AWS-18

医療業界に求められるセキュリティ対策と AWS が提供するソリューション

岡本 真樹
パブリックセクター技術統括本部 シニアソリューションアーキテクト
アマゾン ウェブ サービス ジャパン合同会社

自己紹介

岡本 真樹（Masaki Okamoto）

シニア ソリューション アーキテクト：

公共部門のお客様のクラウド活用の検討を支援

略歴：

通信機器ベンダーにて通信事業者のサービス開発を技術面で長年サポート
政府関係者のセキュリティ対策の支援、ISMAP の社内対応を経験後、AWS へ

好きな AWS サービス：

AWS Security Hub, AWS Trusted Advisor

本セッションの対象者とゴール

対象者

- 医療情報システムのクラウド移行を検討している IT 部門のご担当者、事業者
- クラウド上の医療情報システムのセキュリティ運用管理を担当する方

ゴール

- 医療情報システムに対するガイドラインに沿ったセキュリティ管理を AWS サービスを用いて実現する考え方を学ぶ
- リスクベースの対応としてランサムウェアに対するバックアップ対策と、様々な脅威をモニタリングから検知する方策についての関連サービスと技術を習得する

お話ししない内容（このセッションで触れないこと）

- 省庁のガイドラインの中身そのものの詳細な説明

本日のアジェンダ

1. 医療業界のクラウド活用とガイドラインへの対応

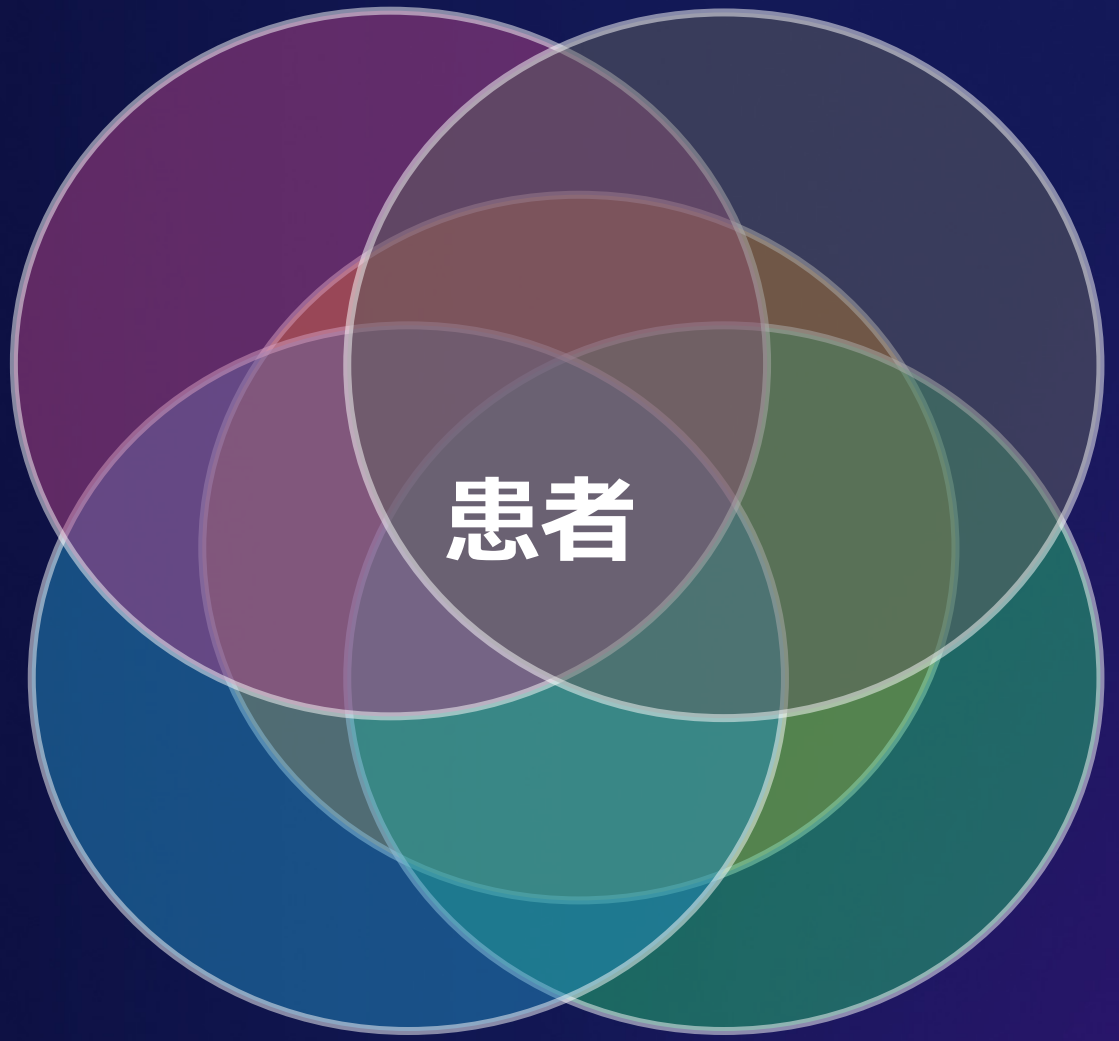
2. セキュリティのリスクに対応するためには
   - ランサムウェア対策としてのバックアップ
   - 脅威を継続的に検知するモニタリング

医療業界のクラウド活用と
医療情報ガイドラインへの対応

AWS と医療分野の関わり- 患者様を中心に

医療機関
病院システム
グループ診療とクリニック
看護 /リハビリ/ LTC
臨床検査医
学術医療センター
在宅医療
薬局

ベンダー
ヘルスケア IT ISV
診断
医療機器
グローバル SI



政府機関
公衆衛生
科学研究機関
規制当局
国レベルの保健省庁

保険会社
医療保険
雇用主

NGO と NPO
健康組合
研究機関

国内における医療関連のお客様

(一部抜粋)

京都大学 KYOTO UNIVERSITY

国立循環器病研究センター National Cerebral and Cardiovascular Center

日本医師会ORCA管理機構

AOI 国際病院 医療法人社団 葵会 AOI UNIVERSAL HOSPITAL

特定機能病院 / 地方独立行政法人 大阪府立病院機構 大阪国際がんセンター

東京都済生会中央病院 TOKYO SAISEIKAI CENTRAL HOSPITAL

平成医療福祉グループ HEISEI MEDICAL WELFARE GROUP

Abbott

OMRON

sysmex Lighting the way with diagnostics

TERUMO

CureApp

SUSMED Sustainable Medicine

welby

LPIXEL

DeepEyeVision

Dental Systems

AIIm SHAPING HEALTHCARE

京都ProMed

flixy

Media Contents Factory

MEDLEY

MICIN

Integrity Healthcare

JMDC

MDV medical.data.vision

Antaa

スギ薬局

MedPeer

KAKEHASHI

Solamichi System

MG-DX Medication Guidance Digital Transformation

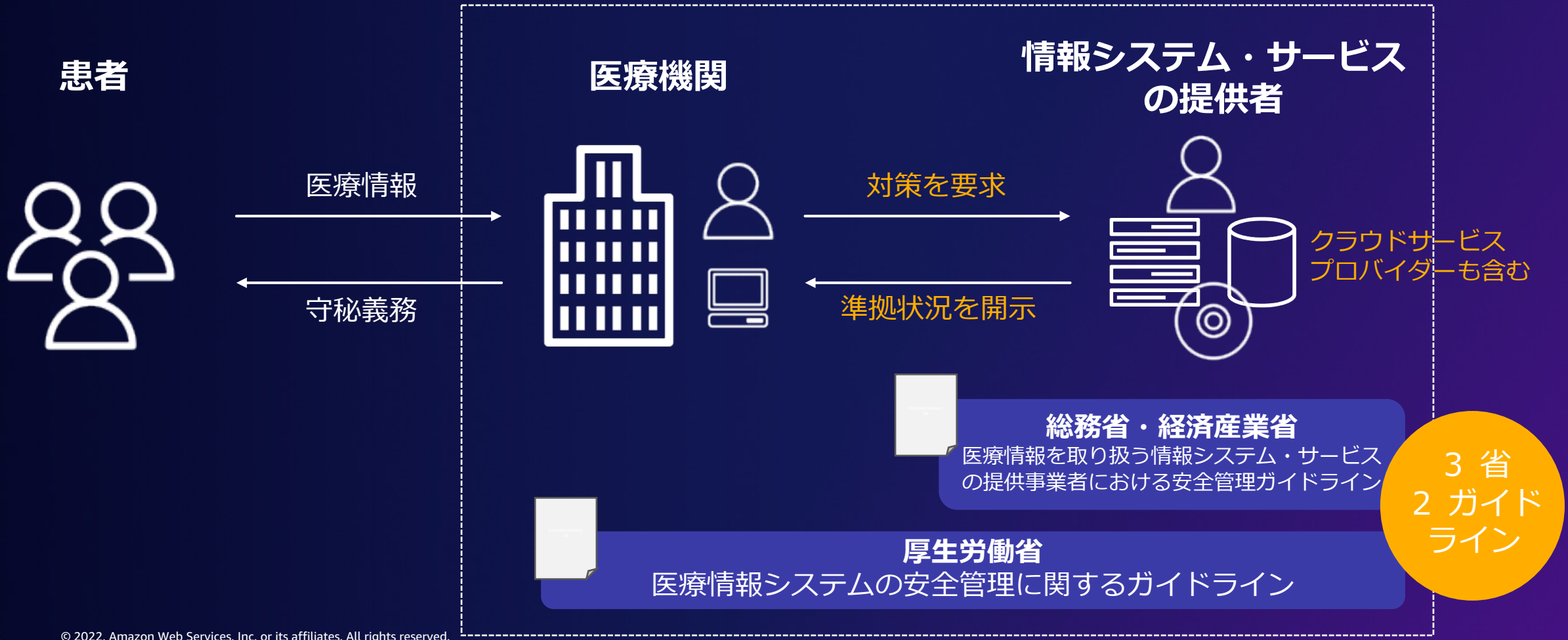
医療情報の扱い

- 医療情報は、個人情報保護法における「要配慮個人情報」に該当
- 医療情報の取扱いにおいても、「収集」「保管」「破棄」を通じて、法令や指針等に定められている要件を満たす適切な取扱いを求められる
- 厚生労働省、総務省、経済産業省の3 省が定めた 2 つの医療情報システムに関する各ガイドライン（「3 省 2 ガイドライン」）

医療情報システムの安全管理に関するガイドライン　第 5.1 版（令和 3 年 1 月）
https://www.mhlw.go.jp/stf/shingi/0000516275.html
医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン
https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html

医療情報を扱うシステムのガイドライン

3 省 2 ガイドラインの位置付け



医療情報システムにおける責任共有モデル

責任共有モデル

お客様

クラウド内の
セキュリティ
に対する責任

AWS

クラウドの
セキュリティ
に対する責任

医療情報システム

医療情報
システム

- **データの統制権・所有権はお客様**
- お客様自身または、
情報システム・サービスの提供事業者
が責任を持つ範囲
- アプリケーションの機能およびAWSの
各種セキュリティサービスの活用により
ガイドラインにそった対策を実施

AWS
インフラ
ストラクチャ

- AWSが責任を持つ範囲
  - コンピュートサービス
  - ストレージサービス
  - ネットワークサービス
  - グローバルインフラストラクチャ　等
- **AWS は統制およびコンプライアンスに関するドキュメントを提供**
- **お客様はガイドラインが求める要求事項に対する AWS の対応状況を確認可能**

ガイドライン

**総務省・
経済産業省**

医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン

医療情報システム向け AWS 利用リファレンス


日本の医療情報ガイドライン

概要

医療情報ガイドライン

日本では全ての医療行為は医療法等で医療機関等の管理者の責任で行うことが求められており、クラウドサービスを利用する場合も、医療情報システムの構築や運用に関連して、安全かつ適切な技術的及び運用管理方法を確立し、安全管理や e-文書法の要件等への対応を行っていく必要があります。

さらに、該当するシステムで利用される医療情報は、個人情報保護法における「要配慮個人情報」に該当し、医療情報の取扱いにおいても、「収集」「保管」「破棄」を通じて、諸法令をはじめ、通知や指針等に定められている要件を満たす適切な取扱いができる仕組み作りが必要です。医療情報システムの場合には、具体的には、厚生労働省、総務省、経済産業省の 3 省が定めた医療情報システムに関する各ガイドラインに対して、必要に応じて医療情報に係る関連事業者や責任者が対策を施す必要があります。クラウド環境の導入を検討する場合には、これらのガイドラインの要求事項を整理検討し、必要となる対策項目の洗い出しや対応する情報、実施策の検討等を行う必要があります。

AWS パートナー

- **キヤノンITソリューションズ株式会社**
- **日本電気株式会社**
- **株式会社日立システムズ**
- **フィラーシステムズ株式会社**

本リファレンスにより、
ガイドラインの要求事項に対する

- ✓ AWS のセキュリティ対応の内容と、その根拠と成る文章とその記載箇所
- ✓ ガイドラインに適合する AWS サービス

医療情報システム向け AWS 利用リファレンスの紹介ページ
https://aws.amazon.com/jp/compliance/medical-information-guidelines/

リスクベースのアプローチ

経済産業省「医療情報を取り扱う情報システム・サービスの 提供事業者における安全管理ガイドライン」の
リスクマネジメントプロセス

リスクシナリオの一例

「正当な利用者以外により、医療情報システム等の情報が閲覧・操作される。」

リスク ”低減” としての人/組織的・技術的 対応の例

医療機関の方々
- パスワードの定期的な変更、類推されないパスワードの設定

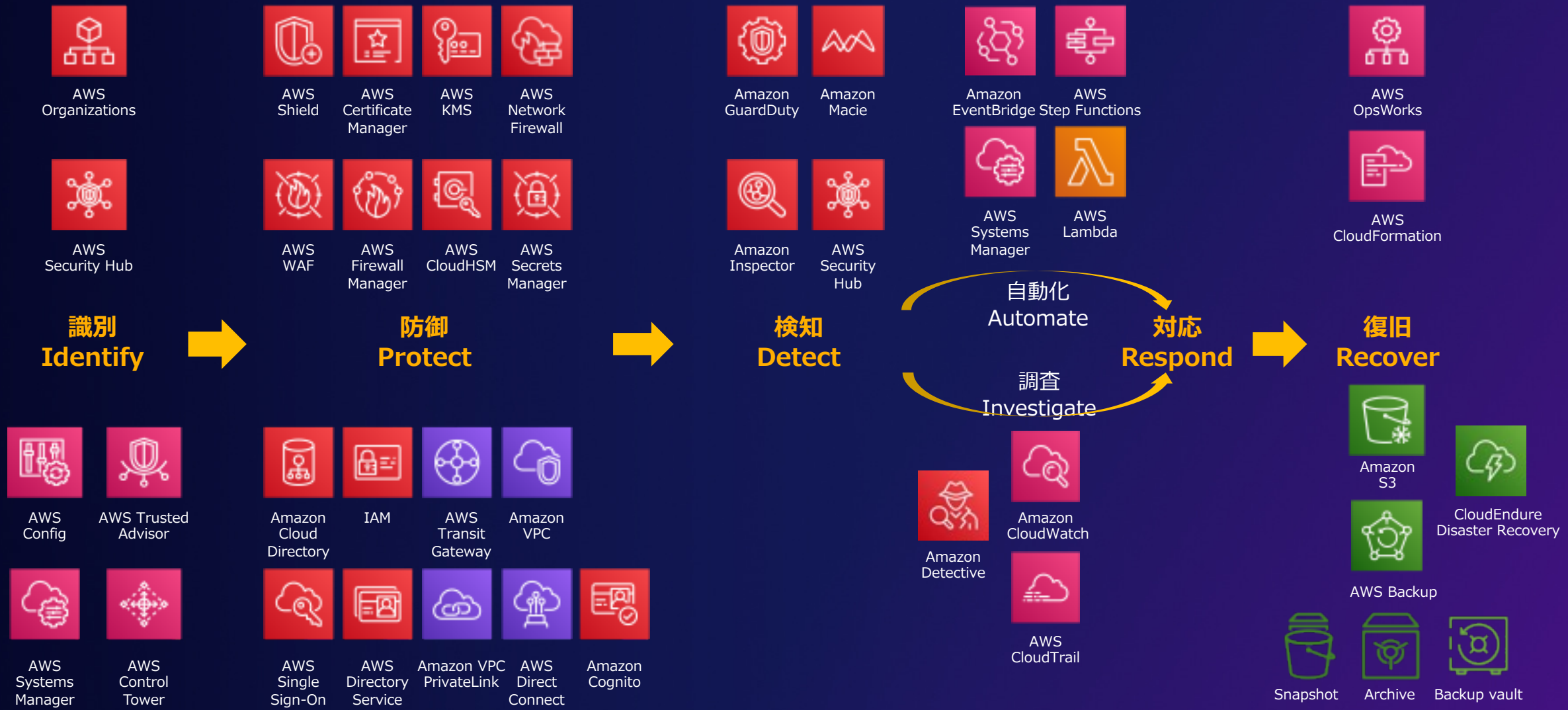
情報システムの提供事業者
- パスワードポリシーの強制機能の実装　　等

関連する AWS サービス
- **AWS Identity and Access Management (IAM)**

AWS インフラストラクチャ関連事項
- **「AWS リスクとコンプライアンスの概要」アクセス制限に関する SOC の統制について**

「医療情報システム向け AWS 利用リファレンス」より一部抜粋

5 つの機能もとにしたセキュリティ対策の基盤



まず見ていただきたい - AWS Trusted Advisor

AWS 環境を最適化する自動リアルタイムガイダンス

AWS 環境を自動監視し推奨設定をお知らせ

例）
- ! IAM パスワードポリシー
- ! Amazon S3 のバケット許可

- ✓ CloudWatch アラートによる通知
- ✓ 週次の日本語レポート
- ✓ 組織のレポートを統合
- ✓ AWS Trusted Advisor が AWS Security Hub と統合

100 以上のチェック項目の追加
（関連リンクを最終ページに掲載）

＊AWS ビジネスサポートと AWS エンタープライズサポートにご契約のお客様はすべてのチェック項目を評価可能

前半の部分のまとめ

- 医療情報システムのガイドライン - 3 省 2 ガイドラインへの対応
- AWS におけるセキュリティの考え方　責任共有モデル
- ガイダンスに対応したセキュリティ対策の考え方
  - 「医療情報システム向け の AWS 利用リファレンス」を活用
  - 5 つの機能をもとにセキュリティ対策の設計をすることも大切
- まず見ていただきたい – AWS Trusted Advisor による継続的なチェック

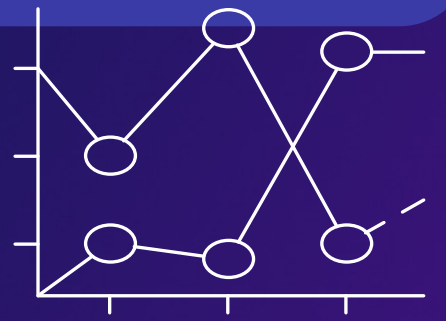
セキュリティのリスクに対応するには

後半のトピックス

医療機関のセキュリティ対策の重要なポイント

ランサムウェア対策としての
バックアップ

脅威を継続的に検知する
モニタリング



バックアップの重要性

厚生労働省
ガイドライン
5.1 版

見読性の確保（7.2）
- バックアップサーバ
- 遠隔地のデータバックアップを使用した見読機能

保存性の確保（7.3）
- 不適切な保管・取り扱いによる情報の滅失、破壊の防止
- バックアップの内容に改ざん等が行われていないよう検査する機能

厚生労働省のガイドライン改定の方向性

- ”ランサムウェアによる対応を重視”
- 特にランサムウェアの被害が
  バックアップ データまで拡大しないよう対策

ランサムウェア対策
を見据えた
バックアップ戦略が重要

ランサムウェア対策

病院の業務をいち早く再開する
＝レジリエンス
に重点をおくことの重要性が高まっています。

対策検討のキーファクター

- 保護する最も重要なデータは何ですか？
- 一部のデータの回復は、他のデータよりも優先されるべきですか?
- 許容できる回復時間はどの位ですか?
- 予算、時間、およびデータの完全性の間でどのようなトレードオフを行う必要がありますか?

ランサムウェア ”復旧” のポイント

イミュータブル (不変)

バックアップを作成後に変更できない状態にする

S3 Object Lock

Backup Vault Lock

分離（復旧の準備）

インフラストラクチャのテンプレート、ファイル、およびアプリケーションのコピーを物理的および論理的に分離しておく

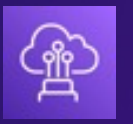
AWS Storage Gateway

AWS Directory Service

Amazon Route 53

Amazon VPC

AWS Direct Connect



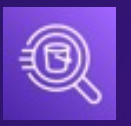
インテリジェンス（分析機能）

機械学習やコンテンツのスキャンデータから、バックアップ破損の兆候・状況を把握する

Amazon EC2，Amazon ECS，または Amazon Lambda 分析のためのシステム

Amazon GuardDuty

Amazon Athena

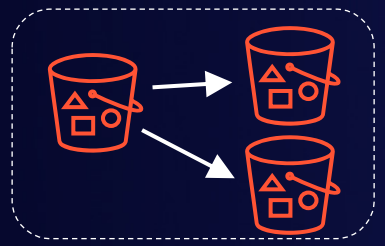


S3 Storage Lens

オンプレミスからのバックアップ

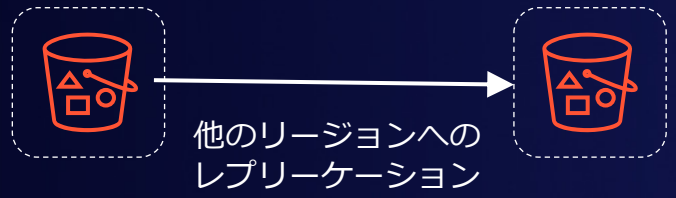
Amazon S3 バックアップの活用

- データ容量の制限なし
- 99.999999999% の耐久性



3つのアベイラビリティゾーン
への分散配置

- 暗号化によるデータ保護
- ディズアスタリカバリ対策



Amazon S3 Object Lock

- イミュータブルなデータの保存の実現
  - *Write Once Read Many* (WORM) モデル
  - 削除または上書きされることを、
    一定期間または無期限に防止

- ガバナンスモード
  - 特別アクセス許可をもたない限り
    オブジェクトのバージョンの上書きや
    削除、ロック設定を変更ができない
- コンプライアンスモード
  - AWS アカウント の root ユーザーを含め、
    ユーザーからの変更ができない

クラウド上でのバックアップ

AWS Backup

- バックアップの集中管理
  - 対応サービスの一例

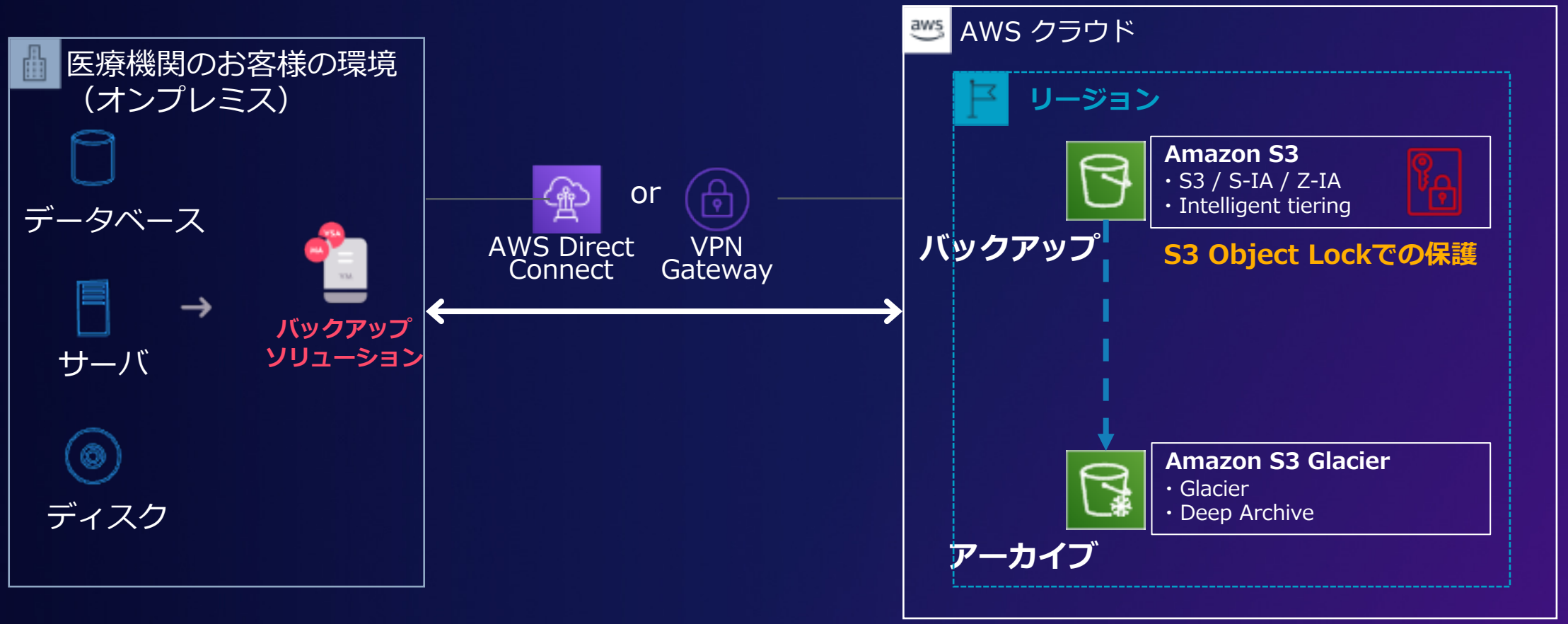
- バックアップの自動化、ライフサイクル管理
- バックアップデータの暗号化
  - 本番環境とバックアップで異なる暗号キー

AWS Backup Vault Lock

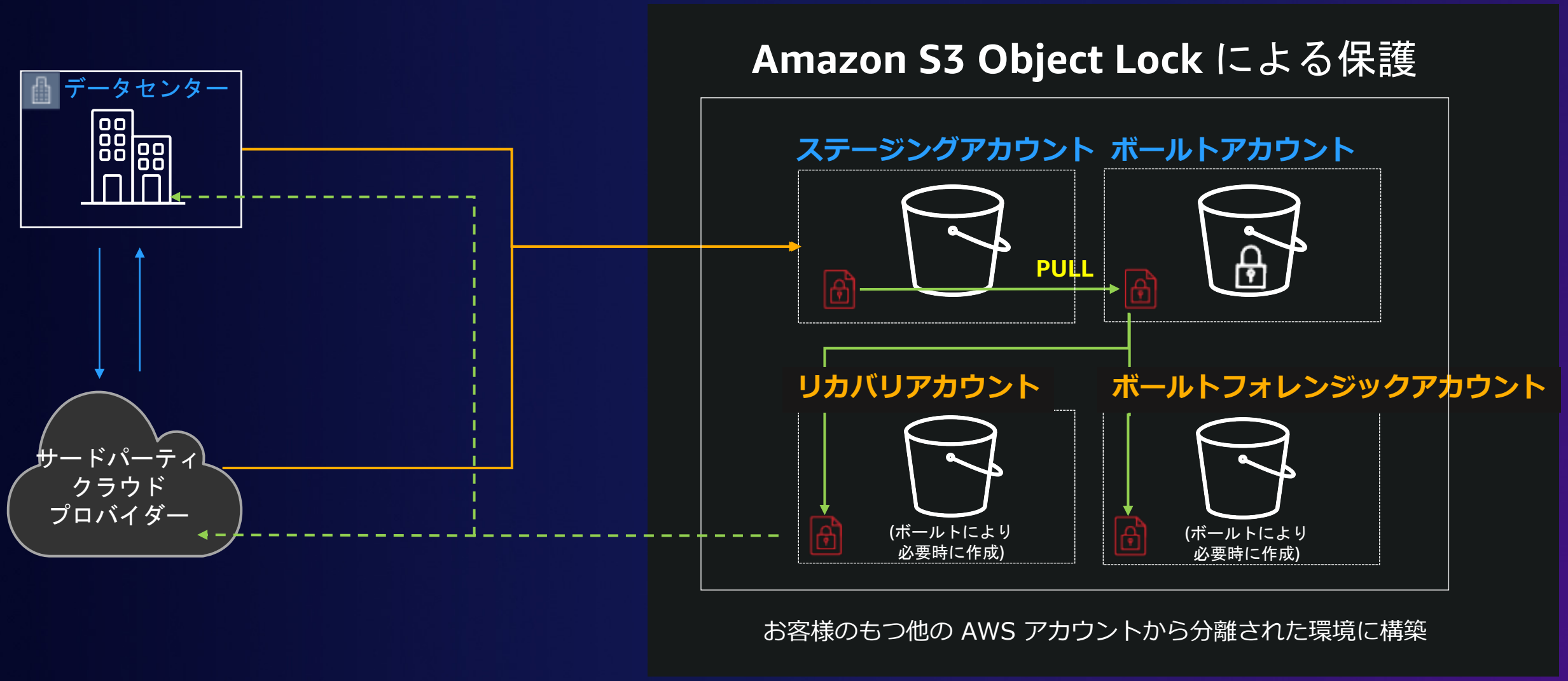
- イミュータブルなデータの保管庫
  - WORM 設定を適用
  - **保持期間の設定**
- ボールトロックによる保護
  - データの削除
  - 保持期間を変更
- AWS Backup API, CLI, or SDKからも設定が可能

オンプレミスからのバックアップの利用例

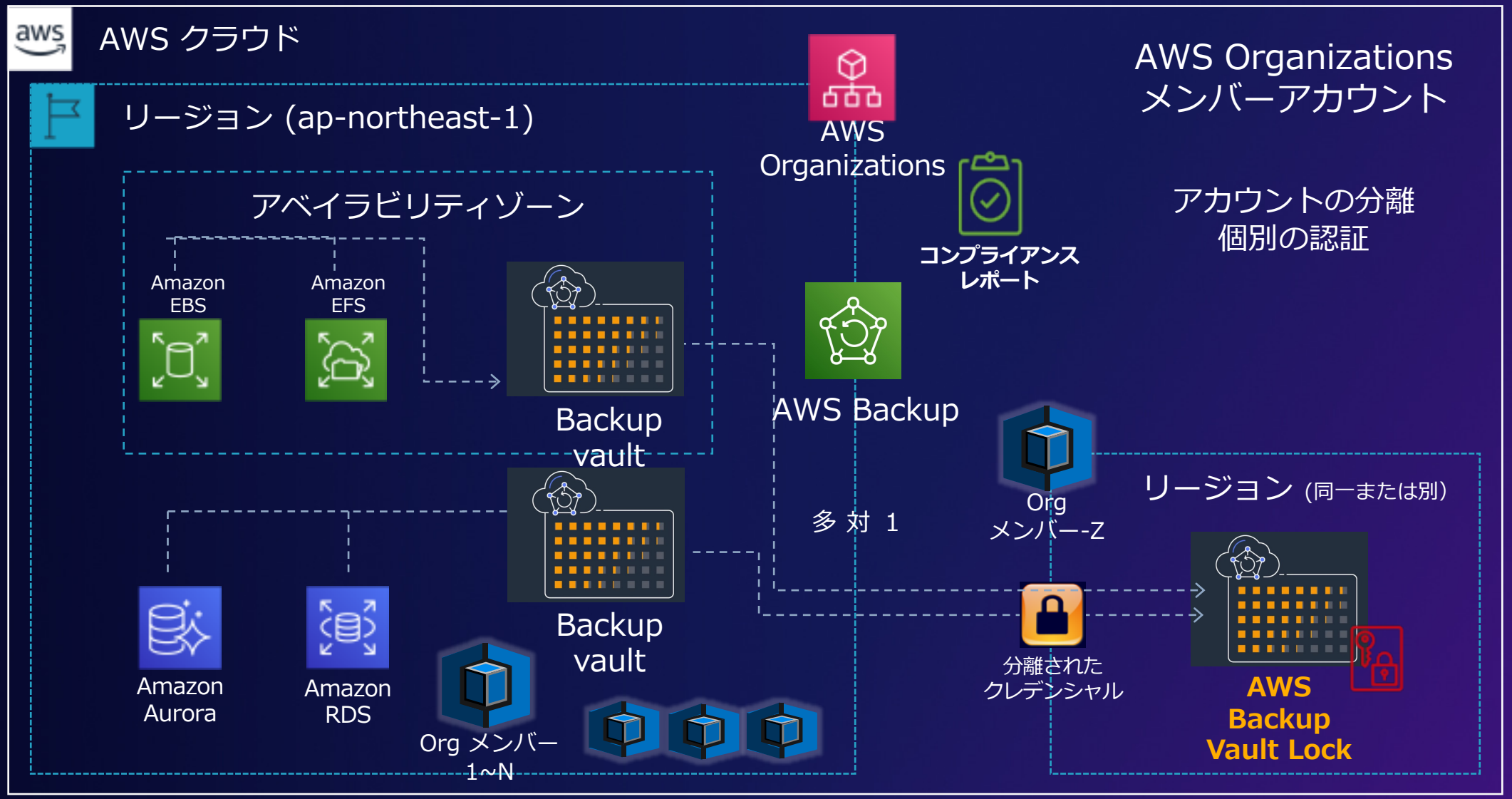
Amazon S3 Object Lock の活用



AWS ランサムウェア リカバリソリューション



AWS 上でのバックアップの利用例



モニタリングの重要性

総務省・経済産業省ガイドライン

想定されるリスクの例（一部）

- 業務上通信する必要のない IP アドレスや TCP/UDP ポートにより、ネットワークを経由した攻撃を受ける。
- 不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。

✓ **閉域のシステムであってもリスクは存在**
- 保守用や、パッチ適用のためのルートを通じた外部との接続
- 端末のマルウェア感染をもとにしたサーバへの侵入

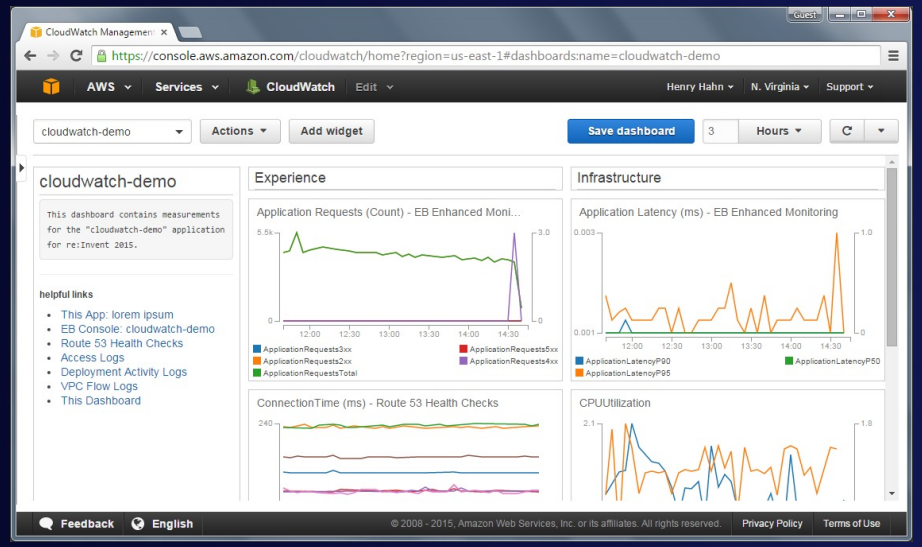
✓ **外部システムとの接続・データ交換の機会の増加**

システム/ネットワークの**脅威を継続的に検知する仕組み**が重要

AWS のログ保管・モニタリングの基本

AWS CloudWatch

- メトリクスの収集と追跡
- ログのモニタリングと保存
- アラームの設定
- グラフと統計の表示（ダッシュボード）



AWS CloudTrail

- アカウントのAPIコールを記録

AWS Config

- リソースの設定変更を継続的に記録

VPC フローログ

- Amazon VPC、サブネット、または単一インターフェイスのネットワークトラフィックのログ記録

変化する環境に対して脅威を検知するには

Amazon GuardDuty

脅威インテリジェンスと継続的監視により
拡大していく AWS アカウントやリソースを効果的に保護

ワンクリックで
有効化
性能影響も無し

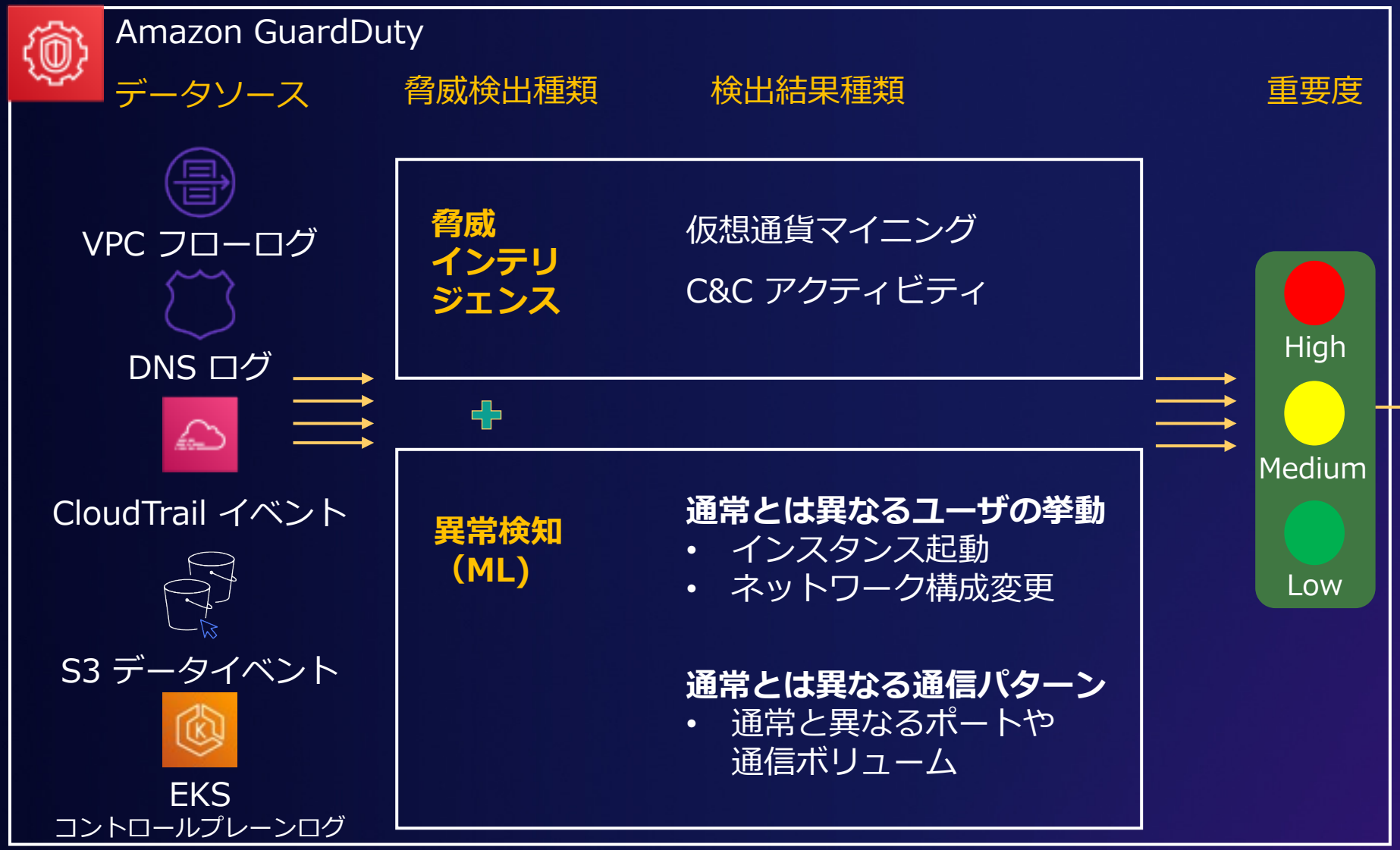
AWS アカウント
とリソースの
継続的監視

各リージョンの
結果による
グローバル対応

既知の脅威と
未知の脅威を
検出

組織全体の統合
と管理

Amazon GuardDuty 動作



実際に何が検出されるのか

100 以上の検出結果（以下は一部）

- Backdoor
  バックドア
- CredentialAccess
  認証情報へのアクセス
- Crypto Currency
  暗号通貨関連の
  アクティビティ
- Persistence
  永続化
- Policy
  ポリシー関連
- Privilege Escalation
  権限昇格
- PenTest
  侵入テスト
- Trojan
  トロイの木馬
- Recon
  偵察行為
- Discovery
  リソースの検出
- Exfiltration
  データ流出
- Unauthorized Access
  許可されないアクセス

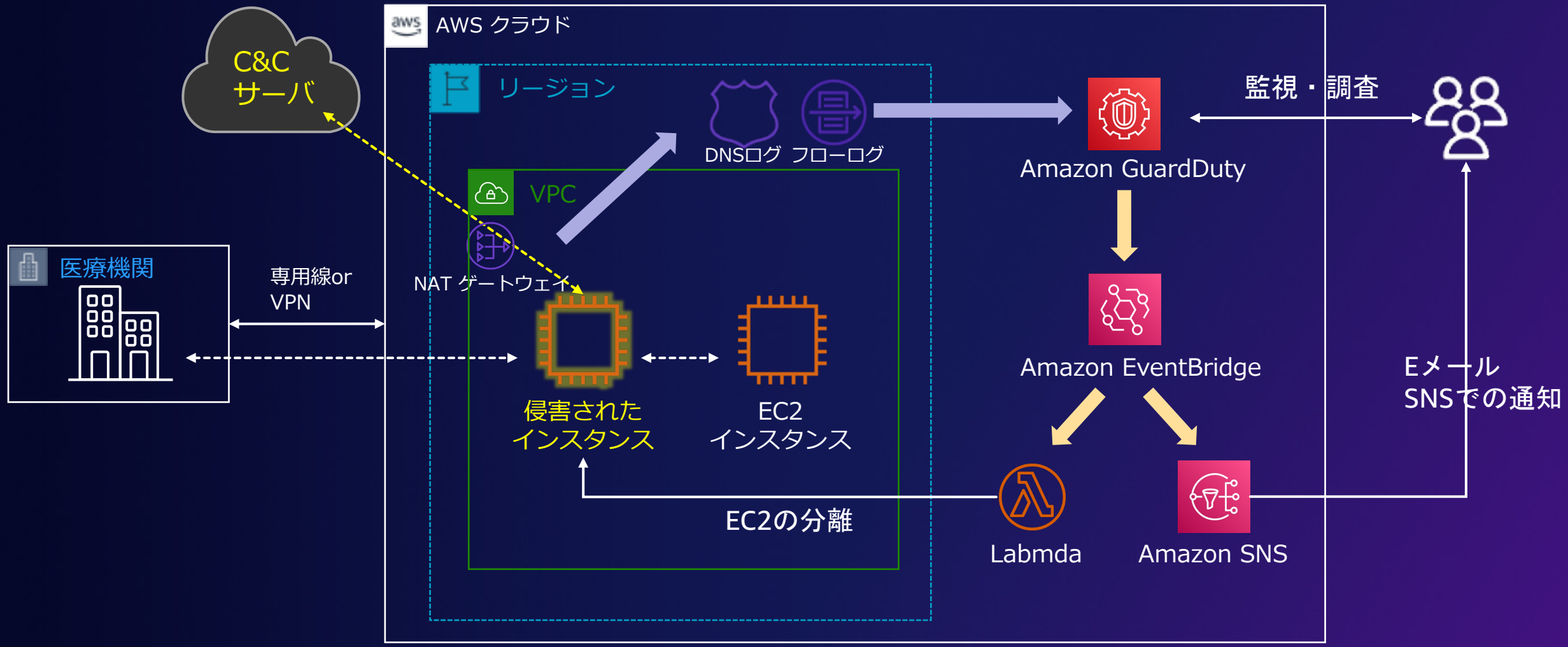
重大度（Severity）

直ちに修正を推奨

できるだけ早く
調査することを推奨

侵害されなかった
不審なアクティビティ
の試行

GuardDuty の対応の自動化の例



更なる調査のために – 情報の集約と分析

他のデータソース
からの検出結果

AWS
Security Hub

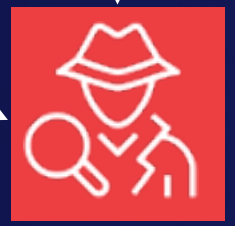
- 組織内の様々なセキュリティデータを集約
- 一元的に可視化してリスクを評価

Amazon
GuardDuty

集約

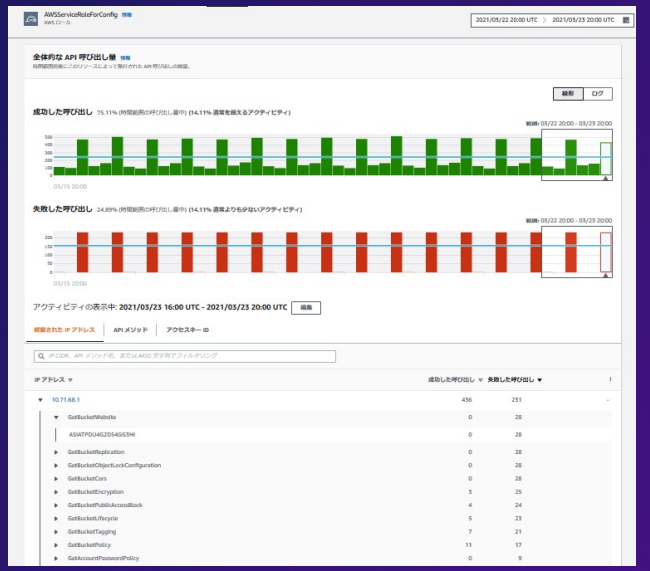
分析

! 重要度 High

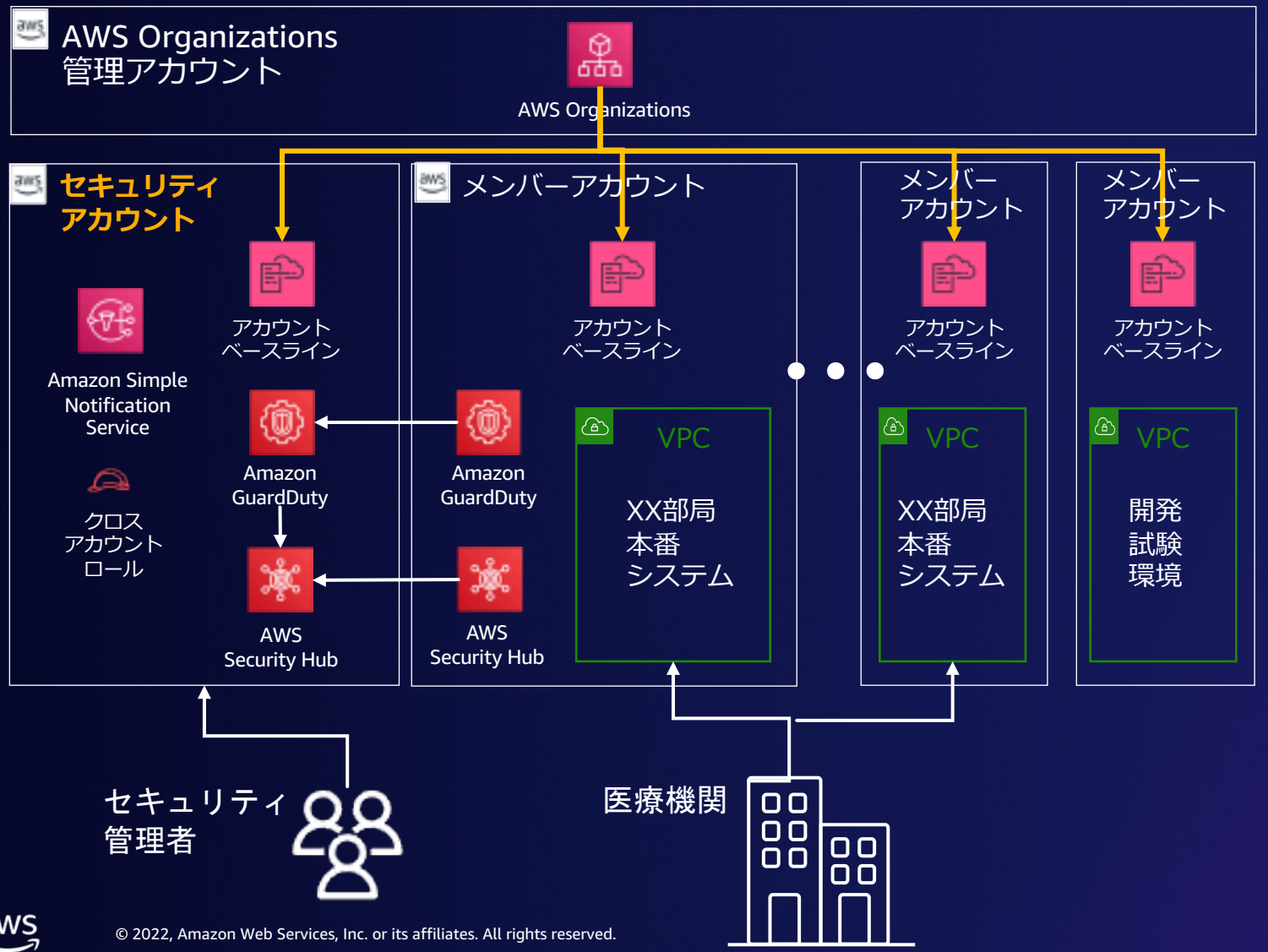


Amazon
Detective

- 検出結果の分析
（正しい検出か）
- インシデントの
影響範囲の特定
- 障害痕跡の調査



セキュリティアカウントによる集中管理



- AWS Organizations による医療機関全体のアカウント管理
- 各部局の本番システム、開発・試験の環境を分離
  - 適切な分離により影響範囲の限定
- セキュリティ管理の統合
  - Amazon GuardDuty, AWS Security Hub の権限移譲された管理アカウント (Delegated Administrator) にセキュリティアカウントを指定する

再掲：5 つの機能もとにしたセキュリティ対策の基盤

まとめ

- 医療業界のクラウド活用と医療情報ガイドラインへの対応
  - ✓ 責任共有モデルをもとにお客様のシステム側のセキュリティ対策を自ら実施
  - ✓ 医療情報ガイドラインへの対策の AWS 利用リファレンスをパートナーが提供
  - ✓ 5 つの機能をもとにセキュリティ対策の設計をすることも大切

- セキュリティのリスクに対応するためには
  - ✓ ランサムウェア対策としてのバックアップ
    → Amazon S3 Object Lock / AWS Backup Vault Lock の活用
  - ✓ 脅威を継続的に検知するモニタリング
    → Amazon GuardDuty の活用

参考資料

- 医療情報システム向け AWS 利用リファレンス
  - https://aws.amazon.com/jp/compliance/medical-information-guidelines/
- AWS Trusted Advisor が AWS Security Hub と統合
  - https://aws.amazon.com/jp/about-aws/whats-new/2022/01/aws-trusted-advisor-security-hub/
- Amazon S3 Object Lock ドキュメント
  - https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/object-lock-overview.html
- Amazon Backup Vault ドキュメント
  - https://docs.aws.amazon.com/ja_jp/aws-backup/latest/devguide/vaults.html
- AWS ブログ：” セキュアなバックアップを実施するための10のベストプラクティス (2022/01/12)”
  - https://aws.amazon.com/jp/blogs/news/top-10-security-best-practices-for-securing-backups-in-aws/
- Amazon GuardDuty （AWS Black Belt OnlineでのAWSサービス別資料）
  - https://d1.awsstatic.com/webinars/jp/pdf/services/20180509_AWS-BlackBelt_Amazon-GuardDuty.pdf

参考：AWS ブログ
″ AWS でバックアップを保護するためのセキュリティベストプラクティス Top 10″

https://aws.amazon.com/jp/blogs/news/top-10-security-best-practices-for-securing-backups-in-aws/

- #1 – バックアップ戦略を策定する
- #2 – バックアップを DR と BCP に組み込む
- #3 – バックアップ操作の自動化
- #4 – アクセス制御の仕組みを実装する
- #5 – バックアップデータとボールトを暗号化する
- #6 – イミュータブルストレージでバックアップを保護する
- #7 – バックアップの監視とアラートを実装する
- #8 – バックアップ設定の監査
- #9 – データ復旧機能をテストする
- #10 – インシデント対応計画にバックアップを組み込む

Thank you!