やはりタグ　タグは全てを解決する

aws dev day

2021/09

所属先紹介 & 自己紹介

- 名前: 鈴木研吾 (@ken5scal)
- 所属:
  - LayerX株式会社 CTO室
  - 三井物産デジタルアセット・マネジメント出向
- 来歴
  - 証券向けManaged Security Service、家計簿・クラウド会計、証券会社
- 個人の活動
  - 同人「Secure旅団」にてPodcast「Secure Liaison」や同人誌作成
  - 週刊「忙しい人のためのセキュリティ・インテリジェンス」発行
  - PodCast「Secure Liaison」を（ほぼ）Weeklyでリリース
  - 書籍
    - O'Reilly「Zero Trust Network」監訳
    - インプレスR&D「アイデンティティはだれのもの？Hyperledger Indy & Ariesで実現する分散アイデンティティ」著作

弊社のミッション

すべての経済活動を、デジタル化する。

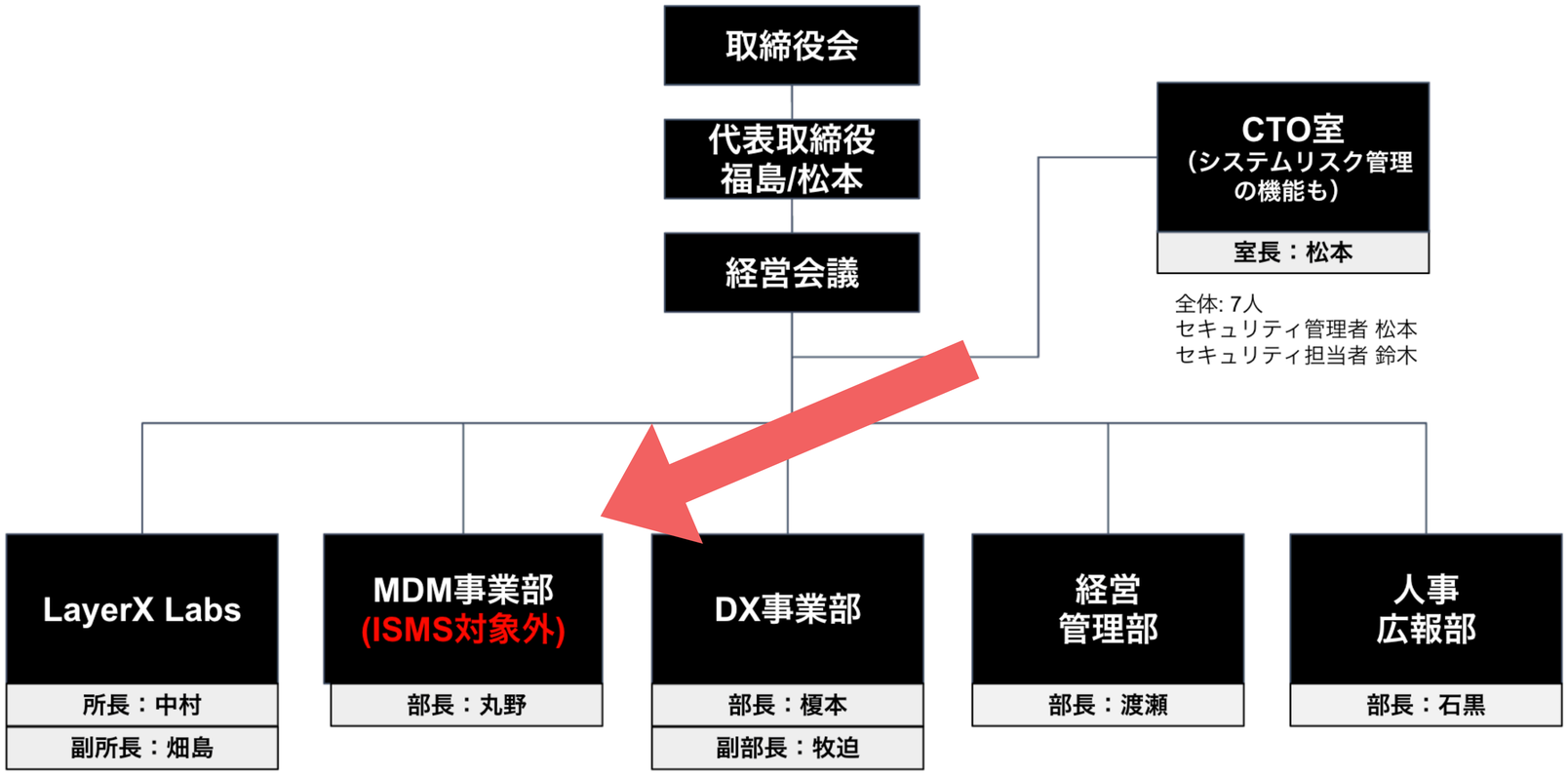
ブロックチェーン技術をもとに、「新たな経済基盤」をつくりだす。
それは、信用や評価のあり方を変え、
業務や生産をはじめとした経済活動の摩擦を解消し、
この国の課題である生産性向上を実現する。
私たちは、そう信じて行動し続けます。

ブロックチェーンが実装された社会、
そこには、これまでの延長にはないまったく新しい可能性が広がっている。
LayerXは、デジタル社会への発展を後押しすることで、
経済史に新たな1ページを刻んでいきます。

ブロックチェーンの会社
ではないです

https://note.com/fukkyy/n/n7f60e18db2c6

所属先その①

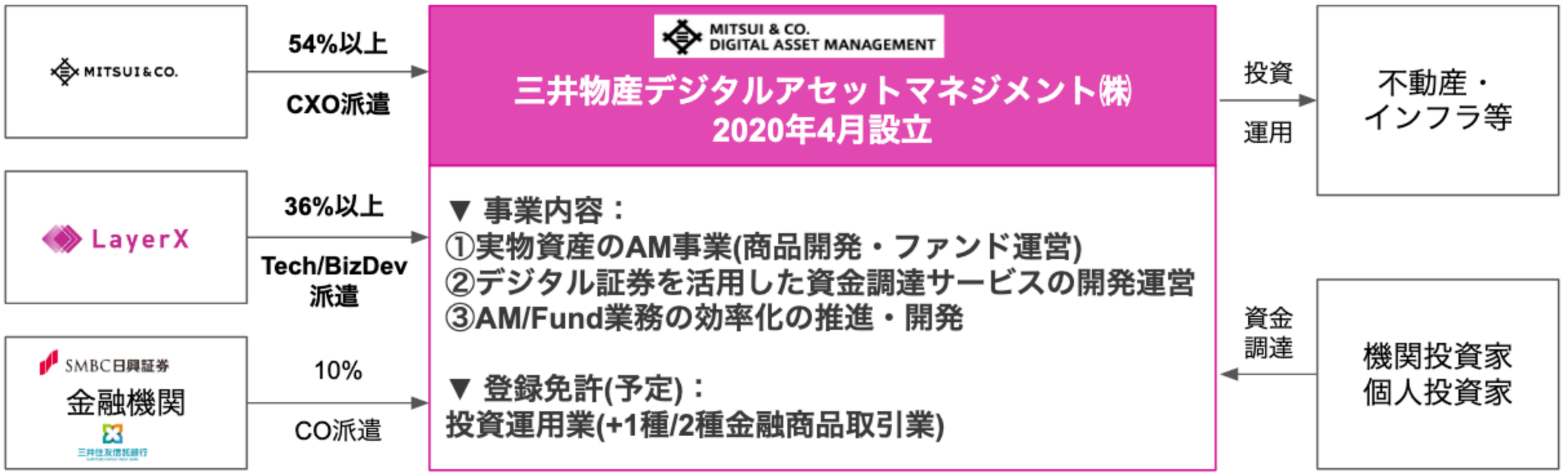

取締役会
代表取締役
福島/松本
経営会議
CTO室
（システムリスク管理の機能も）
室長：松本
全体: 7人
セキュリティ管理者 松本
セキュリティ担当者 鈴木
LayerX Labs
所長：中村
副所長：畑島
MDM事業部
(ISMS対象外)
部長：丸野
DX事業部
部長：榎本
副部長：牧迫
経営
管理部
部長：渡瀬
人事
広報部
部長：石黒

取組事例: 三井物産とアセットマネジメント領域で協業

JVを設立、共同事業として証券発行プロセスやファンド期中管理のDXを推進

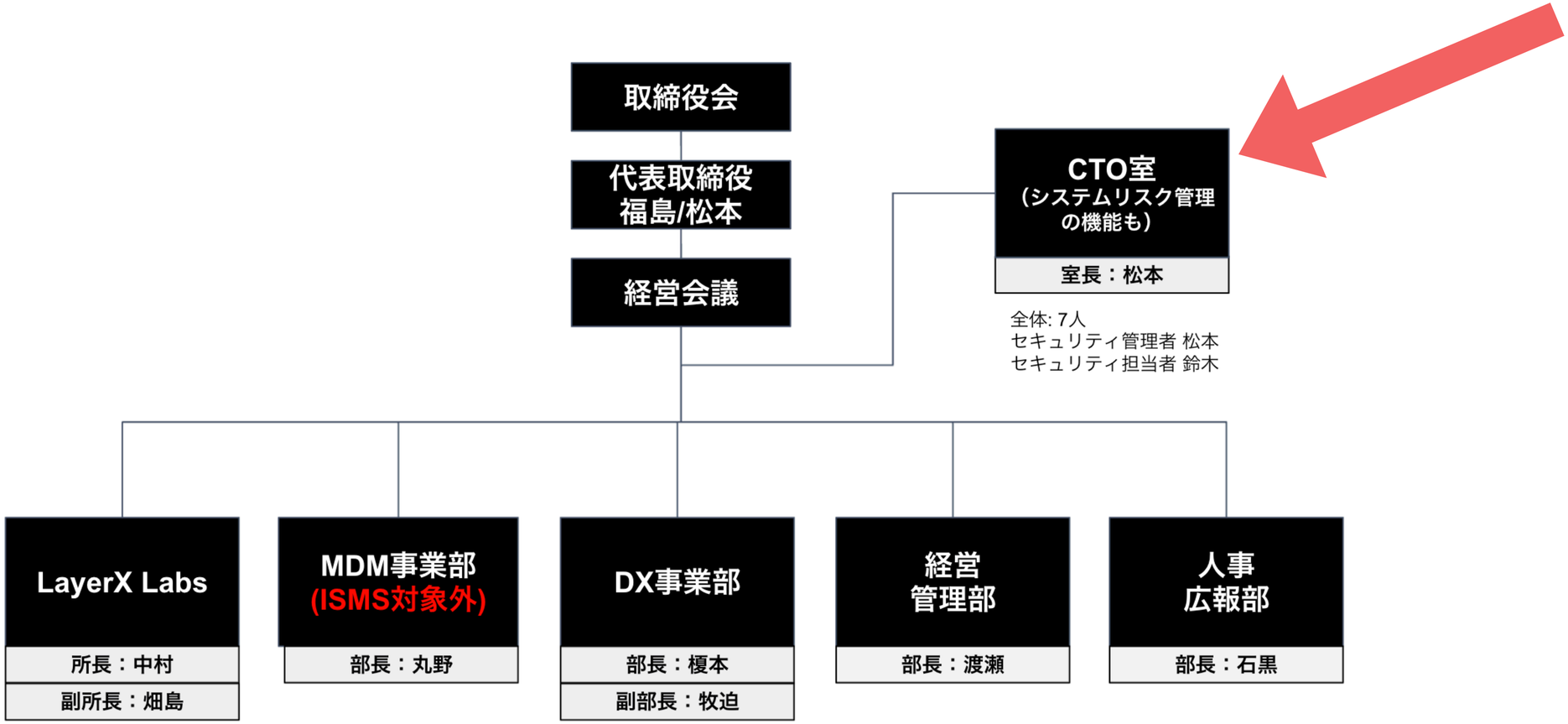
- アセットマネジメント領域にデジタル技術をフル活用
- 紙とFAXがはこびるファンド商品組成・資金調達・運用プロセスを効率化し、商品の収益性を向上
- デジタル証券を活用し、今まで証券化されなかった新たな投資商品を創造する

ジョイント・ベンチャーを通じた事業共創



インフラ・デザインドキュメント

所属先その②


取締役会
代表取締役
福島/松本
経営会議
CTO室
（システムリスク管理の機能も）
室長：松本
全体: 7人
セキュリティ管理者 松本
セキュリティ担当者 鈴木
LayerX Labs
所長：中村
副所長：畑島
MDM事業部
(ISMS対象外)
部長：丸野
DX事業部
部長：榎本
副部長：牧迫
経営
管理部
部長：渡瀬
人事
広報部
部長：石黒

2021-09-03

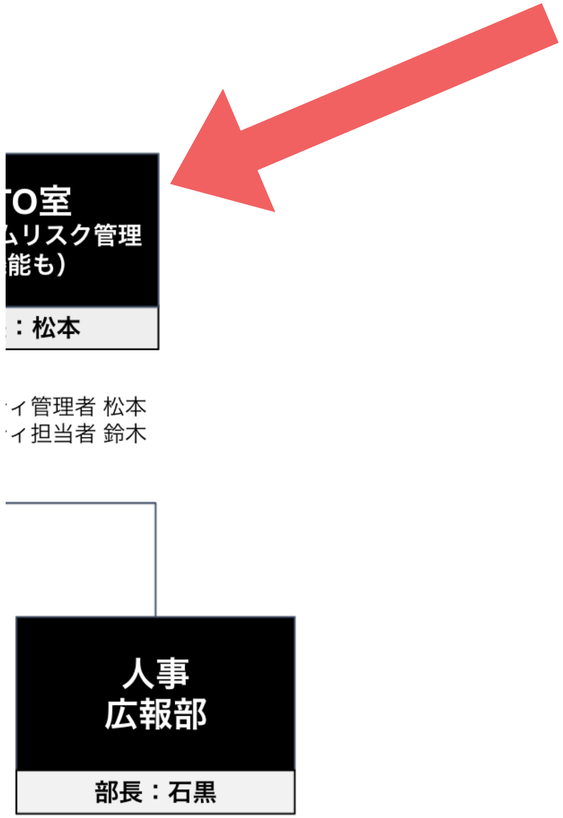
ISMSもとったし、エンジニアだけどITガバナンス主導してきた話をする

セキュリティ　組織・文化

CTO室 @ken5scal です。座右の銘は「当社はブロックチェーンの会社ではもうありません」です。 主にインフラ構築・運用をしたり、社内の基盤を整えたり、不具合を特定して `git blame` したら自分のcommitで泣いたりしています。

当社は「すべての経済活動を、デジタル化する」というミッションを掲げており、生産性向上の達成という価値を新しいサービスによって提供しています。

しかしながら、新しい価値にはリスクが伴います。信頼できない価値を提供するサービスを採用する合理的な判断はありませんので、お客様に価値を価値のまま提供しなければlose-loseな関係になってしまいます。



2021-09-03

ISMSもとったし、エンジニアだけどITガバナンス主導してきた話をする

セキュリティ　組織・文化

47 B!ブックマーク　12 シェア　ツイート

CTO室 @ken5scal です。座右の銘は「当社はブロックチェーンの会社でん」です。 主にインフラ構築・運用をしたり、社内の基盤を整えたり、不`git blame` したら自分のcommitで泣いたりしています。

当社は「すべての経済活動を、デジタル化する」というミッションを掲げ上の達成という価値を新しいサービスによって提供しています。

しかしながら、新しい価値にはリスクが伴います。信頼できない価値を提採用する合理的な判断はありませんので、お客様に価値を価値のまま提供loseな関係になってしまいます。

ISM
てき

ナンス主導し

セキュ

4
B!ブッ

CTO
ん」
git

当社
上の

しか
採用
lose

【CTO室】屋台骨エンジニア

株式会社LayerX

【共通_CTO室】Corporate Ops

応募

動物的に
大胆に
100
Layer

本日のお話

CTO室 屋台骨エンジニア

本日のお話

本日のお話

本日のお話

エン

【CTO室】屋台骨エンジニア

株式会社LayerX

【共通_CTO室】Corporate Ops

応募

動物的に
大胆に

100
Layer

本日のお話

話さないこと

- 話すこと
  - 当社のタグ管理の変遷
- 話さないこと
  - 当社のタグを活用した運用

アジェンダ

- Whyタグ管理
- 当社のタグ管理
  - Tag ver0
  - Tag ver1
  - Tag ver2
  - Tag ver3(未来の話)

Whyタグ管理

（いきなり脱線）ゼロトラスト

Amazon Web Services ブログ

ゼロトラストアーキテクチャ: AWS の視点

by Koichiro Watanabe | on 11 DEC 2020 | in Foundational (100), Security, Identity, & Compliance | Permalink | Share

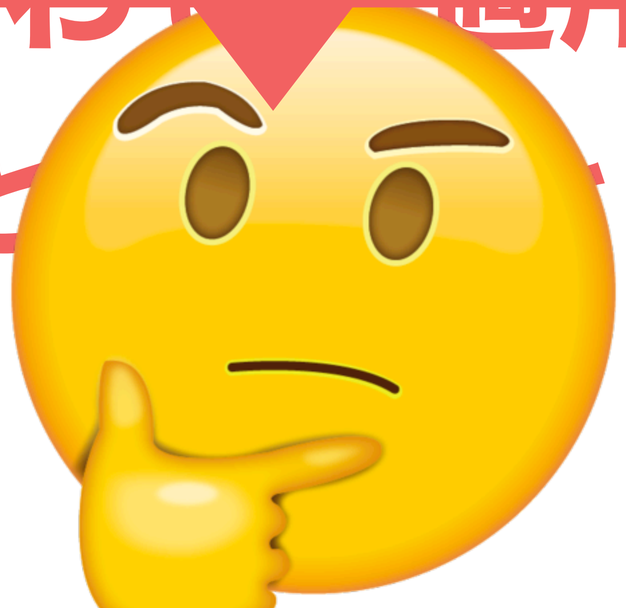
本投稿は、AWS の CISO オフィスのディレクターを務める Mark Ryland と AWS Identity の専門家である Quit Van Deman による寄稿を翻訳したものです。

アマゾン ウェブ サービス（AWS）の使命は、安全なシステムの構築、デプロイ、迅速な反復処理を行う際に行う作業がより少なくなるようにお客様に代わってイノベーションを行うことです。お客様からはセキュリティの観点について以下のような質問をよくいただきます、*“システムとデータの機密性、完全性、可用性を適切なレベルに確保し、スピードと俊敏性を向上させるのに最適なパターンは何ですか？“*。*ゼロトラスト・アーキテクチャ*または*ゼロトラスト・ネットワーキング*のカテゴリーに該当するセキュリティアーキテクチャパターンが、これらの質問にどのように答えることができるか、お客様から具体的な質問を受ける機会が増えてきました。

NIST
National Institute of Standards and Technolog
U.S. Department of Commerce
SP 800-207

第三の指針は、ゼロトラストの概念は、保護対象のシステムとデータの組織的価値にあわせて適用する必要があるということです

保護対象の
システムとデータについて
何もわからん場合は？



対象が既知でないとできないこと

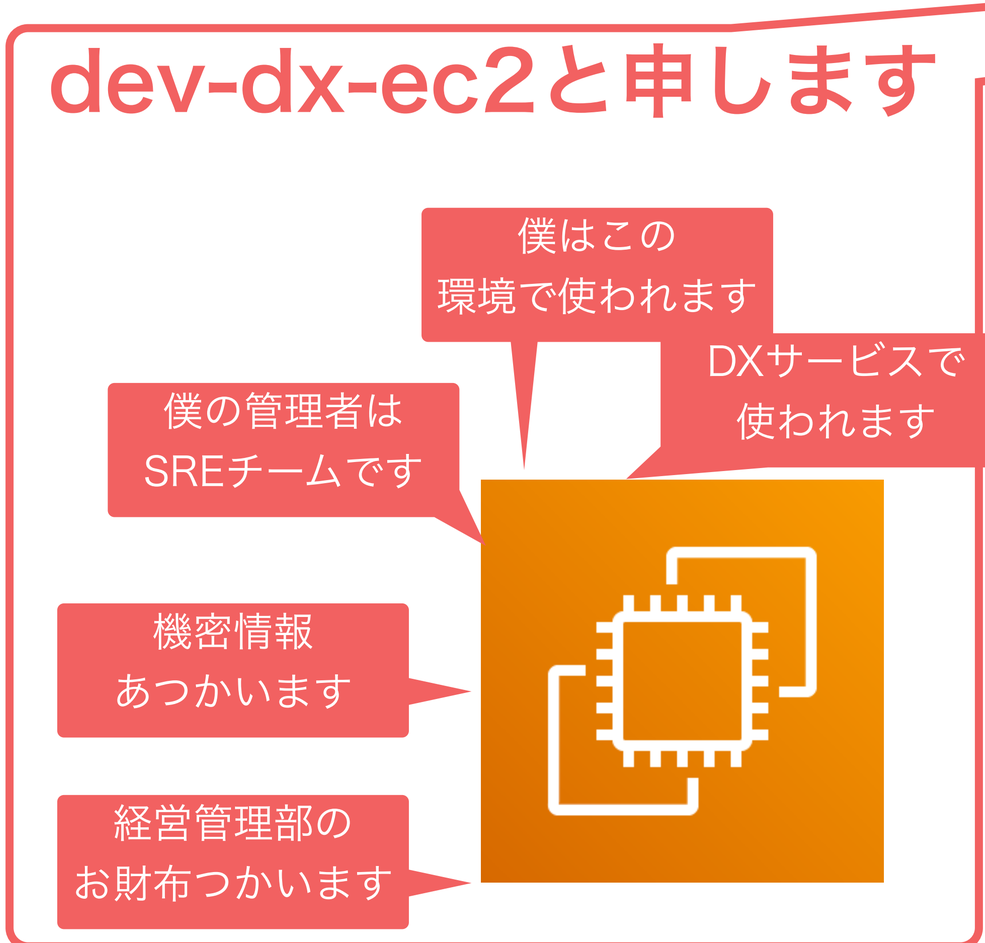
- 資産管理
- 予実管理
- アクセス管理
- （平時の）リスク管理
- インシデント対応
- 自動化

NIST SP800-207「ゼロトラスト・アーキテクチャ」

- to move to ZTA, an enterprise must have a system to discover and record physical and virtual assets to create a usable inventory

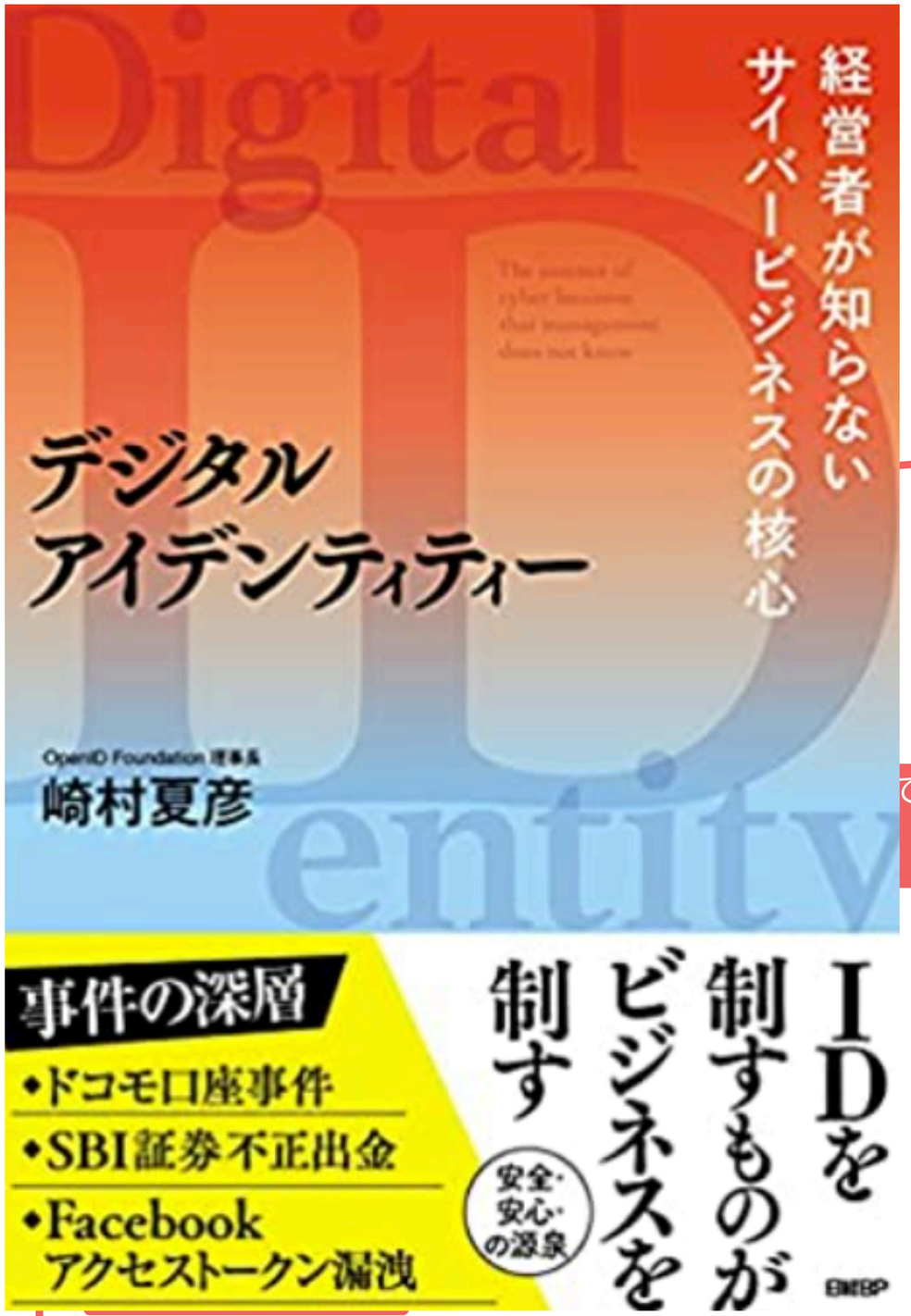
AWSのタグとは？

- 各リソースに付与されたメタデータ
- 各種運用における必要不可欠な参照先データ
- 組織特有のリソースIdentityを構築するClaim



AWSのタグとは？

- 各リソースに付与されたメタデータ
- 各種運用における必要不可欠な参照先データ
- 組織特有のリソースIdentityを構築するClaim



タグはすごい

- サーバーに架空のデータを付与できるようになった
  - 「妄想という名の想像力がホモ・サピエンスを進化させた」
- たくさんつけられる（~50)
- キー・値の自由度が高い（〜128, 256 unicode文字、case sensitive, 記号利用化）
- ワークロードの動作に直接的な影響を与えることなく運用できる
  - VPCのNameタグ…?知りませんね…
- API管理できる
  - データを実際のリソースに事前埋め込んだ上で、資産管理DBやエクセルを補完できる
  - 逆方向も可
  - 管理者による統制もできる

タグしか勝たん

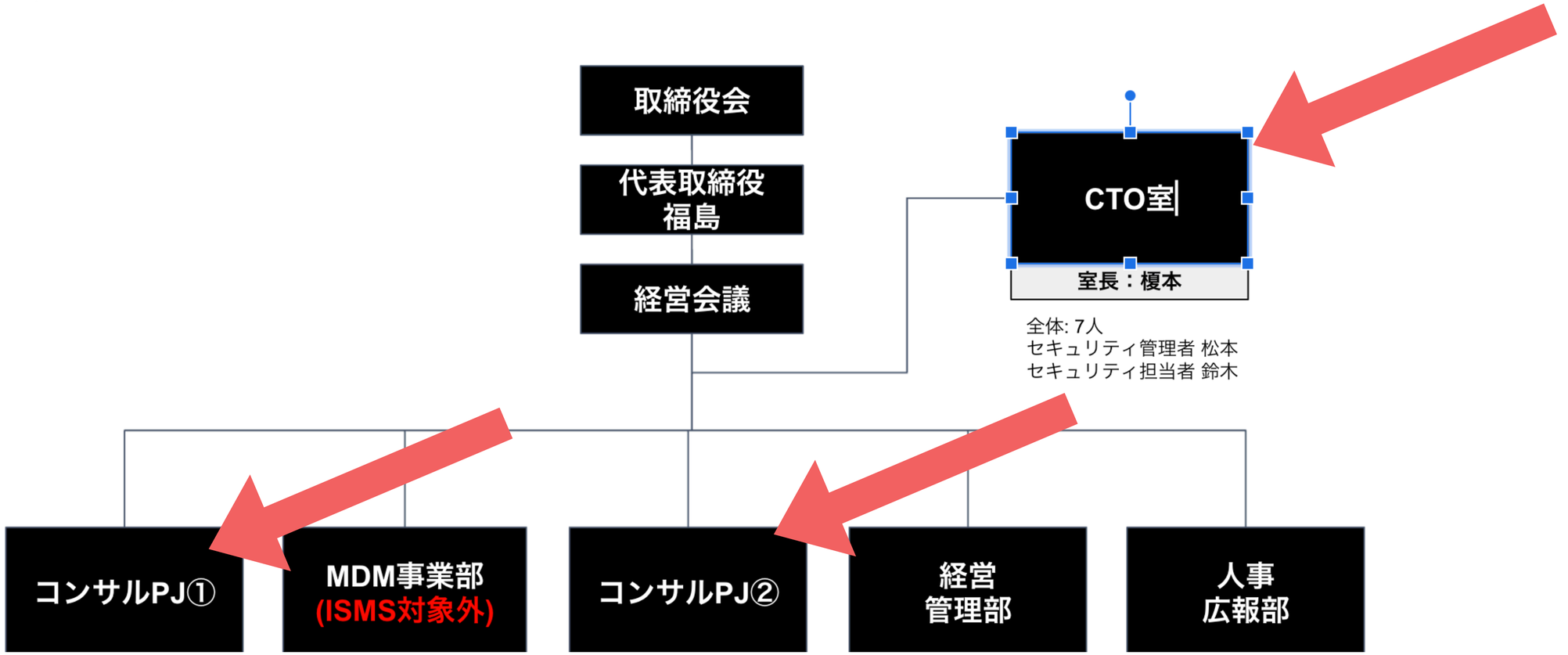
当社の話

Tag Ver 0

Tag ver0 (2020/03)

- BCコンサル事業がメインだったため、具体的な期間限定的なワークロードしかなかった
- PoCプロジェクトに伴う短期的な情報資産しかなかった（AWS上では）
- インフラ的整備を２人で実施
- ゆる〜く隗より始めよ
- （影響もないし）ガンガンいこうぜ

体制(昔)


取締役会
代表取締役
福島
経営会議
CTO室
室長：榎本
全体: 7人
セキュリティ管理者 松本
セキュリティ担当者 鈴木
コンサルPJ①
MDM事業部
(ISMS対象外)
コンサルPJ②
経営
管理部
人事
広報部

参考文献x2

Tagging Best Practices: Implement an Effective AWS Resource Tagging Strategy

PDF | RSS

Publication date: **December 2018** (Document Revisions)

AWS allows customers to assign metadata to their AWS resources in the form of tags. Each tag is a simple la
customer-defined key and an optional value that can make it easier to manage, search for, and filter resourc
owner, environment, or other criteria. AWS tags can be used for many purposes.

Did this page help you?

Yes | No

Provide feedback

Next topic: Introduction: Tagging Use Cases

Need help?

- Connect with an AWS IQ expert

AWS TAGGING STRATEGIES

"How should I tag my AWS resources?"

Overview

Amazon Web Services (AWS) allows customers to assign metadata to their AWS resources in the form of *tags*. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Although there are no inherent types of tags, they enable customers to categorize resources by purpose, owner, environment, or other criteria. This document describes commonly used tagging categories and strategies to help AWS customers implement a consistent and effective tagging strategy. The following sections assume basic knowledge of AWS resources, tagging, detailed billing, and AWS Identity and Access Management (IAM).

General Best Practices

When creating a tagging strategy for AWS resources, make sure that it accurately represents organizationally relevant dimensions and adheres to the following tagging best practices:

- Always use a standardized, case-sensitive format for tags, and implement it consistently across all resource types.
- Consider tag dimensions that support the ability to manage resource access control, cost tracking, automation, and organization.
- Implement automated tools to help manage resource tags. The Resource Groups Tagging API enables programmatic control of tags, making it easier to automatically manage, search, and filter tags and resources. It also simplifies backups of tag data across all supported services with a single API call per AWS Region.
- Err on the side of using too many tags rather than too few tags.
- Remember that it is easy to modify tags to accommodate changing business requirements, however consider the ramifications of future changes, especially in relation to tag-based access control, automation, or upstream billing reports.

Tagging Categories

Companies that are most effective in their use of tags typically create business-relevant tag groupings to organize their resources along technical, business, and security dimensions. Companies that use automated processes to manage their infrastructure also include additional, automation-specific tags to aid in their automation efforts.

Technical Tags

Name – Used to identify individual resources

Application ID – Used to identify disparate resources that are related to a specific application

Application Role – Used to describe the function of a particular resource (e.g. web server, message broker, database)

Cluster – Used to identify resource farms that share a common configuration and perform a specific function for an application

Environment – Used to distinguish between development, test, and production infrastructure

Version – Used to help distinguish between different versions of resources or applications

Tags for Automation

Date/Time – Used to identify the date or time a resource should be started, stopped, deleted, or rotated

Opt in/Opt out – Used to indicate whether a resource should be automatically included in an automated activity such as starting, stopping, or resizing instances

Security – Used to determine security requirements, such as encryption, enabling Amazon VPC Flow Logs, and also to identify route tables or security groups that deserve extra scrutiny

Business Tags

Owner – Used to identify who is responsible for the resource

Cost Center/Business Unit – Used to identify the cost center or business unit associated with a resource; typically for cost allocation and tracking

Customer – Used to identify a specific client that a particular group of resources serves

Project – Used to identify the project(s) the resource supports

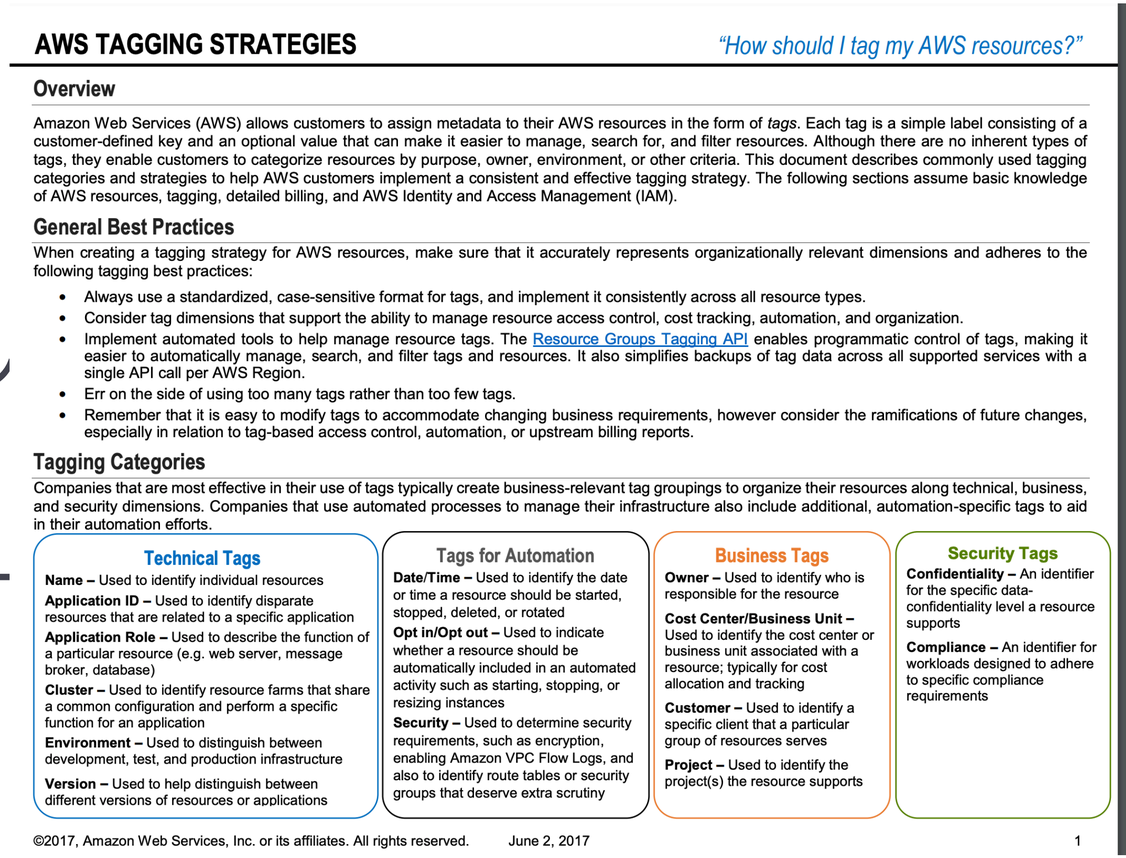
Security Tags

Confidentiality – An identifier for the specific data-confidentiality level a resource supports

Compliance – An identifier for workloads designed to adhere to specific compliance requirements

AWS Tagging Strategies

- ベスプラ
  - Case sensitive
  - リソースへのアクセスコントロール
  - タグ管理の自動化
  - タグは少ないより、多い方がベター
- 主にタグカテゴリを参照



AWS TAGGING STRATEGIES *"How should I tag my AWS resources?"*

Overview

Amazon Web Services (AWS) allows customers to assign metadata to their AWS resources in the form of *tags*. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Although there are no inherent types of tags, they enable customers to categorize resources by purpose, owner, environment, or other criteria. This document describes commonly used tagging categories and strategies to help AWS customers implement a consistent and effective tagging strategy. The following sections assume basic knowledge of AWS resources, tagging, detailed billing, and AWS Identity and Access Management (IAM).

General Best Practices

When creating a tagging strategy for AWS resources, make sure that it accurately represents organizationally relevant dimensions and adheres to the following tagging best practices:

- Always use a standardized, case-sensitive format for tags, and implement it consistently across all resource types.
- Consider tag dimensions that support the ability to manage resource access control, cost tracking, automation, and organization.
- Implement automated tools to help manage resource tags. The Resource Groups Tagging API enables programmatic control of tags, making it easier to automatically manage, search, and filter tags and resources. It also simplifies backups of tag data across all supported services with a single API call per AWS Region.
- Err on the side of using too many tags rather than too few tags.
- Remember that it is easy to modify tags to accommodate changing business requirements, however consider the ramifications of future changes, especially in relation to tag-based access control, automation, or upstream billing reports.

Tagging Categories

Companies that are most effective in their use of tags typically create business-relevant tag groupings to organize their resources along technical, business, and security dimensions. Companies that use automated processes to manage their infrastructure also include additional, automation-specific tags to aid in their automation efforts.

Technical Tags

Name – Used to identify individual resources

Application ID – Used to identify disparate resources that are related to a specific application

Application Role – Used to describe the function of a particular resource (e.g. web server, message broker, database)

Cluster – Used to identify resource farms that share a common configuration and perform a specific function for an application

Environment – Used to distinguish between development, test, and production infrastructure

Version – Used to help distinguish between different versions of resources or applications

Tags for Automation

Date/Time – Used to identify the date or time a resource should be started, stopped, deleted, or rotated

Opt in/Opt out – Used to indicate whether a resource should be automatically included in an automated activity such as starting, stopping, or resizing instances

Security – Used to determine security requirements, such as encryption, enabling Amazon VPC Flow Logs, and also to identify route tables or security groups that deserve extra scrutiny

Business Tags

Owner – Used to identify who is responsible for the resource

Cost Center/Business Unit – Used to identify the cost center or business unit associated with a resource; typically for cost allocation and tracking

Customer – Used to identify a specific client that a particular group of resources serves

Project – Used to identify the project(s) the resource supports

Security Tags

Confidentiality – An identifier for the specific data-confidentiality level a resource supports

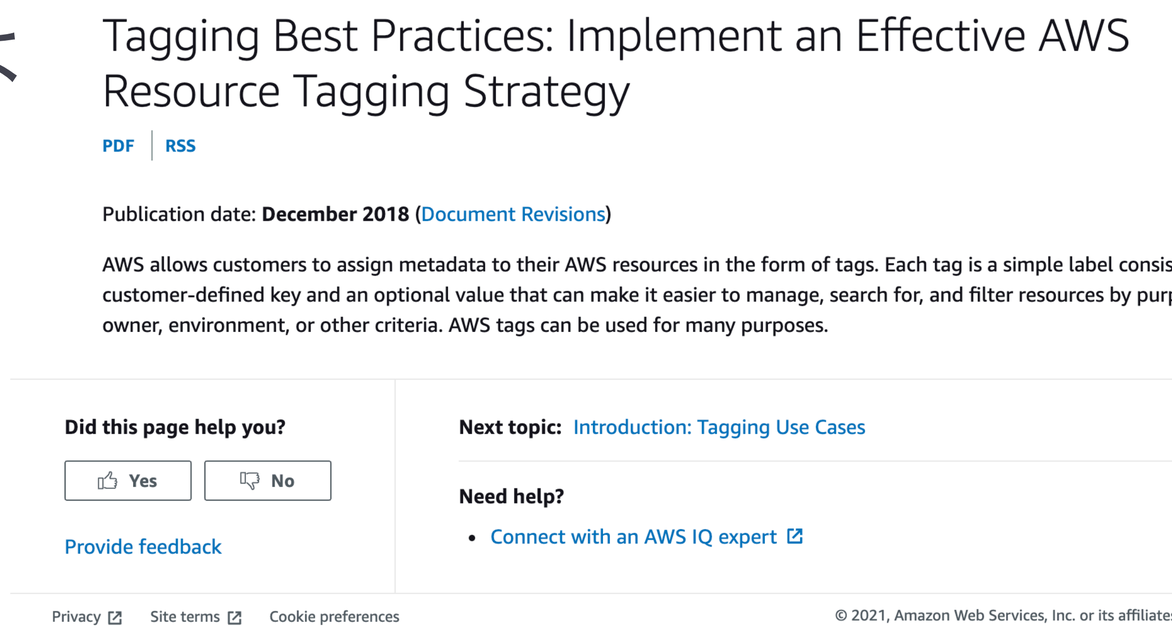
Compliance – An identifier for workloads designed to adhere to specific compliance requirements

 June 2, 2017 1

https://d0.awsstatic.com/aws-answers/AWS_Tagging_Strategies.pdf

Tagging Best Practices

- AWS Tagging Strategiesをより詳細化



Tagging Best Practices: Implement an Effective AWS Resource Tagging Strategy

PDF | RSS

Publication date: **December 2018** (Document Revisions)

AWS allows customers to assign metadata to their AWS resources in the form of tags. Each tag is a simple label consis
customer-defined key and an optional value that can make it easier to manage, search for, and filter resources by purp
owner, environment, or other criteria. AWS tags can be used for many purposes.

Did this page help you?

Yes No

Provide feedback

Next topic: Introduction: Tagging Use Cases

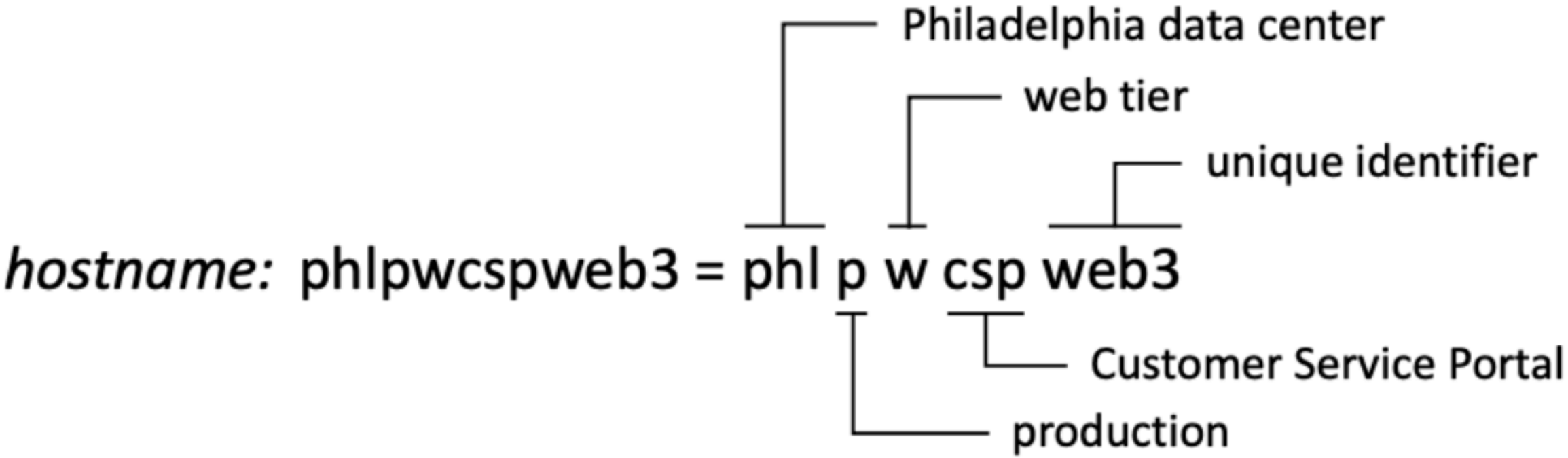
Need help?

- Connect with an AWS IQ expert

Privacy Site terms Cookie preferences

© 2021, Amazon Web Services, Inc. or its affiliate

https://docs.aws.amazon.com/whitepapers/latest/tagging-best-practices/introduction-tagging-use-cases.html



そんなにタグの値につめこまんでもよくない…？

当社独自カスタマイズ①

sensitive data, you may require a tag to identify the correspon
such as Personally Identifiable Information or Protected Healt

When identifying tagging requirements, focus on required and
tags. Allow for optional tags, as long as they conform to your
governance policies, to empower your organization to define r
or bespoke application requirements.

Start Small; Less is More

Tagging decisions are reversible, giving you the flexibility to ec
the future. However, there is one exception—cost allocation ta
ports. The data for these repor
d monthly. As a result, when yo
rting from that point in time. T

AWS TAGGING STRATEGIES

"How should I tag my AWS resources?"

言ってることが違うので、
「大は小を兼ねる」ということで
後から変えること上等でつけまくることにした。
タグ変更であれば影響はなく，
かつ、現在の予実管理ではそこまでタグを活用してないため

Overview

Amazon Web Services (AWS) allows customers to assig
customer-defined key and an optional value that can ma
tags, they enable customers to categorize resources by p
categories and strategies to help AWS customers implem
of AWS resources, tagging, detailed billing, and AWS Ide

General Best Practices

When creating a tagging strategy for AWS resources, make sure that it accurately represents organizationally relevant dimensions and adheres to the following tagging best practices:

- Always use a standardized, case-s e format for tags, and implement it consistently across all resource types.
- Consider tag dimensio th port the ability to manage resource access control, cost tracking, automation, and organization.
- Implement automate s to help manage resource tags. The Resource Groups Tagging API enables programmatic control of tags, making it easier to automatically ma age, search, and filter tags and resources. It also simplifies backups of tag data across all supported services with a single API call per AWS Region.
- Err on the side of using too many tags rather than too few tags.
- Remember that it is easy to modify tags to accommodate changing business requirements, however consider the ramifications of future changes, especially in relation to tag-based access control, automation, or upstream billing reports.

Tagging Categories

Companies that are most effective in their use of tags typically create business-relevant tag groupings to organize their resources along technical, business,

Tagging Best Practices

- AWS Tagging Strategiesをより詳細化

ビミョーに言ってることが違うので
Tagging Best Practicesの考え方を基に、
Tagging Strategiesの実装方法をメインに実装

https://docs.aws.amazon.com/whitepapers/latest/tagging-best-practices/introduction-tagging-use-cases.html

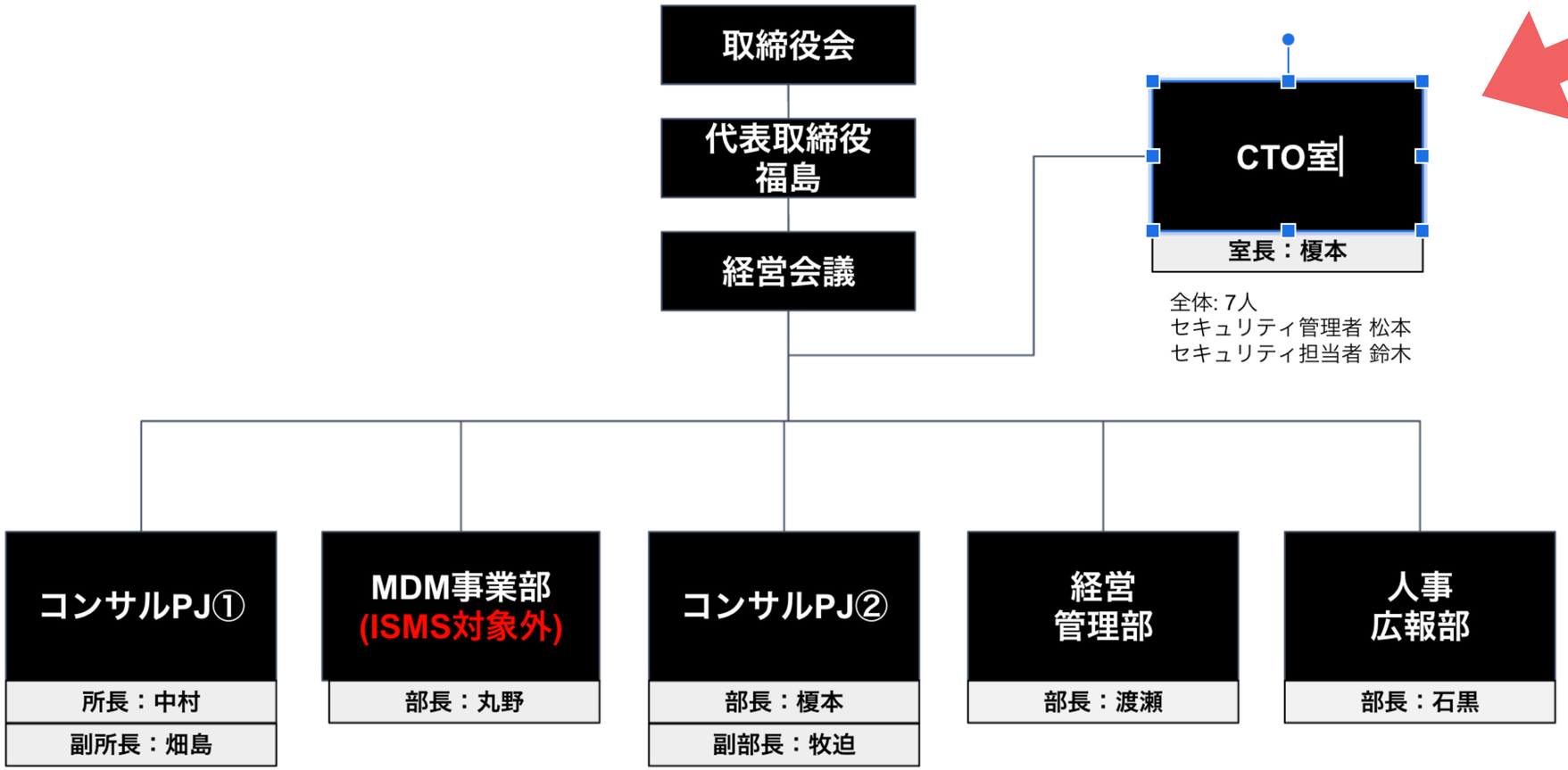
当社独自カスタマイズ②

- タグ命名規則: ケバブケース -> スネークケース
  - インベントリってDBだし、じゃあスネークケースだよね
  - Terraformのベスプラもアンスコだし。
- リソース名規則:
  - {environment}-{service_id}-{リソース特有の値}
  - S3やALBについては name タグのような 語句間を _ な形式だとできないので、 - でつなげる。

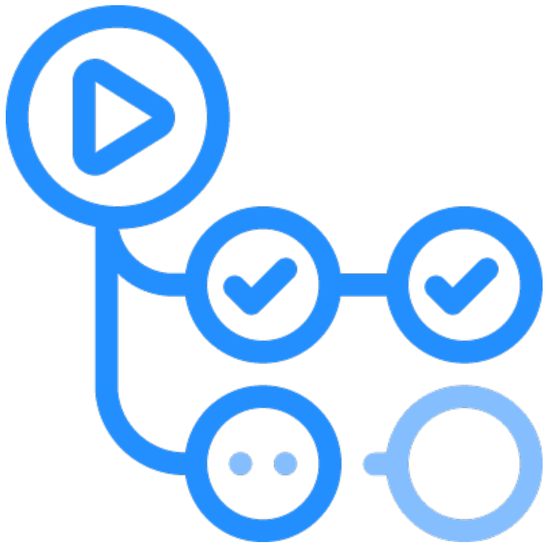
https://www.terraform-best-practices.com/naming

当社独自カスタマイズ③

タグ管理を
受け持つ



当社独自カスタマイズ④



タグ名	カテゴリ	必須	例
name	リソース名	○	${service_id}.${environment}.${service_role}.${name}
service_id	アプリ・サービスID	○	dx
service_role	サービス内の役割	○	web, db, log_storage
cluster			ecs クラスターとか
environment	環境	○	dev, stg, prd
version			
owner	責任先	○	
cost_center		○	xxx, yyy, layerx (顧客名)
project	プロジェクト名	○	
customer	特定のお客様向け用		エンプラプランにはお客様専用サーバを提供します。的な
confidentiality	機密度合い	○	
managed_by	どのIaCか	○	manual(デフォルト), terraform, cfn
compliance	規制・コンプラ		PII, [pii, iso27002]

Confidentialityに関する補足

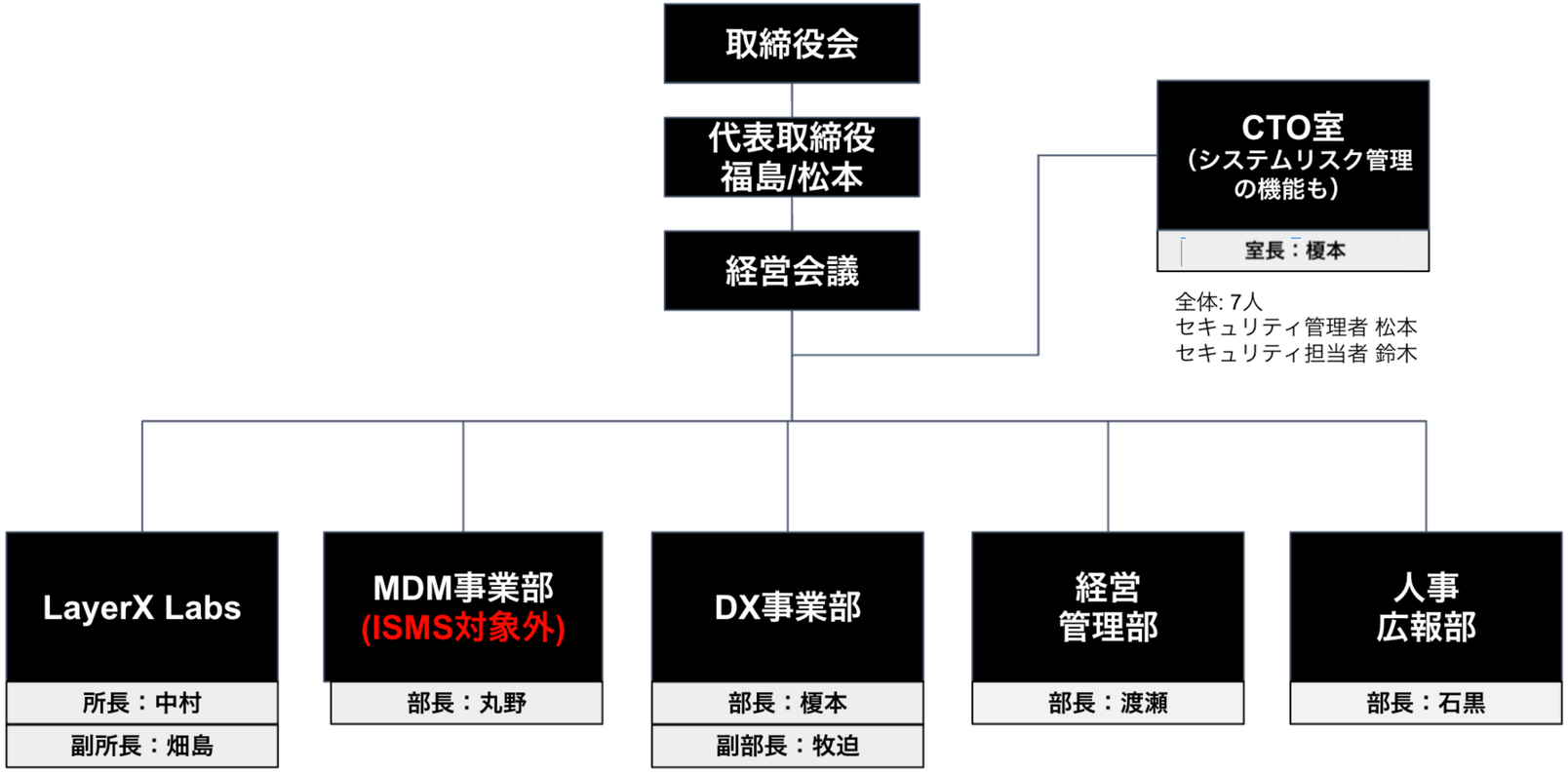
分類	機密性	完全性	外部共有	競争優位性	危殆時のリスク	例
sensitive	低~高	要		有	競争優位性を含めた深刻な影響	財務取引、規約情報、取引情報
confidential	低~高				深刻な影響	機微情報, 顧客情報
private	低~中				直接リスクはないものの、2次的リスクあり	人事情報, 従業員情報
proprietary	低		有	有	競争優位性	コード, 技術
public						公開情報

Tag Ver 1

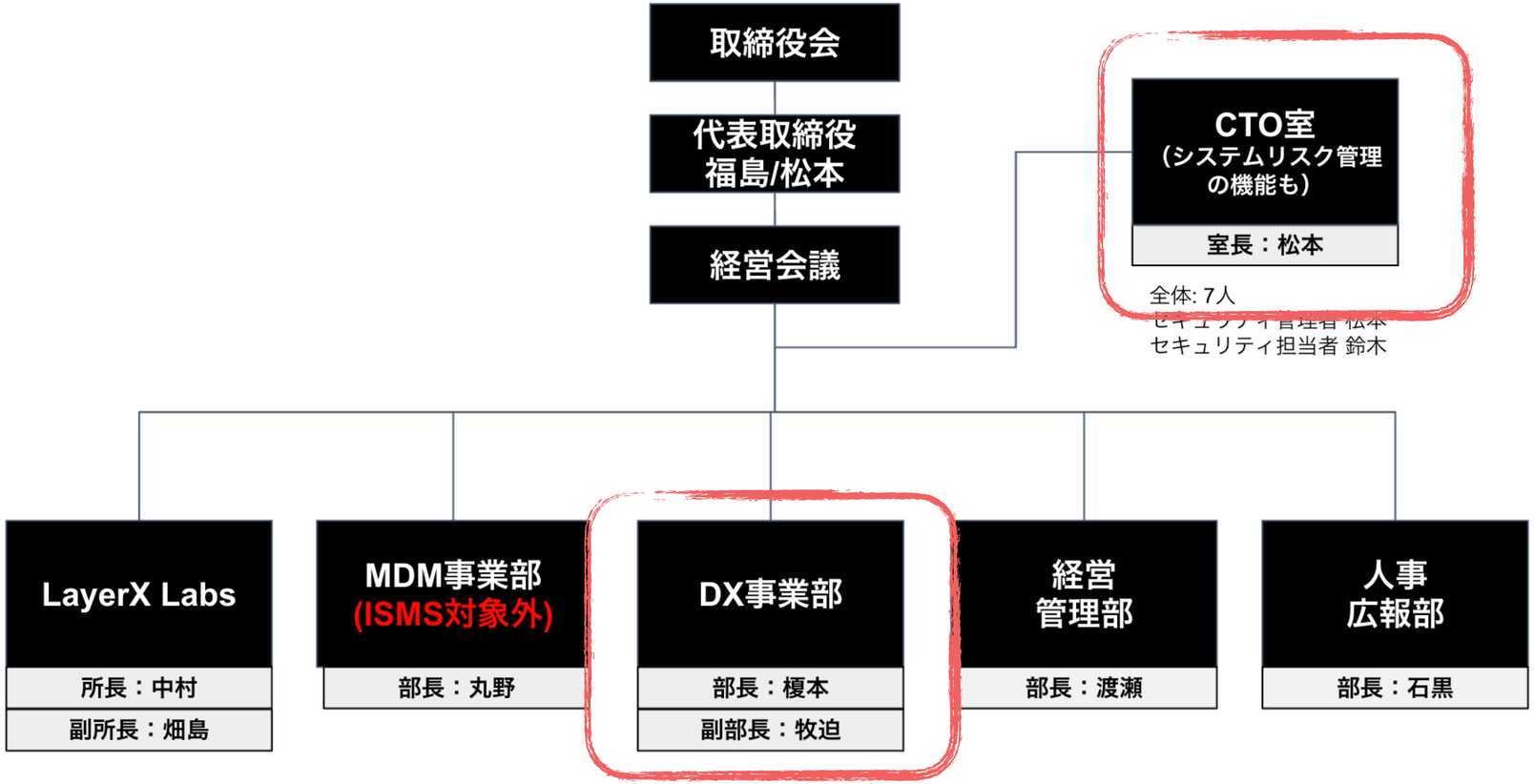
Tag ver1 (2021/01)

- 事業部制へ
- 永続的な情報資産が発生した
- インフラ的整備をする２人は事業部に派遣へ

体制(Now)


取締役会
代表取締役
福島/松本
経営会議
CTO室
（システムリスク管理の機能も）
室長：榎本
全体: 7人
セキュリティ管理者 松本
セキュリティ担当者 鈴木
LayerX Labs
所長：中村
副所長：畑島
MDM事業部
(ISMS対象外)
部長：丸野
DX事業部
部長：榎本
副部長：牧迫
経営
管理部
部長：渡瀬
人事
広報部
部長：石黒

共有会


取締役会
代表取締役
福島/松本
経営会議
CTO室
（システムリスク管理の機能も）
室長：松本
全体: 7人
セキュリティ担当者 鈴木
LayerX Labs
所長：中村
副所長：畑島
MDM事業部
(ISMS対象外)
部長：丸野
DX事業部
部長：榎本
副部長：牧迫
経営
管理部
部長：渡瀬
人事
広報部
部長：石黒

diff from ver.0

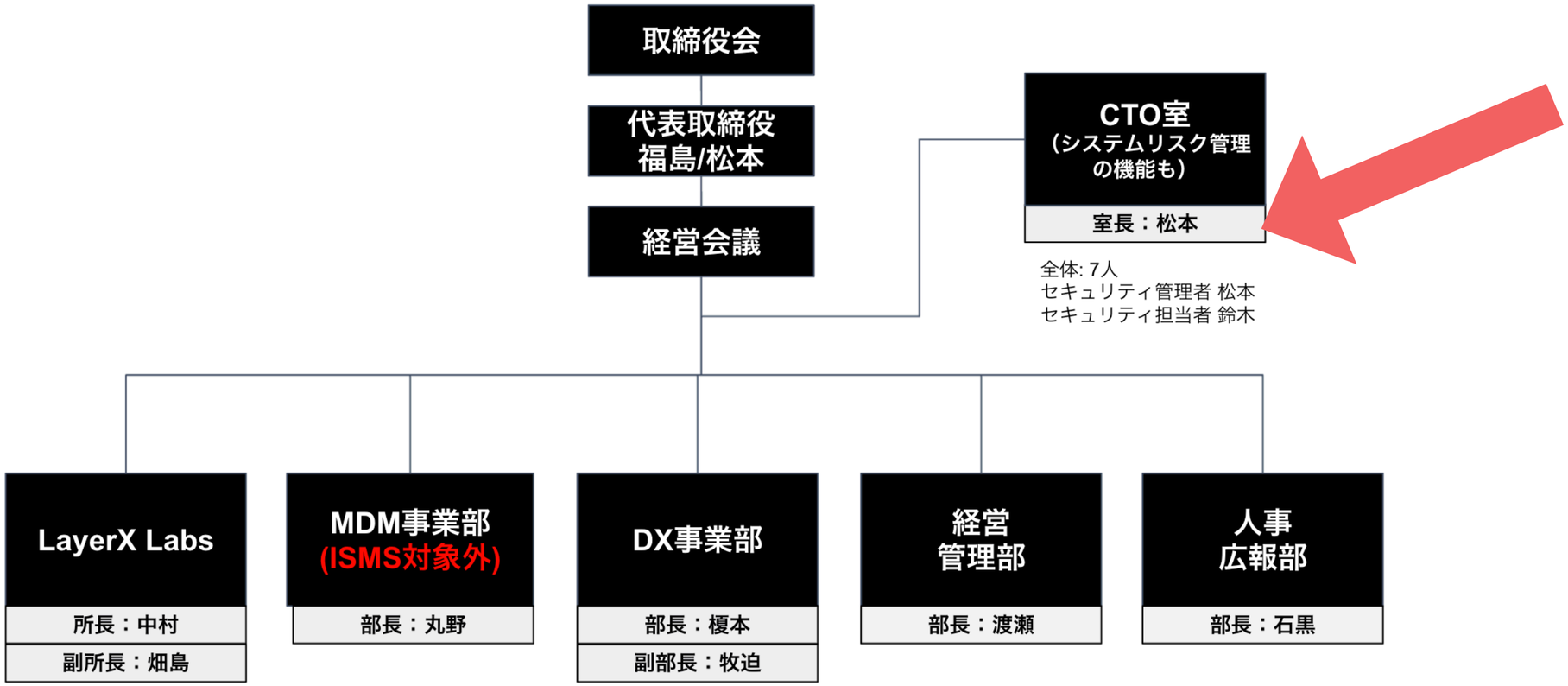
- cost_centerの値に各事業部が入るように
- nameタグを廃止
- タグ名(layerx:タグ名)のprefixを廃止

Tag Ver 2

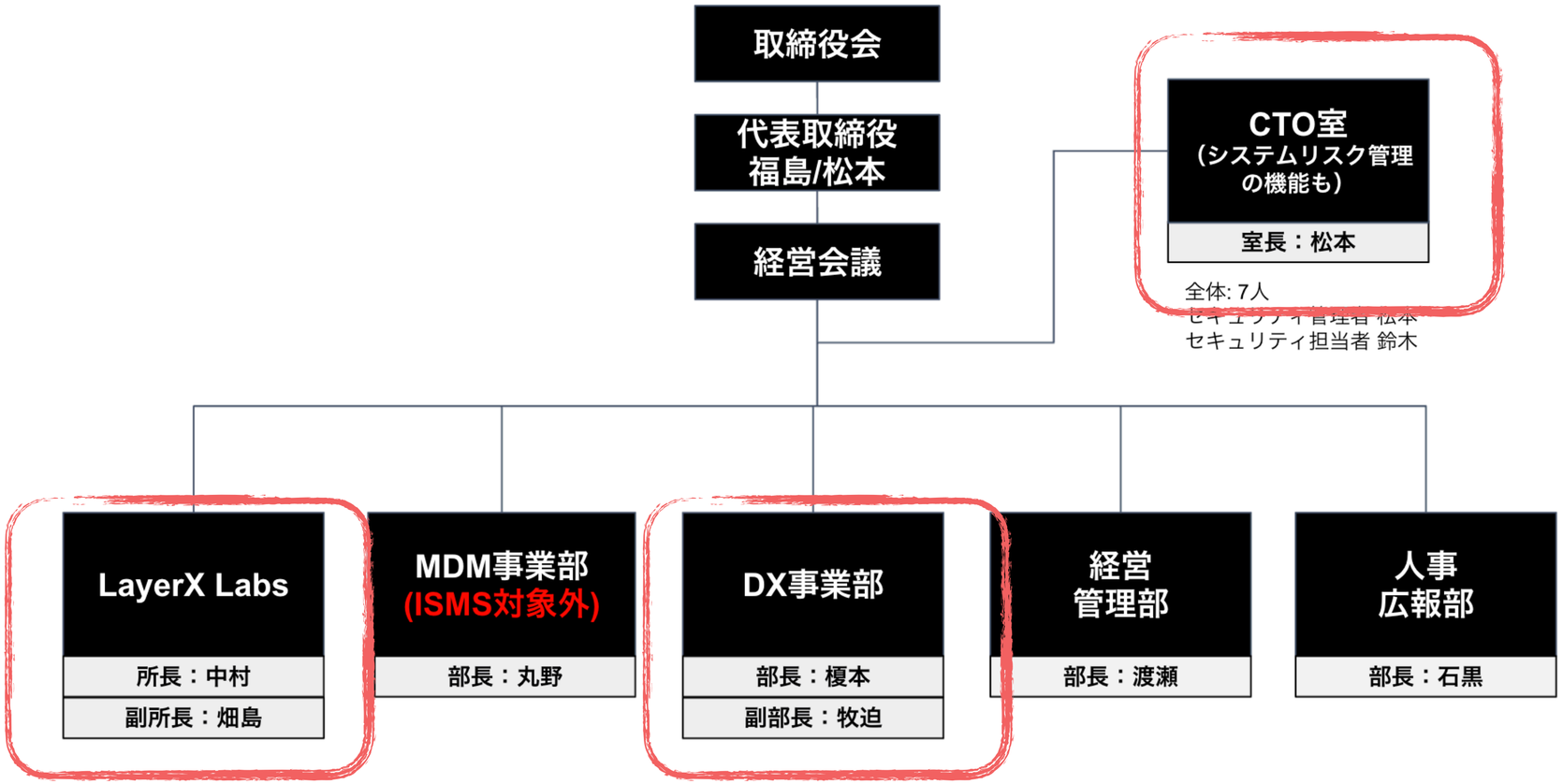
Tag v2(2021/04)

- Terraform provider v3.38
- CTO交代
- ISMS取得開始

体制(Now)


取締役会
代表取締役
福島/松本
経営会議
CTO室
（システムリスク管理の機能も）
室長：松本
全体: 7人
セキュリティ管理者 松本
セキュリティ担当者 鈴木
LayerX Labs
所長：中村
副所長：畑島
MDM事業部
(ISMS対象外)
部長：丸野
DX事業部
部長：榎本
副部長：牧迫
経営
管理部
部長：渡瀬
人事
広報部
部長：石黒

共有会


取締役会
代表取締役
福島/松本
経営会議
CTO室
（システムリスク管理の機能も）
室長：松本
全体: 7人
セキュリティ担当者 鈴木
LayerX Labs
所長：中村
副所長：畑島
MDM事業部
(ISMS対象外)
部長：丸野
DX事業部
部長：榎本
副部長：牧迫
経営
管理部
部長：渡瀬
人事
広報部
部長：石黒

Terraform AWS Provider v3.38のリリース

- default_tagsさいこー

```
resource "aws_kms_key" "cloudtrail" {
  description         = "key to encrypt/decrypt cloudtrail"
  tags = {
    environment   = prd
    service_role    = var.service_role.kms
    project             = guardrail
    service_id        = guardrail
    cost_center     = layerX
    Owner             = sre
    managed_by    = terraform
    github_repository - guardrail
  }
}
```

```
provider "aws" {
  region = var.region
  default_tags { tags = var.default_tags }
}

resource "aws_kms_key" "cloudtrail" {
  description         = "key to encrypt/decrypt cloudtrail"
  tags = {
    service_role    = var.service_role.kms
  }
}
```

diff from ver1

- github_repository追加
- 情報区分の見直し
  - 前: sensitive, confidential, private, proprietary, public
  - 後: confidential, private, public
- service_roleを実態であるリソースの粒度にあわせる
  - 例: secrets manager -> vault

今後

Tag v3 (future)

- タグ統制
  - タグ everywhere
  - タグ管理の管理
- タグへのアクセス管理を緻密化
- タグを使ったABAC？
  - 正直あまりメリットを感じてない…

採用してます!!!
個人カジュアル面談からで
もOK!!!

【CTO室】屋台骨エンジニア

株式会社LayerX

応募する

【共通_CTO室】Corporate Ops

動物的に大胆に 100X Layer

採用はこちら ->
https://herp.careers/v1/layerx

カジュアル面談はこちら ->
https://meety.net/articles/t2--w06w1j36j

【CTO室】Corporate Engineering

株式会社LayerX

応募する

動物的に
大胆に
100X
LayerX

【CTO室】Corporate Engineering

https://meety.net/matches/jAbffzvLqjNa

https://herp.careers/v1/layerx/yr-q1HGTPR9x

#わたしのシゴト

LayerXから三井物産デジタルアセットマネジメント（以下、MDM）という会社に出向しています。

Thank you!