

情報リスクアセスメント マネジメント要領

株式会社三重県農協情報センター

改廃履歴

R e v	改 廃 内 容	実 施 日
1.0	新規作成	2005.04.01
1.1	情報資産再調査に伴う記述追加	2005.08.01
1.2	詳細リスク分析表の記載項目追加	2006.01.20
2.0	JIS_Q_27001 対応により、管理策の有効性評価の記述追加	2006.11.01
2.1	9. 本文書の改訂 改定の承認者 社長→副社長	2008.10.30
2.2	規程名称の変更等	2010.11.22
2.3	「脅威・脆弱性一覧表（情報セキュリティ）」（別表１）、「分類基準表」（別表２）追加	2012.03.01
3.0	ISO/IEC27001:2013(JIS_Q_27001:2014)への移行に伴う見直し	2014.09.10
4.0	ISMS 情報資産管理台帳の改善に伴い、「7. 詳細リスク分析表に記載する項目」を修正	2016.09.01
4.1	情報資産ツールの利用停止に伴う修正	2017.10.15
4.2	元号改正に伴う改正（別表３）	2019.05.01
4.3	パスワード管理にかかる脆弱性の評価基準見直し （別表２：分類基準表）	2021.12.01
5.0	I S M S 規格改訂対応	2024.10.01

情報リスクアセスメントマネジメント要領

規程番号 0301-0000-03-要

制 定 日 2005年 4月 1日

改 正 日 2024年10月 1日

1. 本文書の位置付け

本文書は、リスクアセスメントおよびリスクマネジメントの手順について詳細を定める文書である。

2. リスクアセスメントの目的

ISMS を確立するためには、ISMS の適用範囲内にある情報資産を洗い出し、その情報資産が持つ事実上の価値を明確にし、資産価値に応じて様々な脅威から適切に保護できる環境を構築する必要がある。そのために、個々の情報資産の管理状況を正確に把握し、存在する脅威およびその脅威に対して情報資産が持つ脆弱性、問題が発生した場合の事業上の影響等を明確にすることがリスクアセスメントの目的である。

社内業務や受託業務サービスの運用環境に変化が生じた場合、または情報資産の価値を見直し、情報資産の存在を確認するため、定期的（少なくとも年一回）に情報資産の再調査（棚卸し）を実施し、以降に示すリスクアセスメント、リスクマネジメントの作業を繰り返し行なう。

3. リスクアセスメントの対象

リスクアセスメントの対象は、「情報資産洗い出し要領」に則って作成された「資産評価グループ一覧表」の評価グループ単位とする。

4. リスクアセスメントの方法

ISMS 範囲内の情報資産とその責任者を特定し、それらに対する脅威と脆弱性を明確にし、情報資産の機密性、完全性および可用性の喪失による影響を明確にする。

（1）情報資産の洗い出し

ISMS 適用範囲における情報資産の保有状況を確認し、属性や価値を明確にするために、「情報資産洗い出し要領」に従い情報資産管理台帳を作成する。

（2）情報資産のグループ化

リスクアセスメント作業およびセキュリティ管理の効率化を図るため、洗い出した情報資産を「情報資産洗い出し要領」に従いグループ化し「資産評価グループ一覧表」を作成する。

（3）情報資産グループと管理策のマトリックス表

情報資産グループと JIS_Q_27001 付属書 A・JIS_Q_27002「管理策および管理目的」との対応表を作成する。

（4）ギャップ分析

ギャップ分析とは、ISMS 適用範囲の情報セキュリティ現状と JIS_Q_27001 付属書 A・JIS_Q_27002「管理策および管理目的」の管理策が求めるレベルとの乖離を評価することである。ギャップ分析をおこなうことによって、ISMS の有効性測定の一

環として対応度合いをチェックする。

(5) 脅威・脆弱性の明確化と評価

リスクが顕在化する要因（以下、リスク因子という）は、それぞれの情報資産がさらされている脅威と管理上の問題点による脆弱性の組み合わせである。リスク因子を特定するために、脅威と脆弱性の識別を行なう。

① 脅威の識別と評価

脅威とは、情報セキュリティを要求される水準以下に引き下げる潜在的な原因のことである。「脅威・脆弱性一覧表（情報セキュリティ）」（別表1）を基準に、当社の情報資産に対する脅威を明確にする。また、「脅威・脆弱性評価基準表」（別表2）を基準に脅威の大きさを「詳細リスク分析表」で評価する。

② 脆弱性の識別と評価

脆弱性とは、情報資産や人員の管理方法に関連する弱点のことである。もし管理方法に問題があれば（弱点が大きければ）、脅威が表面化する可能性が高くなる。しかし、たとえ大きな脅威が存在していても、適切な管理がなされていれば（弱点が小さければ）深刻な問題には陥らないはずである。

このように、脅威と脆弱性は常に関連付けて検討しなければならない。脅威は、通常完全には取り去ることができないが、脆弱性については適切な管理策を講じることで大幅に低減させることができる。つまり、脆弱性の低減が、問題の発生を抑止し、結果的にリスクを減少させることに繋がると言える。

「脅威・脆弱性一覧表（情報セキュリティ）」（別表1）を基準に、①で識別した脅威に対する脆弱性を明確にする。また、「脅威・脆弱性評価基準表」（別表2）を基準に脆弱性の大きさを「詳細リスク分析表」で評価する。

(6) リスク値の算出


リスク値は、上記（1）から（3）までの作業で明確になった「情報資産の価値」、「脅威の大きさ」、「脆弱性の大きさ」を用いて、簡易的に次の式で算出する。

$$\text{リスク値} = \text{「情報資産の価値」} \times \text{「脅威」} \times \text{「脆弱性」}$$

(7) リスク評価

詳細リスク分析により明確になった「情報資産の価値」「脅威」「脆弱性」から、「機密性」「完全性」「可用性」のそれぞれのリスク値を算出する。

	脅威								
	1			2			3		
	脆弱性								
資産価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27

 リスクに対して何らかの対策を講じる範囲
(その他についてはリスクを受容できる範囲)

(8) 管理策の有効性測定と評価

JIS_Q_27001 付属書A・JIS_Q_27002「管理策および管理目的」の管理目的を一つの管理策グループとし、管理策グループに関連する情報資産グループ((3)にて作成したマトリックス表による)のリスク値から最大リスク値を求め、当該リスク値を管理策グループの評価値として有効性を評価する。(4)で実施したギャップ分析結果と合わせることで、対応度合いとの関連からも管理策グループごとの有効性を評価する。

有効性評価の結果に基づき、必要であれば管理策グループに対する新たな管理策の追加(適用宣言書への反映)および管理策実施の為の具体策の追加を検討する。

以下に記す規程にもとづく記録、日常点検等の記録も含めて総合的にISMSの有効性評価を実施する。

①規程にて定めている有効性評価の記録

NO	規程名	条文等	記録の名称等	備考
1	セキュリティ教育実施規程	第12条	教育予定表兼実施結果報告書	必要に応じて研修終了後一定期間置いて実施も考慮
2	是正予防処置実施規程	第8条、第14条	是正・予防対策計画書	

②日常点検等の記録

NO	記録の名称等	備考
1	クライアントPCセキュリティ調査結果報告書	
2	m-FILTER調査結果報告書	
3	F/Wログ調査結果報告書	
4	ウィルス調査結果報告書	
5	障害報告書	
6	サーバ別稼働状況報告書	
7	情報セキュリティ遵守状況チェックリスト	
8	監査報告書(内部監査、外部監査・審査)	

なお、これらは単に件数の推移で定数的に見ることではなく、むしろ内容を検証した上で、有効性評価することが必要。問題発生件数は一つの指標ではあるが、多い少ないに注目しすぎると正確な報告がなされなくなり報告件数自体が意味のない数値となる。影響の度合い、原因を分析し、管理策に結び付けて有効性評価を行なう。

管理策の有効性測定と評価にかかる詳細手順は以下のとおり。

- ① 詳細管理策ごとのギャップ分析を行なう。
- ② 管理策グループごとのギャップ値を求め、対応度を数値化する。
Y=2、P=1、その他0ポイントとし管理策グループの詳細管理策ポイントを集計

して分子とし、(管理策グループの詳細管理策の数－N/Aの数) × 2 ポイントを分母として対応度合いとしての%を求める。

- ③ 情報資産グループと詳細管理策の対応マトリックスを作成する。
- ④ 対応マトリックスにより、詳細リスク分析表から詳細管理策グループごとの最大リスク値を求め、有効性評価値を算出する。
 - ア 管理策グループごとの最大リスク値算出 (Aとする)
 - イ リスク最大理論値を 27 (= 3 × 3 × 3) とする
 - ウ 管理策グループの有効性値 = (27 - A) / 27
- ⑤ 対応度と有効性評価値から管理策グループごとの値でレーダーチャートを作成し、同一グラフ上に記述する。
 - ア 対応度合いが高くて有効性が低い→新たな管理策および具体策を導入しなくてよいか?
 - イ 対応度合いが低い有効性は高い→他の情報資産にも当該管理策を適用できるか?
 - ウ 対応度、有効性ともに高い→対応度合いを下げても十分ではないか、過剰な対応になってないか?
 - エ 対応度、有効性ともに低い→対応度を上げられるか? 別の管理策導入が必要ではないか?

5. リスクマネジメントの目的

リスクマネジメントの目的は、リスクアセスメントで明確になったリスクを適切に管理し、ISMS を確立することである。事業上のリスクは、社会情勢の変化や情報技術の進捗等に応じて絶えず変化するものである。従って、採用したリスクの管理方法が適切であるかを定期的に見直すこととする。

6. リスクマネジメントの方法

リスクマネジメントでは、存在するリスクをそのリスクが持つ大きさや特徴により受容、低減、移転あるいは回避することを判断する。

(1) リスクの受容

当社では、リスクアセスメントの結果、リスク値が『 9 』未満のものについては、事業上影響がないと判断したため、存在するリスクを受容し、それ以外の管理策を講じない。

受容したリスクについては、残存リスクとして管理し、情報資産の価値、脅威、脆弱性等に変化が生じた際には、適時リスクの見直しを図る。

(2) リスクの低減

リスク低減とは、管理策を適用することによってリスクを減少させることである。

リスクアセスメントの結果、リスク値が『 9 』以上のものについては、可能な限りリスクを低減するよう努める。

リスクを低減する際、管理策を適用することによって業務に支障をきたさないよう、無理のない適切な管理策を選択する。

(3) リスク移転

リスク移転とは、アウトソーシングの利用によって業務を委託したり、保険等の利用によって債務を他者（他社）に移すことである。

管理策を適用できない場合、あるいは適用してもリスク値が組織が定めた許容範

囲内に低下しない場合、リスクを移転することを検討する。

脅威が表面化した場合、事業に与える影響は大きい、比較的发生する可能性が低いリスク（地震等の天災など）については、保険の利用を検討する。

（４）リスク回避

リスク回避とは、リスクの発生源となる業務や業務プロセスを停止あるいは全く別の方法に変更することによってリスクが発生する可能性を取り去ることである。

管理策を適用できない場合、適用してもリスク値が組織が定めた許容範囲内に低下しない場合、あるいはリスクを移転できない場合、リスクを回避することを検討する。

脅威が表面化した場合、事業に与える影響が大きいにもかかわらず、比較的发生する可能性が高いリスクについては、回避することを検討する。

7. 詳細リスク分析表に記載する項目

評価内容は、「詳細リスク分析表」（別表 3）のフォーマットに従って記載する。

項目名	説 明
項番	表示形式：n－n 先頭の数字は「情報資産洗出し要領__別表 1（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」 「－」の後ろの数字は洗出した「脅威」に付番する当該資産評価グループ内の一連番号
評価グループ名称	「情報資産洗出し要領__別表 1（資産評価グループ一覧表）」にて定義された「評価グループ名称」を転記
資産価値（C・I・A）	「情報資産洗出し要領__別表 1（資産評価グループ一覧表）」にて定義された評価グループの「C・I・A」と同じ。
脅威	評価グループに関する「脅威」を記述する。 洗出しにあたっては、別表 1「脅威・脆弱性一覧表（情報セキュリティ）」を参照。 どういう状況の時にどういうリスクが発現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」などできるだけ具体的に特定する。 ・「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？）」・・・起ころ得る状況を文章で記す。手段・方法なども含め具体的に記述する。
導入済み管理策	当該脅威について、その発現を抑止する、あるいは発現した場合に被害を低減するために、既に実施している対策を記す。
関連 C I A	当該脅威が、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ことも可（「C」、「CI」、「C・I・A」などと組み合わせて記す。）

脅威評価値	当該脅威の評価値。評価基準は、別表 2「分類基準表」を参照。
脆弱性	当該脅威に関する導入済み管理策の有効性を評価して、残存する脆弱性を明らかにする。 洗出しにあたっては、別表 1「脅威・脆弱性一覧表（情報セキュリティ）」を参照。 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。あるいは、管理システムが導入されていても、機能不足や、運用の抜け道が有ったりすれば脆弱性は残存するといった点に留意する。
脆弱性評価値	当該脆弱性の評価値。評価基準は、別表 2「分類基準表」を参照。
リスク値（C・I・A）	「資産価値（C・I・A）」に、当該脅威の「関連 C I A」についてそれぞれ「脅威評価値」「脆弱性評価値」を乗じた値。 当該脅威が関連しない C I A については、資産価値（C・I・A）のまま。
リスク対策	残存する脆弱性の排除、低減をはかる新たな対策や改善策を記す。 有効性が無い導入済み管理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、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して記録する。
予定リスク値（C・I・A）	リスク対策実施後の、脆弱性評価値の予定値を求め、リスク値を再計算する。
管理責任部署	資産評価グループを管理している責任部署。「情報資産洗出し要領_別表 1（資産評価グループ一覧表）」の「管理責任者」「管理部署」と同じ。

8. リスク対応計画の策定

リスクマネジメントの結果、情報リスクを管理するための経営陣の適切な活動、責任および優先順位、実施時期が明確にされたリスク対応計画を策定する。リスク対応計画は、必要な資金の拠出を考慮し、役割および責任を割り当てることも考慮する。

検討されたリスク対応策の導入や運用については経営陣の承認を持って実施する。経営陣は、リスクの重大さおよび対応策に係るコスト、技術的な適用可能性、法的な要求事項等を考慮した上でリスク対応の可否を判断し、承認した残留リスクを認識およびリスク対応に必要な資源などを割り当てなければならない。

9. 本文書の改訂

本文書は、以下のいずれかの条件で見直す。

- ・対象とする組織、資産、情報処理施設／設備などの変更
- ・重大なセキュリティ問題の発生
- ・セキュリティ上の新たな脅威の発生
- ・1年に1度