ブロックチェーンを活用してIoTのセキュリティを向上させるソフトウェアアーキテクチャの設計
―スマートホーム内外のセキュアな接続の確保を目的に―

M2019SE005 奥村康平
指導教員：沢田篤史

1　はじめに

近年，Internet of Things（以下，IoT と呼ぶ）の普及に伴い，制御機器や家電製品，センサなどがホームネットワークを介しての協調や相互利用が可能になっている．しかし，IoT には相互運用性の低下，IoT 機器のリソース制約，セキュリティなどの課題が存在する．IoT の応用の一つとしてスマートホームがある．スマートホームでは，ネットワーク接続された家電製品やスマートデバイス，センサなどを連携させることで，利用者の状況に応じたサービスの提供を行うアプリケーションを作ることができる．また，スマートホームのホームネットワークには認証情報（ID やパスワード）や利用者のプリファレンス情報などの個人情報が含まれている．

外出先からスマートホーム内の機器を利用する場合，機器利用に必要なデータをスマートホーム外部に保存し，外出先からアクセス可能とする必要がある．保存されたデータへ外部からアクセス可能となることから，データの保存先に対するセキュリティの確保が求められる．また，セキュリティ確保するためには暗号化やアクセス制御が必要となり，アクセス制御や暗号化を行うためには，守るべきデータ（アクセス制御リストや暗号鍵など）が増える．さらに，外出先で利用することで，利用する機器の数や場所の組み合わせ，一時的な機器の利用なども増える．保存するデータの増加と多様化に対し柔軟に対応するために，スケーラビリティを確保する必要がある．

本研究の目的は，スマートホームにおける IoT 機器間の相互接続のための既存アーキテクチャを，セキュリティとスケーラビリティの確保が可能なよう再設計することである．そのアーキテクチャにより，スマートホーム内外でのセキュアで柔軟な機器接続を実現させる．本研究では，上述した目的を達成するために，横山らが提案する既存アーキテクチャにブロックチェーンとブロックチェーン上で動作するスマートコントラクトを適用する．また，アクセス制御方式として，ロールベースアクセス制御（RBAC）を適用して，柔軟なアクセス制御を実現する．ブロックチェーンに保存されたデータを基に，スマートホームでの動的適応を可能とするソフトウェアアーキテクチャを設計し，安全に多種多様な IoT 機器とその機能の利用を目指す．

2　背景技術

2.1　横山らの研究

横山ら [2] の研究では，スマートホームで用いられる IoT アプリケーションにおける柔軟性と相互運用性の確保を可能とするソフトウェアアーキテクチャを提案している．Adapter パターンと PBR パターンの２つを適用し，IoT デバイスを相互に連携させる論理を IoT 機器構成ポリシモジュールに記述し，動的再構成を行う．また，利用者の状況や嗜好に適用させる論理をアダプタモジュールに記述し，プロトコルなどの変換を行う．これにより，柔軟性に関する論理と相互運用性に関する論理それぞれをアプリケーション論理から分離している．異なる関心事を明確にモジュールとして分離する構造により，IoT アプリケーション開発を容易にするための基盤を提供している．横山らは，提案したアーキテクチャに基づいて，IoT 機器間の動的適応が可能であることを示すために，機器間の簡単なメッセージアプリケーションを実装している．図 1 に横山らが提案するアーキテクチャの基本構造を示す．

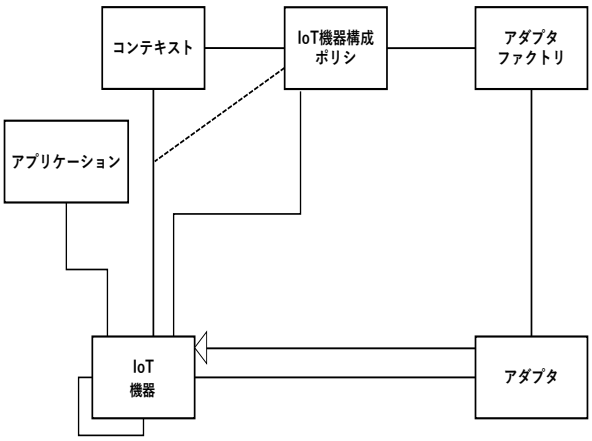

図 1　横山提案するアーキテクチャの基本構造 [2]

2.2　ブロックチェーン技術

ブロックチェーン技術 [4] は，Satoshi Nakamoto によって仮想通貨 Bitcoin[5] を実現させるために考案された分散型台帳である．現在では，分散型アプリケーションやスマートコントラクトを構築するために使用される Ethereum など Bitcoin 以外のブロックチェーン基盤が開発されている．トランザクションをまとめたブロックと呼ばれる一連のデータのリストを，複数のノードで管理・運営する．また，コンセンサスアルゴリズムを用いたマイニングによりブロックの正当性を担保する．

2.3　スマートコントラクト

スマートコントラクト [4] とは，Nick Szabo によって作られた用語で，「当事者が他の約束を実行する手順まで含んだ，デジタル形式で規定された一連の約束」と定義されている．

スマートコントラクトは執行条件と執行内容をあらかじめプログラムで定義しておくことで，条件に合致したイベ ントが発生すると自動執行することができる．実行が当事者の独立した行動に依存する従来の契約とは異なり，スマートコントラクトは，当事者の直接の介入なしに，コンピューターによる契約の合意を実行することができる．ブロックチェーンはスマートコントラクトを実装し，参加者間で共有することが可能である．また，スマートコントラクトのトランザクションは，P2P ネットワーク上の ブロックチェーンに記述されるので，トランザクションの信頼性や透明性が確保できる．

2.4 ロールベースのアクセス制御（RBAC）

ロール ベース アクセス制御 (RBAC) [6] は，アクセス権限を持つロールを割り当てられたユーザかどうかを認証し，システムやリソースへのアクセス制限を行うアクセス制御方式の 1 つである．さまざまな役割に応じて複数のロールが作成することができ，特定の操作を実行するための権限が，特定のロールに割り当てられる．特定のロールが割り当てられると，そのロールの権限によって，コンピューターシステムの特定の機能を実行するための権限を取得することができる．ユーザの権限は直接割り当てられるのではなく，ロールを通じてのみ取得できるので，個々のユーザのアカウントに適切なロールを割り当てることで利用者権限を管理できる．また，ユーザの追加や役割の変更などの一般的な操作が容易にできる．

3 ブロックチェーンを活用したアーキテクチャの設計

3.1 提案するアーキテクチャの概要

本研究の目的は，スマートホーム内外でのセキュアで柔軟な機器接続を実現させるために，スマートホームにおける IoT 機器間の相互接続のための既存アーキテクチャを，セキュリティとスケーラビリティの確保が可能なよう再設計することである．スマートホーム内の機器を外出先で利用することを想定し，横山らのアーキテクチャを対象に，スマートホーム外への接続を想定したコンポーネントの追加や修正を行う．

本研究では，IoT におけるセキュリティとスケーラビリティの確保とスマートホーム内外での柔軟な機器接続を実現させるために，横山らのアーキテクチャにブロックチェーンとブロックチェーン上で動作するスマートコントラクトを適用する．ブロックチェーンに保存されたデータを基に，スマートホームでの動的適応を可能とするソフトウェアアーキテクチャを設計する．また，アクセス制御方式として，ロールベースアクセス制御（RBAC）を適用する．集中的に ACL を管理する中で，RBAC を用いることで，一時的に利用者のロールを変更するなど，柔軟なアクセス制御を実現する．

具体的シナリオとして，スマートホーム内のドアホンの通知先を，コンテキストである利用者の位置（スマートホームの内か外など）に応じたディスプレイに切り替えること想定する．ホーム内でスマートホーム機器を利用する場合は，ホームネットワーク内で管理されたデータを利用して，通知先ディスプレイの動的再構成を行う．外出先でスマートホーム機器を利用する場合は，ブロックチェーンに管理されたデータを利用して，通知先ディスプレイの再構成を行う．

スマートホームの内か外といったコンテキストによる切り替えは，通知先だけではなく，通知先を切り替えるために必要なデータや，発生したデータの保存先も切り替える必要がある．通知先がホームネットワーク内ならば，ホームネットワーク内に保存されたデータの利用と，また，発生したデータをホームネットワーク内で管理を行う．通知先がホームネットワーク外ならば，ブロックチェーン上に保存されたデータの利用と，発生したデータをブロックチェーン上で管理を行う．利用者がスマートホーム内で機器を利用する場合は，ブロックチェーンにデータを保存する必要がないので，横山らのアーキテクチャを用いた，通知先の切り替えを行う．利用者が外出先で機器を利用する場合は，コンテキストが切り替わってブロックチェーンを用いた，通知先の切り替えを行う．

3.2 設計指針

スマートホーム内でのスマートホーム機器を利用する場合は，ホームネットワーク内のデータと PBR パターンを用いて，データの保存先と通知先の IoT 機器の切り替えを行う．実行手段構成ポリシには，利用者の位置に応じたデータ保存先の切り替え（ホームネットワークかブロックチェーンか）に関する振る舞いを定義する．IoT 機器構成ポリシには，利用者の位置とホームネットワーク内に保存されたデータに応じた IoT 機器の切り替えに関する振る舞いを定義する．外出先でスマートホーム機器を利用する場合は，ブロックチェーン上のデータとブロックチェーン上で動作するスマートコントラクトを用いて，接続先のディスプレイを決定し，PBR パターンを用いて，データの保存先と通知先の IoT 機器の切り替えを行う．スマートコントラクトを用いて接続先のディスプレイを決定するには，利用者・ドアホン・ディスプレイそれぞれが契約を行う．スマートコントラクトの実行結果とブロックチェーン上に保存された利用者のプリファレンス情報を元に PBR パターンによってディスプレイの切り替えを行う．以下にそれぞれの契約について示す．

- 利用者とドアホンの契約：利用者がドアホンの利用登録を行い，ドアホンのメッセージをディスプレイに通知を送ることができる状態にする．スマートコントラクトには利用者情報（利用者のロール）に利用の権限があれば，ドアホンの利用を許可する振る舞いを定義．
- 利用者とディスプレイの契約：利用者がディスプレイの利用登録を行い，利用者のディスプレイとして登録する．スマートコントラクトには利用者情報に利用の権限があれば，利用の位置に応じたディスプレイの選択と利用の許可をする振る舞いを定義．
- ドアホンとディスプレイの契約：ドアホンが押された時，利用者とドアホンの契約と利用者とディスプ

レイの契約を元に，利用者のディスプレイを検索し，接続を許可する．スマートコントラクトにはドアホンとディスプレイの利用許可があれば接続許可をする振る舞いを定義．

利用者がドアホンを利用する場合，利用者がドアホンを利用できるかを認証する必要があるので，利用者とドアホンの契約を行い，ドアホンの利用登録を行う．同様に，利用者がディスプレイを利用する場合，利用者がどのディスプレイを利用するかやディスプレイを利用できるかの認証をする必要があるので，利用者とディスプレイの契約を行い，ディスプレイの利用登録を行う．ドアホンと利用者に登録されたディスプレイとが接続をする場合，共に利用者が利用できる状態であるかを確認する必要があるので，ドアホンとディスプレイの契約を行い，接続を許可する．一方，アクセス制御方式としての RBAC を利用し，あらかじめ決められたロールに基づいて，利用者がドアホンやディスプレイにアクセスできるようにする．

3.3 ブロックチェーンを用いた接続機器の切り替え

本研究では，外出先でスマートホーム機器を利用する場合は，ブロックチェーン上で管理されたデータを利用して，通知先ディスプレイの動的再構成を行う．図 2 にはブロックチェーンによる IoT 機器切り替えの全体構造を示す．IoT 機器の切り替えについて，IoT 機器構成ポリシには，ブロックチェーン上のデータ（IoT 機器情報，利用者のプリファレンス情報，アクセス制御リストなど）に基づいて，コンテキスト（利用者の位置）に応じた IoT 機器の切り替えに関する振舞い記述をする．IoT 機器構成振舞活性機は IoT 構成ポリシからのメッセージによって，IoT 機器の切り替えを行う．また，実行手段構成ポリシにはコンテキスト（利用者の位置）に応じたデータの保存先切り替えに関する振舞い記述をする．実行手段構成振舞活性機は実行手段構成ポリシからのメッセージによって，保存先の切り替え（ブロックチェーン）を行う．このように IoT 機器の切り替えを行うことで，IoT 機器の動的再構成を行う．

IoT 機器の切り替えについても，センサによるコンテキストの変更をきっかけに行われる．IoT 機器切替ポリシがセンサからのメッセージを横取りし，変更後のコンテキストとブロックチェーン上のデータとスマートコントラクトの実行結果に応じて，通知先の IoT 機器を切り替えるように，IoT 機器構成振舞活性機に再構成の指示を行う．IoT 機器構成振舞活性機は指示を元に，通知先の IoT 機器を切り替える．スマートコントラクトは，ブロックチェーンから利用者の位置を取得し，利用者情報や利用者の位置情報・プレファレンス情報を元に，ドアホンとディスプレイと利用の契約を行う．利用者とドアホン，利用者とディスプレイの契約の結果によって，ドアホンとディスプレイの接続を許可する．

保存先の切り替えについては，ホームネットワークのデータ利用時と同様に，センサによるコンテキストの変更をきっかけに行われる．実行手段構成ポリシがセンサからのメッセージを横取りし，変更後のコンテキストに応じて，データの保存先をブロックチェーンに切り替えるように，実行手段構成振舞活性機に再構成の指示を行う．実行手段構成振舞活性機は指示を元に，データの保存先をブロックチェーンに切り替える．図 3 に保存先構成の動的振舞い，図 4 にブロックチェーン上のデータ利用時の動的振舞いを示す．

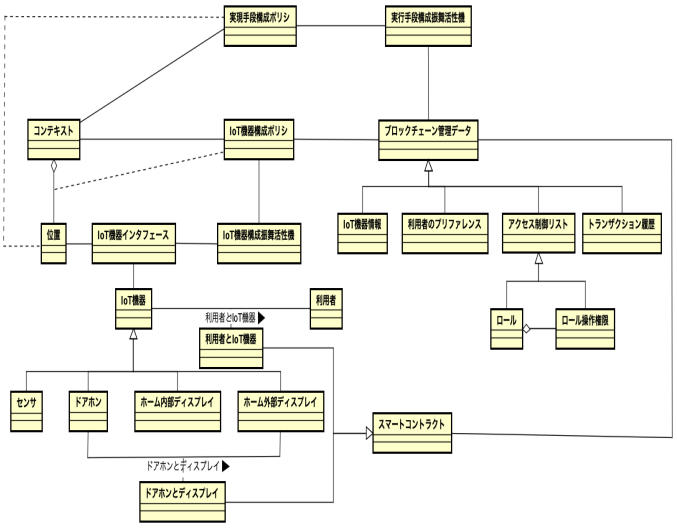

図 2 ブロックチェーンによる IoT 機器切り替えの全体構造

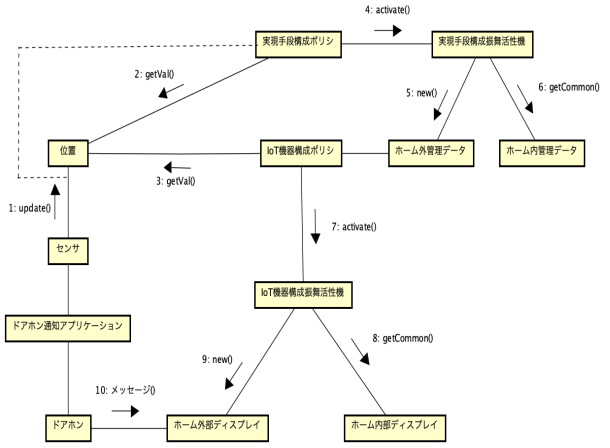

図 3 保存先構成（ブロックチェーン）の動的振る舞い

4 考察

4.1 提案したアーキテクチャ有用性

本研究のアーキテクチャを用いることで，スマートホームにおける IoT 機器間の相互接続のための既存アーキテクチャに対するセキュリティとスケーラビリティの確保が可能になる．横山ら [2] のアーキテクチャを用いてスマートホーム内の機器を外出先で利用する場合，外部に機器利用に必要なデータを保存する必要があるので，外部攻撃に対するセキュリティリスクが増える．また，機器利用に伴い，保存するデータが増加するので，データの保存先にスケーラブルな仕組みが求められる．

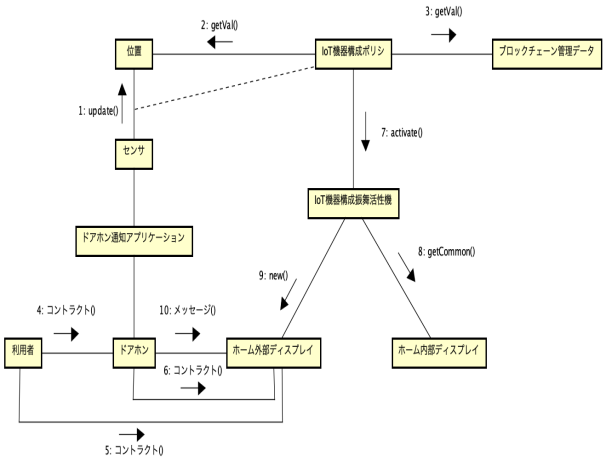

図 4 ブロックチェーン上のデータ利用時の動的振舞い

本研究では，横山らのアーキテクチャにブロックチェーンを用いることで，ブロックチェーンの特徴であるハッシュ化や暗号化により，保存されたデータに対するセキュリティを確保した．また，データを分散して管理し，保存するデータの増加と多様化に対し柔軟に対応することで，安全に多種多様な機器とその機能の利用を可能とした．

4.2 ブロックチェーン以外の適用によるセキュリティの確保

ブロックチェーンの適用以外にも，VPN（Virtual Private Network）を用いることで IoT 機器のセキュアな接続が実現可能であると考える．VPN とはインターネット上に仮想的なプライベートネットワークを構築し，セキュリティを確保して通信を行うことができる技術である．VPN を適用することで，外出先でスマートホーム機器を利用する場合でも，外部にデータを保存することなくスマートホーム機器を利用することが可能である．しかし，VPN を利用する場合，VPN ルータを複数用意し，ルータそれぞれに対して接続の設定をする必要がある．本研究で想定しているシナリオでは，コンテキスト（利用者の位置）や利用するディスプレイは繰り返し変更されるので，機器を利用するごとに，スマートホームと利用するディスプレイを VPN 接続する必要がある．様々な場所でスマートホーム内の機器の利用を想定した場合，接続の設定に多くのコストや時間を要する．スマートホーム内の機器の利用を容易するために，機器の利用に必要なデータを外部で一元管理することが重要である．

一方，外部にデータを保存する方法として，クラウドストレージで管理することも考えられる．クラウドに機器利用に必要なデータを一括管理し，外出先から機器やデータへのアクセスをすることで，スマートホーム機器同士の連携が容易になる．しかし，データを管理するサーバが集中しているので，外部攻撃に対するセキュリティの確保が必要である．また，利用する IoT 機器が増えるとサーバに対する負荷が大きくなるので，データの増加に対する柔軟な対応が求められる．

本研究で提案したアーキテクチャは，機器利用に必要なデータをブロックチェーン用いてデータの一括管理を行う．ブロックチェーンを用いることで，機器を利用するごとにスマートホームとの接続を行う必要はなく，暗号化やハッシュ化などの暗号化メカニズムによって保存したデータのセキュリティを確保できる．また，データを分散管理することで，利用する IoT 機器の増加によるサーバへの負荷を軽減させることや，データの増加に対する柔軟な対応が可能となる．

5 おわりに

本研究の目的は，スマートホームにおける IoT 機器間の相互接続のための既存アーキテクチャを，セキュリティとスケーラビリティの確保が可能なよう再設計することである．そのアーキテクチャにより，スマートホーム内外でのセキュアで柔軟な機器接続を実現させる．本研究では，上述した目的を達成するために，横山らのアーキテクチャにブロックチェーンとブロックチェーン上で動作するスマートコントラクトの適用を行なった．設計するアーキテクチャをコンテキスト指向によって実現することで，外部環境に応じて柔軟に対応することを可能とする．また，アクセス制御方式として，ロールベースアクセス制御（RBAC）を適用して，柔軟なアクセス制御を実現した．ブロックチェーンに保存されたデータを基に，スマートホームでの動的適応を可能とするソフトウェアアーキテクチャを設計し，安全に多種多様な IoT 機器とその機能の利用を可能にする．今後の課題として，RBAC とスマートコントラクトを組み合わせた実装の検証や横山らのアーキテクチャの枠組みと組み合わせた実現を検討する．また，ブロックチェーンに格納するデータ（機器情報，プリファレンス情報，ACL）がより複雑になった場合や制約がある場合に，それらのデータとブロックチェーンとの整合性を示す必要がある．

参考文献

[1] 江坂篤侍，野呂昌満，沢田篤史，“インタラクティブシステムのための共通アーキテクチャの設計”, コンピュータソフトウェア，Vol. 35, No. 4, pp. 3-15，2018.

[2] 横山史明，沢田篤史，野呂昌満，江坂篤侍，“IoT の柔軟な相互運用性を実現するソフトウェアアーキテクチャの提案”，ソフトウェア工学の基礎 XXVI（日本ソフトウェア科学会 FOSE2019），pp. 93-102，2019.

[3] A. Panarello，N. Tapas，G. Merlino，F. Longo，A. Puliafito，“Blockchain and IoT Integration: A Systematic Survey”，Sensors 2018，Vol. 18 ，No. 8，2018.

[4] A. M. Antonopoulos，G. Wood，マスタリング・イーサリアム：スマートコントラクトと *Dapp* の構築オライリー・ジャパン，2019.

[5] S. Nakamoto，“Bitcoin: A Peer-to-Peer Electronic Cash System” ，https://bitcoin.org/bitcoin.pdf. (Accessed 2020-09-20).

[6] R. S. Sandhu，E. J. Coyne，H. L. Feinstein，C. E. Youman，“Role-based access control models”，Computer．Vol. 29，Issue. 2，1996.