【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７部門第３区分
【発行日】平成29年11月9日(2017.11.9)

【公表番号】特表2016-535476(P2016-535476A)
【公表日】平成28年11月10日(2016.11.10)
【年通号数】公開・登録公報2016-063
【出願番号】特願2016-521642(P2016-521642)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/44　(2013.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０６Ｆ　21/44
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】平成29年10月2日(2017.10.2)
【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】
セキュリティオブジェクトをオーケストレートするためのプロセスであって、
ポリシーエンジンに接続されたデータベースにおいて、複数のポリシーを定義し、記憶することと、
前記ポリシーエンジンによって、少なくとも１つの通信デバイスに配布するための前記セキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性を受け取ることと、
前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記複数のポリシーの少なくとも１つとに少なくとも部分的に基づいて、前記ポリシーエンジンでもって、前記セキュリティオブジェクトの容認可能性を決定することと、
前記セキュリティオブジェクトが容認可能であると決定されることに応答して、前記ポリシーエンジンに関連付けられた前記少なくとも１つの通信デバイスに、同じ前記セキュリティオブジェクトを配布することと、ここにおいて、前記少なくとも１つの通信デバイスは、前記セキュリティオブジェクトに少なくとも部分的に基づいて通信を確立する、
を備えるプロセス。
【請求項２】
前記セキュリティオブジェクトは暗号化鍵である、請求項１に記載のプロセス。
【請求項３】
前記少なくとも１つのオブジェクト属性は、前記セキュリティオブジェクト、前記セキュリティオブジェクトを生成する第１のデバイス、前記セキュリティオブジェクトを送る第２のデバイス、前記セキュリティオブジェクトを受け取る第３のデバイス、前記第１のデバイスに関連付けられた第１のユーザ、前記第２のデバイスに関連付けられた第２のユーザ、および、前記第３のデバイスに関連付けられた第３のユーザの内の少なくとも１つの特徴を備える、請求項１に記載のプロセス。
【請求項４】

前記少なくとも１つのオブジェクト属性は、セキュリティオブジェクトサイズ、前記セキュリティオブジェクトが生成された時間、前記セキュリティオブジェクトが生成された地理位置、前記セキュリティオブジェクトの分類、鍵ソースに関連付けられた役割、ソースデバイスに関連づけられた役割、および、ターゲットデバイスに関連付けられた役割の内の少なくとも１つを備える、請求項１に記載のプロセス。
【請求項５】
前記複数のポリシーは、前記セキュリティオブジェクトサイズが所定のサイズ範囲の中にある場合に前記セキュリティオブジェクトを容認することを備える、請求項４に記載のプロセス。
【請求項６】
前記複数のポリシーは、前記セキュリティオブジェクトが所定の時間間隔の中で生成された場合に前記セキュリティオブジェクトを容認することを備える、請求項４に記載のプロセス。
【請求項７】
前記複数のポリシーは、前記セキュリティオブジェクトが生成された前記地理位置が所定のエリアの中にある場合に前記セキュリティオブジェクトを容認することを備える、請求項４に記載のプロセス。
【請求項８】
前記複数のポリシーは、前記セキュリティオブジェクトの前記分類が所定のセキュリティオブジェクト分類グループと関連付けられている場合に前記セキュリティオブジェクトを容認することを備える、請求項４に記載のプロセス。
【請求項９】
前記複数のポリシーは、前記鍵ソース、前記ソースデバイス、または、前記ターゲットデバイスに関連付けられた前記役割が役割の所定のグループに関連付けられている場合に前記セキュリティオブジェクトを容認することを備える、請求項４に記載のプロセス。
【請求項１０】
鍵ソースに不認可インジケータを送ることと、
前記鍵ソースに前記セキュリティオブジェクトの不適当な点を知らせるヒントを送信することと、ここにおいて、前記セキュリティオブジェクトは、前記鍵ソースから受信される、
を更に備える、請求項１に記載のプロセス。
【請求項１１】
前記ポリシーエンジンによって、前記セキュリティオブジェクトを受け取ることは、
前記ポリシーエンジンによって、前記セキュリティオブジェクトを生成するための要求を受け取ることと、
前記ポリシーエンジンによって、前記セキュリティオブジェクトを生成することと、を備える、請求項１に記載のプロセス。
【請求項１２】
セキュリティオブジェクトをオーケストレートするためのプロセスであって、
第１の鍵オーケストレーションデバイスの第１のデータベースにおいて第１の複数のポリシーを定義し、記憶することと、前記第１のデータベースは、第１のエンタープライズに関連付けられる、
前記第１のエンタープライズに関連付けられた前記第１の鍵オーケストレーションデバイスでもって、第２のエンタープライズに関連付けられた第２の鍵オーケストレーションデバイスから、少なくとも１つの通信デバイスに配布するための前記セキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性とを受け取ることと、
前記第１の鍵オーケストレーションデバイスでもって、前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記第１の複数のポリシーの内の少なくとも１つとに少なくとも部分的に基づいて、前記セキュリティオブジェクト

の容認性を決定することと、
前記第１のエンタープライズに関連付けられた第１の通信デバイスに、同じ前記セキュリティオブジェクトを配布することと、
を備えるプロセス。
【請求項１３】
前記第２の鍵オーケストレーションデバイスの第２のデータベースにおいて第２の複数のポリシーを定義し、記憶することを更に備え、
少なくとも、前記第１の複数のポリシーの第１の部分と前記第２の複数のポリシーの第２の部分は同じである、
請求項１２に記載のプロセス。
【請求項１４】
前記第１の鍵オーケストレーションデバイスから前記第２の鍵オーケストレーションデバイスに、前記セキュリティオブジェクトを送ることと、
前記第２のエンタープライズに関連付けられた第２の通信デバイスに、前記セキュリティオブジェクトを配布することと、ここにおいて、前記第１の通信デバイスと前記第２の通信デバイスは、前記セキュリティオブジェクトに基づいて通信を確立する、
を更に備えた、請求項１２に記載のプロセス。
【請求項１５】
前記第１の鍵オーケストレーションデバイスから前記第２の鍵オーケストレーションデバイスに、前記セキュリティオブジェクトを送ることと、
前記第２の鍵オーケストレーションデバイスでもって、前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記第２の複数のポリシーの内の少なくとも１つとに少なくとも部分的に基づいて、前記セキュリティオブジェクトの容認性を決定することと、
前記第２のエンタープライズに関連付けられた第２の通信デバイスに前記セキュリティオブジェクトを配布することと、ここにおいて、前記第１の通信デバイスと前記第２の通信デバイスは、前記セキュリティオブジェクトに基づいて通信を確立する、
を更に備える、請求項１３に記載のプロセス。
【請求項１６】
第２の鍵オーケストレーションデバイスから、前記セキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性を受け取ることは、
前記第２の鍵オーケストレーションデバイスから前記第１の鍵オーケストレーションデバイスによって、前記セキュリティオブジェクトを生成するための要求を受け取ることと、
前記第１のエンタープライズに関連付けられた鍵ソースでもって、前記要求に応答して前記セキュリティオブジェクトを生成することと、
を備える、請求項１２に記載のプロセス。
【請求項１７】
実行されたとき、プロセッサに、
データベースの中に複数のポリシーを定義させる、
少なくとも１つの通信デバイスに配布するためのセキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性を受け取らせる、
前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記複数のポリシーの内の少なくとも１つとに少なくとも部分的に基づいて、前記セキュリティオブジェクトの容認性を決定させる、
前記セキュリティオブジェクトが容認可能と決定されることに応答して、前記プロセッサに関連付けられた少なくとも１つの通信デバイスに、同じ前記セキュリティオブジェクトを配布させる、ここにおいて、前記少なくとも１つの通信デバイスは、前記セキュリ

ティオブジェクトに少なくとも部分的に基づいて通信を確立する、
コンピュータ読出し可能命令を備えるコンピュータ読出し可能な一時的ではない媒体。
【請求項１８】
前記セキュリティオブジェクトは暗号化鍵である、請求項１７に記載のコンピュータ読出し可能な一時的ではない媒体。
【請求項１９】
前記少なくとも１つのオブジェクト属性は、セキュリティオブジェクトサイズ、セキュリティオブジェクトが生成された時間、セキュリティオブジェクトが生成された地理位置、セキュリティオブジェクトの分類、鍵ソースに関連付けられた役割、ソースデバイスに関連付けられた役割、および、ターゲットデバイスに関連付けられた役割の内の少なくとも１つを備える、請求項１７に記載のコンピュータ読出し可能な一時的ではない媒体。
【請求項２０】
前記複数のポリシーは、前記セキュリティオブジェクトサイズが所定のサイズ範囲にある場合、前記セキュリティオブジェクトが生成された前記時間が所定の時間間隔の中にある場合、前記セキュリティオブジェクトが生成された前記地理位置が所定のエリアの中にある場合、前記セキュリティオブジェクトの前記分類が所定のセキュリティオブジェクト分類グループの中に含まれている場合、前記鍵ソース、前記ソースデバイス、または、前記ターゲットデバイスに関連付けられた前記役割が役割の所定のグループに関連付けられている場合の少なくとも１つの場合に前記セキュリティオブジェクトを容認することを備える、請求項１９に記載のコンピュータ読出し可能な一時的ではない媒体。
【請求項２１】
前記少なくとも１つのオブジェクト属性は、前記セキュリティオブジェクトの暗号法の特徴を備える、請求項１に記載のプロセス。
【請求項２２】
前記少なくとも１つのオブジェクト属性は、前記セキュリティオブジェクトの暗号法のアルゴリズムを備える、請求項１に記載のプロセス。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０１３７
【補正方法】変更
【補正の内容】
【０１３７】
[0145] この中に開示された実施形態は、限定としてではなく、例示として、全ての観点で考慮されるべきである。本開示は、決して、上述の実施形態に限定されることはない。様々な修正や変更が、その開示の意図や範囲から逸脱しないで、実施形態に対してなされ得る。特許請求の範囲の意味や均等の範囲の中にはいる様々な修正や変更は、本開示の範囲の中に入ることを意図される。
以下、本願出願時点で添付された特許請求の範囲に記載された発明を付記する。
［Ｃ１］
セキュリティオブジェクトをオーケストレートするためのプロセスであって、
ポリシーエンジンに接続されたデータベースにおいて、複数のポリシーを定義し、記憶することと、
前記ポリシーエンジンによって、前記セキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性を受け取ることと、
前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記複数のポリシーの少なくとも１つとに少なくとも部分的に基づいて、前記ポリシーエンジンでもって、前記セキュリティオブジェクトの容認可能性を決定することと、
前記セキュリティオブジェクトが容認可能であると決定された場合、前記ポリシーエンジンに関連付けられた少なくとも１つの通信デバイスに前記セキュリティオブジェクトを配布することと、ここにおいて、前記少なくとも１つの通信デバイスは、前記セキュリテ

ィオブジェクトに少なくとも部分的に基づいて通信を確立する、
を備えるプロセス。
［Ｃ２］
前記セキュリティオブジェクトは暗号化鍵である、［Ｃ１］に記載のプロセス。
［Ｃ３］
前記少なくとも１つのオブジェクト属性は、前記セキュリティオブジェクト、前記セキュリティオブジェクトを生成する第１のデバイス、前記セキュリティオブジェクトを送る第２のデバイス、前記セキュリティオブジェクトを受け取る第３のデバイス、前記第１のデバイスに関連付けられた第１のユーザ、前記第２のデバイスに関連付けられた第２のユーザ、および、前記第３のデバイスに関連付けられた第３のユーザの内の少なくとも１つの特徴を備える、［Ｃ１］に記載のプロセス。
［Ｃ４］
前記少なくとも１つのオブジェクト属性は、セキュリティオブジェクトサイズ、前記セキュリティオブジェクトが生成された時間、前記セキュリティオブジェクトが生成された地理位置、前記セキュリティオブジェクトの分類、鍵ソースに関連付けられた役割、ソースデバイスに関連づけられた役割、および、ターゲットデバイスに関連付けられた役割の内の少なくとも１つを備える、［Ｃ１］に記載のプロセス。
［Ｃ５］
前記複数のポリシーは、前記セキュリティオブジェクトサイズが所定のサイズ範囲の中にある場合に前記セキュリティオブジェクトを容認することを備える、［Ｃ４］に記載のプロセス。
［Ｃ６］
前記複数のポリシーは、前記セキュリティオブジェクトが生成された前記時間が所定の時間間隔の中にある場合に前記セキュリティオブジェクトを容認することを備える、［Ｃ４］に記載のプロセス。
［Ｃ７］
前記複数のポリシーは、前記セキュリティオブジェクトが生成された前記地理位置が所定のエリアの中にある場合に前記セキュリティオブジェクトを容認することを備える、［Ｃ４］に記載のプロセス。
［Ｃ８］
前記複数のポリシーは、前記セキュリティオブジェクトの前記分類が所定のセキュリティオブジェクト分類グループと関連付けられている場合に前記セキュリティオブジェクトを容認することを備える、［Ｃ４］に記載のプロセス。
［Ｃ９］
前記複数のポリシーは、前記鍵ソース、前記ソースデバイス、または、前記ターゲットデバイスに関連付けられた前記役割が役割の所定のグループに関連付けられている場合に前記セキュリティオブジェクトを容認することを備える、［Ｃ４］に記載のプロセス。
［Ｃ１０］
鍵ソースに不認可インジケータを送ることと、
前記鍵ソースに前記セキュリティオブジェクトの不適当な点を知らせるヒントを送信することと、ここにおいて、前記セキュリティオブジェクトは、前記鍵ソースから受信される、
を更に備える、［Ｃ１］に記載のプロセス。
［Ｃ１１］
前記ポリシーエンジンによって、前記セキュリティオブジェクトを受け取ることは、
前記ポリシーエンジンによって、前記セキュリティオブジェクトを生成するための要求を受け取ることと、
前記ポリシーエンジンによって、セキュリティオブジェクトを生成することと、を備える、［Ｃ１］に記載のプロセス。
［Ｃ１２］

セキュリティオブジェクトをオーケストレートするためのプロセスであって、
第１の鍵オーケストレーションデバイスの第１のデータベースにおいて第１の複数のポリシーを定義し、記憶することと、前記第１のデータベースは、第１のエンタープライズに関連付けられる、
前記第１のエンタープライズに関連付けられた前記第１の鍵オーケストレーションデバイスでもって、第２のエンタープライズに関連付けられた第２の鍵オーケストレーションデバイスから、前記セキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性とを受け取ることと、
前記第１の鍵オーケストレーションデバイスでもって、前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記第１の複数のポリシーの内の少なくとも１つとに少なくとも部分的に基づいて、前記セキュリティオブジェクトの容認性を決定することと、
前記第１のエンタープライズに関連付けられた第１の通信デバイスに前記セキュリティオブジェクトを配布することと、
を備えるプロセス。
［Ｃ１３］
前記第２の鍵オーケストレーションデバイスの第２のデータベースにおいて第２の複数のポリシーを定義し、記憶することを更に備え、
少なくとも、前記第１の複数のポリシーの第１の部分と前記第２の複数のポリシーの第２の部分は同じである、
［Ｃ１２］に記載のプロセス。
［Ｃ１４］
前記第１の鍵オーケストレーションデバイスから前記第２の鍵オーケストレーションデバイスに、前記セキュリティオブジェクトを送ることと、
前記第２のエンタープライズに関連付けられた第２の通信デバイスに、前記セキュリティオブジェクトを配布することと、ここにおいて、前記第１の通信デバイスと前記第２の通信デバイスは、前記セキュリティオブジェクトに基づいて通信を確立する、を更に備えた、［Ｃ１２］に記載のプロセス。
［Ｃ１５］
前記第１の鍵オーケストレーションデバイスから前記第２の鍵オーケストレーションデバイスに、前記セキュリティオブジェクトを送ることと、
前記第２の鍵オーケストレーションデバイスでもって、前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記第２の複数のポリシーの内の少なくとも１つとに少なくとも部分的に基づいて、前記セキュリティオブジェクトの容認性を決定することと、
前記第２のエンタープライズに関連付けられた第２の通信デバイスに前記セキュリティオブジェクトを配布することと、ここにおいて、前記第１の通信デバイスと前記第２の通信デバイスは、前記セキュリティオブジェクトに基づいて通信を確立する、を更に備える、［Ｃ１３］に記載のプロセス。
［Ｃ１６］
第２の鍵オーケストレーションデバイスから、前記セキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性を受け取ることは、
前記第２の鍵オーケストレーションデバイスから前記第１の鍵オーケストレーションデバイスによって、前記セキュリティオブジェクトを生成するための要求を受け取ることと、
前記第１のエンタープライズに関連付けられた鍵ソースでもって、前記要求に応答して前記セキュリティオブジェクトを生成することと、
を備える、［Ｃ１２］に記載のプロセス。
［Ｃ１７］

実行されたとき、プロセッサに、
データベースの中に複数のポリシーを定義させる、
セキュリティオブジェクトと前記セキュリティオブジェクトに関連付けられた少なくとも１つのオブジェクト属性を受け取らせる、
前記少なくとも１つのオブジェクト属性と前記少なくとも１つのオブジェクト属性に対応する前記複数のポリシーの内の少なくとも１つとに少なくとも部分的に基づいて、前記セキュリティオブジェクトの容認性を決定させる、
前記セキュリティオブジェクトが容認可能と決定された場合に、前記プロセッサに関連付けられた少なくとも１つの通信デバイスに前記セキュリティオブジェクトを配布させる、ここにおいて、前記少なくとも１つの通信デバイスは、前記セキュリティオブジェクトに少なくとも部分的に基づいて通信を確立する、
コンピュータ読出し可能命令を備えるコンピュータ読出し可能な媒体。
［Ｃ１８］
前記セキュリティオブジェクトは暗号化鍵である、［Ｃ１７］に記載のコンピュータ読出し可能な媒体。
［Ｃ１９］
前記少なくとも１つのオブジェクト属性は、セキュリティオブジェクトサイズ、セキュリティオブジェクトが生成された時間、セキュリティオブジェクトが生成された地理位置、セキュリティオブジェクトの分類、鍵ソースに関連付けられた役割、ソースデバイスに関連付けられた役割、および、ターゲットデバイスに関連付けられた役割の内の少なくとも１つを備える、［Ｃ１７］に記載のコンピュータ読出し可能な媒体。
［Ｃ２０］
前記複数のポリシーは、前記セキュリティオブジェクトサイズが所定のサイズ範囲にある場合、前記セキュリティオブジェクトが生成された前記時間が所定の時間間隔の中にある場合、前記セキュリティオブジェクトが生成された前記地理位置が所定のエリアの中にある場合、前記セキュリティオブジェクトの前記分類が所定のセキュリティオブジェクト分類グループの中に含まれている場合、前記鍵ソース、前記ソースデバイス、または、前記ターゲットデバイスに関連付けられた前記役割が役割の所定のグループに関連付けられている場合の少なくとも１つの場合に前記セキュリティオブジェクトを容認することを備える、［Ｃ１９］に記載のコンピュータ読出し可能な媒体。