システム監査学会
2019年度　「情報セキュリティ対策の診断」研究プロジェクト　報告

クラウドサービスの活用と評価に関する調査研究
（Study to utilization and evaluation of cloud service）

研究中間成果物
クラウド導入への実践的課題と検討内容

＜別紙資料＞
添付資料１　ガイドライン一覧

研究期間　2019 年 7 月～2020 年 5 月
報告書作成　2020 年 5 月 29 日

この資料の内容は発表者個人及び研究プロジェクトメンバーの見解です。
発表者個人及び研究プロジェクトメンバーの所属組織等とは関係ありません。

研究プロジェクト主査　木村　裕一
研究プロジェクトメンバー
尾崎　孝章（株式会社デンカク）、
赤尾　嘉治（経営情報学会会員、元 ISMS・QMS 主任審査員）、
牧野　博文（株式会社東芝 IT ストラテジスト、システム監査技術者、IT コーディネータ、
情報処理安全確保支援士,CISA）

ご質問、お問い合わせは、システム監査学会経由でチーム主査までご連絡ください。
問合せフォーム　→ https://www.sysaudit.gr.jp/toiawase/index.html
連絡先：システム監査学会　→ https://www.sysaudit.gr.jp
〒106-0032　東京都港区六本木１丁目 9-9　六本木ファーストビル　JIPDEC 内

目次

I. 総論

はじめに

「情報セキュリティ対策の診断」研究プロジェクトでは、2015 年に ISO270017 が発行された事を踏まえ、中小企業に安全でセキュアなクラウドの利用普及と促進につなげる事を目的としてクラウドセキュリティのチェックリストなどを提供する事を検討した。

検討の結果、クラウドの利活用の促進につながるチェックリストだけでなく、必要に応じて関連資料も提供するなどを模索する事も検討してきた。

チェックリストを提供する上では、提供目的や提供先である中小企業のおかれている市場動向を踏まえて、何をチェックするのかについて明確化する事も検討する事とした。具体的には、中小企業の動向や経営者にとってのサイバーセキュリティリスクの認識などである。

当研究プロジェクトでは中小企業の方々がクラウドサービスの導入に当たり、実際に直面する問題を調査し、検討した結果を以下の項目でまとめたのである。

Ⅰ. 総論
Ⅱ. 導入手順
・クラウド導入の流れと、各局面の留意事項、潜在的リスクの認識
Ⅲ. 対象業務の選定
・クラウド導入における対象業務の選定と留意事項
Ⅳ. ITガバナンス
・クラウド導入に当たって求められるITガバナンス
Ⅴ. 維持管理
・クラウド維持管理と企業目標達成への取り組み方
Ⅵ. チェックリスト
・クラウド導入される企業向けクラウド移行のチェックリスト

6つのテーマはそれぞれ独立して利用することもできるし、全てをまとめてクラウド導入の実践的のマニュアルとしても利用することもできることを意図して構成してある。

1. クラウドの定義

平成30年総務省情報通信白書[※1]によると、下記の様に定義されている。
クラウドとは「クラウドコンピューティング（Cloud Computing）」を略した呼び方で、データやアプリケーション等のコンピューター資源をネットワーク経由で利用する仕組みのことである。今やスマートフォンや携帯電話を使って、メールをやり取りしたりゲームをしたりすることは当たり前になっている。しかし、これらのアプリケーションは、スマートフォンや携帯電話上だけで動作しているのではない。ネットワークでつながるデータセンターと呼ぶ大規模施設に置かれたサーバーやストレージ、各種のソフトウェアなどと連携することで、電子メールやゲームといった“サービス”が実現されている。ネットワークにつながった PC やスマートフォン、携帯電話などにサービスを提供しているコンピューター環境がクラウドである。クラウドが提供するサービスは、その構成要素から大きく下記の3種類がある。

（1）IaaS（Infrastructure as a Service）：サーバー（インフラ）を提供するクラウドサービス
（2）PaaS（Platform as a Service）：開発環境を提供するクラウドサービス
（3）SaaS（Software as a Service）：ソフトウェアを提供するクラウドサービス

2. 中小企業におけるクラウド利活用の課題

現在クラウドの利活用の動向は、総務省から発行されている「通信利用動向調査※1-2」が平成25年から実施されている。

また、平成28年度、平成30年度の総務省発行の情報通信白書※1の第3節「組織をつなぐ事で生産性向上をもたらすICT」にて、クラウドサービスの国内利用状況の調査が行われている。

情報通信白書の調査※1では、クラウドサービスの種類として、IaaS/PaaS/SaaS、パブリッククラウドとプライベートクラウドを合わせた調査が実施された。その中で、クラウドサービスを利用する目的として、①システムを構築の迅速さ、②初期費用・運用費の削減、③可用性の向上、④利便性の向上が挙げられている。

利用状況としては、一定規模以上の企業は情報システムに投資をしてサービス基盤を整備するのが一般的であり、一方で資金力が十分でない企業は情報システムを業務に利活用することが困難であった。

全体の設備投資額に占めるソフトウェア投資比率を見ると、大企業が 10%程度であるのに対し、中小企業では 4%程度と、大企業の方がソフトウェア投資割合は高い」結果となっている。

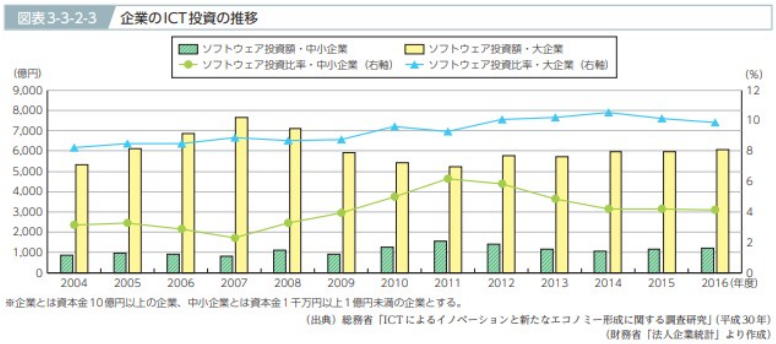

図 1: 企業の ICT 投資の推移（情報通信白書）

また、”クラウドサービス未導入者に対してクラウドサービスの課題に対する認識を聞いたところ、日本企業においては「課題がわからない」という回答が諸外国と比較して大きな割合を占めている。我が国企業においてクラウドサービスの導入が進まない背景には明確な課題が認識されているわけではなく、どのような課題があるかも認識されていない状況にあることが示唆される”と指摘されている。

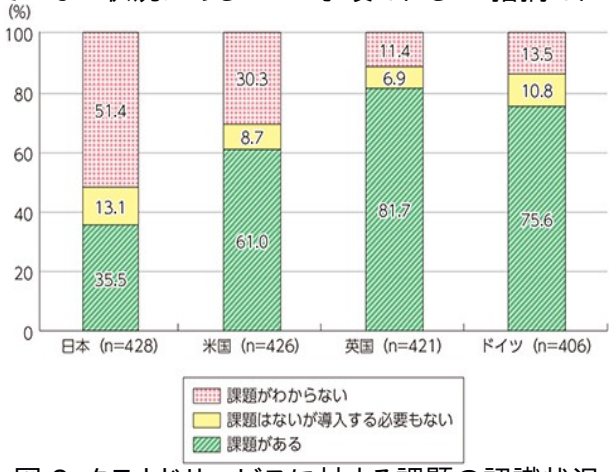

図 2: クラウドサービスに対する課題の認識状況

また、「クラウドサービス未導入者が認識している課題の内容としては、全調査対象国においてセキュリティの担保に関する項目の回答率が高くなっている。特に日本企業においては他の項目と比較してセキュリティの不安に対する回答率が高く、API 公開と同様にセキュリティ面への不安は依然強いことがわかる」　とされている。

上記の結果を検討した結果、当研究プロジェクトとしては、下記の課題があるものとして検討を進めた。

- 中小企業向けにクラウドサービス導入がすすまない課題の明確化
- 中小企業のクラウド導入に伴うセキュリティ面の不安解消のためのリスクと対策の明確化

3. 中小企業でのクラウドの利活用の状況

本研究プロジェクトでは、クラウドサービスの課題やセキュリティリスクを明確化するため、どのような業種で効果があるのかを確認した。

中小企業とクラウドの概況について、通信利用動向調査※1−2で詳細な調査が行われている。 現在、大企業を含む全業種の調査では、およそ3割の企業が「全社的に利用」しており、 一部の利用している企業、利用していないが今後利用する予定があるを含めると、過去3年において増加しており、最新の平成29年度の状況では7割近い状況で、多くの企業で利用されている結果となった。

利用希望まで含めると情報通信産業ではおよそ9割が利用予定であり、不動産業、金融業でも8割となっており、建設業やその他サービス業でも7割を越える程度となっており、最も低いサービス業でも6割5分が利用予定となっている。

表 1: 業種別クラウドサービスの利用状況

単位：%

	集計企業数	クラウドサービスの利用状況							
		利用している	全社的に利用している	一部の事業所又は部門で利用している	利用していない	利用していないが、今後利用する予定がある	利用していないし、今後も利用する予定もない	クラウドサービスについてよく分からない	無回答
全体	2,592	56.3	29.1	27.2	35.2	13.2	21.9	7.6	1.0
[産業分類]									
建設業	311	57.2	32.9	24.2	35.5	14.2	21.3	7.0	0.4
製造業	379	57.1	25.7	31.4	37.0	16.7	20.3	4.9	1.0
運輸業・郵便業	325	48.6	22.5	26.1	40.1	13.8	26.3	9.9	1.4
卸売・小売業	312	57.3	34.6	22.7	36.9	13.8	23.1	4.8	1.0
金融・保険業	138	70.4	41.9	28.5	29.6	10.6	19.0	−	−
不動産業	139	68.3	41.9	26.4	24.9	12.9	11.9	5.2	1.7
情報通信業	644	78.1	50.8	27.4	19.3	10.5	8.7	2.1	0.5
サービス業、その他	344	52.6	25.3	27.3	34.0	10.2	23.8	12.2	1.2

また、同調査における、資本規模や従業員数による調査結果を分析すると下図の様になった。
中小企業の定義では資本金が1億円や3億円、大企業以外ととらえる場合もあるなど定義がいくつか存在している。その上で、資本金5億円未満あるいは1億円未満の平均を取ると、「利用している」、「利用していないが今後利用する予定がある」割合が過半数を超えており、「クラウドサービスについてよくわからない」と回答している企業が多い場合でも2割を満たない事から、中小企業の多くは、利用しているとは言えないまでも、クラウドが分からない可能性は低いと言わざる負えない事が分かった。

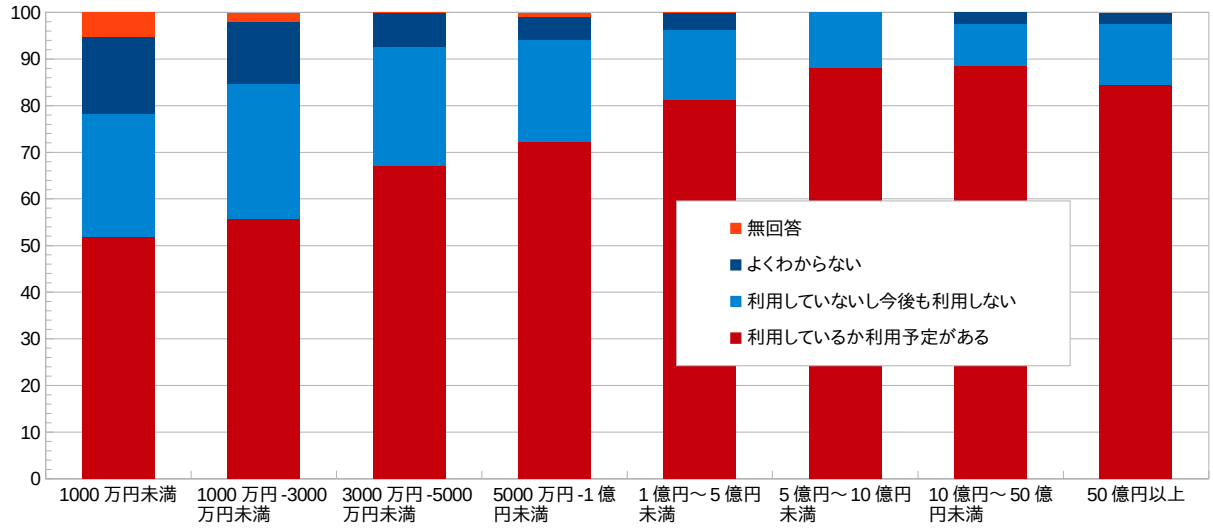

図 3: 資本金別クラウド利用状況

上図の分析を踏まえ、中小企業におけるクラウド利活用の状況を分析した結果、クラウドが分からない可能性が低い事から、下記の状況であるとした。

- 中小企業の多くが既にクラウドを経験済み

更に、2014年度の調査結果にはなるが、中小企業の事業者別事業者数の中でサービス業は1,574,494 者であり、全産業の41%となっている。
業種の定義が異なるものの、中小企業の4割がサービス業であり、サービス業のクラウド利用が6割5分を超えている事を考えると、サービス業向けのチェックリスト効果が最も大きいと考えられた。
その結果を踏まえて、下記の様な業種を対象とする事とした。

- 対象業種をサービス業を中心とした業種とできるかどうか検証する。

4.サービス業の分類

前述のサービス業にあたる定義について中小企業庁の定義※1−3によると、下記の様になっている。
①. 情報通信業:「放送業」、「情報サービス業」、「映像情報制作・配給業」、「音声情報制作業」、「広告制作業」、「(映像・音声・文字情報制作に附帯するサービス業」
②. 不動産業、物品賃貸業:「駐車場業」、「物品賃貸業」、
③. 学術研究
④. 専門・技術サービス業、宿泊業・飲食サービス業のうち、宿泊業、旅行業以外の「(生活関連サービス業、娯楽業」、
⑤. 教育、学習支援業、
⑥. 医療・福祉、複合サービス業、
⑦. その他サービス業となっている。
サービス業の定義は広域の業務となっており、放送業から学術研究、宿泊業、医療まで含まれている。

例えば宿泊業の通常のシステムアーキテクチャを考える場合、観光庁の「宿泊施設予約通知フォーマット標準化事業」※1−5などと連動した PMS(Property Management System)や GDS(Global Distribution System),CDS(Computer/Central Reservation System)などとの連携が重要なテーマとなってくると推定される。

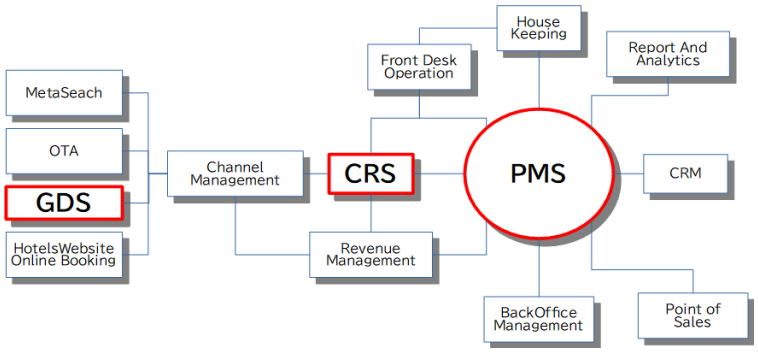

図 4:CDS、GDS システム構成※1−4

一方で製造業向けのシステムとしては、下図の製品ライフサイクル※1−6のアーキテクチャに企画・開発・生産準備・生産・輸送・配送・保守・廃棄等とシステムが構築される事が多く、一般的に考えて当然 PMS との相関は見られない。

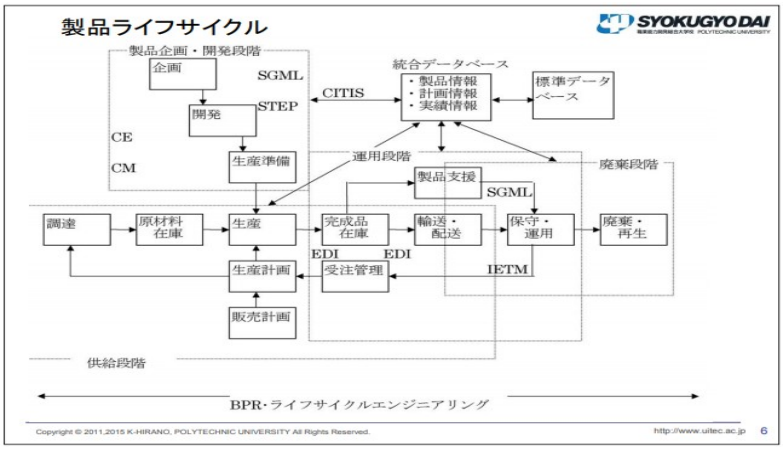

図 5: 製品ライフサイクルの対象プロセス

このように、サービス業内の各分野で主要なシステムや機能であっても、広域にわたり調査され取得可能な統計上の定義はより広いため、各分野の主要なシステムであってもサービス業全体を網羅しているとは考えにくいことがわかる。

今回の目的は、クラウドセキュリティの利活用を評価する事により、中小企業のクラウド利用上のリスクを低減させ、セキュリティの高いクラウドの利活用を促進することである。 中小企業で利用の多いシステムに特化する方向であるが、業務システムに特化するよりも、*メールやファイル共有のようなどのサービス業でも利用されいるか、あるいは経理や人事関連システムなどの共通性の高いシステムであることが望ましい*と考えられる。

上記結果を踏まえて、次の様に検討を進めるとする事とした。

- クラウドサービスの課題とセキュリティリスクは、対象業種をサービス業に特定せず、業種に関わらない共通業務に利用できるクラウドサービスの課題とセキュリティリスクについて研究を進める

5. 利用されているクラウドサービスの種類

具体的なクラウドサービスの課題を調査するため、実際に利用されいるクラウドを調査した。
総務省「通信利用動向調査[※1−2]」によれば、ファイル保管では50.2%、サーバ利用46.7%、電子メールが45%、社内共有が37%となっている。

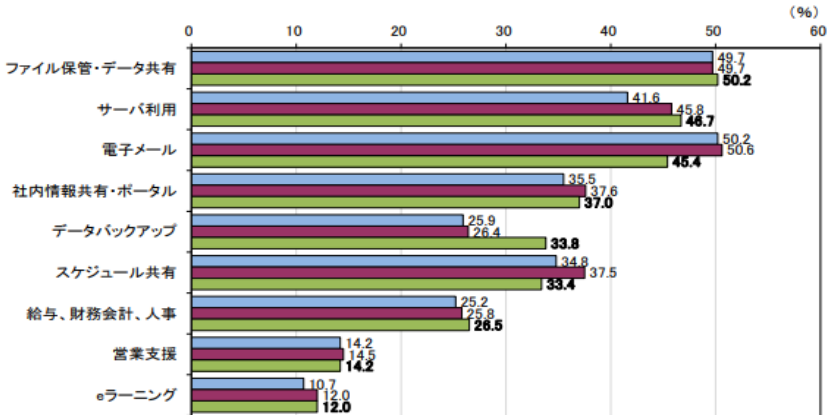

図 6: クラウド利用サービス分類

一方、利用しない企業においては、「必要がない」が39.3%であり、情報漏洩などセキュリティに不安があるが37.3%と次いでいる。
しかし、利用企業においては、サービスの信頼性や情報漏洩へのセキュリティが高い効果が得られたと答える企業が29%もあり、セキュリティが効果とセキュリティリスクの相反する2面性がある事が明らかとなった結果となった。

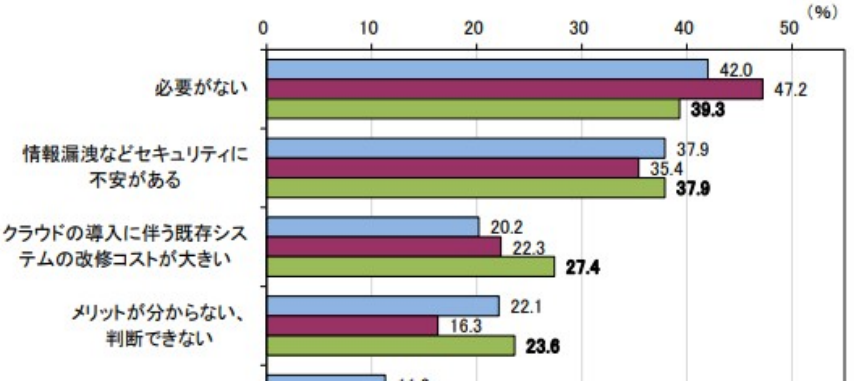

図 7: クラウドの必要性

この結果を踏まえて、次の様に検討を行う事とした。

- メールやファイルサーバ等の共通的に利用されるクラウドサービスを対象にする。
- クラウド利用上のリスクとクラウドセキュリティの正しい情報提供について確認する。

6. サイバーセキュリティ対策への投資に対する認識の状況

2019 年4月に発表された、「サイバー保険に関する調査 2018[※6]」では、「サイバーセキュリティの観点から対応が必要なもの」として、「クラウドコンピューティングの普及」(56.2%)と「サイバーテロの増加・巧妙化」(52.2%)が 50%を超えているとされており、上述のクラウドセキュリティに対するリスクとしての意識の高さと同様の傾向がみられた。

6.1.サイバーセキュリティ事故による企業イメージの低下意識が少ない中小企業

50人未満の従業員数の企業で、サイバーセキュリティ事故により想定される自社への影響として「企業イメージの低下」が54.4%となっており1000人以上大企業の96.4%と比べて4割も低いことがアンケートの結果で明らかとなった。

6.2. サイバーリスクに対する専門部署の設置・人材育成が少ない中小企業

「サイバーリスクに対する現在の対応状況 」としては、従業員50人未満の企業では、セキュリティ専門部署の設置は6.2%にとどまり、「サイバーセキュリティ人材の育成・採用」は4.6%にとどまっている。 「外部専門家からの助言を受ける」対策も20.2%となっており、大企業の58.0%と比較すると半分にも満たない状況となっている。

6.3.セキュリティ専門部署設置や外部専門家の助言相談の意欲は高い中小企業

50人未満の企業で、今後のサイバーセキュリティ対策としての対策意欲は軒並み高い事がうかがえる。例えば、「サイバーセキュリティ人材の育成・採用」21.6%であり、現状認識の4.6%と比べると5倍になっており、「外部専門家からの助言を受ける」も30.0%となっており、現状の20.2%と比べると1割高い結果となった。

6.4. 自社のサイバーセキュリティ対策の充足度が「わからない」中小企業

サイバーセキュリティ対応の充足度については、50人未満の企業では「わからない」が60%を越えており、「十分である」の5.5%の10倍になっている。

これは、50人未満の経営者の多くが、セキュリティ対策の必要性は認識しており、対策を実施したいものの、よくわからない状況になっているのではないかと推察される。

企業規模が大きくなるほど、サイバーセキュリティ対応の充足度について自覚的に認識している傾向がある事から、サイバーセキュリティについての認知を深める活動の必要性が高いと推定される。

この結果を踏まえて、本プロジェクトでは中小企業の現状を次の様に分析した。

【中小企業におけるクラウド利用の現状】
- 中小企業の多くが既にクラウドを経験済み
- 中小企業の多くがメールやファイルサーバ等の業種に依存しない共通サービスの本格的利用を実際に導入しているか検討している。
- 中小企業の多くがサイバーセキュリティ専門部署の設置・人材育成が進んでいない。
- 中小企業の多くが外部の専門家への相談意欲は高いが、助言を受けたことは少ない。
- セキュリティ対策の必要性は認識しており、対策を実施したいものの、よくわからない状況になっている

Ⅱ. 導入手順

1. クラウド導入の全体像の俯瞰

クラウドサービスの全体的な俯瞰を下図にように見てみる。ステークホルダーが網羅されているか確認する。

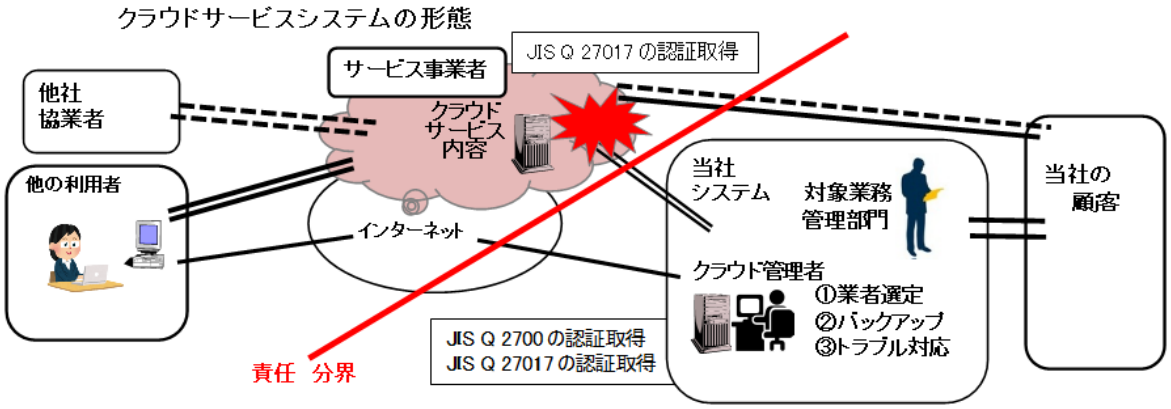

図 8: クラウドサービスの形態

2. クラウド化に伴う組織向けの攻撃の脅威

2. 1. 企業等の組織向け攻撃の脅威

サイバーセキュリティの脅威は年々複雑・巧妙になってきている。サイバー攻撃による被害は、顧客や従業員の個人情報の漏えい、ウイルスや詐欺メールによるハッキング被害、Web サイトの改ざんや妨害によるサービス停止、スマホ決済の不正利用など、金銭的な要求をする人質的・脅迫犯罪、など多岐にわたっている。攻撃者の目的は個人情報や機密情報の取得、金銭を得る、営業・サービスの妨害などさまざまな内容へと変化している。

「情報セキュリティ 10 大脅威 2020」[※2−1](組織向けの脅威)　　独立行政法人情報処理推進機構(IPA)が公表されているので自社で想定される被害、影響について下記に記載して、確認しておくことが望ましい。

表 2: 組織向けの脅威

	脅威	倒産の有無	売上激減	顧客離れ
1 位	標的型攻撃による被害			
2 位	ビジネスメール詐欺による被害			
3 位	ランサムウェアによる被害			
4 位	サプライチェーンの弱点を悪用した攻撃の高まり	影響大		
5 位	内部不正による情報漏えい		影響大	
6 位	サービス妨害攻撃によるサービスの停止			影響大
7 位	インターネットサービスからの個人情報の窃取			
8 位	IoT 機器の脆弱性の顕在化			
9 位	脆弱性対策情報の公開に伴う悪用増加			
10 位	不注意による情報漏えい			

脅威に備えるには、ウイルス対策以外にも、ランサムウェア、フィッシングメール、悪意のあるサイトへの誘導、脆弱性の放置、ファイル転送による情報の流出、USB デバイスを使う不正なデータコピー、ソフトの誤操作、印刷ドキュメントによる持ち出しなどに対しても、ガードを固める

必要がある。最近の事例を見ると、内部関係者による情報持ち出し、不正・犯行も起きることを前提にせざるを得ない。

2.2. クラウドサービスにおける事故事例

クラウドサービスの事故事例でWeb上で紹介されているのは下記のものがある。

① レンタルサーバー・クラウドサービス事業者
・5000 件を超える顧客データが消失
・事業者側のシステムメンテナンスの作業ミスが原因
・バックアップは同一サーバー内に取得

② ファイル転送サービス事業者
・480 万件を超える利用者の個人情報とログイン情報が漏えい
・サーバーの脆弱性に対するサイバー攻撃が原因

③ 国立研究開発法人
・5000 件を超える個人情報や未公表の研究情報がクラウドサービス（メールシステム）と内部システムから漏えい
・クラウドサービスへの不正アクセスを契機としたサイバー攻撃が原因

④ 国立大学法人「鹿屋体育大学」
・不正アクセスによって約 2,500 件のメールアドレスが外部に流出した
・さらに、そのアカウントを利用して「成り済ましメール」を 319 件送信されていたことも発覚
・学生のクラウドサービスアカウントが悪用されたこと

3. 中小企業が何故攻撃されるのか

最近では、大企業を標的にして攻撃しようとしても、強固なセキュリティ対策を講じている状況のため、大企業と取引をしていて、セキュリティ対策が充分ではない中小企業を攻撃・突破し、メールなどを通じて大企業のシステム内部に侵入するサプライチェーン攻撃[※2−2]が知られる様になった。

3.1中小企業は標的になりやすい

「我が社くらいの規模なら狙われることはない」、「機密情報なんて保持していない」、「狙われるようなデータもない」と安易に考えることなど油断は禁物である。
攻撃されやすい企業の特徴を幾つか紹介することとする。

①大手企業を取引先に持つ
- 貴社のホームページに取引先として大手企業を列挙している。下請的な関係が明確に分かる企業

②サプライチェーンの一環となっている
- ある業界の上流工程から、下流工程まで明示され、その環の一翼を担う企業として位置づけられている企業
  - 万が一、自社を踏み台にされて取引先の大企業へのサイバー攻撃が行われてしまったら、当該企業との取引がなくなってしまう可能性もある。
  - 今は中小企業がサイバー攻撃の対象になっていることを認識し、必要な対策を講じていかなくてはならない。

3.2. 対策ガイドラインの推奨対策

情報処理推進機構（IPA）が発表している『中小企業の情報セキュリティ 対策ガイドライン　第3版』[※2−3]では、下記の５つの対策を推奨している。

① OS やソフトウェアは常に最新の状態にする
②ウイルス対策ソフトを導入する
③パスワードを強化する
④共有設定を見直す
⑤脅威や攻撃の手口を知っておく

また、ファイルをバックアップし、復元できる機能も必要である。

3.3. 中小企業のサイバー攻撃対策高度化の必要性

前述の「中小企業の情報セキュリティガイドライン」は、「中小企業」に特化されており、サイバー攻撃対策が重要な対策のみに限定されている様にも捉える事ができる。

クラウドが利用されるサイバー空間において、中小企業の場合のみ、脅威が軽減されたり、被害が減少したりするサイバー攻撃などは存在しないと考えると、先の限定的な対策のみでは不十分であると考えられる。

しかし、資金も人材も限られている中小企業向けに、適切なサイバー攻撃対策を検討する必要がある。サイバー空間の脅威と中小企業の資源不足の2つの問題の解決策の一つとして、段階的にクラウドを導入する方法を検討した。

3.4. クラウド導入の脅威や脆弱性

サイバー攻撃への対策を考える上で、他人のコンピュータシステムを使って、自社の業務を行う上ではクラウド導入に応じた脅威や脆弱性への対応は避けて通れない課題である。企業経営上、クラウド導入とセキュリティ対応へのアプローチを整理してみると下記のようになる。

表 3: クラウド導入の課題とアプローチ

クラウド導入での課題	アプローチ
• クラウドの持つ潜在的なリスクが、自社業務に影響を与えないか。	事前の想定リスクでシミュレーションしておく。メリットもあるがデメリットもある。
• サイバーセキュリティの脅威はどのようなものか。	具体的なサイバーセキュリティリスクを特定する。 リスクアセスメントにより適切に脅威を特定する事が望ましく、対策を考える上でも専門部門や専門家に委託する事でムダを省く視点でも望ましい。
• 被害、損失に基づいて逆算して、企業の経営を危うくする脅威を推定する。	リスクレベルの推定は経験が必要とされており、顧客や自社が納得する方法を採用する。外部の有資格の専門家に委託する事も検討する。
• 推定脅威から、中小でも守らなければならない脅威を、予算・人員の許す限り選定する。	守るべきものと、予算・人員のバランス クラウドセキュリティ人材の育成も検討する。
• 選定された脅威について対応策、管理策を決定する。	不可能な場合はその理由の説明責任が必要 発生時はやむを得なかったと許してもらえるか
• 各種対策をしても残るリスク（残留リスク）を推定して被害、損失を計数化しておく。	リスクが残るのは想定内だが、不幸にして発生したら最悪となるケースを覚悟しておくことが必要である

上記のような、クラウド化に伴うリスク対応として、次の事項との整合性は取れるか。
①クラウドへ移行したとき情報セキュリティ対策がどのように変化するのかその内容を確認したか。
②サードパーティのセキュリティサービスプロバイダが提供するセキュリティ保証機能はあるのか。
③必要に応じて、又は顧客の要請に応じて、情報セキュリティの国際認証「JIS Q 27001（ISO/IEC 27001）」や「JIS Q 27017（ISO/IEC 27017）」の認証を取得するか。
以上の確認事項を課題として認識して導入を進める

3.5. クラウド導入の企業経営状態

クラウドサービスを利用する企業の経営状態の説明は確実で整合性がとれているか。事前にしておかなければならない条件を満たしているか、経営者は確認する必要がある。
企業の本来ビジネスとの整合性とは、①自転車操業的なビジネス企業や②基本的なビジネスは回っている企業では結果としての導入効果が出ないので、経営の安定化に専念することが第一である。

特に、自転車操業的なビジネス企業は問題を抱えながら、かろうじて経営している。その結果クラウド導入が問題解決に寄与する、との甘い考えに陥る可能性がある。

そのため、経営上での説明責任との整合性は取れる事が必要である。
①企業としてはどのガイドラインに従って対策を講じており、企業の社会的責任を果たしていたかを説明できるか。
②従って、どのガイドラインや事業者が社会的に一番知名度が高いか、やむを得ないとされる許容範囲のガイドや事業者はどれかを確実に認識していたか。
③所属する業界、多くの顧客が認知しているガイドライン・事業者であるならば、企業が生き残れるクラウド導入であろう。

4. テレワークにおけるクラウド導入

4.1. 新型コロナウイルス感染症対策のためのテレワーク緊急導入支援

本来テレワークにはクラウドの活用が当然考えねばならない、インフラの一環である。特に、働き方改革への取り組みとして、時間外労働や勤務形態の改善のために計画性をもって導入しなければならない。

今、中小企業が、新型コロナウイルス感染症に関する対策のため、在宅又はサテライトオフィスにおいて就業するテレワークに取り組むことを目的として、テレワーク用通信機器の導入・運用、就業規則・労使協定等の作成・変更等を実施して業務改善の推進を図ることを目的とする支援が実施されている。（新型コロナウイルス感染症対策のためのテレワーク緊急導入支援[※2−4]）

しかし、ここで推進されているのは、新型コロナウイルス対策として在宅勤務者を確保して感染拡大を防ぐことを目的にしている。そのため、クラウド化に伴う働き方の形態の変化を考慮した上で導入する必要がある。例えば労使間の合意等が必要な契約を十分に確認する事が求められる。

機器導入・利用・運用や情報管理は、適切なリスク管理とセキュリティ対策が求められる。厚生労働省よりテレワークガイドライン、米国NISTSP800−171などが発行されており適切な対応が求められる。一方でクラウドが前提となるため、下記の様なインシデントへの適切な運用方法と維持管理策を策定する必要があるが、個別の条件に合わせて判断する必要がある。

- 設定ミスや知識不足などにより非公開の情報を誤操作によりインターネットに開示してしまう。
- アクセス権の設定が誤っていて非公開のファイルのはずがだれでも閲覧可能になっていた。

5. クラウド化を実施しようとしている企業の実践手順

5.1. 基本的な流れ

下図では、これからクラウド化を実施しようとしている企業を例に基本的な流れを説明する。既にクラウド導入している企業は、下図の「定期的なクラウド運用チェックと評価」から始める。

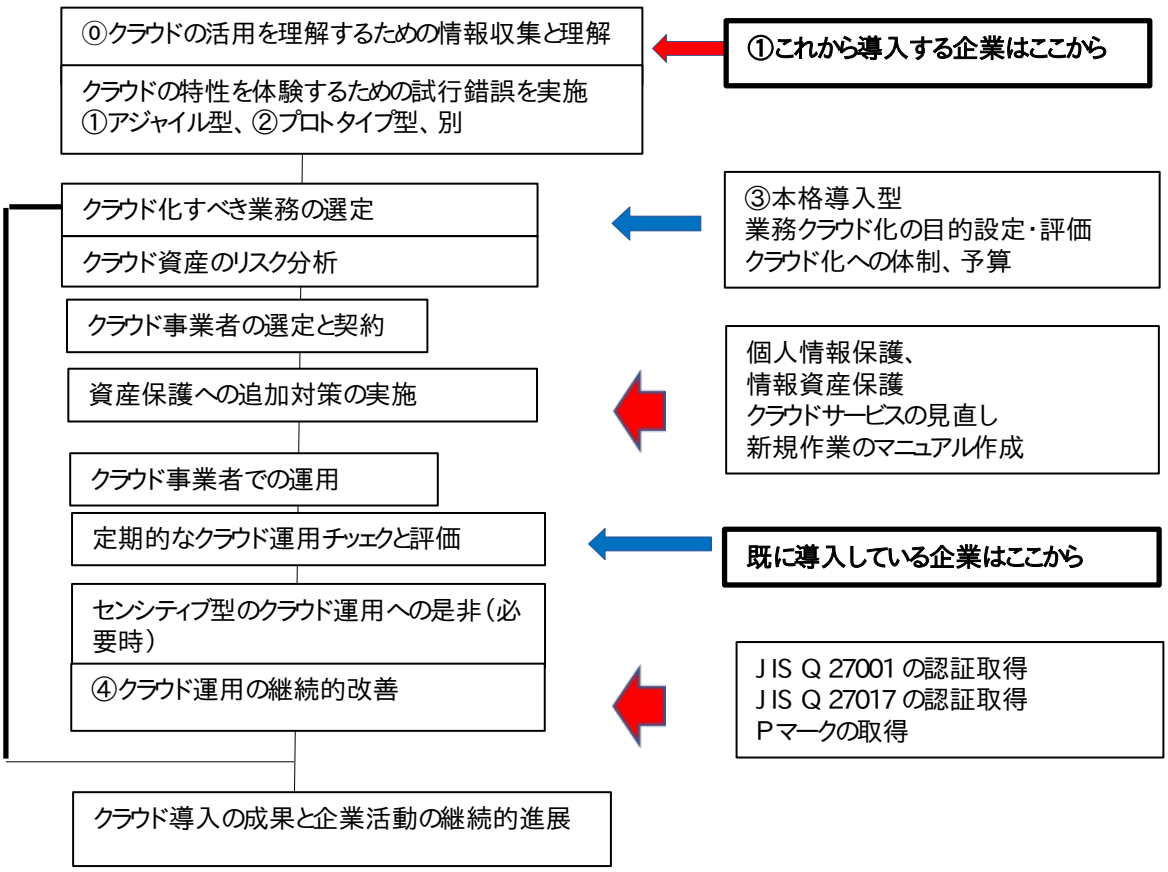

図 9: クラウドの活用を理解するための情報収集と理解

5.2. 手順策定時の留意点

クラウド導入を検討するたたき台として、小規模から取り組め、段階的に理解でき、他人に説明できることを考慮した下表の企業の実践手順を仮定した（ただし、新型コロナウィルスへの対応に伴うテレワークによって、検討フェーズがないままクラウドサービスの利用に踏み切ったケースが多数あると見受けられる。例えばオンラインミーティングツール）。

・中小の経営者に受け入れやすい（分かりやすい）手順。
・今まで議論されていなかった実践的手順。
・各段階はステップバイステップでより高度なクラウド利用を目指している。
・段階は第 0～4、X の6段階を設定している。
・各段階は最低でも1年以上実施する事が望ましい。 （0, 1, X の段階は例外で半年程度でもよい）
・本研究では中小経営者の壁となる、第1～3段階の研究を中心に行う。

表 4: クラウド利用の実践的構成

段階	特徴及び実践内容	備考
第0段階	・経営者がクラウドについての理解を深める ・自社をクラウド化する必要性について、経営者として説明責任を果たす ・具体的な作業を担当する人材の候補はいるのか確認する ・担当候補とのコミュニケーションと参加の同意	ここでは検討のみ 導入はしない
第1段階 アジャイル型	・クラウド導入に当たっての体験を重視する試行的段階と考える ・リスクを許容できる業務を選定する ・クラウド経費は最小限にする ・第 2 段階へ移行するのに必要な判断情報・データの記録を取る	
第2段階 プロトタイプ型	・クラウド形態が最も効果・効率の上がる業務での再体験をする ・必要に応じて第三者の意見も取り入れる ・クラウド経費は見積を取ってサービス内容との確認をする	
第3段階 本格導入型	・当社の基幹業務をクラウド化する ・失敗したら業績不振、最悪倒産の可能性があるのでセキュリティ保険等に加入する。	
第4段階 ライフサイクル型	・当社のクラウドシステムの寿命について常に確認しながら運用する ・改善・改良・新規サービスを柔軟に取り入れる ・ベンダーロックインを防ぐ様にクラウドサービスを常に確認しながら運用する	
第x段階 センシティブ型	・個人情報等リスクの高い業務のクラウド化を計画する ・実施は第3～4の段階で実施する	

6. 各段階における詳細な手順・評価

上記各段階のクラウド導入手順と、次の段階に進めるための判断を示す。

6.1. 第0段階

	実践内容	備考
第0段階	⓪経営者のポリシー・実践内容 • クラウドに興味を持つが自社の役に立つのか自問自答する • 経営者向けのクラウド関連セミナーに参加する • 業界で既にクラウド化をしている経営者とコミュニケーションする • クラウドセキュリティやクラウド監査に関わる人材育成を行う ⓪担当者のポリシー・実践内容 • 自社に役立つかどうか各種資料などを参考に検討する • クラウドセキュリティやシステム監査の資格取得のため学習する	
評価・決断	兎に角やってみて、体験してみる事に決める	

6.2. 第1段階

	実践内容	備考
第1段階 アジャイル型	⓪ポリシー • クラウド導入に当たっての体験を重視する試行的段階と考える ①対象業務 • リスクを許容できる業務を選定する ②事業者選定 • クラウド経費は、例えば第1段階50～100万円程度 ③バックアップ • クラウドバックアップに即した方法を試行し、対応方法を学習する ④トラブル対応 • クラウド対応に即した方法を試行し対応方法を学習する。 ⑤システム監査と ISMS クラウド監査 • 第 2 段階へ移行するのに必要な判断情報・データを記録する	
評価・決断	• 経営者及びクラウド管理者が第1段階の情報・データで安全性、有効性、効率性を評価する • 必要に応じて第三者の評価も取り入れる • 第2段階へ進む事を決定する	

6.3. 第2段階

	実践内容	備考
第2段階 プロトタイプ型	⓪ポリシー • 第1段階の経験を踏まえる • センシティブ情報の位置付けと取り扱い等、リスクマネジメントとガバナンス体制を検討する ◦ リスク回避する場合でもポリシーを策定する ①対象業務 • クラウド形態が最も効果・効率の上がる業務を選定する	

	○ 例：メール、ファイルサーバ等 • 新規ビジネスでの展開でも良い ②事業者選定 • サービス内容の確認と、当社の狙いが一致しているか確認 • クラウド経費は第2段階100～500万円程度 ③バックアップ • クラウド事業者のサービスのバックアップ状況を確認しサービス要求との合目的適合性を確認する。 ④トラブル対応 • 事業者にマニュアルが在ることを確認、トラブル訓練を実施 ⑤監査　　システム監査とISMSクラウド監査 • 第3段階へ移行するのに必要な判断情報・データを確実に記録する	
評価・決断	• クラウド化が効果・効率への貢献度合を数値化して評価する • 自社のリスク管理の視点から見て、安全性・妥当性・整合性に関し評価をする • 必要に応じて第三者の評価も取り入れる • 第3段階へ進む事を決定する	

6.4. 第3段階

	実践内容	備考
第3段階 本格導入型	⓪ポリシー • 当社の基幹業務をクラウド化する ①対象業務 • 第x段階・センシティブ型の業務以外の全業務を選定対象とする ②事業者選定 • 第1, 2段階の選定を踏襲する • 事業者との信頼関係をステークホルダーに説明できる情報を確実にする • 契約は損害賠償にも言及する ③バックアップ • JIS Q 27001 に規定されているバックアップ関連の手順に従い実施する。 • 例：IaaS の場合、マルチクラウドやクラウド外へのバックアップ ④トラブル対応 • サイバーセキュリティ保険への加入を検討する • 情報セキュリティへの対応として JIS Q 27001 を取得 ⑤監査　　システム監査とISMSクラウド監査 • 27001、27017、22301、15001 等の取得した規格の内部監査でも良い	
評価・決断	• 第 3 段階（本格導入開始時）のリスク評価を再確認する。 • 定期的に監査等によるリスク評価をする。	

6.5. 第4段階

	実践内容	備考
第4段階 ライフサイクル型	⓪ポリシー • 当社のクラウドシステムの寿命について常に確認しながら運用する • クラウドシステムの分散化を一部施行・運用する ①対象業務 • クラウド化が相応しくない業務以外の全業務 • 対象としない業務の選定手順、説明責任を確実に果たせること ②事業者選定 • 自社の企業風土との相性が良い業者 ③バックアップ • 復旧時間の想定範囲内の情報・データ ④トラブル対応 • 情報セキュリティへの対応として JIS Q 27001 を継続 • クラウドへの対応として JIS Q 27017 を取得 • 事業継続マネジメントシステム JIS Q 22301 に準拠 ⑤システム監査と ISMS クラウド監査 • 27001、27017、22301、15001 等の審査の実施でも良い • 導入したクラウドシステムの寿命（賞味期限）のチッェク • 改善やリニューアルで延命を図れるかの情報・データの収集 • 後継人材育成のための継続的教育とその成果	
評価・決断	• 27001、27017、22301、15001 等の審査をもって評価に代えても良い • クラウドシステムの寿命についての決定	

6.6. 第X段階

	実践内容	備考
第x段階 センシティブ型	⓪ポリシー • 当社のセンシティブな業務をクラウド化する • これらの業務のクラウド化の段階はケースバイケースで導入する ①対象業務 • 個人情報を扱う業務のクラウド化 • 営業・顧客情報を扱う業務のクラウド化 • 経営企画、財務・会計等の業務のクラウド化 ②事業者選定 • センシティブ業務に関わるクラウドサービス事業者のリスク対応要件を満たすこと ③バックアップ • デュアルクラウドで保証する ④トラブル対応 • 第4段階の対応を踏襲する • EU一般データ保護規則（GDPR）対応の手引き（システム監査学会発表資料）を参考にして対策をする ⑤監査　　システム監査と ISMS クラウド監査 • 個人情報保護法に基づく対応を要求される • EU における個人データの保護は GDPR（General Data Protection Regulation）に基づくので対応を要求される	
評価・決断	• EU一般データ保護規則（GDPR）対応の手引き（システム監査学会発表資料）を参考にして評価する	

7. 実践手順の評価、見直し

7.1. この手順における今後の検討課題

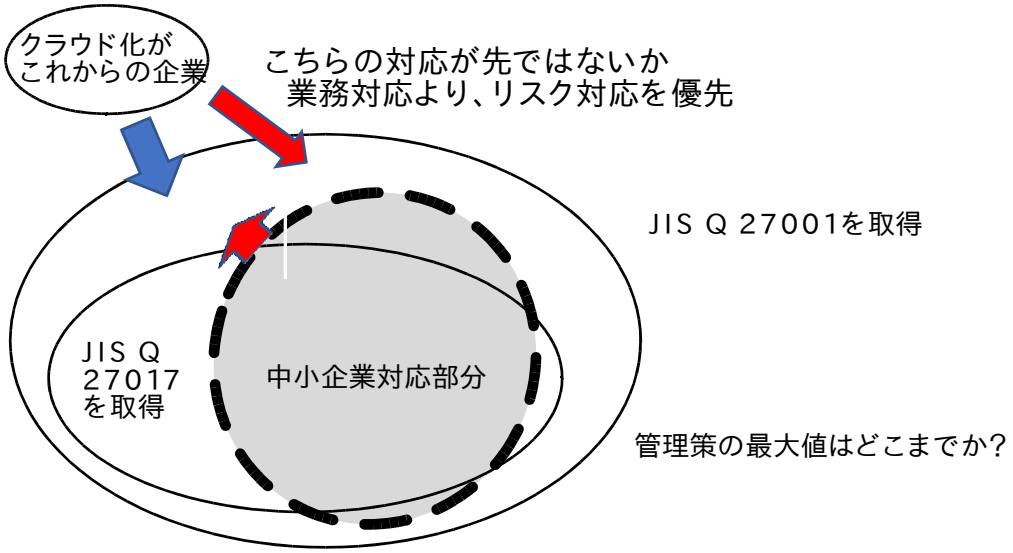

図 10: 中小企業とセキュリティリスク

上記の図表に、コンピュータシステムへの脅威は脆弱性対策とクラウドの利便性、生産性との調整にあると考えられる。

①具体的内容が JIS Q 27017 の内、中小企業の対応部分となるが、それが最適な答えか、に不安を感じる
② JIS Q 27001 の認証取得が前提条件ではないか?
③ JIS Q 27017 の読み込みと理解を必要とする
④中小向けのサイバーセキュリティガイドを実施済みである事こと
⑤これらを満たした上でのクラウド化のメリットを享受する。

Ⅲ. 対象業務の選定

1. 本格的なクラウド導入

クラウド導入の具体的な手順と対応、運用は第 0～4、X の6段階で、「第3段階　本格導入型」を中心に取り上げる。特に重点的に対応しなければならない、クラウドサービスの利用上の「JIS Q 27001 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」の紹介をする。

段階	取り組み方
第3段階 本格導入型	①ポリシーは経営者が自社のクラウド化の趣旨を明確にする。 ②対象業務　　本稿で紹介する。 ③業者選定は第1, 2段階の選定を踏襲する。信頼関係を確実にし、損害賠償も明確にする。 ④バックアップ、トラブル対応、監査等は JIS Q 27001 及び JIS Q 27017 を取得、又は同等の対策をとる。
リスクと対処	失敗したら業績不振や最悪倒産 リスクを回避する選択肢の評価

2. 試行錯誤の段階での業務選定

前項でクラウド導入へのアプローチ手順を紹介したが、対象業務選定はアプローチの各段階で選定基準が変わる。

何故アプローチ手順の中に、試行錯誤の段階を入れたかは、導入にあたっての失敗を上手く「経験」に代えることを狙いとしている。この段階を踏まないで、本格的導入をする企業は、必ず導入前に復旧できる、バックアップと経費、復旧手順を用意しておくことが必要となる。

第 1 段階、第 2 段階の試行錯誤の段階では、次のような留意点がある。

①リスクが許容できる業務を選択する。

②クラウド形態が最も効果・効率の上がる業務で体験をする。

更にこの段階の終了時に、下記の様な事象で第3段階の本格的にクラウド導入を進めるかの判断ができるか、の現体験が重要な留意点である。

①クラウド化の効果・効率、自社業務への貢献度合を評価できる。

②経営者、クラウド管理者、社員がクラウド化への理解と納得ができる。

③自社のリスク管理の視点から見て、安全性・妥当性・整合性を評価できる。

3. 本格的導入段階での業務選定

１つの中小企業においては、クラウド化対象となる業務の数はそれほど多くないと考える。だがその中で優先してクラウド化する業務を選定することは必要である。それはクラウド化により「Ⅰ. 総論」にあるメリットが確保され、自社への貢献向上が図れる業務を優先することになる。

本格的導入段階での業務選定の考え方を、次の3パターンで紹介する。この業務選定の考え方に異論が出ることに十分理解しているが、その多くはこの3パターンのいずれか、または複数の目的をもって、社内環境と比較の上で導入していると考える。

①システム担当者や保守会社がいないため、管理が容易なクラウドにデータを置く（コストを重視）。

②どこからでもアクセスできるよう、利便性の観点からクラウドにデータを置く（利便性を重視）。クラウドサービスの多様化の中で、利用したい機能がクラウドサービスで実現できる（利便性を重視）。
③重要な情報については、事業継続の観点からクラウドへデータを置く（セキュリティを重視）。

なお、新型コロナウィルスによるテレワークへの対応によって活用されているクラウドサービス（ファイル共有、オンラインミーティング、勤怠管理等）は、②の「利便性」を第一の重要事項として導入判断をしたと考えている。

3.1. コンピュータシステム中心の対象業務選定手順

コンピュータシステム中心では、コンピュータに関連するものを、ハード、ソフト、アプリ、通信、等の視点で管理するするときのメリットに着目して選定する方法である。
①コンピュータシステムのハードウェア、ソフトウェア、及びその運用、
コンピュータ室に設置されている機材の一部又は全てを対象とするか
②コミュニケーションツール、記録
電子メール、グループウェア、LINE、テレビ会議、テレワーク、ブラウザ等のツールと利用の記録、
パブリックアドレスとしての、HP、ホームページ作成、採用情報、IR、の公開
③業務用のツール、
文書、表計算、プレゼン資料、データベース、ファイル転送、
④業務の処理アプリ、
財務会計、税務申告、給与計算、労務管理 などの経営管理アプリケーション
顧客管理、販売管理、営業管理、サービス管理、名刺管理、総務庶務、EC サイト などの業務アプリケーション
購買管理、受発注管理、在庫管理、納期管理、協力会社、などの製造アプリケーション
経営計画、年度事業計画、研究開発、市場調査、社内情報システム管理、など
⑤情報の蓄積と活用、
上記の業務活動に基づく、データ・情報のエビデンスとしての記録、蓄積、及びデータ（ビックデータ）の分析、加工、利用　など
⑥クラウド固有業務
運用・バックアップ・リカバリー、トラブル対応、監査の必要性

3.2. 個人情報保護法中心の対象業務選定手順

個人情報保護法が施行され、個人情報は全てのビジネス活動の局面で守らなければならない。
これに対応するものとして、プライバシーマーク（通称Pマーク）と言われる認証制度がある。
クラウド利用時のリスクと被害範囲を特定し、管理策を構築するのだが、個人情報以外の重要と思われる情報についての保護が明確でなかったり、個人情報保護法に100％対応しているとも言い切れない面がある。また、クラウド導入した時のクラウド上の情報はクラウド利用者とクラウド事業者の責任分解をどのように考えるべきか、議論の余地がある。

自社として、実地に様々な制約がある業務の中からクラウド化によりその実行が効率化できる、安全性が強化できる等の改善の大きな業務を選定する。

表 5: 情報の側面から見た影響

リスクカテゴリー	クラウド事業者	クラウド利用者	利用者の顧客
個人情報①	アップロードしない	自社内で対応	被害規模は人数
顧客個人情報②	セキュリティ対応	法律義務違反	被害規模は人数
顧客所有物情報	セキュリティ対応	法律義務違反	被害規模は人数

法規制情報	セキュリティ対応	法律義務違反	限定的
基幹業務情報	セキュリティ対応	停止時間の範囲	SL A
IT維持管理情報	アップしない	あらゆるリスクの想定	波及被害
その他情報	免責範囲	信用喪失	SL A
データ改竄	免責範囲	信用喪失	SL A
サービス停止	停止時間の範囲	停止時間の範囲	機会損失
事業継続	想定外	あらゆるリスクの想定	利用者としてのリスク
生産性	自動化	有効性	コストパフォーマンス
テレワーク	免責範囲	有効性	無関係？
契約	標準契約書	個別契約書	契約・商慣習

＊SLA；Service Level Agreement サービスレベルアグリーメント

3.3. ISMS 認証中心の対象業務選定手順

ISMS　情報セキュリティマネジメントシステム（JIS Q 27001）では資産の管理を要求している。つまり業務を選定するのでなく、業務遂行に必要なデータ・情報には財産的価値があるとして、優先度を付けて情報資産の抽出と選別をして、管理する方法である。

このために資産を分類し、資産目録（情報資産を含む）の作成をおこなっている。クラウド化の対象にするかしないかを、この資産目録に基づいて決める事も一案である。

具体的な、情報資産目録の例を下記に示す。

この目録で行った作業は、

①売上げが1億円ほどの企業を想定している。

②そのビジネスを構成している情報資産をリストアップして、データ件数等を把握する。

③情報資産を値踏みする。例では、お得意様台帳は1件15万円とした。

④それぞれの情報資産のデータ件数と値踏み額を掛け合わせとものが、その情報の資産総額とする。

⑤全ての資産額を合算したものが、このビジネスの売上げ総額と一致すれば、資産モデルとして成立する。

⑥ランクは自社に及ぼすリスクの度合に応じて決め、そのランクに見合うセキュリティ対策を講ずる。

ここでは、安全性向上、省力化のみならず付加価値の高い情報をリストアップするのが本来の姿である。

	情報資産名	媒体	内容	場所	資産の責任者	データ総件数	ランク	千円	資産総額	
1	お得意様台帳	電子媒体	会員番号、住所、TEL、趣味、家族、口座番号	事務室PC	販売管理	200	A	150	3,000	万
2	会員Mカード台帳	電子媒体	会員番号、住所、TEL、趣味、家族、ポイント	事務室PC	営業課	1,000	B	50	5,000	万
3	会員M売上DB	電子媒体	会員番号、日時、品名、数量、売上、ポイント	サーバ室	販売課	10,000	B	2	2,000	万
4	電話注文票	紙	会員番号、品名、数量	事務室	販売課	150	B	0.5	8	万
5	Web注文データ	電子媒体	会員番号、品名、数量	サーバ室	NW	500	B	0.5	25	万
6	宅配業者情報	紙	会員名、住所、TEL	事務室	総務	30	C	0.5	2	万
7	社員名簿	電子媒体	氏名、年齢、学歴、住所、TEL、家族、	事務室PC	人事	10	B	10	10	万
									10,044	万

図 11: 資産目録の例

3.4業務中心　（クラウド化の対象業務の優位性識別）の対象業務選定手順

業務中心では、次の観点から優先順位を決めておく必要がある。
優先順位を決めるのに当たって、次を考慮する。
①自社における利益の源泉の商品・サービス又は経営戦略の要となるビジネスの取扱、
②自社の事業優位性から見たインパクト要素、と守るべき資産を考慮する。また、将来性を重視する。

表 6: 業務中心の対象業務選定手順

自社の優位性のテーマ	自社の優位性の対象業務例	過去の優先順位	将来の優先順位
物では	製品開発、開発中の製品	高	中
設備、施設では	製造ラインの機器、コスト	中	中、高
ソフトウェアでは	コンテンツの確保	低	低
情報では	情報資産	中	高
人では	クリエイター、従業員	高	中、高

この図表で業務選定するには、今後は情報が最も高いとしてあるのは、
①物であれば設計情報が在れば造れる、
②設備機器を自作するほどであればやはり設計情報、
③ソフトは市販品中心となるか、クラウド事業者の提供、
④人材はAI化を進めなければならないので過渡期は別としてノウハウ情報優先となる。
従って、情報管理、特に情報セキュリティが重要な要件であることが浮かび上がってくる。これらの情報をクラウド化したとき、どのように「組織向けの脅威」から護るかが対策の主流になると考える。

4. 守るべき情報財産（資産）

ここでは、守るべき情報資産の対策をISMSの規格にそって事例として紹介する。

4.1. クラウド化での資産目録

クラウド化の対象業務を組織向けの脅威等を勘案して、「資産目録」を作成して企業を護っていこうとする考え方がある。その一つがJIS Q 27001規格であり、更にクラウド化をした場合はJIS Q 27017を追加して対策をたて、実行することが要求されている。これらのJIS規格を総称して「ISMS」と呼んでいる。

ISMS では情報資産を、優先度でなく付加価値の高い情報を明確にして選別することが重要である。

表 7: 資産目録の細分化

リスクカテゴリー	基本	センシティブ	例外的
個人情報①	氏名、住所	人事、評価、健康、	採用、解雇
顧客個人情報②	名刺	戦略評価	
顧客所有物情報	発注、仕様、納品	見積、履歴	
法規制情報	雇用、税、保険、	リアルタイムの改定・変更	
基幹業務情報	マニュアル、	事業継続	
IT維持管理情報	パスワード	システム脆弱性	
その他情報漏洩			

4.2. 資産目録作成　(事業の特定と資産目録の作成規程　例示)

資産目録の作成の手順は以下のとおりである。
①当社の各業務を職務分掌、業務フロー等で明確にする。また、必要に応じて業務に使用される情報・設備等の課題、リスクを業務フローで特定する。

②各業務で使用される情報、設備等を下記の分類区分で特定する。必要に応じて管理番号や管理シールを付ける。分類区分における情報・データ・ソフトウェアを総称して情報資産と呼ぶ。

表 8: 資産の分類区分

No	資産の分類区分	詳細
1	情報・データ資産 個人情報、顧客情報、基幹業務情報、IT関連情報など	情報資産目録参照
2	ソフトウェア資産 開発ソフト、市販ソフト、スプリクトなど	情報資産目録参照
3	物理的資産 事務所、開発環境、ﾈｯﾄﾜｰｸ環境、作業環境、各種装置など	固定資産台帳参照
4	サービス 電力、インフラ、など	情報資産目録参照

③情報資産を下記の分類区分でグループ化して特定する。

表 9: 情報資産グループ

No	情報資産グループ	資産の例
1	個人情報	会員等の個人情報
		顧客所有物の中の個人情報
		協力会社個人情報
		社員の個人情報
		上記データのバックアップデータ
2	顧客所有物情報	業務上、顧客から支給された情報 上記データのバックアップデータ
3	法規制情報	法令、規則等で管理を規制されている情報（個人情報を除く） 上記データのバックアップデータ
4	基幹業務情報	当社の基幹業務を形成する不可欠な情報・データ 営業、生産、販売、在庫、など 上記データのバックアップデータ
5	IT 維持管理情報	コンピュータ等のインフラ・アプリを維持していくための情報 上記データのバックアップデータ
6	その他の情報	企業の管理上の情報
		その他の付帯情報

④上記に基づき、資産目録で資産の目録を作成、維持する。
a)個人情報については法規制で求められている部分の欄も作成する。
b)情報の原本・控えの区別なく、ありのまま記載する。複数ある場合もそれぞれ記載する。
c)同一組織のクライアント PC は同一の情報資産グループとみなす。

⑤資産目録の中に、その資産の管理責任者を指定する。
この管理責任者は原則としてリスク所有者の役割・責任が割り当てられる。
⑥資産の利用の許容範囲に関しては、情報資産については資産目録の中の管理責任者が明確にし、実施する。PC、電子メール、インターネット、モバイル装置、等については各管理策の中で記載する。

5. 情報セキュリティの脅威への対応策

情報セキュリティの脅威への対応策として、JIS Q 27001 及び JIS Q 27002（ISMS）の規格があり、その認証活動が行われている。更にクラウド化をした場合は JIS Q 27017 で追加対策を実施する事が要求されている。ここでは、クラウド化を導入した時に認証を取得するしないに関わりなく、実施するべき対策を抜粋して紹介する。

5.1. 情報セキュリティ管理策の実践の規範

JIS Q 27002 クラウドサービスのための情報セキュリティ管理策の実践の規範、及び、“附属書 A（規定）クラウドサービス拡張管理策集には次の項目が明示されている。
各項目番号は JIS（ISMS）の項番をそのまま表示している。

表 10: クラウドサービスカスタマの対応部分 抜粋

5.1.1 情報セキュリティのための方針群
6.1.1 情報セキュリティの役割及び責任
6.1.3 関係当局との連絡
以下: 掲載可否を著作者に確認中

5.2. 情報セキュリティ規格で作成する文書

情報セキュリティ規格（ISMS）では文書や記録の作成や維持管理が要求されておりその一部を例示する。

表 11: ISMSで必要とされる作成文書一覧（例示）

ISMS マニュアル
リスク管理マニュアル
ISMS テキストブック（教育教材）
0410-組織の状況
0520-ISMS 方針
0530-ISMS 体制図
0530-ISMS 役割責任
0530-誓約書
0611-リスク一覧表
0613-適用宣言書
0720-年度教育訓練計画
0720-教育訓練記録
0751-ISMS 文書記録一覧
0920-年度内部監査計画
0920-監査チェック表
0920-内部監査実施計画／記録
0930-マネジメントレビュー記録
1010-改善処置票
A080101-資産目録
A080101-固定資産台帳
A080104-廃棄・返却・引継チェック表
A090201-業務システム利用申請書
A090201-ネットワーク利用申請書
A110101-セキュリティ境界
A110102-入館受付票
A110203-電気配線図
A110203-LAN配線図
A110205-情報資産持出し記録
A110207-廃棄マニフェスト伝票
A120401-ログ
A120403-セキュリティ監視月報
A120403-セキュリティ作業日報
A130101-ネットワーク構成図
A150200-ISMS 関係組織表
A150200-契約書
A160100-インシデント処置票
A170101-事業継続計画
A170102-事業継続実施（検証）報告
A180101-法的規制要求事項

表 12: クラウド導入で追加される文書

クラウドリスク管理マニュアル（追加分）
A080101-クラウド資産目録
A150100-クラウドサービス契約書

JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」のISMSで必要とされる作成文書一覧（例示）を希望される企業は連絡先にご一報ください。

6. クラウドサービス事業者との契約

選定した業務について、その業務をクラウド化するに当たり、クラウドサービス事業者に満たしてもらう要求事項を可能な限り明らかに記述する。

6.1. 契約書に盛り込まれる項目

項目契約書に盛り込まれる一般的な項目を例示する。[※3−1]

1サービスの種類（SaaS,aaS,ストレージサービス等）
2サービスの提供範囲（クラウドサービス事業者が責任を持つ範囲）
3契約の締結に関すること
4サービスが提供できなくなった場合の対応
5契約内容の変更
6付加サービス機能
7通信、回線のサービスレベル
8価格体系や適用条件別料金
9価格の変更に関する規定（通知期間、通知方法、不同意の場合の処理 等）
10保守事項、保守の優先順位
11損害賠償
12利用者の義務
13守秘義務（事業者側、利用者側、双方同等。事業者側の利用者情報に関 する守秘義務や利用者側の義務について注意が必要）
14契約の満期終了と更新に関する規定（契約期間は、自動更新規定がある か、更新しない（する）場合の通知期間・通知方法等）
15契約の解除に関する規定（事業者側が一方的に解除できる条件でないか、利用者側が解除する場合のペナルティ等はないか、等）
16契約の終了・解除に伴う処理等の規定（終了時の事業者の義務、利用者 の権利が規定されているか、それは妥当か。終了時のデータの返還や、返還後にクラウド上のデータを完全消去すること等が明記されているか 等）
17データ等の情報のセキュリティレベルやバックアップの範囲

クラウドサービス事業者と実際に締結する契約書（又は約款）でどのように表現されるか、自社の場合に引当てて各クラウドサービス事業者の特徴を把握する。

なお、次のような一般的な企業として評価も参考にする。

a) 財務情報、上場の有無
b) セキュリティ方針
c) 売上高
d) 顧客数
e) サービス、メニューから見た強み
f) セキュリティ体制、認証取得状況など
g) 相談体制、ツールの豊富さ
h) サービスの利用が終了したときの、データをどのように取扱うか
i) クラウド安全性評価（ISMAP）の評価をされているか

6.2.選定した業務と事業者との適合

本格的導入段階で選定した業務をクラウド化するのに、どのような条件が必要であるか整理して、どのクラウド事業者が適合するか選定の参考にする。 記載事項は例示

業務：〇〇産物販売業務
利用の種類：SaaS 利用
データ移行：移行が必要なデータ 3 種類。30 項目、約 1TB
インターフェイス：生産者連携システムとデータ連携要
導入までの切り替え期間：
運用体制：年末年始以外稼働。8：00～19：00
障害対応：障害は半日以内に回復のこと
稼働率：99.7%(年間停止 0.5 日以内)
端末：汎用 PC、利用拠点3箇所、端末台数 15 台
稼働・運用相談：出来るだけ欲しい

Ⅳ.ITガバナンス

1.クラウド導入時のITガバナンス

クラウド導入の局面では経営判断の役割は極めて重要である。
具体的な判断をする事象は次のようなものが考えられる。

①クラウド化の推進体制　　・推進組織や体制、経営者の役割、担当者の指名
②クラウド化の必要経費　　・概算の導入経費と見直し時期
③クラウド導入のキックオフミーティングや情報システム戦略委員会等
　　・開始時期及び第一段階の完了時期、メリット・デメリットの明示
④クラウド化のガイドライン選定　・所属する業界、団体のガイド、相談窓口
⑤クラウド事業者の選定　　・事業者との相性、

次の2項は【**Ⅲ.対象業務の選定**】参照
⑥クラウド化対象業務の選定　・クラウド化の対象業務を選定
⑦守るべき情報財産（資産）　・情報財産の概念理解と情報資産の抽出

これら経営陣の意思決定の行動様式については、次の様な資料を参考して行う。
『サイバーセキュリティ対応を躊躇する経営陣の意思決定行動に関する考察, 経営情報学会秋全国研究発表大会,2016[※4-1]』

2.クラウド化推進体制の構築と経費の算定

2.1.クラウド化の推進体制

クラウドの導入に当たっての推進組織や体制を決め、経営者の役割や担当者の指名を行う。
特に経営者の役割として以下の様な内容が紹介されている。
（IPA資料:「中小企業の情報セキュリティ対策ガイドライン第3版」）

・経営者がクラウドについての理解を深める　特に顧客への影響内容とクラウド事業者の信頼性
・自社をクラウド化する必要性について、経営者としてリーダーシップを取り、社内外への説明責任を果たす
・具体的な作業を担当する人材の候補はいるのか確認する
・担当候補とのコミュニケーションと参加の同意

また、実行すべき「重要７項目の取組」として以下を実施する。

1 情報セキュリティに関する組織全体の対応方針を定める
2 情報セキュリティ対策のための予算や人材などを確保する
3 必要と考えられる対策を検討させて実行を指示する
4 情報セキュリティ対策に関する適宜の見直しを指示する
5 緊急時の対応や復旧のための体制を整備する
6 委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
7 情報セキュリティに関する最新動向を収集する

ここで期待されていることは、リーダーシップを取ることと、今まで経験の無かった役割を行わなければならない事が留意点である。これらのスキルを導入活動と併行しながら身につけていくことが大切である。

2.2. クラウド化の必要経費

クラウド化の必要経費の概算見積を行うこと、また進捗に応じてその見直しを行うことが大切である。必要経費には、①担当者の人件費、②クラウド事業者とのサービス契約の金額、③必要なハード、ソフトの経費、④ネットワークの通信料、⑤有識者への相談料、コンサルト経費等である。

また、クラウド化が進めば、それに伴う経費や想定外の経費も発生するので注意すること。

3. クラウド導入のキックオフミーティング

クラウド導入はプロジェクトでもある。周知内容としては次のようなことが考えられる。

・クラウド化の狙い（メリット・デメリットの明示を含む）
・推進体制（体制、コスト、導入に伴う変化）
・開始時期及び第一段階の完了時期（各段階の導入内容とスケジュール概要を含む）　　等

4. クラウド化のガイドライン選定

クラウド化に当たってのより所となるガイドラインを選定する

所属する業界や団体のガイドがあれば、ガイドラインを提案している組織体と連絡を取り、相談窓口や導入サービスがあるか確認する。

ガイドがあれば良いが、無いときは、元請け会社や大手顧客、有識者への相談、コンサルトの採用などを必要に応じて行う。

現在公表されているクラウド関連ガイドラインは**【クラウド導入の実践的ガイドー添付資料】**参照

5. その他の参考とする国内外の基準等

① JIS Q 27001（ISO/IEC 27001）ISMS（Information Security Management System）
（情報セキュリティマネジメントシステム）
② JIS Q 27002（ISO/IEC 27002）（情報セキュリティ管理策の実践のための規範）
③ JIS Q 27017（ISO/IEC 27017）（JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）
④ NIST SP800-53 rev.4（National Institute of Standards and Technology）連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策
⑤ Australian Government Information Security Manual（ISM）
オーストラリア政府情報セキュリティマニュアル

6. クラウド事業者の選定

クラウド事業者の選定に当たっては、事業者との相性が大切である。候補者となる幾つかのクラウド事業者を選定し、そのサービスを比較して最適な事業者を選ぶこととなる。

最適な事業者の選定に重要と考えられるクラウドサービスの安全性評価は、検討が行われているものの、未だ登録事業者や評価されたサービスなどはないため、現時点での事業者の選定方法を述べる。

（クラウドサービスの安全性評価に関する検討会中間とりまとめ（案）　平成 31 年 3 月[※4−2]）

6.1. クラウドサービス事業者選定

（1）サービス事業者が提供するサービスに関する認定・情報公開制度等

利用者がクラウド事業者選択時に比較のための　パラメータはⅢ.6.1. 項でクラウドサービス事業者と契約を取り交わす際に考慮する項目とする。そのため「事業者」の選定と提供される「サービス」の選定に関しての情報を収集・活用する。

①事業者が公表している財務情報を確認する。
②利用者数などの実績を問い合わせる。
③事業者の情報セキュリティ方針や関連した認証・認定制度＊1 の取得状況を確認する。
④クラウドサービスの安全・信頼性を確認する情報を提供しているか。
⑤サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証を確認する。
⑥店舗にクラウド型 POS レジを導入するにあたりサービスが常時に動いているかの稼働実績を確認する。
⑦事業者またはプラットフォーム事業者が公表している品質保証基準（SLA＊2）を確認する。
⑧システムの障害でデータ消失などの被害が発生したときに、どこまでが事業者の責任で、どこからが利用者の責任なのか利用規約で確認する。
⑨クラウド利用にあたり長期間利用でき、セキュリティ対策を常に改善している事業者を選択する、

（2）利用実態から見た評価項目とクラウド事業者選定

これまでの議論で念頭に置いたクラウドサービス事業者は、グローバルにサービスを展開する大手の事業者、国内で回線やデータセンタ設備を保有しクラウドサービスを提供する事業者である。中小企業は SaaS 形態でクラウドサービス事業者の提供するアプリケーションを利用することを考える。また、他に自社の既存のソフトウェア資産を活用して PaaS 形態で利用する場合も考えられる。

クラウドサービス事業者を選定するため、HP 上でサービス内容やレベルを確認すること、更に現在利用している会社からの評価の情報を入手することができればよい。しかし、実際には利用者の声を聴くことや、それら利用者の評価をまとめた情報を得ることはなかなか困難である。クラウドサービス事業者は HP 等により自社のサービスの特徴をアピールしている。事業者の特徴、得意分野のほか、サービスメニュー、セキュリティ面の特徴、価格、他のクラウドサービスとの連携、利用者サポートなどである。実際の利用状況に代わるものとしてこれが参考になる。。

SaaS 形態で利用する場合、クラウドサービス事業者が提供するアプリケーションをそのまま利用出来ればよいが、出来ない場合には企業はクラウドサービス事業者が提供するアプリケーションと適合度合いを見極めることが必要になる。また PaaS 形態で利用する場合にはクラウド化にはそれなりの IT 技術の対応が必要になる。

クラウド化には、クラウド導入支援のほか、導入後に運用のための維持管理や監視業務、またセキュリティ対応が必要である。クラウドサービス事業者との契約により明確になることであるが、これらを必ずしもすべてクラウドサービス事業者に任せることは出来ない。一方中小企業としては本業以外のこのようなクラウド化移行技術、運用のための工数や技術を持たないし、持ちにくい。このことを考えると、クラウドサービス事業者の選定としては、クラウド導入支援と併せて、運用管理代行の MSP(マネージドサービスプロバイダ)やセキュリティ対応支援を代行する機能を持つ MSS（マネージドセキュリティサービス）を選定するのがポイントとも考えられる。世の中には自社では設備を持たず、持っても小規模に特定の目的に特化した設備を導入し、大手事業者と連携してサービスメニューの効率的・効果的な利用の導入支援を中心に、運用に関わる対応も引き受け実施する企業が多くある。大手事業者のサービスと連携する「クラウド導入支援事業者」が多いことは、クラウド利用にはそれだけのノウハウが必要であることを表している。利用者である中小企業は、このようなことを念頭にメニューを見て自社の業務との適合性を判断するほか、利用の容易性、既存データの移行の容易性、導入スピード、料金、契約内容などの項目について自社業務をクラウド化するための適合するサービス事業者を探す切り口として参考に見てほしい。また導入手順で紹介した試行錯誤を体験することを推奨する。【Ⅱ.導入手順】参照

表 13: クラウド事業者のアピール、メニュー、特徴など

クラウドサービス事業者（名称）	各社の URL 事業者のアピール、サービスメニュー、セキュリティの特徴、サポートなど
Amazon （AWS）	https://aws.amazon.com/jp/ • 最も包括的　サービスを提供　　コスト削減　俊敏性 • ソリューション　機械学習、分析とデータレイク、IoT、コンテナ、エンタープライズアプリケーション、ストレージ 業種別、規模別ユースケース別　メニュー表示が豊富 • 高い利用実績を持つ　軍隊、銀行など • リモートワーク（テレワーク）及びリモート学習 • セキュリティ標準90をクリア • システムインテグレータと独立ベンダによるサポート • 無料利用　AWS 無料利用枠あり
Google （Google Cloud）	https://cloud.google.com/ • 本質はソリューションの提供、必要ツールをパッケージで利用できる • 大手企業の利用実績多い • メニュー多彩 データ分析に強い　BigQuery • シームレス利用 • セキュリティ　セキュリティ重視設計、Google のお客様サービスの使用と同じレベル • 無料利用の制度有　最大 12 か月
Microsoft （Azure）	https://azure.microsoft.com/ja-jp • 信頼できる Azure 製品とサービスを使用してアイデアをイノベーションに変える • 大手ｸﾗｳﾄﾞプロバイダ-の中でも先進的ガバナンス機能を備えている • 障害対応を含むサポ-とプランが basic レベルから 4 種 • 開発は未来に備える　思いのままにビルド • 価格　ーコスト削減、AWS の 1/5 • ハイブリッド環境のシームレス運用　エキスパートチーム支援、 •—セキュリティ　コンプライアンス認証90上 • 無料利用有　無料のアカウント（アプリのテスト、データ分析）
IBM (IBM.Cloud)	https://www.**ibm**.com/jp-ja/**cloud** • Iビジネス用**クラウド。**AI のビジネス活用、既存システムを**クラウド**に移行、**クラウド**ネイティブ・アプリケーション開発の両方に対応できる。・スマートビジネス GARAGE • IBM クラウド製品　業務に最適なツールを選択 • 20 業種数千社が信頼して利用 • 他ｻｰﾋﾞｽとの連携　S AP　・オラクル　・セキュリティマネジメント • ハイブリッド、マルチｸﾗｳﾄ、プライベートクラウドを統合、ﾞ環境を管理 • データ価値評価、AI に移行、オープンソーステクノロジ • セキュリティ　アプリ、サービス、インフラに組み込む
Alibaba (Alibaba Cloud)	https://jp.alibabacloud.com • 中国ビジネスに強い、中国での活躍を支援、平昌オリンピックパートナー • 業界別、機能別ソリューション • 製品　コンピューティング、ストレージ、データベース、分析、ネットワーキング、モバイル、開発者用ツール、管理ツール、セキュリティ、40 以上のプロダクトが利用可

	• セキュリティ　Web 攻撃への防御技術、中国国内と国外のセキュリティ基準を遵守
NTT communications (Enterprise Platform　service)	https://www.ntt.com/business/service/services/cloud.html
	• ICT 基盤　NTTcom のハイブリッドクラウドは通信キャリアならでの安全性、信頼できる。プラットフォームに優れたパブリッククラウドを組み合わせ、ビジネス基盤の最適化に貢献 • Enterprise cloud　　ネットワーク、データセンター、マネジメントサービス、を連携したクラウドサービス • レンタルサーバー　ホスティング　オンラインストレージ • 他サービスとの連携　office365　Google Suite 提供 • 柔軟なパブリッククラウド • ネットワークとデータセンタを一体化、災害に強い ICT 基盤 • 無料利用　無料トライアル（ファイル転送、オンラインストレージサービス）
KDDI (KDDI Cloud)	https://big.kddi.com/service/cloud-data-center/
	• トータル ICT ソリューション　データセンタやクラウド、・SaaS, ネットワークなど幅広いラインナップ • クラウドサービス　CiscoWebex Zoom　GSuite MS365 ベーシックパックプラス　LINEWorks Chatwork • 高品質、低価格、低コスト　ファイルストレージ • 通信キャリアで、障害に強い • 他ｻｰﾋﾞｽとの連携　Oracle　AWS GCP Azure • マルチｸﾗｳﾄﾞ環境対応 • データセンター　万全な運用監視、国内センター、サポート体制 • 無料利用　３ヶ月無料制度
ソフトバンク（ソフトバンク Cloud）	https://www.softbank.jp/biz/cloud
	• 多種多様なクラウドサービスで、お客様のビジネス課題解決に応える。自社活用の実績をもとにクラウドコンピューティングの可能性を最大限に引き出したインテグレーションサービスを提供 • どのクラウド製品が最適かサービスをさがす • 提供するクラウドサービス　複数の製品導入　グループウェア、オフィスツール、ファイル共有、会議ソリューションなど • 他者サービスとの連携　Google、Microsoft、Alibaba, IBM クラウド・クラウドソリューションをお客のニーズに合わせて利用する • セキュリティ　「Cybereason」「CloudGuard Dome9」など強固なセキュリティ対策の実現をサポート • 対策メニューから顧客の環境に合わせた対策を講じる • セミナー開催（オンラインも含む）
インテック（クラウドサービス EINS/SPS 仮想サーバ基盤サービス）（バックアップサービス EINS/BRS）	http://www.intec.co.jp/service/solution/cloud.html
	• 高品質・高可用な国内データセンタで運用するビジネス向けクラウドサービス • ソリューション　業種・産業別サービス　金融、製造、流通、医療、公共 • セキュリティ、ﾈｯﾄﾜｰｸサービスメニュー　・訓練、認証、診断 • セキュリティ　多要素認証システム、マルウェア感染診断サービス等 • 他ｻｰﾋﾞｽとの連携　MicrosoftAzure、IBM、オラクル、グーグルクラウドプラットフォーム • セキュアサイトの構築・運用・監視・診断を提供 • 国内サーバー

Ⅴ. 維持管理

1. クラウド導入後の維持管理

クラウド導入後の維持管理についても、(A)人まかせにするか又は成り行きに任せるか、(B)自社で意識的にクラウド活用管理をするか、考えておかなければならない。(A)の場合は依頼経費を用意する予算確保だけとなる。(B)自社で管理を考えるのなら、下記の事象を、計画し、実施し、評価する。注意して行わなければ、往々にしてトラブルを発生する元凶にもなる。主要な維持管理項目は次の通りである。

①クラウド運用のチッェクと評価(オペレーション)
②追加の管理策等の改善処置
③契約内容の見直し
④クラウド業務監査(社内、事業者)
⑤トラブル対応

2. クラウド運用のチッェクと評価　(オペレーション)

クラウド運用を自社で行う場合にしても、アウトソースする場合でも、次のような項目での評価を行う必要があると考えられる。稼働監視等のシステム運用、インフラストラクチャー運用、セキュリティ運用の3種類に分けた場合の主な評価項目を記載する。

2. 1. オペレーション管理

マニュアル維持管理	オペレーションマニュアル作成、変更管理
オペレーション監視	システム稼働監視、モニタリング、処理終了通知
オペレーションログ分析	ログ分析による処理の完了確認、処理量の計測値記録
障害管理	事前準備、特別監視、終了確認、残留リスク経過監視
レポート	運用状況の定期レポーティング

2. 2. セキュリティ管理

セキュリティ監視	24 時間 365 日のモニタリング、インシデント通知
セキュリティログ分析	原因追及トレース、原因の特定、真の脅威の抽出、予防策の設定
緊急遮断措置	影響拡大防止のための通信緊急遮断(FW、Proxy 等)
レポート	インシデントレポーティング
CSIRT 運営支援	CSIRT の相談対応、セキュリティ専門家との意見交換
脆弱性診断	Web やアプリケーションの診断
	システムのプラットフォーム診断(リモート/オンサイト)
	ネットワーク診断
	クライアント診断
データの入出力	クラウド／オンプレミスの入出力機器の設定等妥当性確認

2. 3. インフラストラクチャー・デバイス管理

機器機材監視	24 時間 365 日、セキュリティ機器の故障監視、稼働監視
機器の設定変更	ポリシー変更、ブラックリスト、ホワイトリスト追加等
パッチ・シグネチャー適用	必要に応じたパッチ・シグネチャー適用

3. 追加の管理策等の改善処置

3.1. ファシリティーマネジメント

(1)不要な施設、不足な施設、不適当な施設の使われ方が明らかになり、設備投資、施設運営費の最小化(コストミニマム)が実現する。だだし、情報管理施設として、ストレージの容量、データベースの容量など、タイトにすると、レスポンスが落ちるなどの副作用があるので注意を要する。
(2)IT 関連設備について、将来の発展、変化への柔軟な対応が自由度(フレキシビリティ)が高く維持される。ファシリティの最適化、最先端化ができる。
(3)ネットワークについて、速度、容量、の監視とバイパスの確保
(4)IT を利用して顧客に関する情報を適切に管理する CRM(Customer Relationship Management)や工場の生産ラインに IT を利用し、生産を総合的に管理する CIM(Computer Integrated Manufacturing)等への貢献が期待される。

3.2. ソフトウェア

(1)提供を受けているサービスのソフトウェアのアップデートや脆弱性チッェクの必要性はないがバージョンアップがタイムリーに実施されているかの情報管理は定期的に行う必要がある。
(2)ソフトウェアの更新や新規ソフトウェアの導入で、整合性に齟齬がでたり、テンポラリーファイルの不良などの発生がないように、事前に整合性チッェクを行うこと。
(3)市販ソフトが利用できなくなる事への注意。

3.3. アプリケーション

新たに業務をクラウド化するに当たって、対象となる業務のアプリケーションをどのように調達するか。
①クラウドサービス事業者のアプリ
②市販のアプリ
②新たにアプリを開発

4. 契約内容の見直し

4.1. 外部委託、アウトソーシング

クラウドサービス事業者への委託に関するポリシーの主な項目を例示する。委託ポリシーは情報システム戦略委員会等で IT ガバナンスとの整合性を保ち各々の組織で策定されることが前提となる。

表 14: クラウドサービス事業者への委託ポリシーの例

段階	特徴及び実践内容	備考
品質	• 自社で行っていたサービスレベルを下回らないこと	
セキュリティ	• 自社の技術者が判断できなければ、専門家を信頼するしかない（クラウドサービス事業者や独自に依頼するコンサル等）	
事業継続	• 影響範囲（顧客、サプライチェーン、従業員） • 復旧時間	
費用対効果	• 妥当性、自社満足度、顧客満足度 • 一次経費、継続的経費で評価	

5. クラウド業務の監査　（社内、事業者）

5.1. 有効性のアセスメントとしての監査

（1）提供を受けているサービスについて、例えば、メール、HP、グループウェア、オフィス（Office 製品）、ファイル管理、ファイル転送、テレビ会議等の有効性の評価をする事が望ましい。単純な評価であれば、クラウド化の前後での、コストの比較であろうが、果たして細かい原価の算出と、その比較評価ができるか、はなはだ心許ないと考える。
（2）顧客の満足度も一つの尺度である。サービスや情報提供がタイムリーでスムーズであれば、評価は高くなる。
（3）最終的には、利便性についてコスト対パフォーマンスを計数的にも、感覚的にも評価してサービスの継続をするか、他の選択肢を検討するかの作業を行い、判断する。
クラウド業務の有効性のアセスメントとして、システム監査や内部監査、外部監査を活用する。
自社の監査を具体的に希望される企業は連絡先にご一報ください。ご相談に応じます。

5.2. JIS Q 27001 及び JIS Q 27017 における維持管理

（1）JIS Q 27001 及び JIS Q 27017 を取得しているならば、審査の状況を監査と見なして対応する。
（2）取得していなければ、審査と同等の監査を社内で行うのは要員の確保や監査力量の保持が難しいので、第三者に委託する。

6. トラブル対応

6.1. 情報セキュリティインシデント対応

（1）オペレーション監視ルールに基づき、「・日時業務確認、・週次業務確認、・月次業務確認、・変更業務確認」を通して、セキュリティ事象及びセキュリティ弱点に関する、「・問題あり、・規定値オーバー、・アラーム値、・疑い、・誤動作、・誤操作、・違反、・未遂」などの検出・発見に努める。
（2）インシデント（トラブル、事件、事故、障害）が発生したか又は発生が予測される場合、その情報を入手した者は、緊急連絡網に従い遅滞なく報告する。
（3）インシデントの報告情報は、①顧客に影響を及ぼすか、②法規制の違反が発生したか、③社会的影響があるか、などの状況把握と判断をして対応する。
（4）サービスデスク機能も備えて、予防・抑制が充実する対応策である。
（5）新しいセキュリティ関連情報をキャッチする。日々進化する攻撃に対応するための仕組み（CSIRT）を構築しておく。
（6）専門的な対策スキルを持つ技術者（セキュリティ資格取得者）の確保かサポートが受けられる体制構築。

6.2. 事業継続計画（BCP）

インシデント・トラブルの中には不慣れで対応が遅れ、致命的な状況に陥ることがある。
そのため、想定するべき災害として、①地震、台風等の広域災害、②火災等の局所災害、③サプライヤーの被災等での外部サービスの停止、④悪性インフルエンザ、疫病等の感染系人的災害、⑤食中毒、交通事故等の非感染系人的災害の5種類があるとされている。

今回の新型コロナウイルスでの経験で、その範囲と影響力、対応必要性は全世界的な問題まで考慮せざるを得なくなった。

（1）自社が情報セキュリティインシデント等のトラブルが発生したときの対応として、事業継続計画を策定する。
（2）事業継続計画では、自社の危機管理として情報以外のケースも含めて、生き残りに関するポリシーとして作成する。
（3）内容はインシデントに対するリスクアセスメント、発生時の組織体制、職務と責任、対応手順を計画する。特に、復旧のための復旧対応の想定時間を設定し、顧客との合意があれば更に良いものと考える。
（4）事業継続計画書の試験を定期的に実施し、事業継続実施記録、計画の検証、計画書が最新で効果的なものであるための見直し修正を行う。

7. クラウド化の総合的評価

7.1. クラウドサービスの有益性

ビジネス上、製品・サービスのライフサイクル（Product life cycle）は市場に登場してから退場するまで、①導入期、②成長期、③成熟期、④衰退期、と4つの段階に分けられるのが普通である。各段階にある自社の製品・サービスをどのように管理して、企業業績を高めていくかが経営の鍵である。

これらは情報やデータによって管理し、下記に対応する事が求められる。

①中軸の製品・サービスに関するライフサイクル
②新規開発の製品・サービスの市場投入時期
③成熟した製品・サービスの収益性の拡大
④陳腐化製品の縮小・撤退のタイミング

7.2. クラウドサービスの将来性

クラウド化の総合的評価は将来的な要因を含めて、詳細な検討が必要なテーマが在ると考えたので、次に列挙した。

①生き残りに関するポリシー
②コンピタンスに関するポリシー
③外部委託に関するポリシー
④品質マネジメントシステムー要求事項ポリシー
⑤情報セキュリティ技術－要求事項ポリシー
⑥情報プラットフォームポリシー
⑦サプライチェーンに関するポリシー
⑧イノベーションに関するポリシー

Ⅵ. チェックリスト

1.1. 前提条件チェック

中小企業向けのクラウドサービス安全性の手引き※6−1によるチェックリストが既に提供されており、多種多様に独自性のある中小企業のセキュリティ状況の現状を踏まえて分かりやすさに重点が置かれている。しかし、Ⅱ.3.3. 中小企業のサイバー攻撃対策高度化の必要性で述べたように、リスクに企業規模の大小が無い事を踏まえ、中小企業であっても大企業と同様のクラウドセキュリティ対策が必要であるとの結論に至った。しかし、大企業のクラウドセキュリティ対策の構築は容易ではないため、Ⅱ.6. 各段階における詳細な手順・評価による段階的クラウドセキュリティ対策を実施する事が望ましいと考えられた。

しかし、各種調査の結果によると、特定の業種、企業規模、経営環境、リスク認識等もばらつきが多く、モデル化が容易ではなく、特定のステレオタイプに集約したチェックリストを策定する事も困難であった。

そこで、先ず、総務省情報通信白書※1にて報告されている中小企業のマジョリティを対象かどうかを判別し、該当する場合、後述のチェックリストを行う事を前提としています。

No	項目 補足説明	結果
1.1.	貴組織では、クラウドを何らかの形で経験した事があるか？ 中小企業の多くがクラウドを経験している調査結果があり、クラウド経験が全くない企業を本書が対象としていないため	Yes ・ No
1.2.	貴組織では、共通的なメールやファイルサーバのクラウドを利用したことがない 中小企業の割合ではサービス業が最も多く、製造業、卸売業等が利用する様な業種により利用傾向にばらつきの発生しており、どのようなシステムを利用するのかを特定が困難であった。効果の大きい共通業務に必要なクラウドを導入する事により共通業務以外のクラウドシステムやクラウドセキュリティ導入を促すことができると考えられる。既に全面的に導入されている中小企業を対象とはしていないため	Yes ・ No
1.3.	貴組織では、クラウド利用上のセキュリティリスクが高いまたはその認識があると考えているか？ 中小企業の経営者の多くがクラウドのセキュリティリスクを認識していると推定される。クラウドセキュリティリスクを認知されていない企業のためのチェックリストとしては本書は効果が得られにくいと考えられるため。	Yes ・ No
1.4.	貴組織では、クラウド利用と比較して、クラウドセキュリティの理解に経営者が積極的かどうかわからないと感じる事がある クラウドセキュリティリスクは認知しているものの、クラウドセキュリティの理解が得られにくい傾向があると調査結果がありました。クラウドセキュリティ導入に対して理解のある企業で、積極的にクラウドセキュリティが導入済の企業には本チェックリストの効果が得られない可能性があります。	Yes ・ No
1.5.	貴組織では、経営者が情報セキュリティ全般に対して充足していないと考えている 経営者の多くが情報セキュリティの充足度に対して分からないと回答している調査結果があり、ISMSにおける資産管理が十分に実施済みの場合にはチェックリストの効果が得られない可能性があります。	Yes ・ No
1.6.	貴組織では、経営リスクの優先度を考えた場合、実際のところ、サイバー攻撃や情報漏洩のリスクは低いと考えている 調査と議論の結果、セキュリティ全般としてセキュリティリスクの脅威の認識が低くインターネットに接続されている事によるセキュリティリスクは企業規模には無関係である認識はあるものの、経営上リスク対策の優先度との相関が見られない傾向がある事が明らかとなりました。サイバー攻撃リスクや情報漏洩リスクの優先度が既に高い経営者の企業では効果が得られない可能性があるため	Yes ・ No
1.7.	貴組織では、セキュリティ部門や専門家へに相談してみたいと考えている セキュリティ部門や専門家への相談意欲は高い傾向がある事が分かり、その前提でチェックリストを構成するため。当該企業としてそのような取り組みを考慮できない状況では本書のチェックリストの効果が得られない可能性があるため	Yes ・ No
1.8.	貴組織では、第三者認証を取得する検討をしたことやしてみたいと考えるが、自組織ではハードルが高	Yes

	いと考えている。	・
	セキュリティ部門や専門家に相談したいという意思はあるものの、第三者認証を取得するにはハードルが高いと考えている経営者が多いと推定される前提でチェックリストを検討しているため	No
		Yes の合計 ／8

1.2. クラウド移行チェックリスト

前述のチェックリストの結果、大半がYesとなる場合には、本書6.2. 第1段階に該当すると考えられ、第2段階へのクラウド移行が効果を得らる可能性が高いと診断した。

検討の結果、第一段階であれば、6.3. 第2段階へ移行する事でクラウドの有効性を安全に高める事ができる可能性が高いとの結論に至った。下記のチェックですべて Yes になる状態にすることで適切に第2段階へ進める様にしている。

No	項目 補足説明	結果
4.1.	オンプレミスのサーバの老朽更新など、ライフサイクルにおける老朽更新時期を迎えているか • 大企業では、従来の顧客ネットワークを活用し、デジタルサービスを面的に提供することで、新たな市場を創出するビジネスモデルによるクラウドの活用がみられる • 中小企業向け Windows2008 の切り替えを迎えた際に Windows2012 に切り替えをせずに Office365 を導入して SaaS 利用を検討した事例有 • オンプレミスに問題があったという点では、中小企業向け Windows2008 にファイル数の上限等の課題があり Office365 では制限がなくなるメリット等もある。 • 老朽更新時期にオンプレミスのサーバ更新としてクラウドを検討するのは適切な機会と考えられる。	Yes ・ No
4.2	貴組織では、共通的なメールやファイルサーバのクラウドを利用したことがなくコスト低減手法として大手サービスを利用する事に抵抗がないか • 大企業では専門の部門や専門家がいるため、フリーソフトウェアの活用も考えられる • 大手サービスによる専門性と外部サービスの利用による費用面を考慮した結果大手サービスを利用した方が安心で安価だと判断した事例もある • フリーソフトによる導入コスト抑制が、専門性が不足するために結果的に高くなる可能性があるため	Yes ・ No
4.3	自然災害対策としてのクラウド利用を検討しているか • 最近ではオンプレミスでの自然災害リスクも高まっていることからオンプレミスの安全性についても以前に比べて低下し、クラウドの安全性が高まっていると考えている。 • 水害、火災、地震などを想定したリスクマネジメントとしてクラウド利用を検討いただきたい	Yes ・ No
4.4	クラウド利用にあたり、プログラムの開発やデータベースの操作ではない設定だけのオペレーションであっても手順書の作成に時間をかけられるか • アクセス権設定は誤操作を防止するため、手順書を作成した事例があった。 • クラウドベンダからの手順書をダウンロードしただけでは抽象的なため、心配であったため念のため作成した事例があり、手順書があるのでダウンロードして利用するのではなく、クラウドセキュリティを確実にするため、個別に手順書を作成する事が必要と考えられるが、一見重複した無駄な作業にも見えるため、関係者の理解が必要と考えられる。	Yes ・ No
4.5	クラウド利用にあたりテストのために通常負担費用が増加する事に納得できるか • アクセス権設定はテストのため別アカウントを作成して実際にアクセス権が設定されている事を確認した事例があった。 • 一時的に想定費用よりも増加する事が想定される。その対応を踏まえた費用を予め想定する必要があるため	Yes ・ No
4.6	クラウド操作のためのマニュアル作成に費用がかかる事に合意できるか • 従来のオンプレミス等と異なり実際のハードウェアがある訳ではないものの、操作を間違えると費用がかかったり、費用がかかるため操作ができなかったり異なる操作をする事が懸念される。 • 慣れて覚えるという事が困難な為、詳細な操作説明書が必要となるがそのために時間と手間をかける事を理解いただく必要があると考えている	Yes ・ No
4.7.	通信の暗号化についての対策を検討しているか • クラウドまでの通信ついては SaaS 利用でブラウザの SSL 通信の他通信の暗号化状況について対策を検討している必要があるものと考えている。	Yes ・ No
4.8.	クライアントセキュリティを検討しているか	Yes

	• ブラウザ側の XSS（Cross Site Scripting)、CSRF（CrossSite Request Forgery)に対しては PC のアクセス数が少ない事から全ての PC のウィルス対策を充実させ、最新にする事を怠らず、オンプレミスの FW 等は確実に実施することが必要と考えられる。 • クラウドの SaaS にはアクセス権設定をして自社のネットワーク以外からはアクセスできないようにしてプライベートクラウドに近い状態を構築。	・ No
4.9.	クラウドで必要となる利用者のバックアップ対策を実際に行う想定をしているか	Yes ・ No
	• データのバックアップは、安価な PC と共有する設定にしてバックアップ可能にすることも必要と考えられる。 • 中小企業の場合、バックアップ容量は大企業と比べるとそれほど大きくない可能性が高い。対象のファイル容量は予め計算して確認することが必要と考える。 • クラウド上のバックアップを利用する事も考えられるが、自社で持つことを考えたため PC にバックアップできる可能性もある。	
	Yes の合計	／9

なお、更に進んだ6．4．第3段階と推定される組織では、III．対象業務の選定で指定される、資産目録の策定、ISO/ISMS 認証等、セキュリティの専門組織や専門家への委託が必須な状況と診断している。

有資格のサイバーセキュリティの専門家と相談できない状態にある場合にはリスクが高い状態にある可能性が高いと考えており、システム監査やセキュリティ監査、コンサルティング及び専門人材の育成も含め実施する事を強く推奨することが望ましいという結論となった。

参考文献

※1『平成30年総務省情報通信白書』
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd133210.html

※1−2『通信利用動向調査』
https://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html

※1−3『中小企業基本法上の類型 第13回改訂（平成26年4月1日施行）』https://www.chusho.meti.go.jp/soshiki/kaitei_13.pdf

※1−4『PMS システム概要（下記サイトの Structure of Hotel PMS より筆者作成）』
https://medium.com/@AltexSoft/hospitality-connectivity-landscape-choosing-solutions-for-your-hotel-7db9d1d9f33d

※1−5宿泊施設予約通知フォーマット標準化事業 https://www.mlit.go.jp/common/000116859.pdf

※1−6資料9：生産管理分野テキスト生産管理の要素を導入した訓練技法の開発（P180,職業訓練大学校,平野,2015）
http://www.tetras.uitec.jeed.or.jp/files/kankoubutu/b-162-14_01.pdf

※2−1『情報セキュリティ 10 大脅威 2020』https://www.ipa.go.jp/security/vuln/10threats2020.html

※6『サイバー保険に関する調査 2018』http://www.sonpo.or.jp/cyber-hoken/data/pdf/cyber_report2018.pdf

※2−3『中小企業の情報セキュリティ 対策ガイドライン　第 3 版』
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

※2−4『新型コロナウイルス感染症対策のためのテレワーク緊急導入支援』
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/jikan/telework_10027.html

※2−2サプライチェーンのセキュリティ脅威に備える
https://www.ipa.go.jp/files/000073868.pdf

※3−1. クラウドサービス安全利用の進め
https://www.ipa.go.jp/files/000011594.pdf

※4−1赤尾嘉治, サイバーセキュリティ対応を躊躇する経営陣の意思決定行動に関する考察, 経営情報学会秋全国研究発表大会,2016

※4−2『クラウドサービスの安全性評価に関する検討会中間とりまとめ（案）　平成 31 年 3 月』
http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000277.html

※6−1『中小企業のためのクラウドサービス安全利用の手引き』
https://www.ipa.go.jp/files/000072150.pdf