防衛庁における情報セキュリティ関連研究開発・技術開発の現状

平成17年8月22日

高セキュリティ品質保証レベル評価実験装置の研究試作

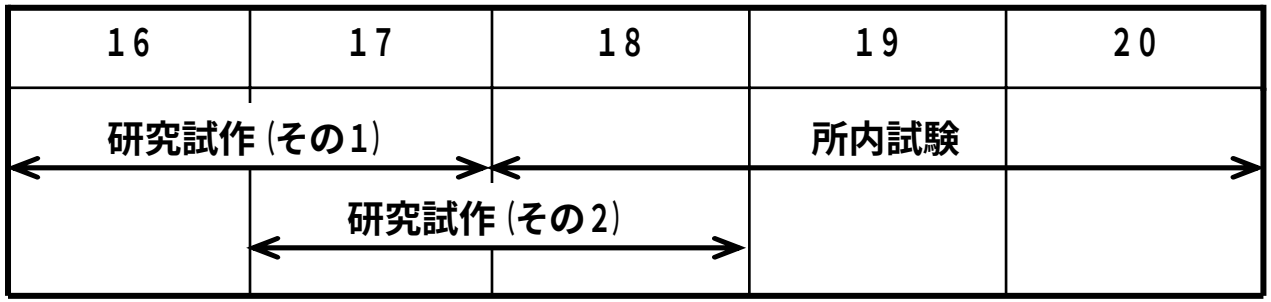
1　目的

情報セキュリティ基準ISO/IEC15408における、評価保証レベルEAL6を満足する情報システムのセキュリティ機能を評価するための技術資料を得る。

2　成果のイメージ

(1) EAL6で規定される評価用ドキュメントの作成手法を明らかにする。

(2) 隠れチャネルや脆弱性の分析等の系統的、網羅的かつ再現性のある評価手法を明らかにし、EAL6での評価手法を確立する。



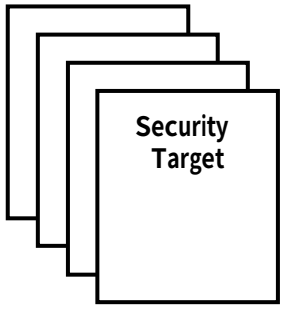
・EAL － 評価保証レベルのこと。レベルの低い方から順に、EAL1～EAL7の7段階に分かれる。一般的には、EAL5以上が軍用またはそれと同等のセキュリティを要求される銀行等で用いられ、そこまでには至らないEAL4以下が民生用と言われている。

・隠れチャネル － システムのセキュリティポリシーに反する方法による情報伝達が可能な通信チャネル。例えば、あるファイルを直接読むことができないユーザAに対し、そのファイルを読むことができる別のユーザBが予め取り決められた方法でシステムの負荷を上げ下げすることにより、システムのチェックを回避しながらBからAへとファイルの内容を間接的に送ることができる。

試作品の構成

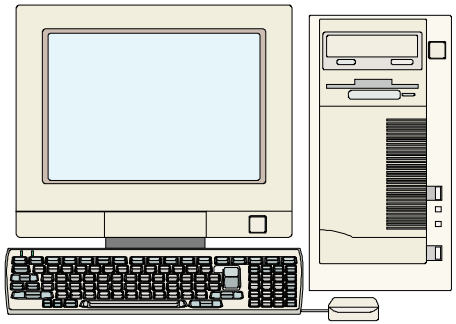
評価対象部
（研究試作（その1））

評価対象装置
（ファイアウォール）

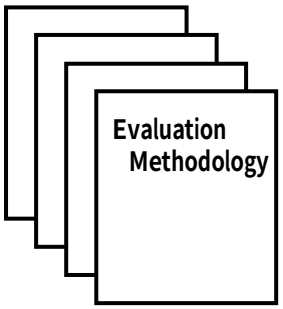


評価用ドキュメント一式

評価部
（研究試作（その2））



解析装置
（脆弱性データベース、
攻撃ツール等）



評価手順書
（評価手法）

ネットワーク･セキュリティ技術の研究

1　目的

防衛庁のネットワークを模擬した大規模コンピュータ･ネットワークへのサイバー攻撃シミュレーションを実施し、対処手法に関する技術資料を得る。

本研究では、まずサイバー攻撃実験を実機環境で行うことができるサイバー戦テストベットを構築する。次にこのテストベッドを用いて、一般的な攻撃検知センサ（FW、IDS）からの検知情報に加えてサーバのログ情報を統合処理することにより、サイバー攻撃を早期に検出し、対処する手法の有効性を評価する。

2　研究の結果

(1) 実機環境のサイバー戦テストベット構築技術を確立し、仮作品の基本特性及びサイバー攻撃シミュレーションが可能であることを確認した。

(2) 複数センサからの情報を得て統合的に検知･対処する手法を確立し、一般的なサイバー攻撃（偵察、侵入、改ざん等）、IDS回避攻撃、DDoS（DoS）攻撃、ワーム系ウイルスに対して有効であることを確認した。

(3) 成果の公表　　本年10月を目途に成果報告書を作成する予定。

12	13	14	15	16	17
	←	特 別	研 究	→	

サイバー戦テストベッドの構成