

QZSS(準天頂衛星)を利用した早期警戒放送システムの アーキテクチャ

嶋津恵子¹ 五十嵐由衣¹ 青羽真利¹ 大島真言¹
平岡恵里¹ 及川航平² 湯浅廣之² 芝田朋世³

概要: 本書では、システムズエンジニアリング・プロセス標準 (ISO/IEC/IEEE15288) およびそれを基盤とするシステムズアーキテクチャ記述標準 (ISO/IEC/IEEE 42010) に準拠して設計したシステム・アーキテクチャの事例を報告する。対象事例は、QZSS (準天頂衛星システム)の L1 帯域の災害通報用に割り当てられた放送タイミングを利用した災害発生時の早期警戒通知システムである。

キーワード: GNSS,QZSS,MBSE

How to Design of Systems Architecture for QZSS Application

KEIKO SHIMAZU^{†1} YUI IGARASHI^{†1} MARI AOBA^{†1}
MAKOTO OSHIMA^{†1} ERI HIRAOKA^{†1} KOHEI OIKAWA^{†2}
HIROYUKI YUASA^{†2} TOMOYO SHIBATA^{†3}

Abstract: This paper reports a practical study of a systems architecture designed in accordance with the Systems Engineering Process Standard (ISO / IEC / IEEE15288) and the Systems Architecture Description Standard (ISO / IEC / IEEE 42010). The target case is an early warning system in the event for an acute period of a disaster occurrence. This system uses the broadcast timing assigned for disaster reporting in the L1 band of the QZSS (quasi-zenith satellite system).

Keywords: GNSS,QZSS,MBSE

1. はじめに

現在の日本には、情報工学、自然科学、人工知能、航空宇宙工学など、それぞれの専門分野で世界一流の専門家が揃っている。それにも拘わらず、2011年3月11日に発生した未曾有の大震災とそれによって引き起こされた大津波による甚大な被害からの復興に長期間を要し、日本の代表的な銀行は顧客用のネットワークシステムが一年間に何度も停止するような有様である。これらの社会システムの致命的なトラブルは、そのアーキテクチャが最適化されないまま実装になだれ込み、運用が開始したためであると考えられる。これは日本国内で頻繁に取り上げられる“上流工程”で、運用後に発生する期待や要望が反映されていないことが原因という話題に帰結する。

欧米の産業界では、システムのアーキテクチャを最適にデザインするために、システムズエンジニアリング・プロセス標準 (ISO/IEC/IEEE 15288) とそれを基盤としたシステム・アーキテクチャ記述標準 (ISO/IEC/IEEE 42010) が利用されている。

今回我々は、QZSS (Quasi-Zenith Satellite System : 準天頂衛星システム)の、L1 帯域の災害通報用に割り当てられた放送タイミングを利用するアプリケーションシステムを開発した。これにあたり、この両標準に準拠した設計を行った。本書では、実際の設計結果 (モデル図) を報告する。

本書は次の構成を採る。第2章に、我々が利用するシステムズエンジニアリング・プロセス標準 (ISO/IEC/IEEE 15288) を概説する。第3章に今回開発したシステムの導入ドメインを紹介する。第4章に ISO/IEC/IEEE 15288 に準拠してシステム・アーキテクチャを記述する方法を、システム・アーキテクチャ記述標準 (ISO/IEC/IEEE 42010) の要点を示す方法で説明する。第5章でこれら標準に従ってデザインした実際のモデルを紹介し、第6章でまとめを述べる。無尚、本書では、以降この両標準をそれぞれ、15288, 42010 と表記する。

2. 世界標準と最適化されたシステム・アーキテクチャ

15288 は、システムのライフサイクルの全フェーズに渡り、米国国防省や欧米の航空宇宙局からベストプラクティ

1 東京都立産業技術大学院大学
Advanced Institute of Industrial Technology
2 横浜国立大学
YOKOHAMA National University

3 東京都立大学
Tokyo Metropolitan University

スを収集し、それらに産業界に展開した結果を反映させ、一般に利用できるモデルとフレームワークとして整理したシステム構築手法である。1959年に軍事産業標準として用意され、1990年代に一般産業用標準に拡張された。これ以降、これを基盤としたソフトウェア工学標準(ISO/IEC/IEEE 12207)や要求工学標準(ISO/IEC/IEEE 29148)など、システムを成功裏に開発するための標準が網羅的に提供されている。特に、システム・アーキテクチャの基本的なデザイン方法となるISO/IEC/IEEE 42010は、システムの基盤構造特定の際に、欧米豪の産業界で広く活用されている[1]。

15288が提供する工学フレームワークの本質は、対象問題をシステムの構築と導入によって解決するまでにおいて、遺漏なく進めることにある。これを実現するために、①実現したいシステムを単純な部品とインタフェースに分解し、②それらを正しく統合する方法が採用されている。これにより、特に大規模・複雑な対象を、取り扱い易くしている。一方、分解の際、特定の視点に従って分解すると、完成したシステムは別の視点では最適化されていないことがある。代表的な例は、物理的な視点で最適に分解し、それを統合した完成形が、必ずしも利用者の操作性を満足するものではないというものである。そこで、15288では、ViewとViewpointで区別される異なる観点で、それぞれ独立して分解作業を行う。それぞれの分解結果が異なる観点を横断して整合する状態を、最適なシステム・アーキテクチャとしている。この複数の観点群を横断した整合性担保の効率性を上げるために、MBSE(Model Based Systems Engineering)が注目されている。

本書で報告するモデル群は、MBSEをQZSSのアプリケーション開発に採用した結果である。

3. アプリケーション外観

3.1 災害急性期避難指示網としてのGNSS

我々は、2011年に発生した東日本大震災の経験から、大規模災害が発生すると被害が甚大な地域ほど日常利用している情報インフラが壊滅することを学習した[2]。そしてこの状況下で被災者にとって必要な情報は、動画像によるリッチなコンテンツではなく、命をつなぐための重要なキーワードであることを知った[3]。これを受け、災害時でも利用可能な通信設備の構築技術の研究とともに、緊急避難に必要な情報を配信する暫定通信網を、衛星通信網を介して実現することが必要であると考えた。特にGNSS(Global Navigation Satellite System)に代表される測位システムは、地上で常時その信号を受信できる。その一方で、送信容量は非常に限定的である。そこで我々は、この限定的なメッセージ領域を最大限有効に活用し、緊急時に避難情報を放

送するためのメッセージをEC(European Committee)のGalileo衛星担当官と共同で開発した[4]。

3.2 日欧共通設計による緊急避難情報構造

我々は、ECのGalileoのチームと協力し、発災時に自分で避難行動をとるのに必要な情報を、標準の災害用語や災害およびそれを取り扱う際に必要になる標準のコード体系から抽出した。より具体的には、災害群として、Common Alerting Protocol(CAP)[5]を参照し、国や地域の指定にISOを参照した。CAPは、世界中で開発されている危機警告発信システム間で、公開された警告や緊急情報を相互交換することを旨とした災害情報体系であり、XMLフォーマットで定義されている。CAPを使用することで、Google Public AlertsやCell Broadcastなど多くの一般のアプリケーションに、個別の危機警告発信システムを介して同時に情報配信が可能となる。また、情報の前処理を簡素化することも可能になる。

測位情報を放送することを目的として設計されたGNSSのメッセージ領域は、必要とする情報量が小さいため放送可能容量が非常に限定的である。Galileoでは測位情報メッセージのうち122ビット長が避難のための緊急災害情報に割当て可能であり、一方日本のQZSSのそれは、191ビット長である。そこで、我々は、122ビット長に、避難に必要な最低限の情報を搭載できるよう設計した。

表1に、メッセージ全体の構造を示す。特にここで、Field12から同16に注目されたい。一般に災害、特に自然災害は緯度経度による点ではなく、面的に被害を及ぼす。そこで、これを表現するために、我々の設計では楕円による被災範囲の表現方法を採用した。つまり、被災地を楕円で表現した時の中心点の緯度(A11 - Ellipse Center Latitude)、その経度(A12 - Ellipse Center Longitude)、そして楕円の長半径と短半径(A13 - Ellipse semi-major axis length, A14 - Ellipse semi-minor axis length)、さらに楕円の方角(A15 - Ellipse Azimuth Angle)の5つの値で囲まれた領域を、避難指示を発令する対象の区域として利用する。

表 1 Common EWS Message for the Signal-in-Space

Common EWS Message for the Signal-in-Space				
Field	Message field	Element name	Start bit	#bits
1	Message Identifier	A1 - Message type	0	2
2		A2 - Country ID	2	10
3		A3 - Provider ID	12	4
4		A4 - Message Reference Number	16	4
5	Event	A5 - Event Category	20	3
6		A5 - Event Sub-Category	23	4
7		A6 - Severity	27	2
8	Event chronology	A7 - Event Onset	29	16
9		A8 - Expected Duration	45	2
10	Guidance to react	A9 - Guidance Library	47	1
11		A10 - Guidance to React Database	48	8
12	Target Area	A11 - Ellipse Center Latitude	56	16
13		A12 - Ellipse Center Longitude	72	17
14		A13 - Ellipse semi-major axis length	89	4
15		A14 - Ellipse semi-minor axis length	93	4
16		A15 - Ellipse Azimuth Angle	97	5
17	Additional	A16 - Specific Setting	102	20

3.3 フィジー共和国向け QZSS アプリケーションの狙い

我々が試作する緊急避難情報を QZSS から放送するアプリケーションシステムは、フィジー共和国向け災害急性期警報システム (Fijian Early Warning System: F-EWS) として試作した。

同国は、南太平洋に点在する 300 余の火山島と珊瑚礁から成り、総面積 1 万 8270 平方キロメートルに約 85 万人が居住している。主な産業は、農業と観光である。全島が熱帯雨林気候であるが、南東貿易風の影響下にはいる 5 月から 11 月は降雨も少なく、タロイモとココナツの自生により食生活に困窮している様子は無い。

一方、11 月から 4 月の間、つまり 1 年の半分がサイクロン到来期間となる。フィジー共和国の島々は、気候変動の影響を受け、“カテゴリー5”指定される巨大サイクロンに毎年襲われる [6]。大雨や暴風そして洪水で学校等の公共施設を含む多くの家屋が損壊し、さらに腰ほどの高さの浸水で、道路をはじめとする多くのインフラストラクチャの機能が停止する。カテゴリー5 のサイクロンが上陸すると、フィジーの全人口の 62% に相当する 54 万人が被災し、避難所になるはずの学校の 55% が倒壊する。

災害発生時は、住民は身を守るための情報を求め、インターネットやテレビ、そしてラジオから配信される警報と避難指示に頼る。これにより、一旦避難した場所がサイクロンの影響を極端に受ける危険がある場合は、別の避難所に移動することが可能になる。ところが、サイクロンの影響を最大に受ける場所ほどインフラストラクチャーの停止が多く発生する。インターネットやテレビだけでなく、ラジオの電波塔までもが倒壊し、被災した住民が避難指示や警報を受けられない事例が発生している。

そこで、最後の避難指示受信手段となることが、我々の開発する F-EWS の狙いである。

4. 世界標準準拠型システム・アーキテクチャ設計

42010 は、15288 に準拠したシステム開発を行うことを前提とし、アーキテクチャをどう記述するか整理している。その外観が同標準書内の Figure 2 — Conceptual model of an architecture description である (図 1)。ここで、この図は、ISO/IEC 19501 に準拠した統一モデリング言語 (Unified Modeling Language: UML) で表現されている。この図に示している重要なオブジェクトに関し、同標準書の別箇所に、詳細を同じく UML を用いて説明している。一方、本書には書面に限りがあるため、図 1 のうち、“Architecture Nationals”と“Correspondence Rule”さらに“Correspondence”を除く残りのオブジェクトを使って、アーキテクチャの記述に必要な情報を概説する。

システムの“Architecture”は、“Architecture Description”で表現される。システム開発においてアーキテクチャが設計される前は、情報が構造的に整理されていない、つまりシステムとして成り立っていない状態 “System-of-Interest” である。“Architecture Description”が完成することで、どういう構造体であるかが特定される。アーキテクチャをどう設計するかは“Stakeholder”の“Concern”をどのように解決するかに依存する。“Stakeholder”は、システム化対象領域である“System-of-Interest”が、システムとして構造化される、もしくはその過程で影響を受ける対象である。つまり“Stakeholder”は、システム開発に対し何らかの“Concern”も持ち、それぞれの“Concern”は、“Architecture Viewpoint”を構成するいずれかの表現方法 “Model Kind” でどのように解決されるかが示される。“Architecture Description”は、同一の設計結果を異なる観点 “Architecture Viewpoint” で表現した結果である。“Architecture Viewpoint”の一般的 (すべてのシステム開発で用いられる) なものが、「運用と機能と実装の整合」であり、“Architecture View”として operational

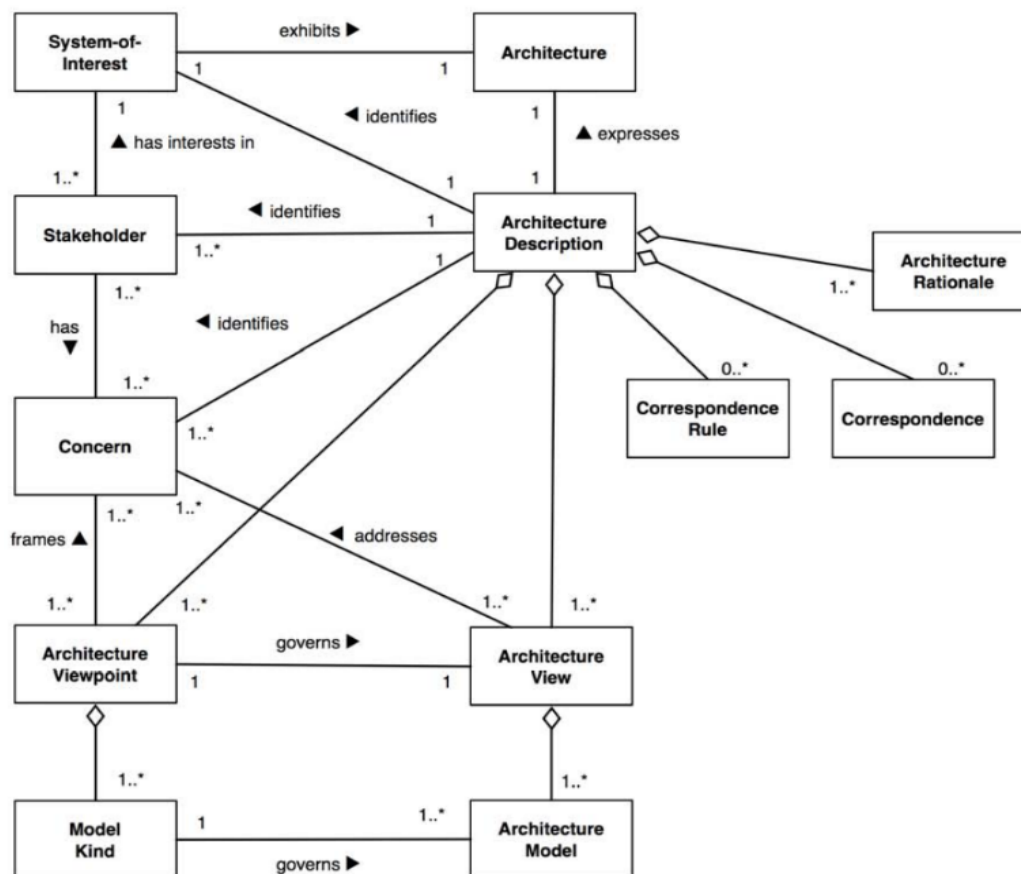


図 1 Conceptual model of an architecture description (転載)

view と functional view そして physical view が用いられることが多い。そして、これらのモデル群が互いに整合している場合、“Architecture Model”となる。

5. フィジー共和国向け QZSS アプリケーション開発での実践例

5.1 Concern

我々は、“concern”を特定するために“System-of-Interest”に関し、サイクロン発災時の現状の警報発令手順を調べた。図2に示したとおり、警報発令には主に二つの組織が関わっている。FMS (Fiji Meteorological Service)と NDMO (National Disaster Management Office)である。

FMSは気象データを観測し、サイクロンが発生しその上陸が予想されると警報発令を決定する。警報は、FMSが運営するWebサイト上とSNSを介して国民に知らせる。同時にFAXやemailを利用して、NDMOにも通知する。NDMOは、地区ごとの避難指示を決定し、記者会見とSNSで国民に周知する。

図3は、FMSとNDMOがこれらの作業フローで取り扱っているデータのモデルである。FMSが発する警報は、災害種(今回はサイクロン)、警報、対象地区、発令

時刻から成る情報と、サイクロンの中心点の経度と緯度である。NDMOは、避難行動指示を、それを発令する対象地区ごとに発令する。ここで、避難行動指示が取りうる値域は、{Take precautions, Move to the Evacuation Center, Move to higher ground, Stay indoors}である。この現行システムにQZSSの災危通報の情報経路を加え、停電時でも各地区の避難情報をリアルタイムに通知させようとした際に、それが期待通りに機能しなくなる状況を整理した。つまり、System-of-InterestのConcernの特定をContext分析でおこなった(図4)。図4には、機能しなくなる状況をグルーピングし、それを構成する属性とその値で示した。赤字で取り消し線文字であるものは、該当する属性の値がそれである場合、期待通りに機能しなくなるが、今回concernとして取り扱わない。つまり、この状況が発生した時は、システムは機能しないことを示す。一方、青字で示したものは、(いずれの対策もとらなければ)同様にシステムが期待通りに機能しなくなるが、開発するシステムの設計過程で、機能設計上もしくは性能設計上の工夫によって、これを回避することを示している。

換言すると図4に示した青字の箇所が、今回の開発するシステムのconcernである。

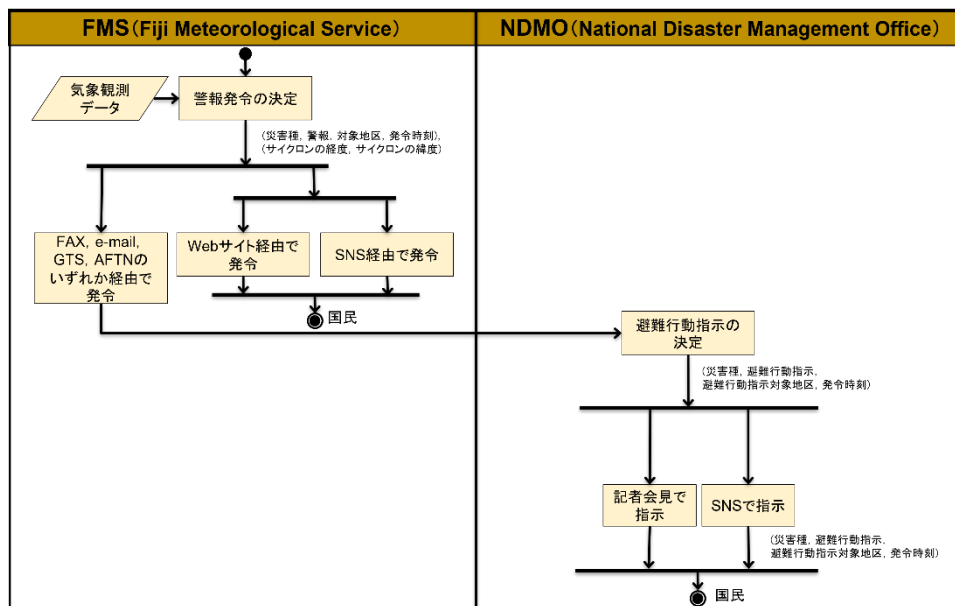


図 4 サイクロン上陸時の避難指示発令手順

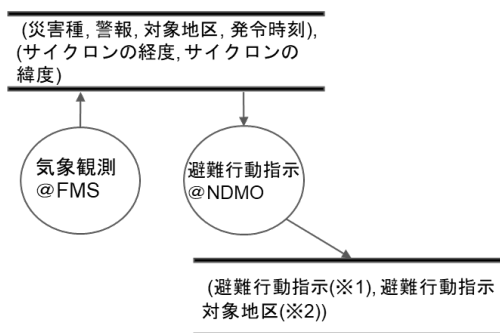


図 3 避難指示発令手順で用いるデータの構造

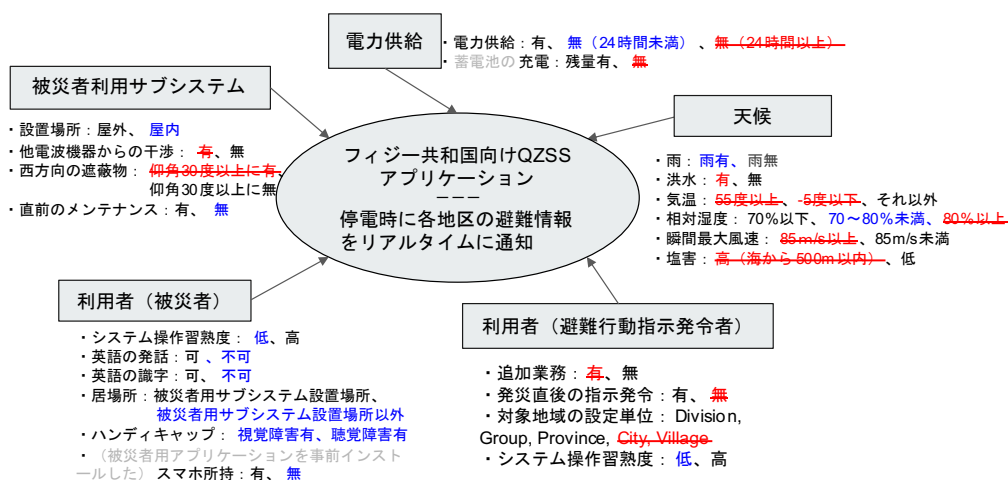


図 2 対象システムのコンテキスト分析結果

5.2 Architecture Viewpoint

コンテキスト分析の結果から、「運用と機能と実装の整合」の viewpoint だけでなく、(a)電力供給が途絶えたときでも機能すること、(b)衛星受信機から離れている場所にいる被災者にも通知されること、さらに(c)デジタルデバイス等利用に制約ある利用者にも認識できること、そして(d)現在の NDMO の作業より複雑性と煩雑性を高めないことの 4 つの viewpoint によるモデルが必要であると特定した。図 5 は、(a)と(b)をどのように可能にするかを示したモデルである。(c)は、操作画面設計と受信機が組み込まれる装置の物理構成図で示すが、本書ではこれらの掲載を割愛する。図 5 は、被災者が避難情報を受け取る環境は、QZSS の信号受信機が組み込まれた装置が設置された屋内、もしくは、拡声器の使用とスマートフォン上のアプリケーションへの転送による屋外であることを示す。また、屋内外の設備には無停電措置 (UPS) から電力が供給されることを示している。さらに、避難指示を出す NDMO の作業環境は、非常電源で動作させる。そして図 6 と図 7 に、(d)をどのように解決するかを、システム開発後の避難指示発令手順と、その際に取り扱うデータモデルで示した。

図 6 は、図 2 に「F-EWS」列が追加されている。衛星を経由した避難行動指示信号を送信する操作を行うと、受信機への配信と、それと同時に従来の作業でおこなっていた SNS 投稿も行う。また EWS メッセージが送信されていない日常は、昼 12 時に時報を流すことで、正常動作監視を行う。つまり、サイクロン上陸時には、これまでと同じ手数の操作で従来のメディアと衛星信号受信機の両方に避難指示を送ることができる。そして平時には日常メンテナンス作業を最小に抑える工夫がされていることがわかる。

さらに図 7 では、「F-EWS」の導入により赤字でしめされたデータが、従来のそれに追加し取り扱える部分である。具体的には、衛星からのメッセージを受け取った際、地区ごとの避難指示と同時に (GNSS を利用していることで) 受信装置が設置されている場所が把握できる。これにより避難指示を受信した際、それが現在地に相当しているかどうかを自動的に判別し出力する。

これらのモデルは、現行動作中システムの作業手順を複雑化・煩雑化することなく、より効率的・効果的な情報配信を可能にしていることを示していると言える。

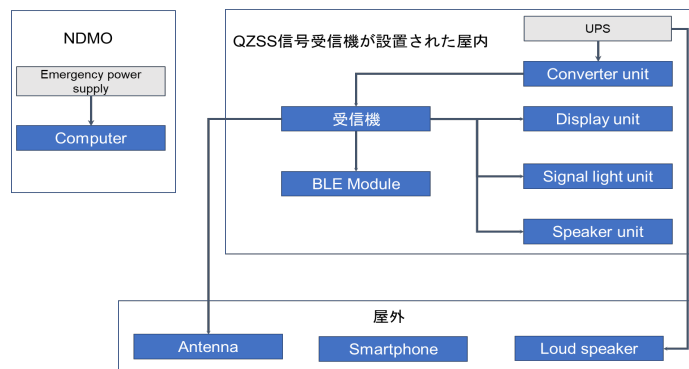


図 6 電力供給 viewpoint によるモデル

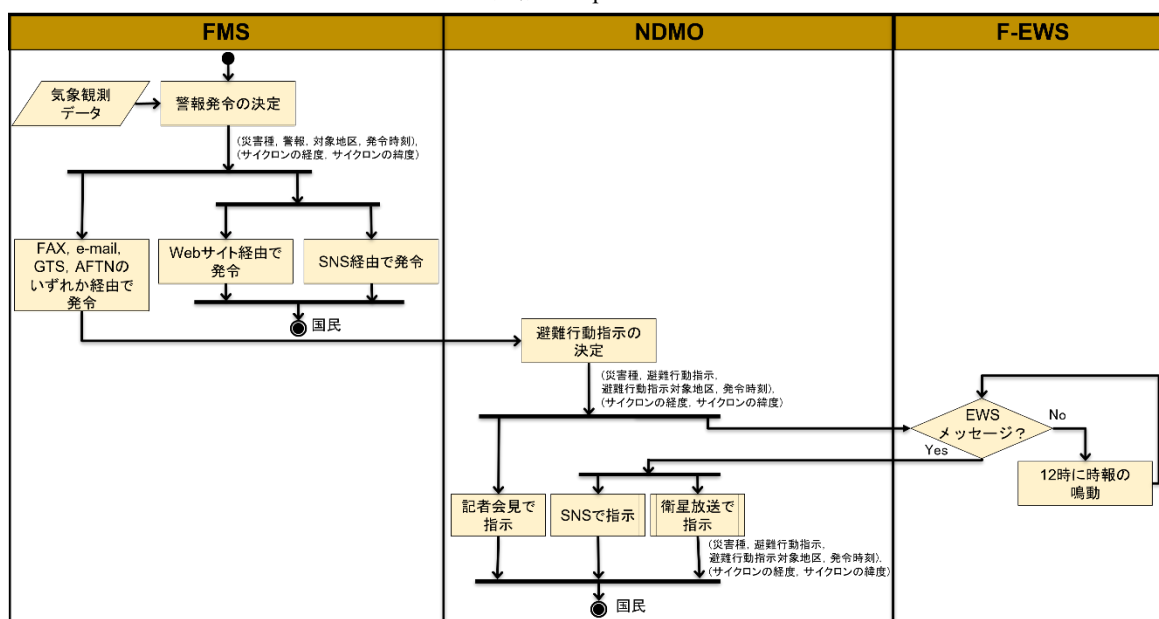


図 5 F-EWS の避難指示発令手順

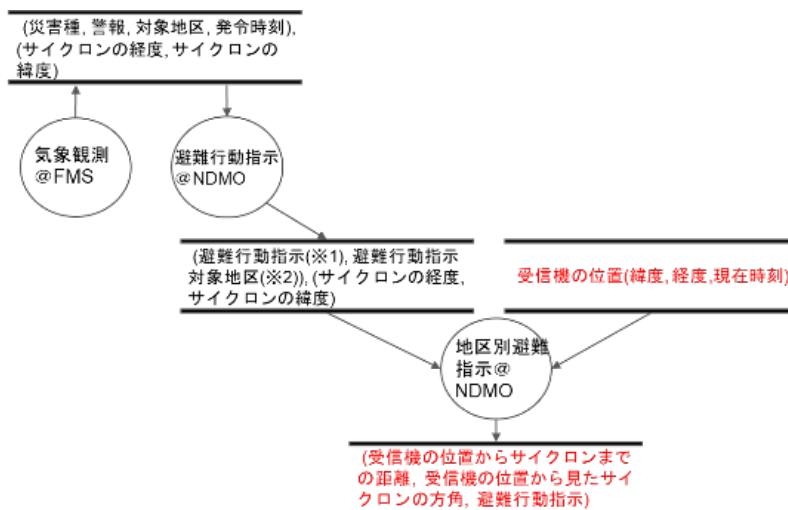


図 7 F-EWS で用いるデータ構造

5.3 Function Model のデザイン開始

開発したシステムが導入された後、現場で期待通りの成果を上げるかどうかは、「運用と機能と実装の整合」の viewpoint でデザインした運用モデル、つまりユーザーモデルの目指す姿を、完璧かつ正確に実現する機能モデルを設計できるかどうかにかかっている。機能仕様の作成、特に機能コンポーネントの整備に際し、直感的に必要な機能要素を集めがちだが、我々が採用した世界標準は、論理的に機能を整備する方法を示している。本書では、そのスタートポイントの実践例を紹介するにとどめるが、論理的に機能コンポーネントを整備する出発点の説明には十分である。

5.3.1 ユーザーモデル

F-EWS を導入した際のユースケースをユーザーモデルで用意した。具体的には、ユースケース図による静的モデル(図 8)とそれぞれのユースケースでユーザーがどのようなワークスルーを体験するかをフローチャートで表現した動的モデル(図 9 および図 10)である。図 9 および図 10 は、それぞれ図 8 で示した主たる 2 つのユースケース「EWS メッセージを送信する」と「EWS メッセージを放送する」のそれぞれのワークスルーである。前者は、NDMO が避難指示の放送のために QZSS の地上局へデータを送る作業であり、後者は、QZSS 経由で被災者に警報を流すそれである。

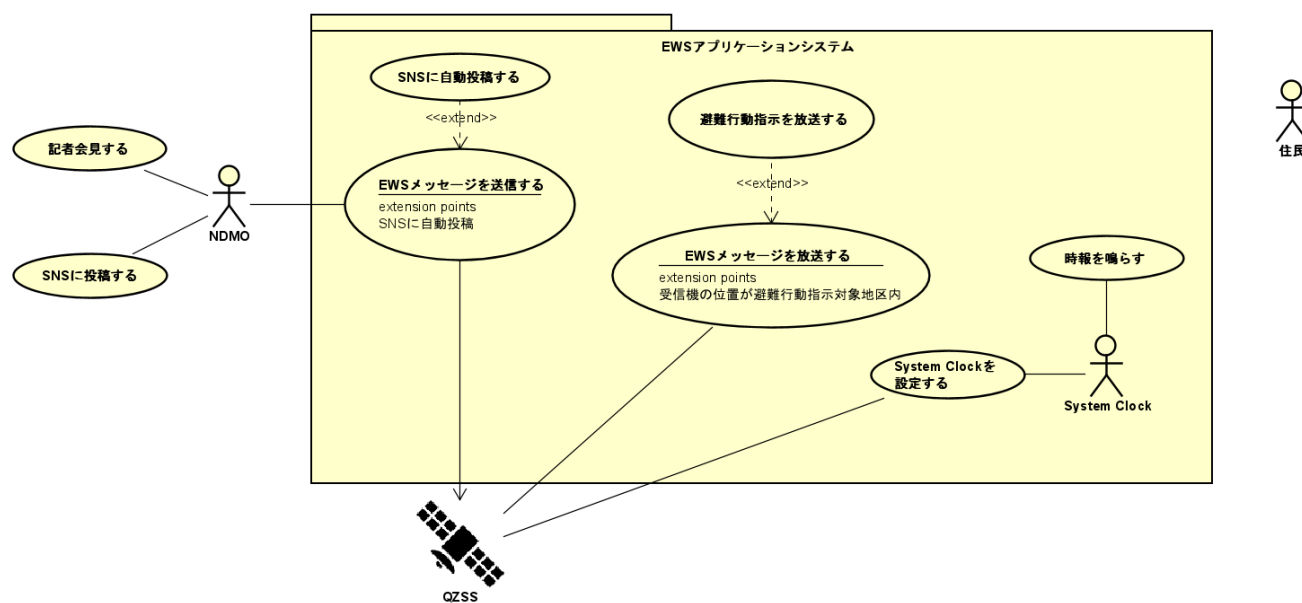


図 8 F-EWS 導入時のユースケース

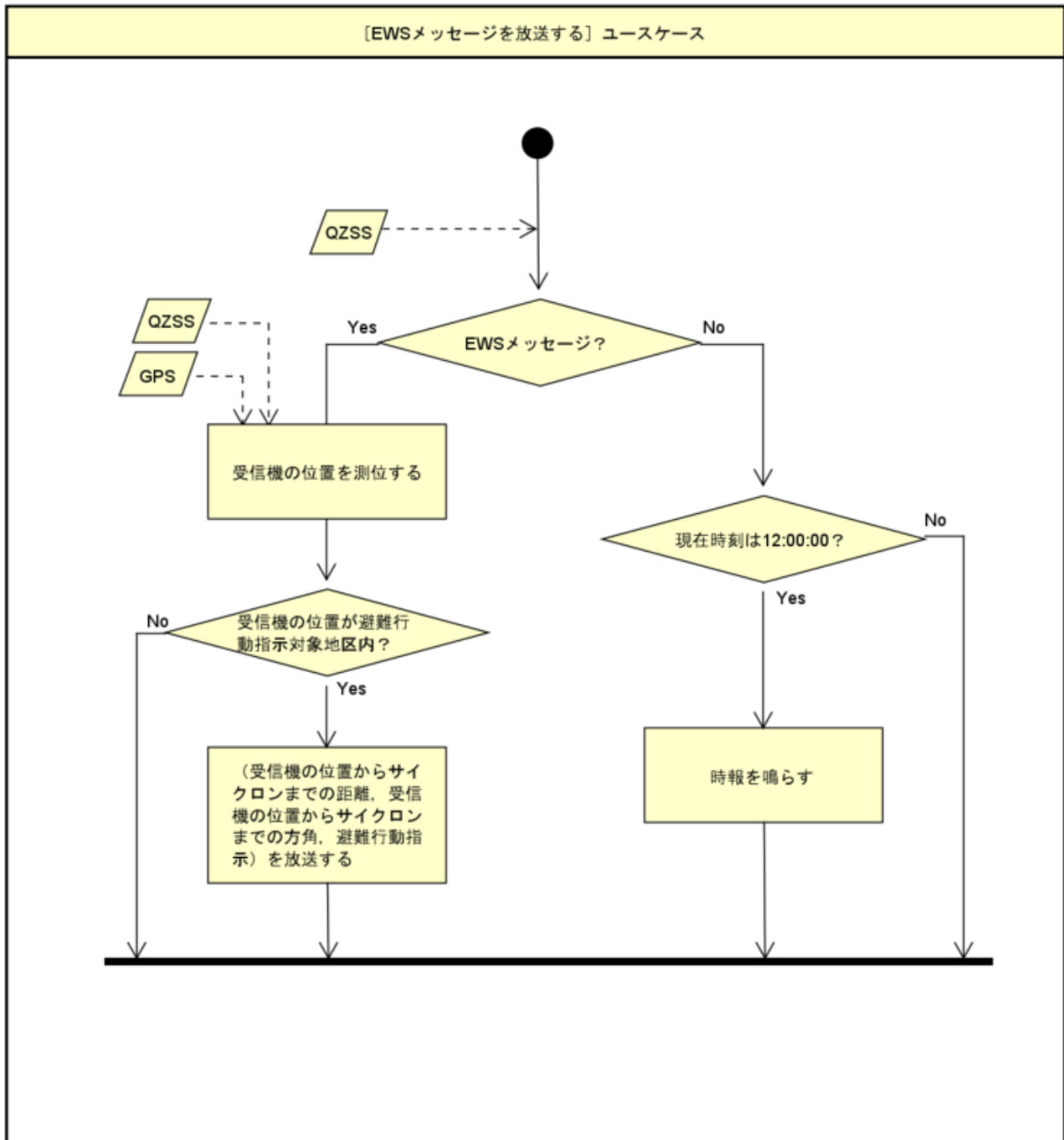


図 9 「EWS メッセージを送信する」のワークスルー

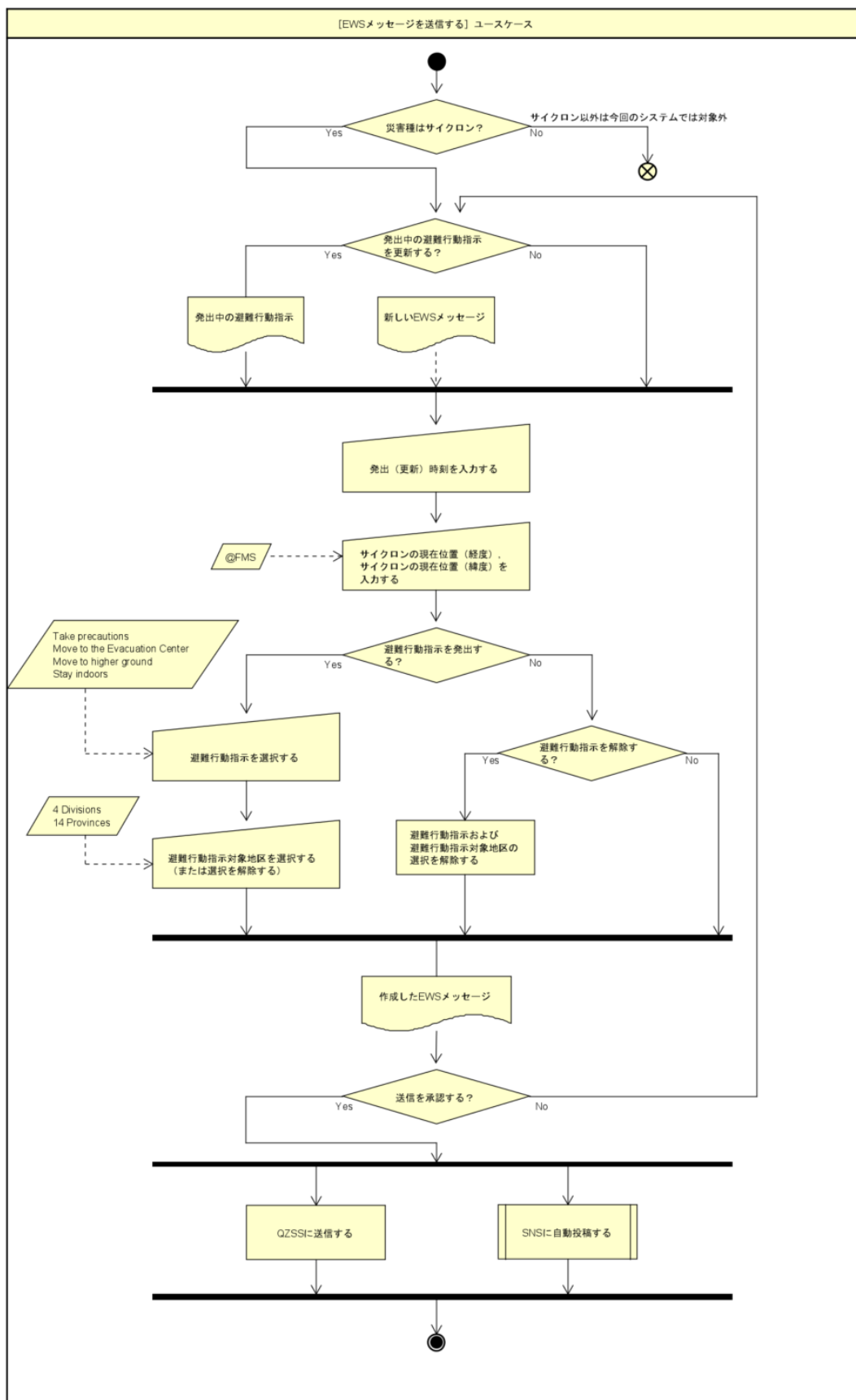


図 10 「EWS メッセージを放送する」のウォークスルー

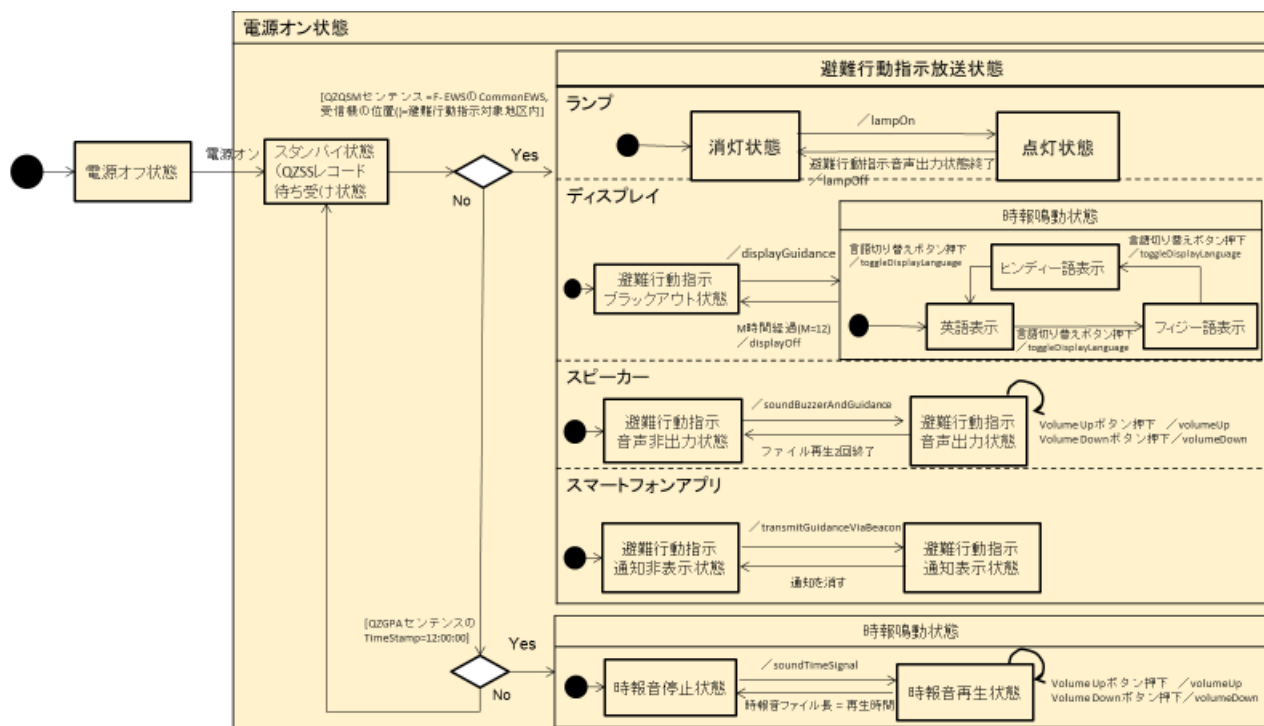


図 11 F-EWS の再上位機能群

5.3.2 最上位機能コンポーネント

15288 に従うと、機能 (Function) とは、プロセスの特殊系であり、具体的には入出力を持つだけでなく何らかの対象を変化させる。最上位に位置する機能コンポーネント群は、システムの利用者からその挙動が確認できるものであり、これがシステムに対する Validation の対象となる。つまり、変化する対象はシステムの利用者が認識できるものであり、変化の前と後のそれぞれの状態が評価の対象となる。これに従い、前節にフローチャートで示した動的ユーザーモデルを参照し、「どのタイミング」で「何が」「何に変化」すると、構想したウォークスルーが実現するかを特定した。その結果を図 11 に示す。

図 11 は一般に広く用いられている State Machine 図を使って表現しているが、長方形で示すすべてが Function の起動により変化する対象であり、今回は開発するシステムの状態、もしくはシステムを構成する部分の状態である。従って、矢印の箇所に対象を変化させる Function が必要であることがわかる。この後、最上位機能を分解し、必要なすべての Function を特定する作業に移行するがその際も同様に、どのタイミングで「何が」「何に変化」するかを焦点に作業を行う。

6. おわりに

本書では、システム・アーキテクチャ記述標準(ISO/IEC/IEEE 42010)と、システムズエンジニアリング・プロセス標準 (ISO/IEC/IEEE 15288) に準拠し、システム・アーキテ

クチャをモデルでデザインした実際の事例を紹介した。紙面の都合上、最上位の機能モデルの提示までになったが、今後開催される別の研究会で、機能モデルの詳細化とそれに対応する物理モデル (実装モデル) を発表する予定である。

謝辞 本研究の一部は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム (SIP) 「国家レジリエンス (防災・減災) の強化」(管理法人: 防災科研) と、産業技術大学院大学 国際共同研究事業によって実施した。

参考文献

- [1] Systems And Software Engineering - Architecture Description, ISO/IEC/IEEE 42010:2011
- [2] 嶋津恵子, 橋田要一, 巨大災害発生時の急性期における減災と救命のための情報集配信システム構想, METHANE レポートの電子テキスト配信化による準天頂衛星安否確認サービスの有効利用 -, 測位航法学会ニューズレター 第V巻第3号 2014年9月25日, pp.3-6
- [3] 小滝昇, 東日本大震災 緊急対策本部の90日間 - 政府の初動・応急対応はいかになされたか -, ぎょうせい, 2013年08月20日
- [4] Keiko Shimazu, others, Emergency Warning Services via GNSS Signals, IEEE Aerospace Conference, Vol.4, pp.214-220, Big Sky, Montana, USA, Mar. 8th-14th 2020
- [5] "Common Alerting Protocol, OASIS Standard". <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html>, (参照 2021-08-06)
- [6] "台風・ハリケーンの強さ比較". <https://www.eorc.jaxa.jp/TRMM/data/trmmxge/images/TyphoonLevel.pdf>, (参照 2021-08-06)