

請求の範囲

- [請求項1] コンピュータに、
通信データをセッション毎に分割して分割データ群を生成し、
前記分割データ群のうちから、同一の識別情報を有し、かつセッション間隔が閾値以下である分割データを抽出し、
抽出した前記分割データを連結して連結データを生成し、
前記連結データに含まれる特定情報にもとづいて通信の危険度を決定し、
前記連結データに含まれるファイルから、前記危険度にもとづくファイル情報を収集する、
処理を実行させる情報処理プログラム。
- [請求項2] 前記特定情報は、前記連結データに含まれるコマンド、および前記連結データに含まれる前記ファイルのファイルサイズである請求項1記載の情報処理プログラム。
- [請求項3] 前記ファイル情報は、前記ファイルのメタ情報、ファイルハッシュ値、およびファイル本体の少なくとも1つである請求項1記載の情報処理プログラム。
- [請求項4] 前記コマンドは、リモート管理操作に使用される請求項2記載の情報処理プログラム。
- [請求項5] 前記処理は、
前記コマンドが情報の参照を行うための参照系コマンドである場合、前記連結データの前記危険度を最も低い第1の危険度に決定し、
前記コマンドが共有リソースに接続するための接続系コマンドである場合、前記連結データの前記危険度を前記第1の危険度よりも高い第2の危険度に決定し、
前記コマンドがデータ処理の更新を行うための更新系コマンドであり、かつ前記ファイルのファイルサイズが閾値以上である場合、前記連結データの前記危険度を前記第2の危険度に決定し、

前記コマンドが前記更新系コマンドであり、かつ前記ファイルのファイルサイズが閾値未満である場合、前記連結データの前記危険度を前記第2の危険度よりも高い第3の危険度に決定する、

請求項2記載の情報処理プログラム。

[請求項6]

前記処理は、

前記第1の危険度に決定された前記連結データに含まれる前記ファイルから前記ファイル情報として、メタ情報を収集し、

前記第2の危険度に決定された前記連結データに含まれる前記ファイルから前記ファイル情報として、前記メタ情報およびファイルハッシュ値を収集し、

前記第3の危険度に決定された前記連結データに含まれる前記ファイルから前記ファイル情報として、前記メタ情報、前記ファイルハッシュ値およびファイル本体を収集する、

請求項5記載の情報処理プログラム。

[請求項7]

前記処理は、

前記コマンドが情報の参照を行うための参照系コマンドである場合、前記連結データの前記危険度を最も低い第1の危険度に決定し、

前記コマンドが共有リソースに接続するための接続系コマンドである場合、前記連結データの前記危険度を前記第1の危険度よりも高い第2の危険度に決定し、

前記コマンドがデータ処理の更新を行うための更新系コマンドである場合、前記連結データの前記危険度を前記第2の危険度よりも高い第3の危険度に決定し、

前記第1の危険度に決定された前記連結データに含まれる前記ファイルから前記ファイル情報として、メタ情報を収集し、

前記第2の危険度に決定された前記連結データに含まれる前記ファイルから前記ファイル情報として、前記メタ情報およびファイルハッシュ値を収集し、

前記第3の危険度に決定された前記連結データに含まれる前記ファイルから前記ファイル情報として、前記メタ情報、前記ファイルハッシュ値およびファイル本体を収集し、前記ファイルのファイルサイズが閾値以上である場合は、収集した前記ファイル本体を除去する、
請求項2記載の情報処理プログラム。

[請求項8] 前記処理は、前記セッション間隔の閾値を、前記通信データが観測される環境内における前記セッション間隔の平均値とする請求項1記載の情報処理プログラム。

[請求項9] 前記処理は、前記通信データが観測される環境内で過去に利用された拡張子とファイル種類が異なる前記ファイルのサイズ、または実行形式の前記ファイルのサイズから平均を算出し、前記平均に標準偏差を加算した値をファイルサイズの閾値とする請求項5または請求項7に記載の情報処理プログラム。

[請求項10] コンピュータが、
通信データをセッション毎に分割して分割データ群を生成し、
前記分割データ群のうちから、同一の識別情報を有し、かつセッション間隔が閾値以下である分割データを抽出し、
抽出した前記分割データを連結して連結データを生成し、
前記連結データに含まれる特定情報にもとづいて通信の危険度を決定し、
前記連結データに含まれるファイルから、前記危険度にもとづくファイル情報を収集する、
情報処理方法。

[請求項11] 通信データを格納する記憶部と、
前記通信データをセッション毎に分割して分割データ群を生成し、前記分割データ群のうちから、同一の識別情報を有し、かつセッション間隔が閾値以下である分割データを抽出し、抽出した前記分割データを連結して連結データを生成し、前記連結データに含まれる特定情報

にもとづいて通信の危険度を決定し、前記連結データに含まれるファイルから、前記危険度にもとづくファイル情報を収集する制御部と、
を有する情報処理装置。