【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30年5月17日(2018.5.17)

【公表番号】特表2017-511072(P2017-511072A)
【公表日】平成29年4月13日(2017.4.13)
【年通号数】公開・登録公報2017-015
【出願番号】特願2016-561300(P2016-561300)
【国際特許分類】
Ｈ０４Ｌ　12/70　(2013.01)
Ｈ０４Ｌ　12/717　(2013.01)
Ｈ０４Ｌ　12/66　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　12/70　１００Ｚ
Ｈ０４Ｌ　12/717
Ｈ０４Ｌ　12/66　Ｂ

【手続補正書】
【提出日】平成30年3月28日(2018.3.28)
【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】
ネットワークトラフィックを検査する、コンピュータによって実装される方法であって、
トラフィックフローが第１の条件を満たすと判断することと、
前記トラフィックフローが前記第１の条件を満たすとの前記判断に基づき、前記トラフィックフローの第１の部分をネットワークサービスに送信することと、
前記第１の条件に基づき、第１の詳細レベルで前記トラフィックフローの前記第１の部分を、前記ネットワークサービスで検査することと、
前記検査に基づき、前記トラフィックフローが第２の条件を満たすと判断することと、
前記トラフィックフローが前記第２の条件を満たすとの前記判断に基づき、前記トラフィックフローの第２の部分を前記ネットワークサービスに送信することと、
第２の詳細レベルで前記トラフィックフローの前記第２の部分を、前記ネットワークサービスで検査することであって、前記第２の詳細レベルでの前記検査は、前記第１の詳細レベルでの前記検査とは異なるコンピューティングリソース量を必要とする、段階と、
を備える、方法。
【請求項２】
前記第１の条件は、ヒューリスティック、前記トラフィックフローに関連するポリシー、又は関心のあるイベントのうちの１つを備える、
請求項１に記載の方法。
【請求項３】
前記第２の条件は、ヒューリスティック、前記トラフィックフローに関連するポリシー、又は関心のあるイベントのうちの１つを備える、
請求項１または２に記載の方法。
【請求項４】
前記第２の詳細レベルでの前記トラフィックフローの前記第２の部分の前記検査は、前

記第１の詳細レベルでの前記トラフィックフローの前記検査より高い前記トラフィックフローのコンテンツを検査することを有する、
請求項１から３の何れか一項に記載の方法。
【請求項５】
トラフィックフローの第１の部分は、複数のパケットのランダムサンプルを備える、
請求項１から４の何れか一項に記載の方法。
【請求項６】
前記第２の詳細レベルでの前記トラフィックフローの前記検査に基づき、前記トラフィックフローの第３の部分を前記ネットワークサービスに送信することと、
第３の詳細レベルで前記トラフィックフローの前記第３の部分を、前記ネットワークサービスで検査することと、
を更に備える、
請求項１から５の何れか一項に記載の方法。
【請求項７】
前記トラフィックフローがもはや前記第２の条件を満たさないと判断することと、
前記トラフィックフローがもはや前記第２の条件を満たさないことが判断された場合に、前記第１の詳細レベルで前記トラフィックフローの第３の部分を、前記ネットワークサービスで検査することと、
を更に備える、
請求項１から６の何れか一項に記載の方法。
【請求項８】
第２の詳細レベルでの前記トラフィックフローの前記第２の部分の前記検査は、侵入検出分析を実行することを有する、
請求項１から７の何れか一項に記載の方法。
【請求項９】
前記第１の条件は、前記トラフィックフローに関連するパラメータと、前記トラフィックフローのために所望されるセキュリティのレベルとを備える、
請求項１から８の何れか一項に記載の方法。
【請求項１０】
前記トラフィックフローの前記第２の部分は、前記トラフィックフローの前記第１の部分より多くの情報量を有する、
請求項１から９の何れか一項に記載の方法。
【請求項１１】
トラフィックフローが第１の条件を満たすと判断する分析モジュールと、
コントローラであって、
前記トラフィックフローが前記第１の条件を満たすとの前記判断に基づき、前記トラフィックフローの第１の部分をネットワークサービスに送信するよう、１又は複数のルータを設定するコントローラと、
ネットワークサービスであって、
前記第１の条件に基づき、第１の詳細レベルで前記トラフィックフローの前記第１の部分を検査し、
前記検査に基づき、前記トラフィックフローが第２の条件を満たすと判断するネットワークサービスと、
を備え、
前記コントローラは、前記トラフィックフローが前記第２の条件を満たすという前記判断に基づき、前記トラフィックフローの第２の部分を前記ネットワークサービスに送信するよう１又は複数のルータを更に設定し、
前記ネットワークサービスは、第２の詳細レベルで前記トラフィックフローの前記第２の部分を更に検査し、前記第２の詳細レベルでの前記検査は、前記第１の詳細レベルでの前記検査とは異なるコンピューティングリソースの量を必要とする、

システム。
【請求項１２】
前記第１の条件は、ヒューリスティック、前記トラフィックフローに関連するポリシー、又は関心のあるイベントのうちの１つを備える、
請求項１１に記載のシステム。
【請求項１３】
前記第２の条件は、ヒューリスティック、前記トラフィックフローに関連するポリシー、又は関心のあるイベントのうちの１つを備える、
請求項１１または１２に記載のシステム。
【請求項１４】
前記第２の詳細レベルでの前記トラフィックフローの前記第２の部分の前記検査は、前記第１の詳細レベルでの前記トラフィックフローの前記検査より高い前記トラフィックフローのコンテンツの検査を有する、
請求項１１から１３の何れか一項に記載のシステム。
【請求項１５】
トラフィックフローの第１の部分は、複数のパケットのランダムサンプルを備える、
請求項１１から１４の何れか一項に記載のシステム。
【請求項１６】
前記第２の詳細レベルでの前記トラフィックフローの前記検査に基づき、前記トラフィックフローの第３の部分を前記ネットワークサービスに送信することと、
第３の詳細レベルでの前記トラフィックフローの前記第３の部分を、前記ネットワークサービスで検査することと、
を更に備える、
請求項１１から１５の何れか一項に記載のシステム。
【請求項１７】
第２の詳細レベルでの前記トラフィックフローの前記第２の部分の前記検査は、侵入検出分析を実行することを有する、
請求項１１から１６の何れか一項に記載のシステム。
【請求項１８】
前記第１の条件は、前記トラフィックフローに関連するパラメータと、前記トラフィックフローのために所望されるセキュリティのレベルとを備える、
請求項１１から１７の何れか一項に記載のシステム。
【請求項１９】
前記ネットワークサービスは、
前記トラフィックフローがもはや前記第２の条件を満たさないと判断し、
前記トラフィックフローがもはや前記第２の条件を満たさないことが判断された場合に、前記第１の詳細レベルで前記トラフィックフローの第３の部分を、前記ネットワークサービスで検査する、
請求項１１から１８の何れか一項に記載のシステム。
【請求項２０】
前記トラフィックフローの前記第２の部分は、前記トラフィックフローの前記第１の部分より多くの情報量を有する、
請求項１１から１９の何れか一項に記載のシステム。
【請求項２１】
少なくとも１つのコンピューティングデバイスにより実行される場合に、前記少なくとも１つのコンピューティングデバイスに複数のオペレーションを実行させるプログラムであって、
複数のオペレーションは、
トラフィックフローが第１の条件を満たすと判断するオペレーションと、
前記トラフィックフローが前記第１の条件を満たすとの前記判断に基づき、前記トラフ

ィックフローの第１の部分をネットワークサービスに送信するオペレーションと、
前記第１の条件に基づき、第１の詳細レベルで前記トラフィックフローの前記第１の部分を、前記ネットワークサービスで検査するオペレーションと、
前記検査に基づき、前記トラフィックフローが第２の条件を満たすと判断するオペレーションと、
前記トラフィックフローが前記第２の条件を満たすとの前記判断に基づき、前記トラフィックフローの第２の部分を前記ネットワークサービスに送信するオペレーションと、
第２の詳細レベルで前記トラフィックフローの前記第２の部分を、前記ネットワークサービスで検査することであって、前記第２の詳細レベルでの前記検査は、前記第１の詳細レベルでの前記検査とは異なるコンピューティングリソースの量を必要とする、検査するオペレーションと、
を備える、
プログラム。
【請求項２２】
前記第１の条件は、ヒューリスティック、前記トラフィックフローに関連するポリシー、又は関心のあるイベントのうちの１つを備える、
請求項２１に記載のプログラム。
【請求項２３】
前記第２の条件は、ヒューリスティック、前記トラフィックフローに関連するポリシー、又は関心のあるイベントのうちの１つを備える、
請求項２１または２２に記載のプログラム。
【請求項２４】
前記第２の詳細レベルでの前記トラフィックフローの前記第２の部分の前記検査は、前記第１の詳細レベルでの前記トラフィックフローの前記検査より高い前記トラフィックフローのコンテンツを検査することを有する、
請求項２１から２３の何れか一項に記載のプログラム。
【請求項２５】
前記トラフィックフローの前記第２の部分は、前記トラフィックフローの前記第１の部分より多くの情報量を有する、
請求項２１から２４の何れか一項に記載のプログラム。