汎用性という脆弱性への処方箋

Mitigating Vulnerability of Versatility

井上洋樹・システム分科会・情報セキュリティ大学院大学

The versatility provided by the OS etc. makes a product development more efficient, but makes attack easy and defense difficult. Since these functionalities are not always necessary for finished products, it is desirable to limit them in operation. Effectively utilizing security features of platforms can suppress the additional cost and effort to install and maintain security appliances for protecting products. Secure OS and hardware-supported security mechanisms such as TrustZone meat the requirement.

汎用性の利点と問題点

・ユーザのニーズの応じた様々な機能を実装するのが容易になる。
・一方で、アタックサーフェスが拡がる、正常／異常な動作を識別するのが困難になる、意図しない動作を引き起こされる等の問題がある。

時代背景

・データセンター等の保護下にない大量のコンピュータデバイスがネットワークに接続される。
・システム資源に乏しい場合も多い。
・一つ一つの機器を個別にセキュリティ製品で保護するのは困難。

あるべき姿

開発時には汎用性を活用し、運用時には汎用性を制限するのが望ましい。

あるべき姿

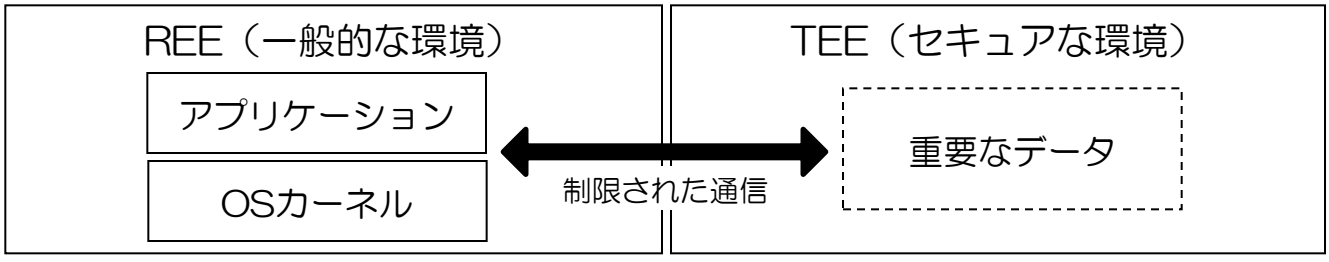
製品に元々備わっている保護機構を有効活用するのが望ましい。

セキュアOS
（e.g. TOMOYO Linux）

×

ハードウェアに備わる保護機構
（e.g. TrustZone）

汎用性を制限する手段として、セキュアOSが利用できる。
更に、ハードウェアの支援を受けたセキュリティ機構を活用した多層防御によって、セキュアOSによる保護を強化する。



ハードウェアの支援を受けたセキュリティ機構の概念図