組込みLinux に“プラス”して
長期間の製品ライフサイクルをサポート

cybertrust

EM+PLS

EMbedded + Product Lifecycle Service

- **産業機器向けのLinux**と、脆弱性対応のパッチを**長期間提供**
- IoT機器の認証情報を管理し、**なりすまし防止**や**安全なリモート更新**を実現
- 脆弱性検査ツールで製品の**脆弱性リスク**を**定期的にチェック**

ライフサイクル	Linuxの長期利用		なりすまし改ざんのリスク	脆弱性のリスク
開発	産業向けLinux OSの提供 ・IoTで必要なネットワークやGUIなどのソフトウェアパッケージ ・OSSコミュニティと連動し制約の無いオープンな開発を実現	+	IoT機器の本物性を担保する仕組みを提供 製品のなりすましを防ぐため機器内部に信頼の基点(Root of Trust)を実装	開発中の意図しない脆弱性リスクを検査 テスト用バックドアの混入や不適切なOS設定による脆弱性を出荷前に検知
運用	OSの脆弱性に対してパッチを10年間提供		IoT機器認証の為の電子証明書の配付と管理の機能	定期的な脆弱性検査で出荷後のリスクを検知
	カーネルエンジニアによる技術サポート		更新ファイルの改ざんを防ぐ安全なリモート更新(OTA)機能	重要度毎に分類された検査レポートでスマートなリスク対応

EM+PLSは「IEC62443-4-2」対応を支援

今後の対応必須？「IEC62443-4-2」

IoT化が進む産業制御システムでは、サイバー攻撃のリスクに対して国際電気標準会議（IEC）の「IEC62443-4-2」を調達要件に盛り込むケースが海外を中心に増えています。「IEC62443-4-2」に準拠するにはOSの設定や不正アクセス検知の機能だけではなく、機器認証の方法や電子証明書の安全な保管・管理システムの設計、脆弱性発見時の対応フローなどの対応も産業機器ベンダー・メーカーで行う必要があります。

「IEC62443-4-2」取得を支援

EM+PLSではIEC62443-4-2に準拠したLinux OSの設定方法や機器認証情報の安全な管理方法など開発時に必要な機能だけでなく、証明書の更新や脆弱性発生時のオペレーションまで一気通貫で提供することで産業機器ベンダー・メーカー様の認証取得を支援します。また、製品特性や業界業種によって特別な対応が必要な場合は別途、IEC62443-4-2対応コンサルティングを提供予定です。

産業機器向け Linux OS『EMLinux』

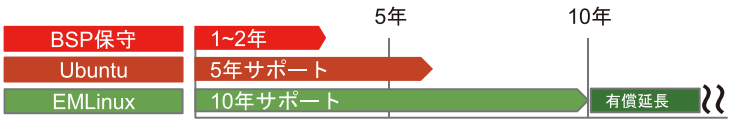
◆組込みもIoTも対応可能なLinux OS
EMLinuxは組込み機器やIoT機器に必要なネットワークやGUI用のソフトウェアパッケージが標準で揃っている為、独自開発部分に注力した開発をすぐに始めることができます。また、サイバートラストの組込みLinuxの実績を生かした高速起動、LinuxとRTOS共存などの開発支援※も可能です
※別途有償

◆10年間の長期パッチ提供
産業機器など運用期間が長い場合、一般的なLinuxではその途中で脆弱性に対するパッチ提供が終了してしまいます。EMLinuxでは脆弱性パッチを10年間提供するので、産業機器など長期間運用する製品にも採用可能。

◆EMLinuxの搭載パッケージ(一部抜粋)

Multimedia	ALSA
Network	DHCP
	iproute
	openssl
Language	Python
	Perl
GUI	Wayland/Weston
	GTK+3
Utilities	Git
	sqlite3

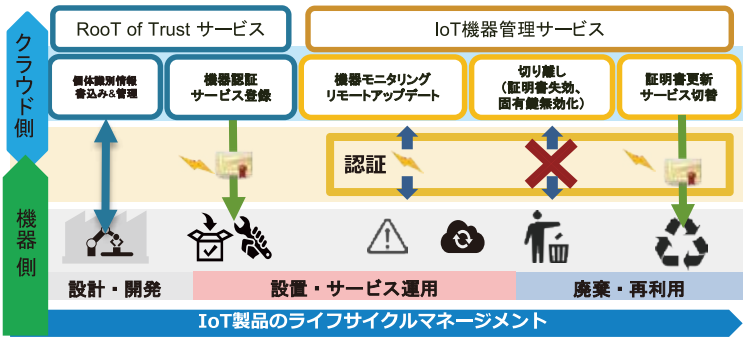
◆無償のLinux OSに比べ長期のパッチ提供期間(延長可)



IoT機器管理『セキュア IoT プラットフォーム』

◆IoT機器の個体認証
IoT機器に信頼の基点(Root of Trust)を実装することでなりすましのリスクを防ぎ、IoTサービス側からすべての機器を個体識別することができます。

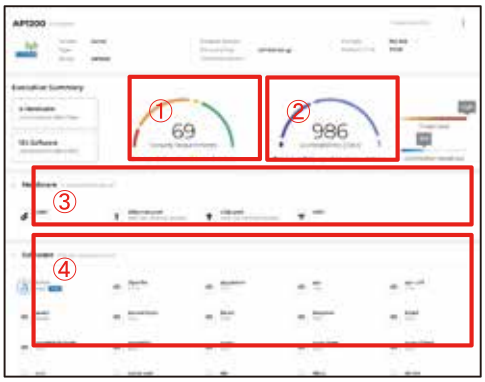
◆IoT機器の一元管理とリモートアップデート
信頼の基点により、個々のIoT機器がどのような状態か、WEB画面で一元管理することが可能。また。ファームウェアバージョンを確認して任意の機器にたいしてリモートアップデート(OTA)を実行できます。



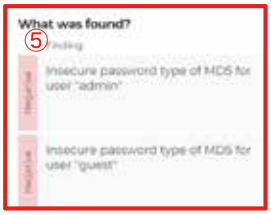
脆弱性検査ツール『VDOO Vision』

◆バイナリ状態のFWに対して脆弱性検査
製品出荷前、バイナリ状態となったFWに対して脆弱性を解析することでビルド時のミスなどで発生する意図しない脆弱性を検知します。また、提供後のイメージに対して定期的に検査を実施することで新たな脆弱性が発見されても検知が可能です。

◆対策方法まで記載されたレポートを発行
脆弱性検査の結果は、発見された脆弱性の重要度や対応方法などの情報も記載されているので、発見後の対策がスムーズに行えます。



脆弱性レポート画面
①重大な脆弱性の数
②検知された脆弱性の総数
③検査対象のHW構成
④パッケージのバージョン
⑤対策案の提示



提供メニュー

サブスクリプション メニュー

	Bronze 720万円／年	Silver 1,500万円／年	Gold 2,400万円／年
脆弱性検査ツール			脆弱性レポート
			脆弱性検査
IoT機器管理		リモートアップデート	
		IoT機器の一元管理	
		IoT機器の個体識別	
産業機器向けLinux	脆弱性パッチの長期提供		
	IoT機器向けLinux OS		

ランタイムライセンス ／オプション

	機能一覧
ランタイムライセンス	デバイス用証明書(HW / SW)
	SIOTP ユーザー証明書
	SIOTP テナント追加
オプション	IoT向けセキュリティツール『VDOO ERA』
	Linux-RTOS 共存ソリューション『EMDuo』
	商用OP-TEEサポート『EMTee』
	Linux 高速起動『Warp!!』
	技術サポート 延長 (20H)
	開発支援サービス

※サブスクリプションメニューは1プロジェクトにつき1ライセンスの購入が必要です。
プロジェクトの定義：① SoCが同一であること　② 担当者が同一であること　③ 最終製品、用途、動作するアプリケーションが同一であること

cybertrust

サイバートラスト株式会社
所在地 〒106-0032 東京都港区六本木1-9-10 アークヒルズ仙石山森タワー35階
ウェブサイト https://www.cybertrust.co.jp
お問い合わせ
info@cybertrust.co.jp
03-6234-3800

お問合せ先