令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

これからの企業経営で必要な攻めと守りのIT活用および
サイバーセキュリティ対策

サイバーセキュリティ
人材育成
社内体制整備支援

目次

第4章. 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

4-1.これからの企業経営で必要な観点：社会の動向

4-2. 守りのIT投資と攻めのIT投資

4-3. 経営投資としてのサイバーセキュリティ対策

章の目的
第4章では、これからの企業経営で必要な観点となる社会の動向、「守りのIT投資」や「攻めのIT投資」などのIT投資について学ぶことを目的とします。また、経営投資としてのサイバーセキュリティ対策の重要性を明確にすることを目的とします。

主な達成目標
◘ 社会の動向を把握し、現実社会とサイバー空間の繋がりを理解すること
◘ IT投資としての「守りのIT投資」と「攻めのIT投資」を理解すること
◘ 経営投資としてのサイバーセキュリティ対策の重要性を理解すること

4-1-1. 現実社会とサイバー空間の繋がり

日々の生活や企業活動において、ITの活用は広範囲にわたって浸透しています。インターネット利用率（個人）は1997年には9.2%でしたが、2022年には84.9%まで上昇しました。急速なITの普及により、現実社会とサイバー空間が密接に結びつき、私たちの生活やビジネスに大きな変革をもたらしています。

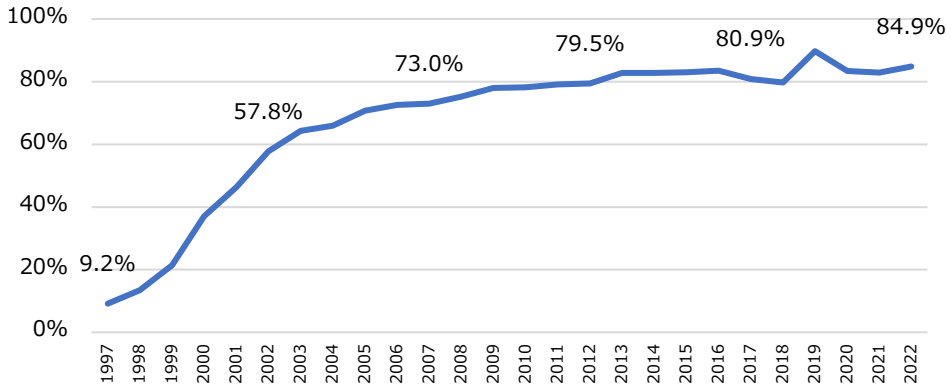


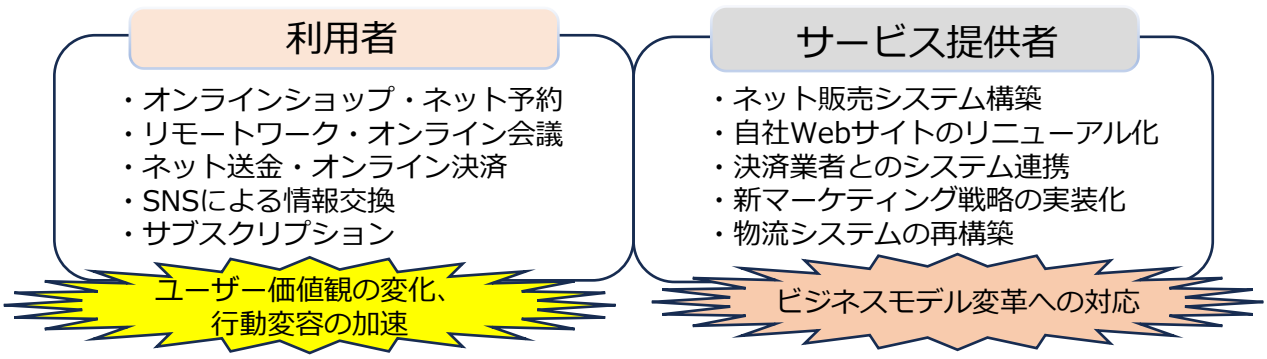
図17. インターネット利用率（個人）の推移
（出典） 総務省「通信利用動向調査」を基に作成

ITの普及により、サービスの利用者はより価値のあるサービスを選択することが可能になりました。例えば、インターネットを介して情報を瞬時に入手したり、オンラインショッピングで広範囲の商品を比較したりすることができます。このように、より便利で効率的な方法でサービスを利用できるようになりました。

さらに、スマートフォンなどの普及により、利用者の意見や情報が即座に国境を超えて広がることが可能になりました。SNSやオンラインコミュニティを通じて、個人が持つ意見や情報が一瞬で共有され、世界的な話題になることも少なくありません。これにより、社会の意識形成や情報伝達において、ITの役割がより大きくなっています。

一方で、ITサービスの提供者は、新たなサービスの提供が日々求められます。技術の進化が速く、競争が激化しているため、常に最新のサービスを提供し続ける必要があります。それに伴い、企業の経営戦略やビジネスモデルも変化しており、革新的なアイディアと素早い行動が求められる時代と言えます。

また、今後の社会では、さらなる経済発展と社会的課題の解決をするため、サイバー空間とフィジカル空間を融合させたシステムによる新たな社会の姿（Society5.0）が提唱されています。



4-1-1. 現実社会とサイバー空間の繋がり

Society5.0で実現する社会では、企業を中心に付加価値を生み出すための一連の活動であるサプライチェーンも変化します。サプライチェーンは、製造、物流、在庫管理、販売などの過程を通じて製品やサービスが供給される経路全体を指します。これまでは、主にサービスが供給される物理的な流れであるフィジカル空間が中心とされていましたが、今後の社会では、サイバー空間との繋がりが重要視されています。

サプライチェーンで利用される技術として、IoTデバイスやAIが挙げられます。IoTデバイスやAIが導入されることにより、製造や物流などのプロセスにおいてセンサーやネットワークが活用され、物理的な動作をサイバー空間で制御・監視できるようになります。さらに、クラウドコンピューティングの普及により、サプライチェーンにおける情報共有やデータのやり取りが容易になり、他社との連携が可能になります。これにより、サプライチェーン全体が可視化され、フィジカル空間とサイバー空間が融合し、サプライチェーンを構成する企業同士の関係は、フィジカル空間だけでなく、サイバー空間においても密接になります。

今後の社会では、サプライチェーンにおけるフィジカル空間とサイバー空間との繋がりが重要視されています。そして、Society5.0に合ったサプライチェーンに変化することで、従来のサプライチェーンもより柔軟で効率的なものになります。

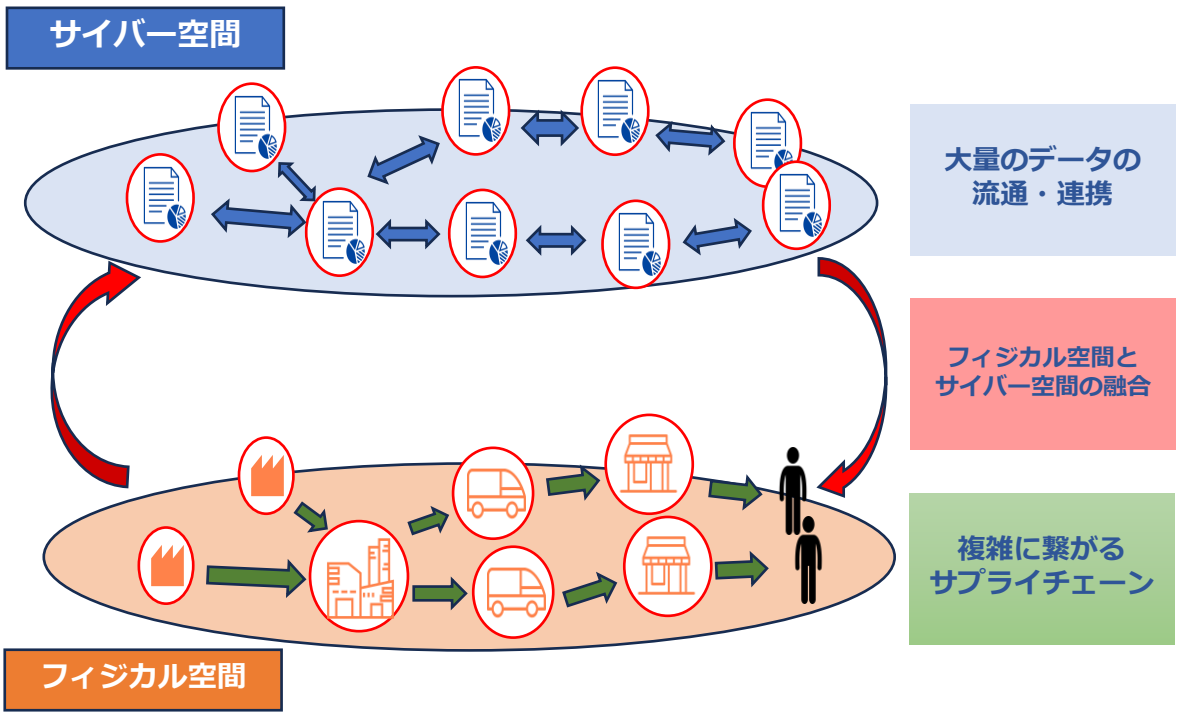


図18. サイバー空間とフィジカル空間の関係図
（出典） 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークVer.1.0」を基に作成

4-1-2. IT活用における課題

我が国のデジタル化について、デジタルインフラ整備などの一部については世界的に見ても進んでいるものの、全体としては大幅に後れていると言えます。様々な理由が複雑に絡み合い、我が国のデジタル化の後れが生じていると考えられます。[9]
ここでは日本社会がデジタル化で後れを取った理由についてみていきます。

我が国がデジタル化で後れを取った６つの理由

1. ICT投資の低迷

我が国におけるICT投資は、1997年をピークに減少傾向にあります。また、我が国におけるICT投資の8割が現行ビジネスの維持・運営に当てられているなど、従来型のシステム（レガシーシステム）が多く残っており、その頃の考え方やアーキテクチャから抜け出せていないと言われています。これらを背景として、我が国では、オープン化やクラウド化への対応、業務やデータの標準化が遅れ、業務効率化やデータ活用が進んでいない状況にあると考えられます。

2. 業務改革等を伴わないICT投資

ICT投資が効果を発揮するためには、業務改革や企業組織の改編等を併せて行うことが重要とされていますが、外部委託に全面的に依存することで、業務改革等をしない形でのICT導入となり、十分な効果が発揮できなかったため、デジタル化に向けた更なるICT投資が積極的に行われなかった可能性があります。

3. ICT人材の不足・偏在

我が国のICT人材は、量も質も十分ではないとユーザー企業に認識されています。また、その人材についても、外部ベンダーへの依存度が高く、ICT企業以外のユーザー企業に多く配置されており、ユーザー企業では、組織内でICT人材の育成・確保ができていません。

4. 過去の成功体験

我が国は、高度経済成長期を経て、世界有数の経済大国となりましたが、ICT関連製造業についても生産・輸出が1985年頃まで増加傾向にあり、「電子立国」とも称されていました。
2000年代に入ってからは、ICT関連製造業の生産額が減少傾向に転じ、2000年代後半には輸出額も減少傾向にありますが、それ以前の成功体験により、抜本的な変革を行うよりも、個別最適による業務改善が中心となり、デジタル社会の到来に対応できていないと言われています。

5. デジタル化への不安感・抵抗感

デジタル化が進んでいない理由として最も多く挙げられたのが「情報セキュリティやプライバシー漏洩への不安があるから」（52.2%）でした。また、パーソナルデータの企業等による不適切な利用、インターネット上に流布する偽情報への対応、慣れないデジタル操作等への習熟など、様々な要因により、デジタル化に対する不安感・抵抗感が生じる場合があると考えられます。

6. デジタルリテラシーが十分ではない

デジタル化が進んでいない理由として2番目に多く挙げられたのが「利用する人のリテラシーが不足しているから」（44.2%）でした。このようにデジタルリテラシーが十分ではないと考えられることから、デジタル化推進に対して消極的になる場合があると考えられます。

（出典） 総務省「情報通信白書令和３年版」を基に作成

[9]:総務省.”情報通信白書令和３年版”. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf, (2023-07-25).

4-1-2. IT活用における課題

現在、日本においてDXの取組状況がどのような状態かを確認するため、DXに取組む企業が多いとされる米国と比較します。

1. DXの取組状況

日本でDXに取組んでいる企業の割合は2021年度調査の55.8%から2022年度調査では69.3%に増加、2022年度調査の米国の77.9%に近づいており、この1年でDXに取組む企業の割合は増加しています。ただし、全社戦略に基づいて取組んでいる割合は米国が68.1%に対して日本が54.2%となっており、全社横断での組織的な取組として、さらに進めていく必要があります。

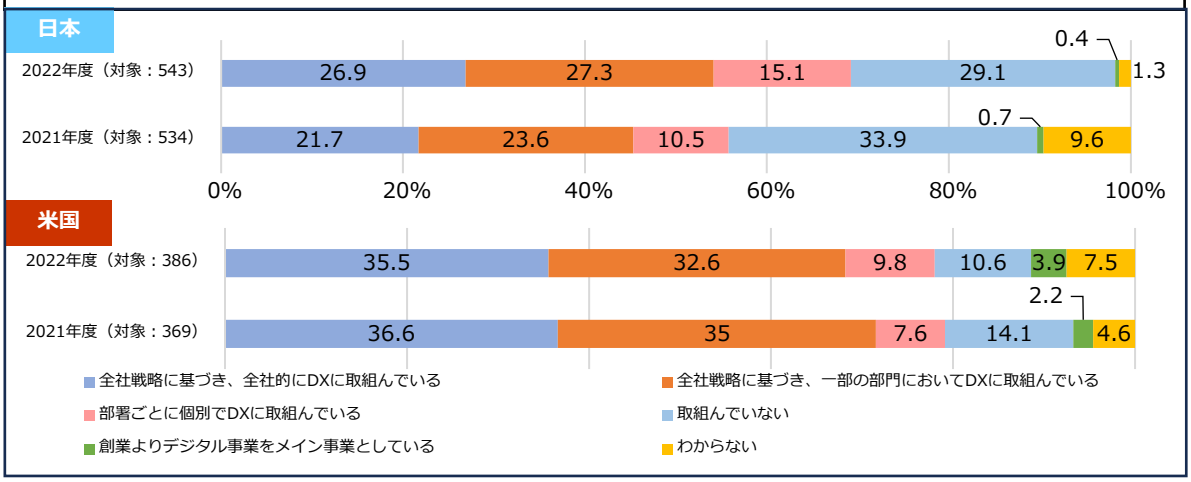


図19. DXの取組状況
（出典）IPA「DX白書2023」を基に作成

2. DXの取組の成果

DXの取組において、日本で「成果が出ている」の企業の割合は2021年度調査の49.5%から2022年度調査は58.0%に増加しました。一方、米国は89.0%が「成果が出ている」となっており、日本でDXへ取組む企業の割合は増加しているものの、成果の創出において日米差は依然として大きいです。

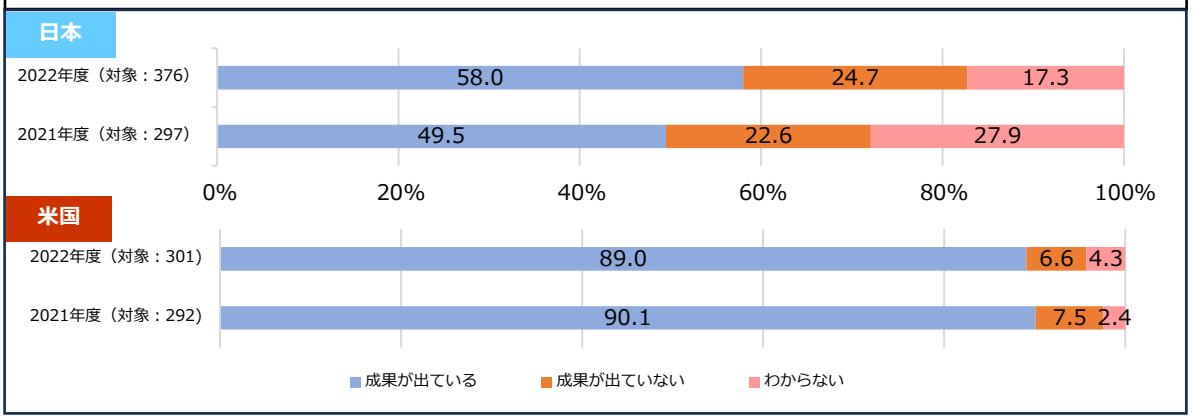


図20. DXの取組の成果
（出典）IPA「DX白書2023」を基に作成

4-2-1. 守りのIT投資、攻めのIT投資の概要

企業のIT投資は、「攻め」と「守り」の2種類に分けて論じられることがあります。「攻めのIT投資」とは、ITを活用して既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規顧客獲得、収益拡大、販売力のアップを目指すことです。一方、「守りのIT 投資」とは、ITによる業務の効率化やコスト削減を目的としています。IT投資に攻めと守りがあることを意識して、両者のバランスをとることが理想です。日本の企業は「守りのIT投資」に偏っていると言われているので、従来より「攻めのIT投資」に重点を置くとよいでしょう。

ここでは、「守りのIT投資」（デジタルオプティマイゼーション）と、「攻めのIT投資」（デジタルトランスフォーメーション）について紹介します。次に、近年特に重要性が増している攻めのIT投資に関して、具体的な実施手順を事例とともに説明します。最後に、近年注目されている主要なデジタル技術に対する取組み方や活用方法を含めて紹介します。

「守りのIT投資」
（デジタルオプティマイゼーション）
目的：生産性向上

・業務の効率化
・コストの削減

「攻めのIT投資」
（デジタルトランスフォーメーション）
目的：ビジネス継続・競争力強化

・新たなビジネスの展開
・顧客視点で新たな価値の創造

One Point

攻めのIT活用指針

経済産業省は、「攻めのIT活用指針」を策定しています。この指針を活用することで、自社の現在のIT活用状況を確認することができます。現状を把握し、これからどのようなIT投資を行っていくかを検討する際の参考になります。

STEP1 IT導入前の状況
ITを導入していない （例）口頭連絡、電話、帳簿での業務
STEP2 置き換えステージ
紙や口頭でのやり取りをITに置き換え （例）社内メール、会計処理や給与計算にITを使用
STEP3 効率化ステージ/ 守りのIT投資（デジタルオプティマイゼーション）
ITを活用して社内業務を効率化 （例）顧客・商品・サービス別の売上分析
STEP4 競争力強化ステージ/ 攻めのIT投資（デジタルトランスフォーメーション）
ITを自社の売上向上などの競争力強化に積極的に活用 （例）マーケティング・販路拡大・新商品開発・ビジネスモデル構築

図21. 攻めのIT活用指針の概要
（出典）経済産業省「攻めのIT活用指針」を基に作成

4-2-2. 経済産業省のDXレポートから見る、「攻めのIT」に取組む方針について

2025年の崖

「2025年の崖」とは、経済産業省が2018年に発表した「DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～」にて提示されているキーワードです。このレポートでは、2025年は、基幹系システムのサポート終了に伴う維持費の増加や人材不足の深刻化などが集中する年であると予測されています。また、こうした既存のITシステムを巡る問題を解消しない限りは、DXを本格的に展開することは困難であると指摘しています。さらに、レポートによれば、日本企業がDXを推進できなかった場合の経済的な損失は、年間最大で12兆円に上ると算出されています。[10]

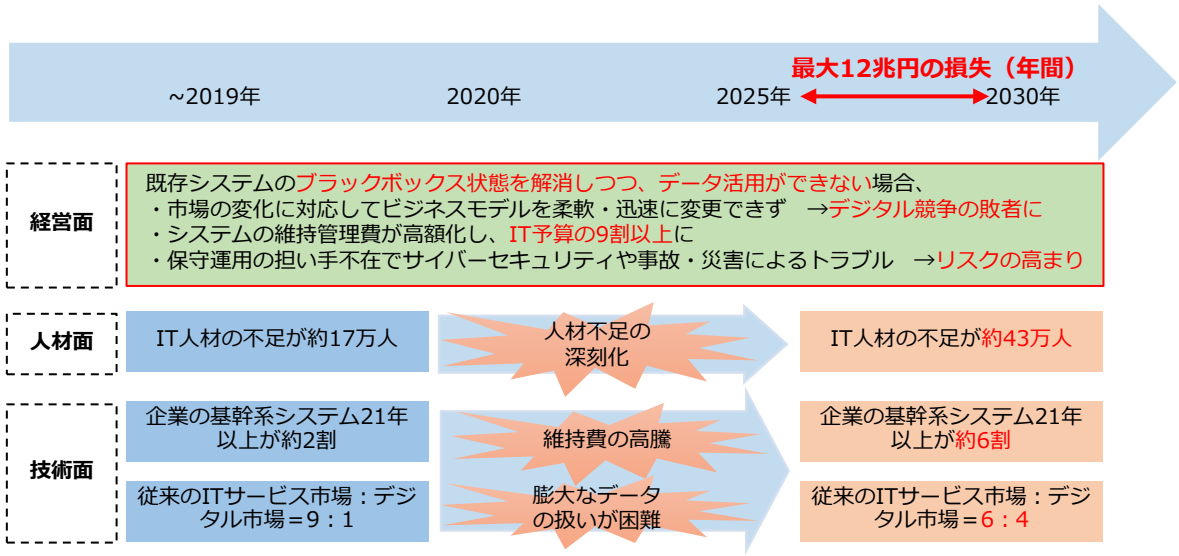


図22.「2025年の崖」の概要図
（出典）経済産業省「DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～」を基に作成

「2025年の崖」に陥らないための対応策

- 「見える化」指標、診断スキームの構築
- DX推進ガイドラインの策定
- ITシステムの刷新
- ユーザ企業・ベンダー企業との新しい関係性構築
- DX人材の育成・確保

[10]:経済産業省." DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～".https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/pdf/20180907_03.pdf, (2023-07-12).

4-2-3. ITを活用した生産性の向上（デジタルオプティマイゼーション）

「守りのIT投資」：デジタルオプティマイゼーション

現代の市場は絶えず変化し続けており、その市場の変化に迅速に対応するため、業務を変革させ、生産性を向上させることが企業にとって重要な課題となっています。生産性を向上させるためには、ITの活用が不可欠であり、「守りのIT投資」、デジタルオプティマイゼーションがその一つとして注目されています。

必要な理由

業務効率化・コスト削減

例えば請求業務はこれまで、表計算ソフトウェアや紙などを使用して手作業で業務を行ってきましたが、その業務には時間がかかってしまう課題が生じていました。そこで、例えば電子契約サービスを導入することで、紙で文書を作成し、その文書に直接押印するというプロセスを省くことができ、業務プロセスを効率化することが期待できます。この改善により、従来の業務にかかっていた時間を短縮し、その削減された時間を他の業務に充てることが可能になります。

デジタル活用するための環境整備

デジタルトランスフォーメーションを実現するには、データの活用が不可欠です。これまでの業務では、表計算ソフトウェアや紙を使用していたため、データを有効に活用することが難しい状況でした。しかし、守りのIT投資を行うことで、データを収集・利用する環境を整えることが可能です。これにより、将来的にデジタルトランスフォーメーションを実施する際の障壁を低減することができます。

「守りのIT投資」には、以下のようなものがあります。
・定期的なシステム更新サイクル・ITによる業務効率化／コスト削減・法規制対応など

進め方

手順１：業務内容・業務フローの可視化

現在の業務プロセスやフローを明確にし、可視化することで全体像を把握します。

手順2：削減・短縮可能な業務の洗い出し

可視化された業務から、削減や短縮が可能な業務を特定します。

手順3：改善や対応の実施

洗い出された業務の中から、優先度や重要度に基づいて順位付けを行い、事前に計画した改善策や対応を実施します。

手順4：業務改革の実現

業務の効率化や品質向上を実現します。

4-2-3. ITを活用した生産性の向上（デジタルオプティマイゼーション）

事例 某エンジニア商社（東京都・製造業）

東京のオフィスに通勤していましたが、新型コロナウイルスの影響により、テレワークへの切り替えを迫られました。書類処理のため、交代で出社しなければならない問題がありましたが、出社が必要な業務をRPAに切り替えていくことができたため、暫定的にテレワークに移行することができました。その後、問題が特に生じなかったため、三つの拠点を一つに統合し、一つの拠点とテレワークに集約することができました。

手順１：業務内容・業務フローの可視化
問題となる業務は、「会社に出社し、お客様や仕入れ先様からFAXで届いた見積書や注文書に対して、紙で返信する業務」であることが判明しました。
手順2：削減・短縮可能な業務の洗い出し
紙ベースの書類を電子データに切り替えることで、出社する手間を削減しました。
手順3：改善や対応の実施
RPAを導入し、FAXデータをPDFファイルに変更しサーバに保存することで、パソコンからどこからでもアクセス可能になりました。
手順4：業務改革の実現
出社する必要が激減し、完全テレワークが実現しました。

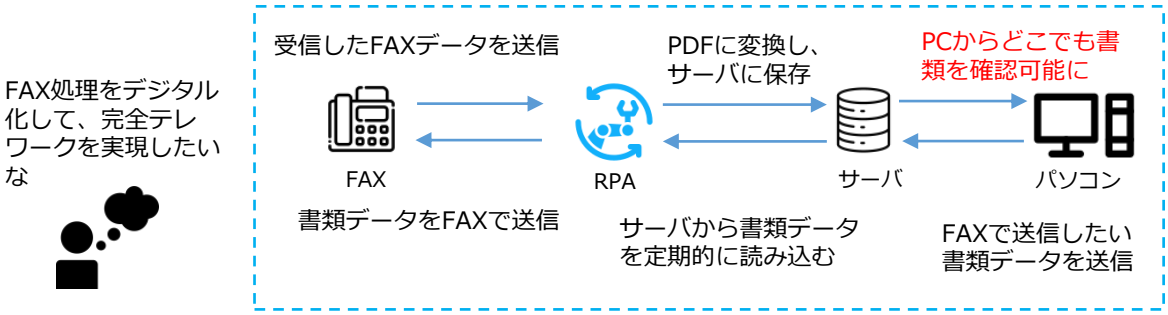


図23. RPAのイメージ図

4-2-4. ITを活用した新たなビジネスの展開（デジタルトランスフォーメーション）

「攻めのIT投資」：デジタルトランスフォーメーション

業務効率化やコスト削減のためにデジタル技術やツールに投資する「守りのIT投資」だけでなく、デジタル技術を用いて、ビジネスモデルを変革したり、顧客視点で新たな価値を創出するデジタルトランスフォーメーションを推進させるため、「攻めのIT投資」を行うことが必要です。

必要な理由

ビジネス環境の急激な変化に対応するため

デジタル技術の普及により、新たな競合他社が市場に参入し、従来のビジネスの常識が変化しています。この状況下で企業がビジネスを継続していくためには、「攻めのIT投資」によって、製品・サービスの品質向上や新規開発、ビジネスモデルの変革などを行い、企業の競争力を維持および強化することが必要です。

多様化する顧客のニーズに応えるため

デジタル時代において、顧客のニーズや期待は大きく変化しています。そのため、「攻めのIT投資」によってデジタルトランスフォーメーションを推進させ、顧客視点で新たな価値を創出し、顧客満足度を高めていくことが必要です。

「攻めのIT投資」には、以下のようなものがあります。

・新規事業の立ち上げ、事業発展　・既存製品の品質向上　・新製品やサービスの開発
・ビジネスモデルの変革など

進め方

手順１：経営ビジョン・戦略の策定

デジタル技術によって市場や顧客のニーズがどのように変化するのかを検討した上で、企業の存在意義や企業理念を再認識し、5～10年後の中長期的な視点で顧客にどのような価値を提供していきたいのか、ビジョンを明確にします。

手順2：変革の準備・課題の抽出

将来のビジョンと現状のギャップから、課題を抽出します。また、関係者に将来のビジョンを説明し、変革を受け入れてもらえるような意識改革を行い、全社的に取組める体制を整えます。

手順3：デジタル技術・業務改革による課題の解決

デジタル技術の活用や業務プロセスの見直し、企業文化の改革などにより、課題を解決していきます。

手順4：顧客に新たな価値を提供・他社のDXに貢献

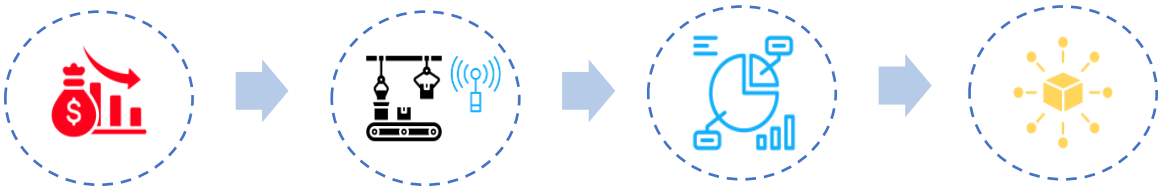
新たな価値を創出し、顧客に提供します。さらに、サプライチェーン全体に対しても貢献していきます。

詳細理解のため参考となる文献（参考文献）	
中堅・中小企業等向け「デジタルガバナンス・コード」実践の手引き	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/contents.html

4-2-4. ITを活用した新たなビジネスの展開（デジタルトランスフォーメーション）

事例：某金属製作所（大阪府・製造業）

2008年の米金融危機により受注が半減し、従来の受注を待つだけの機械加工ではビジネスの継続が困難であるという危機感から、自らサービスを提供できるビジネスモデルへの転換に着手しました。自社の機械加工プロセスのデータを分析することで、新規事業の展開に繋がりました。結果、自社の経営を立て直し、自社だけでなく、他社のものづくりを担う人材を育成することに貢献できるようになりました。[11]



（出典）経済産業省 「中堅・中小企業等向け『デジタルガバナンス・コード』実践の手引き」を基に作成

手順１：実現したいことを明確にする
ビジネスモデルを、受注を待つだけでなく自らサービス提供していくモデルへ転換することに設定しました。
手順2：課題の明確化、関係者の意識改革を実施する
機械加工による製品の開発や販売だけでなく、自ら市場を開拓できるような新たな価値の創出を課題として挙げました。
手順3：デジタル技術による、課題解決
機械加工を行う機器にデータを計測するセンサーをつけ、加工データをリアルタイムで計測してデータを抽出し分析して得た情報をもとに、新規事業の展開に繋げました。
手順4：顧客に新たな価値を提供・ビジネスモデルの転換
機械加工の現場における生産性の向上や品質の改善、人材の育成などの課題を解決するサービスを提供できるようになり、受注だけに頼らないビジネスモデルを構築できました。

[11]:経済産業省. “中堅・中小企業等向け『デジタルガバナンス・コード』実践の手引き”. https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf, (2023-07-10).

4-2-5. 次世代技術を活用したビジネス展開

デジタルトランスフォーメーションを推進していく際、ただ単にデジタル技術を導入すれば良いというわけではありません。自社の実現したいこと（将来のビジョン）から、実現に必要な課題を明確にし、その課題を解決するためにデジタル技術の活用が求められます。現在は、AI、IoTなど新しいデジタル技術が多くあります。

以下では、主なデジタル技術を紹介します。次に、デジタル技術を活用して自社の課題を解決してもらうための参考情報として、既にデジタルトランスフォーメーションを実践している企業の事例を紹介します。

デジタル技術は手段であり、導入自体が目的ではない

AI、IoTなど最新のデジタル技術を用いて、何かできないかな？

自社の課題を解決するためには、このデジタル技術を活用する必要があるな

項目	概要	活用方法例
AI	AIは、膨大な情報を処理し、判断や予測を行うことができます。	• 需要の予測や在庫の最適化 • 不良品の自動検出 • 対話型AIによる、問い合わせ対応の自動化。近年、学習したデータを元に新しいコンテンツを生成できるAIの登場により、複雑な問い合わせにも対応可能
IoT	現実世界の様々なモノが、インターネットと繋がることです。収集したデータが、インターネットに送信・蓄積され、データを分析・活用することで、新たな価値の創出に繋がります。	• 生産設備にセンサーを設置し、振動データを取得し分析することで、部品の故障予知や性能維持が可能 • 生産設備の稼働状況を可視化したことで、全ての拠点での生産状況をリアルタイムに把握可能
クラウドサービス	自社で機器やシステムを保有しなくても、インターネット経由で、様々なサービスを利用できます。	• 社内情報の一元管理、情報共有の利便性向上 • システムを開発・実行するためのツールや環境構築の作業の省略 • 場所やデバイスに依存せずに作業の継続が可能。リモートワーカーや複数拠点のチームとの協業がしやすくなる

4-2-5. 次世代技術を活用したビジネス展開

実際にデジタル技術を活用して課題解決、競争力の強化を実践していく際の参考として、既にDXを実践している企業が自社の課題に対して、どのようにデジタル技術を活用して解決し、競争力を強化しているのか紹介します。

事例1：某ユニット型制御基板製造企業（愛媛県・製造業）

課題	システム開発において、設計時に仕様変更がかなり多く、適切な情報共有ができないため、製造工程のやり直しや製品の品質低下の恐れがあること。
解決への取組み	社内SNSとしての機能を備え、情報共有がしやすく、簡単にシステムを構築できるクラウドサービスを導入しました。それにより、システムを短期間で開発することが可能となり、業務の変化に応じて修正を即座に反映できるようになりました。その結果、情報の共有、工程管理の効率化を実現しました。さらに、この一連の経験を同じ地域の製造業者に共有するために、他の企業と協力してワークショップを開催しました。その結果、ある企業から、効率化システムのコンサルティング、開発の依頼を受注することができました。これらの経験を生かし、地域のDX推進事業をビジネスとすることを目指しています。

（出典）経済産業省 「DX Selection 2022」を基に作成

事例2：某マッシュルーム生産販売業（山形県・農業、販売業）

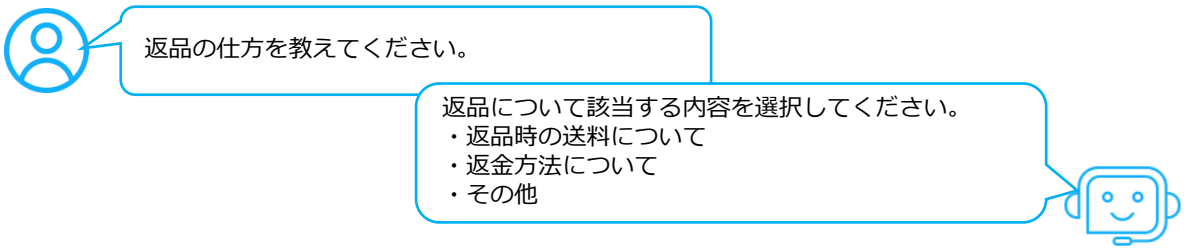
課題	「つくる力」と「とどける力」を将来にわたってさらに強化するために、管理面の強化を行うこと。
解決への取組み	作業の安全性や生産性の向上、栽培作業の平準化を目的に栽培ハウスの温湿度やCo2などの栽培環境の点検作業をIoTを用いて自動化することにしました。IoT導入にあたり、電子機械に詳しい人材を確保し、機器の設置や保守、従業員へのIoTに関する知識の向上や理解を深める指導を行いました。また、システムの使い方を担当者に熟知してもらうために、IoT機器を設置するだけでなく、どのように活用するかの検証やマニュアルづくりを、実際に現場で作業する人員と一体となって進めました。結果、栽培ハウスの点検システムの自動化により、リアルタイムで栽培ハウスのデータを把握でき、勘と経験に頼らない栽培作業の平準化が可能になりました。また、測定で得られたデータをAIを用いて分析することで、最適な栽培条件を絞り込み、マッシュルームの品質向上、栽培作業の平準化、生産量の増大が期待できるようになりました。

（出典）経済産業省 「DX Selection 2023」を基に作成

4-2-5. 次世代技術を活用したビジネス展開

チャットボット

チャットボットとは自動会話プログラムのことです。自動で発信・返答を行うプログラムであるボットは、事前に設定したルール、選択肢などに基づいて、文字形式で利用者とコミュニケーションをとることができます。例えば、よくある質問などを設定しておくことで、お問い合わせ対応を自動で行うことができます。そしてチャットボットでは対応できない内容のみオペレータに対応させることで、人的費用を削減することができます。



予想・今後の発展

近年、AIを搭載したチャットボットが登場しています。これまでのチャットボットとは異なり、蓄積されたデータを学習するため、決められた内容や選択肢に限定されず他の質問にも対応できたり、ユーザからの質問に表現の揺らぎがあった場合でも、一定程度対応できたり、さらには複雑な質問にも回答できるようになっています。

生成AIの登場

生成AIとは、様々なコンテンツを生成することができるAIのことです。従来のAIが主にデータを分析・学習し、その結果に基づいて予測を行うのに対して、生成AIは新たなコンテンツの創造を目的として学習します。生成AIは学習量が多いため、回答の精度や質が従来のものより高く、またコンテンツの生成速度も非常に速いという特徴があります。従来のチャットボットは主にオペレータ業務のサポートなど、お問い合わせ対応に限定されていましたが、生成AIでは以下のような活用ができることが期待されています。

生成AIの活用事例

文章生成

商品やサービスの広告文を作成する際に、商品の特徴やターゲット顧客の特性などを入力するだけで、瞬時に文章を生成することができます。

レポート作成

大量のデータを分析し、要約やレポートを自動的に生成することができます。これにより、データの処理時間を短縮し、意思決定に役立つ情報を迅速に提供することができます。

製品開発と設計

顧客ニーズや市場のトレンド、予算、顧客の意見などの情報を分析させることにより、新製品やサービスのアイデアを効率的に提案することが期待されています。

4-3-1. サイバーセキュリティ対策の重要性

デジタルトランスフォーメーションを推進していく際に、並行してサイバーセキュリティの確保に取組むことが重要です。変化の激しい現代社会でビジネスを継続していくためには、従来のITを活用して業務効率化や生産を向上させることだけでなく、データやデジタル技術を活用して、顧客視点で新たな価値を創出する、デジタルトランスフォーメーションを推進していくことが求められています。しかし、データやデジタル技術を活用する際に、サイバーセキュリティ対策を行わなければ、サイバー攻撃の標的となり、経営を揺るがすような被害を被ってしまう可能性があります。このような被害を受けないためにも、デジタルトランスフォーメーションの推進と並行してサイバーセキュリティの確保に取組むことが重要です。

サイバーセキュリティ対策を行うことで、リスクを経営上許容可能な範囲までに減少させることができます。また、サイバーセキュリティ対策には経営判断が必要になるため、経営者が主体となって指揮をすることが大切になります。

次のページから、経営者目線でサイバーセキュリティ対策を行わなければならない理由を以下のポイントごとに説明していきます。

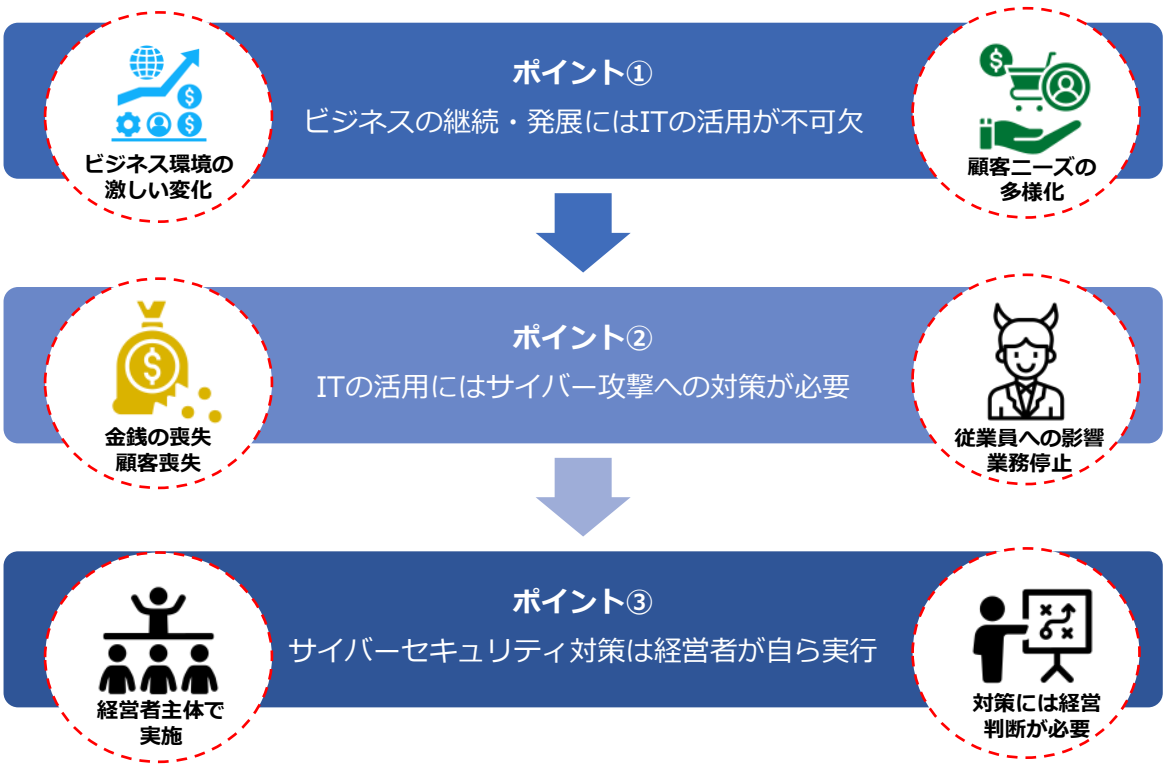


図24. ITの活用とサイバーセキュリティ対策の関係性
（出典） 東京都産業労働局.” MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響”.
https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/201/index.html,(参照 2023-07-10).

4-3-2. 経営者が重要視すべき3つのポイント

ポイント1：ビジネスの継続・発展にはITの活用が不可欠

中小企業にとって、業務や生産の効率化、人材確保は重要な課題です。業務・生産工程などの運用コストの削減・効率化のために、ITの活用が不可欠になっています。また近年では、競争力維持・強化のために、デジタルトランスフォーメーション（DX）を進めることが求められており、ITの活用が必須になっています。

中小企業の課題

ポイント2：ITの活用にはサイバー攻撃への対策が必要

ITの活用が不可欠な中、サイバーセキュリティ対策を行うことが必須となっています。サイバーセキュリティ対策を怠ることで、金銭・顧客の喪失、法的責任、事業の中断・停止、従業員への悪影響など、経営を揺るがすような被害を引き起こす可能性があります。近年は、サプライチェーンを介して、セキュリティ対策が不十分な企業を踏み台にして攻撃されることもあります。攻撃を受けた企業だけが責任を追及されるだけでなく、踏み台にされた企業も加害者として責任を追及されてしまいます。

事例：サプライチェーン攻撃による情報流出被害
某生命保険会社（2社）

某生命保険会社の2社は、顧客情報の一部が流出したことを公表し、謝罪しました。情報流出の原因としては、外部委託先の企業のサーバが不正アクセスを受けたことです。
A社は、氏名、年齢、性別、証券番号、保険種類番号、保障額、保険料などの情報が、1,323,468人分も漏えいしました。
B社では、氏名、性別、生年月日、メールアドレス、証券番号、顧客ID、車名、自動車保険契約にかかる事項が、最大で698,767人分漏えいしました。クレジットカード番号、銀行口座番号は含まれていないとのことでしたが、全員に対してお詫びとしてクオカード500円分を送付しました。これだけでも3億円以上の損害が発生したことになります。また、多くのお客様に対する信頼を低下させてしまったことも経営上重大な問題です。

4-3-2. 経営者が重要視すべき3つのポイント

ポイント3：サイバーセキュリティ対策は経営者が自ら実行

経営者は自ら主体となって指揮をとり、サイバーセキュリティ対策を行う必要があります。理由は、主に2つあります。1つ目は、セキュリティ対策を行うにあたり、サイバー攻撃のリスクの許容範囲をどの程度にするのか、セキュリティ投資をどこまで行うのかなど、経営者による経営判断が必要になるからです。2つ目は、セキュリティインシデントが発生した際に、経営者が「法的責任」や「社会的責任」を負わなければならないからです。経営者は民法や会社法により、善管注意義務という「取締役として期待される水準の注意をもって業務を行う義務」を負い、その任務を怠った際に生じた損害を株式会社に対して賠償する責任「任務懈怠」を負うことが規定されています。そのため、サイバーセキュリティ対策にベストを尽くさなかった結果、サイバー攻撃による情報漏えいや事業停止が起き、第三者に損害が生じた場合、善管注意義務違反や任務懈怠に基づく損害賠償責任を問われてしまいます。

法令	条項	要約
民法	415条 債務不履行による損害賠償責任	サイバー攻撃により仕事が停滞した場合、会社および第三者に対する、契約違反による賠償義務を負う。
	644条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して、善管注意義務違反による賠償義務を負う。
会社法	330条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対する、善管注意義務違反による任務懈怠（けたい）に基づく損害賠償義務を負う。
	423条 1項 任務懈怠による損害賠償責任	
	429条 1項 第三者に対する注意義務違反	

図25. 情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律
（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」から抜粋

会社法の第三者責任や民法の不法行為責任が認められると、経営者が個人として損害賠償責任を負う場合もあります。この他にも、法律によっては違反などが発生した場合、経営者だけでなく、取締役、担当者に対しても刑罰が科せられることもあります。上記の事態を引き起こさないためにも、サイバーセキュリティ対策は経営者が主体となって取組むことが大切です。

編集後記

セミナー2日目では、現代社会の急速な変化の中で企業経営に必要とされるIT活用の重要性と経営者主体のサイバーセキュリティ対策について解説しました。

最初に、社会の動向について説明しました。社会の動向から現実社会とサイバー空間の繋がりとIT活用における課題を説明しました。次に、企業がセキュリティ対策と同時に行う必要があるIT活用について説明しました。ここでは、従来の業務効率化やコスト削減などの守りのIT投資と、近年特に重要性が増しているデジタルトランスフォーメーションに向けた攻めのIT投資の特徴や違い、実施手順についてそれぞれ説明しました。さらに、デジタルトランスフォーメーションの推進において注目されている主要なデジタル技術の選び方や活用方法についても紹介しました。最後に経営者が主体となってサイバーセキュリティ対策を行う必要がある理由から、サイバーセキュリティ対策の重要なポイントを説明しました。

第二回のテキストを通じて、企業経営には守りのIT投資（社内業務の効率性や生産性向上、働き方の変革など）、攻めのIT投資（ビジネスの発展や売上・企業価値の向上など）、さらにサイバーセキュリティ対策の投資が必要であることを解説してきました。次回以降は、国の政策や戦略と合わせてIT活用とサイバーセキュリティ対策について詳しく解説していきます。

引用文献

サイバー・フィジカル・セキュリティ対策フレームワークVer.1.0

https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf

DX白書2023

https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf

【本編07】中小企業が組織として実施すべきサイバーセキュリティ対策【実施手順・実務者マニュアルレベル】＜セキュリティ関連知識の保管庫（ナレッジベース2023）＞

https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/464/index.html

MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響

https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/201/index.html

サイバーセキュリティ経営ガイドライン Ver3.0

https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～

https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/pdf/20180907_03.pdf

攻めのIT活用指針

https://www.smrj.go.jp/doc/tool/guide4youshiki_1.pdf

中堅・中小企業等向け『デジタルガバナンス・コード』実践の手引き

https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf

「DX Selection 2022」選定企業レポート

https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dx-selection2022-2.pdf

「DX Selection 2023」選定企業レポート

https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf

参考文献

中堅・中小企業等向け『デジタルガバナンス・コード』実践の手引き
https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf

用語集

■AI
Artificial Intelligenceの略。「AI（人工知能）」という言葉は、1956年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。1950年代後半から1960年代が第一次AIブーム、1980年代が第二次AIブーム、現在は2000年代から始まる第三次AIブームである。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている
…… 1-1-1、4-1-1、4-2-2、4-2-5

■BCP
Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画
…… 2-3-2

■CSIRT（シーサート）
Computer Security Incident Response Teamの略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う
…… 2-1-3

■DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attackの略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることで、過剰な負荷をかけてサービスを利用できなくする攻撃手法
…… 2-2-2、2-2-5、第一回コラム

■EDR
Endpoint Detection and Responseの略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する
…… 2-2-4、2-2-5、3-1-1、3-4-1

■Fortinet
セキュリティ製品の開発、製造を行う米国のメーカー。ファイアウォールやセキュリティソフトを提供している
…… 2-3-2

■ICSCoE中核人材育成プログラム
2017年4月にIPA内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている
…… 2-1-2

■ICT
Information and Communication Technologyの略。IT（情報技術）だけでなく、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる
…… 4-1-2

■IoT（アイ・オー・ティー）
Internet of Thingsの略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやりとりしたりする概念や仕組み、技術のこと
…… 1-1-1、2-1-2、2-2-2、4-1-1、4-2-5

■IPS
Intrusion Prevention Systemの略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。IPSは、異常を検知した場合、管理者に通知するだけではなく、その通信を遮断する
…… 2-2-2、3-4-2

用語集

■IPアドレス
コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意の数字の組み合わせのこと。 IPアドレスは、127.0.0.1のように0～255までの数字を4つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれらの4つの数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電等で大量にIPアドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6では、アドレス空間の増加だけでなく、情報セキュリティ機能の追加などの改良も加えられている
…… 2-3-1

■ISMS
Information Security Management Systemの略称。ISMSは情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的な対策を含む、経営者を頂点とした総合的で組織的な取組み。組織がISMSを構築するための要求事項をまとめた国際規格がISO/IEC 27001（国内規格はJIS Q 27001）であり、審査機関の審査に合格すると「ISMS認証」を取得できる
…… 3-3-1

■ITリテラシー
コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能
…… 3-1-1

■LockBit2.0
「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される
…… 2-3-2

■NIST サイバーセキュリティフレームワーク（CSF）
米国政府機関の重要インフラの運用者を対象として誕生し、防御にとどまらず、検知・対応・復旧といったステップも含み、インシデント対応を含めており、日本においても、今後普及が見込まれる
…… 3-3-1

■RPA
Robotic Process Automationの略。定型的な業務をソフトウェアのロボットにより自動化すること
…… 4-2-3

■SASE（サシー）
Secure Access Service Edgeの略。ガートナー社が2019年に提唱したゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウド上で統合して提供するサービス、また、その考え方・概念
…… 2-2-4

■SDP
Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、全ての通信をチェックおよび認証する。VPNは、ネットワーク接続前に一度だけ認証を行うのに対し、SDPは、ユーザの情報（デバイス、場所、OSなど）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う
…… 2-2-5

■SECURITY ACTION
中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度
…… 2-1-2、3-2-1

■Society 5.0
サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）
…… 1-1-1

■SWG
Secure Web Gatewayの略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することでセキュアな通信環境を実現
…… 2-2-4

■UTM
複数のセキュリティ対策機能を１つに集約した製品のこと。ウイルスや不正アクセスなど外部からの脅威から、内部のネットワークを包括的に保護することができる
…… 3-1-1

用語集

■VPN
Virtual Private Networkの略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぐ。このようにVPNを使用することで、ユーザは物理的な専用線で通信しているかのような安全な通信を行うことができる
…… 2-1-3、2-2-2、2-2-5、2-3-1、2-3-2、2-3-3

■WAF（ワフ）
Web Application Firewallの略。 従来のファイアウォールが、IPアドレスとポート番号で通信を制御していたことに対して、Webアプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと
…… 2-2-2

■アクセス制御
特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザを制限する機能のこと
…… 2-2-5、第一回コラム

■アセスメント
システムや運用環境等を客観的に調査・評価すること。現在の利用状況を把握することで、システムの再構築や運用改善の参考情報となる
…… 2-2-4

■暗号化
データの内容を変換し、第三者には、内容を見ても解読できないようにすること
…… 2-1-3、2-2-1、2-2-5、2-3-2、3-2-3、3-3-1、第一回コラム

■アンダーグラウンドサービス
合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス
…… 2-1-3

■インターネットバンキング
インターネットを利用した銀行や金融機関との取引を行うサービスのこと。銀行の窓口やATMに出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振込や残高照会などの取引を行うことができる
…… 3-2-2

■ウイルス定義ファイル（パターンファイル）
セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの
…… 3-2-2、3-2-3

■エンドポイントデバイス
ネットワークに接続して、ネットワークを介して情報を交換するデバイス（デスクトップコンピュータ、仮想マシン、サーバなど）
…… 2-2-4

■改ざん
文書や記録などの全てまたは一部に対して、無断で修正・変更を加えること。IT分野においては、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為
…… 2-1-2

■可用性
許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性
…… 第一回コラム

■完全性
参照する情報が改ざんされていなく、正確である特性
…… 第一回コラム

■機密性
許可された者だけが情報や情報資産にアクセスできる特性
…… 第一回コラム

用語集

■クラッキング
悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為を行うこと
…… 第一回コラム

■個人情報保護委員会
個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱を確保することを任務とする、独立した機関のこと。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱に関する監視・監督、認定個人情報保護団体に関する事務などの業務を行う行政機関（組織的には内閣府の外局）
…… 2-2-3

■サイバー攻撃
インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまで様々である。ネット社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人等を攻撃する行為やその防御をサイバー戦争と呼ぶこともある。
…… 2-1-2、2-1-3、2-2-2、2-2-5、2-3-2、3-3-1、4-1-1、4-3-1、4-3-2

■サイバーセキュリティお助け隊サービス制度
中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービス
…… 2-1-2

■サイバーセキュリティ戦略
組織や企業がセキュリティに関する目標を達成するための計画やアプローチ
…… 3-3-1

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク
…… 3-3-1

■サプライチェーン
製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される
…… 2-1-3、2-2-2、2-2-4、4-1-1、4-2-4、4-3-2

■情報資産
営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報
…… 3-3-1

■情報セキュリティの3要素「CIA」
情報セキュリティの3つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ
…… 第一回コラム

■真正性
情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある
…… 2-1-3、第一回コラム

■信頼性
システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性
…… 第一回コラム

■スクリーンロック
デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない
…… 2-2-2

■脆弱性
情報システム（ハードウェア、ソフトウェア、ネットワーク等を含む）におけるセキュリティ上の欠陥のこと
…… 2-1-1、2-1-3、2-2-1、2-2-2、2-2-4、2-2-5、2-3-1、2-3-2、2-3-3、3-3-1、第一回コラム

用語集

■脆弱性診断
システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること
…… 2-3-1

■責任追跡性
情報資産に対する参照や変更等の操作を、どのユーザが行ったものかを確認することができる特性
…… 第一回コラム

■セキュリティインシデント
セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらに繋がる可能性のある事象等がインシデントに該当
…… 2-1-1、2-1-2、2-1-3、2-2-1、4-1-1、5-1-1、5-1-2

■セキュリティ・キャンプ
情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した22歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している
…… 2-1-2

■セキュリティホール
情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある
…… 3-3-1

■セキュリティポリシー
企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的
…… 2-1-1、2-2-1、3-3-1

■ゼロデイ攻撃
OSやソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと
…… 2-1-3

■ゼロトラスト
従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、全てのネットワーク通信を信用できない領域として扱い、全ての通信を検知し認証するという新しいセキュリティの考え方
…… 2-2-4、4-1-3

■ソリューション
問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」
…… 2-2-5

■ダークウェブ
特別な手法でないとアクセスできない、匿名性の高い非公開のWebサイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている
…… 2-1-3

■多要素認証
多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年ではFIDO2と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている
…… 2-2-5、2-3-3

■データサイエンス
数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること
…… 1-1-1

用語集

■デジタル化
紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネス・プロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードをCD（コンパクトディスク）にするのがデジタイゼーション、音楽をダウンロード販売するのがデジタライゼーションである
…… 1-1-1、2-1-1、2-2-1、3-3-1、4-1-2、4-2-3

■デジタル情報
0、1、2のような離散的に（数値として）変化する量
…… 第一回コラム

■内部監査
内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO27001の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する
…… 3-3-1

■ビジネスメール詐欺
攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Email Compromiseとも略される
…… 2-1-3

■ビッグデータ
全体を把握することが困難な程、膨大な規模のデータ群
…… 1-1-1

■否認防止性
システムに対する操作・通信のログを取得したり、本人に認証させることにより行動を否認させないようにする特性
…… 第一回コラム

■標的型攻撃
機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルス付きメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている
…… 2-1-2、2-1-3

■標的型メール攻撃
特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある
…… 2-2-4

■ファイアウォール
本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンのOSに付随しているもの、セキュリティソフトに付いているもの、専用のハードウェアになっているものなど形態は様々である
…… 2-3-1、3-4-1、3-4-2

■不正アクセス
利用権限を持たない悪意のあるユーザが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、2000年2月に施行された不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）により、法律で固く禁じられている
…… 2-1-1、2-1-2、2-1-3、2-2-1、2-2-2、2-2-3、2-2-5、2-3-1、4-3-2

■踏み台
不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ
…… 2-1-3、4-3-2

用語集

■フォレンジック
犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組みを指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる
…… 2-2-3、2-3-2

■ブラックマーケット
広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するネット上の市場（闇市）
…… 2-1-3

■フレームワーク
フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃など様々なセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな形」としてまとめたもの
…… 2-2-4、3-3-1

■ブロックチェーン
複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する仕組み
…… 1-1-1

■ベストプラクティス
何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論
…… 2-1-3、2-3-1

■マルウェア
パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる
…… 2-2-2、2-2-4、2-2-5、第一回コラム

■無線LAN
LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線LANを通じて、コンピュータはインターネットにアクセスすることができる
…… 3-2-3

■ランサムウェア
悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する
…… 2-1-2、2-1-3、2-2-1、2-2-2、2-2-5、2-3-2、2-3-3

■リスクアセスメント
企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外については何らかの対策を講じる必要がある
…… 3-3-1

■リスク評価
組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス
…… 2-3-2、3-3-1

■リモートデスクトップ接続
パソコン、タブレット、スマートフォン等のデバイスを使用して、遠隔地から特定のパソコンに接続する方法
…… 2-2-2

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業