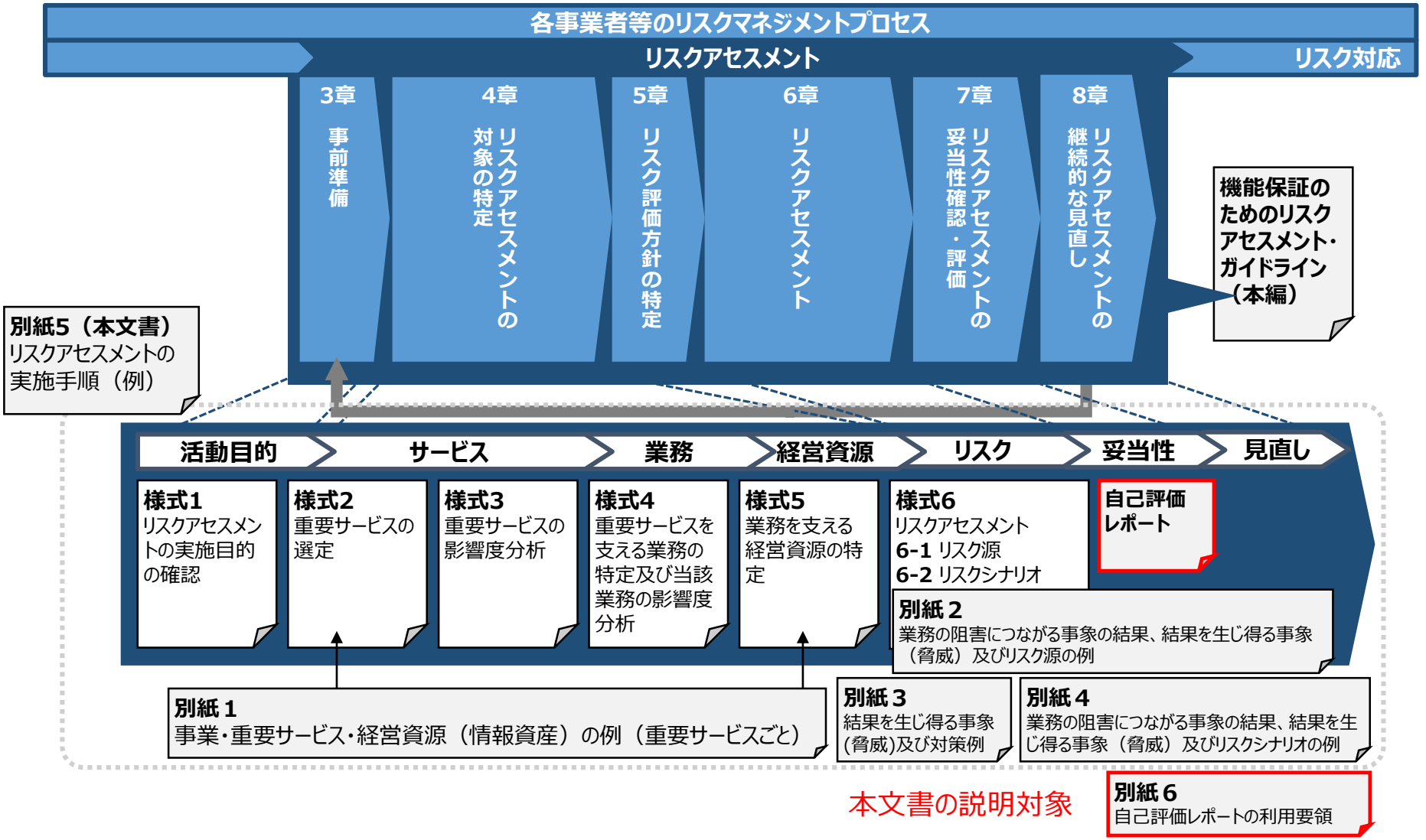
v.1.0.0 別紙６

自己評価レポートの利用要領

～社会経済を支えるサービスを提供する事業者等による自律的なリスクマネジメントに向けて～

本文書の目的・位置づけ

リスクアセスメントの実施主体自らが、リスクアセスメントの実施内容の妥当性を確認する際に参考となる、リスクアセスメントの集計結果やグラフ等を表示する「自己評価レポート」の利用方法を、主に作業担当者に向けて解説するものです。



自己評価レポートの概要

「自己評価レポート」は、社会活動を支えるサービスを提供する事業者等の皆様が、事業のサイバーセキュリティリスクや情報セキュリティリスクをアセスメントする際、その結果の充足度を確認する目的で利用できます。

この自己評価レポートを利用することで、アセスメントの実施結果の概要を確認することができます。
また、セキュリティリスクの考慮が不足している可能性がある事項を確認することもできます。

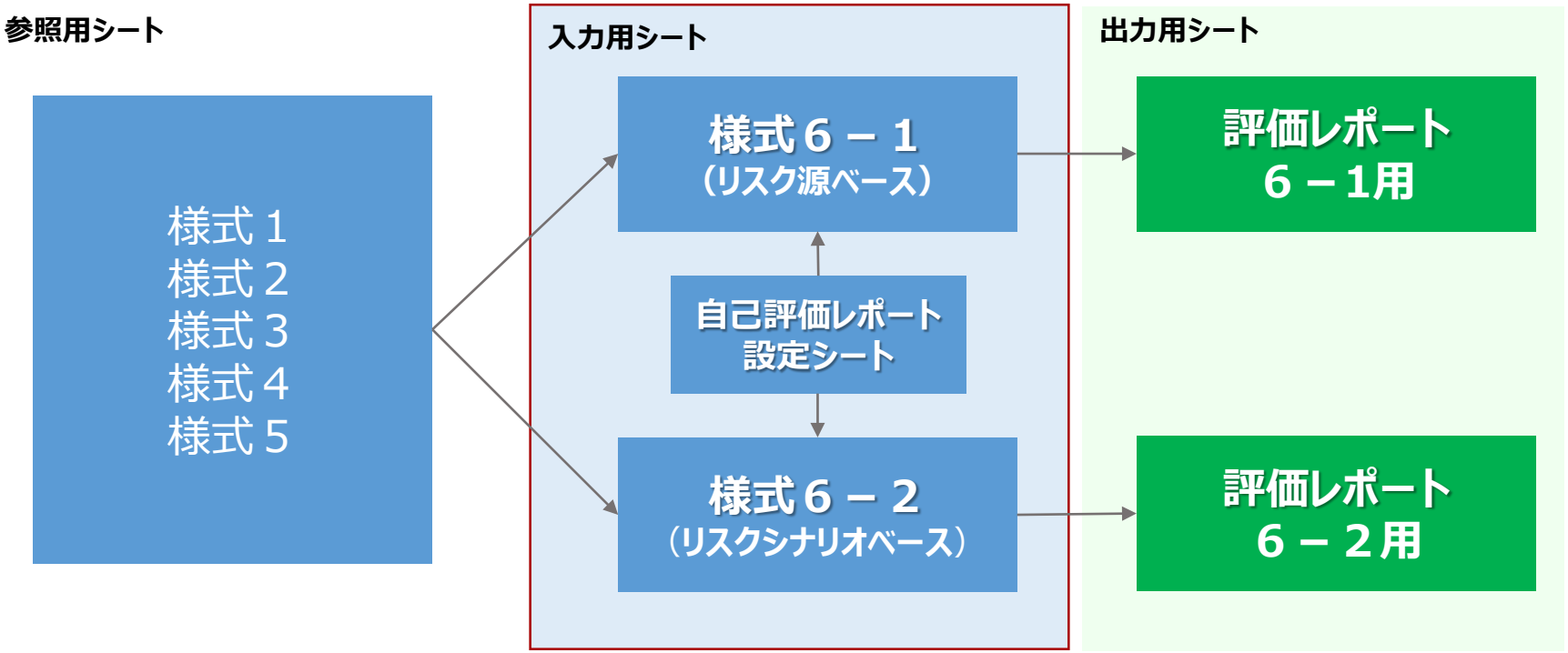
様式１～６及び自己評価レポート.xlsx

自己評価レポートはMicrosoftのExcelで作成されています。
マクロを使わず、全て関数でツールを実現しました。
セキュリティ警告が表示されず、安心して活用して頂けます。

注意:関数で実現しているため、**行や列の追加、移動、削除はできません。**

自己評価レポートは、1つのブック（ファイル）の中に、複数のシートが含まれています。
「様式６－１」又は「様式６－２」の入力を進めることで、自己評価レポートを作成できるようになっています。

自己評価レポート利用の流れ



様式１～５の記載方法については、別紙５（リスクアセスメントの実施手順）を参照してください。

様式６からは実際のリスク評価に入りますが、その際
リスク源をベースとした評価方法（様式６－１）と、
リスクシナリオをベースとした評価方法（様式６－２）に分かれます。

「様式６－１」又は「様式６－２」のシートに記入することで、対応する評価レポートのシートに結果が表示されます。

【利用の前に】 自己評価レポート設定シートで評価レンジを設定

「影響度・発生頻度の最大値」「影響度・発生頻度のレンジ」「残留リスク値のレンジ」を設定してください。

様式６-２_記入例 | 自己評価レポート設定シート | 自己評価レポート６－１（概要） | 自己評価レポート６－１（重要サービス別） | 自己評価レポート６－２（概要） | 自己評価レポ- ...

このシートでは「自己評価レポート」を出力する際の、**値の最大値**と、**範囲の重み付け**を設定します。
デフォルトでは５段階に設定していますので、自組織の基準に合わせて必要に応じて設定値を変更してください。

影響度、及び発生頻度の最大値を変更する際には、まず「**1 影響度・発生頻度の最大値**」の値を変更してください。設定可能な最大の値は20となります。その後「**2 影響度・発生頻度のレンジ**」や「**3 残留リスク値のレンジ**」を設定します。ここで設定された任意の範囲をもとに、５段階に換算して集計し、グラフ化します。換算するにあたり、自組織に適当なレンジを設定してください。

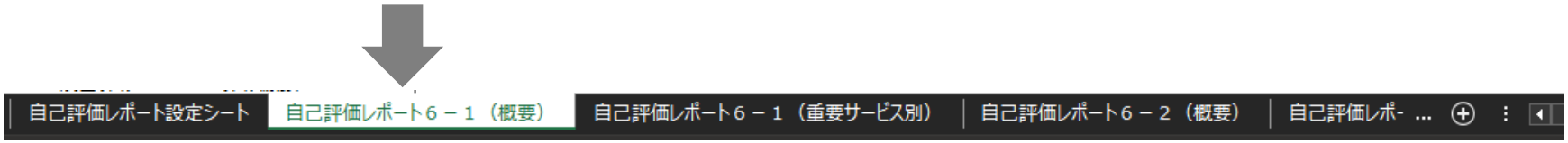
なお、例えば「５段階での表示」では割り切れない９段階で評価する場合、「1,2,3」は１として評価、「4,5」は２、「6,7」は３、「8」は４、「9」は５、と読み替えて（重み付けを行って）レポートを表示することができます。

注意:関数の連携が破損するため、**行や列の追加、移動、削除はできません。**

様式６－１　自己評価レポート（リスク源）

自己評価レポート６－１（概要）

様式６－１の記入が完了すると、関数により
「**自己評価レポート６－１（概要）**」シートにレポートが生成されます。



レポートには、以下の結果が含まれます。

出力レポート①　残留リスク値の高いリスク源Top５

出力レポート②　影響度・発生頻度・残留リスク値別リスク源数

出力レポート③　情報セキュリティ三要素及び要因別リスク源数

このシートは3種類のレポートを纏めてA4で印刷ができるように、印刷レイアウトが設定されています。

また、重要サービスごとの**詳細なリスク源数を知りたい場合**は、「**自己評価レポート６－１（重要サービス別）**」シートをご覧ください。

様式６－１　出力レポート①　残留リスク値の高いリスク源Top５

出力レポート①では、残留リスク値の高い上位５つのリスク源が表示されます。

様式６－１に入力されたデータから、関数によって「**残留リスク値の高い、上位5つのリスク源**」が表示されます。その結果を視覚的に表したものが右下の棒グラフとなっています。また、左下のマトリクスは「影響度」と「発生頻度」を含めた一覧となっています。

１．残留リスク値の高いリスク源Top５

影響度と発生頻度から算出された残留リスク値の高い上位５つのリスク源を表示します。

リスク源概要

リスク源5　：　電子カルテシステム/システム・装置が停止する/標的型ランサムウエアによる攻撃（サイバー犯罪）/エンドポイントの監視・防御の未導入

：　影響を受ける事業（病院事業/医療情報管理）

リスク源10　：　電子カルテシステム/システム・装置が停止する/標的型ランサムウエアによる攻撃（サイバー犯罪）/情報セキュリティ要員のスキル不足

：　影響を受ける事業（病院事業/医療情報管理）

リスク源7　：　電子カルテシステム/システム・装置が停止する/標的型ランサムウエアによる攻撃（サイバー犯罪）/バックアップサイトの未設置

：　影響を受ける事業（病院事業/医療情報管理）

リスク源8　：　電子カルテシステム/システム・装置が停止する/標的型ランサムウエアによる攻撃（サイバー犯罪）/不十分なセキュリティ訓練

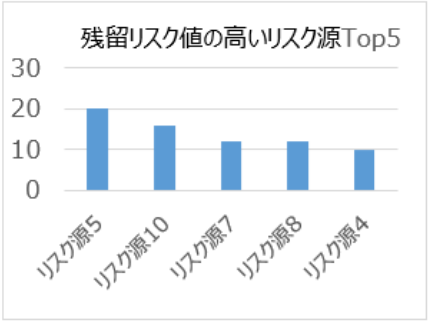
：　影響を受ける事業（病院事業/医療情報管理）

リスク源4　：　電子カルテシステム/システム・装置が停止する/標的型ランサムウエアによる攻撃（サイバー犯罪）/USB、可搬媒体が接続できる環境有

：　影響を受ける事業（病院事業/医療情報管理）

リスク分析結果

リスク源No.	影響度	発生頻度	残留リスク値
リスク源5	5	4	20
リスク源10	4	4	16
リスク源7	4	3	12
リスク源8	4	3	12
リスク源4	5	2	10



様式６－１　出力レポート②　影響度・発生頻度・残留リスク値別リスク源数

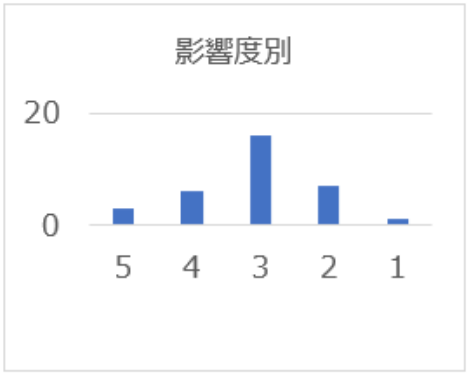
出力レポート②は、**影響度・発生頻度・残留リスク値ごとに分類したリスク源の数**が表示されます。

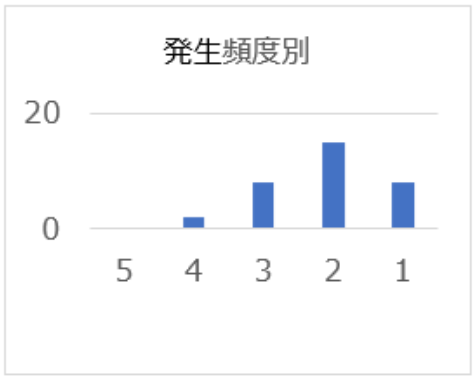
様式６－１に入力されたデータから、値の程度ごとに「影響度」と「発生頻度」「残留リスク値」が集計され、一覧で表示されます。
その結果を視覚的に表したものが下の棒グラフとなっています。

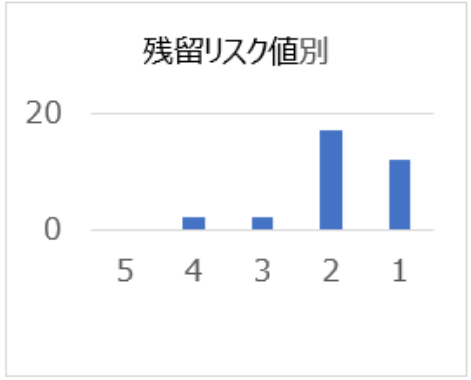
２．影響度・発生頻度・残留リスク値別リスク源数

影響度・発生頻度・残留リスク値ごとに、リスク源数を集計して表示します。
（影響度・発生頻度・残留リスク値は事業者等ごとに最大値が異なるため、影響度・発生頻度は最大5段階、評価は５段階に標準化して集計・表示しています。
（例：影響度10が最大値の場合、影響度9~10を5と表示。）なお、標準化の範囲指定は「自己評価レポート設定シート」で設定ください。）

影響度		発生頻度		残留リスク値	
影響度： 5	リスク源数 3	発生頻度： 5	リスク源数 0	残留リスク 5	リスク源数 0
影響度： 4	リスク源数 6	発生頻度： 4	リスク源数 2	残留リスク 4	リスク源数 2
影響度： 3	リスク源数 16	発生頻度： 3	リスク源数 8	残留リスク 3	リスク源数 2
影響度： 2	リスク源数 7	発生頻度： 2	リスク源数 15	残留リスク 2	リスク源数 17
影響度： 1	リスク源数 1	発生頻度： 1	リスク源数 8	残留リスク 1	リスク源数 12







様式６－１　出力レポート③　情報セキュリティ三要素及び要因別リスク源数

出力レポート③では、**情報セキュリティ三要素と、要因別のリスク源の数**が表示されます。

様式６－１に入力されたデータから、それぞれ「情報セキュリティ三要素」と「要因別」にリスク源の件数を集計し、マトリクスで表示しています。左のマトリクスは総件数、右のマトリクスは設定したリスク基準値を超えたリスク源の数を表しています。また、備考に評価観点で考慮漏れの可能性がある事項を表示していますので、評価の抜け漏れのチェックにご活用下さい。※重複を含むので、合計値は全リスク源数と一致しません。

3. 情報セキュリティ3要素及び要因別リスク源数

情報セキュリティ3要素及び要因別にリスク源数を集計して表示します。

3要素（機密性/可用性/完全性）
<総件数>

	機密性	可用性	完全性
外部不正	8	18	11
内部不正	4	6	3
外部事故	0	2	0
内部事故	2	4	1

3要素（機密性/可用性/完全性）
<リスク基準超過分のみ>

	機密性	可用性	完全性
外部不正	6	14	9
内部不正	3	2	3
外部事故	0	0	0
内部事故	2	2	1

備考（下記欄に表示された場合、評価の観点の漏れ等がないかご確認下さい。）

「別紙1 事業・重要サービス・経営資源（情報資産）の例」に示す経営資源において、評価されていない経営資源があります。
医療情報管理における「オーダエントリシステム」「看護支援システム」これらの経営資源の評価を行う必要が無いか、今一度ご確認下さい。
検査・診断における「生体情報モニタシステム」「ナースコールシステム」「臨床検査情報システム」「病理情報システム」「生体検査システム」「医用画像システム」これらの経営資源の評価を行う必要がないか、今一度ご確認下さい。

様式６－１　自己評価レポート（リスク源）を最大限活用いただくために

様式６－１ 自己評価レポート（リスク源）利用の流れ

１．**自己評価レポート設定シート**で評価レンジを設定

まず自己評価レポート設定シートで、何段階の評価とするか？を設定します（５頁参照）。

２．**様式６－１_リスクアセスメント**のシートを記入

・様式6-1_リスクアセスメントのシートに入力を進めていきます。
・**行や列の挿入、移動、削除はできません。**かならず予め用意されているフォーマットに沿って、入力を進めてください。

・(1)事業、(2)重要サービスの項目は、様式２の「分析を踏まえた重要サービスの選定」でアセスメント対象に選んだ「事業」と「サービス」を記載します。この際、「別紙1 事業・重要サービス・経営資源（情報資産）の例」を参照し、該当する事業名があるかどうかをご確認ください。「該当モデルケース」の項目はプルダウンによる選択となります。該当する事業名、重要サービス名を選択してください。プルダウンに該当する選択肢がない場合は、「－（ハイフン）」のままにします。

・(4)リスクの特定の項目では、「経営資源（情報資産）」の「該当モデルケース」の項目は、上記同様プルダウンによる選択となります。該当する経営資源（情報資産）名を選択してください。プルダウンに該当する選択肢がない場合は、「－（ハイフン）」のままにします。

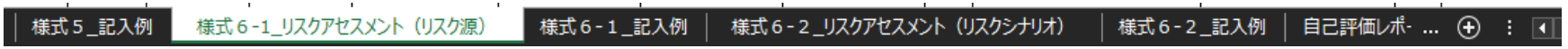
・同様に「情報セキュリティ3要素」、「要因」の項目も上記同様プルダウンによる選択となります。該当する選択肢を選んでください。情報セキュリティ3要素は単一回答だけでなく、複数回答も選択できるようになっています。（例 :機密性、可用性）

・(5)リスクの分析の項目では、リスク源ごとの事象の結果の影響度合いと、事象の発生頻度を入力します。それぞれ「対策前」および「対策後」に数値で入力することで、残留リスク値が自動で表示されます。ここで**設定できる値の範囲**は「自己評価レポート設定シート」で設定した範囲となります。

・最後に「リスク基準」を数値で入力します。自組織のリスク基準値を入力します。ここで**設定できる値の範囲**は「自己評価レポート設定シート」で設定した範囲となります。また、先頭行（リスク源01）に入力した「リスク基準」の値が、以降の行に自動入力されます。

【参考】 様式６－１の記入　リスク源ベースの評価

リスク源ベースのアセスメントを行う際には、「**様式６－１_リスクアセスメント（リスク源）**」シートを選び、入力していきます



該当モデルケースにあたる事業やサービス、情報資産がアセスメントされているか？を確認しましょう。「別紙1 事業・重要サービス・経営資源（情報資産）の例」を参照し、該当する経営資源名を選択してください。**入力はプルダウンから行います**。プルダウンに該当する選択肢がない場合は、「－（ハイフン）」のままにします。

「情報セキュリティ3要素」と、**「要因」**も**プルダウン**から選択。

STEP6:重要サービスの提供に必要な業務に係る経営資源を整理した上、当該経営資源に係るリスク（情報資産に係るリスクに限定）を特定、分析及び評価します。

(1)事業		(2)重要サービス		(3)重要サービスの提供に必要な業務	(4)リスクの特定							
	該当モデルケース		該当モデルケース		経営資源（情報資産）		該当モデルケース	業務の阻害につながる事象の結果	結果を生じ得る事象	情報セキュリティ３要素	要因	リスク源
病院事業（医療）	病院事業	医療情報管理	カルテ管理	医療情報（電子カルテ、各種オーダー、看護記録等）管理業務	電子カルテシステム	電子カルテシステム	電子カルテシステム	システム・装置が停止する	標的型ランサムウェアによる攻撃（サイバー犯罪）	機密性、可用性	外部不正	01 不正検知システムの未導入・不備
												02 インターネットへの接続環境有
												⋮
												1000 インターネットへの接続環境有

最大1,000のリスク源を記載可能
※行の追加や列の追加はできません。

事象の結果の**影響度**と**発生頻度**がどの程度か？**プルダウンで**入力します。入力する数値の範囲は「自己評価レポート設定シート」の「**１．影響度・発生頻度の最大値**」で**設定した範囲**です。初期設定は**5段階**となっています。

リスク源		(5)リスクの分析								(6)リスクの評価		
		事象の結果の影響度合い				事象の発生頻度			残留リスク値	リスク基準	リスク評価	リスクオーナーの選任（部門・部署）
		事象の結果の影響	対策前	現在講じている対策	対策後	対策前	現在講じている対策	対策後				
01	不正検知システムの未導入・不備	電子カルテシステムの停止を引き起こす攻撃が実行され、診療業務が停止する	5	ログ管理システムによりアクセスログの収集、保管、監視、分析・活用を実施	4	3	ファイアウォールを導入	2	8	5	●	
02	インターネットへの接続環境有	同上	5	ログ管理システムによりアクセスログの収集、保管、監視、分析・活用を実施（不正なアクセスが確認された際には、アラートで知らされる仕組みになっている）	4	3	ファイアウォールを導入					

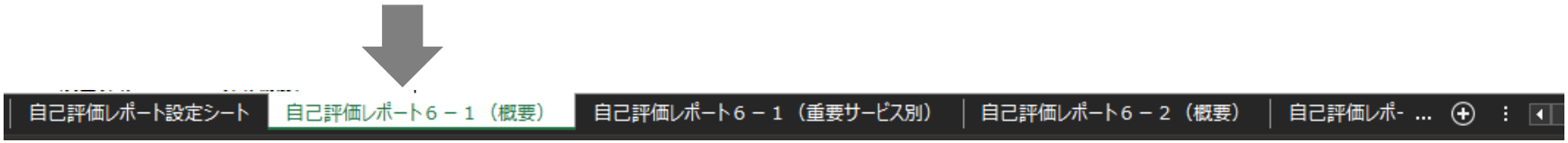
自組織のリスク基準値（「リスク評価方針の特定」において**定めた値**）**を入力**します。６－１における以降のリスク基準値はここで設定された値が自動で反映されます。

注意:関数の連携が破損するため、**行や列の追加、移動、削除はできません。**

様式６－２　自己評価レポート（リスクシナリオ）

自己評価レポート６－２（概要）

様式６－２の記入が完了すると、関数により
「**自己評価レポート６－２（概要）**」シートにレポートが生成されます。



レポートには、以下の結果が含まれます。

出力レポート①　残留リスク値の高いシナリオTop５

出力レポート②　影響度・発生頻度・残留リスク値別シナリオ数

出力レポート③　残留リスク値の高いシナリオにおける対策状況

出力レポート④　情報セキュリティ三要素及び要因別シナリオ数

このシートは３種類のレポートを纏めてA4で印刷ができるように、印刷レイアウトが設定されています。

また、重要サービスごとの**詳細なリスクシナリオ数を知りたい場合**は、「**自己評価レポート６－２（重要サービス別）**」シートをご覧ください。

様式６－２　出力レポート①　残留リスク値の高いシナリオTop５

出力レポート①では、残留リスク値の高い上位５つのシナリオが表示されます。

様式６－２に入力されたデータから、関数によって「**残留リスク値の高い、上位5つのリスクシナリオ**」が表示されます。その結果を視覚的に表したものが右下の棒グラフとなっています。また、左下のマトリクスは「影響度」と「発生頻度」を含めた一覧となっています。

１．残留リスク値の高いシナリオTop５

影響度と発生頻度から算出された残留リスク値の高い上位５つのシナリオを表示します。

シナリオ概要

シナリオ8　：　大規模な地震が関東地方を遅い、データセンターが倒壊する

：　影響を受ける事業（病院事業/医療情報管理）

シナリオ1　：　悪意ある第三者がVPN装置の脆弱性を悪用し、正規のVPN接続IDパスワードを盗むことで内部ネットワークに侵入。さらに内部ネットワークに残る脆弱性とマルウェアの悪用によって管理者のアカウントが奪われる。この管理者アカウントでADにアクセスされたことで、電子カルテシステム内の情報が盗まれ、ランサムウェア

：　影響を受ける事業（病院事業/医療情報管理）

シナリオ3　：　悪意のある第三者が、職員に標的型メールを送付し、騙された職員の端末が感染。そこから管理者のアカウントが盗まれ、患者の個人情報や電子カルテデータが盗まれる。

：　影響を受ける事業（病院事業/医療情報管理）

シナリオ2　：　悪意のある第三者が、不正な処理・機能の実行（コントローラへの不正コマンド発行）を行い、システムが停止し、重要サービスが停止する。

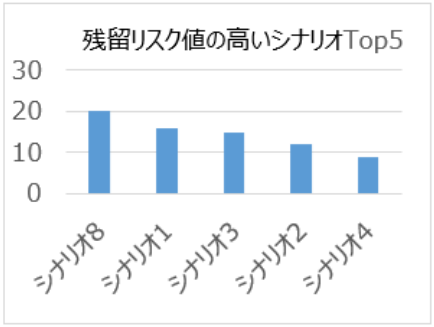
：　影響を受ける事業（病院事業/医療情報管理）

シナリオ4　：　悪意のある第三者が、職員に標的型メールを送付し、騙された職員の端末が感染。そこから管理者のアカウントが盗まれ、患者の個人情報や電子カルテデータが盗まれる。

：　影響を受ける事業（病院事業/医療情報管理）

リスク分析結果

シナリオNo.	影響度	発生頻度	残留リスク値
シナリオ8	4	5	20
シナリオ1	4	4	16
シナリオ3	5	3	15
シナリオ2	3	4	12
シナリオ4	3	3	9



様式６－２　出力レポート②　影響度・発生頻度・残留リスク値別シナリオ数

出力レポート②では、影響度と発生頻度・残留リスク値ごとに分類したシナリオの数が表示されます。

様式６－２に入力されたデータから、値の程度ごとに「影響度」「発生頻度」「残留リスク値」が集計され、一覧で表示されます。
その結果を視覚的に表したものが下の棒グラフとなっています。

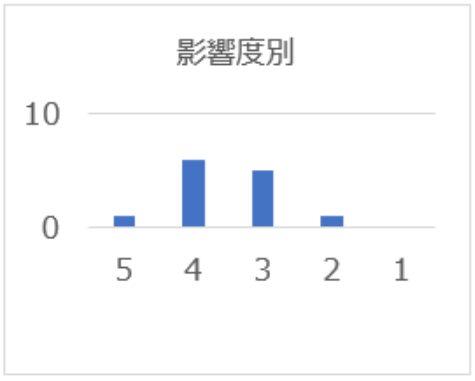
２．影響度・発生頻度・残留リスク値別リスクシナリオ数

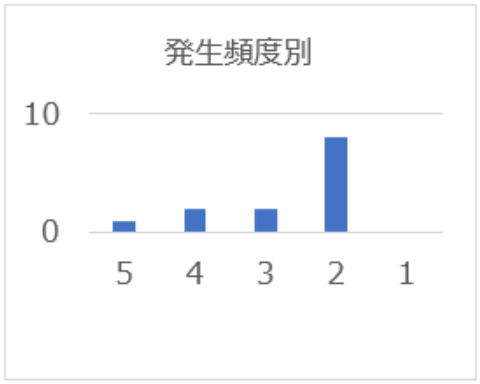
影響度・発生頻度・残留リスク値ごとに、シナリオ数を集計して表示します。
（影響度・発生頻度・残留リスク値は事業者等ごとに最大値が異なるため、影響度・発生頻度は最大5段階、評価は５段階に標準化して集計・表示しています。
（例：影響度10が最大値の場合、影響度9~10を5と表示。）なお、標準化の範囲指定は「自己評価レポート設定シート」で設定ください。）

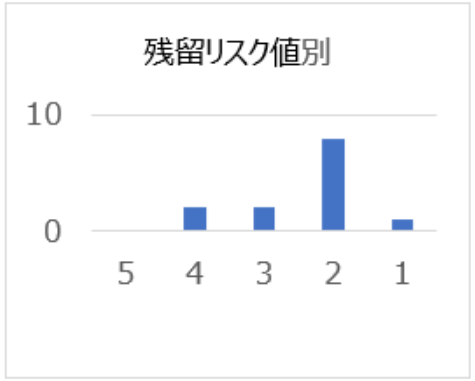
影響度			
影響度：	5	シナリオ数	1
影響度：	4	シナリオ数	6
影響度：	3	シナリオ数	5
影響度：	2	シナリオ数	1
影響度：	1	シナリオ数	0

発生頻度			
発生頻度：	5	シナリオ数	1
発生頻度：	4	シナリオ数	2
発生頻度：	3	シナリオ数	2
発生頻度：	2	シナリオ数	8
発生頻度：	1	シナリオ数	0

残留リスク値			
残留リスク	5	シナリオ数	0
残留リスク	4	シナリオ数	2
残留リスク	3	シナリオ数	2
残留リスク	2	シナリオ数	8
残留リスク	1	シナリオ数	1







様式６－２　出力レポート③　残留リスク値の高いシナリオにおける対策状況

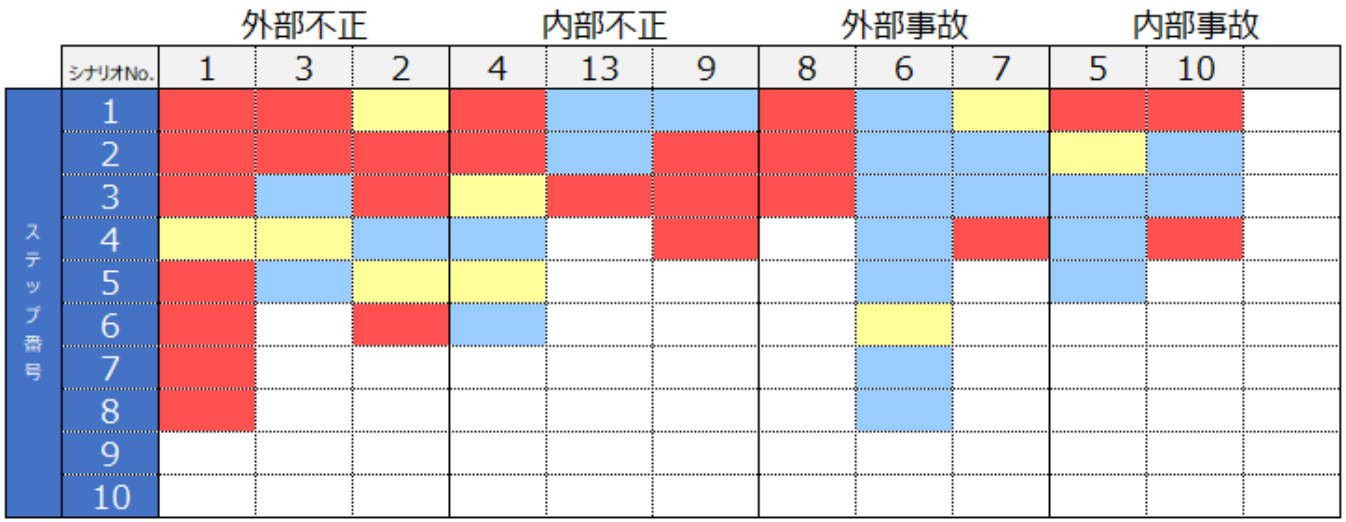
出力レポート③では、残留リスク値の高いシナリオの各ステップの対策状況を可視化します。

様式６－２に入力されたデータから、「外部不正」「内部不正」「外部事故」「内部事故」それぞれの領域について、残留リスク値の高いシナリオのステップごとに、発生頻度に応じた色付けがされています。リスクの高いシナリオについて、どこで攻撃を止められる可能性があるのか、を俯瞰することができます。

３．残留リスク値の高いシナリオにおける対策状況

残留リスク値の高いシナリオについて、各ステップの対策状況（ステップが成立する可能性）を可視化します。

（発生頻度に基づき５段階に標準化し、4~5は赤色（ステップが成立する蓋然性が高い）、3は黄色、1~2は青色で表示しています。）



様式６－２　出力レポート④　情報セキュリティ三要素及び要因別シナリオ数

出力レポート④では、**情報セキュリティ三要素と要因別のシナリオ件数**を集計して表示します。

様式６－２に入力されたデータから、それぞれ「情報セキュリティ三要素」と「要因別」にリスクシナリオの件数を集計し、マトリクスで表示しています。左のマトリクスは総件数、右のマトリクスは設定したリスク基準値を超えたリスクシナリオの数を表しています。また、備考に評価観点で考慮漏れの可能性がある事項を表示していますので、評価の抜け漏れのチェックにご活用下さい。※重複を含むので、合計値は全シナリオ数と一致しません。

４．情報セキュリティ3要素及び要因別シナリオ数

情報セキュリティ3要素及び要因別にシナリオ数を集計して表示します。

3要素（機密性/可用性/完全性）
＜総件数＞

	機密性	可用性	完全性
外部不正	2	3	1
内部不正	3	1	3
外部事故	0	3	2
内部事故	1	1	2

3要素（機密性/可用性/完全性）
＜リスク基準超過分のみ＞

	機密性	可用性	完全性
外部不正	2	2	1
内部不正	3	1	3
外部事故	0	2	2
内部事故	0	1	1

備考（下記欄に表示された場合、評価の観点の漏れ等がないかご確認下さい。）

「別紙1 事業・重要サービス・経営資源（情報資産）の例」に示す経営資源において、評価されていない経営資源があります。
医療情報管理における「電子カルテシステム」「オーダエントリシステム」「看護支援システム」これらの経営資源の評価を行う必要が無いか、今一度ご確認下さい。
検査・診断における「生体情報モニタシステム」「ナースコールシステム」「臨床検査情報システム」「病理情報システム」「生体検査システム」「医用画像システム」これらの経営資源の評価を行う必要がないか、今一度ご確認下さい。

様式６－２　自己評価レポート（リスクシナリオ）を最大限活用いただくために

様式６－２ 自己評価レポート（リスクシナリオ）利用の流れ

１．**自己評価レポート設定シート**で評価レンジを設定

まず自己評価レポート設定シートで、何段階の評価とするか？を設定します（５頁参照）。

２．**様式６－２_リスクアセスメント**のシートを記入

・様式6-2_リスクアセスメントのシートに入力を進めていきます。
・**行や列の挿入、移動、削除はできません。**かならず予め用意されているフォーマットに沿って、入力を進めてください。

・(1)事業、(2)重要サービスの項目は、様式２の「分析を踏まえた重要サービスの選定」でアセスメント対象に選んだ「事業」と「サービス」を記載します。この際、「別紙1 事業・重要サービス・経営資源（情報資産）の例」を参照し、該当する事業名があるかどうかをご確認ください。「該当モデルケース」の項目はプルダウンによる選択となります。該当する事業名、重要サービス名を選択してください。プルダウンに該当する選択肢がない場合は、「－（ハイフン）」のままにします。

・(4)リスクの特定の項目では、「経営資源（情報資産）」の「該当モデルケース」の項目は、上記同様プルダウンによる選択となります。該当する経営資源（情報資産）名を選択してください。プルダウンに該当する選択肢がない場合は、「－（ハイフン）」のままにします。

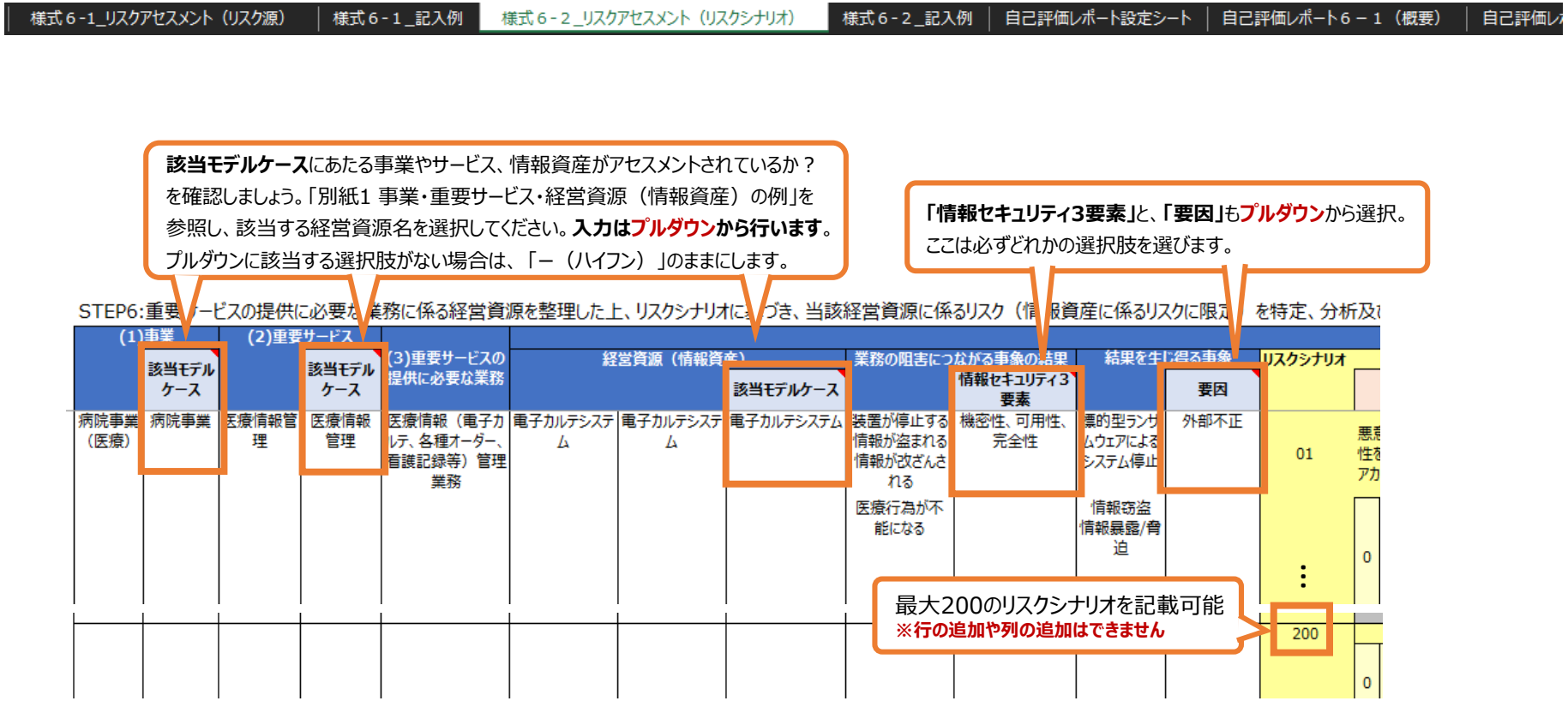
・同様に「情報セキュリティ3要素」、「要因」の項目も上記同様プルダウンによる選択となります。該当する選択肢を選んでください。情報セキュリティ3要素は単一回答だけでなく、複数回答も選択できるようになっています。（例 :機密性、可用性）

・(5)リスクの分析の項目では、リスク源ごとの事象の結果の影響度合いと、事象の発生頻度を入力します。それぞれ「対策前」および「対策後」に数値で入力することで、残留リスク値が自動で表示されます。ここで**設定できる値の範囲**は「自己評価レポート設定シート」で設定した範囲となります。

・最後に「リスク基準」を数値で入力します。自組織のリスク基準値を入力します。ここで**設定できる値の範囲**は「自己評価レポート設定シート」で設定した範囲となります。

【参考】 様式６－２の記入　リスクシナリオベースの評価

リスクシナリオベースのアセスメントを行う際には、「**様式６－２_リスクアセスメント**（リスクシナリオ）」シートを選び、入力していきます。



注意：関数の連携が破損するため、**行や列の追加、移動、削除はできません。**

【参考】 様式６－２の記入　リスクシナリオベースの評価

［様式６－２］

		(5)リスクの分析							(6)リスクの評価		
		事象の結果の影響度合い			ステップ毎・事象の発生頻度			残留リスク値	リスク基準	リスク評価	リスクオーナーの選任（部門・部
	ステップNo.	対策前	現在講じている対策	対策後	対策前	現在講じている対策	対策後				
から脆弱 管理者											
比し、テ											

⋮

	5				5	ログ収集＋異常検知時分析 操作者認証（ID/PW）	4				
、『重要	6				5	ログ収集＋異常検知時分析 操作者認証（ID/PW）	4				
	7				5	アンチウイルス ログ収集＋異常検知時分析 操作者認証（ID/PW）	4				
	8				5	アンチウイルス ログ収集＋異常検知時分析 操作者認証（ID/PW）	5				
社が盗ま 入院患 う手作		5	データバックアップ（定期実施Q毎）	4	5	アカウント管理 アンチウイルス ログ収集＋異常検知時分析 操作者認証（ID/PW）	4	16	9	●	医療法人 ○○会 GIT部門

1シナリオの最大ステップ数は**10**
（この例では8ステップまで記載）

自組織のリスク基準値（「リスク評価方針の特定」において**定めた値**）**を入力**します。
６－２におけるリスク基準値はリスクシナリオ毎に記入します。

シナリオの**影響度**と**発生頻度**がどの程度か？**プルダウン**で入力します。
入力する数値の範囲は「自己評価レポート設定シート」の「**１．影響度・発生頻度の最大値**」で**設定した範囲**です。
初期設定は**5段階**となっています。

注意：関数の連携が破損するため、**行や列の追加、移動、削除はできません。**