

レポート

中堅・中小企業の実践的セキュリティ対策

～対策の選択と集中～

コンサルティング事業本部
デジタルイノベーションビジネスユニット デジタルビジネスコンサルティング部
マネージャー 庄田智祐

1. はじめに

企業活動における IT サービスへの依存度は年々高まっている。基幹システムや人事給与システム、クラウドストレージなど、多くの業務が IT サービスの活用が前提となっている。そのため、IT サービスが停止すれば受注や購買などの事業活動に深刻な影響を及ぼしかねない。とりわけ、中堅・中小企業は「IT サービスへの依存度は高まる一方で、セキュリティに十分な人員や予算を割けない」という構造的な課題を抱えている。大企業と比べて組織規模や収益規模が小さく、予算や人材が不足していることが、その背景にある。

独立行政法人情報処理推進機構 (IPA) の「情報セキュリティ 10 大脅威 2026」では、組織向け脅威の第 1 位がランサム攻撃による被害、第 2 位がサプライチェーンや委託先を狙った攻撃、第 3 位が AI の利用をめぐるサイバーリスク、第 4 位がシステムの脆弱性を悪用した攻撃となっている。連続で選出されている項目が多い中、3 位の AI の利用をめぐるサイバーリスクは 2026 年に初めて選出された【図表 1】。このように、情報セキュリティにおける脅威の様相は、技術の進化や社会の変化によって徐々に変化していく¹。

¹ 独立行政法人 情報処理推進機構 「情報セキュリティ 10 大脅威 2026」(2026 年 5 月 21 日)
<https://www.ipa.go.jp/security/10threats/10threats2026.html>(最終確認日:2026/10/07)

【図表 1】情報セキュリティ 10 大脅威 2026 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い (2016年以降)
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

(出所) 独立行政法人 情報処理推進機構「情報セキュリティ 10 大脅威 2026 [組織]」

一方で、中堅・中小企業が大企業と同じようにセキュリティ人材や予算を確保し、新たな脅威が現れるたびに網羅的なセキュリティ対策を講じることは理想ではあっても現実的ではない。

IPA も「中小企業の情報セキュリティ対策ガイドライン」を第 4.0 版へ改定した背景の一つとして、「中小企業等の内部でセキュリティ対策を推進する人材の著しい不足」²を挙げている。こうした制約の下では、「網羅的なセキュリティ対策」を行うのではなく、対策範囲の選択と集中が必要となる。また、セキュリティツールの導入やセキュリティ管理規程の整備、社員へのセキュリティ教育など複数の対策を別々の施策として扱うのではなく、複数の対策を連動させながら機能する一連の仕組みとして設計しなければならない。

また、どれほど強固な対策を実施してもインシデントを完全に防ぐことは不可能である。人的ミスや未知の脆弱性、取引先におけるインシデントなど、完全にはコントロールできないリスクが常に残るためである。したがって、インシデントは起こりうるものという前提³に立ち、予防的対策だけではなく、インシデント発生後の早期検知や早期復旧までを見据えた対策を講じる必要がある。

こうした現状を踏まえ、本レポートでは中堅・中小企業におけるセキュリティ対策として、形骸化させず機能し続ける仕組みづくりと、インシデント発生後の準備・対応について論じる。その中でも特に、「事業に直結する領域に対策を集中し、その対策を継続的に機能させる」という選択と集中・継続性の視点を主眼とする。

² 独立行政法人 情報処理推進機構「プレス発表『中小企業の情報セキュリティ対策ガイドライン』第 4.0 版を公開」(2026 年 3 月 27 日)
<https://www.ipa.go.jp/pressrelease/2025/press20260327.html> (最終確認日:2026/10/07)

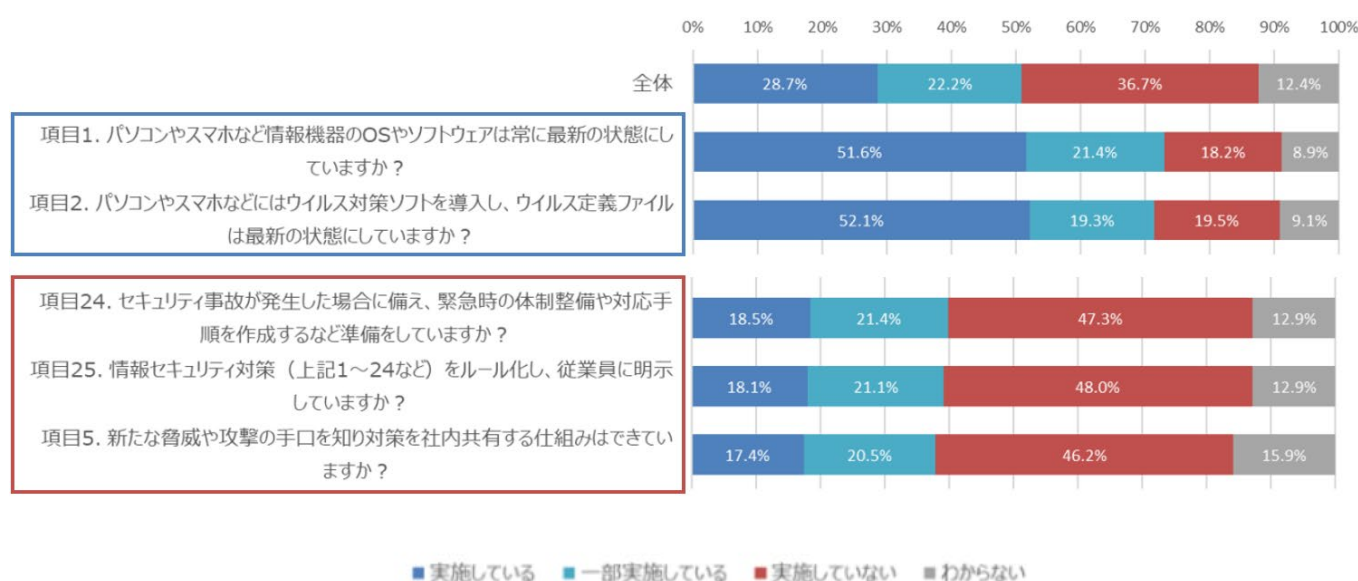
³ 独立行政法人 情報処理推進機構「情報セキュリティ 6 か条(解説編)p17」(2026 年 9 月 30 日)
<https://www.ipa.go.jp/security/guide/sme/about.html> (最終確認日:2026/10/07)

2. 中堅・中小企業の現状と課題

IPA が 2025 年 5 月に発表した全国 4,191 社の中小企業を対象とする情報セキュリティ対策に関する調査では、OS・ソフトウェアの最新化は 73.0%、ウイルス対策ソフトの導入・最新化は 71.4%が「実施している」または「一部実施している」と回答した。一方で、緊急時の体制や対応手順の整備を「実施している」または「一部実施している」企業は 39.9%、情報セキュリティ対策をルール化して従業員に明示する取り組みは 39.2%、新たな脅威や攻撃手口を把握し社内共有する仕組みは 37.9%にとどまった⁴。

【図表 2】中小企業における情報セキュリティ対策に関する実態調査に関する設問と回答

「自社診断」25 項目の実施状況 (n=4,191)



(出所) 独立行政法人 情報処理推進機構『2024 年度 中小企業における情報セキュリティ対策に関する実態調査』報告書
について」より一部抜粋

【図表 2】のとおり、中小企業では OS・ソフトウェアの最新化やウイルス対策ソフトの導入に比べ、緊急時対応体制やルールの整備、脅威情報の共有といった「運用面の対策」が十分とはいえない。すなわち、中小企業ではセキュリティ対策ツールの導入など、目に見える対策は実施できているものの、実際にインシデントが発生した場合の対処手順や体制が機能せず、適切に対応できないリスクが示唆される。

例えば、ウイルス対策ソフトや EDR (Endpoint Detection and Response) などのセキュリティ対策ツールを導入しても、それらから発出された警告を「いつ・誰が確認し」「どのような条件で端末を隔離し」「どこへ報告するか」の初動対応が決まっていなければ、十分な効果を発揮できない。また、業務データのバックアップを取得していても、復旧手順が明示されていないければ、迅速かつ適切に復旧できない可能性がある。

⁴ 独立行政法人 情報処理推進機構『2024 年度 中小企業における情報セキュリティ対策に関する実態調査』報告書について」(2025 年 5 月 27 日) <https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html> (最終確認日: 2026/10/07)

情報セキュリティのルール化についても同様である。セキュリティ管理規程そのものが存在していても現場の担当者には内容が十分に周知されていないケースや、業務変化に伴う規程の見直しが放置され規程の内容と実際の業務運用に乖離が生じるケースなど、類似の事例は数多く存在する。この背景には、各種規程が作成時で止まり、その後に必要不可欠となる社員へのセキュリティ教育や遵守状況の確認、環境変化を踏まえた規程の改定手順までを含めた一連の運用として設計されていない点がある。これでは、規程があっても運用の実効性は期待できない。

つまり、セキュリティ対策の有効性を確認するためにはセキュリティ対策ツールや規程の有無にとどまらず、現在の業務に即した内容になっているか、内容が社員に周知され、浸透しているか、定期的に更新されているかなども含めた評価が欠かせない。

3. 優先すべき6つの対策

前述のとおり、中堅・中小企業ではウイルス対策ソフトの導入のような比較的分かりやすい技術的対策に比べ、セキュリティ管理規程の整備やセキュリティ教育、インシデント発生時の対応手順の整備など、対策を組織ぐるみで機能させる点に遅れが生じている。

こうした「ツール導入は進んでいるが、運用面の対策が不十分」という現状に鑑みれば、中堅・中小企業が限られた資源の中で優先すべき対策領域は必然的に絞られる。重要になるのは、対策範囲を無制限に広げることではなく、事業への影響が大きく、かつ対策効果の高い領域を特定し、そこへ経営資源を優先配分することである。限られた条件下で最大の効果を得るためには、次の6つの対策を優先することが有効だと考えられる【図表3】。

【図表3】中堅・中小企業が優先すべき6つのセキュリティ対策

No.	対策名	主な目的	具体例(概要)
1	情報資産の可視化	重要な情報資産の把握・分類	資産管理台帳の作成・重要度評価
2	管理規程の整備と定着化	ルール策定と現場への浸透	規程策定・教育・理解度確認
3	アカウント・権限の適正化	不正アクセス防止と被害範囲の抑制	最小権限付与・多要素認証導入
4	侵入経路の遮断	攻撃の入り口の削減	パッチ適用・不要な公開サービス閉鎖
5	復旧手段の確立	インシデント発生後の早期復旧	バックアップ取得・復旧テスト実施
6	インシデント対応体制の整備	オペレーションの確立によるインシデントへの早期対応	手順書整備・訓練・連絡体制整備

(出所) 当社作成

(1) 情報資産の可視化

第一に、情報資産管理台帳(以下、資産管理台帳)を用いた情報資産の把握・分類である。保有する情報資産と管理責任を明確にした上で、インシデント発生時の影響範囲を特定する。その上で、機密性・完全性・可用性などの観点から情報資産の重要度を判定し、対策を検討する。まだ情報資産を整理できていない企業は、IPAの「中小企業の情報セキュリティ対策ガイドライン第 4.0 版」の付録の一つである「資産管理台帳」⁵の活用を推奨する。初めて資産管理台帳を作成する場合は、すべての資産を一度に洗い出す網羅性を求めず、「主要な業務システム」「クラウドストレージ」「共有フォルダ」のように、事業への影響が大きい領域から対象を絞り込むのが現実的である【図表 4】。

【図表 4】資産管理台帳のサンプル

業務 分類	情報資産名称	備考	利用者 範囲	管理 部署	管理者名	管理者連絡先	媒体・保存先	評価値				保存 期限	登録日
								機密性	完全性	可用性	重要度		
人事	社員名簿	社員基本情報	人事部	人事部	〇〇〇	090-XXXX-XXXX	事務所PC	3	1	1	3		2026/4/1
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	〇〇〇	090-XXXX-XXXX	書類	3	3	2	3	5年	2026/4/1
経理	給与システム データ	税務署提出用 源泉徴収票	給与計 算担当	人事部	〇〇〇	090-XXXX-XXXX	事務所PC	3	3	2	3	7年	2026/4/1
経理	当社宛請求書	当社宛請求書の原本 (過去3年分)	総務部	総務部	△△△	090-XXXX-XXXX	書類	2	2	2	2		2026/4/1
共通	電子メールデータ	Gmailに転送	担当者	総務部	△△△	090-XXXX-XXXX	社外サーバー	3	3	3	3		2026/4/1
営業	顧客リスト	得意先(直近5年間に 実績があるもの)	営業部	営業部	×××	090-XXXX-XXXX	可搬電子媒体	3	2	2	3		2026/4/1
営業	顧客リスト	得意先(直近5年間に 実績があるもの)	営業部	営業部	×××	090-XXXX-XXXX	モバイル機器	3	2	2	3		2026/4/1
営業	受注契約書	受注契約書原本(過去 10年分)	営業部	営業部	×××	090-XXXX-XXXX	書類	2	3	2	3		2026/4/1
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	×××	090-XXXX-XXXX	社内サーバー	1	2	2	2		2026/4/1

(出所) 独立行政法人 情報処理推進機構「資産管理台帳」より一部抜粋

(2) 管理規程の整備と定着化

第二に、情報資産の取り扱いやインシデント対応手順などを含めたセキュリティ管理規程の整備である。規程の形骸化を防ぐ鍵は、継続的な社員に対する周知や定期的な教育である。また、各部署における業務内容や環境の変化に応じて規程を見直せるような仕組みを構築する。さらに、社員の理解度や遵守状況をテストや研修などによって確認し、理解度が低い内容についてはフォローアップを行うことが重要である。

(3) アカウント・権限の適正化

第三に、アカウント・権限の適正化である。具体的には、退職者や異動者などの不要なアカウントの即時停止・適切な権限付与、一般利用者と管理者のアカウントの分離、社員や委託先への必要最小限の権限付与が挙げ

⁵ 独立行政法人 情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン第 4.0 版 付録 6: 資産管理台帳(サンプル)」(2026 年 9 月 30 日) <https://www.ipa.go.jp/security/guide/sme/about.html> (最終確認日: 2026/10/07)

られる。また、メール、VPN、主要なクラウドサービス、管理者アカウントなど、不正利用された場合の影響が大きい経路から優先して多要素認証を導入する。これは不正アクセス防止だけではなく、万が一アカウントが不正利用された際に被害の範囲を最小限に食い止める上でも有用である。

(4) 侵入経路の遮断

第四に、侵入経路の遮断である。OS やウイルス対策ソフトだけでなく、VPN やファイアウォール、外部へ公開しているサーバなどについても脆弱性情報を定期的に確認し、必要な更新を実施する体制を整える。また、利用していない外部公開サービスは速やかに閉鎖する。これによって、悪意ある第三者が不正に利用可能な入口を抑制し、サイバー攻撃の被害に遭うリスクを低減していく。

(5) 復旧手段の確立

第五に、インシデント発生を想定した復旧手段の確立である。業務データのバックアップは取得すること自体ではなく、インシデント発生後に速やかに業務が再開できるかが重要である。そのためには、バックアップデータを使った復元手順を整理した上で、実際に復旧テストを実施して所要時間を把握する必要がある。さらに、ディスク容量の不足などによりバックアップの取得が失敗するケースもあるため、定期的なログの確認も欠かせない。

また警察庁は、ランサムウェアによってバックアップデータが暗号化される事例が多数確認されていることから、ネットワークから切り離してオフラインで保存するなどの対策を推奨⁶している。

(6) インシデント対応体制の整備

最後に、インシデント対応体制の整備である。インシデントは発生し得るものと捉え、その検知、隔離、報告、影響範囲の特定など、復旧に至るまでの一連の流れを「インシデント対応手順」として整備する。この中では、「誰が検知するか」「誰に報告するか」「誰がネットワーク遮断などによる隔離を判断するか」「対外的な連絡は誰が担うか」といった役割分担まで具体的に定めておく。

併せて、インシデント発生後に初めてセキュリティの専門家を探すのではなく、平時から支援先と連絡体制を確保しておくことも重要である。警察庁はランサムウェアへの備えとして、被害を想定した訓練の実施や、関係者の連絡先やバックアップ復旧手順などの事前確認を推奨⁷している。インシデント対策は手順書の作成のみならず、インシデントを想定した訓練を定期的に行って常日頃から改善に努めることで、より高い効果を発揮する。

⁶ 警察庁 「ランサムウェア被害防止対策 ランサムウェア被害を想定した備え バックアップを取得する」
<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html> (最終確認日:2026/10/07)

⁷ 警察庁 「ランサムウェア被害防止対策 ランサムウェア被害を想定した備え 被害を想定した訓練を行う」
<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html> (最終確認日:2026/10/07)

4. 対策の運用と改善

前述の対策は、一度きり、あるいは一定期間で完了するものではない。情報資産は新規システムやクラウドサービスの導入によって増減し、組織変更や人事異動によって必要なアクセス権限も変動する。業務で生成 AI の利用が始まれば、それに伴う規程や教育内容の見直しが必要となる。つまり、セキュリティ対策は「導入」や「整備」といった一度きりの活動ではない。導入した対策を運用し、実際に機能しているかを点検し、見つかった問題を改善するサイクルを継続的に回すことが重要である。ここで注意すべき点は、対策が「存在すること」と、対策が「運用できていること」を混同しないことである。

資産台帳やセキュリティ管理規程の整備やバックアップデータの取得、EDR の導入、インシデント対応手順書の作成などは、対策の枠組みが存在するにすぎず、それだけではインシデント時に運用できる保証にはならない。実効性のある対策とするためには、項目ごとにポイントを押さえて確認することが有効である【図表 5】。

【図表 5】6 つの対策と確認事項

6 つの対策	対策別の確認事項
1. 情報資産の可視化	資産管理台帳を定期的に更新しているか
	資産管理台帳の記載内容と実際の管理状況が一致しているか
2. 管理規程の整備と定着化	セキュリティ管理規程を定期的に見直し、社員へ周知しているか
	セキュリティ管理規程に関する社員の理解度と遵守状況を確認しているか
3. アカウント・権限の適正化	アカウントや権限を定期的に見直しているか
	人事異動などのタイミングで遅滞なく権限を見直しているか
4. 侵入経路の遮断	OS やソフトウェア、各種サービスの脆弱性情報を定期的に確認し、セキュリティパッチを適用しているか
	利用していない外部公開サービスがあれば遅滞なく閉鎖しているか
5. 復旧手段の確立	バックアップの取得状況を定期的に確認しているか
	バックアップからの復旧テストを実施しているか
6. インシデント対応体制の整備	インシデント時の役割分担や外部支援先への連絡体制などの対応手順が整備されているか
	インシデント訓練を定期的の実施し、想定通り社員が動けることを確認しているか

(出所) 当社作成

さらに、こうした状態を定量的に把握するため、資産管理台帳の更新状況、バックアップ復旧テストの実施結果、教育・訓練の受講率や理解度など、少数の指標を定めて定期的にモニタリングすることも有効である。重要なのは、指標の数を増やすことなく、対策が現在も機能しているかを観測し、検知した課題は改善につなげることである。事業内容や IT 環境、脅威が変化し続ける以上、セキュリティ対策に終わりはなく、対策もまた絶えずアップデートする必要がある。この継続的な改善こそが、限られたリソースの中でセキュリティの有効性を維持するための鍵となる。

5. 選択と集中

前章では、対策を「整備して終わり」ではなく、運用・点検・改善する仕組みとして維持することの重要性を述べた。一方で、すべての情報資産やシステムに対して同水準で対策していくことは、リソースが限られる中堅・中小企業にとっては現実的ではない。仕組みを適用する対象範囲をどこまで広げ、どこに重点配分するかという「選択と集中」の視点も欠かせない。

限られた経営資源を優先すべき領域に集中させるため、各資産について、(1)事業影響性、(2)外部露出性、(3)侵害波及性、(4)復旧困難性という4つの観点から対策の優先順位を判断する【図表6】。

【図表6】4つの観点と優先度の判断

判断の観点	判断の内容	優先度の判断軸	優先度が高い例
(1) 事業影響性	システムや情報資産が停止・漏えいした場合、売上・信用・法的責任などにどの程度影響するか	影響が大きいほど、対策の優先度を高くする	受注・出荷・決済など、停止すると事業活動がまひする基幹システム／大量の顧客情報を扱うデータベース
(2) 外部露出性	インターネットなどの外部から直接アクセス可能か、攻撃対象になりやすい構成か	露出が大きいほど、侵入防止・監視などの対策を優先する	社外公開している Web サーバ／外部ネットワークから利用される VPN・クラウドサービス
(3) 侵害波及性	一つのアカウントやシステムが侵害された場合、どこまで影響が広がるか	影響範囲が広いほど、権限管理や権限の分離などを優先して強化する	管理者権限を持つアカウント／複数システムを連携・制御しているシステム
(4) 復旧困難性	インシデント発生後に、どれだけ早く・どれだけ容易に元の状態へ戻せるか	復旧が困難なほど、事前のバックアップ・代替手段などの対策を優先する	古いオンプレシステムで代替手段がない／設定やデータの復旧に多くの手作業が必要なシステム

(出所) 当社作成

この4つの観点をを用いることで、「他社もやっているから」といった受動的な理由ではなく、自社の事業リスクを起点とした合理的な優先順位付けができる。例えば、外部公開されておらず停止時の影響も小さいシステムと、インターネットからアクセス可能であったり、停止すると主要業務の停止に直結したりするシステムを同じ優先度で扱う必要はない。また、すべての対策を内製化する必要もない。24時間体制の異常監視やログの解析など、専門性の高い業務は外部の専門機関を活用できる。IPAの「中小企業の情報セキュリティ対策ガイドライン第4.0版」でも、社内の人手・知識が不足する場合は「適切な異常監視、インシデント対応を実施するために、外部のセキュリティサービスを導入⁸⁾」することが推奨されている。ただし、自社にとっての重要業務の選定や、インシデント発生時に許容できる停止時間、何を優先して再開するか判断は、経営そのものであり外部へ委ねられない。つまり、専門作業は外部から調達できても、どのリスクを受け入れるかという経営判断まで外注することはできない点は留意しなければならない。

⁸⁾ 独立行政法人 情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン第4.0版 付録1: 中小企業のためのセキュリティ人材の確保・育成の実践ガイドブック p.8」(2026年9月30日) <https://www.ipa.go.jp/security/guide/sme/about.html> (最終確認日: 2026/10/07)

6. おわりに

中堅・中小企業のセキュリティ対策において重要なことは、単に多くの製品やツールを導入することではなく、守るべき対象と優先順位を明確にし、自社にとって必要な対策を絞り込み、それらを確実に機能させる仕組みを構築することである。具体的に取り組んでいく際は、本稿で提示した情報資産の可視化、管理規程の整備と定着化、アカウント・権限の適正化、侵入経路の遮断、復旧手段の確立、インシデント対応体制の整備の 6 つの対策を中心に検討し、環境の変化に合わせて継続的に改善していくことが効率的である。

人材や予算が限られているからこそ、対策を絞り込み、優先順位をつけ、それらを途切れさせずに機能させることが、中堅・中小企業にとって現実的なセキュリティ強化につながる。限られた資源の中で「事業を守るために必要な対策を選び抜き、それを継続的に機能させること」が実効性のある防衛策となるだろう。

【関連資料】

[【資料ダウンロード】「情報セキュリティ診断サービス」](#)

【関連サービス】

[サイバーセキュリティ](#)

－ ご利用に際して －

- 本資料は、執筆時点で信頼できるとされる各種データに基づいて作成されていますが、当社はその正確性、完全性を保証するものではありません。
- また、本資料は、執筆者の見解に基づき作成されたものであり、当社の統一的な見解を示すものではありません。
- 本資料に基づくお客さまの決定、行為、およびその結果について、当社は一切の責任を負いません。ご利用にあたっては、お客さまご自身でご判断くださいますようお願い申し上げます。
- 本資料は、著作物であり、著作権法に基づき保護されています。著作権法の定めに従い、引用する際は、必ず出所:三菱 UFJ リサーチ&コンサルティングと明記してください。
- 本資料の全文または一部を転載・複製する際は著作権者の許諾が必要ですので、当社までご連絡ください。