【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4年9月7日(2022.9.7)

【公開番号】特開2022-17889(P2022-17889A)
【公開日】令和4年1月26日(2022.1.26)
【年通号数】公開公報(特許)2022-014
【出願番号】特願2020-120721(P2020-120721)
【国際特許分類】
Ｇ０６Ｆ 11/30(2006.01)
Ｇ０６Ｆ 11/34(2006.01)
【ＦＩ】
Ｇ０６Ｆ 11/30 １７２
Ｇ０６Ｆ 11/30 １４０Ｇ
Ｇ０６Ｆ 11/34 １５２
Ｇ０６Ｆ 11/30 １４０Ｄ

【手続補正書】
【提出日】令和4年8月30日(2022.8.30)
【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】
セキュリティセンサが生成したログを受信するログ収集部（１０１）と、
前記ログを保存する保存部（１０２）と、
複数の前記ログの統計分析を行うことで統計計算結果を求める統計分析部（１０４）と、
所定の条件に応じて、前記ログを送信するか前記統計計算結果を送信するかを判定する制御部（１０３）と、
前記ログ又は前記統計計算結果を送信する送信部（１０６）と、を有する、
ログ管理装置（１００）。
【請求項２】
さらに、前記ログに基づき攻撃検知を行う攻撃検知部（１０５）を有し、
前記統計分析部は、攻撃検知が所定の回数以上の場合に、統計分析を行うことで前記統計計算結果を求める、
請求項１記載のログ管理装置。
【請求項３】
さらに、前記ログに基づき攻撃検知を行う攻撃検知部（１０５）を有し、
前記所定の条件は、攻撃検知の回数である、
請求項１記載のログ管理装置。
【請求項４】
前記送信部は、
前記攻撃検知が所定の回数以下の場合に、前記ログをセンタ装置に送信し、
前記攻撃検知が所定の回数以上の場合に、前記センタ装置からのアップロード要求を待って前記統計計算結果を前記センタ装置に送信する、
請求項３記載のログ管理装置。
【請求項５】

前記セキュリティセンサの設置場所又は前記セキュリティセンサが接続されている通信バスの重要度に応じて、前記所定の条件としての攻撃検知の回数を設定することができる、
請求項３記載のログ管理装置。
【請求項６】
さらに、センタ装置から前記ログ又は前記統計計算結果のアップロードを要求するアップロード要求を受信する受信部（１０７）を有し、
前記所定の条件は、前記アップロード要求である、
請求項１記載のログ管理装置。
【請求項７】
前記所定の条件は、前記アップロード要求に加え、前記ログの量である、
請求項６記載のログ管理装置。
【請求項８】
前記送信部は、
前記ログの量が所定の量以下の場合に、前記ログをセンタ装置に送信し、
前記ログの量が所定の量以上の場合に、前記統計計算結果を前記センタ装置に送信する、
請求項７記載のログ管理装置。
【請求項９】
前記送信部は、前記ログ又は前記統計計算結果が送信できない場合を経て送信可能となった場合、最新の前記アップロード要求に応じて前記ログ又は前記統計計算結果を送信する、
請求項６記載のログ管理装置。
【請求項１０】
当該ログ管理装置は、移動体に搭載されている、
請求項１～９いずれかに記載のログ管理装置。
【請求項１１】
ログ管理装置で実行されるログ管理方法であって、
セキュリティセンサが生成したログを受信し、
前記ログを保存し、
複数の前記ログの統計分析を行うことで統計計算結果を求め、
所定の条件に応じて、前記ログを送信するか前記統計計算結果を送信するかを判定し、
前記ログ又は前記統計計算結果を送信する、
ログ管理方法。
【請求項１２】
ログ管理装置で実行可能なログ管理プログラムであって、
セキュリティセンサが生成したログを受信し、
前記ログを保存し、
複数の前記ログの統計分析を行うことで統計計算結果を求め、
所定の条件に応じて、前記ログを送信するか前記統計計算結果を送信するかを判定し、
前記ログ又は前記統計計算結果を送信する、
ログ管理プログラム。
【請求項１３】
ログ管理装置（１００）及びセンタ装置（２００）からなるセキュリティ攻撃検知・分析システム（１）であって、
前記ログ管理装置は、
セキュリティセンサが生成したログを受信するログ収集部（１０１）と、
前記ログを保存する保存部（１０２）と、
複数の前記ログの統計分析を行うことで統計計算結果を求める統計分析部（１０４）と、

所定の条件に応じて、前記ログを送信するか前記統計計算結果を送信するかを判定する制御部（１０３）と、
前記ログ又は前記統計計算結果を送信する送信部（１０６）と、を有し、
前記センタ装置は、
前記ログ又は前記統計計算結果を受信する受信部（２０１）と、
前記ログ又は前記統計計算結果を分析するとともに、分析結果に基づき追加のログ又は追加の統計計算結果のアップロードを要求するアップロード要求を生成する分析部（２０３）と、
前記ログ管理装置に対し、前記アップロード要求を送信する送信部（２０５）と、を有する、
セキュリティ攻撃検知・分析システム（１）。
【請求項１４】
前記ログ管理装置は、移動体に搭載されており、
前記センタ装置の前記送信部は、前記移動体の前記ログ管理装置及び／又は同種の他の移動体に搭載されたログ管理装置対し、前記アップロード要求を送信する、
請求項１３記載のセキュリティ攻撃検知・分析システム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正の内容】
【０００９】
本開示のログ管理装置（１００）は、
セキュリティセンサが生成したログを受信するログ収集部（１０１）と、
前記ログを保存する保存部（１０２）と、
複数の前記ログの統計分析を行うことで統計計算結果を求める統計分析部（１０４）と、
所定の条件に応じて、前記ログを送信するか前記統計計算結果を送信するかを判定する制御部（１０３）と、
前記ログ又は前記統計計算結果を送信する送信部（１０６）と、を有する。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００６７
【補正方法】変更
【補正の内容】
【００６７】
図６は、車両のログ管理装置１００からセキュリティログ又は統計計算結果を受信した場合の動作である。
センタ装置２００の受信部２０１は、特定の車両から送信されたセキュリティログ又は統計計算結果を受信する（Ｓ２０１）。ここで受信するセキュリティログ又は統計計算結果は、図４に示すような、特定の車両のログ管理装置１００の定常的なログ収集に基づくセキュリティログ（Ｓ１０５）又は統計計算結果（Ｓ１０３）であっても、図５に示すような、センタ装置２００からのアップロード要求に対して送信するセキュリティログ（Ｓ１１４）又は統計計算結果（Ｓ１１５）であってもよい。すなわち、図６のフローチャートは、図４や図５に接続されて実行される。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００６８
【補正方法】変更
【補正の内容】

【００６８】
分析部２０３は、Ｓ２０１で受信したセキュリティログ又は統計計算結果を用いて攻撃分析を行う（Ｓ２０２）。攻撃分析は、車両のログ管理装置１００の攻撃検知部１０５と同様のアルゴリズムでもよいが、更に精緻な攻撃分析を行ってもよい。攻撃分析の手法は、公知の手法を用いることができる。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００７１
【補正方法】変更
【補正の内容】
【００７１】
受信部２０１は、特定の車両である単数の車両、又は特定の車両と同一車種の一部又は全部である複数の車両からセキュリティログ又は統計計算結果を受信する。そして、分析部２０３はこれらの情報を用いて攻撃分析を行う（Ｓ２０５）。複数の車両の中には、特定の車両を含めても、含めなくてもよい。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００７６
【補正方法】変更
【補正の内容】
【００７６】
３．その他
（１）対象ログ送信と統計計算結果の送信条件の変更
図４のＳ１０４や図５のＳ１１３で、所定の条件を攻撃検知回数やセキュリティログの数としたが、セキュリティセンサの設置場所（例えば特定のＥＣＵ）やセキュリティセンサが接続されている通信バスの重要度に応じて、所定の条件を自動又は手動で設定するようにしてもよい。例えば、所定の条件としての攻撃検知の回数を設定することができるようにしてもよい。