【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】平成30年2月8日(2018.2.8)

【公表番号】特表2017-502442(P2017-502442A)
【公表日】平成29年1月19日(2017.1.19)
【年通号数】公開・登録公報2017-003
【出願番号】特願2016-561597(P2016-561597)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
Ｇ０６Ｆ　 8/70　　(2018.01)
【ＦＩ】
Ｇ０６Ｆ　21/56　　３６０
Ｇ０６Ｆ　 9/06　　６２０Ｋ

【手続補正書】
【提出日】平成29年12月21日(2017.12.21)
【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】
複数の第一オブジェクトを受け付け、当該複数の第一オブジェクトを分析することにより、当該複数の第一オブジェクトの部分集合であり、当該複数の第一オブジェクトの数以下である複数の第二オブジェクトを容疑エクスプロイトとして特定するように構成された侵入防止システム（ＩＰＳ）ロジックと、
前記複数の第二オブジェクトの各々に含まれるコンテンツを処理し、処理中におけるエクスプロイトを示す異常挙動を監視することにより、当該複数の第二オブジェクトの第一部分集合に含まれる少なくとも一つの実証済みオブジェクトを分類するように構成された少なくとも一つの仮想マシンを含む仮想実行ロジックと、
少なくとも一つの非実証済みエクスプロイトの視覚表現とは異なる表示がなされる、前記少なくとも一つの実証済みエクスプロイトに関連付けられたエクスプロイト情報の視覚表現を含む表示を生成するように構成された表示生成ロジックと、
を備えており、
前記少なくとも一つの実証済みエクスプロイトに関連付けられたエクスプロイト情報の視覚表現は、前記少なくとも一つの非実証済みエクスプロイトの視覚表現よりも強調される、
脅威検出システム。
【請求項２】
前記少なくとも一つの実証済みエクスプロイトに関連付けられたエクスプロイト情報の表示は、インタラクティブダッシュボードを含んでおり、
前記インタラクティブダッシュボードは、第一表示領域を有しており、
前記第一表示領域は、
前記実証済みエクスプロイトのうち第一実証済みエクスプロイトの名前と、
前記第一実証済みエクスプロイトの検出に関連付けられた時刻と、
前記ＩＰＳロジックによる検出または前記第一実証済みエクスプロイトの実証に使用されたパターンと、
を示している、

請求項１に記載の脅威検出システム。
【請求項３】
前記インタラクティブダッシュボードは、ユーザに選択された実証済みエクスプロイトに係る追加情報へのアクセスを提供する第二表示領域を含んでいる、
請求項２に記載の脅威検出システム。
【請求項４】
侵入防止システム（ＩＰＳ）ロジックによって複数の第一オブジェクトを受け付け、
前記複数の第一オブジェクトの各々に対してエクスプロイトシグネチャチェックと脆弱性シグネチャチェックの一方を行なうことにより当該複数の第一オブジェクトの部分集合であり、当該複数の第一オブジェクトの数以下である複数の第二オブジェクトを容疑エクスプロイトとして特定することを含む分析を前記ＩＰＳロジックによって行ない、
前記複数の第二オブジェクトの各々に含まれるコンテンツを処理し、処理中におけるエクスプロイトを示す異常挙動を監視するように構成された少なくとも一つの仮想マシンを含む仮想実行ロジックによって、当該複数の第二オブジェクトの第一部分集合がエクスプロイトであることを自動的に実証し、
前記複数の第二オブジェクトの前記第一部分集合に関連付けられたエクスプロイト情報の視覚表現と、非実証済みエクスプロイトを含む前記複数の第二オブジェクトの第二部分集合に関連付けられた視覚表現を含む表示を生成し、
前記複数の第二オブジェクトの前記第二部分集合に関連付けられた前記エクスプロイト情報の視覚表現は、前記複数の第二オブジェクトの前記第一部分集合に関連付けられた前記エクスプロイト情報の視覚表現とは異なった表示がなされ、
前記少なくとも一つの実証済みエクスプロイトに関連付けられたエクスプロイト情報の視覚表現は、前記少なくとも一つの非実証済みエクスプロイトの視覚表現よりも強調される、
コンピュータ制御された方法。
【請求項５】
前記表示は、インタラクティブダッシュボードを含んでおり、
前記インタラクティブダッシュボードは、第一表示領域と第二表示領域を含んでおり、
前記第一表示領域は、
前記複数の第二オブジェクトの前記第一部分集合に含まれる第一実証済みエクスプロイトの名前と、
前記第一実証済みエクスプロイトの検出に関連付けられた時刻と、
前記第一実証済みエクスプロイトの検出または実証に使用されたパターンと、
を示しており、
前記第二表示領域は、前記複数の第二オブジェクトの前記第一部分集合に含まれる選択された実証済みエクスプロイトに係る追加情報へのアクセスを提供する、
請求項４に記載のコンピュータ制御された方法。
【請求項６】
少なくとも一つのエンドポイントデバイスのために報告を生成するように構成された報告ロジックを備えており、
前記報告は、情報とフィールドを含んでおり、
前記情報は、
複数の疑わしいオブジェクトの部分集合である少なくとも一つの強調されたオブジェクトと、
前記少なくとも一つのエクスプロイトの各々と、
を特定しており、
前記フィールドは、選択されることによって、前記疑わしいオブジェクトに関連付けられた前記少なくとも一つのエクスプロイトのうち選択されたエクスプロイトに関するより詳細な情報を提供する、
請求項１に記載の脅威検出システム。

【請求項７】
表示は、前記少なくとも一つのエクスプロイトに含まれる少なくとも一つのソースデバイスのアドレス情報を含む、
請求項６に記載の脅威検出システム。
【請求項８】
前記表示生成ロジックにより生成された前記表示は、前記少なくとも一つのエクスプロイトに含まれる少なくとも一つのソースデバイスのアドレス情報を含む、
請求項１に記載の脅威検出システム。
【請求項９】
少なくとも一つのエンドポイントデバイスのために報告を生成し、
前記報告は、情報とフィールドを含んでおり、
前記情報は、
複数の疑わしいオブジェクトの部分集合である少なくとも一つの強調されたオブジェクトと、
前記少なくとも一つのエクスプロイトの各々と、
を特定しており、
前記フィールドは、選択されることによって、前記疑わしいオブジェクトに関連付けられた前記少なくとも一つのエクスプロイトのうち選択されたエクスプロイトに関するより詳細な情報を提供する、
請求項４に記載のコンピュータ制御された方法。
【請求項１０】
前記表示は、前記少なくとも一つのエクスプロイトに含まれる少なくとも一つのソースデバイスのアドレス情報を含む、
請求項９に記載のコンピュータ制御された方法。