各　　位

2023 年 3 月 30 日
株式会社インプレス

米 O'Reilly Media 刊行『Container Security』の日本語版を 4 月 12 日に発売！

インプレスグループでIT関連メディア事業を展開する株式会社インプレス（本社：東京都千代田区、代表取締役社長：小川 亨）は、米O'Reilly Media刊行『Container Security: Fundamental Technology Concepts That Protect Containerized Applications』の日本語版、『コンテナセキュリティ　コンテナ化されたアプリケーションを保護する要素技術』を、2023年4月12日（水）に発売します。

■スペシャリストが執筆したコンテナセキュリティ要素技術の解説書！

スケーラビリティと復元力を促進するために、現在多くの組織がコンテナとオーケストレーションを使用してクラウドネイティブ環境でアプリケーションを実行しています。しかし、そのデプロイの安全性については、どのように判断すれば良いのでしょうか。本書は、開発者、運用者、セキュリティ専門家がセキュリティリスクを評価し、適切なソリューションを決定するために、コンテナの主要な要素技術を検証する実践的な書籍です。

著者のLiz Rice（Isovalent社 Chief Open Source Officer）は、コンテナベースのシステムでよく使われるビルディングブロックが Linuxでどのように構築されているかに着目しています。コンテナをデプロイする際に何が起きているかを理解し、デプロイされたアプリケーションに影響を与える可能性のある潜在的なセキュリティリスクを評価する方法を学ぶことができます。コンテナアプリケーションをkubectlやdockerで実行し、psやgrepなどのLinuxコマンドラインツールを使用していれば、すぐにでも始めることができます。

■本書の主な内容

○コンテナへの攻撃経路について知る

○コンテナを支えるLinuxの構造について知る

○コンテナの堅牢化のための方法を検討

○設定ミスによるコンテナへの侵害の危険性を理解する

○コンテナイメージビルドのベストプラクティスを学ぶ

○既知のソフトウェア脆弱性を持つコンテナイメージを特定する

○コンテナ間のセキュアな接続を活用する

○セキュリティツールを使用して、デプロイされたアプリケーションに対する攻撃を防止する

■本書の特徴

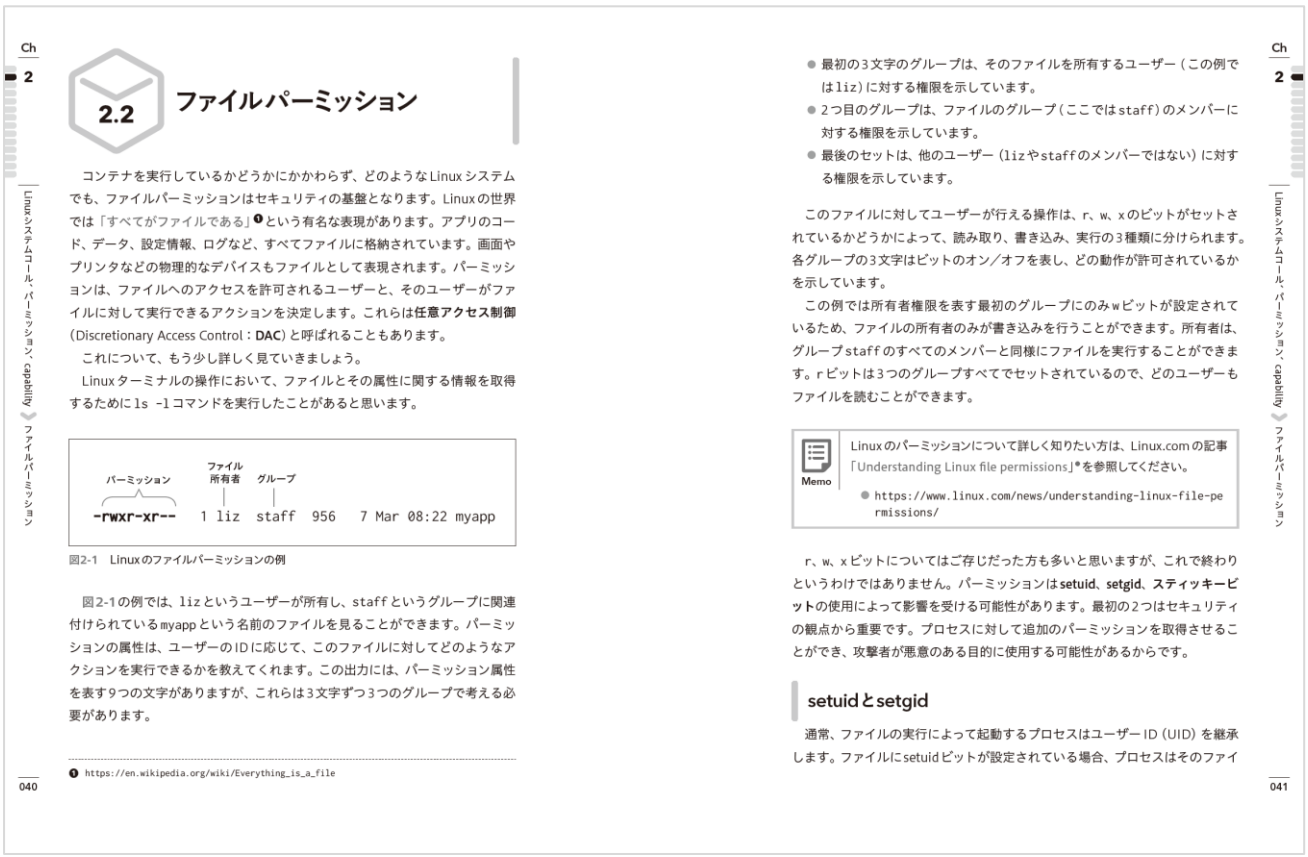
○コンテナセキュリティのスペシャリストが執筆した解説書
○コンテナのセキュリティの要素技術を学ぶことができる
○コンテナの仕組みと脆弱性（開発・運用時に注意すべき箇所）、その対策方法がわかる

■対象読者

○コンテナのセキュリティの要素技術に興味がある人
○コンテナ化を行う開発者・運用者

ほか

■紙面イメージ



Ch 2 Linuxシステムコール、パーミッション、capability ファイルパーミッション

2.2 ファイルパーミッション

コンテナを実行しているかどうかにかかわらず、どのようなLinuxシステムでも、ファイルパーミッションはセキュリティの基盤となります。Linuxの世界では「すべてがファイルである」❶という有名な表現があります。アプリのコード、データ、設定情報、ログなど、すべてファイルに格納されています。画面やプリンタなどの物理的なデバイスもファイルとして表現されます。パーミッションは、ファイルへのアクセスを許可されるユーザーと、そのユーザーがファイルに対して実行できるアクションを決定します。これらは**任意アクセス制御**（Discretionary Access Control：**DAC**）と呼ばれることもあります。

これについて、もう少し詳しく見ていきましょう。

Linuxターミナルの操作において、ファイルとその属性に関する情報を取得するためにls -lコマンドを実行したことがあると思います。

```
                ファイル
パーミッション   所有者  グループ
-rwxr-xr--   1 liz  staff  956  7 Mar 08:22 myapp
```

図2-1　Linuxのファイルパーミッションの例

図2-1の例では、lizというユーザーが所有し、staffというグループに関連付けられているmyappという名前のファイルを見ることができます。パーミッションの属性は、ユーザーのIDに応じて、このファイルに対してどのようなアクションを実行できるかを教えてくれます。この出力には、パーミッション属性を表す9つの文字がありますが、これらは3文字ずつ3つのグループで考える必要があります。

❶ https://en.wikipedia.org/wiki/Everything_is_a_file

040

- 最初の3文字のグループは、そのファイルを所有するユーザー（この例ではliz）に対する権限を示しています。
- 2つ目のグループは、ファイルのグループ（ここではstaff）のメンバーに対する権限を示しています。
- 最後のセットは、他のユーザー（lizやstaffのメンバーではない）に対する権限を示しています。

このファイルに対してユーザーが行える操作は、r、w、xのビットがセットされているかどうかによって、読み取り、書き込み、実行の3種類に分けられます。各グループの3文字はビットのオン／オフを表し、どの動作が許可されているかを示しています。

この例では所有者権限を表す最初のグループにのみwビットが設定されているため、ファイルの所有者のみが書き込みを行うことができます。所有者は、グループstaffのすべてのメンバーと同様にファイルを実行することができます。rビットは3つのグループすべてでセットされているので、どのユーザーもファイルを読むことができます。

Memo
Linuxのパーミッションについて詳しく知りたい方は、Linux.comの記事「Understanding Linux file permissions」*を参照してください。
- https://www.linux.com/news/understanding-linux-file-permissions/

r、w、xビットについてはご存じだった方も多いと思いますが、これで終わりというわけではありません。パーミッションは**setuid**、**setgid**、**スティッキービット**の使用によって影響を受ける可能性があります。最初の2つはセキュリティの観点から重要です。プロセスに対して追加のパーミッションを取得させることができ、攻撃者が悪意のある目的に使用する可能性があるからです。

setuidとsetgid

通常、ファイルの実行によって起動するプロセスはユーザーID（UID）を継承します。ファイルにsetuidビットが設定されている場合、プロセスはそのファイ

041

コンテナの主要な要素技術を検証する実践的な書籍です

■監訳者のことば（抜粋）

本書はコンテナセキュリティについて有効な設定を紹介するだけの書籍ではありません。コンテナを構成するLinuxの要素技術から解説し、コンテナの仕組みを把握したうえで、根拠に基づいたセキュリティ強化を行えるよう理解を促します。後半では、Kubernetes のセキュリティを取り扱います。こちらもLinuxのセキュリティ機能やコンテナランタイムといった、低レイヤーの機能を紹介するだけでなく、正しく利用しなかった場合のセキュリティリスクについても解説しています。

本書で紹介する技術は、コンテナを利用するときに必ずしも必要なものではありません。Docker、Kubernetesの公式ドキュメントやベストプラクティスに従うだけでも、十分なセキュリティレベルを担保できる場合もあります。

コンテナを構成する要素技術や分離の仕組み、Kubernetesの技術的詳細を理解することは蛇足のように感じるかもしれません。しかし、たとえば新規に発表されたコンテナ脆弱性について攻撃手法を調査したり、Kubernetes環境におけるリスク分析を行ったりする場面で、これらの知識は不可欠なものです。また、開発段階からコンテナのセキュリティを意識し、各機能の有効性を考慮した最適なセキュリティ設定を行うことができるようになります。

コンテナの仕組みや、Linuxの要素技術についての理解を深めていくと、Dockerや各コンテナランタイムを使用せずとも、コンテナのような分離プロセスを容易に起動できることがわかります。プロセス分離の理解が深まれば、攻撃者が利用するコンテナエスケープの方法が複数存在することに気がつくでしょう。コンテナに対する攻撃手法をあらかじめ知っておくことで、コンテナの安全な運用について、開発のより早い段階から意識できるようになります。コンテナの低レイヤー領域に興味のある方は、手を動かしながら楽しく学習できると思います。

本書を通して、皆さんがコンテナの仕組みに関心を持ち、コンテナのセキュリティ強化について考える機会となれば幸いです。安全なコンテナ環境の実現を目指し、共に取り組んでいきましょう。

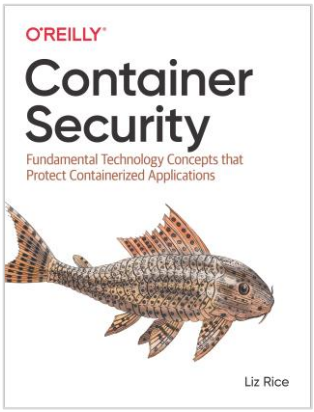
■本書の構成

■書誌情報

書名：コンテナセキュリティ　コンテナ化されたアプリケーションを保護する要素技術
著者：Liz Rice　著
監修：株式会社スリーシェイク
訳：水元 恭平、生賀 一輝、戸澤 涼、元内 柊也
発売日：2023年4月12日（水）
ページ数：280ページ
サイズ：A5判
定価：3,520円（本体3,200円＋税10%）
電子版価格：3,520円（本体3,200円＋税10%）※インプレス直販価格
ISBN：978-4-295-01640-3

◇Amazonの書籍情報ページ　：　https://www.amazon.co.jp/dp/4295016403
◇インプレスの書籍情報ページ　：　https://book.impress.co.jp/books/1122101051

■原書情報



Container Security

by Liz Rice

Released April 2020

Publisher(s): O'Reilly Media, Inc.

ISBN: 9781492056706

https://www.oreilly.com/library/view/container-security/9781492056690/

■著者・監修・訳者プロフィール

■著者

●Liz Rice（リズ・ライス）
コンテナセキュリティを専門とするAqua Security社で、VP of Open Source EngineeringとしてTrivy、Tracee、kubehunter、kube-benchなどのプロジェクトを統括。CNCFのTechnical Oversight Committeeであり、コペンハーゲン、上海、シアトルで開催されたKubeCon＋CloudNativeCon 2018では共同議長を務めた。ネットワークプロトコルや分散システム、VOD、音楽、VoIPなどのデジタル技術分野での仕事において、ソフトウェア開発、チーム、プロダクトマネジメントの豊富な経験を持つ。コードに触れていないときは、生まれ故郷のロンドンよりも天気の良い場所で自転車に乗ったり、Zwiftでのバーチャルレースに参加したりしている。

■監修

●株式会社スリーシェイク（3-shake Inc.）　https://3-shake.com/
SREコンサルティング事業「Sreake（スリーク）」を中心に、AWS/Google Cloud/Kubernetesに精通したプロフェッショナル集団が技術戦略から設計・開発・運用まで一貫してサポートするテックカンパニー。

■訳

●水元 恭平（みずもと きょうへい）

Windows環境でのアプリケーション開発を経験後、株式会社スリーシェイクでSRE/CSIRTとして技術支援を行っている。専門分野はコンテナ・クラウドセキュリティとKubernetes。CloudNative Days Tokyo 2021実行委員。

●生賀 一輝（しょうか いっき）
事業会社のインフラエンジニア、株式会社ユーザベースのSREとして従事後、株式会社スリーシェイクに入社。日々、クライアントの要件に応じて多角的なSRE支援を行っている。専門分野はクラウドインフラとKubernetesエコシステム。過去にGoogle Cloud Anthos DayやKubernetesイベント等に登壇。

●戸澤 涼（とざわ りょう）
株式会社スリーシェイクに新卒入社。現在3年目。AWS/Google Cloud領域でKubernetesを活用したいお客様に対して、SREとして技術支援を行っている。クラウドネイティブやKubernetesをテーマに社内外での登壇経験あり。

●元内 柊也（もとうち しゅうや）
インフラエンジニアとしてホスティングサービスの開発、運用を経て、現在は株式会社スリーシェイクにてソフトウェアエンジニアとして勤務。Webシステムの歴史、運用、開発について興味があり、SREのような信頼性の観点からのプラクティスや運用技術をプロダクトに落とし込めるように日夜開発を行っている。

以上

【株式会社インプレス】 https://www.impress.co.jp/
シリーズ累計 7,500 万部突破のパソコン解説書「できる」シリーズ、「デジタルカメラマガジン」等の定期雑誌、IT 関連の専門メディアとして国内最大級のアクセスを誇るデジタル総合ニュースサービス「Impress Watch シリーズ」等のコンシューマ向けメディア、「IT Leaders」、「DIGITAL X」、「Web 担当者 Forum」等の企業向け IT 関連メディアブランドを総合的に展開、運営する事業会社です。IT 関連出版メディア事業、およびデジタルメディア＆サービス事業を幅広く展開しています。

【インプレスグループ】 https://www.impressholdings.com/
株式会社インプレスホールディングス（本社：東京都千代田区、代表取締役：松本大輔、証券コード：東証スタンダード市場 9479）を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「航空・鉄道」「モバイルサービス」「学術・理工学」を主要テーマに専門性の高いメディア&サービスおよびソリューション事業を展開しています。さらに、コンテンツビジネスのプラットフォーム開発・運営も手がけています。

【本件に関するお問合せ先】
株式会社インプレス　広報担当：丸山
E-mail: pr-info@impress.co.jp URL： https://www.impress.co.jp/
※弊社はテレワーク推奨中のため電話でのお問合わせを停止しております。メールまたは Web サイトからお問合わせください。