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

サイバーセキュリティに関する国の方針・施策
およびサイバー脅威の動向

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5章. デジタル社会の方向性と実現に向けた国の方針

5-1. 国の基本方針および実施計画の要約

5-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

章の目的

第5章では、政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について学ぶことを目的とします。

主な達成目標

- 国の基本方針にデジタルがどのように影響を与えており、それによりどのような社会を目指しているかを理解すること
- デジタル社会におけるサイバーセキュリティ対策の重要性を理解すること

5-1-1. 経済財政運営と改革の基本方針2023

国の方針の一つである「経済財政運営と改革の基本方針」は、政府の経済財政政策に関する基本的な方針を示すとともに、経済、財政、行政、社会などの分野における改革の重要性とその方向性を示すものです。この方針は通称「骨太の方針」と言われています。

各省庁の利害を超えて官邸主導で改革を進めるため、内閣総理大臣が議長を務める経済財政諮問会議において毎年策定します。

IT及びセキュリティ関連の施策についてもこの基本方針に沿った形で実施計画が策定されています。2023年の骨太の方針では、本文中だけで50回以上「デジタル」という言葉が使われており、デジタル技術の活用やデジタル社会の構築に向けた変革が重要な課題になっていることがわかります。

ここでは、2023年に策定された基本方針の中から、「新しい資本主義の加速」を構成する「投資の拡大と経済社会改革の実行」に掲げられているいくつかの施策において、特にIT戦略に関係する内容について説明します。

投資の拡大と経済社会改革の実行（2023年度方針）

①官民連携による国内投資拡大と**サプライチェーンの強靭化**
②GX、**DXなどの加速**
③スタートアップの推進と新たな産業構造への転換、インパクト投資の促進
④官民連携を通じた科学技術・イノベーションの推進
⑤インバウンド戦略の展開

IT戦略に関係する施策例

サプライチェーンの強靭化

国際環境の不確実性が増す中にあって、海外からヒト、モノ、カネ、アイデアを積極的に呼び込むことで、国内全体の投資を拡大させ、イノベーション力を高めることを目指します。特に、次世代半導体を含めたグローバルサプライチェーンの中核となることを目指し、政府を挙げて投資拡大に取組んでいきます。 ITは、サプライチェーンを支える重要な役割になると同時に、セキュリティリスクへの対策も併せて重要です。

DXの加速

新型コロナウイルス感染症が拡大したことによって、日本国内において様々な課題が浮き彫りとなりました。デジタル化やオンライン化の遅れもその一つであり、2020年度の「経済財政運営と改革の基本方針」以降、DX（デジタルトランスフォーメーション）の推進が謳われるようになりました。2023年度の方針においても同様に、DXの加速が謳われています。

DXへの対応については、デジタルの力を活用して国が地方を支える事を目指しての行政サービスの見直しや、マイナンバーカードの制度における安全・信頼確保および利便性・機能向上への取組みなどが掲げられています。また、中堅・中小企業の活力を向上させるため、DX、人手不足などの事業環境変化への対応を後押しすることが明記されています。

また、「サイバーセキュリティ戦略」に基づく取組みを進める旨が記載されており、日本のDX方針にサイバーセキュリティの観点が組み込まれている事が確認できます。中堅・中小企業に対して、インボイス制度の円滑な導入、サイバーセキュリティ対策を支援することが謳われています。サイバーセキュリティ戦略の詳細については後述します。

（出典）内閣府「経済財政運営と改革の基本方針 2023」を基に作成

5-2-1. デジタル社会の実現に向けた重点計画

政府は経済財政運営と改革の基本方針で掲げているデジタル社会の実現を目指すにあたって、「デジタル社会の実現に向けた重点計画」を閣議決定しています。
日本が目指すデジタル社会について、「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」と定義し、以下の6つの姿を挙げています。[12]

デジタル社会で目指す6つの姿
1. デジタル化による成長戦略 国・地方公共団体や民間との連携の在り方を含めたアーキテクチャの設計やクラウドサービスの徹底活用、デジタル原則を含む規制改革の徹底、調達改革の推進、データ戦略の推進、データ連携やDXの推進、AIの適切かつ効果的な活用などにより、我が国全体のデジタル競争力が底上げされ、成長していく持続可能な社会を目指す。
2. 医療・教育・防災・こどもなどの準公共分野のデジタル化 必要なデータの連携などを通じて、国民一人ひとりのニーズやライフスタイルに合ったサービスが提供される豊かな社会、継続的に力強く成長する社会を目指す。
3. デジタル化による地域の活性化 地方の共通基盤を国が支援することなどにより、地域からデジタル改革、デジタル実装を推進、デジタル田園都市国家構想の実現、地域で魅力ある多様な就業機会の創出などを図り、地域の課題が解決され、各地域で培われてきた地域の魅力が向上する社会を目指す。
4. 誰一人取り残されないデジタル社会 地理的な制約、年齢、性別、障害や疾病の有無、国籍、経済的な状況などにかかわらず、誰もが（デジタルに不慣れな方にも・デジタルを利用する方にも）日常的にデジタル化の恩恵を享受でき、様々な課題を解決し、豊かさを真に実感できる「誰一人取り残されない」デジタル社会を目指す。
5. デジタル人材の育成・確保 全国民が当事者であるとの認識に立ち、ライフステージに応じた必要なICTスキルを継続的に学ぶことで、デジタル人材の底上げと専門性の向上を図り、デジタル人材が育成・確保される社会を目指す。
6. DFFT（Data Free Flow with Trust）：「信頼性のある自由なデータ流通」の推進を始めとする国際戦略 国際連携を図ることで、データがもたらす価値を最大限引き出し、国境を越えた自由なデータ流通が可能な社会を目指す。

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

[12]:デジタル庁.”デジタル社会の実現に向けた重点計画”.https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf, （2023-07-28）.

5-2-1. デジタル社会の実現に向けた重点計画

デジタル社会の実現に向けた戦略・施策

日本がデジタル社会を実現していくための政府の取組みについて、7つの戦略的な政策が掲げられています。 7つの戦略的な政策の中では、サイバーセキュリティに関する取組みも盛り込まれています。サイバーセキュリティの施策が重要視されていることを理解するため、該当の項目について説明していきます。

目指す姿を実現する上で有効な戦略的取組（基本戦略）

① デジタル社会の実現に向けた構造改革
② デジタル田園都市国家構想の実現
③ 国際戦略の推進
④ **サイバーセキュリティなどの安全・安心の確保**
⑤ 急速なAIの進歩・普及を踏まえた対応
⑥ 包括的データ戦略の推進と今後の取組
⑦ Web3.0の推進

サイバーセキュリティなどの安全・安心の確保

国家安全保障上の課題へと発展していく可能性のある国際情勢の変化、感染症の蔓延、自然災害などへの対応として、国民の生命・財産を守り、国民生活を維持することのできる安全・安心なデジタル社会の構築に取組みます。

1. サイバーセキュリティの確保

・ 2023年度（令和5年度）に、政府情報システムにおけるクラウドサービスの利用拡大などを見据え、政府統一基準を改定。
・デジタル庁はNISCと連携し、デジタル庁整備・運用システムなどの情報システム整備方針の実装を推進。
・安全保障などの機微な情報などに係る政府情報システムの取扱いを参照した利用促進。

2. 個人情報などの適正な取扱いの確保

・改正後の個人情報保護法を踏まえ、個人情報などの適正な取扱いの確保、個人情報保護委員会の体制強化。

3. 情報通信技術を用いた犯罪の防止

・不正アクセスの防止などに向けた官民連携。
・国際連携、サイバー事案の警察への通報促進などの取組を実施。

4. 高度情報通信ネットワークの災害対策

・ネットワークの冗長性の確保・電気通信事故の検証、災害発生時における移動電源車などの派遣などを推進。

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

5-2-1. デジタル社会の実現に向けた重点計画

各分野における基本的な施策

デジタル社会の実現に向け、6つの分野に分けて、基本的な施策が掲げられています。6つの分野における産業のデジタル化には、中小企業を対象とした施策が盛り込まれているため、その分野に焦点を当てて説明していきます。

各分野における基本的な施策

① 国民に対する行政サービスのデジタル化
② 安全・安心で便利な暮らしのデジタル化
③ アクセシビリティの確保
④ 産業のデジタル化
⑤ デジタル社会を支えるシステム・技術
⑥ デジタル社会のライフスタイル・人材

産業のデジタル化

行政サービスのデジタル化を通じて事業者にとって利用しやすい環境を整備し、支援を必要とする事業者に迅速に支援が届く環境の実現を目指します。

1. デジタルによる新たな産業の創出・育成

クラウドサービス産業の育成 / ITスタートアップなどの育成

2. 事業者向け行政サービスの質の向上に向けた取組

・電子署名、電子委任状、商業登記電子証明書の普及
・法人共通認証基盤（GビズID）の普及
・事業者に対するオンライン行政サービスの充実
・レベルに応じた認証の推進
・eKYC（electronic Know Your Customer）などを用いた民間取引などにおける本人確認手法の普及促進

3. 中小企業のデジタル化の支援

・中小企業の事業環境デジタル化サポート
・中小企業のサイバーセキュリティ対策の支援

4. 産業全体のデジタルトランスフォーメーション

・市場評価を通じたDXの推進、産業におけるサイバーセキュリティの強化、データの利活用や規制改革などを通じた産業のDX

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

5-2-1. デジタル社会の実現に向けた重点計画

以下では、前述の産業のデジタル化のうち、中小企業を対象とした施策が盛り込まれている「事業者向け行政サービスの質の向上に向けた取組」と「中小企業のデジタル化の支援」について説明します。

事業者向け行政サービスの質の向上に向けた取組

電子署名、電子委任状、商業登記電子証明書の普及
電子署名、電子委任状、商業登記電子証明書について、事業者による活用の機会が増加し、多様化していることから、普及を更に強力に推進する。
法人共通認証基盤（GビズID）の普及
法人が様々なサービスにログインできる認証サービスを実現する「GビズID」について、2023年度中にマイナンバーカードを利用した審査の効率化、連携行政サービスの拡充などを進める。
事業者に対するオンライン行政サービスの充実
ア：e-Gov の利用促進 安定運用を確保しつつ、クラウドサービス利用による柔軟なリソース活用に向けて、ガバメントクラウドへの移行の整備を2023年度中に行うことを目指す。 **イ：J グランツの利便性向上と利用補助金の拡大** 申請簡素化や事務局の審査プロセス迅速化の観点から、2024年度（令和６年度）を目途に、システムアーキテクチャ及びUIの刷新を行い、申請時の事業者・事務局双方の負担軽減を図る。 **ウ：中小企業支援のDX推進** 事業者の申請などデータを一元化し官民で利活用するためのデータ基盤（ミラサポコネクト）を通じて、自社の経営特性に合った多様な支援がリコメンドされる環境を実現する。 最適な支援策や支援者・民間サービスなどについて情報交換できるコミュニティサイトの構築を目指す。
レベルに応じた認証の推進
ア：民間事業者への周知・相談支援の強化 マイナンバーカードの普及などに伴い、利用のインセンティブが大きく高まる民間事業者への周知・相談支援を強化する。 **イ：利用要件・利用手続などの改善** 民間事業者の視点に立ち、利用要件・利用手続などの継続的な改善を実施する。
eKYCなどを用いた民間取引などにおける本人確認手法の普及促進
デジタル空間での安全・安心な民間の取引などにおいて必要となる本人確認について、公的個人認証サービス（JPKI）の利用を促進する。その上で、安全性や信頼性などに配慮しつつ、具体的な課題と方向性を整理し、簡便な手法の一つである eKYCなどを用いた本人確認手法の普及を進める。

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

5-2-1. デジタル社会の実現に向けた重点計画

中小企業のデジタル化の支援

中小企業の事業環境デジタル化サポート
・デジタル化支援ポータルサイト「みらデジ」の設置 ・IT専門家との相談を受けられる体制の整備 ・IT導入補助金 ・取引全体のデジタル化 ・会計・経理全体のデジタル化 ・クラウドサービス利用やハードウェア調達の支援 ・業務効率化やDXに向けたITツール導入の支援
中小企業のサイバーセキュリティ対策の支援
・「サイバーセキュリティお助け隊サービス」の普及促進 ・相談体制の強化 ・情報集約・共有促進機能の強化

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

5-2-2. Society5.0

Society5.0は、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）です。狩猟社会（Society1.0）、農耕社会（Society2.0）、工業社会（Society3.0）、情報社会（Society4.0）に続く、新たな社会を指すもので、第5期科学技術基本計画において我が国が目指すべき未来社会の姿として初めて提唱されました。

Society5.0では、IoT（Internet of Things）で全ての人とモノがつながり、様々な知識や情報を共有することによって、これまでにない新たな価値を生み出すとともに、社会が抱える課題を解決し、困難を克服できます。また、人工知能（AI）、ロボット、自動走行車などの利用によって、少子高齢化、地方の過疎化、貧富の格差などの課題も解決できるでしょう。こうした社会の変革（イノベーション）が進むことによって、希望の持てる社会、世代を超えて互いに尊重し合う社会、一人ひとりが快適で活躍できる社会が生まれることが期待されます。

これまでの情報社会（Society4.0）では、人がサイバー空間にあるクラウドサービスにアクセスすることで、情報やデータを入手し、分析を行ってきました。Society5.0では、フィジカル空間のセンサーから膨大な情報がサイバー空間に集積されます。サイバー空間では、この集積されたデータ（ビッグデータ）を人工知能（AI）が解析し、その結果をフィジカル空間の人間に様々な形で、フィードバックしていきます。今までの情報社会では、人間が情報を解析することで、価値が生まれましたが、Society5.0では、AIが解析した膨大なビッグデータの結果がロボットなどを通して、人間にフィードバックされることで、これまでに実現しなかった新たな価値が産業や社会にもたらされます。[13]

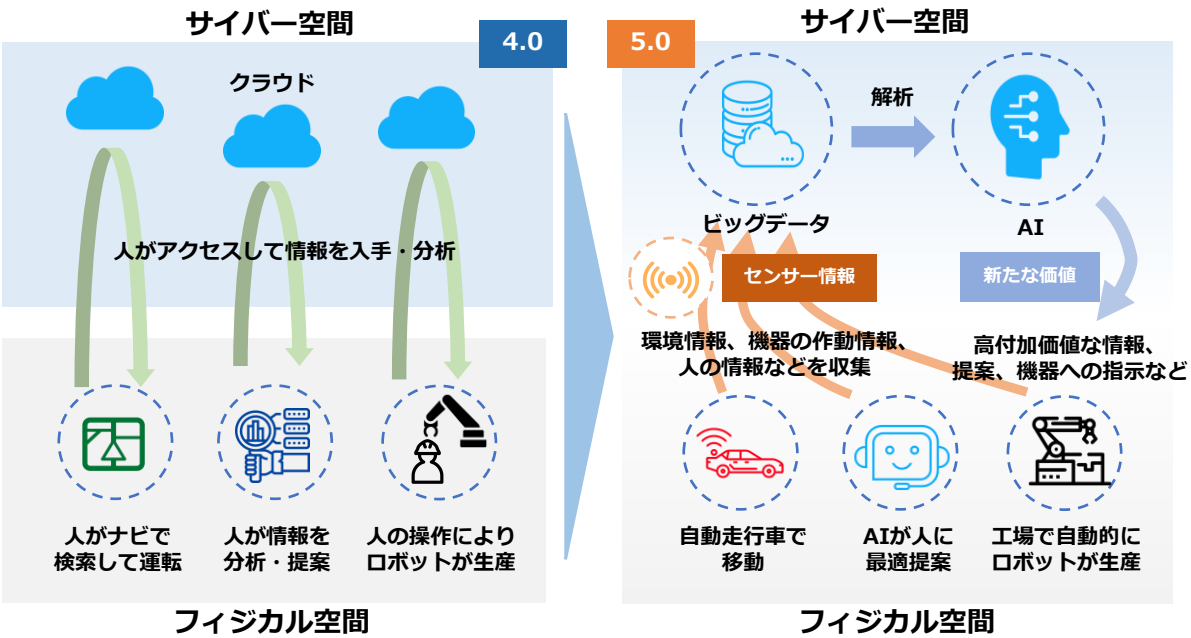


図26. Society4.0とSociety5.0の比較
（出典）内閣府.“Society5.0”.https://www8.cao.go.jp/cstp/society5_0,（2023-08-03）.

[13]:内閣府.“Society5.0”.https://www8.cao.go.jp/cstp/society5_0,（2023-08-03）.

5-2-2. Society5.0

社会の変化に対するセキュリティ上の脅威

Society5.0におけるサイバー空間の急激な拡大は、サイバー攻撃の対象が増えることを示しています。サイバー空間とフィジカル空間の相互作用により、サイバー攻撃がフィジカル空間にも影響を及ぼす可能性が高まります。例えば、医療機器やインフラシステムなどがサイバー攻撃によって操作されたり、停止したりすると、人命や社会生活に重大な影響を及ぼす恐れがあります。

Society 5.0では、多様な人々がサービスの効果を享受できる包摂的な社会を目指していますが、そのためにはサービスの利用可能性や継続性を確保する必要があります。しかし、サイバー攻撃によってサービスが利用できなくなったり、中断されたりすると、包摂的な社会の実現に支障をきたす可能性があります。また、IoTデバイスやセンサーが収集したデータをサイバー空間で改ざんし、偽情報を拡散するといったフィジカル空間とサイバー空間の情報転送への脅威も考えられます。さらに、IoTやAIなどの技術を活用することで、大量のデータが生成されますが、そのデータは個人情報や企業情報などの重要な情報を含む場合が多く、その漏えいや改ざんによってプライバシーや知的財産権などが侵害される危険性が高まります。

また、Society5.0においては、IoTから得られる大量データの受け渡しなど、サイバー空間とフィジカル空間の融合によって新たな処理が発生します。その新たな処理がサイバー攻撃の対象となる可能性を認識すべきです。Society5.0においては、サプライチェーンも変化します。サイバー空間とフィジカル空間が融合されることで、サプライチェーンを構成する企業同士の関係が複雑に繋がります。その結果、サイバー攻撃の影響範囲がこれまで以上に拡大することが予測されます。

Society5.0における 社会の変化	社会の変化に対する セキュリティ上の脅威
大量データの 流通・連携	・データの性質に応じた適切な管理の重要性が増大
フィジカル空間と サイバー空間の融合	・サイバー空間からの攻撃がフィジカル空間まで到達 ・フィジカル空間から侵入してサイバー空間へ攻撃を仕掛けるケース ・フィジカル空間とサイバー空間の間における情報の転換作業への介入
複雑に繋がる サプライチェーン	・サイバー攻撃による影響範囲が拡大

（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Ver1.0」を基に作成

Society5.0の進展に伴い、サイバーセキュリティ対策の重要性が増し、組織や個人がより綿密な対策を講じる必要があります。また、サプライチェーン全体でサイバーセキュリティ対策を実施し、企業間で意識を共有することも重要です。

5-2-3. DXの推進

デジタルトランスフォーメーション（DX）の推進における中小企業の優位性について説明します。デジタルトランスフォーメーションとは、デジタル技術やツールを導入すること自体ではなく、データやデジタル技術を使って、顧客目線で新たな価値を創出していくことです。中小企業の中には、デジタルトランスフォーメーションを推進し、売上高を5倍、利益を50倍に増加させた企業が存在します。中小企業ならではの優位性を理解し、積極的にデジタルトランスフォーメーションに取組むことで、大きく成長できる可能性があります。以下では、デジタルトランスフォーメーションを推進する際に、中小企業の優位な点を説明します。そして、優位性を利用してビジネスモデルや企業文化などの変革に取組んでいる企業の事例を紹介します。

中小企業がデジタルトランスフォーメーション推進における優位な点

参考情報が豊富

DXを既に手掛けている中小企業や、デジタルトランスフォーメーションを順調に進めている企業のやり方を参考にすることができる

環境が整備されている

先行者や大企業などにより既に整備されたプラットフォームを利用し、新たなビジネスに取組むことができる

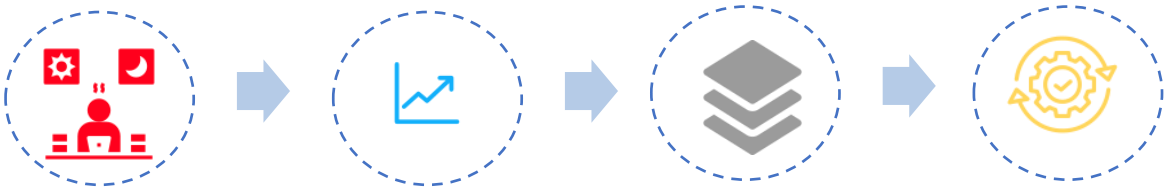
環境の変化に素早く対応しやすい

経営者が即断即決し、新しい取組みに臨みやすい利点がある。そのため、変革のスピードにおいて優位性を持つことができる

事例（企業文化の改革）：精密機械部品加工

産学官連携で開発された中小企業向けの共通業務システムプラットフォームを導入し、長年の業務を支えた基幹システムを刷新しました。その結果、無駄な業務や無理な計画などが判明しただけでなく、各部署のデータが繋がるようになりました。これにより、各部署がそれぞれ自部署のことのみを考えていた状態から、他部署に正しいデータを流さなければならないという意識が生まれました。全社で「正しいデータ」を集める意識を持つ企業文化への変革に効果が出始めました。

（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



皆が懸命に働いているが収益が上がらず、賃金を上げられない

従業員の可処分所得３％向上を目指す。そのために生産性を130%に高めることを目指す

産学官連携で開発された中小企業向けシステムプラットフォームを導入

基幹システムが刷新され、業務・組織の変革に効果が出始める

5-2-3. DXの推進

データ活用の流れ

顧客視点で新たな価値を創造するためには、製品やサービス、業務の変革が必要です。また、デジタル技術（IoT、ビッグデータ、ロボット、AIなど）を用いてデータを活用していくことが大切です。ここでは、デジタル技術を用いてデータを活用し、製品やサービス、業務を変革していく流れを具体的な事例と合わせて説明します。

以下は、データを活用し、業務を改革していくための手順となります。

手順	概要
1.データの収集	IoTやセンサー、カメラなどの機器を用いて情報を収集します。
2.データの蓄積	収集した膨大なデータ（ビッグデータ）を集積します。
3.データの解析	AIを用いてデータを解析します。
4.解析結果の反映	解析の結果をもとに改革を進めます。

事例（業務改革）：製造メーカー

製造現場の加工機にセンサーを設置して、機械の動作を非常に細かい間隔でデータ収集・可視化出来る製品を開発しました。また、取得したデータを専門技術者が遠隔で確認し、動作不良の原因調査や製品の適切な使用方法の指導を実施したり、AIによるデータ解析によって使いやすい製品の設計・開発にいかすことが可能となりました。

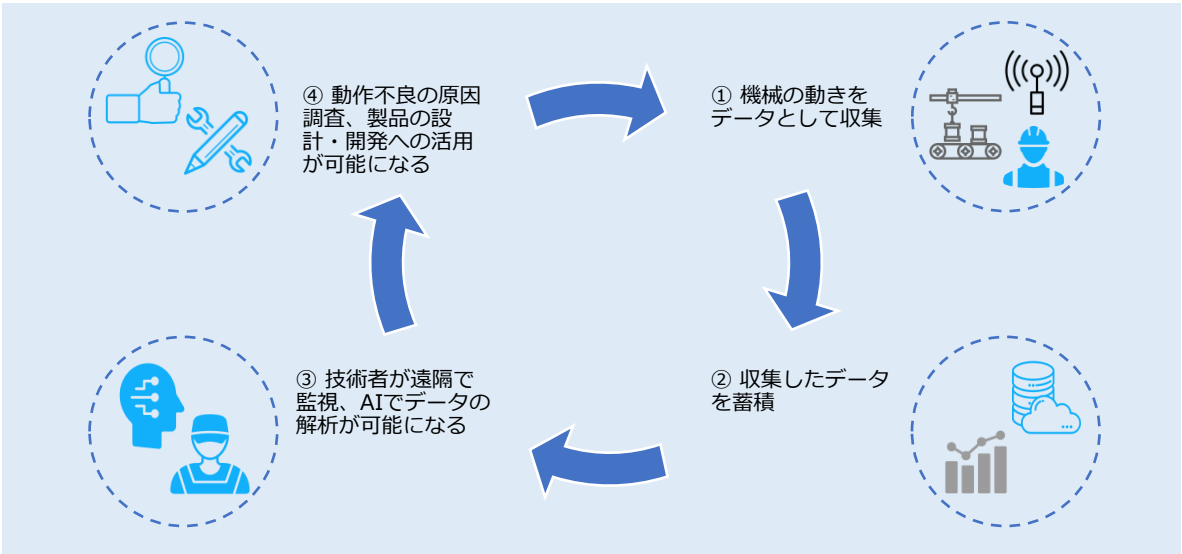


図27. データ活用による業務改革の流れ
（出典）IPA"製造分野のDX事例集".
https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf,
（参照 2023-07-28）.

5-2-3. DXの推進

DX with Cybersecurityの概要

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で、企業は新たな価値を創造して競争力を強化していくことができます。しかし、デジタルトランスフォーメーションを推進することは、デジタル技術の利用を拡大することにつながり、サイバー攻撃やデータ漏洩などのセキュリティ上のリスクが増大することにもなります。したがって、デジタルトランスフォーメーションを推進すると同時に、サイバーセキュリティ対策も強化すること（DX with Cybersecurity）が求められることになります。

デジタルトランスフォーメーションの推進によって、自社の製品やサービスの価値を向上させることができます。しかし、デジタル技術の活用によって増大するセキュリティ上のリスクに対応しなければ、企業の存続を脅かすインシデントが発生するかもしれません。したがって、サイバーセキュリティ対策は、やむを得ない費用ととらえるのではなく 、企業価値や競争力の向上に不可欠なものとしてとらえることが大切です。

DX with Cybersecurityの詳細に関しては、後述のページで説明します。

デジタルトランスフォーメーションの推進とサイバーセキュリティ対策を同時に進める必要がある

第6章. サイバーセキュリティ戦略および関連法令

6-1. NISC：サイバーセキュリティ戦略

6-2. 関連法令

章の目的
第6章は、NISCによるサイバーセキュリティ戦略を通じて、DXとサイバーセキュリティの確保を同時に推進する重要性について理解することを目的とします。また、サイバーセキュリティに関連する法令として、個人情報保護法とGDPRについて説明します。
主な達成目標
◘ 日本におけるサイバーセキュリティに関する方針や施策について理解すること ◘ サイバーセキュリティに関する知識やスキルを身につける必要性について理解すること ◘ 個人情報関連の法令を理解すること

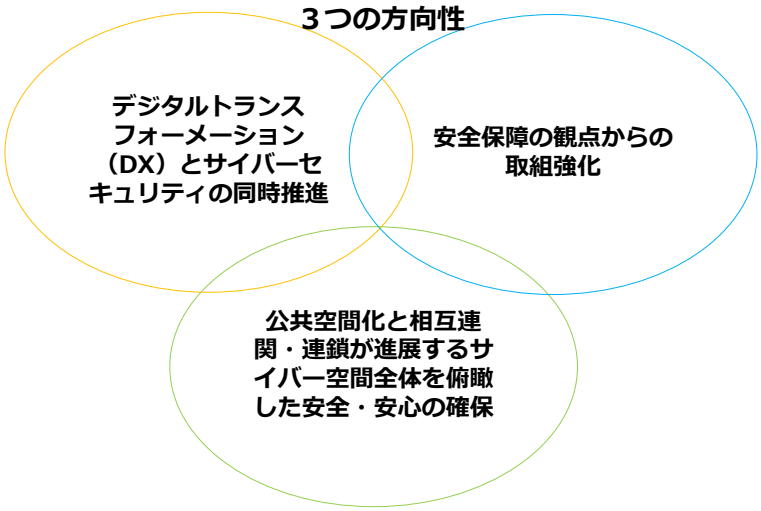
6-1-1. サイバーセキュリティ戦略

サイバーセキュリティ戦略とは、国家レベルでサイバーセキュリティの確保に取組むための基本的な方針や目標を定めたものです。日本においては、内閣サイバーセキュリティセンター（NISC）が、サイバーセキュリティ戦略の策定や実施に関する総合調整役を担っています。現行のサイバーセキュリティ戦略は、2021年9月28日に閣議決定され、「今後3年間に執るべき諸施策の目標や実施方針を示す」ものとされています。この戦略に基づき、政府はサイバーセキュリティの確保に向けた取組みを進めています。

サイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識：「ニューノーマル」とデジタル社会の到来
（デジタル改革の推進、新型コロナウイルスの影響、SDGsなど）
サイバー空間をとりまく課題認識：国民全体のサイバー空間への参画
（サイバー攻撃の巧妙化、サイバー空間の公共化、現実世界との相互連関など）

「Cybersecurity for All」
誰も取り残さないサイバーセキュリティ



「自由、公正かつ安全なサイバー空間」の確保

図28.サイバーセキュリティ戦略の課題と方向性の概要
（出典）NISC「 サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」を基に作成

現在、あらゆる人々にとって、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）となってきています。また今後、サイバー空間とは繋がりのなかった主体も含め、あらゆる主体がサイバー空間に参画することになります。そのため、デジタル化の進歩と共に「誰一人取り残さない」サイバーセキュリティの確保に向けた取組みを進める必要があります。この考え方のもと、本戦略では、「自由、公正、かつ安全なサイバー空間」を確保するため、3つの方向性に基づいて施策を推進する方針を示しています。

6-1-1. サイバーセキュリティ戦略

３つの政策目標として、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせるデジタル社会の実現」、「国際社会の平和・安定及び我が国の安全保障への寄与」が掲げられています。これらの目標を達成するために、それぞれの方向性に基づいた様々な施策が挙げられています。

経済社会の活力の向上及び持続的発展

方向性

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進
▶ デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進

「経済社会の活力の向上及び持続的発展」のためには、「デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進」が必要となります。

課題

・DXの推進が必要とされている中、サイバーセキュリティに対する意識や、サイバー空間を構成する技術基盤やデータなどに対する信頼が醸成されなければ、積極的な参加・コミットメントを得られず、変革を伴わない表層的なデジタル化に留まるおそれがある

・業務、製品・サービスなどのデジタル化が進む中、サイバーセキュリティの確保は企業価値に直結する重要なものとなっており、製品の企画・設計の段階からセキュリティを考慮する「セキュリティ・バイ・デザイン」が重要視されるなど、デジタル投資とセキュリティ対策を同時に進める必要がある

課題に対する具体的施策

主な具体的施策

経営層の意識改革

デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組みの可視化やインセンティブ付けを行い、更なる取組みを促進

地域・中小企業におけるDX with Cybersecurityの推進

中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業のセキュリティ対策強化の推進

新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり

Society5.0に対応したフレームワークなども踏まえ、各種取組みを推進

・サプライチェーン	：産業分野別及び産業横断的なガイドラインなどの策定や活用の促進
・データ流通	：送信元のなりすましやデータ改ざんを防止する仕組みの整備
・セキュリティ製品・サービス	：第三者検証サービスの普及による信頼性確保の取組み
・先端技術	：情報収集・蓄積・分析・提供などの共通基盤構築

誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

情報教育推進の中、「デジタル活用支援」と連携して各種取組みを推進

（出典）NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」を基に作成

6-1-1. サイバーセキュリティ戦略

国民が安全で安心して暮らせるデジタル社会の実現

方向性

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

▶ 国は、様々な主体と連携しつつ、
① 自助・共助による自律的なリスクマネジメントが講じられる環境づくりと、
② 持ち得る手段の全てを活用した包括的なサイバー防御の展開などを通じて、
サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築し、国全体のリスク低減、レジリエンス向上を図る。

「国民が安全で安心して暮らせるデジタル社会の実現」のためには、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」が必要となります。

課題

・サイバー空間の公共空間化、相互連関・連鎖の深化、サイバー攻撃の組織化・洗練化

課題に対する具体的施策

主な具体的施策

（1）国民・社会を守るためのサイバーセキュリティ環境の提供

① 安全・安心なサイバー空間の利用環境の構築
② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）
③ サイバー犯罪への対策
④ 包括的なサイバー防御の展開
⑤ サイバー空間の信頼性確保に向けた取組

（2）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

（3）経済社会基盤を支える各主体における取組

① 政府機関など　：監査・CSIRT訓練・GSOCによる監視などを通じたセキュリティ水準の向上
クラウドサービスの利用拡大を見据えた政府統一基準群の改定
運用やクラウド監視に対応したGSOC機能の強化
② 重要インフラ　：「重要インフラの情報セキュリティ対策に係る第４次行動計画」の改定
環境変化に対応した防護の強化や経営層のリーダーシップを推進
③ 大学・教育研究機関など　：先端情報を保有する大学などへの対策強化支援など
（リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策）

（4）多様な主体による情報共有・連携と大規模サイバー攻撃事態などへの対処体制強化

（出典）NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」を基に作成

6-1-1. サイバーセキュリティ戦略

国際社会の平和・安定及び我が国の安全保障への寄与

方向性

安全保障の観点からの取組強化
▶サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、以下を一層強化する。

「国際社会の平和・安定及び我が国の安全保障への寄与」のためには、「安全保障の観点からの取組強化」が必要となります。

課題

・我が国をとりまく安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取などを企図したサイバー攻撃を行っているとみられている

・一方、同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められており、サイバー事案やサイバー空間に関する国際ルールなどをめぐる対立などに対して同盟国・同志国などが連携して対抗している

・加えて、安全保障の裾野が経済・技術分野にも一層拡大している中で、サイバー空間に関する技術基盤やデータをめぐる争いに対しても、同盟国・同志国が連携して対抗し、「自由、公正かつ安全なサイバー空間」を確保するため、我が国の基本的な理念に沿った国際ルールを形成していく必要がある

課題に対する具体的施策

主な具体的施策

（1） 自由・公正かつ安全なサイバー空間の確保

→サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）

→サイバー空間におけるルール形成（信頼性のある自由なデータ流通や5Gセキュリティなど）

（2）我が国の防御力・抑止力・状況把握力の強化

→サイバー攻撃に対する防御力の向上（防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、先端技術・防衛産業などのセキュリティ確保のための官民連携・情報共有など）

→サイバー攻撃に対する抑止力の向上（サイバー空間の利用を妨げる能力の活用、外交的手段・刑事訴追などを含めた対応の活用、日米同盟の維持・強化）

→サイバー空間の状況把握力の強化（サイバー攻撃の更なる実態解明の推進）

（3） 国際協力・連携

→知見の共有・政策調整（国際連携の重層的な枠組みの強化）

→サイバー事案などに係る国際連携の強化（国際サイバー演習の主導などによる国際的なプレゼンスの向上）

→能力構築支援（産学官連携や外交･安全保障を含めたASEANを含むインド太平洋地域における取組み強化）

（出典）NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」を基に作成

6-1-1. サイバーセキュリティ戦略

横断的施策

３つの政策目標を達成するためには、サイバーセキュリティ戦略の３つの方向性を意識し、その基盤として、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組んでいくことが重要です。

サイバーセキュリティ戦略の３つの方向性

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進	公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保	安全保障の観点からの取組強化

上記の推進に向け、
横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取組む

- **研究開発の推進**
  産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進
  （1）国際競争力の強化・産学官エコシステムの構築（研究・産学官連携振興施策の活用など）
  （2）実践的な研究開発の推進（サプライチェーンリスクへの対応、攻撃把握・分析・共有基盤、暗号などの研究推進など）
  （3）中長期的な技術トレンドを視野に入れた対応（AI技術の進展、量子技術の進展）

- **人材の確保・育成・活躍促進**
  （1）DX with Cybersecurityの推進（「プラス・セキュリティ」知識を補充できる環境整備など）
  （2）巧妙化・複雑化する脅威への対処（人材育成プログラムの強化、資格制度活用など）
  （3）政府機関における取組み（外部高度人材活用の仕組み強化など）

- **全員参加による協働・普及啓発**
  テレワークの増加やクラウドサービスの普及など、近年の人々の行動や企業活動の変化に応じて、ガイドラインや様々な解説資料などの整備の推進

（出典）NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」を基に作成

One Point

サイバーセキュリティ基本法

サイバーセキュリティ基本法は、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念や国の責務などを定めています。また、サイバーセキュリティ戦略の策定およびその他サイバーセキュリティに関する施策の基本となる事項を規定します。

6-1-1. サイバーセキュリティ戦略

サイバーセキュリティ2023

NISCは、サイバーセキュリティ戦略に基づく今年度の2022年度年次報告・2023年度年次計画を整理した「サイバーセキュリティ2023」を策定しています。サイバーセキュリティ戦略に基づく施策を的確に実施するため、各年度の施策の進捗状況を検証し、次年度の計画に反映することとしています。

2023年度の「サイバー空間を巡る状況変化と情勢、及び政策課題」と「今後の取組の方向性（今年度特に強力に取り組む施策について）」は以下の通りです。

サイバー空間を巡る状況変化と情勢、及び政策課題

- **昨今の状況変化**
  - ・サイバー空間への依存度の高まり/情報システムの利用拡大/サプライチェーンの多様化・複雑化の進展/生成AIなどの新たな技術普及
  - ・新たな技術・サービスの普及に伴うサイバー攻撃を受けるシステム側の侵入口（セキュリティホール）増加
  - ・サイバー攻撃手法の変化（深刻化・巧妙化）/サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取
- **サイバー空間の現下の情勢 ～サイバー攻撃の深刻化・巧妙化～**
  - ・ランサムウェアが依然とした脅威、不正プログラムEmotetが活動と停止の繰り返し/暗号資産交換業者もサイバー攻撃の対象
- **昨今の状況変化を踏まえた政策課題**
  - ・政府による「国家安全保障戦略」の策定：サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保
  - ・実効的なサイバーセキュリティ対策を実現するための課題：①各主体による対策の強化・対処能力の向上/②政府による支援などの充実・強化/③国際連携・協力の強化が政策課題に

今後の取組の方向性（今年度特に強力に取り組む施策について）

1. 経済社会の活力の向上及び持続的発展 ～DXの推進に向けたリスク対策の強化～
✓ これまでICTの利活用に必ずしも積極的ではなかった地域・中小企業における対策の促進
✓ サプライチェーンリスクの増大を踏まえたソフトウェアセキュリティの高度化に関する取組強化

2. 国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラのレジリエンスの向上～
✓ サイバー空間における脅威動向の把握・対処や分析能力の向上を通じた政府情報システムのレジリエンス向上
✓ 重要インフラ分野において、組織全体でのサイバーセキュリティ対応の促進・インシデント発生時の初動対応支援等を進めている医療分野など

3. 国際社会の平和・安定及び我が国の安全保障への寄与 ～同盟国・同志国との国際連携・協力の推進～
✓ 同盟国・同志国とのサイバー協議や対話の実施
✓ 日米豪印における協力、ランサムウェア対策を推進するための同志国間の協力枠組みの推進

サイバーセキュリティ2023のポイント
（出典）NISC「サイバーセキュリティ２０２３の概要」を基に作成

6-1-1. サイバーセキュリティ戦略

「今後の取組の方向性（今年度特に強力に取り組む施策について）」に記載がある「１．経済社会の活力の向上及び持続的発展～DXの推進に向けたリスク対策の強化～」の中で、中小企業に主に関連する内容を説明します。

［１］ 中小企業のサイバーセキュリティ対策促進

１．背景及び課題

✓ サプライチェーンの中で比較的弱い中小企業へのサイバー攻撃を経由して、発注元の大企業も被害を受けている実態への取組強化が必要である。

✓ 他方で、そのリスクを自分事として認識していない、あるいは、何をしてよいか分からない状況にある中小企業や、対策費用や人材の確保に課題を感じている中小企業も多数存在する。

✓ 中小企業の経営者の意識改革や中小企業が使いやすいセキュリティサービスの普及促進・運用改善、大企業が取引先の中小企業に対してセキュリティ対策の支援・要請を行う際の関係法令の適用関係にかかる懸念の払拭を更に進めていくことが必要である。

２．取組の概要

①手法

✓ 「サイバーセキュリティお助け隊サービス」につき、サービス基準の改定による同サービスの拡充等を通じて、中小企業側の様々なニーズに応え、個々の中小企業の要望に応じたサイバーセキュリティ対策の支援を実現する。

✓ こうした取組を、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携して実施し、中小企業への対策の浸透を図る。

②取組によって期待される成果・効果

✓ お助け隊サービスの普及を通じて、中小企業のセキュリティが向上するとともに、中小企業におけるサイバー攻撃被害の実態について、サービス提供事業者を通じて把握することが可能になる。あわせて、関係機関への通報や共有が促進されることも期待される。

✓ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）との連携により、産業界全体のサイバーセキュリティ強化が期待される。

［２］ サプライチェーンリスクを踏まえたソフトウェアセキュリティの高度化に関する取組

１．背景及び課題

✓ サイバー空間とフィジカル空間が密接に関係していく世界にあって、サイバー攻撃のリスクも増大する中、これに対応するための考え方を整理したフレームワークを整備しているところであり、この社会実装を進めることでセキュリティ対策のレベルを向上させることが必要である。

✓ 特に、ソフトウェアを構成する部品情報を管理し、脆弱性管理等に活用可能なSBOM導入の重要性に対する認識が米国を中心に広まっていることから、こうした動きに対応しつつ、SBOMが有するメリットを生かしていくための仕組み作りや様々な分野への普及が重要である。

✓ 通信システムのソフトウェアでのOSSの普及拡大に伴って多発するサイバー攻撃への対処のため、通信分野におけるSBOM導入が急務である。

２．取組の概要

①手法

✓ 脆弱性管理の効率化等を図るため、脆弱性情報とSBOMの紐付けを機械的に行う手法の実証など、2022年度までの取組を深化する。

✓ 代表的な通信システムを対象にSBOMを作成・評価するなど、通信分野でのSBOM導入に向けた取組を進める。

②取組によって期待される成果・効果

✓ SBOMに関する知見の整理、契約モデル等のツールの整備等を通じた、安心してソフトウェア活用を行うことができる環境の構築、ひいてはあらゆる産業で生産性の向上や新たなサービスの創出といった付加価値の増大が見込まれる。

✓ 通信分野でのSBOM導入により、OSS等のソフトウェア部品の脆弱性が確認された際の対応の迅速化等が期待される。

サイバーセキュリティ2023のポイント
（出典）NISC「サイバーセキュリティ２０２３の概要」を基に作成

6-1-2. 企業経営のためのサイバーセキュリティの考え方

企業経営のためのサイバーセキュリティの考え方

サイバーセキュリティ対策にかかる支出をやむを得ない費用とするのではなく、経営のために必要な投資と位置付け、自発的にサイバーセキュリティ対策に取組むことが重要です。デジタルトランスフォーメーションの推進にあたり、IoTなどのデジタル技術を積極的に取り入れる中、安全性が高い品質の製品やサービスを実現していく取組は、企業価値や競争力の向上に繋がります。そのため、デジタルトランスフォーメーションの推進とサイバーセキュリティ対策の強化の両方に取組むことが大切です。

サイバーセキュリティ対策を行うにあたって、以下の基本的認識や留意事項を理解し、自社の現状のIT活用状況や、セキュリティ対策の取組レベルに応じた対策を行うことが大切です。

2つの基本的認識

<①挑戦>
サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

<②責任>
全てがつながる社会において、サイバーセキュリティに取組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。

3つの留意事項

<①情報発信による社会的評価の向上>
・セキュリティ対策を、仕方なくやるものではなく、企業価値を高め、品質向上に有効な経営基盤の一つとして位置付けることが必要。
・サイバーセキュリティに関する取組みや方針を情報発信することによって、関係者の理解を深め、社会的評価を高めることができる。

<②リスクの一項目としてのサイバーセキュリティ>
・提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
・経営層のリーダーシップが必要。

<③サプライチェーン全体でのサイバーセキュリティの確保>
・サプライチェーンでつながるどこかの企業のセキュリティ対策が不十分だと、そこから自社の重要情報が流出してしまうなどの問題が起きる可能性がある。そのため、サプライチェーン全体で一定レベルのサイバーセキュリティの確保が必要。
・一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加などが必要。

図29.ITの活用またはサイバーセキュリティ対策の取組み状況に応じた分類と対策
（出典）NISC「企業経営のためのサイバーセキュリティの考え方の策定について」を基に作成

6-1-2. 企業経営のためのサイバーセキュリティの考え方

企業のIT活用状況、サイバーセキュリティ対策の取組みのレベルに応じた、実施すべき対策について説明します。企業のIT活用状況および、サイバーセキュリティ対策の意識や実施レベルは、以下の6つに分類できます。「理想的」な状態が一番良く、この状態を実現していくためには、自社が置かれているレベルに応じた対策を進めることが重要です。必要な対策の一例を「もっと積極的」、「無駄な投資」、「危険」に該当する分類ごとに紹介します。

レベル	分類	概要・対策	
理想的に	1	**ITの利活用を事業戦略上に位置付け、サイバーセキュリティを強く意識し、積極的にITによる革新と高いレベルのセキュリティに挑戦する企業**	
もっと積極的に	2	**IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略としての組み込みはできていない企業**	
		対策	ITを積極的に活用してビジネスの展開を目指すことが重要であり、攻めのIT投資に関する取組みを行うことです。
無駄な投資	3	**過剰なセキュリティ意識により、ITの利活用を著しく制限し、競争力強化に活用させていない企業**	
		対策	リスクを再評価して、サイバーセキュリティ対策が過剰になっている部分については見直しを行うことが必要です。
危険	4	**サイバーセキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策ができていないにもかかわらず、ITの利活用を進めている企業**	
		対策	情報セキュリティポリシーの策定と実践が必要であり、まずはサイバー攻撃を受けたときのための緊急時対応用マニュアルを作成すべきです。
	5	**サイバーセキュリティの必要性を理解していない企業や、自らセキュリティ対策を行う上で事業上のリソースの制約が大きい企業**	
		対策	コストがあまりかからない最低限のセキュリティ対策から実施することが重要であり、例えば「情報セキュリティ5か条」の対策を行うべきです。
対象外	6	**ITを利用していない企業**	

図30.ITの活用またはサイバーセキュリティ対策の取組み状況に応じた分類と対策
（出典）東京都「 ITおよびサイバーセキュリティに関する組織の視点６分類」を基に作成

6-1-3. DX with Cybersecurity

業務や製品・サービスのデジタル化が進む中、サイバーセキュリティの確保は企業の価値に直結する重要な要素となっています。このため、デジタルトランスフォーメーションとサイバーセキュリティ確保に向けた取組みを同時に推進すること（DX with Cybersecurity）が不可欠になっています。しかしながら、中小企業がDX with Cybersecurityを推進するにあたり、人材や予算などのリソース不足などさまざまな課題が存在しています。これらの課題に対処するため、国が実施している施策の一部について説明します。

経営層の意識改革

【課題】経営層が主体性をもってデジタルトランスフォーメーションとサイバーセキュリティ対策に取組むためには、専門家とのコミュニケーションが重要
【施策】経営者がITやセキュリティに関する専門知識を持っていない場合でも、セキュリティ専門家と協力し、「プラス・セキュリティ」知識を習得する環境を整備

地域・中小企業におけるDX with Cybersecurityの推進

【課題】中小企業は、セキュリティ対策に予算を割く事の必要性を理解する
【施策】中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策を推進

新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり

サプライチェーンの信頼性確保
【課題】サイバー攻撃の起点となり得る箇所の拡大に伴う、リスク管理が重要
【施策】産業分野別、または産業横断的なガイドラインの策定や活用促進を通じて、産業界におけるセキュリティ対策の具体化・実装を促進

データ流通の信頼性確保
【課題】データの真正性や流通基盤の信頼性を確保することが重要
【施策】データマネジメントの定義、送信元のなりすましやデータの改ざんなどを防止する仕組みを整備

セキュリティ製品・サービスの信頼性確保
【課題】市場において提供されるセキュリティ製品・サービスが信頼できるか、客観的な評価が必要
【施策】一定の基準を満たすセキュリティサービスの審査・登録する仕組みを整備

先端技術・イノベーションの社会的実装
【課題】デジタル化の進展に伴い、効率的なセキュリティ対策が必要
【施策】研究機関の知識や技術を民間企業が活用しやすい環境の整備や、企業が社外の知識や技術を取り入れ、組織の改革（セキュリティ対策の強化など）を進められる環境の整備を推進

施策の理解のため参考となる文献（参考文献）	
目的や所属・役割から選ぶ施策一覧	https://security-portal.nisc.go.jp/curriculum/

6-1-3. DX with Cybersecurity

ここからは、デジタルトランスフォーメーションを推進するために必要なスキルや人材について説明します。デジタルトランスフォーメーションを進めていくには、社内にデジタルトランスフォーメーションの素養を持った人材が必要ですが、中小企業において重要なのは、デジタルトランスフォーメーションに関する高度な知識を持った人材を確保・育成することよりも、まずは経営層を含め社内の全ての人々がデジタルトランスフォーメーションに理解や関心を持ち、自らの業務を変革して新たな付加価値を生み出そうとするような意識を持つことです。そのために必要となるデジタルトランスフォーメーションに関するリテラシー（基礎的な知識やスキル、マインドセット）を説明していきます。

DXに関するリテラシーを身につけたことによる効果（個人）

世の中で起きているDXや最新の技術へのアンテナを広げ、日々生まれている新たな技術、キーワードなどにも興味を向けられるようになります。
知らない内容に接した際は、自ら調べてDXの知識を広げていけるようになります。

DXに関するリテラシーを身につけたことによる効果（会社）

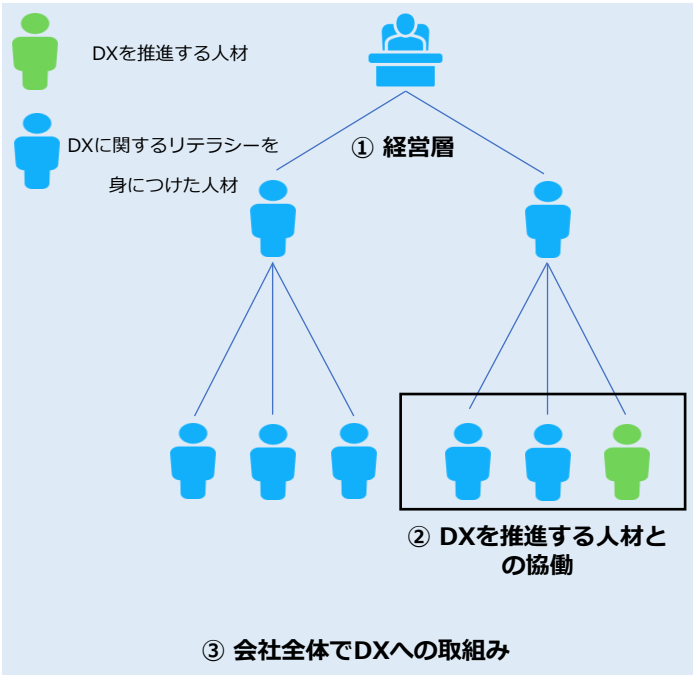


図31. DXリテラシー標準に沿った学びによる効果の概要
（出典）IPA、経済産業省「デジタルスキル標準ver.1.0 」を基に作成

①経営層

社会やビジネス環境の変化において有益な技術・考え方を知ることで、自社のDXの方向性を思案し、社員に示すことができる

②DXを推進する人材との協働

事業内容に知見がある人材とDXを推進する人材（DXに関する専門性が高い人材）との協働が進み、企業としてのDXが進みやすくなる

③会社全体でDXへの取組み

社員全員がDXに関するリテラシーを身につけることで、DX推進に伴う組織内の変化に対する受容性が高くなる

6-1-3. DX with Cybersecurity

デジタルスキル標準（DSS）

経済産業省とIPAがまとめた「デジタルスキル標準（DSS）」では、すべてのビジネスパーソンがデジタルトランスフォーメーションに関する基礎的な知識、スキル、マインドセットを身につけるための学習指針を「DXリテラシー標準」として策定しています。企業は、社員に対して、デジタルトランスフォーメーションに関するリテラシーを身につけさせるための育成方法を検討する際に、指針として活用することができます。

DXリテラシー標準は、特定の産業や職種、部署などに依存しない汎用性を重視して作成されています。そのため、企業や組織がこれを適用する際には、自身が属する産業や事業の方向性に合わせる必要があります。

DXリテラシー標準 → **自社の事業の方向性に合わせることが必要**

DXリテラシー標準は、以下のように構成されています。

標準策定のねらい
ビジネスパーソン一人ひとりがDXに関するリテラシーを身につけることで、DXを自分事ととらえ、変革に向けて行動できるようになる

Why （DXの背景）	What （DXで活用されるデータ・技術）	How （データ・技術の利活用）
DXの重要性を理解するために必要な、社会、顧客・ユーザー、競争環境の変化に関する知識を定義 → DXに関するリテラシーとして身につけるべき知識の学習の指針とする）	ビジネスの場で活用されているデータやデジタル技術に関する知識を定義 → DXに関するリテラシーとして身につけるべき知識の学習の指針とする	ビジネスの場でデータやデジタル技術を利用する方法や、活用事例、留意点に関する知識を定義 → DXに関するリテラシーとして身につけるべき知識の学習の指針とする

マインド・スタンス
社会変化の中で新たな価値を生み出すために必要な意識・姿勢・行動を定義

→個人が自身の行動を振り返るための指針かつ、組織・企業がDX推進や持続的成長を実現するために、構成員に求める意識・姿勢・行動を検討する指針とする

項目一覧

Why（DXの背景）	What（DXで活用されるデータ・技術）		How（データ・技術の利活用）	
社会の変化	データ	社会におけるデータ	活用事例・利用方法	データ・デジタル技術の活用事例
顧客価値の変化		データを読む・説明する		ツール利用
競争環境の変化		データを扱う	留意点	セキュリティ
		データによって判断する		モラル
	デジタル技術	AI		コンプライアンス
		クラウド		
		ハードウェア・ソフトウェア		
		ネットワーク		

マインド・スタンス				
デザイン思考/アジャイルな働き方	顧客、ユーザへの共感	常識にとらわれない発想	反復的なアプローチ	
新たな価値を生み出す基礎としてのマインド・スタンス	変化への適応	コラボレーション	柔軟な意思決定	事実に基づく判断

図32.DXリテラシー標準の全体像
（出典）IPA、経済産業省「デジタルスキル標準ver.1.1 」を基に作成

6-1-3. DX with Cybersecurity

デジタルスキル標準の改訂について

急速に普及する生成AIは、各企業におけるDXの進展を加速させると考えられ、企業の競争力を向上させる可能性があります。あわせて、ビジネスパーソンに求められるスキル・リテラシーも変化し、より重要になる部分もあると想定されます。その状況に対応するため、2023年８月にDXリテラシー標準に関する内容が改定されました。

追加された生成AIに関する内容を以下の図で説明します。

DXリテラシー標準策定のねらい

「DXを自分事ととらえ、変革に向けて行動できるようになる」という位置付けは不変

Why DXの背景	What DXで活用されるデータ・技術	How データ・技術の利活用
✓ 産官学で生成AIの利用が進んでおり、社会環境へ影響を与える可能性があるため、「社会の変化」に人材育成・教育や労働市場の変化等の学習項目例を追加	✓ 生成AIは、ビジネスの場で急速に普及・利用されているため、「AI」に生成AIの技術動向や倫理などの学習項目例を追加 ✓ 現在の利用状況に鑑み「ネットワーク」にネットワークの種類、インターネットサービスの学習項目例を追加 ✓ 個人や企業などで扱うデータがデジタル技術・サービスに活用されるため、「データを扱う」に活用しやすいデータの入力や整備の手法等の内容・学習項目例を追加 ✓ 適切でないデータから生み出される結果は、誤った判断・損害につながり得るため、「データによって判断する」に適切なデータを用いて判断することの重要性などの内容・学習項目例を追加	✓ 生成AIは、ツールなどの基礎知識や指示（プロンプト）の手法を用いて業務の様々な場面で利用できるため、「データ・デジタル技術の活用事例」に生成AIの活用事例、「ツール利用」に生成AIツールの概要、指示（プロンプト）の手法等の学習項目例をそれぞれ追加 ✓ 情報漏洩や法規制、利用規約等に正しく対処しながら生成AIを利用することが求められるため、「モラル」にデータ流出の危険性等、「コンプライアンス」に法規制や利用規約等の学習項目例をそれぞれ追加

マインド・スタンス

- ✓ 他項目と比べてより普遍的な要素を定義しているため、生成AI利用においても同様に重要となる
- ✓ 適切なデータを用いることにより、事実に基づく判断が有効になるため、「事実に基づく判断」に適切なデータ入力の重要性や行動例等を追加
- ✓ 生成AIをビジネスパーソンとしてのスキルと掛け合わせ生産性向上やビジネス変革等へ適切に利用しようとしていること、生成AI利用における注意点を理解していること、生成AIの影響に対して変化をいとわず学び続けることは、今後、全ビジネスパーソンが身に着けるべきマインド・スタンスとして重要性が増すため、「生成AI利用において求められるマインド・スタンス」として既存項目と分けて追加

図33.DXリテラシー標準の改訂（ 2023年８月）の概要
（出典）IPA、経済産業省「デジタルスキル標準ver.1.1 」を基に作成

One Point

DXリテラシー標準の学習方法

「マナビDX」という、すべての社会人にとって必須であるデジタルスキルを学べるコンテンツを紹介しているポータルサイトがあります。このポータルサイトでは、DXリテラシー標準の各項目ごとに学習できる講座が掲載されており、DXリテラシーを学ぶことができます。

6-1-3. DX with Cybersecurity

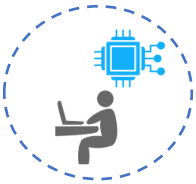
プラス・セキュリティ

プラス・セキュリティとは

自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと[14]

企業は、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への対策が求められています。この状況の中、経営層をはじめ、法務や広報といった、必ずしもITやセキュリティに関する専門知識や業務経験を有していない人も「プラス・セキュリティ」知識を習得することが重要です。なぜなら、デジタルトランスフォーメーションが進む中、サイバーセキュリティ担当部署だけでは、サイバーセキュリティ対策への対処が難しい状況になっているためです。そのため、サイバーセキュリティ対策が不十分な場合、インシデントが生じる可能性がある業務を担っている人材には、業務に必要なセキュリティに関する知識・スキルを身につけてもらう必要があります。

クラウドを活用した新規プロジェクトの担当者



組み込みソフトウェアの機能を設計する担当者

自社の電話、インターネット、複合機などの保守契約を扱う担当者

サイバーセキュリティの知識が不十分な場合の問題例

- 目的にそぐわないクラウドを選定することや、自社のサイバーセキュリティ担当者が把握していないクラウドの導入により、情報漏洩などのリスクが高まる恐れがあります
- ソフトウェアにサイバー攻撃に対する脆弱性が生じる恐れがあります
- 不適切な設定で運用することで、機器を介した情報漏えいの原因となる恐れがあります

[14]:経済産業省.”サイバーセキュリティ経営ガイドラインVer2.0付録Fサイバーセキュリティ体制構築・人材確保の手引き～ ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第1.1版”. https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf, （2023-07-28）.

6-1-3. DX with Cybersecurity

プラス・セキュリティ人材の育成

プラス・セキュリティ知識を身につける方法として、主に試験・資格を活用したり、教育プログラムを受けたりする方法があります。ここでは、具体例も含めて紹介します。

試験・資格の活用

各分野の人材がプラス・セキュリティ知識を身につける方法の1つとして、試験や資格の活用が挙げられます。資格を活用することの利点は、特定の役割や業務を担うために必要なスキルを効率よく習得できることです。

（例）

- **情報セキュリティマネジメント試験**

【対象】企業の戦略マネジメント層や実務者層のサイバーセキュリティ担当者
【内容】本試験は、情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定するものです。

教育プログラム・コミュニティ活動の活用

NISC（内閣サイバーセキュリティセンター）では、経営層、管理職、一般社員ごとにそれぞれ初級、中級、上級で難易度が分けられたプラス・セキュリティ知識を補充できる研修、セミナー、講義などが紹介されています。

（例）

- **戦略マネジメント系セミナー（IPA）**

【対象】管理職、一般社員（特に、「セキュリティ統括責任者」である部課長級の責任者層、今後責任者層になることが期待される実務者層・技術者層、「プラス・セキュリティ」人材の方に向いています）
【難易度】中級
【内容】セキュリティ統括責任者として認識しておくべき事項を、「有識者講演」、「プログラム講義」、「ディスカッション（グループワーク）」の３つのプログラムで学習するセミナーです。
座学だけでなく、受講者間でのディスカッション・意見交換の場を設け、より実践的で深い理解が得られるアクティブラーニングの機会を提供しています。

- **実践サイバー演習「RPCI」**（NICT）

【対象】経営層、管理職、一般社員（特に、CISO、CSIRT管理者、CSIRTメンバー、インシデントが発生した際の対応に携わる方、情報システムの管理・運用・調達・企画・開発に携わる方に向いています）
【難易度】中級～上級
【内容】本番に近いリアルな環境でのインシデント対応を行う演習です。擬似的に発生させたサイバー攻撃にCSIRTとしてチームで対処します。実際の対応に近い体験をすることで、多くの気づきや学びを得ることができます。

6-2-1. 個人情報保護法

インターネットが普及し、ネットショッピングなど、様々なサービスの利用を通して個人情報のやり取りが当たり前になった現在、個人情報の保護は人々にとって身近なテーマとなりました。企業にとって、個人情報は事業へ有効に活用することのできるものですが、漏えいなどの事故が起きた場合、社会的な信用の失墜に直結するため、事業経営に及ぼす影響は非常に大きいです。

そのため、消費者や取引先から預かっている個人情報を適切に取扱うことは、企業の権利や利益を守ることに繋がる非常に重要な取組みとなります。ここでは、サイバーセキュリティに関連する法令として、個人情報保護法について説明します。

個人情報保護法とは

インターネットの普及や情報技術の進歩などを背景として、個人の権利や利益を守ることを目的として「個人情報保護法」（正式名称：個人情報の保護に関する法律）が2005年4月に全面施行されました。施行後も、デジタル技術の進展やグローバル化などの経済・社会情勢の変化や、世の中の個人情報に対する意識の高まりなどに対応するため、今までに3度の改正が行われています。

個人情報保護法では、どのような情報が個人情報になるのか、個人の権利や利益を守るためには個人情報をどのように取り扱わなければいけないのかなどが規定されています。

個人情報の定義

個人情報保護法において「個人情報」とは、生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報のことを指します。これには他の情報と容易に照合でき、それにより特定の個人を識別できるものも含まれます。

個人情報を取り扱う時の基本ルール

① 取得・利用	② 保管・管理
・利用目的を特定して、その範囲内で利用する。 ・利用目的を通知又は公表する。	・漏えいなどが生じないように、安全に管理する。 ・従業者や委託先にも安全管理を徹底する。
③ 提供	**④ 開示請求などへの対応**
・第三者に提供する場合は、あらかじめ本人から同意を得る。 ・第三者に提供した場合、提供を受けた場合は一定事項を記録する。	・本人から開示などの請求があった場合はこれに対応する。 ・苦情に適切かつ迅速に対応する。

（出典）内閣府大臣官房政府広報室.”「個人情報保護法」をわかりやすく解説 個人情報の取扱いルールとは？”. https://www.gov-online.go.jp/useful/article/201703/1.html,（2023-07-28）.

One Point

個人情報保護法の罰則規定

2022年4月施行の法改正により、法令違反に対する罰則が強化されました。法人に対しては、個人情報保護委員会の措置命令に違反したり、個人情報データベースを不正流用した場合１億円以下、報告義務違反の場合50万円以下の罰金となっています。

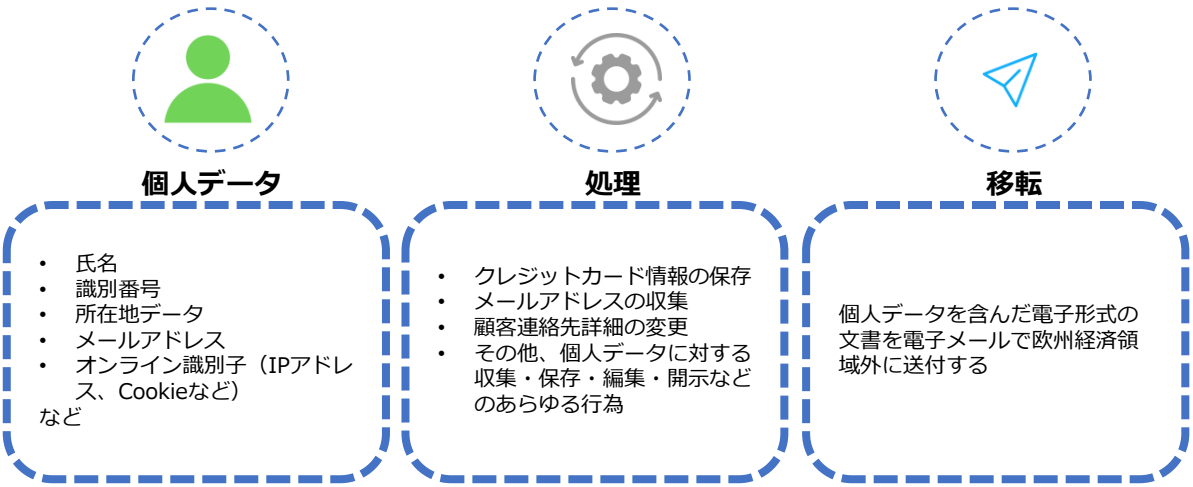
6-2-2. GDPR

GDPR（EU一般データ保護規則）とは、個人データの保護とプライバシーの権利を強化するために、欧州連合（EU）加盟国に適用される重要な法令です。EUで活動する企業だけではなく、EU加盟国の居住者の個人データを取り扱う企業は、企業規模に関係なく、GDPRが適用されるため、GDPRを理解し遵守することが必要です。以下では、GDPRの概要および日本企業の関わりについて説明します。

GDPR（一般データ保護規則）とは

EUで策定された新しい個人情報保護の枠組みであり、個人データ保護やその取扱いについて詳細に定められた欧州経済領域内の各国に適用される法令のことです。欧州経済領域内で取得した「個人データ」を「処理」し、欧州経済領域外の第三国に「移転」するために満たすべき要件が定められています。GDPRの特徴として、インターネット上で収集できる個人データのほとんどが保護対象となっています。

GDPRの概要



GDPRと日本企業の関係

GDPRはEU内で適用される法令ですが、支店など物理的な拠点をEU内に持っていなくても、**インターネットを利用して日本からEU域内に商品販売やサービス提供、情報収集を行っている企業にもGDPRが適用されます**。また、ターゲティング広告を配置した自社サイトに対して、EU域内からアクセスがあった際もGDPRの適用対象となる可能性があります。GDPRに違反した場合はかなり重い制裁金が課されるため、適切な対策が求められます。

GDPRに向けた対策例

GDPRでは、Cookieが「個人情報」とみなされるため、WebサイトでCookieを利用する際は、Webサイト閲覧者からCookie取得の同意を得る仕組みを構築することが必要です。Cookieについての本人の同意を取得するには、企業とユーザーとの間で個人データの利用における同意の実施・管理を行うツール（CMP）を導入することが推奨されています。

コラム

“デジタルトランスフォーメーション”と“デジタル化”の関係について

テキスト内では、国の方針や計画を解説する中で”デジタルトランスフォーメーション”という言葉が随所に出てきます。それと同時に、 ”デジタル化”という言葉もあります。両者は異なる定義の言葉ですが、無関係なものではありません。

“デジタルトランスフォーメーション”は、データとデジタル技術を活用してビジネスモデルを変革し、新たな価値を創出することを指します。

”デジタル化”に含まれる概念には、「デジタイゼーション」と「デジタライゼーション」があります。本テキストの用語集”デジタル化”に説明がありますが、デジタイゼーションはアナログや物理的な情報をデジタル化すること、デジタライゼーションはビジネスプロセスをデジタル化することを意味します。
紙で管理していた情報をシステム上に入力することでデータをデジタル化すること、紙資料で行っていたプレゼンテーションをタブレットで行うようにすることなどがデジタイゼーション、それにより業務のやり方が変化し、効率化されるなどの変化がデジタライゼーションです。

“デジタルトランスフォーメーション”は、デジタイゼーション、デジタライゼーションといった”デジタル化”の先にあるものです。”デジタル化”により課題をクリアした後に、新たな価値を創出することが”デジタルトランスフォーメーション”となります。”デジタルトランスフォーメーション”の実現に向けて、”デジタル化”は不可欠なステップです。

編集後記

セミナー3日目では、国によるデジタル社会に関する方針や政策、デジタル分野での取組みにおけるサイバーセキュリティの位置付けについて解説しました。コロナ禍により日本のデジタル化の後れが露見し、政府の方針にデジタルトランスフォーメーションの推進が盛り込まれ、デジタル庁という行政機関も設置され、デジタル社会の実現に向けて社会全体が急速に変化しつつあります。社会全体がデジタル化していくとともに、あらゆる主体にとってサイバーセキュリティ対策を含むデジタルリテラシーが重要になっていることを認識していただきたいと思います。

本テキストでは、デジタル社会の実現に向けた国の基本方針として「経済財政運営と改革の基本方針2023」と「デジタル社会の実現に向けた重点計画」を、政府が目指しているデジタル社会としてSociety5.0を取り上げ、DXについては事例を交えて中小企業の優位性を解説しました。さらに、サイバーセキュリティについては、NISCの「サイバーセキュリティ戦略」などを紹介するとともに、DX with Cybersecurityの考え方などを解説しました。デジタルの活用が進むとともに、サイバー攻撃などのサイバーセキュリティのリスクも高まっています。企業は自社のIT活用状況を認識しつつ、必要な知識・スキルを身につけた人材を育成・確保することが必要です。その上で、適切なサイバーセキュリティ対策を実施しなければなりません。次回以降は、実際に組織で活用できるサイバーセキュリティ対策の体系や基準について詳しく解説していきます。

引用文献

経済財政運営と改革の基本方針2023　加速する新しい資本主義～未来への投資の拡大と構造的賃上げの実現～

https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2023/2023_basicpolicies_ja.pdf

デジタル社会の実現に向けた重点計画

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf

Society5.0

https://www8.cao.go.jp/cstp/society5_0

情報通信白書 令和2年版

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.pdf

サイバー・フィジカル・セキュリティ対策 フレームワークVer1.0

https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.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2.0

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

MISSION 3-12 IoT、ビッグデータ、AI、ロボットの活用

https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/212/index.html

製造分野のDX事例集

https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf

サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ

https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf

サイバーセキュリティ2023の概要

https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023_gaiyou.pdf

企業経営のためのサイバーセキュリティの考え方の策定について

https://www.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf

ITおよびサイバーセキュリティに関する組織の視点6分類別に実施すべき対策

https://www.cybersecurity.metro.tokyo.lg.jp/security/docs/Sec01-11-02.pdf

ITおよびサイバーセキュリティに関する組織の視点６分類

https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/205/index.html

デジタルスキル標準ver.1.1 2023年8月

https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf

引用文献

「プラス・セキュリティ知識」とは？

https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf

サイバーセキュリティ経営ガイドラインVer2.0付録Fサイバーセキュリティ体制構築・人材確保の手引き
～ ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第1版

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

「個人情報保護法」をわかりやすく解説 個人情報の取扱いルールとは？

https://www.gov-online.go.jp/useful/article/201703/1.html

参考文献

目的や所属・役割から選ぶ施策一覧

https://security-portal.nisc.go.jp/curriculum/

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、5-2-1、5-2-2、5-2-3、6-1-1

■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、6-1-3

■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

■DFFT
Data Free Flow with Trustの略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している
…… 5-2-1

■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

■eKYC
electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと
…… 5-2-1

■GビズID
行政手続などにおいて手続を行う法人を認証するための仕組み。1つのID・パスワードで本人確認書類なしで様々な政府・自治体の法人向けオンライン申請が可能になる
…… 5-2-1

■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、5-2-1

■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、5-2-2、5-2-3、6-1-2

用語集

■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

■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、今後情報家電などで大量に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。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

■NISC
National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当
…… 5-2-1、6-1-3

■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

■OSS
Open Source Softwareの略。利用者の目的を問わず、誰でもソースコードの使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称。
…… 6-1-1

■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。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

■SBOM（エスボム）
Software Bill of Materialsの略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOMは、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOMは、ソフトウェアのリスクを把握・管理するのに役立つ
…… 6-1-1

用語集

■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

■Society5.0
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

■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などを客観的に調査・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

用語集

■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、5-2-2、6-1-3

■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

■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、5-2-1、6-2-1

■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、個人など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、5-2-2、5-2-3、6-1-1、6-1-2、6-1-3

■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、5-1-1、6-1-1

■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、5-1-1、5-2-2、6-1-1、6-1-2、6-1-3

■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

用語集

■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、6-1-3

■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、6-1-1、6-1-3

■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、ネットワークなどを含む）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

■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などの操作を、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など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

■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、6-1-2

■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

用語集

■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

■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、5-1-1、6-1-1、6-1-3

■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、5-2-2、5-2-3

■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

用語集

■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などに関する法律（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、5-2-1

■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

■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

■ミラサポコネクト
ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤
…… 5-2-1

用語集

■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、スマートフォンなど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