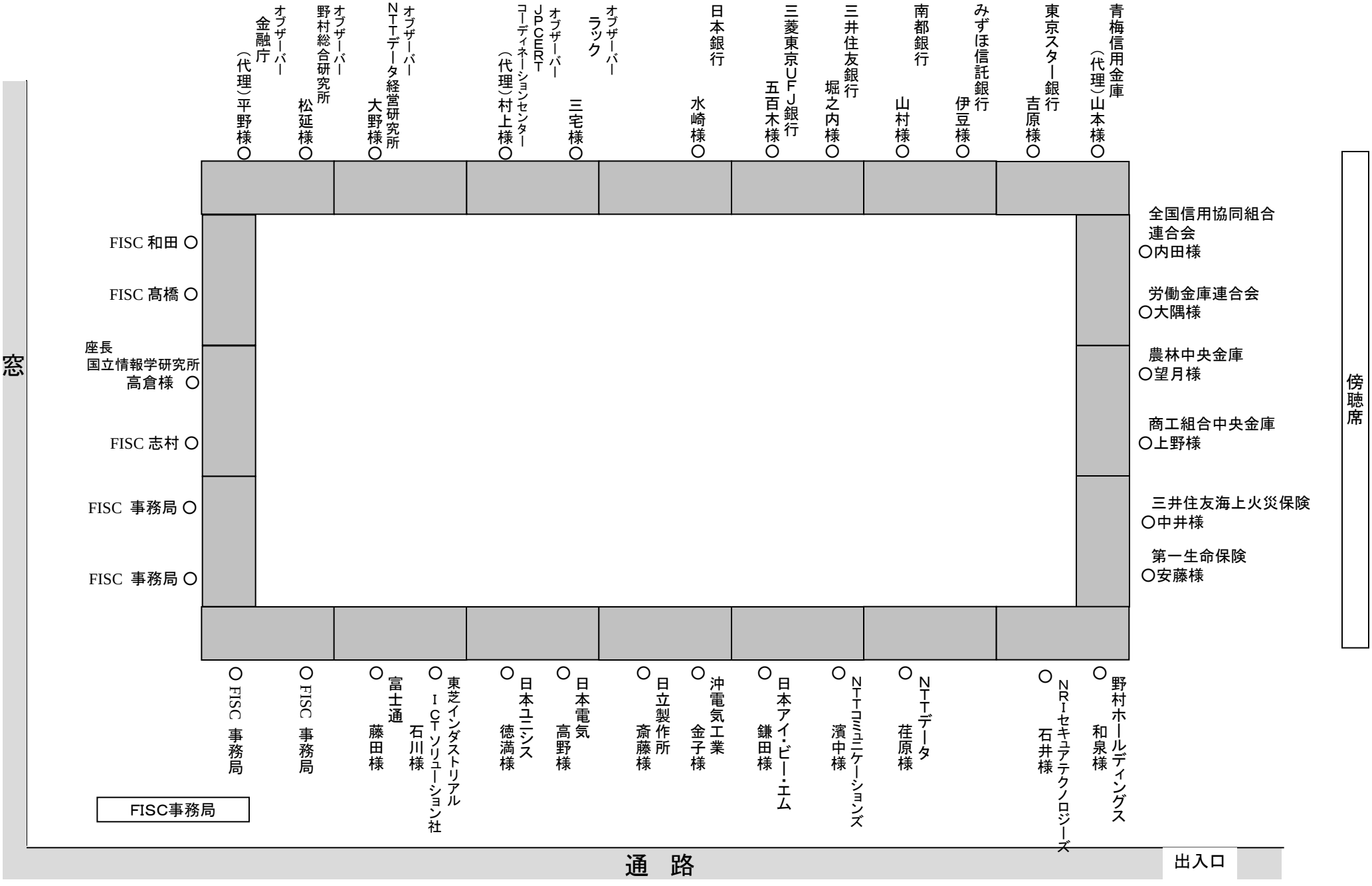
第3回「IT人材検討部会」座席表

平成29年9月26日



平成 29 年 9 月 26 日
公益財団法人 金融情報システムセンター

平成 29 年度　第３回 ＩＴ人材検討部会　議事次第

Ⅰ．時間：15：30～17：00

Ⅱ．場所：FISC 会議室

Ⅲ．議事次第

１．手引書原案の修正に関する検討

・各委員からのご意見反映について

２．第 58 回 安全対策専門委員会への上程資料（案）について

・平成 29 年度ＩＴ人材検討部会の検討結果について

・FISC 会員企業への意見募集実施について

Ⅳ．資料

資料番号	資料名
人材３－１－①	手引書原案に対する各委員からのご意見（対応方針）
人材３－１－②	『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』 【原案】修正案
人材３－１－③	手引書原案 第３編　図表修正案（図表４・図表８・図表９）
人材３－１－④	手引書原案 第４編　図表追加・修正案（図表 11・図表 13・図表 14・図表 15）
人材３－２－①	平成 29 年度ＩＴ人材検討部会の検討結果について
人材３－２－②	『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』 に関する FISC 会員企業への意見募集実施について
人材３－３	平成 29 年度　第３回ＩＴ人材検討部会検討事項に関するご意見 （メール回答用）
参考資料	ＩＴ人材検討部会　委員名簿

Ⅴ．連絡事項

１．第 58 回安全対策専門委員会の開催

本検討部会の検討内容を踏まえ、平成 29 年 10 月 26 日（木）に第 58 回安全対策専門委員会を書面開催の予定。

２．検討事項に関するご意見

本日の検討部会の検討事項について、ご意見がございましたら、10 月４日（水）までに、電子メール＜fisc40@fisc.or.jp＞あてにお送りください。

フォームにつきましては【人材３－３】をご使用ください。

３．委員名簿の確認依頼

【参考資料】ＩＴ人材検討部会　委員名簿の確認を、10 月４日（水）までにお願いします。

４．次回（第４回　ＩＴ人材検討部会）の開催予定

平成 29 年 12 月 15 日（金）15：30～17：00　FISC 会議室（終了後、懇親会を予定）

以　上

議事１

■手引書原案に対する各委員からのご意見（対応方針）

【人材３－１－①】
平成29年9月26日
公益財団法人　金融情報システムセンター

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況
1	p4	第１編　はじめに 2．本手引書の位置付け、構成	各委員から意見がありました通り、実用的な手引書としていきたいと思っています。つきましては、その旨を本文中、または脚注に書き加えて頂きたいです。 【追記案】 （また、本手引書は～該当する項目を選択して利用することを想定している。） なお、本手引書が実用的なものとなるよう、将来的な改訂の際には、金融機関等におけるIT人材の確保・育成計画の策定に関する実例等を記載する予定。	三井住友銀行 堀之内様	ご指摘を踏まえ、個別の事例を機関誌やフラッシュにて還元する予定である旨、冒頭の「手引書発刊にあたって（仮題）」に記載する予定です。	要	未
2	p14,15	第３編　IT人材の確保・育成に向けた実務 手順１－１－１　現状のIT業務の洗い出しを行う　考慮事項　図表３，４	人材２－２－②の１ページ目、黄色の網かけの部分で、個別システム案件管理の部分になります。下から2つ目のベンダー選定及びベンダー委託管理の部分が、順番として置き場所がおかしいかと思われます。 　加えて、この箱の中に2つの要素が入れ子になっており、分かりにくいので、ベンダー選定とベンダー委託管理については異なる要件として箱を分けるべきだと思います。かつ、ベンダー選定については、この箱の置き場所がもっと川上かと思われます。その修正をお願いできればと思っています。	NTTD経営研 大野様	ご指摘を踏まえ、「ベンダー選定」と「ベンダー委託管理」に項目を分けます。また、図表3と図表4の関連性が読み取れるように、各業務の頭にアルファベットを付与します。	要	済
3	p23～28	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表８，９	システムの上流工程からの観点からすると「３業務設計・システム導入」と「４プロジェクト管理」は順序を入れ替えた方がよいと思います。	南都銀行 山村様	ご指摘を踏まえ、「３　プロジェクト管理」と「４　業務設計・システム導入」の順に記載します。 （図表9も同様）	要	済
4	p24	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表８	６システム運用の人材像 　以下の人材像も必要ではないかと考えます。 ・自機関システムのOS・ミドルウェアなど基盤となるソフトウェアを俯瞰的に把握管理できる人材 （サイバーセキュリティとも重複しますが、ソフトウェアの脆弱性に素早く対応できることも想定しています） ・ハード面の性能・リソースなどが適正であるかを管理・評価できる人材	南都銀行 山村様	ご指摘を踏まえ、図表８の「求められるIT人材像」に追加します。	要	済
5	p24	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表８	『安定稼働を確保』という表現ですと、IT人材のスキルとの直接的な関係が読み取りにくいと思われる点、および『障害』と『トラブル』は同様の意味と捉えられる可能性がありますので、以下のとおり記載を変更頂きたいです。 （現） ・安定稼働を確保し、障害発生時において被害の最小化を図るとともに、継続的な改善、 品質管理などに主導的な役割を果たせる人材 ・トラブル対処ができる、運用業務の改善ができる人材 （新） ・システムの安定稼働を維持するための運用設計や運用環境の改善を継続的に提言できる人材 ・障害等の異例事態発生時において被害の最小化を図るとともに、品質管理などに主導的な役割 を果たせる人材	三井住友銀行 堀之内様	ご指摘を踏まえ、図表８の「求められるIT人材像」を修正します。	要	済
6	p24	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表８	運用部署は完成されたシステムを引き受けるだけでなく、要件定義の段階から積極的に参画し、 運用要件の整理を主体的に行うことで「工程の後戻り防止」や、「運用品質の向上」に貢献する ことを期待する観点から、以下の通り記載を追記願います。 ・システム運用に関する要件定義に参画し、「工程の後戻り防止」や、「運用品質の向上」が図れる人材	三井住友銀行 堀之内様	ご指摘を踏まえ、図表８の「求められるIT人材像」に追加します。	要	済
7	p25	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表８	８リスク管理の人材像 　１つ目の人材像と少し重複するかもしれませんが、「システムリスク」をキーワードにして、 ・サイバーセキュリティを含めシステムリスクを俯瞰的に管理・対応できる人材 を追加してもよいと考えます。	南都銀行 山村様	ご指摘を踏まえ、図表８の「求められるIT人材像」を修正します。	要	済
8	p28	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表８，９	IPAのIT人材育成（https://www.ipa.go.jp/jinzai/itss/itssplus.html）にて、データサイエンス領域について新スキル標準の策定に関し取り纏め・公開されていますので、ここから引用する、あるいはここを参照する貌が望ましいと考えます。 ※スキルの具体的な定義は、一般社団法人データサイエンティスト協会が公開する 　スキルチェックリスト（https://www.datascientist.or.jp/common/docs/skillcheck.pdf）に掲載	三井住友銀行 堀之内様	データサイエンス領域のスキルについては、ご意見いただいた主旨のとおり認識しています。 今回、ご意見№.9の対応に伴い「IT人材の役割の分類」を“データ分析”から“データ利活用”に変更しますので、現段階ではデータ利活用領域のスキル標準を含む『iコンピテンシ ディクショナリ（iCD2017）』を参考文献として紹介する貌にしたいと考えます。	否	原案の通りとさせていただきたいと考えております。
9	p25,28	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表８，９	「12データ分析」を、１つのIT人材分類として定義するのであれば、もう少し担うべき業務を明確にしたほうが良い。マーケット分析だけでなく、様々な分野の業務で必要とされている。業務に何かを追加するのかも含めて、検討したほうが良いと思われる。	NRI　松延様	「12データ分析」は、「経営戦略・事業戦略の策定（マーケットや顧客ニーズの分析）」業務を担う人材として例示していましたが、それに加えた業務例として「データ整備」に関する業務を、図表４に追加します。 また、それに伴い図表８，図表９の「IT人材の役割の分類」名を“データ分析”から“データ利活用”に変更します。	要	済
10	p27	第３編　IT人材の確保・育成に向けた実務 工程２－１　IT人材・スキルの定義　考慮事項　図表９	６システム運用　スキルの知識の欄 　３つ目　「・業務システムの主管部門と担当者」とあるが、どういった知識なのかわかりにくいと思います。	南都銀行 山村様	当該スキルは、知識として記載する内容ではないと考え、削除します。	要	済
11	p29	第３編　IT人材の確保・育成に向けた実務 手順２－２－２　システム戦略に必要な中長期的なIT人材の人数とスキルを定義する	適正な人数を求めることは難しいと考える。経営層への説明も求められる性格のものであり、「人材の定義」「スキルの定義」とともに人数の求め方・考え方などにふれるべきではないかと考える。	南都銀行 山村様	中長期的に必要なIT人員の適正人数の把握について、個別の事例として機関紙やフラッシュにて還元する予定です。	否	原案の通りとさせていただきたいと考えております。
12	p30	第３編　IT人材の確保・育成に向けた実務 手順２－２－２　システム戦略に必要な中長期的なIT人材の人数とスキルを定義する　考慮事項	「業務の優先度を勘案する」とありますが、「システム戦略」に基づいて人数・スキルを整理している時点で、業務の優先度は考慮済みだと思いますので、この記載は不要ではないでしょうか。	第一生命 安藤様	ご指摘を踏まえ、削除します。	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況
13	p30	第3編　IT人材の確保・育成に向けた実務 手順2－2－2　システム戦略に必要な中長期的なIT人材の人数とスキルを定義する　考慮事項	人材2－2－①の25ページ目になります。下の6行、赤字で書かれている部分で、下から2行目の真ん中あたりの「外部委託先の業務の理解」とありますが、「外部に委託する業務の理解」というのが正しいと思っております。	NTTD経営研 大野様	ご指摘を踏まえ、修正します。	要	済
14	p30	第3編　IT人材の確保・育成に向けた実務 手順2－2－2　システム戦略に必要な中長期的なIT人材の人数とスキルを定義する　考慮事項	・基幹システムを共同センター等に外部委託し利用している場合 　共同システムを有効利用するための業務知識とシステム分析能力を兼ね備えたIT人材が必要であり、自社の独自システムとの連携をマネジメントできる人数とスキルを維持する。 （当初と比較し項目が無くなったと思われるが必要ではないか？）	青梅信金 金丸様	ご指摘を踏まえ、追加します。	要	済
15	p31	第3編　IT人材の確保・育成に向けた実務 手順2－2－3　現状と中長期的な目標とのギャップ分析を行う　考慮事項	図表10に「Level」の例示がありますが、確かに「Level」の定義、定義した「Level」により判定することは有効かと思います。本文のどこかに「Level」に関する言及があった方がよろしいのではないでしょうか。	第一生命 安藤様	ご指摘を踏まえ、手順2－2－1　考慮事項に「レベル判定の基準を設定する（図表10参照）などにより」という文言を追加します。	要	済
16	p32	第3編　IT人材の確保・育成に向けた実務 工程3－1　IT人材の確保・育成計画を策定する 基本的な考え方	第二回のセッションの中で質問も出たように、各金融機関の事情により対応は異なるため、必ずしも具体的に記載することが良いとは限らず、概念的な記載に止めているという点は、その旨を補足記載しておくことが良いと考える。 「･･･を検討する」といった記載に対しては、「機関誌等から斯く斯く然々の情報を得て参考としつつ」といった補足を加えるようなイメージを想定。	みずほ信託銀行 伊豆様	ご指摘を踏まえ、個別の事例を機関誌やフラッシュにて還元する予定である旨、冒頭の「手引書発刊にあたって（仮題）」に記載する予定です。	要	未
17	p32	第3編　IT人材の確保・育成に向けた実務 工程3－1　IT人材の確保・育成計画を策定する 基本的な考え方	「育成」とは、自機関のIT業務に必要な人材を、自機関の要員として育成する事であり、IT人材の中には金融機関業務にもある程度精通した人材も確保する事が重要である。	青梅信金 金丸様	ご指摘の通り、金融業務を理解するためには、他部門や営業店等への異動も含めたジョブローテーションが考えられます。そのため、ジョブローテーションについて工程3－1にて既に記載済であること、また、個別の事例として機関紙やフラッシュにて還元する予定であることから、原案の通りとさせていただきます。	否	原案の通りとさせていただきたいと考えております。
18	p33	第3編　IT人材の確保・育成に向けた実務 手順3－1－6　各適正化方策を補助する施策を検討する	「2. IT人材のスキル評価とそのフィードバック方法を検討する」とありますが、これは「補助する施策」として「手順3－1－6」に記載することが相応しいでしょうか。スキル評価は人材育成における重要な項目ですので、どこかに切り出して記載するのがよろしいではないでしょうか。	第一生命 安藤様	ご指摘を踏まえ、手順3－1－6から削除し、新たに「手順3－1－7　IT人材のスキル評価とそのフィードバック方法を検討する」として手順を追加します。	要	済
19	p33	第3編　IT人材の確保・育成に向けた実務 手順3－1－6　各適正化方策を補助する施策を検討する	「4. 」について、研修や資格取得の補助制度を検討すべきとありますが、「知識レベル」に限定しなくてもよろしいのではないでしょうか。	第一生命 安藤様	ご指摘を踏まえ、知識レベルに限定しない記載に修正します。	要	済
20	p34	第3編　IT人材の確保・育成に向けた実務 手順3－1－3　配置転換による適正化を検討する 考慮事項	「業務に必要のない個々人のスキルは把握されない可能性がある」との記載について、意味がわかりづらいかと思いました。	第一生命 安藤様	ご指摘を踏まえ、修正します。	要	済
21	p35	第3編　IT人材の確保・育成に向けた実務 手順3－1－6　各適正化方策を補助する施策を検討する 考慮事項	本来、金融機関のIT部門に従事している職員（＝プロフェッショナル）は、日進月歩の技術革新に対応して、自らが積極的にスキルアップを図る必要があるが、昨今はこれが希薄になっている。 今回のIT人材育成手引書を活用して、各金融機関が組織的にIT人材育成の実効性を高めるには、人事部門との連携が欠かせない、と思量する。特に、中小金融機関の場合は、ITに対する理解が乏しく、人事部門が積極的にIT人材育成に関与する事が求められる。（中途採用を含む） これは、金融機関によって事情が異なるので、本手引書には概要程度の記載しか出来ない。『具体的なものは、各金融機関の事例を参考にする』 IT職員がスキルアップを怠る要因には、下記の様なものがある。（金融機関によってバラつきがある） ①金融業務関連の研修制度（内部･外部）は、金融機関内部でしっかりと確立され、人事評価とも連動しているが、”IT関係の研修制度”は、人事評価との連動を含めて不十分である。『IT関係を特別扱いしない点が肝要』 ②IT部門に従事している職員であっても、人事上は他の職員と同等であり、特別扱いされている訳ではない。 　＊国家資格取得者には、多少の”＋”評価はあるが僅かなものである。〃 ③ITに従事している職員は、永久的にIT部門に従事する訳ではなく、他の部署（本部･営業店等）への異動がある。 ④細かい点では、仕事がきつい（徹夜、休日出勤等）割りに、収入が少なく、他部署の職員と比較して業務上の実績が見え難い為、評価は低い。『スキルを加味した人事評価基準や手法等が曖昧。特に、中小金融機関』 上記の点から、IT部門職員は、自らのスキルアップに消極的になり易く、IT人材育成とIT専門家の中途採用においては、人事部門と連携した対応が欠かせない。『IT部門職員のモチベーション向上が必須』 更に、IT部門職員が積極的にスキルアップを図る為には、各人に人事と連動している点をしっかりと認識させる必要がある。『”低スキル者”→”低評価”を認識させる』 ∵組織として「人材育成」を唱えても、各人に甘えがある限り、実効性は上がらない。 ＊甘えとは：ITは、従事している者にしか分からない、との誤解。	日本ユニシス 徳満様	個別の事例については、機関紙やフラッシュにて還元する予定です。その際、いただいたご意見を参考にさせていただきます。	否	原案の通りとさせていただきたいと考えております。
22	p39	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項	「CIO、CISO等」、「CISO等」、「CISO」という用法が混在しており、読者にとって分かりにくくなっているため、本手引書としての考え方を整理した方が良いように思われる（その際、「コンテ手引書」等との整合性を確保する必要）。リスク管理の観点から、CIOとは別にCISOを設置することがより望ましいとする考え方がある一方で、現状、わが国においては、CIOがサイバーセキュリティに関する責任者を兼ねている金融機関等が少なくないと思われる。「図表14は必要か」という議論も、その点を踏まえて検討すべきではないか。	日銀 水崎様	ご指摘を踏まえ、「CISO等」で平仄を合わせます。なお、文献の引用力所につきましては、文献原文の記載とします。 図表14は、サイバーセキュリティに関する業務全体について記載します。（No27参照） 参考：『コンテ手引書』では「サイバーセキュリティに関する責任者（CIO、CISO等）」と定義しています。	要	済
23	p42	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順1－1－1 現状のIT業務の洗い出しを行う　考慮事項 　1（2）①　インシデント対応組織の態勢の在り方について	（P37）①インシデント対応組織の態勢の在り方について インシデント対応組織の役割について図表12で平時の運用などの役割も例示しており、「a専任組織による態勢」や「b兼任組織による態勢」についても平時の運用などに関する内容の記載も追加すべきではないかと思います。	南都銀行 山村様	ご指摘を踏まえ、専任組織及び専任組織においてもインシデント発生時だけでなく、平時の運用についても追記します。	要	済
24	p43	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順1－1－1　現状のIT業務の洗い出しを行う　考慮事項	「③外部委託先の活用」の記載について、人材育成の話から少し逸れているように読めました。	第一生命 安藤様	ご指摘を踏まえ、本節記載内容の主旨に合わせて表題を「外部委託先が分担する役割の範囲の明確化について」として修正いたします。	要	済
25	p46	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する 考慮事項	「2. サイバーセキュリティにおける「橋渡し人材層」の必要性」について、1段落目に「橋渡し人材層が必要となる」とありますが、なぜ必要となるのか･なぜサイバーだけなのか、その「理由」を付記しておくのがよろしいのではないでしょうか。	第一生命 安藤様	第4編の第2工程における人材の定義の箇所で、「橋渡し人材層」を取り上げた理由について追記します。 また、前回原案で、手順2－1－1「人材像の定義」に「橋渡し人材層」のスキル定義と確保・育成に関して集約し記載していた点に唐突感があったため、手順2－1－2「スキル定義」及び手順3－1－2「育成による適正化」に考慮事項を振り分けて記載します。	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況
26	p46	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する考慮事項	3. サイバーセキュリティ人材について 　専門的な人材定義だけでなく、現場の認識および対応力の底上げの必要性等についても記載した方が良いと思います。 　例えば、本部・営業店とも管理職登用条件に、「情報セキュリティマネジメント試験」を採用する等の必要性も考えられると思います。	青梅信金 金丸様	今回の手引書の育成対象は、営業店などのシステム利用者は、確保・育成の対象となる「人材」から外しているため、現状の記載内容とします。	否	原案の通りとさせていただきたいと考えております。
27	p47	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する考慮事項 　3（2）　自機関でのサイバーセキュリティ人材に望まれる役割の例	サイバーセキュリティの必要人材の概念は、組織上の位置づけと一体で捉えることも一つではないかと考えます。 3.(2)に、「図表14 の人材は、必ずしも専任化する必要はなく、兼任も可能であると考えられます。また、システム部門に限らず、様々な部門が協働して役割を担っていくことが考えられる」とありますが、図表14の「②情報セキュリティ」と「③インシデント対応管理」の機能は、セキュリティ統括部門が所管することが望ましく、当該部門は（外部コンサルティングを利用する等の手段を含めて）社内・社外のネットワークおよびシステム環境の全体像を掌握するだけの知見を備えた人材を確保するよう努めることも必要ではないかと考えます。	南都銀行 山村様	ご指摘を踏まえ、図表14「サイバーセキュリティ人材の役割・人材像の例」で、情報セキュリティ戦略を策定・遂行する業務や現状評価を行う業務を記載し、業務および人材像を再整理します。	要	済
28	p44～51	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する 図表14　サイバーセキュリティ人材の役割・人材像の例	本手引書の位置付けは、「より大きな枠組みで」「システム部門以外の部門に所属しているIT業務に携わる人材についても」として、「実情に即して」「該当する項目を選択して利用することを想定」している。 これはサイバーも含め全体にかかるものとの理解。 どこまで自機関で入り込むべきかの議論については、従前も、例えばネットワークやサーバークラスタ構築等々、基盤技術系の業務を金融機関のプロパー社員がどこまでやるべきか、やれるか、という議論はあり、サイバーも基本は同様と考える。 技術の進歩や専門性、複雑度の高度化が加速的に早まる中、総合的な見地からどこまで入るべきか適時的確に提言あるいは判断していくことが、IT人材に求められる力で、工程1-1のシステム戦略の策定につながる要素。サイバーや先端技術は、この見極めを従前より速いスピードで行わなければならない領域と考える。 その点から、「サイバーセキュリティ業務のすべてを自機関で遂行することが難しい場合は、外部委託先を活用する。」「…どの役割を委託するか決める必要がある。」「外部委託先を含めた全体の総括や業務影響の評価…金融機関等で担うべき機能と考えられる」といった辺りの記載、そして図表14の取り扱いについての議論を踏まえると、図表14の「役割」に代えて機能を並べ、従前の基盤技術系のように、超上流の方針策定から個別セキュリティ技術のハンドリングまでの間で、自機関での入り込みの深さを選ぶようにして、また、横軸に対峙する対象の脅威を並べるイメージでどうか。 それに、脅威毎の高度化、対策技術の進歩、一般的な選択状況等を付して、各金融機関の選択に際しての参考情報として利用できるようにする等。 機能の中には、利用部門におけるリテラシー向上のリード・支援、という点も含める想定。	みずほ信託銀行 伊豆様	ご指摘を踏まえ、図表14「サイバーセキュリティ人材の役割・人材像の例」は、「サイバーセキュリティに関係する業務」として、サイバーセキュリティに関する戦略や平時・インシデント発生の運用業務、リスク管理等、想定される業務を網羅して記載し、業務および人材像を再整理します（※1）。 なお、図表14については、「役割」として整理を行い、各役割に対する自機関の入り込みの深さについては、外部委託について言及することで対応します。	要	済
29	p44～51	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する 図表14　サイバーセキュリティ人材の役割・人材像の例	サイバーセキュリティ人材とその役割については，多数の参考文献があるため，その整理を行い，例示が必要な状況にあると考えます．図表14は機能とプロセスが混在しているようにも見え，再整理が必要と考えます．機能群が人材にアローケンションされたとき，意味的に持続する文脈の中で，人材の側から，人材が担う機能の集合体を役割とします．平事に担う役割と，有事に担う役割は異なります．例えばサイバーセキュリティの文脈の中で，有事には，平事に想定できない事象が生じるため，いわゆる「例外状態」への対応機能が含まれます．また，例外状態の対応が適切であったのかを検証する第三者（利益相反原則に基づく）の役割も必要になります．	富士通 藤田様	No28（※1）参照。	要	済
30	p44～51	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する 図表14　サイバーセキュリティ人材の役割・人材像の例	（P41）図表14を自機関内に保持することが望ましい人材の例示とするならば、文献ごとに記載する必要はなく、望まれる人材だけの例示だけでよいと思います。 また、図表11、図表12、図表14はかなり重複感があるので1つにまとめ、対応の分類、人材像、その担い手、自機関に保持することが望ましい人材、外部委託可能な役割などで整理したほうが理解しやすいのではないかと思います。	南都銀行 山村様	No28（※1）参照。 図表14の位置付けとして、自機関で判断し、整理できるような参考例を望まれるご意見が多かったこともあり、手引書としてはサイバーセキュリティに関係する業務を網羅的に洗い出した図表として記載します。	要	済
31	p44～51	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する 図表14　サイバーセキュリティ人材の役割・人材像の例	ここの役割の①～⑤までは、有事のプロセスを念頭に置いた対応すべき人、あるいはそのミッションというものが記載されているように見受けられます。ここまで踏み込んで記載するのであれば、逆に平時に担うべきミッション、プロセス、役割といったものを相応に組み込むべきかと思います。	NTTD経営研 大野様	No28（※1）参照。	要	済
32	p44～51	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－1　IT業務に求められる役割からIT人材を定義する 図表14　サイバーセキュリティ人材の役割・人材像の例	サイバーセキュリティの特徴は、一般的なコンテと比べ想定外のことをいかに想定しておくかということ。一般的な障害と比べてアタックされているから予想しにくい想定外のことに対してメタなベースで記述、規定しておくことが、いわゆる有事の際の方法である。平時の場合も同様に決めておくということ。そのような本質が図表14から読み取れるかという観点でチェックされるべきである。悪い意味ではないが、粒々のところに目が行くとその本質が見えなくなる。	富士通 藤田様	No28（※1）参照。	要	済
33	p52	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－2　求められるIT人材のスキルを定義する 考慮事項	サイバーセキュリティ人材に求められるスキルセットとして，もう少し詳細に記載すべきと考えます．その際スキルセットは，多軸の位相となるため，この軸にあたる項目を例示すべきと考えます． 例えば，平事から有事への相転移と，有事から平事の相転移とでは，その履歴が異なる二重安定性を持つ自己組織化のプロセスであり，対応するコアスキルも異なります．また脆弱性（vulnerability）を低減するためのスキルと，回復性（resilience）を強化するためのスキルセットは直交概念であり，異なるスキルセットになります．	富士通 藤田様	ご指摘を踏まえ、図表15「サイバーセキュリティ人材に求められるスキルの整理例」として、スキルに関してより具体的な例示としてサイバーセキュリティ人材に求められるスキルを記載することとします。 なお、スキルにおいては、IT人材と重複するものもあることから、サイバーセキュリティ固有の知識に関して図表にいくつか例示し、基本となるスキル（知識、経験、技量）は本文中に記載します。	要	済
34	p54	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－2　求められるIT人材のスキルを定義する 考慮事項	（P46）1.サイバーセキュリティ人材に求められるスキル サイバーセキュリティ人材に求められるスキルの1つとして、BCP関連のマネジメントスキルも必要ではないかと考えます。	南都銀行 山村様	No33参照。	要	済
35	p52	第4編　サイバーセキュリティ人材の確保・育成に関する考慮事項 手順2－1－2　求められるIT人材のスキルを定義する 考慮事項	「（3）業務知識」について、「経営層への報告ができる知識」が求められるとありますが、サイバー人材にこの知識が求められており身につくであろうという前提に立てば、「橋渡し人材」の役割を既に担っているのではないかと思いました。 上記に記載しました「橋渡し人材が必要となる理由」と合わせて整理をいただければと思います。	第一生命 安藤様	「橋渡し人材」についてはNo25を踏まえ再整理を行い、業務知識については、「金融業務知識」として記載内容を整理いたします。	要	済

議事１

【人材３－１－②】
平成 29 年 9 月 26 日
公益財団法人 金融情報システムセンター

金融機関等における IT人材の確保・育成計画の 策定のための手引書 【原案】 修正案

平成〇年〇月

公益財団法人　金融情報システムセンター

目次

第１編　はじめに

１．手引書作成の背景

わが国の金融機関等におけるＩＴの利活用が大きく進展したことから、金融機関等の業務とＩＴは密接に関係しており、経営戦略・事業戦略とシステム戦略は不可分一体となっている。そのため、ＩＴを担う人材の役割はこれまで以上に大きくなっている。

これまでは、金融機関等におけるＩＴを担う人材と言えば、システムの開発及び運用に従事する人材がイメージされることが多かった。ところが、最近では以下に述べるような金融情報システムを巡る環境変化に伴い、システム戦略を実現するために必要な業務（以下「ＩＴ業務」という）は、システム部門だけに留まらず、システム部門以外の様々な部門に関わりが広がってきており、部門間、更には外部委託先や関係機関等、社外との連携がより一層重要となっている。そして、ＩＴ人材[1]に求められる役割・スキルは、各金融機関の特性や実情に応じて多様化してきている。

(1) 金融機関等における業務のＩＴ化・多様化

金融機関等における業務がＩＴなしでは成り立たなくなっている現状において、金融機関等は新たな金融サービスの提供や、顧客サービス向上として、例えばインターネットバンキング用のセキュリティブラウザの提供、生体認証をはじめとした認証機能の高度化など、多岐に渡る対応を推進している。このため、金融機関等のＩＴ業務や、それを担うＩＴ人材に求められる役割・スキルは急速に多様化している。

(2) リスク管理の高度化・複雑化

システム戦略は経営戦略、事業戦略と一体であり、ＩＴに関係する分野が広がるに伴い、そのリスクも高度化・複雑化してきており、それらのリスク管理に携わるＩＴ人材の重要性が増している。

(3) 新しい技術やサービスへの対応

近年、クラウド・FinTech・高度なデータ分析など、新しい技術やサービスが登場しており、それらをビジネスや業務にどのように活用していくのかという点を検討・提案するＩＴ人材が求められている。

(4) サイバーセキュリティ対応

金融機関等におけるサイバー攻撃は、DDoS 攻撃、標的型メールや不正送金などがあり、日々、高度化・巧妙化している。各金融機関にはその対策を行う人材を必要としており、サイバーセキュリティ業務を担うための人材（以下「サイバーセキュリティ人材」という）が求められている。

---

[1] システム戦略を実現するために必要な人材を指す。本手引書における、ＩＴ人材の対象とする範囲は、システム部門も含めた全社とする（企画部門・リスク部門等の本部・本社組織とする。但し、営業店などシステムを利用する人材については含まない）。

これらＩＴ人材に求められる役割・スキルの多様化により、ＩＴ業務の外部委託の位置づけにも変化が生じている。従来はシステム開発・維持費の低減がその主な理由であったが、現在ではそれに加え、高度な専門性や最先端の知識を必要とする業務等、ＩＴ人材の育成が困難であり即戦力が求められる業務において、積極的な外部委託や外部サービスの利用がみられる。一方、外部委託の進展やその他の理由により、自機関のＩＴ人材が減少してきた金融機関等においては、システム案件の企画立案・推進、外部委託先の管理、リスク管理、サイバーセキュリティ業務の遂行に必要な人材を維持することの重要性についてもクローズアップされてきている。

金融機関等はこのような環境の変化を踏まえ、ＩＴ人材の確保・育成はシステム部門だけではなく、全社的に取り組んでいくことが求められている。そのためには、金融機関等の実務部門のみならず、経営層[2]についても、システム戦略に基づく、ＩＴ人材の確保・育成に向けた取組みに積極的に関わり、態勢を整える必要があると考えられる。

また、当センターで開催した「金融機関における外部委託に関する有識者検討会（平成 27 年 10 月～平成 28 年 6 月）」においても、「安全対策上必要となるＩＴガバナンス」として、経営層は（１）中長期計画等における安全対策に係る重要事項の決定や（２）安全対策に係る態勢等の改善事項の決定について、役割と責任を果たすことが必要であるとしている。そしてまた、経営層は、システム戦略方針の１つとして、人員計画の決定に際して、（１）人員数・スキルの種類とレベル・配置の把握、（２）全体の中長期計画に沿った人員の育成計画の策定について留意することが必要であると提唱されている。

このような状況に鑑み、当センターでは、金融機関等が個々の経営判断によりＩＴ人材の確保・育成を進める場合の参考に資することを目的として、「ＩＴ人材検討部会」を設置し、その検討結果に基づき、『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』を作成した。

[2] 重要事項の内容に応じて、取締役会に限らず、権限移譲を受けた取締役・執行役等までを指す。

２．本手引書の位置づけ、構成

これまで述べてきたようにＩＴ業務を推進していくためには、システム部門と関係する他部門、あるいは外部委託先等との連携が重要になってきている。したがって、本手引書では、システム部門以外の部門に所属しているＩＴ業務に携わる人材についても、「ＩＴ人材」と位置づけたうえで、より大きな枠組みでＩＴ人材の確保・育成に取り組んでいくことを前提としている。

また、本手引書は、各金融機関等の特性や実情（規模やシステムの運用状況、外部委託状況等）に即して利用されることを想定している。すなわち、ＩＴ人材の確保・育成計画の策定について画一的な手順を示したものではなく、策定の考え方や留意すべき事項を記載したものであり、各金融機関等では記載内容のうち、該当する項目を選択して利用することを想定している。

本手引書~~の構成~~は、~~まず、~~第２編~~で~~~~において~~経営層の役割について、第３編で経営層から指示を受けた実務部門が実際に計画を策定していくための手順について記載している。

なお、サイバーセキュリティへの対応には、他のＩＴ業務と異なるスキルが求められていること、また、人材の数と質の不足が喫緊の課題となっていることから、第４編を設けてサイバーセキュリティ人材を確保・育成する上での考慮事項を記載している。

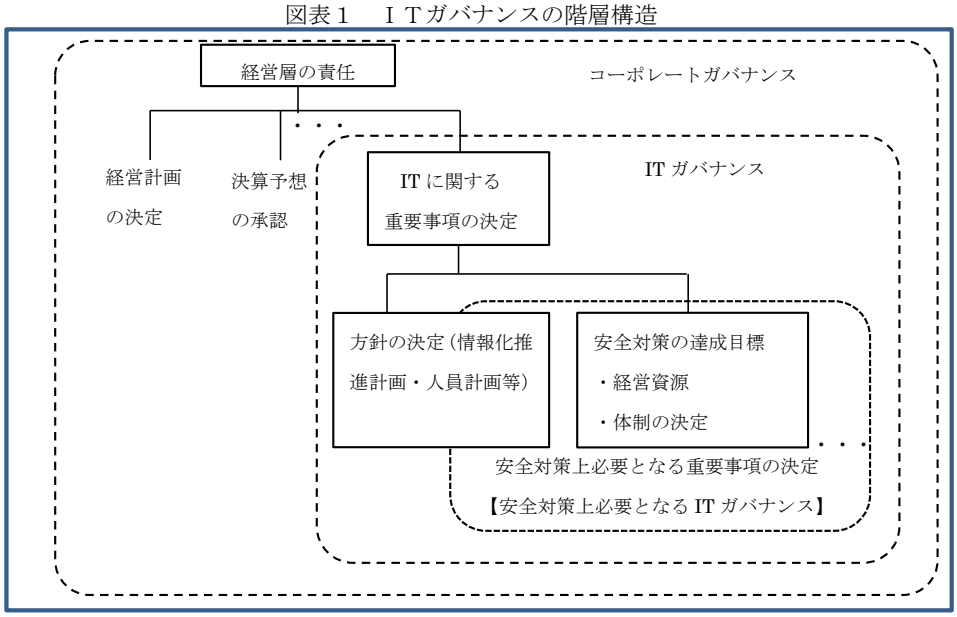
第２編　経営層の役割

１．ＩＴ人材の確保・育成における経営層の関与の重要性

経営層は、経営戦略・事業戦略とシステム戦略が不可分一体であることを理解した上で、ＩＴガバナンス[3]を機能させることが必要である。

ＩＴに関する重要事項の中には、システム戦略方針、システムリスク管理方針、ＩＴに投下する経営資源、ＩＴ業務の執行体制及びＩＴ業務のモニタリング体制等の決定がある。これらの決定事項を実現するためには、ＩＴ人材の確保・育成は重要な事項の１つであり、経営層が積極的に関与していくべき事項である。（図表１ を参照）

図表１　ＩＴガバナンスの階層構造



（『金融機関における外部委託に関する有識者検討会報告書』より引用）

[3]一般的にＩＴガバナンスとは、コーポレートガバナンスの中で、ＩＴに関する重要事項について経営層が意思決定を行うための仕組みのことを指す。

２．ＩＴ人材の確保・育成における経営層の関与の留意事項

経営層が、ＩＴ人材の確保・育成に関与する際、以下の点に留意する。

(1) システム戦略を実現するための人員数・スキルの種類とレベル・配置の把握

経営層は、金融機関等の経営の基盤となるＩＴの維持・活用において、必要となるＩＴ人材の人員数や質について、具体的に把握すること。

システム戦略を実現するためには、システム開発や運用のみならず、各システム案件の企画立案・調整・推進と、それらを支える外部委託先の管理や、システムリスクなどのリスク管理、サイバーセキュリティ対応、そしてシステム監査等も重要な業務となる（詳細はＰ15参照）。したがって、経営層は、それらの業務を担う組織の実態を把握することが必要である。

そのうえで、経営層は、システムに対する投資額と同様、ＩＴに係る経営資源の重要な要素であるＩＴ人材について、数及び質（保有するＩＴに関するスキルの種類とレベル・配置・年齢構成等）の実態を把握し、システム戦略を実現するために必要なＩＴ人材とのギャップを把握することが必要である。

なお、金融機関等の業態等によっては、人員の数が少数である現状も踏まえて、特定の人員が複数のスキルを包括的に保有することにも考慮が必要である。

(2) 全体の中長期計画に沿ったＩＴ人材の育成計画の策定

経営層は、ＩＴ人材の現状を踏まえたうえで、中長期経営計画と整合性がとれたＩＴ人材の中長期的な確保・育成計画を策定すること。

ＩＴ人材の確保・育成計画は、中長期経営計画やシステム戦略と整合性を取れたものにする必要がある。そのため、経営層は、その計画策定にあたり、各金融機関の特性にあわせて、対象範囲[4]や対象期間[5]等を明示し、加えてＩＴ人材の評価・処遇や登用の方法に関しても考慮する。

また、策定されたＩＴ人材の確保・育成計画が、全体の計画等に反映させるよう積極的に関与する必要がある。

[4]システム関連会社の業務を対象とするか等。

[5]例えば、システム更改や長期の人材育成等を行うための 10 年計画、中期経営計画に合わせた３年～５年計画、あるいは当該年度計画等。

(3) ＩＴ人材の確保・育成計画策定時の態勢整備

経営層は、ＩＴ人材の確保・育成計画策定に際して、必要に応じて部門横断での組織を立ち上げるなど、関連部門の相互協力が得られる態勢を整備すること。

システム戦略を策定・実現していくためには、システム部門だけに留まらず、システム部門以外の様々な部門（経営企画・営業企画・リスク管理・事務企画・監査・サイバーセキュリティ）、或いは外部委託先等の社外関係者との連携が重要となっている。そのため、ＩＴ人材の確保・育成に関する計画策定は、全社一体で取り組むべき課題として、経営層の積極的な関与のもと、関連部門の相互協力を得られる態勢で進めることが必要である。

協力が得られる態勢として、部門横断での組織を立ち上げる、あるいは計画策定の取りまとめを推進する部門を明確にする等が考えられる。

(4) ＩＴ人材の確保・育成計画策定後の態勢整備

経営層は、ＩＴ人材確保・育成計画を滞りなく遂行できる態勢を整備し、遂行状況を適宜確認し、必要に応じて計画を見直すこと。

ＩＴ人材の確保・育成は継続的に取り組んでいくものであり、その遂行状況や環境変化に応じて、ＰＤＣＡサイクル（ＰＬＡＮ⇒ＤＯ⇒ＣＨＥＣＫ⇒ＡＣＴＩＯＮ）を回しながら、必要に応じて計画を見直すことが必要である。

また、全社の計画と部門単位の計画について連携を取りながら、効果的にＰＤＣＡサイクルを回すことが必要である。

なお、遂行状況の評価を行う期間を設定する際には、以下の観点が考えられる（複数の組~~み~~合せも可~~わせることも考えられる~~）。

・定期的（１年ごと等）な期間設定~~を行う。~~
・ＩＴ中長期計画に沿った期間設定~~を行う。~~
・システムライフサイクルに沿った期間設定~~を行う。~~

また、業務の追加・変更・廃止があった場合や、システムライフサイクルの変更があった場合等には、予め設定した期間に関わらず、計画の見直しが必要になることが考えられる。

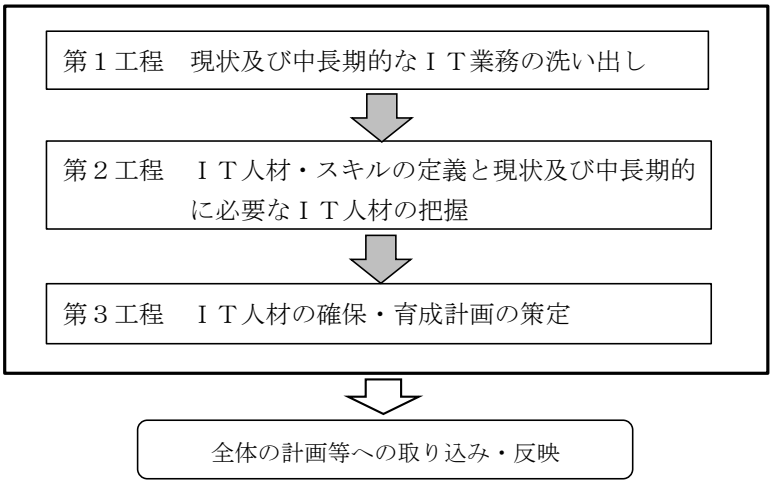
第３編　ＩＴ人材の確保・育成に向けた実務

１．ＩＴ人材の確保・育成計画の策定の流れ

経営層から指示を受けた実務部門は、システム戦略や全体の人材育成方針等を踏まえ、ＩＴ人材の確保・育成計画を策定する。

実際に計画を策定していくための工程を、以下の図表２に示す。

図表２　ＩＴ人材の確保・育成計画の策定の流れ



(1) 第１工程：現状及び中長期的なＩＴ業務の洗い出し

自機関のＩＴ業務を網羅的に把握したうえで、それぞれのＩＴ業務を担うＩＴ人材の役割を明確にする。そのうえで、中長期的に必要となるＩＴ業務の洗い出しを行い、各ＩＴ業務に求められる具体的な役割を明確にする。

(2) 第２工程：ＩＴ人材・スキルの定義と現状及び中長期的に必要な人材の把握

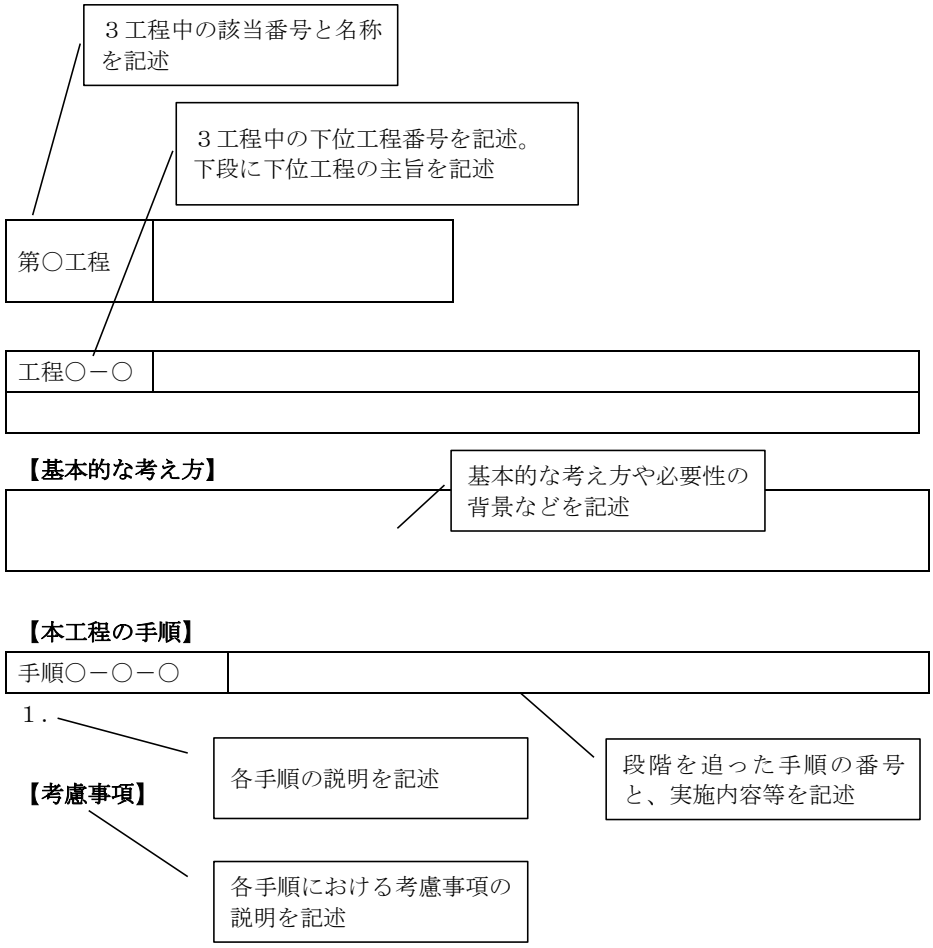
洗い出したＩＴ業務に基づき、必要となるＩＴ人材像と人数、そのＩＴ人材に求められるスキルを定義する。そのうえで、現在及び中長期的なＩＴ人材の過不足を確認する。

(3) 第３工程：ＩＴ人材の確保・育成計画の策定

過不足が見込まれるＩＴ人材の人数とスキルを適正化する施策を検討し、ＩＴ人材の確保・育成計画を取りまとめる。

そして、策定した計画は全体の計画等へ取り込まれ、反映される。なお、ＩＴ人材の確保・育成計画は、一度策定すれば完了するものではなく、必要に応じて見直しを図っていく。

２．本手引書の記述様式


３工程中の該当番号と名称を記述
３工程中の下位工程番号を記述。下段に下位工程の主旨を記述
第〇工程
工程〇－〇
【基本的な考え方】
基本的な考え方や必要性の背景などを記述
【本工程の手順】
手順〇－〇－〇
１．
各手順の説明を記述
段階を追った手順の番号と、実施内容等を記述
【考慮事項】
各手順における考慮事項の説明を記述

３．計画策定の手順

本編では、経営層から指示を受けた実務部門が実際に計画を策定していくための手順や考慮事項を記載する。

第１工程	現状及び中長期的なＩＴ業務の洗い出し

工程１－１	現状のＩＴ業務の洗い出し
ＩＴ人材の確保・育成に関する計画を策定するにあたり、自機関においてＩＴ人材が担うＩＴ業務の洗い出しを行い、各ＩＴ業務に求められる具体的な役割を明確にする。	

【基本的な考え方】

ＩＴ人材の確保・育成に関する計画を策定するにあたっては、まず自機関のＩＴ業務を網羅的に把握したうえで、それぞれのＩＴ業務を担うＩＴ人材の役割を明確にする。

【本工程の手順】

手順１－１－１	現状のＩＴ業務の洗い出しを行う。

１．自機関のすべてのＩＴ業務を把握する。

２．１.にて把握した業務を必要な程度まで細分化する。
　その過程において、外部へ委託している業務の範囲についても明確にする。

手順１－１－２	現状においてＩＴ業務を担当する組織を把握する。

１．洗い出しを行ったＩＴ業務について、担当する組織を把握する。

【考慮事項】

○手順１－１－１（現状のＩＴ業務の洗い出しを行う）

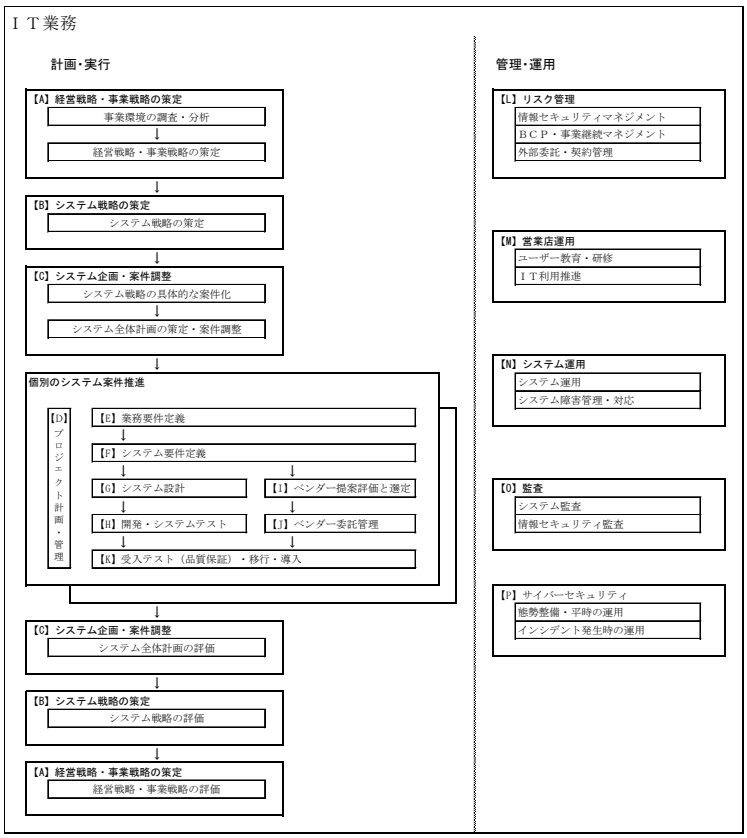
以下では、ＩＴ業務の洗い出しを行う際の作業例を記載するが、業務の定義・配置については、新たに作成するのではなく、既存のものを利用することも考えられる。

１．ＩＴ業務全体の洗い出し

システム開発及びシステム運用に関する業務だけでなく、関連部門におけるＩＴ業務も含めて洗い出しを行う。システム戦略を実現するため、計画・実行サイクルを繰り返して推進する業務と、そのベースとなる恒常的な管理・運用業務に分けて整理する等、全体に漏れが無いよう考慮する。

なお、図表３・図表４に示すＩＴ業務の洗い出しと業務分類は、１つの例であるため、自機関の特性（業態・規模・外部委託している業務範囲等）に応じた、ＩＴ業務の洗い出しと整理を行う必要がある。特に、外部委託している業務については、システム関連~~子~~会社や共同センター、ベンダー等、委託先の形態により、その内容が大きく異なる点についても十分留意する。

図表３　　ＩＴ業務の洗い出しの例



（FISC にて作成）

コメント [A1]:
ご意見 No2 に基づく修正

【人材３－１－③】参照

図表４　ＩＴ業務の洗い出し例（詳細）

業務の分類例	ＩＴ業務の洗い出し例
【A】経営戦略・事業戦略の策定 【B】システム戦略の策定	・自機関を取り巻くＩＴ関連の内外環境を把握・分析する。 ・新しい技術や他金融機関のシステム導入状況に対して、高くアンテナを張り情報収集する。 ・マーケットや顧客のデータ分析により、顧客ニーズを把握・分析する。 ・経営層の意向等を踏まえ、経営戦略を策定するうえで、ＩＴの利活用や新たなＩＴの取込みを検討する。 ・重要なシステム課題を経営課題の１つとして経営層の理解を得たうえで、その対応を反映した経営戦略を立案する。 ・経営戦略に基づき、投資配分の調整や各部門からの要望について優先度を判断・調整のうえ、システム戦略を策定する。 ・策定したシステム戦略に対し、全社の取り組み状況を把握し、経営層に対して進捗等を説明する。 ・サイバーセキュリティなどリスクに関する内外の動向を把握し、情報セキュリティ戦略を策定する。
【C】システム企画・案件調整	・システム戦略を実現するため、具体的なシステム化案件を取りまとめ、全体スケジュールや工数の調整を行う。 ・ユーザー部門からのシステム化要望に対して、最新のＩＴ動向に基づき、導入するパッケージの提案、留意事項の助言などのサポートを行う。 ・データ利活用に必要となるデータ基盤の構築やデータ整備など、自機関システムの俯瞰的な課題に対応する。
【D】プロジェクト計画・管理	・個別システム案件の目的と制約条件を踏まえ、プロジェクト計画を策定する。 ・予算、工程、品質などを管理し、プロジェクトを円滑に運営する。 ・進捗状況を把握し、問題や将来見込まれる課題を早期に把握・認識し、適切な対策・対応を実施することによって、プロジェクトの目標を達成する。
【E】業務要件定義	・営業店や顧客目線でビジネスモデルを企画し、その業務要件をシステム部門やベンダー等に伝える。 ・現場目線による端末オペレーションの改善や、法制度改正で必要となるシステム対応要件を、システム部門やベンダー等に伝える。 ・システム導入を外部発注する場合には、他社事例の調査や複数ベンダーから情報提供を受ける等により、提案依頼書に盛り込む業務要件を検討する。
【F】システム要件定義	・システム案件の目的と業務要件を踏まえた、システム要件を定義する。 ・ユーザー部署と連携し、詳細な業務要件を検討のうえ、システム仕様をまとめる。 ・システム導入を外部発注する場合には、他社事例の調査や複数ベンダーから情報提供を受ける等により、提案依頼書に盛り込むシステム要件を検討する。
【G】システム設計	・システム仕様書に基づき、詳細なシステム設計を行う。 ・システム基盤やメンテナンス方針の検討など、システム運用設計を行う。
【H】システム構築・システムテスト	・システム仕様書に基づき、プログラミングなどシステム構築を行う。 ・システムテスト（単体・結合）及び検証を行う。
【I】ベンダー提案評価と選定	・業務要件とシステム要件を取りまとめ、ベンダーに提案依頼書を発行する。 ・ベンダーから提示を受けた提案内容やコストについて、評価及び契約交渉を行う。
【J】ベンダー委託管理	・ベンダーと連携し、発注するシステムについて要件定義と詳細設計にかかる工程を推進する。 ・ベンダーによる製造・テストの進捗及び課題の管理を行う。
【K】受入テスト移行・導入	・システム部門及びベンダー等と連携し、業務とシステム双方の視点を盛り込んだ、受入テストを行う。 ・システムの導入に向け、一定の試行期間を設けるなど、品質保証にも留意した移行計画・導入計画を策定し、システム部門及びベンダー等と連携して推進する。 ・システムの仕様や変更点などを理解したうえで、操作マニュアルや業務連絡文書を作成し、営業店の役職員に周知・説明する。

コメント [A2]:
ご意見 No2 に基づく修正

【人材３－１－③】参照

業務の分類例	ＩＴ業務の洗い出し例
【L】リスク管理	・システムリスクを含めた、オペレーショナルリスクを把握し、他リスクとの統合管理を行う。 ・システムリスクを定性・定量的に分析し、リスクマネジメント計画を立てる。 ・マネロンなど金融機関として対応が求められる法規制等に対して、規定と態勢を整備する。 ・リスク事象が発生した場合の影響を最小限にする施策をリスクの対応計画にまとめる。 ・情報セキュリティにかかる規程やマニュアル等を策定する。
ＢＣＰ	・災害発生時、中核となる事業の継続あるいは早期復旧を可能とするため、システム面を含めた事業継続計画（BCP）を策定するとともに、訓練等を通じて実効性を高める。
外部委託管理	・情報システムの外部委託に係る方針を決定する。 ・外部委託先の各管理フェーズ（利用検討時・契約締結時・開発時・運用時・終了時・障害発生時等）における、安全対策のチェック事項など基準及び態勢を整備する。 ・外部委託におけるリスク管理に係る改善対策を実施する。
【M】営業店運用	・オペレーション研修の実施等により、自機関におけるシステム利活用を推進し、役職員のＩＴリテラシー向上をはかる。 ・営業店への事務指導、事務ミス事例の分析・改善対応等を通じて、自機関の事務リスク削減を図る。
【N】システム運用	・ハード、ＯＳ、ミドルウェア、ネットワークなどシステム基盤・インフラの運用や管理を行う。 ・安定稼働を確保し、障害発生時において被害の最小化を図るとともに、継続的な改善、品質管理を行う。 ・システム障害などトラブル発生時、関連部門と連携をはかり適切な対応を行う。
【O】監査	・経営戦略及びシステム戦略に基づき、安全対策上必要なＩＴマネジメント（業務執行体制等）が適切に機能していることを点検・評価する。 ・独立した監査部門の視点で、システム部門等の運用状況を監査する。 ①システム開発･運用・障害対応の円滑性･妥当性（サービス・費用　等） ②システム関連資源の管理状況（人・モノ・カネ　等） ③システム関連犯罪、システム障害等の様々な問題への対応と再発防止策の妥当性･実効性の状況 ・経営層に対して、システム監査の結果を報告するとともに、改善のための提言を行う。
【P】サイバーセキュリティ	・本手引書「第４編」を参照。

（金融機関等のヒアリング結果に基づき FISC にて作成）

２．ＩＴ業務の細分化

・ＩＴ業務全体を整理したうえで、それぞれのＩＴ業務を段階的に細分化する。その際、ＩＴ人材が担っている役割がイメージできる程度まで細分化する。

・外部委託している業務についても対象外とせず、ＩＴ業務として定義する。

・サイバーセキュリティ業務など、他の業務分野よりも詳細な分類が必要となる業務については、別表として定めることも考えられる。

図表５　業務の細分化の手順例

ＩＴ業務（大分類）		ＩＴ業務（中分類）	ＩＴ業務（小分類）	外部委託の有無
1	事業環境の調査・分析	経営環境の調査・分析と課題の抽出	・・・・・・・	無
			・・・・・・・	無
			・・・・・・・	無
		顧客ニーズ・マーケティング分析	・・・・・・・	無
			・・・・・・・	有
		業界動向の調査・分析	・・・・・・・	無
			・・・・・・・	無
2	・・・・・			有（共同ｾﾝﾀｰ）

細分化

ＩＴ業務の整理については、以下の資料が参考になる。

（参考）

・『ｉコンピテンシ ディクショナリ（iCD2017）（タスクディクショナリ）』（独立行政法人　情報処理推進機構（IPA）：平成 29 年 6 月）

○手順１－１－２（現状においてＩＴ業務を担当する組織を把握する）

１．細分化したＩＴ業務について、現在担当している組織を把握する。

・部門横断で担当しているＩＴ業務については、主管部門と関連部門に区分けして把握する。

・一時的なプロジェクトチームなど、部門横断の人選によって組成され、部門による担当定義が困難なケースでは、当該組織を部門とみなして担当を定義する。

・外部委託している業務については、委託先を管理している組織を把握する。

・ＩＴ人材の確保・育成を検討する対象範囲にシステム関連会社を含む場合、当該会社が担当するＩＴ業務についても把握する。

図表６　業務の担当組織を把握する手順例

（◎：主管部門　○：関連部門　□：外部委託元）

ＩＴ業務	ＩＴ業務（中分類）	ＩＴ業務（小分類）	外部委託の有無	経営企画部門	営業企画部門	リスク管理部門	事務企画部門	システム部門	…	…
事業環境の調査・分析	経営環境の調査・分析と課題の抽出	・・・・・	無	◎	○	○				
		・・・・・	無	◎		○	○			
		・・・・・	無	◎						
	顧客ニーズ・マーケティング分析	・・・・・	無	○	◎					
		・・・・・	有		□					
	業界動向の調査・分析	・・・・・	無	○				◎		
		・・・・・	無		○			◎		
		・・・・・	無							◎

第１工程	現状及び中長期的なＩＴ業務の洗い出し

工程１－２	中長期的なＩＴ業務の明確化
中長期的に必要となるＩＴ業務の洗い出しを行い、各ＩＴ業務に求められる具体的な役割を明確にする。	

【基本的な考え方】

現状のＩＴ業務に加え、中長期的なシステム戦略や経営層のビジョン等に基づき、必要となるＩＴ業務を明確にする。

【本工程の手順】

手順１－２－１	中長期的に必要なＩＴ業務を明確にする。

１．ＩＴ人材の確保・育成計画の対象となる期間において、新たに必要となる、あるいは不要となるＩＴ業務を明確にする。

２．業務を必要な程度まで細分化する。

手順１－２－２	中長期的なＩＴ業務を担当する組織を明確にする。

１．ＩＴ業務を担当する組織を検討し、明確にする。

【考慮事項】

○手順１－２－１（中長期的に必要なＩＴ業務を明確にする）

１．中長期的に必要なＩＴ業務を検討、明確にするにあたっては、中長期的なシステム戦略や経営層のビジョンに基づいた検討を行う必要がある。また、その際、ＩＴ業務を外部委託するかどうかについても検討し、外部委託する場合はその範囲を明確にする。

２．環境変化の考慮

ＩＴ業務が現状から変化するケースとしては、例えば以下のようなことが考えられる。

・制度対応や規制対応が必要な場合。
・新しいＩＴへの対応が必要な場合。
・ＩＴを利用した事業の改廃がある場合。

３．自機関のシステムライフサイクル状況の考慮

中長期的な観点から、自機関のシステムライフサイクルの状況を把握したうえで、必要なＩＴ業務を決定する必要がある。例えば、大規模なシステム更改が予定されているのであれば、それに応じた人員配置を行う必要が生じるほか、システム更改後の運用フェーズについても考慮することになる。これは外部委託先についても同様であの考慮をすることになる。

○手順１－２－２（中長期的なＩＴ業務を担当する組織を明確にする）

１．中長期的に必要となるＩＴ業務を担当する組織を検討するとともに、現状のＩＴ業務を担当する組織を見直すケースとしては、例えば以下のようなことが考えられる。

・複数部門で同一業務を実施していることが分かり、単独部門への統合を予定している場合。

・単独部門で実施していた業務を、関連部門を含めた部門横断の業務へと変更する場合。

２．部門横断で担当しているＩＴ業務については、主管部門と関連部門を区分けして、後工程でＩＴ人材配置を検討するうえで、求められるレベルをイメージしやすいよう考慮する。

３．一時的なプロジェクトチームなど、部門横断の人選によって組成され、部門による担当定義が困難なケースは、当該組織を部門とみなして、担当を定義する。

４．外部委託している業務については、委託先を管理する組織を定義する。

外部委託の検討においては、多岐にわたるＩＴ業務全体を俯瞰し、まず業務単位で外部へ委託するものがあれば、それを明確にしておく。外部へ委託するかどうかは組織の規模、ＩＴ予算、情報資産に対するリスク、セキュリティポリシーなどにより変化することが考えられ、自機関の状況に沿った選択が必要となる。

図表７　中長期的なＩＴ業務・担当組織の整理の手順例

＜経営層のビジョン（例）＞

・データ分析に関する業務が重要となるため、自機関でＩＴ人材を育成したい。

・ＩＴ動向は経営戦略・事業戦略内容にも大きく影響するため、経営戦略・事業戦略を策定する主管部門が、ＩＴ業界動向の調査・分析を主体的に行い、理解を深めるべき。

（◎：主管部門　○：関連部門　□：外部委託元）

ＩＴ業務	ＩＴ業務（中分類）	ＩＴ業務（小分類）	外部委託の有無	経営企画部門	営業企画部門	リスク管理部門	事務企画部門	システム部門	…	…
事業環境の調査・分析	経営環境の調査･分析と課題の抽出	・・・・・	無	◎	○	○				
		・・・・・	無	◎		○	○			
		・・・・・	無	◎						
	顧客ニーズ･マーケティング分析	・・・・・	無	○	◎					
		・・・・・	外部委託から内製化を図る。		□→◎					
	業界動向の調査・分析	・・・・・	無	○→◎				◎→○		
		・・・・・	無		○→◎			◎→○		
		・・・・・	無							◎
・・・・	・・・・・		無							

第２工程	ＩＴ人材・スキルの定義と現状及び 中長期的に必要となるＩＴ人材の把握

工程２－１	ＩＴ人材・スキルの定義

自機関のＩＴ業務において必要となるＩＴ人材（人材像）を定義する。
求められるＩＴ人材のスキルを定義するとともに、その評価方法を検討する。

【基本的な考え方】

自機関にて対応すべきＩＴ業務を明確にした後、その業務を実際に遂行するＩＴ人材像とスキルを定義する。

ＩＴ人材像やスキルについては、現場へのヒアリングなどを通して新たに作成することも考えられるが、既存の資料（自機関で既に使用しているスキルマップや計画書等）をカスタマイズして作成することも考えられる。なお、ＩＴ人材像については、必ずしも役職を設定する必要はなく、役割等として定義し、既存の役職者が担うことも考えられる。また、スキルについては、詳細なものを作成する場合もあれば、概要のレベルに留めることも考えられる。~~後者の場合、必要に応じて細分化できるよう情報を整理しておくことが考えられる。~~

【本工程の手順】

手順２－１－１	ＩＴ業務に求められる役割からＩＴ人材を定義する。

１．第１工程で整理したＩＴ業務をもとに、それぞれの業務で求められる役割毎にグループ化して必要となるＩＴ人材を定義する。

手順２－１－２	求められるＩＴ人材のスキルを定義する。

１．求められるＩＴ人材のスキル（~~例として、~~知識、~~／~~業務経験、~~／~~技量[6] 等）~~とその評価方法~~を定義する。

２．定義したスキルについて、その評価方法を検討する。スキルの評価方法としては、知識については受講研修・保有~~取得~~資格、業務経験については実務上の立場・経験プロジェクト規模、技量~~(※)~~については面談や適性診断による確認等が考えられる。

~~※「技量」とは、コミュニケーション能力等のヒューマンスキルや、「新規開拓を求める」「安定維持を求める」などの行動特性・思考特性を総称している。~~

[6] 「技量」とは、コミュニケーション能力等のヒューマンスキルや、「新規開拓を求める」「安定維持を求める」などの行動特性・思考特性を総称している。

【考慮事項】

○手順２－１－１（ＩＴ業務に求められる役割からＩＴ人材を定義する）

１．ＩＴ人材の役割を整理する。

ＩＴ人材の役割の名称や区分けについては、必ずしも新たに定義する必要はなく、既に使用している名称など、自機関で馴染みのあるものを使用することが考えられる。

２．求められるＩＴ人材像を定義する。

１．に基づき、求められるＩＴ人材像を定義する。例としては、以下のような整理が考えられる。

図表８　ＩＴ人材の役割・人材像の整理例

ＩＴ人材の役割の分類		担うべき業務		求められるＩＴ人材像
1	戦略策定 経営戦略・ 事業戦略 システム戦略	経営・事業環境の調査・分析	経営環境の調査・分析と課題抽出 業界動向の調査・分析	・IT に関する知識は、専門家レベルである必要はないが、IT ソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をシステム戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やシステム戦略の企画・立案ができる人材。 ・戦略に基づく計画の管理に関して、実行だけでなく評価と改善ができる人材。
		経営・事業戦略の策定	基本構想の策定 アクションプランの策定 事業戦略実行体制の確立	
		経営・事業戦略の評価	戦略全体の評価 費用対効果の検証 次期戦略への反映	
		システム戦略の策定	現状分析・IT 動向分析 システム基本方針の策定 システム中期計画の作成 情報セキュリティ戦略の策定	
		システム戦略評価・改善	戦略全体の評価 費用対効果の検証 次期戦略への反映	
2	システム企画	システム戦略の具体的な案件化	現行業務・システムの分析 投資規模の策定 全体構想のシステム案件化	・ＩＴに関するコスト感覚を持ち、システム工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。
		システム全体計画の策定	全体開発スケジュールの作成 費用と投資効果の予測 全体工数による案件調整	
		システム全体計画の評価	計画全体の評価 投資管理・費用対効果の検証 次期計画への反映	
3	プロジェクト管理	プロジェクト計画・管理	プロジェクト立ち上げ・終結 プロジェクト計画策定 プロジェクト実行管理	・システムに関する幅広い知識と経験があり、開発全体の流れを把握できる人材。 ・システム開発の進捗管理、システム登録、品質管理までできる人材。 ・スケジュール管理とプロジェクトの統制ができる人材。

コメント [A3]:
ご意見 No3～9 に基づく修正

【人材３－１－③】参照

ＩＴ人材の役割の分類		担うべき業務		求められるＩＴ人材像
4	業務設計・システム導入	業務要件定義	対象業務の課題整理 新業務モデルの作成 業務要件の定義	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、システム部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価及び交渉することができる人材。 ・ベンダーからの提示見積もりに対して、相見積りをとる等により妥当性を判断できる人材。 ・システム部門やベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受入れテストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。
		（外部委託） ベンダー提案評価と選定	提案依頼書の作成と発行 提案書の比較検討・委託先選定 発注契約手続	
		（外部委託） ベンダー開発管理	委託業務の開始・管理 進捗状況の把握とリスク対策 成果物の検収	
		移行・導入	受入れテスト マニュアル作成・研修 移行・導入実施	
5	システム設計・開発	システム要件定義	システム要件定義 セキュリティ要件定義 概算工数の見積り	・業務要件を整理し、システム要件を定義できる人材。 ・業務部門からの要請に対して対応できる人材。 ・業務部門からの業務要件を補えることのできる人材。 ・システム設計書、仕様書が書ける人材。 ・システム運用を考慮したシステム設計により、「工程の後戻り防止」や、「運用品質の向上」が図れる人材。 ・システム構築・プログラミングができる人材。 ・システム検証・プログラム検証ができる人材。
		（自営開発） システム設計	方式設計･アプリケーション設計 システム運用設計 保守計画・移行計画の策定	
6	システム運用	システム運用	システム監視・資源管理・性能管理 構成管理・変更管理・リリース管理 保守管理・予防保守	・ハード面の性能・リソースなどが適正であるかを管理・評価できる人材。 ・自機関システムのＯＳ・ミドルウェアなど基盤となるソフトウェアを俯瞰的に把握し、ライセンスや保守等を含め管理できる人材。 ・ネットワークがわかる人材。 ・システムの安定稼働を維持するための運用設計や運用環境の改善を継続的に提言できる人材。 ・ベンダーからの運用報告を確認、分析し、会話のできる人材。 ・オペレータの人的管理ができる人材。 ・障害等のインシデント発生時において、被害の最小化を図るとともに、品質管理などに主導的な役割を果たし、上層部に事態や対応策等について説明できる人材。
		システム障害管理・対応	システム障害検知 システム障害の初動処理 システム障害の分析・復旧・再発防止	

ＩＴ人材の役割の分類		担うべき業務		求められるＩＴ人材像
7	サイバーセキュリティ	本手引書「第４編」参照		本手引書「第４編」参照
8	リスク管理	情報セキュリティマネジメント	情報セキュリティ方針の策定 情報セキュリティの運用/見直し サイバーセキュリティ対策	・システムリスクを含め、各部署のリスクを俯瞰的に管理・対応できる人材。 ・リスクの存在に気付ける人材。 ・経営層など上層部に対して、リスクの所在や事態を説明できる人材。 ・訓練実施など企画立案ができる人材。
		ＢＣＰ・事業継続マネジメント	事業継続計画の策定 事業継続計画の運用・訓練 事業継続計画の見直し	
9	システム監査	システム監査	システム監査計画の策定 システム監査の実施 システム監査結果の報告	・情報システムを総合的に点検、評価できる人材。 ・監査結果を関係者に説明して改善を勧告できる人材。 ・点検レベルではなく、ルールの提案までできる人材。
10	外部委託管理	外部委託・契約管理	外部委託先の調査 委託契約内容の確認 定期モニタリング	・チェックリストに基づく確認だけに留まらず、中身まで分かる人材。 ・外部委託先からの報告内容を把握し、必要に応じ提案等できる人材。 ・経営層など上層部に対して、外部委託に関するリスクの所在を説明できる人材。 ・外部委託先のシステムリスクを評価し、改善点を勧告できる人材。
11	自機関内教育・業務運用	ユーザー教育・研修	ヘルプデスク オペレーション研修 臨店事務指導	・営業店にて対して事務の指導ができる人材。 ・営業店事務の知識と経験がある人材。 ・現場目線で必要とする機能を集約し、具体的なシステム改善案を提案できる人材。
		ＩＴ利用推進	ＩＴシステム活用促進 全体のＩＴ活用能力底上げ 活用シナジーの促進	
12	データ利活用	経営・事業環境の調査・分析	顧客ニーズ・マーケティング分析	・データベース等の知識があり、必要な情報を抽出して利活用できる人材。 ・データ分析の目的を理解し、目的に応じたシナリオを設定のうえ、データ分析や加工が出来る人材。 ・システム部門から提供されるデータを活用できる人材。 ・データ利活用に向け、自機関が保有するデータの整備やデータ基盤の構築に対応できる人材。
		システム企画	データ利活用に必要なデータ整備	

○手順２－１－２（求められるＩＴ人材のスキルを定義する）

１．ＩＴ人材像（ＩＴ人材に求められる業務役割）から、求められるスキル（~~例として、~~知識、~~／~~業務経験、~~／~~技量~~等）と評価方法を定義する。スキルの評価方法の策定については、試行・評価・改善を繰り返して精度を高めていく。そのため、まず小規模な範囲で試行する等を考慮する。また、評価方法については、評価対象者に合意されていることや、評価者向け研修等により自機関内の標準として認知されていることも考慮する。

図表９　ＩＴ人材に求められるスキルの整理例

ＩＴ人材の役割の分類		求められるＩＴ人材像	スキル		
			知識	経験	技量
1	戦略策定 経営戦略 事業戦略 システム戦略	・IT に関する知識は、専門家レベルである必要はないが、IT ソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をシステム戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やシステム戦略の企画・立案ができる人材。 ・戦略に基づく計画の管理に関して、実行だけでなく評価と改善ができる人材。	・自機関内外の事業環境 ・ＩＴ基礎知識 ・金融機関のＩＴ動向 ・新しいＩＴ技術 ・ＩＴの活用事例 ・ＳＷＯＴ分析 ・業務改善技法 ・開発投資対効果 ・評価指標（ＫＧＩ・ＫＰＩ）	経営企画部門 〇年以上	・コミュニケーション ・ネゴシエーション ・マネジメント ・創造力
2	システム企画	・ＩＴに関するコスト感覚を持ち、システム工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。	・自機関内のＩＴ全般に関する知識 ・ＩＴポートフォリオ ・新しいＩＴ技術 ・ＩＴの活用事例 ・開発スケジュール立案に関する知識 ・開発投資対効果	システム部門 〇年以上	・コミュニケーション ・マネジメント ・本質（目的）思考力
3	プロジェクト管理	・システムに関する幅広い知識と経験があり、開発全体の流れを把握できる人材。 ・システム開発の進捗管理、システム登録、品質管理までできる人材。 ・スケジュール管理とプロジェクトの統制ができる人材。	・自機関内のＩＴ全般に関する知識 ・プロジェクト管理 ・開発スケジュール立案に関する知識 ・評価指標（ＫＧＩ・ＫＰＩ） ・問題解決手法	業務設計・システム導入 〇件以上	・コミュニケーション ・マネジメント ・問題発見・解決力 ・プレゼンテーション
4	業務設計・システム導入	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、システム部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価及び交渉することができる人材。 ・ベンダーからの提示見積もりに対して、相見積等をとる等により妥当性等を判断できる人材。 ・システム部門やベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受入れテストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。	・営業店業務知識 ・情報システム関連法規 ・ＩＴ基礎知識 ・担当する業務システムの知識（預金・融資・為替・対外等） ・新しいＩＴ技術 ・ＩＴの活用事例 ・業務改善技法 ・開発投資対効果 ・品質マネジメント	営業店業務 〇年以上 業務・商品の企画業務 〇年以上	・コミュニケーション ・ネゴシエーション ・本質（目的）思考力 ・実行・実践力

コメント [A4]:
ご意見 No3～10 に基づく修正

【人材３－１－③】参照

ＩＴ人材の役割の分類		求められるＩＴ人材像	スキル		
			知識	経験	技量
5	システム設計・開発	・業務要件を整理し、システム要件を定義できる人材。 ・業務部門からの要請に対して対応できる人材。 ・業務部門からの業務要件を補えることのできる人材。 ・システム設計書、仕様書が書ける人材。 ・システム運用を考慮したシステム設計により、「工程の後戻り防止」や、「運用品質の向上」が図れる人材。 ・システム構築・プログラミングができる人材。 ・システム検証・プログラム検証ができる人材。	・プログラム知識 ・開発ツールの知識 ・データベース知識 ・システム基盤構築の知識 ・業務知識 ・担当する業務システムの知識（預金・融資・為替・対外等） ・テスト手法・テストツール		・論理的思考 ・問題分析・解決力 ・継続力 ・コミュニケーション
6	システム運用	・ネットワークがわかる人材。 ・ハード面の性能・リソースなどが適正であるかを管理・評価できる人材。 ・自機関システムのＯＳ・ミドルウェアなど基盤となるソフトウェアを俯瞰的に把握し、ライセンスや保守等を含め管理できる人材。 ・システムの安定稼働を維持するための運用設計や運用環境の改善を継続的に提言できる人材。 ・ベンダーからの運用報告を確認、分析し、会話のできる人材。 ・オペレータの人的管理ができる人材。 ・障害等のインシデント発生時において、被害の最小化を図るとともに、品質管理などに主導的な役割を果たし、上層部に事態や対応策等について説明できる人材。	・自機関内のシステム基盤及びインフラに関する知識（ハード、ＯＳ、ミドルウエア、ネットワークなど） ・ＩＴ基礎知識 ・セキュリティ動向		・問題発見・分析力 ・継続力 ・コミュニケーション
7	サイバーセキュリティ	本手引書「第４編」参照	本手引書「第４編」参照		
8	リスク管理	・各部署のリスクを統合管理・分析することのできる人材。 ・サイバーセキュリティを含めシステムリスクを俯瞰的に管理・対応できる人材。 ・リスクの存在に気付ける人材。 ・経営層など上層部に対して、リスクの所在や事態を説明できる人材。 ・訓練実施など企画立案ができる人材。	・業務知識 ・情報システム関連法規 ・ＩＴ基礎知識 ・リスク分析・管理手法 ・情報セキュリティ管理手法 ・ＢＣＰ関連知識	システム部門 ○年以上	・コミュニケーション ・ネゴシエーション ・マネジメント ・創造力
9	システム監査	・情報システムを総合的に点検、評価できる人材。 ・監査結果を関係者に説明して改善を勧告できる人材。 ・点検レベルではなく、ルールの提案までできる人材。	・自機関内のＩＴ全般に関する知識 ・情報システム関連法規 ・システム監査手法 ・品質マネジメント ・リスク分析・管理手法 ・情報セキュリティ管理手法 ・業務改善手法	システム部門 ○年以上	・コミュニケーション ・マネジメント ・本質（目的）思考力 ・論理的思考 ・問題分析・解決力
10	外部委託管理	・チェックリストに基づく確認だけに留まらず、中身まで分かる人材。 ・外部委託先からの報告内容を把握し、必要に応じ提案等できる人材。 ・外部委託先のシステムリスクを評価し、改善点を勧告できる人材。	・業務知識 ・情報システム関連法規 ・外部委託先に関する情報 ・ＩＴ基礎知識 ・情報セキュリティ管理手法		・コミュニケーション ・ネゴシエーション ・マネジメント

ＩＴ人材の役割の分類		求められるＩＴ人材像	スキル		
			知識	経験	技量
11	社内教育・業務運用	・営業店にて対して事務の指導ができる人材。 ・営業店事務の知識と経験がある人材。	・営業店業務知識 ・担当する業務システムの知識（預金・融資・為替・対外等）	営業店業務 ○年以上	・コミュニケーション ・創造力 ・実行・実践力
12	データ利活用	・データベース等の知識があり、必要な情報を抽出して利活用できる人材。 ・データ分析の目的を理解し、目的に応じたシナリオを設定のうえ、データ分析や加工が出来る人材。 ・システム部門から提供されるデータを活用できる人材。 ・データ利活用に向け、自機関が保有するデータの整備やデータ基盤の構築に対応できる人材。	・自機関内データベースの知識 ・社内外の事業環境 ・データ分析手法 ・マーケティング分析手法 ・セグメンテーション		・本質（目的）思考力 ・実行・実践力 ・継続力

スキルの整理については、以下の資料が参考になる。

（参考）

・『ｉコンピテンシ ディクショナリ（iCD2017）　（スキルディクショナリ）』（独立行政法人情報処理推進機構（IPA）：平成 29 年 6 月）

第２工程	ＩＴ人材・スキルの定義と現状及び 中長期的に必要となるＩＴ人材の把握

工程２－２	現状のＩＴ人材の把握と中長期的に必要となるＩＴ人材の確認
現状のＩＴ人材の人数とスキルを把握し、システム戦略の実現に必要なＩＴ人材の人数とスキル、及び、それらの過不足を解消すべき時期を確認する。	

【基本的な考え方】

具体的なＩＴ人材像（又は役割）、スキル、スキルマップ等、全体像の把握が可能なものを作成し、ＩＴ人材の現状とシステム戦略を実現するために理想的な状況とのギャップを把握する。

【本工程の手順】

手順２－２－１	ＩＴ人材の現状（人数・レベル）と想定される今後の推移を把握する。

１．定義したＩＴ人材・スキルの自機関内／自機関外（外部委託先等）の実態を整理する。

２．現状の各部門におけるＩＴ人材の人数とスキルを確認する。自機関外（外部委託先等）については、人員規模と提供を受けているスキルを把握する。

３．中長期的に~~み~~見込まれる~~た~~ＩＴ人材の増減（退職等による減少など）を把握する。

手順２－２－２	システム戦略に必要な中長期的なＩＴ人材の人数とスキルを定義する。

１．システム戦略に基づき、必要となるＩＴ人材の人数とスキルを定義する。

２．定義したＩＴ人材・スキルの自機関内／自機関外（外部委託先等）の区分けを行う。

手順２－２－３	現状と中長期的な目標とのギャップ分析を行う。

１．自機関内において、ＩＴ人材の人数とスキルの過不足を分析する。

２．各業務のＩＴ人材不足が業務遂行に与える影響度を勘案しながら、ＩＴ人材の人数とスキルの過不足を解消すべき時期を検討する。

【考慮事項】

○手順２－２－１（ＩＴ人材の現状と想定される今後の推移を把握する）

現状のＩＴ人材の人数とスキルを把握するにあたり、実際には関連部門に対して判定作業の依頼が必要となる場合もある。その場合、~~スキルのレベルを導入する~~レベル判定の基準を設定する（図表 10 参照）などにより、部門間でスキル判定などの基準が大きく相違しないよう考慮する。

~~なお~~ただし、部門ごとに判定作業を行う場合は、以下の~~本手順において、現在、スキルを持った人材がＩＴ業務を行っていない組織に配置されている場合、ＩＴ人材として認識されない可能性がある。また、ＩＴ業務を行っている組織に配置されている場合でも、業務に必要のない個々人のスキルは把握されない可能性がある。そのため、配置転換検討など、第３工程で確保・育成計画を策定する際には、これらの点について考慮する~~ＩＴ人材やスキルが把握されない可能性がある点を考慮する。

・ＩＴ業務を行っていない部門に配置されているＩＴ人材（その部門が、判定作業の対象外となる可能性）

・部門のＩＴ業務に必要のない個々人のスキル（そのスキルが、部門における判定作業の対象外となる可能性）

○手順２－２－２（システム戦略に必要な中長期的なＩＴ人材の人数とスキルを定義する）

~~中長期的に必要なＩＴ人材の人数・スキルの整理にあたっては、業務の優先度を勘案する。~~

~~なお、~~自機関におけるＩＴ人材の人数とスキルの維持については、自機関のシステムの保有形態に合わせて、以下のような方針が考えられる。

・自機関でシステム構築を行う場合、システム部門が開発の中心となり、自機関で実際の開発を行える人数とスキルを維持する。

・システム構築を外部へ委託する場合、外部~~委託先の~~に委託する業務の理解、外部委託先との円滑なコミュニケーション等により、外部委託先を管理できる人数とスキルを維持する。また、自機関にて構築しているシステムとの連携を管理できる人数とスキルを維持する。

コメント [A5]:
ご意見 No15 に基づく修正

本文のどこかに「Ｌｅｖｅｌ」（図表 10）に関する言及があった方がよい。

コメント [A6]:
事務局にて修正

コメント [A7]:
ご意見 No12 に基づく修正

この記載は不要。

コメント [A8]:
ご意見 No13 に基づく修正

「外部委託先の業務の理解」より、「外部に委託する業務の理解」が正しいと思う。

コメント [A9]:
ご意見 No14 に基づく修正

基幹システムを共同センター等に外部委託し利用している場合、共同システムを有効利用するための業務知識とシステム分析能力を兼ね備えたＩＴ人材が必要であり、自社の独自システムとの連携をマネジメントできる人数とスキルを維持する。

○手順２－２－３（現状と中長期的な目標とのギャップ分析を行う）

ＩＴ人材とスキルの過不足の解消時期については、中長期計画との整合性を意識して整理する。

図表 10　ＩＴ人材の現状把握とギャップ分析例

	レベル判定の基準(例)
Level 4	全社的な第１人者として、主体となって推進できる。 他部署を含めて下位者の指導ができる。
Level 3	部署内の第１人者として、主体となって推進できる。 部署内の下位者を指導・サポートできる。
Level 2	担当する部分的な業務を独力で推進できる。
Level 1	上位者の指導・サポートを受けながら役割を遂行する。

必要に応じて各部門に基準を示し、判定作業を依頼する。

ＩＴ人材の役割の分類		求められるＩＴ人材像	業務配置（◎：主管部門　○：関連部門　□：外部委託元）													
			経営企画		営業企画		事務企画		システム		リスク管理		・・・・	全社合計	
			レベル	Asis	Tobe	Asis	Tobe	Asis	Tobe	Asis	Tobe	Asis	Tobe		Asis	Tobe
1	経営戦略・システム戦略	・ITに関する知識は、専門家レベルである必要はないが、ITソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をＩＴ戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やＩＴ戦略の企画・立案ができる人材。		◎主管部門					○関連部門							
			Level 4	1	2					0					1	2
			Level 3	0	2					1					1	2
			Level 2	2						1	2				3	2
			Level 1	2						0					2	0
2	システム企画	・ＩＴに関するコスト感覚を持ち、システム工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。		○関連部門					◎主管部門							
			Level 4	0						1	3				1	3
			Level 3	1	2					1	3				2	5
			Level 2	3	2					3					6	2
			Level 1	2						2					4	0
3	プロジェクト管理	・システムに関する幅広い知識と経験があり、開発全体の流れを把握できる人材。 ・システム開発の進捗管理、システム登録、品質管理までできる人材。 ・スケジュール管理とプロジェクトの統制ができる人材。				○関連部門		○関連部門		◎主管部門						
			Level 4			0		0		1	3				1	3
			Level 3			0	1	0	2	2	4				2	7
			Level 2			1	2	2	2	2					5	4
			Level 1			2		2		2					6	0
4	業務設計・システム導入	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、システム部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価および交渉することができる人材。 ・ベンダからの提示見積もりに対して、相見積等をとる等により妥当性等を判断できる人材。 ・システム部門やベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受け入れテストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。				◎主管部門		◎主管部門		○関連部門						
			Level 4			0		1	1						1	1
			Level 3			0	2	2	4						2	6
			Level 2			1		3		8	6				12	6
			Level 1			4		2		6					12	0

・ＩＴ業務の主管部門と関連部門では、ＩＴ人材として求められるスキルにも違いが生じるものが考えられる。

・ＩＴ人材適正化の方法（育成・配置転換等）を検討するうえで、部門毎の各スキルに対応した人員数を確認し、あるべき姿とのギャップを把握することが考えられる。

第３工程	ＩＴ人材の確保・育成計画の策定

工程３－１	ＩＴ人材の確保・育成計画の策定
過不足が見込まれるＩＴ人材の人数とスキルの適正化を検討し、ＩＴ人材の確保・育成計画として取りまとめる。	

【基本的な考え方】

具体的なＩＴ人材確保・育成の手段を策定する。

「確保」とは、自機関において要員を確保することに加えて、ＩＴ人材を外部から調達することも含まれる。「育成」とは、自機関のＩＴ業務に必要な人材を、自機関の要員として育成することである。

中長期的な観点からＩＴ業務を洗い出し、担当部門のＩＴ人材が不足した場合、組織に与える影響の大きさ、業務の優先度などを勘案して適正化の方策を検討する必要がある。

【本工程の手順】

手順３－１－１	過不足が見込まれるＩＴ人材の適正化方針をの検討する。

１．過不足が見込まれるＩＴ人材の適正化策として、育成、採用、配置転換、外部の人的資源[7]の活用等が考えられ、どのような方法を選択するかについて検討する。

手順３－１－２	育成による適正化をの検討する。

１．現状における育成施策を把握する。

２．知識レベルの向上策として、研修、資格取得等が考えられ、どのような方法を選択するかを検討する。

３．経験レベルの向上策として、キャリアパス設定、ジョブローテーション制度等が考えられ、どのような方法を選択するかを検討する。

４．技量レベルの向上策として、研修、実務での経験等が考えられ、どのような方法を選択するかを検討する。

[7]委託、派遣等、各種の契約形態を含めた外部の人員。

手順３－１－３	配置転換による適正化を~~の~~検討する。

１．現状における配置転換施策を把握する。

２．過不足のあるＩＴ人材の配置転換の方法を検討する。

手順３－１－４	外部の人的資源の利用による適正化を~~の~~検討する。

１．現状における外部の人的資源の利用施策を把握する。

２．過不足のあるＩＴ人材について、外部の人的資源の利用方法を見直す。

手順３－１－５	採用による適正化を~~の~~検討する。

１．現状における採用施策を把握する。

２．不足しているＩＴ人材を採用するための方法を検討する。

手順３－１－６	各適正化方策を補助する施策を~~の~~検討する。

１．現状における補助施策~~を~~の把握~~する~~と必要とされる補助施策を検討する。

コメント [A10]: 事務局にて修正

~~２．ＩＴ人材のスキル評価とそのフィードバック方法を検討する。~~

~~３~~２．人員が定着するための制度を検討する。

３~~４~~．育成における知識や技量レベルについては、研修や資格取得の補助制度を検討する。

コメント [A11]:
ご意見 No19 に基づく修正

「知識レベル」に限定しなくてもよい。

手順３－１－７	ＩＴ人材のスキル評価とそのフィードバック方法を~~の~~検討する。

１．各種適正化を検討する際、具体的なスキルの評価とそのフィードバック方法を検討する。

コメント [A12]:
ご意見 No18 に基づく修正

「２．IT 人材のスキル評価とそのフィードバック方法を検討する」とあるが、これは「補助する施策」として「手順３－１－６」ではなく、どこかに切り出して記載するのがよい。

【考慮事項】

○手順３－１－１（過不足が見込まれるＩＴ人材の適正化方針~~の~~を検討する）

１．ＩＴ人材の適正化施策を検討する際には、その施策のコストと予算確保に留意する必要がある。また、限られた経営資源の中で、すべてのＩＴ人材について適正化を同時に進めることが困難な場合は、システム戦略等の観点から、優先度を考慮して、各ＩＴ人材にお

ける適正化の時期を検討する。

２．ＩＴ人材の適正化施策を検討する際には、組織全体としての採用、育成、配置転換、外部の人的資源の活用方針等との整合性を取ることが考えられる。

○手順３－１－２（育成による適正化~~の~~を検討する）

育成策としては、次のようなことが考えられる。

１．現場での実践（OJT）

２．資格取得の奨励

資格取得は、客観的な評価手段として活用可能であり、モチベーションアップにもつなげることができる。

３．外部研修への参加

外部研修等への参加については、ベンダーやセキュリティベンダーが提供する研修への参加、大学が提供する社会人教育への参加などが考えられる。

４．外部への出向

外部出向の効果として、以下が挙げられる。

・現場経験を積むことにより、不足しているスキルを向上させる機会を得ることができる。

・違う立場、違う組織で、違う価値観に触れる機会を得ることにより、ものの見方を培うことができるとともに、人脈を築くことができる。

なお、出向先の候補として、以下が挙げられる。

・システム関連~~子~~会社への出向

・共同センターへの出向

・ＩＴベンダーへの出向等

５．外部からのＩＴ人材の受入れによるノウハウの習得

ベンダーやシステム関連~~子~~会社からの出向者を自機関のシステム部門等に受入れ、自機関の社員とともに業務を担ってもらうことで社員にノウハウを吸収させることも考えられる。

○手順３－１－３（配置転換による適正化~~の~~を検討する）

１．手順２－２－１にて記載の「現状のＩＴ人材の把握」が実施された時点で、スキルを持った人材がＩＴ業務を行っていない組織に配置されている場合、ＩＴ人材として認識されない可能性がある。また、ＩＴ業務を行っている組織に配置されている場合でも、部門のＩＴ業務に必要のない個々人のスキルは把握されない可能性がある~~その~~

~~業務に必要のない個々人のスキルは把握されない可能性がある~~。組織の人的資源をさらに有効活用するための配置転換を検討するにあたっては、これらの点について考慮する。

２．高いスキルを持つ人材の定年退職やジョブローテーション等に備え、後進を育成できるような配置について考慮する。

○手順３－１－６（各適正化方策を補助する施策~~の~~を検討する）

１．スキル評価と人事評価との関連

スキル評価と人事評価（待遇・報酬に結び付く評価）との関連については、スキルの評価基準・評価方法を定義し、その評価プロセスが適切に運用されるよう整備した上で検討することが考えられる。

２．研修の奨励

自機関内外の研修による育成を行う場合、その研修期間は業務を離れることになるため、そのことを奨励あるいはある程度の強制力を持った制度を作ることも考えられる。また、業務の現場にて各人がその必要性を認識するような教育も考えられる。

コメント [A13]:
ご意見 No20 に基づく修正

「業務に必要のない個々人のスキルは把握されない可能性がある」との記載について、意味がわかりづらい。

第４編　サイバーセキュリティ人材の確保・育成に関する考慮事項

１．本編の使用にあたって~~方法~~

本編の使用にあたっては、第３編「ＩＴ人材の確保・育成に向けた実務」にて記載のＩＴ人材の確保・育成に向けた各工程・手順に沿うことを前提としている。また、同様に第３編に記載の考慮事項と合わせて参照することを想定している。

また本編では、サイバーセキュリティに関係する業務の分類やインシデント対応組織の役割など当センターが発刊した『金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）』（以下、『コンテ手引書』という）から引用している。詳細については、『コンテ手引書』を参照のこと。

２．~~３．~~本編で使用する用語

本編で使用する用語について、以下のとおり定義する。

・インシデント

一般的には、自組織のシステムにおいて発生する可能性のある事故・事象を指す。[8]

本編では、特にサイバー攻撃等により発生する事故・事象を指す。

・インシデント対応組織

インシデントに実際に対応する組織を指す。代表的なものとして、CSIRT（Computer Security Incident Response Team）がある。

・サイバーセキュリティ

サイバー攻撃により、情報の漏えいや、期待されていた情報システム等の機能が果たされないといった不具合が生じないようにすること。[9]

・サイバーセキュリティ業務

インシデントの検知及び対応等のインシデント発生時の業務のみならず、平時の運用を含めたサイバー攻撃対応を主体とした業務。

・サイバーセキュリティに関係する業務

サイバーセキュリティ業務のみならず、戦略策定・経営戦略・事業戦略・システム戦略や、個別システム案件管理、リスク管理等、企業活動の中でサイバーセキュリティに関係する業務全般。

・サイバーセキュリティ人材

サイバーセキュリティに関係する業務を担う人材を指す。

[8] インシデントハンドリングマニュアル、一般社団法人　JPCERT コーディネーションセンター、平成 27 年。
[9] 同上。

３．計画策定のための考慮事項

本編では、サイバーセキュリティ人材に関して、経営層から指示を受けた実務部門が実際に計画を策定していくための考慮事項を記載する。

第１工程	現状及び中長期的なＩＴ業務の洗い出し

工程１－１	現状のＩＴ業務の洗い出し
ＩＴ人材の確保・育成に関する計画を策定するにあたり、自機関においてＩＴ人材が担う業務の洗い出しを行い、各業務に求められる具体的な役割を明確にする。	

【本工程の手順】

手順１－１－１	現状のＩＴ業務の洗い出しを行う。

【考慮事項】

１．サイバーセキュリティに関係する業務における役割の洗い出し

本工程では、第３編において洗い出されたサイバーセキュリティに関係する業務に求められる具体的な役割について記載する。

（1）役割の分類

金融機関等は、サイバー攻撃を受けた際に迅速かつ的確に対応するために、サイバーセキュリティを含む情報セキュリティに関する責任者（CIO[10]、CISO[11]等）を配置することが有効である。

自機関のサイバー攻撃対応に必要な役割を検討したうえで、それらを担うインシデント対応組織を整備する。インシデント対応組織は、インシデントの検知及び対応等のインシデント発生時の役割のみならず、平時の運用を担うことにより、サイバー攻撃対応態勢の実効性を高めることができる。

経営層と十分に連携できる組織を整備することで、自機関としての対応方針の決定や社外への公表等を迅速に行うことができる。

図表 11 のサイバーセキュリティに関係する業務・役割の洗い出しの例は、『コンテ手引書』に記載の経営層など組織の責任者等及びインシデント対応組織の役割を参照している。なお、この図表は１つの例であるため、自機関の特性（業態・規模・外部委託している業務範囲等）に即した、サイバーセキュリティに関係する業務・役割の洗い出しと整理が必要である。

すなわち、インシデント発生時の運用と平時の運用だけではなく、戦略策定・経営戦略・事業戦略・システム戦略や、個別システム案件管理、リスク管理等の業務・役割について

10 「Chief Information Officer。企業の情報システム部門の最高情報責任者を指す。経営層に含まれる。システム戦略策定やコスト管理・リスク管理方針等、情報システムのパフォーマンスの最大化に向けてバランスを取りながら推進する。」日本 CIO 協会。

11 「Chief Information Security Officer。経営陣の一員、もしくは経営トップからその役を任命された、情報セキュリティ対策を実施する上での責任者を指す。」サイバーセキュリティ経営ガイドライン Ver1.1、経済産業省、独立行政法人 情報処理推進機構、平成 28 年。

も整理する等、業務・役割の洗い出しにあたって漏れが無いように業務全体を考慮する必要がある。

コメント [A14]:
ご意見 No27~No32 に関連する修正

図表 14 の見直しに伴い、業務の洗い出しに関する図表も修正する。
【人材３－１－④】参照

図表 11　サイバーセキュリティ業務・役割の洗い出しの例

業務の分類例		業務・役割の洗い出し例	
	戦略策定 経営戦略・事業戦略・システム戦略	情報セキュリティ戦略	情報セキュリティ戦略の策定
			情報セキュリティ戦略の遂行
	サイバーセキュリティ	態勢整備・平時の運用	現状評価
			脆弱性対応
			システム・ネットワーク運用・監視
			情報収集・分析
			教育・訓練・演習
		インシデント発生時の運用	インシデント対応管理
			インシデント対応
			フォレンジック
			情報収集・共有
	個別システム案件管理	システム要件定義・システム設計	セキュリティ要件定義・設計
		システム構築・システムテスト	セキュリティを意識したプログラミング・テスト
	リスク管理	リスク管理	サイバー攻撃リスクの管理・評価・報告
		外部委託管理	外部委託管理・評価・報告
	監査	情報セキュリティ監査	情報セキュリティ監査

以下の文献を参考に FISC にて作成。
「金融機関におけるコンティンジェンシープラン策定のための手引書　第３版追補３」、公益財団法人　金融情報システムセンター、平成 29 年。
「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年。

(2) 組織の責任者等の役割について

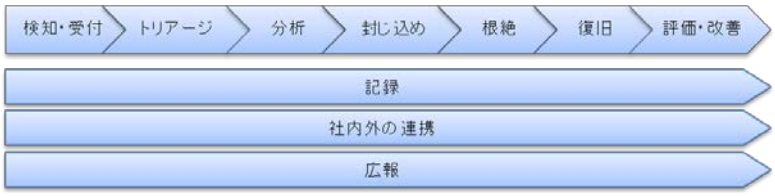
経済産業省が定める『サイバーセキュリティ経営ガイドライン Ver.1.1』の、情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」の中に、「方針に基づく対応策を実装できるよう、経営者とセキュリティ担当者、両者をつなぐ仲介者としての CISO 等からなる適切な管理体制を構築すること。その中で、責任を明確化すること。」といった記載があり、サイバーセキュリティに関する責任者の役割の明確化が示されている。

(3) インシデント対応組織の役割の例

外部との連携では、平時の運用における情報の受付・連携や情報取集・情報共有、またインシデント発生時における監督官庁や金融 ISAC、JPCERT コーディネーションセンター等の外部機関や同業他社との連携、さらに自機関内部での連携を行うための窓口の役割が重要になる。

なお、インシデント発生時の運用におけるインシデントの受付、インシデントへの対応については、『コンテ手引書』において図 12 のように定義している。詳細については『コンテ手引書』を参照のこと。

図表 12　インシデントの発生から対応収束までのプロセス



出所：(『コンテ手引書』より引用)

(4) サイバーセキュリティに関係する業務を所管する組織について

サイバーセキュリティに関係する業務を所管する部門は、各社の体制に応じて異なるものであり、一意に特定はできない。自機関で検討しているサイバー攻撃対応態勢を踏まえ、業務・役割について各部門と適切に協議し、それに相応した配置を行う。

それぞれのサイバーセキュリティに関係する業務の特性や、対応要員及びそのスキルといった自機関の実態を踏まえて、外部委託を行うことも考えられる。

『コンテ手引書』では、自機関内において行う業務と、外部委託を行う業務とを明確~~する。ただし~~にし、外部委託先を含めた全体統括や業務影響の評価、対応策の判断等については、自機関内で担うことが望ましいとしている。

(~~2~~5) インシデント対応組織に関する考慮事項

インシデント対応組織の在り方については、自機関のサイバーセキュリティに対する方針によってさまざまな対応態勢となる。~~インシデント対応組織は、自機関の方針に適した態勢を取ることが望ましい。~~このような事情から、インシデント対応組織に求められるサイバーセキュリティ人材についても自機関の方針が反映されることが想定される。

インシデント対応組織を考えるにあたっては、設置する際の観点も含め、以下の点を考慮する。

①インシデント対応組織の態勢の在り方について

インシデント対応組織と、その対応要員については、以下の２つの態勢があり、この違いによって育成すべき人材にも違いが現れると考えられる。

a. 専任組織による態勢

自機関に専任のサイバーセキュリティ人材を配置する方法のことである。自機関内外に対するサイバー攻撃に関する問合せなどのインシデントの受付業務や、インシデント対応業務、さらに平時における情報収集・分析等に専任者を配置できる場合、迅速な情報連携・共有が可能になり、インシデント発生時の迅速な対応につながることが考えられる。

b. 兼任組織による態勢

ＩＴ部門やリスク管理部門等、インシデント対応組織を担う人材が本業と共にサイバーセキュリティ業務を担う方法のことである。専任者を配置することは人員数等の都合上から困難である場合が多いために、兼任という考え方がある。兼任組織では、複数の部門から選出された要員を組織に含める態勢を取ることもできる。

例えば、システム部門、リスク管理部門、事務部門、広報部門等が該当する。このような態勢では複数部門の横の連携が取りやすいために、インシデント発生時には関係部門と密な連携が可能となる。

ただし、本来業務の都合でサイバーセキュリティ業務に注力できず、迅速な対応が困難になる可能性~~がある~~も考慮する必要がある。

なお、短期的には兼任組織として運用し、人材育成も含め、中長期的に専任組織に切り替えていく方策も考えられる。

②インシデント対応組織の主管部門について

インシデント対応には複数の部門が関わることが想定されるため、自機関の方針に基づき、関連する部門の中で、事務局に該当するインシデント対応組織の主管部門をあらかじめ決める。例えば、主管部門となるのは、以下のような部門が考えられる。

a.　システム部門

サイバーセキュリティ分野をＩＴ分野の延長線上にあるものとして、システム部門が主導する場合には、インシデントをシステム障害対応業務の一環と捉え、システム部門を主管としたインシデント態勢を構築することになる。

b.　リスク管理部門

サイバーセキュリティ分野をリスク管理分野の延長線上にあるものとして、リスク管理部門がリードする場合には、リスク管理部門を主管としたインシデント態勢を構築することになる。

c.　経営管理部門

コメント [A15]:
ご意見 No23 に基づく修正

平時の運用についての記載が必要。

経営管理部門に配置することで、全社的な取り組みとしてインシデント対応組織を構築することになる。

（6）外部委託先が分担する役割の範囲の明確化について

サイバーセキュリティに関係する業務・役割のすべてを自機関で遂行することが難しい場合は、外部委託を活用することになる。その際、サイバーセキュリティに関係する業務・役割を整理した上で、どの役割を委託するかを決める必要がある。また、外部委託先や、外部委託の一形態である共同センターを利用している場合には、~~サイバーセキュリティ業務の内、共同センター~~それらが担う範囲と自機関が担う範囲を明確に~~する~~したうえで連携方法も明確化する必要がある。

外部委託先がサイバー攻撃を受けた場合、金融機関等に被害が発生する可能性がある。そのため、リスクに応じて外部委託先のサイバー攻撃対応態勢の整備状況について自機関が求める水準と同等またはそれ以上であることを確認する必要がある。

外部委託先を利用する場合、利用するサービスや取り扱う情報の重要度に応じて、適切なリスク管理レベルが確保されているか考慮する。

また、他社へのサイバー攻撃によって、自機関にシステム停止等の被害が波及する可能性がある。他社への攻撃に起因して自機関にも影響が及ぶ場合における、情報連携や補償について契約や SLA の内容を確認する。

外部委託先におけるリスク管理の在り方については、「金融機関における外部委託に関する有識者検討会報告書」を参照のこと。

2．サイバーセキュリティに関係する業務の細分化

サイバーセキュリティに関係する業務の全体を整理したうえで、段階的に業務を細分化し、役割を導き出す。自機関におけるサイバーセキュリティに関する戦略・方針や外部委託の状況などを踏まえて整理することで、各役割の過不足を認識できる。また、中長期的なシステム戦略やビジョン等に基づき必要となるサイバーセキュリティに関係する業務の役割の分担状況（すなわち、自機関における確保・育成、外部委託、共同センターの利用）を把握することができるようになる（図表 13 参照）。

コメント [A16]:
ご意見 No24 に基づく修正

記載内容と標題が一致していない。

コメント [A17]:
ご意見 No27~No32 に関連する修正

図表 14 の見直しに伴い、業務・役割の細分化と分担整理に関する図表を追加する。
【人材３－１－④】参照

図表 13　サイバーセキュリティ業務・役割の細分化と分担整理の例

業務の分類例		業務・役割の洗い出し例				自機関内	外部委託	共同センター
	戦略策定 経営戦略・事業戦略・ｼｽﾃﾑ戦略	情報セキュリティ戦略	情報セキュリティ戦略の策定	・情報セキュリティ戦略の策定	・・・・			
			情報セキュリティ戦略の遂行	・情報セキュリティ戦略の遂行	・・・・			
	サイバーセキュリティ	態勢整備・平時の運用	現状評価・報告	・現状の評価と経営層への報告	・・・・			
					・・・・			
				・業務的視点及び専門的視点の双方を踏まえた対応方針の確認	・・・・			
					・・・・			
			脆弱性対応	・脆弱性診断	・・・・			
			システム・ネットワーク運用・監視	・監視・分析	・・・・			
				・脆弱性情報・脅威情報への対応	・・・・			
				・ログの取得・保全	・・・・			
			情報収集・分析	・情報収集	・・・・			
				・情報分析	・・・・			
				・情報共有	・・・・			
				・自機関内外の対応窓口の設置・周知	・・・・			
			教育・訓練・演習	・サイバー攻撃対応に関する教育・訓練・演習の企画・推進	・・・・			
					・・・・			
					・・・・			
		インシデント発生時の運用	インシデント対応管理	・執行部門と経営層との連携・調整・対応指示	・・・・			
					・・・・			
				・コンティンジェンシープランを発動した該当事象に関する発生状況の報告	・・・・			
					・・・・			
			インシデント対応	・インシデントの受付	・・・・			
				・インシデントへの対応	・・・・			
			フォレンジック	・フォレンジック	・・・・			
					・・・・			
			情報収集・共有	・経営層や関係部門等との調整・報告	・・・・			
				・外部機関との連携	・・・・			
				・情報共有	・・・・			
	・・・・	・・・・	・・・・	・・・・				

自機関の現状、将来像に合わせて区分け

細分化

以下の文献を参考に FISC にて作成
「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年
「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 版」、特定非営利活動法人　日本ネットワークセキュリティ協会（JNSA）、平成 29 年
「CSIRT 人材の定義と確保（Ver.1.0、1.5）」、日本コンピュータセキュリティインシデント対応チーム協議会（NCA）、平成 29 年
「セキュリティ対応組織の教科書～機能・役割・人材スキル～　第 1.0 版」、日本セキュリティオペレーション事業者協議会、平成 28 年
「産業横断　人材定義リファレンス　～機能と業務に基づくセキュリティ人材定義」、産業横断サイバーセキュリテ

ィ人材育成検討会、平成 28 年
「National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework」,NIST,2017
「金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）」、公益財団法人　金融情報システムセンター、平成 29 年

第２工程	ＩＴ人材・スキルの定義と現状及び 中長期的に必要となるＩＴ人材の把握

工程２－１	ＩＴ人材・スキルの定義
自機関のＩＴ業務において必要となるＩＴ人材（人材像）を定義する。 求められるＩＴ人材のスキルを定義するとともに、その評価方法を検討する。	

【本工程の手順】

手順２－１－１	ＩＴ業務に求められる役割からＩＴ人材を定義する。

【考慮事項】

１．組織の責任者等の必要性

サイバー攻撃を受けた際に迅速かつ的確に対応するために、経営層はサイバーセキュリティを含む情報セキュリティに関する責任者（CIO、CISO 等）やインシデント対応組織の責任者を配置する。そして、それらの者が平時からサイバー攻撃が自機関に与える影響を十分に認識するとともに、インシデント発生時には主導的・中心的な立場で対応を牽引する態勢を構築する。また、適切な権限を委譲することも有効である。

２．サイバーセキュリティにおける「橋渡し人材層[12]」の必要性

サイバーセキュリティ業務では、縦の橋渡しとして経営層と実務部門との間を取り持つとともに、横の橋渡しとして自機関における関連部門間の調整、セキュリティ機関や外部委託先など外部との連携を行う橋渡し人材層が必要となる。

このような橋渡しを担う人材は、IT 業務全般にも必要であると考えられるが、特にサイバーセキュリティの分野で求められている。この理由として、たとえばサイバー攻撃対応時には、経営層は、事業への甚大な被害を想定して限られた時間の中で適切な判断を行う必要があるが、そのために必要となる程度のＩＴやサイバーセキュリティに関する知識を必ずしも保有しているとは言えない状況にある。一方で、実務者層の管理者は、的確な情報を経営層に報告する必要があるが、そのために必要となる程度の経営に関する知識を必ずしも保有しているとは言えない状況にある。

このような現状にあって、両者をつなぐ人材として、橋渡し人材層が求められている。

~~橋渡し人材層は、実務部門の報告を理解し、指示できるだけのＩＴおよびサイバーセキュ~~

12　サイバーセキュリティ戦略本部では、 経営層の示す経営方針に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらに、組織内の関係部局間の統合調整や実務者層をまとめリードすることができる人材層をサイバーセキュリティ業務における「橋渡し人材層」とし、その必要性及び育成を示している。以下、参考文献。
・『サイバーセキュリティ人材育成総合強化方針』（サイバーセキュリティ戦略本部：平成 28 年３月。
・『サイバーセキュリティ人材育成プログラム』（サイバーセキュリティ戦略本部：平成 29 年４月）。

コメント [A18]:
ご意見 No25 に基づく修正

「橋渡し人材像」に関してサイバーセキュリティ対策本部での用語定義を脚注に示すとともに、サイバーセキュリティに関係する業務における「橋渡し人材像」の必要性について、記載する。

~~リティの知識、自機関の金融業務および自機関のＩＴについても経験・知識が必要となる。さらに、経営層や実務部門、外部との円滑な連携を行うためのコミュニケーション力が必要となる。~~

~~このため、橋渡し人材層は、外部から即戦力を確保することが困難であり、所要の知識・経験を習得するには相応の時間を要するものと考えられるために、自機関において育成することが望ましい。~~

コメント [A19]:
事務局にて修正。

「橋渡し人材層」のスキル及び確保・育成に関することのため、工程２－１「IT 人材・スキルの定義」工程３－１「IT 人材の確保・育成計画の策定」に記載する。

３．サイバーセキュリティ人材について

(1) サイバーセキュリティ人材の定義

サイバーセキュリティ人材に関する文献~~の定義集~~やレポートは複数のものが存在しており、特にインシデント対応組織に属すると考えられる人材に関する定義を行っているものが多い。その理由としてはサイバーセキュリティにおいてインシデント対応が重要な位置を占めるためという点が考えられる。

サイバーセキュリティ人材の定義について、主だったものを参考として以下に挙げる。

（参考）
①『セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版』（NPO 日本ネットワークセキュリティ協会（JNSA）：平成 29 年８月）
②『「産業横断サイバーセキュリティ人材育成検討会」第一期最終報告書』（産業横断サイバーセキュリティ人材育成検討会：平成 28 年９月）
③『セキュリティ対応組織の教科書～機能・役割・人材スキル～　第 1.0 版』（日本セキュリティオペレーション事業者協議会：平成 28 年 11 月）
④『CSIRT 人材の定義と確保（Ver.1.5)』（日本シーサート協議会：平成 29 年３月）
⑤『i コンピテンシ ディクショナリ（iCD2017)』（独立行政法人　情報処理推進機構（IPA）：平成 29 年６月）

(2) 自機関でのサイバーセキュリティ人材に望まれる役割の例

コメント [A20]:
ご意見 No27～32 に基づく修正

【人材３－１－④】参照

サイバーセキュリティ人材が担う役割のいくつかは、外部に委託することが考えられる一方、自機関内に担うことが望ましい役割も存在すると考えられる。

『コンテ手引書』では、自機関内で保有が望まれる役割に関して、サイバー攻撃対応の考慮事項におけるインシデント対応組織の整備及び役割の明確化の項において、「外部委託先を含めた全体の統括や業務影響の評価、対応策の判断等については、金融機関等で担うべき機能と考えられる」としている。

このような考え方を踏まえると、共同センター利用を含む外部委託先を管理統括やインシデント対応管理などの役割等については、自機関内で確保・育成することが望ましい。また、自機関内で担う業務・役割についても、必ずしも専任化する必要はなく、他の業務との兼任も想定した効率的・効果的な人材の配置が考えられる。

さらに、システム部門に限らず、経営企画部門、情報セキュリティ部門、人事部門等、様々な部門が分担して役割を担っていくことが考えられる。

図表 14 の役割と人材像の定義は、上記参考文献を元に作成した例である。

図表 14　サイバーセキュリティ人材~~に望まれる役割の例~~の役割・人材像の例

サイバーセキュリティ人材の役割の分類		担うべき業務・役割			求められる人材像
	戦略策定 経営戦略・ 事業戦略・ システム戦略	情報セキュリティ戦略	情報セキュリティ戦略の策定	ー	・自機関または外部委託における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定ができる人材。 ・自機関または外部委託の情報セキュリティ対策に関連する業務全体を俯瞰し、外部委託を含むリソース配分の判断・決定ができる人材。
			情報セキュリティ戦略の遂行	ー	・組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むことができる人材。 ・情報セキュリティ*対策の立案や実施（指示・統括）、及びその見直しができる人材。 ・自機関または外部委託における情報セキュリティ対策の具体化や実施を統括できる人材。 ・自機関または外部委託における情報セキュリティ戦略の啓発や教育の計画を立案・推進できる人材。
	サイバーセキュリティ	態勢整備・ 平時の運用	現状評価・報告	・現状の評価と経営層への報告 ・業務的視点及び専門的視点の双方を踏まえた対応方針の確認	・サイバーセキュリティ業務の監視や分析、評価ができる人材。 ・サイバーセキュリティ関連業務に関して現状評価や課題定義を経営層等へ分かりやすく報告できる人材。
			脆弱性対応	・脆弱性診断	・ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行うことができ、判明した脆弱性に対して対策を検討することができる人材。
			システム・ネットワーク運用・監視	・監視・分析 ・脆弱性情報・脅威情報への対応 ・ログの取得・保全	・システムやネットワークの各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を行うことができる人材。 ・システムが提供しているサービスの運用・監視（ネットワーク監視等）を行い、インシデントの発生を判断できる人材。 ・サイバーセキュリティに関する知識を持ち、問い合わせ対応などのヘルプデスク業務ができる人材。 ・サイバーセキュリティ製品の有効

					性の判断及びそれらの導入・運用・管理ができる人材。
サイバーセキュリティ人材の役割の分類		担うべき業務・役割			求められる人材像
	サイバーセキュリティ	態勢整備・平時の運用	情報収集・分析・共有	・情報収集 ・情報分析 ・情報共有 ・自機関内外の対応窓口の設置・周知	・インシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集することができる人材。 ・収集した情報を元に自機関への影響を検討し、検討した結果、自機関または外部委託に適用すべきかの選定ができる人材。 ・分析した情報を報告書にまとめ、情報セキュリティに関する責任者に分かりやすく報告できる人材。
			教育・訓練・演習	・サイバー攻撃対応に関する教育・訓練・演習の企画・推進	・自機関のサイバーセキュリティリテラシーの向上や底上げのための教育及び啓発活動ができる人材。 ・自機関内での実施や外部委託先等の関係組織と共同で実施されるサイバー攻撃に備えた訓練や演習への企画や推進ができる人材。
		インシデント発生時の運用	インシデント対応管理	・執行部門と経営層との連携・調整・対応指示 ・コンティンジェンシープランを発動した該当事象に関する発生状況の報告	・発生したインシデントに対する全体統制ができる人材。 ・発生したインシデントに対する対応の優先順位を判断ができる人材。 ・重大なインシデントか否かを判断し、経営層や情報セキュリティに関する責任者への報告を分かりやすく迅速に行える人材。 ・経営層や情報セキュリティに関する責任者がインシデントへの対応を意思決定する際の支援・アドバイスができる人材。 ・インシデント終息後にインシデント対応内容の振り返りを行うことができる人材。
			インシデント対応	・インシデントの受付 ・インシデントへの対応	・インシデントの対応状況を管理できる人材。 ・自機関または外部委託におけるインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理ができる人材。 ・セキュリティベンダーに処理を委託している場合には作業指示や対応状況管理ができる人材。
			フォレンジック	ー	・インシデント発生時のシステムやネットワークを対象とした証拠保全ができる人材。 ・消されたデータを復元したり、痕跡を追跡したりするためのシステ

					ム的な鑑識、精密検査、解析、報告ができる人材。
			情報収集・共有	・経営層や関係部門等との調整・報告 ・外部機関との連携 ・情報共有	・JPCERT/CC、NISC、警察、監督官庁、NCA、金融 ISAC、他 CSIRT との情報連携ができる人材。
サイバーセキュリティ人材の役割の分類		担うべき業務・役割			求められる人材像
	サイバーセキュリティ	インシデント発生時の運用			・サイバーセキュリティ関連業務を担う社内の法務、渉外、IT 部門、広報等の関係部署と情報連携ができる人材。
	システム設計・開発	システム要件定義 システム設計	セキュリティ要件定義・設計	ー	・サイバーセキュリティの確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務ができる人材。 ・サイバーセキュリティ対策に関する企画・設計・最新技術調査、製品評価ができ、システムの要求定義に反映がすることができる人材。
		システム構築 システムテスト	セキュリティを意識したプログラミング・テスト	ー	・サイバーセキュリティを考慮したシステムの基盤部分（OS・ネットワーク）の全体設計・運用設計・方式設計、開発ができる人材。 ・サイバーセキュリティを考慮したアプリケーションの開発、DB 設計ができる人材。 ・仕様書や設計書に従って、セキュアプログラミングができる人材。 ・サイバーセキュリティの観点からソースコードの解析を行うことができる人材。 ・テストで脆弱性を発見・除去することができる人材、または脆弱性情報を基にテストを行い、脆弱性を除去できる人材。
	リスク管理	リスク管理	サイバー攻撃リスクの管理・評価・報告	・態勢整備計画の策定 ・サイバー攻撃対応手順等の策定・見直し	・サイバーセキュリティ対策の現状に関するアセスメントが実施でき、あるべき姿とのギャップ分析をもとにリスクを評価できる人材。 ・リスク評価の結果から自機関または外部委託の事業計画に合わせて導入すべきサイバーセキュリティ対策を検討できる人材。 ・導入されたサイバーセキュリティ対策の有効性を確認し、改善計画を立案できる人材。
		外部委託管理	外部委託管理	・外部委託先を含めた態勢整備の実施状況の管理・評価・報告	・外部委託先の提供するサービスに関して調査・評価ができる人材。 ・委託契約内容を確認・見直しを行い、有事の際の外部委託先の業務と自機関の業務を明確にし、サイバーセキュリティ関連業務の役割分担を整理することができる人材。 ・外部委託先のサイバーセキュリティ業務及び関連業務の実施状況の

					監視や報告などの外部委託管理ができる人材。
	監査	情報セキュリティ監査	情報セキュリティ監査	ー	・情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、助言ができる人材。

以下の文献を参考に FISC にて作成。

「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年
「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 版」、特定非営利活動法人　日本ネットワークセキュリティ協会（JNSA）、平成 29 年
「CSIRT 人材の定義と確保（Ver.1.0、1.5）」、日本コンピュータセキュリティインシデント対応チーム協議会（NCA）、平成 29 年
「セキュリティ対応組織の教科書～機能・役割・人材スキル～　第 1.0 版」、日本セキュリティオペレーション事業者協議会、平成 28 年
「産業横断　人材定義リファレンス　～機能と業務に基づくセキュリティ人材定義」、産業横断サイバーセキュリティ人材育成検討会、平成 28 年
「National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework」,NIST,2017
「金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）」、公益財団法人　金融情報システムセンター、平成 29 年

手順２－１－２	求められるＩＴ人材のスキルを定義する。

【考慮事項】

１．サイバーセキュリティ人材に求められるスキル

金融機関等におけるサイバーセキュリティ人材に求められるスキルとして、知識／業務経験／技量等がある。その中で知識については、以下の３つが考えられる。なお、業務経験、技量については、第３編　工程２－１　手順２－１－２を参照のこと。

また、これらのスキルは、複数の種類が存在するサイバーセキュリティ~~人材~~の人材像に対して、一様に必要となるわけではなく、人材像によって求められるスキルレベルが異なることに留意が必要である。

(1) ＩＴ知識

求められる知識の範囲やレベルは異なるが、サイバーセキュリティに関係する業務・役割の遂行にあたっては、基盤となるＩＴ知識が求められる。

サイバーセキュリティに関係する業務・役割におけるネットワークモニタリングや、異常な通信のログの保全・解析はＩＴ知識が必要となる。また、脆弱性情報に基づいて行われる OS やアプリケーションのアップデート、ウイルスソフトのパターン更新などは通常のＩＴ業務の延長線上で対策が行われる。

サイバーセキュリティに関係する業務・役割の一部を外部委託している場合であっても、委託先への指示や、委託先からの報告を適切に理解できるだけのＩＴ知識が求められる。

(2) サイバーセキュリティ固有の知識

サイバーセキュリティに関係する業務・役割によって求められる知識の範囲、レベルは異なることが想定される。たとえば、各業務・役割においてはセキュリティマネジメント、サイバー攻撃手法、デジタルフォレンジック等に関して、総論としての知識が求められる。一方、たとえば、デジタルフォレンジック知識を高いレベルで理解する必要があるのは、デジタルフォレンジック業務に携わる人材であり、情報セキュリティ戦略等の業務に携わる人材には、必ずしもデジタルフォレンジック業務に携わる人材に求められるまでのレベルを要求する必要はない。

サイバーセキュリティに関する攻撃は、日々、高度化・巧妙化しており、変化し続ける環境や攻撃手法に対応するため、研修等を通して知識・情報の最新化を行う。

インシデント対応組織の役割の一部を外部委託している場合であっても、外部委託先への指示や、外部委託先からの報告を適切に理解できるだけのサイバーセキュリティ固有の知識が求められる。

(3) 金融業務知識と自機関の情報システムに関する知識

自機関の体制や業務及び業務に関連する情報システムなどの知識が挙げられる。インシデント対応時に、そのインシデントがどの情報システムに影響を及ぼし、結果としてどの

コメント [A21]:
ご意見 No33、34 に基づく修正

スキルに関してはもう少し詳細に記載すべき。

コメント [A22]:
事務局にて修正

コメント [A23]:
ご意見 No35 に基づく修正

橋渡し人材に関する記載の整理が必要。

業務に影響が出るのかを把握できなければ、適切な対処を行うことができない。インシデント対応時には、どのような影響があるかを分析・判断し、適切な対応や経営層への報告ができるだけの業務知識が求められる。また平時においても、情報セキュリティ戦略策定やコンティンジェンシープランの策定等においても必要となる。

（参考）
・『CSIRT 人材の定義と確保（Ver.1.0、1.5）』（日本シーサート協議会：平成 29 年 3 月）
・『組織内 CSIRT の要員』（JPCERT コーディネーションセンター）
・『セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版』（特定非営利活動法人 日本ネットワークセキュリティ協会：平成 29 年 8 月）
・『ｉコンピテンシ ディクショナリ（iCD2017）』（独立行政法人　情報処理推進機構（IPA）：平成 29 年 6 月）

２．スキル定義の整理例

図表 15 として例示する各役割に必要となるスキル整理表を作成することで、確保・育成する際に必要となるスキルについて考察ができるようになり、第 3 工程において実施すべきスキルの適正化に繋げることができるようになる。たとえば、自機関内における育成においては、実際に存在する人材の現状のスキルと、必要とされるスキルを比較してギャップを見出すことにより、育成すべきスキルの明確化ができるものと考えられる。また、確保においては、自機関内にそのスキルを保有する人材がいるかどうかを把握することで、自機関外に求める人材に必要なスキルを明確にすることができるものと考えられる。

さらに、共同センターを含め外部委託した役割においては、その役割に必要なスキルを明確化することで、外部の実務者のスキルレベルを測るのに役立つものと考えられる。

なお、図表 15 に整理例として記載しているスキルの知識項目は、その役割に特徴的と思われる知識の一部を参考文献から引用し記載している。

コメント [A24]:
事務局にて修正。

図表 14 の記載修正により、サイバーセキュリティ人材の各役割に特に特徴的と思われるスキルの一部について例示。

【人材３－１－④】参照

図表 15　サイバーセキュリティ人材に求められるスキルの整理例

サイバーセキュリティ人材の役割の分類		担うべき業務・役割	求められる人材像	スキル例（知識）
	戦略策定 経営戦略・事業戦略・ｼｽﾃﾑ戦略	情報セキュリティ戦略の策定	・自機関または外部委託における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定ができる人材。 ・自機関または外部委託の情報セキュリティ対策に関連する業務全体を俯瞰し、外部委託を含むリソース配分の判断・決定ができる人材。	IT ガバナンス(IPA) システム戦略立案手法(IPA) システム企画立案手法(IPA) 事業継続計画(IPA) 法規・基準・標準(IPA)　等
		情報セキュリティ戦略の遂行	・組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むことができる人材。 ・情報セキュリティ*対策の立案や実施（指示・統括）、及びその見直しができる人材。 ・自機関または外部委託における情報セキュリティ対策の具体化や実施を統括できる人材。 ・自機関または外部委託における情報セキュリティ戦略の啓発や教育の計画を立案・推進できる人材。	
	サイバーセキュリティ	現状評価･報告	・サイバーセキュリティ業務の監視や分析、評価ができる人材。 ・サイバーセキュリティ関連業務に関して現状評価や課題定義を経営層等へ分かりやすく報告できる人材。	セキュリティマネジメント(JNSA) サイバー攻撃手法(JNSA) 等
		脆弱性対応	・ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行うことができ、判明した脆弱性に対して対策を検討することができる人材。	OS、NW、アプリ、DB の脆弱性に対する知識(NCA) ペネトレーションテストやツールに関する知識(NCA) サイバー攻撃手法(JNSA) ネットワークセキュリティ(JNSA)　等
		システム･ネットワーク運用・監視	・システムやネットワークの各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を行うことができる人材。 ・システムが提供しているサービスの運用・監視（ネットワーク監視等）を行い、インシデントの発生を判断できる人材。 ・サイバーセキュリティに関する知識を持ち、問い合わせ対応などのヘルプデスク業務ができる人材。 ・サイバーセキュリティ製品の有効性の判断及びそれらの導入・運用・管理ができる人材。	ＯＳセキュリティ【共通】（セキュアＯＳ）(JNSA) セキュリティ運用（定時運用時のセキュリティ確保）(JNSA) 攻撃手法の概論(JNSA) ファイアーウォール(JNSA) 侵入検知(JNSA) 事業継続管理(JNSA)　等
		【平時の運用】情報収集・分析・共有	・インシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集することができる人材。 ・収集した情報を元に自機関への影響を検討し、検討した結果、自機関または外部委託に適用すべきかの選定ができる人材。 ・分析した情報を報告書にまとめ、情報セキュリティに関する責任者に分かりやすく報告できる人材。	サイバー攻撃手法(JNSA) サイバーセキュリティ問題に関する外部組織と学術機関に関する知識(NCA)　等

サイバーセキュリティ人材の役割の分類		担うべき業務・役割	求められる人材像	スキル例（知識）
	サイバーセキュリティ	教育・訓練・演習	・自機関のサイバーセキュリティリテラシーの向上や底上げのための教育及び啓発活動ができる人材。 ・自機関内での実施や外部委託先等の関係組織と共同で実施されるサイバー攻撃に備えた訓練や演習への企画や推進ができる人材。	セキュリティマネジメント(JNSA) サイバー攻撃手法(JNSA) 等
		インシデント対応管理	・発生したインシデントに対する全体統制ができる人材。 ・発生したインシデントに対する対応の優先順位を判断ができる人材。 ・重大なインシデントか否かを判断し、経営層や情報セキュリティに関する責任者への報告を分かりやすく迅速に行える人材。 ・経営層や情報セキュリティに関する責任者がインシデントへの対応を意思決定する際の支援・アドバイスができる人材。 ・インシデント終息後にインシデント対応内容の振り返りを行うことができる人材。	リスクマネジメント手法(IPA) セキュリティマネジメント(JNSA) セキュリティ運用(インシデント対応)(JNSA) 法規・基準・標準(IPA) サイバー攻撃手法(JNSA) 自機関のセキュリティアーキテクチャ、ビジネスに関する知識(NCA)　等
		インシデント対応	・インシデントの対応状況を管理できる人材。 ・自機関または外部委託におけるインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理ができる人材。 ・セキュリティベンダーに処理を委託している場合には作業指示や対応状況管理ができる人材。	セキュリティマネジメント(JNSA) セキュリティ運用(インシデント対応)(JNSA) 法規・基準・標準(IPA) サイバー攻撃手法(JNSA) 自機関のセキュリティアーキテクチャに関する知識(NCA)　等
		フォレンジック	・インシデント発生時のシステムやネットワークにを対象とした証拠保全ができる人材。 ・消されたデータを復元したり、痕跡を追跡したりするためのシステム的な鑑識、精密検査、解析、報告ができる人材。	ネットワークセキュリティ(JNSA) サイバー攻撃手法(マルウェア)(JNSA) 法規・基準・標準(IPA) 脆弱性診断に関する知識(NCA) デジタルフォレンジックに関する知識(NCA)　等
		【インシデント発生時の運用】 情報収集・共有	・JPCERT/CC、NISC、警察、監督官庁、NCA、金融 ISAC、他 CSIRT との情報連携ができる人材。 ・サイバーセキュリティ関連業務を担う社内の法務、渉外、IT 部門、広報等の関係部署と情報連携ができる人材。	サイバー攻撃手法(JNSA) サイバーセキュリティ問題に関する外部組織と学術機関に関する知識(NCA)　等
	システム設計・開発	セキュリティ要件定義・設計	・サイバーセキュリティの確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務ができる人材。 ・サイバーセキュリティ対策に関する企画・設計・最新技術調査、製品評価ができ、システムの要求定義に反映がすることができる人材。	セキュアシステム設計・構築知識(JNSA) セキュリティプログラミング技法知識(JNSA) 攻撃手法の概論(JNSA) 等

サイバーセキュリティ人材の役割の分類		担うべき業務・役割	求められる人材像	スキル例（知識）
	システム設計・開発	セキュリティを意識したプログラミング・テスト	・サイバーセキュリティを考慮したシステムの基盤部分（OS・ネットワーク）の全体設計・運用設計・方式設計、開発ができる人材。 ・サイバーセキュリティを考慮したアプリケーションの開発、DB 設計ができる人材。 ・仕様書や設計書に従って、セキュアプログラミングができる人材。 ・サイバーセキュリティの観点からソースコードの解析を行うことができる人材。 ・テストで脆弱性を発見・除去することができる人材、または脆弱性情報を基にテストを行い、脆弱性を除去できる人材。	ＯＳセキュリティ【共通】(JNSA) セキュリティプログラミング技法知識(JNSA) セキュリティ運用(JNSA) サイバー攻撃手法(JNSA) 等
	リスク管理	サイバー攻撃リスクの管理・評価・報告	・サイバーセキュリティ対策の現状に関するアセスメントが実施でき、あるべき姿とのギャップ分析をもとにリスクを評価できる人材。 ・リスク評価の結果から自機関または外部委託の事業計画に合わせて導入すべきサイバーセキュリティ対策を検討できる人材。 ・導入されたサイバーセキュリティ対策の有効性を確認し、改善計画を立案できる人材。	リスクマネジメント手法知識(IPA) 機関システムに関する知識(NCA) 法規・基準・標準知識(IPA) 等
		外部委託管理	・外部委託先の提供するサービスに関して調査・評価ができる人材。 ・委託契約内容を確認・見直しを行い、有事の際の外部委託先の業務と自機関の業務を明確にし、サイバーセキュリティ関連業務の役割分担を整理することができる人材。 ・外部委託先のサイバーセキュリティ業務及び関連業務の実施状況の監視や報告などの外部委託管理ができる人材。	セキュリティマネジメント(JNSA) サイバー攻撃手法(JNSA) 法規・基準・標準(IPA)　等
	監査	情報セキュリティ監査	・情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、助言ができる人材。	IT ガバナンス(IPA) システム戦略立案手法(IPA) システム監査手法(IPA) 法規・基準・標準(IPA)　等

以下の文献を参考に FISC にて作成
「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年
「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 版」、特定非営利活動法人　日本ネットワークセキュリティ協会（JNSA）、平成 29 年
「CSIRT 人材の定義と確保(Ver.1.0、1.5)」、日本コンピュータセキュリティインシデント対応チーム協議会(NCA)、平成 29 年
「National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework」,NIST,2017
「金融機関等におけるコンティンジェンシープラン策定のための手引書（第 3 版追補 3）」、公益財団法人　金融情報システムセンター、平成 29 年

2．橋渡し人材層に求められるスキル

サイバーセキュリティ業務を遂行するためには、実務部門や外部の関連会社や機関等からの報告を理解し、指示できるだけのＩＴ知識、サイバーセキュリティ固有の知識及び自機関の金融業務や自機関の情報システムについても経験・知識が必要となる。さらに、経営層や実務部門、内部組織だけでなく外部関連会社等とも円滑な連携を行うためのコミュニケーション力などの技量が必要となる。

コメント [A25]:
事務局にて修正

第３工程	ＩＴ人材の確保・育成計画の策定

工程３－１	ＩＴ人材の確保・育成計画の策定
過不足が見込まれるＩＴ人材の人数とスキルの適正化を検討し、ＩＴ人材の確保・育成計画として取りまとめる。	

【本工程の手順】

手順３－１－２	育成による適正化の検討

【考慮事項】

第３編　工程３－１　手順３－１－２　項番１～５を参照のこと。

サイバーセキュリティに関係する業務・役割には、サイバーセキュリティ固有の知識が必要となるものの、求められるスキルには他のＩＴ業務と共通する部分も多く、また、インシデント対応に関しても、その対応フローなどはシステム障害対応と共通する部分も多い。

このため、サイバーセキュリティ人材の確保・育成にあたっては、基盤となるＩＴ業務のスキルを有する人材にサイバーセキュリティ業務の固有の知識等を身につけさせ、育成することも考えられる。

６．訓練、演習等

インシデント対応組織を中心とした自機関で実施する訓練・演習、外部委託先等の関係組織と共同で実施する訓練、官公庁や業界団体が実施する共同演習などに参加することで、経営層へのサイバーセキュリティに関する意識啓発を図るとともに、サイバーセキュリティ業務におけるサイバー攻撃対応手順等の内容理解やスキルの向上を図る。

７．キャリアについて

自機関で確保・育成するサイバーセキュリティ人材については、ジョブローテーションの実施、及び自機関におけるキャリアパスの構築を検討することが考えられる。

(1) ジョブローテーションの実施について

サイバーセキュリティに関係する業務・役割に携わる部門等の間を、自機関のセキュリティ戦略に沿ってジョブローテーションを行うことで、必要な知識や経験を獲得することができる。サイバーセキュリティに関係する業務・役割に携わる部門等の間で、適切な配属期間と育成計画を組み合わせて~~配置転換~~ジョブローテーションを行う。

(2) キャリアパスの構築について

自機関で、ある職位（セキュリティ責任者等）に就くまでに辿ることとなる経験や順序を

構築することが想定される。なお、自機関の戦略や、人材の適性などを考慮して判断することが考えられる。

（参考）
・『平成 24 年度情報セキュリティ対策推進事業（情報セキュリティ人材の育成指標等の策定事業）事業報告書　～第 5 編～情報セキュリティ人材のモデルキャリア』（経済産業省、みずほ情報総研株式会社：平成 25 年）
・『CSIRT 人材の定義と確保（Ver.1.0）』（日本シーサート協議会：平成 27 年 12 月）

８．橋渡し人材層の確保・育成について

橋渡し人材層は、外部からの確保及び内部における育成の双方の場合において、所要の知識・経験・技量を得るには相応の時間を要するものと考えられる。

確保・育成にあたっては、たとえば、外部から人材を確保する際には、自機関が遂行する金融業務知識及び自機関の情報システムの構成など、自機関内の事情に関して深い理解を身に着けさせる必要がある。逆に、自機関内で金融業務等に精通している人材を配置する場合には、ＩＴ知識やサイバーセキュリティ固有の知識を身に着けさせる必要がある。

コメント [A26]:
事務局にて修正

手順３－１－５	採用による適正化の検討

【考慮事項】

１．採用

産学連携に基づく教育機関におけるサイバーセキュリティ教育は近年充実し、演習などを交え、より実践的な教育が行われていることから、新人の採用にあたっては、知見を保有した人材を採用することができるようになってきていると考えられる。

中途採用にあたっては、自機関に必要なサイバーセキュリティに関係する業務を洗い出し、その業務に求められる役割を考慮し、採用したい人物のスキルを明確にする必要がある点に留意する必要がある。

サイバーセキュリティに関係する業務に必要となるスキルの保有の有無を採用の根拠とした場合、新人材用、中途採用、いずれの場合でも、金融業務に関する知識や自機関~~社~~システムに関する知識等の教育が必要となる。

２．システム部門からサイバーセキュリティ人材への登用

システム部門に配属された人員を~~対象に~~サイバーセキュリティ人材に登用し、必要があればスキルギャップを明確にした上で不足しているスキル~~を育成等で補うことで、対応要員として早期の対応が見込まれる~~の教育を行う。

議事１

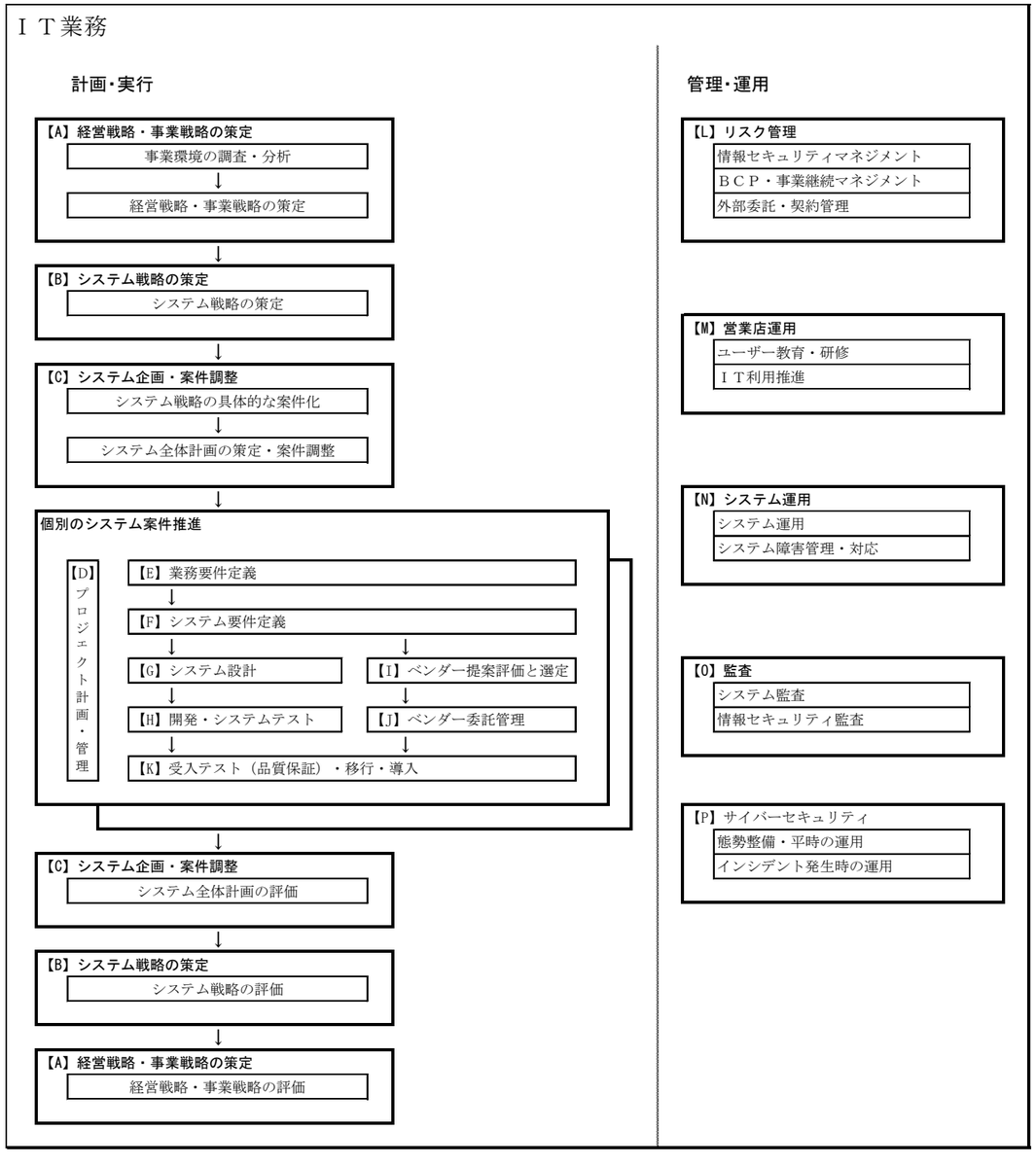
手引書原案　第３編　図表修正案（図表４・図表８・図表９）

【人材３－１－③】
平成 29 年 9 月 26 日
公益財団法人　金融情報システムセンター

手引書修正案（P14）　第３編　工程１－１　現状のＩＴ業務の洗い出し　図表３・４

一覧No.	ご意見内容と図表修正方針
2	個別システム案件管理の部分について、「ベンダー選定」及び「ベンダー委託管理」は、異なる要件として箱を分けるべき。また、ベンダー選定については、この箱の置き場所がもっと川上かと思われる。 →図表４の「ベンダー選定」と「ベンダー委託管理」を分けて記載します。 　また、図表３（全体図）と対比ができるよう、業務分類に符号（【A】～【P】）を記載します。

図表３　ＩＴ業務の洗い出しの例



図表４　ＩＴ業務の洗い出し例（詳細）

業務の分類例			ＩＴ業務の洗い出し例
【A】経営戦略・事業戦略の策定 【B】システム戦略の策定			・自機関を取り巻くＩＴ関連の内外環境を把握・分析する。 ・新しい技術や他金融機関のシステム導入状況に対して、高くアンテナを張り情報収集する。 ・マーケットや顧客のデータ分析により、顧客ニーズを把握・分析する。 ・経営層の意向等を踏まえ、経営戦略を策定するうえで、ＩＴの利活用や新たなＩＴの取込みを検討する。 ・重要なシステム課題を経営課題の１つとして経営層の理解を得たうえで、その対応を反映した経営戦略を立案する。 ・経営戦略に基づき、投資配分の調整や各部門からの要望について優先度を判断・調整のうえ、システム戦略を策定する。 ・策定したシステム戦略に対し、全社の取り組み状況を把握し、経営層に対して進捗等を説明する。 ・サイバーセキュリティなどリスクに関する内外の動向を把握し、情報セキュリティ戦略を策定する。
【C】システム企画・案件調整			・システム戦略を実現するため、具体的なシステム化案件を取りまとめ、全体スケジュールや工数の調整を行う。 ・ユーザー部門からのシステム化要望に対して、最新のＩＴ動向に基づき、導入するパッケージの提案、留意事項の助言などのサポートを行う。 ・データ利活用に必要となるデータ基盤の構築やデータ整備など、自機関システムの俯瞰的な課題に対応する。
個別システム案件管理	【D】プロジェクト計画・管理		・個別システム案件の目的と制約条件を踏まえ、プロジェクト計画を策定する。 ・予算、工程、品質などを管理し、プロジェクトを円滑に運営する。 ・進捗状況を把握し、問題や将来見込まれる課題を早期に把握・認識し、適切な対策・対応を実施することによって、プロジェクトの目標を達成する。
	【E】業務要件定義		・営業店や顧客目線でビジネスモデルを企画し、その業務要件をシステム部門やベンダー等に伝える。 ・現場目線による端末オペレーションの改善や、法制度改正で必要となるシステム対応要件を、システム部門やベンダー等に伝える。 ・システム導入を外部発注する場合には、他社事例の調査や複数ベンダーから情報提供を受ける等により、提案依頼書に盛り込む業務要件を検討する。
	【F】システム要件定義		・システム案件の目的と業務要件を踏まえた、システム要件を定義する。 ・ユーザー部署と連携し、詳細な業務要件を検討のうえ、システム仕様をまとめる。 ・システム導入を外部発注する場合には、他社事例の調査や複数ベンダーから情報提供を受ける等により、提案依頼書に盛り込むシステム要件を検討する。
	自営開発	【G】システム設計	・システム仕様書に基づき、詳細なシステム設計を行う。 ・システム基盤やメンテナンス方針の検討など、システム運用設計を行う。
	自営開発	【H】システム構築 システムテスト	・システム仕様書に基づき、プログラミングなどシステム構築を行う。 ・システムテスト（単体・結合）及び検証を行う。
	外部発注	【I】ベンダー提案 評価と選定	・業務要件とシステム要件を取りまとめ、ベンダーに提案依頼書を発行する。 ・ベンダーから提示を受けた提案内容やコストについて、評価及び契約交渉を行う。
	外部発注	【J】ベンダー委託 管理	・ベンダーと連携し、発注するシステムについて要件定義と詳細設計にかかる工程を推進する。 ・ベンダーによる製造・テストの進捗及び課題の管理を行う。
	【K】受入テスト 移行・導入		・システム部門及びベンダー等と連携し、業務とシステム双方の視点を盛り込んだ、受入テストを行う。 ・システムの導入に向け、一定の試行期間を設けるなど、品質保証にも留意した移行計画・導入計画を策定し、システム部門及びベンダー等と連携して推進する。 ・システムの仕様や変更点などを理解したうえで、操作マニュアルや業務連絡文書を作成し、営業店の役職員に周知・説明する。
【L】リスク管理			・システムリスクを含めた、オペレーショナルリスクを把握し、他リスクとの統合管理を行う。 ・システムリスクを定性・定量的に分析し、リスクマネジメント計画を立てる。 ・マネロンなど金融機関として対応が求められる法規制等に対して、規定と態勢を整備する。 ・リスク事象が発生した場合の影響を最小限にする施策をリスクの対応計画にまとめる。 ・情報セキュリティにかかる規程やマニュアル等を策定する。
	ＢＣＰ		・災害発生時、中核となる事業の継続あるいは早期復旧を可能とするため、システム面を含めた事業継続計画（BCP）を策定するとともに、訓練等を通じて実効性を高める。
	外部委託管理		・情報システムの外部委託に係る方針を決定する。 ・外部委託先の各管理フェーズ（利用検討時・契約締結時・開発時・運用時・終了時・障害発生時等）における、安全対策のチェック事項など基準及び態勢を整備する。 ・外部委託におけるリスク管理に係る改善対策を実施する。
【M】営業店運用			・オペレーション研修の実施等により、自機関におけるシステム利活用を推進し、役職員のＩＴリテラシー向上をはかる。 ・営業店への事務指導、事務ミス事例の分析・改善対応等を通じて、自機関の事務リスク削減を図る。
【N】システム運用			・ハード、ＯＳ、ミドルウェア、ネットワークなどシステム基盤・インフラの運用や管理を行う。 ・安定稼働を確保し、障害発生時において被害の最小化を図るとともに、継続的な改善、品質管理を行う。 ・システム障害などトラブル発生時、関連部門と連携をはかり適切な対応を行う。
【O】監査			・経営戦略及びシステム戦略に基づき、安全対策上必要なＩＴマネジメント（業務執行体制等）が適切に機能していることを点検・評価する。 ・独立した監査部門の視点で、システム部門等の運用状況を監査する。 ①システム開発・運用・障害対応の円滑性・妥当性（サービス・費用　等） ②システム関連資源の管理状況（人・モノ・カネ　等） ③システム関連犯罪、システム障害等の様々な問題への対応と再発防止策の妥当性・実効性の状況 ・経営層に対して、システム監査の結果を報告するとともに、改善のための提言を行う。
【P】サイバーセキュリティ			・本手引書「第４編」を参照。

（金融機関等のヒアリング結果に基づき FISC にて作成）

手引書原案　第３編　図表修正案（図表４・図表８・図表９）

手引書修正案（P23）　第３編　工程２-１　ＩＴ人材・スキルの定義　図表８

一覧No.	ご意見内容と図表修正方針
3	システムの工程からの観点からすると「３業務設計・システム導入」と「４プロジェクト管理」は順序を入れ替えた方がよい。 ⇒ご意見に基づき、「３プロジェクト管理」「４業務設計・システム導入」の順に記載します。
9	「12 データ分析」を、１つのＩＴ人材分類として定義するのであれば、もう少し担うべき業務を明確にしたほうが良い。マーケット分析だけでなく、様々な分野の業務で必要とされている。業務に何かを追加するのかも含めて、検討したほうが良いと思われる。 ⇒「12 データ分析」は、「経営戦略・事業戦略の策定（マーケットや顧客ニーズの分析）」業務を担う人材として例示していましたが、それに加えた業務例として「データ整備」に関する業務を、図表４に追加します。 また、それに伴い図表８・９の「ＩＴ人材の役割の分類」を「データ分析」から「データ利活用」に変更します。
4, 5, 6, 7	いただいたご意見に基づき、図表８の「求められる IT 人材像」に追加・修正をいたします。 【５システム設計・開発】【６システム運用】【８リスク管理】

図表８　ＩＴ人材の役割・人材像の整理の手順例

ＩＴ人材の役割の分類		担うべき業務		求められるＩＴ人材像
1	戦略策定 経営戦略・ 事業戦略 システム戦略	経営・事業環境の調査・分析	経営環境の調査・分析と課題の抽出 業界動向の調査・分析	・IT に関する知識は、専門家レベルである必要はないが、IT ソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をシステム戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やシステム戦略の企画・立案ができる人材。 ・戦略に基づく計画の管理に関して、実行だけでなく評価と改善ができる人材。
		経営・事業戦略の策定	基本構想の策定 アクションプランの策定 事業戦略実行体制の確立	
		経営・事業戦略の評価	戦略全体の評価 費用対効果の検証 次期戦略への反映	
		システム戦略の策定	現状分析・IT 動向分析 システム基本方針の策定 システム中期計画の作成 情報セキュリティ戦略の策定	
		システム戦略評価・改善	戦略全体の評価 費用対効果の検証 次期戦略への反映	
2	システム企画	システム戦略の具体的な案件化	現行業務・システムの分析 投資規模の策定 全体構想のシステム案件化	・ＩＴに関するコスト感覚を持ち、システム工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。
		システム全体計画の策定	全体開発スケジュールの作成 費用と投資効果の予測 全体工数による案件調整	
		システム全体計画の評価	計画全体の評価 投資管理・費用対効果の検証 次期計画への反映	
3	プロジェクト管理	プロジェクト計画・管理	プロジェクト立ち上げ・終結 プロジェクト計画策定 プロジェクト実行管理	・システムに関する幅広い知識と経験があり、開発全体の流れを把握できる人材。 ・システム開発の進捗管理、システム登録、品質管理までできる人材。 ・スケジュール管理とプロジェクトの統制ができる人材。
4	業務設計・システム導入	業務要件定義	対象業務の課題整理 新業務モデルの作成 業務要件の定義	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、システム部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価及び交渉することができる人材。 ・ベンダーからの提示見積もりに対して、相見積りをとる等により妥当性を判断できる人材。 ・システム部門やベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受入れテストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。
		（外部委託） ベンダー提案評価と選定	提案依頼書の作成と発行 提案書の比較検討・委託先選定 発注契約手続	
		（外部委託） ベンダー開発管理	委託業務の開始・管理 進捗状況の把握とリスク対策 成果物の検収	
		移行・導入	受入れテスト マニュアル作成・研修 移行・導入実施	
5	システム設計・開発	システム要件定義	システム要件定義 セキュリティ要件定義 概算工数の見積り	・業務要件を整理し、システム要件を定義できる人材。 ・業務部門からの要請に対して対応できる人材。 ・業務部門からの業務要件を補えることのできる人材。 ・システム設計書、仕様書が書ける人材。 ・システム運用を考慮したシステム設計により、「工程の後戻り防止」や、「運用品質の向上」が図れる人材。 ・システム構築・プログラミングができる人材。 ・システム検証・プログラム検証ができる人材。
		（自営開発） システム設計	方式設計・アプリケーション設計 システム運用設計 保守計画・移行計画の策定	
6	システム運用	システム運用	システム監視・資源管理・性能管理 構成管理・変更管理・リリース管理 保守管理・予防保守	・ハード面の性能・リソースなどが適正であるかを管理・評価できる人材。 ・自機関システムのＯＳ・ミドルウェアなど基盤となるソフトウェアを俯瞰的に把握し、ライセンスや保守等を含め管理できる人材。 ・ネットワークがわかる人材。 ・システムの安定稼働を維持するための運用設計や運用環境の改善を継続的に提言できる人材。 ・ベンダーからの運用報告を確認、分析し、会話のできる人材。 ・オペレータの人的管理ができる人材。 ・障害等のインシデント発生時において、被害の最小化を図るとともに、品質管理などに主導的な役割を果たし、上層部に事態や対応策等について説明できる人材。
		システム障害管理・対応	システム障害検知 システム障害の初動処理 システム障害の分析・復旧・再発防止	
7	サイバーセキュリティ		本手引書「第４編」参照	本手引書「第４編」参照
8	リスク管理	情報セキュリティマネジメント	情報セキュリティ方針の策定 情報セキュリティの運用/見直し サイバーセキュリティ対策	~~・各部署のリスクを統合管理・分析することのできる人材。~~ ・システムリスクを含め、各部署のリスクを俯瞰的に管理・対応できる人材。 ・リスクの存在に気付ける人材。 ・経営層など上層部に対して、リスクの所在や事態を説明できる人材。 ・訓練実施など企画立案ができる人材。
		ＢＣＰ・事業継続マネジメント	事業継続計画の策定 事業継続計画の運用・訓練 事業継続計画の見直し	
9	システム監査	システム監査	システム監査計画の策定 システム監査の実施 システム監査結果の報告	・情報システムを総合的に点検、評価できる人材。 ・監査結果を関係者に説明して改善を勧告できる人材。 ・点検レベルではなく、ルールの提案までできる人材。
10	外部委託管理	外部委託・契約管理	外部委託先の調査 委託契約内容の確認 定期モニタリング	・チェックリストに基づく確認だけに留まらず、中身まで分かる人材。 ・外部委託先からの報告内容を把握し、必要に応じ提案等できる人材。 ・経営層など上層部に対して、外部委託に関するリスクの所在を説明できる人材。 ・外部委託先のシステムリスクを評価し、改善点を勧告できる人材。
11	自機関内教育・業務運用	ユーザー教育・研修	ヘルプデスク オペレーション研修 臨店事務指導	・営業店にて対して事務の指導ができる人材。 ・営業店事務の知識と経験がある人材。 ・現場目線で必要とする機能を集約し、具体的なシステム改善案を提案できる人材。
		ＩＴ利用推進	ＩＴシステム活用促進 全体のＩＴ活用能力底上げ 活用シナジーの促進	
12	~~データ分析~~ データ利活用	経営・事業環境の調査・分析	顧客ニーズ・マーケティング分析	・データベース等の知識があり、必要な情報を抽出して利活用できる人材。 ・データ分析の目的を理解し、目的に応じたシナリオを設定のうえ、データ分析や加工が出来る人材。 ・システム部門から提供されるデータを活用できる人材。 ・データ利活用に向け、自機関が保有するデータの整備やデータ基盤の構築に対応できる人材。
		システム企画	データ利活用に必要なデータ整備	

議事１

手引書原案　第３編　図表修正案（図表４・図表８・図表９）

手引書修正案（P26）　第３編　工程２-１　ＩＴ人材・スキルの定義　図表９

一覧No.	ご意見内容と図表修正方針
3	システムの工程からの観点からすると「３業務設計・システム導入」と「４プロジェクト管理」は順序を入れ替えた方がよい。 ⇒ご意見に基づき、「３プロジェクト管理」「４業務設計・システム導入」の順に記載します。
8	IPA の IT 人材育成（https://www.ipa.go.jp/jinzai/itss/itssplus.html）にて、データサイエンス領域について新スキル標準の策定に関し取り纏め・公開されているので、ここから引用する、あるいはここを参照するのが望ましい。 ⇒データサイエンス領域のスキルについては、ご意見いただいた主旨のとおり認識しています。 今回、ご意見№９の対応に伴い「ＩＴ人材の役割の分類」を“データ分析”から“データ利活用”に変更しますので、現段階ではデータ利活用領域のスキル標準を含む『i コンピテンシ ディクショナリ（iCD2017)』を参考文献として紹介したいと考えます。
10	知識の例として「・業務システムの主管部門と担当者」とあるが、どういった知識なのかわかりにくい。 ⇒当該スキルは、知識として記載する内容ではないと考え、削除します。

図表９　ＩＴ人材に求められるスキルの整理の手順例

ＩＴ人材の役割の分類		求められるＩＴ人材像	スキル		
			知識	経験	技量
1	戦略策定 経営戦略 事業戦略 システム戦略	・ITに関する知識は、専門家レベルである必要はないが、ITソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をシステム戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やシステム戦略の企画・立案ができる人材。 ・戦略に基づく計画の管理に関して、実行だけでなく評価と改善ができる人材。	・自機関内外の事業環境 ・ＩＴ基礎知識 ・金融機関のＩＴ動向 ・新しいＩＴ技術 ・ＩＴの活用事例 ・ＳＷＯＴ分析 ・業務改善技法 ・開発投資対効果 ・評価指標（ＫＧＩ・ＫＰＩ）	経営企画部門 〇年以上	・コミュニケーション ・ネゴシエーション ・マネジメント ・創造力
2	システム企画	・ＩＴに関するコスト感覚を持ち、システム工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。	・自機関内のＩＴ全般に関する知識 ・ＩＴポートフォリオ ・新しいＩＴ技術 ・ＩＴの活用事例 ・開発スケジュール立案に関する知識 ・開発投資対効果 ~~・業務システムの主管部門と担当者~~	システム部門 〇年以上	・コミュニケーション ・マネジメント ・本質（目的）思考力
3	プロジェクト管理	・システムに関する幅広い知識と経験があり、開発全体の流れを把握できる人材。 ・システム開発の進捗管理、システム登録、品質管理までできる人材。 ・スケジュール管理とプロジェクトの統制ができる人材。	・自機関内のＩＴ全般に関する知識 ・プロジェクト管理 ・開発スケジュール立案に関する知識 ・評価指標（ＫＧＩ・ＫＰＩ） ・問題解決手法	業務設計・システム導入 〇件以上	・コミュニケーション ・マネジメント ・問題発見・解決力 ・プレゼンテーション
4	業務設計・システム導入	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、システム部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価及び交渉することができる人材。 ・ベンダーからの提示見積もりに対して、相見積等をとる等により妥当性等を判断できる人材。 ・システム部門やベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受入れテストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。	・営業店業務知識 ・情報システム関連法規 ・ＩＴ基礎知識 ・担当する業務システムの知識（預金・融資・為替・対外等） ・新しいＩＴ技術 ・ＩＴの活用事例 ・業務改善技法 ・開発投資対効果 ・品質マネジメント	営業店業務 〇年以上 業務・商品の企画業務 〇年以上	・コミュニケーション ・ネゴシエーション ・本質（目的）思考力 ・実行・実践力
5	システム設計・開発	・業務要件を整理し、システム要件を定義できる人材。 ・業務部門からの要請に対して対応できる人材。 ・業務部門からの業務要件を補えることのできる人材。 ・システム設計書、仕様書が書ける人材。 ・システム運用を考慮したシステム設計により、「工程の後戻り防止」や、「運用品質の向上」が図れる人材。 ・システム構築・プログラミングができる人材。 ・システム検証・プログラム検証ができる人材。	・プログラム知識 ・開発ツールの知識 ・データベース知識 ・システム基盤構築の知識 ・業務知識 ・担当する業務システムの知識（預金・融資・為替・対外等） ・テスト手法・テストツール		・論理的思考 ・問題分析・解決力 ・継続力 ・コミュニケーション
6	システム運用	・ネットワークがわかる人材。 ・ハード面の性能・リソースなどが適正であるかを管理・評価できる人材。 ・自機関システムのＯＳ・ミドルウェアなど基盤となるソフトウェアを俯瞰的に把握し、ライセンスや保守等を含め管理できる人材。 ・システムの安定稼働を維持するための運用設計や運用環境の改善を継続的に提言できる人材。 ・ベンダーからの運用報告を確認、分析し、会話のできる人材。 ・オペレータの人的管理ができる人材。 ・障害等のインシデント発生時において、被害の最小化を図るとともに、品質管理などに主導的な役割を果たし、上層部に事態や対応策等について説明できる人材。	・自機関内のシステム基盤及びインフラに関する知識（ハード、ＯＳ、ミドルウェア、ネットワークなど） ・ＩＴ基礎知識 ~~・業務システムの主管部門と担当者~~ ・セキュリティ動向		・問題発見・分析力 ・継続力 ・コミュニケーション
7	サイバーセキュリティ	本手引書「第４編」参照	本手引書「第４編」参照		
8	リスク管理	・各部署のリスクを統合管理・分析することのできる人材。 ・サイバーセキュリティを含めシステムリスクを俯瞰的に管理・対応できる人材。 ・リスクの存在に気付ける人材。 ・経営層など上層部に対して、リスクの所在や事態を説明できる人材。 ・訓練実施など企画立案ができる人材。	・業務知識 ・情報システム関連法規 ・ＩＴ基礎知識 ・リスク分析・管理手法 ・情報セキュリティ管理手法 ・ＢＣＰ関連知識	システム部門 〇年以上	・コミュニケーション ・ネゴシエーション ・マネジメント ・創造力
9	システム監査	・情報システムを総合的に点検、評価できる人材。 ・監査結果を関係者に説明して改善を勧告できる人材。 ・点検レベルではなく、ルールの提案までできる人材。	・自機関内のＩＴ全般に関する知識 ・情報システム関連法規 ・システム監査手法 ・品質マネジメント ・リスク分析・管理手法 ・情報セキュリティ管理手法 ・業務改善手法	システム部門 〇年以上	・コミュニケーション ・マネジメント ・本質（目的）思考力 ・論理的思考 ・問題分析・解決力
10	外部委託管理	・チェックリストに基づく確認だけに留まらず、中身まで分かる人材。 ・外部委託先からの報告内容を把握し、必要に応じ提案等できる人材。 ・外部委託先のシステムリスクを評価し、改善点を勧告できる人材。	・業務知識 ・情報システム関連法規 ・外部委託先に関する情報 ・ＩＴ基礎知識 ・情報セキュリティ管理手法		・コミュニケーション ・ネゴシエーション ・マネジメント
11	社内教育・業務運用	・営業店にて対して事務の指導ができる人材。 ・営業店事務の知識と経験がある人材。	・営業店業務知識 ・担当する業務システムの知識（預金・融資・為替・対外等）	営業店業務 〇年以上	・コミュニケーション ・創造力 ・実行・実践力
12	~~データ分析~~ データ利活用	・データベース等の知識があり、必要な情報を抽出して利活用できる人材。 ・データ分析の目的を理解し、目的に応じたシナリオを設定のうえ、データ分析や加工が出来る人材。 ・システム部門から提供されるデータを活用できる人材。 ・データ利活用に向け、自機関が保有するデータの整備やデータ基盤の構築に対応できる人材。	・自機関内データベースの知識 ・社内外の事業環境 ・データ分析手法 ・マーケティング分析手法 ・セグメンテーション		・本質（目的）思考力 ・実行・実践力 ・継続力

スキルの整理については、以下の資料が参考になる。

（参考）
・『ｉ コンピテンシ ディクショナリ（iCD2017）　（スキルディクショナリ）』（独立行政法人　情報処理推進機構（IPA）：平成 29 年６月）

手引書原案　第４編　図表追加・修正案（図表 11・図表 13・図表 14・図表 15）

手引書修正案（P.40）　第４編　工程１-１　現状のＩＴ業務の洗い出し　図表 11

図表 11　サイバーセキュリティ業務・役割の洗い出しの例

業務の分類例		業務・役割の洗い出し例	
サイバーセキュリティに関係する業務	戦略策定 経営戦略・事業戦略・ システム戦略	情報セキュリティ戦略	情報セキュリティ戦略の策定
			情報セキュリティ戦略の遂行
	サイバーセキュリティ	態勢整備・平時の運用	現状評価
			脆弱性対応
			システム・ネットワーク運用・監視
			情報収集・分析
			教育・訓練・演習
		インシデント発生時の運用	インシデント対応管理
			インシデント対応
			フォレンジック
			情報収集・共有
	個別システム案件管理	システム要件定義・ システム設計	セキュリティ要件定義・設計
		システム構築・ システムテスト	セキュリティを意識したプログラミング・テスト
	リスク管理	リスク管理	サイバー攻撃リスクの管理・評価・報告
		外部委託管理	外部委託管理・評価・報告
	監査	情報セキュリティ監査	情報セキュリティ監査

以下の文献を参考に FISC にて作成。
「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年
「金融機関におけるコンティンジェンシープラン策定のための手引書　第３版追補３」、公益財団法人　金融情報システムセンター、平成 29 年

図表 11 を参照する上での留意事項（本文記載内容）
（P.39） 図表 11 のサイバーセキュリティに関係する業務・役割の洗い出しの例は、『コンテ手引書』に記載の経営層など組織の責任者等及びインシデント対応組織の役割を参照している。なお、この図表は１つの例であるため、自機関の特性（業態・規模・外部委託している業務範囲等）に即した、サイバーセキュリティに関係する業務・役割の洗い出しと整理が必要である。 すなわち、インシデント発生時の運用と平時の運用だけではなく、戦略策定・経営戦略・事業戦略・システム戦略や、個別システム案件管理、リスク管理等の業務・役割についても整理する等、業務・役割の洗い出しにあたって漏れが無いように業務全体を考慮する必要がある。

手引書追加案（P.44）　第４編　工程１-１　現状のＩＴ業務の洗い出し　図表 13

図表 13　サイバーセキュリティ業務・役割の細分化と分担整理の例

業務の分類例		業務・役割の洗い出し例				自機関内	外部委託	共同センター
サイバーセキュリティに関係する業務	戦略策定 経営戦略・事業戦略・システム戦略	情報セキュリティ戦略	情報セキュリティ戦略の策定	・情報セキュリティ戦略の策定	・・・・		自機関の現状、将来像に合わせて区分け	
			情報セキュリティ戦略の遂行	・情報セキュリティ戦略の遂行	・・・・			
	サイバーセキュリティ	態勢整備・平時の運用	現状評価・報告	・現状の評価と経営層への報告	・・・・			
					・・・・			
				・業務的視点及び専門的視点の双方を踏まえた対応方針の確認	・・・・			
					・・・・			
			脆弱性対応	・脆弱性診断	・・・・			
			システム・ネットワーク運用・監視	・監視・分析	・・・・			
				・脆弱性情報・脅威情報への対応	・・・・			
				・ログの取得・保全	・・・・			
			情報収集・分析	・情報収集	・・・・			
				・情報分析	・・・・			
				・情報共有	・・・・			
				・自機関内外の対応窓口の設置・周知	・・・・			
			教育・訓練・演習	・サイバー攻撃対応に関する教育・訓練・演習の企画・推進	・・・・			
					・・・・			
					・・・・			
		インシデント発生時の運用	インシデント対応管理	・執行部門と経営層との連携・調整・対応指示	・・・・			
					・・・・			
				・コンティンジェンシープランを発動した該当事象に関する発生状況の報告	・・・・			
					・・・・			
			インシデント対応	・インシデントの受付	・・・・			
				・インシデントへの対応	・・・・			
					・・・・			
			フォレンジック	フォレンジック	・・・・			
					・・・・			
			情報収集・共有	・経営層や関係部門等との調整・報告	・・・・			
				・外部機関との連携	・・・・			
				・情報共有	・・・・			
	・・・・	・・・・	・・・・	・・・・	・・・・			

細分化

以下の文献を参考に FISC にて作成
「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年
「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 版」、特定非営利活動法人　日本ネットワークセキュリティ協会（JNSA）、平成 29 年
「CSIRT 人材の定義と確保（Ver.1.0、1.5）」、日本コンピュータセキュリティインシデント対応チーム協議会（NCA）、平成 29 年
「セキュリティ対応組織の教科書～機能・役割・人材スキル～　第 1.0 版」、日本セキュリティオペレーション事業者協議会（ISOG-J）、平成 28 年
「産業横断　人材定義リファレンス　～機能と業務に基づくセキュリティ人材定義」、産業横断サイバーセキュリティ人材育成検討会、平成 28 年
「National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework」,NIST,2017
「金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）」、公益財団法人　金融情報システムセンター（FISC）、平成 29 年

図表 13 を参照する上での留意事項（本文記載内容）

（P.43）
　サイバーセキュリティに関係する業務の全体を整理したうえで、段階的に業務を細分化し、役割を導き出す。自機関におけるサイバーセキュリティに関する戦略・方針や外部委託の状況などを踏まえて整理することで、各役割の過不足を認識できる。また、中長期的なシステム戦略やビジョン等に基づき必要となるサイバーセキュリティに関係する業務の役割の分担状況（すなわち、自機関における確保・育成、外部委託、共同センターの利用）を把握することができるようになる（図表 13 参照）。

手引書修正案（P.48）　第４編　工程２-１　ＩＴ人材・スキルの定義　図表 14

図表 14　サイバーセキュリティ人材の役割・人材像の例

サイバーセキュリティ人材の役割の分類		担うべき業務・役割			求められる人材像
サイバーセキュリティに関係する業務	戦略策定 経営戦略･事業戦略・システム戦略	情報セキュリティ戦略	情報セキュリティ戦略の策定	―	・自機関または外部委託における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定ができる人材。 ・自機関または外部委託の情報セキュリティ対策に関連する業務全体を俯瞰し、外部委託を含むリソース配分の判断・決定ができる人材。
			情報セキュリティ戦略の遂行	―	・組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むことができる人材。 ・情報セキュリティ*対策の立案や実施（指示・統括）、及びその見直しができる人材。 ・自機関または外部委託における情報セキュリティ対策の具体化や実施を統括できる人材。 ・自機関または外部委託における情報セキュリティ戦略の啓発や教育の計画を立案・推進できる人材。
	サイバーセキュリティ	態勢整備・平時の運用	現状評価・報告	・現状の評価と経営層への報告 ・業務的視点及び専門的視点の双方を踏まえた対応方針の確認	・サイバーセキュリティ業務の監視や分析、評価ができる人材。 ・サイバーセキュリティ関連業務に関して現状評価や課題定義を経営層等へ分かりやすく報告できる人材。
			脆弱性対応	・脆弱性診断	・ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行うことができ、判明した脆弱性に対して対策を検討することができる人材。
			システム･ネットワーク運用・監視	・監視・分析 ・脆弱性情報・脅威情報への対応 ・ログの取得・保全	・システムやネットワークの各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を行うことができる人材。 ・システムが提供しているサービスの運用・監視（ネットワーク監視等）を行い、インシデントの発生を判断できる人材。 ・サイバーセキュリティに関する知識を持ち、問い合わせ対応などのヘルプデスク業務ができる人材。 ・サイバーセキュリティ製品の有効性の判断及びそれらの導入・運用・管理ができる人材。
			情報収集・分析・共有	・情報収集 ・情報分析 ・情報共有 ・自機関内外の対応窓口の設置・周知	・インシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集することができる人材。 ・収集した情報を元に自機関への影響を検討し、検討した結果、自機関または外部委託に適用すべきかの選定ができる人材。 ・分析した情報を報告書にまとめ、情報セキュリティに関する責任者に分かりやすく報告できる人材。
			教育・訓練・演習	・サイバー攻撃対応に関する教育・訓練・演習の企画・推進	・自機関のサイバーセキュリティリテラシーの向上や底上げのための教育及び啓発活動ができる人材。 ・自機関内での実施や外部委託先等の関係組織と共同で実施されるサイバー攻撃に備えた訓練や演習への企画や推進ができる人材。
		インシデント発生時の運用	インシデント対応管理	・執行部門と経営層との連携・調整・対応指示 ・コンティンジェンシープランを発動した該当事象に関する発生状況の報告	・発生したインシデントに対する全体統制ができる人材。 ・発生したインシデントに対する対応の優先順位を判断ができる人材。 ・重大なインシデントか否かを判断し、経営層や情報セキュリティに関する責任者への報告を分かりやすく迅速に行える人材。 ・経営層や情報セキュリティに関する責任者がインシデントへの対応を意思決定する際の支援・アドバイスができる人材。 ・インシデント終息後にインシデント対応内容の振り返りを行うことができる人材。
			インシデント対応	・インシデントの受付 ・インシデントへの対応	・インシデントの対応状況を管理できる人材。 ・自機関または外部委託におけるインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理ができる人材。 ・セキュリティベンダーに処理を委託している場合には作業指示や対応状況管理ができる人材。
			フォレンジック	―	・インシデント発生時のシステムやネットワークを対象とした証拠保全ができる人材。 ・消されたデータを復元したり、痕跡を追跡したりするためのシステム的な鑑識、精密検査、解析、報告ができる人材。
			情報収集・共有	・経営層や関係部門等との調整・報告 ・外部機関との連携 ・情報共有	・JPCERT/CC、NISC、警察、監督官庁、NCA、金融 ISAC、他 CSIRT との情報連携ができる人材。 ・サイバーセキュリティ関連業務を担う社内の法務、渉外、ＩＴ部門、広報等の関係部署と情報連携ができる人材。
	システム設計・開発	システム要件定義 システム設計	セキュリティ要件定義・設計	―	・サイバーセキュリティの確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務ができる人材。 ・サイバーセキュリティ対策に関する企画・設計・最新技術調査、製品評価ができ、システムの要求定義に反映がすることができる人材。
		システム構築 システムテスト	セキュリティを意識したプログラミング･テスト	―	・サイバーセキュリティを考慮したシステムの基盤部分（OS・ネットワーク）の全体設計・運用設計・方式設計、開発ができる人材。 ・サイバーセキュリティを考慮したアプリケーションの開発、DB 設計ができる人材。 ・仕様書や設計書に従って、セキュアプログラミングができる人材。 ・サイバーセキュリティの観点からソースコードの解析を行うことができる人材。 ・テストで脆弱性を発見・除去することができる人材、または脆弱性情報を基にテストを行い、脆弱性を除去できる人材。
	リスク管理	リスク管理	サイバー攻撃リスクの管理・評価・報告	・態勢整備計画の策定 ・サイバー攻撃対応手順等の策定・見直し	・サイバーセキュリティ対策の現状に関するアセスメントが実施でき、あるべき姿とのギャップ分析をもとにリスクを評価できる人材。 ・リスク評価の結果から自機関または外部委託の事業計画に合わせて導入すべきサイバーセキュリティ対策を検討できる人材。 ・導入されたサイバーセキュリティ対策の有効性を確認し、改善計画を立案できる人材。
		外部委託管理	外部委託管理	・外部委託先を含めた態勢整備の実施状況の管理・評価・報告	・外部委託先の提供するサービスに関して調査・評価ができる人材。 ・委託契約内容を確認・見直しを行い、有事の際の外部委託先の業務と自機関の業務を明確にし、サイバーセキュリティ関連業務の役割分担を整理することができる人材。 ・外部委託先のサイバーセキュリティ業務及び関連業務の実施状況の監視や報告などの外部委託管理ができる人材。
	監査	情報セキュリティ監査	情報セキュリティ監査	―	・情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、助言ができる人材。

議事１　手引書原案　第４編　図表追加・修正案（図表 11・図表 13・図表 14・図表 15）

以下の文献を参考に FISC にて作成
「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年
「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 版」、特定非営利活動法人　日本ネットワークセキュリティ協会（JNSA）、平成 29 年
「CSIRT 人材の定義と確保（Ver.1.0、1.5）」、日本コンピュータセキュリティインシデント対応チーム協議会（NCA）、平成 29 年
「セキュリティ対応組織の教科書～機能・役割・人材スキル～　第 1.0 版」、日本セキュリティオペレーション事業者協議会（ISOG-J）、平成 28 年
「産業横断　人材定義リファレンス　～機能と業務に基づくセキュリティ人材定義」、産業横断サイバーセキュリティ人材育成検討会、平成 28 年
「National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework」,NIST,2017
「金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）」、公益財団法人　金融情報システムセンター（FISC）、平成 29 年

図表 14 を参照する上での留意事項（本文記載内容）
（P. 47） サイバーセキュリティ人材が担う役割のいくつかは、外部に委託することが考えられる一方、自機関内に担うことが望ましい役割も存在すると考えられる。 『コンテ手引書』では、自機関内で保有が望まれる役割に関して、サイバー攻撃対応の考慮事項におけるインシデント対応組織の整備及び役割の明確化の項において、「外部委託先を含めた全体の統括や業務影響の評価、対応策の判断等については、金融機関等で担うべき機能と考えられる」としている。 このような考え方を踏まえると、共同センター利用を含む外部委託先を管理統括やインシデント対応管理などの役割等については、自機関内で確保・育成することが望ましい。また、自機関内で担う業務・役割についても、必ずしも専任化する必要はなく、他の業務との兼任も想定した効率的・効果的な人材の配置が考えられる。 さらに、システム部門に限らず、経営企画部門、情報セキュリティ部門、人事部門等、様々な部門が分担して役割を担っていくことが考えられる。

手引書追加案（P.54）　第４編　工程２-１　ＩＴ人材・スキルの定義　図表 15

図表 15　サイバーセキュリティ人材に求められるスキルの整理例

サイバーセキュリティ人材の役割の分類		担うべき業務・役割	求められる人材像	スキル例（知識）
サイバーセキュリティに関係する業務	戦略策定 経営戦略･事業戦略・システム戦略	情報セキュリティ戦略の策定	・自機関または外部委託における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定ができる人材。 ・自機関または外部委託の情報セキュリティ対策に関連する業務全体を俯瞰し、外部委託を含むリソース配分の判断･決定ができる人材。	IT ガバナンス(IPA) システム戦略立案手法(IPA) システム企画立案手法(IPA) 事業継続計画(IPA) 法規・基準・標準(IPA)　等
		情報セキュリティ戦略の遂行	・組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むことができる人材。 ・情報セキュリティ*対策の立案や実施（指示・統括）、及びその見直しができる人材。 ・自機関または外部委託における情報セキュリティ対策の具体化や実施を統括できる人材。 ・自機関または外部委託における情報セキュリティ戦略の啓発や教育の計画を立案・推進できる人材。	
	サイバーセキュリティ	現状評価・報告	・サイバーセキュリティ業務の監視や分析、評価ができる人材。 ・サイバーセキュリティ関連業務に関して現状評価や課題定義を経営層等へ分かりやすく報告できる人材。	セキュリティマネジメント(JNSA) サイバー攻撃手法(JNSA)
		脆弱性対応	・ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行うことができ、判明した脆弱性に対して対策を検討することができる人材。	OS、NW、アプリ、DB の脆弱性に対する知識(NCA) ペネトレーションテストやツールに関する知識(NCA) サイバー攻撃手法(JNSA) ネットワークセキュリティ(JNSA)　等
		システム・ネットワーク運用・監視	・システムやネットワークの各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を行うことができる人材。 ・システムが提供しているサービスの運用・監視（ネットワーク監視等）を行い、インシデントの発生を判断できる人材。 ・サイバーセキュリティに関する知識を持ち、問い合わせ対応などのヘルプデスク業務ができる人材。 ・サイバーセキュリティ製品の有効性の判断及びそれらの導入・運用・管理ができる人材。	ＯＳセキュリティ【共通】（セキュアＯＳ）（JNSA) セキュリティ運用（定時運用時のセキュリティ確保）（JNSA) 攻撃手法の概論(JNSA) ファイアーウォール(JNSA) 侵入検知(JNSA) 事業継続管理(JNSA)　等
		【平時の運用】 情報収集・分析・共有	・インシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集することができる人材。 ・収集した情報を元に自機関への影響を検討し、検討した結果、自機関または外部委託に適用すべきかの選定ができる人材。 ・分析した情報を報告書にまとめ、情報セキュリティに関する責任者に分かりやすく報告できる人材。	サイバー攻撃手法(JNSA) サイバーセキュリティ問題に関する外部組織と学術機関に関する知識(NCA)　等
		教育・訓練・演習	・自機関のサイバーセキュリティリテラシーの向上や底上げのための教育及び啓発活動ができる人材。 ・自機関内での実施や外部委託先等の関係組織と共同で実施されるサイバー攻撃に備えた訓練や演習への企画や推進ができる人材。	セキュリティマネジメント(JNSA) サイバー攻撃手法(JNSA)　等
		インシデント対応管理	・発生したインシデントに対する全体統制ができる人材。 ・発生したインシデントに対する対応の優先順位を判断ができる人材。 ・重大なインシデントか否かを判断し、経営層や情報セキュリティに関する責任者への報告を分かりやすく迅速に行える人材。 ・経営層や情報セキュリティに関する責任者がインシデントへの対応を意思決定する際の支援・アドバイスができる人材。 ・インシデント終息後にインシデント対応内容の振り返りを行うことができる人材。	リスクマネジメント手法(IPA) セキュリティマネジメント(JNSA) セキュリティ運用(インシデント対応)(JNSA) 法規・基準・標準(IPA) サイバー攻撃手法(JNSA) 自機関のセキュリティアーキテクチャ、ビジネスに関する知識(NCA) 等
		インシデント対応	・インシデントの対応状況を管理できる人材。 ・自機関または外部委託におけるインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理ができる人材。 ・セキュリティベンダーに処理を委託している場合には作業指示や対応状況管理ができる人材。	
		フォレンジック	・インシデント発生時のシステムやネットワークにを対象とした証拠保全ができる人材。 ・消されたデータを復元したり、痕跡を追跡したりするためのシステム的な鑑識、精密検査、解析、報告ができる人材。	ネットワークセキュリティ(JNSA) サイバー攻撃手法(マルウェア)(JNSA) 法規・基準・標準(IPA) 脆弱性診断に関する知識(NCA) デジタルフォレンジックに関する知識(NCA)　等
		【インシデント発生時の運用】 情報収集・共有	・JPCERT/CC、NISC、警察、監督官庁、NCA、金融 ISAC、他 CSIRT との情報連携ができる人材。 ・サイバーセキュリティ関連業務を担う社内の法務、渉外、IT 部門、広報等の関係部署と情報連携ができる人材。	サイバー攻撃手法(JNSA) サイバーセキュリティ問題に関する外部組織と学術機関に関する知識(NCA)　等
		捜査	・インシデントや犯罪行為に関する動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象の絞り込みができる人材。	尋問に関するコミュニケーション能力と知識(NCA) 攻撃者の戦術・技術・手順に関する知識(NCA) サイバー犯罪に関する法律的知識 NCA)　等
	システム設計・開発	セキュリティ要件定義・設計	・サイバーセキュリティの確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務ができる人材。 ・サイバーセキュリティ対策に関する企画・設計・最新技術調査、製品評価ができ、システムの要求定義に反映がすることができる人材。	セキュアシステム設計・構築知識(JNSA) セキュリティプログラミング技法知識(JNSA) 攻撃手法の概論(JNSA)　等
		セキュリティを意識したプログラミング・テスト	・サイバーセキュリティを考慮したシステムの基盤部分（OS・ネットワーク）の全体設計・運用設計・方式設計、開発ができる人材。 ・サイバーセキュリティを考慮したアプリケーションの開発、DB 設計ができる人材。 ・仕様書や設計書に従って、セキュアプログラミングができる人材。 ・サイバーセキュリティの観点からソースコードの解析を行うことができる人材。 ・テストで脆弱性を発見・除去することができる人材、または脆弱性情報を基にテストを行い、脆弱性を除去できる人材。	ＯＳセキュリティ【共通】（識別・認証）（JNSA) セキュリティプログラミング技法知識(JNSA) セキュリティ運用(JNSA) サイバー攻撃手法(JNSA)　等

議事１　手引書原案　第４編　図表追加・修正案（図表 11・図表 13・図表 14・図表 15）

平成 29 年 9 月 26 日
公益財団法人　金融情報システムセンター

サイバーセキュリティ人材の役割の分類		担うべき業務・役割	求められる人材像	スキル例（知識）
	リスク管理	サイバー攻撃リスクの管理・評価・報告	・サイバーセキュリティ対策の現状に関するアセスメントが実施でき、あるべき姿とのギャップ分析をもとにリスクを評価できる人材。 ・リスク評価の結果から自機関または外部委託の事業計画に合わせて導入すべきサイバーセキュリティ対策を検討できる人材。 ・導入されたサイバーセキュリティ対策の有効性を確認し、改善計画を立案できる人材。	リスクマネジメント手法知識（IPA） 機関システムに関する知識（NCA） 法規・基準・標準知識（IPA）　等
		外部委託管理	・外部委託先の提供するサービスに関して調査・評価ができる人材。 ・委託契約内容を確認・見直しを行い、有事の際の外部委託先の業務と自機関の業務を明確にし、サイバーセキュリティ関連業務の役割分担を整理することができる人材。 ・外部委託先のサイバーセキュリティ業務及び関連業務の実施状況の監視や報告などの外部委託管理ができる人材。	セキュリティマネジメント（JNSA） サイバー攻撃手法（JNSA） 法規・基準・標準（IPA）　等
	監査	情報セキュリティ監査	・情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、助言ができる人材。	IT ガバナンス（IPA） システム戦略立案手法（IPA） システム監査手法（IPA） 法規・基準・標準（IPA）　等

以下の文献を参考に FISC にて作成
「i コンピテンシ ディクショナリ 2017」、独立行政法人　情報処理推進機構（IPA）、平成 29 年
「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 版」、特定非営利活動法人　日本ネットワークセキュリティ協会（JNSA）、平成 29 年
「CSIRT 人材の定義と確保（Ver.1.0、1.5）」、日本コンピュータセキュリティインシデント対応チーム協議会（NCA）、平成 29 年
「セキュリティ対応組織の教科書～機能・役割・人材スキル～　第 1.0 版」、日本セキュリティオペレーション事業者協議会、平成 28 年
「産業横断　人材定義リファレンス　～機能と業務に基づくセキュリティ人材定義」、産業横断サイバーセキュリティ人材育成検討会、平成 28 年
「National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework」,NIST,2017
「金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）」、公益財団法人　金融情報システムセンター、平成 29 年

図表 15 を参照する上での留意事項（本文記載内容）

（P. 53）
図表 15 として例示する各役割に必要となるスキル整理表を作成することで、確保・育成する際に必要となるスキルについて考察ができるようになり、第３工程において実施すべきスキルの適正化に繋げることができるようになる。たとえば、自機関内における育成においては、実際に存在する人材の現状のスキルと、必要とされるスキルを比較してギャップを見出すことにより、育成すべきスキルの明確化ができるものと考えられる。また、確保においては、自機関内にそのスキルを保有する人材がいるかどうかを把握することで、自機関外に求める人材に必要なスキルを明確にすることができるものと考えられる。
さらに、共同センターを含め外部委託した役割においては、その役割に必要なスキルを明確化することで、外部の実務者のスキルレベルを測るのに役立つものと考えられる。
なお、図表 15 に整理例として記載しているスキルの知識項目は、その役割に特徴的と思われる知識の一部を参考文献から引用し記載している。

議事２

【人材３－２－①】
平成 29 年 9 月 26 日
公益財団法人 金融情報システムセンター

第 58 回安全対策専門委員会上程資料（案）

平成 29 年度ＩＴ人材検討部会の検討結果について

『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』(以下『ＩＴ人材手引書』という）の作成に関する検討部会における検討結果について、以下のとおり取りまとめたので報告する。

Ⅰ 検討の経緯

わが国の金融機関等におけるＩＴの利活用が大きく進展したことに伴い、それを支えるＩＴ人材の役割はこれまで以上に大きくなっている。また、最近では、金融情報システムを巡る環境変化に伴い、ＩＴ人材に求められる役割・スキルは、各金融機関の特性や実情に応じて多様化している。そのような状況を踏まえて、金融機関等が個別の経営判断により、ＩＴ人材の確保・育成を進めていく際に参考となる『ＩＴ人材手引書』の作成を行うことを第 51 回安全対策専門委員会において了承を得た。

その後、平成 29 年度「ＩＴ人材検討部会」（以下「検討部会」という）を開催し、以下のとおりＩＴ人材手引書に関する検討を行った。

Ⅱ 開催実績

検討部会は、以下のスケジュールにて計３回開催された。

・平成 29 年６月 12 日　：　第１回検討部会開催
・平成 29 年８月３日　：　第２回検討部会開催
・平成 29 年９月 26 日　：　第３回検討部会開催

Ⅲ 検討結果

１．主な論点

（1）『ＩＴ人材手引書』の構成について

✓ 第１編では『ＩＴ人材手引書』の背景や位置付け等を、第２編では経営層の役割を、そして、第３編では経営層から指示を受けた実務部門が実際にＩＴ人材の確保・育成に関する計画を策定していくための手順を記載する。サイバーセキュリティへの対応は、他のＩＴ業務と異なるスキルが求められること、また、人材の数と質の不足が喫緊の課題となっていることから、第４編を設けてサイバーセキュリティ人材を確保・育成する上での考慮事項を記載する点について、共通認識が得られた。

（２）『ＩＴ人材手引書』作成の背景について

✓ 第１編の『ＩＴ人材手引書』作成の背景では、「業務の外部委託化の進展」を金融情報システムを巡る環境変化の一要素として記載していたが、一要素ではなく、「リスク管理の高度化・複雑化」、「サイバーセキュリティ対応」、「新しい技術やサービスへの対応」等によりＩＴ人材に求められる役割・スキルが多様化した結果であるとし、記載を修正した。

（３）経営層の役割について

✓ 第２編のＩＴ人材の確保・育成では、経営層の関与の重要性や、留意する事項について、共通認識が得られた。また、システム戦略を策定・実現していくためには、システム部門だけに留まらず、様々な部門等との連携が重要である点を、経営層に強く認識してもらう必要があるとの意見を踏まえ、記載を充実させた。

（４）ＩＴ人材の確保・育成に向けた実務について

✓ 第３編のＩＴ人材の確保・育成に向けた実務では、その実効性をより高める上で、各手順の中に具体的な例（ＩＴ業務の洗い出し例、ＩＴ人材の役割・人材像例）の記載が必要である点について、共通認識が得られた。また、より幅広く例を記載することが望ましいとの意見を踏まえ、記載を充実させた。

✓ 金融機関の特性（規模やシステムの運用状況、外部委託状況等）が多様化している中、幅広く例を記載しているが、具体的な取組事例についてフラッシュや機関誌等で紹介していくことにより、更なる実効的の向上に繋がる点について共通認識が得られた。この点は、サイバーセキュリティ人材についても同様である。

（５）サイバーセキュリティ人材の確保・育成について

✓ 経営層と実務者層、また関係部門間や外部との連携を円滑に行うような橋渡しを担う人材では、ＩＴ業務全般にも必要であると考えられるが、特にサイバーセキュリティの分野で求められることから、第４編の「サイバーセキュリティ人材の確保・育成に関する考慮事項」の中でその役割や必要性を明確化するとともに、関連するスキルや確保・育成の考え方についても記載した。

✓ 第３編同様、サイバーセキュリティ人材の確保・育成の実効性を高める上で、各手順の中

に具体的な例（サイバーセキュリティ業務の洗い出し例、サイバーセキュリティ人材の役割・人材像例等）の記載が必要である点について共通認識が得られた。また、より幅広く例を記載することが望ましいとの意見を踏まえ、記載を充実させた。

２．原案の詳細

第 51 回安全対策専門委員会にて提示した原案に対して、検討部会にて検討委員から多数のご意見をいただき、そのご意見に基づき修正を行った。

詳細は【資料●－●】原案のとおり。

以　上

議事２

第 58 回安全対策専門委員会上程資料（案）

【人材３－２－②】
平成 29 年 9 月 26 日
公益財団法人 金融情報システムセンター

『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』に関する FISC 会員企業への意見募集実施について

今般、『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』（以下『ＩＴ人材手引書』という）の作成原案の取りまとめが終了したことから、下記のとおり、広く意見を取り入れるために、FISC 会員企業からの意見募集（以下「意見募集」という）を実施することについてご承認いただきたい。

Ⅰ 意見募集対象

平成 29 年度ＩＴ人材検討部会にて取りまとめた、『ＩＴ人材手引書』の原案について意見募集を実施する。意見募集の実施にあたっては、以下の資料を当センターホームページの会員向け Web サイトへ掲載する。

・『ＩＴ人材手引書』の原案
・『ＩＴ人材手引書』に関するよくあるご質問（FAQ）

Ⅱ 意見募集要領

１．募集期間（予定）

平成 29 年 11 月 1 日（水）～平成 29 年 11 月 22 日（水）17 時必着

２．提出方法

所定の意見提出書式に会社名・部署、氏名、意見等を記入のうえ、電子メール又は郵送により、FISC 事務局までご提出いただく。

３．意見に対する回答

当センターホームページの会員向け Web サイトにて公表する。

Ⅲ 意見募集後の対応

FISC 事務局にて回答案及び改訂案（修正版）を作成し、検討部会で確認し、安全対策専門委員会でご審議いただく。

※誤植・脱字等、軽微な字句・語句の修正については、事務局の判断にて適宜行うこととしたく、ご了承いただきたい。

【参考】意見募集から発刊までのスケジュール（予定）

１．意見募集（Web サイト掲載）【平成 29 年 11 月 1 日（水）～平成 29 年 11 月 22 日（水）】

・当センターホームページの会員向け Web サイトへ『ＩＴ人材手引書』原案等を掲載し、FISC 会員企業から意見募集を行う。

２．意見に対する回答案等作成【平成 29 年 11 月 23 日（木）～平成 29 年 12 月 8 日（金）】（予定）

・FISC 事務局にて、意見に対する回答案及び修正原案を作成する。

３．第４回検討部会開催　【平成 29 年 12 月 15 日（金）】（予定）

・意見に対する回答案及び修正原案についてご確認いただく。

・第 60 回安全対策専門委員会上程資料案についてご確認いただく。

４．第 60 回安全対策専門委員会　【平成 30 年 1 月】（予定）

・意見に対する回答案及び修正原案についてご審議いただく。

・『ＩＴ人材手引書』の発刊についてご審議いただく。

５．意見に対する回答公開（Web サイト掲載）　【平成 30 年２月】（予定）

・当センターホームページの会員向け Web サイトへ意見に対する回答を掲載する。

６．『ＩＴ人材手引書』の発刊　【平成 30 年３月】（予定）

・FISC 事務局にて、編集・製本を行い、会員企業に配付する。

以　上

【人材３－３】
平成29年９月26日
公益財団法人 金融情報システムセンター

平成29年度　第3回IT人材検討部会
検討事項に関するご意見（メール回答用）

電子メールにて、10月4日（水）までにご連絡願います。（fisc40@fisc.or.jp）

会社名：

お名前：

第n編	項番	ご意見
（例） 第3編	（例） 手順１－１－１ 考慮事項2	・・・

参考

平成 29 年 9 月 26 日
公益財団法人 金融情報システムセンター

『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』の作成に関する検討部会委員名簿

（平成 29 年 6 月 12 日～）

（敬称略、順不同）
（所属・役職等は検討部会開催時点）

座　長	高倉　弘喜	国立情報学研究所サイバーセキュリティ研究開発センターセンター長 アーキテクチャ科学研究系教授
委　員	五百木一郎	(株)三菱東京ＵＦＪ銀行システム企画部人事教育グループ上席調査役
〃	堀之内賢吾	(株)三井住友銀行システム統括部統括グループ上席部長代理
〃	山村　　武	(株)南都銀行システム部グループ長
〃	伊豆　良一	みずほ信託銀行(株)ＩＴ・システム統括部企画チーム次長
〃	吉原　丈司	(株)東京スター銀行ＩＴ戦略部部長
〃	金丸　利明	青梅信用金庫事務部システム課専任課長
〃	内田　満夫	全国信用協同組合連合会システム業務部部長
〃	大隅　深雪	労働金庫連合会総務部次長
〃	望月　大輔	農林中央金庫ＩＴ統括部副部長
〃	上野　貴之	(株)商工組合中央金庫システム部次長
〃	安藤伊佐武	第一生命保険(株)ＩＴビジネスプロセス企画部部長
〃	中井　正幹	三井住友海上火災保険(株)ＩＴ推進部ＩＴ企画チーム課長代理
〃	和泉　哲郎	野村ホールディングス(株)ＩＴ統括部ＩＴ統括部長
〃	岸本　広己	三井住友カード(株)システム企画部（東京）グループマネージャー
〃	水崎　　玲	日本銀行金融機構局考査企画課システム・業務継続グループ企画役
〃	安冨　　潔	慶應義塾大学名誉教授･弁護士（渥美坂井法律事務所･外国法共同事業）
〃	荏原　剛樹	(株)ＮＴＴデータ第二金融事業本部第三バンキング事業部課長
〃	濱中　慎一	ＮＴＴコミュニケーションズ(株)ソリューションサービス部 第二プロジェクトマネジメント部門第一グループ担当課長
〃	金子　克己	沖電気工業(株)金融・法人ソリューション事業部 プロジェクトマネジメントオフィスシニアスペシャリスト
〃	石川　浩嗣	(株)東芝インダストリアルＩＣＴソリューション社 インダストリアルソリューション事業部 金融・情報ソリューション技術部 金融・情報ソリューション技術第一担当参事

参考

平成 29 年 9 月 26 日
公益財団法人 金融情報システムセンター

委　員	鎌田美樹夫	日本アイ・ビー・エム(株)グローバル・ビジネス・サービス事業部 金融インダストリー・ソリューション担当部長
〃	高野　幸徳	日本電気(株)金融システム開発本部主席システム主幹
〃	徳満　益範	日本ユニシス(株)ファイナンシャル第三事業部金融企画統括部 次世代ビジネス企画部事業企画室チーフ・コンサルタント
〃	斎藤　宏海	(株)日立製作所金融システム事業部事業推進本部システム統括部 グループリーダー
〃	藤田　雅人	富士通(株)金融・社会基盤営業グループシニアディレクター
〃	石井　晋也	ＮＲＩセキュアテクノロジーズ(株)サイバーコンサルティング部 上級セキュリティコンサルタント
ｵﾌﾞｻﾞｰﾊﾞｰ	遠藤　　修	独立行政法人情報処理推進機構ＩＴ人材育成本部 ＨＲＤイニシアティブセンターグループリーダー
〃	大野　博堂	(株)ＮＴＴデータ経営研究所 パートナー金融政策コンサルティングユニット本部長
〃	松延　智彦	(株)野村総合研究所システムコンサルティング事業本部 ＩＴマネジメントコンサルティング部部長
〃	洞田　慎一	一般社団法人ＪＰＣＥＲＴコーディネーションセンター 早期警戒グループマネージャー
〃	三宅　康夫	(株)ラックＩＴプロフェッショナル統括本部 エンタープライズ・セキュリティサービス事業部 セキュリティコンサルティング部第二グループ グループリーダー
〃	市村　雅史	金融庁検査局システムモニタリングチーム専門検査官
FISC 委員	志村　秀一	公益財団法人金融情報システムセンター調査部長
	和田　昌昭	〃　監査安全部長