kyndryl

サイバーレジリエンシーと レガシー資産のモダナイゼーション における日本の課題

キンドリルと The Asia Group(アジア・グループ)
による市場への見解

エグゼクティブハイライト

- 日本のサイバーレジリエンシーにとって最大の障壁は、レガシーIT資産への過度の依存です。2021 年に総務省が行った調査では、ICT 投資の 80%がこれらレガシーシステムの保守と運用に使用されているとされています。[1]
- 特に、銀行、官公庁、および医療分野では、重要な業務遂行をレガシー技術に依存しています。自動車と同様に、保守のコストは新しいシステムを購入するためのコストを上回っています。そして新しいシステムを導入すれば、その後数十年にわたって、安全性や標準性を担保できるようになります。
- このホワイトペーパーでは、レガシー技術が直面している３つの重要な課題（セキュリティリスク、人材ギャップ、およびデジタル変革へのハードル）に対処し、日本の組織体がレガシーシステムをモダナイゼーションし、安定・安全なサイバーセキュリティの基礎を実現するための9つのステップを示します。

レガシーITを取り巻く3つの課題

課題1: レガシー技術のセキュリティリスク

ITベンダーは、定期的にレガシー技術から撤退し、システムのためのセキュリティパッチのようなサポートや重要な更新の提供を中止します。それらの提供中止に伴い、新しいセキュリティの脆弱性に対する定期的なパッチ適用も終了します。たとえば、マイクロソフトは、2020 年に、Windows Server 2008 のサポートを終了しました。[2] それ以来、1,546 件の脆弱性（各年の平均で 327 件の脆弱性）が発見されています。発見された年間の脆弱性の数は、2020 年のサポート終了が最初に公表された 2018 以降、急激に増えています（図１）。[3] サポート終了の直前、マイクロソフトは、インストールされているユーザーベースの 60%（2000 万インスタンスを超える）が、まだ Windows Server 2008 および SQL Server 2008 上で稼働していると推定していました。[4]

一方で、いまだに多くの組織は、レガシー技術に依存しており、脆弱になるシステムを、ますます頻繁に発生する重大な攻撃にさらすことになります。組織は、サービスが終了し、パッチのためのサポートが終了した資産を定期的に管理する必要があります。ベンダーが公表した、サポート期間を過ぎてリリースされたパッチは、通常、ミッションクリティカルなセキュリティ上の弱点を修正するためにあります。

図1:
Windows 2008 Server System における脆弱性の数

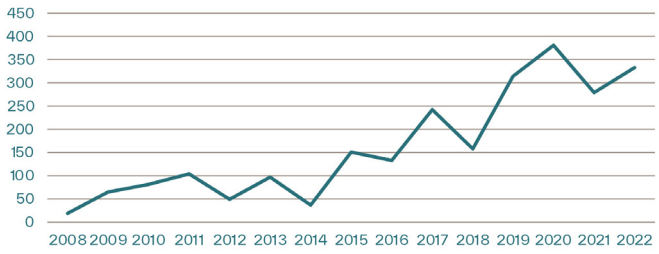

Figure 1: Data from CVEDetails

レガシー技術の多くは、安全性を維持するために必要とされる必須の暗号化規格も欠如しています。例えば、64 ビットまたは 128 ビットを使用してトラフィックを暗号化したWEP（Wired Equivalent Privacy）は、2004 年に廃止されました。現在このレガシー技術は、時代遅れと広く見なされていますが、中にはまだこのレガシー技術に依存し続けている組織もあります。[5] 量子コンピューティングやその他の高度なコンピューティング技術により、レガシー暗号の解読は非常に容易になります。量子コンピューターは、2030 年までに、はるかに堅牢な 2048 ビットの RSA 暗号規格さえ解読すると予想されています。

ツールとおよびメインフレームのサポート

高性能コンピューターであるメインフレームは、大量のメモリとデータプロセッサーを搭載しており、多くの場合、企業内の ICT インフラストラクチャーの基幹として機能し、そこに運用上でのセキュリティおよび信頼性の全てがかかっています。キンドリルが実施した ICT 企業に対する調査(メインフレームモダナイゼーション状況調査レポート) では、調査対象企業の 95%が、メインフレームのワークロードの少なくとも一部をクラウドまたは分散型プラットフォームに移行しており、平均して、ワークロードの 37%をメインフレームの外に移動していることがわかっています。[6] また、予想外のダウンによるコストの増大により、メインフレーム環境のモダナイゼーションを検討しなければならない場合も出てきます。例えば、ミッションクリティカルなワークロードは、多くの場合、メインフレーム環境内で実行され、古いコンポーネントまたはミドルウェアに起因した関連サービスのディスラプションが発生しないようにアップグレードすることが極めて重要になります。キンドリルの調査によると、調査対象企業の 85%がメインフレームをモダナイゼーションする理由となったのはセキュリティに関してであり、その半分がサイバーセキュリティに特に懸念を抱いているからであると答えました。[7]

企業は通常、レガシーなメインフレーム資産における課題に取り組むために、(1)メインフレームそのもののモダナイゼーション、(2)メインフレームをクラウドのような新しい技術との統合、または(3)完全にメインフレームからの脱却、という対応のいずれかを採用します。キンドリルの調査・分析によると、企業はほぼ例外なくハイブリッド手法を選び、メインフレームそのものをモダナイゼーションする場合には2,330 万USドル、クラウドと統合する場合には 2,660 万USドル、そしてメインフレームから脱却する場合には 2,560 万USドルに相当する平均年間コストダウンとなりました。またこれらの対応を取ることで、約 10%の利益増となっています。[8] 企業は、どのプロセスがメインフレーム上で実行するのにより適しているか、どのプロセスをメインフレームの外に移動すべきかを見極めるため、内部調査を行う必要があります。クラウド統合またはより大きいデータアクセシビリティの場合、メインフレームとの統合が最適かもしれません。ただしいずれの場合も、メインフレームが、基礎となるサイバーセキュリティ基準を満たしているか注意する必要があります。

スペクターハードウェアエクスプロイト攻撃とその最も顕著な例であるメルトダウンの出現は、ハードウェアの信頼性に関して、根本的な疑問を投げかけました。スペクターおよびメルトダウンは、中央処理装置(CPU)が、データを読み取り、ユーザーの個人情報にアクセスする過程において、組み込まれた脆弱性を利用し、CPU 自体に影響を与える最初の大規模なハードウェア攻撃です。CPUが散在している以上、CPU にハードウェアの欠陥があれば、企業の電子機器のすべてを脆弱にします。ソフトウェアの脆弱性はパッチと更新によって対処することができますが、ハードウェアの脆弱性は、同じように上書きすることができず、オペレーティングシステムレベルの更新により対処しなければなりません。徐々に、オペレーティングシステムとハードウェアの異なる組み合わせがオペレーティングシステム独自の更新を必要とするようになり、これが技術の乱立につながりました。加えて、これらの解決策は、CPU の処理速度を著しく遅くする要因となることがわかっています。[9]

スペクターとメルトダウンを最初に発見した研究者らは、修正を見つけて展開できるまで攻撃の詳細を非公開としましたが、今後のハードウェアの脆弱性は、サイバーアタッカーにより最初に発見され利用される可能性があります。ハードウェア攻撃は、今後その有効性を考えると、さらに頻繁に利用されるかもしれません。ハードウェア攻撃は、基礎レベルでシステムに影響を与えることができ、サイバーアタッカーが利用できるターゲットの数を大幅に増やします。企業はこれまでは、レガシー技術を内部のファイアウォールで隠すことができましたが、それは完全な解決策ではなくなりました。現在、サイバーアタッカーは、ネットワークに入り込むために人とアカウント、エンドポイントを狙い、ネットワークアクセス取得後、ファイアウォールを回避しています。

課題 2: レガシープログラミングの知識を持つ人材を見つける

企業は、デジタル没入型技術を使い顧客体験を刷新しようとしていますが、その実現に向けて、モノリシックなレガシー技術に依存している組織では、これが大きな障壁になる可能性があります。例えば、銀行、官公庁、および医療分野等でレガシーシステムに依存している組織は、COBOL、Fortran、PERL、Lispのような、1970 年代や 1980 年代によく知られていた言語に基づいてアプリケーションを作成しています。その後、Java および Python が次世代技術の標準になり、その結果こういった組織では、レガシーなコードベースと最新のコードベースの間のギャップを橋渡しすることにかなりのリソースをつぎ込むことになりました。

しかし、開発者がレガシーシステムをモダナイズするにあたり、オリジナルのソースコードが見つけづらい点や資料として残っていない点など、更なる課題に直面しています。これらの課題に対処する際に重要になってくるのが、その場しのぎのアップデート作業ではなく、現代のサイバーセキュリティ理念に基づいた一貫的かつ反復可能なモダナイゼーションのプロセスです。

また、レガシープログラミング言語を知っている人材を見つけることが大きな課題になりつつあります。スタック・オーバーフロー社による 2023 年の調査では、過去 1 年間の開発者の COBOL(0.66%)、Fortran (0.95%)、Perl(2.46%)、および Lisp(1.53%)の利用率が低いということがわかりました。[10] これらのレガシー言語の知識を持つプログラマーが引退し、企業がシステムをモダナイゼーションするのをためらうと、需要が一定のままでありながら、労働力の供給が減少し、この労働力に対するコストが増加し、ソフトウェア開発サイクルの期間が長くなります。

重要なインフラストラクチャーをこれらのレガシー言語に頼っている組織は、運用し続けるためにレガシーアプリケーションをモダナイズするか、または減少する人材を採用することにお金をかけ続けるか、というコストのかかる決定に直面しています。一部の組織は、高給な開発者にレガシー言語を学ばせるため出資することを選んでいますが、レガシー言語を学ぶとキャリア機会が制限されることを知っているため、希望者を見つけることが難航することもあります。例えば、キンドリルの調査によると、調査対象企業の 56%が、新入社員が十分なメインフレームのスキルを持っていないことを懸念しており、47%が、メインフレームの専門知識を持つ社員が引退しつつあることを認めています。[11]

企業は、残っているレガシープログラミング開発者に、そのキャリアについて積極的に尋ね、社内にこれらの言語を学習する意欲のある開発者がいるかどうかを見極める必要があります。それにより、その情報に基づき、モダナイゼーションをどのように進めていくかより適切な決断ができるようになります。

課題 3: デジタル変革の課題と機会

レガシーハードウェアがディスラプションを引き起こす

最近の半導体不足、サーバー機能の向上、およびムーアの法則（コンピューターの処理能力が、おおよそ 2 年ごとに倍増する）の緩やかな減速により、サーバーハードウェアの更新サイクルは長くなっており、アップタイム研究所の調査によると、調査対象組織の49%が、5 年以上の間隔でサーバーを更新していると回答しています。[12] システムのディスラプションおよびサイバー攻撃のリスクを最小限に抑えるには、すべてのレガシーハードウェアをアップグレードする必要があります。組織にとって、ハードウェアの不具合がその主な原因となっています。最近のキンドリルの調査では、ハードウェアの不具合が、キンドリルが行った調査の対象企業において最上位の IT リスク・イベント・カテゴリであることが判明しています。[13]

従来、日本のレガシーインフラストラクチャーおよびガラパゴス化したデジタルエコシステムは、サイバーアタッカーが、アクセスのしやすさ、地政学的、または経済的理由から回避したため、ターゲットにならずに済んだ場合が多く存在します。しかし、この状況は徐々に変化しています。日本は、2023 年の 主要13 市場の中でデータ漏洩の割合が最も低かったものの、漏洩 1 件当たりのコストは、世界平均をはるかに上回っています。[14]さらに、警察庁のデータによると、サイバー攻撃の割合は2019 年から 2022 年までの間にほぼ 2 倍になり、攻撃は2022 年に合計で 12,000 件を超え、急激に増加していることが明らかになっています。[15] この増加の背景には、日本語の壁をなくした洗練された翻訳ソフトウェア、時代遅れのハードウェアへの依存、サイバーセキュリティポリシーの頻繁な見直しや更新をしていないなど、無数の理由が挙げられます。[16]

レガシー技術によるデジタル変革のハードル

マッキンゼー社が、1980年代から1990年代に設計された時代遅れの技術システムで運営されていることが多い伝統的な銀行と、最新のフィンテック企業を比較分析したところ、システムをモダナイズすることで財務的メリットが得られる、ということが判明しました。[17] 分析では、フィンテックのプラットフォーム運用コストが、従来の銀行の 10%程度であるということがわかっています。また、時代遅れのインフラストラクチャー上に構築された革新的なアプリケーションが、最新のシステムを使用して機能するように「転換する」のに、より長い時間がかかり、製品化までの時間を遅らせ、競合他社に対する優位性を失わせることも示唆しています。

キンドリルの調査では、メインフレームの変革が、組織の IT 予算のわずか 3.9%の費用で済み、約 10%の利益の増加をもたらすということがわかっています。[18] 従業員と企業は、今後も技術革新を続けることになりますが、この技術革新がレガシーICT資産上にある場合、成果を実現するのはより困難となります。レガシー言語およびプラットフォームは、時間のかかる困難なテストやリリースプロセスを必要とし、開発者の生産性を低下させ、技術革新に制約を課しています。

レガシー ICT システムをモダナイズするためのステップ

ここで、企業がレガシーICTシステムをモダナイズするための９つのアクションをご紹介します。

1. **組織における「レガシー」の定義の確認：** レガシーとは、次のような ICT 資産のことを指します。(1) ベンダーによるサポートが終了した資産、(2) 最新のセキュリティ暗号化保護を欠いている資産、(3) 組織の最新ニーズに対応する機敏性を欠いている資産、(4) 既存の人材を使用してサポートするのが困難である（すなわち、レガシーコーディング言語で構築された）資産。企業は、モダナイゼーションのためにどの資産が優先されるべきか、自社の予算および必要性に基づいて評価する必要があります。
2. **レガシー資産のマッピング：** どの資産がレガシーの定義に当てはまるかを特定するために、組織が現在使用しているすべての ICT システムの徹底的な見直しを実施すること。徹底的な見直しとマッピングは、どの資産を優先すべきかの戦略を練るのに役立ちます。
3. **レガシー ICT 資産を重要なビジネスプロセスに結び付ける：** 組織は、レガシーアプリケーション、レガシーシステム、およびレガシーハードウェアが中核のビジネス活動にとって不可欠であるため、これらの更新を頻繁に遅延させています。組織が、重要なビジネスプロセスの中でこれらの資産にどのように依存しているかを理解し、これらの資産を更新するために実行可能なスケジュールを立てるための行動計画を作成することが重要です。

4. **コアビジネスプロセスにとって許容可能な最大ダウンタイムを定義する：** 長期的な信頼性の確保には、短期的なディスラプションを必要とすることがあります。レガシー技術、セキュリティプロトコル、バックアップ、および回復機能が、組織のダウンタイムのコスト、回復時間、および回復ポイントの目標を満たすことができるかどうかを判断することが必要です。
5. **メインフレームの必要性を分析する：** 多くの組織は、コアビジネスをメインフレーム技術に依存しています。メインフレームのモダナイゼーションによって、組織の柔軟性を向上させながら、セキュリティおよび信頼性の向上をもたらすことができます。企業は、メインフレームをモダナイズするのか、新しい技術と統合するのか、それともアプリケーションまたはワークロードを外に移動させるのかという、極めて重要な選択に直面します。また企業は、メインフレームをモダナイズする際、セキュリティおよびレジリエンシーを念頭に置く必要があります。
6. **モダナイゼーションのロードマップ：** レガシーアプリケーションの場合、リファクタリング、リホスティング、またはリプラットフォームに非常に手間がかかることがあります。さらに、現在直面するインフレや経済的圧力が、ハードウェア更新サイクルの達成を困難にする可能性があります。経営者は短期の指標に縛られることが多く、モダナイゼーションのために必要となる長期投資優先が困難になることがあります。しかし、意思決定者は、組織を刷新するために今日行う投資が将来的に見返りをもたらし、より素早く技術革新し、世界的な競争力を維持し続けることを可能にするということに気付くでしょう。
7. **ハードウェア資産に対する厳密なライフサイクル管理を実施：** キンドリルの調査データは、世界平均の18%と比較して、日本のデバイス の32%が、サポート終了を過ぎているにもかかわらずまだ使用されていると示しています。これらのデバイスに使用できるセキュリティパッチは存在せず、特に、日本の企業がより国際的に統合されるにつれて、サイバーセキュリティ問題のリスクが著しく高まっています。政府は、システムのモダナイゼーションとクラウド導入に必要な民間設備投資を促進するための施行政策と補助金を検討することができます。
8. **すべてのオペレーティングシステムおよびミドルウェアが最新であることを保証するために、厳密なパッチ適用ポリシーを実施：** 開発者が定期的にサービスを提供しているソフトウェアであっても、手動での更新を必要とすることがあります。企業は、オペレーティングシステムまたはその他のソフトウェアの最新バージョン使用を義務付ける厳密なパッチ適用ポリシーを策定し、従業員がソフトウェアを最新の状態に保ち、安全であることを保証するための企業ポリシーを策定して実施する必要があります。
9. **サーバーおよびメインフレームの正常性チェックを定期的に実施：** 企業は、予防的かつ積極的に重要なハードウェアを定期的にチェックする必要があります。アップグレードに伴うサービスのディスラプションへの懸念が起こす躊躇は、レガシーハードウェアに過度に依存する長期的な問題、および防止可能なはずのハードウェア不具合に起因するさらに長いディスラプションにつながります。

政府の役割

日本政府は、これらのサイバーレジリエンシーの目標を達成させるために民間部門を支援することができます。米国の非営利組織であるMITRE Center for Data-Driven Policy は、米国企業がモダナイゼーションの目標を達成する上で重要な障害となっているのは、次のことであると特定しています。

> *. . . これらのシステムへの集中的注意を求める行政機関の政策および法案、最新化を支援するための複数年の予算、および新しいシステムを導入し、古いシステムを引退させることを保証するための責任の仕組みの欠如* [19]

これらはすべて、企業のモダナイゼーション支援のために、日本政府が積極的な手順を実行できる分野でもあります。

例えば、米国政府の政府監査院（GAO）は、問題に目を向けさせるために中立的な仲介の役割を果たすことがよくあります。GAOによる国税庁（IRS）のICT 政策の見直しは、IRSのレガシーICT資産のモダナイゼーションの促進につながりました。[20] 日本は、政府および民間部門のモダナイゼーションを促進するため、内閣府が関連する省庁と連携し、国レベルでの説明責任制度の実施を検討することも可能です。

欧州連合の 2022 年のデジタル・オペレーショナル・レジリエンス法（DORA）や、カナダで審議中の法案、Bill C-26、重要サイバー・システム保護法（Critical Cyber Systems Protection Act）も、民間部門の重要な ICT インフラストラクチャーにおける最低限のサイバーレジリエンシーの規制要件を規格化して義務付けるための実行可能なモデルをいくつか提供しています。これらのモデルは、強力なサイバーレジリエンシーの実践を理解し、実施し、規則化するために必要な明確さとリソースを民間部門に提供することを目指しています。

日本は、これらの問題を国際的に啓発することもできます。日本はすでに、半導体、医薬品、およびその他の技術においてサプライチェーン協力を推進するリーダーとなっています。サイバーセキュリティは、特に、国境を越えるデータフローが経済成長のより大きな推進力となるにつれて、サプライチェーンの運用にとって不可欠です。日本は、多国間枠組みの中で先頭に立ち、サプライチェーンのサイバーセキュリティの規格化を促進することができます。日本はSP 800-171 を活用する一歩を踏み出していますが、CMMC2 など、さらにいっそう包括的な規格の相互採用を促進すべきです。これらの要点は、QUAD、G7、G20、日米経済政策協議委員会などの既存の対話の中で提起することが可能です。

キンドリルについて

世界最大級のITインフラストラクチャーサービスのプロバイダーとして、私たちキンドリルは、デジタル経済の中心で、システムの健全性と絶え間ない改善の実現に全力を注ぎます。何千ものお客様やパートナーと手を取り合い、各々が最高のデジタル・パフォーマンスを実現できるよう、たゆまない取り組みを続けています。

詳細情報

サイバーレジリエンスについての詳細は、以下のページをご覧ください。
https://www.kyndryl.com/jp/ja/services/cyber-resilience

kyndryl™

THE ASIA GROUP

The Asia Group（「アジア・グループ」米国ワシントンDCに本社、アジア太平洋地域に拠点を置くビジネスアドバイザリー会社）が、本ホワイトペーパーの作成においてキンドリル社のオピニオン・パートナーを務めた。

1 Ministry of Internal Affairs and Communications, Information and Communications in Japan: White Paper 2021, 2021, *https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2021/chapter-introduction.pdf*.

2 Takeshi Numoto, "Announcing New Options for SQL Server 2008 and Windows Server 2008 End of Support," July 2018, *https://azure.microsoft.com/en-us/blog/announcing-new-options-for-sql-server-2008-and-windows-server-2008-end-of-support*.

3 CVE Details. Microsoft Windows Server 2008 Vulnerability Statistics, 2023, *https://www.cvedetails.com/product/11366/Microsoft-Windows-Server-2008.html?vendor_id=26*.

4 Kyle Alspach, "Microsoft Inspire 2019: The 6 Biggest Statements From Gavriella Schuster And Judson Althoff," The Channel Company, *https://www.crn.com/news/channel-programs/microsoft-inspire-2019-the-6-biggest-statements-from-gavriella-schuster-and-judson-althoff*.

5 "WEP, WPA, WPA2 and WPA3: Differences and explanation," Kaspersky, *https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa*.

6 "Kyndryl 2023 State of Mainframe Modernization Research Report," Kyndryl, September 2023. *https://www.kyndryl.com/nz/en/campaign/state-of-mainframe-modernization*.

7 Ibid.

8 Ibid.

9 "Meltdown fix can make some machines slower – Intel," BBC, January 2018, *https://www.bbc.com/news/technology-42636415*.

10 "2023 Developer Survey," Stack Overflow, 2023, *https://survey.stackoverflow.co/2023/#technology-most-popular-technologies*.

11 "Kyndryl 2023 State of Mainframe Modernization Research Report," Kyndryl, September 2023.

12 Rabih Bashroush, "Optimizing server refresh cycles with an aging Moore's law," Uptime Institute, January 2020, *https://journal.uptimeinstitute.com/optimizing-server-refresh-cycles-with-an-aging-moores-law*.

13 "The State of IT Risk 2023: Key Findings from IT Decision Makers," Kyndryl, 2023.

14 2023 Global State of Cybersecurity Study: Japan, Infoblox, June 2023, *https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan*.

15 "Cybercrime in Japan hits record high in 2022 as ransomware cases surge," The Japan Times, March 16, 2023, *https://www.japantimes.co.jp/news/2023/03/16/national/crime-legal/japan-cybercrime-rise*.

16. Akinobu Iwasawa, "Cyberattacks on Japan soar as hackers target vulnerabilities," Nikkei Asia, January 2023, *https://asia.nikkei.com/Spotlight/Datawatch/Cyberattacks-on-Japan-soar-as-hackers-target-vulnerabilities*.

17. "Should US banks be moving to next-generation core banking platforms?", McKinsey & Company, July 2022, *https://www.mckinsey.com/industries/financial-services/our-insights/should-us-banks-be-moving-to-next-generation-core-banking-platforms*.

18. "Kyndryl 2023 State of Mainframe Modernization Research Report," Kyndryl, September 2023.

19. David Power and Nitin Naik, "Ten Recommendations to Modernize Archaic and Insecure Legacy Applications," MITRE, May 2023, *https://www.mitre.org/news-insights/publication/modernize-archaic-insecure-legacy-applications*.

20. U.S. Government Accountability Office, "Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements," January 2023, *https://www.gao.gov/products/gao-23-104719*.