

プロダクトのセキュアな長期運用を支援する 「EMLinux」のご紹介



- 家電/車のような身近なものから、工場/プラント等で使用される産業制御システムにいたるまで、幅広い機器がサイバー攻撃の脅威にさらされている

脆弱性の事例 IoT推進コンソーシアム、総務省、経済産業省「IoTセキュリティガイドライン ver 1.0」より引用

カテゴリ	サブカテゴリ	発表年・会議	概要
自動車関連サービス	・コネクテッドカー ・サブシステム	2015年 Black Hat USA	インターネットから自動車の遠隔操作を可能とする脆弱性を紹介。自動車のマルチメディアシステムのコントローラへインターネット経由で接続し、別のコントローラのファームウェアを書き換え、CAN ^(*) パス上で不正なコマンドを送信することで、自動車のハンドルやエンジン等の遠隔操作に成功。
消費者向けサービス	・ホームエネルギー マネジメント (HEMS)	2014年 Black Hat USA	セキュアでないホームオートメーション開発の危険性の一例を紹介。ホテルの部屋にある機器・設備の通信に利用されているKNX ^(*) net/IPプロトコルをキャプチャ・解析し、機器・設備を不正に遠隔操作することが可能。
産業別のサービス	・医療	2012年 Breakpoint Security Conference	ペースメーカー及び植込み型除細動器へのハッキングのデモを紹介。植込み型除細動器のワイヤレストランスミッタの脆弱性を利用し、近距離から植込み型除細動器に不正な動作を行わせることに成功。

ソフトウェアのセキュリティメンテナンスの必要性

- 各国での法制化、各業界での標準規格/ガイドライン化の例
 - 日本: ルーター等へのソフトウェア更新機能の搭載必須化（平成31年総務省令第12号）
 - 自動車: UNECE WP29 GRVAソフトウェアアップデート法規基準
 - 医療機器: IMDRF 医療機器サイバーセキュリティの原則及び実践に関するガイダンス
 - 産業制御システム: ISA/IEC 62443-4 制御システムセキュリティ標準（コンポーネント）

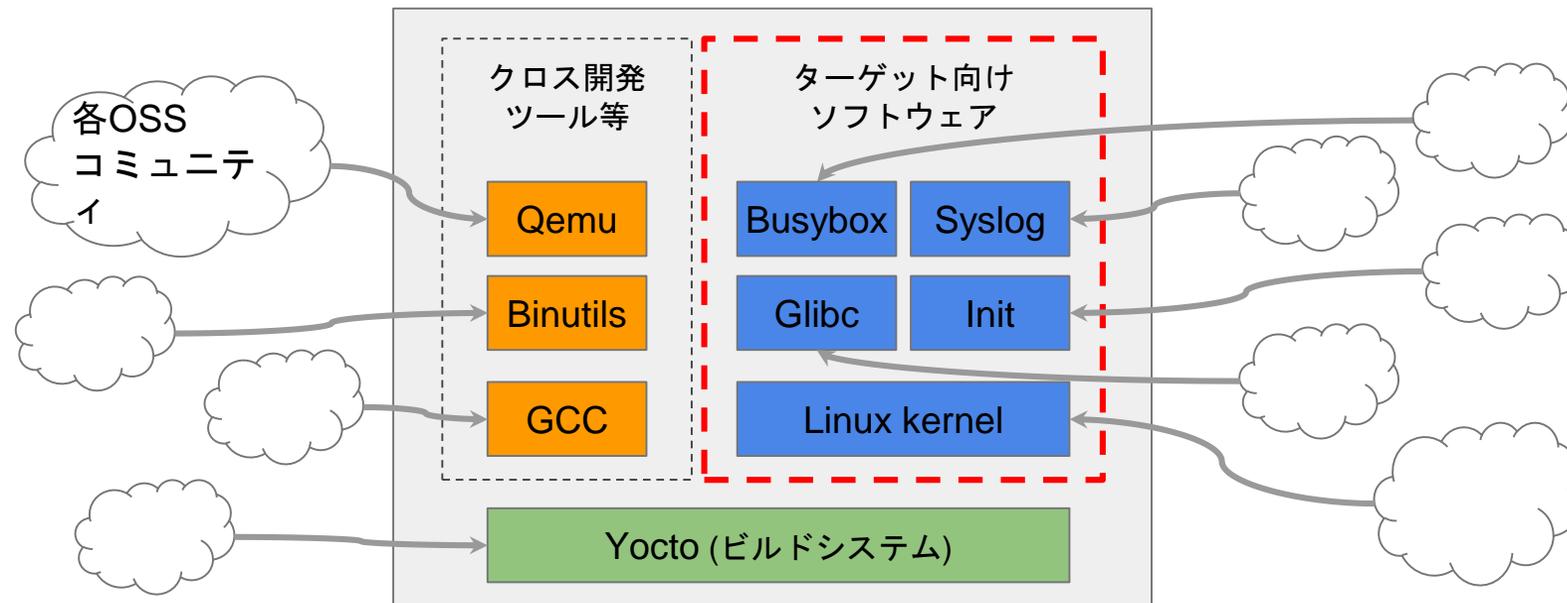
- **製品出荷後も継続的にセキュリティメンテナンスを行うプロセスを確立する必要がある、OSの脆弱性対応も不可欠となっている**

- セキュリティ（脆弱性）の問題はその他のバグと同様に修正される
- しかし、カーネルのセキュリティ修正は必ずしもCVEに紐付いているとは限らない
 - 一部の問題にしかCVEは割当てられない
 - 近年のLinuxカーネルに割当てられるCVEは年間150~350件
 - 実際にはそれ以上の数のセキュリティ修正がコミュニティで行われている
 - CVEをデータベースで見つけた時にはすでに修正済みのケースも多い
 - 平均修正日数は「マイナス」100日
- つまり、CVEだけをチェックして対応するのでは不十分、かつ、遅い
- Linuxをセキュアに保つには、UpstreamやLTSで行われるバグ修正を「すべて」「タイムリーに」取り込む必要がある

参考: Greg Kroah-Hartman [“CVEs are dead, long live the CVE!”](#)

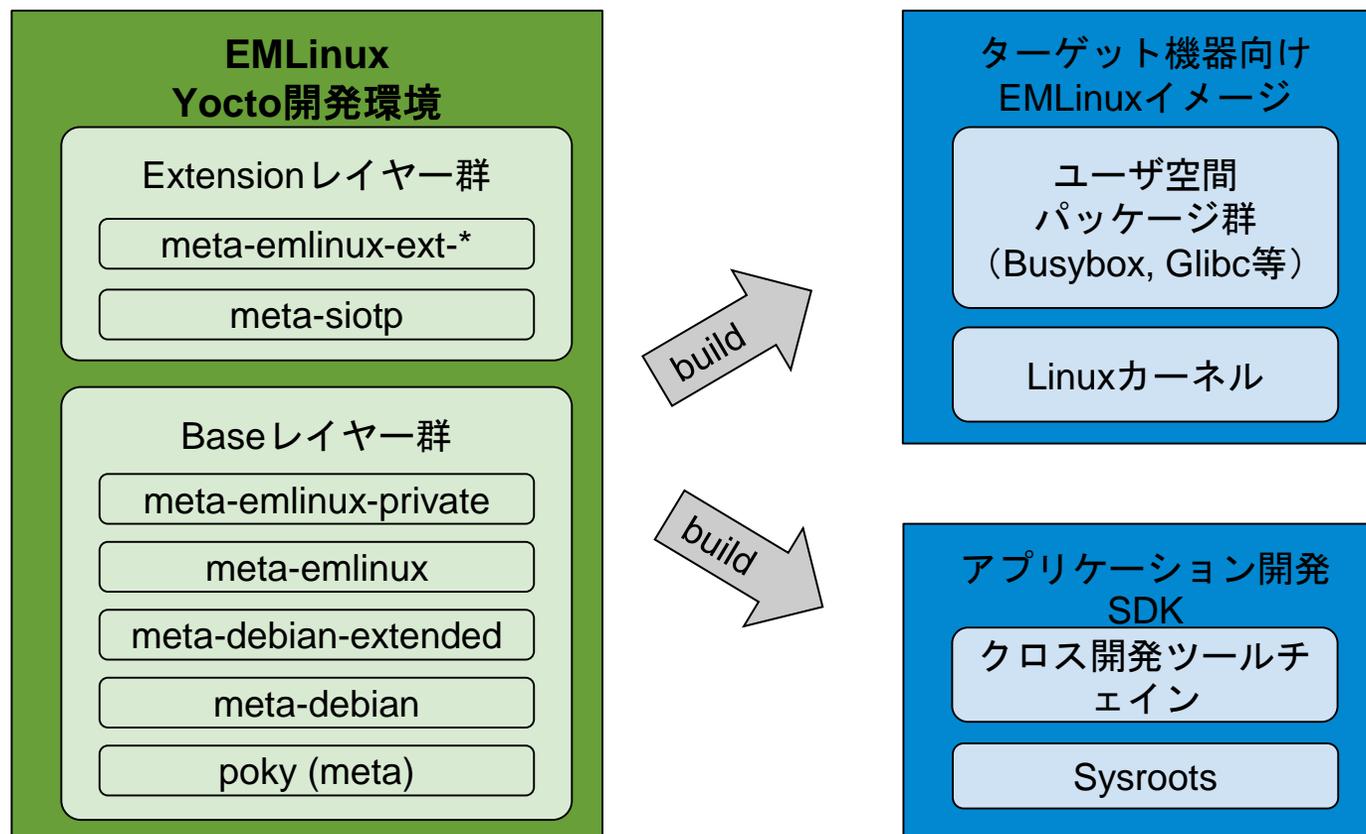
組み込みLinux全体のメンテナンス

- 組み込みLinuxはカーネル以外にも様々なOSSで構成されている
- LTSモデルを選択する場合は、個々の要素がどれだけサポートされるかを把握する必要がある
 - Yoctoは最長2年のLTSを提供。個々のソフトウェアも2年以内にメンテナンスが終了する
 - SoCベンダーのYocto BSPの場合は、多くの場合1年程度。また、メンテナンス頻度や内容もBSPによって様々。



- Yoctoビルドシステムを採用した組込み/IoT機器向けLinux環境
- LTSモデルに基づく10年間の計画された超長期サポートを提供
- 1ヶ月周期でメンテナンスアップデートを提供
- 産業用途のSoCとその評価ボードに標準で対応

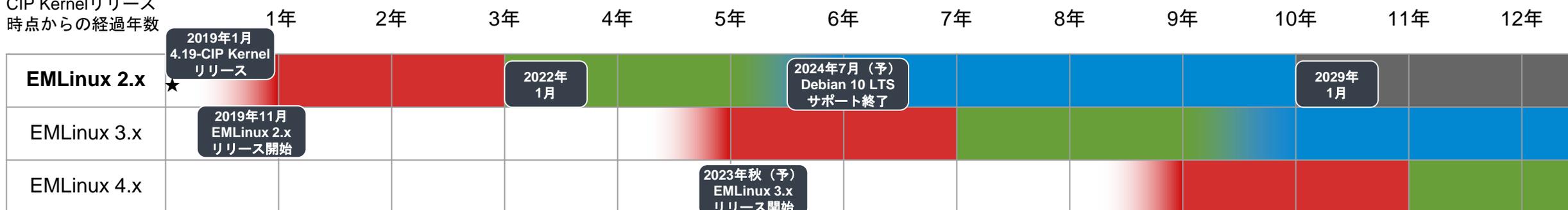
- Yoctoビルドシステムを採用した組込み/IoT機器向けLinux環境
 - 組込みLinux開発のデファクトスタンダードであるYoctoの知識やノウハウをそのまま活用可能



EMLinuxの特徴 (2)

- LTSモデルに基づく10年間の計画された超長期サポートを提供
 - CIP(※)およびDebianコミュニティで長期メンテナンスされるLinux関連ソフトウェアを活用 (※ [Civil Infrastructure Platform](#): Linux Foundationの社会インフラOSSプロジェクト)
 - CIP S-LTS(Super Long-Term Stable)カーネル、CIP Core Packages、Debian Source Packages
 - サイバートラストはCIPのメンバー企業として活動
 - Kernel TeamのChairとして活動。その他リファレンス構成の開発や品質向上においても貢献。
 - CIPはLinuxカーネルやDebianなど様々なOSSに貢献

CIP Kernelリリース
時点からの経過年数



初期phase
中期phase

- CIP/Debianコミュニティの修正をすべて取り込む
- 不足部分はサイバートラストが独自に対応

後期phase

- CIPコミュニティの修正(カーネル、コアパッケージ)をすべて取り込む
- 不足部分はサイバートラストが独自に対応

- 1ヶ月周期^[*]でメンテナンスアップデートを提供 ^[*] 初期/中期phase
 - コミュニティでのメンテナンスを全て取り込む形でセキュリティ修正の製品適用までのリードタイムを短縮
 - Yocto core-image-minimal / -weston の範囲について検証済みのアップデート
 - メンテナンスの共通化により、高額になりがちな完全個別メンテナンスに比べてコストダウン可能
 - カスタマイズ部分やアプリケーションのメンテナンスに資源を集中できる
 - Secure IoT PlatformによるOTAに標準対応済み
 - 出荷済みのIoTデバイスにアップデートをデプロイ可能

EMLinuxの特徴（4）

- 産業用途のSoCとその評価ボードに標準で対応
 - Extensionレイヤーとして用意しており、すぐに評価可能
 - 毎月のメンテナンスアップデートで動作検証をして提供
 - 製品固有のカスタマイズ部分の開発に注力可能
 - 他のSoCやカスタムボードも個別にサポート可能

標準対応SoC	対応ボード
Renesas RZ/G2E	Silicon Linux RZ/G2E evaluation kit
Xilinx MPSoC	ZynqMP ZCU102
NXP QorIQ LS1043A	QorIQ LS1043A-RDB
NXP QorIQ LS1046A	QorIQ LS1046A-RDB
TI Sitara AM335x (予定)	AM335x Starter Kit

- 豊富な実績のあるエンジニアリングサービスを提供
 - カスタムボード対応、デバイスドライバ開発
 - 実機テスト自動化、自動テスト環境の構築・運用
 - セキュア・コンフィギュレーション対応
 - 起動高速化、フットプリント削減
 - 最終製品のOSSライセンスのコンプライアンス対応相談
 - HMI向け多言語入力・表示対応
 - etc.

- 無償で利用可能なOSS版をGithubで公開中
 - <https://github.com/miraclelinux/meta-emlinux>
- 対応ハードウェア
 - Raspberry Pi 3
 - BeagleBone Black
 - Qemu (マシンエミュレータ): aarch32, aarch64
- As-Isでの提供＝通常のOSSと同じ
 - 製品版に付随する各種サポート／ドキュメント／脆弱性情報等の提供はありません。製品版をご希望の方はサイバートラストまでお問い合わせください。

お問い合わせはこちら



サイバートラスト株式会社
IoT 総合お問い合わせ窓口
iot-contact@cybertrust.co.jp



信頼とともに

ソフトバンク・テクノロジー グループ

