4F-03

セキュリティ運用自動化に向けた 環境適応型インシデント対応手順技術の提案

片山　貴大†　　山岸　伶†　　川口　信隆†
重本　倫宏†　　野澤　篤史‡　　向井　亮‡
株式会社日立製作所†　株式会社日立情報通信エンジニアリング‡

1.はじめに

近年のサイバー攻撃の増加および高度化に対し，セキュリティ人材の不足からインシデント対応を自動化する技術が求められている．自動化に向けた課題として，インシデント発生時の対応手順が組織ごとに異なるため，自動化も組織環境に合わせた設計・実装が必要となる点がある．この工数が大きく自動化の障壁となっている．なお，標準的な対応手順として NIST 等からガイドラインが示されているが，抽象度が高く実運用と乖離がある．本稿では実運用と標準的な手順の乖離を，環境ごとに異なる機器の構成要素を役割別に抽象化することで解消する環境適応型インシデント対応手順技術を提案する．

2.インシデントレスポンス運用の問題

セキュリティ機器から発せられるアラートは，脅威の兆候を検視したことを示すものであるが，アラート発信がそのまま脅威の発生に繋がるものではない．アラートは脅威の兆候を示すだけである．特に近年の機器では，シグネチャに存在しない未知なる脅威を検知するために，振る舞いに基づく検知機能を取り入れており，従来のシグネチャ検知と比較して誤検知が多い傾向がある．また，シグネチャ検知であっても，監視対象の環境に存在しない装置の脆弱性に向けた攻撃コードなどの影響の無いものが過検知される場合もある．そのため，システムの管理者は，自身の環境に影響の無いアラートも受け取り，その都度，影響有無を判断する作業が発生する．運用現場において，影響の無いアラートが大部分を占めていることが多く，影響のあるアラートは相対的に少数となる．従って，インシデントレスポンスの担当者は，対応する必要のないアラートへの対応に追われることが問題となっている．

A proposal for Environment Adaptive Incident Response Playbook Technology
† Takahiro Katayama, Yamagishi Rei, Kawaguchi Nobutaka, Shigemoto Tomohiro・Hitachi, Ltd
‡ Nozawa Atsushi, Mukai Ryo・Hitachi Information & Telecommunication Engineering, Ltd

本研究では，このような影響有無の判断作業を自動化することに焦点を置いた．

3.関連技術

インシデントレスポンス自動化に向けた近年の動向として，SOAR(Security Orchestration, Automation and Response)という概念が提唱されている．IT システムを運用する組織では，複数のセキュリティ機器から多角的に防御する傾向があり，7 割以上の組織が 6 社以上の製品を導入しているとの調査結果がある[1]．SOAR とは，このような複数の機器を一元的にコントロールする機能ならびにインシデント発生時の対応手順を記したプレイブックによって機械的に対処機能を有することで，自動的にインシデント対応することを可能とするシステムである．このプレイブックは，基本的に監視対象の環境に合わせて実装する必要がある．例えば，導入されている製品のベンダーが異なると，遮断するための操作手順も異なる為，プレイブックに記述する対処手順も異なる．前項で示した影響有無の判断も同様である．対処手順を記述することはインシデントレスポンスに関する専門的な知見が必要，かつ監視対象の環境を厳密に把握しなければならず，知見の無い組織や外部の有識者による実装が困難となっており導入の障壁が非常に大きい．

ジョンホプキンス大学応用物理学研究所が推進する IACD(Integrated Adaptive Cyber Defense)プロジェクトでは，異なる組織においても共有可能なプレイブック方式を提案している[2]．当該方式では，製品に依存しない抽象的な対処手順を共有するとしており，共有した手順の実行には製品のコマンドレベルまで個別の組織が調整する必要がある．

4.　提案方式

既存技術では環境毎に合わせた実装の必要性が自動化の問題となっていた．本稿で提案する

方式は，異なる環境であったとしても，各脅威への対応の大筋となる手順は変わらない点に着目した．例えば，マルウェアに感染したアラートが発せられた場合，導入しているセキュリティ製品によって発信されるアラート識別子は異なるが，どのような製品・環境であったとしても，被疑端末の調査，被疑ファイルの特定，誤検知確認，対処方針の策定，対処といった対応を取る．このような基本的な対応の流れは，NIST などが示すフレームワークで指針が示されており，ほとんどの環境において変わらない[3]．しかし，製品コマンドの差異，対象となる機器の識別子，システム構成といった項目は環境毎に異なるため，個別の環境に合わせて手順を検討しなければならない．

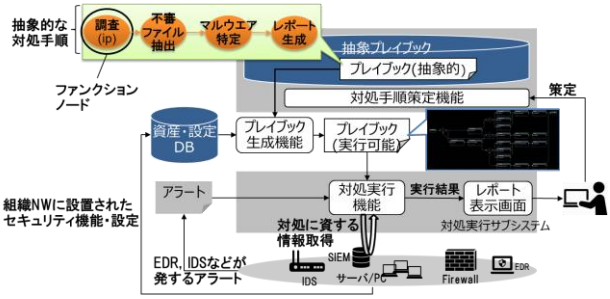
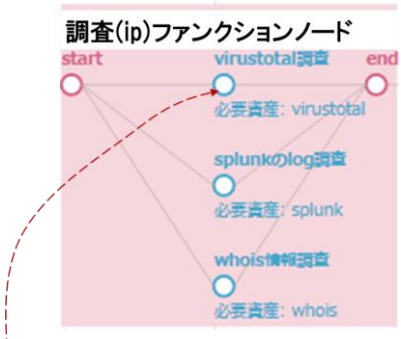


Figure 1　提案方式

提案方式では，大筋となる対応の流れと実際のコマンドの間に存在するギャップを吸収する中間的な抽象レイヤを導入することで，この問題を解決する．本方式では，抽象的な対処手順に対して監視対象の資産情報を参照することで，環境に合わせたプレイブックを機械的に生成する．Figure.1 では，本方式でのプレイブック生成の構成を示している．図に示す抽象的な対処手順は，マルウェア検知時の基本的な対応に基づいた複数ノード(ファンクションノードとする)から構成される．ここで示すファンクションノードは，Table.1 で示す通り，ノードの入力情報，出力情報に基づいて管理される．

Table 1　ファンクションノード一覧

Node	Input	Output
調査(ip)	Dest ip Date	Dest ip's information
不審ファイル抽出	Src ip	Hash list
マルウェア特定	Hash list, Dest ip	True or False (malicious)
レポート	Report format, All data	Report



保有する情報資産

製品	Location	account	Pass word
virustotal	virustotal.com/api/	user	pass
IDS製品β	192.168.xx.xx	root	pass
…			

Figure 2 ファンクションノード

Figure2 では，ファンクションノードの構成を示している．ファクションノードは， table.1 で示した Output を取得する複数の手段から構成される．この複数の手段は，製品コマンドレベルのスクリプトから構成されており，各製品資産が存在する環境でなければ実行できない．Figure,1 で示す通り，情報資産との比較により，各環境に適した手順を選択し，各環境で実行可能なプレイブックを生成することとしている．

このような抽象的な手順と，製品コマンドレベルのスクリプトを分割することで特定の環境に依存しないプレイブック形式で，スクリプトの実装が可能となる．

5.　評価および今後の課題

本方式で実装したプレイブックによる自動的な対処の実現性を検証した．検証のために構成した模擬環境において，cisco 社のアンチウイルス製品からアラートを発生させ，本プレイブックで Virustotal, IDS ログ，AV ログから情報を取得した[4][5]．結果として，アラート発生から報告書が届くまでに最大 20 秒程度で処理が完了することを確認した．今後の課題として，異なる環境においても実行可能なプレイブック形式であることを実証する方向である．

参考文献

[1] cisco 2018 年サイバーセキュリティレポート
[2] IACD, https://www.iacdautomate.org/ ,
[3] 独立行政法人情報処理推進機構（IPA）：「セキュリティ関連 NIST 文書」（2014）
[4] cisco AMP, Advanced Malware Protection
[5] VirusTotal, https://virustotal.com/