その常識、変えてみせる。
SHIFT

Vol.06
May / 2023

# 知の再分配白書

Industry Trend

～ITがよりよく世界に貢献するために～

特集

## 露宇戦争のサイバー領域への示唆

～第3報 サプライチェーン・リスク～

# Index

シリーズ　業界動向解説 SHIFTから世界を読む

# システムの分類
## ～業務システム・基幹システム・情報システム～

事業会社が開発しなければならないシステムを種類別に分けると、大きく3つの種類に分けられると考えています。

**①業務システム**
本業のビジネスを支えるコンピュータシステム
例：銀行のオンラインバンキングシステムなど

**②基幹システム**
企業のバックオフィス業務を支えるシステム
例：会計システム、人事システム、給与システムなど

**③情報システム**
従業員の日々の業務を支えるシステム
例：セキュリティ、オフィス端末、オフィスネットワークなど

事業会社において、システム開発を検討する場合、①～③のIT 予算バランスを考えることと、それぞれをどういう体制でどのような方法で開発していくのか？を決めることが重要です。

①の業務システムは、事業会社にとっての本業であり、他社との差別化を支えるシステムにしていかなければなりません。そうした観点では、提供機能、UI（ユーザーインターフェース）、利用可能ユーザー数、最大処理量など、構築する業務システムがどのくらいの顧客に対応できるか、どのくらいのサービスを提供できるかを考える必要があります。

②の基幹システムは、その会社の会計処理、人事制度、給与制度などを前提にシステムを組み立てなくてはなりませんが、この分野は、ERP パッケージがいろいろ世の中に出ているので、それらのパッケージを上手に組みあわせて、効率よくシステムを構築することが重要です。

③の情報システムは、世の中のIT トレンドに合わせて、従業員が日々行う業務をサポートし、リモート勤務などさまざまな働き方に対応可能なシステムを構築していかなければなりません。世の中に出ている各種 SaaS サービスを組み合わせて、情報システムを構築していくことが重要です。

①から③に必要とされるシステム知見は、それぞれ異なっているため、3種類の専門部署をおいたり、それぞれの分野が得意なベンダーに個々に発注することによって構築していく必要があります。①は本業のシステムに詳しい人やベンダー、②は会計・人事・給与システムに詳しい人やベンダー、③はオフィスシステムに詳しい人やベンダーをそれぞれに配置したり、発注しなければなりません。人選、発注先をしっかりと検討し、最適な体制を構築して、自社に合ったシステム開発を行ってください。

著者

**細田 俊明**　株式会社 SHIFT　上席執行役員 兼 アカウントビジネス推進本部 本部長

大手SIer、証券会社などでCIO室長、品質管理部長を歴任し、2017年1月、SHIFTに入社。同年10月に執行役員に就任し、その後、品質技術部門、コンサルティング部門を設立。2021年9月より、アカウントビジネス推進本部 本部長として、金融領域からゲーム領域までSHIFT事業全般を管掌。

特集

# 露宇戦争のサイバー領域への示唆

～第3報 サプライチェーン・リスク～

## はじめに

日本国政府は、2022年2月24日ウクライナ侵攻直後、ロシアに対する非難とウクライナ支援を表明した[1]。その直後、国内大手自動車メーカーは、子会社がサイバー攻撃を受け、国内全ての工場の稼働を停止する事態に見舞われた。同事例は、ウクライナ支援の支持表明に対する報復に見えるが、攻撃者がサプライチェーンを攻撃する際は、グローバル企業本体ではなく、それを支える脆弱なサードパーティーをターゲットとすることで、グローバル企業全体に影響を与え得るという典型的な攻撃パターンの一例であった[2]。

「サプライチェーン」とは、一般的には原料調達にはじまり、製造、在庫管理、物流、販売などを通じて、使用者（消費者）の手元に届くまでの一連の流れを指し、通常は産業レイヤー以下が対象である。そのリスクは、サプライチェーンのどこかに問題が発生することで、必要とする製品が、必要とする時期に、必要とした量、使用者（消費者）に提供されない不確実性のことを指すのが一般的であり、その問題とは、つまり「サプライチェーンが切れること」を指している。しかしながら、安全保障の観点でさらに掘り下げると、

**●流通物に、第三者が意図する／しないにかかわらず異物が混入すること**

**●そのプロセス内、あるいは流通物から、重要な情報が第三者に漏洩し、優位性が損なわれること**

なども追加され、これらも含めてサプライチェーン・リスクといえる*1。

本論考は、「露宇戦争のサイバー領域への示唆」第3報の位置づけで、オープンソースの情報に基づき、戦時におけるサイバー領域側から見たサプライチェーン・リスクについて概観する。

*1「サプライチェーン・リスク」は、一般的には経済安全保障の用語として使用し、経済、経済活動を円滑に維持していくことが主眼であるが、本論考前半においては、露宇戦争におけるウクライナ軍への武器・弾薬の供給に焦点をあてた上で、軍事組織のサプライチェーン・リスクについて考察する。


著者

**菅野 隆**

株式会社 SHIFT
アカウントビジネス推進本部　金融事業統括部 銀行・公共事業部
マネージャー（ナショナルセキュリティ担当）

防衛大学校卒業後、1989 年陸上自衛隊入隊。陸上幕僚監部防衛部情報通信・研究課総括班長、第35普通科連隊長、ハイチ派遣国際救援隊長、中央即応集団司令部幕僚副長（国内、国際）などを歴任。2022 年に定年退官し、株式会社SHIFT へ入社。
日本安全保障戦略研究所研究員、偕行社安全保障委員会研究員、国際安全保障学会一般会員、博士（工学）
著書「アメリカ合衆国陸軍の基本的運用の変遷と背景」NextPublising, 2022.7

## 全般（キネティック領域に顕在化したサプライチェーン・リスク）

露宇戦争開始から1年、ウクライナに対する軍事（物資）支援は、米国が中心となり、欧米、旧西側の国々と連携しながら実施してきており、ウクライナの兵站[*2]はこれらの国々により支えられている。

武器、弾薬に関していうと、米国は自身の備えである「（軍事物資の）備蓄」を切り崩して、前方（ウクライナ）に供給する要領で支援している。東ヨーロッパでの膨大な弾薬消費により、米国国内での生産能力のバランスを崩し、これを解消するために増産の動きが出てきてはいるものの、米国内の平素の備蓄量への回復が不安視されている声があがっているのが現状である。そして、その悪化した状況を裏付けるかのように2023年2月19日、欧州連合のボレル外交安全保障上級代表は、ウクライナが使用可能な弾薬の在庫が非常に少なくなっており、欧州はこの不足を早急に解決する必要があると警告した。

一方で、米国の備蓄は、台湾危機への対応の可能性にも直結する。加えて現在は、台湾自身も抑止力を強化するために、米国から武器・弾薬の調達を計画して備蓄を整える途上にあり、露宇戦争開始以降、同国の防衛力整備が遅延している可能性がある。

これらは、現在のウクライナと将来に向けた台湾の備え、そして米国自身にとっても、武器・弾薬のサプライチェーンにおいて「米国の防衛産業の製造／増産能力」、「米国の今後の政策判断」がリスクとして顕在化していることに他ならず、我が国の防衛への警鐘とも言えよう。

## ロシアにとってのサイバー作戦の価値と現状

今日の軍隊が関与する紛争においては、サイバー攻撃は、電子戦（EW）、偽情報キャンペーン、衛星攻撃、精密誘導兵器と組み合わせるのが効果的で、その目的は、情報優位性とデータなどの無形資産、通信、諜報資産、および兵器システムを劣化させて、運用上の優位性を生み出すことにある。

具体的に、もっとも損害を与えるアクションは、精密誘導兵器などのキネティック火力と、サイバー攻撃などのノンキネティック火力を組み合わせて、重要なターゲットを無力化または破壊することである。

単独手段としてのサイバー作戦は、指揮・統制、通信、補給などを妨害し、軍事作戦を混乱させる。あるいは、金融、エネルギー、輸送、および政府サービスを混乱させて防御側の意思決定を圧倒することで、社会的混乱を引き起こすことにより、政治的効果にも使用できる。

ただし、これまでのところ、ロシアは意味のある規模で、これらの目標をいずれも達成することができていないと言われている[3]。

## サプライチェーンに対するサイバー攻撃

### ■全般

ロシアの侵攻前の段階において、ウクライナのIT基盤は、従来からロシア製のソフトウェア、ハードウェアで構築されていたため、ロシアが、ウクライナの重要なインフラサービスを麻痺させるのは容易であり、当初のサイバー攻撃でロシア側が圧倒するであろうと予測する声が多かった。

ロシアは、侵攻に合わせてウクライナを混乱させるために、政府、エネルギーおよび通信サービスプロバイダ、金融機関、報道機関などをターゲットとし、サービス妨害、フィッシング、ソフトウェアの脆弱性を突いた破壊的マルウェアのネットワークへのインストールを試みたとされる[3]。

しかしながら、現実には、ウクライナの重要なIT基盤に対する大規模な分散型サービス妨害（DDoS）、ワイパー攻撃は成功せず、ロシアのサイバー攻撃は、

ウクライナの自衛能力を抑制させることができなかった。これはウクライナ側が2014年のクリミア危機以降、協力関係を築いてきた米国をはじめとする友好国や民間アクターからの支援を受けてきた結果であり、ロシアの攻撃的なサイバー作戦の多くを回避（防御）したと評価されている。つまり、サプライチェーン・リスクに適切に対応した事例[*3]と言える（第一報[4]にも記載）[5]。

## ■対象別の攻撃

### 1. 共通の特性とターゲット

一般的に組織は、自らのサイバーセキュリティを優先するため、（その周辺である）サプライチェーンのセキュリティは遅れをとっている（脆弱性が存在する）傾向が高いとされる。また、小規模な組織は、サイバーセキュリティ対策が十分でない可能性が高いとも言われている。攻撃者は、これらの特質を踏まえて弱点を攻撃するとされ、緒言で取り上げた大手自動車メーカー工場の操業停止は、典型的な事例であろう。

この際、留意すべきは、冷戦終了以降、各国は長くグローバリゼーションの下、活動を拡大し、それを基本として経済や産業を進展させてきた点である。その結果、各国が密接に関係する仕組みが構築され、今日の製品に関していえば、それ自体が多くの要素の集合体で、多くの国や企業が関わっている。つまり、サプライチェーンは複雑化し、例え競争国の製品であっても一朝一夕に排除することは困難な状態に至った。このため、サプライチェーンについて考察、対策する場合も「ゼロトラスト」[*4]の考え方を基本に据えることが必要不可欠な時代となったのである。

### 2. ハードウェア

#### (1) 特性

我々が使用するサーバー、コンピュータ、タブレット、スマートフォンなどは、多くの国や企業が関与するグローバル・サプライチェーンで製造されている。専制国家は、その国内で行われるプロセス（コンポーネントの組み立て）において、その製造物に「バックドア」を含めることを要求すること、あるいは、検出ができない特定タイプのゼロデイエクスプロイト[*5]を組み込ませる可能性がある。仮に、国家がバックドアの組み込みを要求しない場合であっても、悪意あるその他のアクターによる不正（賄賂、強要）に従う組み立て作業に従事する従業員が、多くの国に存在している可能性がある。よって、専制国家およびその国内企業をサプライチェーンに組み込むのはリスクと言える。

＊2 戦争を遂行するために必要な人的、物的戦闘力を維持、増強して提供すること。補給、整備、輸送などの支援。（小学館 日本大百科全書）
＊3 2014年のクリミア危機以降、ロシアによるサイバー攻撃に恒常的に晒されてきたウクライナは、米国および同国ベンダーや欧州の支援により、ロシア側のサイバー攻撃に対処し得る態勢をとる準備が整っていた。リスクの高いソフトウェア、ハードウェアの使用を中止するのは攻撃を回避する最初の対策であると考えられる。
＊4 ゼロトラスト(Zero Trust)：「何も信頼しない」を前提に対策を講じるセキュリティの考え方のことで、2010年にジョン・キンダーバグ氏が提唱した概念。
「意外と知らないITトレンド用語」（NTTコミュニケーションズ ICT Business Online）https://www.ntt.com/bizon/glossary/j-s/zero-trust.html
中田 敦「概念の提唱者キンダーバグ氏に聞く、ゼロトラストを今すぐ始めるべき理由」（日経 XTECH 2020.12.15）https://xtech.nikkei.com/atcl/nxt/column/18/01449/121100011/
＊5 ハードウェアに組み込まれたもの。

### (2) 関連トピック(ロシアの事例)

ロシア側は、ウクライナ侵攻において使用した装備品に、非常に多くの西側の部品、しかも輸出を制限する構成品を使用しているとの指摘がある。英国のシンクタンクの調査によれば、ロシアがウクライナに対し運用する数十の兵器システムには、米国あるいは西側の電子部品が使われており、これらの部品なしには機能発揮できない。彼らの運用するシステムの多くはレガシー（旧式）システムである一方で、2021年以降の部品も含まれているとしている。

法治国家である西側先進国の民生品には、(通常バックドアなどは設けられず）専制国家側からすれば「供給されないこと」だけがリスクであり、サプライチェーンが切れることのみに注意を払えばよい。

経済制裁による輸出制限を回避するためにロシアが使用しているサプライチェーンは、旧ソ連が冷戦初期に開発した「ヒューマンネットワーク」と「手法」によるものであり、これまでの西側による経済制裁の多くは、ロシアにはそれほど響いておらず、逆に、自国の企業を攻撃するものであったとしている。

しかし、見方を変えれば、西側の電子部品を使った製造は、ロシアのサプライチェーン、ひいてはシステムに重大な脆弱性を自ら取り込んでいることに他ならない。つまり、ロシアの「サプライチェーン」内で西側国家は複数の先端技術を管理しているともいえ、それゆえ「輸出制限」がもっとも効果的とも指摘する。

今後は、輸出管理に関し実効性を確保し、輸出制限を効果的なものとするため、膨大な量の公開情報データ、通関記録／出荷取引／企業記録などのデータベースを共有、人工知能で処理できる仕組みを構築し、不正な動きに対し瞬時にフラグを立てられる仕組みが必要であるとしている[6]。

### (3) 考察

論考は、西側の国家が専制国家のサプライチェーンの切断のためには、「輸出制限」が最良と主張している。

一方、見方を変えれば、平時に一定レベルの電子部品を供給し、当該国が重要な装備やインフラの心臓部に使用されたとすれば、有事に供給を停止（輸出制限）することにより競争国に対して致命的な影響を与える選択肢を得る可能性が高まることも論考は示唆している。なお、輸出制限時には、前述のロシアの事例にある通り、流出防止対策に万全を期することが必要であろう。

## 3. ソフトウェア

### (1) 特性

ソフトウェア・サプライチェーン・リスクの脅威の多くは、「ソフトウェアを迅速に提供するというプレッシャーの高まり」の一環として、「オープンソース・ソフトウェア・ライブラリ」への依存度が高まっていることに起因するという。それゆえ、ソフトウェアの脅威が、オープンソースの供給に影響を与えるという意見がある。

供給されるソフトウェアにおいて、小さなコードがクリーンかどうか、チェックすることはほとんど不可能であり、攻撃者がマルウェアを流通させることに成功すれば、企業などのIT担当者が実施するアップデートにより、ソフトウェアは汚染される。そして配布されたマルウェアを土台に行われるハッキングにおいては、単にデータが搾取されるのではなく、重要な情報が「人質」に取られ、あるいは破壊される可能性がある[7]。

### (2) 関連トピック(最近の攻撃の一例：Windows インストーラーを使用した攻撃)

最近の事例として、ハッカー達は、偽の Windows

インストーラーを使用したサプライチェーン攻撃で、ウクライナ政府のネットワークを標的にした。脅威アクターは、ウクライナ語およびロシア語のtorrentサイトにおいて、Windows10の正規のインストーラーを装った悪意あるファイルを管理、配布していた。これはスパイ活動の新しい手法の一つと言われている。

2022年7月以降、悪意のあるファイルに感染したウクライナ政府のネットワーク内の複数のデバイスが特定されている。これらのファイルがインストールされると、対象システムに対してデータを搾取するマルウェアが投下される。このマルウェアはウクライナ語の言語パックを使用していることから、ウクライナのユーザーを主ターゲットとして設計されたと考えられている。このマルウェアにより、バックドア機能を持たせることにより、そのコンピュータへのアクセスを維持し、情報の搾取が可能になる。また、このマルウェアは検出防止機能も保持していた。

また、このサプライチェーン攻撃の被害者のなかには、「厳選された」「複数のウクライナ政府機関」が含まれており、その標的は、ロシアを拠点としてサイバースパイ活動を行うハッカー集団の一つであるFancy Bear[8]によって戦争初期にワイパー攻撃された組織と重複しているとしている。つまり、この2つのサイバー攻撃については、攻撃目標のデータベースが共通である可能性が高い。このサプライチェーン攻撃による侵入では、金銭的動機を示す兆候はなく、脅威アクターは、ウクライナ政府から情報を盗むことのみを目的としているようであった。

サプライチェーンへの攻撃は、国家レベルの脅威とされるアクターの間で一般的になっている。攻撃を企図する国家は、標的ネットワークへの広範なアクセスを得るために、彼らに依存している可能性が高い[9]。

**(3)考察**

関連トピックの事例は、一般的に普及したオペレーションシステムの偽インストーラーを普及することで実行された事例の一つである。もっとも基本的なことであるが、ソフトウェアをインターネット経由で入手する場合、最新の注意を払う必要がある。

**■小括**

サプライチェーンに対する攻撃は、

**① 一般的なサイバー攻撃の手段（侵入、分散型サービス妨害（DDoS）、マルウェアによるワイパー攻撃など）をもって直接リアルタイムで実施**
**② 一般的なサイバー攻撃よりも長い時間をかけてターゲットを静かに浸食、情報収集（ソフトウェア、ハードウェア）**
**③ ②の浸食を土台として、緊要な時期に攻撃を発動（輸出制限、バックドアからの侵入、情報搾取、マルウェア攻撃）**

などに整理できる。そして、経済活動、社会活動、あるいは軍事活動を混乱、麻痺させることで、社会的／政治的／軍事的効果を獲得する。

## 総括

前章までの議論を踏まえ、サイバー領域におけるサプライチェーン・リスク（官、軍、民）に対する共通の対策について整理する。

**■共通**

**・ゼロトラストの考え方を基本とする。**
**・リスクのあるソフトウェア、ハードウェア（部品を含む）は排除する。**
**・平素から、信頼のおける国、組織との協力関係を構築。取り引きは、信頼がおける国、組織に限定し、サプライチェーン・リスク局限のために相互に連携する。**
**・サプライチェーン全体のセキュリティに留意する。特に中小企業に配意。**

■ ハードウェア

・サプライチェーン内にリスクとなる可能性のある国家および同国の会社を含めない。（受動的対策）

・平時において、自国の技術を各国に普及、浸透させることで、結果的に同国にとって重要なパートナーである認識も普及。（能動的対策）

■ ソフトウェア

・一般的なセキュリティ対策。

・セキュリティ基準の設定*6。

## おわりに

「露宇戦争のサイバー領域への示唆」第3報の位置づけで、オープンソースからの情報に基づき、本戦時におけるサイバー領域側からサプライチェーン・リスクについて概観した。

ロシアによるウクライナ侵攻の終わりは見えない。動向を引き続きウォッチしつつ、法治が行き渡り、言論の自由が保証された民主主義世界の一員として平和と繁栄に貢献する我が国において、それを支えるIT企業としての重責を認識しつつ努力を継続していく。

＊6 日米の国家安全保障戦略改定に伴い、日米両国政府間で、サイバー防衛で連携するため、政府が調達するソフトウェアについて両国で同レベルの安全基準を構築する。さらに、Quadにこの取り組みを拡大するよう働きかけることを目指す。「ソフトウェアに安全基準 日米、サイバー防衛で覚書へ 政府調達でインフラなどの対策強化」（日本経済新聞，2023.1.5）
https://www.nikkei.com/article/DGXZQOUA0314J0T00C23A1000000

【参考】


［１］「ロシアによるウクライナ侵略を踏まえた対応について」（首相官邸 HP 2022.2.24）
https://www.kantei.go.jp/jp/headline/ukraine2022/index.html

［２］Sean Ashcroft「Supply chain experts share insight on Ukraine war effects」
https://supplychaindigital.com/supply-chain-risk-management/supply-chain-experts-share-insight-on-ukraine-war-effects

［３］James Andrew Lewis,“Cyber War and Ukraine”,CSIS 2022.6.6
https://www.csis.org/analysis/cyber-war-and-ukraine

［４］菅野 隆「ロシアによるウクライナ侵攻開始８ヶ月の段階でのサイバー領域への示唆」知の再分配白書 Vol.1（株式会社 SHIFT 2022.12）
https://service.shiftinc.jp/resources/7887/

［５］Omree Wechsler, “The War in Ukraine: Important lessons to be learnt from Ukraine’s cyber defense success”2022.6.29
https://www.geektime.com/the-war-in-ukraine-important-lessons-to-be-learnt-from-ukraines-cyber-defence-success/

［６］Sean Carberry, "JUST IN: How Russia Is Using U.S. Electronics to Attack Ukraine", National Defense Magazine 2023.1.26
https://www.nationaldefensemagazine.org/articles/2023/1/26/how-russia-is-using-us-electronics-to-attack-ukraine

［７］Steve Banker, "The Russian Invasion, Cyber War, And Global Supply Chains", Forbes 2022.4.5
https://www.forbes.com/sites/stevebanker/2022/04/05/the-russian-invasion-cyber-war-and-global-supply-chains/?sh=46cc30502590

［８］勝村幸博「極悪なのに「ファンシーベア」、五輪狙うサイバー集団名がかわいすぎる理由」（日経 XTECH 2019.11.27）
https://xtech.nikkei.com/atcl/nxt/column/18/00676/111900033/

［９］Daryna Antoniuk, "New supply chain attack targeted Ukrainian government networks", The Record 2022.12.16
https://therecord.media/new-supply-chain-attack-targeted-ukrainian-government-networks

シリーズ

技術特集

Vol.06

# データ分析基盤アーキテクチャ変更の枠組み

## はじめに

本稿では、データ分析基盤のアーキテクチャを変更していくための枠組みを紹介します。

## 企業の競争力を決めるデータ分析基盤

現代の企業活動において、顧客体験の向上や新たなデジタルサービスを構築していくために、データの活用は避けられません。そのためには、データを蓄積するためのシステムが必要となります。データを

著者

**下滝 亜里**　株式会社分析屋　社長室

SIerにて開発に従事した後、事業会社にて基幹システムの開発と保守を経験。分析屋に入社し、データ分析業務や受託事業の推進に従事。

収集、統合、蓄積、可視化、分析するためのデータ分析基盤のシステムです。

顧客との接点やチャネルの増加・複雑化にともなってデータの種類や量が増えていくなかで、どのようにしてデータ分析基盤のアーキテクチャを最適化していくのかは、企業の競争力を決める重要な意思決定となりえます。実際、データ分析基盤がどれだけユーザーによい体験を提供できるかどうか。それが、企業・組織におけるデータ活用の程度を決める要因となります[1]。

しかしながら、当初は最適なアーキテクチャであったとしても、将来も最適とは限りません。既存アーキテクチャの問題を解決する、新たな技術やコンセプトが出現することがその理由の一つです。アーキテクチャ実装のための技術や設計の型（パターン）が、どのくらいの速度で発生するのかは、最適化のための活動の速度に影響します。

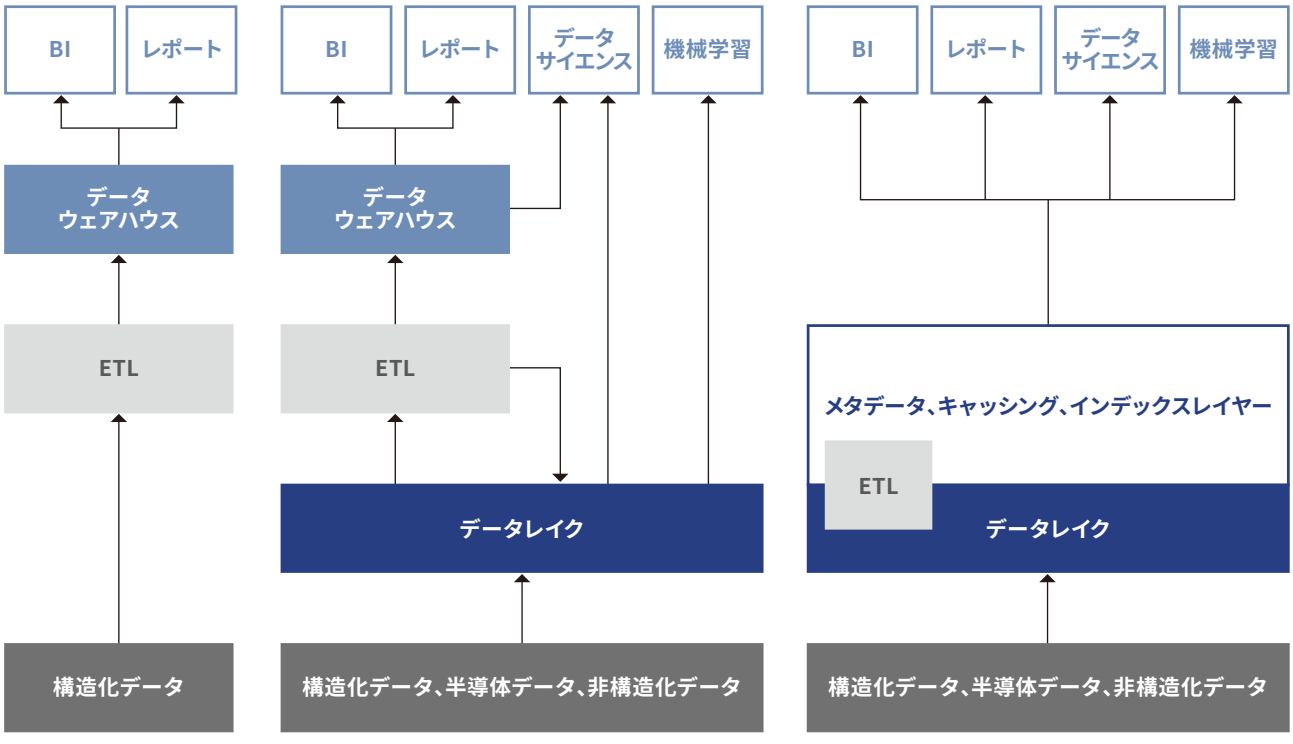
歴史的には、データ分析基盤のアーキテクチャの発展は、どのようなものだったのでしょうか。Armbrust[2] らによれば、最初のアーキテクチャ、現在のアーキテクチャ、次世代のアーキテクチャとして、アーキテクチャの発展が捉えられています（図1）。

1. データウェアハウス：1980年代に登場（図1左）
2. データレイク：2010年に登場（図1中央）
3. データレイクハウス：2020年に登場（図1右）

他にも近年さまざまなアーキテクチャパターンが提案されており[3]、今後もそのような傾向が続くでしょう。このことは、アーキテクチャを設計するにあたっての選択肢が増えることを意味します。

課題は、企業として既存のアーキテクチャをどの

図1　[2] の Figure1 をもとに作成



アーキテクチャに到達するように、いつ変更させていけばいいのかの意思決定が迫られることです。

新たなアーキテクチャパターンは、既存のパターンでは解決できない問題を、解決したいという動機をもとにつくられます。したがって、企業は、2つのケースで競争力を失う可能性があります。

**・既存のパターンに基づくアーキテクチャが、要求の変化に徐々に耐えられなくなり限界を迎え、競争力を失う。**
**・競合企業が自社より速く、従来のアーキテクチャから新たなアーキテクチャに移行することで、競争力を失う。**

アーキテクチャをどのタイミングで変更するのかによって、大きく2つの変更方針が考えられます。

**・問題の発生を起点に変更する**

要求の変化に対応するにつれて、アーキテクチャをもとにして何らかの問題が発生しているときに変更します。問題とは、たとえば、クエリが遅い、コストが増加しているなどです。

**・機会の発生を起点に変更する**

アーキテクチャに問題は発生していないが、アーキテクチャの選択肢が増えた際には、そのアーキテクチャに到達するように変化させることで特定の目的を達成します。たとえば、クエリ速度を速くする、コストを削減するといった目的です。

ここまでは、あるアーキテクチャパターンから別のパターンへの変更に焦点を当ててきました。それよりも小さな変更も考えられます。アーキテクチャを構成する要素を置き換えるような変更です。この場合でも同様の課題が発生します。つまり、設計上の選択肢が増えることと、それに伴う既存の決定の変更です。

## 問題の発生を起点とする変更の事例

本節では、問題を起点に変更したと考えられる、2つの企業事例を見てみます。

### ■アーキテクチャパターンの変更

note株式会社では、データレイクのアーキテクチャから、クラウドデータウェアハウスを用いたアーキテクチャ（Snowflake）に移行した事例が紹介されています[1]。

同社が、Snowflakeに移行したのは、次のような問題が発生していたためです。以下、[1]より抜粋。

**・レコード数が増え、S3のファイルが増えるとともにAthenaのタイムアウトが発生するようになった。**
**・データ分析の要望は増えていくが、インフラの制限により、実現できることに限りが出てきた。**
**・タイムアウトの回避のためデータのETLを行ったが、アーキテクチャが複雑化してしまい、開発の難易度が上がり、増える要望を消化できなくなった。**

このような問題を解決するために、クラウドデータウェアハウスのアーキテクチャへの移行が行われました。移行の結果として以下が得られました。

**・分析業務の効率が大幅アップした。**
**・今まで不可能だった規模の分析が可能になった。**
**・データ活用への興味や関心が向上した。**

### ■アーキテクチャ要素の変更

REVISIO株式会社は、データウェアハウスの要素の変更として、Amazon Redshift からSnowflake への移行を行いました。同社が、Snowflakeに移行したのは、次のような問題が発生していたためです[4]。

**・ビジネス拡大に伴い、データ量・ユーザー・ワークロードが増加した結果、処理速度と安定性が低下した。**
**・それをカバーするためにスケールアップしたが、コストアップとなった。**
**・社内のエンジニアがうまくコントロールできていなかったため、クラスター管理やパフォーマンス・チューニングの運用負荷が発生した。**

移行の結果としては、高速化、安定化、コストダウンの目的が達成できました。

## 機会の発生を起点とする変更の枠組み

機会の発生に基づいてアーキテクチャが最適になるように変更し続けるために、どのような組織的な活動が必要となるでしょうか。本節では素朴な枠組みを考えました。まず、設計とは何かという観点から枠組みの構成要素を特定します。

設計プロセスとは意思決定の一種だと考えられます。意思決定とは、選択肢からの選択です。設計プロセスの結果としての設計は、決定の集まりだと解釈できます。アーキテクチャの設計もまた、特定の粒度での決定の集まりとみなせます。たとえば、どのアーキテクチャパターンを選択するのか、オンプレミスとクラウドプラットフォームのどちらで構築するのか、どのクラウドプラットフォームを選択するのか、どのデータウェアハウスを選択するのかといった選択などです。

設計の変更とは、既存の決定（の集合）を変更することです。たとえば、事例でみたように、データウェアハウスの要素の変更です。

設計は、特定の要求を満たすために行われます。設計は、要求を満たしているかどうか評価されます。評価の結果、設計の変更が必要であることや望ましいことが判明します。たとえばクエリの速度という品質での評価です。

設計の機会とは、新たな技術の出現や設計上のコンセプトの出現により、特定の品質や特性の観点から、既存の設計を改善できる選択肢が増えたことを意味します。たとえば、データレイクハウスといった新たなアーキテクチャパターンの出現は、選択肢が増えたことを意味します。

アーキテクチャの観点からの、枠組みの基本的な構成要素は以下となります。

**・アーキテクチャ設計（意思決定結果の集合）**
**・アーキテクチャへの要求**
**・アーキテクチャの評価結果**
**・アーキテクチャ設計上の選択肢の集合**

設計の機会に基づく変更を行うために、上記の構成要素をもとにした活動（プロセス）を行うわけですが、それは次のようなものが考えられます。

**・アーキテクチャの評価**
現状のアーキテクチャの評価を行い、最適かどうか

を確認します。クエリの速度などの評価項目を定義した上で評価を行います。

**・アーキテクチャの変更**

現状のアーキテクチャを、よりよいアーキテクチャに向けて変更することを意味します。アーキテクチャ要素を変更するだけのこともあれば、アーキテクチャパターンの変更となることもあります。

**・クラウドプラットフォームでの各サービスのアーキテクチャ機能の収集**

特定のプラットフォームでの選択肢の収集です。たとえば、特定のデータウェアハウスを採用したとして、そのデータウェアハウスと連携する新たな機能の出現により、細かな最適化の機会が生まれます。

**・データレイクハウスなど、新たなアーキテクチャパターンの収集**

アーキテクチャパターンレベルで、設計上の選択肢を集めることを意味します。

**・国内／海外のアーキテクチャ事例の収集**

他社の事例をもとに設計上の選択肢を集めることを意味します。自社が今後抱えるかもしれない問題に、他社がすでに直面しており、解決しているかもしれません。解決策がパターンとして整理されていなくとも、選択肢として参考になります。

**・アーキテクチャと関わるユーザーからの要求の吸い上げ**

データ分析基盤に関わるユーザーの視点から、アーキテクチャへの要求が何かを特定します。今は発生しなくとも、将来発生するかもしれない要求を検討することも含まれます。特定できた要求によっては、既存のアーキテクチャに当てはめて評価することで、将来の問題点が明らかになるかもしれません。場合によっては、新たなアーキテクチャパターンを生み出すことに繋がることも考えられます。

**・足りないアーキテクチャ要素の開発**

評価により明らかになった問題に対して、アーキテクチャ要素を開発するプロセスです。

## おわりに

データ分析基盤はビジネスの競争力を決める要因の一つとなりえます。新たな技術やコンセプトによるアーキテクチャ上の選択肢の出現を機会とみなし、アーキテクチャを変更していくことは、企業にとっての課題です。本稿では、データ分析基盤を変更していく上での素朴な枠組みを紹介しました。ぜひ、ご活用いただき、ビジネスの競争力を高めてください。

参考
[1] 久保田 勇喜, Snowflakeがもたらしたnoteのデータ分析の進化, DATA CLOUD WORLD TOUR JAPAN 講演資料, 2022
https://speakerdeck.com/littlekbt/snowflakegamotarasita-notenodetafen-xi-nojin-hua
[2] Armbrust, M. et al. Lakehouse: A New Generation of Open Platforms that Unify Data Warehousing and Advanced Analytics, 2021
https://www.databricks.com/research/lakehouse-a-new-generation-of-open-platforms-that-unify-data-warehousing-and-advanced-analytics
[3] Joe Reis, Matt Housley, Fundamentals of Data Engineering: Plan and Build Robust Data Systems, 2022
[4] 片岡 基, 7年使ったRedshiftから6ヶ月かけてSnowflakeへ移行した話〜手の内全部お見せします〜, Snowday Japan 2023 講演資料, 2023
https://speakerdeck.com/motoy3d/migrating-from-redshift-to-snowflake

# 知の再分配白書

Vol.06
May / 2023

その常識、変えてみせる。

SHIFT