Smart Security Operation with Voice User Interface(VUI)

満永 拓邦[,a)]　松本 悦宣

概要：情報技術の発展に伴い，コンピューターインターフェイス技術の進化してきている． 主にキーボードで操作する CUI，マウスでアイコンをクリックする GUI を経て，最近では音声で動作する Voice User Interface（VUI）により操作できるデバイスの普及も進んでいる． かつて，テレビドラマ「ナイトライダー」や「スタートレック」などにおいて，会話を通じて機器の操作をしていた未来の技術も，今日では実現可能な技術となってきた．本稿では，VUI をセキュリティ運用に応用する”Smart Security Operation”という考えを提案し，実験的な実装を行う．”Smart Security Operation”は CUI や GUI による複雑な操作を必要とせず，声のみでセキュリティ運用を実現する．そのため，セキュリティ初心者であっても操作を習得することなく運用が出来るため，セキュリティ業界における人材不足の解消にも繋がり得る技術である．また，それらの実験により得られた知見と課題について検討する．

キーワード：Smart Security Operation, Voice User Interface, 運用自動化

Takuho Mitsunaga[,a)]　Yoshinori Matsumoto

Abstract: With the advancing information technology, richer computer interfaces have been invented and applied into various devices. It started from classic CUI input into screens, and then shifted to GUI to click on an icon with a mouse, and lately Voice User Interface (VOI), which operates by voice, has been developed. This can be one step towards what we used to think ”futuristic” as in ”Knight Rider” or ”Star Trek”. In the near future, cars and spaceships can be operated just by voice commands using AI and VUI. Such automation technology has the following three advantages (1.Automated, 2.Efficient 3.Simplified security operation) Our system proposes a combined use of AI and Software Defined Network (SDN) for automatic blocking of communication and threat analysis by interacting with machines by voice. which is aiming to apply the voice command technology to accomplish automation, efficiency and simplification in cyber security operations.

Keywords: Smart Security Operation, Voice User Interface, Operation Automation

1. はじめに

情報技術の発展に伴い，コンピューターインターフェイス技術の進化してきている． 主にキーボードで操作する CUI，マウスでアイコンをクリックする GUI を経て，最近では音声で動作する Voice User Interface（VUI）により操作できるデバイスの普及も進んでいる． かつて，テレビドラマ「ナイトライダー」[?] や「スタートレック」[?] などにおいて，会話を通じて機器の操作をしていた未来の技術も，今日では実現可能な技術となってきた．本稿では，VUI をセキュリティ運用に応用する”Smart Security Operation”という考えを提案し，実験的な実装を行う．”Smart Security Operation”は CUI や GUI による複雑な操作を必要とせず，声のみでセキュリティ運用を実現する．そのため，セキュリティ初心者であっても操作を習得することなく運用が出来るため，セキュリティ業界における人材不足の解消にも繋がり得る技術である．また，それらの実験により得られた知見と課題について検討する．

[1] 東京大学
The University of Tokyo
[2] Capy 株式会社
Capy Inc.
[a)] takuho@iii.u-tokyo.ac.jp

2. VUI とセキュリティオペレーション

2.1 Voice User Interface（VUI）

Voice User Interface とは声を用いてデバイスとの情報

のやり取りを行うインターフェースのことを表す．デバイスに対して，人間が声を用いて入力し，デバイスからも声による出力を行う．近年，普及が進むスマートスピーカーは，VUI の代表例と言える． 手が塞がっていたり，スピーカから距離がある場所にいたりしても使用することができ，スクリーンの前で操作する必要がある CUI や GUI と比較して，異なる利便性を提供している．スマートスピーカはそれ単独で動作するわけではなく，バックグランドではクラウド上にあるＡＩやシステム群と連携して動作する．スマートスピーカに入力された音声はクラウドに送信され，そこで音声の意味を解釈して，その操作を実行し，結果をスマートスピーカに返送する．その意味では，まさにインターフェースの役割を担っている，そのような仕組み上，スマートスピーカに対する動作を定めるプログラミングはクラウドサービスに実装することとなる．

2.2 サイバーセキュリティに関する運用（オペレーション）と人材不足

サイバー攻撃はより高度化が進み，被害が増えてきている．セキュリティ機器の上げるアラートやログなどを定常的に監視し，起きた事象を分析・報告する Security Operation Center(SOC) やインシデント発生時に対処する CSIRT を設置する企業も増加している．それらの部署において分析や対応には多くの作業が存在していて，限られたリソースで所定の対応時間 (SLA) に収めるには個々の作業に費やせる時間も限られる．SOC や CSIRT を設置する企業が増える一方，セキュリティ人材を確保することは難しく，NRI の調査では，日本企業の 86.9%が不足と回答している [?]．また，サイバー攻撃に対する完全な事前の対策は現実的には困難であり，サイバー攻撃を早期に検出し，被害を最小限に抑えることが非常に重要となっている．そのため，ISAC などの機関を通じた情報共有が重要となってきており，攻撃に使用されたＩＰアドレスやドメインなど「インディケータ」と呼ばれる情報の迅速な共有も重要となっている．国際的には DHS による AIS[?] や MISP プロジェクトによる MISP[?] などのインディケータ共有スキームが存在し，国内においても NISC の C4TAP[?] や IPA の J-CSIP[?] などがハブ組織として活動している．情報共有スキームでは，指標が被害者組織からハブ組織に送信され，ハブ組織はそれらを分析して他の組織に配布する．配布される情報には，同様の攻撃の検出または防止に役立つ可能性のある対策情報も含まれる場合があり，このような情報を受け取った人は，サイバー攻撃に対して効率的に対策を講じることができる．本稿では，セキュリティ運用のうち，情報共有および通信先のブロックに関して実験的な実装を行う．従来行われている対応フローは以下の通りである．

(1) 入手：受信者は，電子メールやポータルサイトを介してテキスト形式の外部組織からインディケーターを取得し，データサーバー（たとえば，電子メールサーバーまたはファイルサーバー）に保存する
(2) 認知：受信者はテキストベースのインディケータから IP アドレスを取得し，プロキシログに保存されている IP アドレスと比較する．それらが一致する場合，組織内に C&C サーバーと通信する 1 つ以上の感染したコンピューターがあることを意味する．
(3) 判断：ＰＣが感染したことの影響などを分析して，責任者は対応方法に関して判断する
(4) 対応：感染したコンピューターと C&C サーバー間の通信をブロックするため，ファイアウォールやプロキシの ACL 設定を変更する．（感染 PC が組織で見つかった場合，実務上はデジタルフォレンジックなどの端末調査が必要であるが，本稿はネットワークの観点からの対応のみに焦点を当てており，デジタルフォレンジックは範囲外とする．）

3. 提案手法

本稿では，VUI を活用したセキュリティオペレーションのうち，情報共有とその対応に関する手法と実装を提案する．

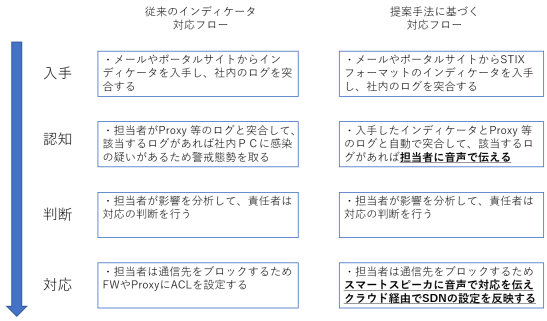

図 1 対応フローの比較

一連の作業を自動化するために，本稿では SDN と STIX の 2 つの技術を用いる．以下，SDN と STIX について説明する．

3.1 STIX（Structured Threat Information eXpression）

従来の脅威情報共有スキームの多くでは，情報は電子メールを介して，人間から人間へテキスト形式で交換されていた．このような情報共有では，送信者が情報パッケージを手動で作成し，受信者に送信する必要があった．受信者側は，情報の内容を正しく読んで理解し，それに応じて対策を講じる必要があった．1 つの例は，マルウェア C&C サーバー情報です．受信者組織は，送信プロキシログの IP アドレスが共有情報の IP アドレスと一致するかどうか

を確認する必要がある．それらが一致する場合，受信者はファイアウォールの ACL（アクセス制御リスト）を変更してアウトバウンド通信をブロックするなどの適切なアクションを実行することとなり，操作には人的なリソースと時間が必要となる．

これらの問題を解決するために，STIX（Structured Threat Information eXpression）と呼ばれる標準形式が MITRE[?] によって導入され，セキュリティ運用とサイバー脅威インテリジェンスの専門家間の議論を通じて米国政府によってサポートされた．STIX は JSON 形式を使用して，C&C サーバーおよび攻撃期間として使用される IP アドレスまたはドメインを示します（リスト 1 は，STIX 形式の例を示す．STIX は，テキストベースの形式ではなく XML または JSON 形式を使用して，脅威情報の詳細を記述するための標準化された言語である．STIX を利用するメリットは以下の通りである．

1. 標準言語なので表現形式が定められており，自然言語と比較すると，送信者・受信者間のズレが生じにくい
2. 標準化されたフォーマットを利用するため，自然言語で記述するテキストベースのインディケータと比較して，機械処理に適している

```
{
  "type": "bundle",
  "id": "bundle--44af6c39-c09b-49c5-9de2",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--d81f86b9-975b-bc0b-
              775e-810c5ad45a4f",
      "created": "2014-06-29T13:49:37.079Z",
      "modified": "2014-06-29T13:49:37.079Z",
      "labels": [
        "malicious-activity"
      ],
      "name": "Malicious site hosting ",
      "pattern":
      "[url:value='http://x4z9arb.cn/4712/']",
      "valid_from":
      "2014-06-29T13:49:37.079000Z"
    },
    {
      "type": "malware",
      "id": "malware--162d917e-766f-4611-b5d6
              -652791454fca",
      "created": "2014-06-30T09:15:17.182Z",
      "modified": "2014-06-30T09:15:17.182Z",
      "name": "x4z9arb backdoor",
      "labels": [
        "backdoor",
        "remote-access-trojan"
..........(omiited)
  ]
}
```

Listing 1
STIX

3.2 SDN

コンピューターネットワークの制御と管理は，複雑さが増しているためますます困難になっている．SDN は，コントロールプレーン（パケットのフローが定義）とデータプレーン（パケットが送受信）を分離することにより，ネットワークの設計と管理の方法を変更できるプログラム可能なネットワークの新しいアーキテクチャである [?]．SDN はネットワークインテリジェンスを集中化し，API を使用してネットワークを制御することを可能にし，ネットワークトポロジに関係なくネットワークを簡単に制御することができる．SDN アーキテクチャは通常，1 つの SDN コントローラーと 1 つ以上の OpenFlow スイッチで構成される．OpenFlow は，SDN コントローラーと OpenFlow スイッチ間の通信に使用されるプロトコルを言う．SDN コントローラーは，OpenFlow プロトコルを使用して，統合された方法でスイッチを管理する．各 OpenFlow スイッチには 1 つ以上のフローテーブルがあり，フローテーブルは，パケットの処理方法に関するルールであるフローエントリの集合である．

パケットフローに関するルールを追加，削除，または変更するには，最初にネットワーク管理者が，意図に従って API を介して SDN コントローラーにコマンドを送信する．次に，SDN コントローラーはコマンドとコマンド OpenFlow スイッチを受信する．OpenFlow スイッチは，受信したコマンドに従ってフローテーブルを更新する．

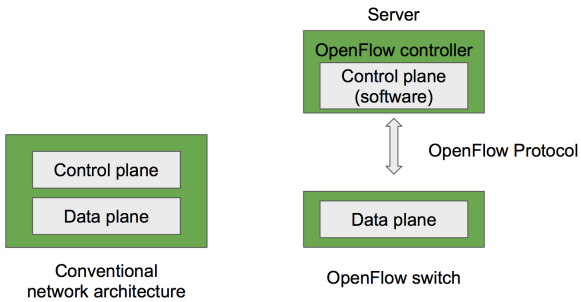

図 2 SDN のアーキテクチャ

3.3 提案手法

STIX と SDN を VUI を組み合わせることにより，音声

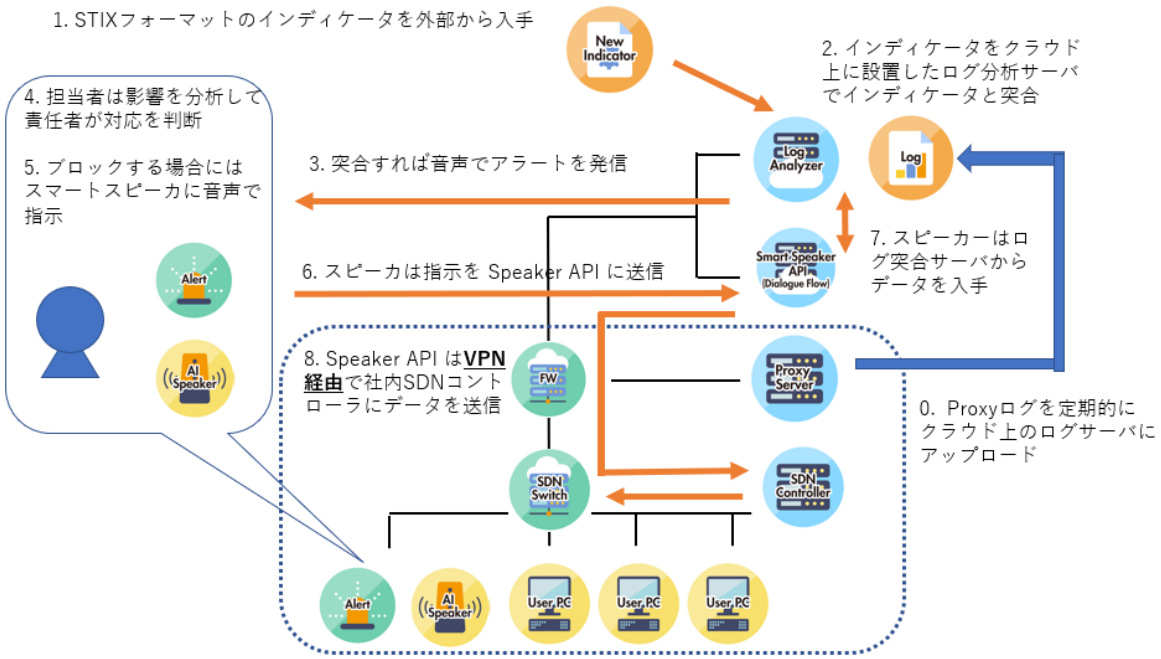

図 3　ネットワークアーキテクチャ

のみでセキュリティ運用を実現する方法を図 3 に示す．まず，外部から入手したインディケータをクラウド上のログ分析サーバで Proxy サーバと突合する．もし，ログの中にインディケータに該当する内容があれば，例えば社内に感染ＰＣが存在する疑いがあるため，アラートを鳴らす．運用者は，スマートスピーカーに対して，当該通信先を止める場合には”Block”，対応しない場合には”Leave”と発話する．”Block”の場合，Smart Speaker の API はドメイン情報をログ分析サーバから得て，その通信先を遮断するように VPN 経由で社内ネットワークの SDN コントローラに指示を送信する．

4.　まとめ

本稿では，VUI を用いた Smart Security Operation という考えを提案し，情報共有を事例に実装を行った．想定通りの動作を実現することはできたが，音声入力であり入力内容が安定しないなどの問題も見つかった．今後は，VUI ｔ単体ではなく，CUI と GUI と組み合わせてより効率的で安定した仕組みの検討を進める．