5-4　Co-Nexus E: 国産セキュリティ製品の検証と実用化支援

5-4　Co-Nexus E: Evaluation and Practical Implementation Support for Domestic Security Products

安部 小百合
ANBE Sayuri

CYNEX Co-Nexus E では、NICT のネットワーク環境に国産セキュリティ製品のプロトタイプを導入し、長期運用を通して機能検証と製品へのフィードバックを行い、国産セキュリティ製品の創出と普及を支援している。本稿では、令和 3 年度から令和 5 年度にかけて Co-Nexus E で実施した検証に関して概要を報告する。

CYNEX Co-Nexus E supports the development and diffusion of domestic security products by introducing prototypes into NICT's network environment, conducting functional verification, and providing feedback on the products through long-term operation. This paper outlines the verification conducted by Co-Nexus E from FY 2021 to FY 2023.

1　まえがき

海外産の製品が多くを占めているセキュリティ製品において、国産製品の研究開発は急務である。CYNEX Co-Nexus-E では、国内の機器製造事業者や運用事業者が研究・開発した国産セキュリティ技術を検証できる環境を構築し、検証を行い、検証結果のフィードバックをしている。検証を行うにはデータや攻撃者に関する情報が必要である。サイバーセキュリティ研究所では、セキュリティデータや NICT ライブネットに届くリアルな通信データ、マルウェア情報、最新の脅威情報の収集や解析を日頃より行っている。それらのノウハウやデータを活用し、検証を行っている。また、CYNEX Red Team（攻撃チーム）を立ち上げ、受動的な通信データのみならず能動的な攻撃試行も行っている。CYNEX RED Team は NICT の社内 CSIRT の一部として、NICT 内のシステムへの攻撃試行によるセキュリティ対策支援や、新たに見つかった脆弱性の検証に取り組んでいる。

これらのノウハウを生かして CYNEX Co-Nexus-E ではセキュリティ製品の脅威への対応力を参画組織に対してフィードバックする取組を行っている。

令和 6 年度当初の参画組織は 7 組織である。参画組織に提供されて実際に検証を開始している製品は 6 製品である。この中には発売中の製品と研究段階の製品が含まれる。本稿では、製品へ検証を行ってきた内容を詳述する。

2　技術検証の要件

ソフトウェアやシステムの製品品質の要件は様々な機関が定義している。ソフトウェア品質の評価に関する国際規格である ISO/IEC 9126-1:2001 [1] では、品質モデルのフレームワークの大項目として機能性、信頼性、使用性、効率性、保守性、移植性の 6 要件が定義されている。IPA の非機能要求グレード 2018 [2] では、システム要件を機能要求と非機能要求の大きく 2 つに分けており、中でも非機能要求は可用性、性能・拡張性、運用・保守性、移行性、セキュリティ、システム環境・エコロジーの 6 要件を定義している。ここでの機能要求は業務実現に関する要求であり、要件を明確化しやすい一方、非機能要求は認識の漏れや認識違いといったギャップが起こりやすいことから、非機能要求を定義している。

セキュリティ機能は一般的なソフトウェアやシステムにおいては非機能要件として定義されるが、セキュリティ製品においてはその製品が対象としている脅威への検知・防御機能や検査製品における攻撃機能の精度は機能要件に含まれる。

NSS Labs [3] では、セキュリティ製品に特化し、主にセキュリティ機能に関する評価を行っていた。攻撃者の振る舞いやマルウェアを検知する EDR（Endpoint Detection and Response）製品においては、脅威を検出する能力、脅威の情報をアナリストへ提供する能力、攻撃を受けたシステムを修復する能力、所有コストの

評価が行われていた。ネットワークにおける通信において従来のファイアウォールに加え、通信内容まで踏み込んで攻撃を検知する機能を持つ次世代FWの評価では、侵入防止機能、大容量の通信を行った際のパフォーマンス、安定性と信頼性、所有コストの評価が行われた。

本プロジェクトにおいては、各製品のセキュリティ機能の機能要件の向上を目的として検証する要件を定義し、検証を行っている。

3　検証対象の技術

3.1　マルウェア検知技術・侵入対策ソフトウェアの検証

マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なプログラムの総称である。依然として脅威であり、情報漏えいのみならず、ワイパー、ランサムウェアといった可用性を損なうマルウェアによる被害は深刻である。

これらのマルウェア及び攻撃者による侵入、情報漏えい対策を行うソフトウェアの検証を行っている。

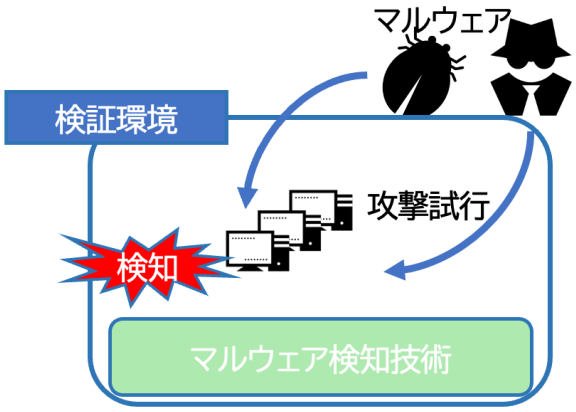

図 1 マルウェア検知技術検証の概要図

本プロジェクトでは、参画組織が開発しているマルウェア検知システムに対しては、マルウェアDB等で公開されているマルウェアやNICTに届いたマルウェアを日々収集し、対象技術を用いて検知できるかを確認し、検知結果や得られたログを用いてフィードバックしている。長期に継続して行うことで最新の攻撃動向にも対応する。

また、STARDUST環境（CYNEX Co-Nexus-Aで提供中）を用いて動的活動観測を行うことでマルウェア検体の実際に実行される環境を再現し、検証を行った。

Redteamでは、攻撃者の実際に用いる手法を日々収集し、検証している。侵入対策ソフトウェアに対して、攻撃者による情報窃取を模した攻撃を行い、その結果をフィードバックすることで製品の機能向上へ貢献している。

3.2　WAF（Web Application Firewall）の検証

WAF（Web Application Firewall）は、Webアプリケーションに対する攻撃から保護することを目的としたセキュリティ技術である。SQLインジェクションやクロスサイトスクリプティング、OSコマンドインジェクションに代表される悪意のあるパラメータを含むリクエストを行う攻撃を検知・遮断する、悪意あるユーザの操作を検知・遮断するサーバに対して大量のトラフィックを送信することで過剰な負荷を与え、正常なサービス提供を妨げるDoS攻撃対策、悪性IPアドレスの遮断など、様々な機能がある。

本プロジェクトでは参画組織が開発しているWAFに対して、主にアプリケーション層における悪性通信の検知精度について検証を行った。Webアプリケーション検査用のデータセットやWebアプリケーション検査ツールを用いてWAF経由の攻撃試行を実施し、検知率、過検知率を検査し、参画組織へフィードバックした。

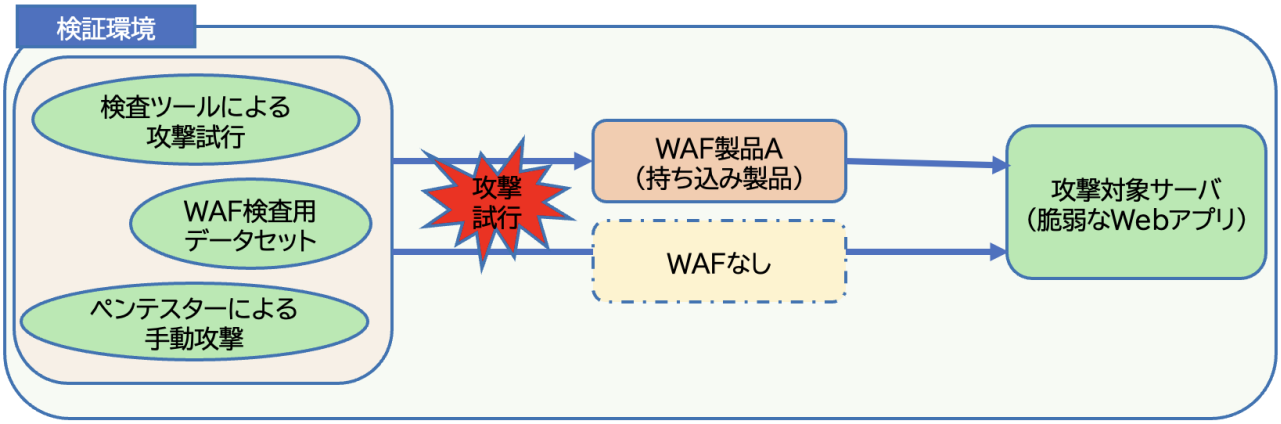

図 2　WAF検証の概要図

3.3　セキュリティデータ提供サービスの検証の検証

セキュリティ対策をするにあたり、攻撃者に関する情報は重要である。IoC（Indicator of Compromise）とは、システムがサイバー攻撃を受けた際に残る指標を指し、セキュリティ侵害インジケーターとも呼ばれる。攻撃時に使用された IP アドレスやマルウェア等悪性ファイルのハッシュ値等、攻撃検知に活用できる情報が含まれる。これらの情報を収集し、配信するサービスがある。前記の WAF や、IPS 等にもこういった情報を活用し、悪性通信を検知する機能がある。

本プロジェクトではこのサービスに対して、NICT ライブネットデータを活用して検証を行った。NICT に届く通信やセキュリティアプライアンスのアラート情報を活用し、このサービスで提供されるデータを活用した場合の有用性の評価を行った。この取組は長期的に行っており、定期的に参画企業へフィードバックをしている。

4　今後の展望

本稿では国産セキュリテイ機器検証の取組について報告した。

今後の展望として、製品品質への認証や評価基準の策定が挙げられる。製品種別は様々であるが、一定の評価基準を定めることで製品の品質を示すことが容易になり、改善点の明確化ができ品質向上に貢献しやすくなることや、対外的に製品品質の説明が容易になり、販売にも生かせるようになると考えられる。このため、製品種別ごとに共通して使用可能な環境構築、国産テスト用データセット作成に取り組みたい。

今後も様々な製品の検証を継続運用し、フィードバックができるよう、検証のできる環境を整えていく。

【参考文献】

1　ISO/IEC 9126-1:2001 (Software engineering --Product quality --Part 1 : Quality model), 2001 年.
2　独立行政法人 情報処理推進機構, “システム構築の上流工程強化 (要件定義・システム再構築・非機能要求グレード),” 2018 年.
3　NSS Labs https://nsslabs.com/

安部 小百合　（あんべ さゆり）
サイバーセキュリティ研究所
サイバーセキュリティネクサス
CYNEX 研究開発運用室
有期研究技術員
サイバーセキュリティ