挑戦する
研究開発者たち
CHALLENGERS

西野卓也

NTTコミュニケーションズ
イノベーションセンター テクノロジー部門
Metemcyber PJ

イノベーションは社会を面白くすることでなくてはならない

社会や産業のDX（デジタルトランスフォーメーション）が加速する現代，サプライチェーンを介して不正なソフトウェアが混入する，サプライチェーンセキュリティリスクが顕在化しています．NTTコミュニケーションズ イノベーションセンター テクノロジー部門の西野卓也氏に研究開発の概要と開発の背景，そして，研究開発者としての姿勢を伺いました．

脅威インテリジェンス流通基盤「Metemcyber」プロジェクトを担う

現在，手掛けている研究開発の概要をお聞かせいただけますか．

「Metemcyber」プロジェクトで，サイバー攻撃をはじめとするサイバーセキュリティ上の脅威に関する情報を取り扱っています．それらを集約して使いやすく加工した，脅威インテリジェンスの運用や活用に関する研究開発が私たちのミッションです．「Metemcyber」は，良質なCTI（Cyber Threat Intelligence：脅威情報）をブロックチェーン上で流通させるための脅威インテリジェンス流通基盤です（**図1**）．ブロックチェーン上でCTIを流通させることで，可観測性が高いCTIの流通をめざすとともに，これまで暗黙知であったインテリジェンス活用状況の可視化を行います．

また，「Metemcyber」では，CTIの共有（売買）をブロックチェーン上でまとめて管理することで，①インテリジェンスに基づく活動の横断的な参照，②セキュリティ対応に関する気付きの共有，③より金銭的な価値の高いActionableな脅威インテリジェンスの生産，といった特徴を実現しています．

さて，私たちはサイバー攻撃を観測する業務に従事して

いたのですが，サイバー攻撃の分析には，観測できる範囲にとどまらない情報が必要になります．サイバー攻撃の発見，事例等をはじめとするサイバーセキュリティ情報の収集を行い，第三者から提供された情報を分析に活用していました．このサイバーセキュリティ情報の提供はボランティアベース，無償で展開されていることも少なくありません．攻撃者が利益を得ている一方で，その攻撃から守ろうと情報提供している人たちが無償で働いていることに，私たちは疑問を感じていました．そこで，有益な情報に対して金銭的なフィードバックをすることで，情報の流通をより活性化させるとともに情報の質を高めることができるのではないかと考え，そのためのプラットフォーム「Metemcyber」のプロジェクトを立ち上げました．

「Metemcyber」は社会課題に呼応し，かかわる人たちにとって「三方良し」の環境をつくり出したのですね．

私たちは「Metemcyber」を構築するにあたり，３つの条件を設けました．まず，誰でも自由に参加できること．次に不健全にみえる通貨に依存しないこと．最後にトレーサビリティの確保です．

「誰でも自由に参加できる」について，限られた人間だけが参加できるプラットフォームは，特定の参加メンバーを攻撃することで活動の妨害が可能です．誰もが自由に参加できるオープンなコミュニティであることは，妨害のコストを上げるシンプルな方法であり，攻撃行為への抑止力にもつながります．また，匿名性も重要です．サイバー攻撃の情報を提供する行為は，それに対する報復と背中合わせであり，情報の提供者や受領者に対するプライバシ保護が必要になる場合もあります．ユーザが安心してサービスを利用するためには，これらの仕組みを提供する必要があります．

「不健全にみえる通貨に依存しないこと」について，米国や中国のようにサイバー攻撃の発信源として知られている国の通貨を利用すると，サイバー防御への投資が国家間の経済活動として不健全にみえてしまう場合があります．私たちは，国家の関係に依存しない決済手段を模索した結果，仮想通貨による支払い方法に気付きました．これは一長一短ある決断だと思いますが，情報提供のコントロールを特定の国に依存させないことで，地政学的なリスクを取り除くことができます．

最後の「トレーサビリティの確保」については，情報提供者を安心させるために重要な仕組みだと考えています．例えば，情報提供者が脆弱性を企業に報告しても，企業の担当者が最優先で対処できないことがあります．最悪の場

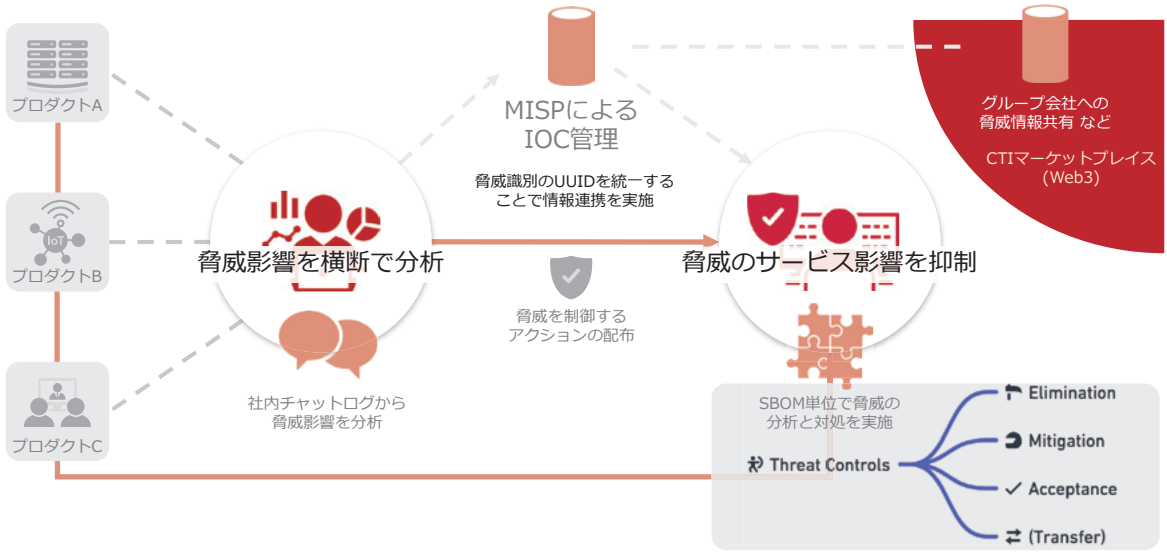

図１　Metemcyber アーキテクチャ

図 2　SBOM を利用したインテリジェンス活用サービス

合は放置され，情報提供者との関係性が悪化した結果，大きなインシデントが発生した事例もあります．この問題を回避するため，情報提供者や受領者だけでなく，脆弱性対応をサポートするコーディネータの活動も含めた可視化が必要になります．これはあくまで脆弱性対応の例ですが，脅威インテリジェンスの運用も同様の配慮が必要になります．関係者が誠実に対応している状況を，プライバシ保護の仕組みと矛盾せずに確認できることが必要でした．

これらを実現する技術がブロックチェーン技術です．私は過去にブロックチェーン技術を手掛けていたこともあり，2020年にブロックチェーン技術を利用した脅威インテリジェンス流通基盤である「Metemcyber」を開発し，プロジェクトのリーダーとして活動を開始しました．同じ年にはEthereum in the Enterprise - Asia Pacific 2020において事例を発表し，実証実験を開始しました．

「明らかになったインテリジェンスをうまく活用できていない」という現実

実証実験は順調に運びましたか．その成果を教えていただけますでしょうか．

実証実験においてアンケート調査やハンズオンを実施する中で明らかになったのは，企業の多くがインテリジェンスを必要だと実感していながら「インテリジェンスをうまく活用できていない」という現実でした．このように，インテリジェンスを共有するプラットフォームを提供しても，活用できていないのであれば，それをサポートする必要があります．ユーザインタビューを分析した結果，企業は自分たちが扱うソフトウェアの問題個所を，正確に把握できていないことに気付きました．そこで私たちは，SBOM（Software Bill Of Materials）を利用したインテリジェンス活用サービスの開発をスタートしました（**図 2**）．SBOMは「ソフトウェア部品表」と呼ばれるもので，一般的には特定のソフトウェアに含まれるコンポーネントの依存関係を記述するために利用されます．

さて，SolarWinds製品への攻撃，Codecovのセキュリティインシデントといった事例を皮切りに，2021年ごろからサプライチェーンを狙ったサイバー攻撃の危険性が本格的に認識されるようになってきました．さらに，Typosquattingはもちろん，Dependency Confusionと呼ばれる新たなサプライチェーン侵害のテクニックも報告されています．このようにソフトウェアサプライチェーンのセキュリティに注目が集まる中，SBOMの重要性は上がり続けており，2022年 9 月には米国政府機関のソフトウェア調達にSBOMの内容が盛り込まれる事態に至りました．世界がSBOMの重要性を受け入れていく一方で，これまで技術者や企業はSBOMを開発のライフサイクルに取り入れてきませんでした．それは，ソフトウェアは複

雑に組み上げられており，分解しても車の部品のように規格化されたモジュールとして取り出すことはできず，サードパーティのパッケージがどのように使用されているかも不明な状況で，プログラムコード断片に一意の識別子やバージョンを付与しても意味のある管理にはならないからです．

さらに，コンポーネントの利用方法を知らなければ実際のリスクを評価することもできません．例えば，タイヤがパンクする欠陥を見つけたとしても，そのタイヤが使われているのは走行中の車なのか，木にぶら下げたブランコのような遊具なのかで対処の優先度は大きく変わります．これはSBOMに限った話ではなく，現場が求めているのは実際のサービスへの影響を考慮した脆弱性評価です．こうした現状を踏まえつつ，私たちは前人未踏ともいえるSBOMの商用化に挑むことにしました．

ニーズにこたえるサービスの商用化を見込んで社内トライアルを開始されたそうですね．

脅威インテリジェンスとSBOMを用いた迅速かつ効果的なサイバー脅威対策手法を発明して，2022年から社内トライアルを展開しています．

実験的に始めたユースケースは，SBOMを利用したアタックサーフェスマネジメントの取り組みでした．私たちが考慮したことは「SBOMの生成や収集が目的になるような運用をしない」ことでした．SBOMのユースケースは，脆弱性の識別，ライセンス管理，ポリシーやコンプライアンスの検証と多岐にわたります．実際の使い道を決めてからT字型に運用の幅を広げていくアプローチを取り，脆弱性管理の観点から最初の取り組みを始めました．その理由は大きく分けて2つで，社内に脆弱性管理をするシステムがすでに存在すること，そして，パッケージの脆弱性を検知し，それを解決するための対策を提案してくれるサービスであるGitHubのDependabotと機能や性能を比較検証できるためです．

これだけ聞くと，すでに脆弱性管理ができているので取り組む意味がないと感じるかもしれません．しかし，「既存の脆弱性管理システムをSBOMでどう改善できるのか」「業界標準のサービスと比較して，新たにSBOMを利用する意味があるのか」という2点は，これまで議論されておらず，その意味で既存の脆弱性管理システムに対するSBOMのメリットやデメリットを確認する素晴らしい試金石になりました．

また，SBOMを利用する立場についても考える必要があります．私たちの議論では対象となる利用者の人物像をプロダクト担当者，脅威アナリスト，ガバナンスマネージャの3つに絞りました．正直なところ，すべてのロールで実際の検証ができたわけではないのですが，誰がどう使うのかを意識しながら検証を進められた点は非常に良かったと思います．

ただ，すべてのプロダクトにいきなりSBOM管理は適用できません．「アトミック性（これ以上細分化できない最小単位）を意識したソフトウェア開発」と「パッケージマネージャ」の存在が不可欠だからです．これらを考慮せずにつくられたプロダクトに対して，大規模なSBOM管理はうまくいきません．SBOM管理が可能なプロダクトに対し，アラート通知の効率化やオートクローズ対応を行うことで，開発者や運用者にセキュリティ対応時の余裕をつくることが最初のポイントであると実感しました．

このように，SBOMによる脅威インテリジェンス利用の効率化に取り組んできたことが注目を浴びて驚いています．2023年3月には，幅広い分野の会員と連携しサイバーセキュリティの観点から安全なICT社会の形成に寄与する活動を推進する団体「ICT - ISAC」に講師としてお招きいただき，私たちのSBOMを活用した脆弱性管理の取り組みについて報告させていただきました．

「面白がる」「流行に踊らされない」姿勢で挑む

ところで，これまで手掛ける研究開発者がいないという現状において，なぜ西野さんとそのチームがSBOMを実現できたのか，客観的に分析していただけますでしょうか．

先述のとおり，技術的な面でいえば，ソフトウェアは複雑に組み上げられていたのですが，プログラミングの方向性としてコンテナ化が進んできたこと，各プログラミング言語でパッケージ管理やライブラリを配布する仕組みが整ってきたことが要因の1つに挙げられます．

さらに，米国でソフトウェアのサプライチェーンにかかわる大きなインシデントが発生し，それがSBOMという

言葉が世界に大きく広がる契機となりました．国内外を問わず，SBOMに取り組むようになったわけですが，私たちのプロジェクトの大きな強みはNTTコミュニケーションズ（NTT Com）という通信インフラを手掛ける企業であるため，サイバー攻撃を観測するための大規模な監視設備が整っているということです．また，セキュリティ情報を理解し，それを監視，検証する人材もいるという有益な環境を整えることができていることです．その中で，自分で言うのは少し恥ずかしいところもありますが，私自身もさまざまな経験や知見を蓄えてこのプロジェクトに携わっていることもユニークなオリジナリティととらえられるかもしれません．私は，2015年にNTT Comに入社しましたが，学生時代はバイオインフォマティクスを専攻し，機械学習や統計の知識を活かしてセキュリティの研究を行っていました．そして，サイバーセキュリティのエンジニアとしてNTT Comに入社し，悪性サイトクローラによる脅威インテリジェンス収集システムの開発に携わりました．マルウェアの自動分析と脅威インテリジェンス管理基盤の開発や運用，マルウェアサンドボックスのマルチベンダ性能比較プラットフォームの開発を手掛け，ブロックチェーン関連にも従事した経験と知見を携えて今を迎えています．一般的なセキュリティ関連の研究者，技術者と比較して，ブロックチェーンの経済面に関する勉強がサービス開発にとても役立っています．経済的なインセンティブをどう扱うか，商品としてどう売り出そうか等について考え，そのうえでユーザに喜ばれることまで意識して，サービス開発をカバーしていることは強みであると考えています．

研究開発者として大切にしていることを教えてください．

私は，イノベーションは社会を面白くすることでなければならないと強く思っています．これを世の中に出したら「皆が楽しめる」と思える技術をめざして頑張ってきました．画家のゴッホの残した言葉があります．“Normality is a paved road: it’s comfortable to walk but no flowers grow.”（普通であるということは舗装された道路みたいなもので歩きやすいが，花は咲かない）．この言葉は，誰かの心に刺さるものは挑戦することでしか創れない，ということを意味しています．当たり前ではつまらない，普通じゃないから面白い．この言葉にならって，技術的な困難に挑戦することで，社会を面白くできると私は確信しています．

また，研究開発者として，最先端技術の可能性を解きほぐし，社会的インパクトを評価することで，企業の新しい道を切り拓く人になりたいという思いを持って仕事をしています．今回のSBOMについても同様に，周囲からは時期尚早ではないかと言われていましたが，私たちのチームが持っているセキュリティの知見を活かせば，実運用に落とし込めると自負して，日本におけるSBOMの道を切り拓くことができました．

こうした姿勢を保つために大切にしてきたことは「面白がる」ことと，「流行に踊らされない」姿勢です．面白いことというのは，自分たちが関心を寄せていることにとても集中できている良い状態です．だからこそ，面白いことを追究していくと自然と最先端をキャッチアップできるようになるし，組織の良い循環を生み出すと思います．

また，私たちはエンジニアとして，技術の中身を理解したうえで流行に乗るから良いプロダクト，良いサービスを提供できると考えています．舗装された道路を，ただ漫然と歩いても面白い花は見つかりません．だからこそ，私はエンジニアとして手を動かすことを大切にしています．陳腐な言葉かもしれませんが，技術を知っていても，それを使えなければエンジニアとしては生き残れません．エンジニアは舗装された道ばかりを進める職業ではないからです．イノベーションは社会を面白くすること．困難への挑戦がイノベーションにつながっていること．技術的な困難に立ち向うためのエンジニアがいること．どれか１つが欠けても，社会を面白がらせるイノベーションは成立しません．流行に踊らされて，つまらないことに取り組む状態を避けるためには，確かな技術力が必要です．

若い研究開発者の皆さん，論理的な追究をするだけではなく，もっと自分自身が面白いと思う感情や感性も大切にし，チームでその感覚を共有してみてください．

最後に，NTTグループはサプライチェーンセキュリティリスクに取り組むオープンコンソーシアム「セキュリティ・トランスペアレンシー・コンソーシアム」の設立に向けて準備しており，私もその一員として活動しています．そして，2023年７月には「Threatconnectome」というSBOMを用いたAttack Surface Management（攻撃対象領域管理）ツールをOSS（Open Source Software）化する予定ですので，ぜひ皆さんにお使いいただければと思います．