【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23年4月14日(2011.4.14)

【公表番号】特表2010-521749(P2010-521749A)
【公表日】平成22年6月24日(2010.6.24)
【年通号数】公開・登録公報2010-025
【出願番号】特願2009-553835(P2009-553835)
【国際特許分類】
Ｇ０６Ｆ　21/20　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　　３３０Ａ

【手続補正書】
【提出日】平成23年2月22日(2011.2.22)
【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】
企業セキュリティ環境内の複数のエンドポイントコンピュータ間でセキュリティ関連情報を共有可能にするセキュリティ関連情報を共有するための方法であって、
前記エンドポイントコンピュータが、前記エンドポイントコンピュータが使用できるセキュリティ関連情報の意味抽象を使用して前記企業セキュリティ環境内のオブジェクトを記述するステップであって、前記意味抽象はタイプ別に分類され、前記エンドポイントコンピュータの各々によって共通に使用可能である、ステップと、
前記エンドポイントコンピュータが、同意する側のエンドポイントコンピュータが同意する前記意味抽象を、前記意味抽象のタイプに基づく同意に従って公開するステップと
を含むことを特徴とする方法。
【請求項２】
前記意味抽象は、事前定義された分類法を使用して、エンドポイントコンピュータによるコンテキストの割り当てを前記セキュリティ関連情報に提供するように構成されたセキュリティアセスメントであることを特徴とする請求項１に記載の方法。
【請求項３】
前記事前定義された分類法は、オブジェクトタイプ及びアセスメントカテゴリを含む、体系化された語彙を使用することを特徴とする請求項２に記載の方法。
【請求項４】
前記オブジェクトタイプは、ホスト、ユーザ、サービス、データ又は企業のうちの少なくとも１つを含むことを特徴とする請求項３に記載の方法。
【請求項５】
前記アセスメントカテゴリは、「脆弱な」、「コンプロマイズド」、「攻撃中」、「対象の」、「破壊されている」、「悪意ある」のうちの少なくとも１つを含むことを特徴とする請求項３に記載の方法。
【請求項６】
前記アセスメントカテゴリの特定のものが、前記オブジェクトタイプの特定のものにマッピングされることを特徴とする請求項３に記載の方法。
【請求項７】
前記セキュリティアセスメントは複数のフィールドを有し、前記複数のフィールドのう

ちの少なくとも１つは、エンドポイントコンピュータが前記セキュリティアセスメントに対して持つ自信のレベルを表すように構成された忠実度フィールドであることを特徴とする請求項２に記載の方法。
【請求項８】
前記セキュリティアセスメントは複数のフィールドを有し、前記複数のフィールドのうちの少なくとも１つは、前記セキュリティアセスメントが有効であると期待される期間の、エンドポイントコンピュータによる予測を表すように構成された存続時間フィールドであることを特徴とする請求項２に記載の方法。
【請求項９】
前記複数のエンドポイントコンピュータのうちの少なくとも１つはセキュリティソリューションオブジェクトを有し、前記セキュリティソリューションオブジェクトは、セキュリティ製品、セキュリティソリューション、管理製品、管理ソリューション、セキュリティサービス、又は管理サービスの１つから選択されたものであることを特徴とする請求項１に記載の方法。
【請求項１０】
エンドポイントコンピュータが企業セキュリティ環境内でセキュリティ関連データを共有できるようにする方法であって、
前記エンドポイントコンピュータが、イベントを記述するためのセキュリティアセスメントを生成するステップであって、前記セキュリティアセスメントは、少なくとも部分的に、前記エンドポイントコンピュータによって監視されるシステムに関するローカルで使用可能な情報に基づいて、前記イベントにコンテキスト的意味を与えるように構成され、前記セキュリティアセスメントが有効であり続ける時間間隔によって画定される、ステップと、
前記エンドポイントコンピュータが、前記企業セキュリティ環境内の他のエンドポイントコンピュータによって生成された、使用可能なセキュリティアセスメントのサブセットへの同意に従って現在のセキュリティアセスメントを受信するステップと、
前記エンドポイントコンピュータが、前記セキュリティアセスメントごとの応答ポリシに従って応答を実行するステップと
を含むことを特徴とする方法。
【請求項１１】
前記応答はローカルアクションを含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
セキュリティコンテキストは、前記サブセットからの１つ又は複数の前に受信したセキュリティアセスメントが有効である限り、前記前に受信したセキュリティアセスメントを含むことを特徴とする請求項１０に記載の方法。
【請求項１３】
前記ローカルで使用可能な情報は、前記エンドポイントコンピュータによって実行された１つ又は複数の過去のローカルアクションをさらに含むことを特徴とする請求項１１に記載の方法。
【請求項１４】
前記エンドポイントコンピュータが、受信したセキュリティアセスメントが有効でなくなったら前記ローカルアクションをロールバックするステップをさらに含むことを特徴とする請求項１１に記載の方法。
【請求項１５】
企業全体のセキュリティポリシを構成する方法であって、
前記エンドポイントコンピュータが、セキュリティイベントのアセスメントが前記企業内の複数のエンドポイントコンピュータによって生成される、セキュリティアセスメントスキーマを定義するステップであって、前記アセスメントは、タイプ別に分類され、事前定義された分類法を使用して前記セキュリティイベントにコンテキスト的意味を与える、ステップと、

前記エンドポイントコンピュータが、前記アセスメントを、各アセスメントタイプへの応答を記述するルールのマトリックスへのアンカーポイントとして使用するステップと
を含むことを特徴とする方法。
【請求項１６】
前記エンドポイントコンピュータが、中央地点にある前記複数のエンドポイントコンピュータによって生成された前記アセスメントを収集するステップをさらに含むことを特徴とする請求項１５に記載の方法。
【請求項１７】
前記エンドポイントコンピュータが、前記エンドポイントコンピュータによって生成され、前記エンドポイントコンピュータによって実行されるローカルアクションに関連付けられた通知を収集するステップをさらに含むことを特徴とする請求項１５に記載の方法。
【請求項１８】
前記アセスメントタイプは、オブジェクトタイプ、アセスメントカテゴリ、又はイベントの重大度のうちの少なくとも２つの組合せによって定義されることを特徴とする請求項１５に記載の方法。
【請求項１９】
前記ルールのマトリックスは、前記アセスメントの忠実度及びイベントの重大度の大きさを含むことを特徴とする請求項１５に記載の方法。
【請求項２０】
前記エンドポイントコンピュータが、前記アンカーポイント及び前記ルールのマトリックスの表示を示すためのグラフィカルユーザインターフェースを表示するステップをさらに含むことを特徴とする請求項１５に記載の方法。