クラウドネイティブセキュリティとCxOの役割

Cloud Security Alliance Secure DevSecOps WG/Serverless WG

Copyright © 2022 Cloud Security Alliance Japan Chapter

http://www.chapters.cloudsecurityalliance.jp/

1. CxO Trust Summit 2022/CSA SECtember 2022 の振り返り
2. アプリケーションコンテナ/マイクロサービスの
   クラウドセキュリティ
3. サーバーレスのクラウドセキュリティ

Cloud Security Alliance Secure DevSecOps WG/Serverless WG

CSAJC cloud security alliance Japan Chapter

Copyright © 2022 Cloud Security Alliance Japan Chapter

1. CxO Trust Summit 2022/CSA SECtember 2022 の振り返り

Cloud Security Alliance Secure DevSecOps WG/Serverless WG

Copyright © 2022 Cloud Security Alliance Japan Chapter

CxO Trust Summit 2022 (9/27) (1)

- **CxO Trust Summitの対象：クラウドユーザー／カスタマー企業のCISOおよびその他の経営層**
- **基調講演：**
  - **Jason Witty, CISO,USAA(元JPモルガンチェースCISO)**
    “*Making your Board of Directors Cyber Security Leaders*”
  - **Bob Lord, Senior Technical Advisor, Cybersecurity and Infrastructure Security Agency (CISA)**
    “*Change Agent: CISA’s Shift to Private/Public Partnering*”
  - **Natalie Pittore, Chief of Enduring Security Framework, National Security Agency (NSA)**
    “*Today’s Cyber Environment: Tackling Strategic Threats with Tactical Efforts*”
- **パネルディスカッション：**
  - **Barth Bailey (Fulton Financial Corporation CISO), Andy Kirkland (元Starbucks CISO), Steve Koinm (Pure IT Credit Union Services CISO), Stacy Hughes (Quantum Computing Digital Media AI/IoTヘッド)**
    “*Panel Discussion: Keeping Businesses Secure and Staying Cyber Aware*”

Copyright © 2022 Cloud Security Alliance Japan Chapter

CxO Trust Summit 2022 (9/27) (2)

- **CSA Research Team & Security Innovation, "*Threat Modeling: A Hands-On Table Top Exercise to Understand Cloud Based Attacks*"**
  - **CSAがSecurity Innovationと連携して開発した経営層向け脅威モデリング卓上演習のデモンストレーションを実施。**
  - **自動車メーカーのケースを想定し、同じテーブル上の参加者を、製品開発事業責任者、製品セキュリティ責任者、CISO、COO、法務責任者、データプライバシー責任者、PR責任者にアサインさせる。**
  - **インシデントの内部把握、ホワイトハッカーからの脆弱性報告など、複数のシナリオを提示して、各々の立場から対策を話し合う。**

Copyright © 2022 Cloud Security Alliance Japan Chapter

CSA SECtember 2022 (9/28) (1)

- **Welcome Address by Jim Reavis, CEO, Cloud Security Alliance**
  - CSAの脅威モデリング
  - グローバルセキュリティデータベース(GSD) WG
  - ゼロトラスト・アドバンスメント・センター
  - 量子コンピューター
  - STAR/CCAK
  - トラステッド・クラウドコンサルタント・サービス
- 基調講演：
  - Joseph “Rich” Baich, Chief Information Security Officer and Director of the Office of Cyber Security, Central Intelligence Agency (CIA), “***Cloud Security or Future Emerging Technologies: Practices For Effective Operational Governance***”
  - Phil Venables, Chief Information Security Officer, Google Cloud, “***The CISO's Corner: A Chat with Phil Venables***”

Copyright © 2022 Cloud Security Alliance Japan Chapter

CSA SECtember 2022 (9/28) (2)

- パネルディスカッション：
  - **Daniele Catteddu, Chief Technology Officer, Cloud Security Alliance and Caleb Sima, Chief Security Officer, Robinhood Markets, “*The CISO's Corner: A Chat with Daniele Catteddu*”**
    - セキュリティ人材の課題、人材採用の課題、サプライチェーンセキュリティの課題
  - **Matthew Hathaway, Chief Marketing Officer, True Fort, Jasmine Henry, Field Security Director, Jupiter One, Matt Lehto, Chief Revenue Officer, Hyper Proof, David Richardson, Vice President of Product, Lookout, John Yeoh, Global Vice President of Research, Cloud Security Alliance, “*Transforming Security Along with the Business*”**
    - デジタルトランスフォーメーション(DX)とセキュリティ、CISOの関係
  - **Jerry Cochran, Deputy Chief Information Officer, Pacific Northwest National Laboratory, Rick Doten, VP, Information Security; CISO, Healthcare Enterprises Centene “*Finding Cloud Security Balance and Perfecting Your Cloud Strategy*”**
    - コンテナ、マイクロサービスの普及期におけるセキュリティ

Copyright © 2022 Cloud Security Alliance Japan Chapter

CSA SECtember 2022 (9/28) (3)

- **Troy Leach, Chief Strategy Officer, Cloud Security Alliance**
  "State of Financial Services in the Cloud"
  - **CSAの金融サービス業界向けロードマップ**
    - **1. 上手くできることをやる**
    - **2. クラウド上の金融サービスを保護するために、提供するものを拡大する**
    - **3. 認識を醸成する**
    - **4. 参加と関与の機会を拡大する**
  - **CSAのミッション**
    - **Educate: 実務家向け業界特化型トレーニング、規制当局／意思決定者向け支援**
    - **Secure: マルチクラウドマイグレーション向けユースケースの研究、産業特化型CVE(GSD)レポーティング**
    - **Empower: CISO向けの調達支援、クラウドサービスプロバイダーの透明性**

Copyright © 2022 Cloud Security Alliance Japan Chapter

CSA SECtember 2022 (9/29) (1)

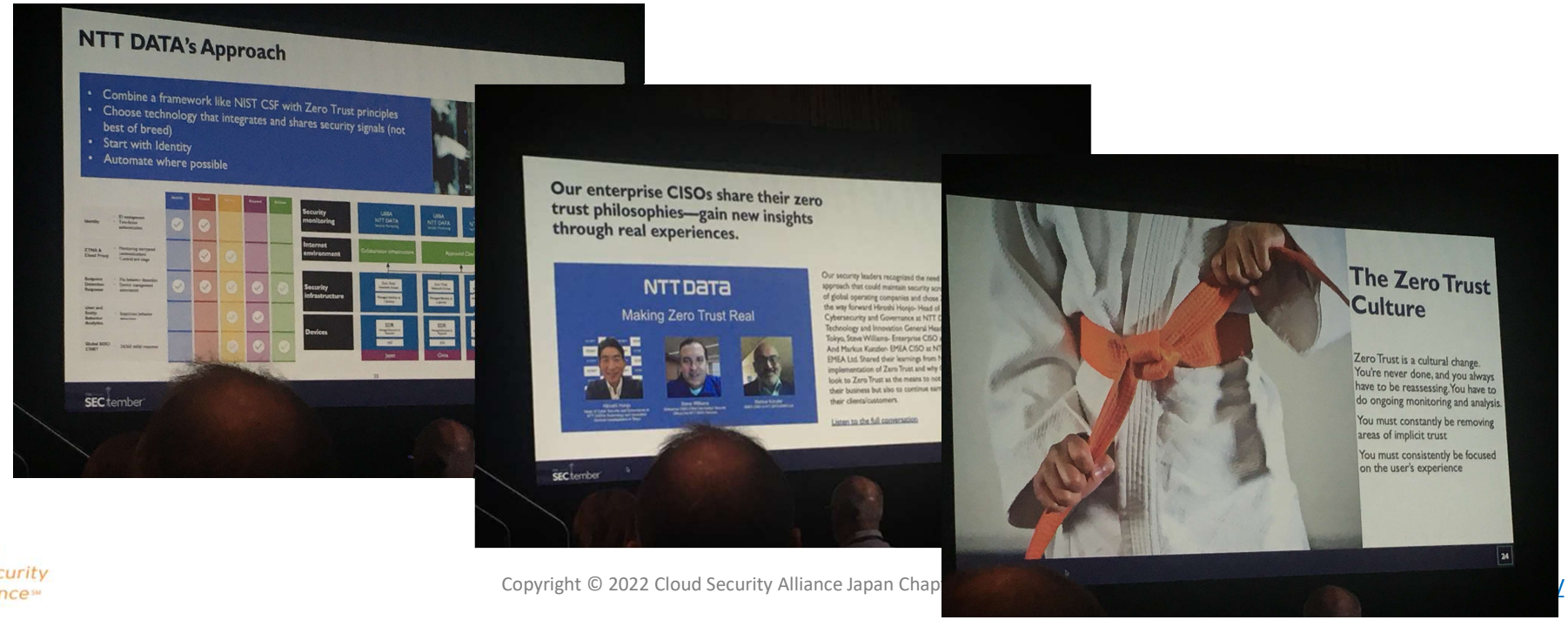
- **Chapter Leader Breakfast**
  - CSA各チャプターのリーダーが参加
    - 海外：メキシコ、ドイツ、イタリア、オランダ、中国、日本
- (事例) シアトルチャプターと教育機関との連携
  - 国家安全保障局(NSA)のサイバーセキュリティ・エデュケーション・センター・オブ・エクセレンスに指定されているシアトル・シティ大学と連携して、サイバーセキュリティ専門プログラム（学士＆修士）を支援している

（参考）City University of Seattle > MS in Cybersecurity
https://my.cityu.edu/program/ms-in-cybersecurity/
Sam Chung, Ph.D., Program Director
E: chungsam@cityu.edu

Copyright © 2022 Cloud Security Alliance Japan Chapter

CSA SECtember 2022 (9/29) (2)

- **基調講演：NTT Data (CSA本部コーポレートメンバー)**
  “How NTT DATA embarked on the Zero Trust Journey”
  (NTTデータグループにおけるゼロトラストモデルのグローバル導入事例)



Copyright © 2022 Cloud Security Alliance Japan Chap

CSA SECtember 2022 (9/29) (3)

- **CSA DevSecOps WG “*Six Pillars Series of DevSecOps*”**
  - 対象：クラウドユーザー企業のクラウド専門チームと開発者
    “The Six Pillars of DevSecOps”（2019年8月7日発行）
    - 6つのPillarごとにサブグループを構成し、ミーティング（隔週）やドキュメント作成を行っている（Pillar 2、3、6のボランティアを募集中）
      - Pillar 1：連帯責任（2020年2月21日発行）
      - Pillar 2：連携と統合（作成作業中）
      - Pillar 3：実用的な展開（作成作業中）
      - Pillar 4：法令遵守と開発の橋渡し（2022年2月8日発行）
      - Pillar 5：自動化（2020年7月6日発行）
      - Pillar 6：評価、監視、報告、行動（作成作業中）
    - 成熟度評価に基づくDevOpsのスケーリングに向けたアプローチ
    - DevOpsマトリクス・評価におけるバリューストリームマップ（VSM）の活用
    - DevOpsによるデリバリーの成功と組織戦略／ITミッション／組織パフォーマンスの関係

2. アプリケーションコンテナ/マイクロサービスのクラウドセキュリティ

Cloud Security Alliance Secure DevSecOps WG/Serverless WG

Copyright © 2022 Cloud Security Alliance Japan Chapter

アプリケーションコンテナのクラウドセキュリティ(1)

- CSA 「*クラウドコンピューティングのためのセキュリティガイダンスv4.0*」（2017年7月）
  - Domain 8：仮想化とコンテナ技術
    - 8.1.4 コンテナ
      =移植性の高いコード実行環境
    - [主要コンポーネント]
      - 実行環境
      - 統合管理とスケジューリングのコントローラ
      - コンテナイメージまたは実行するコードのリポジトリ

Copyright © 2022 Cloud Security Alliance Japan Chapter

アプリケーションコンテナのクラウドセキュリティ(2)

コンテナのセキュリティ要件

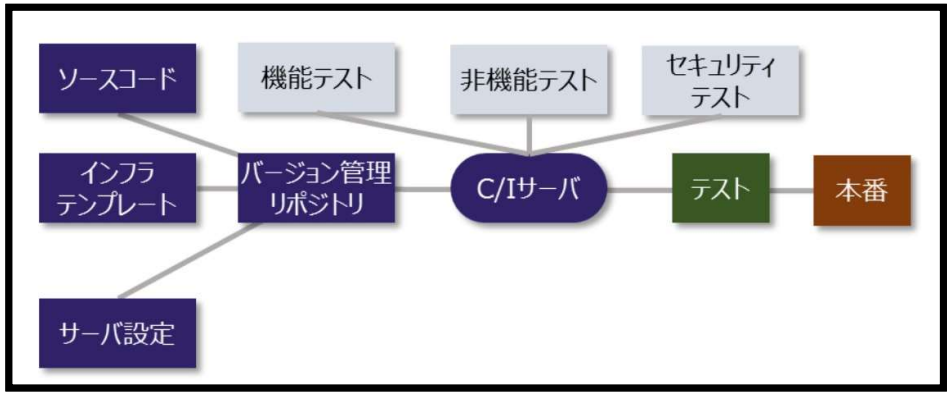
要件
利用するコンテナプラットフォームとその下のOSのセキュリティのための隔離機能を把握し、適切な設定を選択すること
コンテナ間の隔離の実施には物理マシンまたは仮想マシンを用い、同一の物理／仮想ホスト上の同一のセキュリティ要件のコンテナはグループ化すること
配備対象となるのは、確実に、承認済みで認知済みでセキュアなコンテナのイメージかコードだけとなるようにすること
コンテナの統合化・管理およびスケジューラのソフトウェアのセキュリティを適切に設定すること
全てのコンテナとリポジトリ管理に対して、適切なロールベースのアクセス管理と、強度の高い認証を実装すること

Copyright © 2022 Cloud Security Alliance Japan Chapter

アプリケーションコンテナのクラウドセキュリティ(3)

- **DevOpsとは？**
  - アプリケーションの開発と配備を自動化することにフォーカスした、アプリケーション開発の新しい方法論であり考え方である
  - 開発チームと運用チームの間の協力とコミュニケーションを改善してより深く結びつけることを意味し、特にアプリケーション配備とインフラストラクチャ運用の自動化に焦点を当てている
  - コード堅牢化、変更管理、本番アプリケーションのセキュリティを改善するだけでなくセキュリティ運用全般をも強化してくれる

継続的インテグレーション／継続的デプロイ（CI/CD）パイプライン



出典：日本クラウドセキュリティアライアンス「クラウドコンピューティングのためのセキュリティガイダンス v4.0」日本語版1.1（2017年7月）

http://www.chapters.cloudsecurityalliance.jp/

アプリケーションコンテナのクラウドセキュリティ(4)

DevOpsのセキュリティへの波及効果

項目	波及効果と長所
標準化	DevOps では、本番に組み込まれるものはすべて、承認済みのコードと設定用テンプレートに基づき、継続的インテグレーション／継続的デプロイ（CI/CD）パイプラインによって生み出される。開発、テスト、本番（のコード）はすべて完全に 同一のソースファイルから派生しており、周知となっている優れた標準からの逸脱を防いでいる。
自動化されたテスト	広範な種類のセキュリティテストは、必要に応じて補助的に手動 テストを加えることで、CI/CD パイプラインに組み込むことが可能である。
不可変性(immutable)	CI/CD パイプラインは、素早く確実に、仮想マシンやコンテナ、インフラストラクチャスタックのマスターイメージを生成する。これにより配備の自動化と不可変(immutable)なインフラストラクチャを実現する。
監査と変更管理の改善	CI/CD パイプラインはソースファイルにある 1 文字の変更に至るまでの全て を追跡調査できる。バージョン管理リポジトリに格納され たアプリケーションスタック（インフラストラクチャを含む）の全履歴と共に、その変更は変更を行った人物と紐づけられる。
SecDevOps/DevSecOps と Rugged DevOps	SecDevOps/DevSecOps は セキュリティ運用を改善するために DevOps の自動化技術を使う。Rugged DevOps はアプリケーション開発過程にセキュリティテスティングを組み入れることを意味し、よ り強固で、よりセキュアで、より障害耐性の高いアプリケーションを生み出す。

Copyright © 2022 Cloud Security Alliance Japan Chapter

アプリケーションコンテナのクラウドセキュリティ(5)

- **CSA 「*アプリケーションコンテナとマイクロサービスのセキュリティにおける課題*」（2019年7月）[英語版のみ]**

  [構成]

  - **1. 序論**
  - **2. アプリケーションコンテナとマイクロサービスの課題**
  - **3. アプリケーションコンテナとマイクロサービス: ユースケースと機能**
  - **4. マイクロサービス**

Copyright © 2022 Cloud Security Alliance Japan Chapter

アプリケーションコンテナのクラウドセキュリティ(6)

ユーザー/ディベロッパー主導

[主旨]

- アプリケーションコンテナとマイクロサービスのアーキテクチャは、DevOpsのようなアジャイルソフトウェア開発手法を活用して、アプリケーションを設計、開発、展開するために利用される
- セキュリティは、これらのソフトウェア開発手法に組込まれる必要がある
- 本文書では、開発者、運用者、アーキテクトの視点を通して、信頼性のあるセキュアなシステムのエンジニアリングにおいて、アプリケーションコンテナやマイクロサービスのセキュリティに取組む際の課題を特定している

Copyright © 2022 Cloud Security Alliance Japan Chapter

アプリケーションコンテナのクラウドセキュリティ(7)

- **CSA 「*安全なアプリケーションコンテナアーキテクチャ実装のためのベストプラクティス*」（2020年2月）**
  - アプリケーションコンテナの課題に対するリスク緩和策

No.	リスク緩和策
1	環境全体（開発、品質保証、テスト、本番）のコードプロモーション
2	ホストをセキュアにする
3	プラットフォーム/ホストからのコンテナ継続性監視
4	コンテナネットワーク - ホストとコンテナ間の通信
5	コンテナ・ネットワーク - コンテナ間通信
6	イメージの完全性とセキュリティレベルの検証
7	コンテナのフォレンジック
8	コンテナによるトラストチェーン

Copyright © 2022 Cloud Security Alliance Japan Chapter

アプリケーションコンテナのクラウドセキュリティ(8)

アプリケーションコンテナの課題に対するリスク緩和策(続き)

No.	リスク緩和策
9	コンテナのボリューム管理
10	コンテナのシークレット管理
11	プラットフォーム管理 - ライフサイクルイベント通知
12	プラットフォーム管理 - リソース要求
13	プラットフォーム管理 - コンテナリソース管理
14	コンテナ管理 - コンテナリソースのスケーリング
15	コンテナ管理 - データのバックアップとレプリケーション
16	コンテナ管理 – CMP間のコンテナのホスト変更
17	コンテナの暗号化

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(1)

- CSA 「*クラウドコンピューティングのための セキュリティガイダンスv4.0*」（2017年7月）
  - Domain 10：アプリケーションセキュリティ
    - 10.1.5 クラウドのアプリケーション設計とアーキテクチャへの影響
      - 分離が最初から備わっていること
      - イミュータブル（不可変）インフラストラクチャ
      - マイクロサービス利用の拡大
      - PaaSとサーバーレスアーキテクチャ

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(2)

- APIのセキュリティ要件
  - APIとWebサービスは特に入念に堅牢化し、認証を受けたのと受けないのと両方の攻撃者からの攻撃を想定しておくこと。それにはAPI向けに特別に設計された業界標準の認証手段を利用することも含まれる。
  - APIの不正利用や異常な動作を監視すること。
  - APIとWebサービスは特に入念に設計とテストを行い、攻撃やテナント間の不正なまたは偶発的なアクセスを防ぐようにしなければならない。

セキュリティ/プライバシー・バイ・デザイン

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(3)

- **CSA 「*安全なマイクロサービスアーキテクチャ実装のためのベストプラクティス*」（2020年2月）**
  - **マイクロサービスの課題解決のための推奨事項およびベストプラクティス集**

[構成](1)

1. マイクロサービスアーキテクチャの概要

- **サービスオリエンテッドアーキテクチャ（SOA)**
- **モノリシックとマイクロサービスアーキテクチャの比較**
- **マイクロサービスの利点と課題**

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(4)

[構成](2)

2. クラウドネイティブ・アプリケーション向けマイクロサービスアーキテクチャ

- 全体的な脅威モデルと関連するベストプラクティス
- **API**のセキュア化
- マイクロサービス向けの認証とアクセス制御
- マイクロサービスアーキテクチャにおけるセキュアな展開スタイルと戦略
- ステートフルとステートレスのマイクロサービスセキュリティ
- コンテナストレージのインタフェース
- ランタイムセキュリティ

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(5)

[構成](3)

3. マイクロサービスの展開とガバナンス
   - マイクロサービスにおけるコンテナセキュリティのベストプラクティス
   - マイクロサービス検知の制御
   - マイクロサービスのメッセージングパターン
   - マイクロサービスのガバナンス
4. モノリシックアプリケーションの分解
   - マイクロサービス：ユースケース
   - マイクロサービス：機能
   - モノリシックアプリケーション分解のベストプラクティス

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(6)

- 米国NIST 「***NIST SP800-204C: サービスメッシュを利用したマイクロサービスベースアプリケーション向けDevSecOpsの展開***」（2022年3月）
  - 目的：DevSecOps基礎向け参照プラットフォーム(Reference Platform for DevSecOps Primitives)の展開のためのガイダンスを提供する
  - 参照プラットフォームの展開が、高度のセキュリティ保証のためにもたらすベネフィットと、リスク管理ツールとダッシュボードのメトリクスを利用して、継続的な運用権限(C-ATO)を提供するためのパイプライン内におけるアーティファクト利用について記述する

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(7)

[構成](1)

- 1 イントロダクション
- 2 DevSecOps基礎向け参照プラットフォーム
  - 2.1 コンテナオーケストレーションとリソース管理プラットフォーム
  - 2.2 サービスメッシュ・ソフトウェア・アーキテクチャ
- 3 DevSecOps – 組織的な対応準備、 重要な基礎、展開
  - 3.1 DevSecOps向けの組織的な対応準備
  - 3.2 DevSecOpsプラットフォーム
  - 3.3 DevSecOps – 重要な基礎と展開タスク

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(8)

[構成](2)

- 4. 参照プラットフォーム向けDevSecOps基礎の展開
  - 4.1 コードのタイプと参照プラットフォームのコンポーネントの記述
  - 4.2 アプリケーションコードとアプリケーションサービスコード向けのCI/CDパイプライン
  - 4.3 インフラストラクチャ・アズ・コード向けのCI/CDパイプライン
  - 4.4 ポリシー・アズ・コード向けのCI/CDパイプライン
  - 4.5 オブザーバビリティ・アズ・コード向けのCI/CDパイプライン
  - 4.6 CI/CDパイプラインのセキュア化
  - 4.7 CI/CDパイプラインにおけるワークフローモデル
  - 4.8 セキュリティテスト - すべてのコード向けのCI/CDパイプライン共通要求事項
  - 4.9 サービスメッシュのアプリケーションセキュリティに対するDevSecOps基礎のベネフィット
  - 4.10 継続的な運用権限(C-ATO)向けDevSecOpsの活用
- 5. 要約と結論

Copyright © 2022 Cloud Security Alliance Japan Chapter

マイクロサービスのクラウドセキュリティ(9)

- DevSecOpsプラットフォーム
  - A) パイプラインソフトウェア
    - CIソフトウェア – コードレポジトリからコードを取り寄せ、構築ソフトウェアを引き出し、検証ツールを引き出して、検証済アーティファクトをイメージレジストリに戻して保存する
    - CDソフトウェア – アーティファクトやパッケージを引き出し、インフラストラクチャ・アズ・コード(IaC)における計算処理、ネットワーク、ストレージのリソースの記述に基づいて、パッケージをデプロイする
  - B) ソフトウェア開発ライフサイクル（SDLC）ソフトウェア
    - 構築ツール (例. IDEs)
    - 検証 (SAST、DAST、SCA)
  - C) レポジトリ
    - ソースコード・レポジトリ (例. GitHub)
    - コンテナイメージ・レポジトリまたはレジストリ
  - D) 可観測性またはモニタリングツール
    - ロギング・ログ集約ツール
    - メトリクスを生成するツール
    - トレーシングツール (アプリケーションコールのシーケンス)
    - 可視化ツール (ダッシュボード/アラートを生成するために上記からのデータを組み合わせる)

・管理プロセスの自動化
・ノーコード／ローコード開発

Copyright © 2022 Cloud Security Alliance Japan Chapter

3. サーバーレスのクラウドセキュリティ

Cloud Security Alliance Secure DevSecOps WG/Serverless WG

Copyright © 2022 Cloud Security Alliance Japan Chapter

サーバーレスのクラウドセキュリティ(1)

- CSA 「*クラウドコンピューティングのためのセキュリティガイダンスv4.0*」（2017年7月）
  - Domain 10：アプリケーションセキュリティ
    - 10.1.5 クラウドのアプリケーション設計とアーキテクチャへの影響
      - 分離が最初から備わっていること
      - イミュータブル（不可変）インフラストラクチャ
      - マイクロサービス利用の拡大
      - PaaSとサーバーレスアーキテクチャ
        - PaaS やサーバレスのセットアップは、攻撃される要素(attack surface)を劇的に削減する大きな可能性を秘めている。ただしこれは、クラウド事業者がプラットフォームとサーバレスのセットアップに責任を持ち、利用者の要件を満たす場合のみである。

Copyright © 2022 Cloud Security Alliance Japan Chapter

サーバーレスのクラウドセキュリティ(2)

- **CSA 「*安全なサーバーレスアーキテクチャを設計するには*」（2021年9月）**

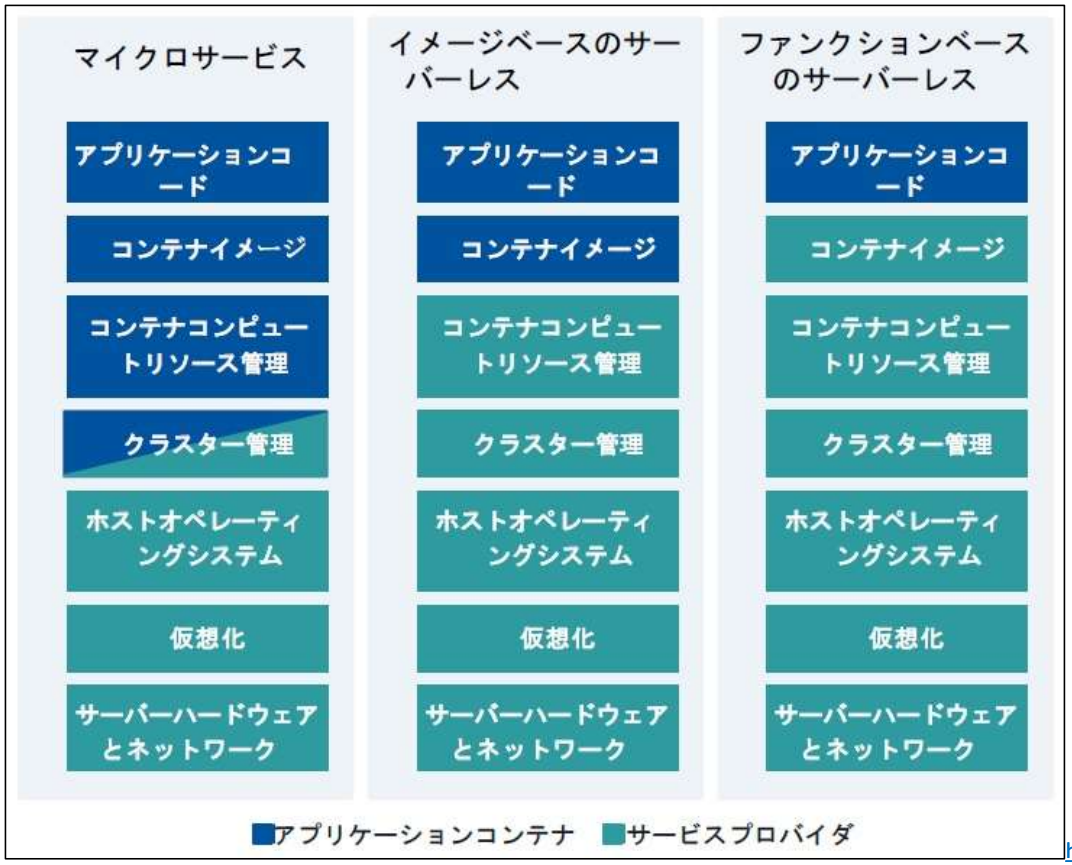
[構成]

- **1. はじめに**
- **2. サーバーレスとは**
- **3. なぜサーバーレスなのか**
- **4. ユースケースと事例**
- **5. サーバーレスのセキュリティ脅威モデル**
- **6. セキュリティのデザイン、コントロール、ベストプラクティス**
- **7. サーバーレスセキュリティの未来像**
- **8.結論**

Copyright © 2022 Cloud Security Alliance Japan Chapter

サーバーレスのクラウドセキュリティ(3)

- プラットフォームプロバイダとアプリケーションオーナーの責任分担



出典：日本クラウドセキュリティアライアンス「安全なサーバーレスアーキテクチャを設計するには」（2021年9月）
http://www.chapters.cloudsecurityalliance.jp/

サーバーレスのクラウドセキュリティ(4)

イメージベースとファンクションベースの責任分担比較

[イメージベースのサーバーレス]

[ファンクションベースのサーバーレス]

出典：日本クラウドセキュリティアライアンス「安全なサーバーレスアーキテクチャを設計するには」（2021年9月）

Copyright © 2022 Cloud Security Alliance Japan Chapter

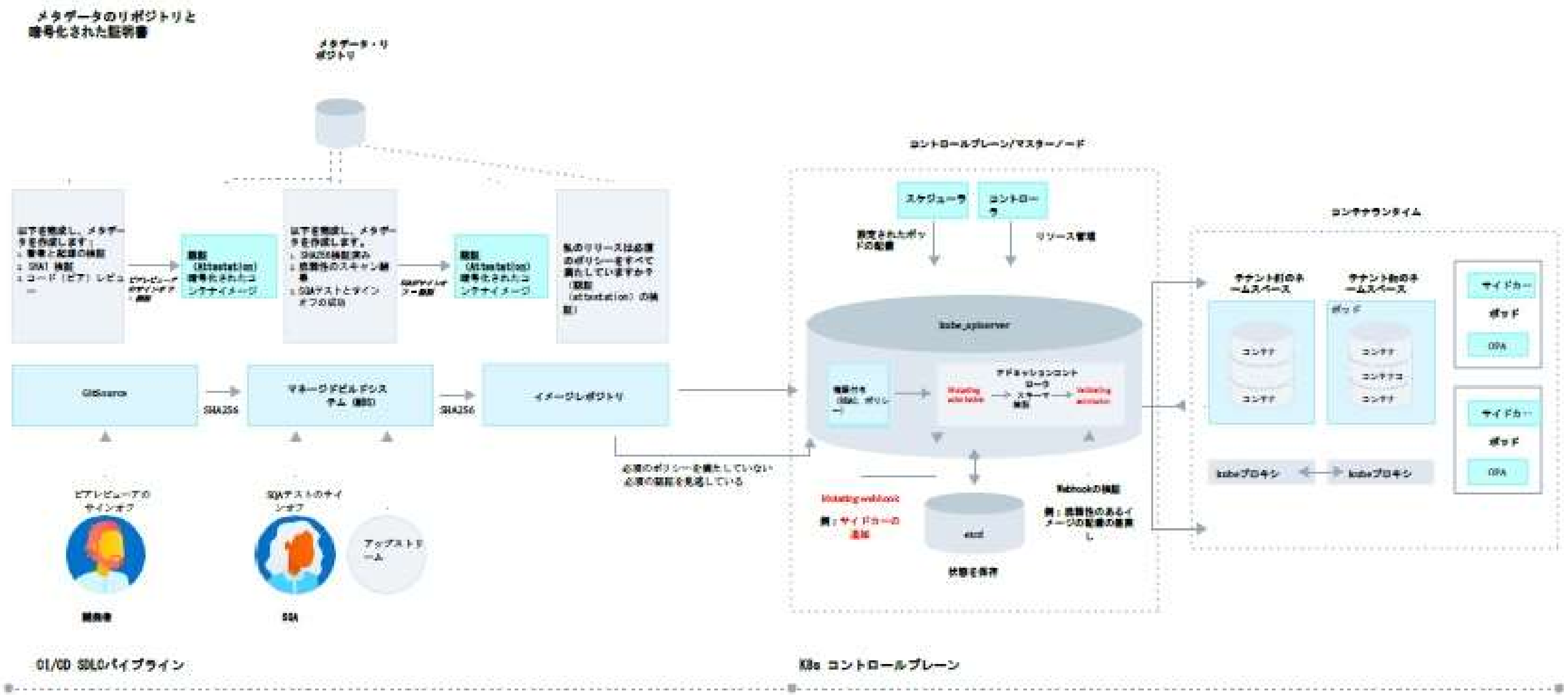
サーバーレスのクラウドセキュリティ(5)

- **CI-CDパイプライン、ファンクションコード、コードスキャン、ファンクションとコンテナのポリシーの実施(1)**

出典：日本クラウドセキュリティアライアンス「安全なサーバーレスアーキテクチャを設計するには」（2021年9月）

サーバーレスのクラウドセキュリティ(6)

- **CI-CD**パイプライン、ファンクションコード、コードスキャン、ファンクションとコンテナのポリシーの実施**(2)**



出典：日本クラウドセキュリティアライアンス「安全なサーバーレスアーキテクチャを設計するには」（2021年9月）

Copyright © 2022 Cloud Security Alliance Japan Chapter

サーバーレスのクラウドセキュリティ(7)

サーバーレスアーキテクチャのセキュリティ脅威

- **イメージ／ファンクションベースのサーバーレスに共通の脅威**
  1. コンテナ化とオーケストレーションの脅威
     - a. コンテナ化／オーケストレーションツールの脆弱性
     - b. コンテナ化／オーケストレーションAPIの悪用
  2. 不適切に割り当てられた無制限／管理権限アクセス
  3. 不正アクセス
  4. ポータル／コンソールの脆弱性

- **その他の脅威**
  1. 自動デプロイメントツールに対する／経由の攻撃
  2. 搾取されたコードのレポジトリ
  3. 搾取されたイメージのレポジトリ
  4. 不十分／安全でないロギング
  5. 安全でないシークレット管理
  6. リソースの浪費
  7. 安全でないまたは意図しないデータのキャッシュ

- **ファンクションベースのサーバーレスの脅威**
  1. 環境の構成ミス
     - a. ユーザーの構成管理ミス
     - b. ポートの露出
     - c. 無効化／デフォルト構成
     - d. 資格情報の露出
     - e. 構成ドリフト
  2. 脆弱な依存関係
     - a. サプライチェーンの脆弱性
     - b. 脆弱なイメージ
  3. 組込型マルウェア
  4. ランタイムの課題
     - a. データのインジェクションとリモートからの実行
     - b. 認証の不備
     - c. 不適切なエラーや例外の処理

Copyright © 2022 Cloud Security Alliance Japan Chapter

サーバーレスのクラウドセキュリティ(8)

- **CSA 「*サーバーレスアーキテクチャのセキュリティを確保するためのCレベルへのガイダンス*」(2022年4月19日)**

1. はじめに - エグゼクティブサマリー

サーバーレスコンピューティングは、開発者の開発とデプロイを高速化し、コンテナ・クラスタや仮想マシンなどのインフラストラクチャを管理せずに、より効果的にクラウド・ネイティブ・サービスに移行することを可能にします。企業が技術的価値をより早く市場に投入するために、サーバーレスプラットフォームは開発者の間で採用が進んでいます。

他の新しいテクノロジーと同様に、サーバーレスも様々なサイバーリスクをもたらします。本書の前半では、アジリティ、コスト、市場投入スピードなど、サーバーレスアーキテクチャがもたらすビジネス上のメリットについて説明します。第2部では、サーバーレスアプリケーションのセキュリティに焦点を当て、業界全体のベストプラクティスと推奨事項を説明します。結論として、経営層がサーバーレスアーキテクチャをどのように捉え、導入する際にどのような要素を考慮すべきかを整理しています。

本書の情報は、サーバーレスコンピューティングを導入し、そのビジネスやセキュリティへの影響を理解する必要がある読者を対象としています。

Copyright © 2022 Cloud Security Alliance Japan Chapter