# ソフトウェアデファインド技術を適用したエレベータークラウドサービスELCLOUDのセキュリティ設計・実装

**Design and Implementation of Security Measures on ELCLOUD Elevator Cloud Service Applying Software-Defined Technologies**

藤松　由里恵 FUJIMATSU Yurie　　福壽　康弘 FUKUJU Yasuhiro　　曽根　祐輝 SONE Yuki

情報技術の進化により，従来のスタンドアローンのOT（制御・運用技術）システムに代わって，クラウド連携による機能追加・拡張やアップデートが容易なソフトウェアデファインド技術を適用したOTシステムの普及が進んでいる。一方，クラウドシステムにつなぐことで，新たなセキュリティリスクの増加が問題になっている。

東芝グループは，ソフトウェアデファインド技術を適用してクラウド連携するシステム向けに，セキュリティ対策の設計・実装技術を開発している。今回，東芝エレベータ（株）のエレベータークラウドサービスELCLOUD（エルクラウド）に対してセキュリティ対策の設計・実装を行った。エレベーター運行の安全・安心を確保したセキュリティ対策が，可能になる。

The popularization of operational technology (OT) systems applying software-defined technologies, which facilitate the addition and expansion of functions and software updates in conjunction with cloud computing, continues to grow as an alternative to conventional standalone OT systems in line with ongoing advances in information technologies (IT). However, the increasing of these OT systems is accompanied by new security risks due to the use of cloud systems.

The Toshiba Group is developing technologies to design and implement security measures on OT systems in conjunction with cloud systems by applying software-defined technologies. We have applied them to the ELCLOUD elevator cloud service developed by Toshiba Elevator and Building Systems Corporation, contributing to safe and secure elevator operation.

## 1. まえがき

情報技術の進展に伴い，システム設計におけるソフトウェアデファインドの概念が急速に浸透している。ソフトウェアデファインド技術では，システムのハードウェアとソフトウェアの機能を抽象化・分離し，柔軟なシステム構成及び制御をソフトウェアによって実現する。また，ソフトウェアをコンテナと呼ばれる軽量な実行単位に分割・構成するアプローチが広く普及しており，このコンテナ技術の活用により，機能の選択・追加・変更や他のシステムへの展開が容易となる。加えて，ソフトウェアデファインド化されたシステムをクラウド環境と連携させることで，他のシステムとの統合やソフトウェアの更新が効率的に行えるようになる。

更に，ソフトウェアデファインド技術はサイバーフィジカルシステム（CPS）への移行を促進し，フィジカル空間とサイバー空間の融合を通じて，データ活用や分析結果のリアルタイムなフィードバックを可能にする。これにより，社会インフラシステムにおける即応性や利便性の向上が期待される。このように，ソフトウェアデファインド技術は，システムの柔軟性向上，高機能化，及び効率化を実現する上で不可欠な要素となっている。

一方，ソフトウェアデファインド化が進むと，クラウド連携などのためにネットワークとの接続機会が増える。その結果，攻撃者がシステムの脆弱（ぜいじゃく）性を突きやすくなり，サイバー攻撃を受ける可能性が増大するおそれがある。

そのため，セキュリティリスクアセスメント（以下，アセスメントと略記）を適切に実施することで，増大するセキュリティリスクを洗い出し，新たな対策を行う必要がある。

今回，東芝グループは，東芝エレベータ（株）で開発を進めるエレベータークラウドサービスELCLOUD[(1)]に対して，セキュリティ対策の設計・実装を行った。

ここでは，エレベーター向けに実施したソフトウェアデファインド化の概要と，ELCLOUDのアセスメント，及びそれに基づくセキュリティ対策の設計・実装について述べる。また，ELCLOUDの事例から得た知見が他のシステムのセキュリティ対策に貢献できることを示す。

## 2. エレベーター制御システムのソフトウェアデファインド化

エレベーター制御の基本機能は，エレベーター制御盤の

ソフトウェアで実現してきた。しかし，スタンドアローン型であったため，新しい機能を追加する際に時間を要することが課題となっていた。特に，付加価値機能の追加は，顧客のニーズにスピーディーに応える必要があるため，短時間化が求められる。また，昇降機は利用者の安全・安心を最優先とする社会インフラシステムであり，機能追加などが安全性に影響を与えてはならないという前提条件がある。

そこで，東芝エレベータ(株)は，安全を第一とした上で，柔軟性・効率性を向上させるエレベーター制御システムの開発を進め，これを搭載したELCLOUDを2023年にリリースした。

ELCLOUDの構成を，**図1**に示す。従来のエレベーター制御盤と，ソフトウェアデファインド技術により各機能をコンテナとして実装したDXコントローラーで，エレベーター制御部を構成した。また，“東芝エレベータクラウド”[2]を開発してエレベーター制御部とつないだものを，新たなエレベーター制御システムとした。クラウド連携により，コンテナごとの機能追加・拡張が可能になり，稼働開始後も継続的に顧客に多様な新規サービスをスピーディーに提供できる。

ELCLOUDには，警備・清掃・搬送などを行うロボットと連携する“ロボット連携サービス”，利用者のスマートフォンのアプリケーションからエレベーターを呼び出す“スマホ呼びサービス”，及びビル管理会社向けに遠隔操作でエレベーターの運行状態を共有する“管理支援サービス”がある。

## 3. ELCLOUD向けセキュリティ設計・実装

2章で述べたとおり，従来はスタンドアローン型だったエレベーター制御の機能を，ソフトウェアデファインド化してクラウド連携したことで，サイバー攻撃の標的になるおそれが生じ，新たなセキュリティリスクが増す。ここでは，“ELCLOUDに対するサイバー攻撃があっても，エレベーターの運用に影響を与えない”ことをセキュリティ要件とする。

この要件を満たすセキュリティ設計・実装を行うためには，次の対応が必要となる。

⑴ 業界の法令・規格への準拠

⑵ エレベーター特有の課題(エレベーター制御機能の不正実行・不正操作を発生させない)への対応

⑶ 複雑化した各システム構成へのセキュリティ対応

### 3.1 業界の法令・規格への準拠

エレベーターのセキュリティに関する法令について調査を行い，調査の範囲では存在しないことを確認したが，規格としてISO 8102(国際標準化機構規格 8102)の「ISO 8102-20:2022 エレベータ，エスカレータ及び動く歩道に対する電気的要求事項-第20部：サイバーセキュリティ」[3]がある。また，エレベーターやエスカレーターの業界団体NEII(National Elevator Industry, Inc.)が，エレベーターに対するサイバーセキュリティのベストプラクティスを提供している[4]。

そこで，これらに基づいて，アセスメント及び対策リストの作成を実施した(**図2**)。まず，アセスメントとして，分析の対象決定と守るべき資産の洗い出し，データフローの可視化，脅威の洗い出し，攻撃手法の調査，及びリスク評価を行う。ここでいう脅威は，情報資産に損害を与えるおそれのある要因や事象を指し，外部からの攻撃や，内部の人的ミス，内部不正など，様々な形態で存在する。これらの脅威に対して，それが実現した場合に発生し得る損害を評価し，リスクとして定量化した。

評価結果に基づき，優先的に対応すべきリスクを抽出し，対策を分析した。その結果を，対象ごとのセキュリティ対策リストとして整理した。これらの手順は，一般的なアセスメントの方法論に基づいている。

### 3.2 エレベーター特有の課題への対応

ここでは，例えば，ELCLOUDのスマホ呼びサービスなどをユースケースとして，それぞれに対してエレベーター制御

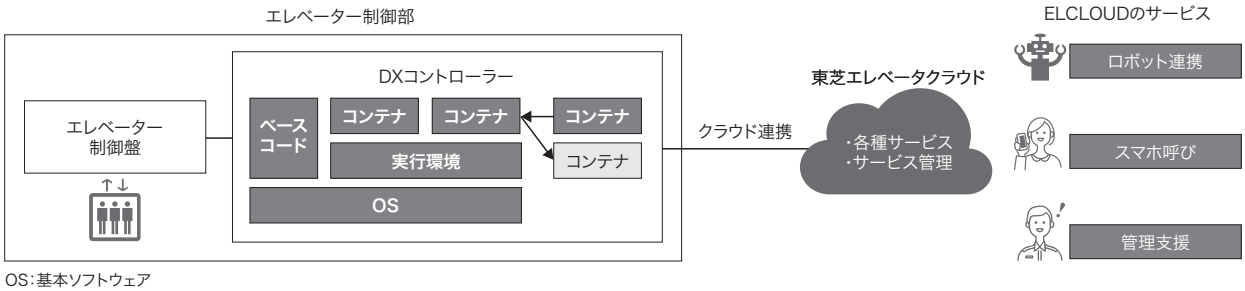


**図1. ソフトウェアデファインド技術を適用したELCLOUDの構成**

従来のエレベーター制御盤にDXコントローラーを追加して，エレベーター制御部を構成し，東芝エレベータクラウドと連携することで，ELCLOUDを実現する。

Configuration of ELCLOUD applying software-defined technologies

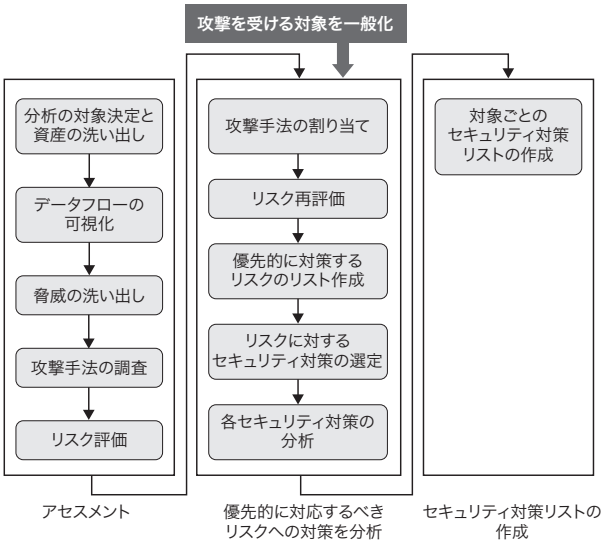


**図2. アセスメント及び対策リスト作成の概要**

分析対象システムであるELCLOUDに対して，ユースケースに沿ってリスク分析を行い，リスクごとの対策の検討までを実施した。

ELCLOUD risk assessment process

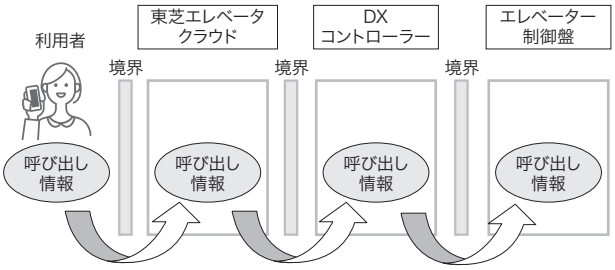


**図3. スマホ呼びサービスの情報の流れと脅威を洗い出すための境界**

サービスごとにどのような情報が流れるかを整理し，管理している組織や境界に着目して，脅威を洗い出す。

Information flow and security threat boundaries when using elevator call service app on user smartphone

システム内で情報がどのように移動するかといったデータフローを可視化して分析した。

スマホ呼びサービスは，利用者が自身のスマートフォンに専用アプリケーションをダウンロードして利用する。専用アプリケーションでエレベーターを呼び出すと，その情報が東芝エレベータクラウドに送信され，更にDXコントローラー経由で，エレベーター制御盤に伝達される(**図3**)。分析にあたって，ELCLOUDに影響を与える場所として，管理している組織やインターフェースが変わるポイント(以下，境界と呼ぶ)に着目し，境界ごとにどのような脅威があるかを網羅的に列挙した。スマホ呼びサービスの場合，スマートフォンと東芝エレベータクラウドの間，東芝エレベータクラウドとDXコントローラーの間，及びDXコントローラーとエレベーター制御盤の間を境界と設定し，脅威を洗い出した。

次に，網羅的に列挙した脅威に対して，安全性への影響，サービスの可用性への影響，及び情報への影響の観点で評価した。この際，ISO 8102に記載されたヒートマップによるリスク抽出手法を採用した。このヒートマップは発生頻度と深刻度によるマトリックスであり，特に，生命に対する被害については深刻なリスクとして判定する。ヒートマップは**表1**のような構成であり，濃いハッチングの部分にマッピングされたリスクに，優先的に対策が必要である。

この結果，ELCLOUDに対する不正実行や不正停止などがセキュリティリスクとして洗い出されたことを確認した。

**表1. リスクの重要度を決定するヒートマップの例**

Example of heatmap to evaluate priority levels of security risks

| Probability level | Level of severity | | | |
|---|---|---|---|---|
| | 1. High | 2. Medium | 3. Low | 4. Negligible |
| A. Highly probable | | | ○○ | |
| B. Probable | | ○○○○○○ | ○○○○○○ | |
| C. Occasional | ○ | ○○○ | ○○○○ | |
| D. Remote | ○○○○○○ | ○○ | ○○○○○○○○○○ | |
| E. Improbable | ○ | | | |
| F. Highly improbable | | | | |

○：一つのリスク
：高リスク　：中リスク　：低リスク
Probability level：発生頻度　Highly probable：非常に発生しやすい
Probable：発生しやすい　Occasional：時々発生する
Remote：まれに発生する　Improbable：発生しそうにない
Highly improbable：非常に発生しそうにない　Level of severity：深刻度
High：高い　Medium：中程度　Low：低い　Negligible：無視できる

### 3.3 複雑化した各システム構成へのセキュリティ対応

複雑化したシステム構成へのセキュリティ対応については，アセスメントを行うセキュリティ専門家，及び組み込みセキュリティ専門家に加え，東芝エレベータクラウドや，DXコントローラー，エレベーター制御盤などの開発メンバーが参加して検討した。関係者で分析結果を共有し，それぞれのシステム構成のハードウェア制約や導入・運用コストを考慮した上で，対策リストを作成した。様々な関係者が協力して検討することで，抜け漏れなく対策をリストアップし，各対策の妥当性を評価した。

## 4. ソフトウェアデファインド技術を適用したシステムのセキュリティ課題と他のシステムへの展開

3章までに，ELCLOUDへのセキュリティ対策の設計・適用について述べた。エレベーターのユースケースに沿って分析を行い，エレベーターの運用に対するセキュリティリスク

を対策の優先度が高いリスクとして，セキュリティ対策の設計・実装までを実施した。この結果，エレベーターのセキュリティ要件に基づいて対策を適用できた。

今回の設計・実装対応で検討したセキュリティ課題のうち，ソフトウェアデファインド技術の適用に関するものを以下に整理する。

⑴ ソフトウェアデファインド化により多機能なソフトウェアが増加するため，ソフトウェアの脆弱性への攻撃を受けるおそれが増す。

⑵ 付加価値機能の追加・拡張を容易にするためにクラウド連携した結果，ネットワークとの接続が増え，サイバー攻撃を受ける可能性があるポイントや経路が増加する。

⑶ 付加価値機能の追加・拡張は，遠隔でのアップデートとパッチ管理により実現する。遠隔でのアップデートは，データを改ざんされたり，不正なデータの更新をされたりすることがあり，新たな攻撃につながる。

これらは，今回のエレベーターシステムに限定したものではなく，ソフトウェアデファインド化やクラウド連携する他のシステムでも，解決の必要がある課題であり，他のシステムへの展開も可能である。特に，稼働中のアップデート・パッチ適用は，ソフトウェアデファインド技術を適用したシステムでは不可欠であり，セキュリティを考慮した設計・実装は必須である。

## 5. あとがき

ソフトウェアデファインド技術を適用したELCLOUDの，セキュリティ対策の設計・実装について述べた。

このセキュリティ対策は，他のシステムへも適用可能であり，今後，東芝グループ内に展開して，製品システムのセキュリティ向上に貢献していく。

## 文　献


⑴ 東芝エレベータ.“東芝エレベータークラウドサービス ELCLOUD エルクラウド”. <https://www.toshiba-elevator.co.jp/elv/eaas/>,（参照 2025-03-15）.

⑵ 木村和生，ほか．エレベーターの新たな価値を創出するElevator as a Service．東芝レビュー．2023，**78**，5，p.6–10，<https://www.global.toshiba/content/dam/toshiba/jp/technology/corporate/review/2023/05/a03.pdf>,（参照 2025-03-15）.

⑶ ISO 8102-20:2022 エレベータ，エスカレータ及び動く歩道に対する電気的要求事項－第20部：サイバーセキュリティ（JSA）.

⑷ NEII. Elevator and Escalator Industry Cybersecurity Best Practices. 2024，29p. <https://nationalelevatorindustry.org/wp-content/uploads/2024/07/NEII-Cybersecurity-Best-Practices-rev2-July-2024.pdf>,（accessed 2025-03-15）.



藤松　由里恵　FUJIMATSU Yurie
総合研究所 AIデジタルR&Dセンター
セキュリティ基盤研究部
Security Research Dept.

福壽　康弘　FUKUJU Yasuhiro
総合研究所 AIデジタルR&Dセンター
エンベデッドシステム技術開発部
Embedded Systems Technology Development Dept.

曽根　祐輝　SONE Yuki
東芝エレベータ(株)
研究開発センター DX開発部
Toshiba Elevator and Building Systems Corp.