ISSN 0915-2318 平成2年3月5日第三種郵便物認可
令和5年10月1日発行　毎月1回1日発行　第35巻第10号（通巻415号）

NTT 技術ジャーナル

10 OCTOBER 2023
Vol.35 No.10

特集

より強靭性の高いネットワークの実現に向けて

NTTテクノクロスのセキュリティ技術・ビジネスの最新動向とSBOMへの取り組み

For the Future

5Gで変わる世界の通信業界:新たなプレイヤー, 新たな通信ネットワークの姿―前編―

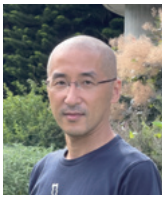
from NTT DATA

新たなクラウドマーケット「エンド・ツー・エンド」で価値を提供するNTT DATAのクラウドアセット

NTT 技術ジャーナル
10 OCTOBER 2023
Vol.35 No.10

CONTENTS

URL https://journal.ntt.co.jp/backnumber/2023/vol3510
DOI https://doi.org/10.60249/23100000



本誌掲載内容についてのご意見，ご要望，お問い合わせ先
日本電信電話株式会社　NTT技術ジャーナル事務局
E-mail　journal@ml.ntt.com

本誌ご購読のお申し込み，お問い合わせ先
日本電信電話株一般社団法人電気通信協会　ブックセンター
TEL（03）3288-0611　FAX（03）3288-0615
ホームページ　http://www.tta.or.jp/

NTT技術ジャーナルは
Webで閲覧できます．
https://journal.ntt.co.jp/

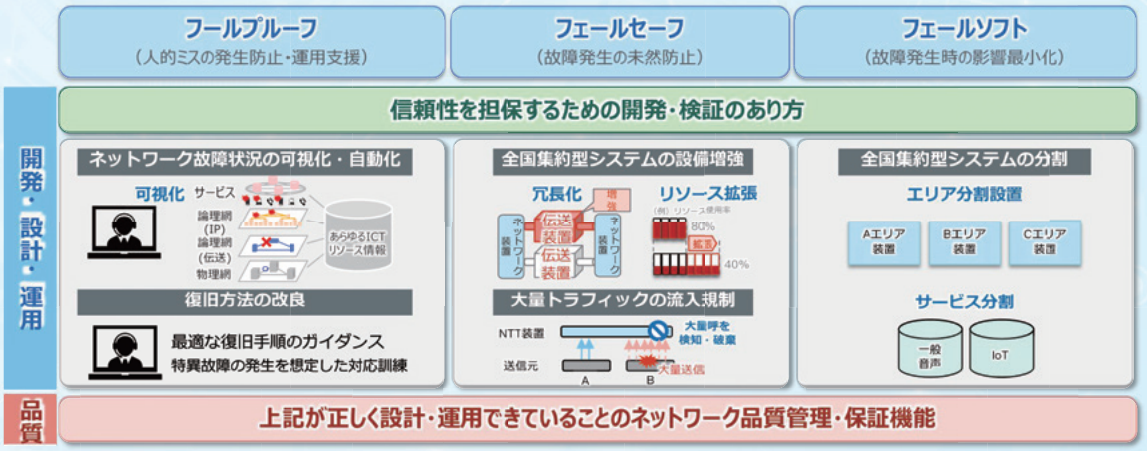
特集 1

より強靭性の高いネットワークの実現に向けて

大規模な通信故障は日常生活や経済活動に甚大な影響を及ぼすため，
より強靭性の高いネットワークが求められる．
本特集では，NTT研究所で推進するシステム故障に対して，
ネットワークの抵抗力を高めることでサービス影響を抑止し，回復力を高めることで
復旧時間短縮するロバストネットワークの実現に向けた取り組みについて紹介する．

強靭性の高いネットワークを支えるオペレーション 6

ネットワークシステム故障の耐性強化に向けたオペレーション技術を中心とした研究開発の取り組みについて紹介する．



URL　https://journal.ntt.co.jp/article/23440
DOI　https://doi.org/10.60249/23105001

強靭性の高いネットワークを支えるオペレーション

大規模な通信故障は日常生活や経済活動に甚大な影響を及ぼすため，より強靭性の高いネットワークが求められます．NTT研究所では，システム故障に対してネットワークの対応力を高めることでサービス影響を抑止し，回復力を高めることで復旧時間を短縮するロバストネットワークの実現をめざしています．本稿では，ロバストネットワークを支えるオペレーション関連技術の研究開発の取り組みについて紹介します．

キーワード：#ロバストネットワーク，#オペレーション，#NW-AI

岡本　淳[†1]／柴田　朋子[†2,3]
田原　光穂[†1,3]／藤原　正勝[†4]
増田　征貴[†1]

NTTネットワークサービスシステム研究所[†1]
NTTアクセスサービスシステム研究所[†2]
NTTネットワークイノベーションセンタ[†3]
NTT情報ネットワーク総合研究所[†4]

ロバストネットワークの実現に向けて

ネットワークは仮想化技術や市販品で複雑に構成されるようになり，サービスの多様化により膨大なデータが流通するため，ネットワークのオペレーションは複雑化しています．また，社会・経済生活のさまざまな分野においてICTの利活用が浸透しており，大規模な通信故障は，人々の日常生活に甚大な影響を及ぼします．そのため，より強靭性の高いネットワークが求められます．NTT研究所では，ネットワークシステムの故障や大規模災害への耐性が強いロバストネットワークの実現をめざして研究開発に取り組んでいます．本稿では，ネットワークシステム故障の耐性強化に向けたオペレーション技術を中心とした研究開発の取り組みについて紹介します．

通信故障対策の方向性

通信故障には，ソフトウェア故障による連鎖的な故障範囲の拡大や異常トラフィックの発生，オペレーションミス，システム異常等，さまざまな要因が存在します．ネットワークシステムの複雑化，多様化，仮想化に加え，海外製品の活用によるシステム内部のブラックボックス化が進むと，装置実装を把握したうえでの対策や，過去事例に基づいて想定した故障事象での事前検証のみでは，あらゆる故障をカバーしきれなくなることが想定されます．そこで，ロバストネットワークの実現に向けては，想定外の事象は必ず起こることを前提に，通信故障対策の基本方針として，フールプルーフ，フェールセーフ，フェールソフトの観点でオペレーション関連技術について検討します（**図1**）．

・フールプルーフ：人的ミスの発生を防止し，人的オペレーションを効果的にサポートする仕組みが必要になります．例えば，ネットワークの故障状況を可視化する機能やオペレータによる復旧対策を支援する機能等を検討します．
・フェールセーフ：通信故障を未然に防ぐ仕組みが必要になります．例えば，通信設備の冗長化やシステムのリソース拡張等により故障頻度を抑制する対策や，故障要因となり得る大容量トラフィックの流入規制等により故障を未然に防ぐための機能を検討します．
・フェールソフト：故障発生時の影響範囲を最小化するための仕組みが必要になります．例えば，１つの装置故障が他のサービスや他のエリアに影響が波

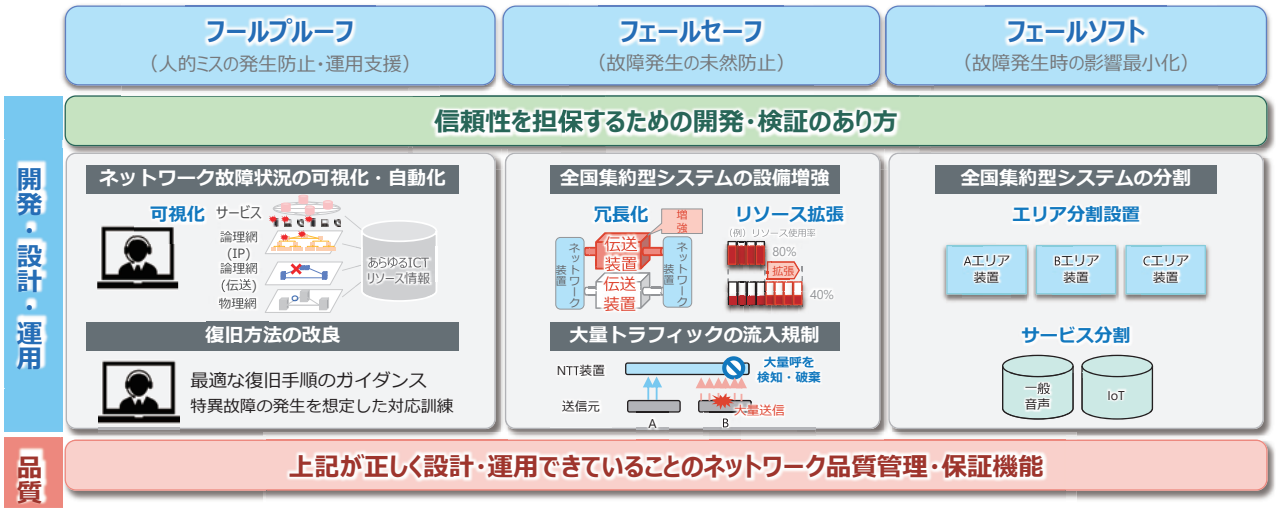


図1　通信故障対策の基本方針

及しないように，エリアやサービスを分割できる機能等の対策を検討します．

ネットワークシステムの信頼性を担保するためには，フールプルーフ，フェールセーフ，フェールソフトの観点に基づき，開発，設計，運用の各業務フェーズで対策を立て，開発や検証のあり方を検討する必要があります．また，検討した対策が正しく設計や運用に反映できていることを監査するネットワーク品質管理・保証機能も検討する必要があります．

NTT研究所では，ネットワークシステム故障への耐性を強化するために，ネットワークシステムの複雑化，多様化，仮想化によるネットワークオペレーションの高難度化に対応し，想定外事象の極小化の実現に向けて，3つの方向性で新たな技術の創出に取り組みます（**図2**）．

⑴　状況の見える化

故障発生時に早期の対策を実施するには，ネットワークの状況を把握し，故障個所や故障要因を特定できることが重要になります．そのため，ネットワーク上の装置から出力されるログやアラーム等の装置実装に依存した情報にとどまらず，ネットワークの内部および外部で取得可能なさまざまな情報を活用し，インテリジェントに状況の見える化を実現する技術の創出をめざします．

⑵　高可用制御のマルチ化

システムの利用可能な状態を維持し，故障を発生しにくくするには，ネットワークシステムに対して，あらゆる救済対策を持つことが重要になります．単一のシステムや単一のサービスに閉じることなく，多面的な救済対策を可能にする高可用制御技術や仕組みを創出することで，故障発生の未然防止やサービス影響の最小化の実現をめざします．

⑶　検証と運用の連携高度化

サービス運用時に想定外の事象が発生すると，早期に対処することが困難になるため，事前のシステム検証において，想定外の事象を最小化しておくことが重要になります．一方，仮想化技術や海外製品の活用によるシステムの複雑化，サービスの多様化により，人知を遥かに超えるレベルでさまざまな事象が複雑に影響し合い，想定外の事象が発生します．過去の経験に基づいて抽出した検証項目のみでは，想定外の事象を減らすことが困難になりつつあります．

そのため，従来の経験に基づく検証手法を脱却する抜本的なアプローチとして，装置やネットワークのデジタルツイン環境を活用し，あらゆる検証条件をAI（人工知能）で抽出し，それに基づいて疑似故障を発生させ，復旧対策を自律的にAIが学習する検証手法と，復旧対策を学習したAIをタイムリーに運用へ適用する高度な連携技術の創出をめざします．

これらの方向性で創出する新たな技術により，ネットワークシステム故障に対するネットワークの対応力を高め，サービス影響を抑止し，回復力を高めることで復旧時間を短縮するロバストネットワークの実現をめざします．また，ネットワークシステムの複雑化や膨大なデータ流通により，高難度化するネットワークオペレーションにおいては，積極的にAIを活用し，将来的に自動化・自律化が実現可能なオペレーション技術の創出をめざします．

状況の見える化

仮想化技術により，ネットワークシステムの複雑化やブラックボックス化が進む中で，異常を早期に把握することは大きな課

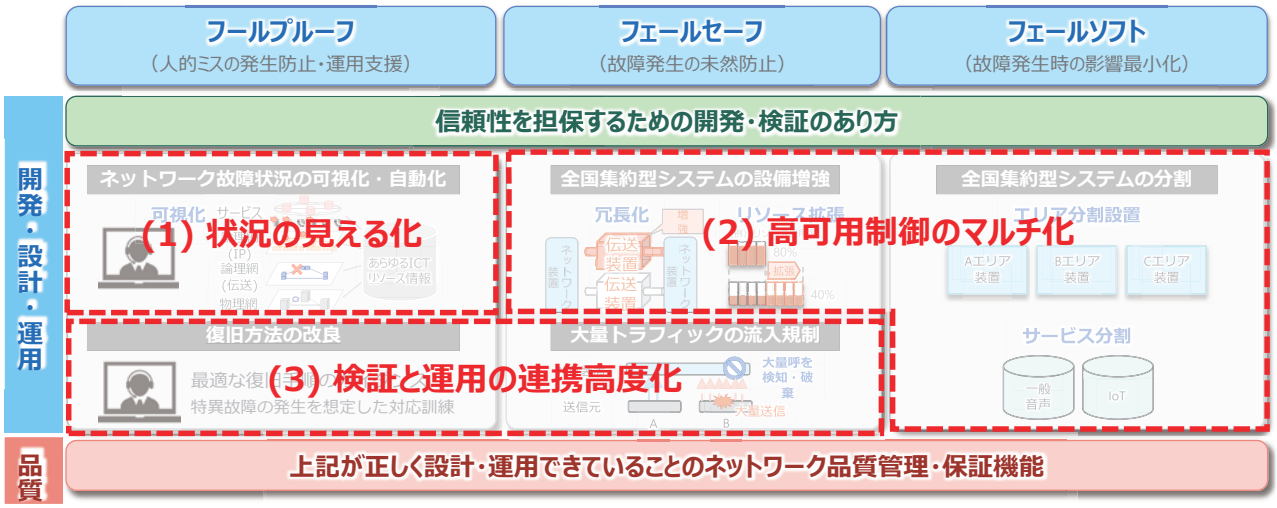


図2　通信故障への耐性強化の取り組みの方向性

題となります．また，フールプルーフの観点でも，オペレーションの人的ミスの防止や効果的なサポートの実現は課題となります．NTT研究所では，これらの課題をAIの活用により解決し，将来的にネットワークオペレーションを自動化・自律化する自己進化型ゼロタッチオペレーションの実現をめざしています．

ネットワークオペレーションを担うAIをNW-AIと呼び，NW-AIを活用した自己進化型ゼロタッチオペレーションの流れを**図3**に示します．まず，ネットワーク内部の構成情報や観測情報と，ネットワーク外部の天気やSNS，地域イベント等のさまざまな情報を収集します．次に，収集した情報をNW-AIにより分析し，次のアクションを判断します．そして，判断結果に基づいて，ネットワークシステムに対して措置を実行します．この一連のループを自動で繰り返し，自律的に学習を行うNW-AIを創出することで，自己進化するゼロタッチオペレーションの実現をねらいます．

NW-AIによる分析・判断のプロセスでは，ネットワークやサービスの状況の見える化を実現します．故障発生時に，ネットワークのどこで何が起きているのか，もしくは，その予兆をシステムから出力されるアラーム情報やトラフィック変動，周辺装置の情報，さらには，ネットワーク外部の情報を活用し，より多角的に判断して異常やその予兆を検出します．次に，発生している事象を特定し，それによるサービスの影響範囲を特定します．そして，故障個所を推定して原因を特定します．従来，これらの状況の見える化は，物理ネットワークレイヤ，論理ネットワークレイヤ，サービスレイヤ等のレイヤごとに出力される大量のアラームを用いてオペレータが手動で分析を実施し，全容を把握するまでに多くの時間を要してきました．これらの業務を支援・自動化するNW-AIを創出することで，故障の早期検知が期待できます．現在，ディープラーニングを用いて多様なデータから各種システムの正常状態をモデル化し，正常状態からの乖離で異常を検知するDeAnoS®(Deep Anomaly Surveillance)[1]，アラームを事象単位に集約するアラームクラスタリング，故障時のサービス影響範囲を可視化可能なNOIM（Network Operation Injected Model）[2]，故障個所を推定するDeAnoS-RCA（Deep Anomaly Surveillance-Root Cause Analysis）やKonan（Knowledge-based autonomous failure-event analysis technology）等の

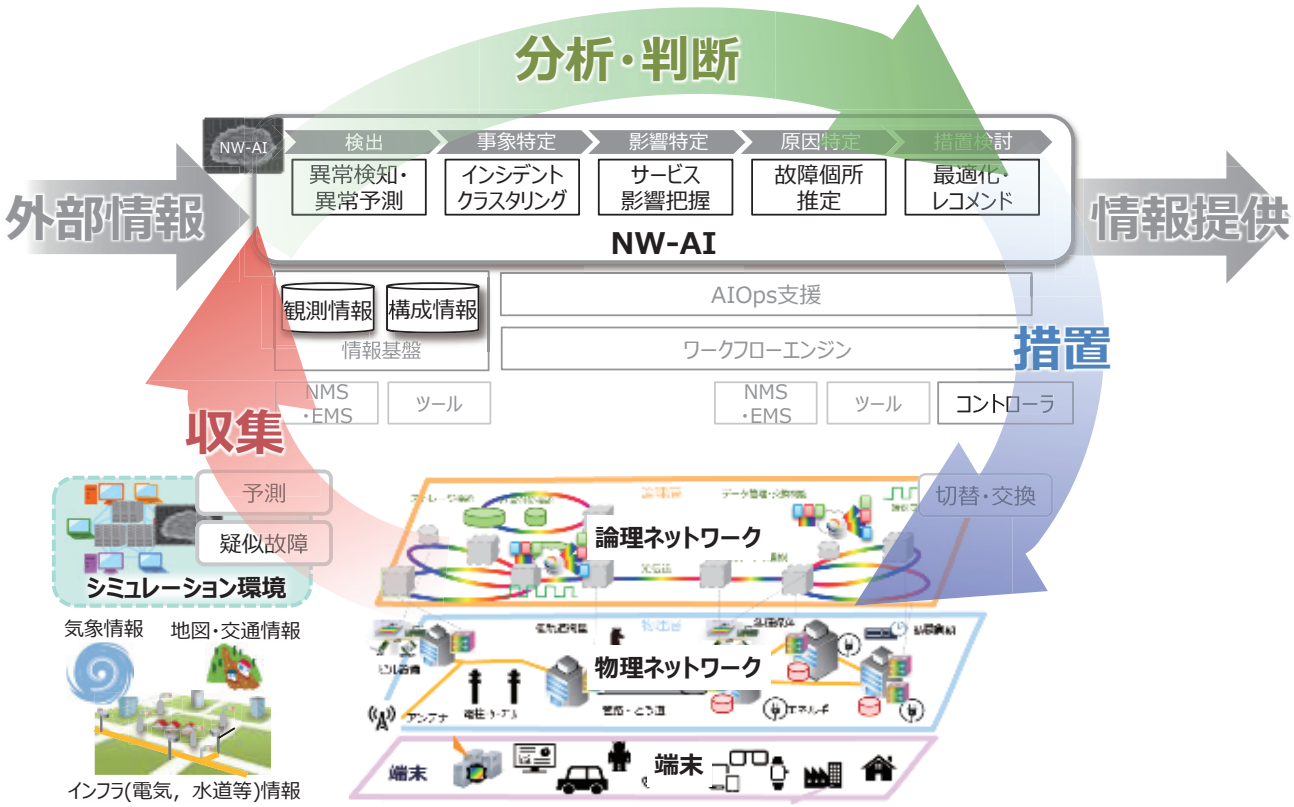


図3　自己進化型ゼロタッチオペレーションの流れ

NW-AIを研究所では研究開発しています．これらの技術や状況の見える化については，本特集記事『大規模システム故障時の「ネットワーク状況の早期把握」』[3]で紹介します．

高可用制御のマルチ化

通信故障発生時のサービスの可用性を高めるために，既存のネットワークシステムにおいて，設備の冗長化や大量トラフィックの流入規制などの対策がとられています．しかし，既存の対策でも早期の故障復旧が困難な場合も存在します．そのため，想定外の事象は必ず起こることを前提に，いかに多くの救済手段を確保できるかが課題となります．また，複数の救済手段の導入によりシステムの信頼性向上は見込めますが，同時に導入コストの増加につながるため，信頼性と経済性のバランスを評価することも課題となります．

故障発生時のサービス影響を最小化するフェールソフトの観点では，単一の装置故障が，他のエリアやサービスに波及しないように，エリア単位や事業者単位で装置を分割・増強することで，故障範囲が拡大するリスクを減らす仕組み等が検討されています．また，故障発生を未然に防ぐフェールセーフの観点では，ネットワークシステムの装置や機能を冗長化することで，早期の故障復旧を可能とする仕組みが検討されています．今後，ネットワークの仮想化が進展することで，より経済的にシステムの冗長化の仕組みを確保できるようになることが期待できます．

サービスの高可用性を高めるための冗長化の例として，リソースのマルチ化，レイヤのマルチ化，ネットワークサービスのマルチ化等が検討されています．

リソースのマルチ化では，仮想化・分散化されたシステムにおいて，ハードウェアリソースプールから各サービスに必要なリソースと冗長化のための予備リソースをあらかじめ最適に割り当てます．異常状態等により予備リソースも不足した際は，異常のスパイラルから脱出するための応急リソースや必要に応じて他サービスに割当て済のリソースを暫定的に割り当てます．また，サービス間の干渉を抑制するために，ハードウェアレベルでのリソースの共用と隔離の仕組みを検討しています．

レイヤのマルチ化では，平常時は伝送ネットワークやイーサネットワーク，IPネットワーク等の各ネットワークのレイヤの独立性を維持しつつ，故障発生時等には，レイヤ間連携による最適制御を実施します．レイヤ間の依存関係を考慮して冗長設計や管理制御を行い，異常な外部イベントに対して最適レイヤで抑止制御する仕組みを検討しています．

ネットワークサービスのマルチ化では，異常発生時に他のシステムに無線アクセスを切り替えるアクセスネットワークのマルチ化，仮想化されたネットワークを想定し，異常発生時のサービスレベルを考慮してネットワークスライスや光パスを切り替えるコアネットワークのマルチ化等，各種ネットワークサービスのマルチ化によりトータルで大規模故障の発生を未然に防ぐ仕組みを検討します．ネットワークサービスのマルチ化，伝送ネットワークの冗長化等の具体的な技術については，本特集記事『ネットワークの強靭化を実現する設計制御技術』[4]で紹介します．

検証と運用の連携高度化

各種サービスを提供する際は，装置やシステムの開発・構築において，さまざまな検証試験が実施されています．しかし，仮想化技術等により複雑に構成され，ブラックボックス化が進むネットワークシステムにおいては，起こり得るすべての事象を網羅することは難しく，装置の開発者やシステムの設計者の想定を超えた想定外の事象に対し，いかに対処するかがオペレーションでの課題となります．また，フールプルーフの観点では，人的ミスをなくし，効率的に想定外事象に対処可能なオペレーションの仕組みを構築することが課題となります．

NTT研究所では，デジタルツイン環境や検証環境を活用し，検証と運用を高度に連携させる仕組みについて検討しています．フレームワークを**図4**に示します．まず，商用サービスが提供されるネットワークシステムと類似する環境を構築します．この類似環境において，疑似故障を発生させるカオスエンジニアリングツールを活用し，さまざまなバリエーションで故障等のイベントを人工的に発生させ，想定外の事象を洗い出す可能性を高めます．そして，イベントに対する自律復旧を行うNW-AIの実現をめざします．技術開発のポイントは以下のとおりです．

⑴　イベント生成

故障等のイベントの検証条件をAIの活用により人工的に生成します．商用サービスで流れるトラフィックデータ等の分析に基づき，故障が発生するイベントの検証条件を効率的に生成します．

⑵　カオスエンジニアリング活用による検証とAI学習

生成されたイベントの検証条件に基づき，カオスエンジニアリングツールを用いて，類似環境でイベントを発生させます．これにより，装置開発者やシステム設計者の想定範囲を逸脱した条件下でのシステムの振る舞いを把握します．そして，このシステムの振る舞いと対処策をNW-AIに自律的に学習させ，商用のサービス提供環境では想定外の事象に対しても対処可能なNW-AIの実現をねらいます．また，類似環境での振る舞いの把握や対処策の学習は，NW-AIの学習にとどまらず，商用サービスのオペレータの訓練にも活用することを想定しています．

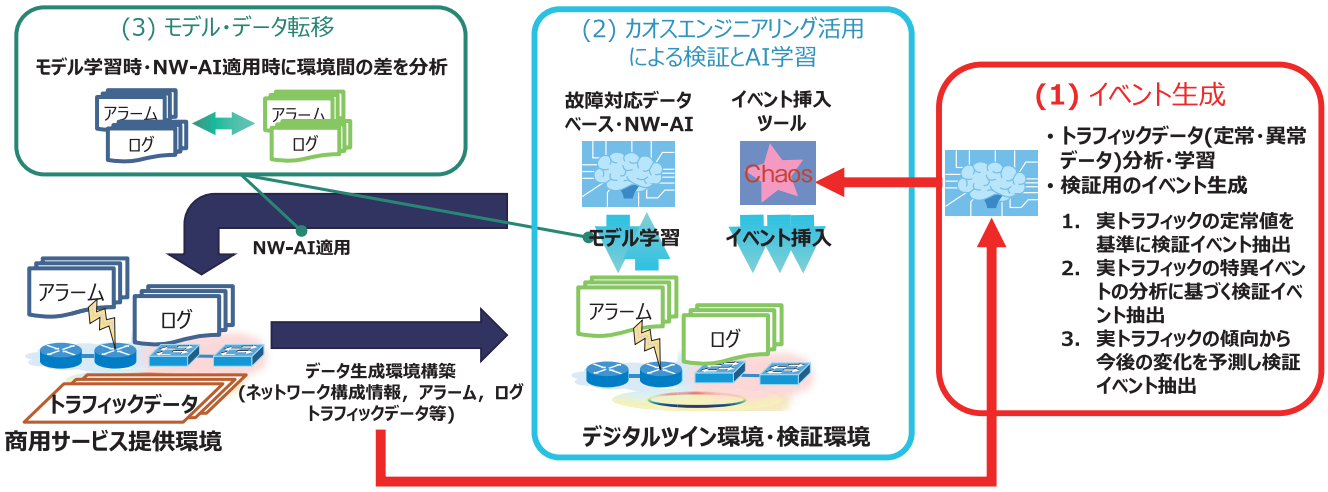


図 4　検証と運用の連携高度化フレームワーク

⑶　モデル・データ転移

類似環境は，サービス導入前に活用した検証環境やデジタル技術で構築したデジタルツイン環境を想定していますが，類似度が高いほど，より商用サービス提供環境に近い検証が可能となります．しかし，商用と検証の環境を完全に一致させることは困難なため，類似環境で学習したNW-AIのモデルやデータを，商用サービス提供環境に適用できるように転移させる技術も検討しています．

本検討の技術の詳細については，本特集記事『障害に強いロバストネットワーク実現のためのNW-AI自己進化フレームワーク』[5]で紹介します．

今後の展開

ロバストネットワークの実現に向けたオペレーション関連技術の研究開発の取り組みについて紹介しました．紹介した研究開発段階にある技術を具現化することにより，通信故障や災害に対してより強靭性の高いネットワークとそれを支えるオペレーションの実現をめざします．また，NW-AIの研究開発を加速し，高難度化が進むネットワークオペレーションを将来的に自動化・自律化する自己進化型ゼロタッチオペレーションの実現をめざします．

■参考文献

(1) 渡辺・田尻・中野：“ディープラーニングに基づく異常検知技術── DeAnoS: Deep Anomaly Surveillance,” NTT技術ジャーナル，Vol.31, No.5, pp.17-18, 2019.
(2) 佐藤・西川・深見・村瀬・田山：“ネットワーク種別に依存しない統一管理モデルを用いたサービス影響把握技術,” NTT技術ジャーナル，Vol.32, No.8, pp.51-53, 2020.
(3) 明石・金井：“大規模システム故障時の「ネットワーク状況の早期把握」,” NTT技術ジャーナル，Vol.35, No.10, pp.11-12, 2023.
(4) 松川・越地・東條：“ネットワークの強靭化を実現する設計制御技術,” NTT技術ジャーナル，Vol.35, No.10, pp.13-16, 2023.
(5) 高橋・池内・渡邉：“障害に強いロバストネットワーク実現のためのNW-AI自己進化フレームワーク,” NTT技術ジャーナル，Vol.35, No.10, pp.17-19, 2023.

（上段左から）岡本　淳／ 柴田　朋子／
田原　光穂
（下段左から）藤原　正勝／ 増田　征貴

NTT研究所では，通信故障に対し，より強靭性の高いネットワークの実現に向け，オペレーション関連技術の研究開発に取り組んでいます．今回紹介した多くの技術は研究段階にありますが，迅速に市中に出せるよう推進していきます．

◆問い合わせ先

NTTネットワークサービスシステム研究所
TEL　0422-59-6946
FAX　0422-59-6364
E-mail　tsue-mng @ ntt.com

URL　https://journal.ntt.co.jp/article/23442
DOI　https://doi.org/10.60249/23105002

大規模システム故障時の「ネットワーク状況の早期把握」

NTT研究所では，ロバストなネットワークの実現に向け，その運用を高度化する技術開発を進めています．本稿では，複雑化・多様化するネットワークサービスのネットワーク状況とサービス影響の迅速な把握を可能とする研究開発の取り組みを紹介します．

キーワード：#通信ネットワーク，#大規模，#故障

明石　和陽（あかし　かずあき）
金井　俊介（かない　しゅんすけ）
NTTアクセスサービスシステム研究所

はじめに

NTT研究所では，ネットワークシステムの故障や大規模災害への耐性が強いロバストネットワークをめざして，ネットワークの故障の発見，故障個所の切り分け，サービス影響の把握を早く正確に行い，故障が発生したときにも迅速な対応を可能とするオペレーション技術の研究開発を進めています．

本稿では，これらを実現する技術の中で，多様な通信プロトコルで構成されるネットワークを一元管理することでサービス影響の早期把握を可能にするネットワークリソース管理技術（NOIM：Network Operation Injected Model）と，ネットワークから取得したアラーム等の情報から異常検知・故障個所推定を行うAI（人工知能）技術〔DeAnoS®（Deep Anomaly Surveillance），Konan（Knowledge-based autonomous failure-event analysis technology for network）〕について紹介します．

ネットワークリソース管理技術

通信事業者のネットワークサービスは，光伝送ネットワークやイーサネットワーク，IPネットワーク等，異なる通信プロトコルを組み合わせたマルチレイヤのネットワークによって提供されています．通常，それらのネットワークは個別のシステムによって管理されているため，あるレイヤのネットワークの故障が他レイヤのネットワークやサービスに及ぼす影響は人手で分析する必要があります．しかし，大規模故障時は故障個所や影響が広範囲に及ぶため，ネットワーク状況やサービス影響の把握に長時間を要する可能性があります．

これまで私たちは，サービス影響の早期把握を実現するネットワークリソース管理技術（NOIM）の研究開発に取り組んできました[1]．本技術は，情報転送の終端点やパスなど，レイヤに依存しない汎用的なデータ形式でネットワーク情報を表現することで，多数の通信プロトコルを組み合わせた複雑なマルチレイヤネットワークを一元管理し，故障に伴うサービス影響を迅速に把握することを可能にするものです．

ネットワークリソース管理技術は，TM Forum[2]で議論されている情報フレームワーク（SID：Shared Information and Data Model）で定義されたエンティティを採用し，汎用的なデータ形式によるネットワークのリソース管理を実現します．具体的には，SIDのPhysical ResourceとLogical Resourceに規定されたエンティティを採用しています．Physical Resourceには，通信装置（PD：Physical Device），光ファイバ等の物理リンク（PL：Physical Link），それらを収容する通信ビル（PS：Physical Structure）やケーブル（AGS：Aggregate Section）など，ネットワークの物理的なリソースを表現するためのエンティティが定義されています．同様にLogical Resourceには，情報転送の終端点（TPE：Termination Point Encapsulation），情報転送が可能な領域（NFD：Network Forwarding Domain）や情報転送のパス（FRE：Forwarding Relationship Encapsulation）など，ネットワークの論理的なリソースを表現するためのエンティティが定義されています．これらの汎用的なエンティティを用いて，**図1**のように各リソースやリソース間の接続関係を表現することで，多様な通信プロトコルで構成されるマルチレイヤのネットワークの管理を可能にします．

なお，ネットワークリソース管理技術は，各通信プロトコル固有の特性を外部定義し，上記の汎用的なエンティティに紐付けて管理する機構を備えています．固有の特性には，例えばIPネットワークにおけるIPアドレスやイーサネットワークにおけるVLAN IDなどが該当します．通信プロトコルによらない共通の特性は汎用的なSIDのエンティティで表現し，通信プロトコルによる固有の特性は外部定義として追加可能にすることで，通信プロトコルやサービスの追加や変更に柔軟に対応できます．

そして，本技術によって一元管理したネットワーク情報を基に，故障が発生したときの影響を迅速に把握可能です．例えば，自然災害によって図1のようにビル間のケーブルが切断された場合を考えます．このと

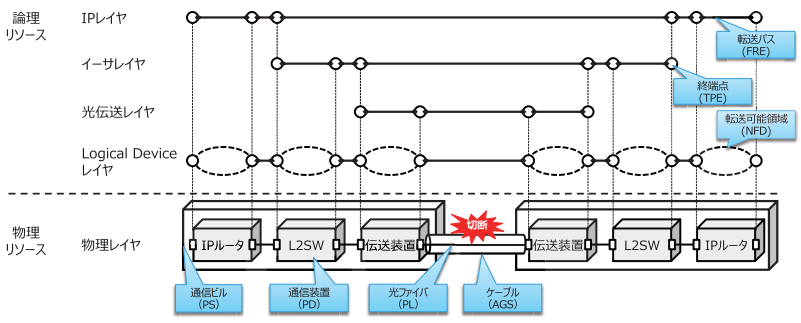


図1　汎用エンティティによるマルチレイヤのネットワークリソース管理

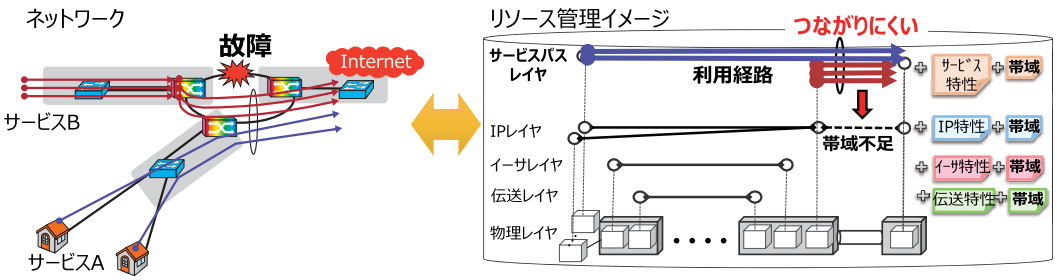


図 2　大規模故障対応支援に向けたネットワークリソース管理技術の拡張

き，そのケーブルに収容されている光ファイバ，ならびに，光ファイバ上の各レイヤの論理リソースが故障の影響を受けます．ネットワークリソース管理技術により各リソース間の関係を保持しているため，それらの関係を辿ることで，ケーブル故障の影響を受ける物理リソースや論理リソースを容易に判定できます．なお，この判定ロジックは，ケーブル（AGS），光ファイバ（PL），情報転送の終端点（TPE）やパス（FRE）といった汎用的なエンティティに基づくものであるため，ネットワークのレイヤ構成が変わった場合もロジックを変更する必要がありません．

一方，自然災害によるケーブル切断やビル停電等と異なり，ネットワークシステムの故障では，ネットワークの一部の通信が不安定になりサービスがつながりにくくなる事象が発生します．このような事象において，システム故障の影響エリアや利用者数を正確に把握するには，各サービスのトラフィックが流れている経路や通信が不安定な経路を考慮して，サービス影響を判定する必要があります．そこで，私たちは大規模故障対応支援に向けて，ネットワークリソース管理技術について以下の拡張に取り組んでいます（**図 2**）．

⑴　サービスパスレイヤの追加

より細かい粒度でサービスの影響を把握可能にするために，通信プロトコルごとのレイヤに加えて，サービスパスレイヤを追加します．このレイヤのリソースは，ネットワーク上で提供されるサービスのエンド・ツー・エンドの接続を表現します．従来は，通信プロトコルとおおむね同等の粒度でサービス影響を判定していましたが，サービスパスレイヤの追加によりエリア単位やユーザ単位といった任意の粒度でのサービス影響把握を可能にします．

⑵　サービスの利用経路を考慮した影響把握

ネットワークシステムの故障によりつながりにくくなっているサービスを把握するために，各サービスのトラフィックが通信の不安定な経路を流れていないかを考慮した判定を行います．各サービスの利用経路（リソース）を汎用的なエンティティで表現し，それらのリソースの故障状況に基づいて影響を判定することで，つながりにくくなっているサービスを把握します．

⑶　不安定な経路の把握

通信が不安定になっている経路を把握するために，各サービスの必要帯域や利用経路情報を基にした判定を行います．各レイヤのリソースに帯域情報を追加し，各サービスの帯域と利用経路のリソースの帯域を比較することで，帯域逼迫により通信が不安定になっている経路を把握できます．ただし，ネットワークが不安定になる要因は帯域逼迫に限らないため，上記の方法に限らず他の技術も活用し，不安定な経路を把握することが必要です．

異常検知・故障個所推定 AI 技術

ネットワークの故障の早期発見，故障個所の迅速な切り分けを実現するために，アラーム等のネットワーク情報から異常検知・故障個所推定を行う AI 技術の研究開発にも取り組んでいます．

- DeAnoS®：潜在的な性能劣化リスク（故障・輻輳等）や需要変化を予見的・早期に検知し，事前の制御，早期・自動復旧を行う「プロアクティブ制御型ネットワーク」をめざす技術です．
- Konan：マルチレイヤのネットワーク故障個所の推定を可能とする技術です．ネットワーク上で故障が起きた際のアラーム等の発生状況をルールとして学習します．故障発生時のアラーム情報とネットワーク構成情報ならびに学習したルールに基づいて物理装置の故障個所だけでなく，論理構成上の故障個所を推定し，効率的に故障の原因となった個所の候補を導出します．

おわりに

本稿ではロバストネットワークを実現するためのオペレーション技術について解説しました．NTT 研究所では個々の技術開発だけではなく，それらの技術群の容易な連携・導入をめざしたゼロタッチオペレーションフレームワークの研究開発も推進し，さらなるネットワーク状況の早期把握ならびに復旧対応の迅速化に貢献していきます．

■参考文献

⑴ 佐藤・西川・深見・村瀬・田山：“ネットワーク種別に依存しない統一管理モデルを用いたサービス影響把握技術，” NTT 技術ジャーナル，Vol.32, No.8, pp.51-53, 2020.
⑵ https://www.tmforum.org/


（左から）　明石　和陽／　金井　俊介

NTT アクセスサービスシステム研究所は，ネットワークリソース管理技術を検討・研究し，多様化・複雑化している社会課題をオペレーションの観点で解決していくことで「つながり続けるネットワーク」の実現に貢献していきます．

◆問い合わせ先

NTT アクセスサービスシステム研究所
アクセスオペレーションプロジェクト
E-mail　ohoug-noim @ ntt.com

URL　https://journal.ntt.co.jp/article/23444
DOI　https://doi.org/10.60249/23105003

ネットワークの強靭化を実現する設計制御技術

NTT研究所では，大規模な災害や障害に対してネットワークのさらなる強靭化を実現するためのネットワーク設計制御技術の研究に取り組んでいます．大規模な災害に対しては，伝送ルートの耐災害性・耐障害性を高めるための研究開発を進めています．また，大規模な故障に対しては，故障の長時間化や大規模化を防ぐための強靭な制御プレーンアーキテクチャの検討を進めています．そして，端末・クラウドとの連携まで実施することによって，ユーザレベルのコネクティビティを向上させる技術について検討しています．本稿では，これら3つの技術について紹介します．

キーワード：#冗長設計，#信号制御，#マルチパス制御

松川　達哉（まつかわ　たつや）
越地　弘順（こしぢ　こうじゅん）
東條　琢也（とうじょう　たくや）

NTTネットワークサービスシステム研究所

エンド・ツー・エンドの信頼性設計

お客さまに常に安定的にネットワークサービスを提供するためには，エンド・ツー・エンドでネットワークの信頼性を高めることが必要です．アクセス網・伝送網・コア網，さらには端末やクラウドサービスも含めてトータルの信頼性を維持・向上させることが重要です（**図1**）．NTT研究所では，設計フェーズにおいてネットワークの信頼性を評価しサービス開始後の運用業務に役立てる技術の研究を進めてきました．一方で，大規模な災害の発生によって長期間通信サービスが利用できない状況やネットワークの障害によって多数のお客さまのサービス利用に影響する事例も発生しています．大規模な災害に対しては，ネットワークを冗長化することで災害の影響を減らすための高度な設計技術が重要となります．また，大規模な障害の対策としては，制御機能を含めて輻輳等の事象を回避する仕組みをネットワーク内に配備することが必要となります．そして，網内の機能に加えて端末やクラウドと連携することで，さらにネットワークを強靭化することが必要と考えています．ネットワークの設計や制御によって災害や障害からネットワークサービスを守るだけでなく，網外の機能やシステムとも連携してリソースを確保することでネットワークのサービスレベルを柔軟に高めることができます．

本稿では，ネットワークの信頼性向上を図るためのエンド・ツー・エンドの信頼性設計として，ネットワークの冗長化，制御プレーンの強靭化，エンド・ツー・エンド通信のロバスト化について紹介します．

冗長ルート設計によるネットワークの高信頼化

ネットワークの高速・大容量化，低遅延化が進む中で，ネットワークに求められる信頼性の要求条件はますます高まっています．特にネットワークの基盤となる伝送ネットワークは多数のユーザやサービスを収容しているため，故障の発生によってサービスが中断すると影響は甚大となります．そこで，設備の冗長化や分散配備等の信頼性対策を組み合わせて実施することで高い信頼性を確保することが重要となります[(1)]．

伝送ネットワークは，災害や障害等のネットワーク外の要因によって損傷する可能性があるため，あらかじめリスク要因を把握し，リスクを避ける物理的なルートを設計することが重要です．また，予備ルートを設定し，万が一の際の代替手段とすることで通信を継続させることが重要です．通常，ネットワークの冗長度を高めることで故障時のサービス影響を最小にしていますが，伝送ルートの耐災害性はルートの長さや形状，地理的配置に依存しています．現用・予備ルートそれぞれが災害に強いことに加えて，災害時にもいずれかのルートが正常に機能することが重要です．そこで，NTT研究所では以下の2つの要件を検討しました．

1番目の要件は，現用・予備系ルート自

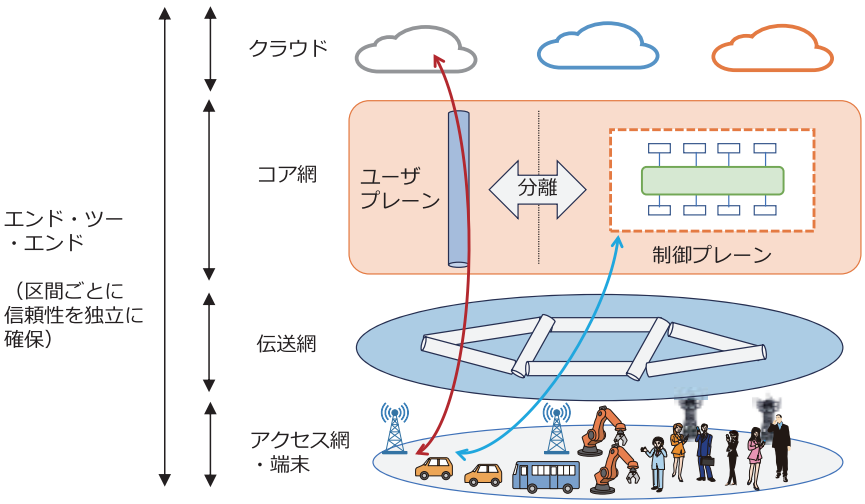


図1　エンド・ツー・エンドの信頼性

体の耐障害性や耐災害性が高いことです．例えば，ルートの長さが短いほうが災害の影響を受けにくく，経由する装置が少ないほうが故障に遭遇する確率も小さくなります（**図 2** ①）．この場合には，ルートの距離や経由装置数を少なくすることが重要となります．また，災害対策用に施工された設備を優先的に選択することで，耐災害性の高いルートを設計することができます（図 2 ②）．この場合は，設計の対象となる対地間において，経由する，あるいは非経由とする通信ビルやリンク等のネットワーク設備を指定してルートを選択する手順が必要となります．

2 番目の要件は，現用ルートにおいて災害や障害発生時にも予備ルートが正常に機能することです．例えば，2 つのファイバルートが同じ管路の中に収容されていると，管路に障害が発生した際に，両方のファイバが損傷するリスクがあります（図 2 ③）．1 件の故障の発生が両ルートに影響を及ぼすため，サービス断につながるリスクになります．共用するネットワーク設備が多いほどリスクが大きく，冗長性が低いとみなします．同一のリスクを複数のネットワーク設備が共用している状態を示す概念として SRLG（Shared Risk Link Group）が知られており，現用ルートと予備ルートが同時的に故障するリスクを考慮してルートを選択することが重要となります．また，現用ルートと予備ルートが物理的に離れていても，地震や洪水等の災害予想区域が両ルートをまたがっていると，災害発生時に両ルートが被災する可能性があります（図 2 ④）．そこで同時に複数の設備に影響するような災害や障害を共有リスクと定義し，リスクを共有する設備に同じリスクグループの ID を付与することで，共有リスクを回避したルートの探索が実行できるようになりました．

ネットワークにおいて最短距離となるルートを探索する手法としてはダイクストラ法等，多数の既存手法があります．一方で，上記の 2 つの要件を満たすルート探索技術は検討されていませんでした．そこで NTT 研究所では，2 つの要件を満たすルートを探索するためのアルゴリズムを検討しシミュレーションによる検証を実施しました．

要件 1 については，指定した対地間の k 本のルートをルートに対するコスト（距離）が小さい順に求めるヒューリスティック解法である k-SPF(Shortest Path First) アルゴリズムを用いた方法について検討しました[(2)]．また，要件 2 については，現用・予備ルートの探索方法について，管路や災害予想区域等の SRLG に ID を付与し，ID を重複しないように現用・予備のルートを生成する手順を考案しました[(3)]．従来の研究[(4)]では，経由地を指定して探索することや始終点間に複数の現用・予備ルートを生成することは想定されていませんでした．従来の研究結果を用いて上記の要件を満たすルートを探索すると計算量が膨大になってしまうため計算に大量のメモリが必要になり，メモリ量が不足すると探索の過程で本来導出すべきルートの候補が得られない可能性があることが分かりました．そこで，現用・予備ルートの探索アルゴリズムにおいて始点と経由地点，経由地点と終点，終点と経由地点，というように探索区間を分割し，始点から経由地点，終点，そして再度始点に戻る順番に探索する方法について検討しました．この方法では，ルート探索を進める中で同じルートを選択しないように探索する対象を絞ることができるため探索する範囲を削減することができます．**図 3** は，提案手法と従来手法を比較した結果の例を示しています．現用・予備系の候補ルート数と経由地を指定した合計数に対する最適なルートの計算結果を表として示しています．既存の方法では，設備数に対して空間計算量（計算に必要となるメモリ量）が指数関数的に増加しますが，提案方法では多項式時間に抑えることができるため，実用上も有効な方法であるということができます．提案するアルゴリズムによってメモリの使用量を抑えることができるため，実際の設計業務に活用することが期待できます．

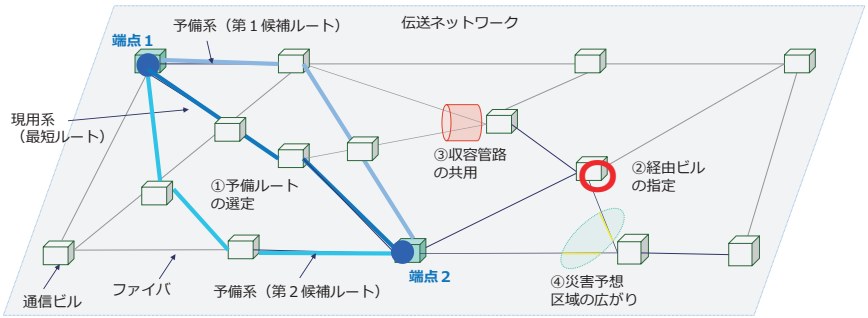


図 2　伝送網における冗長ルート設計

経由地指定の合計数

現用系・予備系ルート候補数	1	2	3	4	5
5	●	●	●	●	●
10	●	●	●	●	●
20	○	○	○	●	●
30	○	○	○	●	●
50	○	●	●	●	●
100	○	●	●	●	●

候補数の設定値が小さいため，従来の手法では適切なルートが解として得られない（●）

従来の手法では適切なルートが解として得られない場合あり（●）

従来の手法でも適切なルートが解として得られた（○）

計算量の増大により，従来の手法ではメモリエラーが発生し処理が完了しない（●）

図 3　提案手法と従来手法の比較例

信号制御バスによる制御プレーンの強靭化

昨今の大規模な通信障害として，移動体通信網において発生している複数の事例が挙げられます．移動体通信網における大規模な通信障害の共通的な原因や特徴としては，①位置登録処理等の高負荷を起点として障害が発生していること，②制御機能の障害がネットワークの輻輳を引き起こしネットワーク全体に波及することで障害が大規模化すること，③データベースの処理に影響が波及しデータの不整合等の問題が発生するとさらに復旧が長期化することが挙げられます．これらの課題については，電子情報通信学会でも関連する論文が発表されています[5]．また，2023年6月に開催された3GPP（3rd Generation Partnership Project）のワークショップにおいても，移動体通信網のコアネットワークの強靭化については課題として提起されており，通信キャリア・ベンダ含めて今後の対策が議論されていく予定です[6]．そこで，NTT研究所では，制御プレーンの強靭化をめざしたアーキテクチャの検討を進めています[7]．ネットワークの制御機能群を構成する信号制御バスを配備し，ネットワーク機能間の信号のやり取りを管理・制御することを検討しています（**図4**）．信号制御バスの特徴としては，制御プレーンとユーザデータプレーンを分離すること，また，制御プレーンについては，SBA（Service Based Architecture）に基づきアプリケーション特性に応じた機能追加やアプリケーションの開発サイクルに合わせたタイムリーな機能追加を実現することです．また，ユーザからのアクセスの集中や処理負荷が高まった状況においては自動的にリソースを追加することで，処理性能の低下を回復する機能を検討しています．さらに，機能間をつなぐ制御バス自体についても冗長化や自動的なリソース追加を可能とすることで，信号輻輳等の影響を回避することが可能となります．3GPPにおいては，同様のコンセプトを持つ機能としてSCP（Service Communication Proxy）が提案されています．NTT研究所では，信号輻輳が発生した際の対応をより柔軟にするための追加的な機能として，サービスや端末の種別，信号制御バス内の信号量に応じた信号制御方式を検討しています．今後，携帯端末だけでなく，IoT（Internet of Things）機器等がさらに増加していくことが予想されますが，端末・機器に応じた信号の制御を実施することで，万が一の際にも優先度の高い通信接続を維持する，あるいはネットワーク内の信号量を削減することで輻輳の影響を緩和することができると考えています．

ネットワーク内の障害や異常を検知し，その影響を迅速に緩和するためには，上記の信号制御バスのアーキテクチャにおいて，障害個所や異常の原因を見える化する，また，素早く予兆検知を実現する仕組みが必要です．ネットワーク内でサービスの異常を検知する仕組みとしては，ネットワーク内の各機能部に異常を検知するためのプローブを配備し，異常を検知した際に信号制御機構に通知する機能を検討しています．ネットワーク内で異常の検知と通知，機能間で連携した制御までを完結することでより迅速な対処を実現することができると考えています．

マルチパス制御技術によるエンド・ツー・エンド通信のロバスト化

NTT研究所では，網内のロバスト化に加えて，端末～クラウド・MEC（Multi-ac-

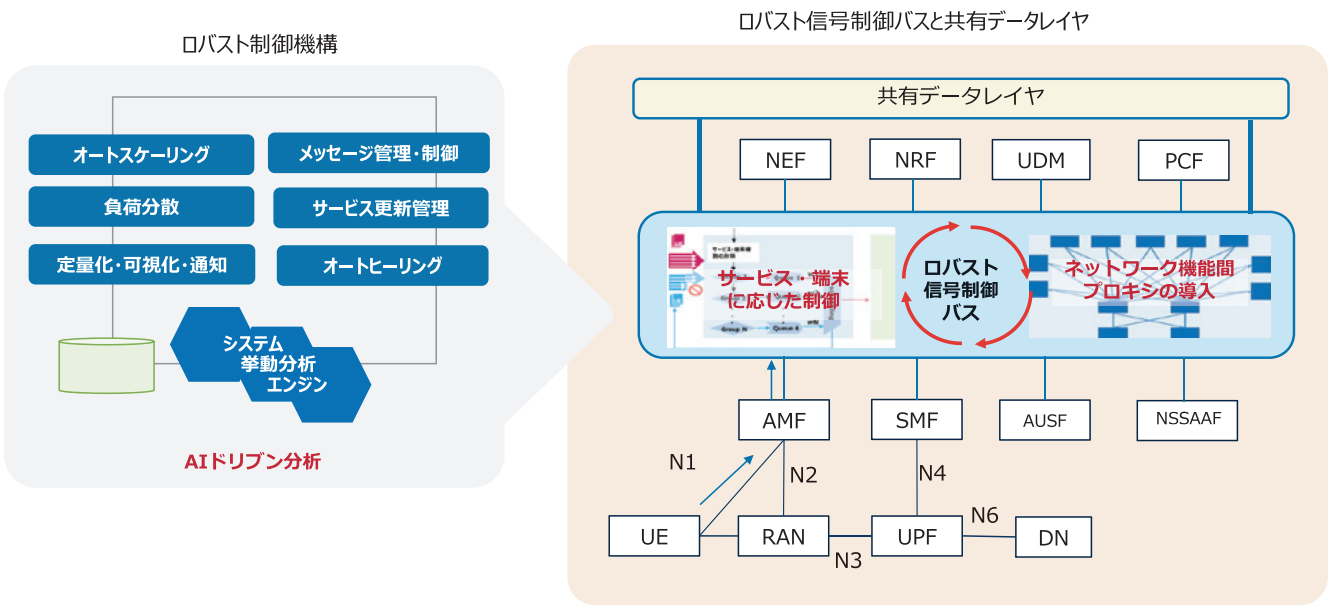


図4　ロバスト信号制御・アーキテクチャ

cess Edge Computing）間において複数のネットワークを使用してエンド・ツー・エンドでロバスト性を高めるマルチパス通信にも取り組んでいます．マルチパス通信は，端末やサーバ間で複数の経路を持つ通信形態であり，異なる通信事業者のモバイル網やローカル5G（第5世代移動通信システム）とキャリア5Gのような特性の異なるネットワークを組み合わせて使用することで，あるネットワークにおける障害の発生，無線の電波状況の悪化等による通信断が起きた際に，正常なネットワークもしくは電波状況の良いネットワークで通信を行うことで，影響を最小限にすることができ，ロバスト性を高めることが可能となります．マルチパス通信においてロバスト性の効果を高めるためには，複数のネットワークを使い分ける制御技術が重要です．NTT研究所ではミッションクリティカルサービスを実現する協調型インフラ基盤[8]に取り組んでおり，端末とクラウド・MECをつなぐマルチパス通信技術として協調マルチパス機能の検討を行っています（**図5**）．協調マルチパス機能は，ユーザやアプリケーションの要求条件に応じて最適なマルチパス通信を提供する制御機能です．具体的には，①平常時は特定のネットワークのみを使用して障害時にネットワークを切り替える動的ネットワーク切替，②パケット単位の振り分けにより複数のネットワークを同時に使用するアグリゲーション，③パケットのコピーを複数のネットワークに送信する冗長化転送の3つのマルチパス通信方式を提供します．ロバスト性の向上としてはどの方式も効果が見込めますが，遅延・帯域・信頼性の点でそれぞれ得られる効果が異なります．動的ネットワーク切替では，平常時は同じネットワークを使用し続けるため遅延やジッタ等のネットワーク品質は安定していることが期待できます．アグリゲーションは，異なるネットワークを使用することで遅延やジッタが変動する可能性がありますが，使用できる帯域の増加が期待できます．冗長化転送は，同じパケットを複数送信するため帯域の利用効率は悪くなりますが，パケットロスへの耐性があり，かつ受信側で先に届いたパケットを処理することができるため遅延の短縮化が期待できます．協調マルチパス機能は，端末とクラウド・MECの協調制御を行う協調制御ゲートウェイと連携し，ユーザやアプリケーションの要求条件とネットワークの通信状態に応じて，適切なマルチパス通信を提供します．

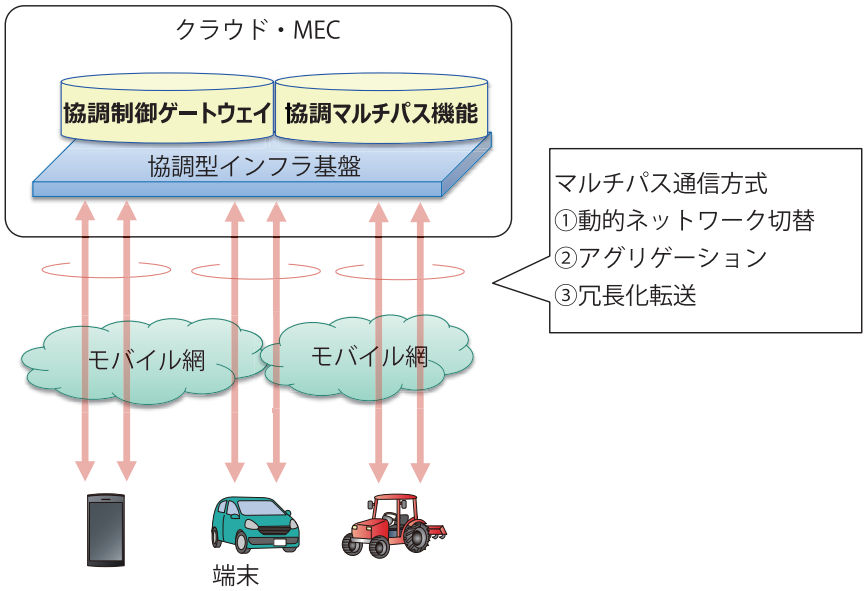


図5　協調型インフラ基盤のマルチパス制御技術

■参考文献

(1) https://www.ntt-east.co.jp/saigai/taisaku/setsubi_01.html
(2) 松浦・越地・金子・横井・松川・藤井・宮村："k-SPFアルゴリズムによる光ネットワーク上での冗長経路設定，" 電子情報通信学会ソサイエティ大会，B-12-2, 2022.
(3) 松浦・越地・金子・横井・松川・藤井・宮村："k-SPFアルゴリズムを用いたSRLGディスジョイントな光冗長経路選択，" 電子情報通信学会NS研究会，NS2022-164，2023.
(4) Y. Yang, H. Mi, and X. Zhang："A Minimum Cost Active and Backup Path Algorithm with SRLG Constraints," Proc. of ICICSE 2012, April 2012.
(5) 春日・中尾："5Gモバイルコアにおける多数接続の輻輳を軽減する制御プレーンスライシング，" 信学技報，Vol. 122, No. 198, NS2022-93, pp. 76-81, 2022.
(6) https://www.3gpp.org/ftp/tsg_sa/TSG_SA/Workshops/2023-06-13_Rel-19_WorkShop/Docs/
(7) https://www.rd.ntt/ns/inclusivecore.html
(8) 桑原・石橋・川上・益谷・山本・安川："ミッションクリティカルなサービス提供を可能とする協調型インフラ基盤，" NTT技術ジャーナル，Vol. 33, No. 8, pp.29-33, 2021.



（左から）　松川 達哉／ 越地 弘順／
東條 琢也

◆問い合わせ先

NTTネットワークサービスシステム研究所
ネットワーク基盤技術研究プロジェクト
TEL　0422-59-3445
E-mail　network-design-ml @ ntt.com

URL　https://journal.ntt.co.jp/article/23448
DOI　https://doi.org/10.60249/23105004

障害に強いロバストネットワーク実現のための NW-AI自己進化フレームワーク

NTT研究所では，ネットワーク障害の早期復旧のためにAI（人工知能）を用いたゼロタッチオペレーションの研究開発に注力しています．AIを用いたネットワークオペレーションを実現するためには，大量のネットワーク障害データを学習することが必要となります．私たちは，疑似環境の中で大量のネットワーク障害を人為的に生成し，それらへの対応方法を学習させることで，AIを自律的に学習させるフレームワークを確立しました．本稿では，提案フレームワークのコンセプトとフレームワークの中でAIがどのように学習していくかを解説しています．

キーワード：#AIの自己進化，#カオスエンジニアリング，#デジタルツイン

高橋　洋介（たかはし　ようすけ）
池内　光希（いけうち　ひろき）
渡邉　暁（わたなべ　あきお）

NTTネットワークサービスシステム研究所

はじめに

NTT研究所は，予期せぬ障害に強いロバストネットワークの実現をめざしています．この目標を達成するために，私たちはネットワーク運用業務の自動化に取り組み，AIを活用したゼロタッチオペレーションの研究開発を進めています．この取り組みの中心には，私たちがNW-AIと呼んでいる，ネットワークの運用を担うAI（人工知能）があります．

ゼロタッチオペレーションでは，人間の介入を最小限に抑え，NW-AIがネットワークの運用と管理を行います．具体的には，NW-AIは異常検知や障害個所の推定といったタスクを自動で実施します．例えば，NW-AIはネットワークにおける通信パターンやパフォーマンスデータを監視し，ネットワークの異常を検知することができます．また，障害が発生した場合，NW-AIはネットワークのトポロジ情報と膨大なログデータを分析することで，その原因となる個所を推定することができます．

このような取り組みの中で，特に難易度が高い課題として，NW-AIによるネットワーク障害の自動復旧が挙げられます．ネットワーク障害の自動復旧は，ネットワークの安定性とサービスの品質を保つために重要な要素であり，その実現はゼロタッチオペレーションの成功にとって不可欠です．

NW-AIによる自動復旧を実現するためには，NW-AIが障害時のパフォーマンスデータやログデータを大量に学習することが必要となります．これにより，NW-AIはさまざまな障害シナリオに対応する能力を獲得し，障害が発生した際に迅速かつ効率的に対応することが可能となります．

しかし，一般的な運用範囲を逸脱した条件下で発生する想定外障害については発生頻度が低いため，十分なデータを収集することが困難であり，その結果，NW-AIにこれらの障害への対応を適切に学習させることは難しいという問題があります．想定外障害は復旧手順が確立されていないため，復旧に長い時間がかかり，ユーザに深刻な影響を及ぼす可能性があります．想定外障害は一般的な運用範囲を逸脱した条件下で発生しますが，人力でこのような発生条件を探索するには莫大な時間と労力がかかるため現実的ではありません．

NTT研究所では，このような課題に対応するために「検証と運用の連携高度化」を実現する研究開発に取り組んでいます．具体的には，ネットワークのデジタルツイン環境と人為的な障害生成を可能にするカオスエンジニアリングツールを組み合わせることにより，さまざまな障害への対応をNW-AIが自律的に学習し続けるフレームワークを構築しました．このフレームワークでは，カオスエンジニアリングツールをデジタルツイン環境上で動作させることで，さまざまな種類の障害を発生させて，対応方法をNW-AIに学習させます．このプロセスを長期間にわたって自動実行させて膨大な量の障害を発生させることで，通常の運用範囲では起こり得ない障害についてもデータを収集することが可能となります．このように，NW-AIを自己進化させて，対応できるネットワーク障害を増やすことで想定外となる障害を極小化することが可能となります．

NW-AI自己進化フレームワークのコンセプト

NW-AI自己進化フレームワークのコンセプトを**図1**に示します．このフレームワークは，現実のネットワークを模倣したデジタルツイン環境をつくり出し，その環境上で人為的に障害状況を発生させることで，NW-AIの学習に必要な障害データを収集します．この障害状況の発生には，カオスエンジニアリングツールを使用します．

カオスエンジニアリングは，システムの弱点を発見し，それを修正することでシステムの耐久性を向上させるための実験的なアプローチです．これは，意図的にシステムに障害を引き起こし，その結果を観察することで行われます．このアプローチの目的は，システムが予期しない問題や障害にどのように対応するかを理解し，それによってシステムの弱点を特定し，改善することです．カオスエンジニアリングツールは，このプロセスを自動化し，管理するためのソフトウェアです．

カオスエンジニアリングツールを使用することで，現実のネットワーク環境では発生頻度の低い障害事例や，まだ発生したことのない障害事例についても，デジタルツ

イン環境で発生させてデータを収集することが可能となります．NW-AIはこれらのデータを学習することで，障害への対応方法を学習します．

このようにして大量のデータを学習したNW-AIを現実のネットワーク環境で動作させることで，ネットワーク障害からの自動復旧を実現します．

NW-AI自己進化フレームワークを用いた自動復旧AIの構築

ここではNW-AI自己進化フレームワークで自動復旧AIを構築する場合の処理をステップごとに説明します[(1)～(3)]．本フレームワークを用いて自動復旧AIを構築する場合のアーキテクチャを**図2**に示します．

本フレームワークはAIエージェントと環境から構成され，その動作はすべてスクリプトで自動化できます．AIエージェントと環境は相互作用し，復旧方策は以下のステップに従って自律的に構築されます．

①　障害の挿入

このステップでは，カオスエンジニアリングツールを用いて，対象システムにさまざまな障害を挿入します．障害の挿入は，システムの弱点を明らかにし，その対策を

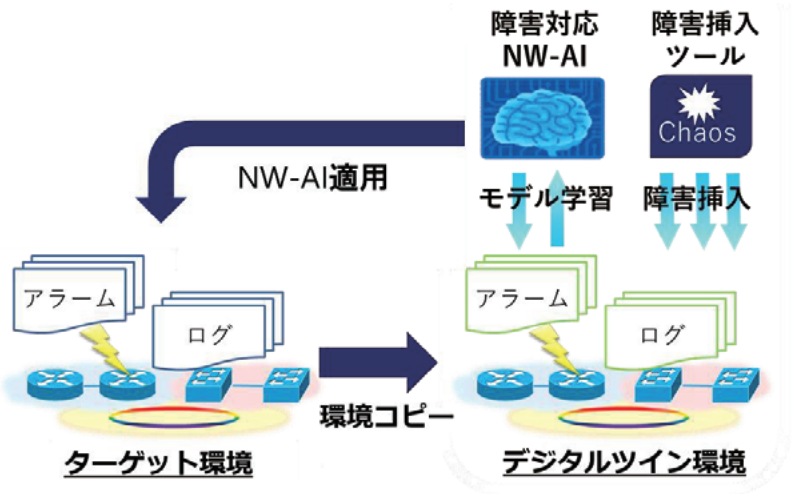


図1　NW-AI自己進化フレームワークのコンセプト

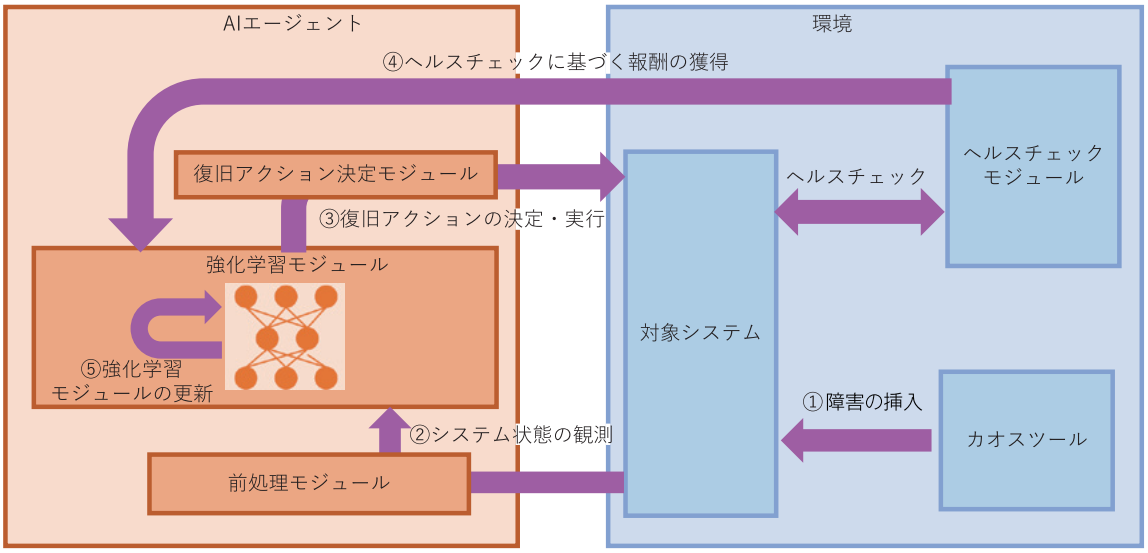


図2　NW-AI自己進化フレームワークによる自動復旧AIの構築

練るための重要なプロセスです．本フレームワークでは，頻繁に発生する障害だけでなく，発生頻度は低いが発生した場合には重大な影響を及ぼす可能性のある障害も挿入します．これにより，システムがさまざまな障害状況に対応できるようになります．

② システム状態の観測

このステップでは，AIエージェントが対象システムの状態を観測し，その情報を収集します．具体的には，一定の時間枠内にシステムから生成される各種メトリクスやログなどのデータをエージェントが収集します．これらのデータはシステムのパフォーマンスや状態を示す重要な指標であり，エージェントがシステムの現状を理解し，適切な行動を決定するための基盤となります．

③ 復旧アクションの決定・実行

このステップでは，観測データと過去の学習結果を基に強化学習モジュールが最適な復旧アクションを決定し，実行します．復旧アクションは，システムの異常状態を正常に戻すための具体的な行動で，その内容は観測データや現在のシステム状態に基づいて決定されます．例えば，特定の装置の障害が観測された場合，復旧アクションとしてその装置の再起動が選択されます．一方，ネットワーク経路に問題が検出された場合には，経路の再設定が行われます．

④ ヘルスチェックに基づく報酬の獲得と新たなシステム状態の観測

このステップでは，ヘルスチェックモジュールがシステムの状態を監視し，その結果に基づいてAIエージェントに報酬が与えられます．報酬の設定は，システムの状態が正常に近いほど高くなるように調整され，これによりエージェントはシステムの正常化をめざす行動を学習します．ヘルスチェックモジュールによる監視と報酬の設定は，エージェントがシステムの状態を適切に理解し，最適な行動を選択するための重要なフィードバックメカニズムとなります．

⑤ 強化学習モジュールの更新

このステップでは，エージェントが観測したシステム状態，選択した復旧アクション，得られた報酬，そして新たに観測したシステム状態の組合せを利用して，強化学習モジュールの更新を行います．エージェントはこれらの情報を記憶し，それらを学習データとして使用します．具体的には，エージェントは選択したアクションがシステム状態をどのように変化させ，それがどの程度の報酬につながったのかを学習します．これにより，エージェントは同様のシステム状態が発生した際に，より良い結果を得るためのアクションを選択する能力を向上させます．この強化学習モジュールの更新は，エージェントがシステムの状態とその変化を理解し，最適な行動を選択するための重要なプロセスです．これにより，エージェントは継続的に学習と進化を行い，システムの効率と安定性を向上させることが可能となります．

今後の展開

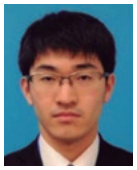
本稿では，障害に強いロバストネットワーク実現のためのNW-AI自己進化フレームワークと本フレームワークを活用した自動復旧AI構築について紹介しました．今後の展開としては，NW-AI自己進化フレームワークを用いて自動復旧を含めた各種オペレーションを自動実行するNW-AIを学習させ，障害が発生した際の迅速な自動対処を可能とすることで，障害に強いロバストネットワークの実現をめざしていきます．

■参考文献

(1) H. Ikeuchi, J. Ge, Y. Matsuo, and K. Watanabe：“A Framework for Automatic Failure Recovery in ICT Systems by Deep Reinforcement Learning,” IEEE ICDCS, pp. 1310-1315, Nov. 2020.

(2) H. Ikeuchi, Y. Takahashi, K. Matsuda, and T. Toyono：“Recovery Process Visualization based on Automaton Construction,” IFIP/IEEE IM, pp. 10-18, May 2021.

(3) 池内・葛・松尾・渡辺：“障害データ生成に基づく要因特定手法の一検討，” 信学会総合大会，B-7-32, 2020.


（左から） 高橋 洋介／ 池内 光希／ 渡邉 暁

障害に強いロバストネットワーク実現のためのNTT研究所の取り組みについて，お伝えできれば幸いです．

◆問い合わせ先

NTTネットワークサービスシステム研究所
通信トラヒック・品質・オペレーション研究プロジェクト
TEL 0422-59-7822
FAX 0422-59-6364
E-mail tsue-mng @ ntt.com

URL　https://journal.ntt.co.jp/article/23450
DOI　https://doi.org/10.60249/23105005

主 役 登 場

高信頼で強靭なネットワークをめざして

高 橋　洋 介　Yosuke Takahashi

NTTネットワークサービスシステム研究所
主任研究員

インターネットは今や，私たちが生活する社会にとって欠かすことができない基盤となっており，その信頼性と強靭性が絶えず求められています．信頼性とは，いつでも必要な情報にアクセスでき，必要なサービスを利用できるという安定性のことです．強靭性とは，さまざまな問題や障害が発生したときでも，その影響を最小限に抑え，迅速に復旧できる能力のことです．これらは，私たちが日々の生活をスムーズに，そして安心して過ごすためには欠かせない要素となっています．

しかし，社会の変化に伴い，このインターネットの信頼性と強靭性を維持することは，日々難しさを増しています．その理由の1つとして，インターネットを基盤としたサービスの急速な増加が挙げられます．新たなサービスが次々と生まれ，それぞれがネットワーク事業者の想定外のトラフィックを発生させることでネットワークの負荷が高まり，安定したサービス提供が難しくなることがあります．さらに，ネットワークの高速化・高機能化に伴い，ネットワークを構成するハードウェアやソフトウェアもまた複雑化しています．この結果，予期せぬハードウェアの故障やソフトウェアのバグが原因でネットワークがダウンしてしまう事態も発生しています．

私たちの研究グループでは，増え続けるネットワークの複雑性に対応するため，AI（人工知能）を活用したネットワークオペレーションの研究開発を推進しています．具体的には，AIを用いたゼロタッチオペレーションの研究に力を入れています．ゼロタッチオペレーションとは，人間の介入を最小限に抑え，NW-AI によってネットワークの運用と管理を行うことを指します．例えば，ネットワーク障害の発生時に人間が介入して復旧作業を行うのではなく，NW-AIが大量の運用データを分析・監視することで，自動で「障害発生の検知」，「障害個所の特定」，「障害からの復旧処理」を実施することができれば，より迅速かつ正確な対応が可能となります．私たちのめざすネットワークは，自己診断し，自己修復する能力を持つことで，高い信頼性と強靭性を併せ持つことができるものです．

AIを用いたゼロタッチオペレーションを実現するためには，ネットワーク障害発生時の運用データを大量に用いて，NW-AIに障害発生時の対応を学習させる必要があります．しかし，実環境ではネットワーク障害が生じる機会が少ないため，AIの学習に必要となるデータを十分に収集することが困難であるという課題があります．そこで，私たちの研究グループでは，ネットワークのデジタルツイン環境の中で人為的にさまざまなネットワーク障害を発生させ，NW-AIがそれらへの対応方法を自律的に学習できる「NW-AI自己進化フレームワーク」を検討しています．これにより，実環境でのネットワーク障害の発生を待つことなく，NW-AIの学習を進めることが可能となります．

私たちの研究グループが開発してきたAIを活用したゼロタッチオペレーションの一部は，すでにグループ会社との共同検証を経て，実際のネットワーク運用業務に導入されつつあります．現場での運用を通じて，新たな課題が見つかることもあります．例えば，特定の種類のネットワーク障害に対するNW-AIの対応がまだ不十分である，といった具体的な問題点が明らかになることもあります．それらは私たちにとって貴重なフィードバックであり，それらの課題を解決することで私たちの技術はさらに洗練され，実用性を増していきます．この一連のプロセスは，一度で完結するものではなく，新たな課題の発見とその解決のサイクルを繰り返すことで，より実践的な技術へとブラッシュアップしていきます．このプロセスを通じて，私たちは学び続け，技術を磨き続けています．

高信頼で強靭なネットワークを実現するためにはまだまだ解決しなければならない課題が多く，その道のりは決して容易ではありません．それでも，今後ますます重要性を増していくインターネットという社会インフラを支える研究開発に携わることには，私自身大きなやりがいを感じています．これからもNTTグループの一員として，そしてネットワーク研究者として，私はこの目標に向かって尽力していきます．私たちの研究が社会全体の利益となり，より高信頼で強靭なネットワーク環境の実現に貢献することを願っています．

特集2

NTTテクノクロスのセキュリティ技術・ビジネスの最新動向とSBOMへの取り組み

本特集では，NTTテクノクロスが取り組んでいる，
セキュリティ関連の最新標準化動向とそれに対応するコンサルティング，
パーソナルデータ利活用促進に向けた匿名化・合成データ生成技術にかかわる取り組み，
ブロックチェーン技術に基づいたVCへの取り組みとその1つのユースケースとして，
SBOMへの応用を紹介する．

セキュリティ標準化

匿名加工技術

合成データ生成技術

ブロックチェーン技術

SBOM

NTTテクノクロスにおけるブロックチェーン技術に基づいたVCへの取り組みとそのSBOMへの応用 30

NTTテクノクロスでは，ブロックチェーン技術を活用したサプライチェーン関連のシステム開発を通じて，VC（Verifiable Credentials）データモデルに着目し，サプライチェーンのモデルに適した階層型VCという技術を考案した．その応用先として，SBOM（Software Bill of Materials）への適用を検討しており，ソフトウェアサプライチェーン全体での安全性向上をめざしている．

URL　https://journal.ntt.co.jp/article/23454
DOI　https://doi.org/10.60249/23105101

セキュリティ関連の最新標準化動向とコンサルティング

NTTテクノクロスでは，ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission）やITU-T（International Telecommunication Union - Telecommunication Standardization Sector）のセキュリティに関する標準化活動等に取り組んでいます．本稿では，ISO/IEC 27001，ISMAP（Information system Security Management and Assessment Program），ITU-T勧告X.1060のセキュリティ関連の最新標準化動向等とその実践を支援する当社のコンサルティング（3種類）について紹介します．

キーワード：#情報セキュリティ，#クラウドセキュリティ，#セキュリティ統括

武井　滋紀（たけい　しげのり）
中田　美佐（なかだ　みさ）
土屋　直子（つちや　なおこ）
NTTテクノクロス

ISO/IEC 27000シリーズ

■ISO/IEC標準化動向

情報セキュリティマネジメントにおいて国内でもっとも主要な第三者適合性評価制度であるISMS適合性評価制度[(1)]の認証基準として知られているISO/IEC 27001（情報セキュリティマネジメントシステム－要求事項）*1と，そのガイドライン規格であるISO/IEC 27002（情報セキュリティ管理策）*2が，2022年に改訂されました．改訂版では，昨今のサイバー攻撃，プライバシー侵害，クラウドサービスの普及などのセキュリティ脅威やセキュリティ技術の変化への対応が強化されました．改訂版で強化された情報セキュリティ管理策について**図1**に示します．

これらの規格は，ISMS適合性評価制度だけではなく，経済産業省の情報セキュリティ管理基準[(2)]や，政府情報システムのためのセキュリティ評価制度であるISMAP（Information system Security Management and Assessment Program）[(3)]の基準のベースとなっており，本改訂は関連制度にも大きな影響を及ぼします．ISMS取得組織は，移行期間である2025年10月31日までに新しい認証基準への移行審査を受ける必要があります．また，ISO/IEC 27002に基づくクラウドサービスのための規格であるISO/IEC 27017*3についても，現在ISOにて改訂中で数年後に改訂版が発行される予定です．

＊1　ISO/IEC 27001:2022：情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項．
＊2　ISO/IEC 27002:2022：情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策．
＊3　ISO/IEC 27017:2015：情報技術－セキュリティ技術－ISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範．

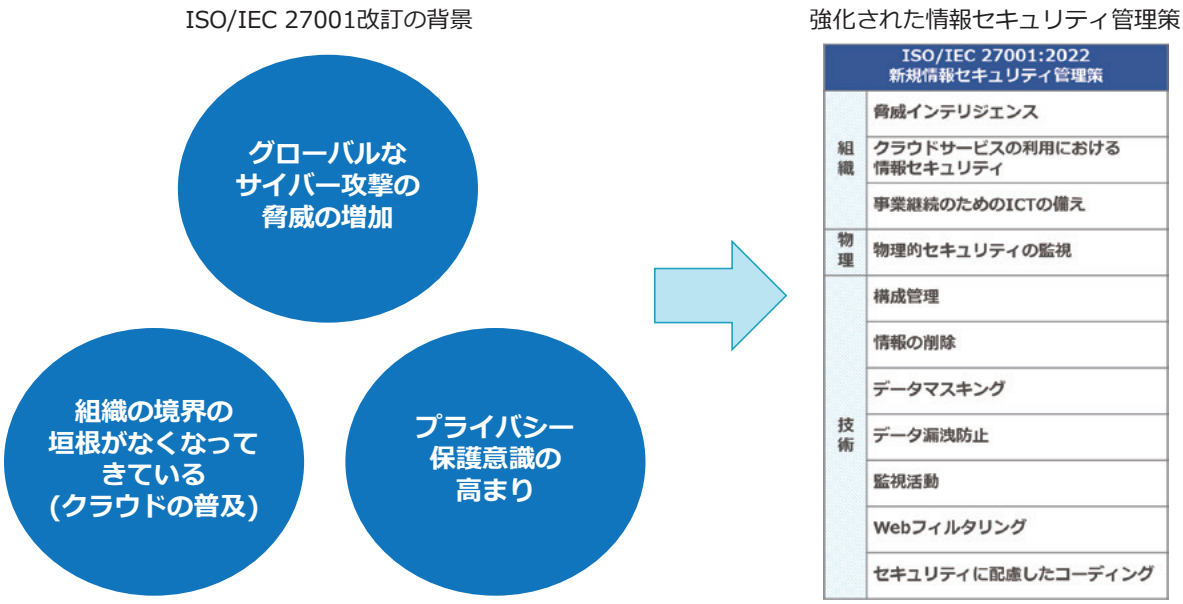


図1　改訂版で強化された情報セキュリティ管理策

■ISO/IEC 27001，ISO/IEC 27017コンサルティング

情報セキュリティマネジメントに課題を感じている，または強化したいと考えている組織は，組織のニーズにこたえるコンサルティングサービスを活用することがポイントになります．ISO/IEC 27001やISO/IEC 27017のコンサルティングサービスを提供する会社は数多くありますが，NTTテクノクロスでは，ISO標準化活動にも参画し規格を熟知したコンサルタントが組織のニーズにきめ細かく対応した，ISO/IEC 27001:2022移行コンサルティングやISO/IEC 27017コンサルティングを行っています．

また，NTTグループのセキュリティ規程は，最新のリスクマネジメントを強く意識し，米国国立標準技術研究所（NIST）のCybersecurity Frameworkや SP800-37，SP800-53[4]も考慮したものに改訂され，NTTグループ各社は新規程に沿った対応が必要となります．このような対応の支援のため，NTTテクノクロスでは，ISOセキュリティ規格に加えNISTやNTTグループ新旧規程にも詳しいコンサルタントが，セキュリティ規程の改訂や強化を行うコンサルティングも提供しています[5]．

ISMAP

■ISMAP最新動向

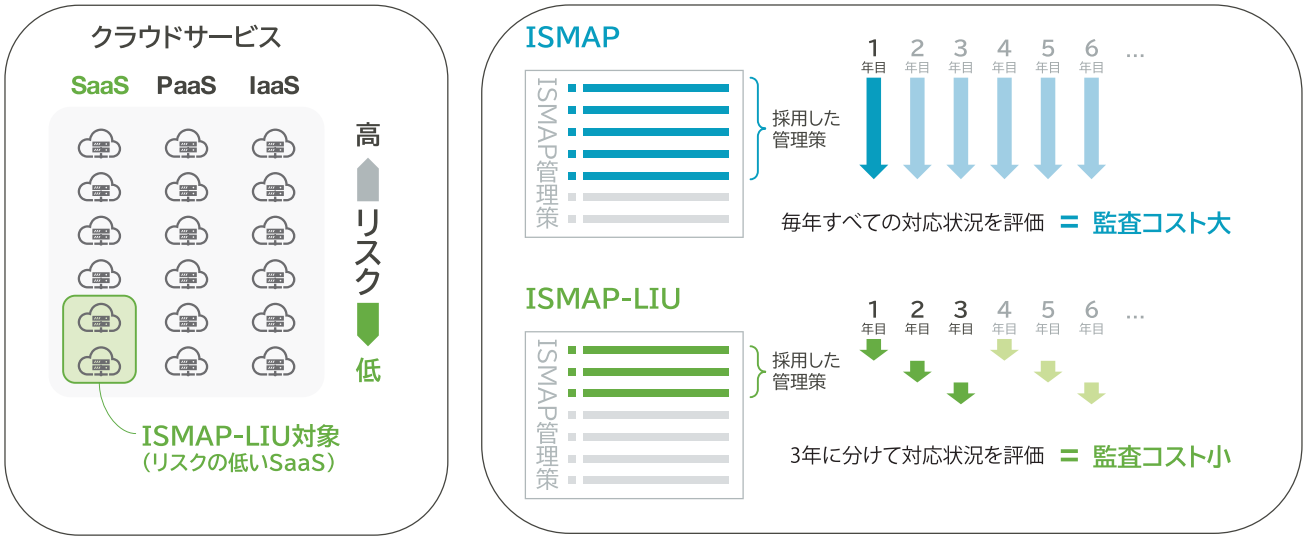
政府機関等が一定のセキュリティ水準を満たしたクラウドサービスを調達できるよう，クラウドサービスのセキュリティを評価し，サービスリストに登録する制度であるISMAPの運用が2020年6月3日に開始されてから，主管省庁により普及に向けてプレスリリースや講演，暫定措置等が行われています．また，制度当初より登録にかかる負担が大きいとの声があったため，2022年11月1日より，リスクの小さな業務・情報の処理に用いるSaaS（Software as a Service）を対象としたISMAP-LIU（Low Impact Use）*4が開始されました．これは，主管省庁が定めた「対象業務一覧」に該当するSaaS，または複数の行政機関による「影響度評価」で「低位」と評価されたSaaSに適用されます．ISMAPではリスクアセスメントによって採用した全管理策への対応を約1年ごとに評価するのに対し，ISMAP-LIUでは3年間で全管理策への対応を評価することで，ISMAP-LIUクラウドサービスリストに登録する制度です（2023年7月時点）．ISMAPとISMAP-LIUの仕組みの違いについて**図2**に示します．なお，ISMAP-LIUへの登録は2023年5月時点では0件であり，デジタル庁はISMAP-LIU登録促進のため，2023年5月19日にさらなる特別措置[6]を公表しています．本特別措置では，移行期間内の一度に限り，監査の負担を軽減できる一方，特別措置登録サービスリストの開示は政府機関等に限定されます．

また，ISMAPの申請から登録までの待ち時間を改善するための検討が現在も進められており，最新の規程類についてはISMAPのHP[3]を参照してください．

■ISMAPコンサルティング

各種普及・促進施策にもかかわらず，新規登録するクラウドサービス数が限られるのは，ISMAP管理基準に規定されている1000個以上の管理策への対応や監査法人による厳格な監査への対応が，クラウドサービス事業者にとって多大な負担になっているためと推測されます．その負担を軽減するために，NTTテクノクロスではISMAP運用開始当初より，ISMAP登録支援コンサルティングを提供しています[5]．今まで

＊4 ISMAP-LIU：ISMAPの枠組みのうち，リスクの小さな業務・情報の処理に用いるSaaSサービスを対象とする仕組み．



（a）ISMAP-LIUの対象範囲　　（b）採用した全管理策の評価方法の違い

図2　ISMAPとISMAP-LIUの仕組みの違い

培ってきたISMAP規程類のベースとなった各種セキュリティ規格・基準の知見，各種監査・認証評価制度における監査ノウハウ，NTTグループおよび一般企業において助言してきた各種管理策への対応事例等を活用し，クラウドサービス事業者が苦労することの多いISMAPの管理策の理解や，自社のセキュリティ対策とISMAPの管理策への対応付け，外部からの監査に対応するための証跡の妥当性評価，各種申請書類の記載方法など，さまざまな支援を行っています．

ITU-T勧告X.1060

■X.1060標準化動向

2021年10月にITU-T勧告X.1060[*5]が公開されました．本勧告は，NTTグループなどが提案したセキュリティも含むビジネスリスクに対応する組織のフレームワークです．2022年２月にはTTC標準JT-X1060[*6]として日本語で日本の標準となりました．

背景には，ビジネス環境が変化しSOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）といった組織だけではビジネスにおけるリスク全体に対応することが難しくなったことがあります．そこで「サイバーディフェンスセンター」という概念が提唱されました．これは日本からの提案として，経済産業省サイバーセキュリティ経営ガイドラインや日本セキュリティオペレーション事業者協議会の知見が盛り込まれています．日本のガイドラインやドキュメントを参考に使いやすくなっていることも特徴です．

X.1060はあくまでセキュリティ対応組織を構築して運用するフレームワークです．実際にどのようにこの勧告を利用するか，概念をどのように理解するかなど現在もITU-Tの場で議論が進められ，各国での利用も進んでいます．今後も引き続き関係する文書が整備されることで活用が期待されます．

■X.1060コンサルティング

X.1060ではSOCやCSIRTも含めて今後のビジネスリスクも考慮したセキュリティ対応組織づくりを示しています．世界各国が合意した標準であるため，国内や他の国の間でセキュリティとして何をすべきかの共通言語にもなります．一方で，組織づくりのフレームワークだけであるため，実際に組織においてはどのように管理策を決めるのかなど，具体的な実施方法は書かれていません．それぞれの組織においてどのようなかたちになるかもさまざまです．また，この勧告は現在のところ規程類や審査，登録制度などはなく，ベストプラクティス的な活用になります．そのためセキュリティの組織をつくる場合や，見直しや改善をする際には各種アセスメントやコンサルティングを活用して，組織に合ったかたちにする必要があります．そのほかに，X.1060では実施すべきセキュリティの64のサービス（役割）も紹介されています．例えば実際にガバナンスをどうするのか，セキュリティの監視運用や脆弱性の診断はどうするのか，といった実務面についても考える必要があります．前述のISO/IECやISMAPのコンサルティングで情報セキュリティ全体のマネジメント面を強化し，X.1060のコンサルティングで組織体制を強化するような各種のコンサルティングや実務面でのソリューションを合わせて活用することで，より良いセキュリティの対策につなげることが可能です．

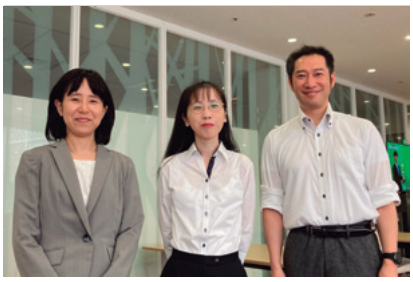
今後の展開

サイバー攻撃の高度化・多様化やクラウドサービスの普及等に対応するため，セキュリティに関する標準化や認証および評価制度も進化しています．そのため各企業や組織において，標準化規格への準拠や認証取得，セキュリティ強化等に取り組む際には，最新規格を参照しつつ規格がつくられた背景や意図，および認証取得の対象となる組織・システムの状況を把握・理解することが非常に重要です．

NTTテクノクロスでは，これらセキュリティ関連の標準化に引き続き貢献するとともに，最新の標準化動向に対応したコンサルティングサービスや最先端の各種セキュリティソリューションの提供を通して，安心・安全な社会の実現に取り組んでいきます．

■参考文献

(1) https://isms.jp/isms.html
(2) https://www.meti.go.jp/policy/netsecurity/is-kansa/
(3) https://www.ismap.go.jp
(4) https://csrc.nist.gov/publications
(5) https://www.ntt-tx.co.jp/products/service/security05.html
(6) https://www.digital.go.jp/policies/security/ismap-liu/



（左から）　土屋　直子／中田　美佐／
武井　滋紀

標準化規格の準拠やその認証取得については，規格のつくられた背景や意図，認証取得の対象となる組織・システムの状況を把握・理解することが非常に重要です．NTTテクノクロスの経験豊かなコンサルティングの活用や最適なセキュリティソリューションの利用により効率良く対応することができます．

◆問い合わせ先

NTTテクノクロス
セキュアシステム事業部　コンサルティング担当
TEL　045-212-7577
E-mail　telework.info-ml@ntt-tx.co.jp

＊5 ITU-T Recommendation X.1060：Framework for the creation and operation of a cyber defence centre.
＊6 TTC標準JT-X1060：サイバーディフェンスセンターを構築・運用するためのフレームワーク．

URL https://journal.ntt.co.jp/article/23456
DOI https://doi.org/10.60249/23105102

パーソナルデータ利活用促進に向けた匿名化・合成データ生成技術にかかわる取り組み

本稿では，世の中の匿名加工技術・合成データ生成技術の実用化動向を紹介するとともに，NTTテクノクロスの匿名加工情報作成ソフトウェア「tasokarena：タソカレナ」で適用している匿名加工技術・合成データ生成技術および群馬大学と連携した共同研究（合成データ生成技術に関する最適な実装方式の共同研究）の取り組み内容を紹介します．

キーワード：#匿名加工情報，#合成データ，#個人情報

石原 一郎[†1] / 角田 進[†1]
宮木 一郎[†1] / 吉岡 甲将[†1]
千田 浩司[†2]

NTTテクノクロス[†1]
群馬大学[†2]

はじめに

昨今，国内DX（デジタルトランスフォーメーション）が加速し，データ利活用が注目されています．その中で，個人情報から特定の個人を識別できないように加工した匿名加工情報は，個人情報保護法や次世代医療基盤法などの関連する法整備とともに利活用が拡大しています．政府機関の個人情報保護委員会によると，匿名加工情報の作成・提供に関する公表を行っている事業者が2020年３月時点で500社にのぼっています[*1]．

海外では個人情報の取り扱いの法令としてGDPR（General Data Protection Regulation：EU一般データ保護規則）やCCPA（California Consumer Privacy Act：カリフォルニア州消費者プライバシー法）がありますが，日本の「匿名加工情報」のようなデータの定義・利用範囲や具体的なデータ加工方針については言及されておらず，多人数のデータの統計的特徴に基づき人工的に作成される架空のデータである合成データ[*2]の利用がさかんです．

匿名加工技術および合成データ生成技術の実用化動向

一般に匿名化というと，誰の情報か分からなくする，氏名を取り除くといったイメージがあるかもしれません．個人情報保護委員会が公開しているFAQ[*3]によれば，匿名化は個人情報から氏名，生年月日，住所，個人識別符号[*4]等，個人を識別することができる情報を取り除くこと，ただし匿名化を行ってもなお特定の個人が識別できる場合には個人情報に該当する，とあります．そして匿名加工情報は，個人情報を個人情報保護委員会規則で定める基準（個人情報の保護に関する法律施行規則[*5]第34条第１～５号）に従って加工したものであり，当該個人情報を復元して特定の個人を再識別できないようにする必要があります（個人情報保護法第２条第６項）．なお本稿では特定の個人に関するデータ（レコード）の集合をパーソナルデータと呼び，１人以上の個人に関するデータであれば，個人情報も匿名加工情報もパーソナルデータに含まれるものとします．

それでは，匿名加工情報を作成するための匿名加工技術にはどのようなものがあるでしょうか．個人情報保護委員会のガイドライン[*6]では個人情報の保護に関する法律施行規則第34条第１～５号を満たす具体例とともに，具体的な匿名加工技術の手法が例示されています（**表**）．そして実際には，匿名性と有用性のバランスの取れた適切な加工が重要となります．ここで有用性とは，所望の利活用において匿名加工情報が元の個人情報と比べてどの程度利用価値を維持しているかを示す指標です．加工が不適切だと，匿名性が損なわれた情報，有用性の低い匿名加工情報となってしまいます．

もっとも有名な匿名性に関する指標の１つとして，k-匿名性[(1)]があります．性別や年齢のように特定の個人を絞り込める属性（準識別子）の値の組について，k人以上が同じ値になるとき，そのパーソナルデータはk-匿名性を満たすといいます．k-匿名性を満たすパーソナルデータを作成するために，表の手法などが用いられます．また近年では，差分プライバシー[(2)]と呼ばれる匿名性・プライバシーに関する指標の研究も進展しています．差分プライバシーは，パーソナルデータに限らず，パーソナルデータから得られる統計値や機械学習・深層学習の生成モデルにも適用できます．統計値や生成モデルからも特定の個人に関するデータを推定されるリスクがあり，攻撃も年々高度化していることから，差分プライバシーの注目度も高まっています．なお匿名加工情報は必ずしもk-匿名性や差分プライバシーを満たす必要はありませんが，これらを満たすことにより匿名性・安全性を理論的に保証できる効果があります．

＊1 パーソナルデータの適正な利活用の在り方に関する実態調査（令和元年度）報告書（個人情報保護委員会）：https://www.ppc.go.jp/files/pdf/personal_date_report2019_1.pdf
＊2 合成データ：個人情報保護委員会のガイドライン[*6]の別表2では疑似データと表現していますが，本稿では合成データと統一します．
＊3 「匿名化」された情報と「匿名加工情報」との違い：https://www.ppc.go.jp/all_faq_index/faq3-q2-12/
＊4 個人識別符号：特定の個人を識別することができるものとして政令に定められた文字，番号，記号その他の符号．指紋や静脈などの身体的特徴を表した符号，運転免許証の番号やマイナンバーなど．
＊5 個人情報の保護に関する法律施行規則：https://elaws.e-gov.go.jp/document?lawid=428M60020000003
＊6 個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）：https://www.ppc.go.jp/personalinfo/legal/guidelines_anonymous/

表　匿名加工技術の例（個人情報保護委員会のガイドライン*6の別表2を引用）

手法名	解説
項目削除／レコード削除／セル削除	加工対象となる個人情報データベース等に含まれる個人情報の記述等を削除するもの．例えば，年齢のデータを全ての個人情報から削除すること（項目削除），特定の個人の情報を全て削除すること（レコード削除），又は特定の個人の年齢のデータを削除すること（セル削除）．
一般化	加工対象となる情報に含まれる記述等について，上位概念若しくは数値に置き換えること又は数値を四捨五入などして丸めることとするもの．例えば，購買履歴のデータで「きゅうり」を「野菜」に置き換えること．
トップ（ボトム）コーディング	加工対象となる個人情報データベース等に含まれる数値に対して，特に大きい又は小さい数値をまとめることとするもの．例えば，年齢に関するデータで，80歳以上の数値データを「80歳以上」というデータにまとめること．
ミクロアグリゲーション	加工対象となる個人情報データベース等を構成する個人情報をグループ化した後，グループの代表的な記述等に置き換えることとするもの．
データ交換（スワップ）	加工対象となる個人情報データベース等を構成する個人情報相互に含まれる記述等を（確率的に）入れ替えることとするもの．
ノイズ（誤差）付加	一定の分布に従った乱数的な数値を付加することにより，他の任意の数値へと置き換えることとするもの．
疑似データ生成	人工的な合成データを作成し，これを加工対象となる個人情報データベース等に含ませることとするもの．

一方，機械学習・深層学習を用いた合成データ生成技術の研究開発および実用化も急速に進展しており，特に画像データは非常に高品質の合成データが作成可能となっています．構造化された表形式のパーソナルデータについても有用性に優れた合成データ生成技術がいくつか提案されており，諸外国では多くのスタートアップ企業がパーソナルデータを対象とした合成データ生成事業を行っています[3]．興味深い話として，自社の作成する合成データがGDPRやCCPAの匿名性要件に準拠していると主張している企業もみられます．しかし筆者らが知る限り，国内では匿名加工情報の基準を満たす，あるいは非個人情報と認められるような合成データの要件に関する議論はほとんど行われていません．

上記を踏まえ，安心・安全なパーソナルデータ利活用促進に向け，データ合成技術評価委員会が国内で発足しました*7．合成データを構成する各レコードは架空のデータであり，一般に特定の個人とは紐付きません．また合成データは多属性のパーソナルデータでも属性間の統計的特徴を維持しやすく，その有用性の高さが注目されています．しかし特定の個人に関するデータの推定リスクは，合成データ生成技術の手法に依存します．そこでデータ合成技術評価委員会では「不適切な合成データの利用」や「リスクを恐れた合成データの利用躊躇」の課題を解決し，健全な合成データ生成技術の利用を推進するため，既存の合成データ生成技術の匿名性やプライバシーレベルを評価し，結果を発信していくことをめざしています．筆者らもデータ合成技術評価委員会の活動に参画しています．差分プライバシーを満たす合成データ生成技術も多数提案されており，前述のスタートアップ企業の一部がすでに実用化していることから，国内でも健全な合成データ生成技術の実用化が進み，データ利活用による社会課題の解決や安心・安全で便利なサービスの普及に資することが期待されます．

tasokarenaで適用している技術と特長

NTTテクノクロスでは「匿名加工情報」の作成を支援するソフトウェア（tasokarena：タソカレナ）[4]を2018年から提供開始し，2021年から合成データの生成機能を追加実装しています．現在では医療・金融・自治体・コールセンタ等さまざまな分野へ導入されています．tasokarenaの製品名は，日が暮れて薄暗くなり相手の顔の見分けがつきにくくなったころに「あなたは誰ですか？」と問いかける言葉「誰そ彼（たそかれ）」が，元のデータから個人を特定できなくする本ソフトウェアのコンセプトと合致していることから命名しています．

tasokarenaの主な特長を紹介します．

⑴　NTT独自技術含む豊富な加工技法を提供

数十種類の加工技法の中から実行する加工技法を組み合わせ，匿名加工情報を作成することが可能です．

特徴的な加工技法としてはNTTが独自に開発した手法である「Pk-匿名化[5]」を実用化し，本ソフトウェアに搭載しています．匿名性の代表的な指標であるk-匿名性を満たすようにノイズ（疑似データ）の付与やデータの入れ替えを行い，データの有用性が損なわれていない匿名加工情報を作成します（**図**）．

また，受診履歴データや購買履歴データといった履歴型データ（1ユーザ複数レコード）についても，k-匿名化，Pk-匿名化を行うアルゴリズムを実装し，履歴型データについても加工と評価を実行することも可能です．

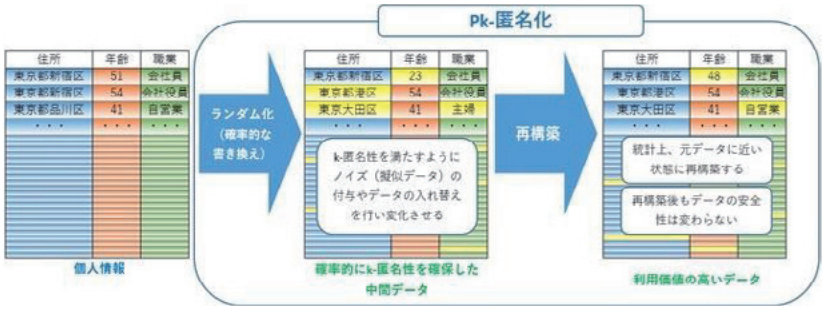
⑵　匿名性・有用性の評価機能

tasokarenaで作成した匿名加工情報は，15種類の評価技法により匿名性と有用性のバランスをグラフで確認することが可能です．このグラフを参考にしながら加工技法の組合せを変えることで，最適な加工ルールを設定していくことが可能になります．

⑶　マスキングツールで情報共有の安全性を向上

同一事業者内での情報共有の安全性を高める目的として，自由記述形式で記載された文章に含まれる個人情報を削除するマスキングツールを提供しています．医師の所

＊7　データ合成技術評価委員会：https://www.iwsec.org/pws/ppsd



NTT公式HPから引用
https://www.rd.ntt/research/PF99-341.html

図　Pk 匿名化イメージ

見や患者の診療記録，コールセンタの対応履歴データ等の文章に含まれる個人情報に対して，自然言語解析によって氏名や住所などを自動で判別し，削除することが可能です．これにより，ユーザの作業負担を軽減しながら，情報共有における安全性の向上を実現しています．

⑷　医療向けオプション

自治体・医療機関・健康保険組合などの共通仕様になっているレセプト*8データをtasokarenaで読み込み可能にする変換ツールを提供しています．レセプトデータのフォーマットはレコード識別情報の値によってレコード項目数や記録内容の形式が異なるため，匿名加工情報を作成する場合には，事前にユーザによるデータの形式を合わせるなどのクレンジング処理が必要でした．変換ツールを使用することでユーザによる手間が削減され，さらに変換後のレセプトデータから作成した匿名加工情報を再び元のレセプトデータのフォーマットに戻すことが可能になり，既存システムでも匿名加工情報を利用できます．

また，医療系のデータを扱う際の標準の1つであるPhUSEの非特定化標準*9を基に，匿名加工したデータセットの整合性をとるツールを提供しています．

⑸　合成データ生成機能

合成データ生成機能として統計的手法と機械学習的手法を提供しています．

統計的手法はNTT社会情報研究所の特許技術を活用しています．各属性の平均など統計値が元データとほぼ等しい合成データを生成する技術等を独自に開発し，これまでプライバシ保護技術では実現できなかった分析に必要な複数の統計値を保持する多属性の合成データを生成することが可能になりました．NTT社会情報研究所は本技術の開発で培った知見を活用し，AI（人工知能）・機械学習分野における難関国際会議の匿名化技術を競うコンペティションで優勝しました(6)．

機械学習的手法はベイジアンネットワーク*10を基に合成データを生成します．

NTTテクノクロスと群馬大学との共同研究の取り組み

合成データについては具体的な利用例はありますが，安全性，有用性についての評価方法は定まっていません．また，合成データ生成手法としてさまざまな技術が提案されていますがどのようなデータにどのような手法を用いると良いかといった確立されたノウハウやコンセンサスがあるわけではありません．そこで，NTTテクノクロスと群馬大学で市中の合成データ生成手法による合成データ生成，および安全性，有用性評価を行い，データ種別による各合成データ生成手法の得手不得手を明らかにする共同研究を行っています．

今後の展開

NTTテクノクロスは，今後，共同研究の取り組みを継続実施していくとともに，その結果を，NTTテクノクロスの製品へ組み込み，ビジネス展開することをめざしています．また，個人情報保護法は個人情報の保護に関する国際的，技術状況等を勘案し，3年ごとに必要に応じて改正されることになっており，個人情報保護法の動向をチェックし，適切な技術を提供することを通じてパーソナルデータの利活用の拡大に貢献していきます．

■参考文献

(1) L. Sweeney：“k-anonymity: A model for protecting privacy,” Int. J. Uncertain. Fuzziness Knowl.-Based Syst., Vol. 10, No. 5, pp. 557–570, 2002.
(2) C. Dwork：“Differential privacy,” Proc. of 33rd ICALP – Volume Part II, LNTCS, Vol. 4052, pp. 1–12, 2006.
(3) 千田・南・寺田・伊藤：“プライバシー保護型合成データの実用動向と今後の展望，”統計，Vol. 73, No. 8, 2022.
(4) https://www.ntt-tx.co.jp/products/anontool/
(5) https://www.rd.ntt/research/PF99-341.html
(6) https://group.ntt/jp/newsrelease/2021/03/02/210302b.html


（左から）　宮木　一郎／石原　一郎／
角田　　進／吉岡　甲将／
千田　浩司

個人情報をより安全に守りながら，より効果的に活用し，企業や個人に利益をもたらすことをめざし取り組みを進めています．

◆問い合わせ先

NTTテクノクロス
セキュアシステム事業部　tasokarena担当
TEL　045-212-7577
E-mail　anontool.info-ml@ntt-tx.co.jp

＊8 レセプト（診療報酬明細書）：医療費の請求明細のことで，保険医療機関・保険薬局が保険者に医療費を請求する際に使用するものです．電子レセプトとは，厚生労働省が定めた規格・方式（記録条件仕様）に基づきレセプト電算処理マスターコードを使って，CSV形式のテキストで電子的に記録されたレセプトのことを指します．

＊9 Pharmaceutical Users Software Exchange：https://phuse.global/

＊10 ベイジアンネットワーク：データの因果関係の強さを，ある事象が起こった場合に他の事象が起こる確率の大きさから判断し，多数の事象間の因果関係をグラフィカルに整理する方法．

URL　https://journal.ntt.co.jp/article/23459
DOI　https://doi.org/10.60249/23105103

NTTテクノクロスにおけるブロックチェーン技術に基づいたVCへの取り組みとそのSBOMへの応用

NTTテクノクロスでは，ブロックチェーン技術を活用したサプライチェーン関連のシステム開発を通じて，VC（Verifiable Credentials）データモデルに着目し，サプライチェーンのモデルに適した階層型VCという技術を考案しました．その応用先として，SBOM（Software Bill of Materials）への適用を検討しており，ソフトウェアサプライチェーン全体での安全性向上をめざしています．

キーワード：#ブロックチェーン，#VC，#SBOM

小森　絵未（こもり　えみ）
津川　天祐（つがわ　ひろまさ）
大竹　孝幸（おおたけ　たかゆき）
NTTテクノクロス

NTTテクノクロスとブロックチェーン

NTTテクノクロスは2015年よりブロックチェーン技術に着目し，NTTグループ内外問わずさまざまな分野の企業様とかかわり，ソリューション提案を実施してきました．ブロックチェーンというと，ビットコインをはじめとする暗号資産やNFT（Non-Fungible Token：非代替性トークン）アートといったイメージが強いですが，当社では投機目的以外の分野での応用を中心に，ビジネス検討，プログラム開発を行っています．ブロックチェーン技術は「改ざん不可能」「データ更新の確実な追跡」「データ共有の透明性」といった特徴があり，これらの特徴を確実にメリットを生む領域に適用することが重要です．多数のステークホルダーが存在するサプライチェーンはその強みを活かせる分野の1つであり，当社ではブロックチェーンを利用したサプライチェーン上でのモノの流れを確実に追跡可能なシステムの開発をこれまで行ってきました．

■サプライチェーンにおけるVCの活用

一方で「データ共有の透明性」というブロックチェーンの特徴は，ネットワークの参加者全員がデータを共有し信頼性を高めるものなので，個社間でのみ共有したい情報をそのまま載せるには適していません．例えば，A社からB社へある製品を納品したとして，その製品の設計・技術情報，構成などの詳細なデータはステークホルダー間だけで共有すればよく，全体ではその詳しい内容を知る必要はありません．こうした中で，当社はVC（Verifiable Credentials）というモデルに注目しました[1]．VCはオンラインで検証可能な証明書であり，W3C（The World Wide Web Consortium）がデータモデルを公開しています．

VC自体はJSON（JavaScript Object Notation）形式で表現された電子データであり，電子署名などの技術を活用し，物理的な証明書よりも信頼性を高めつつ，さまざまな情報の真正性を担保することが可能です．このモデルでは，VCの証明対象（Subject）に対して，発行者（Issuer），保有者（Holder），検証者（Verifier）という役割が定義されており，Issuerにより発行された個々のVCは，主にはHolderにより管理され，必要なVerifierにのみ開示され検証されます．したがって，VCデータ自体はステークホルダー間でのみ共有されます．重要となるのが，検証可能データレジストリ（Verifiable Data Registry）と呼ばれるもので，ここではVCデータ本体ではなく検証に必要な情報のみ（VCデータの真正性を担保するためのハッシュ値やIssuerの電子署名の検証に必要な情報など）を保管します．現在普及しているGAFAMのIDに紐付けて個人の情報等を証明するプロセスでは，VerifierはHolderから提示されたIDの検証を行う際にIssuerであるGAFAMに対して情報の問合せをする必要があり，Holderの情報の用途が意図せずIssuerに開示されてしまう可能性がありました．その点，VCの検証プロセスは，Verifiable Data Registryとさえ通信できれば真正性の検証が可能であり，IssuerとVerifierの間で情報のやり取りを行う必要がないため，Issuerによる行き過ぎた情報の寡占を防ぐことができます．NTTテクノクロスでは，Verifiable Data Registryをブロックチェーン上で実装することにより，信頼性を高めたContractGate/VCという製品を開発しています（**図1**）[2]．

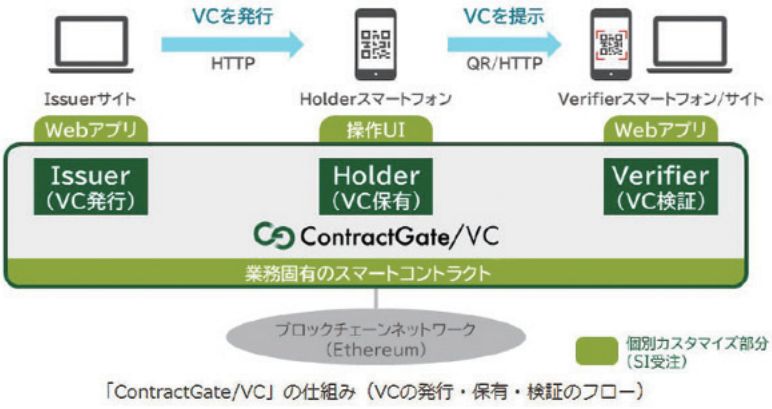


図1　ContractGate/VC

VCを実現するためにはブロックチェーン技術を使うことは必須の要件ではありませんが，多数のステークホルダーにまたがって真正性を担保するという点において，ブロックチェーン技術を活用することは有効と考えています．

■階層型VCモデル

サプライチェーンの話に戻りますが，流通する製品について，納品時に個社間で証明が必要な情報はVCを活用することにより真正性の担保が期待できます．具体的には，製品を納品する際に，製造者がIssuerとなって納品対象の製品に関する情報についてVCを発行し，製品とともに当該VCを発注元に納め，発注元はVerifierとなってVCを検証します．しかし，サプライチェーンにVCを適用するうえで，従来のW3Cの規格のままでは2点課題があります．1点目はVC間の関係性を表現するうえでの課題です．サプライチェーンでは流通の過程で複数の既成部品が組み合わされたり加工されたりして新たな製品ができるため，それらに紐付くVCの関係性を適切に表現できなければなりません．2点目は，Issuerの正当性を評価するうえでの課題です．サプライチェーンの中間業者は，ある区間ではVerifier（納品先）だったが，次の区間ではIssuer（納入者）となります．その際に，中間業者が納品しようとする製品に対して正当な権利がある者かどうかの確認が必要です．上記2点はいずれも既存のVC規格のままでは表現が困難です．そこで，NTTテクノクロスでは階層型VCモデルを考案しました．階層型VCモデルでは，検証時，4つのクレームを主に使用しています（**表**）．inheritancesクレームによってVC間の関連性を表し，サプライチェーン上で発行されるVCを辿って再帰的にその真正性の検証をできるようにしています．また，上記再帰的な検証の中で，検証対象のVCのissuerクレーム（納入者）とinheritancesクレームにより取得できるVCのissuedToクレーム（納品先）を比較することにより，当該VCのIssuerの正当性も併せて確認します．

階層型VCをサプライチェーンに適用することで，悪意あるデータ改ざんや発行者の成りすましが発生した際に，どの時点でそれが発生したのかをサプライチェーンをさかのぼって検証することが可能です．これにより，各ステークホルダー間で情報を改ざんなく，真正性を担保した状態で製品を流通していくことが可能になります．なお，本モデルは現在特許出願中です（**図2**）．

表　階層型VC の検証に用いる主なクレーム

クレーム名	意味
issuer	当該VCの発行者のDID
issuedTo	当該VCが保証する製品の納品先のDID
inheritances	当該VCと関連付けたVCデータ（JWT等）またはURIの配列
originalInfo	当該VCが保証する任意の製品情報

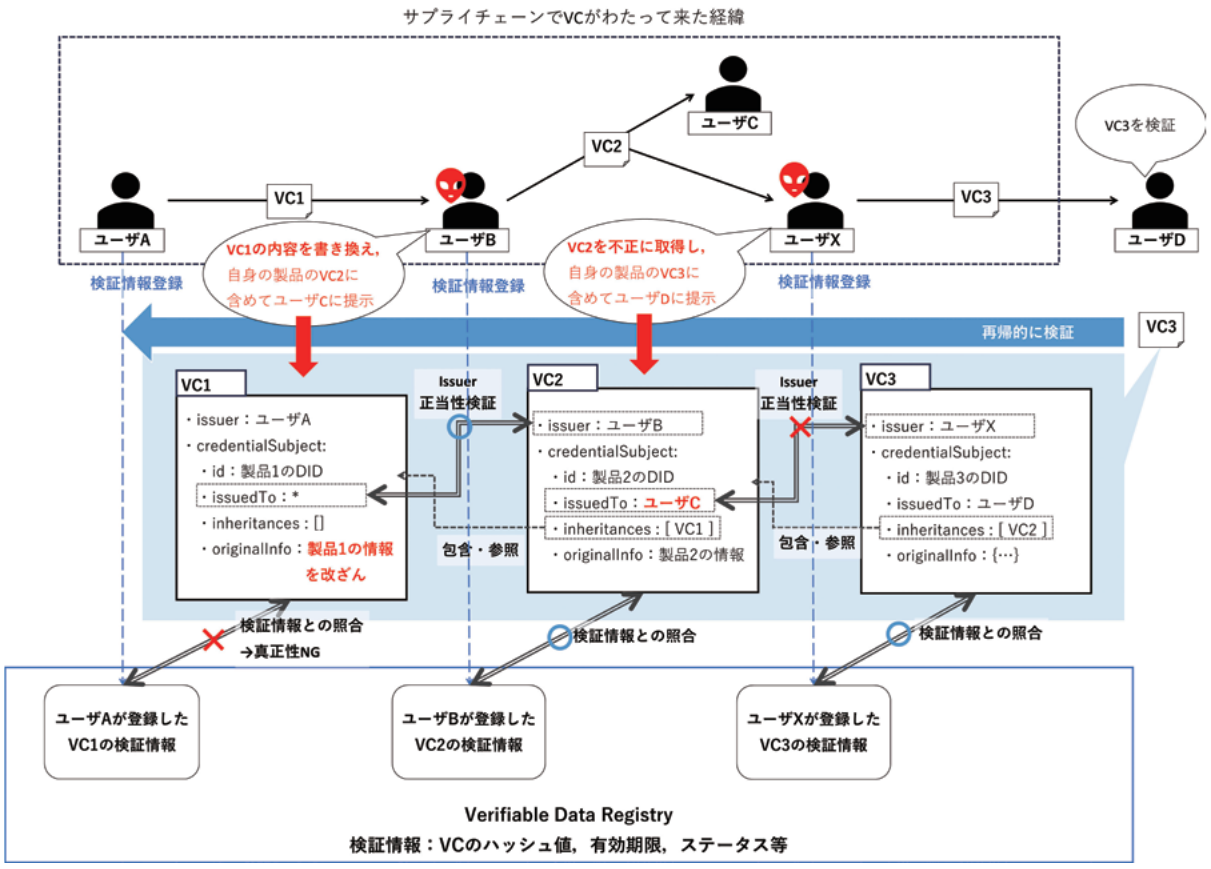


図2　階層型VCの検証イメージ

階層型VCモデルの活用例

NTTテクノクロスでは，ソフトウェアの品質を守るための取り組みとして，SBOM（Software Bill of Materials）に注目しています．SBOMはソフトウェアの部品表になります．製造業のサプライチェーンと同様，ソフトウェア開発においてもさまざまなステークホルダーによってサプライチェーンが形成されます．例えば，ライブラリのみを製造する，ライブラリを利用して新たなソフトウェアを生み出す，ソフトウェアを組み合わせて新たなサービスを提供するなど，ソフトウェア製造にもさまざまなステークホルダーが登場します．ユーザが日々利用するアプリケーションやサービスは，上記のようなステークホルダーによって，階層化されたサプライチェーンを形成します．SBOMも本来は階層化されたサプライチェーンのステークホルダー間で流通・共有するべき情報ですが，現段階においては，サプライチェーンに潜む脆弱性やライセンス違反などの，リスク可視化をめざしているため，サプライチェーンを強く意識した構造となっていません．一方で「SBOM自身の信頼性」に関してはこれまであまり語られていません．現在のSBOM運用モデルは，利用したいステークホルダーが自身でつくり出すか，直接契約関係にある発注先の製造会社につくらせることが一般的というイメージです．要するに一部のステークホルダーに作業が集中していることで，運用のハードルが高い状態であり，SBOM自身も悪意ある攻撃者により改ざんの脅威や，信頼性の低下，地政学的なリスクなどにさらされる可能性があります．

前述の問題を解決するのが，階層型VCモデルです．SBOM自身を各ステークホルダーがVC化することで，耐改ざん性を確保しつつ，誰がつくったSBOMなのかが確認可能です．加えて階層型VCモデルを利用することで，VC化されたSBOM自身も改ざんされることなく各ステークホルダー間で流通することができ，信頼性を確保した状態でSBOM運用を分業化可能となります．

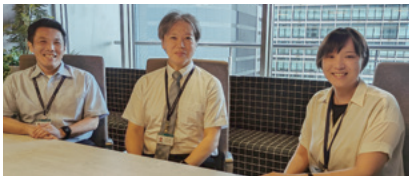
このように階層型VCモデルは，SBOMがソフトウェアと同じサプライチェーンで流通でき，かつ信頼性を確保できる仕組みを提供します．

今後の展開

本稿では階層型VCモデルの活用例としてSBOMを紹介しました．しかし本モデルはSBOMにとどまらず，サプライチェーンを形成するあらゆる情報に応用可能です．ある情報の真正性を確保しつつ，サプライチェーンのさまざまなステークホルダーが対象の情報に対し，付加情報を付け加えていくことが可能となり，情報の作成者や所有者の正当性を確認できる仕組みを提供します．

NTTテクノクロスでは，階層型VCモデルを「氾濫する情報の信頼性を確保する新しい仕組み」ととらえ，今後さまざまな分野に応用することを検討していきます．

■参考文献
(1) https://www.w3.org/TR/vc-data-model/
(2) https://www.ntt-tx.co.jp/products/contractgate/vc.html



（左から）　津川 天祐／ 大竹 孝幸／
小森 絵未

ブロックチェーンは，これまでつながることのなかった人・サービスをつなぐ新たな産業インフラとしてさまざまな分野での応用が期待されています．その中で，多くの人・サービス間で齟齬なく効率的に情報伝達をするために，VCやSBOMといったデータモデルの活用は今後ますます重要となっていきます．

◆問い合わせ先
NTTテクノクロス
デジタルトランスフォーメーション事業部
ContractGate担当
TEL　03-5860-2928
E-mail　contractgate.info-ml@ntt-tx.co.jp

社内での SBOM 活用状況

NTT テクノクロス 品質保証センターにおいては，社内でつくる製品やサービスの品質をより高めるための活動をしています．例えば，開発開始の段階ではプロジェクトのリスク点検を行ってトラブルを未然に防止し，開発完了の段階では納品・出荷時検査を行って開発物に問題がないものかチェックを行うなど，開発プロジェクトメンバと密に連携して品質強化に取り組んでいます．このような活動と SBOM は関連が強く，品質保証センターにおいても SBOM の普及動向に注目をしてきました．昨今のソフトウェア開発では，オープンソースソフトウェア（OSS）などの有用な既存部品をできるだけ活用し，コストを低減して効率的な開発を行うことが一般的です．しかし，他社の既存部品を活用するということは，部品に潜む脆弱性やライセンスの問題といったリスクも加えて取り入れるということになります．このようなリスクに備え，活用した部品の名称や版数といった構成情報を管理し，脆弱性などの問題が世の中で見つかっていないものか定期監視するなど，何らかの対策を行っていくことが重要になってきます．SBOM が，このようなリスク対策を容易に行える手段として展開されてきています．SBOM を作成して脆弱性診断を行うツール類がすでに世の中には存在しており，私たちは，そのようなツール類を調査・試用し，社内の製品を対象とした SBOM 作成をパイロットプロジェクトとして始めました．得られたノウハウを基に社内でリスク対策をする際のガイドラインを作成したいと思っています．SBOM を活用するためには，記述内容の見やすい表示や，真正性を証明するような仕組みも必要となってきます．上述した社内の取り組み，技術と連携して SBOM の活用を促進していきます．

URL https://journal.ntt.co.jp/article/23462
DOI https://doi.org/10.60249/23102001

5Gで変わる世界の通信業界：新たなプレイヤー，新たな通信ネットワークの姿 ―前編―

本稿では，普及が進みつつある5G（第5世代移動通信システム）の現在地について，それまでの歴史を振り返りつつ，技術の面から，また関連主要企業の面からご紹介します．その背景にあるのは，従来の電気通信（テレコム）技術とインターネット技術の接近です．これにより，5Gをめぐる技術トレンドも企業間の競争状況も変わってきました．

テレコムの進化はインターネットへの接近

通信ネットワークは，それを支える技術が進化し，機能や性能が向上することでサービスが多様化・高度化してきました．特にこの30年の進化は，インターネットへつながる基盤としての進化だといえます．

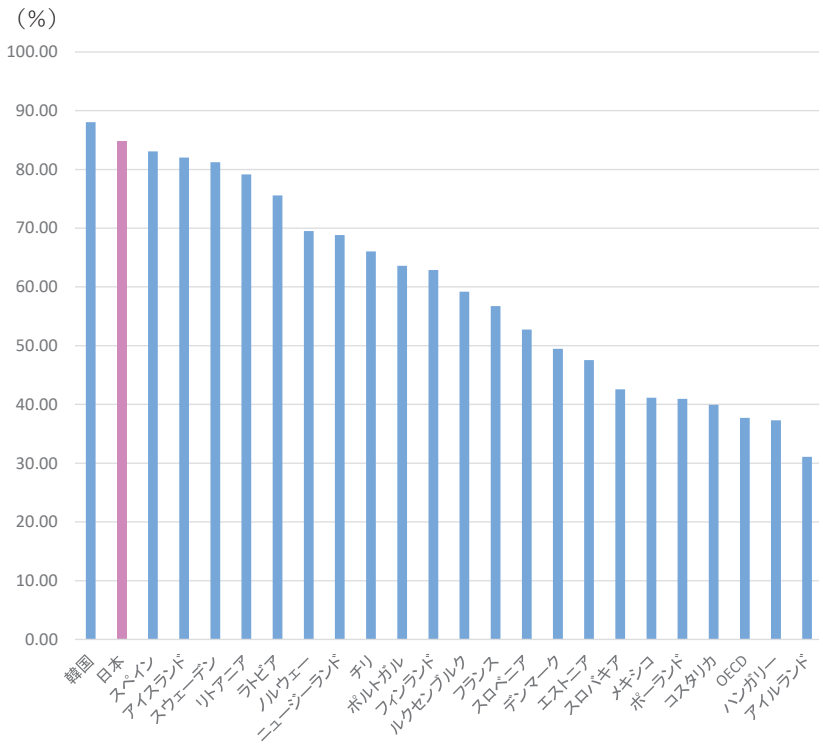
通信ネットワークは，当初電話，すなわち「音声通信」のための設備として整備されてきました．そしてインターネットの普及により新たなタイプの「データ通信」のために整備され，進化を続けてきたわけです．

データ通信もかつては，音声通信のためのアナログ回線上で，デジタルなデータ情報をやり取りする時代がありました．インターネットの普及前（～1990年代前半），「ピーゴロゴロ～」と音がした通信モデムは，そのための機器でした．その後，デジタル信号をよりスムーズにやり取りできる「ISDN」や「ADSL」が登場し，固定ブロードバンド通信が広く一般に手が届きやすい料金で提供され，WWW（World Wide Web）など，インターネットの普及を下支えしました．

そして2000年代に入り「光ブロードバンドアクセス」が登場しました．日本では大手通信事業者がインターネットのさらなる普及を見越して光ブロードバンドアクセス回線を積極的に整備しました．日本は光ブロードバンドの普及では，当時から世界の先進市場であり，現在も日本と韓国が世界をリードする存在です（**図1**）．

また，インターネットの普及と並行して，2000年代は携帯電話の普及も進んだ時期でした．モバイル通信でも，技術の進化は固定通信と似た道を辿ってきたといえます．もともと「音声通信」をいつでもどこでも，を実現してきたのが2G（第2世代移動通信システム）で，「映像通信」を扱うインフラとして期待されたのが3G（第3世代移動通信システム）です．3Gでは当初，テレビ電話がキラーアプリの1つとして考えられていましたが，実際にはインターネットの便利さを携帯電話でも享受できるようになったことが消費者に広く受け入れられました．技術的にはデータ通信対応がそれを実現させた大きな要素であり，日本は世界で唯一「iモード」等のモバイルインターネットが広く普及した市場でした．

そのモバイルインターネットは，4G（第4世代移動通信システム）で世界に広がることになります．4Gでは3Gで実現したデータ通信機能をより強化したのですが，その普及の最大の要因はスマートフォンの登場でしょう．スマートフォンを世界の多くの機器メーカーが製造し，ハイエンド端末に



出典：OECD Broadband statistics. 1.10. Percentage of fibre connections in total fixed broadband, June 2022

図1　各国の固定系ブロードバンドに占める光ファイバの割合

搭載されていた機能が年を追うごとに普及価格帯の機種にも搭載されるようになり，インターネットに常時アクセスできる人が世界で劇的に増えることになりました．日本でも2010年から2013年にかけて，スマートフォンを持つ世帯の比率は 6 倍以上になっています（**図 2**）．

同時に，世界の通信事業者は通信ネットワークの混雑に悩まされることになります．時に人気アプリやOSのデータ一斉更新や，コンテンツへのアクセス集中などで，通信がつながりにくくなることも世界的な現象となっていました．通信事業者が懸命に設備投資をしても，需要の増加がそれを上回る，という状況でした．

特にモバイルアクセスの混雑緩和に世界的に重要な役割を果たしたのがWi-Fiです．Wi-Fiはスマートフォンに標準搭載されました．スマートフォンの利用場所は屋外だけでなく屋内でも多く，特に家庭内ではWi-Fi経由でインターネットにアクセスすることが一般的になりました．4Gの利用料金は基本的にデータ利用量に応じた料金となっていたため，特に動画視聴のようにデータ量がかさむ使い方をしていると，使えば使うほど月額費用が高くなります．しかし，固定ブロードバンド料金はデータ量に関係なく定額料金で提供されてきたため，Wi-Fi経由で固定ブロードバンドを使ったほうが，スマートフォンを多く利用する人にとっては通信料金の節約にもなり，それはモバイル通信網の混雑緩和にもつながりました．言い換えれば，携帯電話から始まったモバイル通信ネットワークと，家庭の電話から始まった固定通信ネットワークは，スマートフォンの登場で，インターネットへアクセスするという目的のために区別なく使われるようになったわけです．

このように，通信ネットワークの進化は，技術的にはインターネットへどんどん接近する流れとなりました．またスマートフォンの普及が，モバイル通信と固定通信を一体的に使うような市場を形成したともいえます．

テレコムの設備をインターネットの技術で構築・運用する時代へ

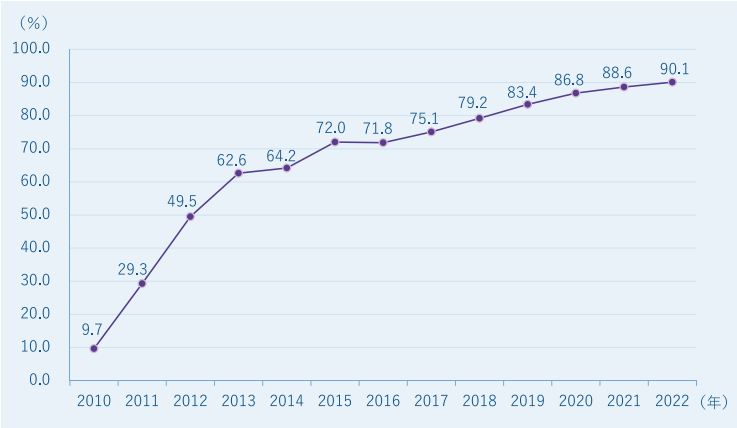
通信ネットワークの技術進化は，2000年代以降は世界的にみて，固定通信よりもモバイル通信における動きのほうが活発でした．それは，モバイル通信の市場の伸びが固定通信のそれよりも劇的であったことが主な要因だったためです．固定通信の市場開拓は，オフィスや世帯ごとに敷かれていた電話回線をブロードバンド回線に切り替える，というものでした．一方，モバイル通信での市場開拓は，もともと通信回線でつながっていなかった個人に電話を持たせることで市場を急成長させ，さらにデータ通信需要が喚起されたことで，個人が支払う通信料金も増えた，というものでした．

したがって，利用者からみると，モバイル通信は「つながるようになった」という体感がまずあり，その後「速くなった・スムーズになった」という体感へ，という流れでした．「つながるように」の進化は，主に電波が届くかどうかですから，設備構築がどれだけ進むかでほとんど決まります．基地局設備をより多く，よりきめ細かく設置するには時間も費用も相応に必要ですが，地道に改善されていきます．

一方「速くなった・スムーズになった」の進化は，通信技術の進化によるところも大きいです．データをいかに効率良く運び，高速に処理するか，になります．それは，2Gから3G，3Gから4Gへと世代交代が進むたびに，利用者は速度を体感できました．分かりやすいのは，動画視聴体験でしょう．世界的には，スマートフォンの登場以降になりますから，4G方式での体感がもっとも顕著だったはずです．3Gではおおむね数Mbit/s程度だった通信速度が，4Gが普及した10年で100 Mbit/s以上になりました．

そして現在，5G（第 5 世代移動通信システム）が徐々に普及しつつある時期にあたります．またスマートフォンの多くは，カメラが4K撮影に対応しています．大画面の4Kテレビと同じ高精細な映像を，スマートフォンで撮影・再生できるわけですが，それほどの大容量データをストレスなく送受信できる性能を，5Gは持ち合わせています．この5Gは，消費者からみれば「4Gよりもさらに高度な」通信を期待させるものですが，実は5Gの通信ネットワークをめぐっては，それまでの「技術的にインターネットへどんどん接近する流れ」が業界構造を大きく変えるかもしれない，という状況に来ています．

要するに，インターネットの構築・運用に活用されている技術で通信ネットワーク設備を構築・運用する，という動きです．専門用語では「仮想化」「クラウド化」がこれにあたります．またこのことが，通信事業者が構築する公衆5G（パブリック5G）だけでなく，企業等が自ら構築する自営5G（プライベート5G）の今後の普及に大きく関与するかもしれません．何が優れていて，利用者にどんなメリットがあるのか，また業界構造がどう変わるのか，について説明します．



出典：総務省「令和4年通信利用動向調査」より情報通信総合研究所作成

図 2　我が国におけるスマートフォンの世帯保有率の推移

仮想化で，設備の構築費用を抑える

まず「仮想化」についてです．仮想化とは，ハードウェアの機能を仮想的に実現する，という意味で使われる用語です．これまでハードウェアで実現していた機能を，ソフトウェアを使って実現します．通信ネットワークの設備機器は，通常は通信ネットワーク向けの専用設計で，非常に多くの利用者が同時に行う通信を瞬時に処理するため，高性能が求められますし，おのずと高価になるものでした．しかし，この仮想化技術によって，専用ハードウェアを使っていた場所に，汎用ハードウェアを使うことができるようになります．ここでいう汎用ハードウェアとは，実際には企業やデータセンタで広く使われているサーバ機器です．サーバ機器は，形状的には世界共通の規格があり，同じような性能の製品が世界中で使われているため，量産効果が働き，廉価なものになっています．そして専用機器でなくても通信ネットワーク機器として動作するのは，主にソフトウェアの進化によるものです．高価な専用機器の代わりに廉価な汎用機器を使えるとなると，通信事業者にとっては，通信ネットワークを構築する費用を抑えることができ，設備投資負担が軽くなります．世界の通信事業者がこの技術に注目するのは当然なわけです．設備に使っていた投資を他の分野へ振り向けることも，また通信料金の値下げ競争に耐える余力も生まれてくることになります．

国内の大手通信事業者は各社とも，これまでモバイル通信設備に毎年4000～5000億円もの規模の投資を行ってきました．それらの機器が専用ハードウェアから汎用ハードウェアに切り替わることで，数10%規模の費用削減が可能だ，と説明する企業もあります．

クラウド化で，設備の運用を高度化する

次に「クラウド化」です．「仮想化」により通信ネットワーク設備は汎用ハードウェアで構成できるようになるのですが，その汎用ハードウェアはデータセンタで採用されているものと説明しました．データセンタの中には大手クラウド事業者が使う設備も多くあり，そうした設備はクラウド技術で運用されています．ということは，通信ネットワーク設備とクラウド設備が同じハードウェアで構成され始めている．言い換えれば，通信ネットワークは，クラウド技術で構築・運用できるようになってきたわけです．

クラウド技術とはインターネット技術の１つでもありますから，通信ネットワークがインターネット技術で運用されるようになる，ということです．これも考えようによっては非常に自然な流れだともいえます．そもそも通信ネットワークは，もとは電話（音声通話）のために運用されていたものが，時代とともにインターネットのために運用されるようになってきたわけです．モバイル通信の開発では，いかにしてインターネットにつなげるか，ということを3Gから技術規格に盛り込んでおり，4Gで音声通話の方式が回線交換からパケット交換ベースになり，電話のための通信ネットワークから卒業したといえます．そして5Gでクラウド技術をベースに運用するとなれば，インターネットのための通信ネットワークとしてより進化するわけです．

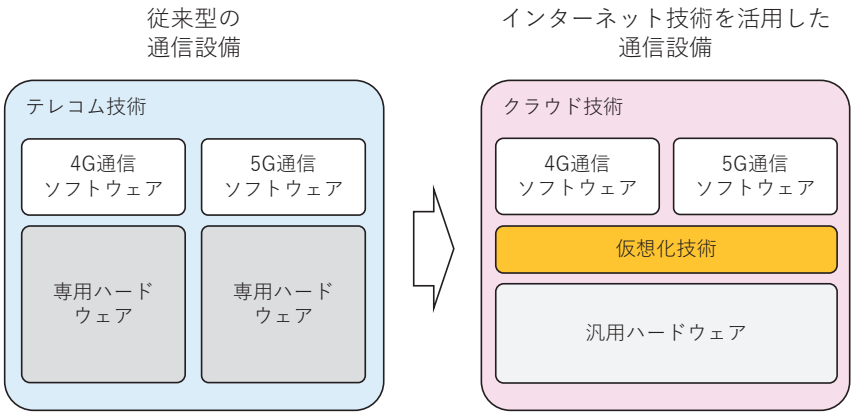
これを，今度はクラウド側からみてみます．3Gまでの通信ネットワークは，クラウドにとっては親和性があまりなく，通信業界側の通信のやり取りを，インターネットの通信方法に合わせる仕組みを使って，インターネットに接続させていました．4Gになり音声通話はデータ通信によるアプリケーションの１つとなりました．そして5Gでやっと通信ネットワークの動作をクラウドのやり方で理解できるようになったといえます．こうなると，大手クラウド事業者にとっては，通信ネットワークがクラウドの延長線上にある設備として感じられるようになるでしょう．5Gの通信ネットワークは「クラウド化」により，インターネットの技術をかなり取り込んだのです（**図3**）．

モバイル通信業界の技術競争の構図

通信ネットワーク技術の進化は，新たな端末機器の登場，新たな利用シーンの開拓，新たな市場の拡大，そしてさらなる設備投資へ，という正のスパイラルを描いてエコシステムが成長し，それは20年以上続いてきました．世界的には，途上国も含めると，固定ブロードバンドよりもモバイルブロードバンドのほうが市場のすそ野が広がったことから，近年の世界の通信業界の成長はモバイルブロードバンド主導で進んできました．

電話ネットワーク等のレガシーなネットワークを除く通信ネットワーク技術においては，かつて企業単位，国・地域単位でさまざまな技術規格が世界に併存していたのですが，機器の量産化が低廉化につながり，サービス料金が低下し普及を加速させるという流れが起こり，技術規格も少数に収れんすることとなりました．

モバイル通信方式の技術規格は，2G方式では企業単位，国・地域単位で乱立して



出典：情報通信総合研究所作成

図３　通信ネットワークの仮想化・クラウド化（概略図）

おり，開発競争は進んだものの，導入規模の拡張に成功した欧州方式が世界の主導的立場を確立しました．3G方式では，欧州方式対北米方式，という構図で開発が進んだものの，結果的には米国方式を主導するクアルコム（米国）が欧州市場への参入を優先するかたちとなり，世界的には欧州方式が一強となりました．しかし当時は，この欧州方式を採用していなかったのが，市場が急成長していた中国です．中国は独自技術の開発を3G方式から積極的に進めており，他国での採用には至らなかったものの自国市場の規模が極めて大きく，技術力を高めていきました．

その中国方式と欧州方式が融合したのが4G方式で，そこに日本も技術，規格化のプロセス等において多大なる貢献をしてきました．したがって，モバイル通信方式は4Gで世界統一が達成されたといえます．

通信方式の乱立からの収れんという流れの中では，それだけ多くの企業が技術開発を進め，主導権争いをする中で，結果として生き残った企業が良いポジションを取ることができます．2Gで世界の主導的立場に立ったのはエリクソン（スウェーデン）とノキア（フィンランド）という北欧勢でした．3Gで米国方式を主導したのはクアルコムでした．中国勢は4Gで急速に世界市場での存在感を増しましたが，その中でもっとも活躍したのがファーウェイ（中国）です．

このように，技術開発においても競争がその進化を促す力となっていたことは間違いありません．ライバルがいれば，負けまいと動くインセンティブも働きやすいわけです．4G時代では，世界の主導的通信機器ベンダは3強となっていました．エリクソン，ノキア，ファーウェイです．世界の通信事業者の多くは，彼らが製造するモバイル通信基地局（アンテナから電波を送受信する通信設備）を数多く設置して，つながるエリアを整備してきました．

では5Gではどうでしょうか．5Gは世界統一のモバイル通信規格として，4Gで実現していた機能をさらに高度化する提案が主に大手機器ベンダ各社からなされ，仕様にそうした提案が盛り込まれていきます．他の企業では，日本はNTT，NTTドコモ，韓国はサムスンなどがこうした技術規格の標準化活動に積極的に参画していますが，この5G時代になって従来とは異なる構図になってきています．それは「通信機器ベンダを含むテレコム業界対インターネット業界」と表現できます．

新たなプレイヤーの登場と変わる競争の構図

前述のとおり，通信ネットワークの進化では「クラウド化」というインターネット業界でこれまで広く使われてきた技術を取り込む動きがみられます．この「クラウド化」により，世界の通信設備市場は従来の大手機器ベンダ3社主導から，インターネット業界からの参入に直面している状況です．

インターネット技術を使って通信ネットワークを構築しようという動きは10年ほど前から一部ではありましたが，なかなか実現には至りませんでした．小規模の企業向けソリューションなどでは導入事例もあったのですが，通信事業者の規模になると商用レベルで実現するのは難しく，それを本格導入しようとする通信事業者もいませんでした．

しかし，そこに現れたのが楽天モバイルです．楽天モバイルは，もとよりクラウドを活用したインターネットサービスをさまざまな事業領域で提供してきましたが，MVNO（通信事業者の設備を借りてサービスを提供する通信事業者）として通信サービスを提供してきた楽天モバイルがMNO（自社で通信設備を構築・運用する通信事業者）として日本市場へ参入しました．この参入にあたっての競争力として掲げたのが，「クラウド化」とそれを構成する技術の1つである「仮想化」です．

楽天モバイルが成熟するモバイル通信事業に，この新技術を使って新規参入する動きは，世界から注目の的となり，その注目度は現在も継続しています．2019年当時，非常識な参入というとらえ方も一部ではされていました．その技術の難しさは，大手通信機器ベンダも指摘していました．

しかし，楽天モバイルは多くの通信機器ベンダやソフトウェアベンダと協業し，試行錯誤を重ね，成熟した先進市場である日本で商用ネットワークの運用にこぎつけます．日本では契約者の獲得で苦心している楽天モバイルですが，海外からはその先進性が評価されています．「クラウド化」「仮想化」した通信設備で，商用サービスが提供できることが証明されたからです．

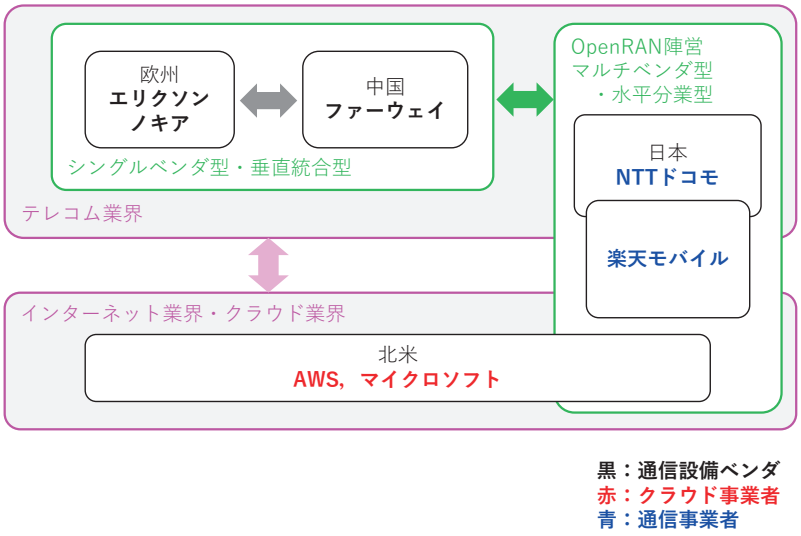
こうした動きと並行して，大手クラウド事業者も通信ネットワーク領域へ参入する準備を整えていきました．その動きが速かったのが，AWS（Amazon Web Services），マイクロソフトという世界のクラウド市場を牽引する2社です．2021年から，彼らは通信事業者に向けてクラウドベースの通信ネットワーク構築を提案するようになりました．テレコム業界からすれば，「黒船来襲」ともいえるでしょうか．

このインターネット業界（クラウド業界）からの参入で，世界のモバイル通信業界における，通信機器ベンダ3強時代が変わるのではないかという見方が浮上してきました．しかし，3強が4強，5強になるのかという主要プレイヤーの数の変化や，順序の入れ替えという単純な話ではありません．このあたりを少し詳しく紹介します．

通信事業者の思いとOpen RAN

ここまで，通信技術の進化の経緯について主に扱ってきましたが，この業界を支えているのは，もちろん通信事業者です．通信事業者が利用者向けにサービスを提供できて初めて，通信市場が形成され，成長できるわけです．

しかし，一部を除いては，世界の通信事業者は各国単位の事業体で，事業規模も大手モバイル通信機器ベンダ3社からみれば小規模です．また十分な技術開発力も持ちません．したがって，各国の通信事業者は世界の大手通信機器ベンダが技術提案し，標準化した技術規格に沿って開発した通信機器を選んで購入するしかないわけです．選択肢が少ない中，価格と性能でベンダの製品を選ぶかしかありませんので，標準化した技術規格以外の通信ネットワークの機能や性能も通信機器ベンダに依存するしかありません．通信事業者は自国内で他社とサービス競争をしているわけですが，ネットワークの機能や性能で差異化しようにも，工夫の余地が限られてしまいます．例えばある通信事業者がファーウェイの最新機能



出典：情報通信総合研究所作成

図 4　5G時代のモバイル通信技術をめぐる競争構図

を導入したいと思っても，ノキアの通信機器で通信ネットワークを構築していれば，それはかなわないわけです．

こうした現状を打破すべく，世界の大手通信事業者数社が手を組みました．通信ネットワークを通信機器ベンダ 1 社に依存するかたちではなく，複数ベンダから通信機器を調達して運用できるようにしようという動きです．これが，Open RANです．RANとは無線アクセスネットワークのことで，電波を届ける基地局設備などがこれを構成する設備にあたります．モバイル通信ネットワークは，大きく「無線アクセスネットワーク（RAN)」と「コアネットワーク（CN)」の 2 つに分類することができます．「無線アクセスネットワーク」は利用者へ電波を届けるための基地局設備が主な設備であり，日本でも通信事業者各社が数万の単位で設置しています．「コアネットワーク」はそうした通信を制御する設備群で構成されており，司令塔の役割を受け持っています．こちらは基地局設備ほどの数はありませんが，高度な処理を大量に行う重要な設備です．

Open RANで変わるベンダ構図

Open RANが実現すると，この無線アクセスネットワークを構成する機器ベンダを複数にすることができます．ノキアの機器によるコアネットワークでエリクソンの機器による無線アクセスネットワークを動かす，といったような運用ができるようになります．こうなると，設備機器自体もさまざまなハードウェア，ソフトウェアベンダの組合せで構成することができ，設計の自由度が増します．「コアネットワーク設備のこのソフトウェアなら」「無線アクセスネットワーク設備のこのハードウェアなら」といったかたちで強みを持つ中小のベンダも，他社と協業することで参入の機会が増えるわけです．

したがって，Open RANの動きが通信ネットワーク構築の手段として定着すると，世界の通信機器ベンダ大手 3 社の寡占であった垂直統合的な市場が，機能ごとに水平に分離されるようになります．この大きな市場で活躍できるプレイヤーの多様化が期待できます．

企業ソリューション向けで実績のある通信機器ベンダや，日本市場では通信事業者向けで実績のあるメーカーは，通信事業者向けの世界市場でシェア上位を占めるには至りませんでした．それは，世界の通信事業者が通信機器ベンダに対し，事業規模の大きさを活かした低価格や通信ネットワークの運用まで含めた総合力を求めたことから，シングルベンダ型・垂直統合型の提案が選ばれてきたためです．しかし，Open RANの導入が進めば，世界シェア上位企業以外にも事業機会の広がりを期待できます（**図 4**）．

では，AWS，マイクロソフトなどはどの領域を狙うのでしょうか．ここまでの彼らの動きを見る限り，コアネットワーク設備，無線アクセスネットワーク設備のソフトウェア領域から参入しようとしています．

特にコアネットワーク設備でいえば，ソフトウェアを彼らの自社クラウド上で運用すればよいわけで，新たなハードウェアを製造しなくてもよいのです．

また，無線アクセスネットワーク設備領域でもそのすべてではなく，自社クラウドで手が届くところまでを提供するような提案を行っています．自社の得意とする領域で，自社が持つ資産を活かした提案ということになり，逆にいえば通信ネットワークのすべてを自社に乗り換えさせよう，という提案までにはなっていません．

AWSやマイクロソフトが通信事業者の通信ネットワーク領域を今後どこまで広げて狙うのかは注目すべきですが，彼らは通信機器ベンダとしてハードウェア販売を生業としているわけではないため，既存のリソースからハードウェア販売に事業拡張するシナリオは想像しにくいといえます．もしそこへ事業領域を広げようとするなら，通信機器ベンダを買収するなどの動きをみせるのではないでしょうか．

株式会社 情報通信総合研究所
ICTリサーチ・コンサルティング部
主席研究員 岸田重行

URL https://journal.ntt.co.jp/article/23464
DOI https://doi.org/10.60249/23101101

NTT物性科学基礎研究所
フェロー

山口浩司 Hiroshi Yamaguchi

ナノメカニクス技術と超高速マグノフォニック技術で，電気，光に続く第三の信号媒体が登場

IOWN（Innovative Optical and Wireless Network）では，ネットワークはもとより，コンピュータの内部も電気信号から光信号への変革をめざしています．これを実現するうえで，光をデバイスの中に閉じ込めるフォトニック結晶により実現できる光トランジスタが大きなカギを握っています．一方，全く異なるアプローチとして，ギガヘルツ領域まで高周波化した音響波（弾性振動波）を用いたデバイス技術も広く研究されています．その技術をさらに進展させ，音響波の伝搬をナノスケール領域で制御することにより，低消費電力の情報処理や超高感度のセンシング技術を実現しようという基礎研究がナノメカニクス技術です．例えばフォノニック結晶と呼ばれるナノスケールの人工構造を用いて，音響波をデバイスの所望の領域に閉じ込めたり伝搬を制御したりする技術はその一例です．こうしたナノメカニカル技術の実現をめざして研究に取り組むNTT物性科学基礎研究所 山口浩司フェローに研究の現状と将来性，また先端研究を取り巻く情勢の変化，さらには，その中での研究の進め方に関する思いを伺いました．

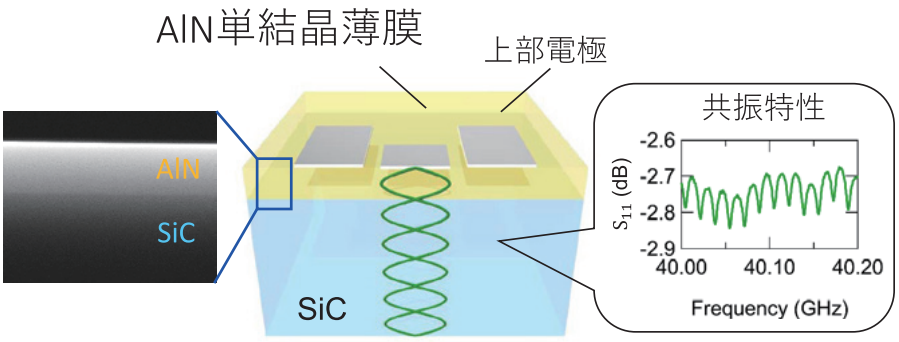
ナノメカニクス技術と超高速マグノフォニック技術の活用で新しい機能デバイスの実現をめざす

現在，手掛けていらっしゃる研究について教えていただけますでしょうか．

ナノメカニクス技術に関する研究を10年以上続けています．光デバイスや半導体デバイス等は，光や電子等の物性的現象を応用したものですが，ナノメカニクスは微細な構造が持つ音響振動の力学的な性質を利用するものです．音響振動とは例えば机の端を「コン」とたたくと，その音が逆の端まで振動として伝わっていくものですが，例えば音叉などを「コン」とたたくと，その振動は決まった音の高さでずっと続くわけですね．デバイス応用としては，「ナノ」の世界ではありませんがクォーツ時計やPCのクロック等に用いられている水晶振動子があります．水晶の切片（薄膜）に電圧を加えることで水晶が非常に精度の高い周波数で振動します．この現象を応用して時計やPCのクロックに精度の高い周波数の信号を提供しています．こうした弾性的な音響振動を素子に活用する技術として，MEMS（Micro Electro Mechanical Systems）が活発に研究されています．ナノメカニクス技術は，MEMS の次世代技術ともいうべきもので，振動特性における非線形性の利用や量子デバイス技術との融合により，MEMSにはない技術を提供しています（**表**）．例えば，「非線形性」というのは耳慣れない言葉かと思いますが，入力と出力が比例しないことを意味します．実はダイオードやトランジスタなどの半導体素子は，コイルやコンデンサ，抵抗などの「線形」な特性を持つ素子にはない非線形性を持つことで，さまざまな機能を持たせることに成功しました．例えば，抵抗器では加えた電圧に比例する電流が流れますが，ダイオードでは，それらは比例しません．さらにトランジスタでは電極に加えた電圧や電流によって，この非線形特性が変化します．音響振動の場合，この特徴は材料に加えた力に対し振動の大きさが比例しないことに相当しますが，微細化に伴い，このような非線形性の影響は顕著になります．この特性を活用した「非線形」ナノメカニカル素子を実現することにより，ダイオードやトランジスタなどと同じような革新的機能を持つナノメカニカル素子をつくり出すことをめざしています．また，量子デバイス技術と組み合わせることにより，新しい機能を出すことも期待されています．例えば，量子ドットと組み合わせることで，原子核の直径に相当する極めて微細な振動検出が可能となります．

表　エレクトロニクスとメカニクスにおける素子と機能の比較

	線形素子	非線型素子		量子素子
		二端子素子	三端子素子	
エレクトロニクス	インダクタ コンデンサ 抵抗器	ダイオード	トランジスタ	量子ビット 量子メモリ
	同調器 フィルタ	検波 整流	増幅・スイッチ メモリ・演算	量子計算 量子計測
メカニクス	共振器	今後の研究対象		
	高周波フィルタ センサ・ジャイロ マイクロフォン			



M. Kurosu et al., Appl. Phys. Lett. 122, 122201 (2023)

図1　窒化物半導体単結晶を用いて作製した音響振動子とその共振特性

また，半導体レーザ等と組み合わせることで，光信号の制御も可能となります．これらの応用にあたっては，GHzを超える周波数による超高速動作が重要となります．

最近取り組んでいるテーマとしては，量子デバイスとナノメカニクスを融合させたフォノンハイブリッドデバイスに着目しています．フォノンとは音響振動の最小単位のことで，量子技術との融合によって重要視される存在になってきています．2019年度まで，文部科学省の新学術領域研究「ハイブリッド量子科学」プロジェクトの研究代表の1人として，フォノンを用いた量子技術を開拓してきました．そこでは，半導体量子構造と組み合わせることにより，新しい機能をナノメカニクス技術に取り込むことに成功しました．その後，新しいフォノンハイブリッドデバイスとして，半導体だけではなく，磁性体，希土類元素，溶液など，さまざまな物理系との融合に取り組んでいます．

例えば，光を閉じ込めるフォトニック結晶に対して，音響振動を閉じ込めるフォノニック結晶という極微細な人工構造の研究をこれまで進めてきました．最近，この構造と強磁性材料を組み合わせることにより，強磁性共鳴という現象を従来手法の10000分の1という小さな領域の中で引き起こすことに成功しました．強磁性共鳴というのは，磁性体が決まった周波数の交流信号に対して敏感に反応する現象で，超高感度の磁気センサや磁性体を使った情報処理などに応用されることが期待されています．これはナノメカニクスと磁性体の新しいハイブリッドデバイスの例です．また，ナノメカニクス技術で基盤技術として利用できる音響振動子の新しい素材として，窒化物半導体単結晶を使って，30 GHz以上という高い周波数で動作する振動子を実現しました（**図1**）．ハイブリッドデバイスとしてさまざまな材料や量子構造と組み合わせることで超高速動作が可能となるだけではなく，携帯端末の高周波フィルタなど，情報端末技術の発展にも今後インパクトを与える可能性のある成果と考えています．

日本学術振興会のプロジェクトも立ち上げたとお伺いしました．

2023年4月より，日本学術振興会（JSPS）のプロジェクトとして，「超高速マグノフォノニック技術」というテーマで東京大学との共同研究を立ち上げました．

PC等のメモリは，半導体の特定の領域に電子がたまっているかどうかで「0」と「1」の状態を記憶していますが，この半導体の代わりに磁性体の持つ「N極」「S極」を「0」「1」に対応させて電子デバイスに情報を記憶する，MRAM（Magnetoresistive Random Access Memory）が登場しています．このMRAMに

代表されるような磁性体を使った技術と，振動を扱う技術を組み合わせるのが「超高速マグノフォノニクス技術」です（**図2**）．

強磁性材料は，高いものでは100 GHzという極めて高い周波数で動作し，一方でその状態を記憶できる不揮発性という特徴を有します．こうした強磁性材料とフォノンを組み合わせて動作させることで，強磁性体が持つ不揮発性を活用した超高速のハイブリッドデバイスを実現できます．例えば，携帯端末に使われているセンサやタイミングデバイスの中で組み合わせてしまえば，高周波信号処理においてプログラム動作ができる可能性があります．また，通常用いられている電気回路では周波数が高くなると，電気信号は電磁波として外に漏れ出てくるので回路間の干渉が強くなりますが，マグノフォノニクス技術を用いてこの干渉を避けることが可能となれば，電気信号に変わる新しい媒体としてフォノン信号が活用できます．さらにその先の応用として，極低温が必要な超伝導量子干渉デバイスに匹敵する感度の磁気センシングが常温で実現できれば，脳磁計などの医療機器への応用が可能となります．マグノフォノニクスデバイスはミクロンサイズの超小型高周波アンテナとしての応用も提案されており，携帯端末の性能を大きく変える可能性もあります．こうした応用を視野に入れながら，まだ解明されていない部分が多い磁性と振動の相互作用など，物性的側面も含めた基礎科学としての研究も展開していきたいと考えています．

内向き志向の脱却と研究協力体制の構築がカギ

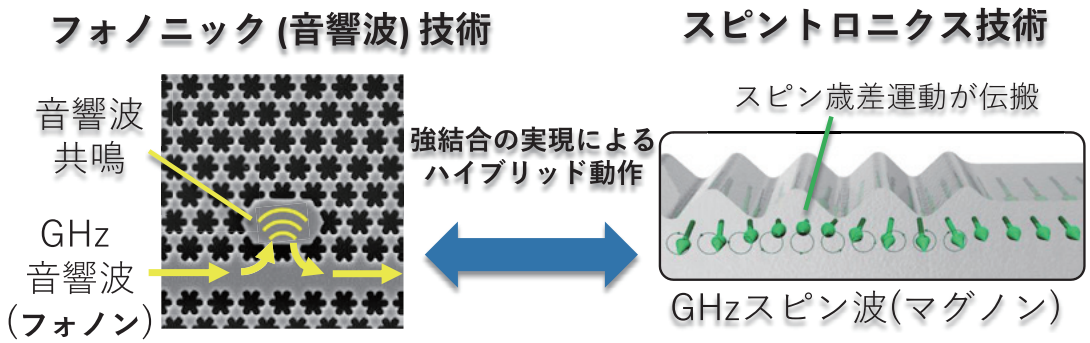
こうした先端研究を取り巻く情勢が大きく変化していますね．

3つの大きな変化を感じています．

まず，海外の研究者とのつながりが薄くなったことです．コロナ禍で国際会議や学会がオンラインにシフトしましたが，リアルな会議ではオンラインにはないコンタクトやディスカッションの密度があります．2023年に入り海外の国際会議で講演を3回ほど行ってきたのですが，新型コロナウイルス感染症が5類へ移行した現在でも，こうした国際会議等への日本人の参加が過去に比較して減少しているように感じています．特に若手研究者の渡航が少ないように思います．理由はコロナウイルスへの警戒心がいまだに高いことに加え，燃料費の上昇やシベリア上空を通過できないことによる長航路化等に起因した航空運賃の高騰が関係しているのではないかと想像しています．研究が先端化するほど単独グループでの研究では対応が困難になり，内外の研究者との研究交流は必須要件にもなってきます．こうしたときに海外の研究者との人的つながりが大きな力を発揮します．若手人材の国際化はさまざまな業種で重要な課題かと思いますが，研究の分野において若手研究者を海外に派遣して共同研究を行うことはとても大きな意義があります．この鍵になるのが海外研究者とのつながりです．日本は最近内向き志向だといわれますが，少しでも海外との接点を増やし，研究の国際化・多角化を進めるべきだと思います．

2番目は，中国，韓国，特に中国の進化が著しいことです．中国は人口も多く研究への資金投入規模も桁違いに多くあります．これを単純に比例計算しても優秀な研究者や優れた環境の研究所の数は圧倒的に多いということになります．特に新しい分野においてこうした傾向が顕著に出ています．従来から日本そしてNTTが得意としてきた光技術や半導体技術は，まだ世界をリードできるポジションにいると思いますが，油断はできません．分野やテーマの選択を含め，共同研究といった研究プロセス等もさらなる工夫が必要になると思いますし，それを模索中です．

そして3番目が生成AI（人工知能）の登場です．論文のabstractやintroductionの執筆はもとより，実験装置のプログラムの自動作成等，生成AIを用いれば多くの作業が効率化できそうです．これはまさに前述の研究プロセスの変化を生むものです．海外では積極的に活用していく方針も見受けられる一方で，著作権や研究成果の信ぴょう性の問題や使う側のリテラシーの問題もあり，各方面で検討が行われています．今後，この技術をどのように私たちの研究に活用していくかは，大きな課題ですね．



D. Hatanaka et al., Phys. Rev. Applied 19, 054071 (2023)

図2　超高速マグノフォノニクス技術の概念図

「寄り道研究」のススメ

研究者として心掛けていることを教えてください.

前回のインタビューのときは，①人と違うゴールを設定すること，②自分の持ち味を軸足にし，もう片方の足を別の分野へ踏み出す，③アンテナを高く・広く張って情報収集する，ということをお話ししましたが，その補足や私の研究スタイルを含み 3 点ほどお話しさせていただきます.

基礎研究の新しい分野では，早い段階で実績を残すことがその後の注目度を大きく左右するため，多くの研究者は明確にストーリーが組めてやるべきことがはっきりしている研究に照準を合わせてきます.

しかし，そのようなターゲットは他の研究者からも容易に考え得るテーマなので，そこに熾烈な競争が出てきます．そこで，最初から人と違うゴールを設定する，というのが前回お話しした内容なのですが，一方，研究の途中で興味のあるテーマが出てきたら，最初のゴールはそのままにしていったんそのテーマに寄り道するアプローチも重要だと考えています．もし，そのテーマがさらに大きなインパクトを与えそうならば，思い切ってその方向にゴールを変更します．一方，うまくいきそうもなければ，元のゴールに戻すだけの話です．最初の考えを貫くのも重要ですが，より自由な発想の下，フレキシブルにテーマを変更していくことも大事だと考えます.

次に，共同研究でも，学会活動でも，チーム内の研究分担でも，何かを共同で行う場合，「give and take」とよくいわれます．このとき，多くの人は50% even，あわよくばtakeを多くということを考えがちです．ところが，パートナーも同じようなことを考えているので，せめぎ合いの状態になります．そこで，7 対 3 くらいでgiveすることを考えると，パートナーにとって「この人と組むのはメリットが大きい」と思ってもらうことができ，物事がうまく進むようになります．これは過去の上司の教えです．7 対 3 で考えていても実際にやってみると結構 6 対 4 になっていたりします．また逆転して 4 対 6 に結果としてなることもあるでしょう．大事なことは，パートナーが前向きに取り組んでくれる条件をどのように整えるか，という点にあるわけです.

さらには，特に基礎研究の場合はそうだと思いますが，それぞれの研究者の考えやアイデアには上も下もない，つまり上司であっても部下であっても対等であるべきと考えています．まさに，上記の 7 対 3 のgive and take を上司と部下の間でも考えるべきです．部下であっても相手の立場を自分と同じレベルで尊重し，正しい知識とロジックに基づいて判断を下すことが重要なのです．その結果遠慮のない情報交換が生まれ，良いアイデアが出てくるのです．これは，NTT基礎研究所の吉田庄司初代所長が掲げた「独善に陥いらず強固な意志と謙虚さをもって自主的・能動的に行動することを所員全員の共通の心得とする」に通じているところでもあります．吉田所長はこの考えを込めて「will」という単語を基礎研究所のめざすものとされました．その重要性は40年近くたった現在でも全く変わっていないと思います.

研究プロセスを効率化して自分の持ち味を大切に

後進の研究者へのメッセージをお願いします.

就職して研究者としての第一歩を歩み出すとき，学生時代の専門分野とは異なる分野の研究に携わる方も多いと思います．私は学生時代，素粒子物理の理論研究がテーマだったのですが，NTTの研究所に入社した際には，全く異なる半導体の実験研究に携わりました．当時はほとんど素人研究者に近い状態で，自分が学生時代に頑張って積み重ねた知識は，結局は全く意味をなさなくなるのではないか，と暗い気持ちになったりしました．しかし，年月を経て，新しく始めたナノメカニクスの研究では，意外に学生時代の知識をうまく活用できることに気が付きました．あるいは，過去の専門知識が潜在的に働き，ナノメカニクスの研究を始めるきっかけになったのかもしれません．このようなことは専門知識に関することだけではなく，例えばクラブ活動やボランティア活動なども含め，過去のあらゆる経験についていえることではないでしょうか．何かに関して過去に大きな努力をした人ほど，その経験を何とか活かそうと考えると思いますし，そのために努力をしたわけです．しかし，新しい環境に入った際，その経験はすぐにはうまく活かせないことが多いと思います．だからといって，すぐにその環境を否定するのではなく，何らかのかたちで活かせるチャンスは必ず訪れると大きく構えて，その後の人生設計を行うことが大事だと思います.

さて，働き方改革やワークライフバランスという言葉が一般化してきて，これまでとは研究に取り組む環境が大きく変化してきています．また，誰でも検索エンジンやAIに聞けばキーボード操作 1 つでさまざまな情報を取り出すことができる，「情報のユニバーサル化」が進んできており，これまで経験を積んだ研究者しかできなかったことが，誰でも簡単にできるような時代になりつつあります．このような環境で独自性の高い研究を進めていくには，自分のもっとも得意とする部分を大事にして効率良く仕事をこなすことが，さらに重要になってきています．研究者本人も自分はいったいどこで勝負をかけるか，という点を改めて整理するとともに，上司や指導者も画一的な方法論を押し付けるのではなく，それぞれの個性を尊重してマネジメントしていくことがとても重要になってきていますね.

URL https://journal.ntt.co.jp/article/23466
DOI https://doi.org/10.60249/23101201

NTTデータグループ　技術革新統括本部
システム技術本部　サイバーセキュリティ技術部

清宮聡史　Satoshi Seimiya

ソフトウェアサプライチェーンにおけるセキュリティの要：SBOM

最近，サイバー攻撃やセキュリティに関する話題が，メディア等に頻繁に登場しています．世の中を便利にする各種システムはもちろんのこと，それを使うためのスマートフォン等の端末に至るまで，ソフトウェアへの依存が高まっている中，サイバー攻撃等の多くはこうしたソフトウェアに内在する脆弱性を突いて行われています．脆弱性をソフトウェア開発の段階から管理して混入を防ぐために，SBOM（Software Bill of Materials）というソフトウェアの部品表を活用する動きがグローバルに展開し始めています．NTTデータグループ 技術革新統括本部 システム技術本部 サイバーセキュリティ技術部 清宮聡史氏に，SBOMを活用したソフトウェア脆弱性管理，SBOMをベースとしたセキュリティの専門家をめざす思いを伺いました．

SBOMによるソフトウェア脆弱性管理がグローバルなトレンド

現在，手掛けている開発の概要をお聞かせいただけますか．

私は，2018年にNTTデータに入社以降，商用システム開発におけるセキュリティ確保施策の推進に取り組んでいます．特に，2022年度からはソフトウェアサプライチェーンセキュリティ関連の開発に包括的に取り組むようになりました．現在，SBOM（Software Bill of Materials）統合管理に関する開発をメインに担当しています．SBOMは，オープンソースソフトウェア（OSS）や商用ソフトウェアを含むソフトウェアライブラリやモジュール等のコンポーネント（群）およびそれらの関連性と補足情報の一覧であるソフトウェア部品表のことです．

NTT DATAは，SIerとして公共，金融，法人，各分野のお客さまへ，サービスやシステムを提供していますが，OSSをベースとしたシステム開発が増加する中で，使っていたOSSの中に，気付かないうちに脆弱性が含まれていたケースも出ています．こうした脆弱性を突いて，悪意のある第三者が攻撃を仕掛けてくるという事例も世の中で増えています．2023年度の独立行政法人情報処理推進機構（IPA）による『情報セキュリティ10大脅威』では，「サプライチェーンの弱点を悪用した攻撃」が2位にランクされています．

NTT DATAでは，2022年度より施策要件を満たすすべてのWebアプリケーション開発プロジェクトにおいて，結合テストの段階で，IAST（Interactive Application Security Testing）という，アプリケーションが動作した個所の処理に脆弱性が含まれていないかを検査するツールの活用を全社的にルール化しており，これにバンドルされているSCA（Software Composition Analysis）ツールにより一部のソフトウェア部品は可視化できていました．しかし，それだけでは，IASTツールがサポートしていないテクノロジを用いてWebアプリケーションを開発される場合や外部から調達した機器・サービス（ネットワーク機器，Software as a Service等）をカスタマイズしてお客さまに納品する場合等において，ソフトウェア部品を可視化できません．そこでSBOMを活用して，IAST対象のソフトウェアだけではなく，サードパーティのソフトウェア部品も管理していくことになりました．

さて，SBOMは，「サプライヤ名」「コンポーネント名」「コンポーネントのバージョン」「依存関係」「SBOMの作成者」「タイムスタンプ」「その他の一意な識別子」等の要素で構成されソフトウェアの脆弱性管理，ライセンス管理の一助になることが世界で期待されています．2021年5月の米国大統領令を受け，米国立標準技術研究所（NIST）等でガイドライン・ガイダンス整備等が進行中であり，欧州でも「EUサイバーレジリエンス法」草案が出され，SBOMの取得を推奨する動きが世界的に広がってきています．日本においても，経済安全保障推進法に基づき，2024年春ごろから段階的に基幹インフラの事前審査が始まる予定であるとともに，内閣サイバーセキュリティセンター（NISC）公開の『サイバーセキュリティ2023』でも，「SBOM」の実証・早期実用展開につ

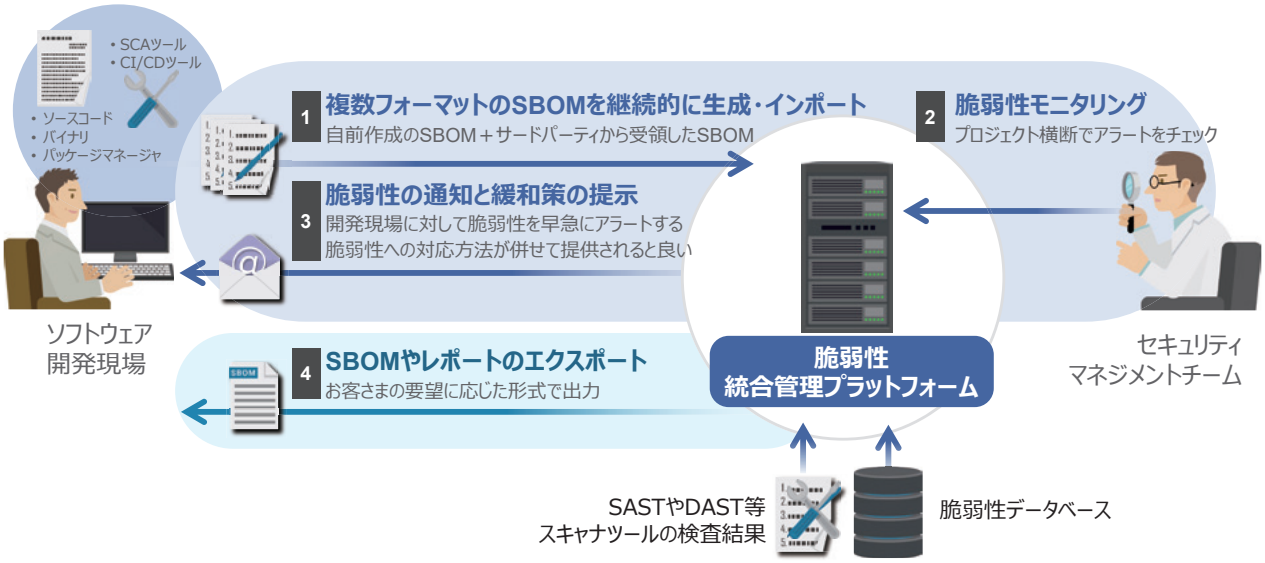


図1　脆弱性統合管理プラットフォーム

いて明記されています．こうした動きの中，私たちは，セキュリティガバナンスの観点から，開発プロジェクトにおける「脆弱性対応の効率化」「お客さまへのSBOM納品」を，セキュリティサービスの観点から，「お客さまへのサプライチェーンセキュリティリスク管理サービスの提供」の実現をめざして，SBOMの利活用を推進しています．

SBOMはグローバルな取り組みが進みつつあるのですね．

SBOMは，グローバルな展開が進みつつありますが，グローバルで統一的なレジストリ管理団体はなく（2023年8月現在），IETF（Internet Engineering Task Force）において，その構想を検討しています．したがって，各企業等で独自にSBOMを作成・活用しているのが現状です．その結果，①SCAツールごとにサポート対象のテクノロジ・参照先の脆弱性データベースが異なる，②大部分のSBOMで米国商務省電気通信情報局（NTIA：National Telecommunications and Information Administration）の定める最小構成要素を満たしていない（Chainguard社の品質調査），③SBOMは開発工程の中で一度作成するだけでは不十分でソフトウェアコンポーネント等の変更の都度作成しなければならない，等の課題があります．

こうした課題への対応策として，NTTデータグループ会社ではSBOMの生成からインポート，データの管理，脆弱性情報と紐付けてソフトウェアのセキュリティリスク管理を包括的に実現するための「脆弱性統合管理プラットフォーム」の開発を進めています．また，SBOMを活用し，NTT DATA海外グループ会社と連携し，お客さまのサプライチェーンセキュリティを包括的に保護するマネージドサービス「サプライチェーンセキュリティマネージドサービス」の開発も進めています．

「脆弱性統合管理プラットフォーム」はNTT関連各社との共同プロジェクトにて開発を進めており，次の4つの機能で構成されています（**図1**）．

まず，自前作成，サードパーティから受領したSBOMにかかわらず複数フォーマットのSBOMを継続的に生成・インポートする機能．2番目は，プロジェクト横断でアラートをチェックする脆弱性モニタリング機能，3番目は，開発現場に対して脆弱性を早急にアラートするとともに脆弱性への対応方法が併せて提示される，脆弱性の通知と緩和策の提示機能，そして，お客さまの要望に応じた形式で出力するSBOMやレポートのエクスポート機能です．「脆弱性統合管理プラットフォーム」により，全社的に必要とされる部品の情報をルールとして定めておくことで品質が悪いソフトウェアを排除するとともに，脆弱性情報とソフトウェア部品表を結びつける情報が一部抜けているような不完全なSBOMに対して，不足情報を付加するかたちで使えるSBOMにするといったことも可能になります．これにより，新規脆弱性発生時の対応稼働を1プロジェクト当り約1.5時間，年間では約53時間削減でき（NTT DATAの社内モデルによる試算値），人為的な確認・報告ミスの削減，脆弱性を放置している時間の削減が見込まれます．また，個々のSCAツールから出力される各SBOMについて，構成要素，記載内容等の整合性について社内標準との照合が可能になるとともに，提供するファイルフォーマットを含むお客さまの要望に応じて，脆弱性統合管理プラットフォームから臨機応変に，納品するシステム全体に関するSBOMを提供可能，といった社内のセキュリティガバナンスへの効果が期待できます．

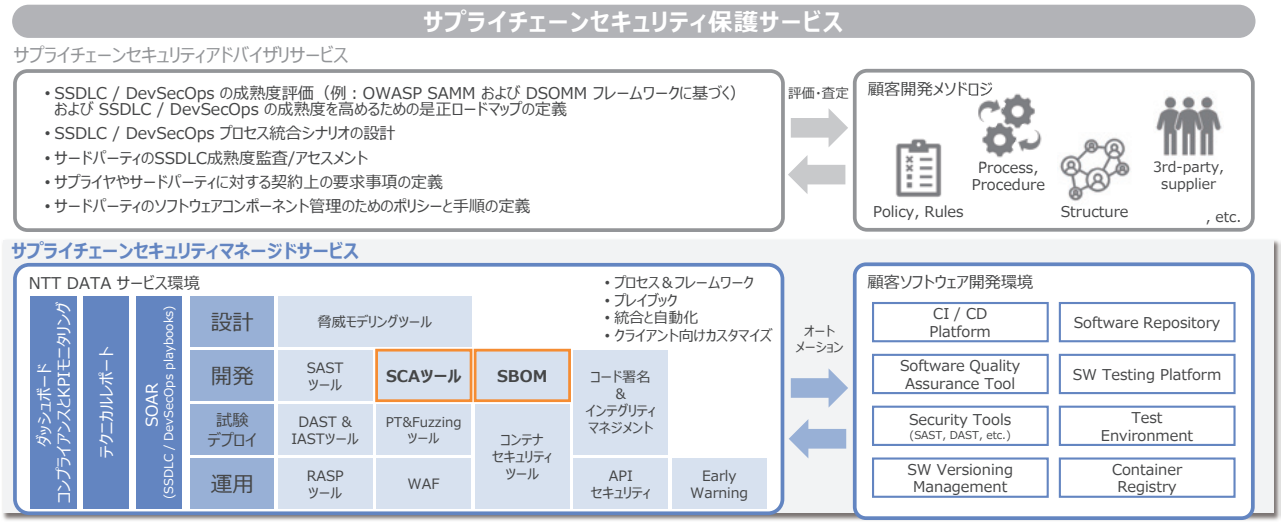


図2　サプライチェーンセキュリティマネージドサービス

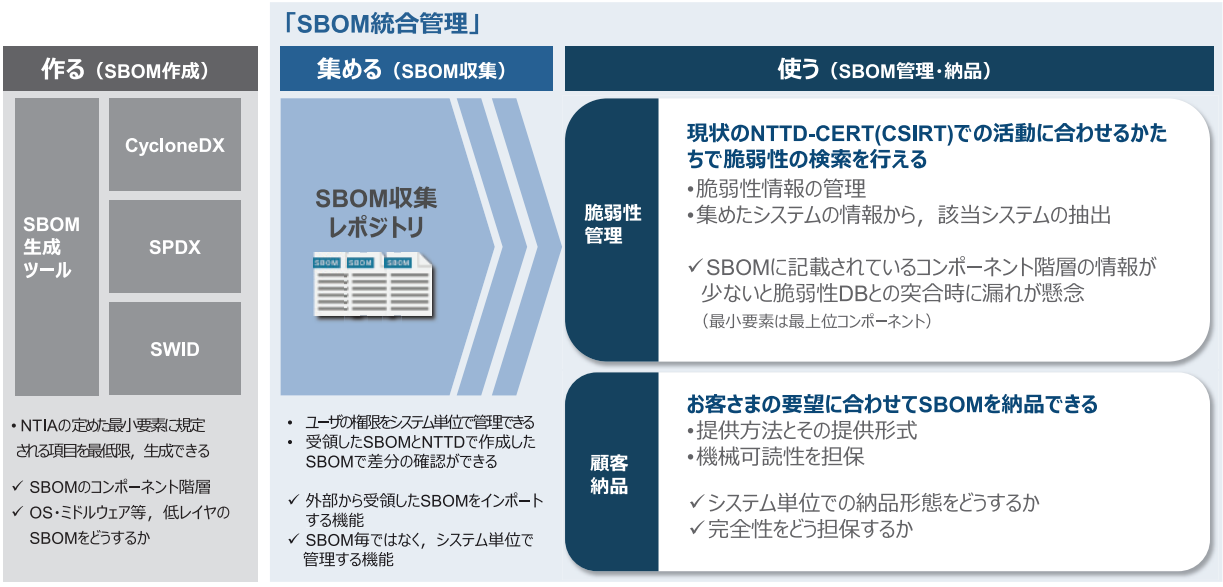


図3　社内でのSBOM統合管理の実現に向けて

「サプライチェーンセキュリティマネージドサービス」は，世の中でSBOMが一般化してその対応が求められてくると，その作成や活用に困るお客さまがたくさん出てくることが容易に想像されます．そういったところにNTT DATAのエンジニアが入ってサプライチェーンセキュリティに関して企画から実装，最終的なレポーティングまでワンストップで行えるようなサービスです（**図2**）．その中のサービスメニューの1つとして，お客さまのアプリケーションのSBOM生成・管理・脆弱性に対応するサービスを，海外から順次提供開始する予定です．

こうしたプラットフォームやサービスをベースとして，社内におけるSBOM統合管理の実現に向けて，SBOMのライフサイクルの3観点（「作る」「集める」「使う」）で，SBOM統合管理のToBe像とAsIsのギャップを抽出し，ツール類，収集体制，SBOM統合管理ガイドライン等の整備といった各課題の達成に向け，PoC（Proof of Concept）を実施しています（**図3**）．また，NTT DATA（海外グループ会社）のお客さまの開発チームとPoCを実施し，商用のソフトウェアを対象にSBOM活用のノウハウを蓄積し，サービス開発にフィードバックするといった取り

組みを継続しています．さらに，2022年11月よりNTTグループとNECで「セキュリティトランスペアレンシー確保技術」に関するフィールド実証を開始しました．2023年度には，SCAツールで出力されたSBOMの利活用，バックドア検索等の技術を使い，ステークホルダーやソフトウェアサプライチェーンの中のリスク低減を検討する，コンソーシアムの設立も予定しており，NTTデータグループ社も社内のPoCで得た知見をベースにこれに参画します．

セキュリティの専門家としてSBOMの普及に貢献できる日をめざして

開発者としてスキルの維持，スキルアップはどうしていますか．

学生時代は，無線情報通信関連の研究をしており，ソフトウェアやセキュリティとは直接関係のないテーマの研究を行っていました．NTTデータ入社後の研修の中でソフトウェアやセキュリティに関する基本的なスキルを習得し，現在の部署においては，セキュリティの診断を実際に実施する等のOJTを含む研修で，技術的なスキルをかなり習得することができました．

こうした中で業務を進めていくうえでは，技術以外に大きく4つのスキルが必要と考えます．まず，情報収集力です．SBOMは世界的に取り組みがなされており，コミュニティにおいてもSBOMの議論が多くなっています．日本のニュースに限らず，海外の人も含めて，SBOMソサイエティの人はどのようなことを考えているかという点も含めて情報収集することが1つポイントと思います．2番目は，分析力です．SBOMに関してさまざまな情報が世界中にあふれていますが，それぞれ正しい情報も不確かな情報もありますので，複数の情報源を比較したり組み合わせたりすることで分析していく力が必要だと思います．3番目が実装力です．仮説を立て，それがうまく進みそうだと思ったら自分で手を動かして試してみるという力です．権威のある論文であってもそれを鵜呑みにせず，どのようなアルゴリズムでつくられているのかといった本質を見極める力が必要だと思います．そして4番目は発信力です．自分なりに考えた結果を発信していかないことには，ディスカッションも，普及も進みません．

現在，SBOMに関して多くのOSSやツールが出てきていますが，単にそれを使っているだけでは，研究開発ではなく運用の話になるので，技術的に新規性を見出していくうえでは，それをブラックボックスにしないことを心掛けています．OSSやツールは省力化につながるから使うという場面ももちろんありますが，独自の視点で新規性を出していく場面では，OSSやツールの中のソースコードを読み解き，どのようなロジックで実装されているかというところまで深く入り込んでみることを意識し，それを通してさまざまなスキル向上を図っています．

事業会社は異動がありますが，こうしたスキルを活かして将来的に何を経験したいのでしょうか．

以前，Apache Log4jというオープンソースログ出力ライブラリの脆弱性対応のときに，うまく情報が集まらず苦労していたのですが，IASTを導入しているところでは情報が取れているのではないかと考え，実際に確認したら情報が取れていました．日常業務として対応してきたところが，世界的なソフトウェアコンポーネントの話をきっかけに，日常業務が別のところに応用できるかもしれないという感覚が印象的でした．

また，2022年12月にNTTデータのセキュリティへの取り組みを紹介する講演を行いましたが，その講演を見ていただいた方から直々に別の講演におけるゲスト登壇のお話をいただきました．自分が一生懸命発信したストーリーが誰かの心を動かして，次の発信につながっていくというのがとても印象に残りました．

こうした経験を通して，私としてはやはりセキュリティはとても面白いし，セキュリティに何かを掛け合わせることが，独自のセキュリティの概念や技術を考えるうえで役に立つと思っています．現在，IASTとSBOMを組み合わせたセキュリティ施策の推進を行っていますが，この先，これ以外のさまざまな組み合わせを考えていきたいと思います．そのうえで，最近，お客さま向けの勉強会の実施やお客さまの課題認識等を伺う機会が増えてきているので，社内だけではなく社外で交流しながら，ソフトウェアサプライチェーンのリスク等の話を通してセキュリティの啓発活動を行い，セキュリティの専門家としてキャリアを磨いていきたいと思います．

まずはできる範囲から試してみよう

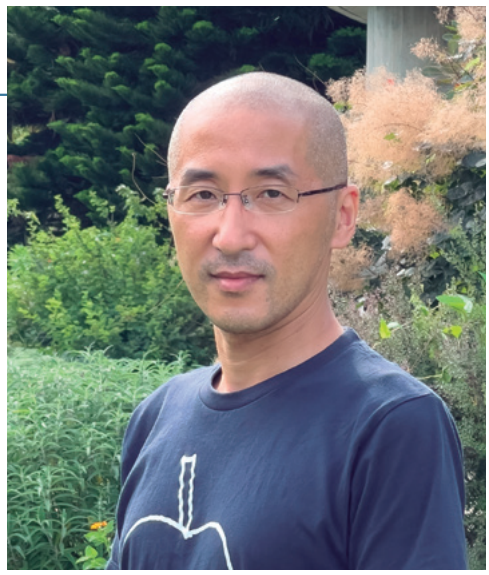
読者，お客さまへのメッセージをお願いします．

現在，SBOMは世界的に各方面でさまざまな方々の間でディスカッションされています．しかし，ソフトウェアサプライチェーンにおけるSBOMは概念的でイメージしづらいうえに，世界統一的なSBOMはまだ存在していないので，活用に当たってはハードルが高いかもしれません．そこで，部品表のサンプルを見てイメージをつかんでいただき，ご自身がかかわっているシステム開発工程の中にその部品表を当てはめて考えてみる等，小さなところから興味を持って試してみることが大切だと感じます．そして，SBOMはさまざまな関連ツールやパッケージも出ているので，できる範囲から試しに使ってみていただけると良いと思っています．

URL https://journal.ntt.co.jp/article/23468
DOI https://doi.org/10.60249/23101301

NTTソフトウェアイノベーションセンタ
特別研究員

藤田智成 Tomonori Fujita



「高信頼なシステムソフトウェア技術」で新たなエコシステムを創出し，グローバルに貢献

インターネットが普及しICTが生活に溶け込んだ現代では，ソフトウェアの信頼性への要求が非常に高まっています．高い性能が求められる分野のソフトウェア開発で現在主流のC言語は，柔軟で自由なハードウェア操作が可能である一方で，開発者の単純な誤りが不具合やセキュリティリスクを招く点が懸念されています．そのため高い性能と現代の要求に合った信頼性を満たすソフトウェア開発のためのプログラミング技術が求められており，C言語に代わる新たなプログラミング言語の取り組みも進んでいます．今回は「高信頼なシステムソフトウェア技術」の研究に取り組む，藤田智成特別研究員にお話を聞きました．

◆PROFILE：2000年早稲田大学大学院理工学研究科修士課程修了．同年，日本電信電話株式会社入社．2015年より特別研究員．オペレーティングシステムをはじめとしたシステムソフトウェアの研究開発に従事．2014年10月日本電信電話株式会社社長表彰，2015年2月情報報処理学会ソフトウェアジャパンアワード等を受賞．

「高性能」「安全性」を両立したRustで新たなソフトウェアを実現

■「高信頼なシステムソフトウェア技術」では，どのような取り組みをされているのでしょうか．

私が研究している「高信頼なシステムソフトウェア技術」とは，ハードウェアの制御を行うシステムソフトウェアがハードウェアの障害やネットワークからの攻撃などに耐え，想定どおりに動作し続けることをめざす技術です．これを達成するにはさまざまな基本技術が必要になり，現在はシステムの停止や外部からの攻撃につながる，ソフトウェアの問題の回避に取り組んでいます．具体的には，システムソフトウェア開発のプログラミング言語として，主流のC言語ではなく「Rust」という開発者の誤りを防ぐための機能（安全性）を備えたプログラミング言語を用いて，高性能なシステムソフトウェアの実現をめざしています．

この研究の背景として，インターネットが普及した現代でソフトウェアの信頼性への要求が高まったことが挙げられます．インターネットが一般に普及し始めた1990年代は，その利用者数も限られていたうえ，用途も生活に影響を与えないものばかりでした．しかし，現在では社会全体でICT活用が活発になり，インターネットが生活インフラに組み込まれ，システムの停止が許容されない状況となっています．さらにクレジットカード番号のような重要な情報をインターネットでやり取りしているため，システムに不備があった場合に金銭的な被害の発生などのセキュリティ事故が起きてしまいます．そのようなトラブルが発生することなく，社会インフラとしてのインターネットが常に想定どおりに動作し続けることが当然とみなされており，インターネットを支えるシステムソフトウェアの信頼性への期待値も非常に上がっています．しかし，信頼性の期待値が大きく変化したにもかかわらず，現在のインターネットを支えるために1990年代に設計されたシステムソフトウェアが数多く使われているという点が大きな問題となっています．

信頼性の高いシステムを実現するためには，ソフトウェアの不具合と外部攻撃の原因となる脆弱性を防ぐ必要があり，プログラミング言語の選択は非常に重要です．現在主流となっているC言語は，開発者がメモリやCPUといったハードウェアに対する柔軟で自由な操作ができるため，ハードウェアの性能を引き出しやすい言語です．しかしC言語は1970年代に開発されたプログラミング言語で，安全性，すなわち不具合や脆弱性を起こす誤りを防ぐために開発者を支援する仕組みは考慮されておらず，リスクが高いことが知られています．2022年にアメリカ国家安全保障局（NSA）は，C言語以外のプログラミング言語を使うことを推奨するガイダンスを発表しています．2000年ごろから，高性能なソフトウェアをターゲットとする安全性を備えたプログラミング言語が数多く提案されていますが，現在ではその中の1つであるRustを用いて，インターネットを支える新しいシステムソフトウェア実現に向けた研究に取り組んでいます．

■プログラミング言語「Rust」の特徴について教えてください.

Rustは「高性能のソフトウェアを安全に実装できる」というのが大きな特徴です．例えばJavaやGo言語のメモリ管理方法は，ソフトウェアの実行中にメモリの使用状況を把握し，使われなくなったメモリ領域を解放する「ガベージコレクション」と呼ばれる仕組みにより不正なメモリ操作を防ぎます．このガベージコレクションは安全なメモリ操作を実現する一方で，ソフトウェアの実行中に動作する仕組みであるため，性能に悪影響を及ぼします．そこでRustでは性能を低下させるガベージコレクションを使わず，ソフトウェアのコンパイル（ソースコード変換）時にメモリの使用状況を割り出し，適切に管理できるように設計されています．「高性能」と「安全性」の両立は難しい問題ですが，Rustは開発者に特有の設計や表現を強制することで，両方を実現しています．

現在私は，オペレーティングシステムとBGP（Border Gateway Protocol）デーモン*の実現に取り組んでいます（**図1**）．オペレーティングシステムに関しては，MicrosoftやGoogleなどの他社の開発者と連携して，Linuxオペレーティングシステムの中核機能（カーネル）をRustで実装することに取り組んでいます．Linuxカーネルのソフトウェア規模や普及状況を考えると，Rustで実装した新たなオペレーティングシステムでLinuxを置き換えることは現実的ではないと考え，C言語で実装されているLinuxカーネルを少しずつRustで置き換えていくことをめざしています．

またインターネットの基幹であるBGPプロトコルをサポートするBGPデーモンは，大規模なクラウドインフラのネットワーク内でも使われるなど，高い性能と信頼性が求められるシステムソフトウェアの1つです．現在C言語で実装されたBGPデーモンが広く使われていますが，複数のCPUを活用するための並列性が低く，最新のハードウェアの性能を引き出せていません．そこでRustが備える並列性を安全に扱う支援を活用し，新たなBGPデーモンを実装したところ，広く使われている実装と比較して5倍以上の性能を実現することができています．

■現在ご研究で苦労されている点について教えてください.

新しいプログラミング技術が広く使われるようになるまでには時間がかかります．特にインフラの基幹となるシステムソフトウェア分野は新しい技術を取り入れるのに時間がかかる傾向があります．

これまでC言語に代わる安全性を備えたプログラミング言語が数多く開発されましたが，システムソフトウェア開発ではいまだにC言語が主流です．その理由の1つは，開発者にとって新しい言語でソフトウェアを開発・保守することが大きな負担であるためだと思われます．

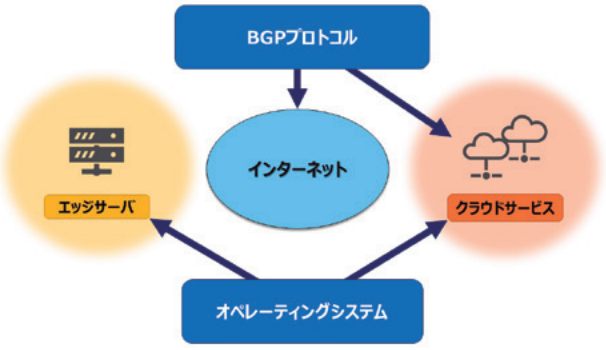


図1　現在ターゲットとしているシステムソフトウェア

またRustの場合は，従来の言語にみられない独自の仕様が普及の障壁になっているといわれています．実際にLinuxカーネルの機能をC言語に加えて，Rustでも実装できるようにする際も賛否両論がありました．議論を経て，Linuxカーネルの機能をRustで実装できるようになりましたが，今のところLinuxカーネルにはRustで実装された機能がありません．

こうした現状を打破する近道はないと思い，まずは「小さな機能から実装して有用性を示す」ことに気を付けています．具体的に，Linuxカーネルのネットワーク通信のハードウェアを制御するデバイスドライバをRustで実装できるようにする機能を提案したところ，開発者から大きな抵抗がありました．そこで影響範囲を小さくして，ネットワークデバイスドライバの一部機能をRustで実装できるようにすることを交渉しています．

オープンソースソフトウェア（OSS）の開発で自分の提案が100%受け入れられることはまれで，私自身も若いころは提案が断られるたびにショックを受けていました．しかしOSSの開発に長年携わる中で，たとえ提案が10%しか通らなかったとしても，他の開発者の意見を取り入れながら提案を改善して進み続ける重要性に気が付きました．

多くの人を巻き込んで世の中に大きなインパクトを与える研究に取り組む

■今後の研究ビジョンについて教えてください.

次のステップとして，Rustのような安全性を備えたプログラミング言語をシステムソフトウェアに適用する価値を示す必要があると考えています．Linuxカーネルの開発コミュニティでも賛否両論あったように，「システムソフトウェアにおいてC言語以外を使うことに十分なメリットがあるか」という問いにはまだ結論が出ていないようです．LinuxカーネルでRustの利用例を増やすためには，Rustで実装された広く使われる機能を採用してもらい，

* デーモン：Linux等のUNIX系OSでメインメモリ上に常駐して特定の機能（利用者の操作とは無関係に処理を行うバックグラウンドプロセス等）を提供するプログラム．

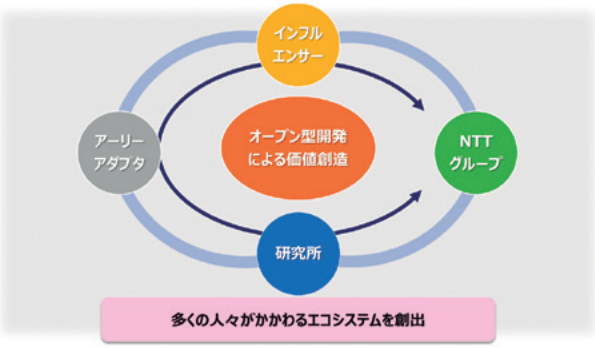


図2　オープン型開発による価値創造のビジョン

不具合や脆弱性に関してメリットを示す必要があるように思います．また安全性を備えたプログラミング言語を使うことですべての不具合や脆弱性を防ぐことはできませんので，例えば設計の不具合を防ぐなど，他のアプローチでも検討を進める予定です．

システムソフトウェアの不具合や脆弱性を防ぐための研究成果をデファクトの技術として普及させることで，業界全体のシステムソフトウェアの信頼性を高めることをめざしています．それによって私たちの生活を支えるインフラの信頼性が向上するだけでなく，従来不具合や脆弱性の対策に費やされてきたリソースが新しい機能開発に使われ，サービスの価値向上につながると考えています．

またNTTが提唱するIOWN（Innovative Optical and Wireless Network）構想において，システムの停止や不正な利用を避けるための技術は非常に重要なものです．IOWNでこれまで以上に生活がデジタルと融合してICTが不可欠になる世界観において，もし「サービスが停止しました」という事態が起きてしまうと利用者の不満はこれまで以上に大きなものになります．そのような事態を回避して安全で快適な社会を実現することをめざして，今後もOSSなどのオープンな開発手法でNTT以外にもさまざまな人がかかわるエコシステムを創出し，グローバルに新たな価値を創造していきます（**図2**）．

■最後に研究者・学生・ビジネスパートナーの方々へ向けてメッセージをお願いします．

私の研究モットーは「多くの人に使われて，人の生活をさらに良くする技術をつくる」ことです．NTTに入社して間もないころに，上司から「研究成果が商用化された場合に，その利益で何人が生活できるのか」と研究テーマについて話をされたのを今でも覚えています．数10名程度の生活しか支えられずグループ内でしか使われない技術をめざすのではなく，「世の中をもっと大きく変えて何万人にも影響するテーマを考えるように」というアドバイスだったと認識しており，現在もこの考え方は大切にしています．

そして技術自体も誰かに使ってもらうことで初めて成長していくものです．多くの人に使ってもらうことで新たなマーケットができて多くの人がそれでお金を稼げるようになる，逆にお金を生み出さない技術は普及しないと考えています．

今後の研究でも新しいマーケットを創出する技術を生み出していくことが目標です．私のグループでは，NTTだけに技術をとどめておくのではなく，OSSなどのオープンな開発手法を使って他社の方と協力しながら世の中に普及させ，そしてより大きなインパクトのある技術に育てていくことでNTTの取り組みが広がるように研究を進めています．国内でNTTと他社が協業する際にはNTTは主導的な立場を取ることもありますが，メジャーなグローバルOSSプロジェクトだとNTTは主要なプレイヤーではありません．そして他社の方と利害関係が完全に一致することはほぼないため，利害関係を調整して自分が向きたい方向に舵を取らなければいけません．そのため新しいコミュニティに参加するたびに，コミュニティのメンバーと直接会って話をする機会を設けたりしています．一見地道な活動ですが，やはりメールやチャットだけだとお互いに伝わらない情報でも，お互いに膝を突き合わせて会話をすることで解像度が上がるため，相手への理解を深めながらコミュニティ内の発言力や影響力を高めています．

インターネットも元々多くの人たちが集まってつくられたもので，これから私自身も世の中にインパクトを与えるために，１人研究室に閉じこもって考えるのではなく，多くの人を巻き込んで協力しながら新たな価値を創出していきます．これから一緒に社会にインパクトを与える活動にぜひ参加していただけることを願っています．

（今回はリモートにてインタビューを実施しました）

URL https://journal.ntt.co.jp/article/23472
DOI https://doi.org/10.60249/23103101

新たなクラウドマーケット「エンド・ツー・エンド」で価値を提供するNTT DATAのクラウドアセット

クラウド市場に新しく追加された「エンド・ツー・エンド」マーケットでは，フルライフサイクルでの対応が求められています．フルライフサイクルにおいてワンストップで価値提供するために注力するのがアセット化の取り組みです．NTT DATAでは，グローバルでの成功体験に基づくベストプラクティスをアセットとして拡充，展開をしています．ここでは，日々進化するNTT DATAのクラウドアセットの全体像を紹介します．

クラウド市場における新たなマーケット

クラウド市場はこれまで，以下のマーケットで定義されていました．

・コンサルティング（Consulting）
・開発（Deployment/Development）
・運用（Managed）
・移行（Migration）

コンサルティング，開発，運用，移行といったライフサイクルを踏まえて複数のマーケットをワンストップで対応するマーケットとして「エンド・ツー・エンド」が新たに定義されました．

従前から定義されていた個別マーケットの規模は小さくなり，年平均成長率（CAGR）がマイナスとなるものがあります．従前からもっとも成長率の高かった運用（Managed）市場は引き続き高い成長率を維持しています．

一方で，エンド・ツー・エンドのマーケットは非常に大きく，2026年には約33兆円（2470億ドル）に到達すると予想されています．

クラウド市場は，単にクラウドを利用するのではなく，ビジネス成果を最大化するためにどのようにクラウドを活用するかというニーズへ変化しています．複雑かつ多岐にわたるクラウドサービスを適切に活用しつつ，ビジネス成果を最大化させることは簡単ではありません．ビジネスプランの検討，計画したプランの実行，ITシステムの運用，ビジネスプランの改善といったフルライフサイクルをエンド・ツー・エンドで対応することが求められています．

フルライフサイクルを実現するアセット

NTT DATAが現在提供しているクラウドテクノロジアセットは以下のとおり，大きく3つのカテゴリに大別されています．

① Cloud Advisory Framework（ベストプラクティス，方法論）（**図1**）
② Cloud IaC（設計テンプレート，開発ツール）（**図2**）
③ Cloud Managed Service（クラウドサービス）（**図3**）

テクノロジアセットの全体像として重要視しているのは，フル

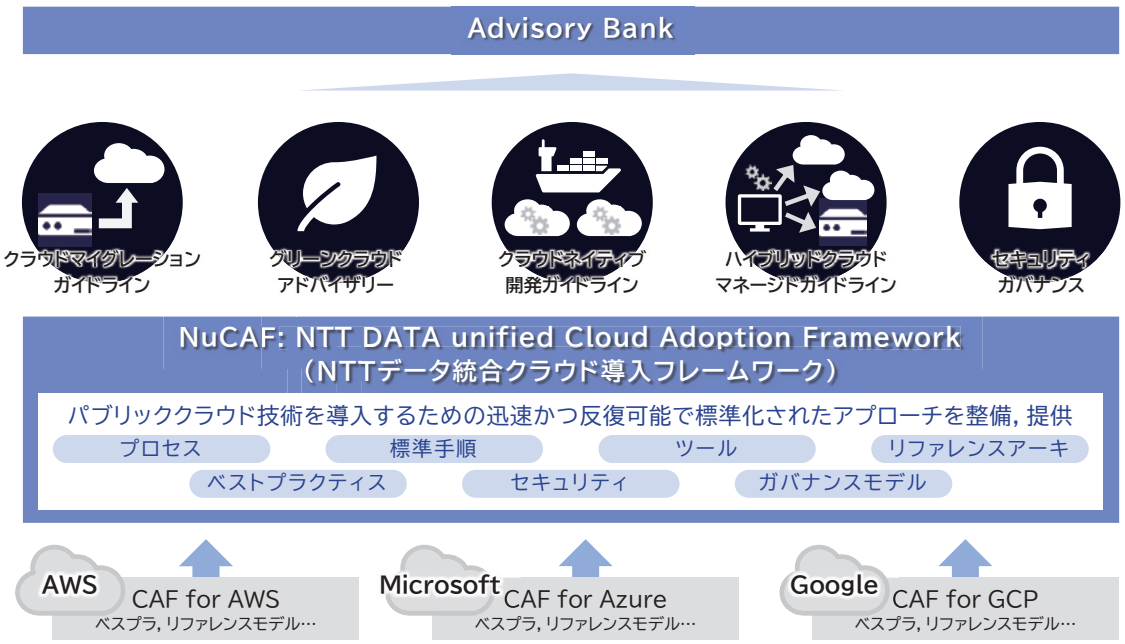


図1　Cloud Advisory Framework（ベストプラクティス，方法論）

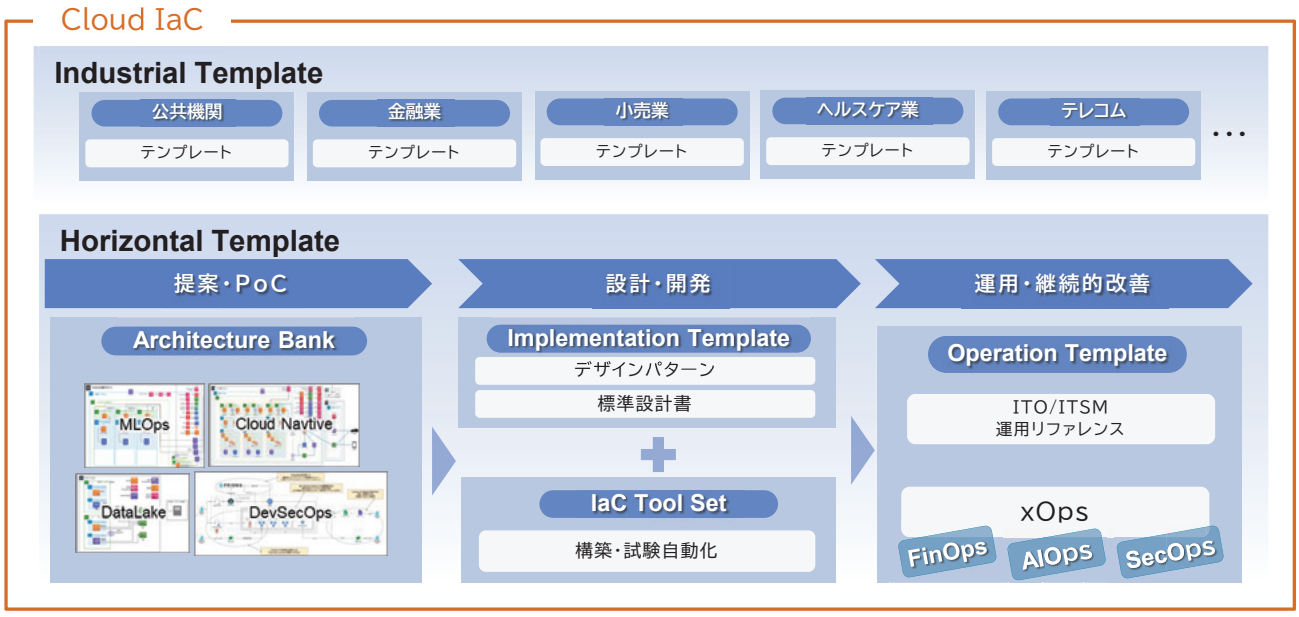


図 2　Cloud IaC（設計テンプレート，開発ツール）

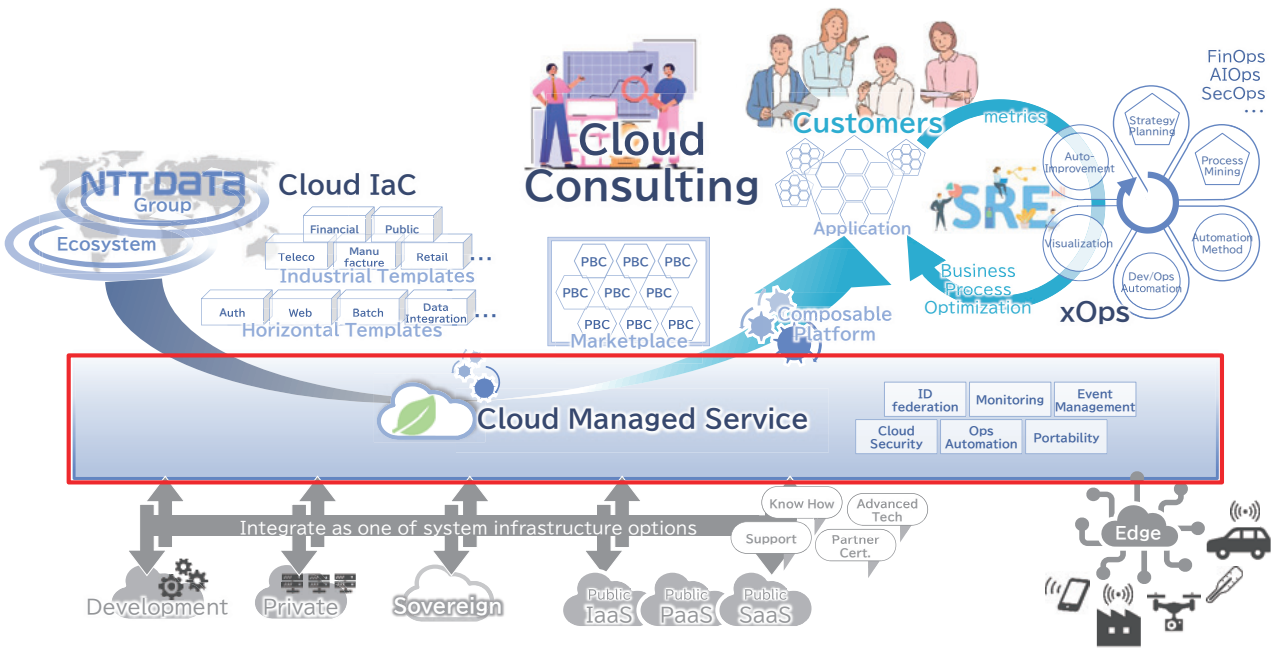


図 3　Cloud Managed Service（クラウドサービス）

ライフサイクルの価値提供です．

・構想立案・企画検討フェーズでお客さまに寄り添い新たな像を描くこと

・開発フェーズで過去の成功例に基づいた高品質なクラウド環境を迅速に提供すること

・運用フェーズで種々のハイブリッド構成となっているインフラ・プラットフォームを一元的に管理する手段を提供すること

など，すべてのフェーズで一貫して付加価値を提供することが

この構成のコンセプトとなっています．これらのアセットと高度なスキルやマインドを持つ人財を組み合わせ，お客さまにワンストップでの価値提供をすることが，NTT DATAが描くクラウドの未来の１つです．

Cloud Advisory Framework（ベストプラクティス，方法論）

Cloud Advisory Frameworkは，NTT DATAが持つクラウドコンサルティング関連のベストプラクティスを集めたアセットの集合体です．各種クラウドサービスプロバイダは各社のクラウドサービス導入から活用までのフレームワーク(CAF：Cloud Adoption Framework)を提供しています．NTT DATAではこれらを統合した方法論として，独自にNuCAF（NTT DATA unified Cloud Adoption Framework：NTT DATA統合クラウド導入フレームワーク）を定義しています．NuCAFは比較的一般的なクラウド導入のための方法論です．マルチ・ハイブリッドクラウドにおけるクラウド導入を促進するための手順・ツール・ガバナンスなどを含み，コンサルタントの技量によらないクラウド導入を推進可能です．

NTT DATAではさらに，マーケットトレンドやお客さまの多様なニーズに応じ，柔軟に組み合わせたコンサルティングができるアセットを開発しています．中でも特色あるのがGreen Cloud Advisory（グリーンクラウドアドバイザリー）で，クラウド導入前後のCO_2消費量に代表されるGreen関連の指標の可視化提案を可能にします．

また，成功裏に終わった技術コンサルティングのケースは，ナレッジとして「Advisory Bank」へ集約します．成功事例をすぐに集合知として横展開でき，各リージョンのお客さまに高付加価値なコンサルティングサービスを提供可能です．

Cloud IaC（設計テンプレート，開発ツール）

IaCはInfrastructure as Codeの略であり，ITインフラをコードとして記述し構成管理することで自動化ツールを利用できるようにする方法を指します．Cloud IaCは，標準的なアーキテクチャを自動構築するIaCツールセットを核としたアセットの集合体です．ベストプラクティスに基づく設計文書やテスト項目，成功体験に基づく事例集，さらには運用行程を高度化する技術検証結果などの要素を含みます．

以下にCloud IaCアセットの構成要素を列挙し端的に紹介します．各要素に共通した目的は，クラウド上のシステム開発の生産性，および品質の抜本的な向上です．これらCloud IaCアセットはグローバルの NTT DATA グループで共有され，標準的な開発パターンや事例を充実させていくことで日々生産性と品質を向上させています．

- Horizontal Template：業界によらないクラウド利活用のためのテンプレート集
- Architecture Bank：お客さまへのアーキテクチャ提供の成功体験集
- Implementation Template：標準アーキテクチャに基づく設計・構築テンプレート
- Operation Template：運用基盤の設計・構築テンプレート
- xOps：クラウド開発運用の最適化プロダクト（FinOps，AIOps，SecOpsなど）利活用のためのガイドラインとテンプレート
- Industrial Template：業界ごとのクラウド利活用のためのテンプレート集

Cloud Managed Service（クラウドサービス）

Cloud Managed Servicesは，お客さまのハイブリッドクラウド環境の運用を一手に引き受ける，ハイブリッドクラウド向けのマネージドサービスです．ITIL（Information Technology Infrastructure Library）*で定義されている機能に加えて種々のサービスを組み合わせることで，複雑化するクラウド運用に必要なすべての運用管理項目を機能として有するアセットをめざしています．特に2022年10月にNTT DATAへ加わったNTT Ltd.はこの領域で有用なアセットや経験を保有しています．NTT Ltd.のケイパビリティを盛り込むことでさらにグローバル対応力を向上させていきます．

エンド・ツー・エンドを支えるコンポーザブルテクノロジ

エンド・ツー・エンドでビジネス成果を迅速に達成するためには，フルライフサイクルといったフェーズの観点だけでなく，お客さまがビジネスにすぐに利用できるバーティカル（業種・業界特化）といったビジネスレイヤの観点も求められます．

特定業種・業界向けをサポートするテクノロジとして注目されているのが「コンポーザブルテクノロジ」です（**図4**）．Gartner社のハイプ・サイクルにおいても，コンポーザブルテクノロジは，今後２～５年の間に飛躍する技術として，現在期待のピークに到達しています．

＊ ITIL：ITサービスマネジメントにおけるベストプラクティスをまとめた一連のガイドブック（ライブラリ）．

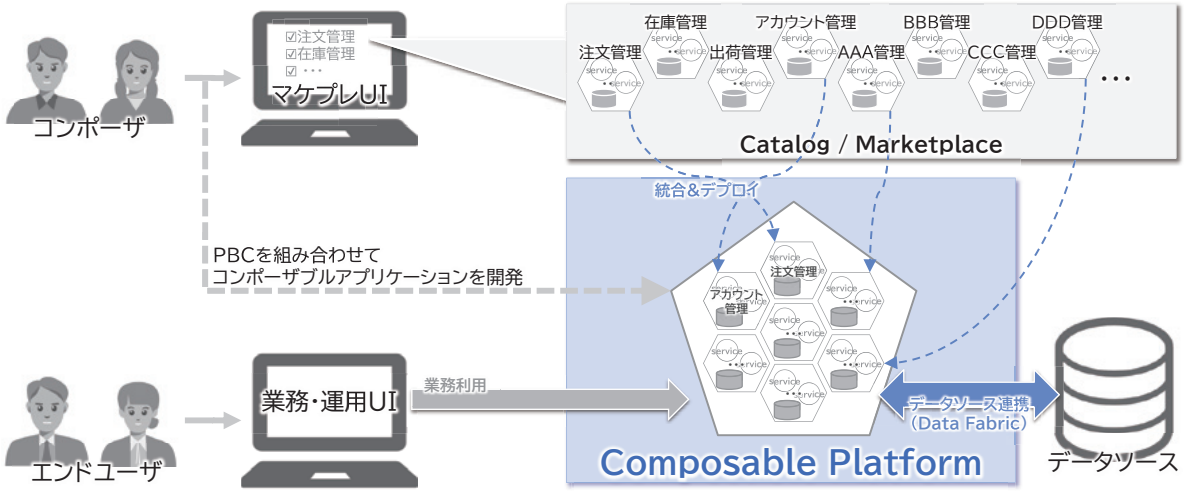


図4　エンド・ツー・エンドを支えるコンポーザブルテクノロジ

これまでシステムアーキテクチャはシステム全体をパッケージングするモノリシックなアーキテクチャから，ある程度の粒度のサービスを組み合わせてシステムを実現するマイクロサービスへと変化してきました．

モノリシックなアーキテクチャでは，システム全体を1つの大きなアプリケーションとして管理するため，管理が容易な反面，すべての機能が密結合されているため，変更が難しい課題があります．

マイクロサービスは，個々のサービスがモノリシックなアプリケーションと比べて小さく，独立しているため変更が容易である反面，それぞれが独立しているため全体の管理が困難という課題があります．

モノリシックとマイクロサービスの中間に位置付けられるのが，コンポーザブルアーキテクチャです．コンポーザブルアーキテクチャは，ビジネス的な意味を持つアプリケーションをPBC（Packaged Business Capability）としてカプセル化し，PBCどうしを連携させてシステムを実現する仕組みです．PBCを組み合わせることで業務アプリケーションの提供速度をあげ，モノリシックな管理容易性とマイクロサービスのような俊敏性を両立できます．

コンポーザブルアーキテクチャに基づくアプリケーション，「コンポーザブルアプリケーション」の開発方法を図に示したのが図4です．さまざまなPBCをマーケットプレイスで管理し，複数のPBCを「コンポーザブルプラットフォーム（Composable Platform）」上へデプロイし，統合することでコンポーザブルアプリケーションを迅速に開発できます．

エンド・ツー・エンドのねらいでもあるビジネス成果を迅速に達成するためには，業種・業界に特化したバーティカルな仕組みが必要です．そのために特定業種・業界の機能をパッケージし，組み合わせて迅速にサービス提供を可能とするコンポーザブルテクノロジの実現が鍵となります．

まとめ

クラウド市場とともにエンド・ツー・エンドのマーケットは大きく成長すると予想され，その中でフルライフサイクルのワンストップ対応やバーティカル（業種・業界特化）への対応が求められると考えられます．

今回紹介したアセット集合体は，いずれもエンド・ツー・エンドの価値提供を目的としたアセットです．

今後もさらなるアセット拡充，利活用を加速し，あらゆるリージョン・業種・業界の経験を基にした高付加価値なサービスを，エンド・ツー・エンドでお客さまに提供します．

◆問い合わせ先
NTTデータグループ
技術革新統括本部 システム技術本部 クラウド技術部
TEL　03-5546-8202
E-mail　cloudsiall@kits.nttdata.co.jp