言語処理系を組み込んだハイパーバイザによるSDN基盤

尾内 智哉[1,a)]　並木 美太郎[1,b)]

1. はじめに

IoT 機器の急速な普及に伴い, 多くの IoT 機器がネットワークに接続されている. それと同時に多くの IoT 機器が攻撃の対象となっている. NICT サイバーセキュリティ研究所の観測結果によると 2020 年に観測したすべてのパケット数の 53.7%が日本国外からの調査目的と見られるスキャンであったと報告されており, その数は年々増加している [1]. IoT 機器は長期間に渡って使用されるためセキュリティに気をつける必要があるが, セキュリティに関する知識がないユーザは攻撃への対策が難しい. 危殆化した IoT 機器はボットとしてスパムの送信や DDos 攻撃を行うことで大きな被害と混乱をもたらすためセキュリティの確保は重要な課題である.

本研究では攻撃の契機となるポートスキャンを防ぐシステムとして軽量なハイパーバイザ BitVisor[2] の保護ドメインで動作する Unikernel に組み込んだ Lua 言語処理系による SDN 基盤を提案する.

2. 目標

BitVisor の保護ドメイン上の Unikernel に組み込んだ Lua 言語処理系で動作する SDN コントローラによってネットワークをプログラマブルに制御する. SDN で制御するネットワーク内の IoT 機器への攻撃を防ぐために, Lua で記述したルールスクリプトによって SDN スイッチから SDN コントローラに送信される Packet In メッセージを分析する. そして, ポートスキャンを検出して SDN スイッチで通信を遮断する. また, ハイパーバイザでゲスト OS のネットワークをフックして Lua で記述したルールスクリプトによってフィルタリングして SDN による通信の制御に活用する.

3. 提案

本研究で提案するシステムの構成を次の図 1 に示す.

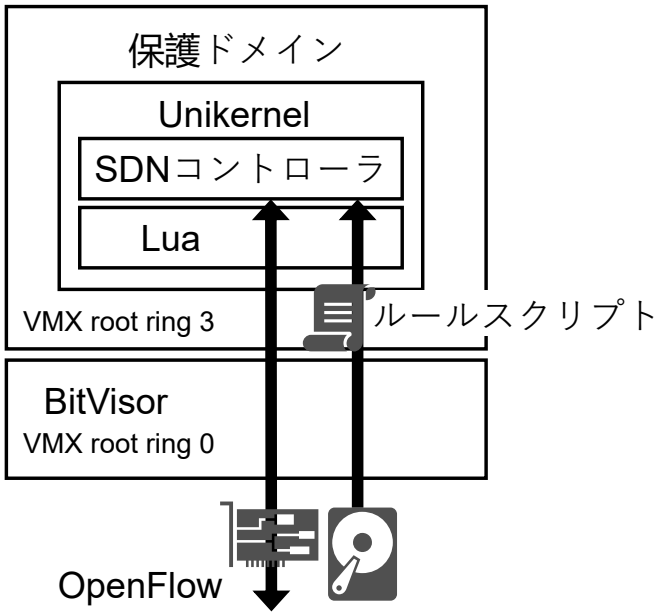

図 1　提案システムの構成

肥沼らが提案した, ハイパーバイザによる高セキュアなコンテナの実行基盤 [3] 上に提案システムを構築する. これは BitVisor の保護ドメインをコンテナの実行基盤として活用する研究であり, コンテナとして Unikernel の IncludeOS を使い, ネットワークデバイスが利用できる. この保護ドメインで動作する Unikernel にスクリプト言語処理系を移植して OpenFlow プロトコルを扱う SDN コントローラが動作する SDN 基盤を構築する.

このシステムはハイパーバイザの保護ドメインで動作するし, ゲスト OS よりも高い特権レベルで動作するため, OS に依存せずに Windows や信頼できない OS でも安全にプログラムを実行することができる

3.1 Lua の移植と活用

スクリプト言語処理系には依存ライブラリが少なく軽量であることから Lua を採用する. IncludeOS は musl libc を使うことができるため Lua を移植することができる.

提案システムでは Lua で記述したスクリプトによって SDN スイッチで通信を制御するためのフローエントリを挿入する. このスクリプトをルールスクリプトと呼び, Uniker-

[1] 東京農工大学
Tokyo University of Agriculture and Technology
[a)] s219821x@st.go.tuat.ac.jp
[b)] namiki@cc.tuat.ac.jp

nel にブロックデバイスのドライバを追加して Unikernel のファイルシステムを使いディスクからルールスクリプトを読み込んで実行する.

ハイパーバイザにスクリプト言語処理系を移植することで, ハイパーバイザに変更を加えることなくスクリプト言語で書いたプログラムをハイパーバイザ上で動作させることができ, ハイパーバイザの拡張性が向上する.

3.2 保護ドメインで動作する SDN コントローラ

Lua でネットワークを扱う SDN コントローラのプログラムを実行するために IncludeOS の TCP/IP プロトコルスタックに変更を加える. IncludeOS では Node.js にインスパイアされて同様のイベントモデルと抽象化を行い, イベントドリブンで非同期にネットワークプログラムが動作する. このため, Lua で扱いやすいように同期型で動作するよう変更を加えて Unikernel 用のネットワークライブラリを作成する.

SDN コントローラは SDN スイッチから受信した Packet In メッセージをディスクから読み込んだルールスクリプトに継続的に渡して分析する. そのために SDN コントローラとルールスクリプトはコルーチンとして協調的に実行する. telnet の通信を遮断するルールスクリプトの例を次に示す.

プログラム 1 Lua で記述した通信を遮断するためのルール

```
1  function filter_telnet(ethhdr)
2    iphdr = string.sub(ethhdr, ETH_HEADER_LEN + 1)
3    ip_type = string.unpack("B", string.sub(iphdr,
         10, 10))
4    if ip_type == TCP then
5      tcphdr = string.sub(iphdr, IP_HEADER_LEN + 1)
6      port_dst = string.unpack(">H", string.sub(
           tcphdr, 3, 4))
7      if port_dst == TELNET then
8        drop(ip_src, port_dst)
9      end
10   end
11 end
```

ルールスクリプトでは SDN コントローラから Packet In メッセージを受け取り, パースして telnet の接続を確認すると drop() によって, その通信を遮断するフローエントリを SDN スイッチに挿入する.

3.3 ハイパーバイザでのゲスト OS のネットワーク監視

アプリケーションレベルの攻撃によってゲスト OS が危殆化した場合にネットワーク内の他の計算機への被害の拡大を防ぐためにハイパーバイザで通信を遮断できるようにする. 図 2 のようにゲスト OS のネットワークをフックして Lua で記述したフィルタリング用のスクリプトによってパケットをフィルタリングしてパケットを通すか遮断する. また, フィルタリングによって得た情報を SDN によるネットワーク制御に活用することもできる.

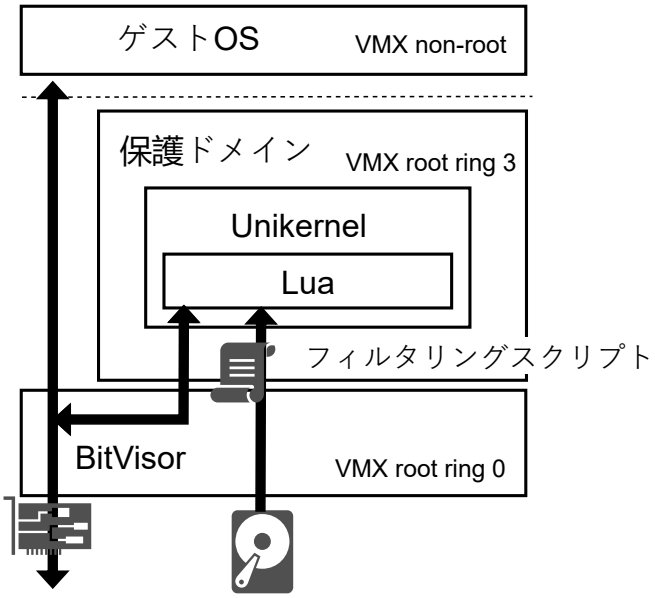

図 2 ゲスト OS のネットワークのフィルタリング

4. おわりに

本研究では BitVisor の保護ドメインを活用した, 言語処理系を組み込んだ SDN 基盤を提案した. このシステムによって攻撃の契機となるポートスキャンを検出して遮断することができ, 計算機のセキュリティの向上に活用できる. 現状, Lua の移植と SDN コントローラの実装, ディスクドライバの追加を完了し, Lua で記述したルールでのゲスト OS のネットワークのフィルタリングに取り組んでいる.

今後の展望としてセキュリティ面での仕様に限らず, より SDN 基盤が汎用的に活用できること示すために BitVisor に組み込まれた VPN の活用や QoS による優先制御などをルールスクリプトで行うことを考えている.

参考文献

[1] 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所. "NICTER 観測レポート 2020". https://www.nict.go.jp/press/2021/02/16-1.html (参照 2021-11-13)
[2] Shinagawa, Takahiro, et al. "Bitvisor: a thin hypervisor for enforcing i/o device security." Proceedings of the 2009 ACM SIGPLAN/SIGOPS international conference on Virtual execution environments. 2009.
[3] 肥沼 健, 並木 美太郎: Unikernel を用いたコンテナのためのハイパーバイザによる軽量高セキュアな実行基盤の検討, 研究報告システムソフトウェアとオペレーティング・システム (OS),Vol.151,No.8,pp.1-7,2021-02-22