セキュアブート –システムの安全な起動

セキュアブートとは、システムに組み込むことで、システムを構成するファイル（プログラムやデータ）に対する不正な改ざんを検知するための仕組みです。

改ざん検知は、予め対象となるファイルのハッシュ値を計算（計測）して期待値として保管しておき、システム起動（ブート）時点で計測した値が期待値と一致するか照合（検証）します。改ざん検知対象のファイルを示決めるものをチェックリストと呼び、その期待値をホワイトリストと呼びます。

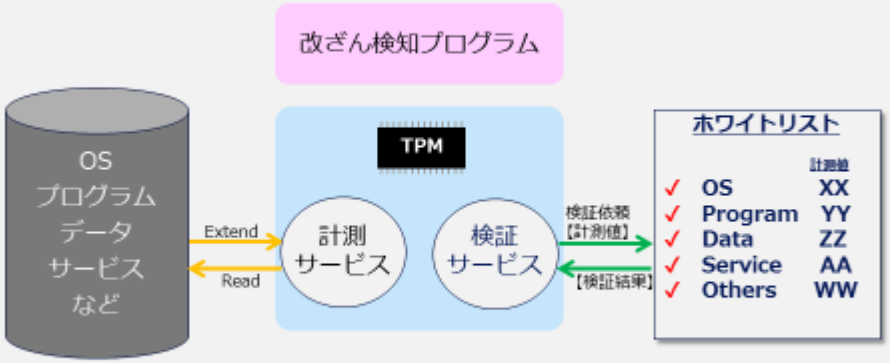
特長：

① 起動前の検証（事前検証）、起動後の検証（事後検証）に対応
② 検証部分を外部サーバーに持たせることが可能

[デモの内容]

①TPM搭載のIntel NUC(Next Unit of Computing)にWebカメラを搭載し、このWebカメラのキャプチャアプリケーションを改ざんします。
②改ざんを行ったNUCを再起動し、改ざんされたことと、そのためにキャプチャアプリケーションが停止したしたことを表示します。

セキュアブート概要



Insight セキュアブートの概要