



Cloud Security Alliance Japan Chapter

*Application Containers and
Microservices Working Group*

Proposed Charter V1

June 2019

Cloud Security Alliance Japan Chapter Application Containers and Microservices Working Group Charter

(日本クラウドセキュリティアライアンス アプリケーションコンテナ&マイクロサービス・ワーキンググループ設立趣意書)

Working Group Executive Overview (ワーキンググループの概要)

The mission of the CSA Japan Chapter Application Containers and Microservices (ACM) working group is to conduct research on the security of application containers and microservices, to publish guidance and best practices for the secure use of application containers and microservices, and to engage in educational activities on security of application containers and microservices.

日本クラウドセキュリティアライアンスのアプリケーションコンテナ&マイクロサービス(ACM)ワーキンググループは、アプリケーションコンテナおよびマイクロサービスのセキュリティに関する基本的な調査研究を行い、セキュアなアプリケーションコンテナおよびマイクロサービス利用のためのガイダンスやベストプラクティスを発行するとともに、アプリケーションコンテナおよびマイクロサービスのセキュリティに関する啓発活動を行うことを目的とする。

Working Group Scope (ワーキンググループのスコープ)

Per NIST Special Publication SP 800-180 (DRAFT), Application Containers are defined as “a construct designed to package and run as application or its’ components running on a shared Operating System. Application Containers are isolated from other Application Containers and share the resources of the underlying Operating System, allowing for efficient restart, scale-up or scale-out of applications across clouds. Application Containers typically contain Microservices.”

Microservices are defined per the same NIST SP as, “a basic element that results from the architectural decomposition of an application’s components into loosely coupled patterns consisting of self-contained services that communicate with each other using a standard communications protocol and a set of well-defined APIs, independent of any vendor, product or technology. Microservices are built around capabilities as opposed to services, builds on SOA and is implemented using Agile techniques. Microservices are typically deployed inside Application Containers.”

Building on the joint NIST / CSA Application Container Security Guidance developed by the NIST Cloud Security Working Group as well as NIST Special Publication SP 800-190 Application Container Security Guide, the scope of this working group is to conduct research on how to secure application containers and microservices, and engage in educational activities on security of application containers and microservices.

NIST Special Publication SP 800-180 (DRAFT)によると、アプリケーションコンテナは、共有 OS 上で稼働するアプリケーションまたはそのコンポーネントとしてパッケージ化し、稼働するように設計された構成物と定義される。アプリケーションコンテナは、他のアプリケーションコンテナから分離され、下にある OS を共有しながら、クラウド上で、アプリケーションの効率的な再スタート、スケールアップまたはスケールアウトを可能にする。通常、アプリケーションコンテナには、マイクロサービスが含まれる。

同じ NIST SP によると、マイクロサービスは、アプリケーション・コンポーネントのアーキテクチャを、疎結合のパターンに分解した結果生まれる基本的要素であり、標準的な通信プロトコルや明確に定義された API を利用して相互に通信する自己充足型サービスを構成し、いかなるベンダー、製品、技術からも独立している。マイクロサービスは、サービスとは対照的に、ケイパビリティの周辺に構築され、SOA 上に構築し、アジャイル技術を利用して展開される。通常、マイクロサービスは、アプリケーションコンテナの内部に展開される。

NIST Cloud Security Working Group により開発された NIST / CSA Application Container Security Guidance および NIST Special Publication SP 800-190 Application Container Security Guide 上で構築される本ワーキンググループは、アプリケーションコンテナおよびマイクロサービスをセキュアにする方法に関する研究を実施し、啓発活動を行うことをスコープとする。

Relationship to Cloud (クラウドとの関係)

For agencies and enterprises moving applications to the cloud, a microservices architecture leveraging application containers represent a smarter and more economical way to move to the cloud.

Application containers can be run “on premise” on physical computer systems owned and maintained by the organization, or on platforms provided by a service provider.

クラウドにアプリケーションを移行する政府機関や企業にとって、アプリケーションコンテナを活用したマイクロサービスのアーキテクチャは、クラウド移行のためのよりスマートで経済的な方法を提供する。アプリケーションコンテナは、組織が所有・維持する物理的なコンピューターシステム上、またはサービスプロバイダーが提供するプラットフォーム上で、「オンプレミス」に稼働させることができる。

Working Group Membership and Organization (ワーキンググループの参加資格および組織)

The working group is composed of volunteers from individual/corporate/affiliate members of CSA Japan Chapter. Under a steering committee and co-chairs, the working group coordinate typical project management, online workspace, technical writing assistance and reporting to Board Member meetings of CSA Japan Chapter.

Kanto sub-work group and Kansai sub-work group are formed to plan or execute any related outreach, awareness or research opportunities.

本ワーキンググループは、日本クラウドセキュリティアライアンスのインディビジュアル／コーポレート／アフィリエイトメンバーからのボランティアによって構成される。

本ワーキンググループは、運営委員会および共同座長の下で、主要なプロジェクトマネジメント、オンラインワークプレイス、テクニカルライティング支援、日本クラウドセキュリティアライアンス理事会への報告をコーディネートする。

これらに関連する周知、認知、研究の機会を計画／実行するために、関東分科会および関西分科会を設置する。

Deliverables (成果物)

[June - August 2019]

- Japanese-language translation of “Challenges in Securing Application Containers - Integrating Application Container Security Considerations into the Engineering of Trustworthy Secure Systems”
- Materials for Workshops by CSA Japan Chapter ACM WG (Topic: TBD)

[September - November 2019]

- Japanese-language translation of “Best Practices for Implementing a Secure Microservices Architecture - Integrating Microservices Security Considerations into the Engineering of Trustworthy Secure Systems”
- Materials for Workshops by CSA Japan Chapter ACM WG (Topic: TBD)

[December 2019 - February 2020]

- Japanese-language translation of documents published by CSA ACM WG (Topic: TBD)
- Materials for Workshops by CSA Japan Chapter ACM WG (Topic: TBD)

[March - May 2020]

- Japanese-language translation of documents published by CSA ACM WG (Topic: TBD)
- Materials for Workshops by CSA Japan Chapter ACM WG (Topic: TBD)

Deliverables will be governed by intellectual property rights policy of CSA Japan Chapter.

[2019年6月-8月期]

- “Challenges in Securing Application Containers - Integrating Application Container Security Considerations into the Engineering of Trustworthy Secure Systems” 日本語翻訳版
- CSA ジャパン ACM WG 研究会作成資料(トピック:未定)

[2019年9月-11月期]

- “Best Practices for Implementing a Secure Microservices Architecture - Integrating Microservices Security Considerations into the Engineering of Trustworthy Secure Systems” 日本語翻訳版
- CSA ジャパン ACM WG 研究会作成資料(トピック:未定)

[2019年12月-2020年2月期]

- CSA ACM WG 発行ドキュメントの日本語翻訳版(トピック:未定)
- CSA ジャパン ACM WG 研究会作成資料(トピック:未定)

[2020年3月-5月期]

- CSA ACM WG 発行ドキュメントの日本語翻訳版(トピック:未定)
- CSA ジャパン ACM WG 研究会作成資料(トピック:未定)

成果物は、日本クラウドセキュリティアライアンスの著作権ポリシーに準拠して管理される。

Communications Methods (伝達手段)

Regular meeting onsite/online and collaboration via mailing lists and social media.

Official language of the working group: Japanese and English.

定期的なオンサイト／オンラインミーティングおよびメーリングリストやソーシャルメディアを利用したコラボレーション活動

ワーキンググループの公用語: 日本語および英語

Duration (活動期間)

The working group will operate until May 31, 2020 for its chartered deliverables, and at that time consider charter renewal.

本ワーキンググループは、本趣意書に定める成果物のために、2020年5月31日まで活動し、その時点で趣意書の更新を検討するものとする。

Working Group Leaders (ワーキンググループ責任者)

Eiji Sasahara, Leader - CSA Japan Application Containers and Microservices (ACM) Working Group

笹原英司 - CSA ジャパン アプリケーションコンテナ&マイクロサービス(ACM) ワーキンググループリーダー