

ソリューションの概要

IBM Kenexa Talent Frameworks for Information Technology (IT)

組織の成功を導くための業界固有のジョブ・スキル



IBM.

今日、組織内で情報技術 (IT) が果たす極めて重要な役割を考えると、IT 機能全体にわたる適切なスキルと人材の確保は、あらゆる組織の成功に不可欠な要素です。スキルのギャップが IT 機能内に存在すると、運用が非効率的になり、費用が増加するだけでなく、組織全体の成功に重大な影響が生じる可能性もあります。IBM Kenexa Talent Frameworks は、業界に關係するスキル・ギャップの特定、測定、および対処に役立つように設計されています。

IBM のソリューションは、役割ごとに特有な詳細スキルと能力のセットにより、新しいデータ・アーキテクトを惹きつけ、迅速にオンボーディングすることを可能にします。将来のキャリア形成機会の明確な見通しを示すことにより、データ・プライバシーおよびセキュリティーの最高の人材を確保します。また、既存のクラウド統合エンジニアがスキルに特化したコンテンツに取り組むようにすることで、日常のパフォーマンス強化と継続的な育成を推進します。

人とビジネスをつなぐ

IBM Kenexa Talent Frameworks for Information Technology (IT) を使用すると、人材管理のあらゆる側面でジョブとスキルを定義する方法がベンチマーク・モデルによって一元化され、一貫性のあるものになります。本製品は、企業の要望と適切な人材と

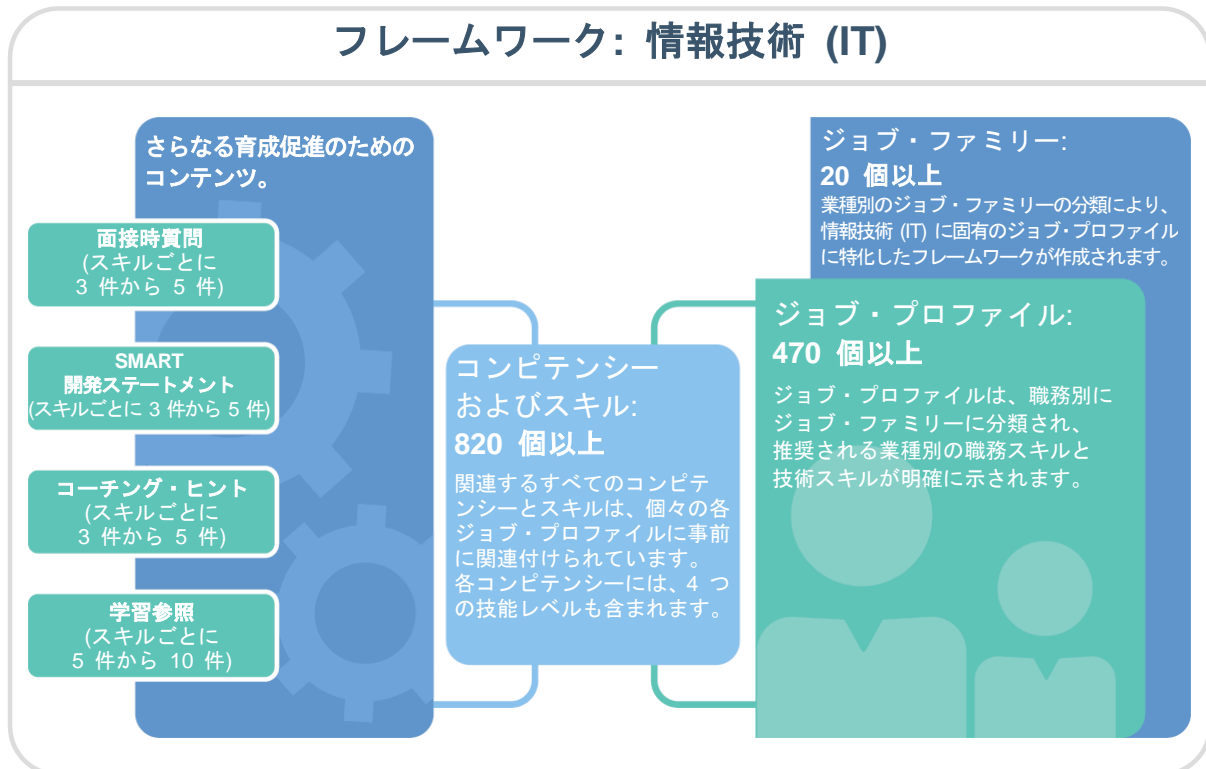
をマッチングするためのデータおよびコンテンツを人事部門に提供し、より優れた業績を達成するための魅力的な従業員エクスペリエンスを創造します。

IBM Kenexa Talent Frameworks には、以下のような複数の主要要素が含まれています。

- 定義済みのジョブ・プロフィールは、従業員が習得すべきスキルと技能レベルを詳しく記述します。
- 標準のジョブ説明は、主要な責務を明確に定義することによって、高い技能を持つ応募者を惹きつけます。
- 面接時の質問は、応募者を正しく評価するためのガイドを提供します。
- ジョブ固有のスキル、行動特性、およびコーチング・ヒントは、管理者が明確で客観的なパフォーマンス・レビューを円滑に実施できるよう支援します。
- SMART 開発ステートメントは、専門的で実施可能な業務手法を従業員に提供し、さらなる改善と達成を支援します。
- 学習参照は、成長と発展のための道筋を提供します。
- ジョブ分類は、明確でわかりやすいキャリア形成の機会に関する取り組みを推進します。

IBM Kenexa Talent Frameworks は、データ・リッチなシステム基盤により人事データ分析とコグニティブな人事管理を可能にします。

図 1: IBM Kenexa Talent Frameworks のアーキテクチャー



具体例を用いた解説: ジョブ・プロフィール

IBM Kenexa Talent Frameworks for Information Technology (IT) のジョブ・プロフィールを詳しくご覧になり、使用可能なデータとコンテンツに関する理解を深めてください。例として、以下の表で強調表示されている「情報セキュリティ専門家」のジョブ・プロフィールについて見てみましょう。

表 1. ジョブ・プロフィールの分類とその説明。

ジョブ・ファミリー・コード	SE
ジョブ・ファミリー名	IT セキュリティー
ジョブ・ファミリーの説明	データの物理的および電子的保護: アクセス制御、侵入検出、ウイルス保護、認証、監査、インシデント対応、セキュリティ・エンジニアリング、セキュリティ・ポリシーと手順の策定および導入
ジョブ・プロフィール・コード	SE-5SEC
ジョブ・プロフィール	情報セキュリティ専門家
ジョブ役割の説明	複数のプラットフォームおよび多様なシステム環境を対象としたセキュリティのための基準、手順、およびガイドラインを策定し、導入する。システム・アクセス、運用、保守を促進する。
ジョブ・バンド ID	5
ジョブの任務	<ol style="list-style-type: none"> (1) 脆弱性評価、マルウェア防御評価、および他の情報セキュリティの通常業務を一貫して実施する。 (2) 情報セキュリティのための方針、基準、および手順に影響する規制変更を特定する。適切な変更を勧告する。 (3) データ・セキュリティ・インシデントについて調査を行い、クライアントおよびプロジェクトの利害関係者に是正措置を勧告する。 (4) IT 環境におけるセキュリティ・リスクおよび脅威の制御に対する解決策を提供する。分散情報セキュリティ管理手順について、スタッフのトレーニングを行う。

* 各ジョブ・プロフィールは、固有のジョブ・コード ID が割り当てられており、ジョブ・ファミリーにマップされて該当するジョブ・バンドにタグ付けされています。
* 各ジョブ・プロフィールには、主なジョブ・ファミリーとジョブ役割の説明の他に、4 つの主要なジョブの任務が含まれています。

表 1.1. ジョブ・バンドのカテゴリーとそれぞれの説明

ジョブ・バンド ID	ジョブ・バンド名	ジョブ・バンドの説明
1	経営管理	ビジョン、方針、戦略、および方向性の設定。企業および業界の視点。組織目標の推進
2	上級管理者	戦略の策定。ビジョンの実現。運営に対する責任。費用およびリスクの管理。企業の視点
3	管理、 上級レベルのコンサルティング	機能、技術、またはプロセスに対するリーダーシップ。複数チームの管理。高い複雑性と不明確性。戦術的任務
4	第一線管理、 上級プロフェッショナル	チームまたは技術の監督。複雑な技術的取り組みに関する専門知識と経験。プロジェクト管理とコンサルティング
5	チーム・リーダー、 技術プロフェッショナル	困難な技術的作業。実装経験。自己完結性。小規模プロジェクトに対する責任。技術監督
6	管理者、 技術者、研修生	通常の技術作業または管理作業。手順に従う。監督の下で作業を行う

* ジョブ・プロフィールはそれぞれ、あらかじめ定義された 6 つのジョブ・バンドのいずれかにマップされます。



具体例を用いた解説: コンピテンシーおよびスキル - 概要

表 1 で強調表示されているサンプルのジョブ・プロフィールに対して、推奨されるコンピテンシーとスキルのデータを見てみましょう。

表 2. 情報セキュリティ専門家へ推奨されるすべてのコンピテンシーのリスト: SE-5SEC。

コンピテンシー・コード	コンピテンシー名	技能レベル	優先順位
B0150	製品およびサービス	2 - 実務経験	2 - 中
B0480	危機管理	2 - 実務経験	2 - 中
B1060	効果測定	2 - 実務経験	3 - 高
B1100	標準操作手順	2 - 実務経験	3 - 高
I0050	能動的学習	2 - 実務経験	2 - 中
I0350	問題解決	2 - 実務経験	3 - 高
I0480	効果的なコミュニケーション	2 - 実務経験	2 - 中
I0800	機密保持	2 - 実務経験	3 - 高
I0950	チームワーク	2 - 実務経験	2 - 中
I0960	正確さと細部にわたる注意力	2 - 実務経験	2 - 中
T0447	コンテンツ管理	2 - 実務経験	2 - 中
T0448	記録の管理およびアーカイブ	2 - 実務経験	2 - 中
T0490	データベースのバックアップおよびマイグレーション	2 - 実務経験	2 - 中
T0535	Web サービス	2 - 実務経験	1 - 低
T0705	ネットワーク管理	2 - 実務経験	2 - 中
T0775	ファイアウォール管理	2 - 実務経験	3 - 高
T0785	暗号化技術	3 - 幅広い経験	3 - 高
T1100	情報セキュリティ管理	2 - 実務経験	3 - 高
T1120	情報セキュリティの技術	3 - 幅広い経験	3 - 高
T1130	情報セキュリティのアーキテクチャー	2 - 実務経験	2 - 中
T1140	情報セキュリティの監査	2 - 実務経験	3 - 高
T1150	情報セキュリティの管理	3 - 幅広い経験	3 - 高
T1170	情報保証	2 - 実務経験	3 - 高
T1175	情報セキュリティ・オペレーション・センター (ISOC)	2 - 実務経験	3 - 高
T1190	サイバー・セキュリティのリスク管理	2 - 実務経験	2 - 中
T1210	コンピューター・ネットワーク防御	2 - 実務経験	2 - 中
T1250	侵入テスト	2 - 実務経験	3 - 高
T1255	侵入の検出および防止	2 - 実務経験	2 - 中
T1260	脆弱性評価	2 - 実務経験	3 - 高
T1270	デジタル脅威管理	2 - 実務経験	1 - 低
T1280	セキュリティ情報およびイベント管理 (SIEM)	2 - 実務経験	3 - 高
T3540	IT インシデント管理	2 - 実務経験	2 - 中



具体例を用いた解説: コンピテンシーおよびスキル - 詳細

表 2 で強調表示されているサンプルのコンピテンシーに対して、使用可能なすべてのデータとコンテンツを見てみましょう。

表 3. 「暗号化技術」のコンピテンシーとスキルの詳細: T0785。

コンピテンシー・コード: T0785 コンピテンシー名: 暗号化技術	
コンピテンシーの説明	組織の情報のプライバシーを確保するために暗号化技術を選択、使用、および改善するための知識および能力。
技能レベル	レベル 1: 基本的な理解
	レベル 2: 実務経験
	レベル 3: 幅広い経験
	レベル 4: 対象分野の深さと広さ
技能レベルの行動特性	<ol style="list-style-type: none"> (1) 暗号化技術の実装プロセス時に発生する問題に対する解決策について他者にコンサルティングを行う。 (2) 組織の全体的なニーズを考慮しながら、ハイレベル暗号化技術製品を評価して選択する。 (3) 業界内のさまざまな暗号化技術の優位性とデメリットを評価する。 (4) 情報の伝送における組織の暗号化技術の有効性およびセキュリティを評価する。 (5) 機密性を保って組織内でビジネス情報を交換するために、暗号化技術の実装を監督する。 (6) 暗号化技術のガイドラインおよび方針に準拠するようにユーザーを監督する。

* 各コンピテンシーは、以下の4つの技能レベルで定義されます - レベル 1: 基本的な理解、レベル 2: 実務経験、レベル 3: 幅広い経験、レベル 4: 対象分野の深さと広さ

表 3.1. 各コンピテンシーの育成促進のためのコンテンツには、面接時質問および SMART 開発ステートメントが含まれます。

コンピテンシー・コード: T0785 コンピテンシー名: 暗号化技術	
面接時質問	<ol style="list-style-type: none"> (1) 2つの一般的に使用されている暗号化方式のメリットとデメリットを比較してください。 (2) これまで作業した暗号化アルゴリズムをリストしてください。 (3) 2つ以上の暗号化技術のブリッジに関して、前職で処理する必要があった典型的な問題について説明してください。 (4) セキュリティのレベルと暗号化解除の効率性のバランスを取るために何をしましたか?
開発ステートメント	<ol style="list-style-type: none"> (1) 1カ月で、情報セキュリティおよびプライバシーを確保するために、組織内で暗号化技術を実装します。 (2) 暗号化機能のアップグレードのプロセスを詳述した、経営者および利害関係者用の週次レポートを提供します。 (3) さまざまな暗号化製品および手法の適用について1カ月に6時間の研修を実施します。 (4) 暗号化情報の暗号化解除時間が、確立されたベンチマークから10秒以内になるようにします。

* 育成促進のためのコンテンツにより、マネージャーと従業員はコンピテンシーとスキルのデータを継続的に活用することができます。



表 3.2. 各コンピテンシーの育成促進のためのコンテンツには、コーチング・ヒントおよび学習参照も含まれます。

コンピテンシー・コード: T0785		コンピテンシー名: 暗号化技術				
コーチング・ヒントの説明		(1) さまざまな暗号化技術の優位性とデメリットの評価で上級管理職を補佐します。 (2) 暗号化方式について詳細を知るためにデータ・セキュリティーの専門家と定期的にコミュニケーションを取ります。 (3) 暗号化の手法および製品の詳細について学習するための研修コースまたはプログラムに参加します。 (4) 既存の暗号化方式の有効性を評価するための定期的なレビュー会議を実施します。				
学習参照						
学習参照タイプ	書籍	書籍	書籍	書籍	組織、団体	外部出版物
学習参照名	Systems Programming	Complete Guide to Internet Privacy, Anonymity & Security	Data-Driven Security	Information Security Analytics	国際電気通信連合	NCSA ニュース
学習参照の説明	サブタイトルは「Designing and Developing Distributed Applications」。本書は、分散アプリケーションの開発が、オペレーティング・システム、ネットワークワーキング、分散システム、およびプログラミングの間の関係の基本的な理解にいかにか依存しているかについて説明します。	本書は、インターネットのプライバシー、匿名性、およびセキュリティーについての優れたガイドで、情報の提供および自身の保護に必要な実用的なあらゆる情報が記載されています。	サブタイトルは「Analysis, Visualization and Dashboards」。本書は、データを利用し、使いこなす方法について、収集および保管から管理および分析まで解説するとともに、可視化とプレゼンテーションについても言及します。	サブタイトルは「Finding Security Insights, Patterns, and Anomalies in Big Data」。本書は分析の実践についての洞察を示します。また、さらに重要な内容として、従来のセキュリティー分析手法では識別できない可能性がある傾向や異常値を特定するための分析手法の利用方法について解説します。	通信プロトコルで使用されるデータの規定を目的とする国際標準です。これは強力な複雑な言語です。その機能は、同種システムや異機種システム間の通信を正確かつ効率的に記述するよう設計されています。	ファイアウォールとインターネット・セキュリティー、在宅勤務者のセキュリティー、暗号化、スーパーネットワークワーキングといったセキュリティーのトピックなど、先進的なコンピューティングに関する資料です。
著者	Richard Anthony	Matthew Bailey	Jacobs および Rudis	Mark Talabis, その他		
出版年	2015	2015	2014	2014		
提供者	Amazon	Amazon	Amazon	Amazon	France Telecom	
URL					http://asn1.libel.tm.fr	http://www.ncsa.uiuc.edu
ISBN_ASIN	ISBN-13: 978-0128007297	ISBN-13: 978-3950309348	ISBN-13: 978-1118793725	ISBN-13: 978-0128002070	-	



最新の状態を維持します

IBM Kenexa Talent Frameworks は、独自の調査手法を使用して専門のチームにより開発されました。そのプロセスの一環として、業界動向に関する変更を特定するために、すべてのフレームワークで総合的なレビューが行われます。これらの変更を検証することで、業界内の現在のスキル要求に合わせてジョブ・アーキテクチャーを最新の状態に保つことができます。

調査ソースは次のとおりです。

- キャリアおよび採用関連の Web サイト
- クライアント調査およびコンテンツ・ワークショップ
- 業界のディスラプション
- テクノロジーまたは新しい業種における新しい分野、ジョブの機能、ジョブの役割、またはスキル
- 組織開発および HR のベスト・プラクティス
- 規制に関する法律および業界のコンプライアンス要件
- 研究機関および専門家協会
- 構想と発想を導く縦思考の専門家

IBM Kenexa Talent Frameworks についての詳細は、IBM 担当員にお問い合わせください。



日本アイ・ビー・エム株式会社

〒103-8510
東京都中央区日本橋箱崎町 19 番 21 号

©Copyright IBM Japan, Ltd. 2018
All Rights Reserved

05-18 Printed in Japan

当資料は、2017 年 9 月に IBM Corporation が発行した資料の抄訳です。

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

本書の情報は最初の発行日の時点で得られるものであり、予告なしに変更される場合があります。すべての製品が、IBM が営業を行っているすべての国において利用可能なものではありません。

本書に掲載されている情報は特定物として現存するままの状態を提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。



Please Recycle

LOS14079JPJA

