Title	中小企業のランサムウェア対策としてのバックアップに関するアドバイスツールの提案
Sub Title	Proposal of a backup advice tool for ransomware mitigation for small and medium-sized enterprises
Author	本郷, 寛(Hongo, Hiroshi) 砂原, 秀樹(Sunahara, Hideki)
Publisher	慶應義塾大学大学院メディアデザイン研究科
Publication year	2024
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2024年度メディアデザイン学 第1162号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40001001-00002024-1162

修士論文 2024 年度

中小企業のランサムウェア対策としての
バックアップに関するアドバイスツールの提案

慶應義塾大学
大学院メディアデザイン研究科

本郷　寛

本論文は慶應義塾大学大学院メディアデザイン研究科に
修士 (メディアデザイン学) 授与の要件として提出した修士論文である。

本郷　寛

研究指導コミッティ：
砂原 秀樹 教授　(主指導教員)
杉浦 一徳 教授　(副指導教員)

論文審査委員会：
砂原 秀樹 教授　(主査)
杉浦 一徳 教授　(副査)
南澤 孝太 教授　(副査)

修士論文 2024 年度

中小企業のランサムウェア対策としての バックアップに関するアドバイスツールの提案

カテゴリ：デザイン

論文要旨

近年ランサムウェアによる被害が継続的に発生しており、被害組織の多くは中小企業となっている。ランサムウェアの被害組織の多くでバックアップは取得されていたが、バックアップも暗号化されてしまったことなどが原因となり、多くの組織でバックアップからデータの復号に失敗している。中小企業がランサムウェア被害にあった場合でもバックアップからデータの復元を可能とするために、ランサムウェア対策について紹介している資料などを参照して、ランサムウェア対策として効果的なバックアップの要件を整理した。次いで、中小企業に聞き取り調査を行い、バックアップは取得しているものの、要件を満たしたバックアップ体制にはなっていないことが明らかとなった。また、要件のチェックリスト作成し、バックアップの体制が要件を満たしたものになっているか確認してもらう調査を実施したところ、具体的な対策例を認識できた場合に、既存のバックアップ体制の改善を検討されようとしていた。そこで本研究では、中小企業において要件を満たしたバックアップの取得が可能となることを支援するために、バックアップ対象のデータや要件の実施状況に関する情報から、バックアップ体制を評価するとともに、要件を満たしていない場合に具体的な対策例を提示するアドバイスツールを作成した。仮想の中小企業のバックアップ体制に対してアドバイスツールを使用したところ、バックアップ体制が要件を満たしているか評価することや、満たしていない場合に具体的な対策例を提示することが可能であることを確認した。

キーワード：

中小企業, セキュリティ, ランサムウェア, バックアップ, IT

慶應義塾大学大学院メディアデザイン研究科

本郷　寛

Abstract of Master's Thesis of Academic Year 2024

Proposal of a Backup Advice Tool for Ransomware Mitigation for Small and Medium-Sized Enterprises

Category: Design

Summary

In recent years, ransomware attacks have been occurring continuously, and many of the victim organizations are small and medium-sized enterprises(SMEs). Although backups were acquired in many of the organizations that were victimized by ransomware, many organizations failed to decrypt data from backups due to the fact that the backups were also encrypted. In order to enable SMEs to restore data from backups even when they are victimized by ransomware, we organized the requirements for effective backups as a countermeasure against ransomware, referring to materials that introduce ransomware countermeasures. Next, we conducted an interview survey of SMEs, and it became clear that although backups were acquired, the backup system did not meet the requirements. In addition, we created a checklist of requirements and conducted a survey to have them confirm whether their backup system met the requirements. When specific countermeasures were recognized, they were about to consider improving their existing backup system. Therefore, in this study, in order to support SMEs in acquiring backups that meet the requirements, we created an advice tool that evaluates the backup system from information on the data to be backed up and the implementation status of the requirements, and presents specific countermeasures if the requirements are not met. When we used the advice tool on the backup system of a hypothetical SMEs, we confirmed that it is possible to evaluate whether the backup system meets the requirements and present specific countermeasures if it does not.

Keywords:

small and medium-sized enterprises, security, ransomware, backup, IT

Keio University Graduate School of Media Design

Hiroshi Hongo

目　　次

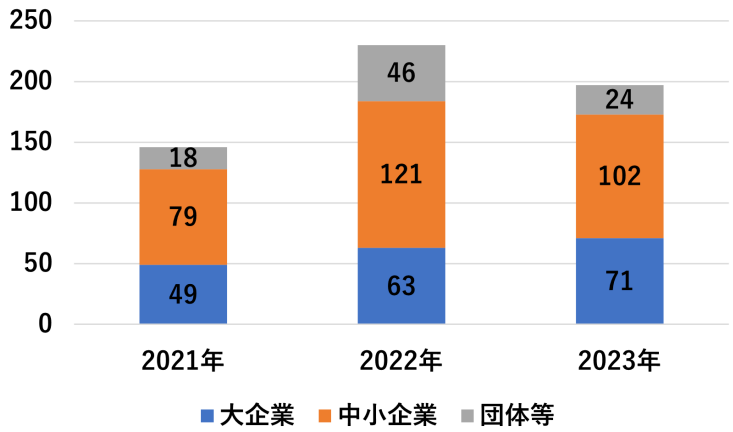
図　目　次

表　目　次

第 1 章
導　　入

1.1. 研究背景

近年、中小企業においても、業務の効率化やビジネスチャンスの拡大等のためにIT利用が進んでいる。その一方で、サイバー攻撃による被害は継続的に発生しており、企業が業務を継続するうえでの脅威となっている。独立行政法人情報処理推進機構（IPA）が公表している「情報セキュリティ10大脅威」[1]によると、2021年以降ランサムウェアによる被害が組織向け脅威の1位となっており、サイバー攻撃の中でもランサムウェアが近年における最大の脅威となっていると言える。ランサムウェアとは、情報機器や利用者に被害を与える悪意のあるソフトウェアであるマルウェアの一種である。攻撃者はパソコンやサーバをランサムウェアに感染させ、パソコンやサーバに保存されているデータを暗号化し、暗号化の解除を条件に金銭の要求などを行う他、金銭が支払われない場合に窃取した情報を公表するといった脅迫を行う。ランサムウェアによる被害を受けると、データが暗号され業務が停止したことによる金銭的被害に加えて、取引先などからの信用失墜といった被害を受けることになる。ランサムウェアの被害に遭う可能性があるのは大企業だけではなく、中小企業もランサムウェアの被害に遭う可能性がある。警察庁の資料によると、図1.1のとおりランサムウェアの被害にあった組織のうち、半数以上が中小企業となっている。そのため、中小企業においても対策を実施することが重要である。



(警察庁 サイバー空間をめぐる脅威の情報等 [2] より筆者作成)

図 1.1 ランサムウェア被害件数

ランサムウェア対策は多数あるが、大きく分けると「感染を防止する対策」と「被害を最小限に抑える対策」の 2 つのタイプに分類することができる。感染を防止する対策として、OS のアップデートやセキュリティ対策ソフトの導入などが考えられる。しかし、近年サイバー攻撃は高度化していることもあり、感染を防止する対策を実施した場合でも攻撃を完全に防ぐことは困難となっている。もう片方のタイプである被害を最小限に抑える対策として、バックアップの取得がある。バックアップからデータを復元することで業務の継続を可能にし、被害を小さくすることが可能となる。ランサムウェア対策を実施する上で、感染を防止する対策と被害を最小限に抑える対策の両方を実施することで、被害にあうリスクを低減するとともに、仮に被害にあってしまった場合でも、被害を小さくすることが重要である。

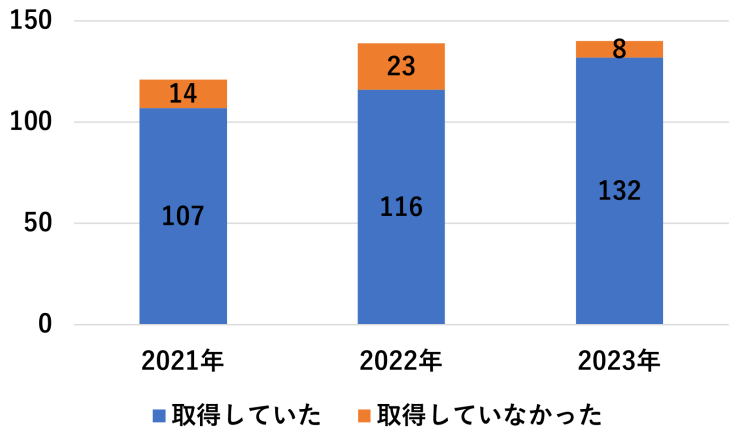
1.2. 研究目的

バックアップとは、情報機器に保存されたデータを別の記録媒体にコピーして保存することである。バックアップは、ランサムウェア対策としてだけではなく、人的ミスや機器の故障などによるデータの損失への対策や自然災害時などの BCP

対策などとしても実施されている。

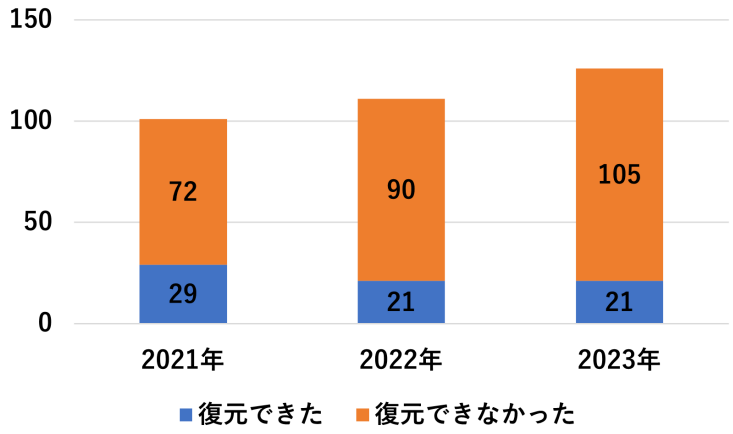
しかし、バックアップの取得はランサムウェアの被害にあった多くの組織でも実施されていた（図 1.2）ものの、バックアップからの復元に失敗するケースが多くなっている（図 1.3）。バックアップも暗号化されてしまったことが、バックアップから復元できなかった主な理由となっている（図 1.4）。ランサムウェア対策としてバックアップを効果的なものにするためには、次章で詳しく述べる要件を踏まえてバックアップを取得することに留意する必要がある。

そこで本研究では、中小企業がランサムウェアの被害にあった場合にデータを復元することが可能となるように、ランサムウェア対策として効果的なバックアップの要件を満たしたバックアップの取得が可能となるような支援方法を提案することを目的とする。



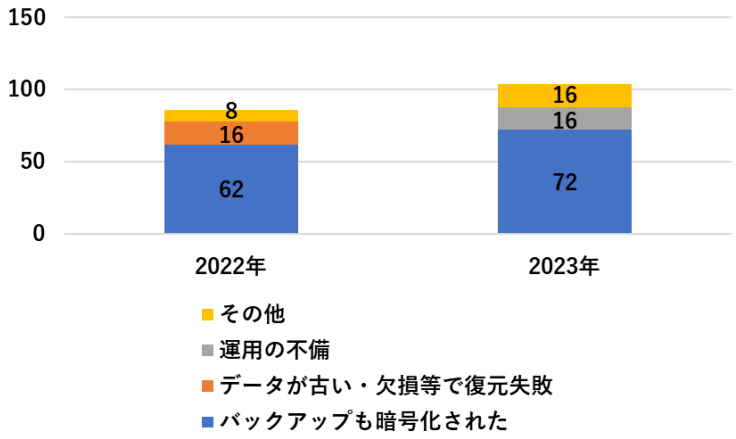
(警察庁 サイバー空間をめぐる脅威の情報等 [2] より筆者作成)

図 1.2 被害組織におけるバックアップの取得有無



(警察庁 サイバー空間をめぐる脅威の情報等 [2] より筆者作成)

図 1.3 被害組織におけるバックアップからの復元結果



(警察庁 サイバー空間をめぐる脅威の情報等 [2] より筆者作成)

図 1.4 被害組織におけるバックアップからの復元できなかった理由

1.3. 中小企業の定義

本研究における中小企業の定義は、中小企業庁 [3] が定めている中小企業の定義に則るものとする。中小企業が定めている中小企業の定義は、表 1.1 のとおりである。

表 1.1 中小企業庁が定めている中小企業の定義

業種分類	中小企業基本法の定義
製造業その他	資本金の額又は出資の総額が 3 億円以下の会社又は
	常時使用する従業員の数が 300 人以下の会社及び個人
卸売業	資本金の額又は出資の総額が 1 億円以下の会社又は
	常時使用する従業員の数が 100 人以下の会社及び個人
小売業	資本金の額又は出資の総額が 5 千万円以下の会社又は
	常時使用する従業員の数が 50 人以下の会社及び個人
サービス業	資本金の額又は出資の総額が 5 千万円以下の会社又は
	常時使用する従業員の数が 100 人以下の会社及び個人

(中小企業庁 中小企業・小規模起業者の定義 [3] より筆者作成)

第 2 章
関 連 事 例

2.1. 中小企業における IT 利用およびセキュリティ対策の実態

2.1.1 2021 年度中小企業における情報セキュリティ対策に関する実態調査

IPA が中小企業における情報セキュリティ対策の実態などを把握するために、2021 年 10 月～12 月にかけて、中小企業を対象としたウェブによるアンケート調査を実施している。当該調査の報告書 [4] に、以下のように示されている。

- 約 9 割の企業が業務用パソコンなどの IT を導入しており、Web サイト、ホームページの開設や電子メール、会計システム・アプリケーションなどの利用が多くなっている。
- 直近過去 3 期の情報セキュリティ対策投資額について、投資していない企業が 3 割強あり、100 万円未満、単純計算で 1 か月あたり 3 万円未満（100 万円/ 3 期/12 か月）の企業が 4 割弱となっていた。
- 情報セキュリティ対策投資を行わなかった理由として、約 4 割が必要性を感じていないと回答しており、費用対効果が見えない、コストがかかり過ぎる、どこからどう始めたらよいかわからないと回答した企業が 2 割程度となっていた。

- パソコンへのセキュリティパッチの適用状況について、常に適用し、適用状況を把握している企業は半数以下であった。
- 被害防止のための組織面・運用面の対策として、重要なシステム・データのバックアップが 4 割弱で最も実施されていた。
- 情報セキュリティ関連製品やサービスの導入状況について、ウイルス対策ソフト・サービスが 8 割弱の企業で導入されており、次いでファイアウォールが 3 割強、VPN が 2 割弱と続いていた。なお、情報セキュリティ関連製品やサービスは従業員規模が大きくなるにつれて導入割合が高くなっている。
- 情報セキュリティ対策の必要性を感じないと回答した企業が 2 割程あり、そのうち 7 割弱が重要情報を保有していないため、3 割弱が情報セキュリティ被害にあうとは思わないためを理由として回答していた。

2.1.2 中小企業に求められるサイバーセキュリティ対策の強化

日本政策金融公庫総合研究所が、2021 年 4 月に情報機器を利用している中小企業を対象にインターネットアンケート調査を実施し、中小企業におけるサイバーセキュリティ対策の現状を調査している。当該調査のレポート [5] に、以下のように示されている。

- 文書の保存方法として、個々の情報機器に保存している企業が約 75 %と最も多くなっていた。
- 個々の情報機器に保存している書類として、経費や資金に関する書類や受発注に関する書類、顧客に関する書類が多くなっていた。
- パソコンの OS アップデート状況について、すべてアップデートしている企業は 7 割弱となっていた。
- パソコンへのセキュリティソフトのインストール状況について、すべてにインストールしている企業は 7 割強であった。

- 情報機器に保存した書類のバックアップをとってある企業は 8 割弱であった。
- バックアップの保存先として USB メモリや CD、DVD が 4 割強と最も多くなっており、次いで外付けの HDD や SSD が 4 割弱となっていた。また、複数個所にバックアップを作成している企業は、バックアップを作成している企業のうち 3 割弱であった。
- 情報セキュリティ対策を進めるうえでの障害について、資金が足りていないことや経営者の知識が足りないことが多く回答されていた一方で、特にないと回答した企業が 5 割強を占めていた。

2.2. 中小企業のセキュリティ対策実施に向けた支援

2.2.1 IPA SECURITY ACTION

中小企業のセキュリティ対策の実施を支援するための取組みとして、IPA が実施している「SECURITY ACTION」がある。「「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度」[6] となっている。取組み目標が 2 段階に分けられており、IPA が公表している「情報セキュリティ5 か条」に取り組むことを宣言する「一つ星」と、「5 分でできる！情報セキュリティ自社診断」の実施と情報セキュリティ基本方針の策定と外部への公開を行う「二つ星」がある。この SECURITY ACTION を宣言することが、補助金申請の要件になっていることがある [7]。ただし、この取組みはあくまで中小企業がセキュリティ対策に取り組むことを自己宣言する制度であり、セキュリティ対策の実施状況を反映するものとはなっていない。

2.2.2 東京都 中小企業サイバーセキュリティ支援事業

東京都が行っている取組みとして、中小企業サイバーセキュリティ支援事業 [8] がある。この支援事業にはいくつか種類があり、「セキュリティ対策の第一歩とし

て機器・ソフトウェアの活用や専門家による情報セキュリティポリシー策定等の支援」[9] や「社内にてサイバーセキュリティ対策の中核を担う人材の育成支援に向けたセミナー・ワークショップや課題解決を実践的にサポートする専門家派遣を実施」[10] するものなど行われる。ランサムウェア対策の 2 つのタイプで言うと、バックアップの取得が含まれる被害を最小限に抑える対策よりも、感染を防止する対策を支援する内容となっている。なお、この取組みの対象となるのは東京都内に主たる事業所を有する中小企業であり、また参加できる企業数にも限りがある。

2.2.3 IPA 5 分でできる！情報セキュリティ自社診断

IPA は、中小企業が自社のセキュリティ対策状況をチェックるためのツールとして、「5 分でできる！情報セキュリティ自社診断」を公開している [11]。このツールでは、25 個の診断項目の対策実施状況を選択することにより点数が付与され、すべての項目の合計点数に応じて対策実施状況が評価される。しかし、各診断項目に対して一般的な対策例は示されているものの、提示された対策例をどのように実施するかは、中小企業が各自で具体的な対策を検討する必要がある。

2.2.4 サイバーセキュリティ基本態勢診断

サイバー保険を提供している保険会社が、セキュリティベンダーと共同開発した診断ツールをウェブサイトに公開している [12]。このツールでは、25 個の質問項目の実施状況を回答することにより対策実施状況が点数化されるが、点数に応じた対策実施状況の評価が行われることにとどまっている。

2.3. バックアップにおける留意事項

2.3.1 ３－２－１ルール

アメリカ合衆国国土安全保障省の外局機関である CISA（サイバーセキュリティー・インフラセキュリティー庁）のセキュリティ組織である US-CERT が、2012 年にすべてのコンピュータユーザに対して、重要なデータを損失や破損から保護することを目的として、「３－２－１ルール」の遵守を提唱している [13]。３－２－１ルールの「３」は、データは１つのプライマリデータと２つのバックアップデータの計３つのデータを作成することを意味している。複数のバックアップを取得しておくことで、データが消失するリスクを低減することが可能になる。「２」は、様々な脅威から保護するために２つの異なる記録媒体に保存することを意味している。データを異なる記録媒体に分散して保存することで、１つの記録媒体が故障したとしても、他の記録媒体からデータを復元することが可能となる。「１」は、コピーのうち１つは自宅や職場以外のオフサイトに保管することを意味している。バックアップデータが保存された記録媒体をプライマリデータが保存された記録媒体と同じ場所に保管すると、自然災害などにより両方とも消失する可能性がある。そこで、バックアップのうち１つをオフサイトに保管することで、自然災害などでプライマリデータが消失したとしても、オフサイトに保管されたバックアップデータから復元することが可能となる。

３－２－１ルールは 2012 年から数年間は手間がかかるため現実的ではないと考えられていたが、ランサムウェアのまん延によって再評価され改めてユーザに推奨されるようになった [14]。

2.3.2 ランサムウェア対策としてのバックアップにおける留意事項

警視庁が公表しているランサムウェアの脅威と対策について紹介しているウェブページ [15] では、ランサムウェアの対策としてデータのバックアップをあげており、以下の点について推奨している。

- ランサムウェアに感染すると、ネットワークに接続された情報機器内データが暗号化される可能性があるため、バックアップデータはネットワークから切り離した状態で保存する
- 攻撃者に窃取されたデータが悪用されることを防ぐため、バックアップデータを暗号化した状態で保存する

IPA [16] は、ランサムウェアに感染した情報機器からの感染拡大によりバックアップも暗号化される可能性があることから、以下の点に留意する必要があることを指摘している。

- バックアップ記録媒体は、バックアップ時のみ情報機器と接続する

  外付け HDD や USB メモリなどは、情報機器と接続されていないとランサムウェアに感染することはないため、バックアップ時のみ情報機器と接続することを推奨している。なお、書き換え不可な光学メディア（CD-R、DVD-R、BD-R、M-DISC 等）は、パソコンに常時接続された状態であっても問題はないとしている。

  また、バックアップをクラウドストレージに保存するケースも考えられるが、バックアップの対象となるデータが保存されている情報機器のフォルダとクラウドストレージのフォルダが同期されている場合、情報機器がランサムウェアに感染しフォルダ内のデータが暗号化されるとクラウドストレージのデータも暗号化される可能性があることを指摘している。
- バックアップ記録媒体は複数用意し、バックアップを取得する

  複数の記録媒体にバックアップを取得しておくことで、仮に 1 つの記録媒体がランサムウェアに感染したり、ハードウェアの故障が発生した場合であっても、他の記録媒体に保存されたバックアップを利用することが可能となることを指摘している。

  また、IPA が公表している「5 分でできる！情報セキュリティ自社診断」[11] では、バックアップに使用する記録媒体を複数用意

することに加えて、そのうち 1 つを遠隔地に保存することを推奨している。

- バックアップの取得方法に問題がないか確認する
  バックアップを取得していも復元ができないと意味がなく、ランサムウェアによるデータの暗号化方法も変化する可能性があることを指摘している。そのため、実際にバックアップから復元することが可能であるか、ランサムウェアによるデータの暗号化方法が変化した場合に現在のバックアップ方法で対処することが可能であるかを確認することが重要であることに言及している。

金融庁及び日本銀行が地域銀行、信用金庫及び信用組合を対象に実施を求めたサイバーセキュリティセルフアセスメントの集計結果に関する公表資料 [17] に、バックアップデータが破壊・改ざんされることを想定した対策として以下のものが示されている。

- バックアップをネットワークから切り離された状態で保存する
- バックアップを書き換え不能な記録媒体で保存する
  上記 2 つの対策は、ランサムウェアによりバックアップデータが暗号化されることを回避するための対策として示されている。
- バックアップデータを複数世代保存する
  前回取得したバックアップがランサムウェアに感染しているリスクに対処するための対策として示されている。
- バックアップデータからの復旧訓練を行う
  実際にバックアップからデータを復元することが可能である確認するための対策として示されている。
- 復旧作業の対応手順を確立しておく
  復旧作業を行う際に、マルウェアに感染しているバックアップデータから復旧することで、復旧したデータが暗号化されてしまうことがないよう、事前にバックアップデータが感染していないことを確認してから復旧することが重要であることが示されている。

保険会社が公開している診断ツール [12] では、バックアップの取得に関する質問として以下のものが示されている。

- ”重要なデータを格納している情報システムやファイルサーバのバックアップは、毎日、毎時間等、定期的にバックアップを取得している”
- ”パソコンのデータのバックアップを定期的に取得している、もしくは、従業員にパソコン上に重要なデータを保存せずファイルサーバーなどの共有スペースに保存するよう指示している”
- ”取得したバックアップデータは、業務に関わる必要最低限の管理者・担当者のものだけがアクセスできるよう制限している”
- ”取得したバックアップデータの保存期間は、半年や 1 年等、情報の重要性に応じて設定している”
- ”取得したバックアップデータは、物理テープに記録して遠隔地に保存するなど、地震などの災害時にも利用できるようにしている”
- ”取得したバックアップデータから、正常にシステムやデータの復旧ができるかどうかを定期的、もしくはシステムを構築した段階でテスト又は訓練している”

2.3.3 ランサムウェア対策として効果的なバックアップの要件

前述した官公庁のウェブサイトや公表資料および民間企業が公開している診断ツールで、ランサムウェア対策として効果的なバックアップの要件があげられていた。ただし、重複しているものや一部でしか記載されていないものもあることから、要件を整理すると以下のものがあると考えられる。

- バックアップの対象となる重要データを整理する
- バックアップをネットワークから切り離した状態で保存する

- バックアップをクラウドストレージに保存している場合、バックアップの対象となるデータが保存されている情報機器のフォルダと同期されないように設定している
- バックアップを書き換え不能な記録媒体に保存する
- バックアップを複数の異なる記録媒体に保存する
- バックアップは取得頻度を決めて定期的に取得する
- バックアップは保存期間や保管する世代数を決めて取得する
- バックアップは管理者や担当者など必要最低限の者だけアクセスできるように制限する
- バックアップを暗号化して保存する
- バックアップからの復旧作業の対応手順を整備する
- バックアップからの復旧訓練を行う

しかし、これらの要件があることに言及し、その要件に応じた一般的な対策例については大まかに触れられたりしているものの、各組織が具体的な対策を検討する必要がある。

第 3 章
予 備 調 査

3.1. 中小企業におけるIT利用状況及びセキュリティ対策状況に関する調査

3.1.1 調査概要

中小企業におけるIT利用状況やセキュリティ対策の実施状況について把握することを目的に、中小企業４社に対して聞き取り調査を実施した。聞き取り調査を実施した中小企業の概要は表3.1のとおりである。

表 3.1 聞き取り調査先

調査先	業種	従業員数	資本金
Ａ社	自動車整備業	５名以下	1,000 万円以下
Ｂ社	飲食店	６～20 名以下	5,000 万円超～１億円以下
Ｃ社	食料品製造業	101～300 名以下	5,000 万円超～１億円以下
Ｄ社	サービス業	５名以下	1,000 万円以下

3.1.2 調査結果

Ａ社

業務で使用している情報機器としてパソコン２台があり、月額３万円のリース契約で利用していた。リース契約には、使い方やトラブル時の相談等ができる保

守サービスとウイルス対策ソフトの利用などが含まれている。2 台のパソコンのうち 1 台は事務所で整備の見積書の作成などの事務作業用として使用しており、もう 1 台は整備場で整備作業用として使用している。

パソコンの OS は Windows11 を使用しており、OS の更新があった際は自動更新されるようにしていた。事務所のパソコンには、見積書や契約関連書類といった書類が保存されており、クラウドストレージなどにバックアップを取得している。

これまでに、ウイルス感染などのセキュリティインシデントの被害を受けたことはなかった。パソコンのリース契約に掛かる月額 3 万円の費用は負担に感じているが、パソコンがないと業務に支障をきたすので必要な経費として受け止められていた。

B 社

業務で使用している情報機器として、パソコン 6 台を利用している。その他タブレット端末をレジとして利用していることに加え、業務連絡用にスマートフォン 4 台を利用している。従業員間でデータを共有するために、クラウドストレージを利用している。外部組織と連絡することなどを目的として、ウェブメールを利用している。調査時点で自社ドメインは利用していないが、自社ドメインの取得を検討している。自社のウェブサイトを公開しており、ウェブサーバは外部のレンタルサーバを利用している。

パソコンの OS は自動更新されるように設定されているはずであるが、正確に設定の確認はしていない状況であった。パソコンには、ウイルス対策ソフトをインストールしている。クラウドストレージではパソコンの操作に不慣れな従業員には閲覧権限のみを付与しており、アクセス権限の管理を行っている。また、クラウドストレージに保存しているデータは、月に 1 回外部記録媒体にバックアップを取得している。従業員とは入社時に秘密保持契約を結んでいる他、機密情報はメールに書かないように教育をしている。また、情報の格付けをする社内文書を作成しており、社員とアルバイトと閲覧可能な業務文書を分けることを規定している。

自社のウェブサイトにお問い合わせフォームに不審なメッセージが届くことがあり、不審な URL が含まれている場合は従業員に注意喚起をしている。どのよう

なサイバー攻撃があるかよく分かっておらず、自社にとって何が脅威であるかということは考えられていない状況である。

C社

C社は従業員数が比較的多い中小企業である。オンプレミスで社内ネットワークを構築し、業務システムを利用していた。自社のウェブサイトを公開しており、ウェブサーバは外部のレンタルサーバを利用している。

C社はランサムウェアの被害を受けたことがある。利用していたVPN機器に既知の脆弱性が存在していたが、バージョンアップの対応をしていなかった。当該脆弱性が悪用されVPN機器経由で社内のLANシステム内にあるサーバに不正アクセスされてしまい、サーバに保存されていたファイルが暗号化されてしまった。不正アクセスを受けたサーバはLAN内に設置していたバックアップ用のサーバにファイルを転送し、バックアップが取得されるようになっていたが、そのバックアップも暗号化されてしまった。バックアップからファイルの復元ができなかったため、前年資料がない状態で業務をするしかない状況になったことが最も業務に影響があった。なお、バックアップからの復元は過去に実施したことがあった。ランサムウェアの被害が発覚した後、感染したサーバをネットワークから隔離する対応を行っていた。そして、警察へ被害を通報し、個人情報保護委員会への報告も行なった。

ランサムウェアの被害を受けたことを踏まえ、ファイルのバックアップは外部記録媒体に数世代保存し、金庫で管理するようにしている。また、どんなにセキュリティ対策を講じても被害を完全に防御することは不可能であり、被害にあった際に素早く復旧させることを最優先と考え、現実に選べる選択肢の一つとしてオンプレミスからクラウドへの移行を進めている。

ランサムウェアの被害後、セキュリティへの投資を行い対策の強化を行っている。脅威は多岐にわたり、セキュリティ対策の実施にはコストがかかることから、最低限実施しておくことが望ましい対策を把握したいという要望があった。

D社

D社は正社員2名と契約社員1名の小規模な企業である。業務で使用している

情報機器として、２台のパソコンを正社員用に用意しており、契約社員は個人のパソコンを業務で使用している。また、クラウド型のグループウェアや会計ソフト、デザインソフトを有償で使用している。

OS のアップデート状況は確認しておらず、社員に任せている状態である。また、パソコンにウイルス対策ソフトをインストールされていなかった。なお、業務で使用するデータのバックアップは、クラウドストレージに保存していた。小規模な企業であることから、専任や兼任でセキュリティ担当者は置かれていなかった。

3.1.3 考察

聞き取り調査を実施した中小企業４社はいずれもパソコンなどの情報機器を業務で使用していた。特に、従業員規模の大きいＣ社においては、社内ネットワークを構築し、業務システムを利用していた。

セキュリティ対策の実施状況について確認したところ、パソコンの OS のアップデートに関して、更新状況を把握できている企業があった一方で、自動更新の設定状況を把握できていなかったり、更新実施状況を把握できていなかったりする企業もあった。業務で使用するパソコンへのウイルス対策ソフトのインストールは概ね実施されていたものの、１社インストールしていない企業があった。セキュリティ対策の実施状況は、中小企業の中でも差がある状況であると言える。ただし、バックアップの取得は４社とも実施しているとの回答があった。

IT 利用やセキュリティ対策についての認識を確認したところ、従業員規模が小さい企業であっても、パソコンがないと業務に支障をきたすので投資は必要であると受け止められていた。また、どのようなサイバー攻撃があり自社にとって何が脅威であるかを把握することが困難であるといった意見や最低限実施しておくことが望ましいセキュリティ対策を把握したいという要望があったことから、中小企業におけるセキュリティ対策の実施を支援する仕組みが求められていると考えられる。

3.2. 中小企業におけるバックアップの実施状況に関する調査

3.2.1 調査概要

バックアップの取得は中小企業でも、比較的実施されているセキュリティ対策となっている。しかし、ランサムウェアの被害にあった組織の多くでバックアップの取得は行われていたものの、多くの組織でバックアップからの復元に失敗している。バックアップからの復元が失敗した主な理由は、バックアップも暗号化されたことであった。このような結果になった背景として、ランサムウェア対策として効果的なバックアップの要件が考慮されずに、バックアップが取得されていることが考えられる。

そこで、中小企業に対してバックアップの取得方法についてヒアリングし、ランサムウェア対策として効果的なバックアップの要件がどの程度満たされているかについて確認する調査を実施した。聞き取り調査では、下記の項目について質問を行った。なお、聞き取り調査を実施した中小企業は、表 3.1 に記載したＡ社とＤ社である。

1. 消失すると業務の継続に影響のあるデータ（以下、重要データ）の把握について
2. 重要データのバックアップの実施について
3. バックアップを取得する重要データが保存されている記録媒体について
4. 取得しているバックアップのサイズについて
5. バックアップの取得頻度について
6. バックアップを保存している記録媒体（以下、バックアップ記録媒体）について
7. 重要データが保存されている情報機器とバックアップ記録媒体の接続について

8. バックアップの保存期間（世代管理の方法）について
9. バックアップから重要データの復元が可能であることの確認について
10. ランサムウェアに対する認識について

3.2.2 調査結果

Ａ社

1. 重要データの把握について
   見積書と契約関連書類といった書類が重要データに該当する。
2. 重要データのバックアップの実施について
   見積書と契約関連書類について、バックアップを取得している。データ形式は両方とも PDF である。電子データでバックアップを取得するようになったのは、数年前からである。パソコンのリース契約を結んでいるベンダが、定期的にバックアップを取得するように設定をしている。しかし、バックアップの取得頻度やバックアップを取得する仕組みについて、経営者は把握していなかった。
3. バックアップを取得する重要データが保存されている記録媒体について
   バックアップを取得する重要データは、事務所に置いているパソコン 1 台に保存している。パソコンには HDD が 2 つ内蔵されており、Ｃドライブと Ｄドライブが割り当てられている。重要データはＣドライブに保存されている。
4. 取得しているバックアップのサイズ
   調査時点の累計サイズで、見積書は約 1 GB、契約関連書類は約 1 MB であった。
5. バックアップの取得頻度について
   バックアップの取得頻度について、経営者は把握できていなかった。自動的

に実施されるためバックアップの取得漏れはないはずであるが、取得状況について特に確認は行っていなかった。

6. バックアップ記録媒体について
   バックアップ記録媒体として、パソコンのDドライブを利用しており、容量は256GBである。以前はクラウドストレージにバックアップを保存していたが、容量が不足したためパソコンのDドライブにバックアップを保存するようになった。

7. 重要データが保存されている情報機器とバックアップ記録媒体の接続について
   重要データが保存されているCドライブとバックアップが保存されているDドライブは、同じパソコンに内蔵されているドライブであり、常に接続されている状況となっていた。

8. バックアップの保存期間（世代管理の方法）について
   バックアップの保存期間は特段定めていない。調査時点でサイズが小さいこともあり、取得したバックアップはすべて保存されたままであった。なお、重要データのコピーをDドライブに追加していく方法でバックアップを取得しており、世代管理は行われていなかった。

9. バックアップから重要データの復元が可能であることの確認について
   データが復元可能であることを確認するために、Dドライブに保存されているバックアップデータをCドライブに戻す作業を実施したことはなかった。

10. ランサムウェアに対する認識について
    ランサムウェアについてネットニュースで見たことがあるが、詳しく調べたことなどはなかった。ランサムウェアの被害に遭うのは従業員が100人以上いるような規模の大きい会社であり、自社にとってあまり関係はないだろうと考えられていた。

Ｄ社

1. 重要データの把握について
   顧客情報、請求書、契約書、写真データや動画データなどのデザイン資料、文書作成ソフトや表計算ソフトなどで作成した業務資料、取引先から受領した資料などが重要データに該当する。なお、バックアップの対象となる重要データについて規定しておらず、どのデータのバックアップを取得するかについては従業員が判断している。

2. 重要データのバックアップの実施について
   従業員がバックアップの取得が必要であると判断した重要データについて、バックアップを実施している。

3. バックアップを取得する重要データが保存されている記録媒体について
   重要データは、パソコンのローカルドライブに保存されている。

4. 取得しているバックアップのサイズ
   調査時で約 20GB であった。調査時が会社の設立から 1 年半程度経過した時期であり、設立時からの累計のバックアップサイズである。

5. バックアップの取得頻度について
   バックアップの取得頻度は決められておらず、バックアップの取得が必要だと判断した時に都度取得している。

6. バックアップ記録媒体について
   重要データのバックアップは、クラウドストレージに保存している。クラウドストレージの容量は 60GB である。クラウドストレージで、アクセス権の設定が異なる 2 つのドライブを使用している。1 つ目は、経営者と社外の税理士にアクセス権が付与されているドライブであり、顧客情報、請求書、契約書のバックアップが保存されている。2 つ目は、従業員全員にアクセス権が付与されているドライブであり、業務資料、デザイン資料、取引先から受容した資料のバックアップが保存されている。業務案件ごとにフォルダを作

成し、関連するデータのバックアップをまとめて保存するように従業員に指示している。

7. 重要データが保存されている情報機器とバックアップ記録媒体の接続について
   基本的には、バックアップの都度クラウドストレージにアクセスし、パソコンのローカルドライブから重要データをコピーしている。なお、パソコンのフォルダとクラウドストレージのフォルダが同期されているかについて、把握されていなかった。

8. バックアップの保存期間（世代管理の方法）について
   バックアップの保存期間は特段定めていない。なお、半年に 1 回程度、不要になったデータがないか確認し、不要なものがあった場合クラウドストレージから削除している。

9. バックアップから重要データの復元が可能であることの確認について
   バックアップから復元可能であることの確認を意図しているわけではないが、業務の中で閲覧したいデータをクラウドストレージからパソコンのローカルドライブにダウンロードした際に、利用できることは確認できている。

10. ランサムウェアに対する認識について
    学生時に授業で聞いたことがあり、ランサムウェアがどういったコンピュータウイルスであるかは何となく理解している。規模の大きい会社が対象になると考えており、自社とってそこまで影響があるとは思われていなかった。

3.2.3 考察

重要データについては、おおよそ把握されていた。しかし、バックアップを取得するかについて従業員の判断により決めている企業があり、場合によってはバックアップの取得が必要な重要データのバックアップ取得漏れが生じている可能性がある。

バックアップの取得頻度について、把握していなかったり、決められていなかった。ランサムウェアによる暗号化や記録媒体の故障など何らかの理由で重要データが使用できなくなった際に、どのくらい前のデータが復元できれば業務に問題ないかについて関心が低い状況であると考えられる。

バックアップ記録媒体として、A社はパソコンに2つあるドライブのうち、バックアップ対象の重要データが保存されているドライブとは異なるドライブにバックアップを保存しており、バックアップをネットワーク切り離した状態で保存することについてあまり意識されていない状況であると言える。また、D社はクラウドストレージを利用していたが、パソコンのフォルダとクラウドストレージが同期されているかについて把握されておらず、情報機器のフォルダとクラウドストレージが同期されていると情報機器がランサムウェアに感染した場合に、クラウドストレージまで感染が拡大する可能性があることを特に警戒されていない状況となっていた。

バックアップの保存期間については、2社とも特段定めていなかった。2社ともバックアップ記録媒体の保存容量に空きがある状況であり、これまでに取得したバックアップをすべて保存した状態となっている。

バックアップから重要データの復元ができることの確認については、意図的に実施されていなかった。一方で、業務の中で閲覧したいデータをバックアップの中からパソコンにデータを戻して閲覧する機会があり、利用可能であることは確認できている状況であった。

聞き取り調査先はいずれも従業員数が5名以下の小規模な企業であり、ランサムウェアの被害にあう企業は自社より規模の大きい会社であると考えており、自社にはあまり関係がないと考えられていた。ランサムウェアは自社にとって脅威であるという認識が薄いことから、ランサムウェア対策を意識してバックアップを取得していない状況にあると言える。

3.3. ランサムウェア対策としての効果的なバックアップの要件の認識に関する調査

3.3.1 調査目的

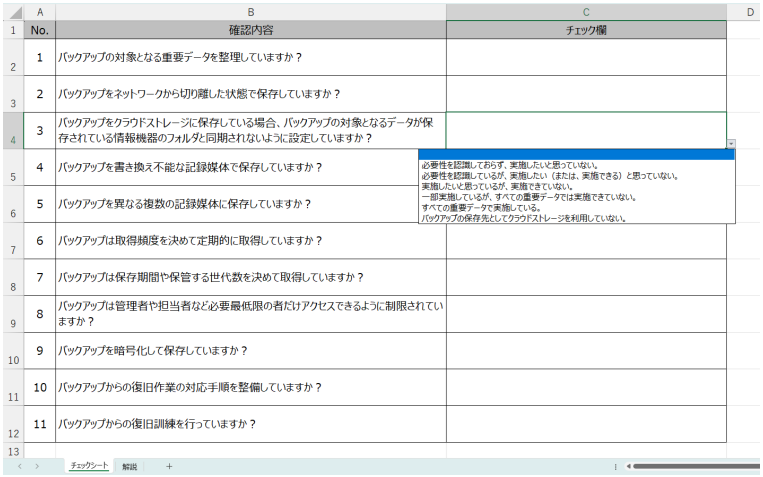
従業員規模が5名以下の比較的小規模な中小企業のバックアップ実施状況について確認した予備調査の結果、ランサムウェアは自社にとって脅威であるという認識が薄く、ランサムウェア対策を意識してバックアップを取得していない状況であることがわかった。また、Barracuda 社が日本の従業員数が 50〜200 名の組織を対象に実施した調査のレポート [18] によると、データを安全に復元・復旧するためにオフラインバックアップまたはイミュータブル（変更不可）バックアップを行っている企業は 23 %となっていた。これらのことから、従業員規模に関わらずランサムウェア対策を意識してバックアップを取得している中小企業は少ないことが推測される。

中小企業がランサムウェアの被害にあった際に、バックアップからデータを復元することで業務の継続を可能にし、被害を最小限に抑えるためには、まずはランサムウェア対策として効果的なバックアップの要件を中小企業に認識してもらう必要があると考えられる。そこで、自社のバックアップがどの程度要件を満たしているかについて確認してもらうことで、中小企業に要件を認識してもらうことが可能であるか確かめることを目的とした調査を実施することにした。

3.3.2 チェックリストの概要

調査を実施するにあたり、自社のバックアップがどの程度要件を満たしているかについて確認してもらうことを補助するために、要件のチェックリストを作成した。

チェックリストは、Microsoft 社の Excel を用いて作成した。Excel ファイルのチェックリストを図 3.1 に示す。確認内容ごとに実施状況について該当するものをプルダウンの中から選択して利用する。



No.	確認内容	チェック欄
1	バックアップの対象となる重要データを整理していますか？	
2	バックアップをネットワークから切り離した状態で保存していますか？	
3	バックアップをクラウドストレージに保存している場合、バックアップの対象となるデータが保存されている情報機器のフォルダと同期されないように設定していますか？	
4	バックアップを書き換え不能な記録媒体で保存していますか？	
5	バックアップを異なる複数の記録媒体に保存していますか？	
6	バックアップは取得頻度を決めて定期的に取得していますか？	
7	バックアップは保存期間や保管する世代数を決めて取得していますか？	
8	バックアップは管理者や担当者など必要最低限の者だけアクセスできるように制限されていますか？	
9	バックアップを暗号化して保存していますか？	
10	バックアップからの復旧作業の対応手順を整備していますか？	
11	バックアップからの復旧訓練を行っていますか？	

図 3.1　Excel ファイルのチェックリスト

また、Excel を使用できない可能性があることを考慮し、PDF ファイルのチェックリストも用意した。PDF ファイルのチェックリストを図 3.2 に示す。No.4 以降の確認内容は、次ページ以降に続いている。

チェックツール

No.	確認内容	チェック欄
1	バックアップの対象となる重要データを整理していますか？	□ 必要性を認識しておらず、実施したいと思っていない。 □ 必要性を認識しているが、実施したい（または、実施できる）と思っていない。 □ 実施したいと思っているが、実施できていない。 □ 一部実施しているが、すべての重要データでは実施できていない。 □ すべての重要データで実施している。
2	バックアップをネットワークから切り離した状態で保存していますか？	□ 必要性を認識しておらず、実施したいと思っていない。 □ 必要性を認識しているが、実施したい（または、実施できる）と思っていない。 □ 実施したいと思っているが、実施できていない。 □ 一部実施しているが、すべての重要データでは実施できていない。 □ すべての重要データで実施している。
3	バックアップをクラウドストレージに保存している場合、バックアップの対象となるデータが保存されている情報機器のフォルダと同期されないように設定していますか？	□ 必要性を認識しておらず、実施したいと思っていない。 □ 必要性を認識しているが、実施したい（または、実施できる）と思っていない。 □ 実施したいと思っているが、実施できていない。 □ 一部実施しているが、すべての重要データでは実施できていない。 □ すべての重要データで実施している。 □ バックアップの保存先としてクラウドストレージを利用していない。

図 3.2　PDF ファイルのチェックリスト

確認内容

チェックリストで確認する内容として、第２章３項３節で整理したランサムウェア対策として効果的なバックアップの要件に基づき、以下のものを用意した。また、各確認内容を用意した意図についても記載する。

1. バックアップの対象となる重要データを整理していますか？
   重要データのバックアップ取得漏れを防止するために確認する項目である。

2. バックアップをネットワークから切り離した状態で保存していますか？
   感染した情報機器からの感染拡大によるバックアップの暗号化を防止するために確認する項目である。

3. バックアップをクラウドストレージに保存している場合、バックアップの対象となるデータが保存されている情報機器のフォルダと同期されないように設定していますか？
   感染した情報機器からクラウドストレージへの感染拡大によるバックアップの暗号化を防止するために確認する項目である。

4. バックアップを書き換え不能な記録媒体で保存していますか？
   バックアップの暗号化を防止するために確認する項目である。
   例として、CD-R、DVD-R、BD-R、M-DISC などがある。

5. バックアップを異なる複数の記録媒体に保存していますか？
   ランサムウェアによる暗号化や記録媒体の故障などにより、バックアップが使用不可となることを防止するために確認する項目である。

6. バックアップは取得頻度を決めて定期的に取得していますか？
   ランサムウェアによるデータの暗号化や記録媒体の故障などが発生した場合に、発生時からどのくらい前の時点のデータに復旧させると業務に影響が小さいかについて予め考慮してバックアップを取得しているかを確認する項目である。

7. バックアップは保存期間や保管する世代数を決めて取得していますか？
   ランサムウェアには感染してから被害が発生するまでに潜伏期間があるため、直近のバックアップが既に感染しているリスクに対処するために確認する項目である。

8. バックアップは管理者や担当者など必要最低限の者だけアクセスできるように制限されていますか？
   バックアップへの不正アクセスのリスクを低減するために確認する項目である。

9. バックアップを暗号化して保存していますか？
   窃取されたデータの悪用を防止するために確認する項目である。

10. バックアップからの復旧作業の対応手順を整備していますか？
    バックアップからの早急な復旧を実現するために、事前に準備がされているかについて確認する項目である。

11. バックアップからの復旧訓練を行っていますか？
    バックアップから復旧可能であることを確かめられているかについて確認する項目である。

選択肢

上記の確認内容に対して、自社の対策状況を確認することができるように、以下の選択肢を用意した。なお、確認内容の３つ目と４つ目に関しては、バックアップ記録媒体としてクラウドストレージと書き換え不能な記録媒体を使用していない場合があることから、それぞれ「バックアップの保存先としてクラウドストレージを利用していない。」と「バックアップの保存先として書き換え不能な記録媒体を利用していない。」を追加している。

1. 必要性を認識しておらず、実施したいと思っていない。

2. 必要性を認識しているが、実施したい（または、実施できる）と思っていない。

3. 実施したいと思っているが、実施できていない。

4. 一部実施しているが、すべての重要データでは実施できていない。

5. すべての重要データで実施している。

3.3.3 調査概要

作成したチェックリストを中小企業に実際に使用してもらい、現在のバックアップがどの程度要件を満たしているかについて確認してもらった。その後、各確認内容について選択肢を選んだ理由やチェックリストの使用感に関してヒアリングを行い、要件を認識してもらうことが可能であるかについて確認した。調査を実施した中小企業は、表 3.1 に記載したＡ社である。調査は 2024 年の 12 月中旬に実施した。

3.3.4 調査結果

1. バックアップの対象となる重要データを整理していますか？
   「一部実施しているが、すべての重要データでは実施できていない」を選択していた。
   取引先から PDF で送られてくる部品の仕入れなどの請求書について、現状は印刷して紙でバックアップを保存しているが、電子データでバックアップを取得することも考えられていた。

2. バックアップをネットワークから切り離した状態で保存していますか？
   「実施したいと思っているが、実施できていない」を選択していた。
   バックアップの保存先がパソコン内のＤドライブになっており、バックアップをパソコンから切り離した状態で保存できていない状態であることから、当該選択肢を選択していた。

3. バックアップをクラウドストレージに保存している場合、バックアップの対象となるデータが保存されている情報機器のフォルダと同期されないように

設定していますか？
「実施したいと思っているが、実施できていない」を選択していた。
以前はクラウドストレージにバックアップを保存していたが容量が上限に達したため、パソコンのDドライブにバックアップを取得するようになった。
Dドライブとは別にバックアップの保存先を用意するとしたら、クラウドストレージを使用することが考えられるが、現状バックアップはDドライブにのみ保存されている状態であったことから、当該選択肢を選択されていた。

4. バックアップを書き換え不能な記録媒体で保存していますか？
「実施したいと思っているが、実施できていない」を選択していた。
CD-R は確かに、ランサムウェア対策を考えた場合に、書き換えができなくて、ネットワークにつながっていない点が良いと感じられていた。

5. バックアップを異なる複数の記録媒体に保存していますか？
「実施したいと思っているが、実施できていない」を選択していた。
バックアップの保存先がDドライブしかないので、当該選択肢を選択されていた。
CD-R に保存することを検討されようとしていた。

6. バックアップは取得頻度を決めて定期的に取得していますか？
「実施したいと思っているが、実施できていない」を選択していた。
サポートベンダが定期的にバックアップするように設定しているが、仕組みや頻度を経営者が把握できていなかったため、当該選択肢を選択されていた。
いつバックアップを取るように設定されているのか、サポートベンダに確認することを検討されようとしていた。
また、経営者自身で CD-R に月 1 回や 2 週間に 1 回などの頻度で定期的にバックアップを取得することを検討されようとしていた。

7. バックアップは保存期間や保管する世代数を決めて取得していますか？
「実施したいと思っているが、実施できていない。」を選択していた。
「世代数」がどういう意味かわからないという意見があった。

8. バックアップは管理者や担当者など必要最低限の者だけアクセスできるように制限されていますか？
   「すべての重要データで実施している」を選択していた。
   会社の中でパソコンを利用しているのは経営者一人であるため、当該選択肢を選択されていた。

9. バックアップを暗号化して保存していますか？
   「実施したいと思っているが、実施できていない」を選択していた。
   簡単に実施できるものなのかわからないと感じられていた。

10. バックアップからの復旧作業の対応手順を整備していますか？
    「実施したいと思っているが、実施できていない」を選択していた。

11. バックアップからの復旧訓練を行っていますか？
    「実施したいと思っているが、実施できていない」を選択していた。
    10 と 11 について、現状だと復旧を実施すると言っても、Dドライブから C ドライブにコピーすることになると考えられていた。
    また、パソコンが何らかのトラブルで使えなくなったとしても、サポートベンダに対応してもらうことになると考えられていた。
    パソコンを使用するのが自分（経営者）だけだからかもしれないが、必要性がないわけではないけれども、差し迫って実施するものではないと考えられていた。

12. その他
    このリストを使用してみて、バックアップ記録媒体として書き換え不能な記録媒体を使用するという今まで見落としていた方法に気付くことができたと感じていた。
    何かあった時のためにちゃんとバックアップを取って保管しておくことの必要性を訴えるようなツールであるが、バックアップを取るにあたり何が必要であるかということを確認すること自体が大切だと感じていた。

3.3.5 考察

チェックリストを使用することで、バックアップの保存先として書き換え不能な記録媒体が有効であることに気づいたり、これまでサポートベンダに設定してもらっていたため把握していなかったバックアップの取得頻度について確認することを検討されるようになるなど、ランサムウェア対策として効果的なバックアップの要件を認識してもらうことにある程度の効果があったと考えられる。

一方で、世代数とは何なのかわからないという意見があった。A社のバックアップ取得方法は、バックアップ対象のデータである見積書や契約関連書類の PDF ファイルをのコピーをバックアップの保存先であるDドライブに追加していく方法であり、バックアップの世代管理が行われていなかったため、世代数という言葉に馴染みがなかったと考えられる。そのため、チェックリスト内で使用する用語は、理解しやすいように説明を工夫する必要がある。

さらに、バックアップからの復旧作業の対応手順を整備することやバックアップからの復旧訓練の実施について、社内でパソコンを使用しているのが経営者一人であることやサポートベンダの支援を受けることができることから、差し迫って実施するものではないと考えているという意見があった。そのため、バックアップ取得前にウイルスチェックを実施しているかを確認する内容や、バックアップ取得後にデータの取得漏れや破損などといったデータの整合性に問題がないか確認する内容を追加することで、バックアップから復旧可能であることの確認を実施してもらうことに繋げるための工夫をすることが考えられる。

また、書き込み不能な記録媒体を使用するという確認項目は、具体的な対策方法がわかりやすく、対策の実施を検討されようとしていた一方で、バックアップの暗号化に関する確認内容に対しては簡単に実施できるかわからないといった反応があった。そのため、具体的な対策方法を提示することで、要件を満たしたバックアップの実施を前向きに検討してもらうことが可能になるのと考えられる。

なお、このチェックリストを使用した調査の 1 か月後である 2025 年の 1 月中旬に確認したところ、バックアップの取得方法に変化は見られなかった。A社の経営者からは、バックアップの取得方法の変更を実施するには 2 ～ 3 か月程度時間が必要であるとの回答があった。

第 4 章
提　　案

4.1. 関連事例に基づく議論

4.1.1 中小企業におけるセキュリティ対策実施の阻害要因

IPA の調査 [4] によると、約 9 割の企業で業務での IT の導入が行われている一方で、セキュリティ対策の実施は十分に進んでいない状況となっていた。また、必要性を感じないことや費用対効果が見えないこと、コストがかかり過ぎること、どこからどう始めたらよいかわからないといった理由から、情報セキュリティ対策に投資していない企業も 3 割強存在している結果となっていた。また、日本政策金融公庫総合研究所の調査 [5] によると、セキュリティ対策を進めるうえでの障害について、特にないという回答が最も多くなっていたが、次いで資金不足や経営者の知識が足りないことなどが多く回答されていた。

これらの調査結果から、中小企業においてセキュリティ対策の実施が十分に進んでいない要因として、セキュリティ対策への関心が低いことが最大の要因となっているが、資金不足や知識不足も主要な要因となっていると言える。

4.1.2 中小企業のセキュリティ対策実施に向けた支援における課題

中小企業のセキュリティ対策を実施を支援する取組みとして、IPA が行っている SECURITY ACTION [6] があるが、あくまで中小企業がセキュリティ対策に取り組むことを自己宣言する取組みであり、セキュリティ対策実施状況の評価が行われているわけではない。また、東京都が行っている支援事業 [8] があるが、ランサムウェア対策の 2 つのタイプのうち、どちらかというと感染を防止する対策

を支援する内容となっている、また、対象となる中小企業の所在地や数が制限されたものとなっている。

また、中小企業のセキュリティ対策実施状況を評価するための診断ツール [11] [12] が公開されている。これらの診断ツールはセキュリティ対策に関する各質問項目に回答することで対策実施状況が数値化され、点数に応じて対策実施状況の評価が行われるものである。中小企業が診断ツールを実施した結果を踏まえてセキュリティ対策を改善する際は、診断ツールにも各質問項目に対する一般的な対策例は示されたりしているものの、具体的に自社でどのような対策を実施するかについては中小企業が各自で検討する必要がある。

4.2. 予備調査の結果に基づく議論

第 3 章に記載した予備調査の結果においても、中小企業で IT の導入にが進んでいる一方で、セキュリティ対策の実施状況には差がある状況となっていた。また、中小企業に対するセキュリティ対策の実施を支援する仕組みが求められていることも確認できた。

バックアップは取得はされていたものの、ランサムウェアが自社にとって脅威であるという認識が薄く、ランサムウェア対策として効果的なバックアップの要件が満たされていなかった。そこで、要件のチェックリストを作成し、当該チェックリストを使用してバックアップがどの程度要件を満たしているかを確認してもらうことで、要件を認識してもらう調査を実施した。結果として、チェックリストを使用してもらうことで、要件を認識してもらうことにある程度の効果があることが確認できた。特に、書き換え不能な記録媒体を使用するという要件について、具体的な対策の実施方法がわかりやすく、既存のバックアップ体制からの改善を検討されてようとしていたことから、具体的な対策例を提示することで、体制の改善を実施をしてもらうことに繋げることができるのではないかと考えられる。

4.3. コンセプト

前節までの議論から、中小企業のセキュリティ対策を阻害している要因として知識不足がある。そのため、既存のツールはセキュリティ対策実施状況を数値化し評価してくれる一方で、対策例については一般的な方法を提示するにとどまり、具体的な対策実施方法は中小企業で判断する必要があることから、既存のツールを使用することで対策実施方法の改善に至ることは困難であると考えられる。また予備調査から、具体的な対策例を提示することにより、対策の改善実施に至る可能性が高くなることが考えられる。

以上のことから、中小企業で現在行っているバックアップ体制を評価し、要件を満たしているかを確認すると共に、効果的なバックアップを実施するための対策例を提示するアドバイスツールを作成し利用して貰うことを提案する。

4.4. 設計

4.4.1 アドバイスツールの概要

アドバイスツールで要件を満たしているか評価したり、具体的な対策例を提示したりするために、バックアップ対象のデータに関する情報と要件の実施状況に関する情報を収集する。これらの情報の収集には、Google フォームを利用する。Google フォームで収集した情報を CSV ファイルで出力し、Python プログラムで読み込んで要件を満たしているかの評価と具体的な対策例を判定し、結果をテキストファイルで出力する。アドバイスツールの構造を図 4.1 で示す。

4.4.2 収集する情報に関する設計

バックアップ対象のデータに関する情報と要件の実施状況に関する情報を Google フォームで収集する。Google フォームへの情報の入力例を図 4.2 で示す。バックアップ対象のデータに関する情報と要件の実施状況に関する情報の詳細は、次のとおりである。

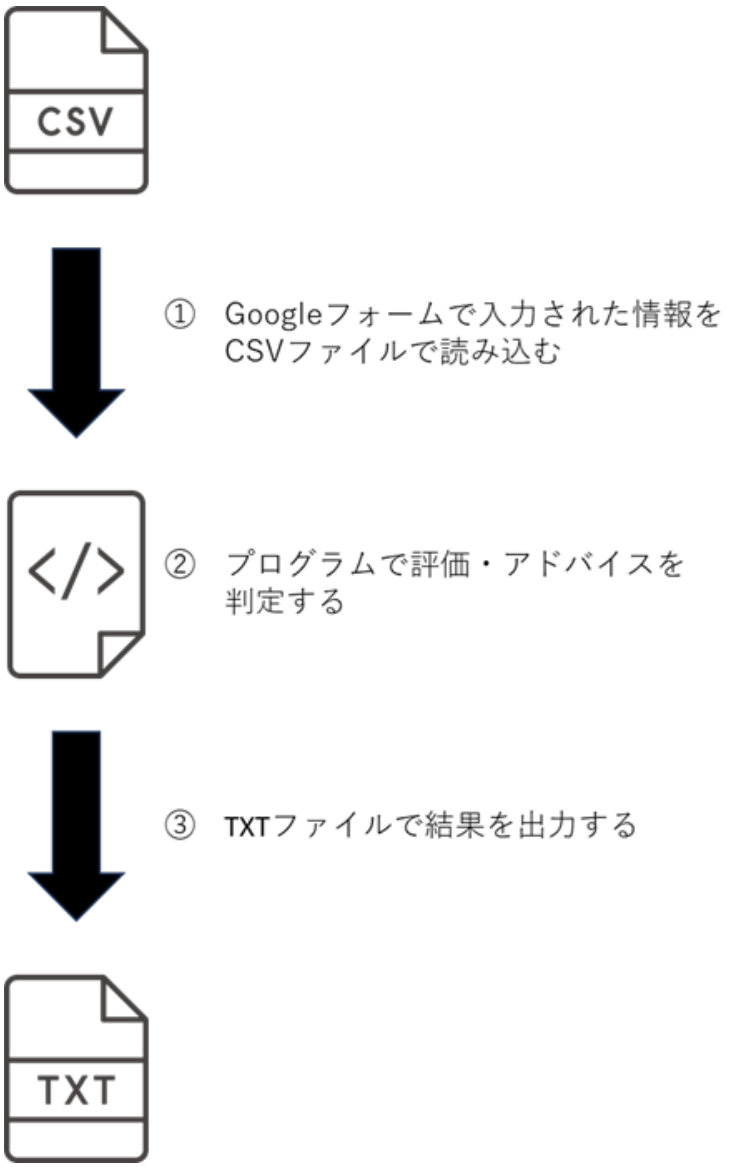


図 4.1 アドバイスツールの構造

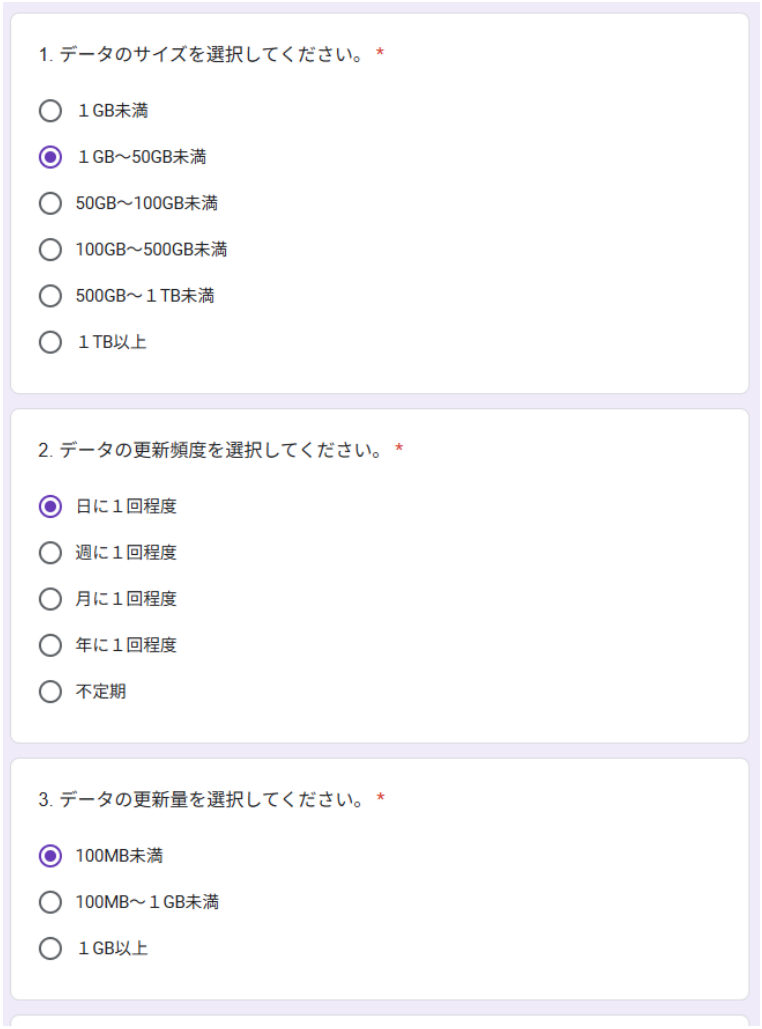


図 4.2 Google フォームでの情報の入力例

バックアップ対象のデータに関する情報

バックアップ対象のデータに関する情報として、以下のものを使用する。アドバイスツールで現状のバックアップ方法がランサムウェアとして効果的なバックアップの要件を満たしているか評価したり、要件を満たしていない場合に提示する具体的な対策例が何であるか判断したりする際に、必要になると考えられるものを挙げている。

- データのサイズ
  「1 GB 未満」「1 GB～50GB 未満」「100GB～500GB 未満」「500GB～1TB 未満」「1 TB 以上」の中から該当するものを選択してもらう。

- データの更新頻度
  「日に 1 回程度」「週に 1 回程度」「月に 1 回程度」「年に 1 回程度」「不定期」の中から該当するものを選択してもらう。

- データの更新量
  「100MB 未満」「100MB～ 1 GB 未満」「1 GB 以上」の中から該当するものを選択してもらう。

- データの重要度
  「高い（消失すると業務に大きな影響がある、再作成が困難である）」
  「普通（消失すると業務に影響がある、再作成が可能である）」
  「低い（消失しても業務への影響は軽微である、再作成が可能である）」
  の中から該当するものを選択してもらう。

- データが保存されている情報機器のインターネットの接続状況
  「インターネットに接続されている」「インターネットに接続されていない」
  の中から該当するものを選択してもらう。

要件の実施状況に関する情報

要件の実施状況に関する情報として、以下のものを使用する。第２章３項３節で整理したランサムウェア対策として効果的なバックアップの要件として整理し

たものを挙げている。また、予備調査の結果を踏まえて、バックアップから復旧可能であることの確認として、「バックアップからの復旧訓練の実施」の他に、「バックアップ前のデータのウイルスチェックの実施」と「バックアップ後のデータの整合性の確認」を追加している。

- バックアップの取得頻度
  「日に 1 回程度」「週に 1 回程度」「月に 1 回程度」「年に 1 回程度」「不定期」の中から該当するものを選択してもらう。

- バックアップの取得方法
  「フルバックアップ」「差分バックアップ」「増分バックアップ」の中から該当するものを選択してもらう。

- バックアップの世代管理
  「実施している（直近のバックアップだけではなく、数回分保存している）」
  「実施していない（直近のバックアップのみ保存している）」
  の中から該当するものを選択してもらう。

- バックアップ記録媒体
  「HDD」「SSD」「バックアップ用サーバ（NAS を含む）」「磁気テープ」「USB メモリ」「SD カード」「書き換え可能な光学メディア（CD-RW、DVD-RW、BD-RE 等）」「書き換え不可な光学メディア（CD-R、DVD-R、BD-R、M-DISC 等）」「クラウドストレージ」「紙」「その他（自由記述）」の中から該当するものをすべて選択してもらう。

- バックアップ記録媒体のネットワーク接続状況
  バックアップ記録媒体として、HDD、SSD、バックアップ用サーバ、磁気テープ、USB メモリ、SD カード、書き換え可能な光学メディアを回答している場合に、以下から該当するものを選択してもらう。
  「バックアップ時のみデータが保存されている情報機器などと接続し、取得後切り離している」
  「データが保存されている情報機器などと常時接続している」
  「わからない」

- クラウドストレージと情報機器のフォルダの同期設定
  バックアップ記録媒体として、クラウドストレージを回答している場合に、以下から該当するものを選択してもらう。
  「同期されていない」「同期されている」「わからない」

- バックアップのアクセス制御
  「バックアップの担当者だけなどにアクセス制御をしている」「アクセス制御をしていない」「わからない」の中から該当するものを選択してもらう。

- バックアップの暗号化
  「暗号化している」「暗号化していない」「わからない」の中から該当するものを選択してもらう。

- バックアップからの復旧作業の手順の整備
  「整備している」「整備していない」の中から該当するものを選択してもらう。

- バックアップからの復旧訓練の実施
  「年に 1 回程度実施している」「実施していない」の中から該当するものを選択してもらう。

- バックアップ前のデータのウイルスチェックの実施
  「実施している」「たまに実施している」「実施していない」の中から該当するものを選択してもらう。

- バックアップ後のデータの整合性の確認
  「確認している」「たまに確認している」「確認していない」の中から該当するものを選択してもらう。

4.4.3 プログラムの設計

要件の実施状況に関する情報とバックアップ対象のデータに関する情報から、ランサムウェア対策として効果的なバックアップの要件を満たしたバックアップが取得されているかについて評価を行い、満たしていない場合に具体的な対策例を判定するプログラムを作成した。収集した要件の実施状況に関する情報ごとに以下の処理を行っている。

バックアップの取得頻度

回答されたバックアップの取得頻度がランサムウェア対策として効果的なバックアップの要件を満たしているか評価するために、基準値を計算する。基準値は、以下の方法で計算する。

基準値 = バックアップ取得頻度 - バックアップ必要度

バックアップ取得頻度には、入力された回答に応じて表4.3の値を付与している。

表 4.1 バックアップ取得頻度・データ更新頻度に付与する値

頻度	値
日に 1 回程度	50
週に 1 回程度	40
月に 1 回程度	30
年に 1 回程度	20
不定期	10

バックアップ必要度は、以下の方法で計算する。

バックアップ必要度 =
データ更新頻度 + データサイズ + データ更新量 + データ重要度 +
データが保存されている情報機器のインターネット接続状況

バックアップ必要度の計算に使用する情報には、入力された回答に応じて以下の値を付与している。

- データ更新頻度
  回答された更新頻度に応じて、バックアップ取得頻度と同様に表 4.3 の値を付与している。

- データサイズ
  100GB 以上を回答された場合に、「-10」を付与している。
  データサイズが大きくなると、バックアップ記録媒体の容量を多く消費し、頻繁にバックアップを取得することが困難になると考えられるためである。

- データ更新量
  1GB 以上を回答された場合に、「-10」を付与している。
  データの更新量が大きくなると、バックアップ記録媒体の容量を多く消費し、頻繁にバックアップを取得することが困難になると考えられるためである。

- データ重要度
  高いを回答された場合に「10」を、低いを回答された場合に「-10」を付与している。
  重要度の高いデータは取得頻度を増やし、低いデータは取得頻度を減らすことが考えられるためである。

- データが保存されている情報機器のインターネット接続状況
  インターネットに接続されていないを回答された場合に、「-10」を付与している。
  インターネットに接続されていない場合、ランサムウェアの被害にあうリスクが低くなるためである。

計算された基準値を基に図 4.3 の処理を行い、バックアップ取得頻度の評価を行う。頻度が低いと評価された場合（基準値が 0 未満の場合）には、データ更新頻度またはバックアップ必要度の値に応じた頻度（例：バックアップ必要度が 40 の場合、週に 1 回程度）でバックアップを取得することを提示する。

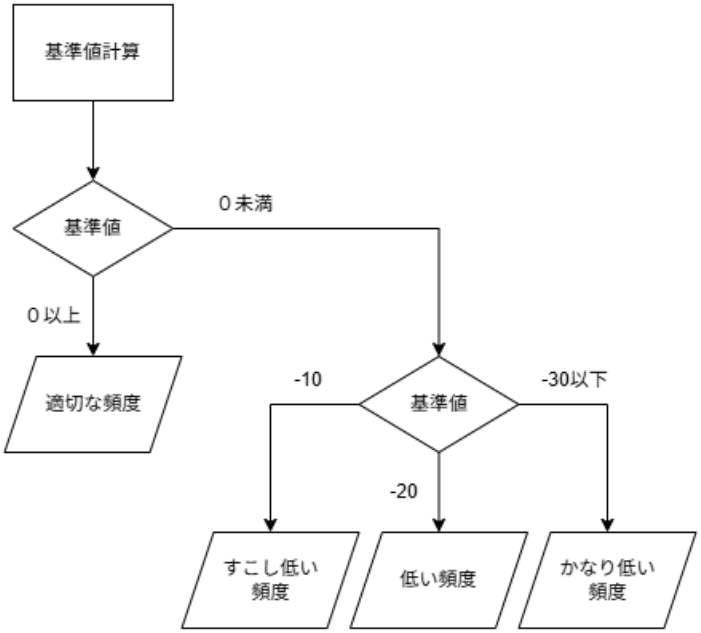


図 4.3 バックアップの取得頻度の評価

バックアップの取得方法

回答されたデータ更新量とデータ更新頻度を基に図 4.4 の処理を行い、バックアップ取得方法の評価を行う。また、フルバックアップを実施しているが、処理結果として差分・増分バックアップが推奨される場合には、差分・増分バックアップの実施を提示し、差分・増分バックアップを実施しているが、処理結果としてフルバックアップが推奨される場合には、フルバックアップの実施を提示する。

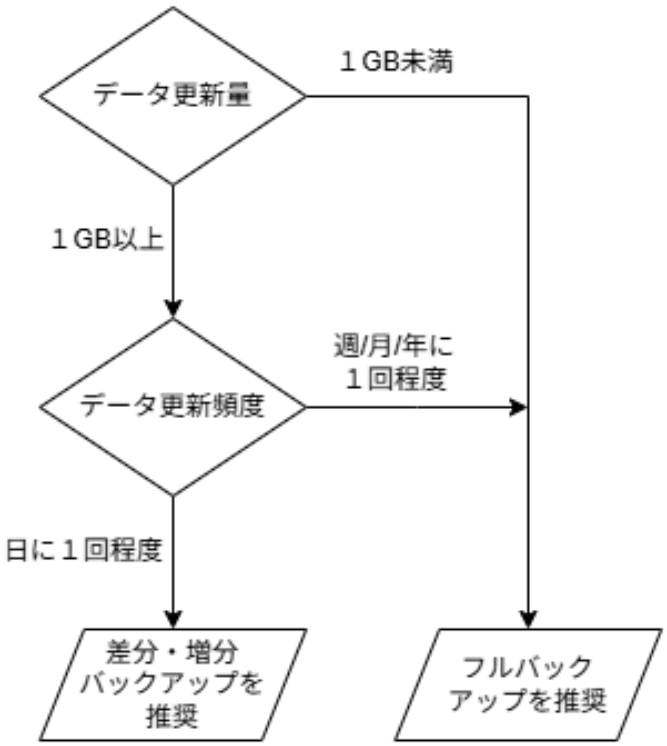


図 4.4 バックアップの取得方法の評価

バックアップの世代管理

回答されたデータ重要度とバックアップの取得方法を基に図 4.5 の処理を行い、バックアップの世代管理の評価を行う。重要度が高いデータについては 3 か月分保存し、普通または低いデータについては 1 か月分保存することを提示する。また、バックアップの取得方法に応じて保存する世代数についても提示する。

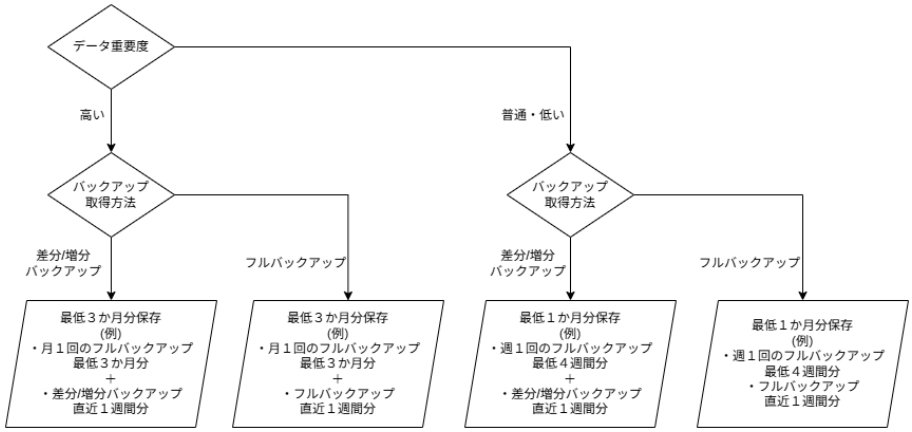


図 4.5 バックアップの世代管理の評価

バックアップ記録媒体

回答されたバックアップの記録媒体の数に応じて、複数の記録媒体でバックアップが取得されているかについて評価を行う。また、回答されたデータ更新頻度とデータサイズを基に図 4.6 の処理を行い、推奨される記録媒体について提示する。データ更新頻度が週 1 回以下でデータサイズが 100GB 以上の場合は、HDD、SSD、バックアップ用サーバ、磁気テープ、クラウドストレージを提示しており、データサイズが 100GB 未満の場合は、バックアップ用サーバと磁気テープを外し、ランサムウェアによる暗号化からデータを保護することができる書き換え不能な記録媒体を追加している。

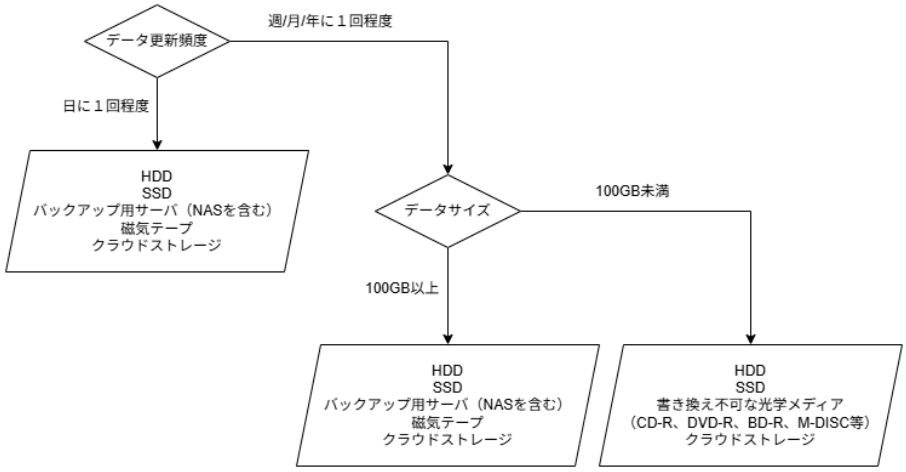


図 4.6 推奨される記録媒体の提示

バックアップ記録媒体のネットワーク接続状況

バックアップ記録媒体として、HDD、SSD、バックアップ用サーバ、磁気テープ、USB メモリ、SD カード、書き換え可能な光学メディアを使用している場合に回答してもうら項目である。「バックアップ時のみ情報機器などと接続し、取得後切り離している」と回答された場合は、バックアップへのランサムウェア感染拡大の対策が実施されていると評価する。「常時接続している」、「わからない」と回答された場合は、バックアップへのランサムウェア感染拡大への対策が実施されていないと評価し、バックアップ時のみ接続することを提示する。

クラウドストレージと情報機器のフォルダの同期設定

バックアップ記録媒体として、クラウドストレージを使用している場合に回答してもうら項目である。「同期されていない」と回答された場合は、バックアップへのランサムウェア感染拡大の対策が実施されていると評価する。「同期されている」「わからない」と回答された場合は、バックアップへのランサムウェア感染拡大の対策が実施されていないと評価し、同期しないように設定することを提示する。

バックアップのアクセス制御

「アクセス制御をしている」と回答された場合は、バックアップへの不正アクセスのリスクを低減させる対策が実施されていると評価する。「アクセス制御をしていない」「わからない」と回答された場合は、バックアップへの不正アクセスのリスクを低減させる対策が実施されていないと評価し、アクセス制御を実施することを提示する。

バックアップの暗号化

「暗号化している」と回答された場合は、攻撃者による窃取されたバックアップの悪用を防止する対策が実施されていると評価する。「暗号化していない」「わからない」と回答された場合は、攻撃者による窃取されたバックアップの悪用を防止する対策が実施されていないと評価し、暗号化を実施することを提示する。併せて、バックアップの暗号化を実施する手段として、暗号化ツールやバックアップソフトウェアを使用する方法があることを提示する。

バックアップからの復旧作業の手順の整備

「整備している」と回答された場合は、バックアップから早急な復旧を実現するための準備がされていると評価する。「整備していない」と回答された場合は、バックアップから早急な復旧を実現するための準備がされていないと評価し、復旧作業の手順を整備することを提示する。併せて、復旧作業の手順の項目例を提示する。

バックアップからの復旧訓練の実施

「年に 1 回程度実施している」と回答された場合は、バックアップからデータの復旧が可能であることの確認が行われていると評価する。「実施していない」と回答された場合は、バックアップからデータの復旧が可能であることの確認が行われていないと評価し、復旧訓練の実施を促している。

バックアップ前のデータのウイルスチェックの実施

「実施している」と回答された場合は、バックアップ時点でマルウェアに感染

していないかについての確認が実施されていると評価する。「たまに実施している」「実施していない」と回答された場合は、バックアップ時点でマルウェアに感染していないかについての確認が実施されていないと評価し、ウイルスチェックの実施を促している。

バックアップ後のデータの整合性の確認

「確認している」と回答された場合は、データの破損や取得漏れなどがないかの確認が実施されていると評価する。「たまに確認している」「確認していない」と回答された場合は、データの破損や取得漏れなどがないかの確認が実施されていないと評価し、データの整合性の確認の実施を促している。また、データの整合性の確認を実施する手段として、ファイルのハッシュ値を比較すること、バックアップソフトウェアの機能を利用すること、バックアップからデータを復元して元データと比較することがあることを提示している。

第 5 章
評　　価

5.1. 目的

前章で作成したアドバイスツールを使用することで、ランサムウェア対策として効果的なバックアップの要件が満たされているか評価可能であるか、満たされていない場合に具体的な対策例を提示することができているかについて確認する。

5.2. 方法

仮想の中小企業 2 社におけるバックアップ体制を設定し、アドバイスツールを使用して要件が満たされているかの評価や具体例の提示を試みる。仮想の中小企業 2 社の概要は、以下の通りである。

X 社

従業員規模は 5 名以下である。バックアップを取得しているデータは、見積書や契約書などの受発注に関する書類である。これらのデータは、業務用 PC に保存されている。なお、これらのデータは消失すると業務に多少の影響があるが、再作成が容易である。バックアップ対象のデータに関する情報と要件の実施状況に関する情報は、表 5.1 のとおり回答している。

Y 社

従業員規模は 6 ～20 名以下である。バックアップを取得しているデータは、顧客情報や請求書、契約書、画像・動画データなどがある。これらのデータは、クラウドストレージに保存されている。これらのデータは消失すると業務に影響が

あり、再作成が困難なものも含まれている。バックアップ対象のデータに関する情報と要件の実施状況に関する情報は、表 5.2 のとおり回答している。

表 5.1 X 社の回答内容

確認項目	回答
データのサイズ	1 GB～50GB 未満
データの更新頻度	日に 1 回程度
データの更新量	100MB 未満
データの重要度	普通（消失すると業務に影響がある、再作成が可能である）
データが保存されている機器のインターネット接続状況	インターネットに接続されている
バックアップの取得頻度	日に 1 回程度
バックアップの取得方法	増分バックアップ
バックアップの世代管理	実施していない（直近のバックアップのみ保存している）
バックアップ記録媒体	紙、その他（パソコンの D ドライブ）
バックアップ記録媒体のネットワーク接続状況	データが保存されている情報機器などと常時接続している
クラウドストレージと情報機器のフォルダの同期設定	非該当
バックアップのアクセス制御	バックアップの担当者だけなどにアクセス制御をしている
バックアップの暗号化	暗号化していない
バックアップからの復旧作業の手順の整備	整備していない
バックアップからの復旧訓練の実施	実施していない
バックアップ前のデータウイルスチェックの実施	実施していない
バックアップ後のデータの整合性の確認	たまに確認している

表 5.2 Y 社の回答内容

確認項目	回答
データのサイズ	100GB～500GB 未満
データの更新頻度	週に 1 回程度
データの更新量	1 GB 以上
データの重要度	高い（消失すると業務に大きな影響がある、再作成が困難である）
データが保存されている機器のインターネット接続状況	インターネットに接続されている
バックアップの取得頻度	月に 1 回程度
バックアップの取得方法	フルバックアップ
バックアップの世代管理	実施している（直近のバックアップだけではなく、数回分保存している
バックアップ記録媒体	HDD
バックアップ記録媒体のネットワーク接続状況	バックアップ時のみデータが保存されている情報機器などと接続し、取得後切り離している
クラウドストレージと情報機器のフォルダの同期設定	非該当
バックアップのアクセス制御	バックアップの担当者だけなどにアクセス制御をしている
バックアップの暗号化	暗号化していない
バックアップからの復旧作業の手順の整備	整備していない
バックアップからの復旧訓練の実施	実施していない
バックアップ前のデータウイルスチェックの実施	実施していない
バックアップ後のデータの整合性の確認	確認していない

5.3. 結果

5.3.1 X 社の結果

バックアップの取得頻度

適切な頻度でバックアップされていると評価された。回答内容に対して、意図していた結果となっていた。

バックアップの取得方法

増分バックアップを行っているが、データ更新量が少ないためフルバックアップでの取得が提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップの世代管理

データの重要度が高くないため、最低 1 か月分のデータを保存することが提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ記録媒体

バックアップ記録媒体を 2 種類使用しており、要件を満たしていると評価されていた。また、推奨される記録媒体として、HDD、SSD、バックアップ用サーバ、磁気テープ、クラウドストレージが提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ記録媒体のネットワーク接続状況

常時接続を行っていると回答しており、バックアップ時のみ接続するように提示されていた。回答内容に対して、意図していた結果となっていた。

クラウドストレージと情報機器のフォルダの同期設定

バックアップ記録媒体としてクラウドストレージを利用していないため、何も表示されていなかった。回答内容に対して、意図していた結果となっていた。

バックアップのアクセス制御

アクセス制御を実施していると回答しており、バックアップへの不正アクセスのリスクを低減させる対策が実施されていると評価されていた。回答内容に対して、意図していた結果となっていた。

バックアップの暗号化

実施していないと回答しており、バックアップの暗号化を実施することを提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップからの復旧作業の手順の整備

整備していないと回答しており、復旧作業の手順の整備を実施することを提示されていた。併せて、復旧作業の手順の項目例も提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップからの復旧訓練の実施

実施していないと回答しており、復旧訓練を実施することを提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ前のウイルスチェックの実施

実施していないと回答しており、バックアップ前にウイルスチェックを実施することを提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ後のデータ整合性の確認　たまに確認していると回答しており、データの整合性の確認を実施することが提示されていた。併せて、データの整合性の確認方法も提示されていた。回答内容に対して、意図していた結果となっていた。

5.3.2 Y 社の結果

バックアップの取得頻度

適切な頻度でバックアップされていると評価された。ただし、バックアップ必

要度に付与された値よりもデータ更新頻度に付与された値の方が大きいため、可能な場合はデータ更新頻度に合わせてバックアップを取得することが提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップの取得方法

フルバックアップを行っているが、データ更新量が 1 GB 以上あるため差分・増分バックアップでの取得も検討するように提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップの世代管理

データの重要度が高いため、最低 3 か月分のデータを保存することが提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ記録媒体

バックアップ記録媒体を 1 種類しか使用していないため、複数の種類の記録媒体を使用することが提示されていた。また、推奨される記録媒体として、HDD、SSD、バックアップ用サーバ、磁気テープ、クラウドストレージが提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ記録媒体のネットワーク接続状況

バックアップ時のみ接続していると回答しており、バックアップへのランサムウェアの感染拡大の対策が実施されていると評価されていた。回答内容に対して、意図していた結果となっていた。

クラウドストレージと情報機器のフォルダの同期設定

バックアップ記録媒体としてクラウドストレージを利用していないため、何も表示されていなかった。回答内容に対して、意図していた結果となっていた。

バックアップのアクセス制御

アクセス制御を実施していると回答しており、バックアップへの不正アクセス

のリスクを低減させる対策が実施されていると評価されていた。回答内容に対して、意図していた結果となっていた。

バックアップの暗号化

実施していないと回答しており、バックアップの暗号化を実施することを提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップからの復旧作業の手順の整備

整備していないと回答しており、復旧作業の手順の整備を実施することを提示されていた。併せて、復旧作業の手順の項目例も提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップからの復旧訓練の実施

実施していないと回答しており、復旧訓練を実施することを提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ前のウイルスチェックの実施

実施していないと回答しており、バックアップ前にウイルスチェックを実施することを提示されていた。回答内容に対して、意図していた結果となっていた。

バックアップ後のデータ整合性の確認

確認していないと回答しており、データの整合性の確認を実施することが提示されていた。併せて、データの整合性の確認方法も提示されていた。回答内容に対して、意図していた結果となっていた。

5.4. 考察

仮想の中小企業であるＸ社とＹ社のバックアップ取得状況に対してアドバイスツールを使用し、ランサムウェア対策として効果的なバックアップの要件が満た

されているか評価を行い、満たされていない場合に具体的な対策例を提示することができることを確認できた。

次のステップとして、実際の中小企業に使用してもらうことで、アドバイスツールの有効性を確認することが考えられる。具体的には、提示された対策方法に基づいてバックアップの取り方を要件を満たした方法に改善することが可能であるかについて、中小企業の方に評価してもらう必要がある。

また、実際の中小企業にアドバイスツールを使用してもらう中で、Google フォームで収集する情報の粒度を修正する必要性が生じる可能性がある。例えば、データ更新量について「100MB 未満」「100MB 以上〜 1 GB 未満」「 1 GB」以上の中から選択することになっているが、「 1 GB 以上」に回答が集中してしまい、 1 GB 以上でさらに選択肢を作成する必要性が生じることなどが考えられる。その場合、バックアップ体制が要件を満たしているかの判断基準についても見直すことが必要になる。

以上のことから、作成したチェックツールはバックアップ体制が要件を満たしているか評価し、満たしていない場合に具体的な対策例を提示することができたので、収集する情報の粒度の修正や要件を満たしているかの判断基準の見直しが必要になる可能性はあるものの、実際の中小企業に使用してもらい、有効性を評価してもらうことが可能であると考えられる。

第 6 章
結論と今後の課題

6.1. 結論

近年ランサムウェアによる被害が継続的に発生しており、被害組織の多くは中小企業となっている。ランサムウェアの被害にあった組織の多くでバックアップは取得されていたものの、バックアップも暗号化されてしまったことなどが原因となり、多くの組織でバックアップからデータの復号に失敗している。

まずは、官公庁がランサムウェア対策について紹介しているウェブサイトや公表資料、インターネット上で公開されているセキュリティ診断ツールを参照して、ランサムウェア対策として効果的なバックアップの要件を整理した。また、中小企業に聞き取り調査を行い、中小企業においてパソコンなどの情報機器が利用されていたが、セキュリティ対策の実施に課題があることや、バックアップを取得しているもののランサムウェア対策として取得することは意識しておらず、要件を満たしたバックアップ体制にはなっていないことが明らかとなった。また、要件のチェックリスト作成し、バックアップの体制が要件を満たしたものになっているか中小企業に確認してもらう調査を実施したところ、具体的な対策例を認識できた場合に、既存のバックアップ体制の改善を検討されようとしていた。

そこで本研究では、中小企業がランサムウェアの被害にあった場合にデータを復元することが可能となるように、要件を満たしたバックアップの取得が可能となることを支援するために、バックアップ対象のデータや要件の実施状況に関する情報から、バックアップ体制を評価するとともに、要件を満たしていない場合に具体的な対策例を提示するアドバイスツールを作成した。仮想の中小企業のバックアップ取得状況を対象に作成したアドバイスツールを使用したところ、バック

アップ体制が要件を満たしているか評価することや、満たしていない場合に具体的な対策例を提示することが可能であることを確認した。

6.2. 今後の課題

実際の中小企業にアドバイスツールを使用してもらい、提示された対策方法に基づいてバックアップの取り方を要件を満たした方法に改善することが可能であるかを中小企業の方に評価してもらうことで、チェックツールの有効性を確認することが考えられる。さらに、チェックツールを使用してもらった後で、バックアップをランサムウェア対策として効果的な要件を満たした方法に改善が行われたかについても、継続して調査することも考えられる。

また、アドバイスツールを使用した結果出力される内容について、生成 AI を活用することが考えられる。評価内容を要約したり、要件を満たしていない場合に提示する対策例を詳細に説明したりすることに生成 AI を活用できる可能性がある。

なお、中小企業のセキュリティ対策が十分に進んでいない要因として、資金不足や知識不足が挙げられるものの、最大の要因はセキュリティ対策への関心が低いことである。そのため、中小企業に要件を満たしたバックアップを取得してもらい、仮にランサムウェアの被害にあった場合でも被害を最小限に抑えることができるようにするためには、作成したチェックツールをどのように中小企業に認識してもらい、使用してもらうことに繋げるかについても検討する必要がある。

謝　　辞

本研究の指導教員であり、幅広い知見から的確な指導と暖かい励ましやご指摘をしていただきました慶應義塾大学大学院メディアデザイン研究科の砂原秀樹教授に深謝いたします。

研究指導や論文執筆など数多くの助言を賜りました慶應義塾大学大学院メディアデザイン研究科の加藤朗教授に心より感謝申し上げます。

本論文作成に当たり、副査としてご助言を賜りました慶應義塾大学大学院メディアデザイン研究科の杉浦一徳教授に心より感謝申し上げます。

研究の方向性について助言や指導をいただきました慶應義塾大学大学院メディアデザイン研究科の南澤孝太教授に心より感謝申し上げます。

研究についてご相談させていただいた際に、親身になってご助言いただきました花田様、千葉様に心より深く感謝いたたします。

実際の被害事例について詳細なヒアリングにご協力いただいた皆様に心より深く感謝いたします。

本研究は、中小企業の皆様に聞き取り調査へご協力いただくことなくして実現しませんでした。お忙しい中、調査にご協力いただいた皆様に厚く御礼申し上げます。

参 考 文 献

[1] 独立行政法人情報処理推進機構. 情報セキュリティ10大脅威. https://www.ipa.go.jp/security/10threats/index.html. (2024/12/18 アクセス).

[2] 警察庁. サイバー空間をめぐる脅威の情勢等. https://www.npa.go.jp/publications/statistics/cybersecurity/index.html. (2024/12/18 アクセス).

[3] 中小企業庁. 中小企業・小規模企業者の定義. https://www.chusho.meti.go.jp/soshiki/teigi.html. (2024/12/18 アクセス).

[4] 独立行政法人情報処理推進機構. 2021年度中小企業における情報セキュリティ対策に関する実態調査－調査報告書－, 2022.

[5] 日本政策金融公庫総合研究所. 中小企業に求められるサイバーセキュリティ対策の強化, 2022.

[6] 独立行政法人情報処理推進機構. SECURITY ACTIONとは？: SECURITY ACTION セキュリティ対策自己宣言. https://www.ipa.go.jp/security/security-action/sa/. (2025/1/31 アクセス).

[7] 独立行政法人中小企業基盤整備機構. 新規申請・手続きフロー詳細 | it導入補助金2025. https://it-shien.smrj.go.jp/applicant/flow/. (2025/1/31 アクセス).

[8] 東京都産業労働局. 東京都の取組. https://www.cybersecurity.metro.tokyo.lg.jp/torikumi/#page1. (2025/1/31 アクセス).

[9] 東京都産業労働局. 中小企業のセキュリティ機器の活用や規程策定等を後押しします！ https://www.cybersecurity.metro.tokyo.lg.jp/torikumi/516/. (2025/1/31 アクセス).

[10] 東京都産業労働局. セキュリティ対策に取り組む中小企業の人材育成・社内体制整備を支援します！ https://www.cybersecurity.metro.tokyo.lg.jp/torikumi/510/. (2025/1/31 アクセス).

[11] 独立行政法人情報処理推進機構. 5 分でできる！情報セキュリティ自社診断, 2024.

[12] 三井住友海上火災保険株式会社. サイバー保険 簡易リスク診断 MS&AD サイバーセキュリティ基本態勢診断. https://www.ms-ins.com/business/indemnity/pd-protector/diagnosis.html. (2024/12/18 アクセス).

[13] US-CERT. Data backup options, 2012.

[14] 日経 BP. 日経コンピュータ 2021 年 4 月 15 日号, pp. 24–27.

[15] 警視庁. マルウェア「ランサムウェア」の脅威と対策（対策編）. https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html. (2024/12/18 アクセス).

[16] 独立行政法人情報処理推進機構. ランサムウェアの脅威と対策～ランサムウェアによる被害を低減するために～, 2017.

[17] 日本銀行金融機構局, 金融庁総合政策局. 地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2022 年度）, 2023.

[18] バラクーダネットワークスジャパン株式会社. 日本の中小企業におけるサイバーレジリエンス vol.2 「人」がセキュリティの成功の鍵を握る, 2024.

[19] 田中啓介, 古川佳和, 野田幹稀, 上原哲太郎ほか. 中小企業における情報セキュリティ対策状況のインタビュー調査. 研究報告インターネットと運用技術 (IOT), Vol. 2022, No. 43, pp. 1–8, 2022.

[20] 菅原颯真, 田中啓介, 榎竜盛, 木村悠生, 上原哲太郎ほか. Wordpress に着目した中小企業におけるセキュリティ対策の実態調査. コンピュータセキュリティシンポジウム 2023 論文集, pp. 567–574, 2023.

付　　録

A. アドバイスツールの使用結果

第５章で仮想の中小企業２社にアドバイスツールを使用した結果が出力されたテキストファイルの内容を掲載する。

X 社

●バックアップの取得頻度
回答:
- バックアップ必要度: 50
- データ更新頻度: 日に 1 回程度（ 50 ）
- バックアップの取得頻度: 日に 1 回程度（ 50 ）

評価結果:
適切な頻度でバックアップが取得できています。

(注) バックアップ必要度の説明:
バックアップ必要度は以下の要素から計算される総合評価です：
バックアップ必要 = データ更新頻度 + データサイズ + データ更新料 + データ重要度 + インターネット接続状況
- データ更新頻度: {'日に 1 回程度': 50, '週に 1 回程度': 40, '月に 1 回程度': 30, '年に 1 回程度': 20, '不定期': 10}
- データサイズ: {' 1 GB 未満': 0, ' 1 GB～50GB 未満': 0, '50GB～100GB 未満': 0, '100GB～500GB 未満': -10, '500GB～1TB 未満': -10, '1TB 以上': -10}
- データ更新量: {'100MB 未満': 0, '100MB～ 1 GB 未満': 0, ' 1 GB 以上': -10}
- データ重要度: {' 高い（消失すると業務に大きな影響がある、再作成が困難である）': 10, ' 普通（消失すると業務に影響がある、再作成が可能である）': 0, ' 低い（消失しても業務への影響は軽微である、再作成が可能である）': -10}

- インターネット接続状況: {'インターネットに接続されている': 0, 'インターネットに接続されていない': -10}
※ 合計値の上限は 50 点に設定されています

●バックアップ方法
回答:
- バックアップ方法: 増分バックアップ
- データ更新頻度: 日に 1 回程度
- データ更新量: 100MB 未満

評価結果:
データ更新量が少ないため、フルバックアップで取得することも考えられます。

●バックアップの世代管理について
回答:
- バックアップの世代管理: 実施していない（直近のバックアップのみ保存している）
- データ重要度: 普通
- バックアップ方法: 増分バックアップ

評価結果:
データ重要度は高くないので、最低 1 か月分のデータを保存してください。
例: 週 1 回のフルバックアップ 4 週間分と増分バックアップ直近 1 週間分を保存
※バックアップ記録媒体のストレージ容量を考慮して、最終的に保存期間を決めてください。

●バックアップ記録媒体
回答:
- j. 紙
- パソコンの D ドライブ

評価結果:
バックアップが複数の記録媒体で取得されており、バックアップ記録媒体の故障やランサムウェアによる暗号化などへの対策が実施されています。

推奨される記録媒体:
- データ更新頻度: 日に 1 回程度

- HDD、SSD、バックアップ用サーバ(NASを含む)、磁気テープ、クラウドストレージ
※クラウドストレージを利用する場合は、セキュリティやストレージ容量に注意してください。

●バックアップ記録媒体のネットワーク接続状況
回答:
データが保存されている情報機器などと常時接続している

評価結果:
感染した情報機器からランサムウェアの感染が拡大し、バックアップも暗号化されることを防ぐため、バックアップ時のみ情報機器と接続するようにしてください。

●バックアップのアクセス制御
回答:
バックアップの担当者だけなどにアクセス制御をしている

評価結果:
バックアップへのアクセス制御が行われており、バックアップへの不正アクセスのリスクを低減させる対策が実施されています。

●バックアップの暗号化
回答: 暗号化していない

評価結果:
バックアップの暗号化を行うことで、攻撃者にバックアップを窃取された場合に悪用を防止する対策を実施してください。
バックアップの暗号化は、暗号化ツールやバックアップソフトウェアを使用することで実施可能です。

●バックアップからの復旧作業の手順の整備
回答:
整備していない

評価結果:
バックアップからの復旧作業の手順の整備をすることで、バックアップからの早急な復旧を実現するための準備をしてください。

(参考) 復旧作業の手順の項目例
・マルウェアに感染しているバックアップで復旧し、再度暗号化されてしまうことがないように、バックアップデータをウイルス対策ソフトでスキャンする。
・復旧を試みる段階で仮に原因が不詳である場合など、その時点で検知できないマルウェアに感染していることを考慮し、仮想環境や開発環境にて復旧を試行する。
出典：日本銀行金融機構局，金融庁総合政策局『地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果』(2023)

●バックアップからの復旧訓練の実施
回答:
実施していない

評価結果:
復旧訓練を年に 1 回程度実施することで、バックアップからデータの復旧が可能であることの確認を行ってください。

●バックアップ前のウイルスチェックの実施
回答:
実施していない

評価結果:
バックアップ前にウイルスチェックを実施することで、バックアップ時点でマルウェアに感染していないかについて確認を実施してください。

●バックアップ後のデータ整合性の確認
回答:
たまに確認している

評価結果:
バックアップ後にデータの整合性を確認することで、データの破損や取得漏れなどがないかの確認を実施してください。

(参考) データの整合性の確認方法
・ファイルのハッシュ値を比較する。
・バックアップソフトウェアの機能を利用する。

・バックアップからデータを復元し、元データと比較する。

Y 社

●バックアップの取得頻度
回答:
- バックアップ必要度: 30
- データ更新頻度: 週に 1 回程度 （ 40 ）
- バックアップの取得頻度: 月に 1 回程度 （ 30 ）

評価結果:
適切な頻度でバックアップが取得できています。

提案:
可能な場合は、月に 1 回程度バックアップを取得することを検討してください。

(注) バックアップ必要度の説明:
バックアップ必要度は以下の要素から計算される総合評価です：
バックアップ必要 = データ更新頻度 + データサイズ + データ更新料 + データ重要度 + インターネット接続状況
- データ更新頻度: {'日に 1 回程度': 50, '週に 1 回程度': 40, '月に 1 回程度': 30, '年に 1 回程度': 20, '不定期': 10}
- データサイズ: {' 1 GB 未満': 0, ' 1 GB〜50GB 未満': 0, '50GB〜100GB 未満': 0, '100GB〜500GB 未満': -10, '500GB〜1TB 未満': -10, '1TB 以上': -10}
- データ更新量: {'100MB 未満': 0, '100MB〜 1 GB 未満': 0, ' 1 GB 以上': -10}
- データ重要度: {' 高い（消失すると業務に大きな影響がある、再作成が困難である）': 10, ' 普通（消失すると業務に影響がある、再作成が可能である）': 0, ' 低い（消失しても業務への影響は軽微である、再作成が可能である）': -10}
- インターネット接続状況: {' インターネットに接続されている': 0, ' インターネットに接続されていない': -10}
※ 合計値の上限は 50 点に設定されています

●バックアップ方法
回答:
- バックアップ方法: フルバックアップ
- データ更新頻度: 週に 1 回程度

- データ更新量: 1 GB 以上

評価結果:
データ更新量が 1 GB 以上あるので、差分または増分バックアップが適している場合があります。
ただし、データ更新頻度が低く、バックアップ記録媒体の容量が十分ある場合は、フルバックアップの取得で問題ありません。

●バックアップの世代管理について
回答:
- バックアップの世代管理: 実施している（直近のバックアップだけではなく、数回分保存している）
- データ重要度: 高い
- バックアップ方法: フルバックアップ

評価結果:
データ重要度が高いので、最低 3 か月分のデータを保存してください。
例: 月 1 回のフルバックアップ 3 か月分とフルバックアップ直近 1 週間分を保存
※バックアップ記録媒体のストレージ容量を考慮して、最終的に保存期間を決めてください。

●バックアップ記録媒体
回答:
- a. HDD

評価結果:
バックアップが 1 つの記録媒体のみで取得されています。
既存のバックアップ記録媒体の故障やランサムウェアによる暗号化などへの対策として、他の記録媒体でもバックアップを取得することを検討してください。

推奨される記録媒体:
- データ更新頻度: 週に 1 回程度 、データサイズ: 100GB～500GB 未満
- HDD、SSD、バックアップ用サーバ (NAS を含む)、磁気テープ、クラウドストレージ
※クラウドストレージを利用する場合は、セキュリティやストレージ容量に注意してください。

●バックアップ記録媒体のネットワーク接続状況
回答:
バックアップ時のみデータが保存されている情報機器などと接続し、取得後切り離している

評価結果:
バックアップ時のみ情報機器と接続されており、情報機器からのランサムウェア感染拡大の対策が実施されています。

●バックアップのアクセス制御
回答:
バックアップの担当者だけなどにアクセス制御をしている

評価結果:
バックアップへのアクセス制御が行われており、バックアップへの不正アクセスのリスクを低減させる対策が実施されています。

●バックアップの暗号化
回答: 暗号化していない

評価結果:
バックアップの暗号化を行うことで、攻撃者にバックアップを窃取された場合に悪用を防止する対策を実施してください。
バックアップの暗号化は、暗号化ツールやバックアップソフトウェアを使用することで実施可能です。

●バックアップからの復旧作業の手順の整備
回答:
整備していない

評価結果:
バックアップからの復旧作業の手順の整備をすることで、バックアップからの早急な復旧を実現するための準備をしてください。

(参考) 復旧作業の手順の項目例
・マルウェアに感染しているバックアップで復旧し、再度暗号化されてしまうことがない

ように、バックアップデータをウイルス対策ソフトでスキャンする。
・復旧を試みる段階で仮に原因が不詳である場合など、その時点で検知できないマルウェアに感染していることを考慮し、仮想環境や開発環境にて復旧を試行する。
出典：日本銀行金融機構局，金融庁総合政策局『地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果』(2023)

●バックアップからの復旧訓練の実施
回答：
実施していない

評価結果：
復旧訓練を年に 1 回程度実施することで、バックアップからデータの復旧が可能であることの確認を行ってください。

●バックアップ前のウイルスチェックの実施
回答：
実施していない

評価結果：
バックアップ前にウイルスチェックを実施することで、バックアップ時点でマルウェアに感染していないかについて確認を実施してください。

●バックアップ後のデータ整合性の確認
回答：
確認していない

評価結果：
バックアップ後にデータの整合性を確認することで、データの破損や取得漏れなどがないかの確認を実施してください。

(参考) データの整合性の確認方法
・ファイルのハッシュ値を比較する。
・バックアップソフトウェアの機能を利用する。
・バックアップからデータを復元し、元データと比較する。