【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７部門第３区分
【発行日】平成21年2月12日(2009.2.12)

【公表番号】特表2008-535304(P2008-535304A)
【公表日】平成20年8月28日(2008.8.28)
【年通号数】公開・登録公報2008-034
【出願番号】特願2008-502525(P2008-502525)
【国際特許分類】
Ｈ０４Ｌ　12/66　(2006.01)
Ｇ０６Ｆ　13/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　12/66　Ｂ
Ｇ０６Ｆ　13/00　３５１Ｚ

【手続補正書】
【提出日】平成20年12月17日(2008.12.17)
【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】
データ通信ネットワークに対する攻撃を検出するための方法であって、
発信側ユーザ・システム（４２０）にアドレスされたリターン・メッセージ（５１１）を監視するステップ（６１０）と、
指定された性質のリターン・メッセージ（５１１）を識別するステップ（６２０）と、
同じ発信側ユーザ・システム（４２０）からの以降のメッセージを侵入検出センサ（１６０）に一時的にルーティングするステップ（６３０）と、
を含む、方法。
【請求項２】
前記侵入検出センサ（１６０）が、前記発信側ユーザ・システム（４２０）にローカルに構成されるように選択される、請求項１に記載の方法。
【請求項３】
前記侵入検出センサ（１６０）が前記発信側ユーザ・システム（４２０）とのやり取りを偽装するステップを更に含む、請求項１または２に記載の方法。
【請求項４】
前記リターン・メッセージ（５１１）が、前記発信側ユーザ・システム（４２０）が宛先アドレスに送信したメッセージ（５０１）に関連し、前記一時的にルーティングするステップ（６３０）が、前記発信側ユーザ・システム（４２０）から前記宛先アドレスへの以降のメッセージ全てに適用される、請求項１から３のいずれか１項に記載の方法。
【請求項５】
前記リターン・メッセージ（５１１）の前記指定された性質が、宛先アドレスがアクセス不可能であることを示すように選択される、請求項１から４のいずれか１項に記載の方法。
【請求項６】
前記リターン・メッセージ（５１１）の前記指定された性質が、接続の失敗を示すインターネット制御メッセージ・プロトコルのメッセージを含むように選択される、請求項１から５のいずれか１項に記載の方法。

【請求項７】
前記一時的なルーティング（６３０）が所定の時間期間だけ適用される、請求項１から６のいずれか１項に記載の方法。
【請求項８】
所定の閾値を超えた数の指定された性質のリターン・メッセージ（５１１）が発信側ユーザ・システム（４２０）にアドレスされていると識別された場合に、前記一時的なルーティング（６３０）をトリガするステップを更に含む、請求項１から７のいずれか１項に記載の方法。
【請求項９】
データ通信ネットワークに対する攻撃を検出するための装置であって、
ルータ（４３０）であって、前記ルータ（４３０）にローカルな発信側ユーザ・システム（４２０）にアドレスされたリターン・メッセージ（５１１）を監視するための機構（４６０）を含む、ルータ（４３０）と、
侵入検出センサ（１６０）と、
を含み、前記機構（４６０）が、
指定された性質のリターン・メッセージ（５１１）を識別するためのメッセージ・チェッカと、
前記発信側ユーザ・システム（４２０）からの以降のメッセージを前記侵入検出センサ（１６０）に一時的にルーティングするためのリルータと、
を含む、装置。
【請求項１０】
前記侵入検出センサ（１６０）が前記ルータ（４３０）にローカルである、請求項９に記載の装置。
【請求項１１】
前記侵入検出センサ（１６０）が前記発信側ユーザ・システム（４２０）とのやり取りを偽装するように設計されている、請求項９または１０に記載の装置。
【請求項１２】
前記侵入検出センサ（１６０）が、各々がサービスを偽装する複数の仮想センサ（３１０～３１５）を有する仮想化インフラストラクチャを含む、請求項１１に記載の装置。
【請求項１３】
前記リターン・メッセージ（５１１）が、前記発信側ユーザ・システム（４２０）が宛先アドレスに送信したメッセージ（５００）に関連し、前記リルータが、前記発信側ユーザ・システム（４２０）から前記宛先アドレスへの以降のメッセージ全てについて動作する、請求項９から１２のいずれか１項に記載の装置。
【請求項１４】
前記リターン・メッセージ（５１１）の前記指定された性質が、宛先アドレスがアクセス不可能であることを示す、請求項９から１３のいずれか１項に記載の装置。
【請求項１５】
前記リターン・メッセージ（５１１）の前記指定された性質が、接続の失敗を示すインターネット制御メッセージ・プロトコルのメッセージである、請求項９から１４のいずれか１項に記載の装置。
【請求項１６】
前記リルータが所定の時間期間だけアクティブである、請求項９から１５のいずれか１項に記載の装置。
【請求項１７】
前記リルータが、発信側ユーザ・システム（４２０）にアドレスされていると識別された指定された性質のリターン・メッセージ（５１１）が所定の閾値を超えたか否かを判定するための判定装置を含む、請求項９から１６のいずれか１項に記載の装置。
【請求項１８】
ルータ（４３０）であって、

前記ルータ（４３０）にローカルな発信側ユーザ・システム（４２０）にアドレスされたリターン・メッセージ（５１１）を監視するための機構（４６０）と、
指定された性質のリターン・メッセージ（５１１）を識別するためのメッセージ・チェッカと、
前記発信側ユーザ・システム（４２０）からの以降のメッセージを侵入検出センサ（１６０）に一時的にルーティングするためのリルータと、
を含む、ルータ（４３０）。
【請求項１９】
データ通信システムであって、
ネットワークにおける複数のデータ処理システムと、
前記データ処理システムへのメッセージおよび前記データ処理システムからのメッセージをルーティングするための、前記データ処理システムにローカルなルータ（４３０）であって、前記ルータ（４３０）にローカルな前記データ処理システムの１つの形態の発信側ユーザ・システム（４２０）にアドレスされたリターン・メッセージ（５１１）を監視するための機構（４６０）を含む、ルータ（４３０）と、
侵入検出センサ（１６０）と、
を含み、前記機構（４６０）が、
指定された性質のリターン・メッセージ（５１１）を識別するためのメッセージ・チェッカと、
前記発信側ユーザ・システム（４２０）からの以降のメッセージを前記侵入検出センサ（１６０）に一時的にルーティングするためのリルータと、
を含む、データ通信システム。
【請求項２０】
請求項１乃至８のいずれか１項に記載の方法の各ステップをデータ処理システムに実行させるためのコンピュータ・プログラム。
【請求項２１】
発信側ユーザ・システム（４２０）からの侵入に対する装備をクライアント・システムに備える方法であって、
侵入検出センサ（１６０）をルータ（４３０）に接続するステップと、
前記ルータ（４３０）に、
前記発信側ユーザ・システム（４２０）にアドレスされたリターン・メッセージ（５１１）を監視し（６１０）、
指定された性質のリターン・メッセージ（５１１）を識別し（６２０）、
同じ発信側ユーザ・システム（４２０）からの以降のメッセージを一時的に前記侵入検出センサ（１６０）にルーティングする（６３０）機能を与える、ステップと、
を含む、方法。