Blockchain WG
IoTサブグループからの発表

2019年11月26日

アイビーシー株式会社
IoTセキュリティ事業部 田沢 一郎

- GDPR（一般データ保護規則、General Data Protection Regulation）
  - EUにおける個人情報保護法

- NIS指令（ネットワーク・情報システムのセキュリティに関する指令全体）
  - インフラをサイバー攻撃から確実に回復できる等のリスク予防措置、ネットワークと情報システムのセキュリティ確保、インシデントへの対応が義務化

- パロアルトネットワークス社の報告
  - フィッシング攻撃に関する総括: 2018年1月～3月
  - 期間中は262の固有ドメインから4213のURLが攻撃に使われ、このうち約3分の1に当たる1010のURLがHTTPSだった。（途中略）多くのユーザーがHTTPSに高い信頼を寄せており、HTTPSを使用したフィッシングサイトのURLには注意を払う必要があると注意を呼び掛けている。

参照）

https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-phishing-nutshell-january-march-2018

「HTTPSだから安全」ではない

・SSL接続は、状況悪化を潜在化してしまい、発見が遅れる可能性がある

・無人運用を前提としたIoTでは致命傷になりかねない

ご参考：IoTセキュリティガイドライン（経済産業省）

IoT 分野共通セキュリティ要件 ガイドライン 2019 年度版（案）（ 重要生活機器連携セキュリティ協議会CCDS）

- ブロックチェーン技術の概要を説明し、IoT機能をセキュアにする技術としてブロックチェーンを使用できるようにする一連のアーキテクチャパターンについて説明したホワイトペーパー

- IoTセキュリティを実現していくうえで必要となる機能要件について解説

CSAJC Japan Chapter cloud security alliance SM

日本クラウドセキュリティアライアンス
（CSAジャパン）

CSAジャパンについて | CSAジャパン関西支部 | 会員企業一覧 | 資格/認証制度 | 日本語資料集 | ワーキンググループ
イベント/勉強会 | ブログ | CSAジャパン入会方法

「IoTセキュリティのためのブロックチェーン技術の活用」を公開しました！

2018年10月3日 morozumi ニュース 0

CSAジャパン　BlockChainワーキンググループが、「IoTセキュリティのためのブロックチェーン技術の活用」を公開しました！

本資料は、CSA本部が公開している「Using Blockchain Technology to Secure the Internet of Things」の日本語訳です。

こちらのウエブページを参照して、資料をダウンロードしてください。

BLOCKCHAIN　CSA　CSAジャパン　IOT　クラウド　クラウドセキュリティ　ワーキンググループ

新着情報

2019年10月31日	NEW! 「クラウドの重大セキュリティ脅威　11の悪質な脅威」を公開いたしました。
2019年10月28日	CSA Japan Congress 2019 は、申込者数が予定数に達したため、受付を終了しました。
2019年10月18日	ベライゾンジャパン合同会社様が新たに企業会員になられました！
2019年10月17日	CSA Japan Congress 2019 の申込受付を開始しました！
2019年10月12日	CSA Japan Congress 2019 を11

https://www.cloudsecurityalliance.jp/site/?p=3908

IoT セキュリティに向けたブロックチェーン技術の選択

ブロックチェーン技術は、IoT デバイスをセキュアにするのに役立つ。IoT デバイスは、パブリックブロックチェーンサービスを使用するか、クラウド内のプライベートブロックチェーンノードと安全な API を介して通信するように構成できる。IoT システムのセキュリティフレームワークにブロックチェーン技術を組み込むことにより、IoT デバイスは安全に互いを検出し、分散鍵管理技術を使用してマシン間のトランザクションを暗号化し、ソフトウェアイメージの更新とポリシーの更新の完全性と真正性を検証することができる。

このレポートで説明しているアーキテクチャパターンが実現すれば、それによって IoT デバイスは API を介してブロックチェーントランザクションノードと通信し、制約のあるデバイスであってもブロックチェーンサービスに参加できる。

セキュリティを確実にするために、特定のブロックチェーンサービスへ接続しようとする IoT デバイスのブートストラップ中、注意が必要となる。以下は、IoT デバイスのトランザクションノードへ参加することをサポートする IoT デバイスの検出の例である。IoT デバイスは、まずトランザクションノードとして追加されるための認可を証明するための資格情報を付与される必要がある。この資格情報の付与は、特定の IoT デバイスエコシステムの脅威に対して保護されている安全な環境で実施する必要がある。

このことを実現することを可能にするブロックチェーン技術と市場のイニシアチブを検討した結果、ブロックチェーン技術を使う IoT をセキュアにするために検討すべき以下の 5 つ機能が浮かび上がる：

1. スケーラブルな IoT の検出
2. 信頼できる通信（トラステッドコミュニケーション）
3. 半自動型 M2M（Machine-to-Machine）操作
4. IoT の構成と更新
5. セキュアなファームウェアイメージの配布と更新

・前掲の５つの機能について 必要とされる要件を精査し、実際に利用するにあたっての
参考資料とすることを検討した

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
1.　スケーラブルなIoTの検出	協働すべき数十～数千万のIoTデバイスをアクティベーションできる。スケーラブルなIoTの検出に利用できる。
	正しいIoTデバイスだけをブロックチェーンサービスに追加するための登録プロセスを実施する。 ※野良IoTの排除

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
2.　トラステッドコミュニケーション	IoTデバイスは、台帳に格納されるトランザクションを構築するために必要なデータを交換するための安全なチャネルを使用している。
	IoTデバイス(送信側）は、ブロックチェーンサービスに格納された受信側IoTデバイスの公開鍵を使用し、IoTデバイス(受信側)に暗号メッセージを送信する。
	IoT送信側は、IoT受信側の公開鍵をブロックチェーン台帳から取得するようにそのトランザクションノードに要求する。
	新しいIoTデバイスが登録されると、新しいトランザクションが作成される。このトランザクションは、公開鍵を含むIoTプロパティで構成される。
	IoTデバイスが証明書を更新する必要がある場合、再登録が行われる。
	失効した証明書をトランザクションとしてブロックチェーンサービスに追加することもできる。
	IoTデバイスの通信を保護するために、トラフィック暗号キー（TEK)またはコンテンツ暗号化キー（CEK)を生成するために使用できる。

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
3.　半自動型M2M（Machine-to-Machine）操作	スマートコントラクト機能を使うことで、自律型トランザクションのセキュリティを実現する役割を果たす。
	スマートコントラクトは、誰(どのIoTデバイス）がトランザクションに参加できるかのアクセス制御を実施できる。 各トランザクションは、IoTノードのウオレット鍵で署名され、ウオレット鍵はハードウエアセキュリティコンテナに格納されなければならない。
	ブロックチェーン上のトランザクション記録は、後で否認されないことを保証する。

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
4.　IoT設定とアップデートコントロール	台帳は、検証されたファームウェアの最新バージョンや設定の詳細などのIoTプロパティをホストする。
	台帳は、検証されたファームウェアの最新バージョンや設定の詳細などのIoTプロパティをホストする。各IoTデバイスの最新の設定ファイルのハッシュ値をホストする。
	IoTデバイスは、毎晩あるいは指定された時間に、最新の信頼できる設定ファイルをダウンロードし、トランザクションノードAPIを使用して、ブロックチェーンに格納されているハッシュ値を入手し照合する。

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
5.　安全なファームウェアイメージの配布と更新	開発者は、そのデバイスファミリの最新の信頼できるイメージをハッシュし、そのハッシュをブロックチェーンにロードする。
	IoTデバイスは、新しいファームウェアイメージを定期的にダウンロードする様にAPIを介して設定する。
	IoTデバイスは、ブロックチェーンベースのイメージ更新プロセスを使用して、ベンダーが提供するすべてのアップデートを検証する。

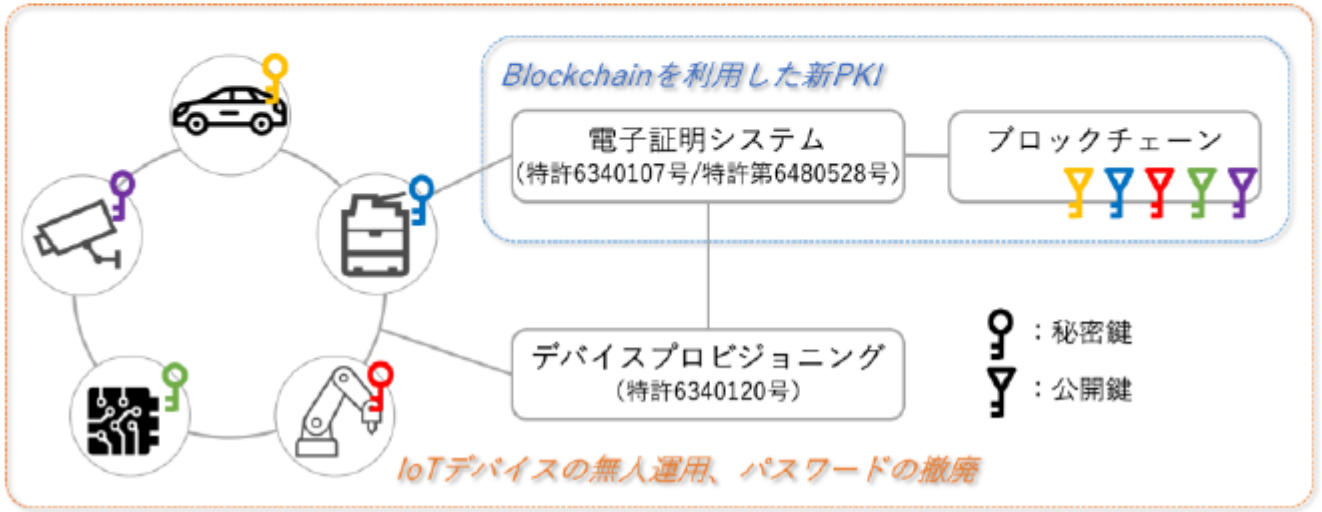
・次に、この要件を進めるにあたり 国産のIoTセキュリティ基盤 kusabi™ を例にあげて、要件を精査した。

参考：kusabi アイビーシー株式会社が提供する『IoT の設計から開発、量産、運用まで、
すべての段階において一貫性のあるセキュリティ対策を提供する “IoT セキュリティ 基盤サービス”』

https://www.ibc21.co.jp/kusabi/

kusabi™は、あらゆる「モノ＝IoT」の安全な相互通信を目指した新 PKI 技術を提供し、
IoT のシステムモデルに最適なセキュリティを実現します。
本書にて説明した主要技術を以下にまとめます。

- 電子証明システム： Blockchain を利用した新 PKI
- デバイスプロビジョニング：IoT デバイスの無人運用、パスワードの撤廃

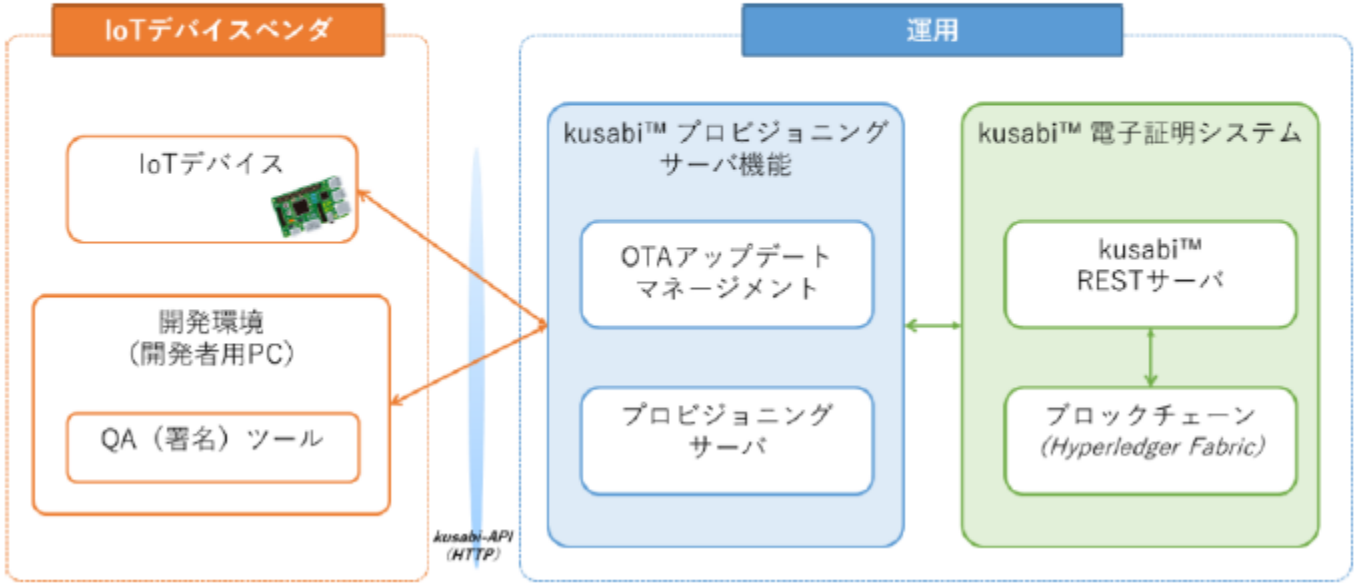


kusabi™の概要図

kusabi™ホワイトペーパーより抜粋

kusabi™のユーザの役割分担を以下に示します。

- IoT デバイスベンダ：IoT デバイスを開発するベンダー
- 運用：kusabi™を利用してサービスするインテグレーター



kusabi™のサービス構成と役割分担

kusabi™ホワイトペーパーより抜粋

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
1.　スケーラブルなIoTの検出	協働すべき数十～数千万のIoTデバイスをアクティベーションできる。スケーラブルなIoTの検出に利用できる。
	正しいIoTデバイスだけをブロックチェーンサービスに追加するための登録プロセスを実施する。 ※野良IoTの排除

対応事例：

kusabi™が、正しいIoTデバイスの登録プロセスを提供します。
起動時及び定刻に、正規のIoTデバイスに製品認証済ファームウェアを
自動OTAする事が可能です。

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
2.　トラステッドコミュニケーション	IoTデバイスは、台帳に格納されるトランザクションを構築するために必要なデータを交換するための安全なチャネルを使用している。
	IoTデバイス(送信側）は、ブロックチェーンサービスに格納された受信側IoTデバイスの公開鍵を使用し、IoTデバイス(受信側)に暗号メッセージを送信する。
	IoT送信側は、IoT受信側の公開鍵をブロックチェーン台帳から取得するようにそのトランザクションノードに要求する。
	新しいIoTデバイスが登録されると、新しいトランザクションが作成される。このトランザクションは、公開鍵を含むIoTプロパティで構成される。
	IoTデバイスが証明書を更新する必要がある場合、再登録が行われる。
	失効した証明書をトランザクションとしてブロックチェーンサービスに追加することもできる。
	IoTデバイスの通信を保護するために、トラフィック暗号キー（TEK)またはコンテンツ暗号化キー（CEK)を生成するために使用できる。

対応事例：

kusabi™は、ブロックチェーンサービスを分散PKI(distributed public key infrastructure)
として機能する仕組みを実現できます。
新しい IoT デバイスが、 kusabi™電子証明システムに登録されることで、真正性のあるデバイスのみの接続を実現します。
コスト増大の要因となるIoTデバイスへのセキュリティ要求事項(例えば、耐タンパ領域、SSL/TLS通信)を必須としないことで、より多様なIoTデバイスへの対応が可能です。

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
3.　半自動型M2M（Machine-to-Machine）操作	スマートコントラクト機能を使うことで、自律型トランザクションのセキュリティを実現する役割を果たす。
	スマートコントラクトは、誰(どのIoTデバイス）がトランザクションに参加できるかのアクセス制御を実施できる。 各トランザクションは、IoTノードのウオレット鍵で署名され、ウオレット鍵はハードウエアセキュリティコンテナに格納されなければならない。
	ブロックチェーン上のトランザクション記録は、後で否認されないことを保証する。

対応事例：

kusabi™はブロックチェーンのスマートコントラクト機能を使うことにより、これらの自律型トランザクションによるセキュリティを実現します。
kusabi™はコンソーシアム型ブロックチェーン(Hyperledger Fabric)を採用し、公開鍵は適切なアクセス制限の下、スマートコントラクトが実行され、保存管理されます。
IoTデバイス毎のkusabi-IDによるデバイス認証に、自律型トランザクションのセキュリティを享受する事で、認証局に頼ることなく電子証明が出来ます。

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
4.　IoT設定とアップデートコントロール	台帳は、検証されたファームウェアの最新バージョンや設定の詳細などのIoTプロパティをホストする。
	台帳は、検証されたファームウェアの最新バージョンや設定の詳細などのIoTプロパティをホストする。各IoTデバイスの最新の設定ファイルのハッシュ値をホストする。
	IoTデバイスは、毎晩あるいは指定された時間に、最新の信頼できる設定ファイルをダウンロードし、トランザクションノードAPIを使用して、ブロックチェーンに格納されているハッシュ値を入手し照合する。

対応事例：

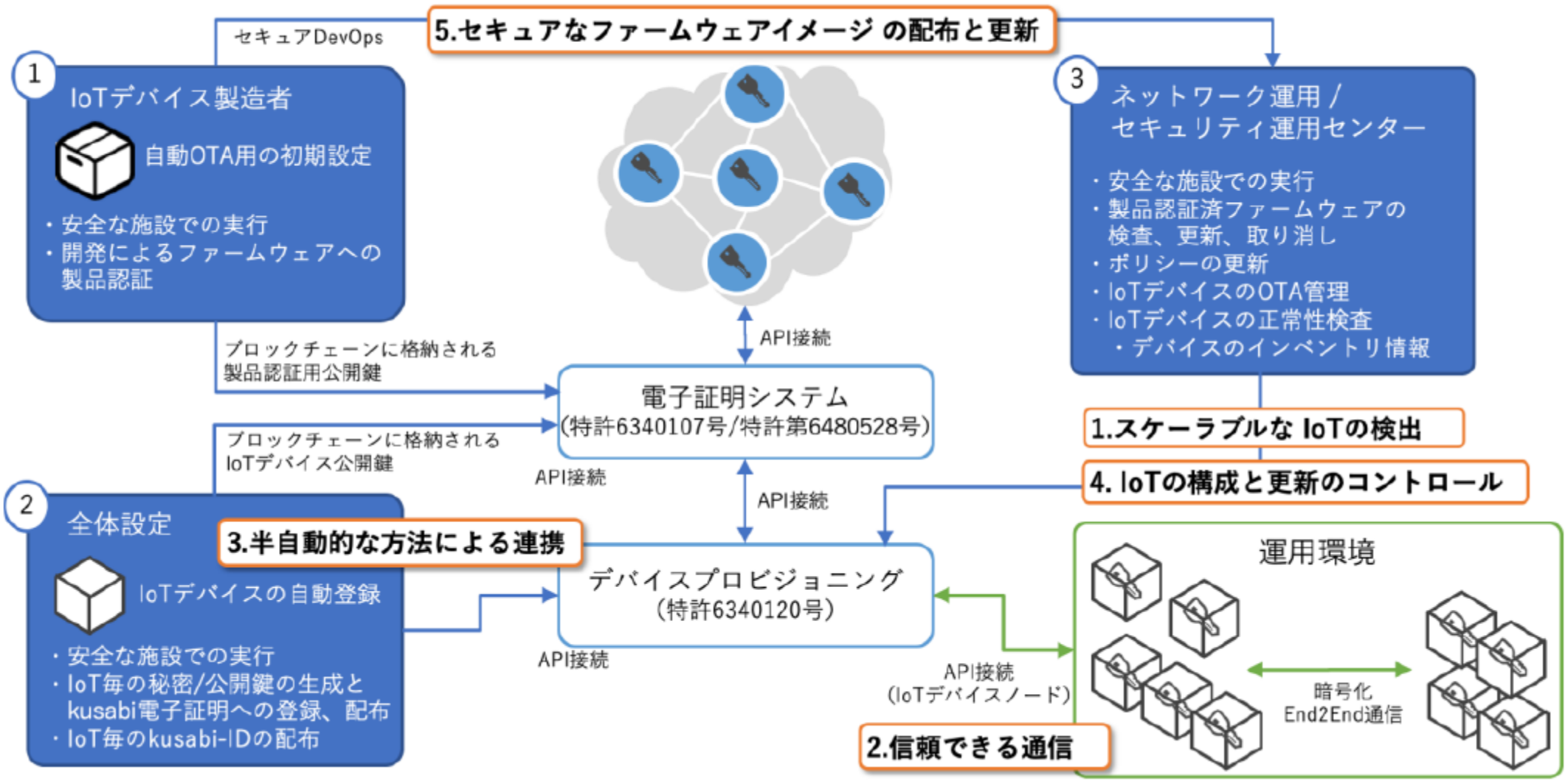
一般的には、情報が読み取られないように台帳内で暗号化する必要があります。
kusabi™電子証明システムは、公開鍵を保存するので、台帳の暗号化が不要であることが大きな特徴となります。
更新のコントロールは、kusabi-APIを経由してデバイス認証のうえ、自動設定を行う事で、
IoTデバイスへの利用者ログイン（いわゆるID・パスワード）を不要とします。
さらに、デバイスプロビジョニングに登録されたIoTデバイスのみ接続を許可するので、
いわゆる野良IoTデバイスは接続できないシステム構築が可能です。

IoTセキュリティのためのブロックチェーン技術の活用　チェックリスト

機能	要件
5.　安全なファームウェアイメージの配布と更新	開発者は、そのデバイスファミリの最新の信頼できるイメージをハッシュし、そのハッシュをブロックチェーンにロードする。
	IoTデバイスは、新しいファームウェアイメージを定期的にダウンロードする様にAPIを介して設定する。
	IoTデバイスは、ブロックチェーンベースのイメージ更新プロセスを使用して、ベンダーが提供するすべてのアップデートを検証する。

対応事例：

セキュアなファームウェアを提供する為には、開発元であるIoTデバイスベンダーが、ファームウェアに
デジタル署名（コードサイニング）を行う必要があります。
kusabi™は、OTAされるファームウェアに、開発元がコードサイニングすることで、 ファームウェアの真正性を
実現します。
IoTデバイスは、起動時または定刻に、情報を収集し送る事で、ファームウェアの真正性情報をチェックし、
常に正規のIoTデバイスのみを接続する制御が可能です。
もしも、ファームウェアの真正性情報をチェックした結果、 不一致の場合、OTA機能により、
自動で最新のファームウェアに復元する事が可能です。



kusabi™による検討課題の解決

ご清聴くださり ありがとうございました

kusabi™ホワイトペーパーの入手をご希望の方は、
タイトルに「ホワイトペーパー希望」とし、
本 文に「所属先」、「所属部署／役職」、「氏名」、「電話番号」、「メールアドレス」を記載の上、
以下のメー ルアドレス宛にお申し込みください。

E-mail : kusabi-info@ml.ibc21.co.jp