中小企業のための
クラウドサービス安全利用の手引き

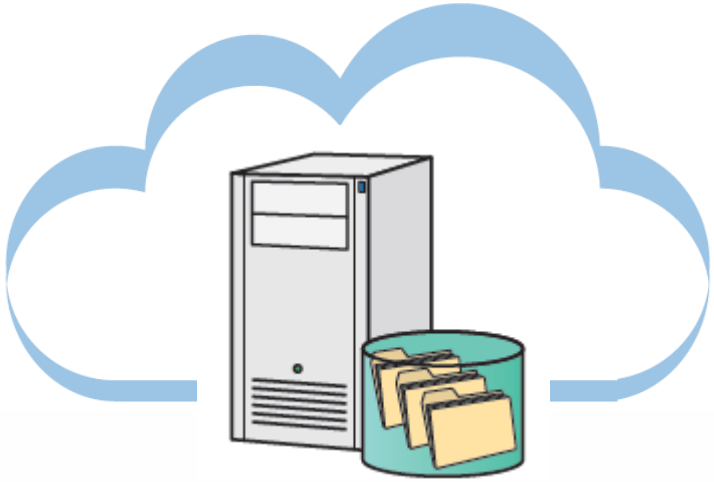
2024年7月

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

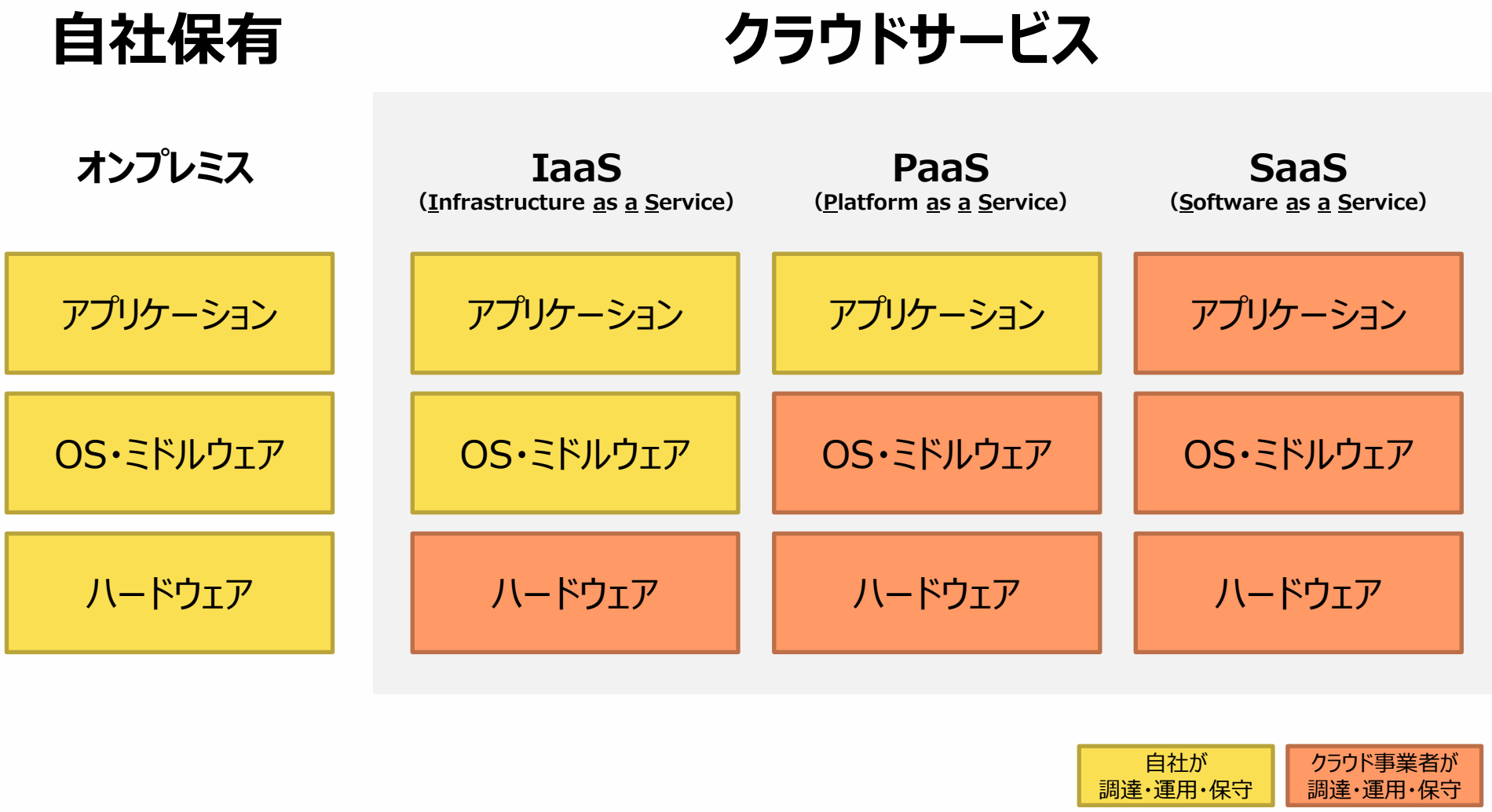
IPA Better Life with IT

クラウドサービスとは？

- インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービス
- インターネットの普及、仮想化技術など、関連技術の進展で、身近になった
- 情報システムは、雲（クラウド）の向こうのように、利用者から見えない



クラウドサービスの形態



身近なクラウドサービス（SaaS）の例

- 経営管理アプリケーション
  - 財務会計、税務申告、給与計算、労務管理など
- 業務アプリケーション
  - 顧客管理、販売管理、名刺管理、ホームページ作成、ECサイトなど
- オフィスアプリケーション
  - ワープロ、表計算、グループウェア、電子メール、オンラインストレージなど

クラウドサービス活用の利点

- ITの調達に関わる負担からの解放または負担の軽減
- ITの運用・保守の負荷からの解放または負荷の軽減
- IT資源利用の柔軟性・拡張性の獲得
- セキュリティ対策の負担と負荷からの解放または負担軽減

クラウドサービス利用上留意すべき事項

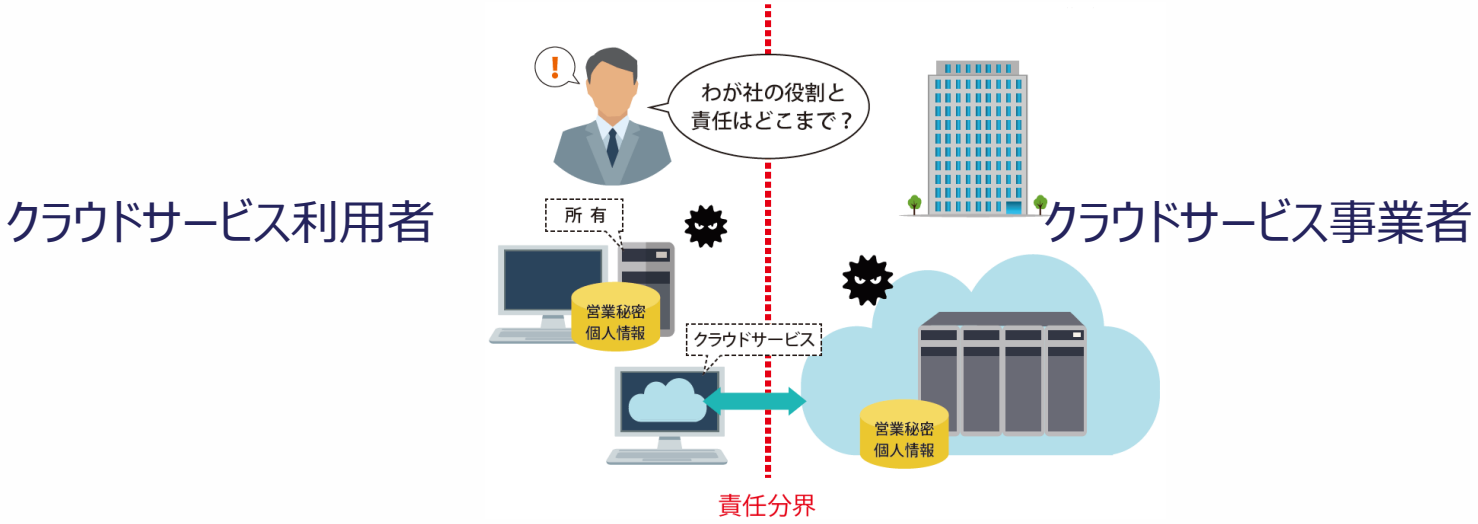
- コンピュータを自ら管理しないことによる制約
- データを自らの管理範囲外に置く、あるいは社外に預ける不安や制約
- 利用量・処理量の異常な増加や意図せぬ増大に伴う使用料の急増のリスク
- 利用できるアプリケーションのカスタマイズの制約
- アプリケーション間のデータ連携実現への制約やコスト増の可能性

クラウドサービスの事故事例

- 国立研究開発法人
  - 5,000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
- レンタルサーバー・クラウドサービス事業者
  - 5,000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
- 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

利用者がやるべきことを知っておきましょう！

- クラウドサービスのセキュリティはサービス事業者と利用者が、役割・責任を分担し、対策を実施することで維持・向上
- クラウドサービス安全利用チェックシートと解説編で利用者の役割・責任を認識して、サービスを活用



中小企業のための
クラウドサービス安全利用の手引き

- 中小企業がクラウドサービスを安全に利用するための確認事項や注意点をまとめた手引き
  - クラウドサービス安全利用チェックシートで確認すべきことが分かる
  - 身近なサービスを例に、何を確認し、どうしたら安全に利用することができるか分かる

クラウドサービスの選定

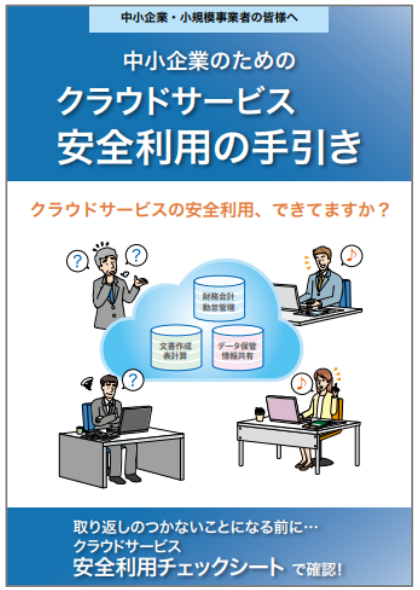
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、**業務のセキュリティ要件に見合ったサービス**を選定しましょう。

クラウドサービスの運用

クラウドサービスは**提供者と利用者が連携して運用**するため、その特性を理解して運用しましょう。

クラウドサービスのセキュリティ対策

クラウドサービス利用者が対応すべきセキュリティ対策を理解して実施しましょう。



クラウドサービス安全利用チェックシート

- 選択するときの確認ポイント（６項目）
  - 何に使うか、どんな情報を扱うか？
  - サービス事業者は信頼できるか？
- 運用するときの確認ポイント（４項目）
  - 誰が使うのか、どう管理するか？
  - 誰が責任を持つか？
- セキュリティ管理のポイント（５項目）
  - 事業者のセキュリティ対策は、サポートは？
  - データ保存先は何処の地域か？

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活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	管理担当者を決める	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、複雑にするなど）	□
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?	□

※No15 クラウドサービスのサーバーは日本国外に設置されている場合もありますが、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。
※No6,11,12,13はスマートSMEサポーター（認定情報処理支援機関）の開示情報で確認できます。

3

クラウドサービス安全利用の手引き

選択するときの確認ポイント

1. どの業務で利用するか明確にする

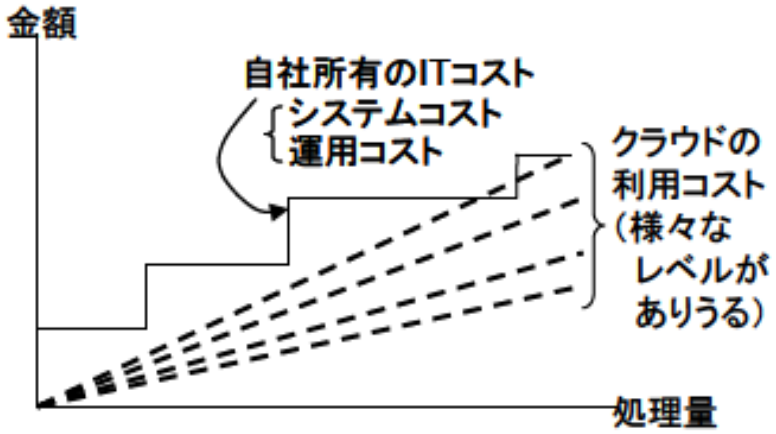
どの業務をクラウドサービスで行い、
どの情報を扱うかを検討し、業務の切り分けや
運用ルールを明確にしましたか？

- クラウドを利用する業務の選定
  （例）社内の情報共有のために
  - グループウェアを利用し、従業員のスケジュール管理を行う
  - オンラインストレージに製品カタログを保存して営業部門で共有する
- 運用ルールの検討

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？

- 業務に最適のサービスを選定
- メリットの確認
  - 業務品質は？
  - 業務コストは？
  - 業務時間短縮は？
  - その他…



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？

- 取り扱うデータの重要性を確認
  （例）個人情報、営業秘密、カタログ情報
- 漏えい、改ざん、消失、停止の影響
  （例）お客様情報の漏えい
  - 謝罪、補償
  - 個人情報保護委員会へ報告
  - 被害拡大防止、再発防止のための費用　…など

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活用との間に
矛盾や不一致が生じませんか？

- 社外に置くことを禁止しているデータ
  （例）マイナンバー、お客様から預かった情報
- ルール変更とセキュリティ対策の検討　…など

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？

- クラウド事業者の信頼性の確認

  （例）確認方法

  - 事業者が公表している財務情報を確認する
  - 利用者数などの実績を問い合わせる
  - 事業者の情報セキュリティ方針や関連した認証・認定制度の取得状況を確認する　…など

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？

- サービスの安定性、信頼性の確認
- 稼働率、障害発生頻度、障害時の回復目標時間等
- 計画的サービス停止の事前通知
- 障害発生時の通知、ユーザ対応、情報提供等
- SLA（サービスレベル合意書）の意味するもの
- サービス状態のリアルタイム情報表示　…など

【参考】クラウドサービス選択時に参考となる制度等

- **ISMAP（政府情報システムのためのセキュリティ評価制度）**
  - 政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です
- **ISMSクラウドセキュリティ認証**
  - 通常のISMS （ISO/IEC 27001）認証に加えてクラウドサービス固有の管理策（ISO/IEC 27017）が適切に導入、実施されていることを認証するものです
- **クラウド情報セキュリティ監査制度**
  - クラウドサービス事業者が基本的な要件を満たす情報セキュリティ対策を実施していることを監査し、その結果をCSマークの表示許諾を通じて利用者に対し、安全性が確保されていることを公開する制度です。
- **ASP・SaaS情報開示認定制度**
  - 安全性・信頼性に係る比較・評価・選択を行うために必要な情報を、クラウドサービス事業者が開示していることを認定する制度です。

クラウドサービス安全利用の手引き

運用するときの確認ポイント

7. 管理担当者を決める

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？

- 管理担当者の選任

  （例）クラウド型顧客間システムの導入にあたり管理担当者を選任

  - 入力項目やその活用 担当：営業部長
  - 技術やヘルプデスク 担当：システム管理者　…など

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？

- サービスが必要なのは誰か？
  （例）社長と営業部門だけ利用者アカウントを作成する
- 誰に、どのような権限を与えるか？
  （例）承認権限は管理職に付与する　…など

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、複雑にするなど）

- パスワード
  - 攻撃に対して破られにくいもの
  - ID・パスワードを共有しない
- その他の認証機能も利用
  - 電子証明書
  - ２段階認証　…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？

- 拡張機能にバックアップがある場合は利用する
- 社内のストレージにバックアップする
- 複数世代取得する　…など

クラウドサービス安全利用の手引き

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？

- 通信の暗号化（https、VPN 等）
- ファイアーウォール、侵入検知
- ウイルス対策
- 脆弱性対応、セキュリティパッチ　…など

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？

- サポート受付時間（週末夜間も受付可能か）
- 連絡方法（メール、電話、チャット、オンラインなど）
- 料金　…など

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？

- 全データの返却、パソコンなどにダウンロード
- データの互換性、移植性
- 残留データの完全消去
- 別の利用者が再利用できないことを保証　…など

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、一般的契約条件の各項目について確認しましたか？

- 利用者のデータにサービス事業者がアクセスする場合の条件や責任
- 設備の保守等を再委託している場合の再委託先の管理監督責任
- 利用者が入力した個人情報に対する個人情報保護法準拠　…など

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？

- 事業者または事業者が利用しているプラットフォーム事業者・インフラ事業者が公表するデータセンターが所在する国・地域
- 個人情報保護に係わる国内および海外の法律・規制
  - 外国にある第三者への提供（個人情報保護法）
  - EU域内　GDPR（一般データ保護規則）　…など

【参考】情報セキュリティ対策に役立つ情報

- **クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省）**
  - クラウドサービスの利用に関わるリスク対応のためにJIS Q 27002から適切な管理策を選択し、導入するための助言とその適切な実施のためのガイドラインです。
- **クラウドセキュリティガイドライン活用ガイドブック（経済産業省）**
  - 実際に発生した事故や、事業者が抱える様々なセキュリティ上の課題をベースに、ITサービスとしてのクラウドサービスに関するリスクと対策を、事業者と利用者のそれぞれについて解説したガイドブックです。
- **クラウドサービスの安全・信頼性に係る情報開示指針（総務省）**
  - クラウドサービスの安全・信頼性を向上させることを目的として、利用者のサービス選定における情報収集の負担を軽減する観点から、クラウドサービス事業者によるクラウドサービスに係る情報開示の在り方を示した指針です。

【参考】中小企業の情報セキュリティ対策ガイドライン

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
  - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載（第1部）
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明（第２部）
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録