将来の脅威に対応できる ISMS 構築のエッセンス

～クラウドセキュリティに役立つ ISO 規格～

2022 年 6 月

JIPDEC
一般財団法人日本情報経済社会推進協会

目 次

1 はじめに

情報セキュリティマネジメントを適切に行うには、情報（資産）に係るリスクを特定し、リスクに対して様々な検討を行うことから始まります。また、リスクはその組織の目的・方針によって変わってくることから、まず最初にリスクを特定する上で組織がもつ情報セキュリティの目的を再確認することが必要になります。

もとより、情報セキュリティマネジメントシステム（ISMS）の要求事項であるISO/IEC 27001:2013（JIS Q 27001:2014）[1]の「0.1 概要」では、「ISMS の採用は，組織の戦略的決定である。組織の ISMS の確立及び実施は，その組織のニーズ及び目的，セキュリティ要求事項，組織が用いているプロセス，並びに組織の規模及び構造によって影響を受ける。影響をもたらすこれらの要因全ては，時間とともに変化することが見込まれる。」とあり、「ISMS を確立し，実施し，維持し，継続的に改善する」ことが、時間とともに変化する環境において、情報セキュリティリスクを最適化し、最大限の利潤を得ることを目的として策定されています。

JIPDEC は、2002 年度の「ISMS 適合性評価制度」開始※以来、その普及活動に注力しています。認証取得事業者及び認証機関の積極的な取組みの結果、本制度の下で現在約 6900 の組織が ISO/IEC 27001 に基づく ISMS 認証を受けており、情報セキュリティの重要な制度として広く普及するに至っています。

一方、我が国におけるデジタル化を通じた事業拡大や新事業進出といったビジネスモデルの変革（デジタル・トランスフォーメーション：DX）は、まだ始まったところであり、一般企業における普及はこれからという状況です。DX の足かせとして、情報セキュリティ分野における人材不足があるとも言われており、ISMS の適切な運用は、DX の推進にも役立つことが期待されます。

そこで、本書では ISO/IEC 27001 をはじめとした ISMS に関する国際規格を活用して情報セキュリティの目的を再確認し、ISMS の計画（セキュリティ計画）に役立て、組織に応じたリスクベースの情報セキュリティを実現するための考え方や方法を示すことにより、DX の推進にも役立てることを目指します。

※2018 年 4 月に「一般社団法人情報マネジメントシステム認定センター（ISMS-AC）」を関連法人として設立し、認定事業を ISMS-AC に移管した。

2 目的に沿った運用にするには

2.1 ガバナンス

情報セキュリティという言葉が注目され始めた頃には、情報セキュリティの目標はまず他社がやっていることを全てやるということでした。その中でビジネスに必要な、特に調達に必要だと言われる認証などを取得することが当初の目標だった組織も多かったと考えられます。

まずは、組織として、様々なガイドラインや認証に利用されるクライテリアを実施することで、必ずしも自社にフィットしない場合があったとしても、情報セキュリティとは何かを体感してきたケースもあったことでしょう。

しかしながら、このような黎明期から 20 年以上が経過し、現在は、自社のビジネスにフィットした情報セ

[1] **ISO/IEC 27001:2013** Information technology - Security techniques - Information security management systems - Requirements （**JIS Q 27001:2014** 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項）。JIS 規格は、ISO 規格の内容を変更することなく日本語に翻訳して発行された国内規格。

キュリティマネジメントが必要になってきたと考えている経営者や情報セキュリティ責任者は少なくないようです。外部からの要請によって取り組んだ情報セキュリティマネジメントを自社のために生かしていこうと考えることは自然な考え方と言えるでしょう。

組織には、トップマネジメントの方針に基づいて設定された、それぞれの事業目標があるはずです。この事業目標を実現するために、デジタル技術を活用するのは当たり前のようになっています。

例えば、商品をオンラインで販売したいとした場合、EC サイトを自ら立ち上げたり、外部事業者が提供するサービスを活用します。どちらの方法を選択するのが良いかについて、利害関係者（例．顧客、規制当局）のニーズや期待を理解した上で、自社のやりたいことが実現できるかどうか、また競争優位性を得るための独自機能を実装できるかなどを検討します。そして、この EC サイトを利用した年間の売り上げ目標などを設定し、デジタル技術を利用することによるメリットを検討するのではないでしょうか。

しかし、EC サイトにはさまざまなセキュリティの懸念もあります。全てを完璧にすることはできないかもしれませんが、自らが許容できる範囲内にリスクを抑えるために、組織における役割や責任、権限を明確化した上で、セキュリティ対策を検討することが重要です。セキュリティにかかるコストは IT の実装・運用費として捉えることができますので、目標の売り上げからその分を差し引くことになります。そのため、これらの経費が売り上げに大きな影響を与えないようにしなければなりません。

また、リスクに対して過大なセキュリティの機能を実装し業務を複雑化することによって、デジタル技術によって期待していたシステムの利便性が損なわれる可能性があります。その結果、生産性が低下するのであれば、それも売り上げに大きく影響し、事業目標の達成を妨げる結果となるでしょう。

つまり、自社に必要かつ十分なセキュリティ対策を超えた過度な管理策を取り入れることによるデメリットを、事業目標から差し引いて考える必要があるということです。このように、セキュリティ対策はコストであるということを考慮しながら、個々の対策の費用対効果を検討し、組織としての説明責任及び事業目標達成の観点から優先順位付けをしなくてはならないということです。

適切に優先順付けをしてセキュリティを実装することは、このコストを投資とすることにつながります。リスクを特定し最小化するための情報セキュリティ対策を実装することで、顧客からの信頼を得て売り上げに貢献するという考え方が重要です。事業の DX を推進して新たなサービスを展開する際に、サービスの品質面だけでなく、セキュリティの側面に対しても適切に対応することで、初めて顧客から信頼を得られる時代です。そのため、セキュリティ対策へ投資することが、市場での優位性を維持することにもつながり、社内の業務全般の統制（ガバナンス）にも役立ちます。

これが、トップマネジメントのリーダーシップ及びコミットメントの下で、事業を前提としたセキュリティ計画を策定する時の基本的な考え方です。その上で、セキュリティに関わる組織内外の利害関係者に向けたコミュニケーション計画を策定する必要があります。

このような企業環境の変化を踏まえて発展してきたのが、情報セキュリティガバナンスの概念及びそれに

基づくISO/IEC 27014[2]です。本規格の対象者には、組織の経営陣及びトップマネジメントが含まれており、情報セキュリティガバナンスプロセスの運用に関して、双方の責任が明記されている点が特徴です。そして、情報セキュリティガバナンスが遵守すべき法規制には、個人情報保護／プライバシー関連法令も含まれます。経営陣／トップマネジメントに対しては、組織全体レベルの視点から、情報セキュリティと個人情報保護／プライバシー双方の取組みを把握しながら調整・支援する役割が求められます。

2.2 リスクマネジメント

リスクマネジメントを行う際、ビジネスに対する影響評価を行うことなく、コンプライアンス（準拠性）としてのベースラインアプローチを実施することがあります。この手法は、ISO/IEC 27002[3]などで提供されるベストプラクティスと呼ばれるセキュリティ対策が実施できているかどうかを判断し、対策ができていない場合、比較的容易に導入しやすい「とりあえず」的な対策は何かなどを、組織のビジネス環境やIT環境を反映せずにセキュリティ対策を安易に実装してしまいがちです。ひとたび実装してしまえば、対策は施されたものと理解し、継続的に改善することもなく、リスクマネジメントの本来の目的であるビジネスに影響を与える可能性があるリスクを特定し、それらが受容基準を上回る場合は、継続的に対策を施し、リスクを最適化するといったスパイラルアップが実現できないことがあります。

このような中で、クラウドサービスの利用などが前提となっている現在では、自組織におけるIT環境の変化にリスクマネジメントの考え方が追いつかず、クラウドサービスの利用に対する不安を払拭できていないのが現状ではないでしょうか。

クラウドサービス固有の対策を記載したISO/IEC 27017[4]を参照すると分かるように、クラウドサービスに対する管理策も従来の情報システムに対する対策（ISO/IEC 27002）も、同じセキュリティ管理目的に対する管理策が記載されていて、クラウドサービス特有のリスクが存在する場合、それらのぜい弱性に対応するための新たなセキュリティ対策が紹介されています。クラウドサービスを利用する際には、必要に応じてこれらを適用し、クラウドサービスの提供又は利用に対するリスクを最適化する必要があります。

また、2022年2月に発行されたISO/IEC 27002改訂版では、最新の情報システム環境を反映した管理策の内容となっており、データや情報の安全な廃棄において暗号化消去（Cryptographic Erasure）やデータの機密性を保護するためにデータをマスキングし、匿名化するなどを推奨しています。

---

[2] **ISO/IEC 27014:2020** Information security, cybersecurity and privacy protection - Governance of information security
ISO/IEC 27014:2020は、2020年12月に発行された（2022年4月に修正版発行）。JIS規格としては、旧版の「**ISO/IEC 27014:2013** Information technology - Security techniques - Governance of information security」対応である「**JIS Q 27014:2015** 情報技術―セキュリティ技術―情報セキュリティガバナンス」が発行されている。

[3] **ISO/IEC 27002:2022** Information security, cybersecurity and privacy protection - Information security controls
ISO/IEC 27002:2022は、2022年2月に発行された。JIS規格としては、旧版の「**ISO/IEC 27002:2013** Information technology - Security techniques - Code of practice for information security controls」対応である「**JIS Q 27002:2014** 情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」が発行されている。

[4] **ISO/IEC 27017:2015** Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services（**JIS Q 27017:2016** 情報技術―セキュリティ技術―JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）

情報セキュリティにおけるリスクマネジメントとは、(1)世の中に存在する関連脅威を正しく認識し、(2)その脅威に対するぜい弱性が組織の中に存在するかを判断し、(3)影響を許容できる範囲になるまで軽減するための対策を実施することです。もちろんシステム環境などが変われば、脅威が顕在化する可能性は変化しますし、そのシステム環境に新たなぜい弱性が発見されることもありますので、これらのプロセスは継続的に実施しなければなりません。ISO/IEC 27001 は、リスクマネジメントに基づきそうした対策を実施するための仕組み（ISMS）について記載しており、適切にリスクマネジメントを実施するのに役立ちます。

では、適切なリスクマネジメントを実施するとはどのようなことでしょうか。

例えば、脅威が特定できず、その脅威の発生の原因となるぜい弱性についても正しく理解できない場合（ゼロディ攻撃など）には、その脅威に対する予防策を実装することができません。適用可能なセキュリティ対策としては、組織や情報システムを脅かす「異常」を速やかに検知し、素早い対応をするといったインシデント対応のための対策を実施するほかありません。また、最近のランサムウェアのように「脅威」が特定できた場合でも、ゼロディ攻撃同様、攻撃にあった被害者からの情報提供が少なく、いつ、どのようにして感染したか、また感染した際、対象となるぜい弱性について適切に把握することができない場合もあります。ランサムウェアに対しては、「見知らぬ者からのメールは開封しない」などの予防策も存在していますが、信用に足るパートナーのシステムに侵入し、アカウント情報などを詐取し、そこからランサムウェアを送付する攻撃も知られており、「メールを開封しない」といった予防策にも限界があります。また、ランサムウェアが侵入すると、侵入されたことを検知したとしても、侵入された端末やサーバのシステムファイル等が暗号化され、即座に保存していた情報やアプリケーションが利用停止に陥ります。そのため、ランサムウェアに対する対応策としては、事故を前提とし、利用停止に陥った情報やシステムを復旧させるためのバックアップを取得しておき、そのバックアップからシステムや情報をリストアし、可能な限り、障害があった前の状態に現状を復帰させることが推奨されています。

Coffee Break

セキュリティ対策において、バックアップは、インシデントが発生する前に取得する必要があるので、「予防」のための対策では？と思うかもしれません。

広義の意味合いにおいては、「予防」にせよ、「復旧」にせよ、重要な概念ですので、その重要性をご認識いただければどちらでも構わないですが、狭義の意味においては、バックアップは、インシデント前に取得するものであっても、「復旧」としての対策であり、「予防」ではありません。

予防策とは、本来、攻撃などに対するぜい弱性を最小化することが目的の対策ですが、バックアップを取得しても、攻撃に対するぜい弱性は残留し、最適化されないためです。一方、「復旧」とは、インシデントからの影響を最適化するものであり、バックアップからリストアをする行為は、これにあたります。

例えば、クラウド上にあるバックアップからリストアする場合には、外部に実施を依頼することで、情報漏洩のリスクが高まることに気を付ける必要があります。緊急時に対応するための適切な準備も整えておくことが重要です。

一方、事前にバックアップを取るといっても、対象となる情報システムの決定やバックアップを採取する頻度、インシデントが生じた場合、どのシステムを優先的に復旧させるのか、データをリストアし、システムが復旧するまでにどの程度時間がかかるのか、復旧するまでの間、どの程度のビジネス機会を喪失するのか、などの事業継続管理、可用性管理を考慮した計画を策定しておくことが重要です。

適切にリスクマネジメントを実施するとは、組織のビジネス環境や IT 環境を考慮したうえで、リスクを特定し、そのために必要な「予防」、「検知」、「インシデント対応」、「障害からの復旧」に最適な対策を施し、リスクを最適化することです。

ISO/IEC 27002 では「予防」に必要なセキュリティ対策だけではなく、「検知」「インシデント対応」「障害からの復旧」などの運用に不可欠なセキュリティ対策も記載されていますので、これらを参考にしながら、運用を前提としたセキュリティ対策（セキュリティ・バイ・デフォルト）の実装について計画し、継続的な改善に繋げることを推奨します。

また、このためには、ISO/IEC 27001 でも触れているようにビジネスの影響を十分に理解し、セキュリティ対策の優先順位づけを行うことも重要です。また、データ、デバイス、アカウント、サービスなどの全ての資産において、ぜい弱性が存在していないかを定期的に、可能であればリアルタイムに把握することができるような仕組みづくりも重要です。

DX を通じて、資産をデジタル化することにより、その構成をリアルタイムに把握することができるようになれば、組織内のぜい弱性の有無を瞬時に認識できるようにもなります。

2.3 運用時の注意事項

組織におけるセキュリティガバナンスやリスクマネジメントを進める際、運用時に特に注意すべき事項を以降に示します。

(1)経営陣の認識不足の解消

セキュリティ対策において、経営陣の果たすべき役割はますます高まっています。

組織におけるセキュリティガバナンスやリスクマネジメントを考える際、クラウドサービスの提供や利用における責任分担への理解が欠かせません。特に、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）等の経営陣が責任分担のモデルを正しく理解し、自組織及びステークホルダーがどのようにセキュリティ対策をすべきかを認識したうえで、事業を推進することが重要です。

経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0」では、「自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要」としています。サプライチェーンの中では、ビジネスパートナーに一方的に責任を求めるのではなく、自らの責任を的確にとらえて実施し、加えてビジネスパートナーにも働きかけを行うなど、相互利益・相互理解に努めることが求められます。

また、JIPDEC「ISMS ユーザーズガイド -JIS Q 27001:2014（ISO/IEC 27001:2013）対応 -リスクマネジメント編-」では、経営陣のリスクマネジメントの力量不足により、経営的な視点が欠けたリスク基準が策定されてしまうことも指摘しています。自組織を取り巻く経営環境の変化を、セキュリティガバナンスやリスクマネジメントの取組みに適時に取り入れることが重要です。

(2)新たなぜい弱性を狙った脅威に対抗できる柔軟な運用

運用フェーズでのサプライチェーンを含めたリスクマネジメントの活動は、環境変化に伴う新たなぜい弱性を狙った脅威に対抗するために必須な取組みです。例えば、クラウド上に新たなシステムを構築した際に、クラウド環境に不慣れな管理者が適切な設定を行えず、情報漏えいや情報喪失につながるケースが散見されます。そうした取組みの際には、新たなぜい弱性に対して追加の対策を考えるのみにとどまらず、費用対効果の高いベストプラクティス等を優先的に適用し、効果が薄くなった無駄なプロセスを取り除くことが大切です。

セキュリティガバナンスやリスクマネジメントは、ISMS 構築・運用の活動の中で、PDCA サイクルを回して定期的な見直しを行うことを基本としています。JIPDEC「ISMS ユーザーズガイド – JIS Q 27001:2014 （ISO/IEC 27001:2013 対応）」においても、ISMS の構築における PDCA モデルの採用や、運用フェーズにおけるリスクマネジメントの適時実施の必要性を示しています。

ISO/IEC 27014 や ISMAP[5]管理基準でも、セキュリティガバナンスの構築において、変化をモニタリングして必要な是正処置を行うことを求めています。その際、自組織のみならず、ステークホルダーを含めたサプライチェーン全体で取り組むことが重要です。

(3)DX 推進とセキュリティ対策

DX 推進とセキュリティ対策は、相反するものではなく、推進力の両輪として位置づけるべきでしょう。

DX 推進により、クラウド等を活用した新たなサービスの提供や利用が増えています。そうした取組みは組織内の様々な部署で個別に実施されてガバナンスが利かなくなった結果、ぜい弱性対策が不十分で予期せぬサービス停止を招いたり、不適切な取扱いにより個人情報が漏えいするといったケースが散見されます。

DX 推進における新たなサービスの提供においては、IT サービスに関する ISO/IEC 20000-1[6]をもとにトップマネジメントによるサービスマネジメントの方針を確立し、サービスのライフサイクルを通じて ITSMS（IT サービスマネジメントシステム）を構築し、ステークホルダーを含めたガバナンスを適切に行うことが重要です。JIPDEC「ITSMS ユーザーズガイド-JIS Q 20000-1:2020（ISO/IEC 20000-1:2018）

[5]**ISMAP :** 政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program）国際標準等を踏まえて策定したセキュリティの基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、クラウドサービスを登録する制度。政府機関は、「ISMAP クラウドサービスリスト」に掲載されたサービスから調達を行うこと原則とする。

[6]**ISO/IEC 20000-1:2018** Information technology - Service management - Part 1: Service management system requirements（**JIS Q 20000-1:2020** 情報技術―サービスマネジメント―第 1 部：サービスマネジメントシステム要求事項）

対応-」では、ITSMS は ISMS と統合して構築することで、SLA（Service Level Agreement）の一環としてセキュリティ対策が実施できることを示しています。また、DX 推進における新たなサービスの利用においては、個人情報に関する JIS Q 15001[7]や ISO/IEC 27701[8]に基づく制度等を活用し、個人情報の適切な管理が求められます。

一方、組織が求めるセキュリティ対策が複雑化していると、その対応に係るコストや作業負荷が足かせとなって、DX 推進のための新たなサービスの提供や利用を阻害しかねません。効果が薄くなった従来型のセキュリティ対策にこだわらず、新たなベストプラクティスを積極的に導入して、セキュリティ対策をシンプルに保つことが大切です。

3 効果的な仕組みづくりのために ～ISMS 適合性評価制度の活用～

2 章で紹介した ISMS に沿ったリスクマネジメントを構築することによって、情報セキュリティ対策のための仕組みを作り、必要な対策を実装・運用して、環境の変化に合わせて改善することができます。また、ISMS 適合性評価制度を活用して、第三者である認証機関から、客観的な評価を受けることによって更なる改善につなげるとともに、顧客や取引先に対して適切に情報セキュリティ対策を実施していることを示すことも可能になります。

現在、本制度の下で、約 6900 の組織が ISO/IEC 27001 に基づく ISMS 認証を受けています。また、本制度では、通常の ISMS 認証に加えて、クラウドサービス固有の情報セキュリティ対策を適切に実施しているかを審査・認証する ISMS クラウドセキュリティ認証も行われています。詳細は、(一社)情報マネジメントシステム認定センター（ISMS-AC）の Web サイトを参照してください。

なお、ISMS 構築や認証等に関する詳細やガイド等（本書でも紹介した ISMS ユーザーズガイド等も含む）は、JIPDEC の Web サイトから参照できます。

- ISMS-AC の Web サイト：https://isms.jp/
- JIPDEC の関連 Web サイト：https://www.jipdec.or.jp/project/smpo.html

※ ISMS 適合性評価制度：組織が ISO/IEC 27001 という国際標準に準拠して情報セキュリティを管理する仕組みを導入しているかを第三者機関が審査・認証する制度で、ISMS-AC が運用しており、ISMS 認証機関や ISMS 認証取得組織の一覧等を公開しています。

[7] **JIS Q 15001:2017** 個人情報保護マネジメントシステム―要求事項
[8] **ISO/IEC 27701:2019** Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines

4 おわりに

本書では、情報セキュリティの目的の意義を再確認し、組織に応じたリスクベースの情報セキュリティを実現することによる効果について説明しました。また、ISO/IEC 27014 を通じて、情報セキュリティガバナンスの考え方や同規格の「7.2.2　目的 2 ：リスクに基づく取り組みを使用して意思決定を行う」について説明すると同時に経営陣の「認識欠如」にかかる課題について解説しました。

また、情報セキュリティマネジメントにかかる部分においては、リスク低減に欠かせない「管理策」である、ISO/IEC 27002 の動向や ISO/IEC 27017 について説明し、クラウドサービスの利用者の立場であっても、その「利用」に対する役割や責任を認識し、日々変化する環境やサービス自体の SLA に対するリスクを見直し、最新の管理策を導入することが、DX に対しても重要な役割を担うことを説明しました。

最後に、DX 推進における新たなサービスの提供を、特に、クラウドサービスを介して展開される事業者にとっては、構築するサービスの開発～リリースまでの「品質管理」を担うマネジメントシステムである ISO/IEC 20000-1 を紹介するとともに、開発当初から顧客や利用者情報を含む情報セキュリティの概念や対策を盛り込み、開発中又は運用中に競って出現する様々な課題や問題にインシデント対応を含む体制づくりに、培ってきた情報セキュリティ人材等をリソースとして活用し、人材不足を補い、サービスの信頼性を高めることが、まさに DX、すなわち、デジタル化の導入により事業をより良く変革し、市場競争上の優位性を確立する目的に望ましい態勢として、本書をまとめました。

本書で紹介したクラウドセキュリティに役立つ ISO 規格は全体の一部に過ぎませんが、クラウドサービスに関連する ISO 規格が ISO/IEC 27001 を基盤とし、他の規格やガイドラインも ISO/IEC 27001 との整合性が図られています。また、超スマート社会の情報インフラは、巨大なクラウド群と無数のセンサ（バイオセンサなどを含む）、アクチュエータ等で構成された IoT 機器群から成ると考えられ、各国の国際レベルの組織でこれらの規格を参照して進められています。本書が、クラウドサービスの安全性や品質を高めるうえで役立ち、また、クラウドサービスを活用し、情報の利活用としての DX が広く定着するようになれば幸いです。

今後は、クラウドサービスにおいては、その継続性（導入後の安定した運用）も重要であり、事業継続のためのマネジメントシステムを定めた ISO 22301 やプライバシーを保護するための要求事項である ISO/IEC 27701 なども検討していく所存です。

最後に、ISMS 専門部会の委員、関係者の皆様に対しては、本書の作成、レビューのために多くの時間を費やしていただいたことに、この場を借りて厚くお礼を申し上げます。

一般財団法人日本情報経済社会推進協会（JIPDEC）
ISMS 専門部会主査　駒瀬 彰彦

ISMS 専門部会

（順不同・敬称略）

氏名	会社・機関名
委員	
【主査】 駒瀬　彰彦	株式会社アズジェント
相羽　律子	株式会社日立製作所
河野　省二	日本マイクロソフト株式会社
笹原　英司	一般社団法人日本クラウドセキュリティアライアンス
佐藤　慶浩	オフィス四々十六
澤部　直太	株式会社三菱総合研究所
中村　良和	日本マネジメントシステム認証機関協議会 （BSI グループジャパン株式会社）
オブザーバ	
星　昌宏	一般社団法人情報マネジメントシステム認定センター（ISMS-AC）

JIPDEC
〒106-0032 東京都港区六本木１丁目９番９号 六本木ファーストビル
一般財団法人 日本情報経済社会推進協会
TEL 03-5860-7561　FAX 03-5573-0561
URL https://www.jipdec.or.jp/