セキュリティとシステム性能を両立した改ざん検知
～ 組込みLinux導入/開発支援サービス 活用 ～

Fsas Technologies

課題

- システムの改ざん検知はセキュリティ向上に有効であるが、各社SoC固有のノウハウが必要となり、導入が難しい。
- 改ざん検知は起動時間など性能とのトレードオフが発生する。この問題を解消、軽減した形で改ざん検知を実装したい。
- 改ざん検知を導入したものの、その効果の検証に関するノウハウが少ない。

効果

- 各社SoCのノウハウを保有したチームにより改ざん検知が円滑に導入できる。
- 改ざん検知の性能を分析し、オンデマンドによる実行に切り替えるなど、セキュリティ面の妥当性を維持しつつ性能のチューニングが行える。
- 有識者により改ざん検知に伴うシステム全体の動作がセキュリティ観点での妥当性を確認できる。

適用のポイント

システム性能を考慮した改ざん検知の導入支援

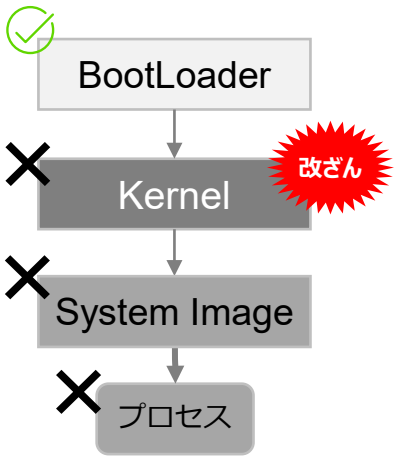
- 各社SoCのノウハウを持つチームが改ざん検知導入を支援
- 性能分析・チューニングで性能要件の達成をサポート

お客様システムの検証対象の範囲などのセキュリティについての要件や、起動時間の制約などの要件とシステムの構成についてヒアリング、分析を実施。

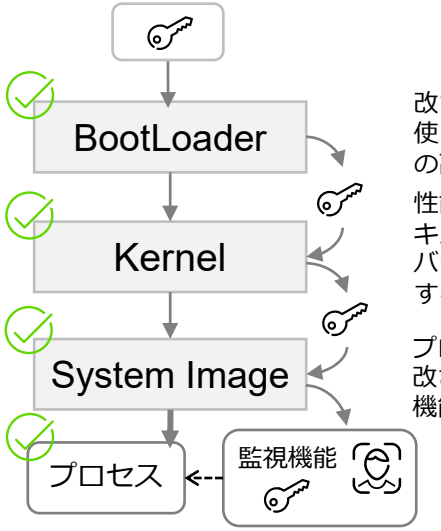
それらのデータを元に、各モジュールごとに検証タイミングと検証方法、検証機能など検討し、システム性能への影響を考慮した改ざん検知方式を提案。

改ざん検知後の動作の検討など、改ざん検知に関連する周辺機能についてもサポート。

システムのいずれかが改ざんされると、改ざんされたプロセス以降の動作が信頼できないものになる。



ハードウェアの秘匿領域にある秘密鍵を使って署名を検証し、改ざんされていないことを確認しながら起動する。



改ざん検知には鍵暗号を使うため、システム負荷の高い処理になる。

性能チューニングやセキュリティとの要件のバランスを考慮して実現する必要がある。

プロセス立ち上げ時に改ざんがないかを監視機能がチェック。

お問い合わせ

Fsas Technologies

- Linuxソリューションや、Linux製品についてのお問い合わせは、
  下記お問い合わせページよりご依頼ください。

  - Linux情報へのお問合せ
    https://www.fujitsu.com/jp/products/software/os/linux/contact/