【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8月30日(2018.8.30)

【公開番号】特開2017-216664(P2017-216664A)
【公開日】平成29年12月7日(2017.12.7)
【年通号数】公開・登録公報2017-047
【出願番号】特願2016-111112(P2016-111112)
【国際特許分類】
Ｈ０４Ｌ　12/70　(2013.01)
Ｈ０４Ｌ　12/813　(2013.01)
Ｈ０４Ｌ　12/815　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　12/70　１００Ｚ
Ｈ０４Ｌ　12/813
Ｈ０４Ｌ　12/815

【手続補正書】
【提出日】平成30年7月20日(2018.7.20)
【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】
受信または送信されるパケットをコピーしたミラーパケットをミラーポートから送信するパケット中継装置であって、
入力ポートからパケットを受け付けるパケット受付部と、
前記パケットが攻撃または攻撃予兆の可能性を含むか否かを判定するセキュリティ判定部と、
前記パケットが攻撃または攻撃予兆の可能性を含むと判定された場合に、当該パケットの複製を前記ミラーパケットとして生成するミラー処理部と、
前記ミラーパケットをミラーポートから送信する送信部と、
を有することを特徴とするパケット中継装置。
【請求項２】
請求項１に記載のパケット中継装置であって、
前記ミラー処理部は、
前記セキュリティ判定部で判定された攻撃または攻撃予兆に関する情報を前記ミラーパケットに付加することを特徴とするパケット中継装置。
【請求項３】
請求項２に記載のパケット中継装置であって、
前記セキュリティ判定部は、
前記攻撃または攻撃予兆に関する情報として、攻撃種別または攻撃予兆種別の情報を判定し、
前記ミラー処理部は、
前記攻撃種別または攻撃予兆種別の情報を前記ミラーパケットに付加することを特徴とするパケット中継装置。
【請求項４】
請求項２に記載のパケット中継装置であって、

前記セキュリティ判定部は、
前記攻撃または攻撃予兆に関する情報として、攻撃または攻撃予兆の影響度を示す情報を判定し、
前記ミラー処理部は、
前記攻撃または攻撃予兆の影響度を示す情報を前記ミラーパケットに付加することを特徴とするパケット中継装置。
【請求項５】
請求項２に記載のパケット中継装置であって、
前記セキュリティ判定部は、
前記攻撃または攻撃予兆に関する情報として、攻撃または攻撃予兆の確からしさを示す情報を判定し、
前記ミラー処理部は、
前記攻撃または攻撃予兆の確からしさを示す情報を前記ミラーパケットに付加することを特徴とするパケット中継装置。
【請求項６】
請求項２に記載のパケット中継装置であって、
前記セキュリティ判定部は、
前記攻撃または攻撃予兆に関する情報として、攻撃経路を示す情報を判定し、
前記ミラー処理部は、
前記攻撃経路を示す情報を前記ミラーパケットに付加することを特徴とするパケット中継装置。
【請求項７】
請求項１ないし請求項６のいずれかひとつに記載のパケット中継装置であって、
前記ミラー処理部は、
前記ミラーパケットにＶＬＡＮ－Ｔａｇを付加し、付加するＶＬＡＮ－ＴａｇのＶＬＡＮ　ＩＤまたはＵｓｅｒ　Ｐｒｉｏｒｉｔｙに前記攻撃または攻撃予兆に関する情報を設定することを特徴とするパケット中継装置。
【請求項８】
請求項１ないし請求項６のいずれかひとつに記載のパケット中継装置であって、
前記セキュリティ判定部は、
予め設定されたパケット情報に基づいて攻撃または攻撃予兆の可能性があるパケットを判定することを特徴とするパケット中継装置。
【請求項９】
請求項１ないし請求項６のいずれかひとつに記載のパケット中継装置であって、
前記セキュリティ判定部は、
予め設定された検索テーブルの検索結果に基づいて攻撃または攻撃予兆の可能性があるパケットを判定することを特徴とするパケット中継装置。
【請求項１０】
請求項１ないし請求項６のいずれかひとつに記載のパケット中継装置であって、
前記セキュリティ判定部は、
複数のパケットのパケット情報の特徴パターンに基づいて攻撃または攻撃予兆の可能性があるパケットを判定することを特徴とするパケット中継装置。
【請求項１１】
請求項１ないし請求項６のいずれかひとつに記載のパケット中継装置であって、
前記セキュリティ判定部は、
特徴量に基づいて攻撃または攻撃予兆の可能性があるパケットを判定することを特徴とするパケット中継装置。
【請求項１２】
請求項１１に記載のパケット中継装置であって、
前記特徴量がパケットのＢｙｔｅ長であることを特徴とするパケット中継装置。

【請求項１３】
請求項１１に記載のパケット中継装置であって、
前記特徴量がパケットの帯域であることを特徴とするパケット中継装置。
【請求項１４】
請求項１１に記載のパケット中継装置であって、
前記特徴量がパケットの統計量であることを特徴とするパケット中継装置。
【請求項１５】
請求項１１ないし請求項１４のいずれかひとつに記載のパケット中継装置であって、
前記セキュリティ判定部は、
前記特徴量の時間的変動に基づいて攻撃または攻撃予兆の可能性があるパケットを判定することを特徴とするパケット中継装置。
【請求項１６】
請求項１に記載のパケット中継装置であって、
前記ミラーポートを複数有し、
前記ミラー処理部は、
前記パケットを複数個コピーしたミラーパケットを、各々異なるミラーポートから送信することを特徴とするパケット中継装置。
【請求項１７】
請求項３に記載のパケット中継装置であって、
前記ミラーポートを複数有し、
前記送信部は、
前記ミラーパケットを送信するミラーポートを、前記攻撃種別毎にハッシュまたはラウンドロビンのアルゴリズムに基づいて選択することを特徴とするパケット中継装置。
【請求項１８】
請求項３に記載のパケット中継装置であって、
前記送信部は、
前記パケットのうちミラーパケットをコピーする比率を前記判定された攻撃種別毎に指定してミラーポートから送信することを特徴とするパケット中継装置。
【請求項１９】
請求項３に記載のパケット中継装置であって、
前記送信部は、
前記ミラーパケットを前記判定された攻撃種別毎にシェーピングまたはポリシングを実施して、前記ミラーポートから送信することを特徴とするパケット中継装置。
【請求項２０】
請求項１９に記載のパケット中継装置であって、
前記送信部は、
前記ミラーパケットに対しシェーピングまたはポリシングを実施する際の優先度を、攻撃種別、攻撃予兆種別、攻撃または攻撃予兆の影響度、攻撃または攻撃予兆の確からしさ、または攻撃経路の判定結果のいずれかに基づいて判定することを特徴とするパケット中継装置。
【請求項２１】
請求項１に記載のパケット中継装置であって、
前記ミラー処理部は、
前記セキュリティ判定部が判定した攻撃種別情報、攻撃影響度情報、攻撃確度情報、攻撃経路情報のいずれかに基づいて、前記ミラーパケットの生成可否、前記ミラーパケットを送信するミラーポート、前記ミラーパケットを送信する優先度のいずれかを決定することを特徴とするパケット中継装置。