東芝IoT基盤サービスHABANEROTSのセキュリティー監視システム

Security Monitoring System for HABANEROTS IoT Platform Service

寺島　芳樹 TERASHIMA Yoshiki　　今井　　功 IMAI Isao　　横山　悠平 YOKOYAMA Yuhei

近年，センサーなどのIoT（Internet of Things）機器データを活用するために，クラウドサービスが広く利用されている。クラウドサービスの利用では，ハードウェアなどの基盤の品質は事業者側で，構築したシステムの品質は全てシステム構築者側で責任を持つ。このため，クラウドシステムの構築とその運用において，セキュリティーの確保は重要な課題となる。

東芝グループは，大量のIoT機器からのデータ収集・遠隔操作機能などを提供する東芝IoT基盤サービスHABANEROTS（ハバネロッツ）を開発し，運用している。今回，HABANEROTSのセキュリティーを確保して継続的な運用をするためのセキュリティー監視システムを開発し，IaC（Infrastructure as Code）によるセキュリティー監視システムの管理とその監視運用の体制を構築した。

Cloud services have become widely used in recent years to realize various services using data obtained by Internet of Things (IoT) devices, including sensors and other equipment. Although the providers of cloud computing platforms ensure the quality of the hardware devices used in these platforms, constructors of cloud systems are entirely responsible for the quality of their systems. In particular, ensuring security in the construction of cloud systems and their operations has become an issue of critical importance.

The Toshiba Group has developed and is operating the HABANEROTS IoT platform service, which provides functions for the collection of data from and remote control of large numbers of IoT devices. In order to further enhance the security of HABANEROTS and ensure its continuous operation, we have now developed a security monitoring system, created a management scheme for the system using Infrastructure as Code (IaC) tools, and established a monitoring operation system to respond to any security incidents that may occur.

1. まえがき

東芝は，CPS（サイバーフィジカルシステム）の共通機能を提供するプラットフォームとしてHABANEROTSを構築し，CPS開発運用基盤の統合による開発運用コストの低減とサービスビジネス競争力の強化を目指している[1]。HABANEROTSの利用により，IoT機器データを活用する新たなCPSサービスを容易にスタートさせることができる。

CPSの実行環境として，近年，クラウドサービスが広く利用されている。一般的なクラウドサービスでは，ハードウェアなどの基盤の品質はクラウドサービスを提供する事業者が責任を持つが，構築したシステムの品質は全てシステム構築者が責任を持つ。特に，東芝が対象とするCPSサービスは，社会インフラシステムに広く関わっており，多くの重要なデータ及びそれを扱うクラウドシステムの管理と運用に責任を持つ。

HABANEROTSも，CPSサービス実現を目的としたクラウドシステムの一つであり，HABANEROTSの運用において，セキュリティーの確保は重要な課題となる。

クラウドシステムは，サービス利用者数増加などの状況に合わせてシステム構成や設定の変更が行われたり，システムで使用している既存ソフトウェアに潜む新たな脆弱（ぜいじゃく）性が公表されたりするなど，日々状況が変化する。このため，システム構築時にセキュリティーの確認をするだけでは不十分であり，運用中も継続的な確認が必要とされる。

そこで，HABANEROTSのセキュリティーを確保し，継続的な運用をするために，以下を実現した。

⑴　セキュリティー監視システムの構築　　HABANEROTS内のソフトウェア，及びHABANEROTSが稼働するクラウドシステムを常に監視し，セキュリティー上の問題があればそれを即座に検知するセキュリティー監視システムの構築

⑵　セキュリティー監視システムの管理　　セキュリティー監視システムの運用を容易にするための，IaCによる設定管理や構築の自動化

⑶　セキュリティー監視システムを活用した監視運用体制　　構築したセキュリティー監視システム，及びクラウドシステム向けSaaS（Software as a Service）の活用による，検知したセキュリティー上の問題の自動通知と，その対応・管理を行う監視運用体制の構築

ここでは，セキュリティー監視システムの概要と，その管理・運用体制について述べる。

2. セキュリティー監視システムの構築

2.1 セキュリティー要件

クラウドシステムを活用したCPSサービスには，様々なセキュリティーリスクが存在する。例えば，「サイバー・フィジカル・セキュリティー対策フレームワーク[2]」や「クラウドサービス利用・提供における適切な設定のためのガイドライン[3]」では，エッジデバイスやクラウドシステムのそれぞれで発生し得るリスクとその対策が示されている。

エッジデバイスに関わる代表的なセキュリティーリスクとしては，エッジデバイス内のソフトウェアの脆弱性顕在化がある。その対策として，デバイス認証技術やソフトウェア更新技術が検討されている[4]。一方，クラウドシステムに関わる代表的なセキュリティーリスクとしては，次の四つが挙げられる。

⑴ システム内ソフトウェアの設定不備や，クラウドシステムの設定不備を狙った，クラウドシステム外部からの不正なアクセス

⑵ システム内ソフトウェアの実装ミスや，システム管理者の悪意ある操作による，クラウドシステム内部からの不正な通信

⑶ システム内ソフトウェアに潜んでいた脆弱性

⑷ システム管理者の設定ミスや悪意ある操作による，データベースの外部公開など，クラウドシステムの不適切な操作

2.2 クラウドサービスを活用したセキュリティー監視システム

HABANEROTSのシステムは，クラウドシステム事業者の一つであるAWS（Amazon Web Services）を活用して構築している。AWSでは，HABANEROTSのようなクラウドシステムの構築を可能とするサービスに加え，クラウドシステムのセキュリティー監視に関わるサービスも提供されている。その一部を以下に示す。

- Amazon GuardDuty：異常な通信や動作を検知
- Amazon Inspector：ソフトウェア脆弱性を検知
- AWS Config：クラウドシステムの設定不備を検知
- AWS CloudTrail：クラウドシステムの操作履歴を保存
- AWS Security Hub：各種セキュリティーサービスの監視結果の集約と確認

これらを組み合わせることで，2.1節の⑴～⑷で示したセキュリティーリスクを監視して検知するシステムを構築した。その構成を**図1**に示す。

セキュリティー監視システムは，AWSサービスが提供するセキュリティー国際標準ルールに従ってシステムを監視する。クラウドシステム構成やHABANEROTS内ソフトウェアに変更があったときだけでなく，新たなソフトウェア脆弱性の公表やセキュリティールール追加にも追随し，セキュリティー違反を自動で検知する。

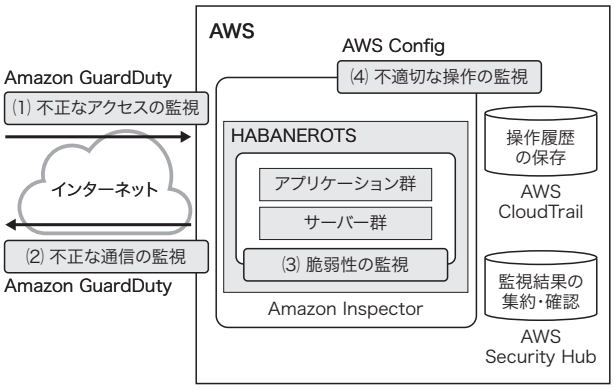

図1. AWSで稼働するHABANEROTSのセキュリティー監視システム
クラウドシステムのセキュリティーリスクを監視し，検知するシステムである。
Security monitoring system for HABANEROTS running on Amazon Web Services (AWS)

HABANEROTSは，可用性やスケーラビリティーの向上や，開発・保守の効率化のため，オーケストレーションツールの標準であるKubernetes®を使用している。Kubernetes®を使用するシステムには，複数のサーバーが存在し，それぞれが独立して稼働する。セキュリティー監視システムがサーバーを構成するソフトウェアのセキュリティー違反を検知した際は，該当サーバーだけの切り離しや該当ソフトウェアだけの更新をする。これにより，被害や影響を最小限に抑えることができる。

3. セキュリティー監視システムの構築と管理

3.1 セキュリティー監視システム構築と管理における課題

2.2節で述べた，AWSの各セキュリティー監視サービスを利用するためには，セキュリティー監視サービスを有効化するだけではなく，セキュリティーの監視ルールに関わるパラメーターや，セキュリティー監視サービスとそれに関連する複数のAWSサービスの利用権限など，様々な項目を適切に設定する必要がある。

AWSでは，Webコンソールやコマンドラインなど，必要項目の設定手段を提供しているが，セキュリティー監視システムの構築と管理においては，複数のサービスにまたがって食い違いがないよう設定する必要がある。このため，セキュリティー監視システム自体の構築や設定変更の作業に掛かるコストの低減や，設定ミスの抑制などが，課題となる。

また，セキュリティー監視では，監視対象としたい環境に応じて，監視の粒度や通知の有無などを個別に設定できることが望ましい。例えば，製品用環境では，開発用環境に比べて，より厳しいセキュリティー監視ルールの適用や，より短い間隔でのセキュリティー違反チェックなどが求められる。このため，環境ごとの設定とその適切な管理が求められる。

3.2　セキュリティー監視システムのIaC化

HABANEROTSのセキュリティー監視システムの，IaCによる設定と構築を，**図2**に示す。

このセキュリティー監視システムは，その構築や管理を容易にするため，Terraformを利用している。Terraformは，クラウドシステムやSaaSの状態をプログラムコードで定義し，クラウドシステムやSaaSの初期構築・更新・無効化などを，プログラム実行により自動的に行うことが可能なIaCツールである。Webコンソールなどでの手動構築と比較して，作業コストや設定ミス発生リスクを低減できる。

また，プログラムコード管理ツールであるGitLabと連携し，セキュリティー監視システムを構築するTerraformのプログラムコードファイルや，セキュリティー監視システムが監視対象とする環境ごとの設定値をまとめたtfvarsと呼ばれるファイルを，GitLabのリポジトリー上でそれぞれ管理している。これにより，セキュリティー監視システムが監視対象とする各環境にとって望ましい設定をそれぞれ定義し，環境ごとの構築と管理とを可能にした。

このセキュリティー監視システムは，AWSが提供する標準的なセキュリティー監視サービスと，クラウドサービスの構築や運用で広く使われているツールやSaaSだけで実現した。また，このセキュリティー監視システムを構築するIaCは東芝グループ内オープンソースとして公開している。このため，HABANEROTSに限らず，東芝グループ内のCPSサービスであれば，セキュリティー監視システムを比較的容易に構築し，適用可能である。

4.　セキュリティー監視システムを活用した監視運用体制

4.1　セキュリティーインシデント解決のための運用体制

HABANEROTSのセキュリティーインシデント対応運用体制を，**図3**に示す。

セキュリティー監視システムで検知したセキュリティーインシデントは，別途監視しているクラウドシステムの資源状況やHABANEROTSのサービス稼働状況と同等に，レベル1相当のオンコールマネジメントSaaSがまず受領する。

オンコールマネジメントSaaSは，事前に設定した条件に基づき，レベル2のオペレーターにセキュリティーインシデントを自動で通知する。

HABANEROTSサービスでは，当初は監視担当からの手動による電話での呼び出しを行っていたが，コストダウンと，通知から対応開始までのリードタイム削減のために，このようなオンコールマネジメントSaaSを採用して無人化した。これにより，オンコール対応体制のローテーションなど柔軟な管理，メール・スマートフォンアプリケーション・SMS（Short Message Service）・電話など通知方式のバリエーションといった利点も同時に獲得できる。

レベル2のオペレーターは，通知内容を基に，保全のための緊急対応が必要か否かのトリアージを行う。オペレーターは，現状復帰に向けた適切な修正を行うとともに，インシデントの内容に応じて，HABANEROTSシステムを管理する各担当者への対応を依頼し，その対応状況を管理する。

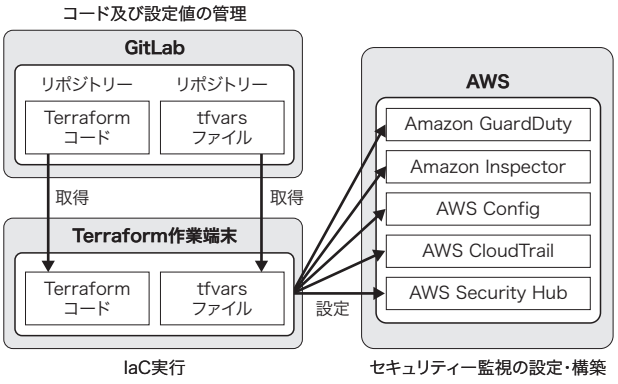

図2.　IaCによるセキュリティー監視システムの設定と構築

セキュリティー監視システムの設定や状態をコードとファイルで管理して，自動構築する。

Setup and construction of security monitoring system using IaC tools

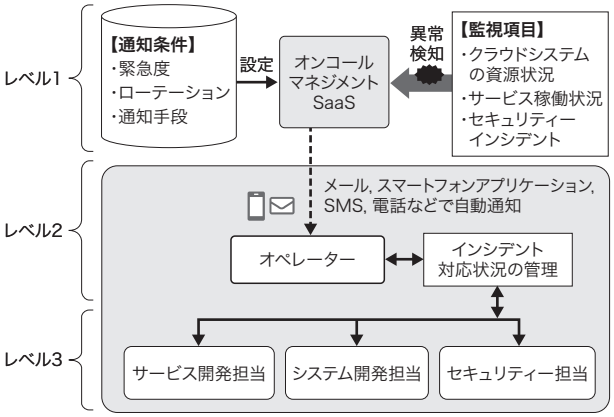

図3.　セキュリティーインシデント対応運用体制

SaaSを活用して，セキュリティーインシデントの通知を自動化できる。

Allocation of security monitoring system operations in response to security incidents

4.2 PSIRT活動

PSIRT（Product Security Incident Response Team）の活動にも，セキュリティー監視システムを活用できる。

PSIRTでは，市場の製品セキュリティーリスクを監視し，入手した脆弱性情報に対してその影響を分析し，必要に応じて速やかに対策を行い，外部組織との調整や情報の公表を行う。

2021年のlog4shellなど，深刻なインシデントの発生時には，クラウドシステム内に多数存在するソフトウェアに脆弱性要因が含まれるか否かについて，短期での報告及び対応が求められる。従来，脆弱性の有無を確認するために，クラウドシステム内にある多数のソフトウェアの調査が必要であり，その情報のまとめと報告に多くの工数を要していた。

HABANEROTSでは，ソフトウェア脆弱性判断の国際的な指標であるCVSS（Common Vulnerability Scoring System）を基に，脆弱性有無の自動チェックを行い，その結果をAWS Security Hubのコンソール上に一覧を表示して確認できる。個々の脆弱性には，AWSが公開し管理している脆弱性情報を基に，推奨される対応方法を速やかに実施できる。

セキュリティー監視システムの活用により，これらの活動を運用の一部として実施することが可能であり，重要インシデント発生時の工数を抑えることができる。

5. あとがき

CPSの共通機能を提供するプラットフォームであるHABANEROTSにおいて，セキュリティーの確保と継続的な運用をするためのセキュリティー監視システムについて述べた。

今後も，東芝グループ全体のクラウドシステムのセキュリティー向上と運用の効率化を，進めていく。

文　献

(1) 内田正之，樋口靖和．CPSサービスの迅速な立ち上げに貢献する東芝IoT基盤サービス HABANEROTSにおけるサービスメッシュの活用．東芝レビュー．2020，**75**，5，p.31–34．<https://www.global.toshiba/content/dam/toshiba/migration/corp/techReviewAssets/tech/review/2020/05/75_05pdf/a09.pdf>，（参照 2023-01-05）．

(2) 経済産業省 商務情報政策局 サイバーセキュリティ課．サイバー・フィジカル・セキュリティ対策フレームワーク Society5.0 における新たなサプライチェーン（バリュークリエイションプロセス）の信頼性の確保に向けて．<https://www.meti.go.jp/policy/netsecurity/wg1/CPSF/CPSF-main_with-LN.pdf>，（参照 2023-01-05）．

(3) 総務省．クラウドサービス利用・提供における適切な設定のためのガイドライン．<https://www.soumu.go.jp/main_content/000843318.pdf>，（参照 2023-01-05）．

(4) 南圭介，ほか．HABANEROTSのエッジデバイス向けセキュリティー機能．東芝レビュー．2021，**76**，5，p.58–61．<https://www.global.toshiba/content/dam/toshiba/jp/technology/corporate/review/2021/05/f03.pdf>，（参照 2023-01-05）．

寺島　芳樹　TERASHIMA Yoshiki
デジタルイノベーションテクノロジーセンター
技術開発室 サービスプラットフォーム開発部
Service Platform Development Dept.

今井　　功　IMAI Isao
デジタルイノベーションテクノロジーセンター
技術開発室 サービスプラットフォーム開発部
Service Platform Development Dept.

横山　悠平　YOKOYAMA Yuhei
デジタルイノベーションテクノロジーセンター
技術開発室 サービスプラットフォーム開発部
Service Platform Development Dept.