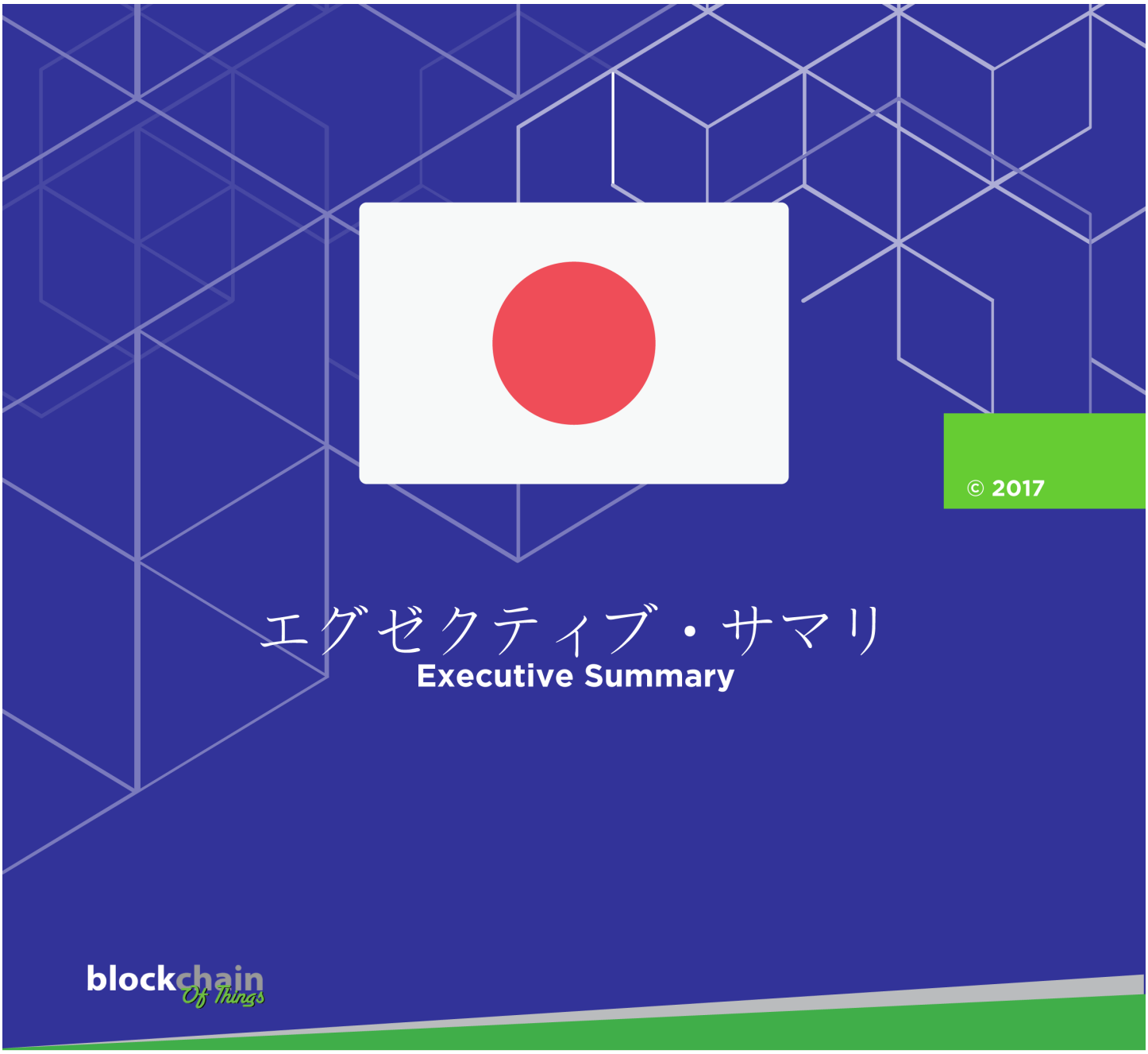


BCOT Global Holdings

# 要約

モノのインターネット（IoT）は安全とは言えず、私たちはその改善を計画しています。

Blockchain of Things, Inc. はビットコイン・ブロックチェーンにコード化された、使い勝手に優れたウェブサービスレイヤーである Catenis Enterprise を正式発表することで IoT セキュリティ問題の解決を図ろうと考えています。ウェブサービスレイヤーのアプローチを用いることで高い適応性を持つ Catenis は、Ethereum、Hyperledger 等の数多くのブロックチェーンをサポートすることができます。Catenis はアクティブないくつかの法人クライアントとのライブネットワーク（ベータ）です。

本書では、最初に IoT セキュリティ脅威の性質およびエンタープライズ IoT 採用にあたって解消すべき主なハードルを特徴付けます。続いて、従来の IoT インフラと比較した際のビットコイン・ブロックチェーンのセキュリティ上の利点を浮き彫りにします。さらに、組織による安全な IoT デバイス・コミュニケーション目的でのビットコイン・ブロックチェーン使用を阻んできた障壁を詳述します。そして、Catenis Enterprise がこうした障壁を解消しつつ、ビットコイン・ブロックチェーンのセキュリティと信頼性を駆使する仕組みを説明します。最後に、Catenis 機能を拡張し従来の IoT の範囲を超越する用途をもたらす重要な属性である、真の認証とスマート資産の概念を紹介します。

# エグゼクティブ・サマリ

モノのインターネット（IoT）は安全とは言えず、私たちはその改善を計画しています。

**IoT は安全ではありません：**500 を超える法人 IoT バイヤーを対象とする Bain スポンサードの調査の結果、工業用 IoT 導入の加速化にあたっての 1 番の障壁がセキュリティ面の不十分さであることが明らかになりました[1]。従来の IoT 市場を苦しめるセキュリティの懸念の大部分は、IoT デバイス・コミュニケーションの集約型サーバーに依存する現状から来ています。より具体的には、IoT の脆弱性は次の 3 つのカテゴリーに分類することができます：

- **サービス妨害（DoS）攻撃：**DoS 攻撃はミッションクリティカルの IoT 対応サービスを無限に混乱に陥れることができます。
- **ハッキング：** デバイス・スプーフィング、中間者攻撃、リプレイ・アタックといった様々なハッキング行為は窃盗あるいはデバイスのハイジャックに発展する可能性があります。
- **監査能力の欠如：**監査トレイルの欠如は、すなわち、デバイスの管理者が数か月あるいは数年にわたって不正な侵入行為を認識しないままとなる可能性があることです。

**ビットコインは安全です：**ビットコイン・ブロックチェーンは、最古にして最も多くの試験で試行されてきた分散型台帳（distributed ledger）であり、中央障害点がないことを考慮すると、こうしたセキュリティ問題を本質的に解決します。ビットコイン・ネットワークは多彩なハッキングや DoS 攻撃に対する耐性を証明してきたと同時に、台帳入力の不可逆性を前提に、自らの監査能力を実証してきました。よって、管理者は、デバイスとビットコインのアドレスの結合およびビットコイン・ブロックチェーンを利用しての当該アドレスへのメッセージ（例：コマンドおよびコントロールのシグナル）送信によって、安全に起動して IoT デバイスとコミュニケーションを図ることが可能なのです。

**Catenis はビットコイン IoT 制約の限界を打破します：**こういったセキュリティ面の利点にかかわらず、ビットコイン・ブロックチェーンは IoT 目的での利用を妨げてきた数々の制約を被っています。Catenis Enterprise はこうした障壁を克服し、ビットコインのセキュリティ面の利点を保持できるような形でそうしたことを実践します。なぜなら、Catenis はビットコイン・ブロックチェーンにコード化されたウェブサービスレイヤーであるからです。工業用 IoT 用途にあたって、ビットコイン・ブロックチェーンの制約および Catenis の対応する重要な特長は以下の 6 つのカテゴリーに分類することができます：

- **80 バイトのサイズ制約：**ビットコインのメッセージ・フィールドはわずか 80 バイトであり、制約されていて IoT デバイス同士の膨大な有意なデータのペイロードを送信する能力に達していません。Catenis はこうした課題について、メッセージが種別やサイズを問わないプログラミングコードやデータファイルを包含することができるよう、サイズ制約を取り除くことで解決します。

- **許認可の欠如：**IoT デバイスがパブリックのビットコイン・アドレスに接続されている場合、接続先のアドレスが誰のメッセージでも受諾することから、不正な存在がデバイスを有効化することが考えられます。Catenis はオープンのビットコイン・ブロックチェーンにコード化されている許認可されたネットワークの創造を通じてこうした課題を解決します。
- **暗号化の欠如：**ビットコイン・ブロックチェーン経由で送信されるメッセージは、暗号化されていないことから、世界中の誰でも見ることができます。Catenis はエンドツーエンドの暗号化を供与することでこうした課題を解消します。.セキュリティ機能はそこで終わりではありません。なぜなら、同時に、Catenis は、システムが IoT デバイスにメッセージを送信するたびに、デバイスに割り当てられる全く新しいビットコインのアドレスを使用するからです。このため、従前に使用されていたビットコインのアドレスに送信されるメッセージは問題のデバイスには一切影響を及ぼしません。このことは、メッセージが、瞬きするようなほんの一瞬しか存在しない一時的なトンネルを通り過ぎるにあたって、PFS（Perfect Forward Secrecy）[2]を徹底します。また、不正な存在が関連メッセージを発見すべく分析を実施するのを阻止します。
- **スピードとスケーリングの課題：**ビットコインの確認時間は遅く、ブロックチェーンは公に知られているスケーリングの課題に苛まれています。Catenis は、瞬時かつスケーラブルなトランザクションの提供を可能とする、Lightning Network 同様の 2 番目のレイヤーファブリックとして実行することでこうした課題を解決します[3]。ただし、Lightning Network とは異なり、Catenis が許認可されたネットワークであることから、取引先リスクを伴うことなく機能することができます。
- **CTO にとっての使用困難：**大半の IT スタッフがブロックチェーンのプロトコルに精通していないことから、ビットコイン・ブロックチェーンは使用が難しいと言えます。Catenis は顧客のためにウェブサービスレイヤーおよび使い勝手に優れた API を作成することでこうした課題を解消します。
- **CEO にとっての管理困難：**ビットコイン・ブロックチェーンは、多くの CFO が暗号通貨の管理を経験していないため、一部の CFO にとって管理が困難であると考えられます。Catenis は秘密裏に必要な暗号通貨トランザクションを実施することでこうした課題を解決します。その結果、法人クライアントの観点から暗号通貨は除去されます。

**Catenis は POA（Proof of Authenticity：真正性証明）を促進します：**Catenis の拡張型特長セットは従来の IoT 範囲の枠にとどまらない用途を可能にします。これにより、真の認証のシステムが包含されます（すなわち、POA（proof of authenticity：真正性証明）。Catenis を備えることで、現実世界の製品の真正性を追跡し、小売およびサプライチェーンの両方の製品詐欺を軽減することが可能となります。これは、推定で年間$1.9 兆相当に達する問題となっています。[4] 認証プロセスには 2 つの鍵となる手順があります：

- **製品メーカーが COA（Certificate of Authenticity：真正性認証）を保持しているか確認します：**メーカーはブロックチェーンに対する COA（certificate of authenticity：真正性認証）の暗号フィンガープリントをログし、製品メーカーが COA（certificate of authenticity：真正性認証）をログしたエンドポイントを保有する旨の独立した暗号確認を可能とする参照 ID を再販者/顧客に提供することができます。
- **COA（Certificate of Authenticity：真正性認証）が本物であることを確認します：** Catenis は独立した暗号アイデンティティ認証を表示することができます。所定の Catenis デバイス・エンドポイントの所有者は、適切なウェブサイトのドメイン、政府登録またはサードパーティ認証へのアクセスあるいは係る所有権を実証することで自らのアイデンティティを証明することができます。以上の 2 つの手順が複合化されることで、信頼に足りない POA（proof of authenticity：真正性証明）を特定してサプライチェーンや小売環境における詐欺を軽減するのに役立てることができます。

**Catenis はカスタマイズ可能なスマート資産を可能にします：**Catenis はクライアントにより多くの事物をデジタル化する能力を与えることで従来の「モノのインターネット」の範囲を超える能力を提供します。この目標は、顧客によるスマート資産の作成およびユーザー間のその移転を可能にすることで成就されます。Catenis のスマート資産は Colored Coin Protocol（カラードコイン・プロトコル）のあらゆる強固な機能性とスマート契約能力を備えています[5]が、次の 4 つの重大な点ではいっそう強力です：

- **実際のデジタル・ペイロードを送達するオプション：** Catenis のスマート資産はそのメッセージング能力と結合し、実際のデジタル・ペイロードを送信すべく構成設定可能ですが、これは、無関係の外部システム経由での要求が必須である、デジタル資産が第三者の約束に裏付けされたペイロードの単なる表意であるところの数多くのその他の暗号プロジェクトと対照的です。Catenis のスマート資産は実際のストック認証、自宅の権利証あるいは MP3 ファイルを送信すべく構成設定可能であることから、実際のペイロードをとあるユーザーから他のユーザーに移転させることができます。
- **デジタル・ペイロードを暗号化するオプション：** Catenis のスマート資産とともに移動するデジタル・ペイロードは目的先エンドポイントのパブリックキーにて暗号化可能であるため、目的先エンドポイントのみがペイロードにアクセスすることができます。このことは、ペイロードが暗号化されずに世界中に可視されるような暗号プロジェクトと対照的です。
- **メッセージに反応するオプション：** Catenis のスマート資産は他のエンドポイントからのメッセージに反応すべく、構成設定可能ですが、このことはデジタル資産が非反応的であるような暗号プロジェクトと対照的です。例えば、Catenis 顧客はメッセージ受領を条件に、スマート資産の自動創造と配布をプログラムすることができます。このことですが、Catenis がトークン販売を含む（ただし、必ずしもこれに限定

されない）効率的で透明なデジタル資産の配布にあたってのプラットフォームになるのを可能にします。

- **許認可されたネットワーク：** Catenis は許認可されたネットワークであることから、スマート資産は不正なエンドポイントからのメッセージには反応しません。このことは、許認可能力を欠く暗号プロジェクトと対照的です。

**Catenis はサードパーティ・アプリケーションにとってのプラットフォームです：**Catenis は、基本的に、サードパーティのデベロッパーが、構成要素として、Catenis のコア機能性（例：安全なメッセージング、スマート資産等）を用いてアプリケーションを構築することのできるプラットフォームです。当社は、サードパーティのプログラマーが将来の開発努力に焦点を当てることのできるような数多くのカテゴリーの中の 4 つを重要視します：:

- **IoT 確保にあたっての産業特有のアプリケーション：**多様な産業および多彩なオペレーション要素は、様々な使用事例から、Catenis の安全な IoT 機能性を用いたいと考えています：結果、サードパーティのデベロッパーは Catenis のセキュリティを活用する産業特有のアプリケーションを構築して様々な IoT 市場のセグメントに注文仕様のソリューションを供与することが可能です。
- **サービスとしてのハードウェア：**Catenis は、スマート資産という形態のデジタルキーが Catenis エンドポイントに結合された遠隔ハードウェアにおける機能性を解除しうることから、「サービス」として、安全でブロックチェーン基盤の「ハードウェア」を実現します。サードパーティのデベロッパーは多彩な産業を対象に、様々な形でこうした機能性を駆使する産業特有のアプリケーションを構築し得ます。
- **チケットのマーケットプレイス：**Catenis はスマート資産の本来の発行者が当該資産の再販による手数料を得るのを可能にします（手数料ベースのスマート資産）。例えば、コンサートチケットの発行者は、係るチケットが二次的マーケットプレイスで再販される場合に手数料を得る可能性があります。サードパーティのデベロッパーは、Catenis レイヤーを駆使するスマート資産意識にてチケットのマーケットプレイスを構築することでこうした機能性を市販化することが可能です。
- **エクイティのマーケットプレイス：**デラウェア州法では、米国法人がブロックチェーンに係る株式をトレードして株式決済プロセスの合理化を図ることが認められています。Catenis は、すでに、実際の株券を移転することのできるスマート資産をコード化するための機能性を備えています。さらに、Catenis は暗号通貨を概念化する機能を備えているため、従来の株式投資家は暗号通貨を直接取引する必要を負うことなく、通常の仲買会社から会社株式を購入することができます。サードパーティのデベロッパーは株式決済プロセスを合理化するようなエクイティのマーケットプレイスを構築し得ます。

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

2 Scott Helme May 2014: “Perfect Forward Secrecy - An Introduction” https://scotthelme.co.uk/perfect-forward-secrecy/

3 Joseph Poon, Thaddeus Dryja: “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments” https://lightning.network/lightning-network-paper.pdf

4 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

5 Colored Coin Protocol: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki