分散システムの耐災害性・耐障害性の検証・評価・反映を行うプラットフォームとビジネスモデルの開発（150202001）

Developments of a platform and its business model to validate, evaluate and reflect disaster tolerance and fault tolerance on distributed systems.

研究代表者
柏崎礼生 大阪大学
Hiroki Kashiwazaki Osaka University

研究分担者
西内一馬 † 市川昊平 †† 近堂徹 ††† 北口善明 †††† 菊池豊 ††††† 中川郁夫 ††††††
Kazuma Nishiuchi† Kohei Ichikawa†† Tohru Kondo††† Yoshiaki Kitaguchi††††
Yutaka Kikuchi††††† Ikuo Nakagawa††††††
†株式会社シティネット ††奈良先端科学技術大学院大学 †††広島大学 ††††金沢大学
†††††高知工科大学 ††††††大阪大学
†Citynet Inc., ††Nara Institute of Science and Technology †††Hiroshima University
††††Kanazawa University †††††Kochi University ot Technology ††††††Osaka University

研究期間 平成 26 年度～平成 27 年度

概要
災害や複雑な障害に強い分散システムを構築・評価するために、分散システム上に擬似的に災害や故障を発生させ、その状況を検証・評価可能なプラットフォームを実現する災害エミュレーションアプリケーションを構築した。本プラットフォームおよび分散システムにおける災害訓練の普及活動を行い、標準化のためのコンソーシアムを立ち上げた。

１．まえがき

東北地方太平洋沖地震以降、組織における事業継続計画の策定は明らかに進捗した。しかし計画は策定されたものの、計画に従った手順の定常的な再確認や見直しは普及しておらず、策定した計画の形骸化が懸念される。この原因として計画の再確認に伴うサービスの中断や再確認・見直しのコストが挙げられる。インターネットやその上で動作するクラウドコンピューティング環境に代表される広域分散システムは、その社会的重要性が高まる一方で事業継続計画の再確認や見直しに要するコストが無視出来ない。

本研究開発は、災害や複雑な障害に強い広域分散システムを構築・評価するために、分散システム上に擬似的に災害や故障を発生させ、その状況を検証・評価可能なプラットフォームを実現する「災害エミュレーションアプリケーション」を構築する、これにより広域分散システムにおける事業継続計画の再確認や見直しに要するコストを軽減し、普及を推進することを目的とする。具体的には、事前に用意したシナリオに沿って同時に多様な故障を同時多発的に発生させ、その状態を観測するアプリケーションを開発することによって実現する。これにより、現実に起こり得る障害を模倣する状況での検証を可能にし、分散システムの耐災害性・耐障害性を確保する手法の確立を目指す。

２．研究開発内容及び成果

本研究課題で設計と実装を行った「災害エミュレーションアプリケーション」は「ユーザインターフェイス部」「災害シナリオ生成部」「障害実装部」からなる。

広域分散システムにおける災害訓練を実施する場合、訓練の実施者は訓練のシナリオ（災害シナリオ）を作成し、このシナリオに従って実際のネットワーク機器（エンティティ）に障害が実装されたあとに全ての機器の状態を確認することで省察を行う。ユーザインターフェイス部はこの「災害シナリオの作成」と「全ての機器の状態の確認」を担う。ユーザインターフェイスは訓練の実施者が直感的にシナリオを作成することができるように Web インターフェイスが提供される。訓練の実施者が把握しているネットワークエンティティの情報をユーザインターフェイスに提供することにより、これらのネットワークエンティティの接続情報が得られ、ネットワークエンティティを節、ネットワークエンティティ同士を接続する回線を枝とする有向グラフのトポロジを得る。訓練実施者はこのトポロジに含まれるネットワークエンティティと回線に対して、訓練開始時刻からの相対的な時刻において発生する障害表現（「ポートダウン」「パケットロス」「トラフィックシェーピング」「遅延追加」およびこれらの障害への「回復」）を組み合わせて災害シナリオを記述する。この災害シナリオは「災害シナリオ生成部」へと渡され、指定された時刻に、災害シナリオを構成する障害表現がネットワークエンティティに対して実装される。実装された障害表現が実際に実装されたかどうかなどの状況情報はネットワークエンティティからユーザインターフェイス部へと送られる。ユーザインターフェイスは災害シナリオに関連する情報のみ抜き出して訓練の進捗を観察することができる。また災害シナリオの問題解決可能性を検証するための初歩的な実装も具備されている。

災害シナリオ生成部はユーザインターフェイス部からの情報を受け取り、ネットワークエンティティと通信を行うことで、指定された災害シナリオを実現する。ユーザインターフェイス部から災害シナリオが提供されると、指定された時刻にその災害シナリオを開始する。災害シナリオは複数の障害表現と、その障害表現を実装する相対時間により構成される。災害シナリオ生成部はこの時間管理を行い、指定された時間になると障害表現に従いネットワークエンティティに対して障害を実装するよう指示を行う。ネットワークエンティティの制御にはオープンソースで開発が行われている SDN コントローラである

OpenDaylight フレームワークを利用した。OpenDaylight フレームワークでは、ネットワークエンティティにおける差異を吸収した標準的な制御インターフェイスを提供することを目指しているが、現状の実装では機種依存性を吸収する作りになっていない。そのため、ネットワーク機器への制御を中継する障害実装部を用意し、OpenDaylight の設計を継承した機種依存性のない API を災害シナリオ生成部に対して提供する設計とした。

障害実装部は、利用するネットワークエンティティの差異を吸収する。今回、ネットワークエンティティ制御プロトコルには YANG（Yet Another Markup Language）データモデルを用いた NETCONF を参考に設計した。YANG データモデルは、ネットワーク機器の構造や各種設置値などを抽象化し、ネットワーク機器の差異を吸収し汎用的に扱うことを目的としたデータモデルである。YANG による各種データのモデル化は、IETF における様々な WG にて盛んに議論されている過程であり、今後の標準的な技術になると考えられる。

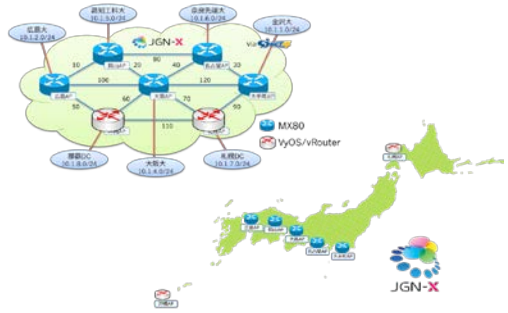

図 1 災害エミュレーションプラットフォーム
DESTCloud の概略図

この災害エミュレーションアプリケーションを用いて様々な広域分散アプリケーションの検証実験を行うために、国内 7 拠点の研究組織が計算機資源とネットワーク資源を提供して災害エミュレーションプラットフォーム“DESTCloud”を構築した。DESTCloud を用いて広域分散ストレージシステムの耐災害性・耐障害性の検証を行い、脆弱性を発見することにより正常向上に寄与することを実現した。

３．今後の研究開発成果の展開及び波及効果創出への取り組み

本研究開発で構築した DESTCloud は JGN-X が提供するサービスを利用したため、DESTCloud への参画には JGN-X のアクセスポイントへの接続性を用意することが事実上の要件となっていた。この制約は本研究開発成果の展開における大きな制約条件となるため、各組織間を VxLAN や NVGRE に代表される L2 延伸技術を用いて接続し合うことで JGN-X 接続性がない組織でも DESTCloud の拠点として参画することができるよう再設計を行っている。既に国内外での接続組織の増大について活動を開始しているが、参画組織と共同研究契約を締結することにより、単なる実証実験拠点の増大ではなく、DESTCloud を用いた新たな取り組みの創発や人材育成を行うことを目的としている。

本研究開発ではネットワークエンティティに特化した研究開発を行った。分散システムはアプリケーションやサービスを提供する計算機群、特定用途のトラフィック処理に特化されたネットワーク機器、計算機やネットワーク機器を接続するネットワーク回線、およびこれらに電力を供給する電力供給装置により動作する。このうち特定用途のトラフィック処理に特化されたネットワーク機器はネットワーク機能仮想化技術の発展とともにその優位性が薄れていくことが考えられる。この観点からすると今後、分散システムを構成する要素は「物理・仮想計算機群」「これらを接続するネットワーク回線」「電力供給」の三種類に集約されていくことが考えられる。これらの構成要素をプログラマブルに制御するための API を実装し、分散システムの災害訓練をより多様に実施することで、運用自動化への寄与することが期待できる。これを実現するため Software Defined Networ だけを利用するのではなく、Software Defined anything (SDX) 技術を用いた DESTCloud の実現に向けて新たなプロジェクトを立ち上げた。

本研究開発の動機付けは「自然」災害に対する事前の備えを行うことであったが、広域分散システムは多様な災害の影響を被る。サイバー攻撃もまた同時多発的に発生する災害に分類される。複数の拠点からサイバー攻撃を行う DDoS は 2011 年からの 5 年間で量的に 6 倍に増大した。自然災害にせよサイバー攻撃にせよ、災害の発生を完全に防ぐことは困難である。そのため、災害に対する対応手段は共通して mitigation (緩和) という言葉が用いられる。大規模災害であれ分散型のサイバーテロであれ、被災がシステムに対してもたらす定性的・定量的な影響を事前に把握し、サービス提供者が想定するサービスレベルがその影響により下回るようであれば増強などの対策を講じなければいけない。広域分散システムを構成する計算機、ネットワーク、電源供給装置の全てをプログラマブルに操作することにより拡張された DESTCloud が、訓練による被害の検証、被害の評価、およびその対策を一連の運用自動化プロセスに組み込み、「その分散システムにおいて解決可能な問題」の集合のうち、どれだけの問題に対してどのように対処することができたかの達成状況を分散システムの耐災害性・耐障害性を定量的に評価する指標として確立することが今後期待できる。

４．むすび

災害による被害とその復興は地域や国家によって多種多様である。本研究成果を世界的に普及させ耐障害性・耐災害性の定量的な評価の重要性を確立させることにより、より効率的な減災の取り組みに結びつけたい。

【誌上発表リスト】

[1]北口善明、柏崎礼生、近堂徹、市川昊平、西内一馬、中川郁夫、菊池豊、"広域分散システムの耐障害性を評価する検証プラットフォームの実装と評価"、情報処理学会論文誌 Vol.57 No.03 pp958-966（2016/03/15）

[2]北口善明、柏崎礼生、近堂徹、市川昊平、西内一馬、中川郁夫、菊池豊、“耐障害性・耐災害性の検証・評価・反映プラットフォームの設計と実装”、研究報告インターネットと運用技術（IOT） Vol.2015-IOT-32 No.13 pp1-6 2016 年 03 月

[3]柏崎礼生、北口善明、近堂徹、市川昊平、西内一馬、中川郁夫、菊池豊、“耐障害性・耐災害性の検証・評価・反映プラットフォームを用いた広域分散ストレージの評価”、研究報告インターネットと運用技術（IOT） Vol.2015-IOT-32 No.14 pp1-6 2016 年 03 月

【本研究開発課題を掲載したホームページ】

http://ricc.itrc.net/DESTCloud