【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】令和5年4月12日(2023.4.12)

【国際公開番号】WO2021/046094
【公表番号】特表2022-547485(P2022-547485A)
【公表日】令和4年11月14日(2022.11.14)
【年通号数】公開公報(特許)2022-209
【出願番号】特願2022-514618(P2022-514618)
【国際特許分類】
*G06F 21/55(2013.01)*
【ＦＩ】
Ｇ０６Ｆ 21/55

【手続補正書】
【提出日】令和5年4月4日(2023.4.4)
【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、前記コンピューティング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１～５のいずれか１項に記載の方法。
【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６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１～７のいずれか１項に記載の方法。
【請求項９】
前記攻撃者をおびき寄せることは、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ことを含む、請求項１～８のいずれか１項に記載の方法。
【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１～１１のいずれか１項に記載の方法。
【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１～１１のいずれか１項に記載の方法。
【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１～１３のいずれか１項に記載の方法。
【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プログラムであって、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とを含み、前記第１の要求は、前記コンピュ

ーティング**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とを含む、コンピュータ読み取り可能なプログラム。**
**【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に記載のコンピュータ読み取り可能なプログラム。**
**【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に記載のコンピュータ読み取り可能なプログラム。**
**【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、前記コンピューティング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】
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とを含む、請求項１９に記載のコンピューティングシステム。