URL　https://journal.ntt.co.jp/article/30152
DOI　https://doi.org/10.60249/24115104

web3とブロックチェーン技術で切り拓くデジタル社会の未来とセキュリティ
―― NTT Digital，NTTセキュリティ・ジャパン対談

NTT Digitalは，2024年3月12日にデジタルウォレット「scramberry WALLET」をリリースしました．scramberry WALLETは，使いやすさと安心・安全に焦点を当てた，暗号資産やNFT（Non-Fungible Token：非代替性トークン）の送信・受信・管理ができるデジタルウォレットです．はじめて暗号資産やNFTを利用される方を含め，より多くの方々にスムーズにご利用いただけることをめざし，秘密鍵のバックアップや生体認証の活用などの機能を搭載し，本ウォレットを通じて，ユーザが安心できるデジタル体験を提供しています．そのセキュリティ対策の技術検討と運用にはNTTセキュリティ・ジャパンも参加し「協創」しています．本稿では，新たな取り組みにおける苦労や得られたものについて，協創の中核を担う4名による対談の模様を紹介します．

キーワード：#デジタルウォレット，#web3，#NFT

遠藤　英輔[†1]／山本　剛[†1]
齊藤　宗一郎[†2]／野村　礼智[†2]

NTT Digital[†1]
NTTセキュリティ・ジャパン[†2]

NTT Digitalがめざす「Free to Trust」にセキュリティは最重要

齊藤：最初に，NTT Digitalがめざしていることと，そこにセキュリティがどのように絡んでくるのか，セキュリティの役割，重要性を教えてください．

遠藤：NTT Digitalでは「Free to Trust」というコーポレートビジョンを発表し，会社の軸としています．インターネットは発展していますが，そこでのトラスト（信頼）はまだ十分ではないと考えています．今後もさまざまな情報が爆発的に増えていき，人と人，人とモノがつながっていく世界では，信頼が1つの重要なキーワードになります．

人は情報を選ぶことができますが，その信頼性に対する明確な指針はありません．そのため，今はどうしても受動的にならざるを得ない状況です．だからこそ，各個人が能動的に情報に対する信頼性を把握し，選ぶ自由度を上げていこうということが「Free to Trust」の考えの1つになっています．

この状況の中で，まだまだ私たちにできることがあると考えて立ち上げたのが「scramberry」というサービスブランドです．その第一弾として「scramberry WALLET」というウォレットをリリースしました．ウォレットというとクリプトやNFT（Non-Fungible Token：非代替性トークン）[*1]を連想するかもしれませんが，私たちはそれら「マネー」，「オブジェクト」に加えて，将来的には「アイデンティティ」を含めた3つを1つのウォレットの中に収めて，これらをボーダーレスにつないでいくことを1つのポイントとしています．

これまでこの3つを連携してデジタル化できていなかったのは，これらに対する真正性や地域性の担保ができなかったためです．しかし，ブロックチェーンをはじめとするさまざまなデジタル技術でそれらを解決できると考えています．そこでも当然ながらセキュリティは重要になるので，私た

＊1　NFT：通常の暗号資産は代替性があるトークンであることに対し，NFTは代替性がない（デジタルデータだが，唯一性を保持）点に特徴があります．NFTとデジタル資産を関連付けることで，デジタル資産とのかかわり，履歴の管理・追跡を可能にします．

（左から）NTT Digital　取締役 CISO サービス開発部 Managing Director　遠藤 英輔／セキュリティマネジメント室 セキュリティ Senior Manager　山本 剛

ちの事業においても大きな柱の１つだと思っています．

山本：私たちがめざしているのは，モノと情報とアイデンティティを，お互いに信じられるかたちで関連付けて，それを表現したり渡したりできる世界です．そして，それを実現していくためには，そのプラットフォームをお客さまが選べるようにすることが大事だと考えています．しかし，大きなプラットフォームが１つあればいいという考え方は，どうしても歪みを生みますし，自由とは少し違うと私たちは思っています．それが「Free to Trust」が持ついろいろな意味の１つだと理解しています．

お客さまが選べるということは，セキュリティが非常に重要になってくるということです．

実際，現在のブロックチェーンを使うには，未知のリスクがたくさんあります．そういった不確実性にどう対峙していけるかということを，お客さまと一緒に考えていく必要があるだろうと思っています．

齊藤：不確実性が含まれてしまうことは「想定外を想定する」ことだと私は理解しました．そこが非常に重要なので，NTTグループの総力で「想定外は何か」に対する洞察を皆で持ち寄って，お客さまを守る．いろいろ選べる中でも信頼性，安全性を持って選べる場を提供したいということですね．

山本：そのとおりです．そして想定外を想定するということは，リスクを評価してマネジメントするということだと考えています．

齊藤：サイバーリスクにおいても，機器が発するアラートやログで見えるものと見えないものがあります．例えば内部不正などは，一見正当な人が正当な操作をしているのでログで判断することは難しいですよね．ただし，振る舞いやソーシャルエンジニアリングの洞察などがあると，おぼろげながら見えてくるものがあります．そこを視野に，今できるところからNTTセキュリティ・ジャパンも一緒に始めさせていただいています．

（左から）NTTセキュリティ・ジャパン　ソリューションサービス部 担当課長　野村 礼智／第二営業本部 本部長，CISOアドバイザー　齊藤 宗一郎

山本：サイバーセキュリティのプラクティスから学ぶことができる手法の１つに，３ラインモデル[*2]があります．これは３つの役割のバランスで適切なリスク管理をめざす仕組みです．３つの役割の第１，つまり第１のラインはお客さまに製品やサービスを提供する立場でリスク管理します．第２のラインは専門家としての立場からのリスクを管理し，第３のラインはリスク管理が妥当で有効に機能しているかをモニタリングします．このたびの連携では，その第１のラインと第２のラインにおいて，NTTセキュリティ・ジャパンにサイバーセキュリティの専門知識，そして専門的なオペレーション能力を大変頼もしいかたちで提供いただいています．会社は違っても同じ価値観のもと，一緒に走るワンチームとして動いていることこそがNTTグループで取り組む意義だと考えています．

齊藤：３ラインモデルは一見煩雑なようにみえますが，実装しないと結局は手戻りが発生しやすくなり，お客さまに不信感を与え，そのリカバリーも大変になります．３ラインモデルを信頼感のあるワンチームで運用することにより，健全な牽制機能を働かせる．これがお客さまや市場のためになると感じました．

山本：不確実性がある世界を相手にしているということ，つまり適切な幅のリスクを取り続けるような活動をめざすには，３ラインモデルが有効だと実感しています．これを実現するには，皆が同じゴールを共有して，時に微妙なさじ加減をすることが必要です．この基礎の上に，お客さまとの約束は絶対に守るというNTTのキャリアとしてのDNA，文化が効いているのだと思います．

齊藤：このプロジェクトが始まる当初も，両社の間で長時間にわたり議論を重ねました．お互い耳に心地良い話だけではありませんでしたが，それを経たことで強い信頼関係が生まれました．私たちも，従来のMSS（マネージドセキュリティサービス）やセキュリティ監視は変わっていく必要があると考えていました．今回の取り組みは，私たちにとっても変革に向けた非常に良いテーマをいただいたと思っています．果敢

＊2 3ラインモデル：第1のラインを業務部門内での日常的モニタリングを通じたリスク管理，第2のラインをリスク管理部門などによる部門横断的なリスク管理，そして第3のラインを内部監査部門による独立的評価として，組織内の権限と責任を明確化しつつ，これらの機能を取締役会または監査役等による監督・監視と適切に連携，とするモデル．

にチャレンジして得た知見は，世の中にも貢献できると考えています．

NTTグループの伝統的な価値観と新しいイノベーションを両立させる試み

齊藤：難しい点やチャレンジだった点について教えてください．

野村：セキュリティに携わる人間は，ベースラインは当たり前のものとして継続すると考えます．例えば，「EDR（Endpoint Detection and Response）が登場したからEPP（Endpoint Protection Platform）は不要」ではなく，EPPはベースラインとして当たり前のものとして必要だということですね．難しいことやチャレンジングなことはあるし議論も重ねましたが，ベースラインの考え方を共有しているので進めやすかったですね．

山本：普段は技術討論などで丁々発止させていただいている関係ですが，同じ方向を向いて信頼感があるからこそできることです．議論することでお互いに理解を深めていくことができます．

齊藤：基本的にセキュリティは減点方式の世界に陥りやすいですよね．普段どんなに頑張っていても，何かが起きたときの対応だけが注目されてしまいます．しかし今回の取り組みは，まだ確固たるセキュリティの方式やスキームが完全に確立していないこの世界にまず飛び込んで，試行錯誤をしながら新しいものをつくっていく．減点方式でなく新しいものを策定していく世界です．それを双方のトップが理解し意思を統一していることは非常に意義がありますよね．

NTT Digitalの皆様がNTTセキュリティのSOC（セキュリティオペレーションセンター）[*3]を訪問されたときに，技術的な説明から徐々に事業展開の話になり，その内容に共感しました．単なる暗号資産の取引所だけでなく，イベントチケットなど広くB2C向け，さらにはB2Bも視野に入れたプラットフォームであり，さまざまな事業者がそこを活用することで新たな付加価値が生まれていくというお話を伺って，非常に広がりがあるビジネスだと思いました．

NFTなどを使ったビジネスモデルを考える際に，自分たちで基盤をつくることだけでは難しいといわれる時代ですが，そのベースの部分を提供することは，社会的使命も担う重要度の高いことです．金融など当局の監督が及ぶことも考えられる領域であり，非常に重要なミッションなので，私たちとしてもセキュリティ冥利に尽きる仕事と感じています．

山本：わずか半年でここまで意思の統一ができたことは，やはりベースに同じ価値観があったからだと思います．重要なことは，こういう価値を信じているという「Why」（理由）があることです．私たちはブロックチェーンなどweb3の新しいインフラをお客さまにお届けすることで世界を変えていくことをめざしているわけですが，その活動を共にさせていただくには，「どうして，どのように世界を変えたいのか」の考えを共有することが鍵でした．そのときに，同じ文化を基本として共有しているからこそ，コミュニケーションを密に取ることができたわけです．

野村：お互いにセキュリティのプロなので，話をすれば分かり合えます．そのベースにも，NTTグループのリモートワーク基本原則があったと思います．離れていても隣にいるのとあまり変わらない状態で仕事ができたことで，非常に助けられました．

実際にお会いして会議するとなると，移動を含めて3時間かかってしまいます．しかしリモートなら5分の会議を5分でできます．このメリットは大きいですね．リモートも慣れが必要ですが，NTT Digitalの皆さんは慣れていて効率が良く，やはり新しいものを創り出す方々だと実感しました．

プロジェクトを進めていくうえで課題となった点

齊藤：web3のセキュリティ監視は大きなチャレンジで，お互いに解決しなくてはならない課題がたくさんあったと思います．その課題を教えていただけますか．

野村：SOC目線では，web3領域はアナリストも今まで見ていなかったログを扱います．アナリストは絶対を保証する責任感があるので，保証できないものはNOと言います．しかし，新しいものを始めるうえで分析ができないと私たちの価値はなくなってしまいます．どこまでのログをどのように分析し「安心・安全」をお届けするのか双方で話し合いを重ねて，お互いに満足できるポイントを探っていきました．

山本：それは，ものすごく議論を重ねてきたポイントですし，引き続き議論させていただければと思っています，私たちはこういうSOCをつくりたい，そういう「Why」から始まっています．ですからその「Why」を「What」に変えるまでのジャーニーを，一緒に議論させていただく必要があり，実際にそのような議論ができるということは大変ありがたく，感謝しています．

例えば，web3の取引ログが正当なものかどうかを判断するには，地理的な情報を考慮します．しかし，それは既存のベンダ技術では難しいことがあります．例えば，大きな取引所が米国政府から訴えられた事件があります．米国市民は利用できないはずのサービスを，米国市民がバーチャルネットワークを使って利用していたことが背景にある一件でした．私たちの考えるセキュリティは，このような問題にも対処できるものでありたいと考えています．

そのためには，ログの分析機能に柔軟性を持たせる必要があります．そのような製品はまだ世の中にないということも珍しくはないので，新しい技術の研究開発を含むかもしれません．そのような長い旅をご一緒させていただくことができれば何よりです．

齊藤：Know Your Customer（KYC）の

＊3 SOC：顧客または自組織を対象とし，セキュリティ機器，サーバなどのログを分析することで，サイバー攻撃を検知・対処を行う組織．

視点も必要になります．NTTとしてはTier1のネットワークプロバイダとして，いろいろなインテリジェンスを組み合わせることによって比類のないセキュリティの潜在能力を持っていると思います．それをお客さまに届けていきたいですね．

山本：認証にも課題が多く，「Why」の大きな背景だと思います．大抵のモノには固有の制約があるし，一方で，お客さまが望むなら換金性のある情報の流通も止められません．こうした問題に，いかにリスクマネジメントで斬り込むのか，日々悩みながらも取り組んでいます．今はまずスモールスタートでクラウドネイティブな環境でサイバー空間の監視に取り組んでいますが，将来的にはサイバーフィジカルにも対応していく必要があると考えていますので，それについても議論を重ねています．

野村：認証周りは特に，予想していなかった手法でセキュリティが破られるケースが年に数回あります．そうした情報を把握し対峙することは，技術者としての腕の見せ所で，お役に立つことができている実感がありますね．また，外部からの攻撃だけでなく内部不正にも対策が必要です．

次のゴールはweb3の情報も扱えるSOCの実現

齊藤：「scramberry」においてウォレットの提供はできました．第一段階が終わったといえると思いますが，次のゴールは何でしょう．

山本：まずは，web3の情報も扱えるSOCを実現すること，そしてそのインフラを使って，お客さまに安心して使っていただけるウォレットを提供することが第一歩と考えています．そういう新しい機能を持ったSOCを成熟させていきたいです．いろいろな課題が見えてくると思いますが，今はない道具が必要になったとしても，NTTグループの研究開発と連携させていただくことができれば，実現できることもあるのではないでしょうか．そのようにして，業界全体をリードするところまで持っていくことができればと思っています．

野村：チャレンジとしては，お客さまの使い慣れたセキュリティの環境にスムーズにつなぐことがあります．セキュリティというとクローズドのシステムが多く，サービスを変更すると管理画面も操作や設定もすべて変わってしまいます．「うちのものしか使わせませんよ」ではなく，お客さまは使い慣れたものを使いつつ，私たちは効率良くオペレーションしていく．オーダーメイド的な要素を取り入れつつ，利便性は追求していきたいですね．現状，「これしか提供できません」というSOCが多いですが，その殻を破るチャンスをいただき，とても良い刺激をいただいています．

齊藤氏：規制への対応も大きな課題になりますよね．

遠藤：確かに規制は厳しくなっていますが，ポジティブにとらえることもできると思います．グレーゾーンが多いと業界の信頼性に対する懐疑的な面はどうしても出てきます．もともと日本の規制は厳しいといわれていますが，実際に海外で深刻な事件が起きていることを考えると，実は日本が先頭にいるという話も聞きます．私たちにはやるべきことが増えますが，web3の社会実装に至るプロセスとして必要な過程なのではないかと思っています．

齊藤：最後に皆さん，一言ずついただけますか．

遠藤：まだまだ始まったばかりで時間もかかると思いますが，セキュリティをしっかりと建て付けていきたいですね．また，一過性のもので終わらせずに，長く続けていくパートナーリングが重要だと考えていますし，ぜひ，この記事を読んだ皆さんにも参加してほしいですね．

野村：身近な同じグループのメンバーであったことと既存のSOCがあったこと，そして何より諦めずにご相談いただけたことに大きな価値があったと思います．いただいた刺激から興味を持ち続けることが，モチベーションや技術を高めていくことにつながっています．ぜひ今後も長く，切磋琢磨していきたいと考えています．

山本：web3で世界を変えていくという新しいジャーニーには，「協創」が欠かせないと考えています．NTTセキュリティ・ジャパンとの取り組みで，キャリアのDNAが根本を支える「力」になることを実感できました．この取り組みを広げていくことができれば大変うれしいです．web3と呼ばれる領域は，今はまだ課題が多くて，まるで西部開拓時代のような世界です．しかし，より多くの人に安心してお使いいただけるようになれば，やがて大都市になる，世界を変える動力になると考えています．

齊藤：大いに意見を戦わせるには，お互いのベースに信頼感が不可欠です．私たちはそこができているので，ときにコンフリクトがあっても一緒に解決していくことができます．引き続き，お互いに大いに意見を戦わせて，いいものをつくっていきたいですね．今日はありがとうございました．

（左から）　山本　剛／野村　礼智／遠藤　英輔／齊藤　宗一郎

web3で世界を変えていくという新しいジャーニーには，「協創」が欠かせないと考えています．対談を読まれた方，ご関心がある方は，ぜひ一緒にチャレンジしませんか．本稿で紹介した取り組みに関して，ご質問がある方は，お問い合わせください．

◆問い合わせ先

NTTセキュリティ・ジャパン
営業本部
E-mail　nsj-pr @ security.ntt