kyndryl

「サイバーレジリエントな日本」がもたらす恩恵

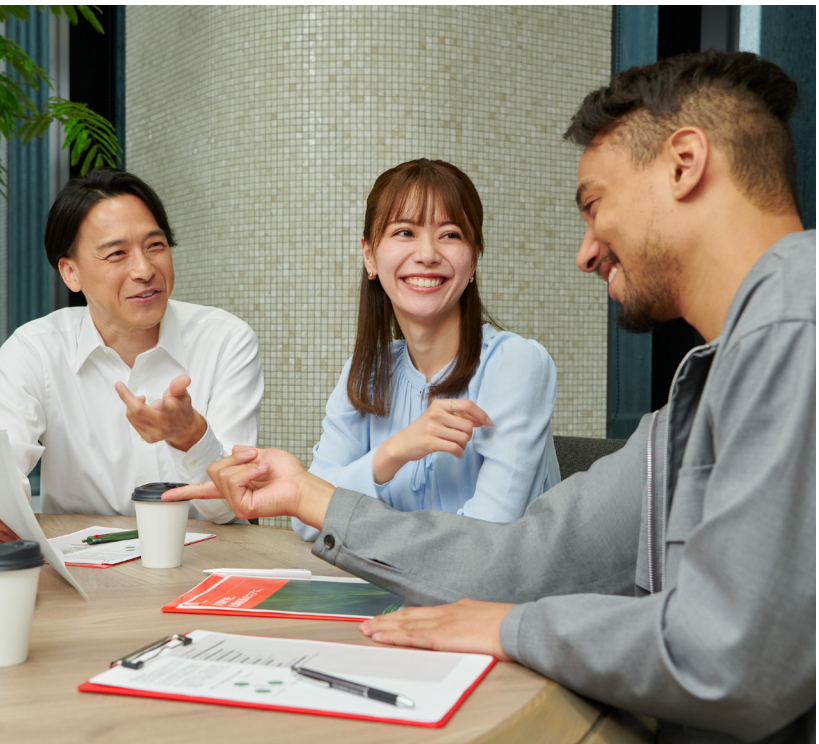
キンドリルとThe Asia Group（アジア・グループ）による市場への見解

エグゼクティブハイライト

- 情報通信技術（ICT）への依存度が高まるにつれ、巧妙なサイバー攻撃、自然災害、地政学的緊張、その他無数の理由によるICTインフラへのディスラプション（中断）は避けられなくなっています。
- サイバーレジリエンシー政策の導入は、日本企業と政府に多大な恩恵をもたらします。サイバーレジリエンシーとは、従来のサイバーセキュリティの基準を拡張し、不可避なディスラプションに耐え、そこから迅速に回復するための積極的かつ予防的対策を組み込んだものです。
- サイバーインシデントが日本企業にとっての最大懸念である中、日本の旧式で維持に法外な費用がかかるレガシーインフラへの過度な依存は、急激で深刻なリスクに日本を晒しています。国内のサイバー攻撃の件数が増加を続ける中、サイバーレジリエンス基準を設けることにより、サイバー攻撃による影響を大幅に軽減することができます。
- サイバーレジリエンシーを取り入れることは、日本のサイバーセキュリティ環境を簡素化し、将来のデジタル革新と成長のための強固な基盤を築くことにもなります。サイバーレジリエンシー向上のために、日本は、レガシーインフラのモダナイゼーション、サイバーレジリエンシー思考の採用、効果的な規制とガバ ナンスの履行に焦点を当てるべきです。民間部門協力、資金インセンティブ、そして情報共有も重要です。

はじめに

企業が中核事業で情報通信技術（ICT）への依存度を高める中、予期せぬ事態によるディスラプション（事業中断）の危険性も高まりつつあります。この脆弱性の増大に伴い、すべてのディスラプションからICTインフラを守ることは現実的に不可能です。内在する技術的リスクはさておき、企業が完璧なサイバーセキュリティ対策を実施したとしても、国家的災害の頻度の増加、サプライチェーンの混乱、地政学的緊張の高まりにより、ディスラプションは避けられません。このような要因が重なり、官民両部門でのディスラプションが近年飛躍的に増加しています。



市場動向と背景

生成AI、量子、その他の先端ICT技術の普及は、破壊性を持つサイバートレンドを加速させるでしょう。生成AIはすでに社会の多くの部門において明らかなディスラプションを引き起こしています。機械処理能力と現実的な言語生成は、既存のサイバーセキュリティ・インフラにさらなるリスクをもたらすでしょう。しかしながら、これはまだ技術の発展に伴うディスラプションの始まりに過ぎません。特に、新量子技術は、早ければ2030年までに現在の暗号化ツールを廃れたものにしてしまうと推定されています[1]。

従来の脅威重視のいわゆる「サイバーセキュリティ」モデルから、サイバーレジリエンスを推進するガバナンス構造に移行することで、企業と政府両方に恩恵をもたらします。サイバーレジリエンスとは、ICTシステムへの逆調、圧力、攻撃、侵害を特定し、予測、防御、対応、そして復旧するプロセスを指しています。

いくつかのトレンドが、サイバーセキュリティにおける世界的な格差の拡大とサイバーレジリエンスへの持続的投資の必要性の要因となっています。その１つが、保護主義的な国内規制を追求する各国のテクノナショナリズムの進行です。自国の技術革新を促進し国民を保護するのは当然のことですが、これが過ぎると規制とデジタル主権のバルカン化、つまり分裂と対立につながります。グローバル企業にとってはコンプライアンスが極めて複雑になり、結果として一部の中小下請け企業を事実上排除することになります。発展途上国はデジタル市場に全く参入できないことが多く、排他的な状況はサイバー犯罪の発生率を高めることにつながります。特にランサムウェア攻撃などは、一度被害に遭うと将来的に同じ攻撃の標的になる確率が高まります。このように、ある国がサイバーセキュリティの標準に準拠していない場合、サイバーオペレーションで標的にされるリスクが飛躍的に高まる可能性があります。この状況がまさに現在の日本で起きているという指摘もあります。[2]

データローカライゼーションはサイバーセキュリティの基準を複雑にし経済成長の妨げとなります。例えば、Information Technology & Innovation Foundationが1998年から2018年までの間OECD加盟46カ国を分析したところ、データ制限性（7段階評価）が1ポイント上昇すると、貿易総生産が7%、生産性が2.9%減少し、小売価格が5年間で1.5%のインフレとなりました。OECD加盟国以外では、データローカライゼーションによる成長の抑制は、同程度の割合でデータ規制の厳しい中国、インドネシア、ロシア、南アフリカで見られました。[3]日本の信頼性のある自由なデータ流通（DFFT）はまさにこの問題に対処するものであり、日本は国際レベルでその運用化を引き続き推進すべきです。日本は世界中のパートナーや民間部門と協力し、プライバシー、サプライチェーンリスク、サイバーレジリエンシーに関する国際的デジタル標準を作成・提唱することで、信頼を高め、データの自由な流れを可能にすることができます。

サイバーインシデントの傾向

キンドリルの定性分析によると、84パーセントの企業が中核事業においてICT資産に大きく依存しており、そのうちの92パーセントが過去2年間に破壊的なサイバーイベントを経験しました。これらのICTに依存している企業のうち、71パーセントがサイバーセキュリティ関連の事案（最も一般的なものはマルウェア、サービス拒否攻撃、その他の侵害、およびインサイダー攻撃やソーシャルエンジニアリングを含むユーザーベースのさまざまな障害）に見舞われており、88パーセントはサイバーセキュリティ以外のシステム障害を経験しています。ICTに依存する企業の５社に１社が異常気象による障害を経験しており、自然災害が企業にいかに頻繁に影響を与えているかを浮き彫りにしています。[4] これらは業務の中断や規制上の問題を引き起こし、評判を傷つけ、事業収益を損失させます。サイバーセキュリティやその他のIT脅威を管理する能力は企業の収益に明確に直結しています。

日本の過剰なレガシーインフラへの依存は日本を急激で深刻なリスクに晒しています。総務省は2021年、日本のICT支出の80％が、攻撃から十分に防護することのできないレガシーインフラの維持に費やされていると算出しました。[5] 2023年に日本企業の半数以上がサイバーインシデントを最大の懸念事項として挙げたのも当然のことと考えられます。インド太平洋地域全体ではトップ3は事業の中断（35％）、サイバーインシデント（32％）、自然災害（27％）であり、日本は地域平均を大きく上回っています。[6]

日本の標的を狙ったサイバー攻撃は増加の一途をたどっています。警察庁の報告によると、2020年の東京オリンピック開催に伴い2021年に顕著な増加が見られたものの、2022年にはサイバー攻撃がさらに増加し、ランサムウェアによる攻撃は58%増加しました。[7] この傾向は2023年も続く可能性があり、日本が4月にG7デジタル・技術大臣会合を開催するのを前に、攻撃は増加しています。[8] 日本が国境を越えたデータの流れなどのデジタル問題に関する多国間対話を主導していても、自国のサイバーセキュリティ基準の遅れにより、サイバー犯罪者の標的となり続けるでしょう。

サイバーレジリエンスのベストプラクティス

レガシーインフラのモダナイズ

日本がより強固なサイバーレジリエンシーを達成するために最も重要な第一歩は、サイバー攻撃を阻止し、それに対応する能力を常に弱体化させてしまっているレガシーインフラをモダナイゼーション（モダナイゼーション）することです。時代遅れのインフラ、特にベンダーによる保守もされなくなったインフラへの過度な依存は、サイバーレジリエンシー改善の努力を無駄にします。インフラが老朽化し初回契約のメンテナンスサポートが終了に近づくと、第三者ベンダーによるセキュリティーツールのサポートも停止する可能性があります。放置されれば安全性が大幅に低下します。レガシーシステムのための新しいベンダーを見つけるだけでは、システムの安全性を十分に確保することは困難で、かえってテクノロジーの乱立とシステムの複雑化を招くことになります。そのため、企業はシステムを簡易かつ安全に運用するために、インフラのモダナイゼーションを積極的に進めるべきです。

日本企業は現状インフラの内部査定を行い、１）中核事業にとって最重要なICTと非ICT資産の確認、２）最も時代遅れのインフラで稼働しているICT資産はどれか、を見極めるべきです。レガシーインフラの完全かつ継続的なモダナイゼーションを最終目標とし、組織の直近の最優先課題として時代遅れのインフラで稼働している重要なICT資産のモダナイゼーションを行う必要があります。モダナイゼーションに向けて日本は、「ゼロトラストの原則」の採用を始めることができます。ゼロトラスト原則とは、ある程度の侵害は避けられない事実を想定し、防御帯を構築することで影響を最小限に抑える方法です。最重要資産の防御にゼロトラスト原則を取り入れることは、公的及び民間組織にとり有益になります。

最終的な目標はすべてのインフラをモダナイズすることですが、企業の直近の取り組みとして、どの既存のインフラがすでにサポートされていないか、またサポートの終了期間はいつか等のモニタリングを積極的に行い、サポートが終了しているインフラのためのクリティカルパッチを即座に行うべきです。ガバナンスレベルでは、多要素認証や社内の危機管理計画の策定や偽ディスラプションシナリオ練習など、簡単に実行できるサイバーセキュリティーの最低限の基本対策を行うことで最大限の備えを整えることができます。

サイバーレジリエント思考の導入

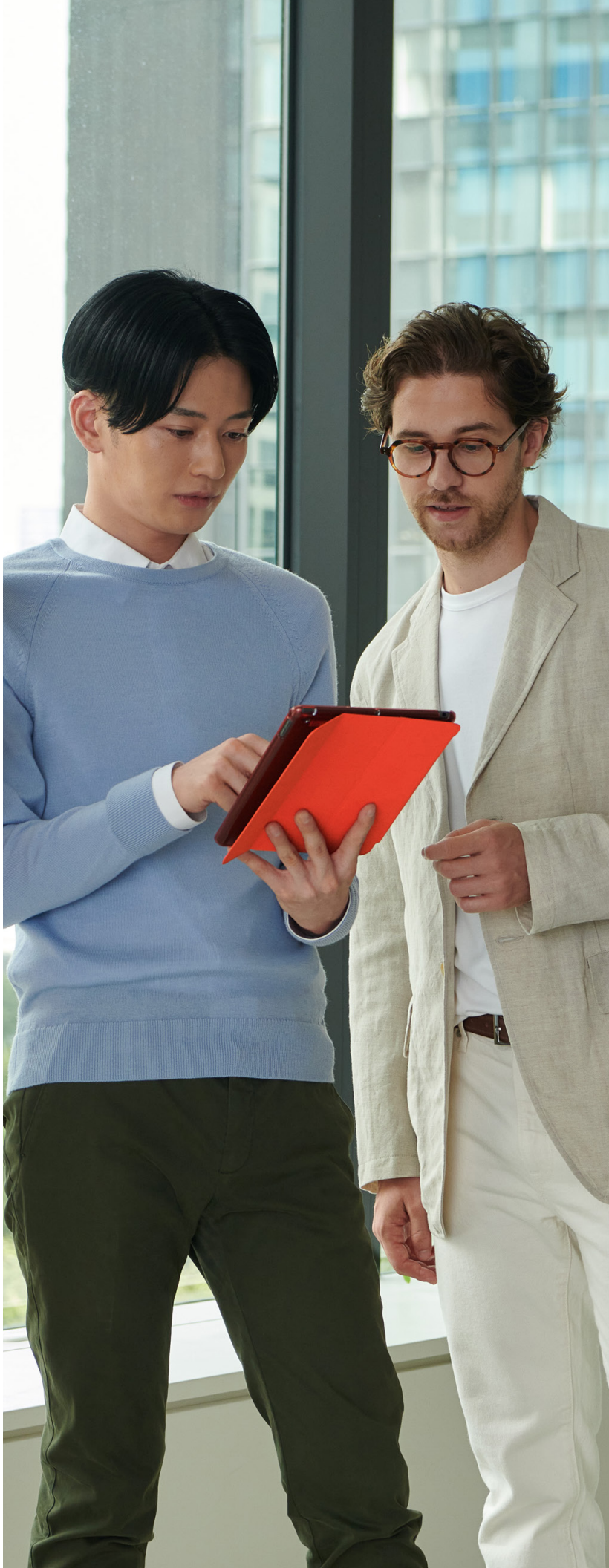
モダナイゼーションへの初期投資は必要ですが、サイバーレジリエンシーには、そもそもレガシーインフラに過度に依存するようになった構造的な背景に取り組むための思考改革も必要です。日本がたとえ一夜にして全てのインフラのモダナイゼーションを達成したとしても、現状を生み出した社会やガバナンスの思考を変えなければ、新しいインフラもすぐに古くなってしまいます。サイバーレジリエンシーを企業のガバナンスの一要素として定着させる必要があります。

重要なのは、経営の視点から、ITインフラのモダナイゼーションと適正化を図る過程で組織のサイバーレジリエンシーをどう最善に維持するかを考えることです。そのために企業は、サイバーセキュリティに関する投資を、短期に重点を置きがちな設備投資費（CAPEX）から、サイバーレジリエンスを長期的かつ一貫したプロセスとする運用費用(OPEX)の一環に置くように転換することが必要になります。これにより、サイバーレジリエンス投資をITシステムの適切な推進に必要な要員費用、そのトレーニング、管理コストの一環として組み込めるようになります。設備投資費としての扱いは、継続的投資を促すよりも、往々にして繰り返される問題に対処するその場限りの投資となってしまいます。

サイバーセキュリティの規制は、業界や専門家のフィードバックに基づいたものである必要があります。SEC（米国証券取引委員会）が提案した「米国証券市場のサイバーセキュリティ・リスクに対処するための新たな要件」にはいくつか良い対策が含まれてはいるものの、企業に真のサイバーレジリエンシーを実践することを求めるには至っていません。[9] 要件にはすべての企業に対して一定の報告要件を満たすことを求めていますが、その内容は主にサイバー障害や使用しているアプリケーションを標的とした攻撃に焦点を当てたものです。これは、サイバーセキュリティの水準を設定する上では一定の利点があるかもしれませんが、「最大の脆弱性はアプリケーションの相互作用に潜んでいる」という重要な懸念には対応していません。対応したくても、企業は自社のアプリケーションやソフトウェアがその他のものと相互作用する可能性のある全ての組み合わせをテストすることは不可能です。

企業が社内での相互作用をチェックしようとしても、直ぐに他社が説明が困難な相互作用のあるものを導入するでしょう。例えば、トヨタ社のサプライチェーンに甚大な被害を与えた2022年の小島プレス社へのサイバー攻撃は、ハッカーが、すでに侵害された第三者のシステムを通して小島プレス社のサーバーに対して行ったものです。[10] 日本では、パートナー同士の緊密な協力関係におけるベクトルや悪用可能な相互作用により、系列企業をこのような攻撃に対して特に脆弱にしている可能性があります。このことはさらに、いくつかの侵害の不可避性を受け入れ、最も重要なハードウェアとソフトウェアの相互作用に起因するリスクの軽減に焦点を当て、企業の負担を軽減し、侵害が発生した場合の稼働時間を増加させる、ゼロトラストセキュリティの必要性を示しています。

大企業や政府はサイバーセキュリティ基準や報告要件を満たすだけのリソースがありますが、政府は中小企業をどう支援するか考える必要があります。日本の中小企業は全体企業数の９９％、労働者人口の７０％以上を占めています。[11] 中小企業は、通常より良い給与を求めて大企業や海外に流出するIT人材の獲得に苦戦しています。最近の調査によると、サイバー攻撃の４０％以上が中小企業を標的としており、これは、中小企業のサイバーセキュリティに対する投資が比較的少なく、サイバー攻撃に対する適切な対応が理解されていないためです。[12] さらに、日本の中小企業経営者の平均年齢は人口の高齢化と後継者の不足に伴い着実に上昇しており、技術的・文化的な変化をさらに妨げる要因となっています。[13] サイバー犯罪者は地方自治体や病院のような組織に加え、こうした日本の中小企業をターゲットと見なしています。政府は、サイバーレジリエンシーを全体的に向上させるたに、こうしたリソースギャップに積極的に対応していくべきです。



規制とガバナンス

政策と規制

国家レベルではサイバーセキュリティーの責任が公平に分散されているとは言えず、中小企業は十分なサイバーセキュリティを実現するために大企業や政府と同様の投資を期待されています。企業ガバナンスでは、逆の問題がある傾向にあり、サイバーセキュリティの責任は縦割りで、最高情報セキュリティ責任者（CISO）のような一人の幹部や、切り離されたIT部門に委ねられていることが多くあります。サイバーレジリエンシーを向上するためには、従業員全員がサイバーセキュリティに貢献するという体制に移行しなければなりません。[14] 組織は、必要なトレーニングや再教育のインセンティブなどの取り組みを通じて、トップダウンのアプローチでこれを実施することを検討すべきです。また、経営幹部や管理職は、サイバー脅威に対する統一戦線を作り出し、モダナイゼーションを実行可能で絶え間ないプロセスにするために、社内の縦割り型経営の排除に積極的に取り組むべきです。

米国では、デジタル問題に対する責任は米国政府全体に広がっています。バイデン政権が推進するサイバーセキュリティの重要な要素の一つは、政府としての対応を一元化し、各方面が連携し、重複する取り組みを削減することです。内閣サイバーセキュリティセンター（NISC）およびサイバーセキュリティ戦略本部は、米国の国家サイバー室（ONCD）が米国政府内を横断して調整しているような形で、官民のステークホルダー間の調整を促し情報共有等を行うための仲介役そして通訳としての役割を担うでしょう。米国のジョイント・ランサムウェア・タスクフォースも喫緊のサイバーセキュリティに関する問題を省庁横断的に推進する機関として参照となります。

サイバー脅威というのは固定的なものではなく、新たな対策方法の発見と共に進化を続けます。例えば、組織がランサムウェアに対処するためのバックアップなどの対策を始めると、悪意のあるハッカーは、ビジネス活動が活発な特定のタイミングにだけ発動するような巧妙なランサムウェアを使用しはじめました。民間企業や専門家の意見を求めるワーキンググループを設置することで、政府はこのような新たな脅威にも柔軟に対応できるでしょう。

民間セクターの協力と資金調達

政府は、強力な調達力とインフラをモダナイズする企業に対する税制優遇措置などのインセンティブを活用し、民間企業だけではできないサイバーセキュリティ基盤の構築におけるギャップを埋めるべきです。日本政府は民間企業に税制優遇措置やその他の補助金を継続的に提供することによりインフラのモダナイゼーションを促すことができます。多くの点で日本は経済安全保障のための世界的な動きの先頭に立っており、補助金や保護措置はすでに経済安全保障法や関連法に組み込まれています。各組織・企業は、利用可能であれば、こうした経済安全保障関連資金を活用するよう努めるべきです。

サイバーセキュリティにおける官民協力を推進するための取り組みの基本的要素は、情報共有です。[15] 官民のサイバー専門家の間の活発かつ率直な情報の流れは重複の無駄を減らし、政府がサイバー攻撃における新興かつ最新の状況を把握することを助け、何よりも大企業のデータへ中小企業がアクセスできれば中小企業にとっても利益をもたらします。情報共有を促すため、政府はノーペナルティの報告制度を維持し、可能な限り機密データは匿名化すべきです。しかし、日本は何よりもまず国民や企業から「自分たちのデータは保護される」という理解を促進しなければいけません。報告することがビジネス上の利益に適うという信頼がなければ、民間が進んで情報共有をする可能性は低いでしょう。

コンプライアンス違反に対する罰則措置は必要ですが、政府が求めようとしている協力的で率直な情報共有を阻害しないよう、慎重に対応するべきです。企業には、罰則措置が取られる前に遵守する機会を与えるべきで、政府は単に違反が疑われた時ではなく、違反が完全に確認された時にのみ公的措置をとるべきです。日本は、最近発表された、政府契約を結ぶために企業が米国国立標準技術研究所（NIST）のサイバーセキュリティの最低基準を満たすことを求めるのと同様のやり方で、政府契約を結ぶ企業に対し、情報共有を義務化する方向に動き始めることを視野に置くこともできます。[16]

予想に反し、サイバーレジリエンシーモデルへの移行は長い目で見れば費用対効果が高いのです。インフラを継続的に更新し、従業員のサイバーセキュリティへの参加を強化するための継続的な投資は、一度に大規模な投資を行う必要性を減らし、悪質なサイバー攻撃から生じるダウンタイム、違反、罰金を削減します。IDCの予備調査によるとサイバーレジリエンスとサイバー防御サービスへの投資は、サイバー攻撃による罰金やその他のコスト影響を回避することになり、その額は5年間で５００％以上の投資対効果を企業にもたらすといいます。[17] より多くの企業がサイバーレジリエンシーの実践を中核となる企業モデルやプロセスに組み込むことができればできるほど、長期的には大きな節約になります。

結論

サイバーレジリエンシーを取り入れることは日本のサイバーセキュリティに対する取り組み全体を簡素化し強靭にすることになります。最も重要なのは民間企業や公的機関がレガシーインフラをモダナイズすることです。サポートされていないハードウエアやソフトウェアに依存し続ける限り日本は決して安全ではありません。このモダナイゼーションの推進はまた、組織の文化の重要な一部となる必要があり、経営レベルからトップダウンでITシステムの適正化に焦点を当てたモデルを採用し、サイバーレジリエンシーを企業運営の絶え間ない一部としなければなりません。機能的で安全なICTインフラは将来のデジタルイノベーションに不可欠な基盤です。日本のビジネスが繁栄し成長するためには、日本の企業や起業家は事業継続性のあるレジリエントでモダナイズされたサイバーセキュリティインフラに信頼を置く必要があります。

キンドリルについて

世の中に必要不可欠なテクノロジー・システムをデザイン、構築、運用し、モダナイズしていく。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きます。

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 National Institute of Standards and Technology, “Report on Post-Quantum Cryptography,” 2016, *https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf*.

2 Leo Lewis, “Japan’s ‘myth of security’ raises cyber attack risk,” Financial Times, *https://www.ft.com/content/bd990583-2948-4769-b090-eac644a2ad69*.

3 Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,” Information Technology & Innovation Foundation, July 2021, *https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost*.

4 Kyndryl State of IT Risk, 2023, *https://www.kyndryl.com/us/en/about-us/news/2023/06/why-cyber-resiliency-planning-is-important*.

5 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*.

6 Allianz Risk Barometer Results Appendix 2023, 2023, *https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023-Appendix.pdf*.

7 “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*.

8 “Cyberattacks increased in Japan ahead of G7 meeting about AI risks, digital infrastructure,” South China Morning Post, April 29, 2023, *https://www.scmp.com/news/asia/east-asia/article/3218860/g7-ministers-focus-ai-risks-digital-infrastructure-pre-summit-meeting-japan*.

9 SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets, 2023, *https://www.sec.gov/news/press-release/2023-52*.

10 “Cybersecurity Nightmare in Japan is Everyone Else’s Problem Too,” Bloomberg, April 17, 2023, *https://www.bloomberg.com/news/features/2023-04-17/rising-cyberattacks-in-japan-show-how-us-europe-are-also-vulnerable?sref=TZEt22gR*.

11 “Japan’s small businesses are in trouble,” The Economist, December 4, 2021, *https://www.economist.com/asia/2021/12/04/japans-small-businesses-are-in-trouble*.

12 Untangle SMB IT Security Report, 2021, *https://get.untangle.com/report_smb_it_2021*.

13 “Japan’s small businesses are in trouble,” The Economist, December 4, 2021, *https://www.economist.com/asia/2021/12/04/japans-small-businesses-are-in-trouble*.

14 Chris Inglis and Harry Krejsa, “The Cyber Social Contract: How to Rebuild Trust in a Digital World,” Foreign Affairs, February 21, 2022, *https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract*.

15 Center for Strategic and International Studies, “A Shared Responsibility: Public-Private Cooperation for Cybersecurity,” March 22, 2022, *https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity*.

16. “Japan to require government contractors meet U.S. cybersecurity rules,” Nikkei Asia, June 23, 2023, *https://asia.nikkei.com/Politics/Defense/Japan-to-require-government-contractors-meet-U.S.-cybersecurity-rules*.

17. Singh et al., “The Business Value of Kyndryl Security and Resiliency Services,” International Data Corporation, 2023.