Vol.2016-DPS-166 No.30
Vol.2016-CSEC-72 No.30
2016/3/4

クラウドシステムの運用時における動的セキュリティ評価方式の開発と評価

関根基晴[†1]　芦野佑樹[†2]　島成佳[†2]
勅使河原可海[†1]　佐々木良一[†1]

概要：近年，サイバー攻撃の巧妙化により設計から運用に至るまでのセキュリティを考慮した IT システムが求められている．そのため，業界団体や政府機関は，セキュリティ標準への準拠を推奨している．IT システムの運用を担うシステム運用者は，このセキュリティ標準を読解した上でシステム構成に適した具体的なセキュリティ機能の落とし込みとその機能が適切に設定されていることを検証する必要がある．システム運用者は，必要に応じて運用中の IT システムを短時間でシステム構成の変更ができるクラウドシステムにおいても同様の対応が求められる．しかし，セキュリティ標準に基づいたセキュリティ機能の検証方法はシステム構成に依存する．クラウドシステムのように柔軟なシステム構成を伴うシステム運用は，システム構成の変更ごとに具体的なセキュリティ機能の落とし込みと検証が必要であるため，クラウド基盤の利点を活かせない上にシステム運用者の負担に繋がる場合がある．そこで筆者らは，クラウド基盤の利点を活かしてセキュリティ機能を維持する目的として，クラウド基盤上で構築した稼働中の IT システムのシステム構成をログ解析から追随して，モデル化したシステム構成とセキュリティ標準に基づいたセキュリティ機能を自動的に検証するセキュリティ評価方式を提案する．この方式を実装して，運用段階でもセキュリティ標準に基づいていることを保証する支援ツールを開発した．さらに，クラウド基盤上での実験により，提案方式の有効性を示すことができた．

キーワード：運用支援，ログ解析，セキュリティ標準，クラウドシステム

Development and evaluation of a dynamic security evaluation method for the cloud system during operation

MOTOHARU SEKINE[†1]　YUKI ASHINO[†2]　SHIGEYOSHI SHIMA[†3]
YOSHIMI TESHIGAWARA[†1]　RYOICHI SASAKI[†1]

Abstract: Because of the sophisticated cyberattacks of these days, the IT systems are requested to be taken into a special consideration of security from its design stage to operational stage. Therefore, industry organizations as well as governments recommend that the IT system should comply with the security standard. It is necessary for the system operator of the IT system to comprehend this security standard, and to verify that specific security functions for the proper system configuration are selected and implemented appropriately. The operator is requested to make corresponding works for the cloud system where the system configuration of the IT system in operation can be changed flexibly and quickly when necessary. However, the verification method of the security functions based on the security standard depends on the system configuration. Since the system operation for such the cloud system with flexible changes of the specific security functions and verification of these installation whenever system configuration changes, it is difficult to make use of advantage of the cloud infrastructure and it may result in burden of the system operator. Therefore, in order to maintain security functions by taking advantage of the cloud infrastructure, the authors propose a security evaluation method to verify security functions automatically based on the modeled system configuration and the security standard by following the log analysis of the IT system in operation constructed on the cloud infrastructure. They developed a support tool to assure that the system complies to the security standard, Moreover, they could show the effectiveness of the proposed method by experimental evaluation on the cloud infrastructure.

Keywords: Operation Support, Log Analysis, Security Standard, Cloud System

1. はじめに

近年，サイバー攻撃の巧妙化により設計から運用に至るまでのセキュリティを考慮した IT システムが求められている．そのため，業界団体や政府機関はセキュリティ標準への準拠を推奨している[1][2]．IT システムがセキュリティ標準に基づいていることを設計段階において保証するツールは検討されてきたが[3]，設計段階だけでなく運用段階においても保証する必要がある．

設計段階から運用段階においても保証するために，IT システムの運用を担うシステム運用者は，セキュリティ標準を読解した上で IT システムを構築する各マシンの配置（以下，ネットワーク構成）とマシン内で動作するアプリケーションの設定（以下，マシン構成）から成るシステム構成に適したセキュリティ機能に落とし込み，運用していく必要がある．しかし，セキュリティ標準はあらゆる IT システムに対応するために汎用的な記述となっている．セキュリティ標準の記述内容とシステム構成の対応付けをする能力

†1 東京電機大学
Tokyo Denki University
†2 NEC クラウドシステム研究所
Cloud System Laboratories, NEC Corporation

を身に付けていないと，具体的な機能に落とし込み，その機能が IT システムに適切に設定されていることを検証するのは困難である．

その一方で，仮想マシンやネットワークなどの仮想資源などの IT システムの基盤を提供するクラウドサービス（以下，クラウド基盤）上に構築した IT システム（以下，クラウド）の利用が普及しており，新規 IT システムの構築には，約 8 割の企業がクラウドの導入を検討している[4]．今後も需要が増加すると予想されているクラウドもセキュリティ標準への準拠が必要となるが，以下に述べる問題がある．

クラウド基盤は仮想化技術によって必要に応じて仮想マシンやインタフェースの追加などによるネットワーク構成の変更ができる利点がある．例えば，サーバへの負荷が増加したことをロードバランサが検知し，自動で仮想マシンを追加して負荷の分散ができる．一方で，セキュリティ標準に基づいたセキュリティ機能の検証（以下，セキュリティ評価）はシステム構成に依存するため，この様なシステム構成の変更に伴い，設計時にはセキュリティ標準に準拠していても，新たなセキュリティ対策の不備が発生する場合がある．運用段階では，ロードバランサから自動で仮想マシンが作成されるなど，システム運用者の意図していないシステム構成の変更もあるため，構成の変更を追随し，変更の度にセキュリティ評価を行う必要がある．その都度に変更後のシステム構成を適切に解釈した上で，具体的なセキュリティ機能への落とし込みと検証を行うことでセキュリティ標準に基づいたクラウドの運用ができるが，手間がかかる．これは先に述べたクラウド基盤の利点を活かせない上に，システム運用者の負担となる場合がある．

そこで筆者らは，クラウド基盤の利点を活かしてセキュリティ機能を維持する目的としたセキュリティ評価方式を提案するとともに支援ツールとしてのシステムデザインチェッカを開発した．本論文の構成は，第 2 章では関連する研究およびツールと本研究との位置付けを述べ，第 3 章でリアルタイムでのセキュリティ評価に関する課題とこれを解決するための提案方式について述べる．第 4 章では本提案方式を実現するための検討を行い，第 5 章ではその実装に基づいた評価，第 6 章では提案方式の有効性について言及した後，第 7 章でまとめを行う．

2. 関連する方式およびツール

設計段階から運用段階にかけてクラウドのセキュリティ機能を維持するために，IT システムのライフサイクルの各工程で適切なセキュリティ対策を行う必要がある[5]．この目的に関連する研究は，以下のように分類できる．

一つは，設計段階で IT システムの設計の妥当性を評価するためのモデルの提案である．もう一つは，運用段階で IT システムの稼働状態を監視するツールである．

以上の方式およびツールについてそれぞれ述べる．

2.1 設計段階のシステムの妥当性評価の研究

設計段階で IT システムのセキュリティ機能を評価するため，独自のモデルを用いて，IT システムをセキュリティポリシの観点からその妥当性の評価を行う研究が存在する．Shaikh らは，クラウドのセキュリティの強度を評価するための新たなモデルを提案している[6]．また Che らは，クラウドの主要なリスクをまとめ上げ，これらの問題を緩和するためのモデルを提案している[7]．これらの研究は独自の評価モデルを提案してシステム構成についての評価を行い，特に設計時の IT システムの構築に利用できる．しかし，利用者の任意のタイミングで評価を行うため，運用段階には常に評価モデルに準拠できている保証はない．本論文では，既存の評価モデルを利用しているが，システム構成の変更に追随して自動でセキュリティ評価を行うため，設計段階だけでなく運用段階においても，システムがセキュリティ標準に基づいていることが保証できる点が特徴となる．

2.2 稼働状態を監視する研究およびツール

運用段階で IT システムのセキュリティ機能を評価するため，ログの管理および解析から IT システムの稼働状態を監視する研究やツールが存在する．Ambre らは内部関係者から攻撃による脅威に対してログ解析による検知システムを提案している[8]．渡邊らや Söderström らは，運用時のセキュリティ監視と監査を効率化するための管理システムを提案している[9][10]．また，IT システムの運用管理行うためのツールとして SIEM（Security Information and Event Management）が注目されている．SIEM は，サーバやネットワーク機器，各種アプリケーションから収集したログを解析し，異常を管理者に知らせるツールで，問題が発生した後の対応のためだけでなく，攻撃の予兆を発見することが期待されている．この SIEM の仕組みを取り入れたツールが存在する[11][12]．これらの研究やツールはリアルタイムで攻撃に対する局所的な問題に対応できるが，全体の構成についての評価は困難である．本論文では，攻撃を防ぐための予防としてシステム構成についてのセキュリティ評価を行う．そのためにログ解析を行うが，変化するシステム構成を解釈するために利用する．

2.3 既存の方式やツールの課題

2.1 節と 2.2 節で述べた既存の方式やツールにおいて，設計段階から運用段階にかけてクラウドのセキュリティ機能を維持することを目的とした場合，以下に挙げる 3 つの観点において課題が考えられる．

（課題 1）人の知識に依存するセキュリティ評価

セキュリティ標準に準拠したセキュリティ機能を持ったクラウドのために，設計段階では 2.2 節で述べた様な評価モデルに適したシステム構成を検証し，この設計を基にクラウドを構築する必要がある．しかし運用段階では，このセキュリティ機能を維持するために，現行のクラウドのシステム構成が評価モデルに適しているかのセキュリティ評

価を行う．しかし，システム構成の変更が容易に行えるクラウド基盤の利点を活かすと，現行のシステム構成は設計段階のシステム構成とは異なる構成になる．2.1 節で述べたログから IT システムの稼働状態の監視を行っても，局所的な情報のみしか得られないため，現行のシステム構成は，システム運用者が解釈できている必要がある．しかし，システム運用者の知識は人によって異なるため，解釈も異なる場合がある．この解釈を適切に行えないと誤ったセキュリティ評価を行ってしまう．

（課題 2）クラウドの構成変更に追随できない

クラウド基盤は，運用段階でもシステム構成の変更を容易に行える利点を持つが，この利点を活かすことで状況に合わせて構成を容易に変更できる．一方で，構成の変更に伴い新たなセキュリティ対策の不備が発生する場合があるため，セキュリティ機能の維持のために構成の変更が発生するたびに直後にセキュリティ評価を行う必要がある．しかし 2.2 節で述べたセキュリティ評価方式は設計段階での利用を想定しており，運用段階では，構成変更に追随した評価を行えない．そのためシステム運用者は，任意のタイミングでセキュリティ評価を行うが，短い周期で評価を行わないと変更直後の評価を行うのは困難である．システム構成の変更が多いほどセキュリティ評価が必要な機会が多くなるため，クラウド基盤の利点を活かしながらセキュリティ機能を維持することは定期的な評価が強いられ，必要のない手間がシステム運用者にかかる．

（課題 3）セキュリティ評価に要する人の手間

従来のセキュリティ評価は，評価基準となるセキュリティ標準と評価対象となるシステム構成のモデル化が正しく行えていることが前提になっている．クラウドのように大規模で複雑な IT システムを組むことが容易である一方で，それらの漏れの無いモデル化を行うためには，運用者の手間がかかることが容易に想像できる[13].

3. 提案方式

3.1 セキュリティ評価の要件

設計段階から運用段階にかけてクラウドのセキュリティ機能を維持するためには，2.3 節で述べた課題に対応する必要がある．その要件を以下に示す．

（要件 1）セキュリティ評価の方式化

運用段階でのクラウドのセキュリティ評価は，設計段階と運用段階においてシステム構成の差異が生じていることがある．そのため，設計段階のシステム構成を基にした評価結果は，運用段階においても永続的に用いることができない．運用段階における正確なセキュリティ評価を行うためには，稼働中のシステム構成をシステム運用者の知識に依存しない形で生成できる必要がある．

（要件 2）構成変更の追随

クラウド基盤の利点である容易な構成変更が伴うシステム運用においてセキュリティ機能を維持するには，定期的なセキュリティ評価が必要で余分な手間がかかる．この余分な手間を削減するためには，セキュリティ評価が必要なシステム構成の変更直後のみにセキュリティ評価を行えれば良い．そのため，システム構成の変更を追随して，構成変更の要素となるマシン構成とネットワーク構成の変更を検知する必要がある．

（要件3）セキュリティ評価の自動化

セキュリティ機能を維持していることをシステム運用者が評価するためには，セキュリティ評価を行わなければならない．しかし，システム運用者の業務内容はセキュリティ評価を行うだけではないことは自明である[14]．また，クラウドの普及に伴いシステム運用者は複数のクラウドを管理する可能性もある．このような状況で，システム運用者の能力だけでセキュリティ評価を行うと，業務の多くをセキュリティ評価で占めてしまう場合がある．そのため，クラウドのセキュリティ評価を可能な限り自動化する必要がある．

3.2 要件を満たすためのアプローチ

クラウドのセキュリティ機能を維持するために，3.1 節で述べた要件を満たすアプローチを以下に述べる．

（アプローチ 1）モデル化に基づいたセキュリティ評価

システム構成の解釈をシステム運用者の知識に依存させないため，指標となるモデルを作成する．このモデルに基づいて，システム構成の変更直後のシステム構成を解釈していく．そのため，各マシンの構成を読み込みモデルに必要な情報を収集する必要があるが，システム構成のモデルを作成する都度に，全てのマシン構成を読み込むのは手間がかかる．そのため，システム構成に変更があれば，変更があったマシンのみを読み直して，変更前のシステム構成のモデルに差分を更新する．変更があったマシンは，後述する（アプローチ 2）のマシン構成変更の検知から特定できる．このマシンのマシン構成のみを読み直して，手間をかけずにシステム構成のモデルが最新に更新されて（要件 1）に対応できる．

（アプローチ 2）システム構成変更の検知

システム構成の変更に伴ってセキュリティ評価を行うためには，システム構成の変更を検知することでシステム構成の変更に追随する必要がある．システム構成に追随したセキュリティ評価を行うためには以下に述べるように，マシン構成とネットワーク構成を監視することで，システム構成の変更を検知するアプローチを用いた．以下に，2 つのアプローチについて述べる．

(a) マシン構成変更の検知

仮想マシン単体の構成を監視することで，システム構成の変更を追随する．アプローチとしては，マシン内のシステム設定を変更した際に出力されるログを解析し，マシン構成の変更を検知する．このログにはマシン内での様々な

活動の記録が記されてあり，その中からアプリケーションの動作状況の変更を読み取り，マシン内の構成の変更を検知する．

(b) ネットワーク構成変更の検知

仮想マシンの追加や削除などに追随するために，仮想マシンの追加や削除などのネットワーク構成の変更をクラウドの構成を管理する API（Application Programming Interface）を用いて検知する[15]．クラウドを構築する各仮想マシンは，1 台のホストとなるマシンから作られたクラウド基盤上に配置されている．そのため，ホストマシンからクラウド基盤の設定を読み込むことで，どの仮想マシンがどこに配置されており，またどの仮想マシンと繋がっているかを解釈できる．この設定を監視して，ネットワーク構成の変更を検知する．また，上記の(a)のアプローチと併せることで，システム構成の変更に追随するためのマシン構成とネットワーク構成の変更を検知して，(要件 2) に対応できる．

（アプローチ 3）セキュリティ評価のシステム化

クラウドにおけるセキュリティ評価を行うためにシステム運用者にかかる手間を削減するために，この評価を自動で行う必要がある．そのため，（アプローチ 1）で述べた各マシン構成から成るシステム構成のモデルを評価モデルに適用して，適切なセキュリティ機能が設定されているかを検討させる．この評価モデルへの適用に必要な情報を各マシンから収集する．マシン内のアプリケーションは設定ファイルの記述を基に動作している．そのため，設定ファイルを読み込み，マシンの IP アドレスやアプリケーションが利用するポート番号などの必要なデータを抽出することで，モデルの基となるマシン構成を取得する．各マシンから取得したマシン構成を統合することで，システム構成のモデルを作成することができる．このモデルを 2.2 節で述べた様な評価モデルに適用することで，クラウドにおけるセキュリティ評価が自動で行え，（要件 3）に対応できる．

3.3 提案方式の概要

3.2 節のアプローチからクラウドのセキュリティを維持する仕組みとして，システムデザインチェッカを開発する．（アプローチ 1）では，クラウド内の仮想マシンの情報を収集して，現行のシステム構成を表現するモデルを作成する．また（アプローチ 2）では，クラウドのシステム構成の変更を追随して，変更箇所を特定する．マシン構成の変更であれば，セキュリティ評価を行うためのトリガとする．ネットワーク構成の変更であれば，システム運用者の誤作動による場合があるため，誤りがないかを報告する．また（アプローチ 3）では，評価モデルに適用するために必要なデータを設定ファイルから読み込み，セキュリティ評価を行いシステム運用者に報告する．

以上をまとめると，システムデザインチェッカの流れは，図 1 に示す通りとなる．第 4 章では，このシステムデザインチェッカの実装について述べる．

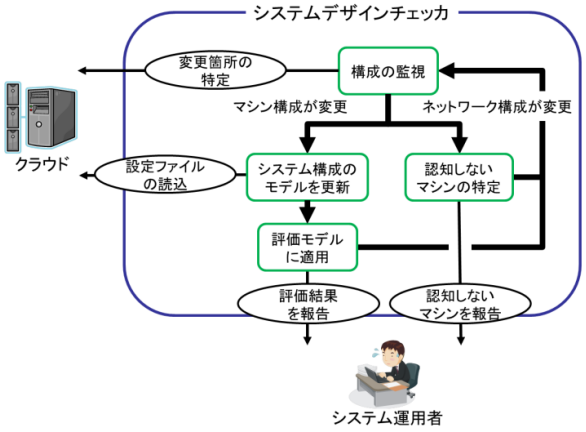

図 1 セキュリティ評価の流れ
Figure 1 Security evaluation process

4. 有効性の検証に向けた実装

本章では，第 3 章で述べたアプローチの実装について述べる．4.1 節では，3.3 節で述べた提案方式の有効性を評価するための方法について述べる．4.2 節では有効性を評価することを目的とした具体的な実装について述べる．

4.1 有効性の評価法

クラウド基盤上に複数の仮想マシンを配置し，仮想マシン内のアプリケーションの設定の変更や，仮想マシンの配置を変更するなどのシステム構成の変更からセキュリティ評価が行えることを評価する．

本論文の実装ではセキュリティ標準として金融機関から策定されたセキュリティ標準の PCI DSS（Payment Card Industry Data Security Standards）を評価モデルとして利用する[16]．PCI DSS は，仮想環境で Web システムを提供することを想定しており，本論文のクラウドへ適用するための方式に適切なセキュリティ標準である．したがって実装は，PCI DSS を評価することを目的としたシステム構成を実装する．PCI DSS の評価において 3 章で述べた課題 1-3 が解決されることを評価するために，以下の検証を行う．

（検証 1）システム構成のモデル化

クラウドを PCI DSS に基づいて評価するために，システム構成から評価を行うためのモデルを作成する．PCI DSS の記述で，マシン構成では Web サーバと DB サーバ，管理者用サーバとそれぞれのファイアウォール（以下，FW）について規定されている．また，ネットワーク構成では，外部ネットワークと DMZ，内部ネットワークの 3 種類のネットワークのゾーンに関して規定されている．以上の規定を満たす Web システムをクラウド基盤上に実装し，そのシステム構成からモデルを作成できることを検証する．具体的な実装については，4.2 節で後述する．

（検証 2）システム構成変更の追随

クラウドは容易にシステム構成を変更できる．この変更をトリガとしてセキュリティ評価を行う必要がある．シス

テム構成の変更の要因は仮想マシン内のアプリケーションの設定が変わりマシン構成に変更があるか，仮想マシンが新たに追加や削除，移動してネットワーク構成に変更があることが挙げられる．この 2 種類の変更を検知し，システム構成の変更に追随できることを検証する．

（検証 3）セキュリティ評価の自動化

PCI DSS に基づいたセキュリティ評価を自動で行う．そのため，(検証 2)のシステム構成の変更を検知し，(検証 1)のシステム構成のモデルが PCI DSS の規定を満たしているか評価する．この流れが自動で行えることを検証する．

4.2 実装

4.1 節で述べた検証を行うための実装を以下に述べる．

（実装 1）現行のシステム構成のモデル作成機能

稼働中の Web システムから PCI DSS に基づいた評価を行うためのシステム構成のモデルを作成する．その Web システムを構築するために，Hyper-V 6.2 を利用する．Hyper-V はマイクロソフト社が無償で提供する仮想化技術で，類似のツールと比べても低コストで同等の性能を発揮するため，仮想化市場で Hyper-V のシェアが高い[17]. Hyper-V のサポートするハードウェアがクラウド基盤にあたり，このハードウェア内に図 2 に示す通りの Web システムを構築する．

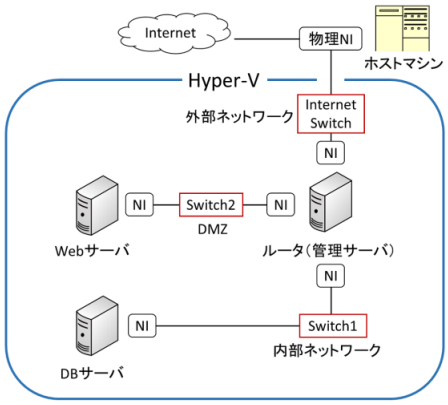

図 2　Hyper-V に構築した Web システム
Figure 2　Web system deployed on the Hyper-V

Web ページを公開する Web サーバを DMZ に配置し，Web サーバで扱うデータを管理する DB サーバを内部ネットワークに配置した．また，外部ネットワークと通信を行うルータを配置し，システム運用者はルータにアクセスして，Web サーバと DB サーバを管理する．各仮想マシンでは，他の仮想マシンと通信するポート以外のアクセスを FW でブロックする設定がされている．また，InternetSwitch，Switch1，Switch2 が仮想スイッチとなる．仮想スイッチに接続した仮想マシンは，その仮想スイッチの属するネットワークゾーンと通信できる．また，Internet の仮想スイッチを通して外部ネットワークと通信する．以上の PCI DSS に規定される最低限の機能を持つ Web システムを構築した．

各仮想マシンの OS やアプリケーションは仮想マシン間で統一されていることとし，OS は Ubuntu 14.04LTS を利用する．この OS を基にセキュリティ評価を行うためのアプリケーションを持ったテンプレートを作成した．テンプレートは 2 種類で，通常に利用するエージェントとエージェントの仮想マシンを管理し，セキュリティ評価の結果を受けるマネージャがある．構築した Web システムではルータがマネージャにあたる．システム運用者は，テンプレートを基に任意のアプリケーションをインストールして Web サーバ等の役割を持った仮想マシンを作成していく．そのテンプレートの構成を表 1 に示す．

表 1　テンプレートの構成
Table 1　Structure of the template

アプリケーション名	アプリケーションの用途
OpenSSH_5.9p1	仮想マシンの管理
OSSEC-HIDS-2.8.1	各仮想マシン内のデータの収集
iptables 1.4.21	パケットフィルタリング / パケット転送
Apache 2.2.22	Web サーバの作成（任意でインストール）
MySQL 14.14	DB の作成（任意でインストール）

またシステムの構成のモデルを作成する基になる各仮想マシンのデータを収集するために，本論文では SIEM の仕組みを導入したツールの 1 つである，利用するための制約が少なく汎用性が高い OSSEC を利用する[18]．OSSEC の基本的な構成としてマネージャとエージェントに分けられ，各マシンに設置されたエージェントがマシン内のログを収集しマネージャへ送信し，受け取ったログを解析する流れとなる．OSSEC を利用して仮想マシンのデータをログに載せて収集することで，最新のデータを基にした表 2 に示す通りの現行のシステム構成のモデルが作成できる．

表 2　システム構成のモデル
Table 2　Model of the system configuration

属性	データの詳細
Object	マシン
	ネットワークインタフェース（以下，NI）
Service	ブリッジ
	Web サーバ
	SSH サーバ
	DB サーバ
	ファイアウォール（以下，FW）
Parameter	NI の属するネットワークのゾーン
	FW のフィルタリングルール
Association	ネットワーク構成（マシン間の繋がり）

モデルは（検証 1）で述べた PCI DSS の規定に対応しており，各仮想マシンの役割と FW の設定，また配置されたネットワークのゾーンと仮想マシン間の繋がりについて記述している．このシステム構成のモデルを用いてセキュリティ評価を行う．またシステム構成のモデルは，OSSEC から収集されたデータを基に作成するため，OSSEC の認識しない仮想マシンが Web システム上に存在する場合は，システムデザインチェッカが適用されていない例外のマシンとして扱う．

（実装 2）システム構成変更の検知機能

セキュリティ評価を行うためのトリガとなるシステム構成の変更を検知する．システム構成はマシン構成とネットワーク構成から成り，この 2 つの変更の検知方式を以下に述べる．

(a) マシン構成変更の検知

マシン構成の変更はログを解析することで検知する．ログ解析は OSSEC で行えるため，これを利用して仮想マシンを監視する．マシン構成は，利用するアプリケーションの設定が基になるため，アプリケーションの動作の基になる設定ファイルと各ポートの利用状況を監視する．変更があればアラートとしてシステム運用者に通知されるため，この通知をトリガにセキュリティ評価を行う．

(b) ネットワーク構成変更の検知

仮想マシンの配置に変更があると，OSSEC の認識を外れるため，該当の仮想マシンを認識させるまでは例外のマシンとして扱われる．その例外となる仮想マシンを特定する．そのため，Web システムを構築する基盤となっている Hyper-V の設定をホストマシン側で読み込み，Web システムのネットワーク構成の変更の情報を管理サーバと共有させる．共有は，ホストマシン上に変更情報を提供する Web サーバを作成し，管理サーバがアクセスする方式とする．設定の読み込みは，Windows のシステム情報の管理を行える Windows Management Instrumentation（以下，WMI）を利用する．設定は，仮想スイッチに繋がっている仮想マシンとその NIC の Mac アドレスをリストとして取得して，XML ファイルで出力する．このファイルを管理サーバの持つシステム構成のモデルと照合して認識できていない仮想マシンおよび NIC を検知する．

（実装 3）セキュリティ評価の自動化機能

PCI DSS に基づいたセキュリティ評価を自動で行う．そのため，設計段階においてシステム構成に PCI DSS に基づいたセキュリティ機能が設定されていることを検証できるようにするため著者らは先に，Web システムのセキュリティ評価を行うナレッジベリファイア（以下，KV）を開発した．これは Web システムの設計時に表 2 に示すシステム構成のモデルを KV に入力することで，PCI DSS との照合を行う．入力されたシステム構成が外部ネットワークから内部ネットワークの DB サーバへのアクセスはブロックする，Web サーバは DMZ に配置する等の PCI DSS の規定を満たせているかを合格か不合格で表示する．これにより問題となる箇所を洗い出し，PCI DSS に基づいた検証を行うことができる．稼働中のクラウドのセキュリティ評価も現行のシステム構成を入力すれば行うことができる．

また（実装 1）で述べた現行のシステム構成のモデルを作成するためには，モデルの基となるマシン構成のデータを収集する必要がある．そのため，設定ファイルから表 3 に示すデータを読み込み XML ファイルで作成する．

表 3　読み込むマシン構成
Table 3　Machine configuration to read

タグ名	取得データ
WebServer	Apache の利用するポート番号/ VirtualHost の利用するポート番号
SSH	利用するポート番号
Database	利用するポート番号
Filter	パケットのフィルタリングルール
Nat	パケットの転送ルール
Interface	IPv4 アドレス / サブネットマスク / MAC アドレス
Bridge	ゲートウェイアドレス / ゲートウェイと通信する NI の IPv4 アドレス

WebServer，SSH，Database タグはアプリケーションが動作していない場合があるため，該当するアプリケーションのプロセスが起動しており，設定ファイル通りのポートを利用しているかを照合する．一致しない場合は，プロセスが正常に動作していないためデータを出力しない．

各マシンで作成したファイルは，OSSEC のログに載せて収集し，システム構成のモデルに統合して表 1 に示す通りに KV へ入力する．仮想マシン間の繋がりは，Bridge タグでは同じゲートウェイアドレスを持つ Bridget タグ同士を接続する．また，ネットワークゾーンの判別は bridge タグの最上位にあるゲートウェイアドレスの属するゾーンを外部ネットワークとし，nat タグの転送ルールから DMZ か内部ネットワークかを判定する．以上のシステム構成のモデルを作成するツールをモデルジェネレータ（以下，MG）とする．

5. 実装に基づいた検証

5.1 検証実験の概要

4.1 節で述べた検証を行うために，図 1 に示す流れに沿った実験を行う．（検証 2）で述べたマシン構成とネットワーク構成の検知によって手順が異なるため，以下に述べる 2 種類の実験を行う．

（実験 1）システム構成変更後のセキュリティ評価

DB サーバの MySQL の利用するポートを変更し，マシン構成を変更する．（検証 2）からこの変更を検知できることを評価する．またマシン構成変更の検知から，（検証 1）の PCI DSS の規定に適した現行のシステム構成のモデルが作成できることを評価する．このモデルを基にセキュリティ評価を行い，（検証 3）のシステム構成の解釈から，セキュリティ機能の検証までの流れが自動で行えていることを評価する．

（実験 2）例外の仮想マシンの特定

4 章で構築した Web システムに新たな仮想マシンを Switch1 の DMZ に配置する．（検証 2）から仮想マシンの追加によるネットワーク構成の変更を検知し，該当する仮想マシンを特定できることを評価する．

5.2 実験結果

5.1 節の検証実験を行った結果を以下に示す．

（実験結果 1）マシン構成の変更

MySQL の利用するポートを変更した結果，管理サーバの OSSEC のマネージャが図 4 に示すアラートを出力した．

```
** Alert 1447596703.752740: mail  - ossec,
2015 Nov 15 23:11:43 (DBserver) 172.18.21.14->netstat -tan |grep LISTEN |grep -v
127.0.0.1 | sort
Rule: 533 (level 7) -> 'Listened ports status (netstat) changed (new port opened
or closed).'
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3307            0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
Previous output:
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

図 4　利用ポートの変更

Figure 4　Change of the using port

変更前は 3306 番ポートを利用して動作していたが，変更後には 3307 番ポートを利用している．これにより，（検証 2）のマシン構成の変更を検知した．このアラートから DB サーバのマシン構成を読み直してシステム構成のモデルを更新する．更新後のデータを図 5 に示す．

```
−<network>
 −<machine id="1000">
    <machineName>DBserver</machineName>
   −<SSH id="3000">
      <port>22</port>
    </SSH>
   −<Database id="3001">
      <port>3307</port>
    </Database>
   −<interface id="2000">
```

図 5　更新したモデル(一部抜粋)

Figure 5　Updated model (excerpt a part)

Database のタグ内の port タグのデータが 3307 になっており，最新のデータに反映されていることが分かる．これにより，PCI DSS の規定に適した現行のシステム構成のモデルが作成され，（検証 1）の検証事項を満たした．このモデルを KV でセキュリティ評価を行った結果を図 6 に示す．ID1001 の Web サーバが ID1002 のルータを通して ID1000 の DB サーバの DB にアクセスできないとある．この DB サーバの iptables のフィルタリングの設定は変更前のままである．そのため，変更後の MySQL の利用するポートへのパケットはブロックされており，Web サーバから DB サーバにアクセスできないことが分かる．以上により，システム構成変更後のセキュリティ評価を自動で行えて，（検証 3）の検証事項を満たした．

（実験結果 2）ネットワーク構成の変更

Agent と言う名前の仮想マシンを作成した結果，管理サーバで図 7 に示す通りの通知を受けた．

```
> 2015/11/16(Monday) 1:26:27
---add machine(NI)'s List
switch1 in the Agent(Hyper-V)
---remove Machine(NI)'s List
```

図 7　仮想マシンの追加の検知

Figure 7　Detection of addition of a virtual machine

Agent と言う仮想マシンの仮想スイッチの Switch1 と繋がった NI が新たに追加されたと記述されている．システム構成のモデルには，この仮想マシンについての記述されていないため，例外のマシンとして扱う．そのため，誤操作で作成していなければシステム構成のモデルに追加するため OSSEC のマネージャと通信するリストに追加する．以上により，（検証 2）のネットワーク構成の変更の検知から，仮想マシンを特定して，（実験結果 1）のマシン構成変更の検知と併せて（検証 2）の検証事項を満たした．

```
−<Result ID="58" EvaluateValue="-1" InputID="1000" InputName="machine" DetailID="1000" DebugInfo=""
 StandardItem="1.2.1.a">
   特定サービス PublicWebServer を持つマシンから特定サービス PublicWebServer を用いて特定サービス CardMemberDB を持つマシンに
   対して特定サービス CardMemberDB にへの通信を禁止されています. 経路: 1001:machine -> 1002:machine(via) -> 1000:machine
 </Result>
```

図 6　セキュリティ評価の結果(一部抜粋)

Figure 6　Result of the security evaluation

以上の実験結果から、検証事項を満たして全ての課題を解決したため，目的としていた設計段階から運用段階にかけてクラウドのセキュリティ機能を維持は，有効だと認められる。

6. 考察

6.1 マルチレイヤによる検証を実施するために

5 章では，MG からシステム構成のモデルを作成し，システム運用者の知識に依存せずに PCI DSS の規定に適したセキュリティ評価を行えた．一方で MG が作成したモデルは KV へ入力するための形式であるが，マシンの内部から読み込んでいるため, 実際には様々なデータを追加できる．MG が読み込むデータを変更すれば，作成したシステム構成のモデルを KV にだけでなく，別の評価モデルに適用することもできると考えられる．そのため，PCI DSS 以外のセキュリティ標準にも適用し，セキュリティ評価の新たな評価項目として連携することを検討する．

6.2 大規模なクラウドでの構成変更の追随について

5 章では，3 台の仮想マシンで構築された Web システムのシステム構成の変更に追随できた．一方で，クラウド基盤を利用すれば数千台の仮想マシンから成る大規模な IT システムも構築できる．このような環境においても，システム構成の変更を追随するために各仮想マシン内のログを解析する，またクラウド基盤にあたるハードウェアの設定を読み込む処理は変わらない．そのため，この処理の負荷に耐える性能を持っていれば大規模なクラウドでもシステムデザインチェッカを適用できると考えられる．

6.3 セキュリティ評価の自動化による付加価値

5 章では，システム構成を基にしたセキュリティ評価が自動で行えた．これにより，システム構成を変更した後でもセキュリティ機能の維持が行えるため，クラウドの規模を変えながらも攻撃を受けないための対策ができる．一方で，システム構成を変更の要因はシステム運用者によるものだけでなく，攻撃により変更されることも考えられる．そのため，変更を検知することで，システム運用者の操作による変更だけでなく，クラウドへの攻撃も検知できるようになった．

7. おわりに

筆者らは，クラウドがセキュリティ標準に基づいていることを，設計段階だけでなく運用段階においても保証できるようにするためリアルタイムでの動的なセキュリティ評価として，システムデザインチェッカを開発した．その要件を満たすために，ネットワーク構成とマシン構成から成るシステム構成のモデル化からセキュリティ評価の自動化を実現した．また，仮想マシン内でのログ解析によるマシン構成の監視とクラウド基盤となるハードウェアの解析によるネットワーク構成の監視から，システム構成の変更を追随し，動的に対応できるようになった．これにより，クラウドのセキュリティ維持の支援とした．

今後は，評価項目の追加を検討すると共に，稼働中の性能の評価を取るための実環境での実験を今後の課題とする．

参考文献

1) 政府機関の情報セキュリティ対策のための統一規範
http://www.nisc.go.jp/active/general/pdf/k305-111.pdf
2) 政府機関の情報セキュリティ対策のための統一技術基準（平成 26 年度版）
http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf
3) 芦野祐樹, 髙橋雄志, 森田陽一郎, 島成佳, 岡村利彦, 勅使河原可海, 佐々木良一: セキュリティ標準に基づいた IT システム設計支援ツールの開発, コンピュータセキュリティシンポジウム (CSS), Vol.4, pp.478-485(2013).
4) MMRI ニュースリリース
http://www.m2ri.jp/newsreleases/main.php?id=010120141104500
5) 安全な情報システムを目指した IPA の取り組み
http://www.ipa.go.jp/files/000039089.pdf
6) Rizwana Shaikh, M. Sasikumar: Trust Model for Measuring Security Strength of Cloud Computing Service, International Conference on Advanced Computing Technologies and Applications(ICACTA), Vol.45, pp.380-389(2015).
7) Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan: Study on the Security Models and Strategies of Cloud Computing, Procedia Engineering, Vol.23, pp.586-593(2011).
8) Amruta Ambre, Narendra Shekokar: Insider Threat Detection Using Log Analysis and Event Correlation, International Conference on Advanced Computing Technologies and Applications(ICACTA), Vol.45, pp.436-445(2015).
9) 渡邊裕治, 水谷正慶, 浦本直彦: IaaS パブリッククラウドにおけるコンプライアンス自動化のためのイベント監視と分析, 研究報告マルチメディア通信と分散処理(DPS), Vol.2015-DPS-162, No.32, pp.1-6(2015).
10) Olof Söderström, Esmiralda Moradian: Secure Audit Log Management, 17th International Conference in knowledge Based and Intelligent Information and Engineering Systems (KES2013), Vol.22, pp.1249-1258(2013).
11) Hinemos とは
http://www.hinemos.info/hinemos
12) ArcSight ESM 概要
https://www.scsk.jp/sp/sys/products/arcsight/
13) ITmedia エンタープライズ
http://www.itmedia.co.jp/enterprise/articles/1312/18/news011.html
14) システム・リファレンス・マニュアル第 4 章 保守・運用
http://www.ipa.go.jp/about/jigyoseika/04fy-pro/chosa/srm/srm4.pdf
15) Hyper-V WMI provider (V2)
https://msdn.microsoft.com/en-us/library/hh850319(v=vs.85).aspx
16) PCI SSC Data Security Standards Overview
https://www.pcisecuritystandards.org/security_standards/index.php
17) @IT Special
http://www.atmarkit.co.jp/ait/articles/1303/14/news004.html
18) OSSEC About
http://www.ossec.net/?page_id=4