

クラウドの情報資産を守るために 必要な管理と対策

この資料はIPA（独立行政法人情報処理推進機構）の「中小企業のためのクラウドサービス安全利用の手引き」のチェックリストをベースに作成しております。

中小企業・小規模事業者の皆様へ

中小企業のための クラウドサービス 安全利用の手引き

クラウドサービスの安全利用、できていますか？

取り返しのつかないことになる前に...

クラウドサービス安全利用チェックシート		
Ⅰ. 選択するときのポイント		
1	どの業務で利用するか明確にする	どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？
2	クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？
3	取扱う情報の重要度を確認する	クラウドサービスで取扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？
4	セキュリティのルールと矛盾しないようにする	自社のルールとクラウドサービス運用との間に矛盾や不一致が生じませんか？
5	クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者ですか？
6	クラウドサービスの安全・信頼性を確認する	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は示されていますか？
Ⅱ. 運用するときのポイント		
7	管理担当者を定める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
8	利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
9	利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、厳密にするなど）
10	バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？
Ⅲ. セキュリティ管理のポイント		
11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取扱い条件について確認しましたか？
14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的な契約条件の各項目について確認しましたか？
15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

出典：IPA「中小企業のためのクラウドサービス安全利用の手引き」より
<https://www.ipa.go.jp/files/000072150.pdf>

Step

1

会社で利用するクラウドサービスを洗い出す

Step

2

業務や部署でクラウドサービスを分類する

Step

3

取り扱う情報の重要度を定義する

Step

4

クラウドサービスごとに管理担当者を明確にする

Step

5

利用者の権限を決める

Step

6

利用者の認証を厳格に行う

クラウドの情報資産を守るためにまずやるべきことは現状把握です。
各カテゴリで現在利用しているクラウドサービスを洗い出してみましょう。

人事 労務	採用管理	人事評価	勤怠管理	マニュアル共有			
財務 会計	給与管理 明細発行	請求書発行	財務/会計	経費精算	販売管理	在庫管理	資産管理
営業 マーケ	CRM SFA	セールス エンゲージメント	カスタマー サクセス	メール配信	電話システム		
コラボ レーション	グループウェア	ワークフロー	SNS	WEB会議			
データ セキュリティ	オンライン ストレージ	バックアップ	ID管理	セキュリティ			

①で洗い出したクラウドサービスで、どのような業務、どのような部署で、どのような情報を扱うかを整理して運用ルールを明確にしましょう。



全社

クラウドサービスA

- ◆ 電子メール
- ◆ グループウェア
- ◆ オフィス
- ◆ オンラインストレージ



経理部

クラウドサービスB

- ◆ 財務会計
- ◆ 税務申告
- ◆ 給与計算
- ◆ 労務管理



営業部

技術部

クラウドサービスC

- ◆ 顧客管理
- ◆ 販売管理
- ◆ 名刺管理
- ◆ 工数管理

それぞれのクラウドサービスで取り扱う情報が、仮に漏洩や改ざん、データの消失やサービスの利用停止などが発生した場合に、どのような影響があるかを考慮して分類しましょう。

高



クラウドサービスA

中



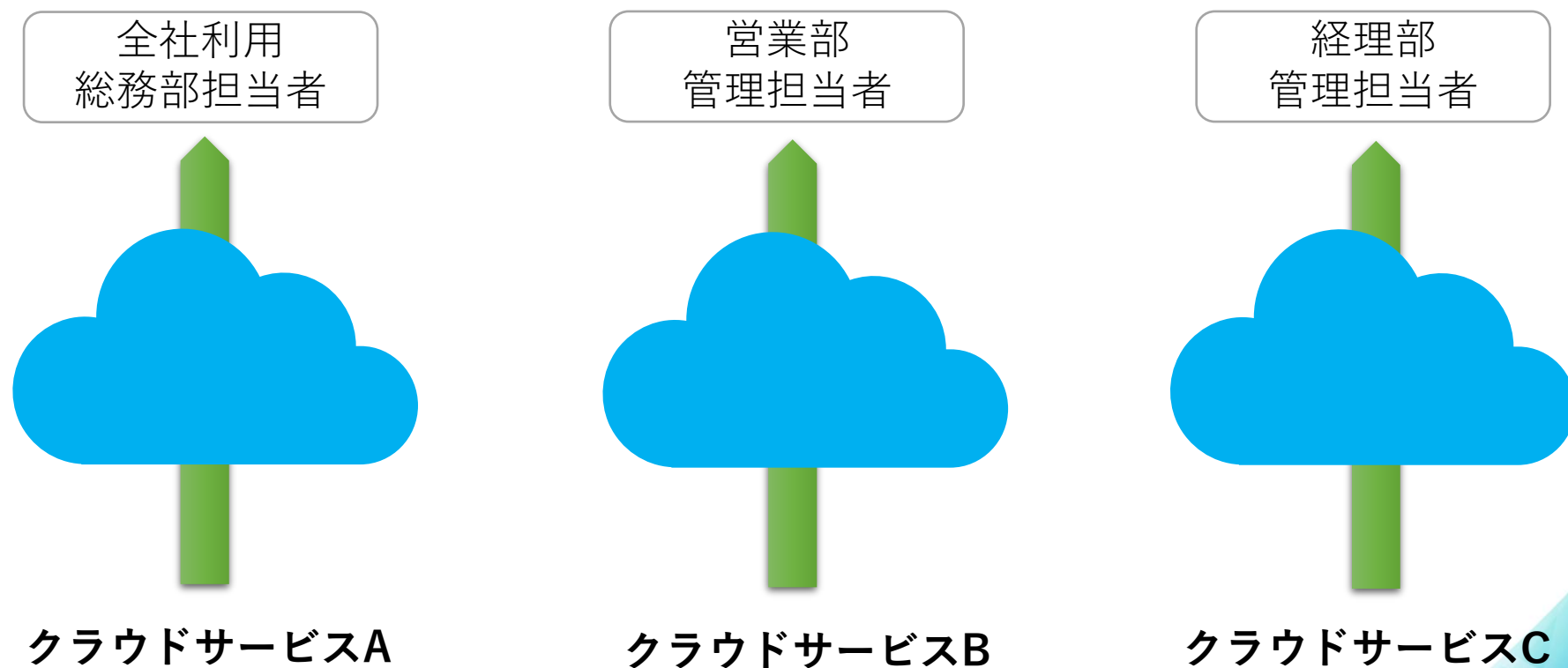
クラウドサービスB

低



クラウドサービスC

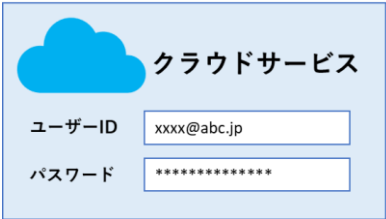
クラウドサービスの技術的な側面を理解した上で、業務に適した運用や設定・操作・ヘルプデスクを行うことができる、管理担当者を社内に設置しましょう



クラウドサービスを利用する人の範囲を決めて、どのような権限を与えるか適切に管理しましょう。

	クラウドサービスA	クラウドサービスB	クラウドサービスC
営業部	閲覧権限	アクセス不可	閲覧権限
経理部	閲覧権限	管理者権限	アクセス不可
技術部	アクセス不可	アクセス不可	管理者権限
総務部	管理者権限	管理者権限	管理者権限

パスワードなどの認証機能を適切に設定して管理しましょう

対策	詳細
パスワードは破られにくい安全なパスワードを利用する	 『*****』 8文字以上大文字、小文字、数字、記号を混ぜる
同じパスワードは使い回さない	 クラウドサービスA 『P@ssw0rd』  クラウドサービスB 『P@ssw0rd』  クラウドサービスC 『P@ssw0rd』
パスワードを不正利用されてもログインできないように「2段階認証」を用いる	 クラウドサービス ユーザーID xxxx@abc.jp パスワード ***** + 

各ステップによるアウトプットのイメージ

Step1-5で管理を行い、Step6は仕組みにまかせましょう！

No	Step 1 会社で利用するクラウドサービスを洗い出す	Step2 業務や部署でクラウドサービスを分類する	Step3 取り扱う情報の重要度を定義する	Step4 クラウドサービスごとに管理担当者を明確にする	Step5 利用者の権限を決める	STEP6 利用者の認証を厳格に行う
例	Dropbox	全社利用	高	総務部〇〇	経営層：xxxx 部長：xxxx 課長：xxxx	
1	クラウドサービスA					
2	クラウドサービスB					
3	クラウドサービスC					
4	クラウドサービスD					
5	クラウドサービスE					
6	クラウドサービスF					
7	クラウドサービスG					
8	クラウドサービスH					

導クラウドに
お任せ下さい



詳しくはこちら