

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)公開番号
特開2024-164054
(P2024-164054A)

(43)公開日 令和6年11月26日(2024.11.26)

(51)国際特許分類

F I

G 0 6 F 21/55 (2013.01) G 0 6 F 21/55 3 2 0

G 0 6 F 21/56 (2013.01) G 0 6 F 21/56 3 6 0

審査請求 有		請求項の数	15	O L	外国語出願	(全59頁)
(21)出願番号	特願2024-130983(P2024-130983)	(71)出願人	502303739			
(22)出願日	令和6年8月7日(2024.8.7)		オラクル・インターナショナル・コーポレーション			
(62)分割の表示	特願2022-514618(P2022-514618)		アメリカ合衆国 9 4 0 6 5 カリフォルニア州 レッドウッド ショアーズ, メール ストップ 5 オーピー 7 オラクル パークウェイ 5 0 0			
原出願日	令和2年9月2日(2020.9.2)	(74)代理人	110001195			
(31)優先権主張番号	62/895,847		弁理士法人深見特許事務所			
(32)優先日	令和1年9月4日(2019.9.4)	(72)発明者	リース, クリストファー・ジェイムズ			
(33)優先権主張国・地域又は機関	米国(US)		アメリカ合衆国、9 4 0 6 5 カリフォルニア州、レッドウッド・シティ、オラクル・パークウェイ、5 0 0、オラクル・インターナショナル・コーポレーション			
(31)優先権主張番号	17/009,634					
(32)優先日	令和2年9月1日(2020.9.1)					
(33)優先権主張国・地域又は機関	米国(US)					
(特許庁注：以下のものは登録商標)						
最終頁に続く			最終頁に続く			

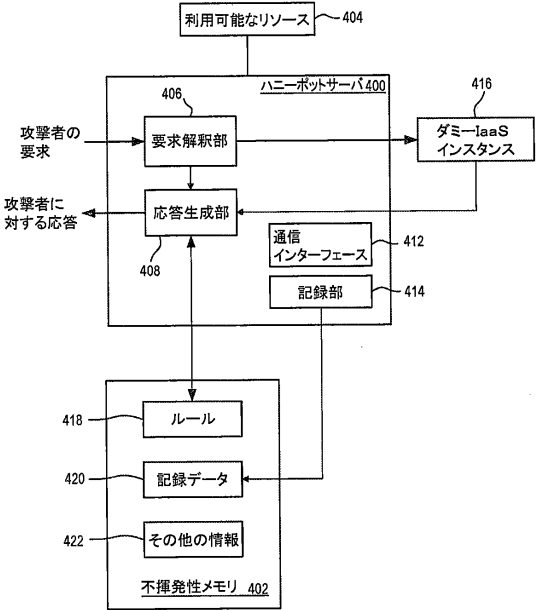
(54)【発明の名称】 サービスとしてのインフラストラクチャの機密保護のためのハニーポット

(57)【要約】 (修正有)

【課題】 ハニーポットを利用して攻撃者をおびき寄せて、IaaS (Infrastructure-as-a-Service: サービスとしてのインフラストラクチャ) インスタンスに対する攻撃パターンについてのデータを収集する方法、記憶媒体およびコンピューティングシステムを提供する。

【解決手段】 コンピューティングシステムにおいて、ハニーポットサーバは、IaaS (Infrastructure-as-a-Service) インスタンスに関する要求を攻撃者から受信し、要求に対する応答を生成し、要求に応じてこの応答を攻撃者に通信し、かつ、攻撃者に関するデータおよび攻撃者によるハニーポットサーバとの1つ以上のやり取りに関するデータを記録する。

【選択図】 図 4



【特許請求の範囲】**【請求項 1】**

方法であって、

コンピューティングインスタンスが、複数のハニーポットサーバを提供するステップを含み、前記複数のハニーポットサーバに含まれる各ハニーポットサーバは、ハニーポット種別を含み、前記方法は、さらに、

前記コンピューティングインスタンスが、攻撃者をおびき寄せて、前記複数のハニーポットサーバのうち少なくとも1つのハニーポットサーバとセッションを確立させるステップと、

前記コンピューティングインスタンスが、前記攻撃者から第1の要求を受信するステップとを含み、前記第1の要求は、前記インスタンスに関する要求であり、要求特性を含み、前記方法は、さらに、

前記コンピューティングインスタンスが、前記要求特性および前記ハニーポット種別の少なくとも一部に基づいて、前記複数のハニーポットサーバのうち特定のハニーポットサーバを特定するステップと、

前記コンピューティングインスタンスが、前記特定のハニーポットサーバと接続するためのセッションを前記攻撃者と確立するステップと、

前記コンピューティングインスタンスの前記特定のハニーポットサーバが、前記攻撃者からの第2の要求に対する応答を生成するステップと、

前記コンピューティングインスタンスの前記特定のハニーポットサーバが、前記第2の要求に応じて前記応答を前記攻撃者まで通信させるステップと、

前記コンピューティングインスタンスが、前記攻撃者に関するデータまたは前記攻撃者による前記特定のハニーポットサーバとの1つ以上のやり取りに関するデータを記録するステップとを含む、方法。

【請求項 2】

前記コンピューティングインスタンスは、IaaS (Infrastructure as a Service) コンピューティングインスタンスを含む、請求項 1 に記載の方法。

【請求項 3】

前記 IaaS コンピューティングインスタンスは、IaaS サービスプロバイダ環境に対応する IaaS サービスプロバイダのコントローラによって実行される、請求項 2 に記載の方法。

【請求項 4】

前記 IaaS コンピューティングインスタンスは、前記 IaaS サービスプロバイダ環境の外部にあるサードパーティサービスプロバイダによって実行される、請求項 3 に記載の方法。

【請求項 5】

前記第2の要求に対する前記応答は、前記 IaaS サービスプロバイダからの応答であるように見えるよう構成される、請求項 4 に記載の方法。

【請求項 6】

前記複数のハニーポットサーバは、前記コンピューティングインスタンスのそれぞれのコンテナに実現される、請求項 1 に記載の方法。

【請求項 7】

前記それぞれのコンテナの各コンテナは、前記複数のハニーポットサーバの各ハニーポットサーバをエミュレートするように構成される、請求項 1 に記載の方法。

【請求項 8】

前記応答を生成するステップは、前記応答を生成するためにルール情報を使用するステップを含む、請求項 1 に記載の方法。

【請求項 9】

前記おびき寄せるステップは、パブリックネットワークで1つ以上のポートを公開する

10

20

30

40

50

ステップを含む、請求項 1 に記載の方法。

【請求項 10】

前記 1 つ以上のポートは、SSH（セキュアシェル）ポート 21、FTP（ファイル転送プロトコル）ポート 22、または SMTP（Simple Mail Transfer Protocol）ポート 25、のうち少なくとも 1 つを含む、請求項 9 に記載の方法。

【請求項 11】

前記 1 つ以上のポートは、ユーザ名とパスワードとのペア、証明書、鍵、またはテナント識別子、のうち少なくとも 1 つを含む 1 つ以上のクレデンシャルを必要とする、請求項 9 に記載の方法。

【請求項 12】

前記攻撃者は、自動ボットである、請求項 1 に記載の方法。

【請求項 13】

前記攻撃者は、前記第 1 の要求または前記第 2 の要求のうち少なくとも 1 つを生成するためのアプリケーションを使用しているユーザである、請求項 1 に記載の方法。

【請求項 14】

前記第 1 の要求または前記第 2 の要求を受信するステップは、GUI（グラフィカルユーザインターフェース）ベースのアプリケーションから前記第 1 の要求または前記第 2 の要求を受信するステップを含む、請求項 1 に記載の方法。

【請求項 15】

コンピュータ実行可能な命令を含むコンピュータ読み取り可能な記憶媒体であって、前記命令は、コンピューティングインスタンスの 1 つ以上のプロセッサによって実行された場合、前記 1 つ以上のプロセッサに動作を実行させ、前記動作は、

複数のハニーポットサーバを提供することを含み、前記複数のハニーポットサーバに含まれる各ハニーポットサーバは、ハニーポット種別を含み、前記動作は、さらに、

攻撃者をおびき寄せて、前記複数のハニーポットサーバのうち少なくとも 1 つのハニーポットサーバとセッションを確立させることと、

前記攻撃者から第 1 の要求を受信することを含み、前記第 1 の要求は、前記インスタンスに関する要求であり、要求特性を含み、前記動作は、さらに、

前記第 1 の要求特性および前記ハニーポット種別の少なくとも一部に基づいて、前記複数のハニーポットサーバのうち特定のハニーポットサーバを特定することと、

前記特定のハニーポットサーバと接続するためのセッションを前記攻撃者と確立することと、

前記コンピューティングインスタンスの前記特定のハニーポットサーバが、前記攻撃者からの第 2 の要求に対する応答を生成することと、

前記コンピューティングインスタンスの前記特定のハニーポットサーバが、前記第 2 の要求に応じて前記応答を前記攻撃者まで通信させることと、

前記攻撃者に関するデータまたは前記攻撃者による前記特定のハニーポットサーバとの 1 つ以上のやり取りに関するデータを記録することを含む、コンピュータ読み取り可能な記憶媒体。

【請求項 16】

前記動作は、さらに、

前記特定のハニーポットサーバが、前記第 2 の要求に対応するアクションを決定することを含み、前記アクションは、仮想コンピューティングインスタンスのインスタンス化を要求するアクションであり、前記動作は、さらに、

前記特定のハニーポットサーバが、コンピューティングリソース、ストレージリソース、またはネットワークリソース、のうち少なくとも 1 つを使用して、前記仮想コンピューティングインスタンスをインスタンス化することを含み、前記応答は、前記仮想コンピューティングインスタンスが正常にインスタンス化されたことを示す、請求項 15 に記載の 1 つ以上のコンピュータ読み取り可能な記憶媒体。

10

20

30

40

50

【請求項 17】

前記動作は、さらに、前記第2の要求は仮想コンピューティングインスタンスを使用してアクションが実行されることを要求していると前記特定のハニーポットサーバが判断することをさらに含み、

前記仮想コンピューティングインスタンスは、前記第2の要求を受信する動作よりも前にインスタンス化され、

前記応答を生成することは、前記仮想コンピューティングインスタンスに前記アクションを適用することによって前記応答を生成することを含む、請求項15に記載の1つ以上のコンピュータ読み取り可能な記憶媒体。

【請求項 18】

コンピューティングシステムであって、
メモリと、

1つ以上のプロセッサとを備え、前記1つ以上のプロセッサは、

コンピューティングインスタンスによって、複数のハニーポットサーバを提供するように構成され、前記複数のハニーポットサーバに含まれる各ハニーポットサーバは、ハニーポット種別を含み、前記1つ以上のプロセッサは、さらに、

前記コンピューティングインスタンスによって、攻撃者をおびき寄せて、前記複数のハニーポットサーバのうち少なくとも1つのハニーポットサーバとセッションを確立させ、

前記コンピューティングインスタンスによって、前記攻撃者から第1の要求を受信するように構成され、前記第1の要求は、前記インスタンスに関する要求であり、要求特性を含み、前記1つ以上のプロセッサは、さらに、

前記コンピューティングインスタンスによって、前記要求特性および前記ハニーポット種別の少なくとも一部に基づいて、前記複数のハニーポットサーバのうち特定のハニーポットサーバを特定し、

前記コンピューティングインスタンスによって、前記特定のハニーポットサーバと接続するためのセッションを前記攻撃者と確立し、

前記コンピューティングインスタンスの前記特定のハニーポットサーバによって、前記攻撃者からの第2の要求に対する応答を生成し、

前記コンピューティングインスタンスの前記特定のハニーポットサーバによって、前記第2の要求に応じて前記応答を前記攻撃者まで通信させ、

前記コンピューティングインスタンスによって、前記攻撃者に関するデータまたは前記攻撃者による前記特定のハニーポットサーバとの1つ以上のやり取りに関するデータを記録するように構成される、コンピューティングシステム。

【請求項 19】

前記ルール情報は、複数のアクションと、前記複数のアクションに含まれるアクションごとに、前記第2の要求において特定されたアクションに対応する少なくとも1つの応答とを含み、

前記ルール情報を用いて前記応答を特定することをさらに含む、請求項18に記載のコンピューティングシステム。

【請求項 20】

前記ルール情報を用いて前記応答を特定することは、

前記ルール情報を検索して、対応するアクションが前記アクションに一致する項目を前記ルール情報から見つけることと、

前記応答を決定するために前記項目を使用することを含む、請求項18に記載のコンピューティングシステム。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本願は、米国特許法第119条(e)の下、2019年9月4日に出願され、「HON

10

20

30

40

50

EY POTS FOR INFRASTRUCTURE-AS-A-SERVICE SECURITY (サービスとしてのインフラストラクチャの機密保護のためのハニーポット)」と題された米国出願第62/895,847号、および、2020年9月1に出願され、「HONEYPOTS FOR INFRASTRUCTURE-AS-A-SERVICE SECURITY (サービスとしてのインフラストラクチャの機密保護のためのハニーポット)」と題された米国出願第17/009,634号の利益および優先権を主張するものであり、それらのすべての記載内容を、あらゆる目的のために引用により本明細書に援用する。

【0002】

技術分野

本開示は、コンピュータセキュリティに関し、特に、ハニーポットを利用して攻撃者をおびき寄せて、IaaS (Infrastructure-as-a-Service: サービスとしてのインフラストラクチャ) インスタンスに対する攻撃パターンについてのデータを収集するための技術に関する。そして、収集されたデータは、解析され、このような攻撃を未然に防ぐために利用され得る。

【背景技術】

【0003】

背景

クラウドベースのサービス (たとえば、SaaS (Software-as-a-Service)、PaaS (Platform-as-a-Service)、IaaS (Infrastructure-as-a-Service)) が急速に増加して普及し、重要な業務運営を行うためにクラウドサービスプロバイダが提供するクラウドサービスにサブスクライブする団体 (たとえば、会社、企業、政府機関、教育機関) が増加している。このようなクラウドが提供する製品が増えているので、クラウドサービスプロバイダは、クラウドサービスを提供するインフラストラクチャに対する悪意のあるユーザによる攻撃からのセキュリティ脅威の増加に直面している。また、クラウドサービスのサブスクライバ (たとえば、団体) も、これらの攻撃による悪影響を受けている。このような攻撃を特定して防げるようになることは、サブスクライバおよびクラウドサービスプロバイダの両者にとって最大の利益に繋がる。

【0004】

しかしながら、クラウド製品に関して、どのように攻撃が起こるのか、および／またはどのように攻撃を防げばよいのかが不明であることが何度もある。この理由は、クラウドセキュリティが比較的非常に新しい、すなわち、従来のネットワークおよび／またはデバイスレベルのセキュリティとは対照的に、新しいタイプのセキュリティであるためである。既存のクラウドセキュリティソリューションは、レベルがとても低く、本質的に事後対応的である。つまり、攻撃されてからどう対処するかを考える。

【0005】

初期のクラウド攻撃は、SaaS サービスおよびPaaS サービスを提供するインスタンスを対象としていたが、最近では、より多くのコンピューティングネットワーク、ストレージネットワーク、および仮想ネットワークが抽象化されてクラウドにされ、様々なIaaS インスタンスを介して公開されると、IaaS インスタンスに対する攻撃が増える。たとえば、ビットコインのような暗号通貨が普及したことにより、大量のコンピューティングリソース、ストレージリソース、およびネットワークリソースを必要とする暗号通貨のマイニング (たとえば、ビットコインのマイニング) を行うためにコンピューティングリソース、メモリリソース、およびネットワークリソースを「盗む」ために、IaaS インスタンスが攻撃される頻度が増えた。SaaS 攻撃およびPaaS 攻撃と比較すると、IaaS 攻撃については、まだまだ理解されていない。

【発明の概要】

【課題を解決するための手段】

【0006】

概要

本開示は、コンピュータセキュリティに関し、特に、ハニーポットを利用して攻撃者をおびき寄せて、IaaS（Infrastructure-as-a-Service：サービスとしてのインフラストラクチャ）インスタンスに対する攻撃パターンについてのデータを収集するための技術に関する。そして、収集されたデータは、解析され、このような攻撃を未然に防ぐために利用され得る。方法、システム、1つ以上のプロセッサによって実行可能なプログラム、コード、または命令を格納する非一時的なコンピュータ読み取り可能な記憶媒体などを含む、様々な実施の形態を、本明細書において説明する。

【0007】

特定の実施の形態では、攻撃者をおびき寄せてハニーポットサーバとのセッションを確立するための技術を提供する。ハニーポットサーバは、IaaSインスタンス（Infrastructure-as-a-Serviceインスタンス）に関する要求を攻撃者から受信する。ハニーポットサーバは、要求に対する応答を生成し、要求に応じてこの応答が攻撃者に通信されるようにする。また、ハニーポットサーバは、攻撃者に関するデータ、および攻撃者によるハニーポットサーバとの1つ以上のやり取りに関するデータを記録する。いくつかの実施の形態では、ハニーポットサーバから構成されるネットワーク（ハニーネットとも称する）が提供され得る。

【0008】

攻撃者から受信した要求を処理することの一部として、ハニーポットサーバは、要求に対応するアクションを決定する。このアクションは、たとえば、IaaSインスタンスのインスタンス化を要求するアクションであり得る。そして、ハニーポットサーバは、コンピューティングリソース、ストレージリソース、またはネットワークリソース少なくとも1つを使用して、要求されたIaaSインスタンスをインスタンス化する。そして、ハニーポットサーバは、IaaSインスタンスが正常にインスタンス化されたことを示す応答を攻撃者に返す。

【0009】

特定の場合、攻撃者から受信した要求は、予めインスタンス化されたIaaSインスタンスを使用して実行されるアクションを要求し得る。そして、ハニーポットサーバは、当該予めインスタンス化されたIaaSインスタンスにアクションを適用することにより、要求に対する応答を生成し得る。

【0010】

特定の実施の形態では、ハニーポットサーバは、IaaSインスタンスをインスタンス化するというアクションが実行されることを要求が求めていると判断し得る。そして、ハニーポットサーバは、実際にIaaSインスタンスをインスタンス化しないで、要求されたIaaSインスタンスが正常にインスタンス化されたことを示す要求に対する応答を生成し得る。場合によっては、攻撃者からの要求は、IaaSインスタンスを使用してアクションが実行されることを要求し得る。ハニーポットサーバは、実際にアクションを実行することなく、また、IaaSインスタンスがインスタンス化されることなく、要求されたアクションに対して適切な応答を生成するように構成される。このようなシナリオでは、ハニーポットサーバは、適切な応答を生成するために、ルール情報を使用してもよい。たとえば、ルール情報は、複数のアクションを特定する情報と、アクションごとに、当該アクションに対応する少なくとも1つの応答とを含み得る。そして、ハニーポットサーバは、このルール情報を使用して、攻撃者が要求したアクションに対する適切な応答を見つけ得る。一実施の形態において、ハニーポットサーバは、ルール情報を検索して、対応するアクションが攻撃者が要求したアクションと一致する項目をルール情報からを見つけ得る。そして、ハニーポットサーバは、項目を使用して、要求されたアクションが正常に実行されたと攻撃者に信じ込ませるように、攻撃者に送信する応答を決定し得る。

【0011】

様々な技術を用いて攻撃者をハニーポットサーバにおびき寄せることができる。たとえば、SSH（シェル）ポート22またはFTP（ファイル転送プロトコル）ポート21な

10

20

30

40

50

ど、攻撃を指揮するために攻撃者が一般的に検索する1つ以上のポートで、一連の1つ以上のクレデンシャルを故意に目立たせ得る。クレデンシャルは、ユーザ名とパスワードとのペア、証明書、鍵、識別子（たとえば、テナント識別子）などを含み得る。

【0012】

攻撃者には、様々なタイプがある。たとえば、攻撃者は、自動ボットであり得る。場合によっては、攻撃者は、ブラウザ、GUIベースのアプリケーションなどのアプリケーションを利用して攻撃を指揮するユーザであり得る。

【0013】

上記の特徴および実施の形態は、その他の特徴および実施の形態とともに、下記の明細書、特許請求の範囲、および添付の図面を参照すると、より明らかになるだろう。

【図面の簡単な説明】

【0014】

【図1】 特定の実施の形態に係る、ハニーボットを備えるハニーネットの実施態様を示す図である。

【図2】 特定の実施の形態に係る、ハニーボットを備えるハニーネットの別の実施態様を示す図である。

【図3】 特定の実施の形態に係る、1つ以上のハニーボットを備えるハニーネットを組み込んだ分散環境の簡略ブロック図である。

【図4】 特定の実施の形態に係る、ハニーボットサーバの簡略ブロック図である。

【図5】 特定の実施の形態に係る、ハニーボットサーバの簡略ブロック図である。

【図6】 特定の実施の形態に係る、ハニーボットサーバの簡略ブロック図である。

【図7】 特定の実施の形態に係る、ハニーボットの実装例のフロー図である。

【図8】 特定の実施の形態に係る、サービスシステムとしてのクラウドインフラストラクチャを実装するためのあるパターンを示す簡略ブロック図である。

【図9】 少なくとも1つの実施の形態に係る、サービスシステムとしてのクラウドインフラストラクチャを実装するための別のパターンを示す簡略ブロック図である。

【図10】 特定の実施の形態に係る、サービスシステムとしてのクラウドインフラストラクチャを実装するための別のパターンを示す簡略ブロック図である。

【図11】 特定の実施の形態に係る、サービスシステムとしてのクラウドインフラストラクチャを実装するための別のパターンを示す簡略ブロック図である。

【図12】 特定の実施の形態に係る、コンピュータシステムの例を示す簡略ブロック図である。

【発明を実施するための形態】

【0015】

詳細な説明

以下の説明において、説明の便宜上、特定の実施の形態を十分に理解してもらうために、具体的な詳細を記載する。しかしながら、これらの具体的な詳細がなくても、様々な実施の形態を実施することができることが明らかになるだろう。図面および説明は、限定ではない。本明細書において用いる「exemplary」という単語は、「例、具体例、例示としての役割を果たす」ことを意味する。本明細書に「exemplary」として記載される実施の形態や設計のいずれも、その他の実施の形態や設計よりも好ましいまたは有利であると必ずしも解釈されるべきではない。

【0016】

より多くの業務運営が抽象化されてクラウドになると、平行して、所与の団体が全体的な脅威の標的になることがさらに高まる。何もしていないとクラウド環境がどのように攻撃されてしまうかについて、内製した脅威インテリジェンスフィードがよく理解している必要がある。

【0017】

本開示は、コンピュータセキュリティに関し、特に、ハニーボットを利用して攻撃者をおびき寄せて、IaaS (Infrastructure-as-a-Service :

10

20

30

40

50

サービスとしてのインフラストラクチャ) インスタンスに対する攻撃パターンについてのデータを収集するための技術に関する。そして、収集されたデータは、このような攻撃を未然に防ぐために利用され得る。

【0018】

特定の実施の形態では、1つ以上のハニーポットサーバ(ハニーポット)を設置する。ここで、各ハニーポットサーバ(ハニーポット)は、攻撃者が極めて悪質な行為を行うためにわざと設置されているエンドポイントノードである。たとえば、偽のバンキングアプリケーション、重要なインフラに関連するアプリケーション(たとえば、決済処理、石油リグの温度)などである。このようなハニーポットは、攻撃者についてのデータを収集するために使われる。

10

【0019】

特定の実施の形態では、ハニーポットは、悪意のあるユーザ(本明細書において、攻撃者とも称する)を欺いて、本物のIaaS(Infrastructure-as-a-Service)インスタンスなど、本物のインスタンスを危険に晒したと思わせるようにデプロイされ得る。実際には、攻撃者は、ハニーポットサーバが提供する隔離されたダミーまたは仮想化されたリソースで操作をしており、保護されているリソースには実際に影響はない。ハニーネット、またはこのようなハニーポットから構成されるネットワークは、クラウドサービスプロバイダが提供するIaaSサービスまたはサービス製品をエミュレートするようにデプロイされ得る。たとえば、Oracle Corporation(登録商標)が提供するOCI(Oracle Cloud Infrastructure) IaaSサービスをエミュレートするためにハニーネット(または、複数のハニーネット)が提供されてもよい。別の例として、ビットコインをマイニングするための、規制がある一連のコンピューティングリソースを有するハニーネットとして、一連のサーバが設置されてもよい。

20

【0020】

SSH(セキュアシェル)またはFTP(ファイル転送プロトコル)のようなプロトコルを使用してハニーポットサーバを設置してもよい。攻撃者がアクセスしてログインできるいくつかのクレデンシャル(たとえば、ユーザ名とパスワードとのペア、鍵など)を有するハニーポットが設置されてもよい。本物のIaaSインスタンスにアクセスすることにより、攻撃者は、「大当たり」したとってしまう。

30

【0021】

攻撃者がダミーIaaSインスタンスとやり取りすると、ハニーネットインフラストラクチャは、攻撃者に適切な応答を提供して、ダミーインスタンスではなく本物のIaaSインスタンスとやり取りしていると信じ込ませるよう攻撃者をだますように構成される。特定の実施の形態では、仮の攻撃者を用いて、予め用意された／予めでっち上げられたやり取りの流れを設置してもよい。

【0022】

攻撃者のハニーポット(および、ハニーネット)とのやり取りは、記録またはログが取られる。記録された攻撃者のデータは、攻撃者の行為(たとえば、脅威の行為者のユーザ挙動パターン、ユーザに一意のその他の属性)、特定の攻撃者の接続属性およびデバイスレベルの属性(たとえば、接続情報、攻撃の呼び出しおよび要求を発信するために攻撃者が利用したデバイスのIPアドレス、ASN(Autonomous System Number: 自律システム番号)トレースルート情報、ドメイン名など)など攻撃者についての一意の属性、および攻撃に関するその他のデータを含み得る。記録されたデータは、攻撃者の一連の行為についてのデータ、攻撃者がアクセスしたオブジェクト、攻撃者が行ったAPI呼び出し(たとえば、攻撃者が行ったREST API呼び出し)などを含み得る。

40

【0023】

そして、ログに記録されたデータを解析して、攻撃パターンについての情報およびアナリティクスを特定できる。たとえば、ログに記録されたデータは、攻撃者がどのように攻

50

撃を指揮したのか、攻撃者が何を攻撃していたのか、攻撃の背後にある目的や意図は何であったのか、攻撃の頻度のどれくらいであったのかなどの質問に答えるために用いられてもよい。

【0024】

ハニーネットは、本明細書で記載する場合、脅威のベクトルが多くの場合バイナリベクトルではないが、むしろ、いくつかの一連のアクションまたは一意の属性から構成される場合の、クラウドセキュリティのための追加の必要な保護メカニズムを提供する。データレイクおよびその抽出メカニズム、ロードメカニズム、および変換メカニズムに組み込まれると、教師なし機械学習技術を利用して、新しいゼロデイ脅威（たとえば、これまで見たことのない脅威）を特定することが可能になる。

10

【0025】

そして、ハニーネットが取り込んだまたは記録したデータを使用して、特定の攻撃者および攻撃者の部類を一意に特定し、攻撃についてのパターンを見つけることができる。ハニーネットを用いて収集されたデータは、攻撃メカニズムを理解するために、および団体が知らないであろうゼロデイ脆弱性を含む、進行中の攻撃を防ぐために重要なデータになる。特定のIPアドレスが不正なアドレスであると特定されたときにフラグを立てられて適切な措置が取られるように、ハニーネットサービスをセキュリティサービスとして提供することができる。

【0026】

ハニーネットが記録またはログを取ったデータを、解析を行うためのアナリティクスプラットフォームに送ることができる。たとえば、記録されたデータは、このような攻撃を特定するための1つ以上のモデルを構築するためのAI（人工知能）ベースのML（機械学習）プラットフォームに送られ得る。ハニーネットシステムが取り込んだデータは、セキュリティ脅威を特定するために用いられている機械学習技術をさらに向上させるために利用できる有用かつ関連性のある訓練データを提供する。ハニーネットがログを記録したデータを用いて、新しい向上したセキュリティモデルを構築できる。

20

【0027】

ハニーネットが記録した1人または複数の攻撃者についてのデータは、様々な目的で使用されてもよい。特定の実施の形態では、1つ以上のハニーネットが収集したデータは、これらのハニーネットから集中ログサーバに転送され得る。そして、ログサーバは、解析するために収集データを転送する、または収集データへのアクセスを提供し得る。たとえば、収集されたデータは、解析のために転送され、攻撃者および同様の脅威を特定するように構成された脅威インテリジェンスツールに利用され得る。たとえば、脅威インテリジェンスツールは、収集したIPネットワーク情報および当該IPネットワーク情報と脅威の行為者との関連を使用して、類似した攻撃を特定し得る。収集されたデータ（たとえば、鍵ペアの値、イベント、オブジェクト情報など）を機械学習パイプラインに供給して、脅威攻撃の特徴についての情報を学習し得る。このデータは、現在のユーザについての一連のイベントを理解するために用いられ得、これらのユーザが脅威を与えているかどうか、当該ユーザのクラウドアクティビティプロファイルから導き出され得る。

30

【0028】

特定の実施の形態では、1つ以上のハニーネットが記録したデータを解析するために用いられる機械学習パイプラインは、Apache Kafkaを用いたパイプラインなど、分散ストリーミングプラットフォームを用いて実現され得る。ハニーネットが収集したイベントおよび監査ログは、Kafkaを用いたパイプラインに提供される。Kafkaを用いたパイプラインは、データをデータレイクに格納する。そして、格納されたデータは、K-meansまたはK-means++アルゴリズムなど、クラスタリングアルゴリズムにかけられて、脅威プロファイルおよび脅威を特定し得る。

40

【0029】

そして、特定した脅威に対して、未然に予防する措置が開始され得る。場合によっては、このような脅威を特定して、悪意のある行為が実行される前であっても予防措置を取る

50

ことが可能になり得る。たとえば、ユーザのアクティビティプロファイルに含まれる情報が、攻撃者についてハニーネットが収集したデータに基づいて生成された情報またはプロファイルと一致した場合、アラートを生成し得る。いくつかのその他の場合、攻撃者が悪意のある行為を行うための時間が少なくなるように、素早い期間で脅威を特定して予防措置を取り得る。たとえば、攻撃のプロファイルに一致する1つまたは2つのアクションが特定されるとすぐに脅威が特定されてもよい。

【0030】

特定の実施の形態では、ハニーネットが提供するセキュリティ機能自体をクラウドサービスとして提供できる。このようなクラウドサービスは、サブスクライブしているテナントについて、リソースへのアクセスを特定し、不適切なアクセスにフラグを立て、適切な対応措置を取るように構成され得る（たとえば、特定のIPアドレスが不正なアドレスであると特定された場合、フラグが立てられて適切な措置が取られる）。

10

【0031】

攻撃者についてのデータを取り込んで収集し、攻撃者の気持ちになってこのような攻撃がどこからどのように発信されて実行されるのか、攻撃されるリソース、このような不正アクセス中の行動パターン、系列情報、動機が何であるのかを理解するためのツールとして、および攻撃者についてのコンテキスト情報（たとえば、どこから攻撃者がやって来るのか、どのような種類のオペレーティングシステムを攻撃者が使用しているのか、何時に攻撃してくるのか、および攻撃に関連するその他の属性）を得るためのツールとして、ハニーネットまたはハニーポットから構成されるネットワークをこのように使用する。ハニーネットを利用して、実際の有用なリソースを危険に晒すことなく、このような攻撃についてより多くのデータを見つけ出すことができる。クラウドサービスプロバイダの場合、1つ以上のハニーポットから各々が構成される1つ以上のハニーネットをプロバイダの1つ以上のデータセンターに設置し得る。ハニーネットにより、新しいタイプの脅威を事前に特定することが可能になり、クラウドセキュリティソフトウェア／クラウドセキュリティの人員が、自律した方法で事前により望ましいデータを得ることによって、攻撃者よりも一歩先に居続けることが可能になる。

20

【0032】

例示的な実施の形態 # 1

以下に、特定の実施の形態に係る、ワークフローの例を説明する。以下に説明するワークフローは、複数のステップを含む。これらのステップおよびその順序は、限定ではない。

30

【0033】

ステップ1：ハニーネットを、攻撃者（たとえば、ダークウェブユーザ）がアクセスできるようにする

第1ステップには、ハニーネットを攻撃者が引き寄せられるように設置するステップを含む。特定の実施の形態では、一連のサーバを設置して、HTTPまたはFTPなどのプロトコルでの攻撃者からの要求を傍受し得る。都合よく、ディレクトリ構造にあるCSVファイルまたはデータベースファイルに、攻撃者が見つけられるように、クレデンシャルを都合よく格納し得る。攻撃者は、サービスのインスタンス（たとえば、IaaSインスタンス）に対するダミークレデンシャルを見つけると、当該ダミークレデンシャルを用いてサービスインスタンスにアクセスして、そのサービスインスタンスを介して利用可能なリソースを使用しようと試みる。

40

【0034】

たとえば、図1および図2に示すように、（セキュアログイン、FTP、ポートフォワーディングなどのために使用される）ポート22またはポート21上のFTP待ち受けモードによって、攻撃者は、おとりノードを傍受し得る。クレデンシャルを一般的な命名規則（すなわち、ルート／パスワード）に設定することができる。攻撃者は、歴代のディレクトリ一覧に目を通して、先頭にテキスト（スーパーユーザ）が付けられる、csv／.dbファイルを見つけるであろう。ダークウェブユーザは、スーパーユーザを指定するこ

50

のファイルの一番上部分に置かれているランダムに生成されたクレデンシャルを見つけるであろう。クレデンシャルは、スーパーユーザ名／パスワードの形式であり得る。これらのクレデンシャルは、「攻撃を受ける」ために設置された、IaaSハニーネットが提供するダミーIaaSインスタンスに攻撃者をアクセスさせるためのクレデンシャルである。

【0035】

攻撃者を特定するために、ハニーネットによって様々な技術が用いられてもよい。一般に、通常のユーザは、インターネット上のおとりノードを探すことはないであろう。たとえば、おとりノードがSSH用のポート22上で動作していた場合、平均的な一般ユーザ（たとえば、クラウドサービスプロバイダの正規クライアントまたは正規テナント）は、そのおとりノードを見つけようとはしないだろうし、したがって、おとりノードに目を通してクレデンシャルを見つけることはしない。おとりノード自体を、ダミークレデンシャルを分散させるためのメカニズムとして用いてもよい。攻撃者は、ダミークレデンシャルに引き寄せられて、これらのクレデンシャルにアクセスして利用し、悪意のある行為を行う。攻撃者は、ポート上で開放されているおとりノード上にクレデンシャルが不注意で残されていると考えるように導かれる。

【0036】

攻撃が発生し得る方法がいくつかあるが、以下の2つの方法が最も一般的である。

(1) 自動ボットを利用する。ボットは、できるだけ多くのクレデンシャルを学習するように構成され得、その後、スクリプトを用いて、学習したクレデンシャルを利用して悪いことをする。

(2) 攻撃者は、たとえば、ブラウザまたはその他のGUIアプリケーションを用いて、自分自身でサービスとやり取りすることに関心を持っている。攻撃者は、GUIを使用してクラウドサービス（たとえば、OracleのOCIサービス）とやり取りする可能性がある。これは、攻撃者の要求に応じてアクションを実行する機能を有するAPIエンドポイントに向かうCLI（コマンドラインインターフェース）（たとえば、REST APIベースの要求）要求によって行われ得る。GUIは、本質的に、CLI要求のラッパーである。CLI要求は、コマンドラインモードを用いて、または、GUIインターフェースを用いて生成され得る。

【0037】

特定の実施の形態では、本明細書に記載のハニーネットは、ボットベースの攻撃およびGUIベースの攻撃の両方に対処可能である。

【0038】

ステップ2A：攻撃者が自動ボットである（CLIモード）

ステップ2Aの目的のために、CLI（コマンドラインインターフェース）モードの自動ボットを用いて攻撃が実行されると想定する。図1は、特定の実施の形態に係る、自動ボットから受信する要求に対処するためのハニーネットシステム100を示す。ハニーネット100は、1つ以上のハニーボットから構成され得る。図1では、ハニーネットが提供するIaaSインスタンス102が点線内に示されている。

【0039】

図1に示すように、おとりノード104は、攻撃者がREST APIノード106にアクセスすることを可能にする。REST APIノード106は、IaaSサービスのインスタンス102へのゲートウェイであり得る。図1（および図2）では、IaaSインスタンス102（図2のインスタンス202）は、点線で示されており、コンピューティングリソース、ストレージリソース、およびネットワークリソースを含む。おとりノード104は、1つ以上のハニーボットから構成されるハニーネットにアクセスするためのクレデンシャルへのアクセスを攻撃者に提供し得る。ここで、これらのハニーボットは、1つ以上の「ダミー」IaaSインスタンス102を提供する。提供されたクレデンシャルにより、攻撃者は、IaaSハニーネットが提供するダミーIaaSインスタンスのうち1つに接続可能になる。

【0040】

REST API（コマンド&コントロール）ノード106（図2の206）は、攻撃者と、攻撃者が極めて悪質なことを実行したいリソースまたはオブジェクトとの間を仲介する役割を果たす。たとえば、REST APIエンドポイント106（図2の206）は、ボット／攻撃者が生成しているCLIのGET要求から作成されたすべてのリソース／アクションを仲介するよう機能する。特定の実施の形態では、REST APIノード106は、攻撃者からCLI要求を受信し、CLI要求を解析して攻撃者が要求したアクションを理解し、要求に対して攻撃者が予想している出力または応答を攻撃者に提供する。

【0041】

また、REST APIノード106には、実際のダミーではないリソースにアクセスしたまたは何らかのアクションを行ったと思わせるように攻撃者をだますための機能がある。これは、攻撃者から受信した要求（たとえば、GET要求、POST要求）に対して正しいダミー応答を提供して攻撃者をだまし、実際に攻撃できた（すなわち、実行するよう攻撃者が要求したアクションが正常に行われた）と思わせることによって行われる。たとえば、応答は、攻撃者をだまして、IaaSインスタンスを設置することができた、当該インスタンスを用いて様々な操作を行うことができたと思わせる。REST APIノード106は、攻撃者に虚偽情報またはダミー情報を供給して、悪意のある行為が正常に行われたと信じ込ませる。すなわち、攻撃者をだまして、攻撃者が要求していることが実際に発生していると信じ込ませる。このノードは、偽りを継続させるためのツールとして用いられる。

【0042】

REST APIノード106には、攻撃者から受信した要求を処理して、攻撃者が予想する情報を攻撃者に供給して攻撃者をだまして、攻撃を続けさせる機能がある。特定の実施の形態では、REST APIノード106は、次のように構成される。

【0043】

（1）攻撃者から要求を受信して解釈し、要求されたアクションを実行するまたは実行するフリをする。これらのアクションは、攻撃者が要求するように正しいリソースを設置する（たとえば、データベース、コンピュータ、コンテナなどをスピンアップする）ことを含み得る。

【0044】

（2）エラー処理の実行を含む、応答を攻撃者に提供し、本物の、ダミーではないインスタンスにアクセスしたと攻撃者に信じ込ませる。

【0045】

要求を解釈してリソースを設置することに関して、サブスクリプション要求に応じてリソースをプロビジョニングするための技術を用いてインスタンスを設置してもよい。特定の実施の形態では、REST APIノード106は、どのリソースを攻撃者が要求しているのかを、サービスプロバイダが用いるプロビジョニング技術に基づいて判断する。いくつかのその他の実施の形態では、Regex（正規表現）スクリプトおよび／またはNLP（自然言語処理）をキャッシュした辞書（たとえば、適切なwebhookの利用）などの技術を用いて攻撃者からのCLI GET要求に対処してもよい。

【0046】

攻撃者が本物のIaaSインスタンスにアクセスしたと信じ込むように導かれるような適切な応答を提供するために、ハニーネットによって様々な技術が用いられてもよい。場合によっては、要求されたアクション（複数可）を実際に行うことなく、要求に対する適切な応答がハニーネットによって生成されて攻撃者に提供されてもよい。いくつかの実施の形態では、ハニーネットは、攻撃者が選んだCLIツールから通信する、POST要求を予めロードしていてもよい。こうする方法の1つに、適切な条件が成立すると攻撃者に自動的に返信される応答と、要求とを有するNLP辞書を設置して利用するなど、NLP（自然言語処理）テクノロジーを用いる方法がある。これに対処できる様々な方法が

10

20

30

40

50

あり、たとえば、文字列解析を用いてどのような要求がされているのかを理解した後に辞書からの適切な応答を決定する方法がある。

【0047】

特定の実施の形態では、図1および図2に示すように、クライアントから追加情報を手に入れてダミーVPC（仮想プライベートクラウド）に設置されたサーバに機密保護および匿名性を提供できる流れの一部として、（図1の）リバースプロキシ112（図2の212）がオプションで設けられてもよい。リバースプロキシ112は、攻撃者または攻撃者が用いたクライアントデバイスの属性を記録するように構成され得る。リバースプロキシ112は、攻撃者がスピンアップしているリソースのプライバシーと機密保護の壁としても機能する。たとえば、攻撃者は、データベースまたはコンピュータもしくはネットワークリソースをスピンアップする場合があります、これらのリソースの識別情報を匿名化するためにリバースプロキシ112が使われてもよい。リバースプロキシノード112は、インスタンス102の匿名性を保持し、これらのインスタンスの本当の識別情報を攻撃者が絶対に分からないようにする。

10

【0048】

攻撃者がやり取りするIaaSインスタンス102のリソースを、コンピューティングリソース、ストレージリソース、およびメモリリソースに限定してもよく、少数の基本的な機能を提供してもよい。攻撃者がアクセスするIaaSサービス／オブジェクトは、IaaSインスタンスの「完全性」を維持するために必要な正しい応答を提供する。

【0049】

20

ステップ2B：攻撃者は、「本物の」ユーザ（GUIモード）である

場合によっては、攻撃者は、たとえばIaaSインスタンスへのアクセスを開始するために他のGUIアプリケーションのブラウザを使用して、たとえば攻撃者のクライアントシステム上で実行されているアプリケーションを介して攻撃を指揮している本物のユーザであり得る。GUIモードの攻撃に関する要求および応答に対処するためのシステム200を図2に示す。

【0050】

GUIモードのための処理は、CLIモードのための処理と非常に似ている。GUIモードでは、攻撃者は、偽のブラウザGUI204を用いて攻撃を開始して、要求を送る場合がある。コンソール（たとえば、クライアントデバイス）およびGUIアプリケーションとの攻撃者のやり取りは、図2のログノード210（図1のノード108）によって記録できる。たとえば、ユーザ／攻撃者のログイン、ブラウザとの攻撃者のやり取り（たとえば、攻撃者がどのリンクをクリックしたか、一連のクリックなど）についてのデータを記録できる。特定の実施の形態では、攻撃者がどのようにGUIコンソールとやり取りしているかについてのデータを収集するための非同期のONイベントリスナー210が利用されてもよい。この収集データを用いて、攻撃者がバックエンドで行っている決定的なアクションがより理解できるだけでなく、コンソール自体の上でどのようなアクションが発生しているのかをより理解できるようになる。

30

【0051】

ステップ2C：エラー処理

40

特定の実施の形態では、IaaSハニーネットAPIコントロール&コマンドサーバは、API GET要求が不正確にフォーマットされない限り、および／または出力型が誤りでない限り、攻撃者にすべてステータス：200という応答を提供する。フォーマットが不正確であった場合および／またはデータ型が誤りであった場合、REST APIノード206は、攻撃者に適正なエラー処理コードを送る。

【0052】

ステップ3：Verboseモードでのログ記録

図1および図2に示すように、特定の実施の形態では、別個のログノード（図1の108および図2の208）を設置して、ハニーネットが提供するハニーネットのIaaSインスタンスにおいてアクセスされるすべてのイベント／リソース／オブジェクト、および

50

攻撃者がアクセスするすべてのイベント／リソース／オブジェクトを記録してもよい。ログ記録は、時系列に実行され得る。

【0053】

ステップ4：E T L／機械学習パイプライン、ネイティブ脅威インテリジェンスフィードなど

特定の実施の形態では、ログノード1108、208またはサーバは、すべての攻撃者のやり取りを格納する。データは、R A Wや、c s vなど、様々なフォーマットで格納され得る。ログに記録されたデータは、解析のために定期的にアナリティクスプラットフォームにエクスポートされ得る。たとえば、毎日のc r o nジョブを用いて、ログに記録されたデータを将来の訓練のためにE T L（抽出、変換、ロード）／機械学習パイプラインにアップロードしてもよい。ログサーバは、セキュリティ監視、検出、および防止プログラムが使用する内部のブラックリストに直接入力されるネイティブ脅威インテリジェンスフィードのために、攻撃者に一意のコア属性を提供して、I a a Sハニーネットを以前攻撃したことの行為者周辺の今後の脅威に備える。

10

【0054】

ハニーネットが設置したダミーI a a Sインスタンスが利用可能になるリソースの量は、攻撃者をおびき寄せて攻撃者のアクティビティ情報を取得するための許容できるコストに基づいて決定され得る。いくつかの実施の形態では、限られた量のコンピューティングリソース、ストレージリソース、およびネットワークリソースが割り当てられてもよい。たとえば、固定の限られた量のコンピューティングリソース、ストレージリソース、およびネットワークリソースを各々が有する、予めでっち上げた特定の数の画像を提供してもよく、これらの予めでっち上げた画像を使用して、攻撃者が要求したI a a Sインスタンスを設置し、攻撃者が要求したアクションを実行してもよい。これらの予めでっち上げた仮想化された画像またはコンテナ化された画像は、予め設定された制約を超えて展開しないよう、ハードコーディングされてもよい。

20

【0055】

ハニーネットは、攻撃者をそそのかして接続を行わせてハニーネットとのセッションを設置させ、本物の／正規リソースを攻撃しており、所望の悪意のある行為を行っていることを攻撃者に信じ込ませて、さらに悪い行為を行うようにさらにそそのかす。どこかの時点で、ハニーネットは、攻撃者の行為を止めて攻撃者のハニーネットとのセッションを遮断すると判断してもよい。場合によっては、たとえば、攻撃者ならびに攻撃者のハニーネットおよびダミーインスタンスとのやり取りについての十分なデータが記録されたことをハニーネットが確認したときに、この時点に達し得る。いくつかのその他の場合、この時点は、時間に基づく時点であってもよい。たとえば、攻撃者のダミーインスタンスおよびハニーネットとのセッションの期間が予め設定された時間しきい値を満たすまたは超えた場合、ハニーネットは、この時点に達したと判断してもよい。様々なその他の要因も利用して、攻撃者を「遮断」するタイミングを判断してもよい。別の実施の形態では、前述の要因とその他の要因との組合せも使われてもよい。

30

【0056】

例示的な実施の形態#2

40

I a a Sインスタンスは、コンピューティングサービス、ストレージサービス、およびネットワークサービスを提供するために処理リソース（たとえば、コア、プロセッサ）と、ストレージリソース（たとえば、メモリリソース）と、ネットワークリソースとが束ねられた構成を含む。I a a Sクラウドインスタンスは、最下層で（メモリ、コンピューティング、およびリソース層で）クラウドの仮想化を提供する。I a a Sクラウドは、ネットワーク機能と絡めて提供されるコンピューティング機能およびストレージ機能に関するサービス製品を提供する。S a a S／P a a Sインスタンスへの攻撃は、コンピューティングリソース／メモリリソース／ネットワークリソースを攻撃するのではなく、S a a S／P a a Sアプリケーションが使用するデータを対象とした攻撃であるため、I a a Sインスタンスへの攻撃は、S a a SインスタンスやP a a Sインスタンスへの攻撃とは非常

50

に異なる。IaaSの場合、いくつかのリソースが関係する可能性があり、これらのリソースの構成は理解するのが難しいため、IaaS攻撃を防ぐための既存のソリューションが不足している。IaaSリソースを監視してこれらのリソースに対する攻撃を特定することは、非常に難しい。その理由は、非常に多くの移動を伴うパーツがあり、その各々が独自の構成を有しており、色々な事が非常に簡単に見逃されてしまうためである。その結果、いくつかのIaaS攻撃がまったく気づかれぬまま進行してしまう。

【0057】

図3は、特定の実施の形態に係る、1つ以上のハニーポットを備えるハニーネットを組み込んだ分散環境300の簡略ブロック図である。図3に示すように、分散環境300は、クラウドサービスプロバイダのデータセンター302を備える。ここで、クラウドサービスプロバイダは、IaaS、PaaS、SaaS、およびその他のクラウドサービスのうち1つ以上を提供し得る。これらのサービスは、1つ以上の本物のサービスインスタンス304を用いて提供され得る。ここでは、「本物」という用語は、これらのインスタンスを、ハニーネットが提供する「ダミー」インスタンスと区別するために使われている。本物のサービスインスタンスは、1つ以上のIaaSサービスを提供する1つ以上の本物のIaaSインスタンス（たとえば、R-IaaS#1）と、1つ以上のPaaSサービスを提供する1つ以上の本物のPaaSインスタンス（たとえば、R-PaaS#1）と、1つ以上のSaaSサービスを提供する1つ以上の本物のSaaSインスタンス（たとえば、R-SaaS#1）とを含み得る。これらの本物のクラウドサービスを提供するためのインフラストラクチャは、クラウドサービスプロバイダによって提供される。たとえば、インフラストラクチャは、データセンター302によって提供されてもよい。顧客またはテナントは、データセンター302を利用するクラウドサービスプロバイダが提供するクラウドサービスのうち1つ以上にサブスクライブできる。

【0058】

図3に示す分散環境300は、一例に過ぎず、クレームされた実施の形態の範囲を必要以上に限定しない。当業者であれば、数多くのバリエーション、別の選択肢、および変更が可能であることが分かるであろう。たとえば、別の実施の形態では、分散環境300は、図3に示すシステムまたは構成要素よりも多い数のシステムまたは構成要素を有してもよく、少ない数のシステムまたは構成要素を有してもよく、2つ以上のシステムを組み合わせてもよく、システムの構成または配置が異なってもよい。図3に示すデータセンター302の構成は、一例に過ぎず、限定ではない。簡略化のために図3には1つのデータセンター302しか示されていないが、一般的な分散環境は、場合によっては、それぞれ異なる地理的な場所に複数のデータセンターを備えることができる。複数のデータセンターは、1つ以上の通信ネットワークを経由して互いに通信可能に連結され得る。通信ネットワークは、インターネット、WAN（ワイドエリアネットワーク）、LAN（ローカルエリアネットワーク）、Ethernet（登録商標）ネットワーク、パブリックもしくはプライベートネットワーク、有線ネットワーク、ワイヤレスネットワークなど、および／またはそれらの組合せなど、様々な種類の通信ネットワークで有り得る。IEEE802.XXスイートのプロトコル、TCP/IP、IPX、SAN、AppleTalk（登録商標）、Bluetooth（登録商標）、およびその他のプロトコルなど、有線プロトコルならびにワイヤレスプロトコルの両方を含む、それぞれ異なる通信プロトコルを用いて、通信を容易にするであろう。

【0059】

データセンター302が提供するリソースに攻撃を行い、悪意を持って不正利用する攻撃者には、それぞれ異なる特徴がある。正式な認可なくデータセンター302に接続しようと試みるまたはデータセンター302が提供するリソースを利用しようと試みるエンティティは、攻撃者とみなされる。たとえば、データセンター302が提供するリソースにダミークレデンシャルを用いてアクセスして利用するエンティティは、攻撃者とみなされる。

【0060】

攻撃者には、自動ボットである攻撃者や人間のユーザである攻撃者を含む、様々な形態がある。図3に示す例では、クライアントデバイス310上で動作する自動ボット308は、データセンター302が提供するリソースを攻撃して不正利用するように試み得る。自動ボット308は、データセンター302内のエンドポイントノードを傍受して接続する方法を探した後、その接続を用いてデータセンター302が提供するリソースを利用するように構成され得る。また、攻撃は、クライアントデバイス316上で動作しているアプリケーションまたはソフトウェア（たとえば、GUIブラウザ314）を用いて、データセンター302が提供するリソースを攻撃して不正利用する人間のユーザ312からも発信され得る。攻撃自体は、C L I（コマンドラインインターフェース）メカニズム、G U Iベースのメカニズムなど、それぞれ異なるメカニズムを用いて行われ得る。

10

【0061】

攻撃者（たとえば、ボットまたは人間のユーザ）がハッキングするまたは悪意を用いて利用するリソースは、データセンター302が提供する本物のインスタンス304のうち1つ以上を含んでもよい。たとえば、攻撃者は、データセンター302が提供する本物のIaaSインスタンスに接続してその本物のIaaSインスタンスが提供するコンピューティングリソースもしくはサービス、ストレージリソースもしくはサービス、および／またはネットワークリソースもしくはサービスの不正利用を試み得る。たとえば、攻撃者は、本物のIaaSインスタンスに接続して、その本物のIaaSインスタンスを使用して、大量のコンピューティングリソース、ストレージリソース、およびネットワークリソースを必要とする暗号通貨のマイニング操作（たとえば、ビットコインのマイニング）を行うためにコンピューティングリソース、メモリリソース、およびネットワークリソースを「盗む」可能性がある。

20

【0062】

図3に示すように、データセンター302は、ハニーネット306を提供する。ハニーネット306は、このような攻撃者をおびき寄せて、データセンター302の本物のリソース（たとえば、本物のインスタンス）を危険に晒すことなく、攻撃者についてのデータを収集するように構成される。ハニーネット306は、ハニーポットサーバ（または、ハニーポット）から構成されるネットワークを含む、様々な構成要素を備える。各ハニーポットは、特定の一連のIaaSリソースへのアクセスを提供する特定のIaaSサービスインスタンスを表し得る。各ハニーポットは、攻撃者をだまして、本物のIaaSインスタンスへのアクセスを正常に取得できたと信じ込ませるように構成される。それぞれ異なる種類のIaaSサービスにそれぞれ異なるハニーポット318、320、322などが提供されてもよい。図3に示す実施の形態では、1つのハニーネットしか図示されていないが、これは限定ではない。データセンターが1つ以上のハニーネットを提供してもよい。

30

【0063】

図3に示す実施の形態では、ハニーネット306は、ログサーバ330も備える。ログサーバ330は、ハニーポットが記録した攻撃についてのデータを受信したり収集したりするように構成される。そして、収集されたデータは、その後の解析のために不揮発性メモリに格納される。図3に示す実施の形態など、いくつかの実施の形態では、ハニーネット306自体がアナリティクスプラットフォームまたはサーバ332を備える。アナリティクスプラットフォームまたはサーバ332は、ハニーポットが収集したデータおよびログサーバ330がログに記録したデータを解析するように構成される。いくつかのその他の実施の形態では、データセンター302のレベルでアナリティクスプラットフォーム332が提供されてもよい。このようなアナリティクスプラットフォームは、データセンター302が提供する1つ以上のハニーネットが収集したデータを受信して解析するために用いられ得る。場合によっては、アナリティクスプラットフォームは、データセンター302から遠隔の場所に位置してもよい。このような場合、ログサーバ330は、データセンター302の通信インターフェース344を用いて、データセンター302のハニーネット306が収集したデータを遠隔のアナリティクスプラットフォームに通信するように

40

50

構成されてもよい。

【0064】

特定の実施の形態では、ハニーネット306のハニーポットが使用するために、特定の一連の利用可能なリソース324を取っていてもよい。利用可能なリソース324は、コンピューティングリソース（たとえば、コア、プロセッサ）、ストレージリソース（たとえば、メモリ）、ネットワークリソース、データベースリソース、コンテナなどを含み得る。ハニーポットは、利用可能なリソース324に含まれるリソースを用いて、攻撃者をだまして本物のIaaSインスタンスに接続して利用していると信じ込ませるダミーIaaSインスタンスをスピンアップしてもよい。いくつかの実施の形態では、利用可能なリソース324に含まれるリソースは、リソースの束（「ポッド」と呼ばれる）に予めパッケージ化されていてもよく、束の各々は、予め設定された構成の特定のコンピューティングリソース、メモリリソース、およびネットワークリソースから構成される。そして、これらの予めパッケージ化された束またはポッドのうち1つ以上を使用して、ハニーポットがダミーIaaSインスタンスをスピンアップしてもよい。

10

【0065】

データセンター302は、図3に示すデータセンター302の様々なサービスおよび構成要素を提供するためのインフラストラクチャを提供する1つ以上のホストマシン（たとえば、コンピュータシステム）を提供してもよい。ホストマシンを用いて、本物のインスタンス304、1つ以上のハニーネット306およびそれらの構成要素、ならびに図3に示すデータセンター302の様々なその他のサーバおよび構成要素が提供されてもよい。たとえば、ハニーネット306に含まれるハニーポットがデータセンター302の1つ以上のホストマシン間でデプロイされてもよい。

20

【0066】

特定の実施の形態では、ハニーネットは、セキュリティ上の理由から、本物のインスタンスから隔離されて分離されている。したがって、ハニーネットを提供するために使われるデータセンター302のインフラストラクチャは、本物のインスタンス304をサポートするために使われるインフラストラクチャと分けられている。たとえば、ハニーネット306を実行およびサポートするために使われるホストマシンは、データセンター302にあるその他のホストマシンから分離されてもよい。

【0067】

ハニーネット306に攻撃者をおびき寄せるために様々な異なる技術が用いられる。自動ポットおよび人間の攻撃者を含む攻撃者は、一般的に、SSHポート22およびFTPポート21を探して、これらのポートの脆弱性を利用して攻撃を行う。図3に示す実施の形態では、攻撃者をおびき寄せるためにおりサーバまたはおりノード336が利用される。おりサーバ336は、SSHポート22およびFTPポート21など、データセンター302の1つ以上のポートで公然と情報を同報通信して、攻撃者の注目をこれらのポートに向けるように構成される。攻撃者がこれらのポートのうち1つに接続すると、ダミーまたは偽のクレデンシャル338が、攻撃者がアクセスできるよう、都合よく置かれている。いくつかの実施の形態では、おりサーバ336は、クレデンシャルが誤って同報通信されたかのように見せながら、ダミークレデンシャル338についての情報を同報通信し得る。ダミークレデンシャル338は、ダミーのユーザ名／パスワード情報、API鍵、MACアドレス、証明書、テナント識別子、パスワードなど、ダミーの制限付き情報を含み得る。この目的は、データセンター302が提供するリソースを攻撃するために使える本物のクレデンシャルを取得したと攻撃者に信じ込ませることである。特定の実施の形態では、ダミークレデンシャルとして、いくつかのデフォルトクレデンシャルが置かれていてもよい。場合によっては、攻撃者がダミークレデンシャル338にアクセスするためにAPI呼び出し（たとえば、GET cred）を送った後、そのAPI呼び出しに対する応答としてダミークレデンシャルが送られる。API呼び出しの対処は、APIゲートウェイサーバ340によって行われ得る。

30

40

【0068】

50

たとえば、一般的なシナリオでは、データセンター 302 を利用してクラウドサービスプロバイダが提供するサービスに正規にサブスクライブしているエンティティ（テナント）の場合、サブスクリプションの時点で（またはその後）、テナントには、そのテナント用にカスタマイズされた 1 つ以上のクレデンシャルが提供される。これらのクレデンシャルによって、テナントは、データセンター 302 にログインして、サブスクライブしているサービスを提供している本物のインスタンス（たとえば、特定の種類の IaaS サービスを提供している本物の IaaS インスタンス）とのセッションを設置することが可能になる。セッションの設置時、テナントは、クレデンシャルを要求される。その後、当該クレデンシャルは、テナントを認証するために使われる。テナントがサブスクライブするサービスを提供する本物のインスタンスが正常に認証されると、テナントのためにセッションが設置される。

10

【0069】

また、ダミークレデンシャルは、攻撃者がセッションを設置することを可能にするが、正規テナントのセッションとは異なり、ダミークレデンシャルを用いて攻撃者のためにハニーネット 306 とのセッションを設置する。ハニーネットに含まれるハニーポットとのセッションを設置してもよく、ハニーポットがスピンアップしたダミー IaaS インスタンスとのセッションを設置してもよい。

【0070】

ダミーへのアクセスを得ると、攻撃者は、インスタンスのセッションを設置する要求と、セッション中に 1 つ以上のアクションを実行する後続する要求とをデータセンター 302 に送ることができる。これらの要求は、攻撃者が行った API 呼び出しの形式であってもよい。図 3 に示す実施の形態では、これらの API 要求は、API ゲートウェイサーバ 340 によって受信されて処理される。API ゲートウェイサーバ 340 は、要求を読み出し、場合によっては要求を認証し、その後、要求を処理するためにデータセンター 302 のバックエンドコンポーネントに転送するように構成され得る。

20

【0071】

たとえば、図 3 に示す実施の形態では、データセンター 302 の特定のポートに自動ポットをおびき寄せて、当該ポートを用いてダミークレデンシャル 338 にアクセスさせてもよい。そして、自動ポット 308 は、攻撃者のためにセッションを設置するよう要求する、取得したダミークレデンシャルを用いて、データセンター 302 に要求を送信する。要求は、API ゲートウェイサーバ 340 によって受信されて処理され、データセンター 302 の正規テナントからの要求ではなく攻撃者からの要求であると判断されると、対処のためにハニーネット 306 に転送される。特定の実施の形態では、攻撃者の要求の API 呼び出しにおいて要求される特定の種類の IaaS サービスを提供するように構成された、ハニーネット 306 の特定のハニーポットに要求が転送されてもよい。

30

【0072】

正規テナントが行う API 呼び出しは、攻撃者が行う API 呼び出しと同じである。API 呼び出し、および API 呼び出しによって受信した情報に基づいて、要求に対処のために適切なバックエンドコンポーネントに転送できるよう、API ゲートウェイサーバ 340 は、正規テナントからの要求であるのか、攻撃者からの要求であるのかを判断しなければならない。API ゲートウェイサーバ 340 は、以下のような異なる方法を用いてこの特定を行ってもよい。

40

【0073】

(1) セッションを設置するよう要求する API 呼び出しの場合、API 呼び出しは、通常、セッションを設置する前に要求側を認証するために使われるクレデンシャル（たとえば、ユーザ名／パスワード）も含んでいる。これらのクレデンシャルがダミークレデンシャルであると判断した場合、API ゲートウェイサーバ 340 は、攻撃者または悪質な行為者からの要求であることが分かっている。そして、API ゲートウェイサーバ 340 は、その要求をさらなる対処のためにハニーネット 306 の構成要素に転送する。

【0074】

50

(2) 攻撃者がログインしてダミー I a a S インスタンスとのセッションを設置できた後、セッション中の攻撃者および攻撃者の行為に関するデータが収集されて、ログが記録される。このログを記録したデータは、たとえば、攻撃要求を発信するために攻撃者が使用したデバイスについてのデバイスレベルの情報を含み得る。特定の場合、このデバイスレベルの情報は、A P I 呼び出し自体から特定できる。したがって、A P I ゲートウェイサーバ 3 4 0 が受信した A P I 呼び出しの場合、A P I 呼び出しに関するデバイスレベルの情報が、格納されている攻撃者のデバイスに関するデバイスレベルの情報（この情報は、攻撃者がデータセンター 3 0 2 とやり取りしている間に以前記録されたことがある可能性がある）と一致したと A P I ゲートウェイサーバ 3 4 0 が判断した後、A P I ゲートウェイサーバ 3 4 0 が、攻撃者からの A P I 呼び出しであると判断してその A P I 呼び出しを対処のためにハニーネット 3 0 6 の構成要素に転送する。

10

【0075】

(3) A P I ゲートウェイサーバ 3 4 0 は、要求を受信したポート番号に関する情報も用いて、攻撃者からの要求であるかどうかを判断してもよい。たとえば、先に説明したように、S S H ポート 2 2 および F T P ポート 2 1 などのポートは、一般的に、攻撃を指揮するために利用される。したがって、これらのポートを経由して受信された要求および A P I 呼び出しは、攻撃者からの要求としてタグ付けされてもよい。たとえば、特定の実施の形態では、接続のポートに基づいて、およびダミークレデンシャルに基づいて、A P I ゲートウェイサーバ 3 4 0 は、要求が正規の要求ではなく、悪質な行為者または攻撃者からの要求であると分かる。

20

【0076】

(4) 攻撃者からの要求を特定するために、上述した様々な情報の組合せを用いてもよい。

【0077】

攻撃者から発信された要求であると特定すると、A P I ゲートウェイサーバ 3 4 0 は、その要求を対処のためにハニーネット 3 0 6 の構成要素に転送する。特定の実施の形態では、攻撃者を特定すると、A P I ゲートウェイサーバ 3 4 0 は、ハニーネット 3 0 6 からの特定のハニーポットサーバとのセッションに攻撃者を接続して当該セッションを開く。たとえば、A P I ゲートウェイサーバ 3 4 0 は、要求で求められた I a a S サービスを提供するように構成された特定のハニーポットとのセッションを攻撃者のために設置した後、要求をさらなる対処のためにそのハニーポットに転送してもよい。

30

【0078】

攻撃者と特定のハニーポットとの間にセッションが確立された後、攻撃者は、I a a S インスタンスをスピンアップするさらなる要求および I a a S インスタンスが提供するリソースを使用するさらなる要求を送信できるようになる。特定の実施の形態では、ハニーポットは、ダミー I a a S インスタンスをスピンアップしてもよい。たとえば、図 3 の H P 1 3 1 8 がスピンアップしたダミー I a a S インスタンス D - I a a S # 1 である。そして、ハニーポットは、要求された I a a S インスタンスが設置されて攻撃者が利用できる準備ができたことを示す応答を攻撃者に返してもよい。この応答は、正規の（ダミーではない）I a a S インスタンスがスピンアップされたと攻撃者を信じ込ませるような応答である。

40

【0079】

ダミー I a a S インスタンスがスピンアップされた後、セッション中、攻撃者は、スピンアップされた I a a S インスタンスに対応付けられたリソースを用いて様々なアクションを行う 1 つ以上の要求を送信する可能性がある。たとえば、攻撃者は、ダミー I a a S インスタンスが提供するコンピューティングリソース、ストレージリソース、およびネットワークリソースを利用して、ビットコインのマイニング操作などのアクションを実行する可能性がある。攻撃者がセッションを確立したハニーポットは、これらの要求を受信し、要求ごとに、要求を解釈して要求によって求められている 1 つ以上のアクションまたは操作を特定し、スピンアップされたダミー I a a S インスタンスを使用してこれらのアク

50

ションを実行し、アクションおよび要求に対応する応答を生成して攻撃者に送信するように構成される。生成される応答は、本物の I a a S インスタンスからの有効な応答である、スピニングされた I a a S インスタンスが提供するサービスおよびリソースを利用できた、と攻撃者が信じ込むように導かれるような応答である。

【0080】

特定の実施の形態では、ハニーポットは、ダミー I a a S インスタンスを実際に設定したりスピニングしたりしないで、要求されたアクションおよび攻撃者から受信した A P I 呼び出しに対応する適切な応答を生成して攻撃者に送信できる。たとえば、ハニーポットは、応答を生成するために、一連のルールを用いてしてもよい。当該一連のルールは、攻撃者が要求できる一連のあり得るアクションと、アクションごとの適切な 1 つ以上の応答とを識別するマッピングを含み得る。攻撃者から要求を受信すると、ハニーポットは、要求を 1 つ以上のアクションに変換した後、このマッピングを用いて、1 つ以上のアクションに対する 1 つ以上の応答を決定し得る。そして、当該 1 つ以上の応答は、受信した要求に応じて攻撃者に返され得る。ハニーポットによって生成される応答は、ダミー I a a S インスタンスでさえスピニングされていないにも関わらず、I a a S インスタンスをスピニングできた、そしてスピニングした I a a S インスタンスが提供するサービスおよびリソースを利用できた、と攻撃者が信じ込むように導かれるような応答である。ルール情報（たとえば、マッピング情報）は、データベース内など、ハニーポットがアクセスできる不揮発性メモリに格納されてもよい。

【0081】

特定の実施の形態では、攻撃者から受信した要求に対する応答を生成するために、ダミー I a a S インスタンスと一連のルールとの組合せがハニーポットによって利用され得る。1 つのこのような実施の形態では、ハニーポットは、スピニングされたダミー I a a S インスタンスに基づいて、アクションと応答との新しいマッピングなど、新しいルールを学習可能である。たとえば、ハニーポットは、ダミー I a a S インスタンスを使用する攻撃者から受信した特定の要求されたアクションに対する応答を学習した後、新しいアクションと応答とのマッピング項目をルール情報に追加してもよい。その後同じアクションが要求された場合、そのアクションに対する適切な応答を生成するために、I a a S インスタンスではなく、ルール情報を使用する。ルール情報マッピングを学習し、構築し、増やすために、1 つ以上の機械学習技術を利用してもよい。

【0082】

要求を処理することに加えて、ハニーポットは、攻撃者および攻撃者の行為ならびにハニーポットとのやり取りについてのデータを収集および記録するように構成される。記録された攻撃者のデータは、攻撃者の行為（たとえば、脅威の行為者のユーザ挙動パターン、ユーザに一意のその他の属性）、特定の攻撃者の接続属性およびデバイスレベルの属性（たとえば、接続情報、攻撃者が利用したデバイスの I P アドレス、A S N (A u t o n o m o u s S y s t e m N u m b e r) トレースルート情報、ドメイン名など）など攻撃者についての一意の属性、および攻撃に関するその他のデータを含み得る。記録されたデータは、攻撃者の一連の行為についてのデータ、攻撃者のハニーポットとのセッション中に攻撃者がアクセスしたオブジェクト、攻撃者が行った A P I 呼び出し（たとえば、攻撃者が行った R E S T A P I 呼び出し）などを含み得る。ログに記録されたデータは、攻撃者から受信した A P I 要求についての情報、ハニーポットが A P I 要求に応じて生成して送信した応答、要求の送信元の I P アドレス、データセンターに接続するために攻撃者が使用したポート番号、J a v a S c r i p t（登録商標）の o n イベント（G U I ベースのやり取りについての。たとえば、クライアントデバイス上のブラウザベースのイベントが監視されてもよい）、デバイスレベルの情報、要求の間隔などを含み得る。

【0083】

特定の実施の形態では、ハニーネット 306 などのハニーネットは、ログサーバ 330 を備えてもよい。ログサーバ 330 は、ハニーネット 306 に含まれるハニーポットが収集したデータを収集するおよび／または受信するように構成される。このような実施の形

態では、個々のハニーポットが収集したデータがログサーバ330に転送されてもよい。ログサーバ330は、データを正しいフォーマットで格納するように構成される。このデータは、ログサーバ330がアクセスできる不揮発性メモリに格納されてもよい。また、ログサーバ330は、収集データにアクセスするためのコントローラとして機能してもよい。

【0084】

特定の実施の形態では、ハニーネット306は、アナリティクスサブシステム332を備えてもよい。アナリティクスサブシステム332は、ハニーネット306に含まれるハニーポットが収集したデータを解析するように構成される。収集データを解析して、攻撃者の動機（たとえば、攻撃する目的および意図）、攻撃パターン、攻撃メカニズム、（接
10 続性（たとえば、IPアドレス、ドメインなど）の観点、地理的観点からの）攻撃開始地点、異なるタイプの攻撃、攻撃中に攻撃者がアクセスしたリソースおよびオブジェクト、攻撃者が何を攻撃しているのか、どのリソースが利用されたのか、どのようにリソースが利用されたのか、攻撃中に実行された操作、攻撃の頻度プロファイルなどについての洞察を得ることができるであろう。特定の実施の形態では、解析に基づいて、攻撃者および攻撃を特定するためのプロファイルを生成する。その後、これらのプロファイルは、攻撃が発生する前に未然に防ぐために使われてもよい。

【0085】

特定の実施の形態では、ハニーネットレベルにアナリティクスプラットフォームを有する代わりに、またはハニーネットレベルのアナリティクスプラットフォームに加えて、データセンター302によって解析プラットフォームが提供されてもよい。このような実施
20 の形態では、データセンター302において1つ以上のハニーネットが収集したデータを解析のためにこのアナリティクスプラットフォームに転送してもよい。特定の実施の形態では、アナリティクスプラットフォームは、データセンター302から遠隔のコンピューティングプラットフォームによって提供されてもよい。このような遠隔のアナリティクスプラットフォームは、1つ以上のデータセンター間に散在する複数のハニーネットが収集したデータを収集および／または受信し、データを集約した後、集約したデータを解析するように構成されてもよい。

【0086】

ハニーネットが収集したデータを解析するために、様々な異なる技術が用いられてもよい。特定の実施の形態では、ML（機械学習）技術が用いられてもよい。ハニーネットが
30 収集したデータは、訓練データとして提供されて、収集データに含まれる様々な基準に基づいて攻撃者および攻撃を特定するためのモデルを構築して訓練するために使われてもよい。そして、このようなモデルは、攻撃者および攻撃を事前に特定し、好ましくは、このような攻撃が発生する前に止めるために使用できる。

【0087】

特定の実施の形態では、収集データを処理するために、ビッグデータパイプラインが設けられてもよい。たとえば、ハニーネットが収集したデータを受信して処理するためのH
a d o o pまたはデータレイクプラットフォームが設けられてもよい。

【0088】

図3に示す実施の形態では、プロキシサーバーの背後にあるデータセンター302のサーバおよびその他の構成要素の機密保護および匿名性を提供するために、リバースプロキシサーバー342が設けられる。リバースプロキシは、クライアントとクライアント（ク
40 ライアント310と316など）との間に存在し、プロキシの背後にあるサーバを匿名化する。クライアントは、どのサーバに接続されるかを知らない。リバースプロキシサーバーによって、負荷分散、キャッシュ、内部トラフィックの隔離、ログ記録など、いくつものメリットがもたらされる。また、リバースプロキシサーバー342は、攻撃者についての属性または攻撃者が用いたクライアントデバイスについての属性を記録するように構成されてもよい。リバースプロキシサーバー342は、攻撃者がスパインアップしているリソースのプライバシーと機密保護の壁として機能する。たとえば、攻撃者は、データベース
50

またはコンピュータもしくはネットワークリソースをスピンアップする場合があります、これらのリソースの識別情報を匿名化するためにリバースプロキシが使われてもよい。リバースプロキシは、インスタンスの匿名性を保持し、これらのインスタンスの本当の識別情報を攻撃者が絶対に分からないようにする。

【0089】

上述したように、ハニーポットは、攻撃者および攻撃者の行為についてのデータを収集しながら、攻撃者から受信した要求に応答するように構成される。どこかの時点で、ハニーポットは、攻撃者の行為を止めて攻撃者のセッションを遮断すると判断してもよい。ハニーポットは、様々な異なる要因、およびこれら要因の組合せを用いてこの決定を行ってもよい。要因の一部として、以下が挙げられる。

10

【0090】

(1) 時間しきい値－攻撃者のセッションの時間が予め設定された時間しきい値を満たすまたは超えた場合、ハニーポットは、ユーザのセッションを停止すると決定してもよい。

【0091】

(2) 間隔－攻撃者がハニーポットとのやり取りを止めた場合、一定の期間待機する。たとえば、攻撃者が関心を持っている間はセッションのアクティビティを続けさせることができる。一般に、ハニーポットによって多くのデータが収集されると、下流の解析に利用可能なデータが増える。

20

【0092】

(3) データ基準－場合によっては、攻撃者およびハニーポットとの攻撃者のやり取りについて十分なデータが記録されたと確認した場合、ハニーポットは、攻撃者のセッションを閉じると決定してもよい。

【0093】

(4) 攻撃者を「遮断」するタイミングを判断するために、様々なその他の要因も用いられてもよい。また、別の実施の形態では、前述の要因とその他の要因との組合せも用いられてもよい。

【0094】

特定の実施の形態では、攻撃者は、ハニーポットとの1つのセッションしか許可されなくてもよい。このような実施の形態では、続く2つ目のセッションを開くという攻撃者の試みは禁止される。いくつかのその他の実施の形態では、複数のセッションが平行して、または連続して許可されてもよい。このような実施の形態では、攻撃者についての情報は、セッション間で残り続けてもよい。

30

【0095】

特定の実施の形態では、1つ以上のハニーネットが提供する機能は、サブスクライブしている顧客に、クラウドサービスとして提供されてもよい。このようなサービスにサブスクライブすることによって、顧客は、自身のリソースに対する攻撃を事前に特定できるようになる。

【0096】

図4は、特定の実施の形態に係る、ハニーポットサーバ400の簡略ブロック図である。ハニーポットサーバ400（ハニーポット400とも称する）は、互いに通信可能に連結された複数のサブシステムを備えてもよい。図4に示す実施の形態では、ハニーポット400のサブシステムは、要求解釈サブシステム406と、応答生成サブシステム408と、通信インターフェースサブシステム412と、記録サブシステム414とを備える。これらのサブシステムは、ソフトウェアのみで実現されてもよく（たとえば、1つ以上のプロセッサによって実行可能なプログラム、コード、または命令）、ハードウェアで実現されてもよく、または、それらの組合せで実現されてもよい。図4に示すハニーポット400は、一例に過ぎず、クレームされた実施の形態の範囲を必要以上に限定しない。当業者であれば、数多くのバリエーション、別の選択肢、および変更が可能であることが分かるであろう。たとえば、いくつかの実施態様では、ハニーポット400は、図4に示す構

40

50

成要素よりも多い数のサブシステムまたは構成要素を有してもよく、少ない数のサブシステムまたは構成要素を有してもよく、2つ以上のシステムを組み合わせてもよく、システムの構成または配置が異なってもよい。

【0097】

要求解釈サブシステム406は、攻撃者から要求を受信して解釈するように構成される。たとえば、特定の実施の形態では、攻撃者からの要求またはAPI呼び出しであると判断すると、APIゲートウェイサーバ340は、（たとえば、図3に示すような）ハニーネット306から特定のハニーポットを選択し、選択したハニーポットに要求を転送する。ハニーポットでは、要求は、要求解釈サブシステム406によって受信される。要求を受信すると、要求解釈サブシステム406は、要求を解釈し、要求に対応して実行する一連の1つ以上のアクションを決定するように構成される。当該1つ以上のアクションは、たとえば、IaaSインスタンスを設置またはスピンアップするためのアクション、IaaSインスタンスが提供する1つ以上のリソースを利用するためのアクションなどを含み得る。

10

【0098】

アクションにIaaSインスタンスのスピンアップが含まれる場合、要求解釈サブシステム406は、利用可能なリソース404のうち1つ以上のリソースを使用して、ダミーIaaSインスタンス416を設置してもよい。ダミーIaaSインスタンス416は、1つ以上のコンピューティングリソース（たとえば、プロセッサ、コアなど、処理リソース）、1つ以上の（たとえば、メモリリソースを提供する）ストレージリソース、1つ以上のネットワークリソース、およびダミーIaaSインスタンス416が提供するその他のリソースの利用を可能にするサービスを提供してもよい。たとえば、実行されるアクションがダミーIaaSインスタンス416が提供するリソースの利用に相当する場合、要求解釈サブシステム406は、攻撃者の要求を満たすためにこのリソースを攻撃者に使わせてもよい。特定の場合、要求解釈サブシステム406は、攻撃者が要求したアクションをダミーIaaSインスタンス416に適用してもよい。ハニーポット400は、1つ以上のダミーIaaSインスタンスをスピンアップして利用するように構成されてもよい。

20

【0099】

応答生成サブシステム408は、攻撃者から受信した要求に対するダミー応答を生成するように構成される。応答生成サブシステム408が生成するダミー応答は、応答が有効であり、有効なIaaSインスタンスによって生成されたと攻撃者が信じ込むように導かれるような応答である。これにより、悪質な行為者または悪意のあるユーザであると検出されていると不安になることなく攻撃者に行為を継続させる。

30

【0100】

アクションと応答との間には、1対1の関係、1対多の関係、または多対1の関係が存在し得る。1対1の関係によると、各アクションには、それ自体の応答があり得る。1対多の関係によると、アクションには、複数の関連する応答があり得る。多対1の関係によると、複数のアクションに対して1つの応答が生成および送信され得る。応答生成サブシステム408は、受信した攻撃者の要求に対して適切な応答を生成する役割を担う。

【0101】

応答生成サブシステム408は、応答を生成するために、様々な技術を用いてもよい。1つの技術によると、要求解釈サブシステム406は、実行されるアクションをダミーIaaSインスタンス416に適用してもよい。そして、ダミーIaaSインスタンス416は、対応する応答を応答生成サブシステム408に送信してもよい。そして、応答生成サブシステム408は、要求に対する応答として、ダミーIaaSインスタンス416から受信した応答を転送してもよい。場合によっては、応答生成サブシステム408は、ダミーIaaSインスタンス416から受信した応答をフォーマットまたは修正して、攻撃者に通信される応答を生成してもよい。

40

【0102】

第2の技術によると、応答生成サブシステム408は、攻撃者の要求に対する応答を、

50

一連のルール 4 1 8 を用いて、ダミー I a a S インスタンス 4 1 6 を用いることなく生成してもよい。このような実施の形態では、ダミー I a a S インスタンスは、ハニーポット 4 0 0 によってインスタンス化されることすらなくてもよい。ルール情報 4 1 8 は、ハニーポット 4 0 0 がアクセスできる、データベースなど、不揮発性メモリ 4 0 2 に格納されてもよい。一連のルール 4 1 8 は、攻撃者が要求できるアクションとそれに対応する応答とのマッピングを指定するマッピング情報を含んでもよい。アクションと応答との間の 1 対 1 の関係、1 対多の関係、または多対 1 の関係がマッピング情報に反映されてもよい。

【0 1 0 3】

攻撃者から要求を受信すると、要求解釈サブシステム 4 0 6 は、要求を解釈して、要求に対応して実行される 1 つ以上のアクションを特定する。そして、応答生成サブシステム 4 0 8 は、ルール 4 1 8 を検索して、要求されたアクションに対する適切な応答を特定し得る。そして、ルール 4 1 8 に基づいて特定された応答は、攻撃者の要求に対する応答として攻撃者に返され得る。ハニーポットによって生成される応答は、ダミー I a a S インスタンスがスピンアップされていないかもしれないにも関わらず、I a a S インスタンスをスピンアップできた、そしてスピンアップされた I a a S インスタンスが提供するサービスおよびリソースを利用できた、と攻撃者が信じ込むように導かれるような応答である。たとえば、ハニーポット 4 0 0 は、要求されたアクションが I a a S インスタンスをインスタンス化する（スピンアップする／設置する）ことである要求を攻撃者から受信する可能性がある。そして、応答生成サブシステム 4 0 8 は、ルール情報（たとえば、マッピング情報）を検索して、I a a S インスタンスを実際に設置しないで、この要求に対する適切な応答を見つけ得るが、応答は、要求された I a a S インスタンスが設置されたとしており、これにより、攻撃者をだまして、有効な I a a S インスタンスを設置できたと信じ込ませる。

【0 1 0 4】

攻撃者から要求を受信すると、要求解釈サブシステム 4 0 6 は、その要求を、実行される特定のアクションに変換し得る。そして、応答生成サブシステム 4 0 8 は、マッピング情報 4 1 8 を検索して、マッピング情報の中に、当該実行される特定のアクションに一致する項目を見つけ得る。応答生成サブシステム 4 0 8 は、この一致する項目を用いて、当該一致する項目に対応する応答を特定する、すなわち、アクションに対する応答を特定する。そして、特定された応答は、受信した要求に応じて攻撃者に応答を送るために使われる。

【0 1 0 5】

特定の実施の形態では、応答生成サブシステム 4 0 8 は、第 1 の技術（すなわち、ダミー I a a S インスタンスを使用すること）と、第 2 の技術（すなわち、ルール情報 4 1 8 を使用すること）との組合せを用いて、攻撃者から受信した要求に対する応答を生成してもよい。要求されたアクションを攻撃者から受信すると、応答生成サブシステム 4 0 8 は、第 1 の応答生成技術を利用するか第 2 の応答生成技術を利用するかを判断し、決定した技術を用いて、攻撃者に返す応答を生成してもよい。

【0 1 0 6】

いくつかの実施の形態では、応答生成サブシステム 4 0 8 は、機械学習ルールを用いてアクションと応答との新しいマッピングを学習し、この学習した情報を用いて当該マッピングをルール 4 1 8 に追加してもよい。そして、これらの学習したマッピングは、続く攻撃者から受信する要求に対する応答を生成するために使われてもよい。

【0 1 0 7】

記録サブシステム 4 1 4 は、攻撃者および攻撃者のハニーポット 4 0 0 とのやり取りに関するデータを記録するように構成される。また、記録サブシステム 4 1 4 は、要求に関する情報、および、要求に応じて応答生成サブシステム 4 0 8 によって生成されて攻撃者に返される対応する応答に関する情報を追跡および格納してもよい。記録サブシステム 4 1 4 は、記録されたデータを記録データ 4 2 0 として不揮発性メモリ 4 0 2 に格納するように構成されてもよい。また、いくつかの実施の形態では、記録データは、ハニーポット

400からその他のハニーポットなどの外部コンポーネント、ログサーバ330、またはデータセンター302から遠隔の場所（たとえば、遠隔のアナリティクスプラットフォーム）にも通信されてもよい。また、ハニーポットサーバ400が収集したデータは、集中収集サーバ（たとえば、ハニーネットログサーバ）に送られてもよい。そして、集中収集サーバは、当該データをその他のアナリティクスサブシステムに送り出してもよい。アナリティクスは、設備内（オンプレミス）に存在してもよく、どこか別の場所に存在してもよい。ハニーネットログサーバは、どのデータをアナリティクスに送信するかを決定でき、または、アナリティクスのためのインターフェースを提供してハニーネットログサーバからデータを引き出してもよい。特定の実施の形態では、通信インターフェース412は、ハニーポット400とのデータの通信を容易にするであろう。

10

【0108】

不揮発性メモリ402は、ハニーポット400がその動作を行うために用いるその他の情報422も格納してもよい。たとえば、その他の情報422は、ダミーIaaSインスタンスを設置するためにハニーポット400が使用できる作成済みのインスタンス（カスタマイズされた、IaaSリソースの「ポッド」の組合せ）に関する情報など、設定情報を含んでもよい。

【0109】

図5は、特定の実施の形態に係る、クラウドサービスプロバイダインフラストラクチャ502に接続されたハニーネット500の簡略ブロック図である。ハニーネット500は、仮想コンピューティングインスタンスであってもよく、および／または1つ以上の仮想マシンから構成されるクラスタであってもよい。上述した1つ以上の攻撃者501および／またはクラウドサービスプロバイダ502がパブリックネットワーク504によってハニーネット500にアクセス可能であってもよい。また、クラウドサービスプロバイダ502は、脅威解析システム506と通信していてもよい。脅威解析システム506は、収集された攻撃者についてのデータを解析して、収集データに基づいて推奨を行う、アラートを行う、および／または脅威を防ぐ決定をするように構成できる。

20

【0110】

いくつかの例では、一連のハニーポットエンドポイント（ハニーポットサーバ（または、ハニーポットのみ）S1～S3）をハニーネット500に設置できる。ハニーネット500では、各ハニーポットは、攻撃者が極めて悪質な行為を行うようにわざと設置されたエンドポイントノードである。ハニーネット500は、1つ以上のホストマシン上でデプロイされてもよい。セキュリティ上の理由で、（たとえば、図5に示すように）これらのホストマシンを残りのクラウドサービスプロバイダ502から隔離することができ、または、（たとえば、HP1～HP3がデータセンター302内に実装される図3に示すように）ホストマシンをクラウドサービスプロバイダ502内で隔離できる。ハニーポットS1～S3をデプロイおよび構成するため、およびローカル処理を実行するためにハニーネット管理システム508を設けることができる。3つの異なるハニーポットS1～S3を図5に示したが、ハニーネット500内に任意の数のハニーポットが実装されてもよい。さらに詳細は後述するが、ハニーポットS1～S3は、様々な形状（たとえば、種別）で実装されてもよい。

30

40

【0111】

ハニーネット500に異なる種別のハニーポットをデプロイして、異なる種類のサービスをエミュレートしてもよい。例として、SSH/TelnetサービスをエミュレートするためのSSHおよび／またはTelnetハニーポット、SMTP（たとえば、電子メールサーバ）、SSL、およびTLSをエミュレートするためのSMTPベースのハニーポット、HTTP（たとえば、ウェブサーバ）をエミュレートするためのHTTPハニーポット、ftp、rdp、https、httpsなどのサービスをエミュレートするための、たとえば、クレデンシャルを収集するためのその他のハニーポット、または、OracleのWebLogiCサーバ環境をエミュレートするためのWebLogiCハニーポットなどが挙げられる。このように、各々それぞれ異なるハニーポットが異なる種

50

類のサーバをエミュレートしてもよく、異なる形状を有してもよい。たとえば、サーバの形状が、このサーバにアクセスするために使われるAPI、ファイル構造などを規定してもよい。（たとえば、クラウドサービスプロバイダ502の）顧客507は、関心のあるハニーポットの形状／種別に基づいて、ハニーポットをデプロイするように要求した後、利用したい特定のハニーポットを決めて選択できる。この選択は、（たとえば、その種類のサービスに関する攻撃者データを収集するために）顧客が実行するサービスの種類に基づいてもよい。

【0112】

これらの様々な種別のハニーポットを実装することによって、異なるネットワークベースのIOC（セキュリティ侵害インジケータ）を収集することが可能になる。攻撃者の要求がハニーネット500に来ると、攻撃者が要求するアクティビティ、要求を受信したポート、またはその他の基準に基づいて要求を適切なハニーポットに対応付けることができる。複数の攻撃者が同じハニーポットと同時にやり取りする可能性があり、各ハニーポットは、攻撃者をだまして、本物の環境におり、ダミーインスタンスではなく本物のIaaSインスタンスとやり取りしていると信じ込ませるために、攻撃者に適切な応答を提供するように構成される。これは、エミュレートを通して行われてもよい。特定の実施の形態では、やり取りにより現実味を持たせるために、ハニーポットは、実際のサーバ（たとえば、WebLogicサーバ）を備えてもよい。このやり取りを通じて、クラウドサービスプロバイダ502の環境内に実装されたハニーネットプラットフォーム509は、特定の攻撃のタイプに関係する特定のマルウェアのサンプルを含む、ネットワークベースのIOCを収集できるようになる。ハニーネット500および様々なハニーポットS1～S3を設定する、デプロイするためのハニーネットプラットフォーム509を設けることができる。特定の実施の形態では、ハニーポットをデプロイして管理するためのDockerインフラストラクチャが使われ、各ハニーポットは、Dockerコンテナ（たとえば、隔離され、仮想化されたソフトウェアの束）として実装される。

【0113】

上記のように、顧客507は、関心に基づいて、デプロイする様々な種別のハニーポットを選択できる。異なる標的を攻撃する複数の異なる攻撃タイプが存在するので、顧客507は、Docker構成コンテナから、欲しい特定のハニーポットを選択できる。たとえば、支払い情報へのアクセスを提供するPOS（Point Of Sale）システム、保健記録およびその他のPII（個人を特定できる情報）へのアクセスを提供するヘルスケアシステムなどが存在し得る。よって、顧客507は、異なる種別のハニーポットをパブリックネットワーク（たとえば、インターネット）で公開することによって異なる種類のデータを収集したいであろう。各ハニーポットは、攻撃者の行為／やり取りに関するデータのログをローカル永続ストアに記録できる。ハニーポットは、生（RAW）の未加工データのログを記録してもよい。そして、このデータをローカルで加工して、加工ハニーポットデータを生成できる。この加工には、ログローテーション（たとえば、5分ごとまたはその他の間隔でデータをローテーションすること）、ログ検証（たとえば、関心のあるデータが収集されたこと、および正しいフォーマットであることを判断する）、データを匿名化するためのPIIスクラブ、およびデータフォーマッティング（たとえば、中央システムに転送するためにデータを正しいフォーマット（たとえば、JSON）にすること）が含まれる。その後、ハニーネットプラットフォーム509に加工データを送信できる。ハニーネットプラットフォーム509は、脅威インテリジェンス解析システム506（たとえば、外部サービス）または内部バージョンの脅威解析モジュール510にこのデータを提供し得る。いくつかの例では、脅威インテリジェンス解析システム506、510のいずれかが、（たとえば、世界中に散在するハニーポットから集めて蓄えられたログデータから検出された）既知の攻撃者のIPアドレスを特定できる。その後、場合によってはこれらのIPアドレスからの特権アクセス要求に対してステップアップ（たとえば、多要素）認証を要求するために、これらのIPアドレスは、様々なセキュリティプロダクトによって利用され得る。

10

20

30

40

50

【0114】

ハニーポットを実装することの1つの大きな懸念は、攻撃者がハニーポットからカーネルレベルのアクセス権を取得し、その後（たとえば、悪意のあるバイナリなどを利用して）メインネットワークに入ってしまうかどうかについてである。これは、クラウドサービスプロバイダ502に対する修復不可能な損害につながり得る。よって、ハニーポットの隔離は非常に重要である。いくつかの例では、この隔離は、（たとえば、ハニーネットプラットフォーム509を実装するクラウドサービスプロバイダ502の外部にある）サードパーティサービスプロバイダを使用してハニーネット500を実装することによって実現できる。このようにすれば、攻撃者がハニーポットを超えて基礎となるシステムに侵入できた場合でも、クラウドサービスプロバイダ502にはやはりアクセスできない。しかしながら、ハニーネット500を隔離する別の方法として、Dockerコンテナ内および／またはユーザのベアメタルにハニーネットを実装する方法がある（たとえば、その他のサービスによって共有されていない、隔離されたシングルテナントの物理マシン）。

10

【0115】

様々な異なる種別のハニーポットを用いてハニーネット500を構成してもよい。ハニーネット512および514は、必要に応じて、ハニーネット500と同じに構成されてもよく、異なるように構成されてもよい。たとえば、ハニーネット512および／または514によって任意の構成のハニーネット500も実装できる。しかしながら、クラウドサービスプロバイダ502内にハニーネット512を実装できるが、ハニーネット514は、（たとえば、サードパーティホスト上で実装されるハニーネット500のように）クラウドサービスプロバイダ502によって実装されるその他のハニーネットに過ぎない。ハニーネット500および514と同様の任意の数のさらなるハニーネットが、たとえば、世界中の様々な場所で実装されてもよい。

20

【0116】

上記のように、ハニーネット500は、複数のハニーポットを備えてもよい。一例として、ハニーネット500は、ポートP1によってアクセスできる第1ハニーポットS1と、ポートP2によってアクセスできる第2ハニーポットS2と、ポートP3によってアクセスできるハニーポットS3とを備える。ポート：P1、P2、P3の各々は、パブリックネットワーク504でアクセス可能であってもよい。したがって、開かれたポートを探して攻撃者501がインターネットの端から端まで見ていくと、これらのポートが明るみになる。これは、意図的であって、攻撃者501をハニーポットにおびき寄せることが可能になる。ハニーネット500は、1つのホストデバイス（たとえば、クラウドサービスプロバイダ502の内部であれ、外部であれ）上でデプロイされてもよい。1つのコンテナに各ハニーポットが含まれた様々なコンテナが存在するように、この1つのホストをコンテナ化できる。必要であれば、（たとえば、ハニーネット500に対して複数のホストがある、および／または1つのコンテナ内の複数のハニーポットがある）その他の構成が実装されてもよい。エンティティ（たとえば、攻撃者）から要求が来た場合、要求の種類および／または要求に対応付けられているポートを用いて、エンティティと接続するハニーポットをどれにするか決定してもよい。たとえば、ポートP1にアクセスするという要求であった場合、ハニーネット管理システム508は、ポートP1にある要求に基づいて、ポート22に対応するS1ハニーポットにエンティティを接続すると決定できる。

30

40

【0117】

様々な種類のサービスが特定のポートを使用することが知られているであろう。たとえば、SSHサービスは、一般に、ポート22を使用し、SMTPサービスは、一般に、ポート25を使用し、FTPサービスは、一般に、ポート21を使用するなど。ハニーネット500内にハニーポットサービスがデプロイされると、ホストに割り当てられているIPアドレスを経由してこれらのサービスが手に届くようになる。そして、これらのサービスは、その他のサーバと本質的に同じ機能を有するようになる。攻撃者501は、IPアドレスを探してインターネットの端から端まで見て、各IPアドレスのどのポートが開かれた状態であるかを見つけることができる。ポートが開かれたIPアドレスは、攻撃者に

50

にとって格好の標的であろう。よって、インターネットで利用可能なこれらの特定のポートを用いてハニーポットを構築できる。もちろん、これらのポートは、一般に、たとえ実世界（たとえば、ハニーポットのポートではないポート）であっても、パスワードを必要とする。場合によっては、パスワード／ユーザ名の組合せが公表されている可能性もある。しかしながら、その他の例では、様々な既知のユーザ名／パスワードの組合せ（たとえば、ユーザ名：admin、パスワード：パスワードは一般的な標準／デフォルトパスワード）を用いてハニーポットが構成されてもよい。ここでは図示されていないが、各ハニーポットポート（たとえば、P1～P3）は、外部に知られていない対応する内部のポート番号を有してもよい。たとえば、ポート22は、外部に公開されている（たとえば、ログインを要求する）特権ポートであるが、ハニーポットと通信する実際のポートは、他のポート番号である場合がある。この場合、ハニーネット管理サービス508は、各外部／特権ポートとその対応する内部（たとえば、特権なしの）ポート番号とのマッピングを保持できる。

10

【0118】

いくつかの例では、ハニーネット管理システム508は、他のポート／未知のポートを通じてアクセス可能であってもよい。攻撃者が確認しようと思わないであろうランダムに利用されたポート／ほとんど利用されていないポートの一覧から、ハニーネット管理システム508のポートが選択されてもよい。これに加えて、ハニーネット管理サービス508により、サービス（たとえば、顧客）は、コンテナをどのように設置するか、環境をどのように設定するか、ハニーポットがどのように動作するかについて管理および／または制御できるようになる。場合によっては、ハニーネット管理システム508がハニーポットを管理および／または制御するために使用する構成設定を、クラウドサービスプロバイダ502が（たとえば、より直接的には、クラウドサービスプロバイダ502のハニーポットプラットフォーム509が）制御できる。場合によっては、ハニーポットプラットフォーム509のコントローラは、（たとえば、ハニーネット500を制御するための）コントロールプレーンおよび（たとえば、ハニーネット500に対応付けられたデータをフェッチするための）データプレーンの両方において動作する。また、ハニーポットプラットフォーム509は、ハニーポットから受信したやり取りについてのデータのログ記録を同期させるように構成される同期部を備えてもよい。ハニーポットプラットフォーム509は、統計収集部も備えてもよい。統計収集部は、収集されたデータ（たとえば、システムログなど）を集約するように構成できる。

20

30

【0119】

上述したように、代わりに、ハニーネット500（たとえば、ハニーネット512）を制御するクラウドサービスプロバイダ502内にハニーネット500を実装できる。これは、セキュリティの観点から、明らかにさらに危険である。その理由は、ハニーポットがホスティングされているコンテナから攻撃者501が脱出できたら、クラウドサービスプロバイダ502のその他の個人的情報／セキュリティ保護された情報および／またはリソースにアクセスできてしまう可能性があるためである。ハニーネット500がサードパーティプロバイダによってホスティングされることによって、そのリスクが軽減されるであろう。しかしながら、クラウドサービスプロバイダ502内でハニーネット510をホスティングすることには、いくつかのメリットおよび利点がある。たとえば、脅威解析システム510は、その特定のサービスプロバイダを悪用しようとするこれらの攻撃者に固有の攻撃者データ。一例は、OracleのWebLogicsサーバである。ハッキングしてOracleのクラウドインフラストラクチャサービスに侵入しようとする攻撃者は、ポート80またはポート443上のWebLogicsサーバを探すであろう。エミュレートされたWebLogicsサーバをハニーポットとして有して攻撃者をおびき寄せることによって、Oracleは、Oracleの既知の脆弱性を意図的にターゲットにしている攻撃者についての有用なデータを収集できるようになるであろう。

40

【0120】

同様の例を用いると、Oracleは、OCI (Oracle Cloud Infra

50

a s t r u c t u r e) サービス内に存在するハニーネット512のようなハニーネットを構築することを選択するであろう。ハニーポットをより本物に見せるために、ハニーポットプラットフォーム509は、ハニーネット512を、コンテナにあるサーバのエミュレートでしかないのに、むしろ本物のOracleサーバに見えるように構成し得る。Oracleにハッキングしようとする攻撃者は、OCIに侵入できた証拠としてWebLogicサーバを確認し得るので、これは機能するはずである。よって、ハニーポットを常駐サービスプロバイダ固有のハニーポットにすることによって、(たとえば、攻撃者は内部の具体的な脆弱性に気付いているため) 特定のOCIアプリケーションを標的にしている高度な攻撃者を捕まえるのに役立てることができる。

【0121】

ハニーポットをより本物に見えるように構成すること(たとえば、Oracleの例では、Oracleがホスティングしているのに関わらず、Oracleであるかのように見せること)のその他の例として、Fusion Applicationsフロントエンド(または、その他のアプリケーション開発スイート)に見えるようにハニーポットを設計することが挙げられる。攻撃者がハニーポットとのセッションを開始すると、攻撃者にシミュレーションFusionデータが提示されてもよく、または、攻撃者がシミュレーションFusionデータにアクセスできるようになってもよい。これに加えて、OracleのIPアドレスを用いてホスティングされるようにハニーポットを構成できる。そして、ハニーポットプラットフォーム509は、攻撃者がマシンと行っているやり取りを追跡してログを記録できるようになり、場合によっては、攻撃者に「印を付けた」データを盗ませる。その後、このデータは、見つかった時/見つかると、特定可能である。すなわち、シミュレーションデータにこのように印をつけることができ、攻撃者にアクセスさせてもよい。その攻撃者がハニーポット以外でそのデータを使おうとした場合、使おうとしたことが発見され、攻撃者も検出され、場合によっては、特定され得る。

【0122】

別のオプションは、サービスプロバイダのコントロールプレーンAPI(たとえば、この例では、OCI)のように見える疑似コントロールプレーンAPIを設置することであろう。そのサービスプロバイダが利用する従来のAPIのように見せて、攻撃者のアクセスを許す弱いクレデンシャルを有するように構成する。ここでも、サービスプロバイダは、攻撃者がネットワーク上にいる間に何をしているかを追跡する。場合によっては、ハイパーバイザーを共有していると思われる顧客を攻撃者が侵害できないようにするために、ベアメタルハードウェアが用いられてもよい。各セッションはタグ付けされ、そのテナンシにあるすべてのネットワークトラフィックが監視される。このようにすれば、ハニーポットプラットフォーム509は、高度な攻撃パターンを追跡して、マシン間を移動するために攻撃者によってどのような手口が使われているかを学習できるであろう。

【0123】

さらなる詳細は後述するが、IaaSプロバイダは、サービステナンシ、データプレーン、コントロールプレーン、特定のサブネット、IPアドレス、ゲートウェイなどを有して構成されてもよい。図9～図11に示すパターン(たとえば、アーキテクチャ)である場合、ハニーポットを構成するときにこれらのパターンを可能な限り互いに似せるようにエミュレートすることは有利であろう。これは、ハニーネットがローカル(たとえば、ハニーネット512)で動作していようが、外部実装(たとえば、ハニーネット500)されていようが当てはまる。よって、ハニーポットプラットフォーム509は、ハニーポット自体がサードパーティサービスプロバイダのマシン上などサービスプロバイダの外部で動作していても、サービスプロバイダをホスティングしているハニーポットプラットフォーム509のインフラストラクチャに見えるようにハニーポットインスタンスを構成しようとするであろう。

【0124】

これに加えて、ハニーポットプラットフォーム509は、他が(たとえば、サブスクライブしている顧客507が)使用できる、サービスとしてのハニーポットというツールを

10

20

30

40

50

提供するように構成されてもよい。この例では、顧客は、計算機能自体には行わせることなく、自身のデータ収集と攻撃者から身を守るためにハニーポットを実行したいと考える。よって、ハニーポットプラットフォーム509は、サービスとしてのあらゆる種別のハニーネットをホスティングできるという機能を他に提供できる。一例において、このサービスを、1つ以上のAPIを介しておよび／またはサブスクリプションサービスを通して提供できる。

【0125】

いくつかの例では、ハニーネットサービスは、複数の異なる顧客がアクセス可能な1つのハニーネットを設けてもよい。しかしながら、その他の例では、個々のハニーネット（たとえば、顧客につき1つのハニーネット）が実装されてもよい。このようなサービスは、顧客507に代ってサービスプロバイダ（たとえば、ハニーネット512を使用しているクラウドサービスプロバイダ502）によってホスティングされ得る、または、顧客507の環境内でホスティングされ得る。これに加えて、各顧客507は、どのハニーポットインスタンスを実行したいかを含む、どのような種類のハニーネットを構築したいかをカスタマイズできる。様々なハニーネット間、様々な範囲、特定の地理上の領域間などにハニーポットを分散させることが求められるであろう。たとえば、顧客507は、特定の地域（たとえば、インド）に特定のハニーポット（たとえば、WordPressサーバ）を実装するよう求めるであろう。そして、この例では、ハニーネットプラットフォーム508は、（可能性として、当該1つハニーポットのみを有する）ハニーネットをインドに構築してこの国のWordPressサーバを標的にしている攻撃者を追跡する。別の例では、すでに複数のコンテナにある複数のそれぞれ異なるハニーポットを用いて様々なハニーネットが構築され、要求があると、ハニーポットプラットフォーム508は、要求された種別のハニーポットコンテナを、適切なハニーネットに自動的にデプロイする。

【0126】

このように、ハニーポットプラットフォーム508は、ハニーネットまたはハニーポットについての要求を顧客から受信するように構成できる。要求は、設定情報を含み得る。設定情報は、ハニーネットの数、ハニーネット（複数可）がデプロイされる場所、ハニーネット（複数可）内にデプロイされるハニーポットの種別および／または数、およびログが記録されるデータの種類を特定する。要求に応じて、ハニーポットプラットフォーム508は、設定情報に基づいて1つ以上のハニーネットおよび／または1つ以上のハニーポットを構築する。データは、収集、ログを記録、処理、ならびに／または解析されてから、脅威解析システム（たとえば、脅威解析システム506および／もしくは脅威解析システム512）ならびに／または顧客自身の元に送信できる。一定時間が経過するまでまたは顧客がサービスの終了を要求するまで、ハニーポットプラットフォーム508は、顧客に代わって、サービスとしてのこれらのハニーネットおよび／またはハニーポットを実装し続ける。

【0127】

図6は、ハニーポットプラットフォームシステム602に代わってハニーネット600をホスティングできる、および／または、ハニーポットプラットフォームシステム602によって制御されるハニーネット600をホスティングできる、コンピューティングシステムの簡略ブロック図である。いくつかの実施の形態では、ハニーネット600をホスティングしているコンピューティングシステムは、（たとえば、ハニーポットプラットフォームシステム602をホスティングしているコンピュータとは異なる）サードパーティサービスプロバイダであってもよい。しかしながら、その他の例では、同じコンピューティングシステムであってもよい。

【0128】

いくつかの例では、ハニーネット600をホスティングするコンピューティングシステムは、ベースオペレーティングシステムを有することができ、1つ以上のハニーポット（たとえば、ハニーポットS1、S2、S3、…、SN；まとめてハニーポットS1～N）をエミュレートできるコンテナ604を実装できる。ハニーポットS1～SNは、任意の

種別のハニーポット（上述したように）で有り得、コンテナ化（たとえば、コンテナ604に実装）でき、（たとえば、永続ストア608のRAWのHPデータ606にデータのログを記録することによって）データをディスクに書き出すことができる。ハニーポットS1～SNのうち1つに攻撃者がアクセスすると、RAWのHPデータ606にあるファイルに書き込むことによってそのアクティビティをログに記録できる。このデータは、JSONフォーマットなどで書き込むことができる。場合によっては、各HP S1～SNは、各HP S1～SNがエミュレートしているサーバの種類に基づいて異なる種類のデータを送り出してもよい。たとえば、各種類のサーバは、異なる種類のデータを利用および／または処理してもよい。この一例として、SSHデータは、メールサーバデータ（たとえば、SMTP）とはかなり違う。

10

【0129】

いくつかの例では、データ処理システム612のログローテーション部610にこのデータを送信できる。データ処理システム612は、ハニーポットS1～SNを可視化システム616と共に管理するように構成されたハニーポット管理システム614の一部に過ぎない。ログローテーション部610は、一定間隔で（たとえば、5分ごとに、または必要に応じて）ログデータをローテーションできる。場合によっては、コンピューティングシステム600は、ハニーポットがデータのログをどのように記録するか（たとえば、毎日1つのファイルにログを記録するか、異なるファイルにログを記録するか）を操作できなくともよい。そのため、ログローテーション部610は、一般的に、データ処理システム612またはホストシステム600にとって望ましい特定の期間でログをローテーションするように構成される。ログデータは、HPデータ同期部618と同期できるよう、期間ごとに細かく分割されてもよい。しかしながら、HPデータ同期部618にデータを送信する前に、データ処理システム612は、先ず、（たとえば、ログ検証部620を用いて）データを検証し、（たとえば、PIIスクラブ部622を用いて）データをスクラブし、（たとえば、データフォーマット部624を用いて）データをフォーマットしてもよい。データ検証部620は、取り込んだデータの種類を確認し、下流にいる消費者626（たとえば、顧客）が関心を持っているフィールドの種類として正しい種類であることを確認してもよい（たとえば、データがIPアドレスである場合、実際に32ビットアドレスであるかどうかなど）。PIIスクラブ部622は、個人を特定できる情報をスクラブして、スクラブしなければ発見され得る身元を難読化するように構成できる。データフォーマット部624は、JSONフォーマット（など）にデータをフォーマットするように構成され、そのフォーマットを理解できるプラットフォーム（たとえば、HPデータ同期部618）と（たとえば、後にパイプラインで）共有できるようにする。処理後、データは、永続ストア608の加工済HPデータ628に格納できる。

20

30

【0130】

場合によっては、永続ストア608は、（たとえば、節約するために）ブロックストレージとして構成される。ハニーポットS1～SNが動作しており（たとえば、並行して動作してもよい）データのログをブロックストレージに常に記録し、先ずはRAWのHPデータ606に記録され、加工されると、加工されたHPデータ628に記録される。いくつかの例では、1つのハニーポットに複数の攻撃者が接続する場合がある。これは、各ハニーポットがエミュレートサーバであるのであり得ることである。そのため、（たとえば、種別ごとに）同じハニーポットインスタンスが複数の攻撃者と同時に通信できるが、当該1つのハニーポットは、各攻撃者には個々のインスタンスであるかのように見える。しかしながら、エミュレートされたハニーポットインスタンスは、各攻撃者との所与のセッションに限ってステートフルである。よって、攻撃者がログアウトすると、新しいログインがあると、同じインスタンスの新しいエミュレートができる。しかし、同じインスタンス上のすべての攻撃者のログを平行して書き込むことができる。

40

【0131】

上述したように、攻撃者に本物のサーバであるようにエミュレートサーバを見せることは、有利である。こうすることによって、攻撃者をより長い時間ログインさせることがで

50

きるので、より多くのデータを収集できるようになる。また、こうすることによって、攻撃者をだましてより高度なテクニックに挑戦させることができる。当該高度なテクニックをログに記録して解析し、攻撃者から学習することができる。エミュレート環境を本物に見せるための技術として、UI（ユーザインターフェース）を提供すること、攻撃者がアクセスできる偽のアカウントを作成すること、ならびに／または、ベアメタルマシン上でインスタンスおよび／もしくはセッション実行することなどが挙げられる。上記のように、ハニーポットS1～SNは、Dockerコンテナ（またはその他の種類のコンテナ）に実装される。このようなコンテナは、要求されている各種類のサーバまたはサービスをエミュレートする仮想環境である。各ハニーポットS1～SNは、環境をエミュレートしている仮想コンテナである。ハッカーがファイルシステムの一覧を要求した場合、エミュレート環境を本物のように見せる適切な応答で返信することは有利である。たとえば、ウェブサーバの場合、サーバがポート80上でApacheを実行していることを攻撃者に応答で示してもよい。また、ハニーポットは、Apacheを実際に実行していたシステム上に格納された標準ファイルであると思われるファイルのリストを作成できる。

10

20

30

40

50

【0132】

簡単に上記したように、攻撃者のセッションは、攻撃者がハニーポットにログインしている間はステートフルであってもよい。いくつかの例では、セッションを特定の期間（たとえば、5分程度）で更新してもよい。ほとんどの攻撃は自動化されており、わずか数秒しか続かないので、1つのセッションにとって5分は十分な時間である。しかしながら、いくつかの例では、攻撃者がログインしてハニーポットを操作している（たとえば、要求を行っている）間はセッションが動作していてもよい。

【0133】

データがログ記録および処理されると、ハニーポットプラットフォームシステム602、たとえば、HPデータ同期部618に直接返すことができる。同期部618は、一定間隔（たとえば、5分）で加工済HPデータ628からデータをフェッチするように構成できる。同期部は、一定間隔のデータ送りの同期を取るのに役立つので、データを失うことがない。そして、同期部618は、下流にいる消費者626および／または脅威解析システムにデータを送ることができる。いくつかの例では、ハニーポットプラットフォームシステム602のコントローラ630は、ハニーポットS1～SNのいずれも追加、分割、再構築、改良、または制御するように構成できる。コントローラ630は、SSHタイプ接続および／またはセキュアシェルアプリケーションを介してハニーポット管理システム614と通信してもよい。これに加えて、システム統計収集部632は、システムログについての情報またはその他のログ情報を収集するように構成される。システム統計収集部632は、ハニーポットプラットフォームシステム602のコントロールプレーンの一部として実装されてもよく、SSHを経由してハニーポット管理システム614の可視化システム616とも通信してもよい。いくつかの例では、監視およびアラートシステム634は、監視するよう定められているファイルおよびファイルシステムをチェックするように構成できる。監視およびアラートシステム634は、データにチェックサムを実行して、一致しないデータがあるかどうかを確認でき、場合によっては、ファイルを復元できる。これは、攻撃者がハニーポットプラットフォームシステム602に実際に侵入し（たとえば、ハニーネット600をホスティングしているコンピューティングシステムがハニーポットプラットフォームシステム602をホスティングしているコンピュータと同じコンピュータであった場合）何か変更を行った場合に有利である。その後、監視およびアラートシステム634は、下流にいる顧客、サードパーティサービス（たとえば、ハニーネット600および／またはハニーポットプラットフォームシステム602をホスティングしているコンピューティングシステム）にアラートを出すことができる。ロガー632は、ログが記録されたデータをUI提示する、または当該データを可視化する準備を行うためのその他のアプリケーションに提示するように構成できる。

【0134】

図7は、本明細書に記載の技術を実行するための例示的な方法700を説明するフロー

図である。方法 700 の一部もしくはすべて（または、本明細書に記載のその他の処理もしくはそれらの変形例および／もしくは組合せ）は、実行可能な命令を有して構成される 1 つ以上のコンピュータシステムの制御のもとで実行されてもよく、ソフトウェア、ハードウェア、またはそれらの組合せによって 1 つ以上のプロセッサ上でまとめて動作するコード（たとえば、実行可能な命令、1 つ以上のコンピュータプログラム、または 1 つ以上のアプリケーション）として実現されてもよい。コードは、たとえば、1 つ以上のプロセッサによって実行可能な複数の命令を含むコンピュータプログラムの形でコンピュータ読み取り可能な記憶媒体上に格納されてもよい。コンピュータ読み取り可能な記憶媒体は、非一時的な記憶媒体である。方法 700 は、図 3 のデータセンター 302、図 4 のハニーポットサーバ 400、図 5 のハニーネット 500 および／もしくはハニーポットプラットフォーム 509、または、図 6 のハニーネット 600 および／もしくはハニーポットプラットフォームシステム 602 をホスティングしているコンピューティングシステム、のうち 1 つ以上もしくはそれらの組合せによって実行されてもよい。

10

20

30

40

50

【0135】

方法 700 は、ブロック 702 から開始し得る。ブロック 702 では、IaaS サービスのコンピューティングインスタンスが複数のハニーポットサーバを提供（たとえば、実装／実行）し得る。各ハニーポットサーバは、コンテナに実装されてもよく、物理サーバのエミュレートであってもよい。これに加えて、各ハニーポットサーバは、ハニーポット種別で識別され得る。たとえば、ハニーポット種別として、SMTP ハニーポット、Weblog ハニーポット、HTTP ハニーポット、FTP ハニーポット、SSH ハニーポットなどが挙げられる。種別に基づいて、各ハニーポットは、ユーザと異なる方法でやり取りする、異なるデータを処理するなどしてもよい。これに加えて、複数のハニーポットは、1 つのハニーネットとして考えられてもよい。このハニーネットは、IaaS サービス内でローカルに動作するまたは外部で（たとえば、サードパーティサービスプロバイダによって）動作する 1 つのコンピューティングインスタンスによって実装され得る。

【0136】

ブロック 704 では、方法 700 は、コンピューティングインスタンスが、攻撃者をおびき寄せて、ハニーポットサーバのうち少なくとも 1 つとセッションを確立させ得る。おびき寄せるステップは、パブリックネットワーク（たとえば、インターネット）で公開されているハニーポットに割り当てられた IP に対応付けられた 1 つ以上のポートに基づいてもよい。また、おびき寄せるステップは、ハニーポットのログインクレデンシャルを公開することを含み得るが、ほとんどの場合、攻撃者をおびき寄せるには、ポートを公開することで十分であろう。その理由は、攻撃者および一般社会で広くに知られている様々なユーザ名／パスワードの組合せがあるためである。

【0137】

ブロック 706 では、方法 700 は、コンピューティングインスタンスが、攻撃者から第 1 の要求を受信し得る。場合によっては、第 1 の要求は、インスタンスに関する要求であり得、および／または要求特性を含み得る。第 1 の要求は、通常、攻撃者が関心のあるポートの向こう側に存在するサービスにログインするという要求である。第 1 の要求特性は、要求が送られたポート、要求されているサービスの種類、要求されているアクションの種類などを識別し得る。

【0138】

ブロック 708 では、方法 700 は、コンピューティングインスタンスが、要求特性およびハニーポット種別の少なくとも一部に基づいて、複数のハニーポットサーバのうち特定のハニーポットサーバを特定し得る。たとえば、攻撃者がポート 25 へのアクセスを要求しており、ポート 25 が SMTP サーバに対応する場合、コンピューティングインスタンスは、その攻撃者のために SMTP サーバをエミュレートしているハニーポットを特定し得る。この例では、要求特性とは、ポート 25、または SMTP（メール）サーバにログインするという要求のいずれかを特定する情報である。この情報を利用して、コンピューティングインスタンスは、この生じ得る接続のための SMTP ハニーポットを（たとえ

ば、種別に対する特性のマッピングに基づいて）特定できる。この例で特定される特定のハニーポットは、SMTPハニーポットである。

【0139】

ブロック710では、方法700は、コンピューティングインスタンスが、特定のハニーポットと接続するためのセッションを攻撃者と確立し得る。このように、短期間（たとえば、5分）状態のセッションが確立され得る。セッション中、攻撃者は、特定された特定のハニーポットサーバへの特権アクセスを有する。攻撃者がログオフすると、同じハニーポットサーバまたは別の種別のハニーポットサーバとの新しいセッションが確立される必要がある。

【0140】

ブロック712では、方法700は、攻撃者に接続される特定のハニーポットサーバが、攻撃者からの第2の要求に対する応答を生成し得る。第2の要求は、セッションが確立された後に行われ得るので、ログインしている攻撃者から受信するであろう。第2の要求は、仮想コンピューティングインスタンスをスピンアップする要求や、セキュリティ保護されたリソースにアクセスする要求などであり得る。本質的に、第2の要求は、ログインしているハニーポットサーバに要求するために攻撃者が選択し得る任意の種類の要求であり得る。生成される応答は、その要求に対して適切な応答でなければならない。たとえば、データにアクセスするという要求であった場合、応答は、そのデータまたはそのデータのダミーを提供しなければならない。仮想コンピューティングインスタンスをスピンアップするという要求であった場合、応答は、そのインスタンス化が確認されたという応答でなければならない。

【0141】

ブロック714では、方法700は、特定のハニーポットサーバが、第2の要求に応じて応答を攻撃者まで通信させ得る。上述したように、本物のサーバに接続していると攻撃者に信じ込ませ続けるために、応答は、与えられた要求に対して適切な応答でなければならない。

【0142】

ブロック716では、方法700は、終了し得る。ブロック716では、コンピューティングインスタンスは、攻撃者に関するデータ、または攻撃者による特定のハニーポットとの1つ以上のやり取りに関するデータを記録し得る。このデータを加工および／または解析されて、将来の攻撃を防ぐのに役立てられ得る。

【0143】

例示的な実施態様

上述したように、IaaS (Infrastructure As A Service) は、1つの特殊な種類のクラウドコンピューティングである。仮想化されたコンピューティングリソースをパブリックネットワーク（たとえば、インターネット）で提供するようにIaaSを構成できる。IaaSモデルでは、クラウドコンピューティングプロバイダは、インフラストラクチャの構成要素（たとえば、サーバ、記憶装置、ネットワークノード（たとえば、ハードウェア）、導入ソフトウェア、プラットフォームの仮想化（たとえば、ハイパーバイザー層）など）をホスティングできる。場合によっては、IaaSプロバイダは、これらのインフラストラクチャの構成要素に付随する多種多様なサービス（たとえば、請求、監視、ログ記録、セキュリティ、負荷分散およびクラスタリングなど）も供給してもよい。よって、これらのサービスはポリシーベースのサービスであり得るので、IaaSユーザは、負荷分散を駆動するポリシーを実施して、アプリケーションの可用性および性能を維持できるようになるであろう。

【0144】

場合によっては、IaaS顧客は、インターネットなどのWAN（ワイドエリアネットワーク）を通じてリソースおよびサービスにアクセスしてもよく、クラウドプロバイダのサービスを利用してアプリケーションスタックの残りの要素をインストールできる。たとえば、ユーザは、IaaSプラットフォームにログインして、VM（仮想マシン）を作成

10

20

30

40

50

、各VM上にOS（オペレーティングシステム）をインストール、データベースなどのミドルウェアをデプロイ、ワークロードやバックアップ用のストレージバケットを作成、さらにはそのVMに企業向けソフトウェアをインストールすることができる。そして、顧客は、プロバイダのサービスを利用して、ネットワークトラフィックの負荷分散、アプリケーションの問題のトラブルシューティング、パフォーマンスの監視、ディザスタリカバリの管理などを含む様々な機能を実行できる。

【0145】

ほとんどの場合、クラウドコンピューティングモデルは、クラウドプロバイダの参加を必要とする。クラウドプロバイダは、IaaSを提供（たとえば、オファー、レンタル、販売）することに特化したサードパーティサービスであってもよいが、そうである必要はない。また、エンティティがプライベートクラウドをデプロイすることを選択して、エンティティ自体のインフラストラクチャサービスのプロバイダになってもよい。

10

【0146】

いくつかの例では、IaaSのデプロイメント（導入）とは、準備したアプリケーションサーバなどに新しいアプリケーションまたは新しいバージョンのアプリケーションを載せる処理である。サーバを準備する処理も含み得る（たとえば、ライブラリ、デーモンなどをインストールすること）。これは、ハイパーバイザー層（たとえば、サーバ、ストレージ、ネットワークハードウェア、および仮想化）よりも下の層でクラウドプロバイダによって管理されることが多い。よって、顧客には、（たとえば、要求に基づいてスピンアップされ得る）セルフサービス仮想マシンなどの上の（OS）、ミドルウェア、および／またはアプリケーションの導入に対処する責任があるであろう。

20

【0147】

いくつかの例では、IaaSプロビジョニングとは、使用するためのコンピュータまたは仮想ホストを取得すること、さらには、それらの上に必要なライブラリまたはサービスをインストールすることを指し得る。ほとんどの場合、導入にはプロビジョニングは含まれず、プロビジョニングは最初に行われる必要があり得る。

【0148】

場合によっては、IaaSプロビジョニングには2つの異なる課題がある。まず、何かを実行する前に初期のインフラストラクチャー式をプロビジョニングするという初期段階の課題である。次に、すべてがプロビジョニングされてから既存のインフラストラクチャーを進化させていく（たとえば、新しいサービスを追加する、サービスを変更する、サービスを削除するなど）という課題がある。場合によっては、インフラストラクチャーの構成を宣言的に定義することを可能にすることによってこれらの2つの課題に対処してもよい。すなわち、1つ以上の設定ファイルでインフラストラクチャー（たとえば、どの構成要素が必要で、それらがどのようにやり取りするか）を定義できる。よって、インフラストラクチャーのトポロジー全体（たとえば、どのリソースがどのリソースに依存しているのか、それらのリソースがどのように連携するのか）を宣言的に定義できる。場合によっては、トポロジーが定義されると、設定ファイルに記述されている異なる構成要素を作成および／または管理するワークフローを生成できる。

30

【0149】

いくつかの例では、インフラストラクチャーには、互いに接続された多くの要素があり得る。たとえば、コアネットワークとしても知られる1つ以上のVPC（仮想プライベートクラウド）（たとえば、コンフィギュラブルなコンピューティングリソースおよび／または共有コンピューティングリソースの、おそらくオンデマンドのプール）があってもよい。いくつかの例では、ネットワークのセキュリティをどのように設置するか、および1つ以上のVM（仮想マシン）を定義する1つ以上のセキュリティグループルールもプロビジョニングされてもよい。ロードバランサ、データベースなど、その他のインフラストラクチャーの要素もプロビジョニングされてもよい。求められるおよび／または追加されるインフラストラクチャーの要素が増えると、インフラストラクチャーは漸進的に進化するであろう。

40

50

【0150】

場合によっては、様々な仮想コンピューティング環境間でインフラストラクチャのコードをデプロイすることを可能にするための断続的デプロイ技術が採用されてもよい。これに加えて、説明した技術によって、これらの環境内でのインフラストラクチャの管理が可能になる。いくつかの例では、サービスチームは、1つ以上の、多くの場合、多くの異なる本番環境（たとえば、様々な異なる地理的位置にまたがる、時として、全世界に及ぶ）にデプロイされることが求められるコードを書くことができる。しかしながら、いくつかの例では、コードがデプロイされるインフラストラクチャを最初に設置しなければならない。場合によっては、プロビジョニングは手作業で行われ得、インフラストラクチャがプロビジョニングされると、プロビジョニングツールを利用してリソースがプロビジョニングされてもよく、および／または開発ツールを利用してコードがデプロイされてもよい。

10

【0151】

図8は、少なくとも1つの実施の形態に係る、IaaSアーキテクチャのパターンの例を示すブロック図800である。サービスオペレータ802は、セキュリティ保護されたホストテナンシ804に通信可能に連結される。セキュリティ保護されたホストテナンシ804は、VCN（仮想クラウドネットワーク）806と、セキュリティ保護されたホストサブネット808とを備え得る。いくつかの例では、サービスオペレータ802は、1つ以上のクライアントコンピューティングデバイスを使用してもよい。クライアントコンピューティングデバイスは、Microsoft Windows Mobile（登録商標）などのソフトウェアおよび／またはiOS、Windows Phone、Android、BlackBerry 10、PalmOSなどのいろいろなモバイルオペレーティングシステムを実行し、かつ、インターネット、電子メール、SMS（Short Message Service）、BlackBerry（登録商標）、または他の通信プロトコルに対応する手のひらサイズのポータブルデバイス（たとえば、iPhone（登録商標）、携帯電話、iPad（登録商標）、コンピューティングタブレット、PDA（Personal Digital Assistant））またはウェアラブルデバイス（たとえば、Google Glass（登録商標）ヘッドマウントディスプレイ）であってもよい。あるいは、クライアントコンピューティングデバイスは、様々なバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、および／もしくはLinux（登録商標）オペレーティングシステムを実行するパーソナルコンピュータならびに／またはラップトップコンピュータを含む、汎用パーソナルコンピュータであり得る。クライアントコンピューティングデバイスは、たとえば、Google Chrome OSなどいろいろなGNU/Linuxオペレーティングシステムを含む各種市販のUNIX（登録商標）またはUNIXに似たオペレーティングシステムを実行するワークステーションコンピュータであり得るが、これに限定されない。これに代えて、またはこれに加えて、クライアントコンピューティングデバイスは、シンクライアントコンピュータ、インターネット対応のゲーミングシステム（たとえば、Kinect（登録商標）ジェスチャ入力装置付きまたは無しのMicrosoft Xboxのゲーミングコンソール）、および／もしくはパーソナルメッセージングデバイスなど、VCN806にアクセスできるネットワークならびに／またはインターネットで通信可能なその他の電子機器であってもよい。

20

30

40

【0152】

VCN806は、LPG（ローカルピアリングゲートウェイ）810を含み得る。LPG810は、SSH VCN812に含まれるLPG810を介してSSH（セキュアシェル）VCN812に通信可能に連結できる。SSH VCN812は、SSHサブネット814を含み得、SSH VCN812は、コントロールプレーンVCN816に含まれるLPG810を介してコントロールプレーンVCN816に通信可能に連結できる。また、SSH VCN812は、LPG810を介してデータプレーンVCN818に通信可能に連結できる。コントロールプレーンVCN816およびデータプレーンVCN818は、サービステナンシ819に含まれ得る。サービステナンシ819は、IaaSプ

50

ロバイダに所有および／または操作され得る。

【0153】

コントロールプレーンVCN816は、境界ネットワーク（たとえば、企業のイントラネットと外部ネットワークとの間の企業ネットワークの一部）として機能するコントロールプレーンDMZ（Demilitarized Zone）ティア820を含み得る。DMZベースのサーバの仕事には制限があり得、セキュリティ侵害を抑えるのに役立ち得る。これに加えて、DMZティア820は、1つ以上のLB（ロードバランサ）サブネット（複数可）822を含み得、コントロールプレーンアプリティア（App Tier）824は、アプリサブネット（複数可）826を含み得、コントロールプレーンデータティア828は、DB（データベース）サブネット（複数可）830を含み得る（たとえば、フロントエンドDBサブネット（複数可）および／またはバックエンドDBサブネット（複数可））。コントロールプレーンDMZティア820に含まれるLBサブネット（複数可）822は、コントロールプレーンアプリティア824に含まれるアプリサブネット（複数可）826と、コントロールプレーンVCN816に含まれ得るインターネットゲートウェイ834とに通信可能に連結でき、アプリサブネット（複数可）826は、コントロールプレーンデータティア828に含まれるDBサブネット（複数可）830と、サービスゲートウェイ836およびNAT（ネットワークアドレス変換）ゲートウェイ838とに通信可能に連結できる。コントロールプレーンVCN816は、サービスゲートウェイ836と、NATゲートウェイ838とを含み得る。

10

【0154】

コントロールプレーンVCN816は、データプレーンミラーアプリティア840を含み得る。データプレーンミラーアプリティア840は、アプリサブネット（複数可）826を含み得る。データプレーンミラーアプリティア840に含まれるアプリサブネット（複数可）826は、VNIC（仮想ネットワークインターフェースコントローラ）842を含み得る。VNIC842は、コンピューティングインスタンス844を実行できる。コンピューティングインスタンス844は、データプレーンミラーアプリティア840のアプリサブネット（複数可）826をアプリサブネット（複数可）826に通信可能に連結できる。アプリサブネット826は、データプレーンアプリティア846に含まれ得る。

20

【0155】

データプレーンVCN818は、データプレーンアプリティア846と、データプレーンDMZティア848と、データプレーンデータティア850とを含み得る。データプレーンDMZティア848は、LBサブネット（複数可）822を含み得る。LBサブネット822は、データプレーンアプリティア846のアプリサブネット（複数可）826と、データプレーンVCN818のインターネットゲートウェイ834とに通信可能に連結できる。アプリサブネット（複数可）826は、データプレーンVCN818のサービスゲートウェイ836およびデータプレーンVCN818のNATゲートウェイ838に通信可能に連結され得る。また、データプレーンデータティア850は、DBサブネット（複数可）830も備える。DBサブネット830は、データプレーンアプリティア846のアプリサブネット（複数可）826に通信可能に連結できる。

30

【0156】

コントロールプレーンVCN816のインターネットゲートウェイ834およびデータプレーンVCN818のインターネットゲートウェイ834は、メタデータ管理サービス852に通信可能に連結できる。メタデータ管理サービス852は、パブリックインターネット854に通信可能に連結できる。パブリックインターネット854は、コントロールプレーンVCN816のNATゲートウェイ838およびデータプレーンVCN818のNATゲートウェイ838に通信可能に連結できる。コントロールプレーンVCN816のサービスゲートウェイ836およびデータプレーンVCN818のサービスゲートウェイ836は、クラウドサービス856に通信可能に連結できる。

40

【0157】

50

いくつかの例では、コントロールプレーンVCN816のサービスゲートウェイ836またはデータプレーンVCN818のサービスゲートウェイ836は、パブリックインターネット854を通過せずにクラウドサービス856にAPI（アプリケーションプログラミングインターフェース）呼び出しを行うことができる。サービスゲートウェイ836からクラウドサービス856へのAPI呼び出しは、一方通行であり得る。すなわち、サービスゲートウェイ836はクラウドサービス856にAPI呼び出しを行うことができ、クラウドサービス856はサービスゲートウェイ836に要求されたデータを送信できる。しかし、クラウドサービス856は、サービスゲートウェイ836に対するAPI呼び出しを開始しないであろう。

【0158】

いくつかの例では、さもないければ隔離されているであろうサービステナンシ819に、セキュリティ保護されたホストテナンシ804を直接接続できる。セキュリティ保護されたホストサブネット808は、LPG810を通じてSSHサブネット814と通信できる。LPG810は、さもないければ隔離されているシステムを通した双方向通信を可能にし得る。セキュリティ保護されたホストサブネット808をSSHサブネット814に接続することにより、セキュリティ保護されたホストサブネット808には、サービステナンシ819内のその他のエンティティへのアクセスが与えられ得る。

【0159】

コントロールプレーンVCN816により、サービステナンシ819のユーザは、所望のリソースを設置またはプロビジョニングできるようになり得る。コントロールプレーンVCN816においてプロビジョニングされた所望のリソースは、データプレーンVCN818においてデプロイまたは使用され得る。いくつかの例では、データプレーンVCN818からコントロールプレーンVCN816を隔離でき、コントロールプレーンVCN816のデータプレーンミラーアプライティア840は、データプレーンミラーアプライティア840に含まれ得るVNIC842およびデータプレーンアプライティア846に含まれ得るVNIC842を介して、データプレーンVCN818のデータプレーンアプライティア846と通信できる。

【0160】

いくつかの例では、システムのユーザ、または顧客は、パブリックインターネット854を通して要求を行うことができる、たとえば、CRUD（生成、読み取り、更新、および削除）操作を行うことができる。パブリックインターネット854は、メタデータ管理サービス852に要求を通信できる。メタデータ管理サービス852は、インターネットゲートウェイ834を通してコントロールプレーンVCN816に要求を通信できる。要求は、コントロールプレーンDMZティア820に含まれるLBサブネット（複数可）822によって受信され得る。LBサブネット（複数可）822は、有効な要求であると判断し得、この判断に応じて、LBサブネット（複数可）822は、コントロールプレーンアプライティア824に含まれるアプリサブネット（複数可）826に要求を送信できる。要求が検証され、パブリックインターネット854への呼び出しを必要とする場合、パブリックインターネット854への呼び出しは、パブリックインターネット854への呼び出しを行うことができるNATゲートウェイ838に送信され得る。格納されるのが望ましいと要求によって求められているメモリを、DBサブネット（複数可）830に格納できる。

【0161】

いくつかの例では、データプレーンミラーアプライティア840は、コントロールプレーンVCN816とデータプレーンVCN818との直接通信を容易にできる。たとえば、構成に対する変更、更新、またはその他の適した修正を、データプレーンVCN818に含まれるリソースに適用することが望まれる場合がある。VNIC842を介して、コントロールプレーンVCN816は、データプレーンVCN818に含まれるリソースに直接通信することにより、当該リソースに対する構成に対してこれらの変更、更新、またはその他の適した修正を行うことができる。

10

20

30

40

50

【0162】

いくつかの実施の形態では、コントロールプレーンVCN816およびデータプレーンVCN818をサービステナンシ819に含めることができる。この場合、ユーザまたはシステムの顧客は、コントロールプレーンVCN816もデータプレーンVCN818も所有または操作しなくてもよい。その代わりに、IaaSプロバイダは、サービステナンシ819に含まれ得るコントロールプレーンVCN816およびデータプレーンVCN818の両方を所有または操作し得る。本実施の形態によって、ネットワークの隔離が可能になり、ユーザまたは顧客がその他のユーザのリソースまたはその他の顧客のリソースとやり取りさせないようにする。また、本実施の形態によって、ユーザまたはシステムの顧客は、希望するレベルのストレージセキュリティではない可能性のあるパブリックインターネット854に頼る必要なく、データベースを内密に格納できるようになる。

10

【0163】

その他の実施の形態では、コントロールプレーンVCN816に含まれるLBサブネット（複数可）822を、サービスゲートウェイ836からの信号を受信するように構成できる。本実施の形態では、コントロールプレーンVCN816およびデータプレーンVCN818は、IaaSプロバイダの顧客によって、パブリックインターネット854を呼び出すことなく呼び出されるように構成され得る。パブリックインターネット854から隔離されて、顧客が利用するデータベース（複数可）がIaaSプロバイダによって制御され得、サービステナンシ819に格納され得るので、IaaSプロバイダの顧客は、本実施の形態を望むであろう。

20

【0164】

図9は、少なくとも1つの実施の形態に係る、IaaSアーキテクチャの別の例示的なパターンを示すブロック図900である。サービスオペレータ902（たとえば、図8のサービスオペレータ802）は、セキュリティ保護されたホストテナンシ904（たとえば、図8のセキュリティ保護されたホストテナンシ804）に通信可能に連結できる。セキュリティ保護されたホストテナンシ904は、VCN（仮想クラウドネットワーク）906（たとえば、図8のVCN806）と、セキュリティ保護されたホストサブネット908（たとえば、図8のセキュリティ保護されたホストサブネット808）とを備えることができる。VCN906は、LPG（ローカルピアリングゲートウェイ）910（たとえば、図8のLPG810）を備えることができる。LPG910は、SSH VCN912に含まれるLPG810を介してSSH（セキュアシェル）VCN912（たとえば、図8のSSH VCN812）に通信可能に連結できる。SSH VCN912は、SSHサブネット914（たとえば、図8のSSHサブネット814）を備えることができ、SSH VCN912は、コントロールプレーンVCN916に含まれるLPG910を介してコントロールプレーンVCN916（たとえば、図8のコントロールプレーンVCN816）に通信可能に連結できる。コントロールプレーンVCN916は、サービステナンシ919（たとえば、図8のサービステナンシ819）に含めることができ、データプレーンVCN918（たとえば、図8のデータプレーンVCN818）は、ユーザまたはシステムの顧客が所有または操作し得る顧客テナンシ921に含めることができる。

30

【0165】

コントロールプレーンVCN916は、LBサブネット（複数可）922（たとえば、図8のLBサブネット（複数可）822）を含み得るコントロールプレーンDMZティア920（たとえば、図8のコントロールプレーンDMZティア820）と、アプリサブネット（複数可）926（たとえば、図8のアプリサブネット（複数可）826）を含み得るコントロールプレーンアプリティア924（たとえば、図8のコントロールプレーンアプリティア824）と、（たとえば、図8のDBサブネット（複数可）830と同様の）DB（データベース）サブネット（複数可）930を含み得るコントロールプレーンデータティア928（たとえば、図8のコントロールプレーンデータティア828）とを備えることができる。コントロールプレーンDMZティア920に含まれるLBサブネット（複数可）922は、コントロールプレーンアプリティア924に含まれるアプリサブネット

40

50

ト（複数可）９２６と、コントロールプレーンＶＣＮ９１６に含めることができるインターネットゲートウェイ９３４（たとえば、図８のインターネットゲートウェイ８３４）とに通信可能に連結でき、アプリサブネット（複数可）９２６は、コントロールプレーンデータティア９２８に含まれるＤＢサブネット（複数可）９３０と、サービスゲートウェイ９３６（たとえば、図８のサービスゲートウェイ）と、ＮＡＴ（ネットワークアドレス変換）ゲートウェイ９３８（たとえば、図８のＮＡＴゲートウェイ８３８）とに通信可能に連結できる。コントロールプレーンＶＣＮ９１６は、サービスゲートウェイ９３６と、ＮＡＴゲートウェイ９３８とを備えることができる。

【０１６６】

コントロールプレーンＶＣＮ９１６は、データプレーンミラーアプリティア９４０（たとえば、図８のデータプレーンミラーアプリティア８４０）を備えることができる。データプレーンミラーアプリティア９４０は、アプリサブネット（複数可）９２６を備えることができる。データプレーンミラーアプリティア９４０に含まれるアプリサブネット（複数可）９２６は、コンピューティングインスタンス９４４を実行できる（たとえば、図８のコンピューティングインスタンス８４４と同様の）ＶＮＩＣ（仮想ネットワークインターフェースコントローラ）９４２（たとえば、８４２のＶＮＩＣ）を備えることができる。コンピューティングインスタンス９４４は、データプレーンミラーアプリティア９４０のアプリサブネット（複数可）９２６と、データプレーンアプリティア９４６（たとえば、図８のデータプレーンアプリティア８４６）に含めることができるアプリサブネット（複数可）９２６との、データプレーンミラーアプリティア９４０に含まれるＶＮＩＣ９４２およびデータプレーンアプリティア９４６に含まれるＶＮＩＣ９４２を介した通信を容易にできる。

【０１６７】

コントロールプレーンＶＣＮ９１６に含まれるインターネットゲートウェイ９３４は、メタデータ管理サービス９５２（たとえば、図８のメタデータ管理サービス８５２）に通信可能に連結できる。メタデータ管理サービス９５２は、パブリックインターネット９５４（たとえば、図８のパブリックインターネット８５４）に通信可能に連結できる。パブリックインターネット９５４は、コントロールプレーンＶＣＮ９１６に含まれるＮＡＴゲートウェイ９３８に通信可能に連結できる。コントロールプレーンＶＣＮ９１６に含まれるサービスゲートウェイ９３６は、クラウドサービス９５６（たとえば、図８のクラウドサービス８５６）に通信可能に連結できる。

【０１６８】

いくつかの例では、データプレーンＶＣＮ９１８は、顧客テナンシ９２１に含めることができる。この場合、ＩaaSプロバイダは、顧客ごとにコントロールプレーンＶＣＮ９１６を提供してもよく、ＩaaSプロバイダは、顧客ごとに、サービステナンシ９１９に含まれる一意のコンピューティングインスタンス９４４を設置してもよい。各コンピューティングインスタンス９４４は、サービステナンシ９１９に含まれるコントロールプレーンＶＣＮ９１６と、顧客テナンシ９２１に含まれるデータプレーンＶＣＮ９１８との通信を可能にし得る。コンピューティングインスタンス９４４によって、サービステナンシ９１９に含まれるコントロールプレーンＶＣＮ９１６においてプロビジョニングされるリソースを、顧客テナンシ９２１に含まれるデータプレーンＶＣＮ９１８においてデプロイまたは使用できるようになる。

【０１６９】

その他の例では、ＩaaSプロバイダの顧客は、顧客テナンシ９２１に収められているデータベースを有してもよい。この例では、コントロールプレーンＶＣＮ９１６は、アプリサブネット（複数可）９２６を備えることができるデータプレーンミラーアプリティア９４０を備えることができる。データプレーンミラーアプリティア９４０は、データプレーンＶＣＮ９１８に存在できるが、データプレーンミラーアプリティア９４０は、データプレーンＶＣＮ９１８に収められていなくてもよい。すなわち、データプレーンミラーアプリティア９４０は、顧客テナンシ９２１へのアクセスを有してもよいが、データプレーン

ンミラーアプリアティア 940 は、データプレーン VCN 918 に存在していなくてもよく、または、IaaS プロバイダの顧客によって所有または操作されなくてもよい。データプレーンミラーアプリアティア 940 は、データプレーン VCN 918 を呼び出すように構成されていればよく、コントロールプレーン VCN 916 に含まれるエンティティを呼び出すように構成されなくてもよい。顧客は、コントロールプレーン VCN 916 にプロビジョニングされたデータプレーン VCN 918 にあるリソースをデプロイまたは使用することを望み得、データプレーンミラーアプリアティア 940 は、顧客がリソースを所望にデプロイまたは利用することを容易にできる。

【0170】

いくつかの実施の形態では、IaaS プロバイダの顧客は、データプレーン VCN 918 にフィルタを適用できる。本実施の形態では、顧客は、どのデータプレーン VCN 918 にアクセスできるかを決定でき、顧客は、データプレーン VCN 918 からパブリックインターネット 954 へのアクセスを制限し得る。IaaS プロバイダは、任意の外部ネットワークまたはデータベースへのデータプレーン VCN 918 のアクセスにフィルタを適用できなくともよく、または制御できなくともよい。顧客テナンシ 921 に含まれるデータプレーン VCN 918 に顧客がフィルタを適用することおよび制御することで、データプレーン VCN 918 をその他の顧客およびパブリックインターネット 954 から隔離するのに役立てることができる。

【0171】

いくつかの実施の形態では、パブリックインターネット 954、コントロールプレーン VCN 916、またはデータプレーン VCN 918 上に存在しない可能性のあるサービスにアクセスするために、サービスゲートウェイ 936 によってクラウドサービス 956 を呼び出すことができる。クラウドサービス 956 とコントロールプレーン VCN 916 またはデータプレーン VCN 918 との接続は、繋がっていなかったり、継続していなかったりしてもよい。クラウドサービス 956 は、IaaS プロバイダが所有または操作する異なるネットワーク上に存在していてもよい。クラウドサービス 956 は、サービスゲートウェイ 936 からの呼び出しを受信するように構成されてもよく、パブリックインターネット 954 からの呼び出しを受信しないように構成されてもよい。クラウドサービス 956 は、その他のクラウドサービス 956 から隔離されていてもよく、コントロールプレーン VCN 916 は、コントロールプレーン VCN 916 と同じリージョンにないクラウドサービス 956 から隔離されていてもよい。たとえば、コントロールプレーン VCN 916 が「リージョン 1」に位置し、クラウドサービス「デプロイメント 8」が、リージョン 1 および「リージョン 2」に位置してもよい。リージョン 1 に位置するコントロールプレーン VCN 916 に含まれるサービスゲートウェイ 936 によってデプロイメント 8 の呼び出しが行われた場合、この呼び出しは、リージョン 1 にあるデプロイメント 8 に送信され得る。この例では、コントロールプレーン VCN 916、またはリージョン 1 にあるデプロイメント 8 は、リージョン 2 にあるデプロイメント 8 に通信可能に連結または通信していなくてもよい。

【0172】

図 10 は、少なくとも 1 つの実施の形態に係る、IaaS アーキテクチャの別の例示的なパターンを示すブロック図 1000 である。サービスオペレータ 1002 (たとえば、図 8 のサービスオペレータ 802) は、セキュリティ保護されたホストテナンシ 1004 (たとえば、図 8 のセキュリティ保護されたホストテナンシ 804) に通信可能に連結できる。セキュリティ保護されたホストテナンシ 1004 は、VCN (仮想クラウドネットワーク) 1006 (たとえば、図 8 の VCN 806) と、セキュリティ保護されたホストサブネット 1008 (たとえば、図 8 のセキュリティ保護されたホストサブネット 808) とを備えることができる。VCN 1006 は、SSH VCN 1012 に含まれる LPG 1010 を介して SSH VCN 1012 (たとえば、図 8 の SSH VCN 812) に通信可能に連結できる LPG 1010 (たとえば、図 8 の LPG 810) を備えることができる。SSH VCN 1012 は、SSH サブネット 1014 (たとえば、図 8 の S

10

20

30

40

50

S Hサブネット814)を備えることができ、S S H V C N 1 0 1 2は、コントロールプレーンV C N 1 0 1 6に含まれるL P G 1 0 1 0を介してコントロールプレーンV C N 1 0 1 6(たとえば、図8のコントロールプレーンV C N 8 1 6)に通信可能に連結でき、データプレーンV C N 1 0 1 8に含まれるL P G 1 0 1 0を介してデータプレーンV C N 1 0 1 8(たとえば、図8のデータプレーン818)に通信可能に連結できる。コントロールプレーンV C N 1 0 1 6およびデータプレーンV C N 1 0 1 8は、サービステナンシ1019(たとえば、図8のサービステナンシ819)に含めることができる。

【0173】

コントロールプレーンV C N 1 0 1 6は、L B(ロードバランサ)サブネット(複数可)1022(たとえば、図8のL Bサブネット(複数可)822)を含めることができるコントロールプレーンD M Zティア1020(たとえば、図8のコントロールプレーンD M Zティア820)と、(たとえば、図8のアプリサブネット(複数可)826と同様の)アプリサブネット(複数可)1026を含めることができるコントロールプレーンアプリティア1024(たとえば、図8のコントロールプレーンアプリティア824)と、D Bサブネット(複数可)1030を含めることができるコントロールプレーンデータティア1028(たとえば、図8のコントロールプレーンデータティア828)とを備えることができる。コントロールプレーンD M Zティア1020に含まれるL Bサブネット(複数可)1022は、コントロールプレーンアプリティア1024に含まれるアプリサブネット(複数可)1026と通信可能に連結でき、コントロールプレーンV C N 1 0 1 6に含めることができるインターネットゲートウェイ1034(たとえば、図8のインターネットゲートウェイ834)と通信可能に連結でき、アプリサブネット(複数可)1026は、コントロールプレーンデータティア1028に含まれるD Bサブネット(複数可)1030と通信可能に連結でき、サービスゲートウェイ1036(たとえば、図8のサービスゲートウェイ)およびN A T(ネットワークアドレス変換)ゲートウェイ1038(たとえば、図8のN A Tゲートウェイ838)と通信可能に連結できる。コントロールプレーンV C N 1 0 1 6は、サービスゲートウェイ1036およびN A Tゲートウェイ1038を備えることができる。

【0174】

データプレーンV C N 1 0 1 8は、データプレーンアプリティア1046(たとえば、図8のデータプレーンアプリティア846)と、データプレーンD M Zティア1048(たとえば、図8のデータプレーンD M Zティア848)と、データプレーンデータティア1050(たとえば、図8のデータプレーンデータティア850)とを備えることができる。データプレーンD M Zティア1048は、L Bサブネット(複数可)1022を備えることができる。L Bサブネット1022は、データプレーンアプリティア1046の信頼できるアプリサブネット(複数可)1060および信頼できないアプリサブネット(複数可)1062に通信可能に連結でき、データプレーンV C N 1 0 1 8に含まれるインターネットゲートウェイ1034に通信可能に連結できる。信頼できるアプリサブネット(複数可)1060は、データプレーンV C N 1 0 1 8に含まれるサービスゲートウェイ1036と、データプレーンV C N 1 0 1 8に含まれるN A Tゲートウェイ1038と、データプレーンデータティア1050に含まれるD Bサブネット(複数可)1030とに通信可能に連結できる。信頼できないアプリサブネット(複数可)1062は、データプレーンV C N 1 0 1 8に含まれるサービスゲートウェイ1036と、データプレーンデータティア1050に含まれるD Bサブネット(複数可)1030に通信可能に連結できる。データプレーンデータティア1050は、D Bサブネット(複数可)1030を含み得る。D Bサブネット1030は、データプレーンV C N 1 0 1 8に含まれるサービスゲートウェイ1036に通信可能に連結できる。

【0175】

信頼できないアプリサブネット(複数可)1062は、1つ以上の主要V N I C 1 0 6 4(1)~(N)を備えることができる。V N I C 1 0 6 4(1)~(N)は、テナントV M(仮想マシン)1066(1)~(N)に通信可能に連結できる。各テナントV M 1

10

20

30

40

50

066(1)～(N)は、各アプリサブネット1067(1)～(N)に通信可能に連結できる。アプリサブネット1067(1)～(N)は、それぞれのコンテナエグレスVCN1068(1)～(N)に含めることができる。コンテナエグレスVCN1068(1)～(N)は、それぞれの顧客テナンシ1070(1)～(N)に含めることができる。それぞれの補助VNIC1072(1)～(N)は、データプレーンVCN1018に含まれる信頼できないアプリサブネット(複数可)1062とコンテナエグレスVCN1068(1)～(N)に含まれるアプリサブネットとの通信を容易にできる。各コンテナエグレスVCN1068(1)～(N)は、パブリックインターネット1054(たとえば、図8のパブリックインターネット854)に通信可能に連結できるNATゲートウェイ1038を備えることができる。

10

【0176】

コントロールプレーンVCN1016に含まれるインターネットゲートウェイ1034およびデータプレーンVCN1018に含まれるインターネットゲートウェイ1034は、メタデータ管理サービス1052(たとえば、図8のメタデータ管理システム852)に通信可能に連結できる。メタデータ管理サービス1052は、パブリックインターネット1054に通信可能に連結できる。パブリックインターネット1054は、コントロールプレーンVCN1016に含まれるNATゲートウェイ1038およびデータプレーンVCN1018に含まれるNATゲートウェイ1038に通信可能に連結できる。コントロールプレーンVCN1016に含まれるサービスゲートウェイ1036およびデータプレーンVCN1018に含まれるサービスゲートウェイ1036は、クラウドサービス1056に通信可能に連結できる。

20

【0177】

いくつかの実施の形態では、データプレーンVCN1018を顧客テナンシ1070と一体化することができる。この一体化は、コードを実行する場合にサポートを希望する場合など、場合によっては、IaaSプロバイダの顧客にとって有用または望ましいであろう。顧客は、破壊的であるかもしれない実行用コードを提供する可能性があり、その他の顧客リソースと通信する可能性があり、または、望ましくない作用効果を生じさせる可能性がある。これに応じて、IaaSプロバイダは、顧客がIaaSプロバイダに提供したコードを実行するかどうかを判断してもよい。

【0178】

いくつかの例では、IaaSプロバイダの顧客は、IaaSプロバイダに一時的なネットワークアクセスを付与して、データプレーンティアアプリ1046にアタッチする機能を要求してもよい。この機能を実行するためのコードは、VM1066(1)～(N)において実行され得、コードは、データプレーンVCN1018上のその他の場所で動作するように構成されなくてもよい。各VM1066(1)～(N)は、1つの顧客テナンシ1070に接続され得る。VM1066(1)～(N)に含まれるそれぞれのコンテナ1071(1)～(N)は、このコードを実行するように構成され得る。この場合、2つの隔離がある可能性がある(たとえば、信頼できないアプリサブネット(複数可)1062に含まれる少なくともVM1066(1)～(N)に含まれ得るコンテナ1071(1)～(N)がコードを実行している。)。隔離が2つあることで、誤ったコードもしくは望ましくないコードがIaaSプロバイダのネットワークに損害を与えないように、または、異なる顧客のネットワークに損害を与えないようにすることに役立つであろう。コンテナ1071(1)～(N)は、顧客テナンシ1070に通信可能に連結され得、顧客テナンシ1070からデータを送信または受信するように構成され得る。コンテナ1071(1)～(N)は、データプレーンVCN1018にあるその他のエンティティからデータを送信または受信するように構成されなくてもよい。コードの実行が完了すると、IaaSプロバイダは、コンテナ1071(1)～(N)を強制終了または廃棄し得る。

30

40

【0179】

いくつかの実施の形態では、信頼できるアプリサブネット(複数可)1060は、IaaSプロバイダが所有または操作し得るコードを実行し得る。本実施の形態では、信頼で

50

きるアプリサブネット（複数可）1060は、DBサブネット（複数可）1030に通信可能に連結され得、DBサブネット（複数可）1030においてCRUD操作を行うように構成され得る。信頼できないアプリサブネット（複数可）1062は、DBサブネット（複数可）1030に通信可能に連結され得るが、本実施の形態では、信頼できないアプリサブネット（複数可）は、DBサブネット（複数可）1030において読み取り操作を行うように構成され得る。各顧客のVM1066（1）～（N）に含めることができ、顧客からのコードを実行し得るコンテナ1071（1）～（N）は、DBサブネット（複数可）1030に通信可能に連結されなくてもよい。

【0180】

その他の実施の形態では、コントロールプレーンVCN1016とデータプレーンVCN1018とは、直接通信可能に連結されなくてもよい。本実施の形態では、コントロールプレーンVCN1016とデータプレーンVCN1018との間に直接の通信がなくてもよい。しかしながら、通信は、少なくとも1つの方法を通して間接的に発生し得る。LPG1010は、コントロールプレーンVCN1016とデータプレーンVCN1018との通信を容易にできるIaaSプロバイダによって確立され得る。別の例では、コントロールプレーンVCN1016またはデータプレーンVCN1018は、サービスゲートウェイ1036を経由してクラウドサービス1056を呼び出すことができる。たとえば、コントロールプレーンVCN1016からクラウドサービス1056に対する呼び出しは、データプレーンVCN1018と通信できるサービスを求める要求を含めることができる。

【0181】

図11は、少なくとも1つの実施の形態に係る、IaaSアーキテクチャの別の例示的なパターンを示すブロック図1100である。サービスオペレータ1102（たとえば、図8のサービスオペレータ802）は、セキュリティ保護されたホストテナンシ1104（たとえば、図8のセキュリティ保護されたホストテナンシ804）に通信可能に連結できる。セキュリティ保護されたホストテナンシ1104は、VCN（仮想クラウドネットワーク）1106（たとえば、図8のVCN806）と、セキュリティ保護されたホストサブネット1108（たとえば、図8のセキュリティ保護されたホストサブネット808）とを備えることができる。VCN1106は、SSH VCN1112に含まれるLPG1110を介してSSH VCN1112（たとえば、図8のSSH VCN812）に通信可能に連結できるLPG1110（たとえば、図8のLPG810）を備えることができる。SSH VCN1112は、SSHサブネット1114（たとえば、図8のSSHサブネット814）を備えることができ、SSH VCN1112は、コントロールプレーンVCN1116に含まれるLPG1110を介してコントロールプレーンVCN1116（たとえば、図8のコントロールプレーンVCN816）に通信可能に連結でき、データプレーンVCN1118に含まれるLPG1110を介してデータプレーンVCN1118（たとえば、図8のデータプレーン818）に通信可能に連結できる。コントロールプレーンVCN1116およびデータプレーンVCN1118は、サービステナンシ1119（たとえば、図8のサービステナンシ819）に含めることができる。

【0182】

コントロールプレーンVCN1116は、LBサブネット（複数可）1122（たとえば、図8のLBサブネット（複数可）822）を含めることができるコントロールプレーンDMZティア1120（たとえば、図8のコントロールプレーンDMZティア820）と、アプリサブネット（複数可）1126（たとえば、図8のアプリサブネット（複数可）826）を含めることができるコントロールプレーンアプリティア1124（たとえば、図8のコントロールプレーンアプリティア824）と、DBサブネット（複数可）1130（たとえば、図10のDBサブネット（複数可）1030）を含めることができるコントロールプレーンデータティア1128（たとえば、図8のコントロールプレーンデータティア828）とを備えることができる。コントロールプレーンDMZティア1120に含まれるLBサブネット（複数可）1122は、コントロールプレーンアプリティア1

1 2 4に含まれるアプリサブネット（複数可）1 1 2 6と通信可能に連結でき、コントロールプレーンV C N 1 1 1 6に含めることができるインターネットゲートウェイ1 1 3 4（たとえば、図8のインターネットゲートウェイ8 3 4）と通信可能に連結でき、アプリサブネット（複数可）1 1 2 6は、コントロールプレーンデータティア1 1 2 8に含まれるDBサブネット（複数可）1 1 3 0と通信可能に連結でき、サービスゲートウェイ1 1 3 6（たとえば、図8のサービスゲートウェイ）およびN A T（ネットワークアドレス変換）ゲートウェイ1 1 3 8（たとえば、図8のN A Tゲートウェイ8 3 8）と通信可能に連結できる。コントロールプレーンV C N 1 1 1 6は、サービスゲートウェイ1 1 3 6およびN A Tゲートウェイ1 1 3 8を備えることができる。

【0 1 8 3】

データプレーンV C N 1 1 1 8は、データプレーンアプリティア1 1 4 6（たとえば、図8のデータプレーンアプリティア8 4 6）と、データプレーンD M Zティア1 1 4 8（たとえば、図8のデータプレーンD M Zティア8 4 8）と、データプレーンデータティア1 1 5 0（たとえば、図8のデータプレーンデータティア8 5 0）とを備えることができる。データプレーンD M Zティア1 1 4 8は、L Bサブネット（複数可）1 1 2 2を備えることができる。L Bサブネット1 1 2 2は、データプレーンアプリティア1 1 4 6の信頼できるアプリサブネット（複数可）1 1 6 0（たとえば、図10の信頼できるアプリサブネット（複数可）1 0 6 0）および信頼できないアプリサブネット（複数可）1 1 6 2（たとえば、図10の信頼できないアプリサブネット（複数可）1 0 6 2）に通信可能に連結でき、データプレーンV C N 1 1 1 8に含まれるインターネットゲートウェイ1 1 3 4に通信可能に連結できる。信頼できるアプリサブネット（複数可）1 1 6 0は、データプレーンV C N 1 1 1 8に含まれるサービスゲートウェイ1 1 3 6と、データプレーンV C N 1 1 1 8に含まれるN A Tゲートウェイ1 1 3 8と、データプレーンデータティア1 1 5 0に含まれるDBサブネット（複数可）1 1 3 0とに通信可能に連結できる。信頼できないアプリサブネット（複数可）1 1 6 2は、データプレーンV C N 1 1 1 8に含まれるサービスゲートウェイ1 1 3 6と、データプレーンデータティア1 1 5 0に含まれるDBサブネット（複数可）1 1 3 0とに通信可能に連結できる。データプレーンデータティア1 1 5 0は、DBサブネット（複数可）1 1 3 0を含み得る。DBサブネット1 1 3 0は、データプレーンV C N 1 1 1 8に含まれるサービスゲートウェイ1 1 3 6に通信可能に連結できる。

【0 1 8 4】

信頼できないアプリサブネット（複数可）1 1 6 2は、主要V N I C 1 1 6 4（1）～（N）を備えることができる。V N I C 1 1 6 4（1）～（N）は、信頼できないアプリサブネット（複数可）1 1 6 2に存在するテナントV M（仮想マシン）1 1 6 6（1）～（N）に通信可能に連結できる。各テナントV M 1 1 6 6（1）～（N）は、それぞれのコンテナ1 1 6 7（1）～（N）においてコードを実行でき、アプリサブネット1 1 2 6に通信可能に連結できる。アプリサブネット1 1 2 6は、データプレーンアプリティア1 1 4 6に含めることができる。データプレーンアプリティア1 1 4 6は、コンテナエグレスV C N 1 1 6 8に含めることができる。それぞれの補助V N I C 1 1 7 2（1）～（N）は、データプレーンV C N 1 1 1 8に含まれる信頼できないアプリサブネット（複数可）1 1 6 2とコンテナエグレスV C N 1 1 6 8に含まれるアプリサブネットとの通信を容易にできる。コンテナエグレスV C N 1 1 6 8は、パブリックインターネット1 1 5 4（たとえば、図8のパブリックインターネット8 5 4）に通信可能に連結できるN A Tゲートウェイ1 1 3 8を備えることができる。

【0 1 8 5】

コントロールプレーンV C N 1 1 1 6に含まれるインターネットゲートウェイ1 1 3 4およびデータプレーンV C N 1 1 1 8に含まれるインターネットゲートウェイ1 1 3 4は、メタデータ管理サービス1 1 5 2（たとえば、図8のメタデータ管理システム8 5 2）に通信可能に連結できる。メタデータ管理サービス1 1 5 2は、パブリックインターネット1 1 5 4に通信可能に連結できる。パブリックインターネット1 1 5 4は、コントロー

10

20

30

40

50

ルプレーンVCN1116に含まれるNATゲートウェイ1138およびデータプレーンVCN1118に含まれるNATゲートウェイ1138に通信可能に連結できる。コントロールプレーンVCN1116に含まれるサービスゲートウェイ1136およびデータプレーンVCN1118に含まれるサービスゲートウェイ1136は、クラウドサービス1156に通信可能に連結できる。

【0186】

いくつかの例では、図11のブロック図1100のアーキテクチャが示すパターンは、図10のブロック図1000のアーキテクチャが示すパターンに対する例外であると考えら得、IaaSプロバイダが顧客と直接通信できない（たとえば、リージョンが切り離されている）場合、IaaSプロバイダの顧客にとってブロック図1100のアーキテクチャが示すパターンは望ましいであろう。顧客ごとにVM1166（1）～（N）に含まれるそれぞれのコンテナ1167（1）～（N）には、顧客はリアルタイムにアクセスできる。コンテナ1167（1）～（N）は、コンテナエグレスVCN1168に含めることができるデータプレーンアプリティア1146のアプリサブネット（複数可）1126に含まれるそれぞれの補助VNIC1172（1）～（N）を呼び出すように構成され得る。補助VNIC1172（1）～（N）は、NATゲートウェイ1138に呼び出しを送信できる。NATゲートウェイ1138は、当該呼び出しをパブリックインターネット1154に送信し得る。この例では、顧客がリアルタイムでアクセスできるコンテナ1167（1）～（N）をコントロールプレーンVCN1116から隔離でき、データプレーンVCN1118に含まれるその他のエンティティから隔離できる。また、コンテナ1167（1）～（N）は、その他の顧客のリソースから隔離され得る。

【0187】

その他の例では、顧客は、コンテナ1167（1）～（N）を使用してクラウドサービス1156を呼び出すことができる。この例では、顧客は、クラウドサービス1156にサービスを要求するコードをコンテナ1167（1）～（N）において実行し得る。コンテナ1167（1）～（N）は、この要求を補助VNIC1172（1）～（N）に送信できる。補助VNIC1172（1）～（N）は、NATゲートウェイに要求を送信できる。NATゲートウェイは、パブリックインターネット1154に要求を送信できる。パブリックインターネット1154は、コントロールプレーンVCN1116に含まれるLBサブネット（複数可）1122にインターネットゲートウェイ1134を介して要求を送信できる。要求が有効であると判断されたことに応答して、LBサブネット（複数可）は、アプリサブネット（複数可）1126に要求を送信できる。アプリサブネット（複数可）1126は、サービスゲートウェイ1136を介してクラウドサービス1156に要求を送信できる。

【0188】

図示したIaaSアーキテクチャ800、900、1000、1100が、図示された構成要素以外の構成要素を有し得ることを理解されたい。さらに、図示した実施の形態は、本開示の実施の形態を組み込み得るクラウドインフラストラクチャシステムのいくつかの例に過ぎない。いくつかのその他の実施の形態では、IaaSシステムは、図示した構成要素よりも多い数の構成要素を有してもよく、図示した構成要素よりも少ない数の構成要素を有してもよく、2つ以上の構成要素を組み合わせてもよく、または構成要素の構成もしくはは配置が異なってもよい。

【0189】

特定の実施の形態では、セルフサービスの、サブスクリプション方式で伸縮自在にスケラブルであり信頼性があり、かつ高い可用性を有するセキュアな方法で顧客に届けられるアプリケーション一式、ミドルウェア、およびデータベースサービス提供物を含んでもよい。このようなIaaSシステムの例として、本願の譲受人が提供するOCI（Oracle Cloud Infrastructure）がある。

【0190】

図12は、本開示の様々な実施の形態が実施され得るコンピュータシステム1200の

例を示す図である。システム1200を使用して、上述したコンピュータシステムのいずれかを実現してもよい。図に示すように、コンピュータシステム1200は、バス・サブシステム1202を介していくつかの周辺サブシステムと通信する処理装置1204を備える。これらの周辺サブシステムは、処理高速化装置1206と、I/Oサブシステム1208と、ストレージサブシステム1218と、通信サブシステム1224とを含んでもよい。ストレージサブシステム1218は、有形のコンピュータ読み取り可能な記憶媒体1222と、システムメモリ1210とを含む。

【0191】

バス・サブシステム1202は、コンピュータシステム1200の様々な構成要素およびサブシステムを互いに意図した通りに通信させるためのメカニズムを提供する。バス・サブシステム1202は、1つのバスとして図示されているが、バス・サブシステムの別の実施の形態は、複数のバスを利用してもよい。バス・サブシステム1202は、各種のバスアーキテクチャを使用するメモリバスまたはメモリコントローラ、周辺バス、およびローカルバスを含むいくつかの種類のバス構造のうちのいずれかであってもよい。たとえば、このようなアーキテクチャは、ISA (Industry Standard Architecture) バス、MCA (Micro Channel Architecture) バス、EISA (Enhanced ISA) バス、VESA (Video Electronics Standards Association) ローカルバス、およびPCI (Peripheral Component Interconnect) バスを含んでもよく、これらは、IEEE P1386.1 標準規格に準拠して製造されるMezzanineバスとして実現され得る。

【0192】

1つ以上の集積回路（たとえば、従来のマイクロプロセッサまたはマイクロコントローラ）として実現され得る処理装置1204は、コンピュータシステム1200の動作を制御する。処理装置1204には、1つ以上のプロセッサが含まれてもよい。これらのプロセッサは、シングルコアプロセッサまたはマルチコアプロセッサを含んでもよい。特定の実施の形態では、処理装置1204は、シングルコアプロセッサまたはマルチコアプロセッサを各々が含んだ1つ以上の独立した処理装置1232および／または1234として実現されてもよい。また、その他の実施の形態では、処理装置1204は、2つのデュアルコアプロセッサを1つのチップに組み込むことによって形成されるクアッドコア処理装置として実現されてもよい。

【0193】

様々な実施の形態では、処理装置1204は、プログラムコードに応答していろいろなプログラムを実行でき、複数の同時に実行しているプログラムまたはプロセスを維持することができる。いつでも、実行されるプログラムコードの一部またはすべては、プロセッサ（複数可）1204に、および／またはストレージサブシステム1218に存在し得る。適したプログラミングによって、プロセッサ（複数可）1204は、上述した様々な機能を提供できる。コンピュータシステム1200は、処理高速化装置1206をさらに備えてもよい。処理高速化装置1206は、DSP (Digital Signal Processor) および／または専用プロセッサなどを含み得る。

【0194】

I/Oサブシステム1208は、ユーザインタフェース入力装置と、ユーザインタフェース出力装置とを含んでもよい。ユーザインタフェース入力装置は、キーボード、マウスもしくはトラックボールなどのポインティングデバイス、タッチパッドもしくはディスプレイに組み込まれたタッチスクリーン、スクロールホイール、クリックホイール、ダイヤル、ボタン、スイッチ、キーパッド、ボイスコマンド認識システムを有する音声入力装置、マイクロホン、および他の種類の入力装置を含んでもよい。また、ユーザインタフェース入力装置は、たとえば、ジェスチャコマンドおよび音声コマンドを用いた自然なユーザインタフェースによってユーザがMicrosoft Xbox（登録商標）360ゲームコントローラなどの入力装置を制御およびそれとやり取りすることを可能にするMic

rosoft Kinect（登録商標）モーションセンサなどの動き検知デバイスおよび／またはジェスチャ認識デバイスを含んでもよい。また、ユーザインタフェース入力装置は、ユーザの目の行動（たとえば、写真を撮影しているおよび／またはメニュー選択を行っている間の「まばたき」）を検出し、目の仕草（eye gesture）を変換して入力装置（たとえば、Google Glass（登録商標））への入力とするGoogle Glass（登録商標）まばたき検出装置などのアイジェスチャ認識デバイスを含んでもよい。これに加えて、ユーザインタフェース入力装置は、ユーザがボイスコマンドによって音声認識システム（たとえば、Siri（登録商標）ナビゲータ）とやり取りすることを可能にする音声認識検知デバイスを含んでもよい。

【0195】

10

また、ユーザインタフェース入力装置は、3D（3次元）マウス、ジョイスティックもしくはポインティングスティック、ゲームパッドおよびグラフィックタブレット、ならびに、スピーカ、デジタルカメラ、デジタルカムコーダー、ポータブルメディアプレーヤ、ウェブカム、イメージスキャナ、指紋スキャナ、バーコードリーダー3Dスキャナ、3Dプリンタ、レーザー測距器、および視線追跡装置などのオーディオ／ビジュアル装置を含むが、これに限定されない。これに加えて、ユーザインタフェース入力装置は、たとえば、コンピュータ断層撮影法、磁気共鳴画像、陽電子放出断層撮影装置、超音波検査デバイスなど、医用画像入力装置を含んでもよい。また、ユーザインタフェース入力装置は、たとえば、MIDIキーボード、デジタル楽器などのオーディオ入力装置を含んでもよい。

【0196】

20

ユーザインタフェース出力装置は、表示サブシステム、インジケータライト、または音声出力装置などの非視覚的表示装置などを含んでもよい。表示サブシステムは、CRT（ブラウン管）、LCD（液晶ディスプレイ）またはプラズマディスプレイを使用するものなどのフラットパネル表示装置、投影装置、タッチスクリーンなどであってもよい。一般に、「出力装置」という用語の使用は、コンピュータシステム1200からユーザまたは他のコンピュータに情報を出力するためのあらゆる種類のデバイスおよびメカニズムを含むことを意図する。たとえば、ユーザインタフェース出力装置は、モニタ、プリンタ、スピーカ、ヘッドホン、自動車ナビゲーションシステム、作図装置、音声出力装置、およびモデムなど、文字、図形、および音声／映像情報を視覚的に伝えるいろいろな表示装置を含み得るが、これに限定されない。

30

【0197】

コンピュータシステム1200は、システムメモリ1210内に現在位置していると図示されているソフトウェア要素を含むストレージサブシステム1218から構成されてもよい。システムメモリ1210は、処理装置1204上でロード可能かつ実行可能なプログラム命令、およびこれらのプログラムの実行中に生成されるデータを格納してもよい。

【0198】

コンピュータシステム1200の構成および種類によっては、システムメモリ1210は、揮発性メモリであってもよく（RAM（ランダムアクセスメモリ）など）、および／または不揮発性メモリ（ROM（読み出し専用メモリ）、フラッシュメモリなど）であってもよい。RAMは、通常、処理装置1204がすぐにアクセスできる、ならびに／または現在操作および実行しているデータおよび／もしくはプログラムモジュールを含む。いくつかの実装形態において、システムメモリ1210は、SRAM（スタティックRAM）またはDRAM（ダイナミックRAM）など、複数の異なる種類のメモリを含んでもよい。いくつかの実装形態において、起動中などで、コンピュータシステム1200内の要素間で情報を転送することを助ける基本ルーチンを含むBIOS（Basic Input／Output System）は、通常、ROMに格納されてもよい。また、一例として、システムメモリ1210は、クライアントアプリケーション、ウェブブラウザ、ミッドティア・アプリケーション、RDBMS（リレーショナルデータベース管理システム）などを含み得るアプリケーションプログラム1212と、プログラムデータ1214と、オペレーティングシステム1216とを含む。一例として、オペレーティングシステム

40

50

1216は、様々なバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、および／もしくはLinuxオペレーティングシステム、いろいろな市販のUNIX（登録商標）もしくはUNIXに似たオペレーティングシステム（いろいろなGNU／Linuxオペレーティングシステム、Google Chrome（登録商標）OSなどを含むが、これに限定されない）、ならびに／またはiOS、Windows（登録商標）Phone、Android（登録商標）OS、BlackBerry（登録商標）12OS、およびPalm（登録商標）OSオペレーティングシステムなど、モバイルオペレーティングシステムを含んでもよい。

【0199】

また、ストレージサブシステム1218は、いくつかの実施の形態の機能を提供する基本プログラミング構成およびデータ構成を格納するための有形のコンピュータ読み取り可能な記憶媒体を提供してもよい。プロセッサによって実行されると上述の機能を提供するソフトウェア（プログラム、コードモジュール、命令）がストレージサブシステム1218に格納されてもよい。これらのソフトウェアモジュールまたは命令は、処理装置1204によって実行されてもよい。また、ストレージサブシステム1218は、本開示に従って使用されるデータを格納するためのリポジトリを提供してもよい。

【0200】

また、ストレージサブシステム1200は、コンピュータ読み取り可能な記憶媒体1222にさらに接続され得るコンピュータ読み取り可能な記憶媒体リーダー1220を含んでもよい。システムメモリ1210と合わせて、必要に応じてシステムメモリ1210と組み合わせて、コンピュータ読み取り可能な記憶媒体1222は、遠隔の記憶装置、ローカル記憶装置、固定記憶装置、および／またはリムーバブル記憶装置、ならびにコンピュータ読み取り可能な情報を一時的におよび／またはさらに永続して含み、格納し、送信し、および取り出すための記憶媒体を包括的に表してもよい。

【0201】

コードまたはコードの一部を含んだコンピュータ読み取り可能な記憶媒体1222は、情報の格納および／または伝送のための任意の方法および技術で実現される揮発性媒体および不揮発性媒体、取り外し可能な媒体および固定型媒体などの記憶媒体および通信媒体を含む、当技術分野で知られているまたは使われている任意の適切な媒体も含んでもよいが、これに限定されない。これは、RAM、ROM、EEPROM（Electrically Erasable Programmable ROM）、フラッシュメモリ、もしくは他のメモリテクノロジー、CD-ROM、DVD（Digital Versatile Disk）、もしくは他の光記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置、もしくは他の磁気記憶装置などの有形のコンピュータ読み取り可能な記憶媒体、またはその他の有形のコンピュータ読み取り可能な媒体を含み得る。これは、データ信号、データ伝送など無形のコンピュータ読み取り可能な媒体、または所望の情報を伝送するために使用され得るその他の媒体、およびコンピューティングシステム1200によってアクセスされ得るその他の媒体なども含み得る。

【0202】

一例として、コンピュータ読み取り可能な記憶媒体1222は、固定型不揮発性磁気媒体から読み出しまたは書き込みを行うハードディスクドライブ、取外し可能な不揮発性磁気ディスクから読み出しまたは書き込みを行う磁気ディスクドライブ、ならびに、CD-ROM、DVD、およびBlu-Ray（登録商標）ディスクなどの取外し可能な不揮発性光ディスクもしくは他の光学媒体から読み出しまたは書き込みを行う光ディスクドライブを含んでもよい。コンピュータ読み取り可能な記憶媒体1222は、Zip（登録商標）ドライブ、フラッシュメモリーカード、USB（Universal Serial Bus）フラッシュドライブ、SD（Secure Digital）カード、DVDディスク、デジタルビデオテープなどを含み得るが、これに限定されない。また、コンピュータ読み取り可能な記憶媒体1222は、フラッシュメモリーベースのSSD（Solid-State Drives）、エンタープライズフラッシュドライブ、ソリッドステー

10

20

30

40

50

トROMなど、不揮発性メモリに基づくSSD (Solid-State Drives) と、ソリッドステートRAM、動的RAM、静的RAM、DRAMベースのSSDなど、揮発性メモリに基づくSSDと、MRAM (Magnetoresistive RAM) SSDと、DRAMとフラッシュメモリとの組合せベースのSSDを使用するハイブリッドSSDとを含んでもよい。これらのディスクドライブおよびそれらの関連するコンピュータ読み取り可能な媒体は、コンピュータ読み取り可能な命令、データ構造、プログラムモジュール、およびその他のコンピュータシステム1200用データの揮発性ストレージを提供してもよい。

【0203】

通信サブシステム1224は、他のコンピュータシステムおよびネットワークへのインターフェースを提供する。通信サブシステム1224は、コンピュータシステム1200からデータを受信し、コンピュータシステム1200から他のシステムにデータを送信するためのインターフェースとして機能する。たとえば、通信サブシステム1224は、コンピュータシステム1200がインターネットを介して1つ以上のデバイスに接続することを可能にしてもよい。いくつかの実施の形態では、通信サブシステム1224は、(たとえば、携帯電話技術、3G、4G、もしくはEDGE (Enhanced Data Rates For Global Evolution) などの次世代データネットワークテクノロジー、WiFi (IEEE 802.11ファミリー標準規格)、他の移動体通信技術、またはそれらの任意の組合せを使用する) ワイヤレス音声ネットワークもしくは／またはデータネットワークにアクセスするためのRF (Radio Frequency) トランシーバコンポーネント、GPS (Global Positioning System) レシーバコンポーネント、および／または他の構成要素を含み得る。いくつかの実施の形態では、通信サブシステム1224は、ワイヤレスインタフェースに加えて、またはワイヤレスインタフェースの代わりに、有線ネットワーク接続性(たとえば、Ethernet)を提供できる。

【0204】

いくつかの実施の形態では、通信サブシステム1224は、コンピュータシステム1200を利用し得る1人以上のユーザに代わって、構造化データフィードおよび／または非構造化データフィード1226、イベントストリーム1228、イベントアップデート1230などの形で入力通信文を受信してもよい。

【0205】

一例として、通信サブシステム1224は、Twitter (登録商標) フィード、Facebook (登録商標) の更新、RSS (Rich Site Summary) フィードなどのwebフィード、および／もしくは1つ以上のサードパーティ情報ソースからのリアルタイム更新など、ソーシャルネットワークならびに／または他のコミュニケーションサービスのユーザからデータフィード1226をリアルタイムで受信するように構成されてもよい。

【0206】

また、これに加えて、通信サブシステム1224は、連続したデータストリームの形でデータを受信するように構成されてもよく、連続したデータストリームは、本質的にはつきりとした終端がない、連続または無限の、リアルタイムイベントおよび／またはイベントアップデート1230のイベントストリーム1228を含んでもよい。連続データを生成するアプリケーションとして、たとえば、センサーデータアプリケーション、チックー、ネットワークパフォーマンス測定ツール(たとえば、ネットワーク監視およびトラフィック管理アプリケーション)、クリックストリーム解析ツール、自動車交通量監視などが挙げられてもよい。

【0207】

また、通信サブシステム1224は、コンピュータシステム1200に接続された1つ以上のストリーミングデータソースコンピュータと通信中であり得る1つ以上のデータベースに、構造化データフィードおよび／または非構造化データフィード1226、イベン

10

20

30

40

50

トストリーム 1 2 2 8、イベントアップデート 1 2 3 0 などを出力するように構成されてもよい。

【0 2 0 8】

コンピュータシステム 1 2 0 0 は、手のひらサイズのポータブルデバイス（たとえば、i P h o n e（登録商標）携帯電話、I P a d（登録商標）コンピューティングタブレット、P D A）、ウェアラブルデバイス（たとえば、G o o g l e G l a s s（登録商標）ヘッドマウントディスプレイ）、P C、ワークステーション、メインフレーム、キオスク、サーバーラック、またはその他のデータ処理システムを含む、様々な種類のうちの 1 つであり得る。

【0 2 0 9】

変わり続けるというコンピュータおよびネットワークの性質のため、図に示すコンピュータシステム 1 2 0 0 の説明は、具体例にすぎない。図に示すシステムよりも多いまたは少ない数の構成要素を有する多くの他の構成が可能である。たとえば、カスタマイズされたハードウェアが使用されてもよく、および／または、ハードウェア、ファームウェア、ソフトウェア（アプレットを含む）、もしくはそれらの組合せで特定の要素が実現されてもよい。さらに、ネットワーク入出力装置など、他のコンピューティングデバイスへの接続を採用してもよい。本明細書に記載の開示および教示に基づいて、当業者であれば、様々な実施の形態を実現するための他のやり方および／または方法が分かるだろう。

【0 2 1 0】

具体的な本開示の実施の形態を説明したが、様々な変更例、代替例、代替的な構成、および均等物も本開示の範囲内に包含される。本開示の実施の形態は、ある特定のデータ処理環境内の動作に制限されず、複数のデータ処理環境内で自由に動作することができる。これに加えて、特定の一続きのトランザクションおよびステップを使用して本開示の実施の形態を説明したが、本開示の範囲は、記載の一続きのトランザクションおよびステップに限られないことは、当業者に明らかであるはずである。上述の実施の形態の様々な特徴および態様は、個々に、または共同で使用されてもよい。

【0 2 1 1】

さらに、ハードウェアとソフトウェアとの特定の組合せを用いて本開示の実施の形態を説明したが、ハードウェアとソフトウェアとの他の組合せも、本開示の範囲内であることを認識されたい。本開示の実施の形態は、ハードウェアのみ、もしくは、ソフトウェアのみで実現されてもよく、またはそれらの組合せを用いて実現されてもよい。本明細書に記載の様々なプロセスは、同じプロセッサまたは任意の組合せのそれぞれ異なるプロセッサ上で実現できる。よって、コンポーネントまたはモジュールが特定の動作を実行するように構成されると説明されている箇所では、このような構成は、たとえば、この動作を実行するように電子回路を設計することによって、この動作を実行するようにプログラム可能な電子回路（マイクロプロセッサなど）をプログラムすることによって、またはそれらの任意の組合せによって達成できる。プロセスは、プロセス間通信のための従来技術を含む、いろいろな技術を使用して通信できるが、これに限定されず、それぞれ異なるペアプロセスは、異なる技術を使用してよく、プロセスの同じペアは、異なる技術を別々のタイミングで使用してもよい。

【0 2 1 2】

明細書および図面は、厳密ではなく一例にすぎないと適宜みなされるべきである。しかしながら、添付の特許請求の範囲に記載された広義の趣旨および範囲から逸脱することなく、追加したり、減らしたり、削除したり、他の変更ならびに変形をそれらに対して行ってもよいことは明白であろう。したがって、具体的な本開示の実施の形態を説明したが、これらは限定ではない。様々な変更例および均等物も、添付の特許請求の範囲に含まれる。

【0 2 1 3】

開示した実施の形態を説明する文脈（特に、添付の特許請求の範囲での文脈）における「a」、「an」および「the」という用語、ならびに同様の指示対象の用語の使用は

10

20

30

40

50

、矛盾のない限り、単数および複数の両方を含むと解釈されるべきである。「comprising」、「having」、「including」、および「containing」という用語は、特に記されていない限り、非限定的な用語であると解釈されるべきである（すなわち、「including、but not limited to（これらを含むが、これらに限定されない）」ことを意味する）。「connected」という用語は、何かが介在している場合であっても、一部または全体が含まれている、取り付けられている、つながり合っていると解釈されるべきである。本明細書において値を範囲で記載していることは、本明細書に特に示されていない限り、その範囲内の個別の各値を個々に参照することを省く手段に過ぎず、個別の各値は、個々に記載されているかの如く明細書に含まれる。本明細書に記載の方法は、すべて、矛盾のない限り、任意の適切な順序で実行できる。本明細書に設けた如何なる例、または例示的な言い回し（たとえば、「such as」）は、本開示の実施の形態により良く光を当てるために過ぎず、特にクレームされていない限り、本開示の範囲を限定しない。本明細書におけるすべての言い回しは、クレームされていない要素が本開示を実施するために必要な要素であることを示す言い回しである、と解釈されるべきでない。

10

【0214】

「X、Y、またはZのうち少なくとも1つ」というフレーズなど、離接的な言い回しは、特に具体的に明示されていない限り、項目や用語などが、X、Y、もしくはZのいずれか、または任意のそれらの組合せ（たとえば、X、Y、および／またはZ）であり得ることを提示するために一般的に使われる範囲内の言い回しであると理解されたい。よって、このような離接的な言い回しは、通常、Xのうち少なくとも1つ、Yのうち少なくとも1つ、またはZのうち少なくとも1つを特定の実施の形態が提示する必要があると、意味する意図はなく、そのように提示する必要はない。

20

【0215】

本開示を実施するために最良であると知られている実施の形態を含む、本開示の好ましい実施の形態を本明細書において説明している。当業者には、上記の説明を読むと、これらの好ましい実施の形態の変形例が明らかになるであろう。当業者であれば、このような変形例を適宜用いることができるはずであり、本開示は、本明細書に具体的に説明した以外の方法で実施されてもよい。したがって、本開示は、適用法によって認められている本明細書に添付の特許請求の範囲に記載の主題の変更例および均等物のすべてを含む。また、それらの想定される変形例における上述した要素の任意の組合せも、本明細書に特に示されていない限り、本開示に含まれる。

30

【0216】

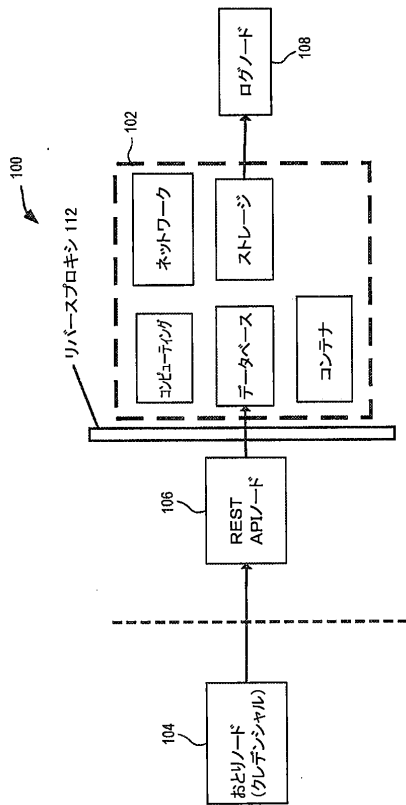
本明細書において引用する刊行物、特許出願文書、および特許文書を含むすべての参考文献は、各参考文献が個々に具体的に引用により本明細書に援用されると示されてその全体が本明細書に記載された場合と同程度に、引用により本明細書に援用する。

【0217】

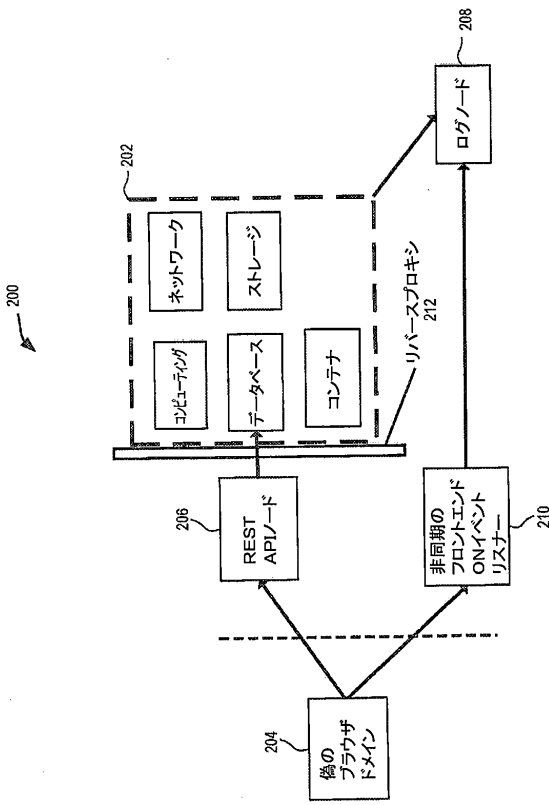
上記の明細書において、本開示の態様をその具体的な実施の形態を参照しながら説明したが、当業者であれば、本開示がこれに限定されないことが分かるだろう。上述した開示のさまざまな特徴および態様は、個々に、または共同で用いられてもよい。さらに、実施の形態は、本明細書のより広義の趣旨および範囲から逸脱することなく、本明細書において記載した環境およびアプリケーションの数を上回る任意の数の環境およびアプリケーションにおいて利用され得る。明細書および添付の図面は、したがって、限定ではなく例示とみなされるべきである。

40

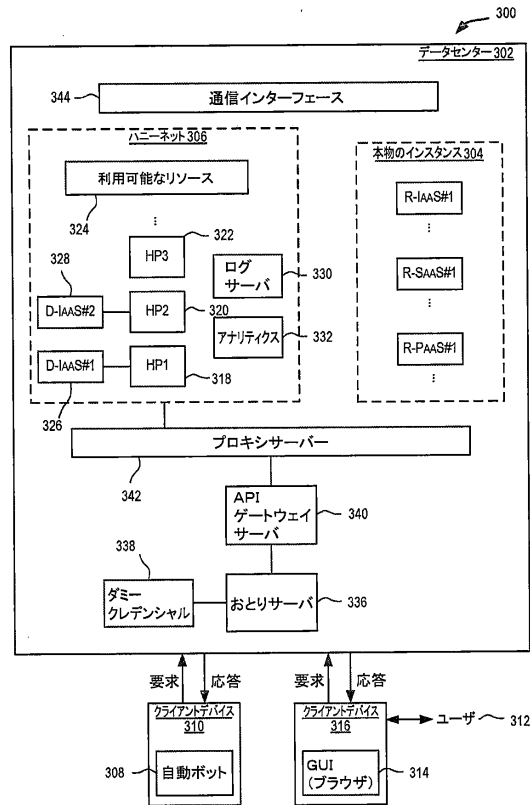
【図面】
【図 1】



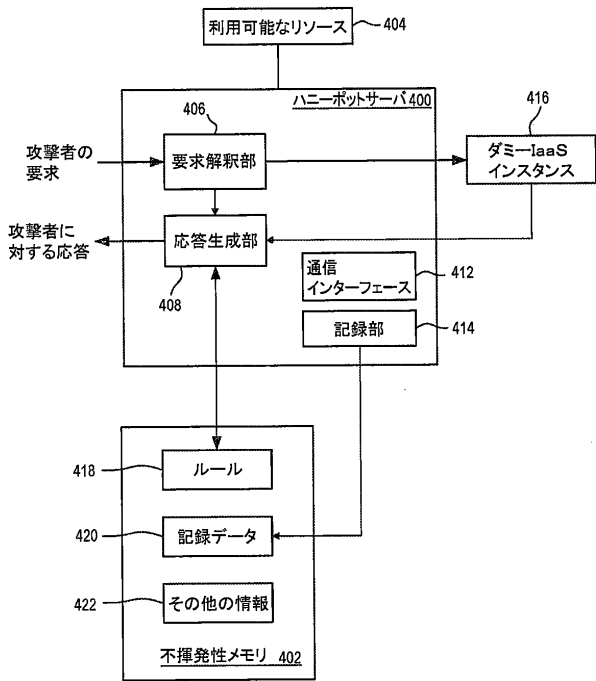
【図 2】



【図 3】



【図 4】



10

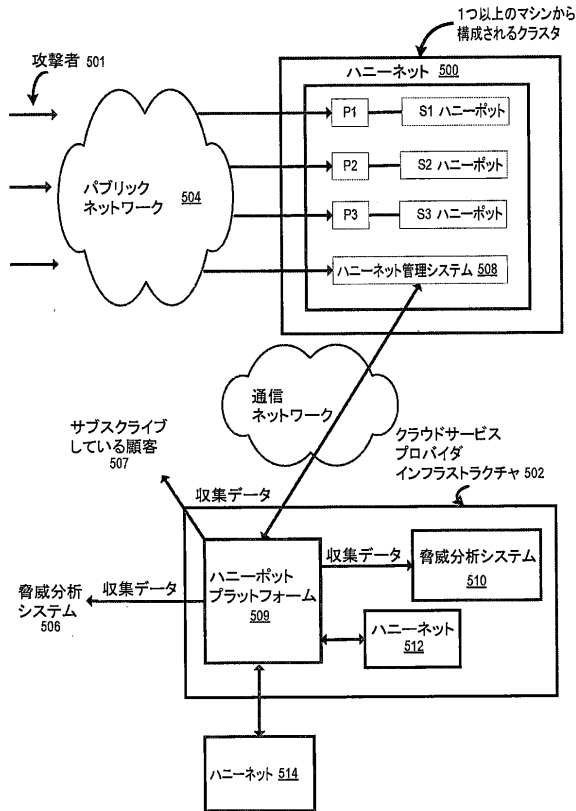
20

30

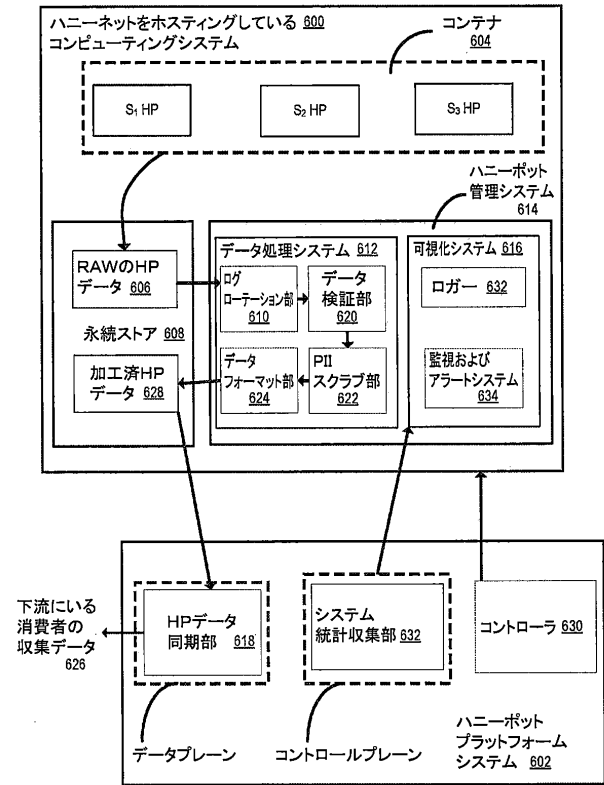
40

50

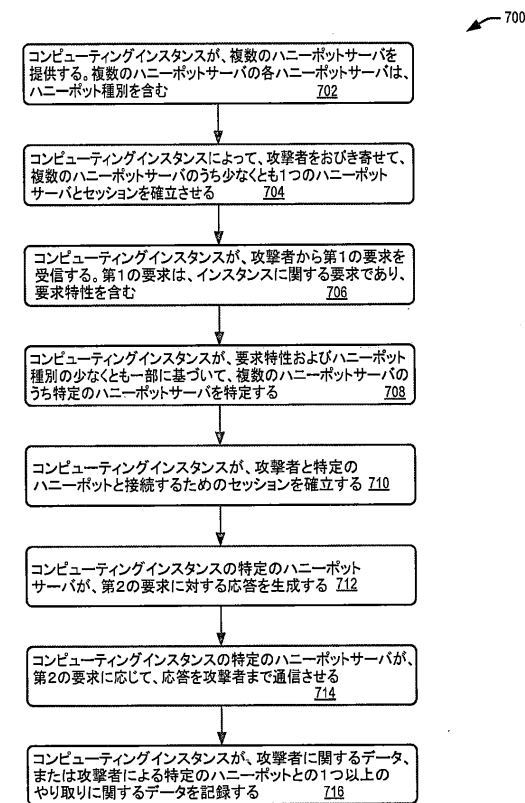
【図 5】



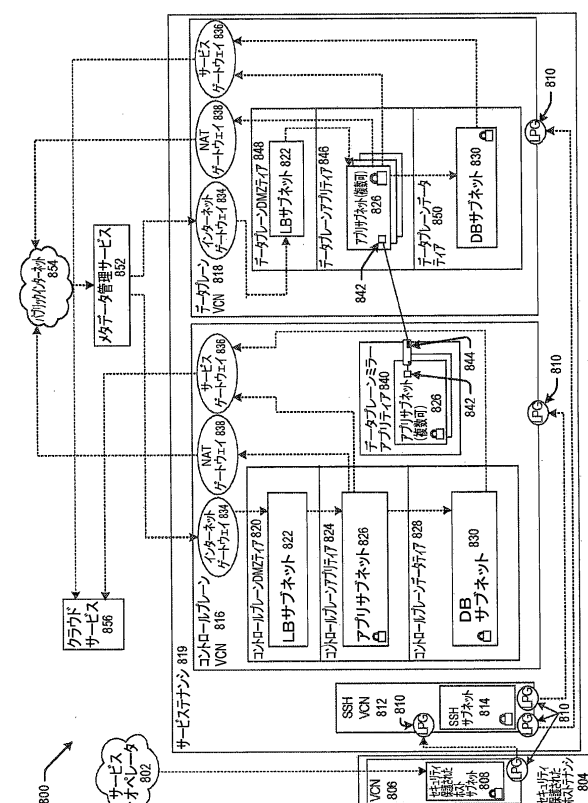
【図 6】



【図 7】



【図 8】



10

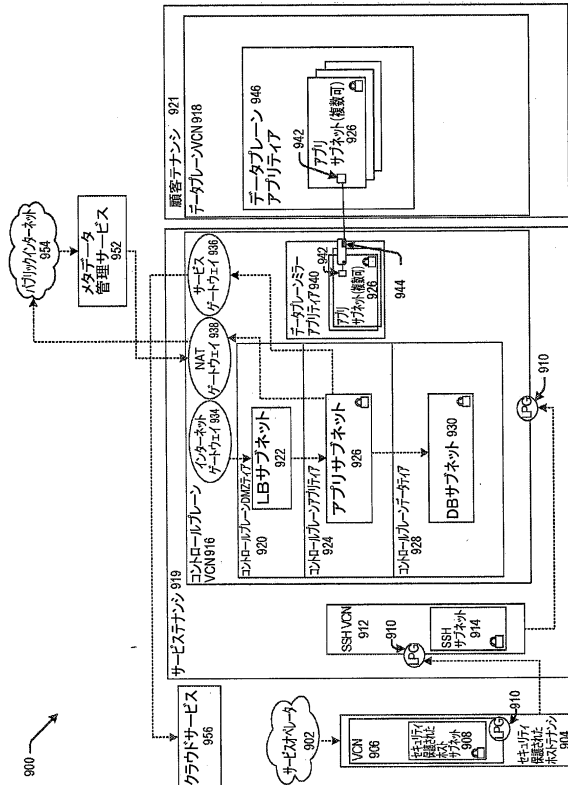
20

30

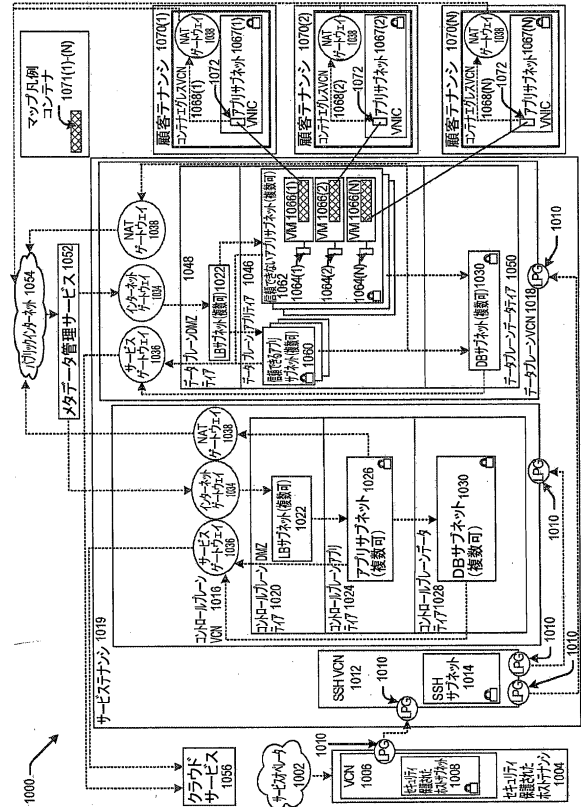
40

50

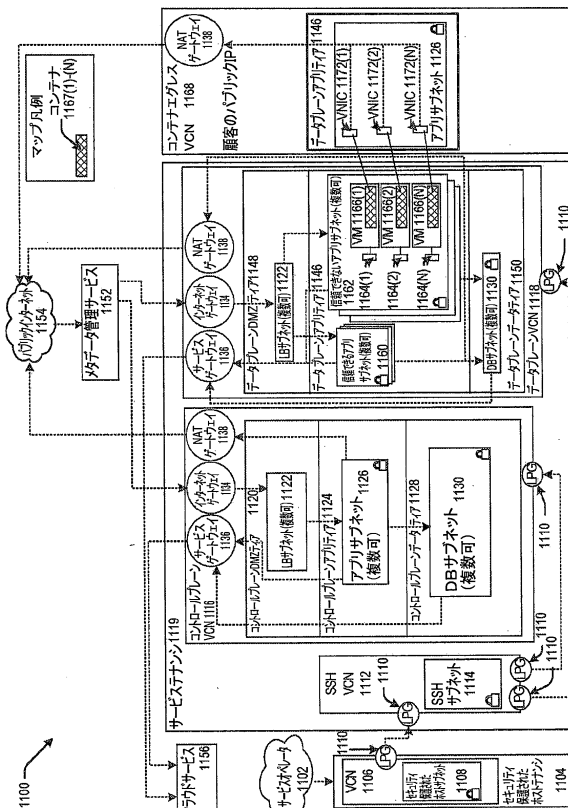
【図 9】



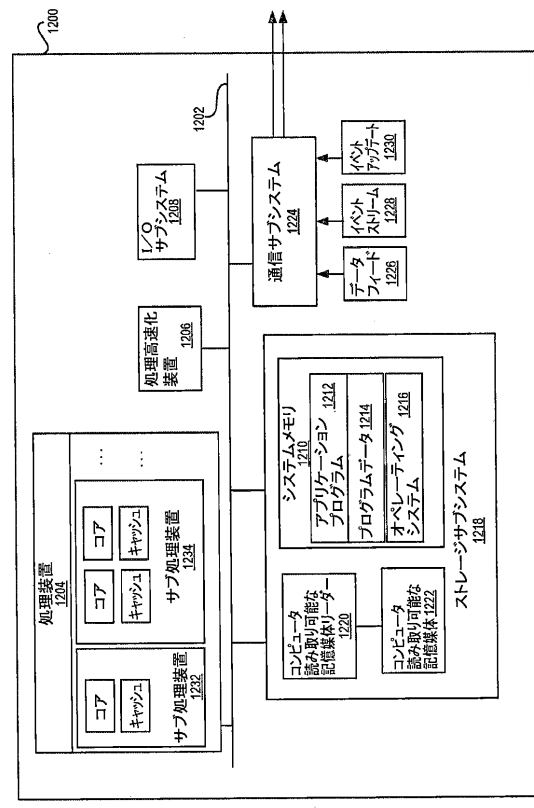
【図 10】



【図 11】



【図 12】



10

20

30

40

50

【手続補正書】

【提出日】令和6年8月28日(2024.8.28)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

方法であって、

コンピューティングシステムが、複数のハニーポットサーバを提供するステップを含み、前記複数のハニーポットサーバに含まれる各ハニーポットサーバは、ハニーポット種別を含み、前記方法は、さらに、

前記コンピューティングシステムが、サードパーティエンティティから、特定のハニーポット種別の特性に対応付けられる第1の要求を受信するステップと、

前記コンピューティングシステムが、前記特定のハニーポット種別の特定のハニーポットサーバと接続するためのセッションを前記サードパーティエンティティと確立するステップと、

前記コンピューティングシステムの前記特定のハニーポットサーバが、前記第1の要求に応じて応答を前記サードパーティエンティティまで通信させるステップと、

前記コンピューティングシステムが、前記サードパーティエンティティに関するデータ、および、前記サードパーティエンティティと前記特定のハニーポットサーバとの間の1つ以上のやり取りに関するデータのうち少なくとも1つを記録するステップとを含む、方法。

【請求項2】

前記コンピューティングシステムが、前記サードパーティエンティティをおびき寄せて、前記複数のハニーポットサーバのうち少なくとも1つのハニーポットサーバとセッションを確立させるステップをさらに含む、請求項1に記載の方法。

【請求項3】

前記おびき寄せることは、1つ以上のポートをパブリックネットワークに公開することを含み、前記1つ以上のポートは、SSH（セキュアシェル）ポート22、FTP（ファイル転送プロトコル）ポート21、またはSMTP（Simple Mail Transfer Protocol）ポート25、のうち少なくとも1つを含む、請求項2に記載の方法。

【請求項4】

前記コンピューティングシステムが、前記第1の要求の特性および前記ハニーポット種別の少なくとも一部に基づいて、前記複数のハニーポットサーバのうち前記特定のハニーポットサーバを特定するステップをさらに含む、請求項1または2に記載の方法。

【請求項5】

前記コンピューティングシステムは、IaaS（Infrastructure as a Service）プロバイダに対応付けられるIaaSコンピューティングインスタンスを含む、請求項1～4のいずれか1項に記載の方法。

【請求項6】

前記コンピューティングシステムの前記特定のハニーポットサーバが、前記サードパーティエンティティからの第2の要求に対する応答を生成するステップをさらに含み、前記応答は、前記IaaSプロバイダからの応答であるように見えるよう構成される、請求項5に記載の方法。

【請求項7】

前記サードパーティエンティティは、前記第1の要求または第2の要求のうち少なくとも1つを生成するためのアプリケーションを使用しているユーザである、請求項1～5の

10

20

30

40

50

いずれか 1 項に記載の方法。

【請求項 8】

システムであって、前記システムは、
1 つ以上のプロセッサと、

命令を含む非一時的なコンピュータ読み取り可能なメモリとを備え、前記命令は、前記 1 つ以上のプロセッサによって実行された場合、前記システムに動作を実行させ、前記動作は、

コンピューティングシステムが、複数のハニーポットサーバを提供することを含み、前記複数のハニーポットサーバに含まれる各ハニーポットサーバは、ハニーポット種別を含み、前記動作は、さらに、

前記コンピューティングシステムが、サードパーティエンティティから、特定のハニーポット種別の特性に対応付けられる第 1 の要求を受信することと、

前記コンピューティングシステムが、前記特定のハニーポット種別の特定のハニーポットサーバと接続するためのセッションを前記サードパーティエンティティと確立することと、

前記コンピューティングシステムの前記特定のハニーポットサーバが、前記第 1 の要求に応じて応答を前記サードパーティエンティティまで通信させることと、

前記コンピューティングシステムが、前記サードパーティエンティティに関するデータ、および、前記サードパーティエンティティと前記特定のハニーポットサーバとの間の 1 つ以上のやり取りに関するデータのうち少なくとも 1 つを記録することを含む、システム。

【請求項 9】

前記コンピューティングシステムが、前記サードパーティエンティティをおびき寄せて、前記複数のハニーポットサーバのうち少なくとも 1 つのハニーポットサーバとセッションを確立させることをさらに含む、請求項 8 に記載のシステム。

【請求項 10】

前記おびき寄せることは、1 つ以上のポートをパブリックネットワークに公開することを含み、前記 1 つ以上のポートは、SSH（セキュアシェル）ポート 22、FTP（ファイル転送プロトコル）ポート 21、または SMTP（Simple Mail Transfer Protocol）ポート 25、のうち少なくとも 1 つを含む、請求項 9 に記載のシステム。

【請求項 11】

前記コンピューティングシステムが、前記第 1 の要求の特性および前記ハニーポット種別の少なくとも一部に基づいて、前記複数のハニーポットサーバのうち前記特定のハニーポットサーバを特定することをさらに含む、請求項 8 ～ 10 のいずれか 1 項に記載のシステム。

【請求項 12】

前記コンピューティングシステムは、IaaS（Infrastructure as a Service）プロバイダに対応付けられる IaaS コンピューティングインスタンスを含む、請求項 8 ～ 11 のいずれか 1 項に記載のシステム。

【請求項 13】

前記コンピューティングシステムの前記特定のハニーポットサーバが、前記サードパーティエンティティからの第 2 の要求に対する応答を生成することをさらに含み、前記応答は、前記 IaaS プロバイダからの応答であるように見えるよう構成される、請求項 12 に記載のシステム。

【請求項 14】

前記サードパーティエンティティは、前記第 1 の要求または第 2 の要求のうち少なくとも 1 つを生成するためのアプリケーションを使用しているユーザである、請求項 8 ～ 12 のいずれか 1 項に記載のシステム。

【請求項 15】

請求項 1 ～ 7 のいずれか 1 項に記載の方法を 1 つ以上のプロセッサに実行させるためのコンピュータ読み取り可能なプログラム。

【外国語明細書】

2024164054000014.pdf

10

20

30

40

50

フロントページの続き

1. WINDOWS PHONE

2. iOS

(72)発明者 ラボラト, ニッコラス・アンソニー

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、500、オラクル・インターナショナル・コーポレーション

(72)発明者 レイモンド, ケビン

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、500、オラクル・インターナショナル・コーポレーション

(72)発明者 アンドリューズ, フィリップ

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、500、オラクル・インターナショナル・コーポレーション

(72)発明者 スクーラ, クリスタ

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、500、オラクル・インターナショナル・コーポレーション