DX 時代に向けたセキュリティアーキテクチャ

石　黒　　怜

要　約　企業のデジタルトランスフォーメーション（DX）推進、クラウドの活用、テレワーク対応について利便性を維持して安全に行うために、企業の DX 推進担当者はシステム環境およびクライアント環境のそれぞれにゼロトラスト・アーキテクチャと呼ばれる新たなセキュリティアーキテクチャの導入を検討することが求められている。しかし、ゼロトラスト・アーキテクチャは単一の機能やソリューションで実現できるものではなく、専門的な知識や経験を持つ人材を要するため、各々の企業が独力で導入および運用することは困難である。また、ゼロトラスト・アーキテクチャの導入が企業にもたらす効果は、セキュリティの向上だけでなく業務効率化や DX 推進による企業の競争力向上などがあるにも関わらず、単純にセキュリティ向上策であると紐付けられることが多いため、企業の経営層にはゼロトラスト＝セキュリティ＝収益につながらないコストと捉えられがちである。この点が、企業の DX 推進担当者によるゼロトラスト・アーキテクチャの導入を阻害する要因の一つとも言える。ゼロトラスト・アーキテクチャの導入におけるポイントは、企業のビジネスや統治においてプラスとなる施策であることを経営層に説明することである。また運用におけるポイントは、アウトソーシングを活用することである。

1. はじめに

ゼロトラスト・アーキテクチャとは、ゼロトラスト・セキュリティの考え方に基づいたアーキテクチャである。ゼロトラスト・セキュリティは、2010 年に Forrester Research 社の John Kindervag により提唱されたセキュリティのモデルであり、何も信頼できない状態を前提に利用者、デバイス、ネットワークなどの検証を積み上げていき、信頼できる状態にのみアクセスを許可するという動的なセキュリティモデルである。「動的」と言う意味は、昨日は信頼できたリソースも今日は信頼できないかもしれないという状況の変化に柔軟に対応することを指している。

2020 年の新型コロナウイルス感染症の発生以降、世界中あらゆる業態において働き方の変革が求められるようになった。日本では、「働く方々が個々の事情に応じた多様で柔軟な働き方を自分で「選択」できるようにするための改革」[1]である「働き方改革」において、新型コロナウイルス感染症対策の一環として、ICT（情報通信技術）を利用し、時間や場所に捉われない柔軟な働き方を実現するテレワーク[2]が広く認知され、普及することとなった。これは、ゼロトラスト・アーキテクチャの導入理由と、求められる要素の部分的な側面を示している。デスクワークの業務を例に考えると、単に業務用端末を企業外に持ち出すだけでテレワークが実現できるものではない。テレワークでは、業務用端末から企業内のシステムやデータへのアクセスが不可欠となる。そのため、テレワークの実現には、業務用端末およびそれを利用する従業員のみがどこからでも接続できる社内リソースの提供やネットワークの確立などが欠かせない。これは「何も信頼できない状態を前提に利用者、デバイス、ネットワークなどの検証を

積み上げていき、信頼できる状態にのみアクセスを許可する」というゼロトラストの考えに合致したものであり、ゼロトラスト・アーキテクチャに求められる要素である。

本稿では、BITS2021[*1]における発表を基に、ゼロトラスト・アーキテクチャが望まれる理由について、2章で述べる。サイバーセキュリティリスクへの対策・予防・低減といったコスト的な側面に加え、デジタルトランスフォーメーション（DX）の実現と紐付けて効率や利便性の改善がもたらされるというメリットにも着目する。また、ゼロトラスト・アーキテクチャの導入後は継続的に運用しなければならず、それには様々な知識や技術が要求されるため、一企業内で全てを担うことは困難であり、アウトソーシングを活用することが最適であると考える。そこで、企業がゼロトラスト・アーキテクチャを運用するにあたり、どのような点をアウトソーシングすれば効率化につながるかについて、3章で述べる。

2. DX推進をとりまく環境の変化

ゼロトラスト・アーキテクチャの重要性が高まった背景にはDX推進がある。企業がスムーズにDXへ対応するためには、新しいIT基盤の形が求められている。2章では、DX推進をとりまく環境について、システム環境とクライアント環境に分けて課題を考察する。また、DX推進によるITの役割の変化について補足する。

2.1 DXによるITの役割変化

DX推進とは、ITを活用していくこととイメージされることがあるが、本来のDXはITの役割そのものを変えていくものと考えるべきである。図1は、DXにおけるITの役割変化について、これまでと今後の役割のイメージを図示したものである。Before DXは、今までのITの役割のイメージである。ITは人のサポートを行い、効率化・省力化・コスト削減といった「既存の改善」の役割を担うものであった。対して、After DXが今後のITの役割のイメージである。ITは、差別化や競争力強化の源泉の役割を担い、人間とITが一体となることで新規性やスピードを生み出して「既存の破壊」、つまり変革をもたらすものだと言える。即ち、ゼロトラスト・アーキテクチャの導入をセキュリティ改善や単なる効率化などの施策と捉えるのではなく、ビジネスを加速させるための新たな価値創出を見据えた投資として捉えることが導入検討のポイントと考える。

図 1　DX における IT の役割変化イメージ

2. 2　DX 推進をとりまくシステム環境

本節では、DX 推進をとりまくシステム環境の変化と課題を考察する。

2. 2. 1　システム環境の変化

図 2 は国内企業におけるクラウドサービスの利用動向を示している。企業におけるクラウドの利用は年々増加しており、クラウドサービスを利用することによる効果を多くの企業が実感していることがわかる[3]。また、2010 年から 2020 年にかけては、一貫してクラウドサービスを利用している事業者が、利用していない事業者と比較して労働生産性が高いことがわかっている[3]。

これらのことから、DX 推進のためには、IT の新規性やスピードを確保し、企業の即応力を高めることができるクラウドサービスの利用が適しており、企業によるクラウドシフトが進んでいると言えよう。

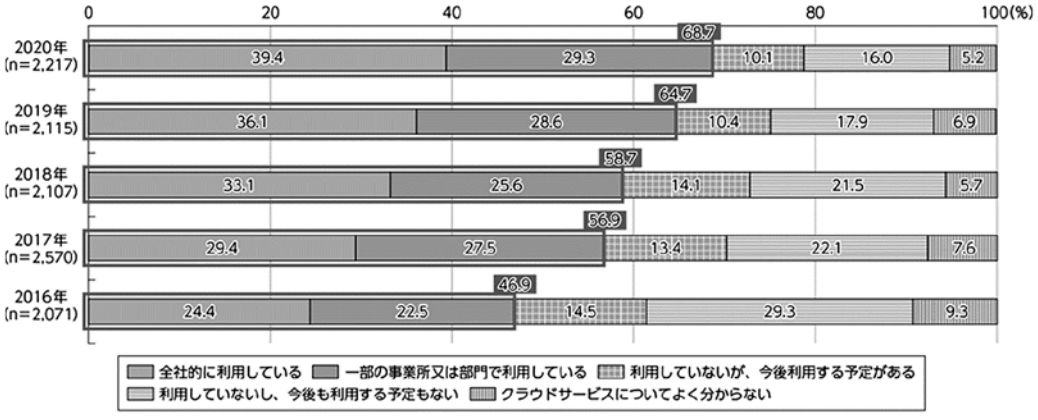

図 2　国内企業におけるクラウドサービスの利用動向[3]

2.2.2　システム環境の課題

クラウドサービスを利用する際に忘れてはならない点は、図3に示す責任共有モデルを理解することである。クラウドサービス形態別のクラウド事業者と利用者の責任分界点を正しく認識し、利用者の責任範囲については利用者で対策しなければならない。

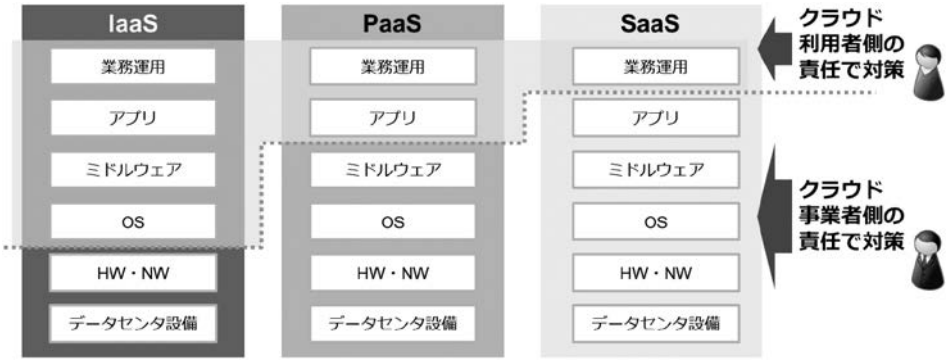

図3　クラウドサービス利用における責任共有モデル

企業によるクラウドサービスの利用が増加しクラウドシフトが進むことで、企業は運用や保守を行わずとも、豊富な機能を持ち誰でも簡単にすぐに利用できるというクラウドのメリットを享受し、DXを推進することができる。しかし、一方でクラウドサービス利用においては、管理コンソールや提供サービスへの不正アクセスや情報漏洩といったセキュリティ事故が多く発生している。原因の多くは利用者による設定不備等であり、上記の責任共有モデルの説明の通り、利用者が対策をしなければならない。そこで、企業のクラウドシフトによるシステム環境の変化に伴うメリットと裏に潜む課題を以下1）～4）に整理する。

1）経験不足な利用者による設定不備の発生

クラウドにより提供されるサービス等は、その技術面の仕様を詳しく知らなくともブラウザなどから誰でも簡単に利用できるが、経験不足な利用者による設定不備が課題である。

2）種々の機能に対する変更管理と設定不備の検知の難しさ

即応力を高めたい企業にとって、豊富な機能を持ち、設定内容を即座に反映できることはクラウドサービスの魅力の一つである。一方、同じ機能であってもクラウドサービスプロバイダーによる設定方法の違いや、多機能が故の複雑なUI等により、変更管理が難しく、設定誤りを発見しにくい点が課題である。

3）インターネットからの広範囲、高頻度の攻撃のハイリスク化

クラウドサービスは企業ネットワーク内のクローズドシステムとは異なり、インターネット上のどこからでも利用できるが、設定に不備があればどこからでも不正アクセスができることを意味するため、攻撃を受ける頻度や攻撃対象者がクローズドシステムとは比較にならない程多い点が課題である。

4）高頻度の機能変更に対する追従の難しさ

クラウドサービスでは日々、機能の追加や変更が行われる。利用者はサービス提供基盤等の開発や運用、保守を行わずに、提供されるサービスの有効活用だけに集中できるが、利用

者は日々の更新に追従し、必要に応じて設定変更をしなければならない点が課題である。

2.3　DX 推進をとりまくクライアント環境

本節では、DX 推進をとりまくクライアント環境の変化と課題を考察する。

2.3.1　クライアント環境の変化

テレワーク未導入事業者と比較して、導入済事業者は労働生産性が高いことがわかっている[3]。また、1 章で述べた通り、新型コロナウイルス感染症対策が進む中でテレワークが普及し、クライアント環境は社内や社外といった物理的な境界に捉われない環境へとシフトしていると言える。システム環境の変化と同様に、クライアント環境からもインターネットを介して提供されるクラウドサービスの活用が増加していると言えるだろう。

2.3.2　クライアント環境の課題

テレワークの普及に加えてクライアント環境からインターネット上のクラウドサービスの利用が増加した。これにより、場所に捉われず柔軟に働けるようになり、クラウドサービスを利用することで業務効率化などが実現できるようになった。しかし、企業ネットワーク外に存在するクライアントを考慮した環境の整備不足や、膨大な通信と数多あるクラウドサービスを認識し評価することの難しさにより、クライアント環境からインターネット上の様々なクラウドサービスを利用することに関して、企業は認識や統制ができなくなっている可能性がある。クライアント環境の変化に伴う課題を以下 1）と 2）に整理する。

1）境界外に配置されるクライアント端末への対応

企業の境界防御外にクライアントが配置されることにより、端末が危険にさらされる可能性が高くなる点、急激な変化に対して社内リソースへのアクセスに用いる VPN 装置等の増強が間に合わない点等が課題である。

2）企業が把握していない従業員個人によるクラウド利用

シャドー IT[*2] と呼ばれる、企業が従業員に利用を認めている以外の企業が把握できていないクラウドサービスへの接続が行われている可能性が高い。また、個人で利用しているクラウドサービスは、アクセス制御やパスワードポリシー等が会社のセキュリティポリシーとは異なるため、これらの業務利用はリスクが高い点が課題である。

3.　DX 時代のセキュリティアーキテクチャ

企業の DX 推進や、クラウドの活用・テレワークに対応するために、システム環境・クライアント環境のそれぞれに新たなセキュリティアーキテクチャの導入が望まれる。本章では、ゼロトラスト・アーキテクチャに求められる要件と実装におけるポイントを述べる。

3.1　ゼロトラスト・アーキテクチャの要件

ゼロトラスト・アーキテクチャを実装する要件の定義として、2 章で述べたシステム環境およびクライアント環境の課題解決を意識する。それぞれの要件を本節で整理する。

3. 1. 1　システム環境の要件

システム環境の課題からは、利用の容易さや利便性、サービスの機能追加・変更の迅速性と引き換えに、利用者による設定不備がセキュリティ事故の原因となりやすく、また、利用者の設定不備は利用者の責任となることを確認した。

これらのことから、システム環境に対しては、IaaS/PaaS/SaaS 等のクラウド環境の責任範囲・特性を認識し、セキュリティ設定を維持・管理することが要件として求められる。

3. 1. 2　クライアント環境の要件

クライアント環境に対しては、シャドー IT を可視化しリスクの高い SaaS 等のサービスを制御することや、どこからでも安全に社内システムやインターネットへアクセスできるようにすることが要件として求められる。さらに、クライアントのセキュリティを強化し、ウイルスの検知と感染した場合の復旧対策も必須である。

3. 1. 3　ゼロトラスト・アーキテクチャの要件と実装イメージ

ゼロトラスト・アーキテクチャの実装イメージを図 4 に示す。また、Forrester Research 社によるゼロトラストモデル「Zero Trust eXtended（ZTX）」[4]から各要件と概要を引用し、各要件に該当すると考えられるソリューション例を分類したものを表 1 に示す。本稿ではゼロトラスト・アーキテクチャそのものの技術的な解説は行わず、紹介に留める。

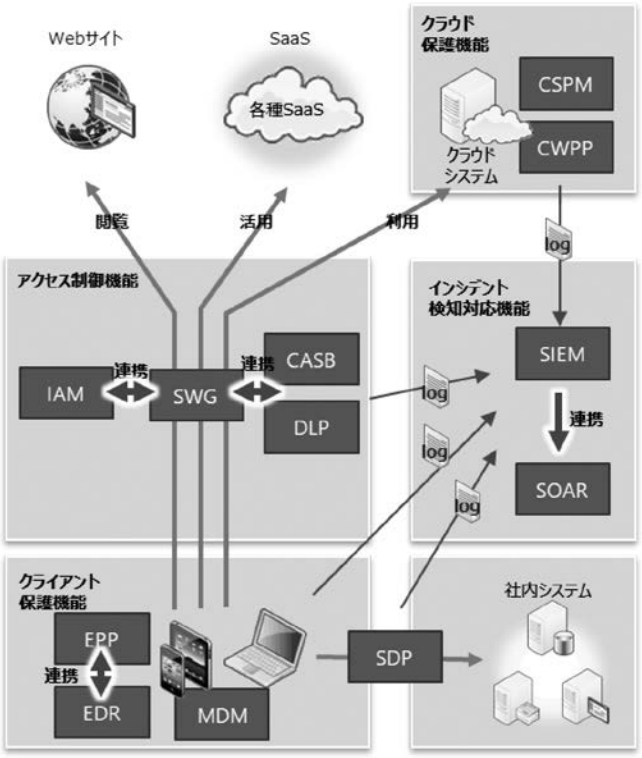

図 4　ゼロトラスト・アーキテクチャの実装イメージ

表 1　要件概要および該当ソリューション

要　　件	概　　要	ソリューション例
ネットワーク セキュリティ	インターネットへの接続環境の中心としてアクセス制御を行う。インターネットセキュリティ強化や脱 VPN の推進となる機能を担う。	SWG（Secure Web Gateway） SDP（Software Defined Perimeter）
デバイス セキュリティ	データへアクセスするデバイスの制限・保護を行う。PC だけではなくスマートデバイスも対象とし、BYOD を含めた管理を行う。	EDR（Endpoint Detection and Response） EPP（Endpoint Protection Platform） MDM（Mobile Device Management）
アイデンティティ セキュリティ	条件設定を含めた多要素による強化されたユーザ認証を行う。様々な SaaS の利用においても統合化された認証によりユーザの利便性向上も担う。	IAM（Identity and Access Management）
ワークロード セキュリティ	主にクラウド上のシステムにおける設定状況の監視やコンテナアプリケーションの保護を行う。また提供するサービスの法令・規制への準拠性を確認する。	CSPM（Cloud Security Posture Management） CWPP（Cloud Workload Protection Platform）
データ セキュリティ	組織が保有する重要なデータの漏洩を防ぐため特定の文字列（クレジットカードナンバー、マイナンバー等）に対する検知を行う。	DLP（Data Loss Presentation）
可視化と分析	様々なログを取得・分析し SaaS を含めたユーザの利用状況等を可視化する。さらに相関分析による不正アクセスの検知を行う。	CASB（Cloud Access Security Broker） SIEM（Security Information and Event Management）
自動化と オーケストレーション	検知されたインシデントへの対応を自動化し、影響範囲の極小化を図る。	SOAR（Security Orchestration and Automation Response）

3. 2　ゼロトラスト・アーキテクチャの導入・運用のポイント

本節では、ゼロトラスト・アーキテクチャの導入時と運用時の要点について述べる。

3. 2. 1　導入におけるポイント

ゼロトラスト・アーキテクチャの導入においては、まず、経営層に導入目的を説明し、了承を得なければならない。しかし、経営層に対して、ゼロトラスト・アーキテクチャをセキュリティインシデントと紐付けて脅威やリスクを低減するための対応という位置づけで説明することは得策とは言えない。なぜなら、企業を運営する経営層にとっては収益をあげ企業を成長させることが命題であり、セキュリティは収益につながりづらい削減可能なコストと捉えられるためである。

そこでポイントとなるのは、ゼロトラスト・アーキテクチャを導入し運用することによるメリットを説明することである。経営層も各部門から構成されることから、様々な視点でメリットを説明することで、各部門の同意を得やすくなる。例えば、人事の立場からすれば、働き方

改革やDX推進がなされている企業をアピールすることができ、人材確保においてメリットがあるだろう。また、企業統制の立場からすれば、ネットワーク管理やデバイス管理の機能によりシステム的にガバナンスを効かせることや、シャドーITの可視化や統制ができるようになる。その他にも、ネットワーク面でのスケールのしやすさやボトルネックの解消、場所や時間に柔軟性を持った働き方の実現、ID管理からクラウドサービスとのシングルサインオン実現等により、情報システム管理部門やセキュリティ担当者、業務端末を使用するエンドユーザー等、幅広くメリットを享受することができる。経営層に対してゼロトラスト・アーキテクチャの説明を行うには、ビジネスと関連付けにくい複雑なコンポーネントの詳細説明や、セキュリティインシデント防止といったマイナスを発生させないための施策という説明をするのではなく、企業のビジネスや統治においてプラスとなる施策という説明をすることが重要である。

3.2.2　運用におけるポイント

ゼロトラスト・アーキテクチャの運用には様々な知識や技術が要求されるため、一企業で運用の全てを担うことは困難であり、アウトソーシングを活用することがポイントである。アウトソーシングするのは、主にセキュリティの専門知識を要する分野が最適だと考える。セキュリティ分野においては、新たな脅威は複雑化・高度化しているため、外部のセキュリティ専門要員を活用することができるマネージドサービスを使うことで、企業は効率的に自社リソースを活用することができる。

4. お　わ　り　に

今回のテーマは、BITS2021において講演した内容をベースとして、企業のDX推進が求められる中で企業をとりまく環境やゼロトラスト・アーキテクチャの必要性、また、経営層への説明や運用時に企業として留意したいポイントを中心として取り上げた。本稿が、未だ途上であり、明確な正解等のないゼロトラスト・アーキテクチャの実装やDX推進を課題として抱える各企業や組織、担当者の一助となれば幸いである。

＊1　BITS2021は、2021年6月2日～4日にオンラインで開催された、BIPROGY（当時は日本ユニシス）グループの総合イベント。

＊2　シャドーITとは、企業・組織側が把握せずに従業員または部門が業務に利用しているデバイスやクラウドサービスなどのITのことである。一般的に企業・組織の情報は管理者が適切に管理している状態を保ち、情報システム部門は各業務部署に情報システムや情報機器を提供する形でIT活用を運用している。スマートフォンやクラウドサービスの普及に伴い、従業員が個人所有の情報機器や外部のWebサービス、ネットワーク回線を利用する状況が広まり、企業や情報システム部門の目の届かないIT活用が増加した。企業・組織が保有する重要情報が管理部門の管理外で利用されることになり、情報流出や、攻撃の踏み台になるなどの情報セキュリティ事故が懸念され、問題となっている。

参考文献　［1］「働き方改革特設サイト（支援のご案内）」，厚生労働省
https://www.mhlw.go.jp/hatarakikata/
［2］「テレワークの推進」，総務省 情報流通行政局情報流通振興課
https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/
［3］「令和3年版情報通信白書」，総務省，2021年7月，P76～78，P313～315
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf

［4］ The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Aug. 2021.
https://www.forrester.com/report/the-zero-trust-extended-ztx-ecosystem/RES137210

※　上記参考文献に含まれる URL のリンク先は 2022 年 4 月 22 日時点での存在を確認。

執筆者紹介　石　黒　　怜（Rei Ishiguro）
2006 年日本ユニシス(株)入社。金融部門にて地銀勘定系パッケージの適用開発、保守に取り組む。2016 年よりセキュリティサービス部門にてプライベート SOC 運用と米国 Unisys 社製セキュリティ製品やセキュリティ関連の販売支援に従事。情報処理安全確保支援士。