Vol.2021-SPT-41 No.46
2021/3/2

セキュリティ知識を必要としない リスクアセスメントツールの開発

中原 加寸美[1]　廣友 雅徳[1]　福田 洋治[2]　毛利 公美[3]　白石 善明[4]

概要：近年の調査でリスクアセスメントを行っていない事業所は過半数であることが報告されている．リスクアセスメントを行うには専門的な知識が必要であり，調査や分析に時間を要する．リスクアセスメントを実施していない理由として，十分な知識を持った人材がいない，実施方法がわからないといった理由が挙げられている．本稿では，リスクアセスメントを行う際に必要な専門知識を使わず，組織の情報資産や情報システムの管理情報を入力するだけでリスクアセスメントを行えるツールを開発する．さらに，そのリスクアセスメントツールを利用する例題を作成し，その例題を利用することでリスクアセスメントの実施方法がわからないという問題を解決することを試みる．

Development of the Risk Assessment Tool for System Administrators without Security Knowledge

Abstract: In a recent investigation, it is reported that most organizations do not carry out risk assessment. Security knowledge is necessary and needs time for an investigation, analysis to perform risk assessment. The reasons are “There are not human resources with enough knowledge”, “A method to investigate is not identified.” In this paper, we develop a tool which only inputs information of assets and the information system of the organization, and can carry out risk assessment without security knowledge. Furthermore, we make an example that uses the risk assessment tool, and try to solve the problem of how to carry out the risk assessment.

1. はじめに

近年，セキュリティ対策の需要が高まっている．対策を行うためには，リスクアセスメントを実施してどこから対策を行うのかを決定する必要がある．近年の厚生労働省の調査では，リスクアセスメントを実施していない事業所は過半数を占めることがわかっている．リスクアセスメントを実施していない理由（複数回答）を見ると，「十分な知識を持った人がいないため」が 27.4 %，「実施方法がわからないため」が 20.4 %と多くを占めている [1]．リスクアセスメントを実施するには専門知識が必要である．リスク分析を実施する際，専門知識がなくともできる手法は存在するが，その場合大まかな結果になり，信頼性は決して高いとは言えない．詳細で正確な分析を行うには専門知識は不可欠であるといえる．また，リスクアセスメントを実施する際に必要な調査や分析には時間を要する．

本稿では，セキュリティに関する専門知識を使わずともリスクアセスメントの実施ができるようにすることを目的とする．そのために，専門知識を使わず，組織の情報資産や情報システムの管理情報を入力するだけでリスクアセスメントを行えるツールを開発する．さらに，作成したリスクアセスメントツールを使用してリスクアセスメントを行える例題を作成することで，実施方法がわからないという問題の解決を試みる．

[1] 佐賀大学
Saga University
[2] 近畿大学
Kinki Uniersity
[3] 岐阜大学
Gifu Uniersity
[4] 神戸大学
Kobe Uniersity

2. リスクアセスメント

2.1 リスクアセスメントとは

リスクアセスメントとは，リスク分析からリスク評価までのすべてのプロセスのことを指す．図 1 に示すように，リスクマネジメントの第一段階であり，リスクアセスメン

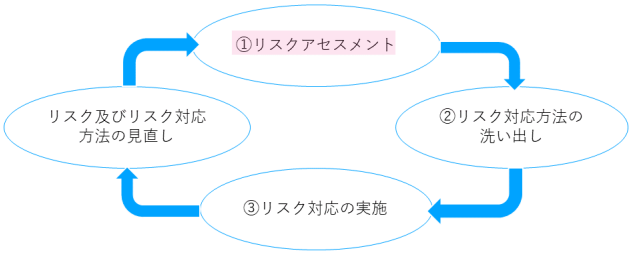

図 1　リスクマネジメントのプロセス

トを行うことで，組織やシステムに内在するリスクとその大きさや影響を知ることができる．そこから，効果的なセキュリティ対策を導くことを目的としている．さらに，結果に基づいたセキュリティ対策を施すことで，限られた予算を有効活用して最大限の効果が得られるというメリットがある．

2.1.1　リスク分析

リスク分析は，リスク因子を特定する，およびリスクを算定するプロセスである．手法や手順によって複数の分析手法が存在するが，デファクトスタンダード的な分析手法はない [2]．それぞれの手法にメリット，デメリットが存在するため，適宜，自組織にあった分析手法を使用する必要がある．

- ベースラインアプローチ
  既存の標準や基準をもとに対策基準を策定し，簡易的にリスク分析を行う手法．時間やコストが少なく特別なスキルは必要ないが，大まかな分析になる．また，選択する標準や基準によって結果が左右される．
- 非形式的アプローチ
  分析者の知識と経験によって分析を行う手法．分析者の能力が高ければ短時間で高品質な結果が得られるが，属人的な判断に偏る恐れがある．
- 詳細リスク分析
  情報資産，脅威，脆弱性の洗い出しと評価を行い，リスクの大きさを評価する分析手法．厳密なリスク評価を行えるが，実施には時間と労力がかかり，分析者に専門的なスキルが必要となる．
- 組合わせアプローチ
  複数のアプローチの併用．よく用いられるのは，ベースラインアプローチと詳細リスク分析の組合せである．両方のメリットを享受できるが，ベースラインアプローチ次第で組織や情報資産の重要度が誤認される可能性がある．

本研究では，詳細リスク分析を用いてツールの開発を行った．

2.1.2　リスク評価

リスクの重大さを決定するために，分析したリスクをリスク基準と比較するプロセスである．

- 定性的評価
  リスクの大きさを金額以外の大・中・小などのレベルや相対的な値などで表す評価手法．定量的評価の前段階として用いられることも多い．評価結果を算出するためのロジックがあれば，専門知識がなくとも比較的短時間で結果を得ることができる．
- 定量的評価
  リスクの大きさを金額で表す評価手法．セキュリティ対策費用を算出する上で有効な評価手法である．実際にどこまで信頼できる値が算出できるかは，評価者の技量に大きく依存する．

本研究では，定性的評価を用いてツールの開発を行った．

2.2　リスクアセスメントの難しさ

2.2.1　実施前の難しさ

リスクアセスメントの難点として最初に挙げられるのが，専門知識が必要という点である．リスクアセスメントを実施していない理由として挙げている事業所も多いように，専門知識がないとどうすればいいのかわからない場合が多い．また，実際にリスクアセスメントを実施しようとする場合には，代表的な分析手法は 4 つ存在するけれども，デファクトスタンダードはなく，適宜選んで使用することになる．したがって，リスク分析のどの手法を使えばいいのかわからないという点も難点として挙げられる．

2.2.2　実施段階の難しさ

リスクアセスメントの実施時の難点としては，まず，時間と費用がかかる点が挙げられる．詳細にリスク分析をしようとすればするほど，コストがかかる．また，リスク分析や評価を主観で行うこともあるため，個人によって結果にばらつきが大きくなる点である．これは，どの分析方法でも起こりうる．特に，分析者の知識や経験に依存する非形式的アプローチの場合は，ばらつきが大きくなる．ばらつきを抑えるため，また，様々な視点から分析できるようにするために複数人でチームを作ってリスクアセスメントを行うことが望ましい．しかし，チームで行う場合，リスクアセスメントに人員を割く必要があるので，通常業務を行う人員が減り，業務に差し支えることもある．

2.3　詳細リスク分析の手順

2.1.1 で説明した通り，詳細リスク分析は情報資産，脅威，脆弱性の洗い出しと評価を行い，リスクの大きさを評価する分析手法である．詳細リスク分析・評価の手順は以下の通りである．

Step1　リスク分析範囲の決定
リスク分析を行う対象とする範囲の決定をする工程である．想定される範囲としては，全社，事業部，情報システムなどが挙げられる．

Step2　対象とする情報資産の種別の決定
対象とする情報資産の種別を決定する工程である．分

析の目的，確保可能時間，人的リソースなどによって，電子化されたもののみが対象，紙媒体を含めたすべてのものが対象，のような情報資産の種別の範囲を明確にする．

Step3 情報資産の洗い出し
Step1，Step2 で決定した範囲に従って，情報資産を洗い出していく工程である．部門間で共有している情報資産については，どこまでが対象かを明確にする必要がある．明確にされていない場合は，協議の上，管理責任範囲を決定する．

Step4 情報資産の分類
Step3 で洗い出した情報資産を分類する工程である．これは，機密性や重要度に応じた対策を施し，適切に取り扱うことを目的としている．情報資産に求められる機密性・完全性・可用性の判断基準をもとに，重要度評価を行う．

Step5 脅威の洗い出し
Step3 で洗い出された情報資産に対して，何らかの影響を与え，損失の直接原因となる脅威を洗い出す工程である．誰が，何が，何を目的に，どこから，どのようにして，何をするのか，に注意して洗い出す．

Step6 脆弱性の洗い出し
リスク分析対象範囲に存在する脆弱性を洗い出す工程である．誰の，何の，どこが，何が，どうなっているのか，に注意して洗い出す．

Step7 リスクの洗い出し
Step6 までで洗い出された情報資産，脅威，脆弱性の関連から想定されるリスクを洗い出す工程である．各要素は 1 対 1 というわけではなく，複数の脆弱性とリスクが結び付くことによって，より大きなリスクになることもある．

Step8 リスクの大きさの評価
Step7 で洗い出されたリスクの顕在化の可能性や，損害を受ける情報資産の重要度などにより，各リスクの大きさを評価する工程である．評価方法は定性的評価，定量的評価の二つがある．

3. 関連研究

3.1 リスク分析シート

リスク分析シート [3] は，詳細リスク分析を実施することを目的とした Excel ファイルである．リスク分析シートには 7 つのシートがあり，利用方法，台帳記入例，重要度定義，情報資産管理台帳，脅威の状況，対策状況チェック，診断結果である．それぞれのシートは以下の通りである．

- 利用方法
  リスク分析シートの構成，各シートの利用方法を記載している．各シートの利用方法については，情報資産の洗い出し，リスク値の算定，情報セキュリティ対策の決定の 3 つについて説明している．
- 台帳記入例
  情報資産管理台帳の記入例．
- 重要度定義
  情報資産管理台帳に記入する評価値の定義．重要度は機密性・完全性・可用性の評価値の最大値となる旨が記載されている．
- 情報資産管理台帳
  事業所の所有する情報資産を記入するためのシート．業務分類，情報資産名称，備考，利用者範囲，管理部署，媒体・保存先，個人情報の種類，重要度，保存期間，登録日の記入をする．
- 脅威の状況
  媒体・保存先ごとに想定される典型的な脅威について 3 段階で評価する．
- 対策状況チェック
  情報セキュリティ対策の種類とそれに対応する情報セキュリティ診断項目を 4 段階で評価する．
- 診断結果
  情報資産の状況，対策の種類ごとの実施率，対策検討・実施の要否を表示するシート．不足する対策を検討・実施する旨を赤字で表示する．

このシートでできることは．管理台帳による情報資産の管理，各媒体・保存先ごとに考えられる典型的な脅威の発生度の確認，情報セキュリティ対策の種類ごとの診断項目の実施状況の確認，対策の実施率の確認，どのような資産がいくつあるかの確認が挙げられる．しかし，分野特有の脅威のような典型的な脅威以外の脅威については確認することができない．また，リスクの可視化ができず，どのようなリスクが存在しているのかは見ることができない．さらに，リスク値は 3 段階となっており，実際にはどの情報資産の何というリスクが高いのかは見ることができない．

3.2 リスク分析・評価ファイル

リスク分析・評価ファイル [4] は，リスク分析とリスク評価を行うことを目的とした Excel ファイルである．リスク分析・評価ファイルには，様式 1 から様式 9 まで用意されている．それぞれの様式は以下の通りである．

様式 1 リスク分析・評価項目表
様式 2，様式 8 に反映する項目や値が，あらかじめ入力されたもの．各団体の事情に応じて項目や値を変更する際に使用する．

様式 2 基本リスク分析・評価シート
基本リスク分析・評価を行う際に使用する．

様式 3 基本リスク分析・評価に関する改善計画表
基本リスク分析・評価終了後，改善計画を策定する際に使用する．

様式 4 対象範囲表

詳細リスク分析・評価を行う際に，情報資産を洗い出す業務，組織範囲の決定に使用する．

様式 5　情報資産洗い出し対象設定表
情報資産の管理者が，実際に洗い出しを行う実施範囲を明確にするために使用する．

様式 6　情報資産台帳
詳細リスク分析・評価を行う際の情報資産台帳の作成に使用する．

様式 7　脅威評価レベル表
様式 8 で脅威の特定の設定等に反映する項目や値が，あらかじめ入力されたもの．各団体の事情に応じて，項目や値を変更する際に使用する．

様式 8　詳細リスク分析・評価シート
詳細リスク分析・評価を行う際に使用する．

様式 9　詳細リスク分析・評価に関する改善計画表
詳細リスク分析・評価終了後に，改善計画を策定する際に使用する．

リスク分析・評価ファイルは，基本リスク分析・評価用，情報システム管理者用，情報セキュリティ管理者用の 3 つに分かれており，それぞれの行うべき作業によって 1 から 9 の様式が組み合わせられている．そのため，それぞれが何を行えばいいのかが明確になっていてわかりやすい．また，様式 1 と様式 7 にはあらかじめ値が入力してあり，入力例になる．しかし，すべての様式についてマニュアルに使用方法が詳しく書いてあるわけではないので，使用方法がわかりにくい．

4. リスクアセスメントツールの開発

4.1 ツールの概要

本ツールは，Microsoft 社の Excel を用いて開発した．処理の自動化は，ExcelVBA を使用してマクロを作成することにより実装した．本ツールで使用している分析手法は詳細リスク分析であり，評価手法は定性的評価である．オフラインで使用できるので，インターネット接続の必要がなく，外部に情報が洩れるといった心配もない．

4.2 各シートの概要

作成したシートは，情報資産，情報資産（個人情報），情報資産（情報システム），分類，脅威，脆弱性，リスク，評価の計 8 枚である．各シートについて説明する．

(1) 情報資産
組織の所有する情報資産を入力するシート (図 2)．シートには名称，種類，主な項目，利用者，管理者，記録媒体，保管方法，廃棄場所を入力する．

(2) 情報資産（個人情報）
組織の所有する個人情報の情報を入力するシート (図 3)．シートには利用目的，利用目的の通知方法，本人の属性，取得方法，取得手段，利用範囲，件数を入力する．

名称		研究データ(ファイル名，帳票名など)
種類		PC内データ
主な項目		卒業研究，修士研究
利用者		研究室所属学生
管理者		研究室所属学生
記録媒体		ハードディスク（紙，ハードディスク，CD，DVDなど）
保管方法	場所	研究室内PC
	期間	1年～3年
廃棄方法		PCの初期化
備考		

図 2　[情報資産] シート

種類	個人情報
利用目的	
利用目的の通知方法	
本人の属性	（社員，顧客など）
取得方法	（本人から直接取得した情報，業務の受託によって取得した情報など）
取得手段	（電話，FAX，電子メール，Web，郵送，手渡しなど）
利用範囲	（社内利用，委託先にて利用，第三者に提供など）
件数	
備考	

図 3　[情報資産（個人情報）] シート

名称	
種類	情報システム
利用者	（社員のみ，特定会員のみ，不特定多数の社外利用者など）
管理者	
設置場所	（データセンタ，サーバ室など）
主な用途	
システム構成	（オンプレミス，パブリッククラウドなど）
取り扱っている情報	
利用形態	（インターネットからの利用，リモートアクセスによる利用など）
アクセス制御/認証の実施方法	
バックアップの実施方法	
ログの取得状況/保存期間	
求められるサービスレベル	（許容されるサービス停止時間など）
備考	

図 4　[情報資産（情報システム）] シート

(3) 情報資産（情報システム）
組織の使用する情報システムの情報を入力するシート (図 4)．シートには名称，利用者，管理者，設置場所，主な用途，システム構成，取り扱っている情報，利用形態，アクセス制限/認証の実施方法，バックアップの実施方法，ログの取得状況/保存期間，求められるサービスレベルを入力する．

(4) 分類
情報資産価値の評価を行うためのシート (図 5)．機密性・完全性・可用性が失われた場合に，事業にどの程度影響があるかを段階的に評価する．評価基準は，機密性に一つ，完全性と可用性に二つずつ設けている．図 6 のように，機密性については，公開範囲による判断基準を設けている．完全性については，改ざん・重複・欠落などによる影響と，どのような媒体に情報が保存されているかについての判断基準を設けている．可用性については，停止許容時間と，その情報資産を

情報資産	重要度評価				
	機密性	完全性①	完全性②	可用性①	可用性②
例：学生用研究室PC	2	3	2	3	3
例:ルータ	2	1	1	3	2

図 5 [分類] シート

レベル	判断基準	管理上の分類	重要度分類
1	公開している情報資産	非機密情報	一般公開
2	権限のないものからアクセスを受けることにより，自社の業務に軽微な影響を及ぼす情報資産	機密情報	社外秘
3	権限のないものからアクセスを受けることにより，自社の業務や社員のプライバシーなどに重大な影響を及ぼす情報資産		部外秘
4	権限のないものからアクセスを受けることにより，自社の業務や社員のプライバシーなどに重大な影響を及ぼしたり，契約違反となる情報資産		極秘

図 6 機密性の判断基準

誰が/何が	コンピュータウイルス
何を目的に	嫌がらせ，盗聴
どこから	インターネット
どのようにして	誤って，正規ユーザに成りすます
何をするのか	感染・発病する

図 7 [脅威] シート

	着眼点
誰が/何が	外部からの侵入者，一般社員，協力会社社員，システム管理者，コンピュータウイルス，不正なモバイルコード，災害，故障
何を目的に	金銭，嫌がらせ，自己顕示，興味本位
どこから	インターネット，社内LAN，無線LAN
どのようにして	ローカル端末の操作，正規ユーザになりすます，誤って，無意識のうちに，突発的に
何をするのか	不正なログインを試みる，物理的に侵入を試みる，パケットを盗聴する，パケットを大量に送り付ける，不正なコマンドを発行する，クライアントパソコンに侵入する，感染・発病する

図 8 脅威の語群

誰の/何の	不足事態発生時の
どこが/何が	方針・手順
どうなっているのか	決められていない

図 9 [脆弱性] シート

利用できなくなることによる影響についての判断基準を設けている．

(5) 脅威

考えられる脅威を入力するシート (図 7)．図 8 に示した着眼点という語群から選ぶ，または，語群になくとも想像されうる脅威を，誰が/何が，何を目的に，どこから，どのようにして，何をするのかという項目に入力する．入力されない項目があっても構わない．

(6) 脆弱性

考えられる脆弱性を入力するシート (図 9)．図 10 に示した着眼点という語群から選ぶ，または，語群になくとも想像されうる脆弱性を，誰の/何の，どこが/何が，どうなっているのかという項目に入力する．入力されない項目があっても構わない．

(7) リスク

組織の情報資産に生じるリスクについて入力するシート (図 11)．洗い出した脅威と脆弱性が結び付いて生じるリスクを洗い出し，入力する．1 つの脅威が 1 つの脆弱性と結びつくとは限らない．1 つの脅威と複数の脆弱性が結び付くことによって，より大きなリスクとなる．

	着眼点
誰の/何の	一般ユーザの、システム管理者の、サーバの、ソフトウェアの、ネットワークの、設備の、組織の、不測事態発生時の
どこが/何が	意識、設定、体制、方針、手順、教育、バージョン、保守
どうなっているのか	低い、古い、決められていない、守られていない、形骸化している、機能していない、実施していない、確認していない、放置されている

図 10 脆弱性の語群

情報資産	脅威	脆弱性	想定されるリスク
例：学生用研究室PC	コンピュータウイルスの侵入	発生時の対策手順が定められていない	情報漏洩・データの破壊
例：学生用研究室PC	盗難	研究室の施錠忘れ	PCの物理的盗難
例：学生用研究室PC	災害（火災）	消火設備が用意されていない	焼失

図 11 [リスク] シート

情報資産			脅威		脆弱性	リスク強度		
名称	レベル		内容	レベル	レベル	機密性	完全性	可用性
例：学生用デスクトップPC	機密性	2	災害（水害）	1	1		3	1
			災害（火災）	1	2		6	2
			災害（地震）	1	2		6	2
			災害（停電）	1	1		3	1
	完全性	3	故障・システム障害	2	3		18	6
			盗難	3	2	12	18	6
			第三者による侵入・改ざん	3	2	12	18	
			内部要員による侵入・改ざん	2	1		6	
	可用性	1	不正操作	3	2	12	18	6
			ウイルス感染	2	3		18	6
			作業ミス	1	1		3	1

図 12 [評価] シート

(8) 評価

組織の各情報資産に対して，機密性・完全性・可用性についてのリスクの大きさを定性的評価を用いて値をつけるシート (図 12)．情報資産のレベルは，[分類] シートから引用する．脅威のレベルは，あらかじめ定めたデフォルト値を入力する．脆弱性のレベルは，リスクの項目に該当する脆弱性がないならば 1，1 つならば 2，2 つならば 3，それ以上ならば 4 といったように値を定めている．

4.3 処理の自動化

ExcelVBA を使ったプログラミングを行い，マクロを作成して処理の自動化を行った．自動化した部分の処理内容は以下の通りである．

Step1 情報資産を分類する

手動入力された組織の情報資産の名称をシートの情報資産に自動入力する．[情報資産] シートでそれぞれの情報資産に入力された種類を使用して，それぞれに設定されたデフォルト値を機密性・完全性・可用性の計 5 種類の判断基準に自動入力する．完全性・可用性は判断基準を 2 つ用意しているので，2 つのうち大きいほうの値を採用する表も用意する．

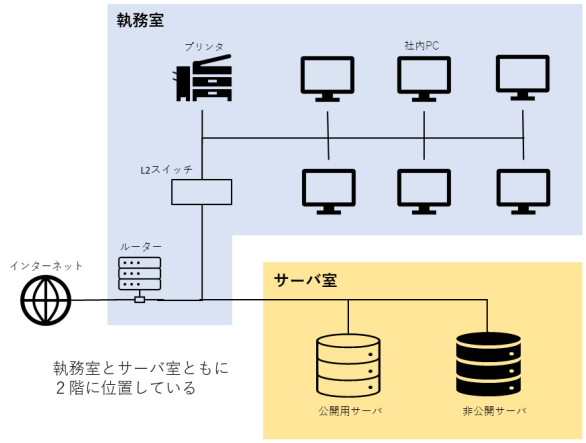

図 13　ネットワーク図

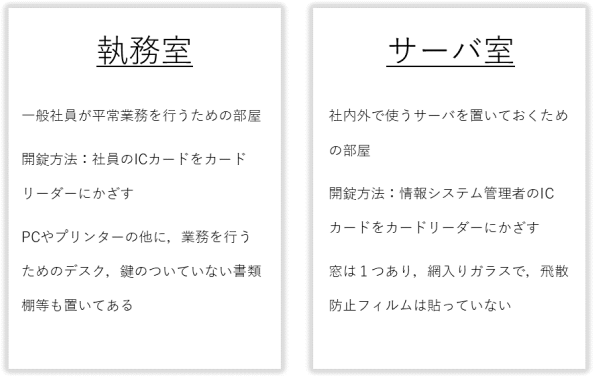

図 14　部屋の説明

Step2　リスクを自動入力する

手動入力された情報資産の種類，脅威，脆弱性とあらかじめ用意しているリスクのテンプレートを照らし合わせ，一致したものをシートに自動入力する．

Step3　リスク評価をする

情報資産のレベルは，分類から引用して自動入力する．脅威のレベルは，デフォルト値を自動入力する．脆弱性のレベルは，Step2 でリスクに入力された情報資産名・脆弱性名を検索し，一致した件数によって値を自動入力する．

本ツールを用いるときの流れとそれぞれの図との対応は次のようになる．図 2，3，4 に保有する情報資産の情報を手動入力する．Step1 の処理を行い，図 5 に自動入力される．図 7，9 に，存在する脅威・脆弱性を手動入力する．Step2 の処理を行い，図 11 に自動入力される．Step3 の処理を行い，図 12 に自動入力される．

5.　リスクアセスメントの例題の作成

リスクアセスメントツールのみでは，どのようにリスクアセスメントを行うのか，また，ツールを使うのかが不明確である．そこで，作成したツールを使用してリスクアセスメントの練習を行うための例題を作成した．例題は仮想の組織を想定しており，この組織についてリスクアセスメントを実施する．作成した例題には，以下の項目を記載した．

5.1　例題

- ネットワーク図
  仮想の組織のネットワーク図を図 14 に示した．それぞれの情報資産がどのようにつながっているのかを知ることで，脅威や脆弱性の洗い出しの手助けになる．
- 部屋の説明
  図 15 にネットワーク図に記載のある部屋の細かい情報を記載した．どのような目的の部屋か，部屋の開錠方法，部屋の中には何がありどのような状況なのかを記載した．

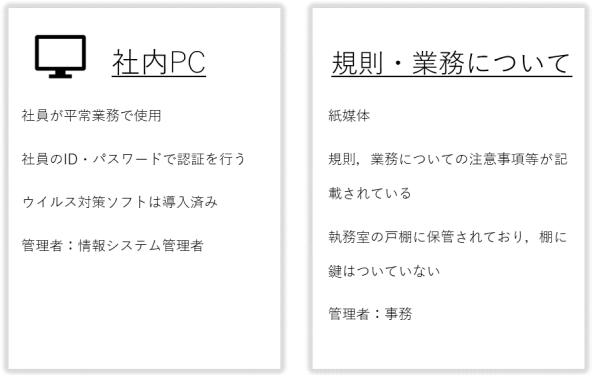

図 15　情報資産の説明

- 情報資産の説明
  図 16 のように，ネットワーク図に記載のある情報資産の説明を記載した．該当の情報資産がどのような目的で使用されるか，管理者は誰か，その資産はどのような状況なのかを記載した．
- 情報資産の廃棄について
  図 17 のように，各情報資産の廃棄について記載した．どの資産をどのように廃棄するかを分類し，廃棄の手順を記載した．
- 周辺環境について
  図 18 のように，会社の周辺環境・設備について記載した．主に，自然災害時にどのような状況になるかに留意して作成した．
- 不測事態発生時について
  図 19 のように，不測事態発生時の対応について記載し

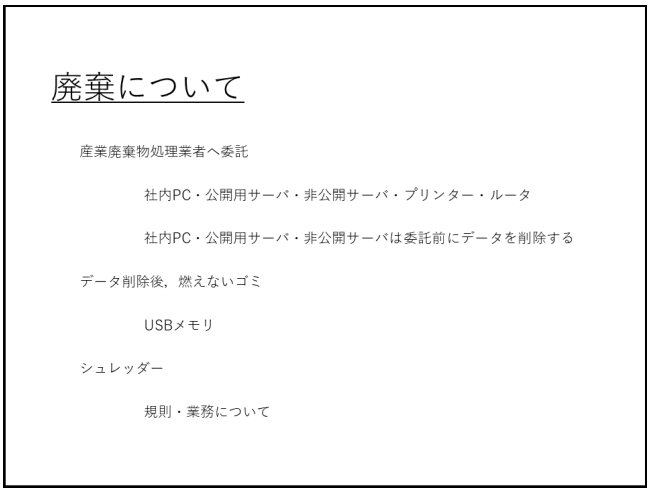

図 16 廃棄について

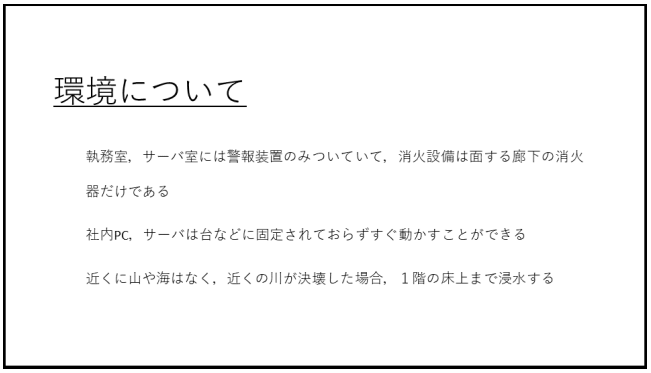

図 17 環境について

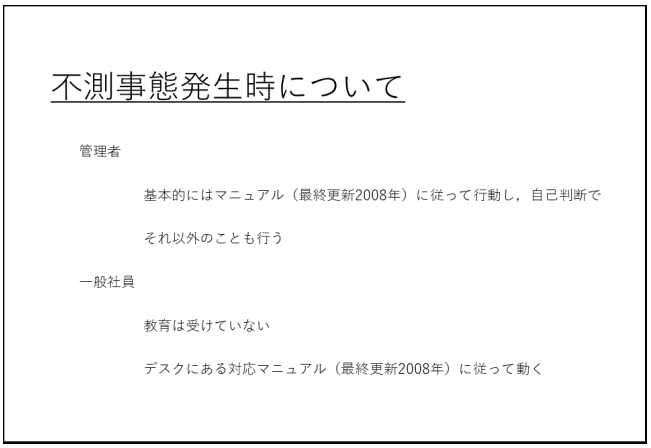

図 18 不測事態発生時について

た．管理者と一般社員についてそれぞれどのような状況なのか，また，マニュアルについても記載している．

5.2 例題の解答

ツールを使用して例題を行うだけでは，正しくリスクアセスメントを行えたかわからないので，例題の解答を用意した．しかし，あくまでも例題の目的はツールの使い方の理解であり，解答はリスクアセスメントの一例である．したがって，必ずしも同じ評価結果にならなければならないわけではない．解答は，例題で使用した仮想の組織に対して，手動でリスクアセスメントをしたものを用意している．手動で評価する理由として，手動で評価を行う方が正確に評価できることが挙げられる．また，リスクの洗い出しも正確に行えることも理由として挙げられる．

6. まとめ

本稿では，セキュリティに関する専門知識がなくてもリスクアセスメントができることを目的として，リスクアセスメントツールの開発を行った．また，開発したリスクアセスメントツールを使用する例題の作成を行った．この例題を使用することで，リスクアセスメントツールの使用方法を理解することができる．さらに，専門知識がなくともリスクアセスメントを実施することができる．本ツールでは，リスクの洗い出しにテンプレートを用いているが，テンプレートを増やしていく，あるいは，入力された情報資産の種類，脅威，脆弱性からどのようなリスクが発生するのかを自動で判断できるようになると，漏れなくリスクを洗い出すことが可能になる．

参考文献

[1] 厚生労働省，平成 29 年　労働安全衛生調査（実態調査）の概況，p.4，Aug.28，2018.
[2] 情報セキュリティマネジメントと PDCA サイクル，https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html，（参照 2021-01-14）
[3] 中小企業の情報セキュリティ対策ガイドライン 付録７，https://www.ipa.go.jp/security/keihatsu/sme/guideline/（参照 2021-01-18）
[4] 総務省，リスク分析・評価ファイル，https://www.soumu.go.jp/denshijiti/02gyosei07_03000041.html，（参照 2020-01-27）