経済産業省

参考資料A: 打ち手のリスト

主要な打ち手のカテゴリー

凡例：組 組織的措置
法 法的措置
技 技術的措置

モニタリング

リスク発生の疑い・予兆を把握	組 法規制を起因とした予兆の把握（政策の検討情報等） 組 企業を起因とした予兆の把握（不審な挙動等）
リスク発生の有無を把握	組 リスク発生件数・実績の把握（法の執行件数、企業内発生件数等）

事前対応

リスク発生確率を下げる・予防	組 ガイドライン策定、保管場所・サービス選定、代替データ・業務等 法 データ取扱いに関する契約の締結 技 アクセス制限や持ち出しの制御、不正アクセスの防止
発生時のインパクトを低減	組 ガイドライン策定、説明責任・透明性の確保 法 データ取扱いに関する契約の締結 技 データの保護・暗号化

事後対応

保護措置、責任追及	組 リスク発生のインパクト把握、初動対応 法 契約・法令に基づく保護措置・責任追及
再発の防止	組 社内業務、取引先、利用サービスの見直し 法 契約の見直し 技 技術的措置における課題の把握、対応の見直し

打ち手・対応措置のリスト：モニタリング 1/2

凡例：組 組織的措置
法 法的措置
技 技術的措置

分類1	分類2	打ち手の対象	主な打ち手（例）
リスク発生の疑い・予兆を把握	組 法規制を起因とした予兆の把握	自社	（特に立法段階において）法規制への検討として、規制内容と施行時期を把握する • 自社・現地子会社の法務部へ問い合わせる • 各国の政府機関・シンクタンクのウェブサイトを活用・参照する（各国省庁・JICA等） • コミュニティ内で情報交換・収集を行う（産業団体等） • 政府・立法機関が主催する検討ウェビナー、意見収集イベントに参加する • 専門家（法律事務所等）に相談する （特に施行後において）規制内容の変更、今後の更新予定を確認する • 同上
	組 企業を起因とした予兆の把握	自社	自社内でのリスク予兆を確認・モニタリングする • PC・デバイスの異常な挙動を検知する、ログを確認する - 通常使用しないIPアドレス・デバイスから/へのアクセス、ネットワークトラフィックの異常、ファイルの大量ダウンロード及びアップロード、ログ削除・変更の履歴等 • 情報取り扱いポリシーの順守状況、従業員の労働状況等を確認する - 資料の回収・処分、アクセス・投影の制限、私物USB・メモリの持ち込み・利用制限等 - 勤務時間外の頻繁な入退出や、業務量に対して異様に長い残業の発生等
		取引先/サービス提供者	取引先/サービス提供者におけるセキュリティ水準を確認する • 取引先/サービス提供者における、提供データの取り扱いポリシーを確認する - 保管方法（ロケーション、仕組み）とその機密性、データのアクセス権、公開範囲等 • 取引先/サービス提供者におけるデータ保護措置の実施状況を確認する（認証取得の有無等） 取引先におけるリスク予兆を確認する • 取引先に対して、定期的な報告を依頼する - 情報の保管状況、データの共有・利活用のステータス、廃棄の報告等 - 提供データの取り扱いポリシーの変更有無と、想定される影響等

打ち手・対応措置のリスト：モニタリング 2/2

凡例：組 組織的措置
法 法的措置
技 技術的措置

分類1	分類2	打ち手の対象	主な打ち手（例）
リスク発生の有無を把握	組 法の執行件数・実績の把握	自社	関連法規制に関して、執行の有無・実績を確認する • 自社・現地子会社の法務部へ問い合わせる • コミュニティ内で情報交換・収集を行う（産業団体等） • 専門家（法律事務所等）に相談する 裁判が行われた場合に、判例内容を確認する • 各国の裁判所の情報を確認する • 専門家（法律事務所等）に相談する
	組 企業におけるインシデント件数・実績の把握	自社	自社におけるインシデント件数を確認する • インシデント件数として、社内データ利活用の規範に対する違反、従業員による不正アクセス・漏洩の件数等を集計・共有する
		取引先/サービス提供者	取引先/サービス提供者におけるインシデント件数を確認する • 契約に対する違反、従業員による不正利用・漏洩件数等について、報告を受け、発生状況を確認する

打ち手・対応措置のリスト：事前対応[1] 1/3

凡例：組 組織的措置
法 法的措置
技 技術的措置

分類1	分類2	打ち手の対象	主な打ち手（例）
リスク発生確率を下げる・予防	組 ガイドライン策定	自社	自社におけるデータ共有・利活用のガイドライン・ポリシーを定義する • 秘密情報の定義・判断、アクセス範囲、データの取り扱い・公開範囲等 国際データガバナンスに対する社内認識を高める • ガイドライン・ポリシーの周知（社内規定、研修等）
	組 保管場所・サービスの選定	自社	データ保管場所及び、重要データの所在を把握する • 重要データごとに、その社内・社外保管場所や、機密性・セキュリティ水準を確認する リスクが懸念されるデータに関して、保管場所及び、提供先・サービス提供者の見直し・選定を行う • リスクが低いと想定される保管場所、サービスを選定する • 特定国でガバメントアクセスが懸念される場合に、ガバメントアクセスの対象とならないように、特定国へのデータ移転を制限する 重要データを分散化させる、複数拠点で保持する • （越境移転自体が制限されていない場合は）国内外複数拠点にデータを複製し、分散して保持する
	組 代替データ・業務の検討	自社	特定データの利用が制限された際に、特定データなしでの業務を検討する • 代替データを活用する • 業務プロセスにおいて特定データを使うプロセスを省略もしくは簡略化する
	組 法規制の要望、例外措置への準拠・対応	自社	法規制の要望事項を確認し、適宜対応の判断を行う • 要望事項を確認する（ローカルデータセンターの設立、国内での運営体制の構築等） • 技術・人材・コスト面での実現可能性を考慮した上で、事業メリット・必然性を踏まえ、対応有無を判断する 例外措置が存在する場合に、要求・条件に準拠する • 例外措置の条件を確認し、対応する（条件付きの越境移転規制等）

1. ガイドライン策定等データマネジメントに係る「事前対応」については、独立行政法人情報処理推進機構（IPA）の「Data Spaces Academy」にて読本・ガイド等の資料を公開しているため、本マニュアルの補足情報として参照されたい。https://www.ipa.go.jp/digital/data/data-spaces-academy.html

打ち手・対応措置のリスト：事前対応 2/3

凡例：組 組織的措置
法 法的措置
技 技術的措置

分類1	分類2	打ち手の対象	主な打ち手（例）
リスク発生確率を下げる・予防	法 契約の締結	自社	従業員との秘密保持契約を締結する • 秘密・機密情報を取り扱う従業員と秘密保持の契約を締結したり、誓約書の提出を要請する（入社時、退職・契約終了時、在職中の移動時等）
		取引先	取引先とデータの取り扱い・利用に関する契約を締結する • データの取り扱い条件や権限に関して、契約を締結する（秘密保持義務/利用対象データの範囲・目的/監査対応/派生データ・知財権の扱い/データ範囲制限等） - 項目の詳細について「AI・データの利用に関する契約ガイドライン[1]」や「データ連携基盤規約Ver.1.0[2]」（経済産業省）において、ひな形となるモデル規約等を参照 • （データ開示の義務化に対して）機器販売者の立場から、機器の販売先に対して第三者開示の範囲や、データ取得・提供の権利・条件等を合意する • （データローカライゼーションにおいて）複数の国の越境移転規制に準拠した条項を組み込んだIntra Group Data Transfer Agreement（IGDTA）がないか確認し、活用を検討する
		サービス提供者	サービス提供者とデータの取り扱い・利用に関する契約を締結する • データの取り扱い条件や権限に関して、契約を締結する（データ加工の対象、加工方法/加工者の制限/加工データの利用権、知財権等）
			プラットフォーム（PF）サービスの利用規約を確認・定義する • PFサービスにおけるデータ利用範囲（データ種類ごとの共有先設定・管理）、PF事業者義務・責任、データ受領者側の義務・権利等を確認する

1. https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pdf
2. https://www.meti.go.jp/policy/mono_info_service/digital_architecture/model_kiyaku.pdf

打ち手・対応措置のリスト：事前対応 3/3

凡例：組 組織的措置
法 法的措置
技 技術的措置

分類1	分類2	打ち手の対象	主な打ち手（例）
リスク発生確率を下げる・予防	技 アクセス制限・持ち出しの制御	自社	システムごとにアクセス制限・制御を設定する • 特定システムとそのデータに対して、アクセス権の管理、ネットワーク・トラフィックの制御、ログ確認・監視・通知等を行う ユーザーIDにアクセス権を付与する、適切なアクセス者の識別・認証を行う • IDへのアクセス権付与によって、特定システムを操作できる従業者を限定する • アクセス者の識別と認証を行う（パスワード、ICカード等）
	技 不正アクセスの防止	自社	外部からの不正アクセスを検知・遮断する • 外部ネットワークとの接続箇所に対するファイアウォールを設置 • 機器におけるOS・ソフトウェアの更新、最新状態の維持 • ログ等の定期的な分析の実施
発生時のインパクトを低減する	組 ガイドライン策定	自社	発生時の社内エスカレーション先・対応アクションを整理する • 発生を検知した際に、社内における連絡窓口を明確にする • 事象ごとの詳細確認先と、対応責任・アクションを定義する • 社外のステークホルダー・説明先と、その連絡先・方法を定義する
	組 説明責任・透明性の確保	自社	外部ステークホルダーに対する透明性を確保する • 自社の情報管理体制、準拠している法令・規制等について、発信・周知する
	法 契約の締結	取引先/サービス提供者	取引先/サービス提供者に対して、リスク発生時の責任及び対応・補償について契約で合意する • ステークホルダーの責任範囲・違反時のペナルティ、紛争解決の方法、ガバメントアクセス等、法的要請がかかった際の対応方法等について合意する
	技 データの保護・暗号化	自社	暗号化によって、外部者がデータを利用できない状況にする • 電子透かし技術を用いたデータの出所等を明示する • 暗号鍵、暗号化技術を用いたデータの保護を行う • データの匿名加工を行う

打ち手・対応措置のリスト：事後対応 1/2

凡例：組 組織的措置
法 法的措置
技 技術的措置

分類1	分類2	打ち手の対象	主な打ち手（例）
保護措置、責任追及	組 リスク発生のインパクト把握、初動対応	自社	発生したリスクの実態を把握する • ガイドライン・社内定義に沿って責任・対応部署を明確にする • データのログ解析、データ流出経路を確認する • リスクによる損害・事業影響の解析・把握を行う
			顧客、取引先等の主要ステークホルダーに対して通知・説明を行う • 早期に発生事項・日時の通知、公表を行う • 適宜発生内容の詳細や、その影響範囲について、詳細説明を行う（顧客・株主説明会等）
	法 契約・法令に基づく、保護措置・責任追及	自社	社内で違反に対する処置を行う • 社内規定もしくは秘密契約に基づく、違反時の処置・処分を行う
			法令に基づく保護措置を要求する • 当該国・地域における保有権利を確認する（関連法規制における保護措置、知財法等） • 当該国が合意する国際ルールとの整合性を確認する（WTO協定、経済連携協定等）
		取引先/サービス提供者	取引先/サービス提供者に対して、契約に基づく保護措置・責任追及を行う • 契約内容に対する違反の通知を行う • 契約内容に沿った、回復措置の要請、賠償の申し立てを行う

打ち手・対応措置のリスト：事後対応 2/2

凡例：組 組織的措置
法 法的措置
技 技術的措置

分類1	分類2	打ち手の対象	主な打ち手（例）
再発の防止	組 社内業務、取引先、利用サービスの見直し	自社	社内業務を停止する、変更する • 対象業務に対して、リスク発生の原因を明確化する • 対象業務に対して、業務を停止する、またはリスクを回避するための確認項目や業務プロセスを検討する（データ送付先の２重チェック等） 利用サービスを停止する、変更する • 代替サービスがないか確認し、入れ替えた際のコスト・品質を比較する 取引先に対するデータ提供範囲・方法を見直す • 自社が取引先に対してデータを提供する方法、範囲を見直す 取引先における再発防止に対する要請を行う • 取引先におけるセキュリティ水準の向上、情報管理・報告の徹底等、再発防止策の検討を要請する • 再発防止策の実施状況、経過について報告を受ける
	法 契約の見直し	自社	社内ガイドラインを見直す • リスク発生要因・内容を踏まえた、社内ガイドラインに新しい条項を付記する
		取引先/サービス提供者	取引先・サービス提供者に対する契約を見直す • リスク発生要因・内容を踏まえた、取引先・サービス提供者との契約事項の見直しを行う
	技 技術的措置における課題の把握、対応の見直し	自社	技術的措置の検討、対応の見直し • リスク発生要因、及び社内におけるシステム、データの管理状況の把握 • 適切な技術的措置の検討、現状対応の見直し（アクセス制限・持ち出しの制御、不正アクセスの防止、データの保護・暗号化等）