マンパワーグループ グローバル本社の 情報セキュリティポリシー

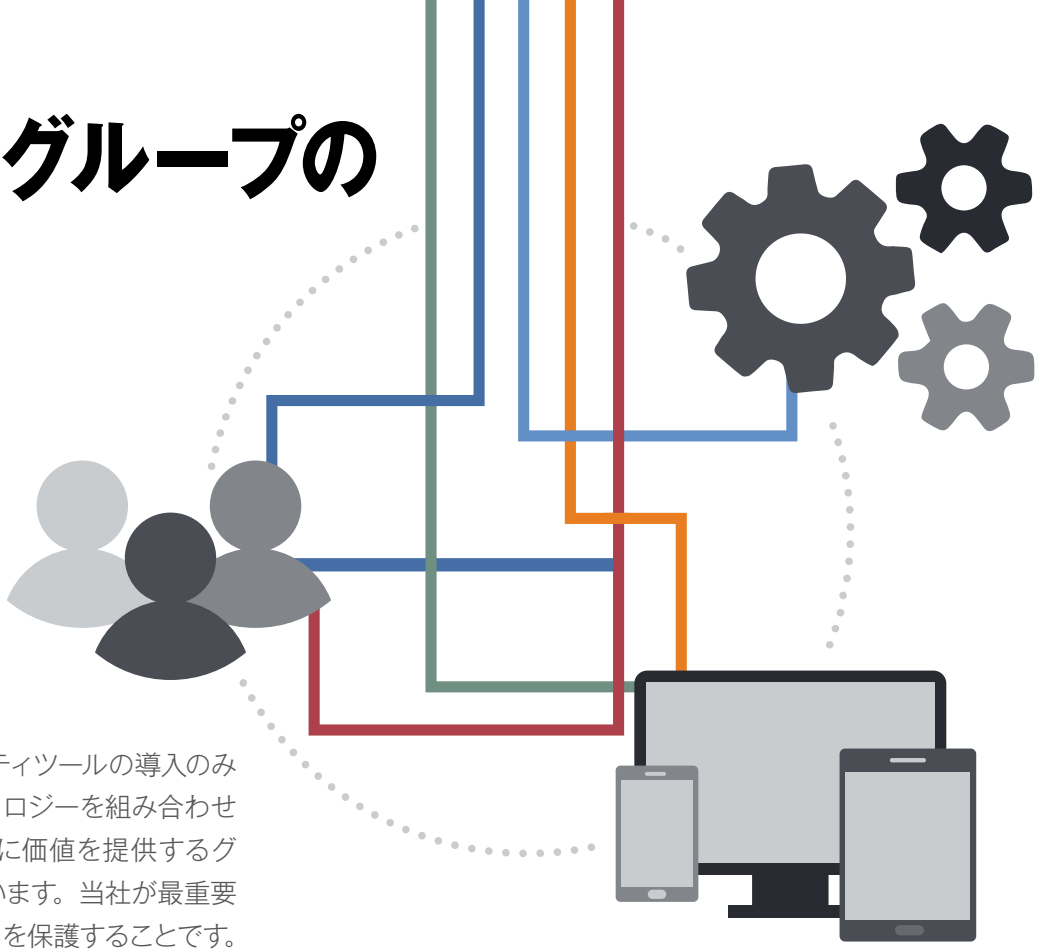
現代のビジネス環境：迅速なデジタルトランスフォーメーション

この数年、サイバー犯罪の深刻度と頻度が高まるとともに、その影響が大きくなっています。リモート環境での業務遂行とデジタル化が急速に進むことで、企業は情報セキュリティに一層注力しなければならなくなりました。ビジネス責任者とセキュリティ責任者は迅速な業務スピード、卓越した障害対応、規制対応の強化を実現しなければなりません。

テクノロジーの発展がもたらす最新ツールの導入やデータ活用・分析を通じて、当社はクライアントおよびアソシエイト、キャンディデイトに高い価値を提供していきます。また、その中で、当社に提供された情報を適切に管理する社会的責任を果たしていきます。情報セキュリティの管理は、従業員、クライアント、アソシエイト、キャンディデイト、そして協力会社から当社が信頼され、透明性を実現するための必須条件です。同時に、サイバー攻撃の頻度が高まり、より巧妙化していることを受け、危機感を持って関係者の意識を高めていかねばなりません。

ランディー・L・ヘロルド
マンパワーグループグローバル本社
最高情報セキュリティ責任者 兼 最高プライバシー責任者

マンパワーグループの基本原則



情報保護にはリスク評価が必要不可欠です。当社の情報セキュリティならびにプライバシー保護プログラムは、セキュリティツールの導入のみに終始せず、人・プロセス・テクノロジーを組み合わせてリスクを削減し、クライアントに価値を提供するグローバルフレームワークを掲げています。当社が最重要視するのは、当社に託されたデータを保護することです。

当社の「職務行動倫理規範」には、高い情報セキュリティとデータプライバシー保護に関わる当社の決意を記載しています。20 カ国語で提供されるこの規範は全従業員と共有され、世界中のステークホルダーにも公開されています。

人

- セキュリティを守る最も重要なポイントは、ツールやプラットフォームではなく全従業員です。
- データ保護のポイントは、情報の保存場所、システム連携、取得から廃棄までの「情報のライフサイクル」全体を通して、「誰が」情報にアクセスしているかを正確に把握することです。
- 例えば、金融サービス情報共有分析センター（FS-ISAC）のような実践モデルの共有とセキュリティ機能の強化に役立つパートナーと連携することで、セキュリティの脅威に対する包括的な見識を得ています。

プロセス

- セキュリティの管理を担う情報セキュリティチームを設置し、当社の情報システムがビジネス要件、法的要件、規制要件を満たすよう管理しています。
- セキュリティ上の対応状況・応答時間をモニタリングし、迅速に対応できるよう体制を整えています。

テクノロジー

- 攻撃防止のテクノロジーだけでは巧妙な攻撃は阻止できない時代がきています。それを受けて、攻撃を素早く検知し、被害を最小化するために迅速に対応するテクノロジーを備えています。
- 特権アクセスの管理機能に重点的に取り組むことで、認証情報の詐取を防止します。

人

当社が保護すべき最も重要なこと、
それはクライアント、アソシエイト、キャンディデイト、従業員

マンパワーグループが提供するサービスは、社内外にさまざまな影響を及ぼします。クライアント、アソシエイト、キャンディデイトからビジネス上の機密データを託されているので、我々は果たすべき責務を認識しています。当社のグローバルプライバシーポリシーでは、当社が収集する個人情報の使用目的、情報の共有先、提供・利用などを拒否できる選択肢について規定しています。プライバシーポリシーは国ごとに策定されており、グローバル基準を満たしつつも各国の法令を遵守しています。

経営陣が率先してセキュリティに取り組む

当社の情報セキュリティの原則は、経営陣からのトップダウンでセキュリティ管理体制を構築し、深刻な被害をもたらすセキュリティ脅威に対処することにあります。グローバル本社の最高情報セキュリティ責任者（CISO）は四半期ごとに取締役会の監査委員会と会合を持ち、セキュリティ戦略と投資プロジェクトの進捗を検証しています。CISO の指揮のもと、グローバルセキュリティプログラムの責任をエグゼクティブメンバーが担っています。

ガバナンスを実現する重層的なアプローチ

CISO は、本ポリシーとコンプライアンスの遵守状況を定期的に取締役会に報告し、さらにエグゼクティブメンバーにも定期的に最新情報を提供しています。当社の情報セキュリティプログラムが最新のセキュリティ脅威に対応しているか、第三者機関によって毎年評価されます。

当社の組織は業務分掌により部門化されていますが、CISO は部門を横断する役割として、ビジネス戦略・連携・管理について直接責任を負います。システム構築、システム運用、ベンダー管理は、CISO の直轄組織が担当しています。

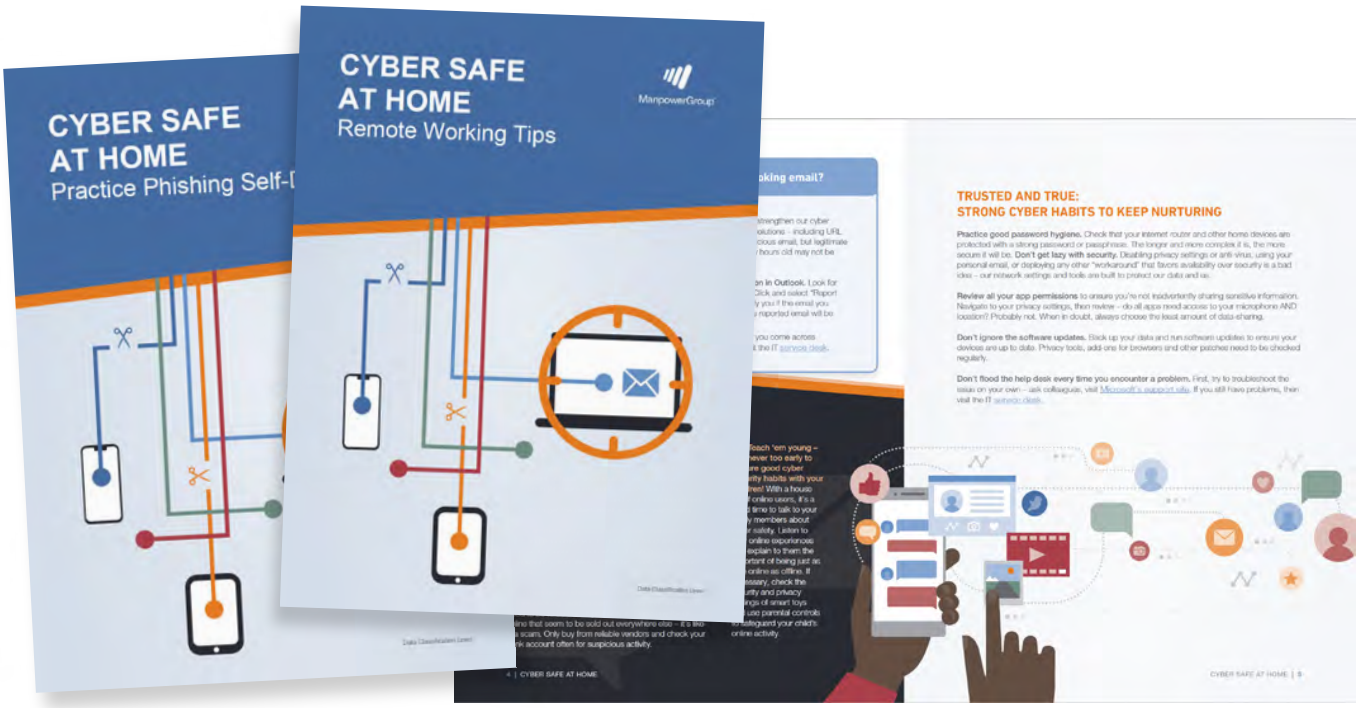
近年、情報セキュリティおよびデータプライバシー専任チームは大幅に拡大しました。グローバル、リージョン、国ごとで戦略的に人材を配置し、一貫したポリシー・プロセス・テクノロジーを提供しています。当社の従業員はスキルを高め、業界の認証資格（CISSP、CISM、CISA、CRISC、CSCP、CCISO、CCSP、CASP、CPDSE、ISO 27001 Lead Auditor、ISO/IEC 27005 Risk Manager、CIPM、CIPP/E、FIP など）を保有しています。

従業員の能力・スキル開発

巧妙なサイバー攻撃を阻止するには、防止型テクノロジーだけでは十分とは言えません。また、セキュリティ脅威に対する最適な防衛策はＩＴツールやプラットフォームではなく、人にあると考えています。

そのため、当社は従業員に向け最新の教育プログラムと意識向上プログラム（オンラインや対面講義の各種トレーニング、定期的なフィッシング防止訓練、全世界で行うサイバー啓蒙イベント、部門単位の啓蒙活動など）を継続的に実施しています。すべてのエグゼクティブメンバーもまた、トレーニングや意識向上キャンペーンに参加しています。これらのトレーニングを通じ、従業員は業務活動で遭遇する「不審な兆候」に対する報告方法を身に付けていきます。例えば、メールソフトにセキュリティ機能を統合することで、ワンクリックで不審なメールを報告できます。また、機密情報や情報システムにアクセスする委託業者にも、当社従業員向けの意識向上トレーニングに参加いただいています。

これらの意識向上プログラムや、CISOと情報セキュリティチームから配信される定期的な注意喚起を通じ、セキュリティ意識の高い組織文化を醸成しています。それによりソーシャルエンジニアリング攻撃に対する防御態勢が毎年強化されていることを、定期調査により確認しています。

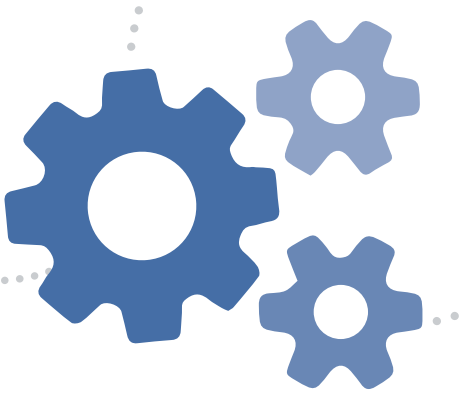


人的・組織的なセキュリティの実施策

マンパワーグループでは、以下の従業員管理項目に「セキュリティの実施策」を組み込んでいます。

- セキュリティ意識向上プログラムにおいて、クライアント、協力会社、従業員がそれぞれどのような情報セキュリティの役割と責任を負っているか定義、文書化し、通知しています。
- 雇用契約締結時に、機密保持契約を締結しています。
- 当社の業務委託先など協力会社にも、情報セキュリティ要件を遵守するよう義務付けています。
- 従業員が最新のセキュリティポリシー、規程、手順書をいつでも閲覧できるよう掲示しています。
- CISO やエグゼクティブメンバーを含む全従業員が、定期的に情報セキュリティ意識向上トレーニングを受講しています。
- 雇用終了時に、業務上で貸与されていた情報資産がすべて返却されたかどうか確認しています。
- 雇用終了時に、当社の情報システムへのアクセス権を削除しています。

プロセス



セキュリティフレームワークの管理

当社は、NIST CSF（米国国立標準技術研究所のサイバーセキュリティフレームワーク）および ISO 27001 規格に準拠したグローバル情報セキュリティフレームワークを構築し、当社の全業務に適用しています。また、文書化されたポリシー・規程・手順書などを従業員に展開し、業務のなかで実践しています。専任担当者を設定し、少なくとも年1回見直しを図っています。さらに、テクノロジーおよび人的作業の検証プロセスを構築し、ポリシーに加えて各種規制要件や契約要件を遵守しています。

業界標準の規格に準拠した情報セキュリティ**ポリシー**

ポリシーの**遵守**

契約要件と法令遵守を**検証**するプロセス

規格に準拠した業務**手順**

プロセスの設計段階でセキュリティを確保

セキュリティの課題解決においてはテクノロジーだけでは不十分です。そこで、当社のすべてのプロセスは重層的なセキュリティ防御を原則としています。あるプロセスがうまく機能しない場合も、後続のプロセスがリスクを補完するよう設計されているのです。セキュリティ制御機能を複数実装し、一元的な監視ソリューションに統合することにより、24 時間 x365 日体制で監視・インシデント対応が実現できています。全プロセスを通じて、*「権限付与は最小限に」*の原則、および*「知る必要のある者のみが情報にアクセス可能」*の原則に基づき、不正アクセスのリスクを最小限とし、攻撃者の侵入拡大を抑制することで、ログイン情報の詐取防止に努めています。

情報セキュリティ分野の業務委託先の監督

当社では、導入したセキュリティツールを最大限に活用できるよう、運用·監視等の日々業務を一部業務委託しています。情報セキュリティの専門家である業務委託先に関しては、契約前に当社のポリシー基準を満たしていることを確認しています。業務委託先は、品質とセキュリティ維持のために SLA（サービスレベルアグリーメント）を満たし、定期監査の対象となります。

業務委託先、協力会社、クライアントなどの外部取引先によってアクセスされる情報資産のセキュリティ保護のために、以下の取り決めを行っています。

- マンパワーグループの有する情報へ外部取引先が「作成・アクセス・保存・転送・処理」する場合、委託内容ごとに定義された情報セキュリティ要件（VISR）を、契約に必ず含むこととする。
- 情報セキュリティ要件を変更するには、CISO または代行者が必ず承認する。
- 外部取引先のビジネスリスクを発見した場合、是正策またはリスク緩和の制御策を必ず求める。
- 機密保持契約書または同等の書面の義務化。
- ビジネス上の必要性がある場合のみ外部取引先にマンパワーグループの情報資産へアクセスを許可する。また、アクセスには当社のエグゼクティブメンバーまたはその代行者が、必ず書面により承認を行う。

ソフトウェア開発ライフサイクル（SDLC）

アプリケーション開発については、明確かつ安全な SDLC プロセスに基づきセキュリティ要件を定義、文書化、テストしています。安全性の高いコーディングを行い、リリースする前にセキュリティ評価を実施します。さらに、開発者向けに安全性の高いコーディングに関するトレーニング資料を提供し、本番環境と非本番環境の間で厳密な職務分掌を実施しています。

リスクの評価

内部環境への対応：

継続的に自社業務を評価し、リアルタイムでセキュリティ施策を実施しています。

1 **データの収集と情報資産の特定**

リスク評価プロセスの第1ステップとして、ビジネスとテクノロジーの各担当者から情報を収集します。テクノロジーに関するエビデンスとテクノロジー以外のエビデンスを示す資料に加え、主要業績指標（KPI）レポートを収集します。

2 **リスクの分析**

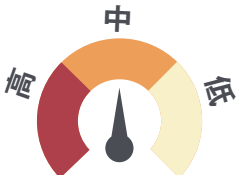
マンパワーグループで定義しているデータ分類基準を活用し、データの重要度、作成・評価・保存・転送・処理の対象となるデータの機密性に基づき、情報資産を分類・ランク付けします。

情報資産を以下の項目に基づいて速やかに分類し、ランク付けしています。

制御機能を定期的に評価し、保護および検知の有効性を確認しています。制御機能は完璧ではないため、一貫性のあるレポートを通じて効果を評価します。物理的な制御機能と技術的な制御機能の両面を評価すると共に、当社と外部取引先のオペレーションの両方を検証対象とし、KPI を用いて改善の必要がある制御機能を特定します。この検証サイクルは継続的に運用されています。

リスク評価プロセスの一貫として、潜在的な脅威と脆弱性を継続的に評価します。

- 脆弱性：情報資産の不正開示、不正利用、変更または破壊を誘引するソリューションや制御機能の弱点
- 脅威：脆弱性によってもたらされる潜在的なアクション・イベント



3 **リスク評価スコアの設定**

最終ステップとして、各情報資産に評価スコア（高・中・低）を設定します。情報資産の量、資産の分類、脅威と脆弱性の評価、および制御機能の妥当性評価を総合的に勘案して評価スコアを設定します。

4 **是正とプロセスの継続**

リスク評価プロセスにおいては、自己評価と是正を常に繰り返し実施します。

外部環境への対応：変化する脅威に対応していく

毎年、独立した外部評価機関がリスク／脅威評価を行い、急速に変化するセキュリティ環境の中で、当社のプログラムの有効性を評価しています。測定基準と KPI とともに、この有効性評価を取締役会に報告しています。さらに、1年を通し、社内外の監査チームによる独自の評価も実施しています。この結果を情報セキュリティチームと共有し、是正策を構築し、セキュリティに関わる運用業務に落とし込みます。

アクセス制御

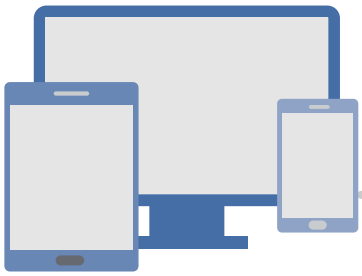
情報保護のために、ビジネス上の必要性に基づき「知る必要のある」データ群にのみアクセスが許可されます。認証情報の不適切な使用防止のために包括的な措置を行います。

- 機密情報へのアクセスに強力な認証を義務付け、全アクセスを監視する
- 「最小権限」の原則に基づき、標準ユーザーレベルとは異なる「独自の認証情報」を発行する
- システムに対し、一定期間アクティビティがない場合、認証情報を無効化する
- 特権 ID が設けられているネットワーク、ハードおよびソフトのすべてを監視する
- ハードウェアベンダーとソフトウェアベンダーが提供する標準アクセス設定を変更する
- 法律、規制または契約に基づき求められるデジタル通信の情報を暗号化する
- 例外なく、リモートアクセスには多要素認証（MFA）を義務付ける

物理的な環境保護

不正な構内侵入・機器破損・業務介入を防止するため、以下のプロセスを実施します。

- ゾーニングと入退室管理を通じて、セキュリティエリアを保護する。
- 紙媒体、顧客貸与の ID 機器、サーバー、ネットワーク、データベース、ストレージ、バックアップなどのすべての情報資産を物理的に保護し、不正アクセスやデータ破損、不正使用から保護する。
- 従業員に離席時の PC ロックを徹底させる。
- 各地域の準拠法、規制および契約要件に基づき、オフィスへの不正侵入を防ぐ。
- 情報の管理・廃棄を行う際は、マンパワーグループの情報管理ポリシーを遵守する。



テクノロジー

アクションの監視とセキュリティイベントの分析

アクションの監視

当社では、全社的なセキュリティ情報イベント管理（SIEM）ソリューションを導入しています。本ソリューションはマンパワーグループのデバイス（IDS/IPS、HIDS、システムイベントログ、ファイアウォールなど）からイベント情報を収集し、セキュリティオペレーションセンター（SOC）で詳細に分析し、悪意の（可能性の）ある挙動を検出します。また、SOC は外部機関での脅威分析から得られる情報を活用し、マンパワーグループの環境で存在する可能性のあるセキュリティ侵害インジケーター（IOC）の検出を行います。

分析と対応

インシデント管理システムを使用して、以下を含むセキュリティイベントを記録・管理します。

イベントの入力

SOC では、報告されたイベントや検出されたイベントを管理システムで管理･更新し、エスカレーションを行っています。

管理

検出された全イベントを管理することで、調査内容を記録し、説明責任を果たし、迅速に問題解決をします。適切な関係者に情報をエスカレーションし、特に法令やクライアントとの契約条件の遵守には、迅速なエスカレーションが必須です。また、根本原因と関係者を特定し、懸念点･問題点の是正を図ります。

是正

懸念点･問題点の是正には、さまざまな部門や関係者の協力が必要となります。情報セキュリティチームが適切な是正策を指示します。

インシデントの解決

必要な是正策・予防策を実施し、リスクを適切なレベルまで低減させたというエビデンスを収集した時点で、インシデントは解決となります。エビデンスの確認には経営陣の承認が必要です。

インシデントの解決後の原因分析

正式にインシデントを解決後、インシデントの包括的な検証（根本原因の分析、報告内容のレビュー、対応プロセスと是正プロセス全般の改善のチャンスの検証など）を実施します。

暗号化

暗号化による制御を通じ、ストレージに保存された機密情報とネットワークを介して転送される機密情報を保護します。防御機能として以下を実装します。

- 暗号化の要件定義を行い、法令と契約要件を満たした暗号化基準を導入する。
- 機密情報を公衆ネットワーク経由で保存・転送する際は、必ず暗号化を行う。
- 当社の IT システムへのリモートアクセスを暗号化する。
- 非標準の暗号化手法を使用する場合は CISO の承認を必須とする。

マルウェア

以下の通り、マルウェアを防止します。

- 定期的な監査により、セキュリティの制御状況を確認する。
- 情報システムを監視し、ログを記録する。
- 情報システムのログを保護し、不正使用・不正アクセスを防止する。
- すべてのハードとソフトを、脆弱性管理プログラム（例えば、マルウェアからの保護、セキュリティパッチ、資産の堅牢化などに関わる業界規格など）の対象とする。
- ワークステーションとサーバーにエンドポイント保護ソフトをインストールし、適切に保守を行う。
- 毎年 1 回以上、社外公開 WEB の脆弱性をスキャンする。
- 定期的に従業員向けの教育啓蒙を実施する。
- WEB やメールシステム上で、技術的にマルウェアをスキャンする。

当社へのお問い合わせ

当社の情報セキュリティポリシーをご覧いただき、ありがとうございます。皆様におかれましてもデータのセキュリティ保護の取組みの強化にご協力をお願いいたします。当社の情報保護への取り組みについてご不明な点があれば、CISO である私までお問い合わせください。また、当社のセキュリティプログラムの詳細情報に関するお問い合わせも受け付けています。マンパワーグループは、今後も皆様のビジネスを支援して参ります。

ランディー・L・ヘロルド
マンパワーグループグローバル本社
最高情報セキュリティ責任者
randy.herold@manpowergroup.com

当社のグローバル情報セキュリティポリシーと取り組みについては、以下をご参照ください。
https://www.manpowergroup.com/sustainability/infosecprivacy

ManpowerGroup®