EdgeTech+ 横浜 2023講演

コンテナ技術活用におけるセキュリティ対策の勘所

～委員会の活動内容のご紹介、コンテナセキュリティ対策の必要性～

2023年11月15日

組込みシステムセキュリティ委員会
副委員長 牧野進二

mailto:buildlab.koha9ru108@gmail.com

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

当委員会の紹介

組込みシステムセキュリティ委員会

技術委員会　配下に組織化
- 委員長　理事 副会長 佐野氏
- 副委員長　牧野
- JASA会員企業、一般企業、団体から参加
- アドバイザー：IPA、情報セキュリティ大学院大学　教授

セキュリティ啓発活動WG

- 都立産業技術研究所との連携を図り、中小企業向けのセキュリティ啓発の活動を実施
  - ET、JASA主催イベント、セミナーなどでの講演
  - 都産技 セミナー
  - 信用金庫の顧客向けセミナー
  - 民間企業との共催セミナー
- EDSA認証やCC認証など組込み機器開発における開発に必要な認証に対する認証方法の普及

外部連携WG

- 経済産業省、総務省、警察庁などの官公庁、YRP、他団体(CCDS、SIoTP協議会、CSAJなど)と連携し、現場技術者に対するセミナーや普及活動の実施

組込みデバイスセキュリティWG

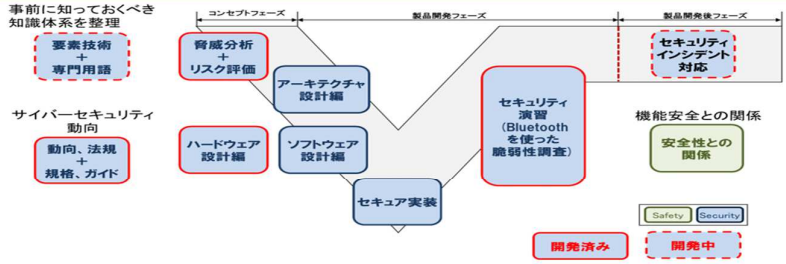
- 組込み技術者のスキル向上を狙い、組込み機器の分解や解析を行った結果からセキュリティ設計における留意点や開発プロセスを定義し、現場技術者が利用できるコンテンツを作成し、発信
- 組込み機器の分解や解析結果から、教育用のコンテンツ作成と、セミナーやJASA試験として立ち上げを実施

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

© Japan Embedded Systems Technology Association 2023

セキュリティ教材のご紹介

セキュリティ教材の開発



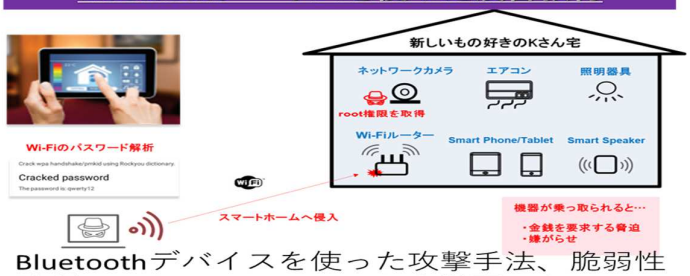
組込みエンジニアが利用できるセキュリティ教材の開発を開始し、2024年1月以降に公開予定。オンライン受講可能なコンテンツとして開発を実施中。

EN303 645規格を解説した教材

一般消費者向けIoTセキュリティ規格調査

各国で始まるラベリング、認定制度に向けて欧州でのRED指令EN303 645規格がベースとなるため、規格を分かり易く解説コンテンツを公開予定

Bluetoothデバイスを使った演習教材



Bluetoothデバイスを使った攻撃手法、脆弱性診断、セキュリティテストを学習できるコンテンツを公開予定。(Keysight様開発)

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

セキュアIoTプログラム(IoT機器の認定制度)

Secure IoT Platform Consortium

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

設立趣旨
セキュアIoTプラットフォーム協議会は、日本の産業界の知見を集約し、全世界のIoT機器およびサービスに対し、安心・安全な新社会基盤を創出する。

事業内容
- ◆ 次世代 IoT セキュリティ標準の規格化およびデファクトスタンダード化に向けての普及活動
- ◆ IoT 利活用推進および事例構築
- ◆ 共同実証実験(POC)の実施
- ◆ 最新 IoT 関連情報の発信
- ◆ セキュリティ人材の育成
- ◆ セキュリティ関連認証事業
- ◆ 上記の項目に付帯する活動

IoTデバイス製造レイヤー	ネットワークレイヤー	データ管理レイヤー	サービスレイヤー
ICチップへの証明書の埋め込みによる暗号・認証でのデバイス工数の低減	高度暗号化、接続の際の成りすましの排除、改ざん防止	ビックデータの匿名化および暗号化データ処理による安全性向上	プライバシー保護、暗号化・改ざん・フィッシング防止

IoT機器適合性評価事業「セキュアIoTプログラム」における共同運営

安心・安全なデジタル社会の実現に向けてIoT機器のサイバーセキュリティ対応力を強化

設立趣旨：組込みシステムにおける応用技術に関する調査研究、標準化の推進、普及及び啓発等を行うことにより、組込みシステム技術の高度化及び効率化を図り、もって我が国の産業の健全な発展と国民生活の向上に寄与することを目的とする。

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

セキュアIoTプログラム(IoT機器の認定制度)

- 「脆弱性検査およびIoTセキュリティ検査」とIoTシステムに求められるセキュリティ要件を以下の点に絞り込み、国際標準への適合性を確認する「セキュアIoT認定」を組合わせたIoT機器のセキュリティ適合性評価基準を満たすプログラム
- 産業用システム、業務システム、コンシューマ機器における最終的なIoT機器だけではなく、IoT機器を構成する部品やソフトウェア、システムも認定対象（対象となる機器に求められるセキュリティレベルにより、１～４までのクラスを設定）
- セキュアIoTプラットフォーム協議会が発行する[IoTセキュリティ手引書」を認定基準(IEC62443、SP-800シリーズなどセキュリティ国際安全基準/ガイドラインの参照し策定）として検査
- JASA / SIOTP協議会が運営事務局,認定機関となり、登録指定検査事業者により、申請された事業者のIoT機器の検査実施、結果を[セキュアIoT認定」として認定

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

医療系機器のサイバーセキュリティ攻撃(ランサムウェア)

半田病院のランサムウェア被害

- **2021年10月31日**: ランサムウェアに感染。電子カルテ利用不可。医事サーバーダウン。外来会計出来ない状態。**記者会見の実施**。
- 2021年11月1日: ネットワークを介さない印刷対応。
- 2021年11月2日: システムベンダー（以下A社）と電子カルテ復旧に向けた協議。
- 2021年11月3日: A社紹介の修復会社（以下B社）にサーバーを送り調査復旧の方針決定。
- 2021年11月4日: ワープロとして端末での診療記録対応
- 2021年11月5日: 端末・サーバーをB社に発送。電子カルテベンダー（以下C社）が来院。
- 2021年11月6日: 端末のウイルススキャンによる感染洗い出し作業の実施。
- 2021年11月8日: B社と協議。VPNを突破された可能性の指摘を受ける。
- 2021年11月10日: 感染の確認されなかった端末を含め全回収。
- 2021年11月12日: ファストフォレンジック（証拠保全）作業開始。
- 2021年11月15日: 小児科の通常診療再開。
- 2021年11月19日: **B社からデータ復元可能**との報告。
- 2021年11月26日: 現状と診療再開に向けての**記者会見実施**。
- 2021年11月30日: サーバー3台がB社から返却（発送から25日後）。
- 2021年12月21日: 感染した端末全体の初期化。
- 2021年12月29日: 電子カルテシステムのデータ復元を確認。
- **2022年1月4日**: 電子カルテシステム再稼働し**通常診療再開**（感染から65日後）。
- 2022年2月4日: 有識者会議設置（感染から約3ヶ月後）。
- 2022年3月1日: 有識者会議・調査事務局による現地調査第１回。
- 2022年6月7日: 有識者会議調査報告書の公開。

詳細は上記参考サイトの調査報告書を参照。

大阪急性期・総合医療センターのランサムウェア被害

- **2022年10月31日**: 電子カルテ利用不可。ランサムノート（身代金要求文書）と暗号化の事実を確認。BCPに基づき紙カルテの運用開始。**記者会見の実施**。
- 2022年11月1日: 電話回線がパンク状態。
- 2022年11月3日: 専門家チームが調査。侵入経路を給食センターからと断定。
- 2022年11月4日: 近隣の病院94ヶ所宛に支援要請をFAX。予定手術の一部再開。
- 2022年11月7日: 電話発信用に10回線追加。二度目の記者会見。
- 2022年11月9日: オフラインバックアップデータから電子カルテ参照可能に（参照のみ）。
- 2022年11月10日: 厚生労働省から全医療機関へ注意喚起の通達。医療分野のサイバーセキュリティ対策について｜厚生労働省
- 2022年11月22日: 全端末（2,200台）初期化開始。
- 2022年12月12日: 基幹システム（電子カルテシステム、オーダーリング、医事会計等）を再稼働。
- 2022年12月22日: 全端末（2,200台）初期化完了。
- 2023年1月10日: 部門システムを再稼働。
- **2023年1月11日**: 通常診療開始（感染から72日後）

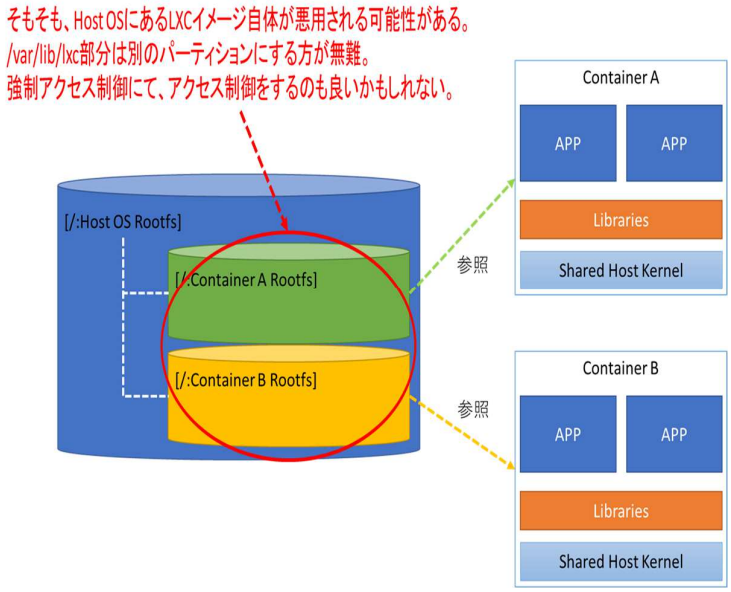
初動対応で連絡した関係各所

- 大阪府立病院機構本部
- 大阪府健康医療部
- 大阪府住吉警察署
- 内閣サイバーセキュリティセンター（NISC）
- 厚生労働省医政局
- 大阪市保健所

厚生労働省医政局に報告を行った際に、初動対応支援の専門家チーム派遣の提案があった。

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

コンテナ活用におけるセキュリティ対策の必要性



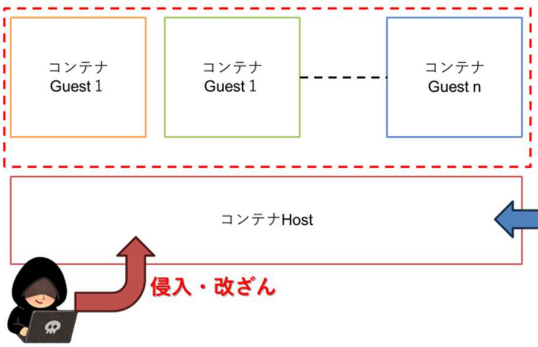
・①強制アクセス制御(SELinux、AppAmor)
・②Seccomp
・③セキュアブート(コンテナイメージに電子署名付与、署名検証)
・④コンテナイメージスキャン(脆弱性スキャン)
・⑤Sysdig Secure(モニター監視)
・⑥Falcoによるコンテナ監視と警告

IoT機器など組込み機器においては、使用できるリソース(CPU、メモリ、記憶領域など)が限られている。
コンテナ環境においては、セキュリティ確保のためには
コンテナホスト本体とコンテナイメージに対するシンプル且つ各自なセキュリティ確保が必要

コンテナ活用におけるセキュリティ対策の必要性

Linux コンテナのセキュリティ検討

当委員会での検討において、一般的には、コンテナGuest→コンテナHostの対策はあるが、コンテナHostに対するセキュリティ対策はないことが多いこと、組込み機器においては、利用できるリソース(CPU、メモリ、ストレージなど)が限られているため、コンテナ環境におけるセキュリティ対策には、コンテナHost、コンテナGuestに対するシンプル且つ、確実なセキュリティ対策が必要になってくると考え、会員企業様の協力を得て、コンテナHostに対するセキュリティ対策を検討を実施した。



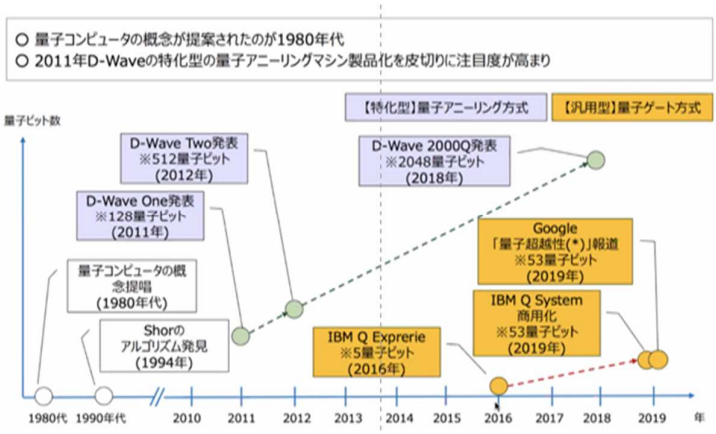
コンテナGuest側の対策例
・①強制アクセス制御(SELinux、AppAmor)
・②Seccomp
・③セキュアブート(コンテナイメージに電子署名付与、署名検証)
・④コンテナイメージスキャン(脆弱性スキャン)
・⑤Sysdig Secure(モニター監視)
・⑥Falcoによるコンテナ監視と警告

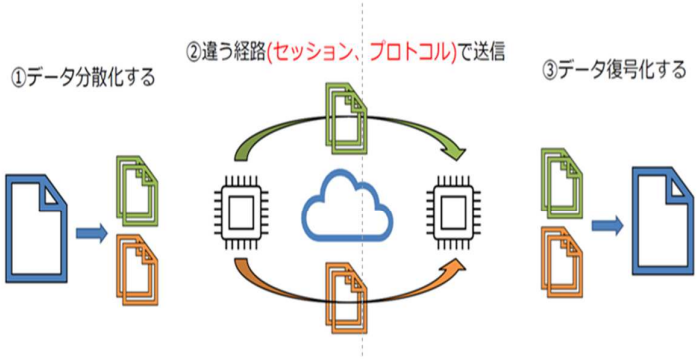
コンテナHost、コンテナGuestイメージに対するセキュリティ対策が必要

コンテナHostとの改ざん検知、改ざん検知後の復旧を迅速い対応できるための対策方法を検討・実装してデモを展示しています。

コンテナ活用におけるセキュリティ対策の必要性

■ 巧妙化するサイバー犯罪、量子コンピュータの実用化による従来型の暗号化だけではない対策が必要
- 「計算的安全性」だけでは守れなくなってきている。
- 「**情報理論的安全性**」が実用になってきている。

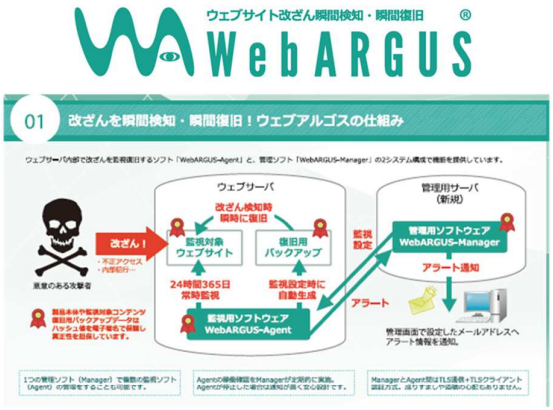




秘密分散技術によるバックアップの活用など

コンテナ活用におけるセキュリティ対策の必要性

会員企業様からのご協力内容

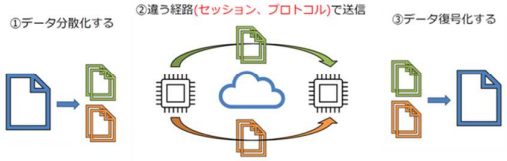


多層防御の防御が突破され、攻撃者の改ざん攻撃の発生を瞬時に検知し、元の正常な状態に復元てきる新しい改ざん対策が実現可能。昨今の巧妙化・悪質化するサイバー攻撃に対する防御が可能となる。

デジタル・インフォメーション・テクノロジー株式会社

会員企業のDIT(デジタルインフォメーションテクノロジー)様、エイチアイ様が開発したソリューションを活用させて頂きLinuxコンテナの改ざん検知・復旧のPoCを行い、検討の内容を活用させて頂けました。

秘密分散を活用したバックアップ



改ざん検知後の復旧には、バックアップの正確性が必要となる。秘密分散を利用することで情報理論的なセキュリティ対策を実現することが可能となる。

HI CORP.

EdgeTech+ 横浜 2023講演

コンテナ技術活用におけるセキュリティ対策の勘所

～コンテナセキュリティ対策の必要性～

2023年11月15日

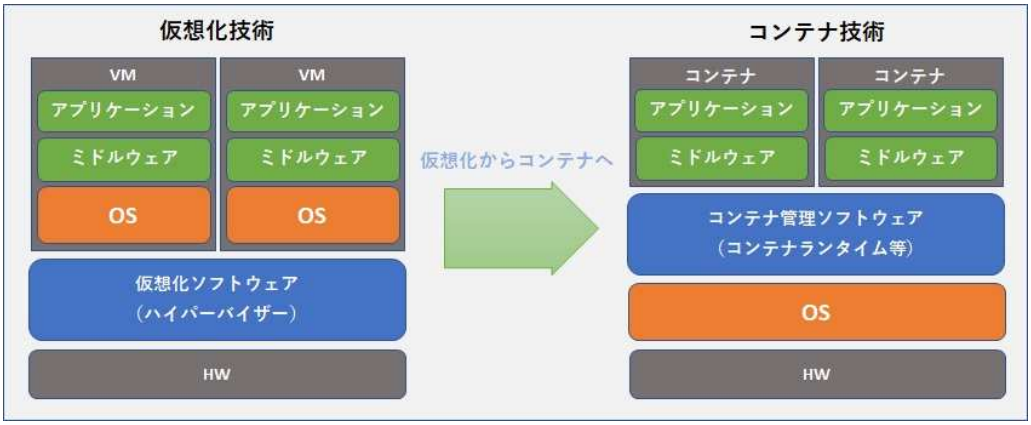
デジタル・インフォメーション・テクノロジー株式会社
ITセキュリティ事業部
飯嶋 範崇

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

1．はじめに

現在、仮想環境として、従来のVMWareをはじめとする仮想マシン（VM）の活用から、Dockerをはじめとするコンテナ技術の活用が飛躍的に拡大しています。
コンテナは、仮想マシンのようなハードウェアスタックの仮想化を行わず、OSレベルで仮想化して、複数のコンテナをホストOSのカーネル上で直接実行する事でコンテナを非常に軽量に稼働させる事が可能です。
また、コンテナはホストOSのカーネルを共有するため、仮想マシンのようにゲストOS全体を起動する場合と比較して起動が非常に速く、また使用するホストOSのリソースも仮想マシンに比べて非常に少なくてすみます。



コンテナは軽量で且つ可搬性も高く、Kubernetes等のコンテナオーケストレーションツールによって、コンテナ化されたアプリケーションの展開、スケーリング、冗長化、および管理を自動化する事ができるようになるためコンテナ環境の活用がサーバ環境のみならず、組込み機器においても活用の検討が進んでいます。

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

© Japan Embedded Systems Technology Association 2023

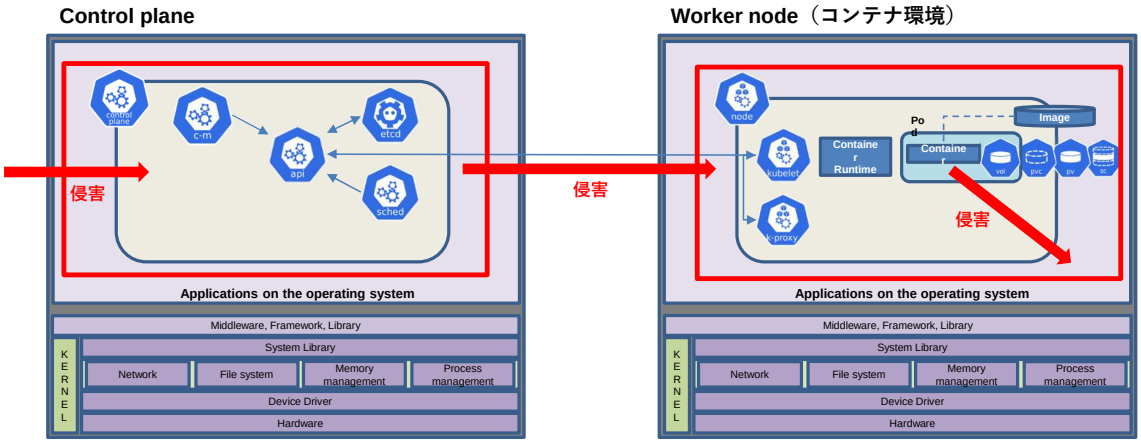
コンテナ環境における
一般的なセキュリティ対策のポイント

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

1．コンテナ環境における一般的なセキュリティ対策のポイント

Kubernetes等の使用におけるコンテナ環境におけるセキュリティ対策の例



コンテナ環境におけるセキュリティ対策としては、コンテナイメージに対するイメージスキャン（脆弱性やマルウェア混入の検知）や、コンテナのモニタリング（コンテナのログ監視、コンテナの発行するシステムコールの監視や抑止）が中心で、オープンソースの物から有償の物まで様々な対策ソリューションが存在します。

確かに重要なセキュリティ対策のポイントではあるものの、あくまでもコンテナを中心に見据えた対策であり、この観点からのセキュリティ対策では不十分であると弊社では考えています。（組込み機器においては、もっと重きを置くべき対策ポイントがあるのでは？）

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

© Japan Embedded Systems Technology Association 2023

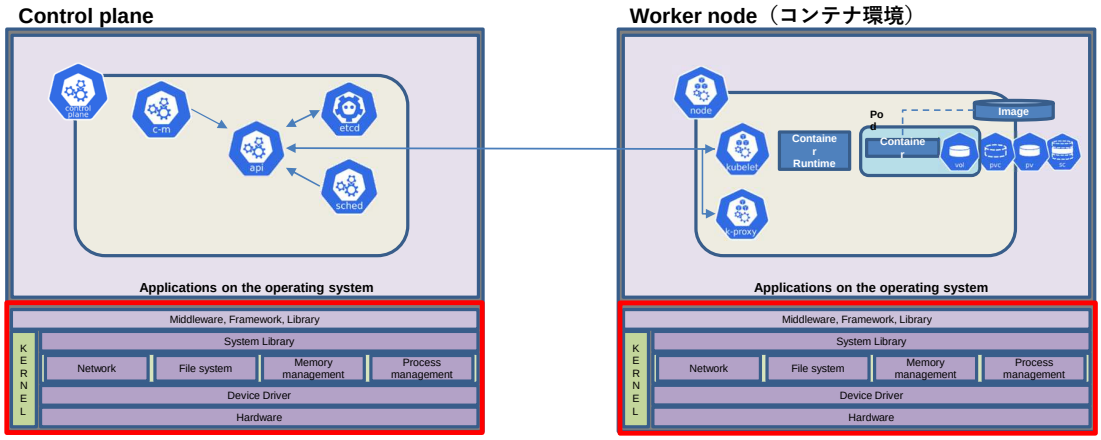
コンテナ環境における
セキュリティ対策の重点ポイント

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

2．コンテナ環境におけるセキュリティ対策の重点ポイント

Kubernetes等の使用におけるコンテナ環境におけるセキュリティ対策の例



コンテナの稼働環境は、通常のLinux（OS上）のアプリケーション層で動作し（特にカーネルを共有して動作している事を意識する必要あり）機能提供されている事を認識しておく必要があり、外部・内部からのサイバー攻撃などに対して正常な状態で稼働し続けるようセキュリティ対策を行う必要があります。

特に組込み機器の場合、OS本体のセキュリティ対策がSELinuxやAppArmorしかなく、使用できるリソースも限られるため、プラットフォームとして必要最低限の機能を搭載し、且つ、Kernelやライブラリを含めたバージョン管理、及び脆弱性管理を定期的に行い、迅速にOTA等によるシステムの更新が行えるようにしておく事が最も重要です。

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

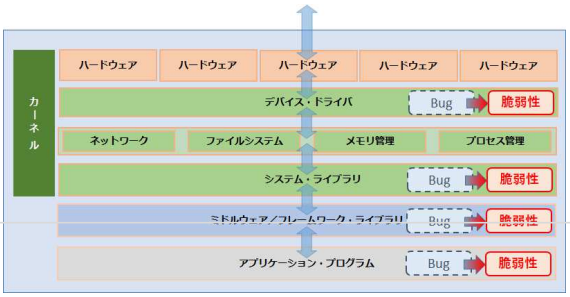
一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

© Japan Embedded Systems Technology Association 2023

3．セキュリティ対策の重点ポイントの背景

★プラットフォームとしてバグのないシステムを提供する事が不可能である事を前提に考える必要がある

→ バグは様々なレイヤに存在し、バグがいつ脆弱性に変わるかは予測できない
→ バグ修正（パッチ）とシステム改善（機能拡張／改修等）は常に行われる
→ システム改善（機能拡張／改修等）を行う事により新たなバグが発生する

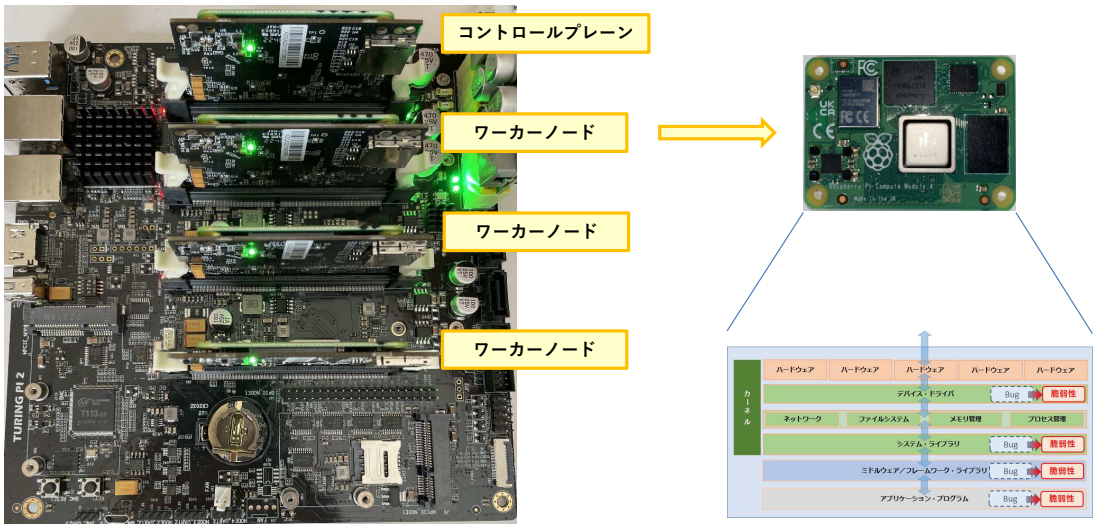


コンテナホスト、コンテナホスト内のコンテナに関わらずシステム内部構造は左図と同じ構造で、システム内部の状態は常に変化するものとして対策を考える必要がある

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

4．セキュリティ対策の重点ポイントの背景



デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

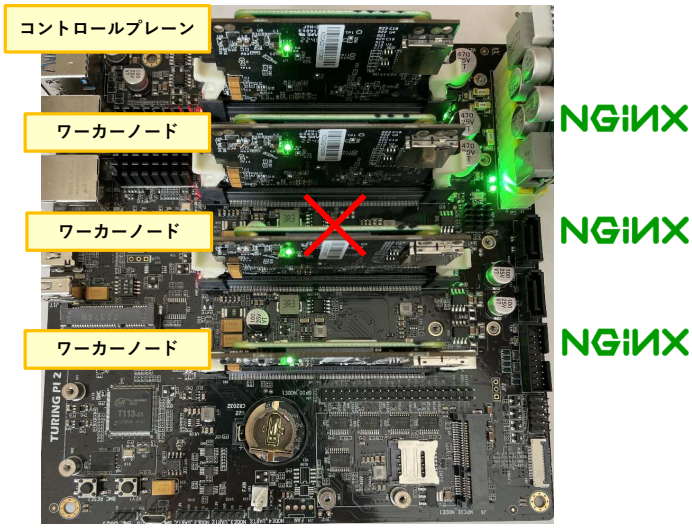
一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

© Japan Embedded Systems Technology Association 2023

コンテナ環境における
セキュリティ対策の盲点

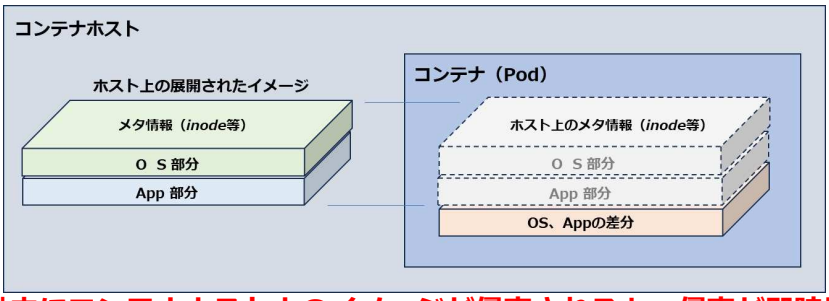
5．コンテナ環境におけるセキュリティ対策の盲点

コンテナ環境においてクラスター構成を組んでいると、ワーカーノードの一つがダウンしても、他のワーカーノードが即時に立ち上がり、機能提供を継続する事ができる。

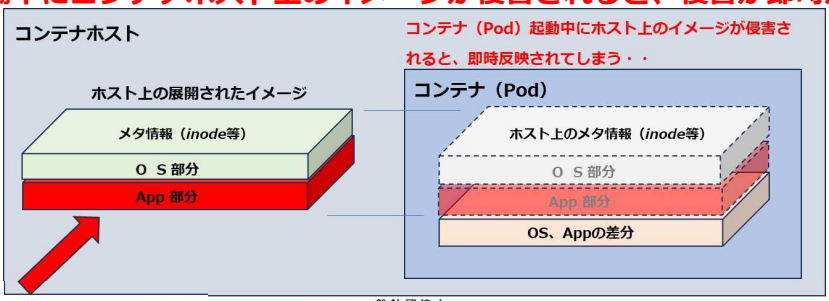


5．コンテナ環境におけるセキュリティ対策の盲点

下図のようにコンテナホスト上に展開されたコンテナイメージを使用する事で、コンテナは迅速に起動する事ができる。



ただし、コンテナ稼働中にコンテナホスト上のイメージが侵害されると、侵害が即時反映されてしまう。

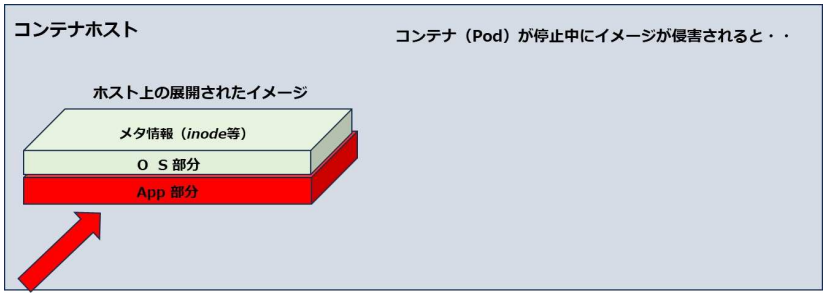


デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

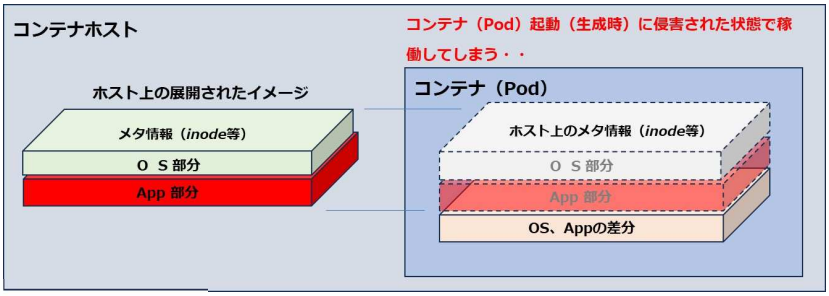
一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

5．コンテナ環境におけるセキュリティ対策の盲点

コンテナ停止中にコンテナホスト上のイメージが侵害されると…



コンテナ起動時に侵害された状態で稼働してしまう。



デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

© Japan Embedded Systems Technology Association 2023

6．コンテナ環境におけるセキュリティ対策まとめ

1．コンテナ稼働中にコンテナホスト上のイメージが侵害されると、侵害が即時反映されてしまう。
2．コンテナ稼働中にコンテナホスト上のイメージが削除されると、コンテナは即時停止してしまう。
3．コンテナ停止中にコンテナホスト上のイメージが侵害されると、コンテナ起動時に侵害された状態で稼働してしまう。
4．コンテナ停止中にコンテナホスト上のイメージが削除されると、コンテナは起動する事ができない。

求められる対策

1．コンテナ稼働中におけるコンテナホスト上のイメージ侵害（変更・削除）に対するリアルタイムな保護。
→　稼働中のコンテナはコンテナホスト上のイメージの物理アドレスを参照し稼働している・・

2．コンテナ停止中におけるコンテナホスト上のイメージ侵害（変更・削除）に対する検知・復旧による保護。
（残念ながらコンテナ側からコンテナホスト上のイメージの侵害（変更・削除）は検知も対応もする事ができない・・）

JASAの展示ブースにて、侵害（変更・削除）に対するコンテナ稼働中におけるイメージのリアルタイム保護、及びコンテナ停止中のイメージの検知・復旧の弊社製品のプロトタイプを展示＆デモしております。

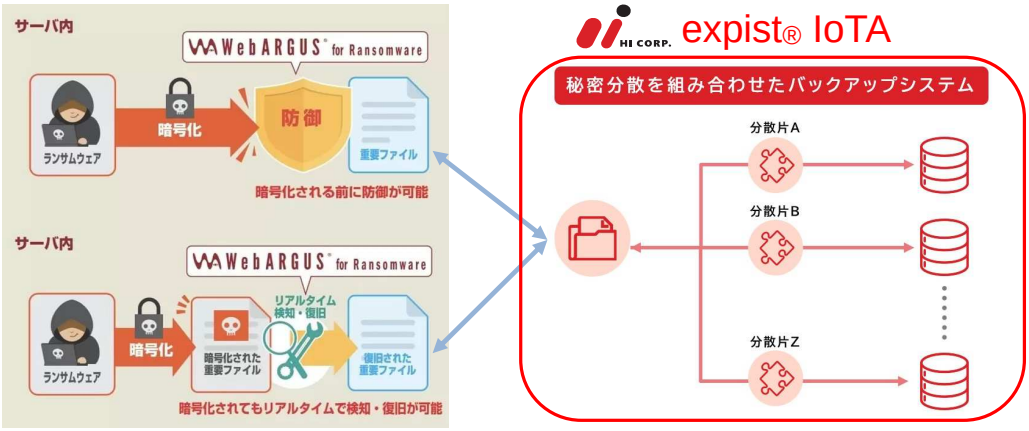
ぜひお立ち寄りください！！

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

ご参考（サーバサイドセキュリティのランサムウェア対策）

弊社では、2022年11月15日に、現在も被害が継続しているRansomwareから重要データを保護するセキュリティソリューション「**WebARGUS for Ransomware**」をリリース致しました。別途バックアップを安全に保持したいとのニーズに関しては、株式会社エイチアイの所有する**expist IoTA**の秘密分散技術を活用する事でに、磁気テープ等ではなく、**オンラインストレージ等にセキュア且つ安全にバックアップを保存する事が可能**となります。



JASAの展示ブースにて、株式会社エイチアイのexpist IoTAの製品説明等を行っておりますので、ぜひお立ち寄りください！！

デジタル・インフォメーション・テクノロジー株式会社
Digital Information Technologies Corporation

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

「コンテナ技術活用におけるセキュリティ対策の勘所」

2023/11/15 発行

発行者　一般社団法人 組込みシステム技術協会
東京都 中央区 入船 1-5-11 弘報ビル5階
TEL: 03(6372)0211 FAX: 03(6372)0212
URL: https://www.jasa.or.jp/