B-006

ドメイン駆動設計に基づくクリーンアーキテクチャにおけるアクセス制御構造記述のためのセキュリティ層の提案

A Proposal of a Security Layer for Describing Access Control Structures in Clean Architecture Based on Domain-Driven Design

上原 宗大 †　和﨑 克己 ††
Sota Uehara　Katsumi Wasaki

1　はじめに

IoT 機器を代表とするインターネット接続機器は年々増加しており，そのソフトウェアの設計は複雑化している．適切なプロセスを経てソフトウェア設計が行われるべきであり，特に IoT 機器ではセキュリティ性も重要である．ソフトウェア設計手法の 1 つであるドメイン駆動設計やそこで用いられるクリーンアーキテクチャでは明確な責務分離を提供するのに対し，アクセス制御のようなセキュリティ要件を表現することができない．そこで本研究では，DDD やクリーンアーキテクチャの考えかたを基盤としつつ，アプリケーション層とドメイン層の間にセキュリティ層を定義することで，設計上でセキュリティを内包するアーキテクチャを提案する．

2　ドメイン駆動設計 (DDD)

ドメイン駆動設計 (DDD) は，エリック・エヴァンス氏が 2003 年に提唱したソフトウェア設計手法である [1][2]．ここでのドメインとはプログラムを適用する対象となる領域のことを指し，これは DDD において最も重要視される．DDD は技術志向の設計手法では無く，ビジネスドメインの知識に重点を置いた設計手法となっており，ドメインエキスパートと呼ばれる対象のドメインについて最も詳しい専門家とソフトウェア開発者の間で対話を繰り返しながらソフトウェア開発が行われる．対話の際にはユビキタス言語と呼ばれる共通言語が用いられ，ドメインモデルを作成しながら戦略的にドメインを理解してソフトウェア開発が行われる．2003 年に提唱された DDD であるが，手法としての完成度の高さから近年再注目されている．

DDD においては，境界付けられたコンテキスト（Bounded Context）によって全てを 1 つのドメインとして扱うのではなく，いくつかのサブドメインをコンテキストに分割し，それぞれの中でモデルやユビキタス言語の統一を目指す．Ozan Özkan らの論文 [3] においても，大規模システムを独立したコンテキストに分割することで，システムの複雑さを減少させ保守性の向上を図ることができている．

3　クリーンアーキテクチャ（Clean Architecture）

クリーンアーキテクチャは 2012 年に Robert C. Martin によって提唱され [4][5]，図 1 のように表現される．

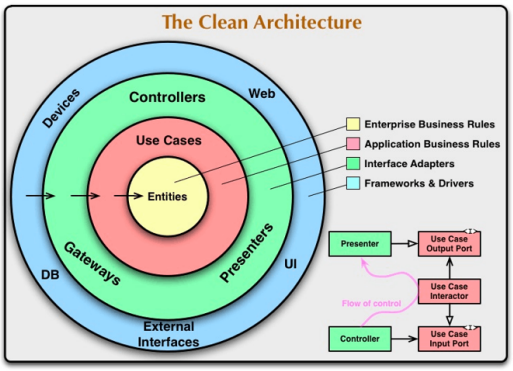

図 1　クリーンアーキテクチャ ([4] より引用)

DDD では，伝統的にレイヤードアーキテクチャという階層構造のアーキテクチャが用いられてきたが，これには DDD の原則に反するいくつかの問題があった．クリーンアーキテクチャでは，図 1 のような同心円の図で表せるように，依存関係の向きを外側から内側に向けて設計することで，ビジネスロジックが UI やデータベースに依存しないソフトウェア設計が可能となる．このように各層の役割が明確に分離されているため，システムの柔軟性や保守性が大きく向上する．一方で，このクリーンアーキテクチャの図においては，各レイヤーでどのような準形式手法を適用するのか明確な定義は無い．準形式的に表現することが可能となれば，システムの構造や振る舞いを理解しやすくし，開発の効率にも寄与すると考えられる．そこで，次節以降において図 2(左) の様に表現される提案手法に関して紹介する．

4　クリーンアーキテクチャとロバストネス図の融合

本研究ではクリーンアーキテクチャを準形式的に記するべく，内側から第 2 層（Use Cases）と第 3 層目（Controllers）に図 2（左）の様にロバストネス図の表記を導入した．ロバストネス図では，バウンダリ・エンティティ・コントロールの 3 要素を用いて表現されるが [6]，このうちのエンティティは既に第 1 層に記述されるため，バウンダリとコントロールをそれぞれ第 3 層と第 2 層に配置する．図 2(右) にあるように，バウンダリはユーザや外部システムとのやり取りを担当し，これはクリーンアーキテクチャの第 3 層の役割と合致する．コントロールはバウンダリとエンティティをつなぎ，システム処理やロジックの実装を担当するため，第 2 層の役割と合致する．これにより，システムの要件や振る舞いを視覚的に表現することができ，ワークフローのような振る舞いを表現することができる．

† 信州大学大学院総合理工学研究科, Graduate School of Science and Technology, Shinshu University
†† 信州大学工学部電子情報システム工学科, Department of Electrical and Computer Engineering, Faculty of Engineering, Shinshu University

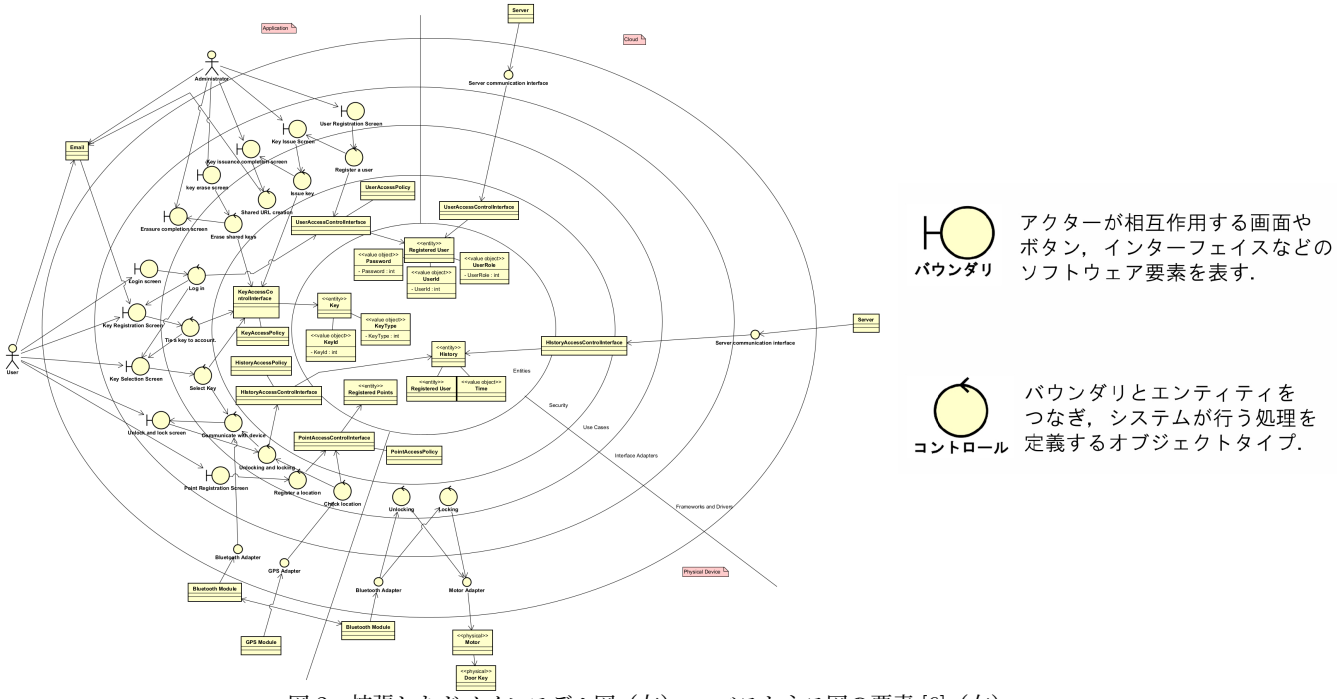

図 2　拡張したドメインモデル図（左），ロバストネス図の要素 [6]（右）

以上の表記法を用いることで設計段階から準形式的な表記が可能となったが，ドメインモデル図上ではエンティティへのアクセス制御に関しての設計がなく，IoT デバイスを代表としたインターネット接続機器に含まれるような秘匿性の高いエンティティ情報へのアクセス制御を記述するべきであると考えた．そこで次節に紹介するセキュリティ層を導入することとした．

5　セキュリティ層の導入

本研究では，エンティティへのアクセス制御を設計段階から一貫して記述するために，クリーンアーキテクチャの第 1 層（Entities）と第 2 層（Use Cases）の中間に，セキュリティ層（第 1.5 層）を導入する．本層は，エンティティに対するアクセス要求に対し，ユーザー属性や操作種別に基づいたアクセス可否の判定および処理実行の媒介機能を担う層であり，アプリケーション層とドメイン層の間に責任を分離する設計構造を形成する．前節で紹介したロバストネス図の表記に加え，本章で提案するセキュリティ層を組み込んだドメインモデル全体は，図 2 に示すようにコンテキストごとに整理された構造で表現される．

この図 2(左) ではスマートロック製品を対象ドメインとして扱っており，同心円上の左上をスマートフォンなどのアプリケーションのコンテキスト，右上をクラウドのコンテキスト，下を物理デバイスのコンテキストとして描かれたモデルである．このドメインにおいては，主にアプリケーションのコンテキストが主たるドメインであり，ユーザ登録や鍵の登録・削除・配布等の手順，実際に鍵の解錠・施錠の処理フローが，ロバストネス図のバウンダリとコントロールによって記述されている．提案手法では，ワークフロー上における一連の操作（例：予約の承認からキャンセル，鍵の発行から削除まで）に対応して，処理単位ごとにアクセス制御ポリシーを柔軟に適用可能な構造を採用している．各操作はそれぞれ異なる実行条件や実行主体を持つため，提案手法では操作単位に応じて動的にポリシーを切り替えられるよう，セキュリティ層を挿入している．これにより，単一のエンティティ操作に閉じない，ワークフロー全体を俯瞰したアクセス制御の設計が可能となる．

現時点では具体的なアクセス制御ロジックの実装手法は検討中であるが，ロバストネス図を含む設計表現との整合性を重視した構成を目指している．

6　まとめと今後の課題

DDD を用いたソフトウェア設計の際に，クリーンアーキテクチャを用いた設計を行うことで，レイヤードアーキテクチャで問題となっていた事象が解決された．一方で，準形式的表現やエンティティのセキュリティに関する課題が残っていたため，ロバストネス図の表記を導入し，セキュリティ層を新たに定義した．それにより，設計段階からアクセス制御についての検討を行うことが可能となった．今後は，アクセス制御方式として動的属性評価やワークフロー状態依存の制御構造を考慮した設計指針の整備が必要であり，実システムにおいてこれを検証可能な環境で適用・評価することが課題である．

参考文献

[1] エリック・エヴァンス，今関剛監訳 (2011)，エリック・エヴァンスのドメイン駆動設計，翔泳社
[2] 成瀬允宣 (2020)，ドメイン駆動設計入門，翔泳社
[3] Ozan Özkan, Önder Babur, Mark van den Brand: “Refactoring with domain-driven design in an industrial context”, Empirical Software Engineering, 28:94, February 2023.
[4] The Clean Architecture, https://blog.cleancoder.com/uncle-bob/2012/08/13/the-clean-architecture.html, 2024 年 9 月 17 日最終アクセス.
[5] 増田了ほか (2024)，［入門］ドメイン駆動設計——基礎と実践・クリーンアーキテクチャ，技術評論社
[6] ダグ・ローゼンバーグ，三河淳一監訳 (2007)，ユースケース駆動開発実践ガイド，翔泳社