

## 付録 1. 使用したプロンプト

(ファイル名: STAMPSTPA分析プロンプト.txt)

貴方はシステム開発の中でのセキュリティ設計の担当です。  
これからSTAMP/STPAによる設計を行おうと考えています。  
対象となるシステムは下記の「分析対象となるシステム」に示されている内容を対象とします。  
すでに実施しているSTAMP/STPAの分析内容は、「分析済みのSTAMPモデル」を参照してください。

### # 指示内容

1. アクシデント、ハザード、安全制約を設定しています。これにシステム要件の内容をもとにレビューし、より適当なアクシデント、ハザード、制約条件を表形式で出力してください。
2. 制御コンポーネント、被制御コンポーネント、コントロールアクション、フィードバックを表形式で出力してください。
3. コントロールアクションごとに与えられないとハザード、与えられるとハザード、早過ぎ、遅過ぎ、誤順序、早過ぎる停止、長過ぎる適用、といったそれぞれの項目に対して評価を行い、UCAを洗い出します。UCAの識別番号、非安全なコントロールアクション、および違反している安全制約を出力してください。なお、該当する内容がない場合は- (ハイフン) を出力してください。
4. 3.で導出したすべてのUCAに対して、以下に示す「HCFを導くためのガイドワード」に基づいて、望ましくない結果に至るまでのハザードを洗い出し、洗い出されたハザード (HCF) シナリオを表形式で出力してください。
5. 3.で導出したすべてのUCAに対して、望ましくない結果に至るまでのハザード (SCF) について、STRIDEに基づき、シナリオを表形式で出力してください。
6. アウトプットは、出力書式に基づいて出力してください。

STPAハンドブックにも下記については書かれているのですが、テキスト情報でないため分析が正しくできないので修正。

### # HCFを導くためのガイドワード

番号, ガイドワード, 説明

1. 上位からの指示や外部情報の誤り・欠落, 上位システムや外部環境からの命令・情報が誤っていたり、届かなかったりすることで、制御が誤る可能性がある。
2. 不十分な制御アルゴリズム, 制御ロジックが設計不良、更新ミス、環境変化に対応できていないなどで、意図した制御ができない。
3. プロセスモデルが不一致、不完全, コントローラーが持つシステムの内部状態の認識 (プロセスモデル) が実際と異なるため、誤った判断をする。
4. 部品故障・経時変化, ハードウェアの故障や劣化により、制御が意図通りに行われない。
5. フィードバックの不十分・欠落・遅延, 制御結果のフィードバックが得られない、遅れる、誤っていることで、次の制御判断が誤る。
6. 不正確な情報、情報がない、測定の不正確さ、フィードバックの遅延, センサーや通信の問題で、制御に必要な情報が不正確または欠落している。
7. 動作の遅れ, アクチュエーターや人の操作が遅れることで、タイミングを逸して制御が失敗する。
8. コントロールアクションが不適切・無効・欠落, 制御命令そのものが間違っている、届かない、実行されない。
9. プロセスへの入力の誤り・欠落, 制御対象に与える入力 (エネルギー、物質、情報など) が誤っている、または不足している。
10. 意図しない、または範囲外の外乱, 制御対象に予期しない外部要因が加わることで、制御が乱れる。
11. プロセスからの出力の誤り, 制御対象が期待通りの反応を示さない。
12. アクチュエーターの不十分な動作, アクチュエーターが命令通りに動作しない。
13. センサーの不十分な動作, センサーが正しく検知できない、誤った値を出す。

### # 私たちの立場

メーカー技術者

分析対象となるシステムの仕様書、およびSTAMP/STPAの分析情報については、ファイル名で指定することにしており、生成AIには、一緒に渡すことによって、パラメータとして渡せるテンプレートとなるようにしています。

### # 分析対象となるシステム

別途「スマートロック 仕様 Ver1.0.txt」を参照してください。

### # 分析済みのSTAMPモデル/IRI

別途「STAMPSTPA\_インプット.txt」を参照してください。

### # 出力書式

#### ## 1. アクシデント、ハザード、安全制約

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A-1	アクシデント1	H-1	ハザード1	SC-1	安全制約1

#### ## 2. 制御コンポーネント、被制御コンポーネント、コントロールアクション

制御コンポーネント	非制御コンポーネント	コントロールアクション	フィードバック
制御コンポーネントの名称	非制御コンポーネントの名称	コントロールアクション	フィードバック

#### ## 3. UCAの洗い出し

コントロールアクション	与えられないとハザード	与えられるとハザード	早過ぎ、遅過ぎ、誤順序	早過ぎる停止、長過ぎる適用
ブレーキ	UCA-1: 着陸滑走中BSCUが作動している時、BSCU自動ブレーキがブレーキコントロールを出さない[SC-4.1]	UCA-2: 通常離陸中にBSCU自動ブレーキがブレーキコントロールアクションを出す[SC-4.3, SC-4.6]	UCA-3: 着陸後BSCU自動ブレーキがブレーキコントロールアクションを出すのが遅過ぎる(>TBD 秒) [SC-4.1]	UCA-4: 着陸時にBSCU自動ブレーキが、ブレーキコントロールアクションを止めるのが早過ぎる (TBDタクシー速度に達する前) [SC-4.1]

#### ## 4. ハザード (HCF) シナリオ

UCA番号	UCA	HCFに至るまでのシナリオ
UCA-1	ベアリング前に開錠許可	1. (2)制御アルゴリズム不十分: 認証処理に誤りがありベアリングしていない機器と通信許可 2. 不正開錠 (A-1/A-8)

#### ## 5. ハザード (SCF) シナリオ

UCA	STRIDEの区分	UCA	SCFに至るまでのシナリオ
UCA-1	Spoofing (なりすまし)	漏洩したパスワードによる不正ログイン	1. 侵入者が、パスワードを辞書攻撃や、ブルートフォース攻撃などで入手 2. 入手したパスワードでシステムにログイン 3. システムに対して不正アクセス

#

### # その他

STAMP/STPAの手順、STRIDE分析については、下記で示した方法のみを利用してください。  
STAMP/STPAの手順は下記に基づいてください。  
[https://psas.scripts.mit.edu/home/get\\_file2.php?name=STPA\\_handbook\\_japanese.pdf](https://psas.scripts.mit.edu/home/get_file2.php?name=STPA_handbook_japanese.pdf)  
STRIDEについては下記を参照してください。  
[https://owasp.org/www-community/Threat\\_Modeling\\_Process](https://owasp.org/www-community/Threat_Modeling_Process)

STEP by STEPIにて実行してください。

## 付録2. STAMP/STPA分析のインプット情報

(STAMPSTPA インプット.txt)

```
# アクシデント, ハザード, 安全制約
| アクシデントID | アクシデント | ハザードID | ハザード | 安全制約ID | 安全制約 |
|-----|-----|-----|-----|-----|-----|
| A-1 | スマートロックが利用できないこと | H-1 | スマートロックが使えない, | SC-1 | スマートロックは常に使える必要がある。 |
| A-2 | スマートロックに蓄積したデータが外部へ漏洩 | H-2 | スマートロックのデータを認証されない第三者がアクセスする | SC-2 | スマートロックは認証した利用者だけがアクセスできる。 |
| A-3 | クラウドサーバー上のデータが外部へ漏洩 | H-3 | クラウドサーバー上のデータが認証されない第三者がアクセスする | SC-3 | クラウドサーバー上のデータは認証した利用者だけがアクセスできる |
| A-4 | 通信データの盗聴 | H-4 | 通信データを第三者が盗聴しデータが漏洩する | SC-4 | 通信データは暗号化され第三者には盗聴できない |
| A-1 | スマートロックが攻撃者によって不正に利用される | H-1 | スマートロックは攻撃者によって不正に利用できる, | SC-1 | スマートロックは攻撃者によって不正に利用できない |

# 制御コンポーネント, 非制御コンポーネント, コントロールアクション, フィードバック
| 制御コンポーネント | 非制御コンポーネント | コントロールアクション | フィードバック |
|-----|-----|-----|-----|
| **スマートロック** | **ルーター** | 施錠・解錠通知 | スマートロックからの施錠・解錠通知応答 |
| **ルーター** | **クラウドサーバー** | 施錠・解錠通知 | スマートロックからの施錠・解錠通知応答 |
| **クラウドサーバー** | **モバイルアプリ** | 施錠・解錠通知 | スマートロックからの施錠・解錠通知応答 |
| **スマートロック** | **モーター** | 施錠・解錠要求 | 施錠・解錠応答 |
| **スマートロック** | **ルーター** | FWアップデート要求 | FWアップデート応答 |
| **ルーター** | **クラウドサーバー** | FWアップデート要求 | FWアップデート応答 |
| **モバイルアプリ** | **スマートロック** | モバイルアプリからの設定情報の登録 (連携情報・パスワード・指紋情報・顔情報・Wi-Fi設定) | 設定情報登録完了の応答 |
| **モバイルアプリ** | **スマートロック** | 施錠・解錠要求 | スマートロックからの施錠・解錠応答 |
| **モバイルアプリ** | **クラウドサーバー** | 施錠・解錠要求 | スマートロックからの施錠・解錠応答 |
| **クラウドサーバー** | **ルーター** | 施錠・解錠要求 | スマートロックからの施錠・解錠応答 |
| **ルーター** | **スマートロック** | 施錠・解錠要求 | スマートロックからの施錠・解錠応答 |
| **認証モジュール** | **スマートロック** | 認証情報の送信 | 認証情報受信応答 |
```

## 付録3. スマートロック仕様(No.1)

(スマートロック 仕様 Ver1.0.txt)

### # システムの仕様

#### ## システム概要

家庭用に利用できるスマートロックを利用したシステム  
戸建て・集合住宅のドアに工事不要で取り付けができ、施錠・解錠の管理を可能にする  
施錠、解錠は複数の方法で利用可能。  
オートロックにより自動で施錠される。

#### ## ステークホルダと役割

利用者：スマートロックを利用する居住者  
メーカー：スマートロックシステムを開発している会社  
来訪者：利用者の自宅に訪問する者  
攻撃者：利用者の許可なく不正に施錠・解錠を試みる攻撃者

#### ## システムのコンポーネントと役割

1. スマートロック  
スマートロック本体  
戸建て・集合住宅などのドアの錠に取り付け、電気錠として利用できるデバイス
2. スマートフォン（モバイルアプリ）  
一般的なスマートフォン（iPhone・android端末）  
専用のスマートフォンアプリを利用することで遠隔でスマートロックの施錠・解錠、施錠・解錠状態の確認ができる。  
スマートロックの各種設定もアプリでおこなう
3. クラウドサーバー  
一般的なクラウドサーバー  
モバイルアプリを利用した施錠・解錠や施錠・解錠時の通知機能の利用時に使用する
4. ドアセンサー  
スマートロック本体に内蔵されるセンサー。  
スマートロックの施錠・解錠状態を検知する。
5. モーター  
スマートロック本体に内蔵されたモーター  
施錠・解錠操作がされた際にモーターを駆動させ、錠の操作をおこなう
6. 認証モジュール  
スマートロック本体に内蔵される認証モジュール  
モジュールとしてパスワード認証時に利用するテンキー、指紋認証・顔認証で利用する認証器がある
7. ルーター  
一般的な家庭用のルーター  
スマートロックとWi-Fi接続し、クラウドサーバー・モバイルアプリと通信するために使用。
8. NFCカード  
一般的なNFCカード  
スマートロックに登録されたNFCカードをかざすことで施錠・解錠を行うことができる。

#### ## システム要件

一般的なスマートロックの機能を持つ  
施錠・解錠は以下の方法で実施できる

- ・ NFCタグ：事前に登録しておいたNFCカードをかざして施錠・解錠できる
- ・ リモートボタン：スマートロックに搭載したりリモートボタンを押して施錠・解錠できる
- ・ パスワード認証：事前に登録したパスワードをスマートロックのテンキーに入力して施錠・解錠できる
- ・ 指紋認証：事前に利用者の指紋を登録し、認証時に指をかざすことで施錠・解錠できる
- ・ 顔認証：事前に利用者の顔情報を登録し、認証器に顔を映すことで施錠・解錠できる
- ・ 連携したモバイルアプリから遠隔で施錠・解錠ができる
- ・ スマートロックの利用や情報登録は専用のモバイルアプリをメインにおこなう

自動設定機能により一定時間、解錠状態が続くと自動で施錠される  
ドアセンサーによって錠の状態が監視され、施錠・解錠された際にモバイルアプリに通知される  
スマートロックは専用のモバイルアプリを利用し、スマートロックとBluetooth接続して各種設定を行う  
NFCタグ、パスワード、指紋情報、顔情報はモバイルアプリを利用してスマートロック本体に情報登録する。  
モバイルアプリから施錠解錠を行うようにするためには、モバイルアプリからスマートロックと連携するよう設定が必要  
モバイルアプリの連携情報はクラウドサーバーに保管され、強固な暗号化がされている  
モバイルアプリによる施錠・解錠や通知はクラウドサーバーを経由してルーター⇒スマートロックの順に通信される  
パスワード・指紋情報・顔情報はスマートロック本体に保管されており、漏洩しても利用できないよう強固な暗号化がされている。

施錠解錠・通知の履歴・モバイルアプリの操作履歴はすべてクラウドサーバーにログとして保管される。  
クラウドサービスはあらかじめ許可された人だけが利用可能  
サービスは24h/365日利用可能。  
必要な冗長化（単一故障点までは許容）を行っており、サービスに問題があった場合は監視が行われる。  
通信内容は盗聴されないように必要な暗号化などを行う。

#### 付録4. スマートロック仕様 (No. 2)

(スマートロック仕様 Ver2.0.txt) ※赤字はNo.1からの変更・追記箇所

##### ■ システムの仕様

###### ## システム概要

家庭用に利用できるスマートロックを利用したシステム  
戸建て・集合住宅のドアに工事不要で取り付けができ、施錠・解錠の管理を可能にする  
施錠・解錠は複数の方法で利用可能。  
オートロックにより自動で施錠される。

###### ## ステークホルダと役割

利用者：スマートロックを利用する居住者  
メーカー：スマートロックシステムを開発している会社  
来訪者：利用者の自宅に訪問する者  
攻撃者：利用者の許可なく不正に施錠・解錠を試みる攻撃者

###### ## システムのコンポーネントと役割

1. スマートロック  
スマートロック本体  
戸建て・集合住宅などのドアの錠に取り付け、電気錠として利用できるデバイス
2. スマートフォン (モバイルアプリ)  
一般的なスマートフォン (iPhone・android端末)  
専用のスマートフォンアプリを利用することで遠隔でスマートロックの施錠・解錠、施錠・解錠状態の確認ができる。  
スマートロックの各種設定もアプリでおこなう
3. クラウドサーバー  
一般的なクラウドサーバー  
モバイルアプリを利用した施錠・解錠や施錠・解錠時の通知機能の利用時に使用する
4. ドアセンサー  
スマートロック本体に内蔵されるセンサー。  
スマートロックの施錠・解錠状態を検知する。
5. モーター  
スマートロック本体に内蔵されたモーター  
施錠・解錠操作がされた際にモーターを駆動させ、錠の操作をおこなう
6. 認証モジュール  
スマートロック本体に内蔵される認証モジュール  
モジュールとしてパスワード認証時に利用するテンキー、指紋認証・顔認証で利用する認証器がある
7. ルーター  
一般的な家庭用のルーター  
スマートロックとWi-Fi接続し、クラウドサーバー・モバイルアプリと通信するために使用。
8. NFCカード  
一般的なNFCカード  
スマートロックに登録されたNFCカードをかざすことで施錠・解錠を行うことができる。
9. スマートホームデバイス  
一般的なスマートホームデバイス  
音声コマンドにより、インターネットを経由してスマートロックの施錠・解錠をおこなうことができる

###### ## システム要件

システム要件は機器ごとに以下に記載する

1. スマートロック  
スマートロックの施錠・解錠は以下の方法で実施できる  
・ NFCタグ：事前に登録しておいたNFCカードをかざして施錠・解錠できる  
・ リモートボタン：スマートロックに搭載したリモートボタンを押して施錠・解錠できる  
・ パスワード認証：事前に登録したパスワードをスマートロックのテンキーに入力して施錠・解錠できる  
・ 指紋認証：事前に利用者の指紋を登録し、認証時に指をかざすことで施錠・解錠できる  
・ 顔認証：事前に利用者の顔情報を登録し、認証時に顔を映すことで施錠・解錠できる  
・ 連携したモバイルアプリから遠隔で施錠・解錠ができる  
・ スマートホーム連携を用いた音声コマンドによる施錠/解錠ができる。  
パスワード・指紋情報・顔情報はスマートロック本体に保管されており、漏洩しても利用できないよう強固な暗号化がされている。  
設定したルーターに接続され、クラウドサーバー・モバイルアプリと通信する。  
定期的にクラウドサーバーと通信し、最新FWがあるかどうか確認する。最新FWがあれば自動でクラウドサーバーからFW要求通知を送信し、受信したFWファイルからFWアップデートを行う  
登録されたNFCタグ、パスワード、指紋、顔情報のいずれかによる認証成功後、定められた時間内に施錠/解錠操作を開始する。  
一時鍵 (ワンタイムパスワード/期間指定パスワード) \*\*の入力による施錠/解錠に対応している  
FWのアップデートは差分アップデートに対応している  
FWアップデートに失敗した場合、必ず元のFWバージョンに安全にロールバックできる機能を持つ  
乾電池残量が低下した場合、本体LEDで警告表示を行う。  
ドアセンサーと連携し、錠の状態をクラウドサーバーに送信する。  
モバイルアプリからの遠隔操作による施錠/解錠に対応し、操作後定められた時間内に操作を完了する。
2. スマートフォン (モバイルアプリ)  
遠隔でスマートロックの施錠・解錠、施錠・解錠状態の確認ができる。  
スマートロックの設定 (モバイルアプリとの連携情報登録、認証情報の登録、Wi-Fi設定、FWアップデート、オートロック設定、NFCカード登録)  
遠隔での施錠・解錠、施錠・解錠通知はクラウドサーバーを経由して送信される  
スマートロックの設定はBluetooth接続でおこなう  
モバイルアプリによる施錠・解錠操作、施錠/解錠通知の受信はスマートロックとの連携情報を設定しクラウドサーバーに保存する必要がある  
モバイルアプリからFWアップデート操作を行うことでクラウドサーバーからFWを取得しスマートロックのFWアップデートを行う。  
主要なOS (iOS/Android) の最新2世代に対応している  
施錠/解錠状態をリアルタイムで表示する。  
スマートロックから送信された施錠・解錠情報の通知をプッシュ通知として受信表示する。  
利用者ごとにアクセス権限を設定できる  
複数のスマートロックをアプリ内に登録し、個別に管理・操作できる。  
モバイルアプリからFWアップデートを開始する操作を行い、進捗状況を表示する。
3. クラウドサーバー  
必要な冗長化 (単一故障点までは許容) を行っており、サービスに問題があった場合は監視が行われる。  
施錠/解錠・通知の履歴・モバイルアプリの操作履歴はすべてクラウドサーバーにログとして保管される。  
ログは十分な情報 (タイムスタンプ、リクエストID、エラーコードなど) を含み、保管期間は最低1年間  
クラウドサーバーは、CPU使用率、メモリ使用率、APIエラー率、応答時間、ディスクI/Oなどを24時間365日監視し、閾値を超えた場合に自動でアラートを通知する。  
容易にデプロイ、監視、ログ収集、設定変更が可能なIaC (Infrastructure as Code) を用いて構築する。  
すべてのログデータは、複数のゾーンに分散してバックアップされ、システム障害によるデータ損失を防止する。  
クラウドサーバーおよびAPIサービスの年間稼働率目標を99.9% (計画メンテナンス時間を除く)。  
モバイルアプリとスマートロック間での施錠/解錠指示、状態情報の取得、通知情報の送信を中継する。  
利用者のアカウント情報およびスマートロック連携情報を安全に管理・保存する。  
すべての施錠/解錠イベント、モバイルアプリからの操作、システムエラーを記録し、改ざん防止を施したログとして保管する。  
スマートロックの動作状態 (電池残量、Wi-Fi強度、モーター駆動回数など) をリモートで診断できる機能を提供
4. 認証モジュール  
生体認証 (指紋、顔) の認証プロセスは、読み取り開始から完了までに規定時間を設ける
5. 全体の仕様  
通信内容は盗聴されないように暗号化などを行う。  
サービスは24h/365日利用可能

付録5. スマートロック仕様 (No. 3)

(スマートロック 仕様 Ver2.0.txt) ※赤字はNo.2からの変更・追記箇所

## システムの仕様

## システム概要

家庭用に利用できるスマートロックを利用したシステム  
戸建て・集合住宅のドアに工事不要で取り付けができ、施錠・解錠の管理を可能にする  
施錠・解錠は複数の方法で利用可能。  
オートロックにより自動で施錠される。

## ステークホルダと役割

利用者：スマートロックを利用する居住者  
メーカー：スマートロックシステムを開発している会社  
来訪者：利用者の自宅に訪問する者  
攻撃者：利用者の許可なく不正に施錠・解錠を試みる攻撃者

## システムのコンポーネントと役割

1. スマートロック  
スマートロック本体  
戸建て・集合住宅などのドアの錠に取り付け、電気錠として利用できるデバイス
2. スマートフォン (モバイルアプリ)  
一般的なスマートフォン (iPhone・android端末)  
専用のスマートフォンアプリを利用することで遠隔でスマートロックの施錠・解錠、施錠・解錠状態の確認ができる。  
スマートロックの各種設定もアプリでおこなう
3. クラウドサーバー  
一般的なクラウドサーバー  
モバイルアプリを利用した施錠・解錠や施錠・解錠時の通知機能の利用時に使用する
4. ドアセンサー  
スマートロック本体に内蔵されるセンサー。  
スマートロックの施錠・解錠状態を確認する。
5. モーター  
スマートロック本体に内蔵されたモーター  
施錠・解錠操作がされた際にモーターを駆動させ、錠の操作をおこなう
6. 認証モジュール  
スマートロック本体に内蔵される認証モジュール  
モジュールとしてパスワード認証時に利用するテンキー、指紋認証・顔認証で利用する認証器がある
7. ルーター  
一般的な家庭用のルーター  
スマートロックとWi-Fi接続し、クラウドサーバー・モバイルアプリと通信するために使用。
8. NFCカード  
一般的なNFCカード  
スマートロックに登録されたNFCカードをかざすことで施錠・解錠を行うことができる。
9. スマートホームデバイス  
一般的なスマートホームデバイス  
音声コマンドにより、インターネットを経由してスマートロックの施錠・解錠をおこなうことができる

## システム要件

1. スマートロック  
スマートロックの施錠・解錠は以下の方法で実施できる  
・ NFCタグ：事前に登録しておいたNFCカードをかざして施錠・解錠できる  
・ リモートボタン：スマートロックに搭載したリモートボタンを押して施錠・解錠できる  
・ パスワード認証：事前に登録したパスワードをスマートロックのテンキーに入力して施錠・解錠できる  
・ 指紋認証：事前に利用者の指紋を登録し、認証時に指をかざすことで施錠・解錠できる  
・ 顔認証：事前に利用者の顔情報を登録し、認証時に顔を映すことで施錠・解錠できる  
・ 連携したモバイルアプリから遠隔で施錠・解錠ができる  
・ スマートホーム連携を用いた音声コマンドによる施錠・解錠ができる。  
パスワード・指紋情報・顔情報はスマートロック本体に保管されており、漏洩しても利用できないよう強固な暗号化がされている。  
設定したルータに接続され、クラウドサーバー・モバイルアプリと通信する。  
定期的クラウドサーバーと通信し、最新情報があるかどうか確認する。最新情報があれば自動でクラウドサーバーからFW更新通知を送信し、変更したFWファイルからFWアップデートを行う  
登録されたNFCタグ、パスワード、指紋、顔情報のいずれかによる認証成功後、定められた時間内に施錠/解錠操作を開始する。  
一時鍵 (ワンタイムパスワード/期間指定パスワード)\*\*の入力による施錠/解錠に対応している  
FWのアップデートは差分アップデートに対応している  
FWアップデートに失敗した場合、必ず元のFWバージョンに安全にロールバックできる機能を持つ  
乾電池残量が低下した場合、本体LEDで警告表示を行う  
ドアセンサーと連携し、錠の状態をクラウドサーバーに送信する。  
モバイルアプリからの遠隔操作による施錠/解錠に対応し、操作後定められた時間内に操作を完了する。  
FWアップデートプロセスに、デジタル署名検証と安全なロールバック機能を実装し、不正な変更を防止する。  
パスワード、PINコード、指紋認証、顔認証の認証失敗が5回連続した場合、スマートロック本体は5分間認証を受け付けないロックアウト機能を実装する。  
NFCタグ、パスワード、指紋、顔情報は耐タンパー性の高い領域に保管され、取り出し不可能な状態で暗号化される。  
スマートロック本体に保存されたデータはすべてAES-256で暗号化される  
スマートロックのパスワードやクラウド接続用のシークレットキーは、工場出荷時にセキュアに注入され、設定ファイルなどに平文で保存されないこと。  
スマートロックを初期化 (リセット) する際、すべてのユーザー認証情報、Wi-Fi設定、連携キーが完全に消去され、第三者による不正な再利用ができないようにすること。
2. スマートフォン (モバイルアプリ)  
遠隔でスマートロックの施錠・解錠、施錠・解錠状態の確認ができる。  
スマートロックの設定 (モバイルアプリ) との連携情報登録、認証情報の登録、Wi-Fi設定、FWアップデート、オートロック設定、NFCカード登録  
遠隔での施錠・解錠、施錠・解錠通知はクラウドサーバーを経由して送信される  
スマートロックの設定はBluetooth接続でおこなう  
モバイルアプリによる施錠・解錠操作、施錠/解錠通知の受信はスマートロックとの連携情報を設定しクラウドサーバーに保存する必要がある  
モバイルアプリからFWアップデート操作を行うことでクラウドサーバーからFWを取得しスマートロックのFWアップデートを行う  
主要なOS (iOS/Android) の最新2世代に対応している  
施錠/解錠状態をリアルタイムで表示する。  
スマートロックから送信された施錠・解錠情報の通知をプッシュ通知として受信表示する。  
利用前ごとにアクセス権限を設定できる  
複数のスマートロックをアプリ内で登録し、個別に管理、操作できる。  
モバイルアプリからFWアップデートを開始する操作を行い、連携状況を表示する。  
利用者ごとにアクセス権限を設定できる機能を実装し、権限昇格のリスクを最小化する。  
スマートロックの設定 (Wi-Fi設定、認証情報登録など) は、必ず認証済みのモバイルアプリを経由し、Bluetooth接続でおこなう。  
スマートロックから送信された施錠・解錠情報の通知を、モバイルアプリでプッシュ通知として確実に受信・表示する。  
ユーザー登録時、モバイルアプリのログインパスワードは、最低12文字以上かつ複雑性 (数字、英大文字、英小文字、記号の組み合わせ) を必須とする。  
モバイルアプリのログイン時、または機密性の高い設定変更 (例：認証情報のリセット、Wi-Fi設定変更) を行う際は、SMSや認証アプリによる多要素認証 (MFA) を必須とする。  
モバイルアプリに一時的に保存される機密データは、OS標準のセキュアストレージを利用して保護されること。
3. クラウドサーバー  
必要な冗長化 (単一故障点までは許容) を行っており、サービスに問題があった場合は監視が行われる。  
すべての施錠/解錠イベント、モバイルアプリからの操作、システムエラーをクラウドサーバーにログとして保管する  
ログは許可された利用者やメーカーが監査できるようにする。  
ログは十分な情報 (タイムスタンプ、リクエストID、エラーコードなど) を含み、保管期間は最低1年間  
クラウドサーバーは、CPU使用率、メモリ使用率、APIエラー率、応答時間、ディスクI/Oなどを24時間365日監視し、閾値を超えた場合に自動でアラートを通知する。  
容易にデプロイ、監視、ログ収集、設定変更が可能なIaC (Infrastructure as Code) を用いて構築する。  
すべてのログデータは、複数のゾーンに分散してバックアップされ、システム障害によるデータ損失を防止する。  
すべてのログデータは改ざん防止を施したうえで保管される。  
クラウドサーバーおよびAPIサービスの年間稼働率目標を99.9% (計画メンテナンス時間を除く)。  
モバイルアプリとスマートロック間での施錠/解錠指示、状態情報の取得、通知情報の送信を中継する。  
利用者のアカウント情報およびスマートロック連携情報を安全に管理、保存する。  
すべての施錠/解錠イベント、モバイルアプリからの操作、システムエラーを記録し、改ざん防止を施したログとして保管する。  
スマートロックの動作状態 (電池残量、Wi-Fi強度、モーター駆動回数など) をリモートで診断できる機能を提供  
クラウドサーバーは、利用者のアカウント情報とスマートロック連携情報を安全に管理・保存し、すべての施錠/解錠要求の際に認証を行う。
4. 認証モジュール  
生体認証 (指紋、顔) の認証プロセスは、読み取り開始から完了までに規定時間を設ける
5. 全体の仕様  
Bluetooth通信を含むすべての通信内容を盗聴されないよう暗号化する  
スマートロックとクラウドサーバー間の通信、およびモバイルアプリとクラウドサーバー間の通信はすべてTLS1.3以上で暗号化されるようにする  
モバイルアプリとスマートロック本体間のBluetooth接続は、LE Secure Connectionsなどの強固なペアリング方法を用い、通信内容が傍受されないよう暗号化する  
すべてのリモートAPI通信にセッショントークンまたはJWTを適用し、検証を行う。  
サービスは24h/365日利用可能

付録6. スマートロック仕様(No.1) 生成AIによる分析結果  
(分析結果.1.docx)

1. アクシデント、ハザード、安全制約

提供された「分析済みのAPモデル」と「システムの仕様」をレビューし、アクシデント、ハザード、安全制約を再構築・統合しました。特に、システムの要件（通信内容は暗号化されないことによる盗聴のリスク）やクラウドサービスはあらかじめ許可された人だけが利用可能）2)に基づき、情報漏洩や不正利用に関する項目を明確化しました。

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A-1	スマートロックが利用できない	H-1	スマートロックが使えない <sup>1)</sup>	SC-1	スマートロックは常に使える必要がある <sup>1)</sup>
A-2	スマートロックに接続したデータが外部へ漏洩	H-2	スマートロックのデータが暗号化されない第三者がアクセスする <sup>3)</sup>	SC-2	スマートロックは認証した利用者だけがアクセスできる <sup>3)</sup>
A-3	クラウドサーバー上のデータが外部へ漏洩	H-3	クラウドサーバー上のデータが暗号化されない第三者がアクセスする <sup>3)</sup>	SC-3	クラウドサーバー上のデータは認証した利用者だけがアクセスできる <sup>3)</sup>
A-4	通信データの盗聴	H-4	通信データを第三者が盗聴しデータが漏洩する <sup>3)</sup>	SC-4	通信データは暗号化され第三者には盗聴できない <sup>3)</sup>
A-5	スマートロックが攻撃者によって不正に利用される	H-5	スマートロックは攻撃者によって不正に利用できる	SC-5	スマートロックは攻撃者によって不正に利用できない <sup>3)</sup>

2. 制御コンポーネント、被制御コンポーネント、コントロールアクション

提供された「分析済みのAPモデル」の制御ループの情報を表形式で整理しました。

制御コンポーネント	被制御コンポーネント	コントロールアクション	フィードバック
スマートロック <sup>1)</sup>	ルーター <sup>1)</sup>	施設・解放通知 <sup>1)</sup>	スマートロックからの施設・解放通知応答 <sup>1)</sup>
ルーター <sup>1)</sup>	クラウドサーバー <sup>1)</sup>	施設・解放通知 <sup>1)</sup>	スマートロックからの施設・解放通知応答 <sup>1)</sup>
クラウドサーバー <sup>1)</sup>	モバイルアプリ <sup>1)</sup>	施設・解放通知 <sup>1)</sup>	スマートロックからの施設・解放通知応答 <sup>1)</sup>
スマートロック <sup>2)</sup>	モーター <sup>2)</sup>	施設・解放要求 <sup>2)</sup>	施設・解放応答 <sup>2)</sup>
スマートロック <sup>3)</sup>	ルーター <sup>3)</sup>	再アップデート要求 <sup>3)</sup>	再アップデート応答 <sup>3)</sup>
ルーター <sup>3)</sup>	クラウドサーバー <sup>3)</sup>	再アップデート要求 <sup>3)</sup>	再アップデート応答 <sup>3)</sup>
モバイルアプリ <sup>3)</sup>	スマートロック <sup>3)</sup>	モバイルアプリからの設定情報の登録（連絡先情報・パスワード・指紋情報・顔情報・Wi-Fi設定） <sup>3)</sup>	設定情報登録完了の応答 <sup>3)</sup>
モバイルアプリ <sup>4)</sup>	スマートロック <sup>4)</sup>	施設・解放要求 <sup>4)</sup>	スマートロックからの施設・解放応答 <sup>4)</sup>
モバイルアプリ <sup>5)</sup>	クラウドサーバー <sup>5)</sup>	施設・解放要求 <sup>5)</sup>	スマートロックからの施設・解放応答 <sup>5)</sup>
クラウドサーバー <sup>5)</sup>	ルーター <sup>5)</sup>	施設・解放要求 <sup>5)</sup>	スマートロックからの施設・解放応答 <sup>5)</sup>
ルーター <sup>5)</sup>	スマートロック <sup>5)</sup>	施設・解放要求 <sup>5)</sup>	スマートロックからの施設・解放応答 <sup>5)</sup>
認証モジュール <sup>5)</sup>	スマートロック <sup>5)</sup>	認証情報の送信 <sup>5)</sup>	認証情報受信応答 <sup>5)</sup>

3. UCAの洗い出し

コントロールアクションに対して、非安全なコントロールアクション(UCA)を洗い出しました。違反する安全制約は、上記1)で定義したIDを使用します。

コントロールアクション	発生しないシナリオ	与えられるハザード	原因、誘因、前提	回避する制約
施設・解放通知 (スマートロック⇒ルーター⇒クラウドサーバー⇒モバイルアプリ)	UCA-1: 暗号化されないため、施設・解放通知が与えられない [SC-1]	UCA-1: 暗号化されないため、施設・解放通知が与えられない [SC-1]	UCA-1: 暗号化されないため、施設・解放通知が与えられない [SC-1]	UCA-1: 暗号化されないため、施設・解放通知が与えられない [SC-1]
施設・解放要求 (スマートロック⇒モーター)	UCA-3: 暗号化されないため、施設要求が与えられない [SC-5]	UCA-4: 暗号化されないため、施設要求が与えられない [SC-5]	UCA-5: 暗号化されないため、施設要求が与えられない [SC-5]	UCA-6: 暗号化されないため、施設要求が与えられない [SC-5]
再アップデート要求 (スマートロック⇒ルーター⇒クラウドサーバー)	UCA-7: セキュリティパッチを含む再アップデートが必要時に、再アップデート要求が与えられない [SC-5]	UCA-8: 暗号化されないため、再アップデート要求が与えられない [SC-5]	UCA-9: 暗号化されないため、再アップデート要求が与えられない [SC-5]	UCA-10: 暗号化されないため、再アップデート要求が与えられない [SC-5]
設定情報の登録 (モバイルアプリ⇒スマートロック)	-	UCA-9: 暗号化されないため、設定情報の登録が与えられない [SC-2]	-	-
施設・解放要求 (モバイルアプリ⇒クラウドサーバー⇒ルーター⇒スマートロック)	UCA-10: 正しい利用者からの施設・解放要求が与えられない [SC-1]	UCA-11: 暗号化されないため、施設要求が与えられない [SC-1]	UCA-12: 暗号化されないため、施設要求が与えられない [SC-1]	UCA-13: 暗号化されないため、施設要求が与えられない [SC-1]
認証情報の送信 (認証モジュール⇒スマートロック)	UCA-13: 暗号化されないため、認証情報の送信が与えられない [SC-1]	UCA-14: 暗号化されないため、認証情報の送信が与えられない [SC-1]	UCA-15: 暗号化されないため、認証情報の送信が与えられない [SC-1]	-

4. ハザード (HCF) シナリオ

HCFを減らすためのガイドワード)に基づき、洗い出したUCAに対してハザード (HCF) シナリオを洗い出しました。

UCA	HCFを減らすためのガイドワード)	HCFを減らすためのガイドワード)
UCA-1	暗号化されないため、施設・解放通知が与えられない [SC-1]	1. (5) フィードバックの不十分、欠落、遅延：ドアカンサーの故障や通信途絶により、解放状態がスマートロックで正しく検知できない、または通知データが送信されない。 2. モバイルアプリの利用者が解放状態を確認できず、不正侵入のリスクが高まる (A-5)。
UCA-2	暗号化されないため、施設・解放通知が与えられない [SC-5]	1. (3) プロセスモデルが不正確、不完全：スマートロック内の状態が「解放」と認識される (プロセスモデル不正確)。 2. 誤った通知がモバイルアプリに送信され、利用者が誤ってセキュリティが破られたと判断し、不要な対応やパッチをきっかけにする (A-5)。
UCA-3	暗号化されないため、施設要求が与えられない [SC-5]	1. (2) 十分な制御アルゴリズム：オートロック機能のロジックに不具合があり、一定時間経過しても施設要求が生成されない。 2. ドアが解放されず、第三者による不正侵入が可能となる (A-5)。
UCA-4	暗号化されないため、施設要求が与えられない [SC-5]	1. (1) 上位からの指示や外部情報の誤り、欠落：モバイルアプリからの施設要求が、認証エラーや不正操作により誤って発行される。 2. 利用者がドア付近にいる間に施設され、閉じ込められる、または解放が必要になる (A-1)。
UCA-7	セキュリティパッチを含む再アップデートが必要時に、再アップデート要求が与えられない [SC-5]	1. (8) コントロールアクションが不適切、無効、欠落：メーカー提供したセキュリティパッチ情報が、クラウドサーバー/ルーターの通信エラーによりスマートロックに届かない。 2. スマートロックの脆弱性が残存し、攻撃者による不正利用のリスクが増大する (A-5)。
UCA-11	暗号化されないため、施設要求が与えられない [SC-5]	1. (1) 上位からの指示や外部情報の誤り、欠落：クラウドサーバーが、モバイルアプリからの要求の認証処理に失敗し、不正な要求をスマートロックへ転送する。 2. 攻撃者によってドアが不正に解放される (A-5)。

5. ハザード (SCF) シナリオ

洗い出したUCAに対して、STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) に基づき、セキュリティハザード (SCF) シナリオを洗い出しました。

UCA	STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)	セキュリティハザード (SCF)
UCA-1	Denial of Service (サービス拒否)	1. 攻撃者が通信経路 (ルーターやWi-Fiなど) にDoS攻撃を仕掛け、スマートロック⇒モバイルアプリへの施設・解放通知の送信を妨害する [SC-1]。 2. 利用者はドアの開閉状態をリモートで把握できなくなる (A-1)。
UCA-4	Tampering (改ざん)	1. 攻撃者が通信経路を盗聴し、モバイルアプリ⇒クラウドサーバーへの施設要求を改ざんし、不正な施設要求として転送する [SC-5]。 2. 意図しないタイミングで施設が行われ、利用者が締め出される (A-5)。
UCA-7	Denial of Service (サービス拒否)	1. 攻撃者がメーカーの再アップデートサーバーや通信経路を攻撃し、再アップデート要求を妨害する [SC-5]。 2. 既知の脆弱性が修正されず、攻撃者がその脆弱性を利用して不正アクセスを行う (A-5)。
UCA-9	Spoofing (なりすまし)	1. 攻撃者が正当なモバイルアプリになりすまし、偽の設定情報登録要求をスマートロックに送信する [SC-2]。 2. スマートロックに不正なWi-Fi情報やパスワードが登録され、攻撃者にアクセス経路を提供する (A-2)。
UCA-11	Spoofing (なりすまし)	1. 攻撃者が正当なモバイルアプリ利用者の認証情報 (ID/パスワード) を盗み出し、なりすまして施設・解放要求を送信する [SC-5]。 2. スマートロックが認証済みの利用者からの要求と誤認し、不正に解放してしまう (A-5)。
UCA-14	Information Disclosure (情報漏洩)	1. 攻撃者が、認証モジュール⇒スマートロック間の認証情報 (パスワードなど) の送信を盗聴する [SC-4]。 2. 盗聴した情報が露見され、攻撃者がその情報を用いて不正に認証を突破する (A-5)。

### 1. アクシデント、ハザード、安全制約

提供された分析済みの内容 (STAMP/PA-インポート) を基に、システムの状態 (スマートロック 仕様 Ver.3.0.1) をシミュレーションし、より具体的なかつ詳細なアクシデント、ハザード、および安全制約を整理しました。

アクシデント/ハザード	アクシデント	ハザード	ハザード	安全制約	
A-1	スマートロックが利用できない	H-1	スマートロックが使えない <sup>1)</sup>	SC-1	スマートロックは使える必要がある。
A-2	スマートロックが利用したデータの外部へ漏洩	H-2	スマートロックのデータを隠蔽されない第三者がアクセスする	SC-2	スマートロックは認証した利用者だけがアクセスできる。
A-3	クラウドサーバー上のデータが外部へ漏洩	H-3	クラウドサーバー上のデータが隠蔽されない第三者がアクセスする	SC-3	クラウドサーバー上のデータは認証した利用者だけがアクセスできる。
A-4	通信データの盗聴	H-4	通信データを第三者が盗聴しデータが漏洩する <sup>1)</sup>	SC-4	通信データは暗号化され第三者には盗聴できない。
A-5	スマートロックが攻撃者によって不正に利用される	H-5	スマートロックが攻撃者によって不正に利用される <sup>1)</sup>	SC-5	スマートロックは攻撃者によって不正に利用できない。
A-6	利用者の施設・解放操作を行っても動作しない	H-6	利用者の施設・解放要求がモーターに伝達されない、またはモーターが動作しない	SC-6	利用者の施設・解放要求は、定められた期間内にスマートロックのモーターを駆動させる必要がある。
A-7	意図しない施設・解放が発生する	H-7	施設・解放されていない、または意図しないタイミングで施設・解放が発生する	SC-7	施設・解放は、認証に成功し、かつ前操作からの明確な操作があった場合にのみ実行される必要がある。
A-8	遠隔操作による施設・解放ができない	H-8	モバイルアプリからの遠隔操作による施設・解放が実行されない	SC-8	モバイルアプリからの遠隔操作による施設・解放は、操作が定められた期間内に完了する必要がある。
A-9	モーターの故障によるシステム停止・悪化	H-9	モーターの故障によりシステムが停止するか、不正な形で動作される	SC-9	モーターの故障に発生した場合は、必ず元のバージョンに安全ロールバックできる必要がある。 <sup>1)</sup> また、最終状態は正常の手続きのみ行われる必要がある。

### 2. 制御コンポーネント、被制御コンポーネント、コントロールアクション

提供された分析済みの内容 (STAMP/PA-インポート) を基に、表形式で抽出します。

制御コンポーネント	被制御コンポーネント	コントロールアクション	フィードバック
スマートロック <sup>1)</sup>	スマートロック	施設・解放通知 <sup>1)</sup>	スマートロックからの施設・解放通知応答 <sup>1)</sup>
ルーター <sup>1)</sup>	クラウドサーバー <sup>2)</sup>	施設・解放通知 <sup>2)</sup>	スマートロックからの施設・解放通知応答 <sup>2)</sup>
クラウドサーバー <sup>2)</sup>	モバイルアプリ <sup>3)</sup>	施設・解放通知 <sup>3)</sup>	スマートロックからの施設・解放通知応答 <sup>3)</sup>
スマートロック <sup>1)</sup>	モーター <sup>4)</sup>	施設・解放要求 <sup>1)</sup>	施設・解放応答 <sup>1)</sup>
スマートロック <sup>1)</sup>	ルーター <sup>1)</sup>	種アップデート要求 <sup>1)</sup>	種アップデート応答 <sup>1)</sup>
ルーター <sup>1)</sup>	クラウドサーバー <sup>2)</sup>	種アップデート要求 <sup>2)</sup>	種アップデート応答 <sup>2)</sup>
モバイルアプリ <sup>3)</sup>	スマートロック <sup>1)</sup>	モバイルアプリからの設定情報の登録・送受信情報・パスワード・接続情報・前操作・前1日設定 <sup>4)</sup>	設定情報登録完了の応答 <sup>4)</sup>
モバイルアプリ <sup>3)</sup>	スマートロック <sup>1)</sup>	施設・解放要求 <sup>4)</sup>	スマートロックからの施設・解放応答 <sup>4)</sup>
モバイルアプリ <sup>3)</sup>	クラウドサーバー <sup>2)</sup>	施設・解放要求 <sup>5)</sup>	スマートロックからの施設・解放応答 <sup>5)</sup>
クラウドサーバー <sup>2)</sup>	ルーター <sup>1)</sup>	施設・解放要求 <sup>6)</sup>	スマートロックからの施設・解放応答 <sup>6)</sup>
ルーター <sup>1)</sup>	スマートロック <sup>1)</sup>	施設・解放要求 <sup>7)</sup>	スマートロックからの施設・解放応答 <sup>7)</sup>
認証モジュール <sup>8)</sup>	スマートロック <sup>1)</sup>	認証情報の送信 <sup>8)</sup>	認証情報受信応答 <sup>8)</sup>

### 3. UCAの洗い出し

上記 2) で洗い出したコントロールアクションについて、UCA (Unsafe Control Action) を洗い出し、関連する安全制約 (SC) を特定します。

コントロールアクション	発生するハザード	発生するハザード	発生するハザード	発生するハザード
施設・解放通知 (スマートロック/ルーター/クラウドサーバー/モバイルアプリ)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
施設・解放要求 (モバイルアプリ/スマートロック/クラウドサーバー/ルーター/スマートロック)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
施設・解放要求 (スマートロック/モーター)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
種アップデート要求 (スマートロック/ルーター/クラウドサーバー)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
モバイルアプリからの設定情報の登録 (モバイルアプリ/スマートロック)	SC-1, SC-4	SC-1, SC-4	SC-1, SC-4	SC-1, SC-4
認証情報の送信 (SC-1, SC-3)	SC-1, SC-4	SC-1, SC-4	SC-1, SC-4	SC-1, SC-4

### 4. ハザード (HCF) シナリオ

3) で導出したUCAの中から、主にセキュリティ上の問題につながるUCA-8, UCA-9, UCA-12, UCA-15に着目し、HCF (Highly Critical Factor) を洗い出し、発生し得るシナリオを洗い出します。

シナリオ	発生するハザード	発生するハザード	発生するハザード
UCA-5	施設・解放通知 (SC-1, SC-4, SC-8)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
UCA-8	施設・解放要求 (SC-1, SC-4, SC-8)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
UCA-12	不正な種への要求が送信される (SC-5, SC-9)	SC-5, SC-9	SC-5, SC-9
UCA-15	施設・解放通知 (SC-1, SC-4)	SC-1, SC-4	SC-1, SC-4

### 5. ハザード (SCF) シナリオ

3) で導出したすべてのUCAに対して、STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) に基づき、セキュリティ上の脅威シナリオ (SCF: Security Critical Factor) を洗い出します。

シナリオ	発生するハザード	発生するハザード	発生するハザード
UCA-5	Spoofing (なりすまし)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
UCA-17	Information Disclosure (情報漏洩)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
UCA-12	Tampering (改ざん) / Elevation of Privilege (権限昇格)	SC-5, SC-9	SC-5, SC-9
UCA-4	Denial of Service (サービス拒否)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
UCA-15	Elevation of Privilege (権限昇格)	SC-1, SC-4	SC-1, SC-4
UCA-10	Denial of Service (サービス拒否)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8
UCA-1	Information Disclosure (情報漏洩) / Repudiation (否認)	SC-1, SC-4, SC-8	SC-1, SC-4, SC-8

付録8. スマートロック仕様(No.2) 生成AIによる分析結果  
(分析結果\_3.docx)

**1. アクシデント、ハザード、安全制約**  
システム要件の「攻撃者」の役割、「不正な再試行ができないようにすること」、「不正な変更を防止する」、「ロックアウト機構を構築する」などの記述。および「分析済みのSTAMPモデル」の内容をレビューし、アクシデント、ハザード、安全制約を再整理しました。特に「不正利用」と「データ漏洩」に関する制約を明確化しています。

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A-1	スマートロックが利用済みの第三者によって不正に施錠/解錠されること	H-1	スマートロックが攻撃者によって不正に施錠/解錠できる	SC-1	スマートロックは、施錠された利用者による操作のみを受け付ける。
A-2	スマートロックに蓄積した認証情報（リワード、指紋など）が外部へ漏洩	H-2	スマートロックのデータが認証されない第三者がアクセスする	SC-2	スマートロックに保存される認証情報および機密データは、クラウドサーバ上の高い信頼性で暗号化して保管され、取り出し不可能であること。
A-3	クラウドサーバ上のデータ（アカウント情報、連携情報、ログなど）が外部へ漏洩	H-3	クラウドサーバ上のデータが認証されない第三者がアクセスする	SC-3	クラウドサーバ上のデータは、施錠された利用者や許可されたメーカのみがアクセスできる。
A-4	通信データが盗聴され、情報が漏洩	H-4	通信データを第三者が盗聴したデータが漏洩する	SC-4	スマートロック、モバイルアプリ、クラウドサーバ間のすべての通信は、[LS]、[3d]、または強制暗号化/リソット方法（[1set]）で暗号化され、盗聴内容が検出できないこと。
A-5	スマートロックが利用できない（施錠・解錠操作の失敗、機能停止）	H-5	スマートロックが故障、または攻撃により機能停止し、施錠・解錠ができない	SC-5	スマートロックは、常に利用可能であること。
A-6	不正なファームウェアがスマートロックが改ざんされること	H-6	不正なファームウェアがスマートロックに適用される	SC-6	OTAアップデートプロセスは、デジタル署名検証および安全ロールバック機能を実装し、不正な変更を防止すること。

**2. 制御コンポーネント、被制御コンポーネント、コントロールアクション**  
「分析済みのSTAMPモデル」のテーブルに基づき、制御コンポーネント、被制御コンポーネント、コントロールアクション、フィードバックを整理しました。

制御コンポーネント	被制御コンポーネント	コントロールアクション	フィードバック
スマートロック	モーター	施錠・解錠要求	施錠・解錠応答 <sup>1)</sup>
スマートロック	ルーター	施錠・解錠通知 <sup>1)</sup> / OTAアップデート要求 <sup>2)</sup>	施錠・解錠通知応答 <sup>1)</sup> / OTAアップデート応答 <sup>2)</sup>
ルーター	クラウドサーバ	施錠・解錠通知 <sup>1)</sup> / OTAアップデート要求 <sup>2)</sup> / 施錠・解錠要求 <sup>3)</sup>	施錠・解錠通知応答 <sup>1)</sup> / OTAアップデート応答 <sup>2)</sup> / スマートロックからの施錠・解錠応答 <sup>3)</sup>
クラウドサーバ	モバイルアプリ	施錠・解錠通知 <sup>1)</sup>	スマートロックからの施錠・解錠通知応答 <sup>3)</sup>
クラウドサーバ	ルーター	施錠・解錠要求 <sup>3)</sup>	スマートロックからの施錠・解錠応答 <sup>3)</sup>
モバイルアプリ	スマートロック	設定情報の登録（連携情報、認証情報、PIN設定） <sup>4)</sup>	設定情報登録完了の応答 <sup>3)</sup>
モバイルアプリ	スマートロック	施錠・解錠要求 <sup>3)</sup>	スマートロックからの施錠・解錠応答 <sup>3)</sup>
モバイルアプリ	クラウドサーバ	施錠・解錠要求 <sup>3)</sup>	スマートロックからの施錠・解錠応答 <sup>3)</sup>
認証モジュール	スマートロック	認証情報の送信 <sup>5)</sup>	認証情報受信応答 <sup>5)</sup>

**3. UCAの洗い出し**  
コントロールアクションに対して、非安全コントロールアクション (UCA) を洗い出し、関連する安全制約 (SC) を特定します。特にセキュリティ関連のハザード (A-1: 不正利用, A-6: 不正OTA) に焦点を当てます。

コントロールアクション	考えられるハザード	関連する安全制約 (SC)	関連するハザード
スマートロックからモーターへの施錠・解錠要求	UCA-1: 認証成功後、定められた時間内に施錠・解錠操作を開始しない [SC-5]	SC-5	UCA-2: 認証失敗または未認証の状態でも施錠・解錠要求を出す [SC-1]
スマートロックからルーターへのOTAアップデート要求	UCA-4: デジタル署名検証に失敗した後にOTAアップデート要求を出す [SC-6]	SC-6	UCA-5: OTAアップデート中に、OTAアップデートプロセスを安全にロールバックできない状態で停止する [SC-6, SC-5]
モバイルアプリからスマートロックへの設定情報の登録	UCA-6: 未認証のモバイルアプリやBluetooth接続を許可する設定情報の登録を許可する [SC-1]	SC-1	UCA-8: 連続認証失敗後、5分以内に認証情報の送信を許可する [SC-1]
認証モジュールからスマートロックへの認証情報の送信	UCA-9: 生体認証（指紋、顔）の認証プロセスが規定時間を超えて完了する [SC-1]	SC-1	

**4. ハザード (HCF) シナリオ**  
3.で洗い出したUCAに基づき、「成り立ち」を洗い出し、関連するシナリオを洗い出します。

UCA番号	成り立ち	関連するシナリオ
UCA-1	認証成功後、定められた時間内に施錠・解錠操作を開始しない [SC-5]	1. (1) 動作の遅れ: スマートロック本体のモーターまたは制御部に予期しない遅延が発生 2. 認証成功しても、定められた時間内に施錠・解錠操作を開始されない 3. ハザード H-5: スマートロックが機能停止し、施錠・解錠ができない (A-5)
UCA-2	認証失敗または未認証の状態でも施錠・解錠要求を出す [SC-1]	1. (3) プロセスモデルが不完全、不完全: スマートロックが持つ認証状態のプロセスモデルが、実際（未認証）と異なる状態（認証済）と認識する 2. 未認証の状態でもモーターへ施錠・解錠要求を出してしまう 3. ハザード H-1: スマートロックが攻撃者によって不正に施錠・解錠できる (A-1)
UCA-4	デジタル署名検証に失敗した後にOTAアップデート要求を出す [SC-6]	1. (2) 不十分な制御アルゴリズム: スマートロックの更新制御アルゴリズムにバグがあり、署名検証の漏れ（失敗）を無視してOTAアップデートを続行する 2. 不正なファームウェアがスマートロックに適用される 3. ハザード H-6: 不正なファームウェアがスマートロックに適用される (A-6)
UCA-5	OTAアップデート中に、OTAアップデートプロセスを安全にロールバックできない状態で停止する [SC-6, SC-5]	1. ハザード H-5: スマートロックが機能停止し、施錠・解錠ができない (A-5)
UCA-7	未認証のモバイルアプリやBluetooth接続を許可する設定情報の登録を許可する [SC-1]	1. (8) コントロールアクションが不適切、無効、欠落: スマートロックが、Bluetoothの強固なペアリング機能（Secure Connectionなど）を必要とせずに設定情報登録の権限を受け付ける 2. 攻撃者が承認済みの状態で、窃盗した通信内容を基にOTA設定や認証情報を不正に登録、変更する 3. ハザード H-1: スマートロックが攻撃者によって不正に施錠・解錠できる (A-1)
UCA-8	連続認証失敗後、5分以内に認証情報の送信を許可する [SC-1]	1. (1) 不十分な制御アルゴリズム: スマートロックのロックアウト機構（5回連続失敗後5分間認証拒否）のタイマーが初期化されず、5分経過後に再度認証を受け付けようとする 2. 攻撃者が短い間隔で認証を繰り返し実行（ブルートフォース）する 3. ハザード H-1: スマートロックが攻撃者によって不正に施錠・解錠できる (A-1)

**5. ハザード (SCF) シナリオ**  
3.で洗い出したUCAに基づき、STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) を用いてセキュリティのハザードシナリオ (SCF) を洗い出します。

UCA番号	STRIDEの成分	関連するシナリオ
UCA-2	Spoofing (なりすまし)	1. 攻撃者が、盗聴した通信パケットをリプレイ攻撃するなど、正規の利用者になりすましてスマートロックに認証要求を送る。 2. スマートロックが、そのなりすまし要求を認証成功と誤認する。 3. ハザード H-1: 攻撃者による不正な施錠・解錠 (A-1)
UCA-4	Tampering (改ざん)	1. 攻撃者が、クラウドサーバからスマートロックへのOTAアップデートファイルを受け取り、不正なコードを挿入してデジタル署名を改ざんする（または署名を消去）。 2. スマートロックが署名検証を無視し、改ざんされたファイルを使用する。 3. ハザード H-6: 不正なファームウェアが適用され、機能改ざん (A-6)
UCA-7	Information Disclosure (情報漏洩)	1. 攻撃者が、ルーター経由でスマートロックとクラウドサーバ間の通信、またはBluetooth通信を盗聴する。 2. 通信が[LS]、[3d]または強固なペアリングで暗号化されていない（初期設定など）があり、攻撃者が認証情報やシークレットキーを侵害する。 3. ハザード H-2, H-3, H-4: 認証情報などの機密データが外部へ漏洩 (A-2, A-3, A-4)
UCA-8	Denial of Service (サービス拒否)	1. 攻撃者が、ロックアウト機構を回避するため、認証モジュールへの認証失敗を意図的に連続して発生させ続ける。 2. ロックアウト（5分間の認証拒否）が頻りに発動し、正規の利用者が一時的に認証できなくなる。 3. ハザード H-5: スマートロックが機能停止し、施錠・解錠ができない (A-5)
UCA-7	Elevation of Privilege (権限昇格)	1. 攻撃者が、モバイルアプリとの連携情報（連携キー）を侵害または不正に入手する。 2. 攻撃者がその情報を用いて、モバイルアプリのアクセス権限を持たないにもかかわらず、連携操作や設定変更（認証情報のリセットなど）を行う。 3. ハザード H-1: 攻撃者による不正な施錠・解錠、および設定改ざん (A-1)
UCA-9	Denial of Service (サービス拒否)	1. 生体認証モジュールが何らかの原因で認証処理に非常に長い時間を要する（規定時間超過）。 2. 利用者が規定時間内に認証を完了できず、何回もやり直さなければならず、施錠・解錠が遅延する。 3. ハザード H-5: スマートロックが機能停止し、施錠・解錠ができない (A-5)

付録9. リスク対策後のシステム仕様に対する再分析の実施結果 (1週目)  
(スマートロック\_分析結果\_評価\_20251219\_1158)

分類	No.1			No.2			No1⇒No2に対する変化					
	UCA番号	UCA	HCF・SCF	UCA番号	UCA	分析結果 1で導出されたHCF・SCF	HCFに至るまでのシナリオ	新規の既存	No1⇒No2の変化に対する評価			
									発生頻度	被害の影響度	評価理由	
HCF	UCA-1	解除されたにも関わらず、施錠・解錠通知が与えられない [SC-1]	・フィードバックの不十分・欠落・遅延 ドアセンサーの故障や通信途絶により、解錠状態が正しく検知できない、または通知データが送信されない。	-	-	-	-	既存	減少	減少	類似のHCFが検出されなくなったため	
	UCA-2	解除されていないにも関わらず、施錠・解錠通知が与えられる [SC-5]	・プロセスモデルの不一致・不完全 スマートロック内部の状態が、実際の物理的な状態と異なり、誤って「解錠」と認識される。	-	-	-	-	既存	減少	減少	類似のHCFが検出されなくなったため	
	UCA-3	施錠すべき状態で、施錠要求が与えられない [SC-5]	・不十分な制御アルゴリズム オートロック機能のログに不具合があり、一定時間経過しても施錠要求が生成されない。	-	-	-	-	既存	減少	減少	類似のHCFが検出されなくなったため	
	UCA-4	施錠すべきでない状態で、施錠要求が与えられる [SC-5]	・上位からの指示や外部情報の誤り・欠落 モバイルアプリからの施錠要求が、認証エラーや不正操作により誤って発行される。	UCA-8	認証失敗後、モーターへの施錠・解錠要求が送信される [SC-5, SC-7]	・プロセスモデルの不一致 ⇒認証失敗のフィードバックがあったにも関わらず、本体が「認証成功」と誤認する	-	1. プロセスモデルの不一致：スマートロック内部の認証モジュールから認証失敗のフィードバックがあったにも関わらず、スマートロック本体が「認証成功」と誤認** (プロセスモデルの不一致) 2. 不十分な制御アルゴリズム：認証失敗時のエラーハンドリングにバグがあり、施錠・解錠要求をモーターへ送信してしまう 3. 不正に施錠・解錠が行われる (A-5, H-5)	既存	減少	変化なし	攻撃可能となる原因が「モバイルアプリからの施錠要求」から「認証モジュールからのフィードバック」に変化している。 モバイルアプリの場合はネットワーク上からの攻撃が可能と考えられるが、認証モジュールの場合は物理的なアクセスが必要と考えられる。 そのため、攻撃の困難性が向上したと考え、発生頻度が減少したと判断する。
	UCA-7	セキュリティパッチを含むFWアップデートが必要な時に、FWアップデート要求が与えられない [SC-5]	上位からの指示や外部情報の誤り・欠落 クラウドサーバー側で、モバイルアプリからの要求に対する認証処理に失敗し、不正な要求を転送してしまう	-	-	-	-	-	既存	変化なし	変化なし	類似のHCFが検出されなくなったため
	UCA-11	認証されていない利用者からの施錠・解錠要求が与えられる [SC-5]	・コントロールアクションの不適切・無効・欠落 通信エラー等により、メーカーが提供したセキュリティパッチ情報 (FWアップデート要求) がスマートロックまで届かない。	UCA-5	認証されていない利用者から、施錠・解錠要求が送信される [SC-2, SC-3, SC-5, SC-7]	・モバイルアプリまたはクラウドサーバーの認証情報管理の不備 (例：脆弱なAPIの悪用)	-	1. 上位からの指示や外部情報の誤り：モバイルアプリまたはクラウドサーバーの認証情報管理に不備があり、攻撃者が正規利用者として振る舞う (例：脆弱なAPIを悪用) 2. コントロールアクションの不適切：認証されていない利用者からの施錠・解錠要求がクラウドサーバーまたはスマートロックに到達 3. 不正に施錠・解錠が行われる (A-5, H-5)	既存	変化なし	変化なし	No1から変化が見られなかったため
	-	-	-	UCA12	不正なFWへの要求が送信される	・不十分な制御アルゴリズム ⇒デジタル署名検証などのプロセスが不完全である	-	1. 上位からの指示や外部情報の誤り：クラウドサーバー上のFW格納場所に不正なFWファイルがアップロードされる (サプライチェーン攻撃) 2. (9) プロセスへの入力情報の誤り：スマートロックがクラウドサーバーから不正なFWファイルをダウンロード 3. (2) 不十分な制御アルゴリズム：FWのデジタル署名検証などのプロセスが不完全で、不正なFWが適用される 4. スマートロックが機能停止または攻撃者に乗っ取られる (A-5, H-5)	新規	-	-	No2から検出された新規のHCF。No1と比較対象となるHCFがないため評価対象外
	-	-	-	UCA15	認証されていない利用者から、設定情報の登録要求が送信される [SC-2, SC-5]	・不正確な情報 (ペアリング認証の不足) ⇒Bluetooth通信において、アプリと本体間の認証が不十分である	-	1. (6) 不正確な情報、情報が無い：Bluetooth通信において、モバイルアプリとスマートロック間のペアリング認証が不十分 2. (8) コントロールアクションの不適切：攻撃者のモバイルアプリ (または偽装端末) からの設定情報登録要求 (例：攻撃者のNFCカード情報) がスマートロックに到達 3. 攻撃者の認証情報が登録され、スマートロックが不正に利用可能になる (A-5, H-5)	新規	-	-	No2から検出された新規のHCF。No1と比較対象となるHCFがないため評価対象外
	UCA-1	解除されたにも関わらず、施錠・解錠通知が与えられない [SC-1]	Denial of Service (サービス拒否) 攻撃者による通信経路 (ルーターやWi-Fi) への妨害攻撃により、施錠・解錠通知の送信が阻害される。	UCA-1	UCA-1: 施錠・解錠後、通知が送信されない [SC-1, SC-6, SC-8]	Information Disclosure / Repudiation (情報漏洩/否認) ⇒通信介入により通知送信を妨害され、利用者が現在の状態を把握できなくなる。	-	1. 攻撃者がスマートロックとルーター間の通信に介入し、施錠・解錠通知の送信を妨害 (Repudiation/Tampering) 2. 利用者がモバイルアプリで施錠・解錠状態を確認できず、施錠状態の把握ができなくなる (A-1, H-1)	既存	減少	減少	攻撃範囲が「スマートロックルーター→モバイルアプリ間」から「スマートロックルーター間」のみに縮小している。 そのため、攻撃の困難性が向上したと考え、発生頻度が減少したと判断する。
	UCA-4	施錠すべきでない状態で、施錠要求が与えられる [SC-5]	Tampering (改ざん) 通信の盗聴および改ざんにより、施錠要求が不当な施錠要求として転送される。	-	-	-	-	-	既存	変化なし	変化なし	類似のSCFが検出されなくなったため
	UCA-7	セキュリティパッチを含むFWアップデートが必要な時に、FWアップデート要求が与えられない [SC-5]	Denial of Service (サービス拒否) FWアップデートサーバーや通信経路への攻撃により、セキュリティ修正の適用が妨害される。	-	-	-	-	-	既存	変化なし	変化なし	類似のSCFが検出されなくなったため
SCF	UCA-9	認証されていない利用者から設定情報の登録が与えられる [SC-2]	Spoofing (なりすまし) 正規のモバイルアプリになりすまし、不正な設定情報 (Wi-Fi情報やパスワード) を登録させる。	UCA-15	認証されていない利用者から、設定情報の登録要求が送信される	Elevation of Privilege (権限昇格) ⇒脆弱なBluetooth設定プロセスを悪用され、攻撃者が正規利用者と同等のアクセス権限を獲得する。	1. 攻撃者が脆弱なBluetooth設定プロセスを悪用し、モバイルアプリ連携の設定情報を不正に登録 (Elevation of Privilege) 2. 攻撃者が正規のモバイルアプリ利用者と同等のアクセス権限を獲得する (A-5, H-5)	既存	変化なし	減少	不正に設定できる項目が「モバイルアプリ連携の設定のみ」となり、不正設定できる項目数が少なくなっている。そのため、分析対象への被害影響度が縮小したと考える	
	UCA-11	認証されていない利用者からの施錠・解錠要求が与えられる [SC-5]	Spoofing (なりすまし) 盗み出したID・パスワードを用いて正規利用者になりすまし、不正な施錠・解錠要求を送信する。	UCA-5	認証されていない利用者から、施錠・解錠要求が送信される	Spoofing (なりすまし) ⇒認証情報の脆弱性を利用し、攻撃者が正規利用者になりますことで、不正な要求を受信させる。	1. 攻撃者がモバイルアプリまたはクラウドサーバーの認証情報の脆弱性を利用し、正規利用者になります (Spoofing) 2. なりすましにより、システムが攻撃者からの施錠・解錠要求を正規のものとして受け付ける 3. 不正な施錠・解錠 (A-5, H-5)	既存	減少	変化なし	パスワードを窃取できれば攻撃可能であったが、脆弱性を突く必要があるようになったため、攻撃難易度が高くなっている。よって、攻撃への困難性が上がり、攻撃頻度が低くなったと考える。	
	UCA-14	不正な認証情報 (盗聴されたパスワード等) が与えられる [SC-5]	Information Disclosure (情報漏洩) 認証モジュールと本体間の通信を盗聴し、パスワード等の認証情報を取得・復号する。	UCA-17	暗号化されていない認証情報が送信される	Information Disclosure (情報漏洩) ⇒通信経路 (Wi-Fi, Bluetooth) の盗聴 (Sniffing) により、暗号化されていない認証情報やパケットが入手される。	1. 攻撃者が通信経路 (Wi-Fi, Bluetooth) を盗聴 (Sniffing) 2. 暗号化されていない認証情報や施錠・解錠要求のデータパケットを入手 (Information Disclosure) 64546464 3. 盗聴した情報 (認証情報や通信プロトコル) を利用して、スマートロックを不正に操作 (A-4, H-4, A-5)	既存	変化なし	変化なし	根本的な攻撃手法は同じ。どちらも通信データの盗聴によって認証が突破されることから変化なしと判断	
	-	-	-	UCA-4	認証成功後、施錠・解錠要求が送信されない	Denial of Service (サービス拒否) ⇒メモリやCPUリソースを枯渇させられ、認証成功後も施錠・解錠の制御ロジックが実行不能になる	-	1. 攻撃者がスマートロックまたはモバイルアプリのメモリやCPUリソースを枯渇させる (Denial of Service) 2. 認証は成功するが、施錠・解錠要求を送信する制御ロジックが実行されない 3. 利用者がスマートロックを働かせない状態になる (A-1, H-1)	新規	-	-	No2から検出された新規のSCF。No1と比較対象となるSCFがないため評価対象外
	-	-	-	UCA-12	不正なFWへの要求が送信される	Tampering / Elevation of Privilege (改竄/権限昇格) クラウド上のFWファイルを改ざん・置換し、スマートロックの完全な制御権限を奪取される。	-	1. 攻撃者がクラウドサーバーのFW格納場所に不正アクセスし、正規のFWファイルを改ざんまたは置換 (Tampering) 2. スマートロックが改ざんされたFWを正規のものとしてダウンロード・実行 3. 攻撃者がスマートロックの完全な制御権限を得る (Elevation of Privilege) (A-5, H-9)	新規	-	-	No2から検出された新規のSCF。No1と比較対象となるSCFがないため評価対象外

付録10. リスク対策後のシステム仕様に対する再分析の実施結果 (2週目)  
 (スマートロック\_分析結果\_詳細\_20251219.xlsx)

分類	UCA番号	UCA	No.2		No.3		No.2⇒No.3に対する変化						
			HCF・SCF	HCF・SCFに至るまでのシナリオ	UCA番号	UCA	HCF・SCF	HCFに至るまでのシナリオ	新規or既存	発生頻度	被害の影響度	評価理由	
	UCA-8	認証失敗後、モーターへの施錠・解錠要求が送信される [SC-5, SC-7]	-	・プロセスモデルの不一致 ⇒認証失敗のフィードバックがあったにも関わらず、本体が「認証成功」と誤認する	UCA-2	認証失敗または未認証の状態での施錠/解錠要求を出す [SC-1]	-	・プロセスモデルの不一致 ⇒本体が持つ認証状態(認証済)と実際の状態(未認証)の乖離	1. (3) プロセスモデルが不一致、不完全：スマートロックが持つ認証状態のプロセスモデルが、実際(未認証)と異なる状態(認証済)と認識する 2. 未認証の状態でもモーターへ施錠/解錠要求を出してしまう 3. ハザード H-1：スマートロックが攻撃者によって不正に施錠/解錠できる (A-1)	既存	変化なし	変化なし	No.2から変化が見られなかったため
	UCA-5	認証されていない利用者から、施錠・解錠要求が送信される [SC-2, SC-3, SC-5, SC-7]	-	・モバイルアプリまたはクラウドサーバーの認証情報管理の不備(例: 脆弱なAPIの悪用)	-	-	-	-	-	既存	減少	減少	類似のHCFが検出されなくなったため
	UCA12	不正なFWへの要求が送信される	-	・不十分な制御アルゴリズム ⇒デジタル署名検証などのプロセスが不完全である	UCA-4	デジタル署名検証に失敗したFWに対してFWアップデート要求を出す [SC-6]	-	・不十分な制御アルゴリズム ⇒署名検証の失敗を無視して実行してしまう制御バグ	1. (2) 不十分な制御アルゴリズム：スマートロックのFW更新制御アルゴリズムにバグがあり、署名検証の結果(失敗)を無視してアップデートを実行する 2. 不正なファームウェアがスマートロックに適用される 3. ハザード H-6：不正なファームウェアがスマートロックに適用される (A-6)	既存	減少	変化なし	不正なFWの適用にはデジタル署名検証の実装が必要となっている。そのため、攻撃の困難性が向上したと考え、発生頻度が減少したと判断する。
	UCA15	認証されていない利用者から、設定情報の登録要求が送信される [SC-2, SC-5]	-	・不正確な情報(ペアリング認証の不足) ⇒Bluetooth通信において、アプリと本体間の認証が不十分である	UCA-7	未認証のモバイルアプリやBluetooth接続を理由で設定情報の登録を許可する [SC-1]	-	・不適切なコントロールアクション ⇒強固なペアリング認証を必須としない通信受付	1. (8) コントロールアクションが不適切・無効・欠落：スマートロックが、Bluetoothの強固なペアリング接続 (LE Secure Connectionsなど) を必須とせず設定情報登録の通信を受け付ける 2. 攻撃者が未認証の状態でも、得られた通信内容を基にWi-Fi設定や認証情報を不正に登録/変更する 3. ハザード H-1：スマートロックが攻撃者によって不正に施錠/解錠できる (A-1)	既存	減少	変化なし	「未認証のモバイルアプリやBluetooth接続を理由せず」とあるため、2回目の分析で検出されたシナリオでの攻撃は対象されていると想定。上記より攻撃の困難性が向上したと考え、発生頻度が減少したと判断する。
	-	-	-	-	UCA-1	認証成功後、定められた時間内に施錠/解錠操作を開始しない [SC-5]	-	・動作の遅れ ⇒モーターや制御部での予期しない遅延の発生	1. (7) 動作の遅れ：スマートロック本体のモーターまたは制御部に予期しない遅延が発生 2. 認証成功しても、定められた時間内に施錠/解錠操作が開始されない 3. ハザード H-5：スマートロックが機能停止し、施錠・解錠ができない (A-5)	新規	-	-	No.3から検出された新規のHCF。No.2に比較対象となるHCFがないため評価対象外
	-	-	-	-	UCA-5	FWアップデート中に、アップデートプロセスを安全にロールバックできない状態で停止する [SC-6, SC-5]	-	・意図しない外乱 ⇒電池残量低下等によるアップデート中の突発的なシャットダウン	1. (10) 意図しない、または範囲外の外乱：FWアップデート中に突発的な停電(電池残量低下によるシャットダウンなど)が発生する 2. スマートロックが元のFWバージョンに安全にロールバックできず、動作が停止する 3. ハザード H-5：スマートロックが機能停止し、施錠・解錠ができない (A-5)	新規	-	-	No.3から検出された新規のHCF。No.2に比較対象となるHCFがないため評価対象外
	-	-	-	-	UCA-8	連続5回認証失敗後、5分以内に認証情報の送信を許可する [SC-1]	-	・不十分な制御アルゴリズム ⇒ロックアウト用タイマー制御の論理バグ	1. (2) 不十分な制御アルゴリズム：スマートロックのロックアウト機構(5回連続失敗で5分間認証拒否)のタイマー制御にバグがあり、5分経たずに認証入力を受け付けてしまう 2. 攻撃者が短い間隔で認証を繰り返し試行(ブルートフォース)する 3. ハザード H-1：スマートロックが攻撃者によって不正に施錠/解錠できる (A-1)	新規	-	-	No.3から検出された新規のHCF。No.2に比較対象となるHCFがないため評価対象外
	UCA-1	UCA-1: 施錠・解錠後、通知が送信されない [SC-1, SC-6, SC-8]	-	Information Disclosure / Repudiation (情報漏洩/否認) ⇒通信介入により通知送信を妨害され、利用者が現在の状態を把握できなくなる	-	-	-	-	-	既存	減少	減少	類似のSCFが検出されなくなったため
	UCA-15	認証されていない利用者から、設定情報の登録要求が送信される	-	Elevation of Privilege (権限昇格) ⇒脆弱なBluetooth設定プロセスを悪用され、攻撃者が正規利用者と同等のアクセス権限を獲得する	UCA-7	未認証のモバイルアプリやBluetooth接続を理由で設定情報の登録を許可する [SC-1]	-	・Information Disclosure (情報漏洩) ⇒番号化されていない通信(初期設定時等)の盗聴による、認証情報やキーの暴露	1. 攻撃者が、ルーター経由でスマートロックとクラウドサーバー間の通信、またはBluetooth通信を盗聴する。 2. 通信がTLS1.3または強固なペアリングで暗号化されていない部分(初期設定など)があり、攻撃者が認証情報やシークレットキーを暴露する。 3. ハザード H-2, H-3, H-4：認証情報などの機密データが外部へ漏洩 (A-2, A-3, A-4)	既存	減少	減少	攻撃シナリオが複雑になっており、強固な暗号化がされていない部分のみを対象とした攻撃に変化している。また、STRIDEの分類としても権限昇格⇒情報漏洩に変化している。よって、発生頻度および被害の影響度も減少したと考える。
	UCA-5	認証されていない利用者から、施錠・解錠要求が送信される	-	Spoofing (なりすまし) ⇒認証機構の脆弱性を利用し、攻撃者が正規利用者になりますことで、不正な要求を受審させる。	-	-	-	-	-	既存	減少	減少	類似のSCFが検出されなくなったため
SCF	UCA-17	暗号化されていない認証情報が送信される	-	Information Disclosure (情報漏洩) ⇒通信経路 (Wi-Fi, Bluetooth) の盗聴 (Sniffing) により、暗号化されていない認証情報やパケットを入手される。	UCA-8	連続5回認証失敗後、5分以内に認証情報の送信を許可する [SC-1]	-	・Denial of Service (サービス拒否) ⇒ロックアウトを回避するための意図的な認証失敗の継続、または正規利用者の認証拒否の誘発	1. 攻撃者が、ロックアウト機構を回避するため、認証モジュールへの認証失敗を意図的に連続で発生させ続ける。 2. ロックアウト(5分間の認証拒否)が頻発に発動し、正規の利用者が一時的に認証できなくなる。 3. ハザード H-5：スマートロックが機能停止し、施錠・解錠ができない (A-5)	既存	減少	変化なし	攻撃シナリオの変化として、通信経路の盗聴から認証モジュールへのアクセスが必要となっている。通信経路の盗聴は異なるネットワークからでも可能だが、認証モジュールのアクセスは同じネットワーク内からしかアクセスできないため、攻撃が可能な範囲が限定的となる。よって、攻撃の困難性が向上したと考え、発生頻度が減少したと判断する。
	UCA-4	認証成功後、施錠・解錠要求が送信されない	-	Denial of Service (サービス拒否) ⇒メモリやCPUリソースを枯渇させられ、認証成功後も施錠・解錠の制御ロジックが実行不能になる	-	-	-	-	-	既存	減少	減少	類似のSCFが検出されなくなったため
	UCA-12	不正なFWへの要求が送信される	-	Tampering / Elevation of Privilege (改竄/権限昇格) ⇒クラウド上のFWファイルが改ざん・置換し、スマートロックの完全な制御権限を奪取される。	UCA-4	デジタル署名検証に失敗したFWに対してFWアップデート要求を出す [SC-6]	-	・Tampering (改ざん) ⇒FWファイルへの不正コード埋め込みや、デジタル署名の書き換え・消去	1. 攻撃者が、クラウドサーバーからスマートロックへのFWアップデートファイルを入手し、不正なコードを埋め込んでデジタル署名を改ざんする(または署名を消去)。 2. スマートロックが署名検証を無視し、改ざんされたFWを適用する。 3. ハザード H-6：不正なファームウェアが適用され、機能改ざん (A-6)	既存	減少	変化なし	FWの改ざんにはデジタル署名検証の実装が必要となっている。上記より攻撃の困難性が向上したと考え、発生頻度が減少したと判断する。
	-	-	-	-	UCA-2	認証失敗または未認証の状態での施錠/解錠要求を出す [SC-1]	-	・Spoofing (なりすまし) ⇒通信パケットのリプレイ攻撃等により、正規利用者になりますまで認証要求を送る。	1. 攻撃者が、盗聴した通信パケットをリプレイ攻撃するなど、正規の利用者になりますまでスマートロックに認証要求を送る。 2. スマートロックが、そのなりすまし要求を認証成功と誤認する。 3. ハザード H-1：攻撃者による不正な施錠/解錠 (A-1)	新規	-	-	No.3から検出された新規のSCF。No.2に比較対象となるSCFがないため評価対象外
	-	-	-	-	UCA-9	生体認証(指紋、顔)の認証プロセスが規定時間を超過して完了する [SC-1]	-	・Denial of Service (サービス拒否) ⇒生体認証モジュールの処理遅延(規定時間超過)による、施錠・解錠機能の事実上の停止。	1. 生体認証モジュールが何らかの原因で認証処理に非常に長い時間を要する(規定時間超過)。 2. 利用者が規定時間内に認証できず、何度もやり直す必要が生じ、施錠/解錠が遅延する。 3. ハザード H-5：スマートロックが機能停止し、施錠・解錠ができない (A-5)	新規	-	-	No.3から検出された新規のSCF。No.2に比較対象となるSCFがないため評価対象外