高まる“デジタルアイデンティティ”の重要性とNTTデータの取り組み

「デジタルアイデンティティ」という言葉を耳にしたことはあるでしょうか．「認証」「ID管理」といったキーワードを連想する方もいらっしゃるかと思います．NTTデータでは，この「デジタルアイデンティティ」を，企業のサイバーセキュリティの中心に位置する重要な要素であるととらえ，これまでさまざまなお客さまの課題を解決に導いてきました．本稿では，その方法論の一部を紹介します．

宍戸（ししど）　りさ
NTTデータ

MDRへの着目とデジタルアイデンティティの重要性

NTTデータでは，これまで自社や国内外グループ会社内のセキュリティ環境を整備してきた経験や，お客さまへのご支援実績をとおして得られた知見を活かし，「MDR（Managed Detection and Response）」を軸にこれからの市場を牽引していこうとしています．MDRとは，ITリソース全般の監視と，トラブルが起きた際には対応・復旧までを行うセキュリティの専門家によるサービスの総称です[(1)]．MDRが重要視される背景には，コロナ禍の影響や，世の中のオンライン化の流れ，そしてそれらに伴うサイバーセキュリティのトレンドの変化の中でも，特に「ゼロトラスト」という概念が定着してきたという点があると考えています．ゼロトラストとは，Microsoft社が「never trust, always verify」と提唱しているとおり[(2)]，ネットワークの境界で強固にリソースを保護する（つまり会社であれば，社内からのアクセスは安全，社外からのアクセスは危険と一律に判断する）のではなく，すべての通信を信用せず，アクセス可否を都度判断する，境界を突破されることを前提にした考え方のことを言います．ゼロトラストな世界では，過去にNTT技術ジャーナルにて紹介[(3)]したNIST（National Institute of Standards and Technology：米国国立標準技術研究所）が提唱するサイバーセキュリティフレームワークのうち，「特定（Identify）」「対応（Respond）」「復旧（Recover）」が特に重要となります．MDRはこれらをまとめて実現するソリューションです．

NTTデータでは，**図1**に示す9つの分野に分けてMDRをとらえています．

9つそれぞれの要素で，どのようにセキュリティ強度を向上させるかを総合的に考えていくことになりますが，

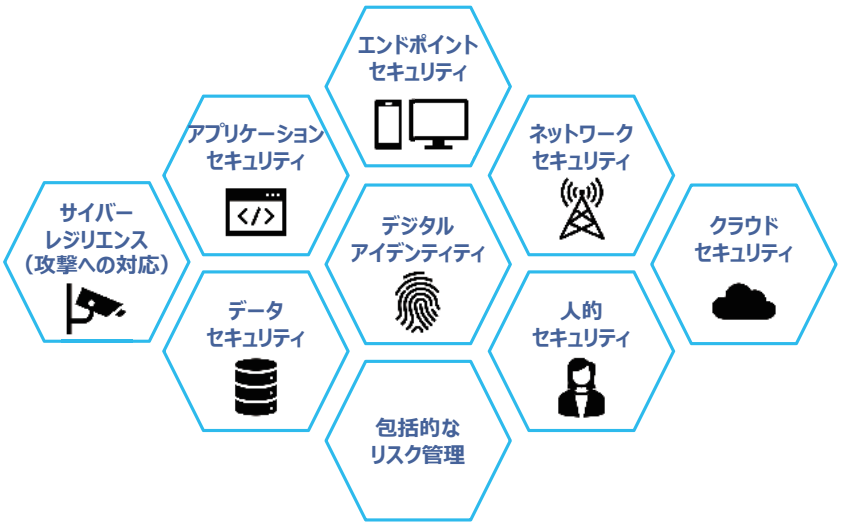

図1　MDRを構成する要素

その中心に位置するのが，「ID管理」や「アクセス制御」「認証」といったキーワードで語られることの多い「デジタルアイデンティティ」という分野です．

MDRにおいてデジタルアイデンティティが中心となる理由はいくつかありますが，もっとも大きな理由は，物理的な人間の存在と，その人が使うさまざまなネットワークやシステムをつなぐ役割を果たすのが「デジタルアイデンティティ」であり，「あなたは誰？」「あなたは本当に本人？」という点をまず確認し保証することが，ゼロトラストな世界を実現するためには必要になるため，ということだと考えています．

企業はデジタルアイデンティティについてまず何を考えるべきか

企業が，ゼロトラストというキーワードで自社内を見つめ直すとき，またはデジタルアイデンティティにまつわる何らかの課題を解決しようとするとき，まずは何が必要になるでしょうか．

私たちがお客さまのデジタルアイデンティティにまつわる課題解決を支援させていただく際には，「課題の全体像整理」のフェーズ（**図2**の赤字部分）を重要視しています．それは，お客さまに見えている課題は氷山の一角であることが多いこと，またそれを解決するだけでは根本的な改善にならなかったり，見えている課題に着手して検討を進めるうちに，それに絡む，より優先度の高いテーマが見つかったりするケースがあるためです．特にデジタルアイデンティティの分野には，「これをこうしておけば大丈夫」というベストプラクティスが少なく，お客さまの状況に合わせてソリューションを選定し，カスタマイズをしたうえで実装していくことが必要な要件も多いため，ゴールまでの最適解を見つけるのは簡単ではありません．

課題を整理するために，NISTやISO（International Organization for Standardization：国際標準化機構）は国際的なガイドラインやフレームワークを定義しています（**表**）．

これらは，日本国内はもちろん，世界で多くの組織や専門家が参考にしている情報です．しかし，実務的な観点で考えると不足する点があるのでは，と私たちは考えています．NTTデータでは，主に企業内部のデジタルアイデンティティの課題整理のためのフレームワークを策定し，多くのお客さまへのコンサルティングを行っていますので，その概要を紹介します．

デジタルアイデンティティについて考えるべき9つの観点

企業のデジタルアイデンティティについて俯瞰するためには，**図3**に吹き出しで示す9つの観点が必要となります．これらをサイバー空間ではなく，企業内の物理的な環境に置き換えた例が**図4**になります．

順番に9つの観点の内容を説明します．

■身元確認（Proofing）

物理的な「その人」をシステムが理解できるように，電子的な「ID＝Identity」に紐付けること．よく「本人確認」という言葉を耳にしますが，身元確認と，後に示す「当人認証」の2つを実施して初めて，本当の意味での「本人確認」ができたといえます[6]．

■ライフサイクルマネジメント（Life-cycle Management）

電子的なIDが生成されてから破棄されるまでの一連の状態と，その遷移を管理すること．ISO/IEC 24760ではこの観点についてモデルとともに説明されています．

企業では，人事イベントや，改姓，組織名変更などと連動してアカウントの状態が正しく変遷しているかが主な確認ポイントとなります．2023年1月25日にIPA（情報処理推進機構）により発表された組織向けの「情報セキュリティ10大脅威2023（IPA10大脅威）」[7]

表　NIST SP800-63 [4] とISO/IEC 24760 [5] の概要

NIST SP800-63	“Digital Identity Guideline” システムへの要求事項として，デジタルアイデンティティに関する保証レベルを定義しているガイドライン
ISO/IEC 24760	“IT Security and Privacy -A framework for identity management-” デジタルアイデンティティの管理（特に状態変化）に主眼をおき，用語や概念を定義している

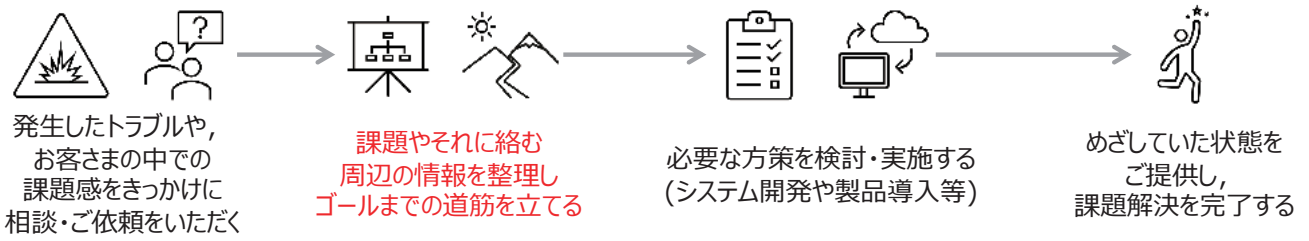

図2　問題解決支援の流れ

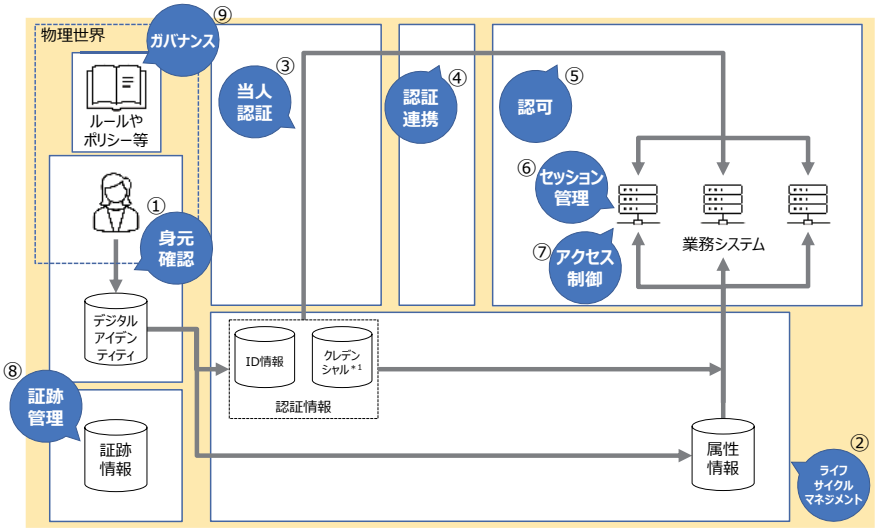

図 3　NTTデータで整理したデジタルアイデンティティの課題整理のためのフレームワーク

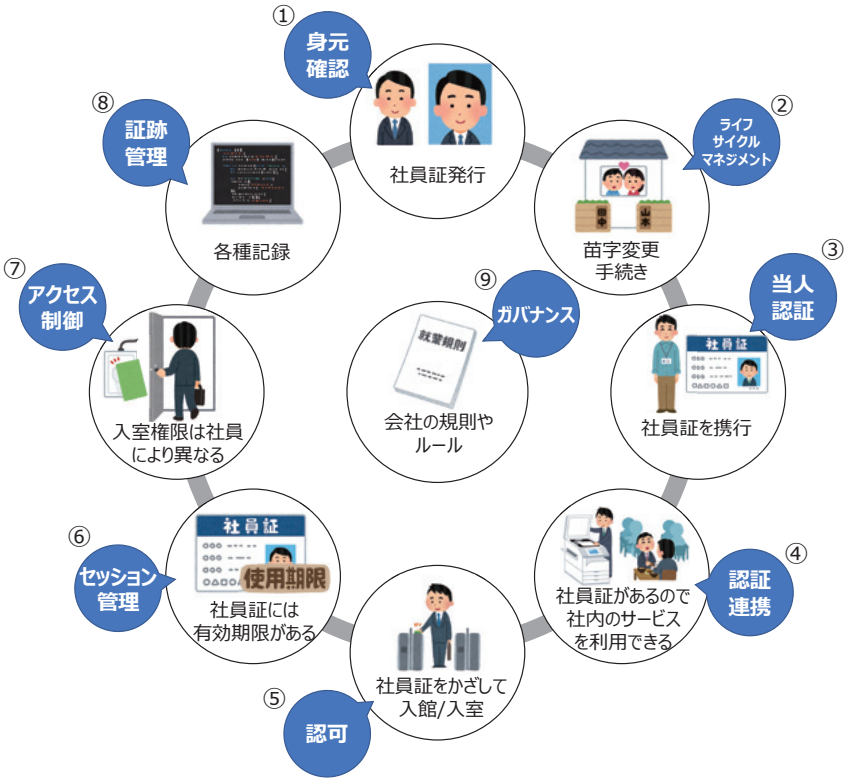

図 4　企業内の物理的な環境におけるデジタルアイデンティティの観点の例

では，脅威第 4 位に選定された「内部不正による情報漏えい」への対策で，「従業員の異動や離職に伴う不要な利用者IDなどは直ちに削除する」べきであると言及されています．

■当人認証（Authentication）

電子的なIDが，持ち主本人によって使用されたかを判定すること．一般的に，認証の 3 要素と呼ばれる「知識」「所持」「生体」のいずれかの情報，またはそれらの組合せで判定します．

始業のために端末にログオンするとき，各システムにサインインするとき，機微な情報の取り扱いがあるシステムを利用するとき，どのような認証情報を使っているでしょうか．IPA10大脅威で指摘されているように，認証情報を窃取・悪用される危険性について十分に検討されているでしょうか．

当人認証については，セキュリティ強度と利便性のバランスなどについてもよく話題に上ります．これまでは，セキュリティ強度を上げようとすると利便性が下がる，両者はトレードオフの関係であるといわれてきました．ですが最近は「パスワードレス認証*2」や「WebAuthn*3」などに代表されるような「セキュリティ強度も利便性もどちらも高い」方法を取ることができるようになってきています．

■認証連携（Federation）

他のシステムで実施した当人認証の結果を受け入れ，自システムで再度当人認証をせずにアクセスを許可すること．認証連携するために，複数サービス間でのSSO（Single Sign On）を実現するケースもあります．

■認可（Authorization）

システムが当人認証の結果を確認し，自らへのアクセスを許可すること．各業務システム側で実施するのか，認証基盤やID管理をするシステム側で実施するのかなどの観点があります．

■セッション管理（Session Management）

当人認証，認証連携，認可をした状態をどの程度の時間保持するかを，要件に沿って決めること．分かりやすい

---

*1　クレデンシャル：パスワードや電子署名，資格証明書など，当人利用であることを確認するために，ユーザ自身が示すことができる情報群のこと．

*2　パスワードレス認証：認証の3要素のうちパスワードに代表される「知識」情報を使わずに当人認証を行う方法．パスワードの漏えいの危険性や，パスワードを覚えなければいけないユーザの負担感を下げることが期待されます．

*3　WebAuthn：Webサービスにおいてパスワードレス認証を実現するための認証技術の仕様の1つ．

判断基準として，機微な情報の取り扱いがあるかどうかという点があります．離席している間，他の作業をしている間，無操作のまま30分経過した後など，どの程度の時間「その情報がその人（例えば離席している間になりすましが発生することも考慮に入れる必要があります）に見える状態になっていて大丈夫か」をシステムごとに整理していきます．

■アクセス制御（Access Control）

各システムが，アクセスしてきたユーザの情報を基にアクセスを許可または拒否（または再度当人認証を要求）すること．IPA10大脅威の第４位「内部不正による情報漏えい」の攻撃手口の１つに「アクセス権限の悪用」が挙げられており，「必要以上に高いアクセス権限が付与されている場合，より重要度の高い情報が窃取」されるおそれがあると述べられています．企業内のシステムにおけるアクセス制御は，ロール（役職などの役割）や属性（アクセス元IPアドレスなどの特徴）の情報を使って行うのが一般的です．各システム側でどのような要件を定めているか，また認証基盤やID管理をするシステムが存在する場合は必要なロールや属性をどのように管理しているかなどについて確認をしていきます．

■証跡管理（Accounting）

利用状況やシステムへのアクセス履歴などを取得・管理すること．「重要情報へのアクセス履歴や利用者の操作履歴などのログ，証跡を記録し，監視すること」は，IPA10大脅威でも重要な対策として挙げられています．昨今ではクラウドサービスの利用が増えていますが，製品によっては社内で規定された期間よりも短いログの保存期間しか保証されないケースもあるため，定期的にエクスポートして別途保管するといった処理が必要になる場合もあります．

また，証跡管理は監査を実施するうえでも重要です．適切なID情報の管理をすることはもちろん必要ですが，定期的な監査を実施し，運用が適切に回っているのかを確認することが求められています．

■ガバナンス（Governance）

デジタルアイデンティティに絡む全要素を企業で正しく運用していくために必要な規程を作成・管理したり，棚卸を実施すること．企業においてガバナンスの維持は非常に重要です．ここまで述べてきた８つの観点について，社内規程やポリシーはあるでしょうか．そしてそれらは適切なタイミングで見直され，現場ではそれに従った運用がなされているでしょうか．

NTTデータが提供できる価値

本稿では，デジタルアイデンティティの重要性，またデジタルアイデンティティについて考えるべき９つの観点を軸にその内容について紹介してきました．NTTデータでは，NISTやISOが定義している既存の標準を参考にしながら，デジタルアイデンティティ全体の課題を体系的かつ網羅的に整理するフレームワークを独自に整備し，それに基づくコンサルティングと，ソリューションの提案を多数実施してきています．冒頭でも述べたとおり，デジタルアイデンティティは社内のセキュリティを考えるうえで避けては通れないテーマであり，土台となる部分です．「デジタルトランスフォーメーション（DX）」「クラウドシフト」「リモート化」など，さまざまなキーワードが流行する中，社内のセキュリティをどのように向上させ，時代に合うかたちにしていくかを考えるとき，ぜひ「デジタルアイデンティティ」を中心に考えてみていただければと思います．全体像を整理する中で，例えば「うちの会社には実はこんなITリソースがあったのか」「明文化されていないがこんな通信経路もあり得てしまう」など，デジタルアイデンティティ以外の課題が見えてくるといった副次的な効果もあり，社内システム全体を見つめ直すきっかけになると，NTTデータは考えています．

■参考文献

(1) https://www.gartner.com/smarterwithgartner/gartner-top-technologies-for-security-in-2017
(2) https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
(3) from NTTデータ：“NTTデータが取り組むゼロトラスト業務環境，” NTT技術ジャーナル，Vol.33, No.9, pp.58-62, 2021.
(4) https://pages.nist.gov/800-63-4/
(5) https://www.iso.org/standard/77582.html
(6) https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html
(7) https://www.ipa.go.jp/security/vuln/10threats2023.html

宍戸 りさ

セキュリティは，業種，業態，規模，国内外を問わず世の中共通のテーマであると考えています．セキュリティと一言でいっても非常に多くの要素を含んでいますが，「デジタルアイデンティティ」という切り口で考えたことのある人は案外少ないのではないでしょうか．本稿で，デジタルアイデンティティという分野の深みを垣間見ていただければと思います．

◆問い合わせ先
NTTデータ
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
TEL 050-5546-2556
E-mail Risa.Shishido＠nttdata.com