第8章

侵入検知/ログ取得/ファイアウォール/鍵管理

セキュリティ強化②…不正アクセスの防止

小林 明

不正侵入検知システム…IDS

チューニング術㊶

不正侵入検知システム(IDS，Intrusion Detection System)は，システムやネットワークに対して外部から不正なアクセスやその兆候を検出するシステムです．IDSでは，遮断などの防御までは行いません．防御が必要な場合は，IPS(Intrusion Prevention System)を検討する必要があります．

● 検知できる内容

IDSの中でもホスト型IDS(Host-based Intrusion Detection System)は特定のホスト上でのイベント(ファイルやディレクトリの追加，変更，削除，アクセス権の変更など)を検知します．オープンソース・ソフトウェアでも幾つかホスト型IDSの取り組みがあります．各ツール単体で実現できる機能に絞って比較した結果を**表1**に示します．また，各ツールで検知可能な内容を**表2**に示します．

● Yocto Projectでの対応状況は要確認

ラズベリー・パイのYocto Project環境には，meta-securityレイヤにAIDE，OSSEC，Samhain，Tripwireがあり，容易に導入できます．

なお，筆者はTripwireしかビルド確認をしていま

表1　オープンソースの不正侵入検知ツールの機能比較

項　目	チェック対象ファイルの選択	遮断機能	リアルタイム性	復旧	アクティブ・レスポンス	署名機能注1
Tripwire	○	×	×	×	×注2	○
AIDE	○	×	×	×	×注2	×
AFICK	○	×	×	×	×注2	×
OSSEC	○	×	○	×	○	×
Samhain	○	×	○	×	○	○

注1：ツール内で使用するデータベースやコンフィグレーションに対する署名機能を指す

注2：アクティブ・レスポンス機能は組み込まれていないが，チェックの返り値などから異常があったことの判別は可能なので，他ツールとの連携も可能とみられる(例えば，遮断機能や復旧機能との連携など)

表2　表1に示す各ツールで検知可能な内容

項　目	Tripwire	AIDE	AFICK	OSSEC	Samhain
アクセス・タイムスタンプ	○	○	○	×	○
割り当てられたブロック数	○	○	○	×	×
iノード・タイムスタンプ(作成/変更)	○	○	○	×	△注1
iノードが存在するデバイスのID	○	△注1	○	×	○
ファイル所有者のグループID	○	○	○	○	○
iノード番号	○	△注1	○	×	△注1
ファイルのサイズが増加している(成長ファイル)	○	○	×	×	×
変更タイムスタンプ	○	○	○	×	○
リンク数(iノード参照カウント)	○	○	○	×	○
権限およびファイル・モード・ビット	○	○	○	○	○
iノードが指すデバイスのID(デバイス・オブジェクトに対してのみ有効)	○	△注1	○	×	△注1
ファイル・サイズ	○	○	○	○	○
ファイル・タイプ	○	×	×	×	○
ファイル所有者のユーザID	○	○	○	○	○
CRC-32ハッシュ値	○	×	×	×	×
Havalハッシュ値	○	×	×	×	×
MD5ハッシュ値	○	×	×	○	○
SHAハッシュ値	○	×	×	○	○
MD5チェックサム	×	○	○	○	○
SHA1チェックサム	×	○	○	○	○
RMD160チェックサム	×	○	×	×	×
Tigerチェックサム	×	○	×	×	○
HAVALチェックサム	×	○	×	×	×
GOSTチェックサム	×	○	×	×	×
CRC-32チェックサム	×	○	×	×	×
ファイル変更差分	×	×	×	○	×

注1：検知するiノード情報についての記述がないので，iノードのどの情報を検知するのかは不明