cybozu.comの
ISMAP登録挑戦苦労話

サイボウズ株式会社 明尾 洋一

2021年11月18日

自己紹介

- 明尾 洋一
- 所属
  - サイボウズ株式会社 セキュリティ室 室長
  - Software ISAC PSIRT推進研究会 主査
- 経歴
  - 2001年 サイボウズ株式会社入社
  - 2009年 開発本部 品質保証部部長
  - 2014年 脆弱性報奨金制度開始 (PSIRT)
  - 2017年 セキュリティ室 室長 (CSIRT)
  - 2020年 PSIRT構築支援コンサルティング

PSIRT構築支援サービス

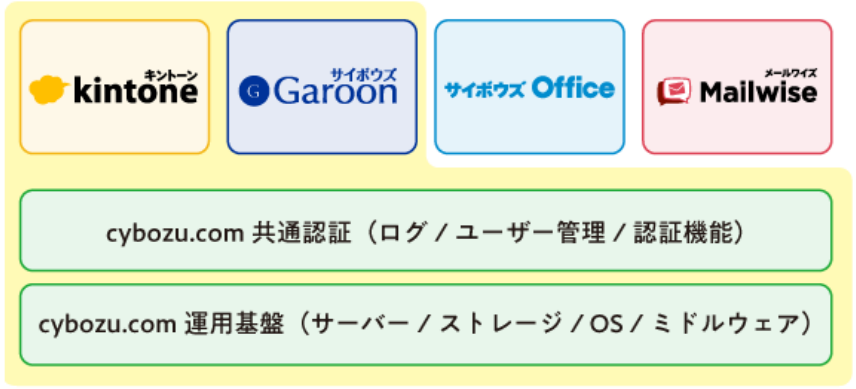
- PSIRT Services Framework (FIRST)をベースに、組織内にPSIRTを構築し、効果的な活動ができるよう支援をしています。

PSIRTに必要な6つの機能を段階的に構築してくことを支援
事例（コラボフロー様）
https://teamwork.cybozu.co.jp/report/psirt-collabo-style.html
現在2社目（メーカー様）の構築支援を実施しています。

サイボウズ株式会社

- cybozu.com（クラウドサービス運用基盤）
  - キントーン （業務改善プラットフォーム）
  - ガルーン （大規模版グループウェア）
  - サイボウズ Office （中小企業向けグループウェア）
  - メールワイズ （メール共有システム）

  をクラウドサービスで利用できるように、運用をしています。



cybozu.com / キントーン / ガルーン について ISMAP 登録完了。

Agenda

- ISMAPリスト掲載にかかった費用
- サイボウズISMAP取得の道のり
  - 内部監査への対応
  - 外部監査への対応
  - IPAへの申請および質問対応
- 利用者鍵管理
- ISMAP取らないとどうなる

ISMAPリスト掲載にかかるコストを把握し、取得の検討をいただけるように
ISMAPは困難と考えているクラウド事業者様へ、今後の施策の検討ができるように

ISMAPリスト掲載にかかった費用

監査を受けることになるので、監査費用や
社内の対応コストなど

cybozu

・監査費用（内部/外部）
・社内対応コスト

- 監査は、内部監査と外部監査の２回必要
  サイボウズでは内部監査をセキュリティコンサルティング会社に依頼
  外部監査は、弊社の会計監査を実施している監査法人に依頼
  （現在、ISMAPの監査ができるのは４大監査法人さんのみです）
- 社内体制は、ISMAPの監査法人からの証跡の要求に直接対応する事務局的な人
  および、クラウドサービスの運用・開発・検証をするメンバーが証跡を準備したり
  監査人からのヒアリングに答えるなどの対応が必要

・内部監査 外注費
・外部監査 費用

- 内部監査（コンサルティング）：ｘｘｘ
- 外部監査：ｘｘｘ
  - 取得範囲 cybozu.com運用(IaaS) / kintone･ガルーン(SaaS)
  - ISMAP管理項目の４割（最小限）を適用し、その範囲で監査を実施

cybozu

・ISMAP事務局
・クラウド運用・開発チーム

- ISMAP事務局：２名×１年
- クラウド運用・開発チーム：メイン担当は４名（情シス、運用、開発、PSIRT）
  - 運用チームの負荷が高い：資料の作成・証跡の提出・ヒアリング
    各チーム１人月(運用は重め)ぐらいを見込む必要がある

社内工数算定の条件

- **前提条件**
  - **ISMS および ISO/IEC 27017 を取得している**
    - ISMAPも、こちらの規格を参考に作られているので、**ベース**ができていた
  - **ISMAP事務局のスキル**
    - ISMS / 27017 の対応を長年実施、**規格の知識**がある
    - **開発・運用に関する知識、事務処理、コミュニケーション能力**
      - 膨大な文書の作成、証跡の収集
      - 監査法人・運用チームの話を理解し翻訳やフォローが必要
  - **開発・運用部門の協力**
    - ISMAPの**必要性を理解**、**監査対応に協力的**だった

社内工数算定の条件

- **前提条件**
  - **情報共有**
    - **ほとんどの情報が kintone** 上に存在
      運用・開発・検証に関する**事例・証跡**が、**全文検索**することで情報を引っ張ってくることが可能
    - 監査法人との情報のやり取り
      kintone ゲストスペースで実施
      ステータス・担当者管理、管理策の証跡、情報のやり取りがスムーズにできた

監査法人さんからも
弊社は、スムーズに対応できたと評価いただきました。

cybozu

サイボウズ
ISMAP取得の道のり

取得までの道のりを解説

苦労した点を中心に

内部監査への対応

Point

- クラウドの運用とは関係ないところへの監査
- 利用者鍵管理は機能の実装は必須ではない
- 制度監査なので、必ずしも証跡は必要でなくルールの存在を重視

監査期間は約3か月
2020年11月2日～2021年1月29日

- 2020年10月からコンサルティング会社さんによる事前調査が開始
- 2020年11月より、コンサルからの質問・要求への対応
- 2021年1月29日、監査終了
- 2021年2月25日、監査結果報告書完成

ISMAP管理策の末尾 P かどうかを重視

Pが付いていない管理策は、会社一般の対応状況の監査を受ける

- ISMSは、クラウドサービスの運用について適用しているため、クラウドサービスの運用・プログラムの開発については、しっかり対応しているが、会社一般のセキュリティ対策がサービス運用ほどの対策ではない部分も存在。

※外部監査では、会社一般の対応はガバナンス関連を除き監査対象にならず

cybozu

整備状況評価のため証跡は不要

- 対外的にクラウド運用について説明している文書
- 社内規則、社内文書が整備されていることが監査対象に
  - 整備状況評価ということで実際に運用されていることを示す証跡の提出は不要

※外部監査では、一定の証跡が必要となった

外部監査への対応

利用者鍵管理は必須

証跡を出さないといけないの？！

監査期間は約1か月の予定が延長
2021年3月15日～2021年4月15日
→ 2021年4月28日

- 2021年2月24日　監査法人と顔合わせ＋認識合わせ
- 2021年3月2日　監査法人より提出書類一覧が配布
  - 監査に近い問い合わせなどは、このころから開始
- 延期の原因
  - データセンターの監査に現地の人へのヒアリングが必要だが、コロナ対策のため実施できなかったことのフォロー（SOC2レポートの取得など）

ISMAPがクラウド運用の安全性を評価する制度であることを重視

P が付いていない管理策も、原則クラウドサービスの運用に関わる事項を監査

- 内部監査時に違和感のあった部分は解消された

cybozu

整備状況評価でも1つの証跡は必要

- 採用している管理策について、すべて運用の実績を示す証跡を探し提出する必要がでてきた
  - 絶望　!(°Д° ||)

利用者鍵管理の管理策は機能実装が要求されていると判断

10.1.2.20.PB クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。

- cybozu.com では、機能がない
  - 採用が必須の管理策なので、もう絶対ムリ。絶望的　!(°Д° |||)

※どう対応したかは、別途詳しく

IPAへの申請および質問対応

データセンターへのヒアリングは必須（SOC2レポート提出しても現地もしくはオンラインでのヒアリングが必要）

利用者鍵管理を除外するチャット機能ではないことが指摘

データセンターのメンバーへのヒアリングは必須

データセンターのSOC2レポートは提出しているのに

- 監査法人に連絡、データセンターと調整を実施
  - 監査法人：DCとのNDA締結は直接の契約相手ではないので難しい
  - DC：コロナ禍でのグローバルの規則なのでムリ
- 双方に歩みよっていただき、NDA締結、リモートでのヒアリングを実施いただき無事終了（8月12日）

cybozu

利用者鍵管理機能が提供されていないけど

- こちらについては、経緯を次の節でまとめました

cybozu

利用者鍵管理

利用者鍵管理とは？

どう対応したか

利用者鍵管理機能とは？

クラウドサービスに保管するデータを暗号化するための暗号鍵を利用者が作成、廃棄などできるようにする仕組み

- クラウドサービスに保管されるデータは一般的に暗号化されて保存されています。
- その暗号化をするための鍵を、利用者が生成し、任意のタイミングで廃棄するなど、ベンダーに鍵管理をさせない仕組みのこと

cybozu

利用者鍵管理すると何がいいの？

クラウドサービスを解約する際に、データの削除が確実に実施されるか不安な場合、暗号鍵を廃棄してしまえばデータを復号できず、ベンダーに不正に利用されたり、漏えいする可能性がなくなる
また、利用者のみアクセス可能な場所に暗号鍵を保管しておくことで、クラウドサービスベンダーによるデータの不正利用を防止できる

- 契約解約時のデータの安全性の確保
- ベンダーの不正利用の防止
- BYOK (Bring Your Own Key) とも呼ばれています
- 参考資料（クラウドサービスの鍵管理 CSA著）：
  (https://www.cloudsecurityalliance.jp/site/?p=17000)

cybozu

BYOKの問題点

いわゆるBYOK（Bring Your Own Key）や同様のモデルをクラウドサービスで使用したBYOKの意味は、通常期待される結果が得られないことを示しています。これらのいわゆるBYOKモデルを使用しようとしているほとんどの組織は、クラウドサービスプロバイダが利用者のデータを裁判所や法執行機関などの第三者に引き渡すことを強制できないことを期待しています。ただし、いわゆるBYOKモデルのほとんどのベンダーにおける実装では、クラウドサービスがデータ暗号化鍵を使用しているため、必要に応じてエクスポート用に暗号化されていないデータを生成できるので、実際にはその結果を防げません。（CSA クラウドサービスの鍵管理 P40 より）

- 一部ベンダーの BYOKの実装はベンダーが必要に応じて鍵を利用するようになっている（単に利用者が鍵を生成･廃棄できるというだけ）
- ベンダーの不正利用防止という目的は達成できないBYOKの実装となっているものも。（鍵を利用できない実装のケースもある）
- SaaS はデータの中身を処理（ソート、抽出など）してサービスを提供しているので、ベンダーがデータを処理できない実装だと、SaaSとしての便利な機能は実装できないことになる

cybozu

内部監査：機能は必須でないので機能がない旨、対外的に告知
外部監査：機能必須とのこと、FAQに除外事由と記載があった
「チャット機能」が存在すると説明
IPAの質問：チャット機能ではないと突っ込み

- 内部監査：安心していました。
- 外部監査：FAQを見てなんとか機能実装できない理由を検討、kintone ゲストスペース機能を「チャット機能」と解釈し、除外事由にあたるので機能実装していないことを説明。
- IPA：FAQでいう「チャット機能」ではないとの見解。

利用者鍵管理/サイボウズの対応　続き

内部監査のコンサルに相談
機能実装が必須となっている、チャット機能と説明していることなどを相談
IPAへの質問への回答に
SaaSでの実装は困難であることを説明

- ISMAP制度設計に関わっていた方もおられたので、各方面にあたってもらう。
- SaaS としての機能を実装するうえで、完全な形での利用者鍵管理の実装は、サービスを提供できなくなることを説明。

必須機能ではなくなりました

FAQが書き換わっています。サイボウズのサービスも無事リストに載りました。

- 機能実装がないSaaSベンダー様も安心して申請してください
  - FAQ:
    https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010098

ISMAPを取得しないとどうなる？

取らないと、政府からの受注は絶対にないの？

ISMAPに載ってなくても採用の可能性はある

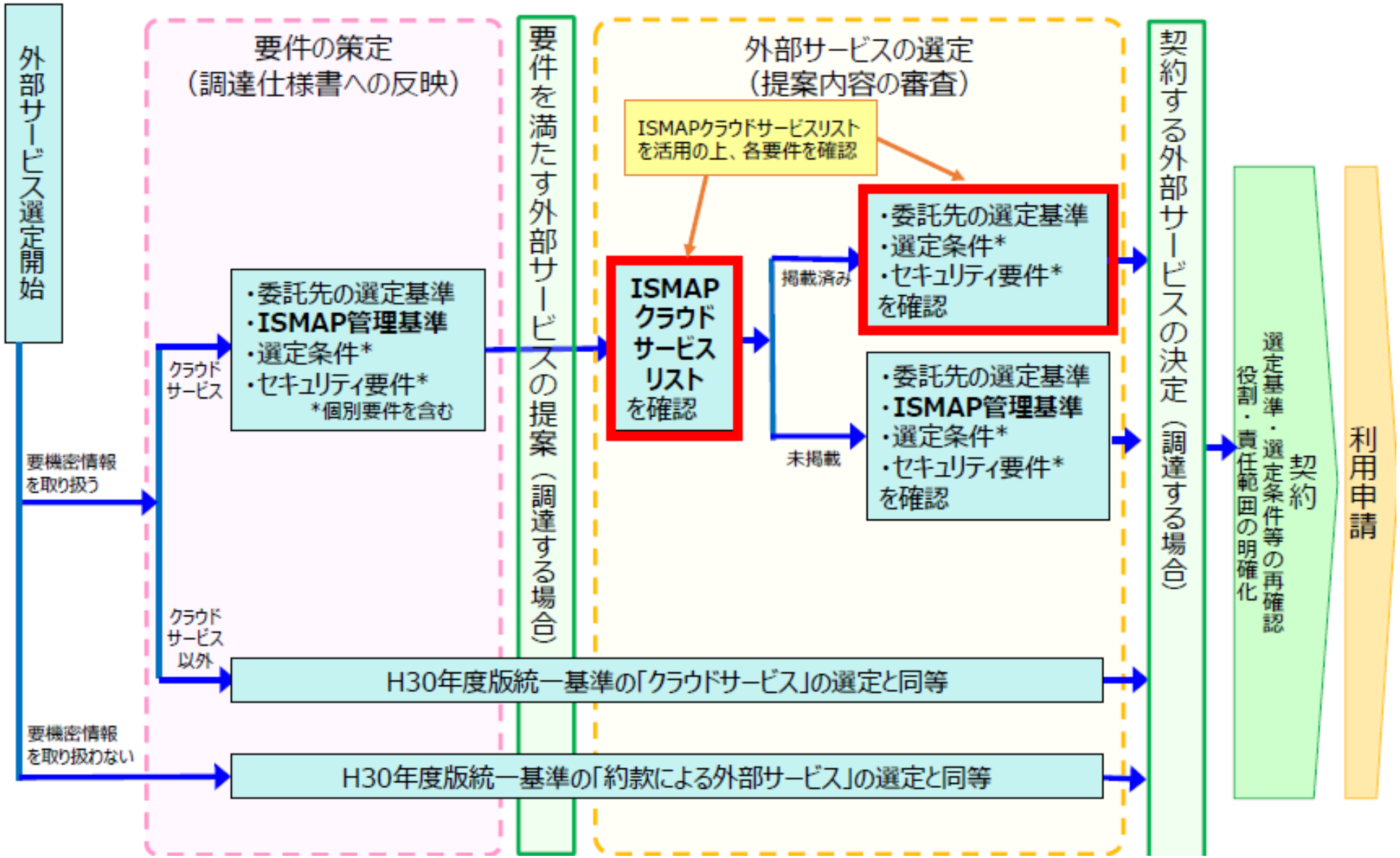
政府機関向け情報として、調達の方法が記載されています。（P13）

https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010265

※統一基準と呼ばれているものはこちら
https://www.nisc.go.jp/active/general/kijunr3.html

- ISMAPリストに掲載がなくても ISMAPの管理基準 を確認し、問題なければ採用可能というフローになっています
  - とはいえ、ISMAP管理策の準拠は必要なので社内対応を進めていただければ

令和３年度版統一基準群に基づくクラウドサービス等の選定の流れ



cybozu

総務省のガイドライン

「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」

https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html

- ISMAPの監査を受けるのが厳しい中小クラウド事業者向けの対策を記載、リスト化することで、最小限のセキュリティ対策をまとめています
- 中小クラウド事業者は、こちらの Annex Ⅱ のリストを対策し、情報公開することで地方公共団体の選定に合致させる策を打つとよいと思われます

まとめ

まとめ

- コストは決して安くない
- ISMAP取得するには、人的な投資も必要
- しかし、今後クラウドファースト、制度の活用（地方公共団体・民間）が進むと取り残されるリスク

- 制度の状況を注視しながら、セキュリティ投資、人的投資を進め
  ISMAP登録リストに載れるような体制づくりを進めていくことをお勧めします

- まずは、総務省の情報セキュリティガイドラインから始めることをお勧めします