【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3年1月21日(2021.1.21)

【公表番号】特表2020-535515(P2020-535515A)
【公表日】令和2年12月3日(2020.12.3)
【年通号数】公開・登録公報2020-049
【出願番号】特願2020-516821(P2020-516821)
【国際特許分類】
Ｇ０６Ｆ　21/57　(2013.01)
Ｇ０６Ｆ　11/34　(2006.01)
Ｇ０６Ｆ　21/56　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/57　３７０
Ｇ０６Ｆ　11/34　１９５
Ｇ０６Ｆ　11/34　１０４
Ｇ０６Ｆ　21/56

【手続補正書】
【提出日】令和2年11月17日(2020.11.17)
【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】
サーバ・グループを管理するためのシステムであって、
コンピュータ実行可能コンポーネントを格納するメモリと、
前記メモリに格納された前記コンピュータ実行可能コンポーネントを実行するプロセッサと、を含み、
前記コンピュータ実行可能コンポーネントは、
第１のサーバ・デバイスに関連する第１のリスクに応答して、前記第１のサーバ・デバイスおよび第２のサーバ・デバイスの脆弱性を軽減するために、前記サーバ・グループにパッチを適用するように動作可能なリスク評価コンポーネントであって、前記サーバ・グループが前記第１のサーバ・デバイスおよび前記第２のサーバ・デバイスからなる、前記リスク評価コンポーネントと、
前記サーバ・グループに対する第２のリスクを軽減するために、前記サーバ・グループに対する前記第２のリスクに関連するデータを監視するように動作可能な監視コンポーネントと、
を含む、システム。
【請求項２】
前記リスクは、マルウェア攻撃に対する前記第１のサーバ・デバイスの脆弱性に関連する、
請求項１に記載のシステム。
【請求項３】
前記コンピュータ実行可能コンポーネントは、前記サーバ・グループの前記第２のリスクを軽減するために、前記サーバ・グループを修正して、サーバ・グループの修正をもたらすように動作可能な調整コンポーネントをさらに含む、
請求項１または２に記載のシステム。

【請求項４】
前記サーバ・グループの修正は、前記第２のリスクを軽減するために、前記サーバ・グループから前記第２のサーバ・デバイスを除去する、
請求項３に記載のシステム。
【請求項５】
前記監視コンポーネントは、前記サーバ・グループが修正されたという示唆を受信するように動作可能である、
請求項１ないし４のいずれか１項に記載のシステム。
【請求項６】
前記リスク評価コンポーネントは、前記第１のサーバ・デバイスに関連するリスクを表すリスク・データを受信するように動作可能である、
請求項１ないし５のいずれか１項に記載のシステム。
【請求項７】
前記サーバ・グループは第１のサーバ・グループであり、前記リスク評価コンポーネントは、前記第１のサーバ・グループではない第２のサーバ・グループの第３のリスクを評価するように動作可能である、
請求項１ないし６のいずれか１項に記載のシステム。
【請求項８】
ワークステーション・デバイスから受信した以前のリスクに関連するリスク・データを分析し、リスク予測をもたらす学習コンポーネントをさらに含む、
請求項１ないし７のいずれか１項に記載のシステム。
【請求項９】
前記リスク予測は、前記サーバ・グループに対する第３のリスクを軽減するために、前記監視コンポーネントへの入力として使用される、
請求項８に記載のシステム。
【請求項１０】
サーバ・グループを管理するためのコンピュータ実装方法であって、
第１のサーバ・デバイスに関連する第１のリスクに応じて、プロセッサに動作可能に結合されたデバイスによって、前記第１のサーバ・デバイスおよび第２のサーバ・デバイスの脆弱性を軽減するために、前記サーバ・グループにパッチ適用することであって、前記サーバ・グループが前記第１のサーバ・デバイスおよび前記第２のサーバ・デバイスからなる、前記パッチ適用することと、
前記デバイスによって、前記サーバ・グループに対する第２のリスクを軽減するために、前記サーバ・グループに対する前記第２のリスクに関連するデータを監視することと、
を含む、コンピュータ実装方法。
【請求項１１】
前記リスクは、マルウェア攻撃に対する前記第１のサーバ・デバイスの脆弱性に関連する、
請求項１０に記載のコンピュータ実装方法。
【請求項１２】
前記デバイスによって、前記サーバ・グループの前記第２のリスクを軽減するために、前記サーバ・グループを修正し、サーバ・グループの修正をもたらすことをさらに含む、
請求項１０または１１のいずれか１項に記載のコンピュータ実装方法。
【請求項１３】
前記サーバ・グループの修正は、前記第２のリスクを軽減するために、前記サーバ・グループから前記第２のサーバ・デバイスを除去する、
請求項１２に記載のコンピュータ実装方法。
【請求項１４】
前記サーバ・グループが修正されたという示唆を受信することをさらに含む、
請求項１０ないし１３のいずれか１項に記載のコンピュータ実装方法。

【請求項１５】
前記第１のサーバ・デバイスに関連するリスクを表すリスク・データを受信することをさらに含む、
請求項１０ないし１４のいずれか１項に記載のコンピュータ実装方法。
【請求項１６】
前記サーバ・グループは第１のサーバ・グループであり、前記方法は、前記第１のサーバ・グループではない第２のサーバ・グループの第３のリスクを評価することをさらに含む、
請求項１０ないし１５のいずれか１項に記載の方法。
【請求項１７】
ワークステーション・デバイスから受信した以前のリスクに関連するリスク・データを分析し、リスク予測をもたらすことをさらに含む、
請求項１０ないし１６のいずれか１項に記載の方法。
【請求項１８】
前記リスク予測は、前記サーバ・グループに対する第３のリスクを軽減するために、監視コンポーネントへの入力として使用される、
請求項１７に記載の方法。
【請求項１９】
サーバ・グループを管理するためのコンピュータ・プログラムであって、
請求項１０ないし１８のいずれか１項に記載の方法の各ステップをコンピュータに実行させる、コンピュータ・プログラム。
【請求項２０】
請求項１９に記載の前記コンピュータ・プログラムをコンピュータ可読記録媒体に記録した記録媒体。