詳細リスク分析表

別表3

第〇〇回リスクアセスメント　YYYY年MM月DD日　作成

資産評価グループ		資産価値			脅威						脆弱性		リスク値			リスク対応	予定リスク値			管理部署	
項番	評価グループ名称	C	I	A	誰が？	どこで？	どうする？（どうなる？）	導入済み管理策	関連CIA	評価	導入済み管理策の有効性を評価し、残存する脆弱性を洗出して記述	評価	C	I	A	新たに実施する対策や改善・廃止すべき対策	C	I	A	管理責任者	管理部署
1－1																					
1－2																					
1－3																					
1－4																					
1－5																					

詳細リスク分析表

第〇〇回リスクアセスメント　YYYY年MM月DD日　作成

資産評価グループ		資産価値			脅威						脆弱性		リスク値			リスク対応	予定リスク値			管理部署	
項番	評価グループ名称	C	I	A	誰が？	どこで？	どうする？（どうなる？）	導入済み管理策	関連CIA	評価	導入済み管理策の有効性を評価し、残存する脆弱性を洗出して記述	評価	C	I	A	新たに実施する対策や改善・廃止すべき対策	C	I	A	管理責任者	管理部署
1－1																					
1－2																					

「資産評価グループ一覧表」にて定義されている
「評価グループ名称」
「対象情報資産」

表示形式：　n－n
先頭の数字は、「資産評価グループ一覧表」の評価グループ名称に対応する「No」
「－」の後ろの数字は、「洗

評価グループに関する「脅威」を記述する。どういう状況の時にどういうリスクが残存するかを脅威として文章にする。
・「誰が？」・・・「内部者」「外部者」のほか「地震」「火災」「災害」なども使用可。「システム管理者」などなるべく特定するのが望ましい。
・「どこで？」・・・「社屋」「事務室」「マシン室」「社外」「外出先」のほか「ネットワーク」なども使用可。
・「どうする？（どうなる？）」・・・起こり得る状況を文章で記す。手段・方法なども記すとよい。
いずれも、上記の例示に関わらず具体的な表現が望ましい。

左記の脅威について、その発生を抑止する、あるいは発生した場合被害を低減するために、既に実施している対策、管理策を記す。

左記の状況（脅威）が、機密性、完全性、可用性のいずれに影響を与えるか、C・I・Aで記す。
複数に影響する場合は、並記する。
「C」、「CI」、「CIA」など組合せて記す。

左記の脅威の評価値

当該脅威に関する既存対策の有効性を評価して、残存する脆弱性を明らかにする。つまり脆弱性の評価値はこの残存する脆弱性にかかる評価値となる。
ルールが定められていても守られていなければ、脆弱性は残存する。管理システムが導入されていても、機能不足が有ったり、運用の抜け道があれば脆弱性は残存する。

左記の脅威にかかる脆弱性の評価値
1～3

「資産価値のCIA」に、当該脅威の「関連CIA」についてそれぞれ「脅威の評価値」「脆弱性の評価値」を乗じた値（当該脅威が関連しないCIAについては、

残存脆弱性の低減をはかる新たな対策や改善策などを記す。
また、有効性がない既存対策については廃止も検討する。
検討した対策の実施について、費用対効果など経営上現実的でない場合は、リスクを認識しながらも受容する判断も有り得る。この場合もその旨記載して記録する。

「資産価値のCIA」に、当該脅威の「関連CIA」についてそれぞれ「脅威の評価値」「脆弱性の評価値」を乗じた値（当該脅威が関連しないCIAについては、

管理部署としては、少なくとも「部」レベルで明確にする。
責任者は当該部の「部長」とする。但、さらに管理権限委譲している場合は、具体的に記載する。
また、特別な管理体制の場合も主管部署のみならず管理体制を明示

■資産価値の評価基準

機密性（C）　1　：情報が漏洩しても大きな問題とならない（社外秘情報）。資産価値「2」「3」以外の情報資産。
　　2　：JA等取引先に影響を及ぼす（社外秘情報／厳秘情報）。社員情報、顧客団体の経営情報。
　　3　：情報漏洩時に社会問題となる又は賠償問題に発展する可能性がある（厳秘情報）
　　個人情報に当たる顧客情報。

完全性（Ｉ）　1　：情報が変更及び改竄された場合、ビジネスへの影響がほとんどない。価値「2」「3」のうち利用範囲が極めて限定的。複写等原本でない。価値「2」「3」以外の情報資産。
　　2　：情報が変更及び改竄された場合、ビジネスへの影響が大きい。価値「3」のうち利用範囲が限定的。複写等原本でない。社員情報、JA情報、ソースプログラム、仕様書、契約書等。
　　3　：情報が変更及び改竄された場合、ビジネスへの影響が甚大かつ重大である。個人情報にあたる顧客情報等。

可用性（Ａ）　1　：翌日以降には利用可能にしなければならない情報資産。価値「2」「3」以外（帳表システム等）。
　　2　：当日には利用可能としなければならない情報資産。口振システム、日経等更新処理、期限付き登録処理等。
　　3　：60分以内に利用可能としなければならない情報資産。価値

■脅威の評価基準

1　：発生する可能性は低い。1年以内に発生する可能性は低い。通常の状態では発生する可能性は低い。
2　：発生する可能性は中程度である。発生頻度は1年以内に1回あるかないかである。特定の状況もしくは特定の担当者の不注意で発生する可能性が高い脅威。
3　：発生する可能性は高い。発生頻度は1ケ月に1回以上である。通常の状態で発生する可能性が高い。

■脆弱性の評価基準

1　：適切な管理策が施されていて、脅威がほとんど顕在化しない。技術的対策、物理的対策、管理的対策（手順の確立、文書化など）が適切に施されている状況。
2　：一部対策が施されているが、脅威が顕在化する可能性がある。技術的対策、物理的対策、管理的対策（手順の確立、文書化など）において一部対策が施されているが、対策の追加、未対策の情報資産への対策の適用等が必要である状況。
3　：対策がほとんど施されておらず、いつでも脅威を顕在化させる事象を誘因する可能性がある。技術的対策、物理的対策、管理的対策（手順の確立、文書化など）のいずれもほとんど施されていな状況。