お客様のセキュリティチェックを乗り越えるための SaaS のアプローチ

Cyber-sec+ Meetup vol.3

2024/03/12 幸田 将司

Who am I?

幸田将司:

所属:

- 株式会社Levii
- 株式会社バラエナテック 代表取締役
- SecuriST(R) 試験委員会 / CEH インストラクター
- ISOG-J(WG1)
- 診断 / 開発 / ISMS支援 ...etc

SNS:

- @halkichisec

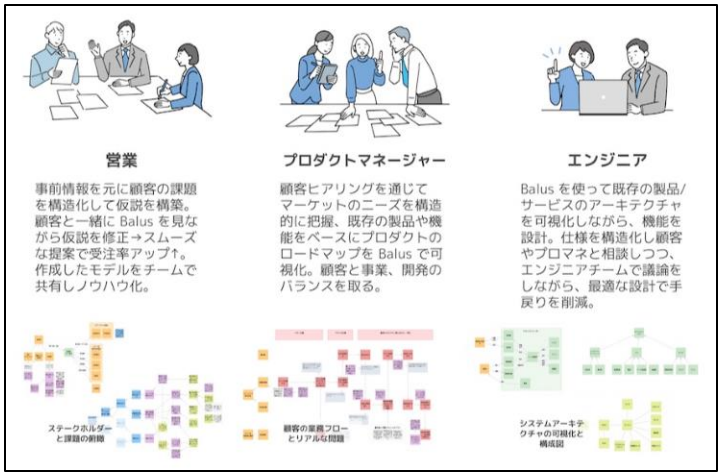
Contents

誰向け?

- **サービス事業者**
  - セールス
  - デリバリー
  - 開発
- **セキュリティ系**
  - CISO
  - 診断員
- **サービス調達/選定する人**
  - 情シス

SaaSを提供しています(ダイマ)

- **Balus**
  - システムモデリングをわかりやすくするツール
  - 名前は某ジブリ作品の呪文より
  - 登録商標で揉めてしまう



これのセキュリティの話

SaaSが苦慮するセキュリティ

- **サービス提供側として苦悩していること**
  - どこまでセキュリティをやるべきか
  - 何にリソースを割くべきか
  - 認証規格を取得するべきか

- **お客様に使って欲しいが…セキュリティ的なハードルは高い**
  - クラウドサービスの調達要件
  - 官公庁は基準が高い

- **我々はコストセンターである😭**

SaaSが苦慮するセキュリティ

- **サービス調達の要求事項としてよくある例**

1. 認証規格を取得しているか

- ISO/IEC 27001(ISMS)
- ISMAP
- SOC2
- SSAE16,18

...etc

SaaSが苦慮するセキュリティ

- **サービス調達の要求事項としてよくある例**

2. セキュリティチェックシートの記入

- サービスが使用できるかどうか質問やチェックリスト形式で構成された文書、大抵はエクセルで送られてくる。
- 顧客 ↔ セールス ↔ 開発でやり取りしてリソースが勿体無い

No.	項目	規定内容	可否	備考
1	ID とアクセス管理（IAM）	利用者のユーザ ID 設定や利用者のデータへのアクセス、システムへのアクセスに関する設定項目がある。	○	
2	ロギングとモニタリング	ロギングは、全てのレイヤに関連し、システムの運用条件によってどこまでモニタリングするかが決まり、それに対応する設定項目がある。	○	
3	オブジェクトストレージ	利用者のファイル等を格納するためのオブジェクトストレージに対する設定がある。オブジェクトストレージの動作等を規定するミ	○	
4	**インフラ管理**			
5	仮想マシン（VM,VPS）	仮想環境レイヤに対応する設定項目がある。	○	

お客様毎に項目やフォーマットが異なるためコストがかかる

何から取り組めば良いか

- **頻発する要件をセキュリティチェックシートとして公開**
  - セキュリティチェックシートの対応ログを残しておき、その結果を社内で共有する。
  - 共有した項目から自社のセキュリティチェックシートを作成して公開
  - コストが下がった

- **開発のメリット**
  - 顧客が要求する機能が把握できるので、実装が予想できる。

- **営業/デリバリーのメリット**
  - 顧客↔セールスのリレーが少なくなるので顧客へのレスが早い

セキュリティチェックシートについて

- **よく聞かれる項目TOP5**

顧客が気にしていること

1. アクセス制御

- IPアドレスによる制限が可能であるか
- Basic/Digest認証が設定可能であるか
- 利用者毎に管理者が設定可能であるか

2. 権限管理

- ユーザと管理者の領域がわかれているか

Basic認証に使うからAPIの認証は
Authorizationヘッダを避けるか…
(safariは上書きしてしまう)

セキュリティチェックシートについて

3. ログの取得/監視(一例)

- ログイン成功と失敗
- 異常ログの検知と通知

4. 脆弱性管理

- 脆弱性診断を実施しているか
  (どこまで実施するかは問われないことが多い)
- 脆弱性管理が行われているかどうか

5. 第三者認証の取得

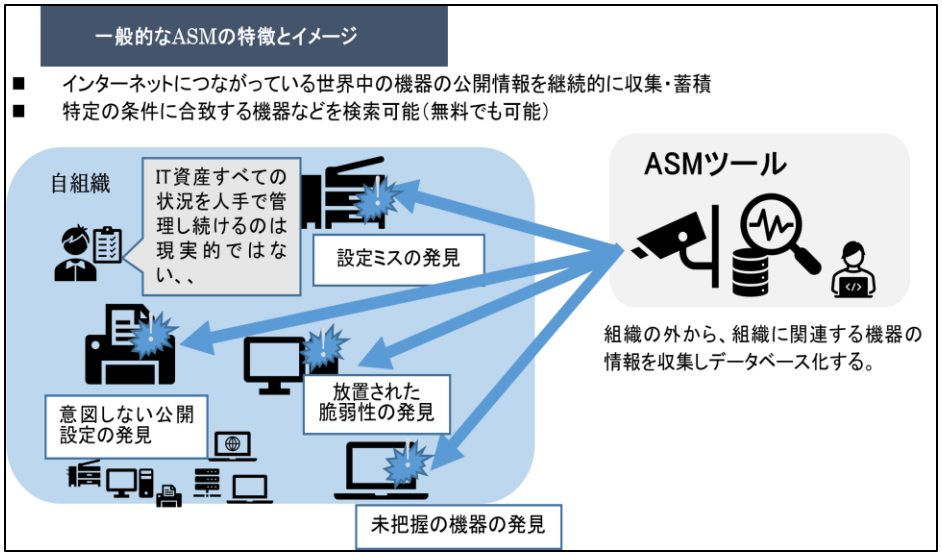
- ISO/IEC、SOC2等々...

コストはかかるが
何かしらの認証はあると良い

どこまで脆弱性管理をすればいい?

- **攻撃表面を元にして考えると良い(ASM)**

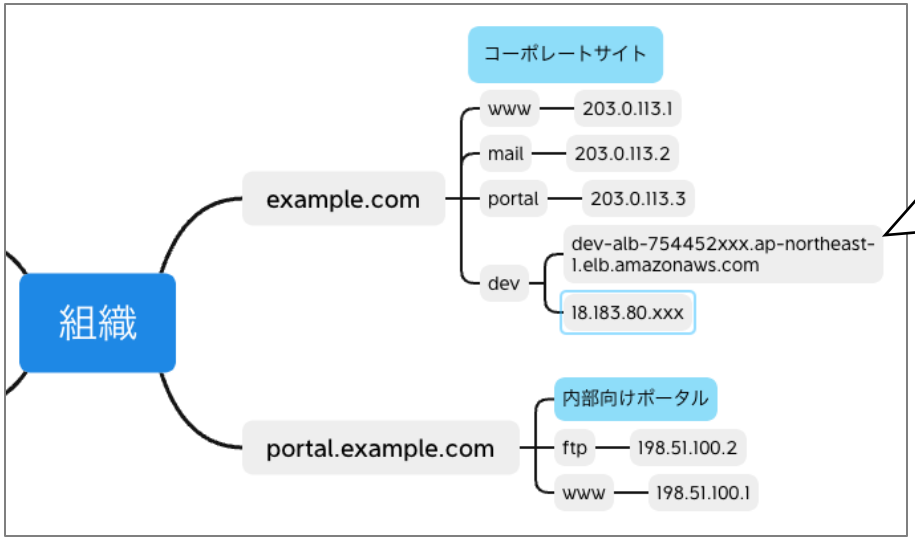
- 例:
  - コーポレートサイト
  - 自社サービス
  - メール/VPN/ファイルサーバ等
  - 担当者のメールアドレス



出典: 経済産業省ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

攻撃表面(Attack Surface)の例

- 自社サービスに紐づいているが、管理が忘れ去られているコンテンツ等



ベンダーのために
開けておいた経路

※IPに紐づくコンテンツサーバがなくともサブドメインテイクオーバーの温床になる可能性も。CNAME、Aレコード等

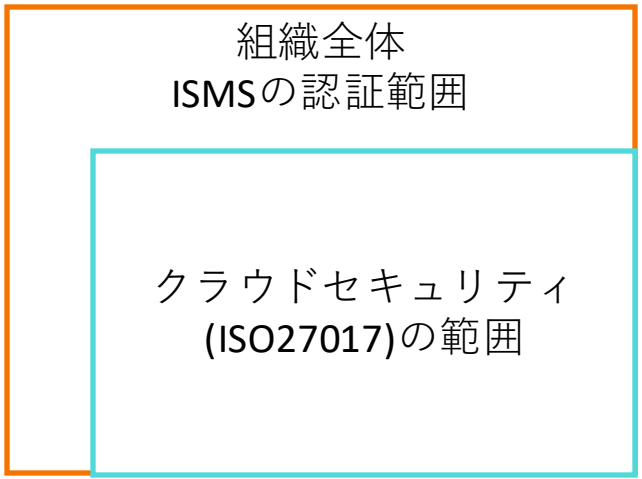
バグバウンティではよく報告されている

第三者認証を推す理由

- **サービス事業者として要求される内容や管理施策が理解できる**
  - SLAの設定
    (稼働率の根拠や、侵害されてはならない理由が説明できる)
  - 情報資産とその監視対象の考え方
- **第三者の審査機関から指摘がある**
  - 問題のある管理に気がつける
  - 外圧がなければ変われない組織におすすめ

認証規格の例(ISO27017 クラウドサービス)

- ISO/IEC27017
  - ISO27001(ISMS)のクラウドサービス版
  - ISMSのアドオンとして存在するため、ISMS + ISO27017で取得する
  - CSP又は、CSPとCSCとして認証する必要がある。
- CSP(クラウドサービス提供者)
  - AWSやGCP等、プラットフォーム提供側
- CSC(クラウドサービス利用者)
  - クラウドサービス利用者側



認証規格の例(ISO27017 クラウドサービス)

- **要件(CSPとしての一例)**
  - 9.2.1 利用者登録及び登録削除... アカウントの登録/削除ができるか
  - 8.2.2 情報のラベル付け... 情報のラベル付けができるか
  - 10.1.1 暗号による管理策の利用方針... 情報の暗号化ができるか
  - 12.3.1 情報のバックアップ
  - 12.6.1 技術的ぜい弱性の管理... 脆弱性管理がされているか

- **要件(CSCとしての一例)**
  - 9.2.3 特権的アクセス権の管理... 管理者アカウントを制限し、他要素認証を使用する
  - 16.1.2 情報セキュリティ事象の報告... インシデント情報の管理

認証規格の例(ISO27017 クラウドサービス)

- 前項の内容で適用宣言書を作成し、審査を受ける

A.3　適用宣言書（SoA）

ISMSクラウドセキュリティ認証では、本文書の4.2.2 d) に基づき適用宣言書を作成する。次に適用宣言書の例を示す。

適用宣言書 (カスタマ/プロバイダ) ※1

※1 いずれか、もしくは両方に○。

※2 ISO/IEC 27017 に実施の手引が示されている管理策

管理策	管理策を含めた理由	27001[管理策]の実施の可否	27017[管理策※2]の実施の可否		除外理由
			カスタマ	プロバイダ	
ISO/IEC 27001:2013 附属書 A					
A.5.1 情報セキュリティのための方針群					
A.5.1.1 情報セキュリティのための方針群	・～のため	○	○	○	
A.5.1.2 情報セキュリティのための方針群のレビュー	・～のため	○	—	—	27017 には追加の実施の手引なし

100項目以上あるため、
コンサル系サービスを利用するのが吉

出典: ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項
https://isms.jp/doc/JIP-ISMS517-10.pdf

クラウドサービスの参考資料

クラウドサービス利用・提供における適切な設定のためのガイドライン：総務省 2022

https://www.soumu.go.jp/main_content/000843318.pdf

- 運用上のベストプラクティスがあるため参考になる

クラウドサービスレベルのチェックリスト：経産省

https://warp.da.ndl.go.jp/info:ndljp/pid/8658576/www.meti.go.jp/press/20100816001/20100816001-4.pdf

- ちょっと古い(2010年)

攻撃可能領域の探し方(内部)

- 内部からの調査は部署を横断する必要がある。

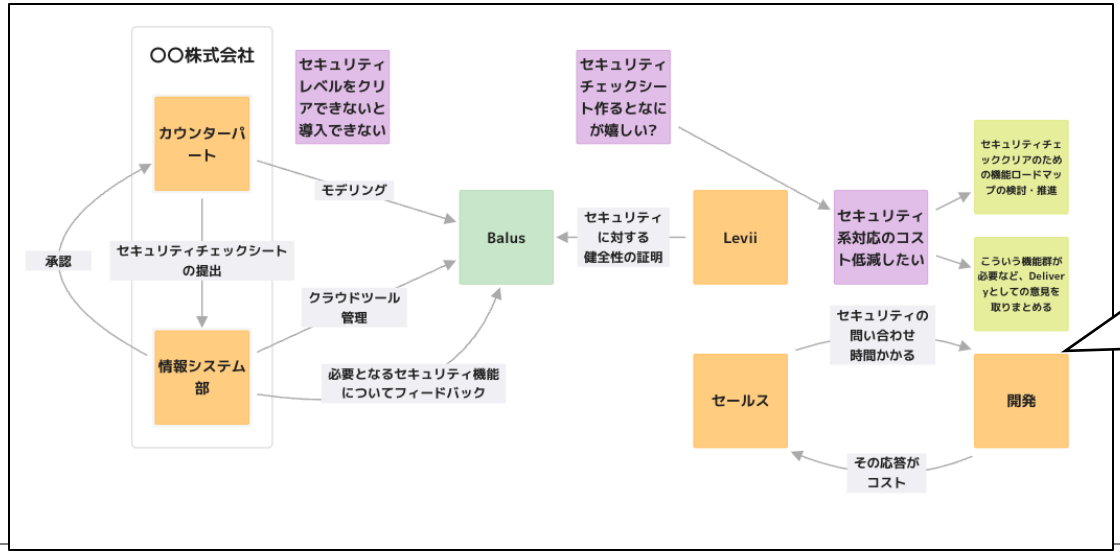
- インシデント例
  - (2021年)内閣サイバーセキュリティセンター(NISC)の情報漏洩
  - 内部で使用していたプロジェクト情報共有ツールへの不正アクセス

- 組織内部で使用している端末やツールの特定を行う
  - ISMS(ISO27001)を取得しているなら情報資産管理/リスク台帳があるはず
  - 管理している部署と連携をとることを推奨
  - シャドーITの制限も忘れずに

参考：組織を巻き込む

- そもそも職務により目的/視点が違うため、各チームの代表をまきこんでモデリングすると、少しスムーズに進むかも

- セキュリティチェックシートを作る際のMTGの例



それぞれのロールの
背景や目的を同じ視点でみるための手法

おわり

- ご清聴ありがとうございました