5B-03

Alloy を活用したインフラ設計段階における正当性検証

中村 雄一郎† 辻尾 良太† 松浦 陽平†

†三菱電機株式会社 情報技術総合研究所

1. はじめに

ウォーターフォール型のオンプレシステム開発におけるインフラ環境構築では，上流設計での検討漏れや担当者間の認識齟齬による設計ミス，設定誤りが発生する．上記が原因となり後工程で手戻りが発生し，工程遅延や人員追加によるコストの増加が問題となっている[1]．上記問題の対策として，設計・設定のレビュー人員を追加することが考えられるが，人手不足の場合は対応できない．また，人による確認では抜け漏れが起こり得る．

本稿では，上流におけるインフラ設計・設定を機械的に且つ，網羅的に確認することを目的として，インフラ設計をモデル化するための制約を事前に定義し，設計ドキュメントに記載のパラメータを用いてモデル検査を行う手法について述べる．

従来手法と本手法の概要を図 1 に示す．本手法を用いることで，インフラ担当者は形式手法の記述を意識する必要がなく，形式手法の習得に必要なコストが発生しない．本手法を用いて，インフラ設計・設定の正誤が容易に検査できることを確認した．

2. 課題

インフラ設計・設定を機械的に且つ，網羅的に確認する手段として形式手法があるが，形式手法を使用するためにはインフラ担当者のスキル向上・教育が必要であり，コストが発生する．そのため，インフラ設計ドキュメントをインプットとし，形式手法を適用できるようにする．

3. 解決策

形式手法である Alloy を使用し，検証として Firewall(以降，FW)を介したクライアントから WEB サーバへの接続構成を事前にモデル化する．モデル化する際に定義した「クライアントから WEB サーバに接続可能」という制約を固定し，インフラ設計ドキュメントに記載されたパラメータをこのモデルに当てはめる．当てはめられたモデルを Alloy Analyzer[2]というツールを用いてモデル検査することで，形式手法の記述を意識せずにインフラ設計・設定の正誤を検査する．

3.1. Alloy の概要

Alloy はモデル化のためのオープンソースの言語である．Alloy はモデルをシグネチャと呼ばれる要素単位で定義し，シグネチャ間を関係として定義することが可能である．定義したシグネチャと関係に制約を与えることも可能である．Alloy Analyzer は，Alloy で定義したモデルを検査することが可能である．また，他の形式手法と異なりモデルを可視化することが可能である．

Validation verification at infrastructure design phase with Alloy
† Information Technology R&D Center, Mitsubishi Electric Corporation.

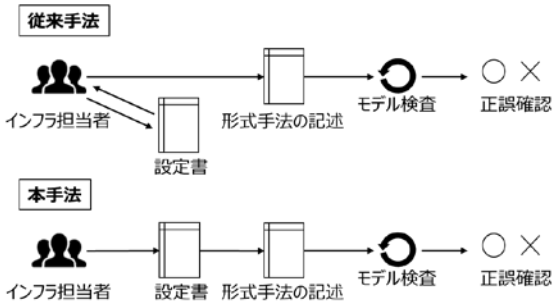

図 1 従来手法と本手法

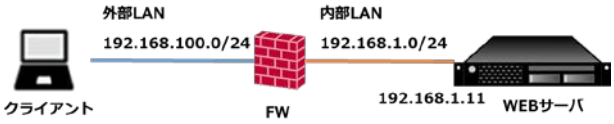

図 2 クライアント，FW，WEB サーバの構成図

表 1 FW ポリシー

送信元	送信先	通信プロトコル	許可/拒否
any	192.168.1.11	HTTPS	許可

3.2. インフラ構成のモデル化

検証として使用した FW を介したクライアントから WEB サーバへの接続構成を図 2 に示す．図 2 ではクライアントと FW が，FW と WEB サーバが同じネットワーク上にあることがわかる．図 2 に記載していないが，FW には表 1 のポリシーを設定している．表 1 の FW ポリシーに従い，クライアントから WEB サーバへの HTTPS 接続を Alloy でモデル化し，Alloy Analyzer により可視化したモデルを図 3 に示す．図 3 では，四角い枠がシグネチャを示しており，矢印がシグネチャ間の関係を表している．Alloy はシグネチャと，シグネチャ間の関係に加えて，fact という不変条件(制約)を定義することができる．

表 2 に，定義した fact を示す．クライアント IP アドレスと WEB サーバ IP アドレスが異なることは明らかだが，①の通り Alloy では明示する必要がある．②，③も同様に明示する必要がある．④，⑤は表 1 のポリシーと一致していることを示しており，⑥はクライアントの接続先 IP アドレスと WEB サーバ IP アドレスが一致することを示している．⑦，⑧はクライアントと FW，WEB サーバと FW が同一ネ

表 2 定義した fact 一覧

No.	fact
①	クライアント IP アドレスと WEB サーバ IP アドレスは異なる
②	クライアント IP アドレスと FW ポリシーの接続先 IP アドレスは異なる
③	クライアント IP アドレスとクライアントの接続先 IP アドレスは異なる
④	WEB サーバ IP アドレスと FW ポリシーの接続先 IP アドレスは等しい
⑤	クライアントの接続先 IP アドレスと FW ポリシーの接続先 IP アドレスは等しい
⑥	クライアントの接続先 IP アドレスと WEB サーバ IP アドレスは等しい
⑦	クライアントの所属 LAN と FW の所属 LAN は等しい
⑧	WEB サーバの所属 LAN と FW の所属 LAN は等しい
⑨	①から⑧が成立し，FW ポリシーと Allow との関係 Judgement が存在すれば，クライアントから WEB サーバへの関係 Access が存在し，それ以外であれば関係 Access は存在しない

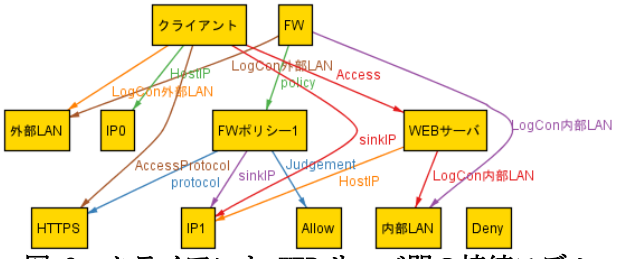

図 3 クライアント-WEB サーバ間の接続モデル

ットワークにあることを示している．⑨はクライアントから WEB サーバへの関係 Access が存在する条件を示している．本ケースでは，関係 Access が存在するため，クライアントから WEB サーバに HTTPS 接続可能ということがわかった．

3.3. 設定書から Alloy への変換とモデル検査

3.2 節では，Alloy を用いて想定しているモデルが出力できることを示した．しかし，インフラ設計・設定に Alloy を使用するためには，インフラ担当者のスキル向上・教育が必要であり，コストが発生する．そこで，Excel のインフラ設定書から Alloy に変換するツールを python で開発した．使用した設定書の一部を図 4 に示す．

開発ツールは，図 4 の値をシグネチャと，シグネチャ間の関係，fact に変換する．4.2 節との違いは fact の定義方法であり，例えば表 2①では，クライアント IP アドレスと WEB サーバ IP アドレスが異なるという fact を手動で定義している．開発ツールは，図 4 のクライアント IP アドレスと WEB サーバ IP アドレスの比較結果を fact として定義する．そのため，表 2①のように異なる場合だけでなく，等しい場合も fact として定義される．これは，設定値が誤っていた場合に，誤った fact が設定されることによって，誤ったモデルが出力され，設定値が誤っていることを発見するためである．ただし，表 2⑨は関係 Access が存在する条件であり，設定値に

クライアント情報

クライアント名	IPアドレス	接続先	接続先IPアドレス	通信プロトコル	所属LAN
クライアント1	*	WEBサーバ1	192.168.1.11	HTTPS	外部LAN

FW情報

FW名	所属LAN1	所属LAN2
FW1	外部LAN	内部LAN

FWポリシー情報

ポリシーNo.	送信元	送信先	通信プロトコル	許可/拒否
1	any	192.168.1.11	HTTPS	許可

WEBサーバ情報

WEBサーバ名	IPアドレス	所属LAN
WEBサーバ1	192.168.1.11	内部LAN

図 4 Alloy に変換するための設定書

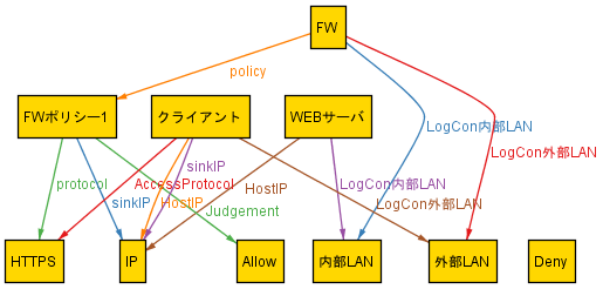

図 5 クライアントと WEB サーバの IP アドレスが同じ場合のモデル

依存しないため固定とした．

図 4 のクライアント IP アドレスを WEB サーバ IP アドレスと同じ 192.168.1.11 に設定し，開発ツールと Alloy Analyzer を使用しモデル検査すると図 5 のような誤ったモデルが出力される．なお，設定値が正しい場合は図 3 の通り出力されることを確認した．

クライアント IP アドレスと WEB サーバ IP アドレスが等しいという fact は表 2⑨の通り関係 Access が存在する条件に該当しないため，図 5 のように関係 Access が存在しないモデルが出力された．この結果から，形式手法の記述を意識する必要なく，出力されたモデルから設定書が誤っていることを確認できた．

4. おわりに

インフラ設計段階の正当性検証として，インフラ設計をモデル化するための制約を事前に定義，固定し，インフラ設計ドキュメントに記載のパラメータを用いてモデル検査を行う手法について述べた．本手法を使用することにより，形式手法の記述を意識することなく，インフラ設計段階での設計・設定の漏れやミスを防止できることを確認した．今後は，WEB サーバ以外のモデルの充実化など複雑な構成への対応を行う．

参考文献

[1] 独立行政法人情報処理推進機構，"厳密な仕様記述における形式手法成功事例 調査報告書"，<https://www.ipa.go.jp/files/000026875.pdf>2020-12-10 アクセス

[2] <https://alloytools.org/about.html>2020-12-10 アクセス