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]．

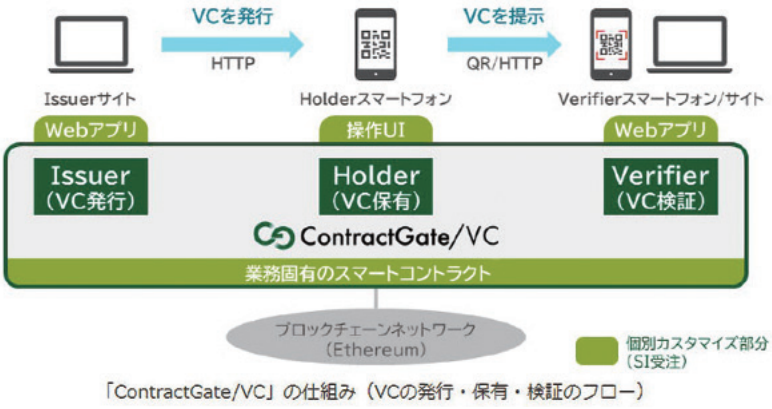


図1　ContractGate/VC

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

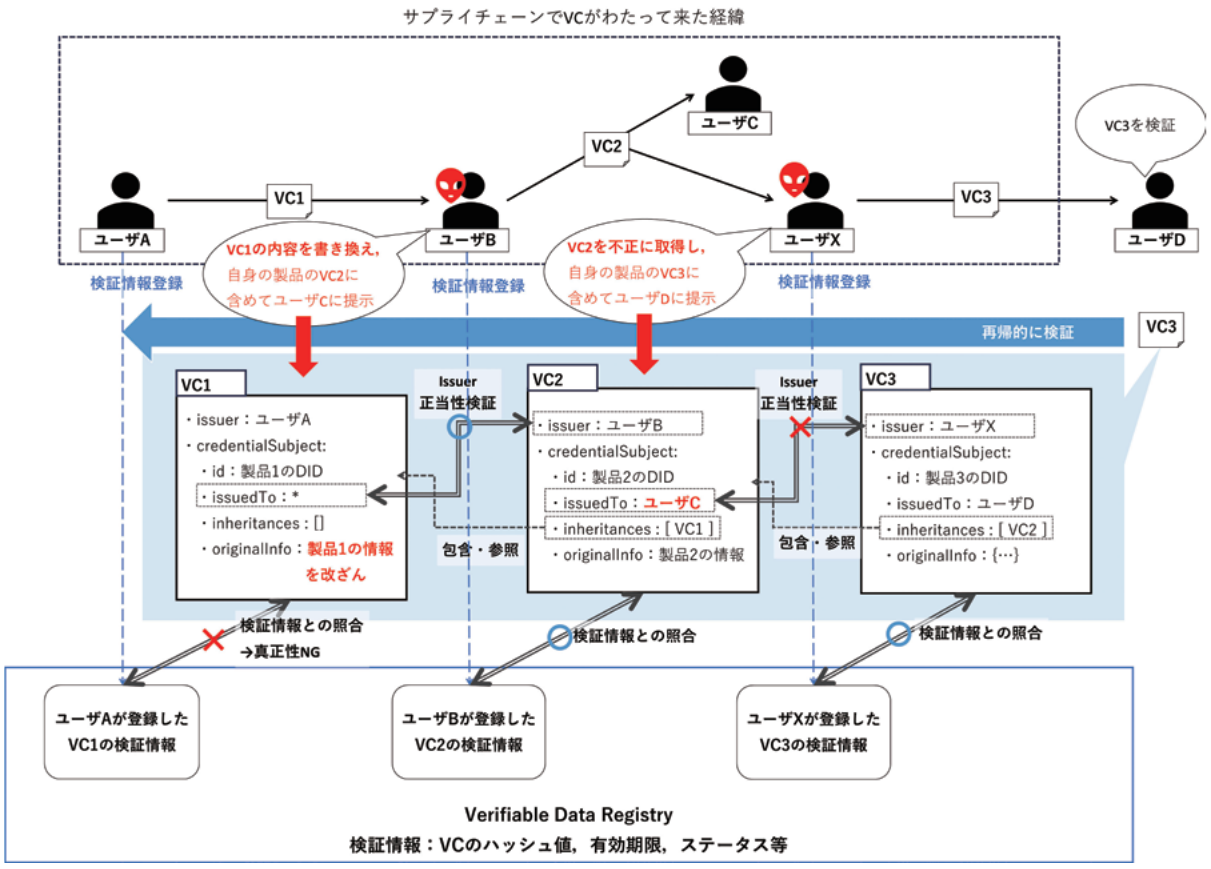


図2　階層型VCの検証イメージ

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．

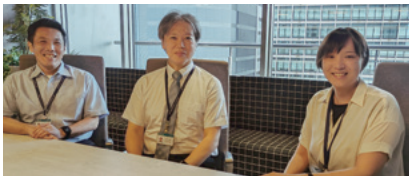
このように階層型VCモデルは，SBOMがソフトウェアと同じサプライチェーンで流通でき，かつ信頼性を確保できる仕組みを提供します．

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．