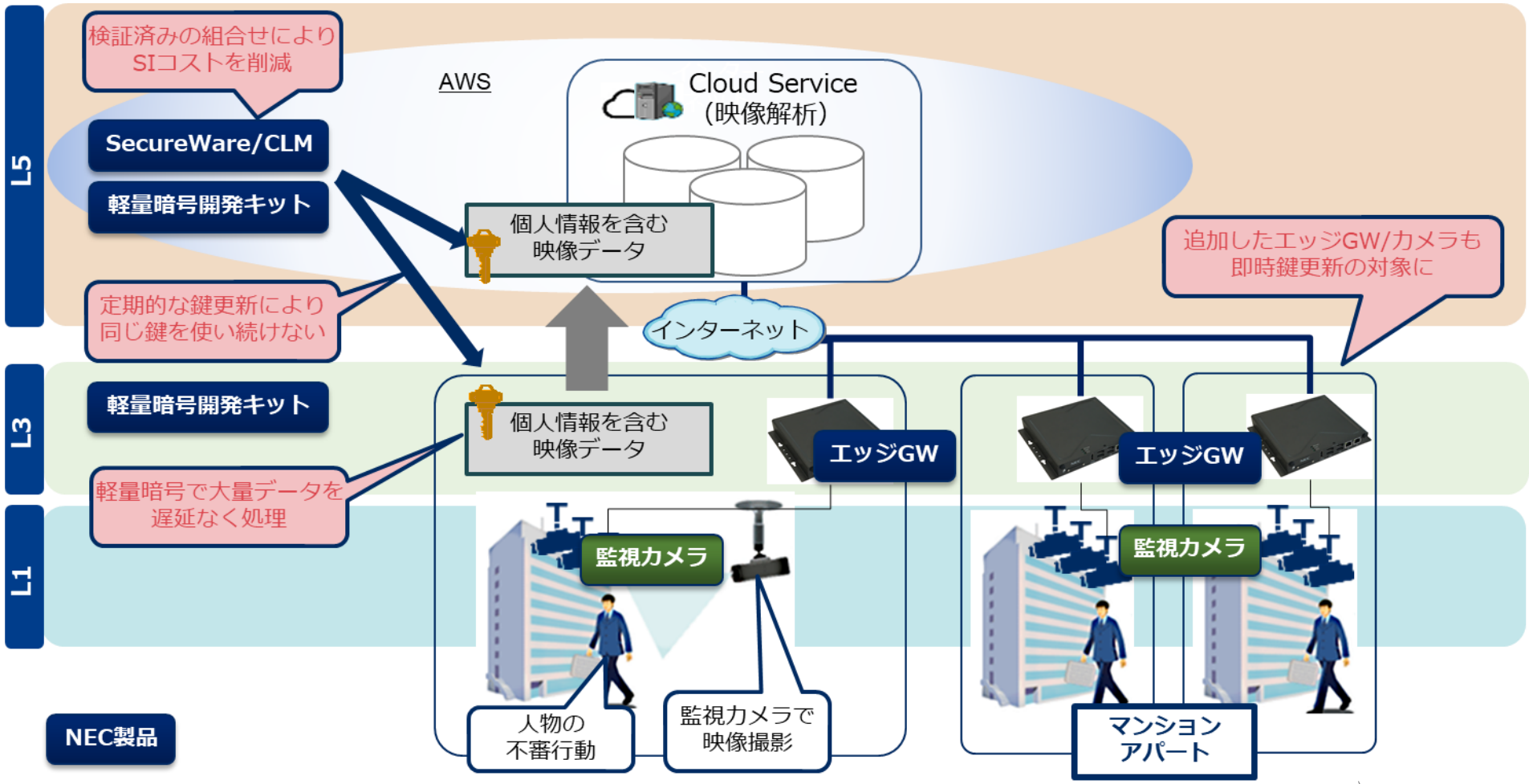
［製品ライセンス］＋［必須製品］＋［オプション製品］で構成されます。

製品種別	製品名
製品 ライセンス	・サーバ製品ライセンス(SecureWare/CLM) ・デバイス管理ライセンス(SecureWare/CLM EDMS) ※上記は、インストールするサーバ/VM台数毎に1つ購入が必要
	・クライアント製品ライセンス(SecureWare/CLA) ※上記は、インストールするエッジ/デバイス台数毎に1つ購入が必要
必須製品	・SecureWare開発キットV5.1 ・軽量暗号開発キット 基本料金クラスS ※上記は、インストールするサーバ/VM台数毎に1つ購入が必要
オプション製品 (必要に応じて購入)	・外部鍵管理連携ライセンス(SecureWare/CLM 外部鍵管理) ※上記は、HSMやAWS IoT、商用プライベート認証局との連携時に必要
	・PostgreSQL透過暗号/PostgreSQL Enterprise Edition(商用版) ※上記は、お客様要件にDB暗号化の要件がある場合に必要
	・InfoCage 不正接続防止 V5.4 NetworkAgent ※上記は、エッジ自動検出機能利用時に必要

導入・提案事例

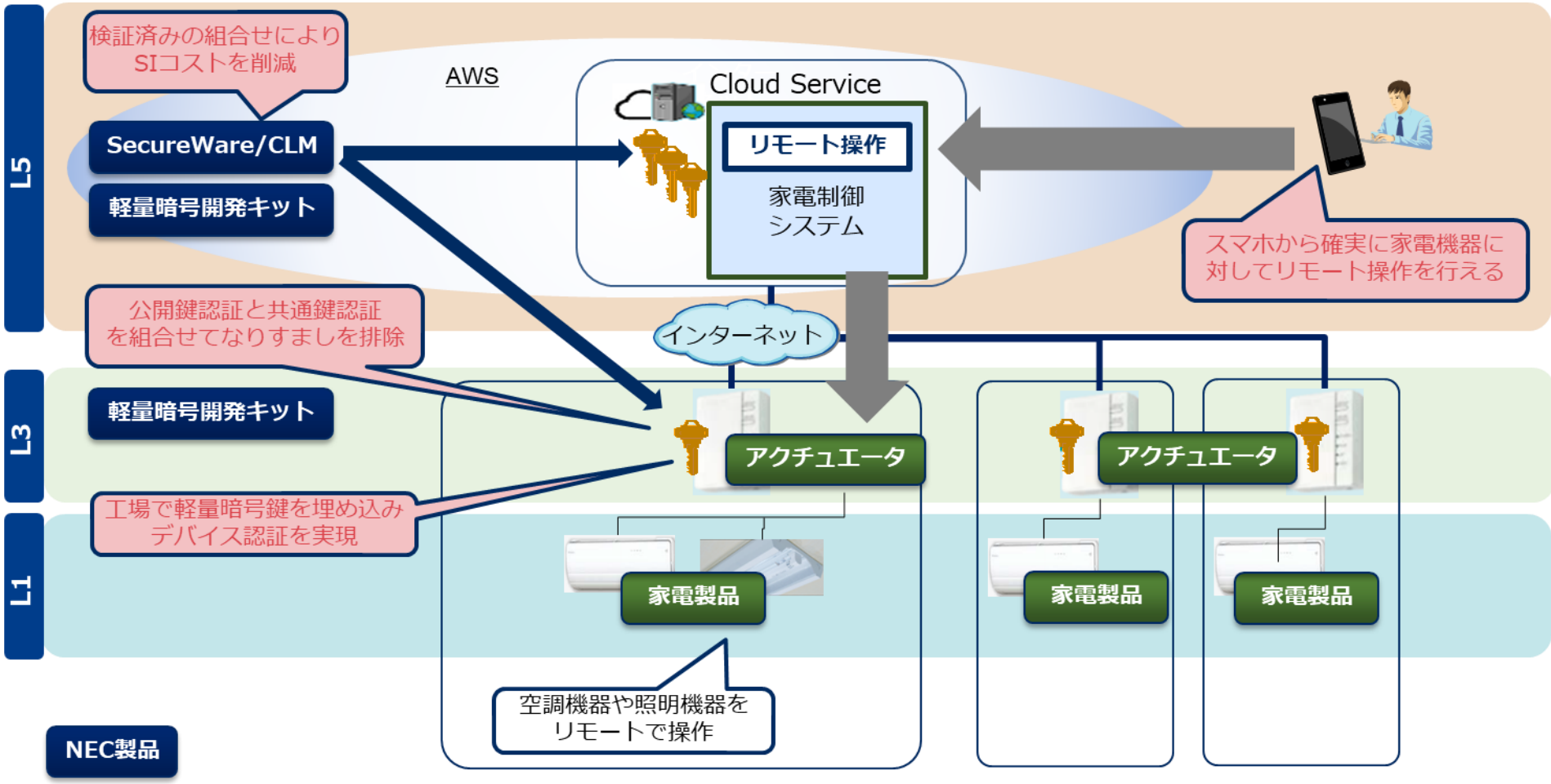
リテール向け適用事例(IoT環境で個人情報を守る)

エッジ層からクラウド層への通信暗号化はキャリア回線で担保しているものの、映像データ自体が個人情報を含むデータであり漏洩を防ぐ必要がある。膨大なデータ量を遅延なく処理するため、軽量暗号化と定期的な鍵更新によりセキュア化を実現



製造業向け提案事例(IoT環境でなりすましを防ぐ)

生産工場で機器毎にデバイス用の鍵を埋め込み、クラウド層からのリモートアクセス時にデバイス認証を行い、
なりすましを排除して確実に接続できる仕組みを提供



【ご参考】
NECが提供するID管理・認証基盤ソリューション

NECが提供するID管理・認証基盤ソリューション

NECで保有する認証基盤製品をはじめ、多くのユーザ様への構築・導入経験をもとに、今まで培ってきたノウハウ・技術を最大限にご提供します。

国内開発/スイート製品群

- **人の認証からものの認証まで幅広く対応**
  ID鍵管理、認証認可、PKI領域をカバーする自社開発製品を保有
- **迅速・柔軟なサポート力**
  自社開発製品は、弊社内でソースコードを持ちお客様／連携製品 との柔軟な対応が可能

豊富な導入実績

- **ミッションクリティカルシステムの導入実績**
  100万人規模の認証基盤をはじめ、 24時間365日無停止運用を伴うシステム構築・運用実績を保有
- **導入実績**
  官公庁/自治体/金融へ認証基盤/認証局導入
  製造/流通/交通へのID管理/認証基盤導入

ハイレベルなセキュリティ技術の組込み

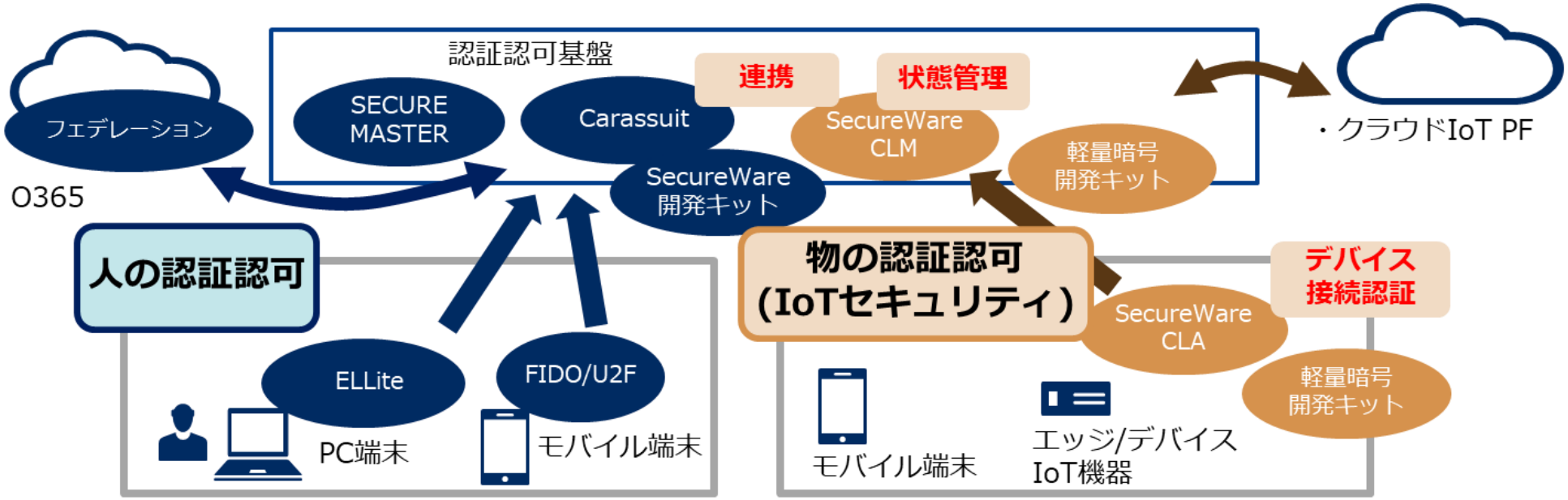
- **安全な認証情報の生成**
  - パスワードポリシーに基づく事前共有キーの生成
  - JCMVP認証取得レベルの安全な鍵生成
  - 共通鍵を用いた強固な認証方式

システムの柔軟性・拡張性

- **お客様の必要とする部分の導入**
  ID鍵管理、認証認可(API)な必要な部分のみの提供が可能
- **エッジ/デバイス管理と認証基盤の連携**
  エッジ/デバイスの状態(有効/無効)と認証認可の連動まで拡張したシステム提供が可能

NECが提供するID管理・認証基盤ソリューション商材

- **SECUREMASTER**
  ID管理、認証認可/SSO/生体認証基盤、フェデレーションによる人の認証基盤を提供
- **Carassuit**
  公開鍵基盤(PKI)システムを実現するための証明書発行局(CA)、登録審査局(RA)を提供
- **SecureWare 開発キット**
  共通鍵暗号/公開鍵暗号/ハッシュ関数などの多様な暗号ライブラリ、PKIアプリケーションを開発するためのAPIライブラリを提供
- **SecureWare/CLM(Credential Lifecycle Manager)**
  IoT環境での相互認証/暗号化通信に必要となる認証情報(ID(証明書)/鍵)を生成・管理
  NECモバイルバックエンド基盤 API GWやエッジデバイス管理、軽量暗号ライブラリと組み合わせて、認証情報を使えるものに。



お問い合わせ先

SecureWare/Credential Lifecycle Manager
のお問い合わせは

製品ホームページ
http://jpn.nec.com/secureware/clm/

からお気軽にお問合せください。


Orchestrating a brighter world
NEC