(19)日本国特許庁(JP)　(12)特許公報(B2)　(11)特許番号
特許第7288045号
(P7288045)
(45)発行日　令和5年6月6日(2023.6.6)　(24)登録日　令和5年5月29日(2023.5.29)

(51)国際特許分類　ＦＩ
Ｇ０６Ｆ　21/62　(2013.01)　Ｇ０６Ｆ　21/62
Ｇ０６Ｆ　21/31　(2013.01)　Ｇ０６Ｆ　21/31

請求項の数　12　（全28頁）

(21)出願番号　特願2021-513372(P2021-513372)
(86)(22)出願日　令和1年5月9日(2019.5.9)
(65)公表番号　特表2021-521575(P2021-521575A)
(43)公表日　令和3年8月26日(2021.8.26)
(86)国際出願番号　PCT/US2019/031472
(87)国際公開番号　WO2019/217649
(87)国際公開日　令和1年11月14日(2019.11.14)
審査請求日　令和2年12月2日(2020.12.2)
(31)優先権主張番号　62/670,073
(32)優先日　平成30年5月11日(2018.5.11)
(33)優先権主張国・地域又は機関　米国(US)
(31)優先権主張番号　62/764,777
(32)優先日　平成30年8月16日(2018.8.16)
最終頁に続く

(73)特許権者　520440124
サイジェント テクノロジー インコーポレイテッド
ＣＩＧＥＮＴ ＴＥＣＨＮＯＬＯＧＹ，ＩＮＣ．
アメリカ合衆国 フロリダ州 ３３９０１ フォート マイヤーズ ウィドマン ウェイ ２２１１ スイート １５０
(74)代理人　100147485
弁理士　杉村 憲司
(74)代理人　230118913
弁護士　杉村 光嗣
(74)代理人　100211395
弁理士　鈴木 裕貴
(72)発明者　トニー エドワード フェッセル
最終頁に続く

(54)【発明の名称】　改良されたデータ制御及びアクセスの方法及びシステム

(57)【特許請求の範囲】

【請求項１】

データアクセスを制御する方法であって、

コンピューティングシステム内のデータストレージデバイスのホストコントローラであって、前記コンピューティングシステムによって実行されるオペレーティングシステムとは別個に動作するように構成された、前記ホストコントローラのメモリに、１つ以上の確立された規則を記憶することであって、前記１つ以上の確立された規則は、複数のデータ項目の第１の部分に関連付けられている、前記記憶することと、

前記ホストコントローラの受信機により、前記オペレーティングシステムによって送信されるデータアクション要求であって、データコマンドと１つ以上の影響を受けるデータ項目とを示す、前記データアクション要求を受信することと、

前記１つ以上の影響を受けるデータ項目が前記複数のデータ項目の前記第１の部分に含まれていると判定することに応答して、

前記ホストコントローラにより、前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定することと、

前記データアクション要求が遵守している場合に、前記ホストコントローラにより、前記１つ以上の影響を受けるデータ項目に対する前記データコマンドを実行することと、

前記データアクション要求が遵守していない場合に、前記ホストコントローラの送信機により、前記１つ以上の影響を受けるデータ項目に対する阻止されたアクセスを示す、前記データアクション要求に対する応答を送信することと、

前記１つ以上の影響を受けるデータ項目が前記複数のデータ項目の前記第１の部分に含まれていないと判定することに応答して、前記ホストコントローラにより、前記１つ以上の影響を受けるデータ項目に対する前記データコマンドを実行することと、
前記ホストコントローラにより、前記オペレーティングシステムに関する潜在的な問題が検出された場合に、前記オペレーティングシステムの代わりにリカバリオペレーティングシステムを実行することと、
を含む、方法。
【請求項２】
前記１つ以上の確立された規則のそれぞれは、複数のデータコマンドのうちの１つに関連付けられ、
前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定することは、前記データアクション要求が、前記１つ以上の確立された規則のうち、前記データアクション要求に示される前記データコマンドに関連付けられた規則を遵守しているか否かを判定することを含む、請求項１に記載の方法。
【請求項３】
前記１つ以上の確立された規則は、地理的領域を含み、
前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定することは、前記コンピューティングシステムが前記地理的領域内にあるか否かを判定することを含む、請求項１に記載の方法。
【請求項４】
前記判定することは、前記コンピューティングシステムとインタフェース接続された全地球測位デバイスから地理的位置を受信することを含む、請求項３に記載の方法。
【請求項５】
前記１つ以上の確立された規則は、セキュリティデバイスの存在を要求する規則を含み、
前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定することは、前記コンピューティングシステム内の前記セキュリティデバイスの存在を検出することを含む、請求項１に記載の方法。
【請求項６】
データアクセスを制御するシステムであって、
データストレージデバイスを含むコンピューティングシステムを含み、
前記データストレージデバイスは、ホストコントローラを含み、
前記ホストコントローラは、前記コンピューティングシステムによって実行されるオペレーティングシステムとは別個に動作するように構成されており、
前記ホストコントローラは、
前記ホストコントローラのメモリに、１つ以上の確立された規則を記憶することであって、前記１つ以上の確立された規則は、複数のデータ項目の第１の部分に関連付けられている、前記記憶することを実行し、
前記オペレーティングシステムによって送信されるデータアクション要求であって、データコマンドと１つ以上の影響を受けるデータ項目とを示す、前記データアクション要求を受信し、
前記１つ以上の影響を受けるデータ項目が前記複数のデータ項目の前記第１の部分に含まれていると判定することに応答して、
前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定し、
前記データアクション要求が遵守している場合に、前記１つ以上の影響を受けるデータ項目に対する前記データコマンドを実行し、
前記データアクション要求が遵守していない場合に、前記１つ以上の影響を受けるデータ項目に対する阻止されたアクセスを示す、前記データアクション要求に対する応答を送信し、
前記１つ以上の影響を受けるデータ項目が前記複数のデータ項目の前記第１の部分に

含まれていないと判定することに応答して、前記ホストコントローラにより、前記１つ以上の影響を受けるデータ項目に対する前記データコマンドを実行し、
前記オペレーティングシステムに関する潜在的な問題が検出された場合に、前記オペレーティングシステムの代わりにリカバリオペレーティングシステムを実行するように構成されている、システム。
【請求項７】
前記１つ以上の確立された規則のそれぞれは、複数のデータコマンドのうちの１つに関連付けられ、
前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定することは、前記データアクション要求が、前記１つ以上の確立された規則のうち、前記データアクション要求に示される前記データコマンドに関連付けられた規則を遵守しているか否かを判定することを含む、請求項６に記載のシステム。
【請求項８】
前記１つ以上の確立された規則は、地理的領域を含み、
前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定することは、前記コンピューティングシステムが前記地理的領域内にあるか否かを判定することを含む、請求項６に記載のシステム。
【請求項９】
前記判定することは、前記コンピューティングシステムとインタフェース接続された全地球測位デバイスから地理的位置を受信することを含む、請求項８に記載のシステム。
【請求項１０】
前記１つ以上の確立された規則は、セキュリティデバイスの存在を要求する規則を含み、
前記データアクション要求が前記１つ以上の確立された規則を遵守しているか否かを判定することは、前記コンピューティングシステム内の前記セキュリティデバイスの存在を検出することを含む、請求項６に記載のシステム。
【請求項１１】
前記１つ以上の影響を受けるデータ項目が前記複数のデータ項目の前記第１の部分に含まれていないと判定することに応答して、前記ホストコントローラにより、前記複数のデータ項目の前記第１の部分に含まれていない前記１つ以上の影響を受けるデータ項目に対する前記データコマンドを実行することを含む、請求項１に記載の方法。
【請求項１２】
前記ホストコントローラは、前記１つ以上の影響を受けるデータ項目が前記複数のデータ項目の前記第１の部分に含まれていないと判定することに応答して、前記複数のデータ項目の前記第１の部分に含まれていない前記１つ以上の影響を受けるデータ項目に対する前記データコマンドを実行するように構成されている、請求項６に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、コンピューティングデバイスにおけるデータの使用及びアクセスの監視及び制御に関し、具体的には、ホストコントローラドライバ及びソフトウェアデバイスを使用して、データストレージレベルでのデータへのアクセスを監視し、その制御を行って、重要なデータの攻撃、悪用、及び消失を阻止することに関する。
【背景技術】
【０００２】
コンピューティングデバイス内のデータは、非常に重要な場合がある。多くの場合、データの消失は、攻撃による場合でも、偶発的な削除による場合でも、極めて重大であり、ある場合には、完全に取り返しのつかないことである。データ保護のほとんどの解決策は、オペレーティングシステムレベルで実行され、オペレーティングシステムで発生する攻撃を監視し、データを定期的にバックアップして、何らかの事態が発生した場合にリカバリできるようにするために、ソフトウェアアプリケーションが使用される。しかしながら

、このようなアプリケーションは、オペレーティングシステムレベルで発生し、そのために検出可能な消失又は攻撃に対してのみ有用である。例えば、オペレーティングシステム自体を攻撃してオペレーティングシステムの起動を阻止するようなネットワークデバイスから来る攻撃は、オペレーティングシステムがアクティブなときにのみ実行されるアプリケーションプログラムでは防ぐことができず、オリジナルのデータと同様にデータバックアップを攻撃することができる。

【０００３】

したがって、オペレーティングシステムよりも下のレベルで実施されるデータ監視及び制御を可能にする解決策が必要とされている。

【発明の概要】

【０００４】

本開示は、データストレージデバイスのホストコントローラ、及び／又はコンピューティングデバイスのオペレーティングシステムとは別個に動作する別のハードウェアデバイスにおける実装を介して、データストレージレベルで発生するデータアクセス監視及び制御のシステム及び方法の記述を提供する。このようなデバイスは、データストレージデバイスの個々のデータセクタ及びブロックへのアクセスを監視して、データ自体の内容に関係なく、その使用及びアクセスを監視することができる。このタイプの実装では、オペレーティングシステムが侵害されている可能性がある場合に、データのバックアップ、攻撃の停止、及びその他のアクションを実行でき、これには、ユーザが変化を認識していなくても、侵害されていない異なるオペレーティングシステムの実行を選択することも含まれる。この結果、オペレーティングシステムレベルではできない、より高いレベルのデータ保護、監視、及び制御が実施される。

【０００５】

データフローを制御する方法は、オペレーティングシステムのユーザに基づいてユーザパーミッションを識別することと、データストレージデバイスのホストコントローラにより、識別されたパーミッションに基づいてデータの取得を制御することと、を含む。

【０００６】

オペレーティングシステムの自動復元の方法は、データストレージデバイスの第１のデータセクタ内に第１のオペレーティングシステムファイルのセットを記憶することと、データストレージデバイスの第２のデータセクタ内に第２のオペレーティングシステムファイルのセットを記憶することと、データストレージデバイスのホストコントローラにより、復元コマンドを受信することと、データストレージデバイスのホストコントローラ内のドライバに送信されたデータ取得要求に、第１のオペレーティングシステムファイルのセットの要求内にある第２のオペレーティングシステムファイルのセットを応答することと、を含む。

【０００７】

データをバックアップする方法は、データストレージデバイスのホストコントローラにより、データストレージデバイス内の１つ以上のデータファイルを識別する脅威イベントのインディケーションを受信することと、ドライバにより、脅威イベントを遅延させることと、ドライバにより、脅威イベントを許可する前に、データストレージデバイス内の１つ以上のデータファイルをバックアップすることと、を含む。

【０００８】

コンピューティングネットワークにおいて相互接続されたセキュリティを提供する方法は、コンピューティングネットワークにより、複数のコンピューティングデバイスを接続することと、複数のコンピューティングデバイスのそれぞれにより、複数のコンピューティングデバイス内の、他のコンピューティングデバイスのそれぞれとの間に、代替のセキュアな通信チャネルを確立することと、複数のコンピューティングデバイスの１つにより、脅威イベントを検出することと、複数のコンピューティングデバイスの１つにより、検出された脅威イベントの通知を、複数のコンピューティングデバイス内の他のコンピューティングデバイスのそれぞれに送信することと、を含む。

【０００９】
異常なシステムアクティビティを検出する方法は、データストレージデバイスのホストコントローラにより、コンピューティングシステムのユーザによって実行される複数のアクションを経時的にログに記録することと、ホストコントローラにより、ログに記録された複数のアクションに基づいて、複数の使用アクションを含むユーザのユーザフィンガープリントを判定することと、ホストコントローラにより、ユーザフィンガープリントに含まれない実行されたアクションに基づいて、異常なシステムアクティビティを検出することと、を含む。
【００１０】
データアクセスを制御する方法は、ハードウェアデバイスにより、データストレージデバイスのホストコントローラとの第１の通信チャネルと、別のデバイスとの第２の通信チャネルとを確立することと、ハードウェアデバイスにより、第１及び第２の通信チャネルを使用して、データストレージデバイスから別のデバイスに送信されるデータを制御することと、を含む。
【００１１】
データアクセスを制御する方法は、データストレージデバイスのホストコントローラにより、１つ以上の確立された規則の遵守を検出することと、ホストコントローラにより、検出された遵守に基づいて、データストレージデバイス内のデータへのアクセスを制御することと、を含む。
【００１２】
データの使用を監視する方法は、データストレージデバイスのファイルシステムレベルで、データストレージデバイスからホストデバイスに転送されたデータ量を検出することを含む。
【００１３】
データ保護をトリガする方法は、ストレージプラットホームコントローラとインタフェース接続された入力回路により、所定のコマンドの有無を検出することと、ストレージプラットホームコントローラにより、検出の結果として所定のアクションを実行することと、を含む。
【００１４】
データストレージアクセスを追跡する方法は、データストレージデバイスのホストコントローラにより、データストレージデバイスの１つ以上のセクタへのアクセスを追跡することを含む。
【００１５】
使用されないフラッシュメモリをクリアする方法は、フラッシュメモリ・ストレージデバイスにおいて、複数のデータ記憶ブロック内の１つ以上のインアクティブなブロックを検出することと、１つ以上のインアクティブなブロックにおいてデータ除去のための１つ以上のアクションを実行することと、を含む。
【００１６】
使用されないフラッシュメモリをクリアする方法は、フラッシュメモリ・ストレージデバイスにおいて、ウェアレベリング・プロセスを実行することと、新たなデータが１つ以上のブロックに転送されることなく、古いデータが１つ以上のブロックから転送されるウェアレベリング・プロセスに含まれる、１つ以上のブロックのデータ除去のための１つ以上のアクションを実行することと、を含む。
【００１７】
データアクセスを制御する方法は、データストレージデバイスのファイルシステム又はセクタ／ブロックレベルにおいて、１つ以上のデータファイルへのアクセスのための２要素認証を必要とすることを含み、この２要素認証は、事前設定された基準に基づく期間内に要求される。
【００１８】
拡張現実（augmented reality）を用いた認証方法は、場所、位置、及びオブジェクト

データを用いて、その場所又は位置におけるユーザの存在をユーザによりキャプチャされた画像データをチェックすること、及び指定されたオブジェクトを見ることにより、ユーザを認証することを含み、ある場合には、拡張現実表示において、追加の認証情報がオブジェクトに、又はオブジェクトの上に表示されてもよい。

【００１９】

タイピングヒューリスティックによるユーザ認証の方法は、タイピングキーストロークから判定されるタイピングパターンに基づいて、ユーザのキーを生成することを含み、ここでは、ユーザがタイピングしたときに新たなキーが生成され、登録されたキーに対する新たなキーの比較がユーザの認証に使用される。

【図面の簡単な説明】

【００２０】

本開示の範囲は、以下の例示的な実施形態の詳細な説明を添付の図面と併せて読むことによって最も良く理解される。図面には、以下の図面が含まれる。

【図１】図１は、例示的な実施形態に係る、データストレージデバイスのホストコントローラを含む実装によりデータアクセス及び使用を監視及び制御するように構成されたコンピューティングデバイスのハイレベルアーキテクチャを示すブロック図である。

【図２】図２は、例示的な実施形態に係る、データストレージデバイスに送受信されるデータパケットを観察及び制御するために、図１のコンピューティングデバイスにおいて使用可能なハードウェアデバイスを示すブロック図である。

【図３】図３は、例示的な実施形態に係る、図１のコンピューティングシステムのデータストレージデバイスのメインコントローラにより実施されるプロセスを示すフロー図である。

【図４】図４は、例示的な実施形態に係る、図３に示されるプロセスの一部としてのコマンドパケットの解析のプロセスを示すフロー図である。

【図５】図５は、例示的な実施形態に係る、図３に示されるプロセスの一部としてのベンダコマンドの処理のプロセスを示すフロー図である。

【図６】図６は、例示的な実施形態に係る、図３に示されるメインコントローラプロセスの一部としてのコマンドの処理のプロセスを示すフロー図である。

【図７】図７は、例示的な実施形態に係る、図３に示されるメインコントローラプロセスにおけるアイドルプロセスを示すフロー図である。

【図８】図８は、例示的な実施形態に係る、図６に示されるプロセスにおけるコマンドの実施を示すフロー図である。

【図９】図９は、例示的な実施形態に係る、コンピュータシステムアーキテクチャを示すブロック図である。

【００２１】

本開示の更なる適用範囲は、以下に提供される詳細な説明から明らかになるのであろう。例示的な実施形態の詳細な説明は、例示の目的のみを意図しており、したがって、必ずしも本開示の範囲を限定することを意図していないことを理解されたい。

【発明を実施するための形態】

【００２２】

＜コンピューティングシステムにおけるデータアクセスの監視及び制御＞

図１は、コンピューティングシステム１００の一実施形態を示す。図１に示されるコンピューティングシステム１００の実施形態は、例示としてのみ提供され、本明細書で説明される機能の実行に適したコンピューティングシステム１００の取り得るすべての構成を網羅するものではないことは、当業者には明らかであろう。例えば、図９に示され、以下で詳細に説明されるコンピュータシステム９００は、コンピューティングシステム１００の適切な一構成とされ得る。

【００２３】

コンピューティングシステム１００は、複数のモジュール、エンジン、デバイス、メモリ、及び、データストレージデバイス１０６へのアクセスの監視及びそこに記憶されたデ

ータの使用を含む、本明細書で説明されるような機能の実行のために特別に構成された他のコンポーネントから構成されてもよい。データストレージデバイス１０６は、ハードディスクドライブ、ソリッドステートドライブ、コンパクトディスク、デジタルビデオディスク、磁気テープなどを含む、データの記憶に適した任意のタイプのデバイスであってもよい。データストレージデバイス１０６は、ホストコントローラ１０８を含んでもよい。ホストコントローラ１０８は、データストレージデバイス１０６内のデータを読み出し及び書き込みするように構成された、データストレージデバイス１０６内のハードウェア、ソフトウェア、又はそれらの組み合わせで実現されるアプリケーションプログラムであってもよい。ホストコントローラは、データストレージデバイス１０６内の１つ以上のデータファイル、セクタ、又はブロックへのアクセスの阻止、セクタ又はブロックの変更からのロックなどを含む、データストレージデバイス１０６に記憶されたデータのアクセス及び変更に関連付けられた任意の機能を実行するように構成されてもよい。本明細書で説明されるように、データストレージデバイス１０６に記憶されたデータに関してコンピューティングシステム１００で実行されるアクションは、ホストコントローラ１０８により、又はホストコントローラ１０８と連携して、実行されてもよい。例えば、図３～図８に示されるプロセスは、ホストコントローラ１０８又はその中にインストールされたアプリケーションプログラム（例えば、ドライバ）により、別のハードウェアデバイス（例えば、以下で詳細に説明される中継装置１１８）により、或いはそれらの組み合わせにより、実行されてもよい。ある場合には、データストレージデバイス１０６は、ホストコントローラ１０８によって使用されるメモリを含み、ホストコントローラ１０８の機能及びコマンドを実行する際に使用されるデータを記憶してもよく、このようなメモリは、コンピューティングシステム１００のモジュール及びエンジンによって使用されるデータストレージデバイス１０６のデータストレージとは別であってもよい。

【００２４】

ホストコントローラ１０８は、コンピューティングシステム１００のデータストレージレベルで動作するように構成されてもよい。換言すれば、コンピューティングシステム１００は、オペレーティングシステム（ＯＳ）アプリケーション１２０を含むことができ、これはコンピューティングシステム１００の処理装置により実行され、コンピューティングシステム１００のユーザ、及びソフトウェアアプリケーションプログラムが実行され得るプラットホームへのインタフェースを提供することができ、ここで、ホストコントローラ１０８は、ＯＳアプリケーション１２０とは別個に動作することができる。例えば、ＯＳアプリケーションは、以下で詳細に説明される通信モジュール１０４を介して、そのホストコントローラ１０８と通信することにより（例えば、情報をやり取りすることにより）、データストレージデバイス１０６にアクセスすることができる。例えば、ＯＳアプリケーション１２０は、プログラムコードとしてデータストレージデバイス１０６に記憶され、独自のファイル、或いはホストコントローラ１０８からの対応するデータの要求によりＯＳ上で実行されるアプリケーションプログラムによって使用されるファイルにアクセスすることができる。

【００２５】

ある実施形態では、コンピューティングシステム１００は、データストレージデバイス１０６に加えてメモリ１１０を含んでもよい。メモリ１１０は、ＯＳアプリケーション１２０の実行及び使用においてコンピューティングシステム１００によって使用され得る、リードオンリーメモリ、ランダムアクセスメモリ、又は他のタイプのメモリである、別のデータストレージデバイスであってもよい。ある場合には、ホストコントローラ１０８は、メモリ１１０のホストコントローラとしても動作するように構成されてもよく、或いはメモリ１１０に記憶されたデータへのアクセス及びその使用を監視するように構成されてもよい。メモリ１１０は、本明細書で説明される機能を実行する際にコンピューティングシステム１００によって使用されるデータを記憶するように構成されてもよい。メモリ１１０は、データストレージデバイス１０６と同様に、適切なデータフォーマット方法及びスキーマを使用してデータを記憶するように構成されてもよく、任意の適切なタイプのメ

モリであってもよい。メモリ１１０は、例えば、暗号化キー及びアルゴリズム、通信プロトコル及び規格、データフォーマット規格及びプロトコル、処理装置のモジュール及びアプリケーションプログラムのプログラムコード、並びに、当業者には明らかなように本明細書で開示される機能の実施においてコンピューティングシステム１００によって使用されるのに適した他のデータを含むことができる。ある実施形態では、メモリ１１０は、そこに記憶された構造化データセットの記憶、特定、変更、更新、アクセスなどのために構造化クエリ言語を使用するリレーショナルデータベースで構成されてもよく、或いはそれを含んでいてもよい。

【００２６】

ある実施形態では、コンピューティングシステム１００は、フラッシュメモリ１１２を含んでもよい。フラッシュメモリ１１２は、データストレージデバイス１０６とは別のソリッドステートメモリデバイス（例えば、該当する場合は、メモリ１１０）であってもよく、ある場合には、コンピューティングシステム１００から取り外し可能であってもよい。フラッシュメモリ１１２は、その中のデータの記憶を実施するために可動機械部品を使用せずに動作することができるので、フラッシュメモリ１１２は、そのデータの記憶及びアクセスのためにホストコントローラ１０８によって実行される、異なるアクション及び／又は変更されたアクションの対象とされてもよい。ある実施形態では、データストレージデバイス１０６のホストコントローラ１０８は、フラッシュメモリ１１２のホストコントローラ１０８として動作してもよい。他の実施形態では、フラッシュメモリ１１２は、別のホストコントローラ１０８を有してもよい。本明細書で説明されるように、ホストコントローラ１０８によって実行される機能はいずれも、コンピューティングシステム１００のそれぞれのメモリ及びデータストレージデバイスのホストコントローラによって実行されてもよい。

【００２７】

コンピューティングシステム１００は、受信装置１０２を含んでもよい。受信装置１０２は、１つ以上のネットワークプロトコルを介して、１つ以上のネットワークでデータを受信するように構成されてもよい。ある実施例では、受信装置１０２は、無線周波数、ローカルエリアネットワーク、ワイヤレスエリアネットワーク、セルラ通信ネットワーク、ブルートゥース、インターネットなどの１つ以上の通信方法を介して、コンピューティングシステム１００のローカルネットワーク上に配置され、或いは、コンピューティングシステムの外部に配置される、他のコンピューティングシステムからデータを受信するように構成されてもよい。ある実施形態では、受信装置１０２は、例えばローカルエリアネットワークを介してデータを受信する第１の受信装置及びインターネットを介してデータを受信する第２の受信装置などの、異なるネットワークを介してデータを受信する異なる受信装置など、複数のデバイスから構成されてもよい。受信装置１０２は、電子的に送信されたデータ信号を受信することができ、データは、データ信号において重畳され、或いは符号化され、受信装置１０２によるデータ信号の受信を介して復号化され、解析され、読み出され、或いは取得されてもよい。ある実施例では、受信装置１０２は、受信されたデータ信号を解析して、その上に重畳されたデータを取得するための、解析モジュールを含んでもよい。例えば、受信装置１０２は、データ信号を受信し、受信されたデータ信号を本明細書で説明される方法及びシステムを実行するために処理装置によって実行される機能で使用可能な入力に変換するように構成された解析プログラムを含んでもよい。

【００２８】

コンピューティングシステム１００は、送信装置１２４を含んでもよい。送信装置１２４は、１つ以上のネットワークプロトコルを介して、１つ以上のネットワークでデータを送信するように構成されてもよい。ある実施例では、送信装置１２４は、無線周波数、ローカルエリアネットワーク、ワイヤレスエリアネットワーク、セルラ通信ネットワーク、ブルートゥース、インターネットなどの１つ以上の通信方法を介して、コンピューティングシステム１００のローカルネットワーク上に配置され、或いは、コンピューティングシステムの外部に配置される、コンピューティングシステムにデータを送信するように構成

されてもよい。ある実施形態では、送信装置１２４は、例えばローカルエリアネットワークを介してデータを送信する第１の送信装置及びインターネットを介してデータを送信する第２の送信装置などの、異なるネットワークを介してデータを送信する異なる送信装置など、複数のデバイスから構成されてもよい。送信装置１２４は、受信側コンピューティングデバイスによって解析され得るデータが重畳されたデータ信号を電子的に送信することができる。ある実施例では、送信装置１２４は、データを送信に適したデータ信号に重畳し、符号化し、或いはフォーマットする１つ以上のモジュールを含んでもよい。

【００２９】

コンピューティングシステム１００は、通信モジュール１０４を含んでもよい。通信モジュール１０４は、本明細書で説明される機能を実行する際に使用され、モジュール、エンジン、データベース、メモリ、及びコンピューティングシステム１００の他のコンポーネント（例えば、コンピューティングシステム１００の「デバイス」又は「ホストデバイス」とも称される）の間でデータを送信するように構成されてもよい。通信モジュール１０４は、１つ以上の通信タイプで構成され、コンピューティングデバイス内の通信のための様々な通信方法を使用することができる。例えば、通信モジュール１０４は、バス、コンタクトピンコネクタ、ワイヤなどで構成されてもよい。ある実施形態では、通信モジュール１０４は、コンピューティングシステム１００の内部コンポーネントと、外部接続データベース、表示装置、入力装置などのコンピューティングシステム１００の外部コンポーネントとの間で通信するように構成されてもよい。コンピューティングシステム１００は、処理装置を含んでもよい。処理装置は、当業者には明らかなように、本明細書で説明されるコンピューティングシステム１００の機能を実行するように構成されてもよい。ある実施形態では、処理装置は、処理装置の１つ以上の機能を実行するように特別に構成された複数のエンジン及び／又はモジュールを含み、且つ／又はそれらで構成されてもよい。本明細書で使用されるように、「モジュール」という用語は、特に、入力を受信し、入力を使用して１つ以上のプロセスを実行し、出力を提供するようにプログラムされた、ソフトウェア又はハードウェアであってもよい。様々なモジュールによって実行される入力、出力、及びプロセスは、本開示に基づいて当業者には明らかであろう。

【００３０】

上述のように、コンピューティングシステム１００は、ＯＳアプリケーション１２０を含んでもよい。ＯＳアプリケーション１２０は、ＯＳアプリケーション１２０をプラットホームとして使用して実行されるアプリケーションプログラムと、データストレージデバイス１０６及びコンピューティングシステムの他のメモリとの間の連絡機構として動作するシステムソフトウェアであってもよい。ある実施形態では、コンピューティングシステム１００は、その中に記憶された複数のＯＳアプリケーション１２０を有してもよく、それらはそれぞれ、データストレージデバイス１０６及び／又はコンピューティングシステム１００の他のメモリに記憶されてもよい。このような実施形態では、単一のＯＳアプリケーション１２０がコンピューティングシステム１００の実行時に実行されてもよく、それはコンピューティングシステム１００のベーシックインプット／アウトプットシステム（ＢＩＯＳ）によって選択されてもよい。以下で詳細に説明されるように、ホストコントローラ１０８は、コンピューティングシステム１００で動作するＯＳアプリケーション１２０の選択を変更し、或いはデータ記憶操作を通じて、選択されたＯＳアプリケーション１０２を変更して、コンピューティングシステム１００への攻撃を防ぐように、或いは効率的な動作を保証するように構成されてもよい。

【００３１】

コンピューティングシステム１００は、ファイルシステムコントローラ１２２を含んでもよい。ファイルシステムコントローラ１２２は、ＯＳアプリケーション１２０の一部であってもよく、コンピューティングシステム１０２のユーザ又はＯＳアプリケーション１０２のアプリケーションプログラムがデータストレージデバイス１０６のファイルシステム又はコンピューティングシステム１０２の他のメモリ１１０にアクセスするためのインタフェースを（例えばアプリケーションプログラミングインタフェースとして）提供する

ように構成してもよい。ある場合には、ファイルシステムコントローラ１２２は、（例えば通信モジュール１０４を介して）それぞれのデータストレージデバイス１０６のホストコントローラ１０８と通信して、そこに記憶されたデータの取得又は変更をしてもよい。例えば、ＯＳアプリケーション１０２を使用して動作するアプリケーションプログラムは、データストレージデバイス１０６に記憶されたデータへのアクセスのために、ファイルシステムコントローラ１２２と相互に作用することができ、ここで、ファイルシステムコントローラ１２２は、読み出し又は書き込みを行うデータに関する命令をホストコントローラ１０８に提供することができ、ホストコントローラ１０８は、データストレージデバイス１０６内の必要な機能を実行して、要求された動作を実行することができる。

【００３２】

ある実施形態では、コンピューティングシステム１００は、中継装置１１８（interposition device）を含んでもよい。中継装置１１８は、データストレージデバイス１０６及びコンピューティングシステム１００の他のハードウェアコンポーネントとは別のハードウェアデバイスであってもよく、通信モジュール１０４を使用してコンピューティングシステム１００を通過するような、データストレージデバイス１０６に送受信されるデータパケットを監視するように構成されてもよい。中継装置１１８の実装については、図２のハードウェアデバイス２００に関して以下で詳細に説明する。ある実施形態では、中継装置１１８は、データストレージデバイス１０６のホストコントローラ１０８に実装されてもよい。他の実施形態では、中継装置１１８は、ホストコントローラ１０８と直接的に通信して、データストレージデバイス１０６に送受信されるデータパケットを監視してもよい。

【００３３】

コンピューティングシステム１００は、１つ以上の入力装置を含んでもよく、或いはそれとインタフェース接続されてもよい。入力装置は、コンピューティングシステム１００の内部にあってもよく、コンピューティングシステム１００の外部にあってもよく、データの送受信のために１つ以上の接続（例えば、有線又は無線）を介して接続されてもよい。入力装置は、コンピューティングシステム１００のユーザからの入力を受け付けるように構成されてもよく、それは、後続処理のために、コンピューティングシステム１００の別のモジュール又はエンジンに（例えば通信モジュール２０４を介して）提供されてもよい。入力装置は、キーボード、マウス、クリックホイール、スクロールホイール、マイクロフォン、タッチスクリーン、トラックパッド、カメラ、光学撮像素子など、本明細書で説明される機能を実行するための入力を受け付けるのに適した、任意のタイプの入力装置を含んでもよい。入力装置は、例えば、キーストローク情報、物理的環境の光学画像、及び本明細書で説明されるような用途の、他のデータを受信するように構成されてもよい。

【００３４】

コンピューティングシステム１００は、表示装置を含んでもよく、或いは表示装置とインタフェース接続されてもよい。表示装置は、コンピューティングシステム１００の内部にあってもよく、コンピューティングシステム１００の外部にあってもよく、データの送受信のために１つ以上の接続（例えば、有線又は無線）を介して接続されてもよい。表示装置は、コンピューティングシステム１００のユーザに対してデータを表示するように構成されてもよい。表示装置は、液晶ディスプレイ、発光ダイオードディスプレイ、薄膜トランジスタディスプレイ、静電容量式タッチディスプレイ、陰極線管ディスプレイ、光投影ディスプレイなど、本明細書で説明される機能の一部としてデータを表示するのに適した任意のタイプの表示装置であってもよい。ある実施例では、コンピューティングシステム１００は、複数の表示装置を含んでもよい。表示装置は、例えば、認証情報、物理領域の拡張現実表示、ＯＳアプリケーション１２０の一部としてのファイルシステムなどを表示するように構成されてもよい。

【００３５】

＜中継装置＞

図２は、コンピューティングシステム１００において中継装置１１８として動作可能な

ハードウェアデバイス２００を示す。図２に示されるハードウェアデバイス２００の実施形態は、例示としてのみ提供され、本明細書で説明される機能の実行に適したハードウェアデバイス２００の取り得るすべての構成を網羅するものではないことは、当業者には明らかであろう。

【００３６】

ハードウェアデバイス２００は、マイクロコントローラ２０２を含んでもよい。マイクロコントローラ２０２は、本明細書で説明される中継装置１１８の機能を実行するように構成された集積回路であってもよく、例えば、コンピューティングシステム１００内のデータストレージデバイス１０６に送受信されるデータパケットを監視するように構成された、プログラムされた処理装置（programmed processing device）であってもよい。ハードウェアデバイス２００は、シリアルアドバンストテクノロジアタッチメント（シリアルＡＴアタッチメント、ＳＡＴＡ）ドライブ２１０を含んでもよく、ハードウェアデバイス２００に関連付けられた機能を実行する際にハードウェアデバイス２００により使用されるデータを記憶するように構成されてもよい。例えば、ＳＡＴＡドライブ２１０は、データパケットの移動の監視などの、マイクロコントローラ２０２により実行されるプログラムコードを記憶するように構成されてもよい。また、ＳＡＴＡドライブ２１０は、例えば、コンピューティングシステム１００のユーザによるレビュのためのデータログ、データ送信に関連付けられた警告を送信するための規則、コンピューティングシステム１００における潜在的な攻撃を識別するためのアルゴリズム等、データパケット監視に関する情報を記憶するように構成されてもよい。

【００３７】

ハードウェアデバイス２００は、ＳＡＴＡを用いて、ホスト２０８とインタフェース接続するように構成されてもよい。ＳＡＴＡホスト２０８は、例えば、通信モジュール１０４又はデータストレージデバイス１０６であってもよく、ハードウェアデバイス２００は、ＳＡＴＡホスト２０８又はそこから受信されたデータを介して、データストレージデバイス１０６へのデータパケットの送受信を監視してもよい。ハードウェアデバイス２００は、例えばマイクロコントローラ２０２によって指示されることで実行されるハードウェアデバイス２００の機能に応じて、ＳＡＴＡドライブ２１０とＳＡＴＡホスト２０８との間を切り替えるように構成される、ポートセレクタ２０６を含んでもよい。

【００３８】

ある実施形態では、マイクロコントローラ２０２は、パラレルＡＴアタッチメント（ＰＡＴＡ）を介して通信するように構成されてもよい。このような実施形態では、ハードウェアデバイス２００は、ＰＡＴＡ／ＳＡＴＡブリッジ２０４を含むことができ、ＰＡＴＡを使用してマイクロコントローラ２０２とインタフェース接続し、ＳＡＴＡを使用してポートセレクタとインタフェース接続し、マイクロコントローラ２０２とＳＡＴＡドライブ２１０とＳＡＴＡホスト２０８との間で交換される通信を可能にするように構成されてもよい。ハードウェアデバイス２００は、ＳＡＴＡドライブ２１０に、その動作のために電力を供給するように構成されたコンポーネントである、駆動電源２１２を含んでもよい。駆動電源２１２は、マイクロコントローラ２０２に接続され、そこから動作の命令を受信してもよく、それにより、ＳＡＴＡドライブ２１０に動作（停止）させてもよい。ある実施形態では、ハードウェアデバイス２００は、ハードウェアデバイス２００のコンポーネント、コンピューティングシステム１００のコンポーネント、ハードウェアデバイス２００とコンピューティングシステム１００とのインタフェース接続、ハードウェアデバイス２００の実施形態のタイプなど、ハードウェアデバイス２００における必要性に応じて、ハードウェアデバイス２００内の電圧の安定化のために、＋３．３電圧レギュレータ及び／又は＋１．８電圧レギュレータ２１６を含んでもよい。

【００３９】

上述のように、ハードウェアデバイス２００は、コマンドパケット及びデータパケットを、データストレージデバイス１０６及びコンピューティングシステム１００の他のメモリ１１０に送受信されるときに検査し、中継するように構成された、コンピューティング

システム１００の中継装置１１８として動作してもよい。ハードウェアデバイス２００は、データストレージデバイス１０６宛てのすべてのインバウンド及びアウトバウンドのデータストレージを観察、制御、及びルーティングするように構成されてもよい。このような動作は、本明細書で説明されるコンピューティングシステム１００に関連付けられた機能の実施のための他の動作と併せて実施されてもよい。例えば、ホストコントローラ１０８は、以下に説明されるように、データアクセスに関連付けられたユーザアクションのルーチンに基づいて、データストレージデバイス１０６に記憶されたデータの潜在的な攻撃又は他の悪用を監視するように構成されてもよく、データストレージデバイス１０６のハードウェアデバイスのインバウンド及びアウトバウンドの通信の観察を使用して、データアクセスが識別されてもよい。

【００４０】

＜ホストコントローラ及び中継装置の例示的な機能＞

上述のように、コンピューティングシステム１００のホストコントローラ１０８及び中継装置１１８は、データストレージデバイス１０６に記憶されたデータへのアクセス及び使用を監視して、データの悪用、データに対する攻撃の試みを阻止し、データのバックアップを容易にするように、或いはコンピューティングシステム１００に記憶されたデータを保護するように構成されてもよい。

【００４１】

一実施形態では、ホストコントローラ１０８は、データストレージデバイス１０６からファイルシステムコントローラ１２２などのデバイス要求側に流れるデータであって、コンピューティングシステム１０２のユーザにより、表示、又は他の方法での使用を要求されたデータを制御するように構成されてもよい。このような実施形態では、ホストコントローラ１０８は、ファイルシステムコントローラ１２２によって送信されるリクエストを理解し、ファイルシステムコントローラ１２２に提供されるデータを変更して、これにより、データストレージデバイス１０６に記憶された基礎となるデータに変更を加えることなく、ホストコントローラ１０８によってデータのユーザのビューが変更されるように構成されてもよい。例えば、コンピューティングシステム１００のユーザは、認証プロセス（例えばＯＳアプリケーション１２０を使用したログイン）を実施してもよく、コンピューティングシステム１００のそれぞれのユーザは、そのユーザが閲覧又は他の方法でアクセス可能なデータに関して、ユーザに関連付けられたパーミッションのレベルを有してもよい。ホストコントローラ１０８は、このパーミッションのレベルに基づいて、ユーザが許可されているデータのみを見ることができるように、データストレージデバイス１０６に記憶されたデータに関してファイルシステムコントローラ１２２に提供される情報を変更してもよい。ユーザが閲覧を許可されていないデータは、ホストコントローラ１０８による変更なしにデータストレージデバイス１０６に記憶され続けてもよいが、ファイルシステムコントローラ１２２は、それに関連付けられた情報をユーザに提示しない。例えば、データは、ユーザの観点からは存在しないが、データストレージデバイス１０６に安全に記憶されている。したがって、このような例では、データストレージデバイス１０６は、権限を有する者による場合を除いて、データの削除又は誤用から保護することができる。

【００４２】

ホストコントローラ１０８は、コンピューティングシステム１００の起動に使用されるＯＳアプリケーション１２０を自動的に選択するように構成されてもよい。例えば、コンピューティングシステム１００が（例えばホストコントローラ１０８、中継装置１１８、又は他のコンポーネントを介して）、ＯＳアプリケーション１２０の動作の不良又はＯＳアプリケーション１２０の侵害などの、デフォルトのＯＳアプリケーション１２０に関する潜在的な問題を検出した場合、ホストコントローラ１０８は、コンピューティングシステム１００で使用される、リカバリＯＳアプリケーション１２０を自動的に選択するように構成されてもよい。ある場合では、リカバリＯＳアプリケーション１２０は、基礎となるデータストレージデバイスの動作を介して選択されてもよい。例えば、ホストコントローラ１０８は、デフォルトのＯＳアプリケーション１２０を記憶するために使用されるデ

ータセクタ及び／又はブロックを、リカバリＯＳアプリケーション１２０を記憶するものと切り替えて、コンピューティングシステム１００が、通常動作を試みるときに、リカバリＯＳアプリケーション１２０を実行するようにしてもよい。このような実施形態では、リカバリＯＳアプリケーション１２０は、自動的に実行され、これにより、侵害されたＯＳアプリケーション１２０がコンピューティングシステム１００に有害な変更を加えることを阻止し、ユーザに侵害を取り除く機会を提供することができる。

【００４３】

ＯＳアプリケーション１２０を自動的に選択する能力は、ＯＳアプリケーション１２０のリストア又はリフレッシュを実行するために、ホストコントローラ１０８によって使用されてもよい。例えば、ホストコントローラ１０８は、データストレージデバイス１０６内の所定の位置に記憶されたＯＳアプリケーション１２０のスナップショット又は保存された状態（saved state）を有してもよい。ＯＳアプリケーション１２０に潜在的な問題（例えば、検出された攻撃、ＯＳアプリケーション１２０の動作エラー）が特定された場合、或いはコンピューティングシステム１００のユーザによって要求された場合、ホストコントローラ１０８は、（例えば、潜在的な問題の前に）保存されたＯＳアプリケーション１２０が代わりに実行されるように、ＯＳアプリケーション１２０を保存された状態に自動的に切り替えることができる。このような場合、ホストコントローラ１０８は、コンピューティングシステム１０２のアイドルサイクル中に、交換後の侵害されたＯＳアプリケーション１２０を上書きして、侵害を取り除き、コンピューティングシステム１００を更に保護することもできる。このような実装では、ＯＳアプリケーション１２０は、ユーザの知識又は行動なしに復元されてもよい。ある実施形態では、リストアは、変更のログを使用して実行されてもよい。例えば、ホストコントローラ１０８は、データストレージデバイス１０６に関して実行されたすべての動作のログを維持することができ、復元動作は、データストレージデバイス１０６（及びその中に記憶されたＯＳアプリケーション１２０）を以前の状態に戻すために、データストレージデバイス１０６に記憶されたデータを変更、移動、又は置換するなど、（例えば事前定義された復元ポイントに戻るように）所定の期間におけるすべての動作を逆行させることを含んでもよい。

【００４４】

ある実施形態では、ホストコントローラ１０８は、データストレージデバイス１０６に記憶されたデータを自動的にバックアップするように構成されてもよい。そのような実施形態では、ホストコントローラ１０８は、コンピューティングシステム１００内で発生した、データに脅威をもたらす可能性があるイベントを監視するように（例えば、中継装置１１８などの別のコンポーネントによって直接的又は間接的に通知されるように）構成されてもよい。例えば、未知の通信、ファイル削除又は変更の要求、データの暗号化又は復号化などは、潜在的なネガティブイベントとしてホストコントローラ１０８によって識別され得る。このようなイベントが検出されると、イベントは、ホストコントローラ１０８がデータをバックアップしている間に、一時停止されてもよく、或いは遅延させられてもよい。ある場合には、バックアップされるデータは、予め判定されてもよい。例えば、（例えば、ＯＳアプリケーション１２０に不可欠なもの、ユーザによって選択されたものなど）試みられているアクションに関係なくバックアップされるデータが存在してもよい。他の場合では、バックアップされるデータは、イベントにより影響を受けるデータであってもよい。例えば、イベントが特定のデータブロックの削除である場合、これらのデータブロックがバックアップされてもよい。ホストコントローラ１０８は、データストレージデバイス１０６内の所定の位置にデータをバックアップしてもよく、バックアップが完了するとイベントを発生させてもよい。このような実施形態では、コンピューティングシステム１００に記憶されたデータは、起こり得る潜在的なイベントに関わらず、保護されたままとされてもよい。ある場合には、バックアップされるデータが、イベント又はそれによって影響され得るデータの種類に基づいて異なるように、或いは実行されるアクションがイベントの種類に基づいて異なるようになど、複数のポリシーが実装されてもよい。

【００４５】

ある実施形態では、コンピューティングシステム１００は、他のコンピューティングシステムのネットワークの一部であってもよい。このような実施形態では、潜在的な脅威イベント又はネガティブイベントは、ネットワーク内の他のコンピューティングシステムによって検出されてもよい。このような場合には、ホストコントローラ１０８は、（例えば、ホストコントローラ１０８又は他のコンピューティングシステム内の中継装置１１８などにより、本明細書で説明される機能を使用して検出される）これらの潜在的な脅威イベントに関する情報を他のコンピューティングシステムから受信してもよく、それに基づいて本明細書で説明されるアクションを実行してもよい。ある実施例では、ホストコントローラ１０８又はコンピューティングシステム１００の他のハードウェアコンポーネントは、ネットワーク内の他のコンピューティングシステムの対応するコンポーネントとの代替のセキュアな通信チャネルを確立してもよい。このようなチャネルは、ネットワークで発生し、ネットワークを侵害する可能性がある脅威イベントが代替のセキュアなチャネルにアクセスできないように、或いは影響を与えることができないように、ネットワークの通信チャネルとは別であってもよい。ある場合には、セキュアチャネルは、そのチャネルを使用する通信をセキュアにする技術（例えば、暗号化）を使用して、そのネットワーク自体の上で動作してもよい。他の場合では、別のプロトコル及び／又は通信パスが使用されてもよい。ある場合には、他のコンピューティングシステムは、他のコンピューティングシステム１００であってもよく、或いは、動き検出器、近接ドアセンサ、バイオメトリックスキャナ、セットトップボックス、ビデオゲームシステム、ウェアラブルコンピューティングデバイスなど、コンピューティングシステム１００とのセキュアな通信チャネルを確立し、脅威イベントを検出することができる任意のタイプのコンピューティングデバイスであってもよい。

【００４６】

ある実施形態では、ホストコントローラ１０８は、データストレージデバイス１０６へのアクセスに関して、ユーザ又はコンピューティングシステム１００の他の動作に関連付けられた過去の使用データのセットを作成するように構成されてもよい。過去の使用データは、データストレージデバイス１０６のデータのアクセス、取得、変更、又は書き込みなど、データストレージデバイス１０６に関連して実行されるアクションのログであってもよい。ログは、数秒のスパン、データストレージデバイス１０６の全寿命、又はそれらの間の任意の長さの時間をカバーしてもよい。ログは、データの読み出し、データの書き込み、データの上書き、データの変更などを含む、データストレージデバイス１０６に関連付けられた任意のアクションをカバーしてもよく、影響を受けるセクタ及び／又はブロックを指定し、そして、それらがどのように影響を受けるかを指定してもよい。ログを使用して、ホストコントローラ１０８は、コンピューティングシステム１００の典型的な使用特性の「フィンガープリント」又は「スナップショット」を構築してもよく、ある場合には、コンピューティングシステム１００のユーザに直接関連付けられてもよい（例えば、それぞれのユーザは個人的なアクションに基づいて独自のフィンガープリントを持つことができる）。このようなスナップショットは、それぞれのユーザ又はコンピューティングシステム１００全体の署名を判定するために、そして、データストレージデバイス１０６を使用するときに、どのようなアクションが標準的又は「通常」と見なされるかを判定するために、考慮されてもよい。ユーザの署名に基づいて標準と考えられるものから外れているイベントが試みられるとき、そのイベントは脅威イベントであると判定されてもよい。それから、ホストコントローラ１０８は、脅威イベントが検出されたときに、（例えば、データの自動的なバックアップ、代替のセキュアなチャネルを使用した他のコンピューティングデバイスの通知、データの暗号化、ファイルシステムデータの変更など）任意の好適なアクションを実行してもよい。ある実施形態では、ホストコントローラ１０８には、既知のウイルス、ランサムウェア、又は他の望ましくないエージェントのための署名が提供されてもよく、署名は、ネガティブなアクションが実行される前に、このようなエージェントの存在を検出するために使用されてもよい。

【００４７】

ある実施形態では、ホストコントローラ１０８は、確立された規則への遵守（compliance）に基づいて、データストレージデバイス１０６へのアクセスを制御するように構成されてもよい。ある実施例では、規則は、追加のハードウェアコンポーネントの使用、又はコンピューティングシステム１００に依存する他の局面を含んでもよい。例えば、規則は、コンピューティングシステム１００が（例えば、全地球測位システムに基づく）特定の地理的領域に位置することを要求してもよく、それは、ホストコントローラ１０８、コンピューティングシステム１００の標準コンポーネント、コンピューティングシステム１００の一部であるが、コンピューティングシステム１００の他のコンポーネントとは独立して動作する別のハードウェアコンポーネント、或いはＯＳアプリケーション１２０によるアクセスが不可能である別のハードウェアコンポーネントによって識別されてもよい。他の実施例では、ホストコントローラ１０８は、データストレージデバイス１０６へのアクセスのためにセキュリティドングルの存在を要求してもよく、また、（例えば、ファイルシステムコントローラ１２２により提示されるデータのビューを変更することに関して上述されたように）セキュリティドングルから受信したクレデンシャルに基づいて、データの閲覧又は使用を阻止してもよい。他の実施例では、規則は、コンピューティングシステム１００と別のデバイスとの間の物理的な接続を要求してもよい。ある場合には、確立された規則に従わないことで、ホストコントローラ１０８により脅威イベントとして識別されてもよく、それに応じて必要なアクションが実行されてもよい。

【００４８】

ある実施形態では、ホストコントローラ１０８は、データストレージデバイス１０６から転送された（例えば、読み出された）データ量を監視するように構成されてもよい。ホストコントローラ１０８は、データストレージデバイス１０６から読み出されたデータ量を追跡し続け、データ量に基づいてアクションを実行してもよい。例えば、読み出されるデータの量の限界が設定されてもよく、限界に達すると、データへのアクセスが阻止又は制限されてもよく、或いは、限界に達したことが脅威イベントとして見なされてもよい。データストレージデバイス１０６から読み出されたデータ量は、ユーザのフィンガープリント又は署名の一部と見なされてもよい。ある場合には、データの量は、時間ごと、日ごと、週ごと、月ごとなどの期間にどれだけのデータがアクセスされるかを測定するなど、期間に関連付けて監視されてもよい。ある実施形態ではホストコントローラ１０８は、データストレージデバイス１０６の特定のセクタ及び／又はブロックから転送されるデータ量を監視してもよく、限界又は規則は、セクタ及び／又はブロックに応じて異なってもよい。例えば、ＯＳアプリケーション１２０のプログラムコード又はバックアップデータを記憶するために使用されるブロックから読み出されるデータには制限がないが、他のデータを記憶するために使用されるブロックには制限が設定されてもよい。ある場合には、ホストコントローラ１０８は、ファイルシステムコントローラ１２２と通信して、アクセスされたデータの監視に使用可能な、ファイルタイプ情報など、アクセスされたデータに関する追加の情報を受信してもよい。例えば、（ビデオ、画像、音楽などの）メディアファイルについて読み出されるデータ量に制限が設定され、一方で、（ダイナミックリンクライブラリ、システムファイルなどの）オペレーティングシステムファイルについては設定されなくてもよい。

【００４９】

ある実施形態では、コンピューティングシステム１００は、データストレージデバイス１０６に記憶されたデータへのアクセスを制御する際にホストコントローラ１０８によって使用される、独立した機械的及び／又は電気的なコンポーネントを含んでもよい。独立コンポーネントは、コンピューティングシステム１００のユーザが、独立コンポーネントの使用を（例えば、該当する、追加の状態の間に）アクティブ化又はインアクティブ化するように構成可能であり、データストレージデバイス１０６内のデータへのアクセスが、独立コンポーネントの状態に基づいて、ホストコントローラ１０８により制御されてもよい。例えば、ホストコントローラ１０８とは別の任意の他のコンポーネントとインタフェース接続されていないボタンがコンピューティングシステム１００に含められてもよく、

このボタンが押されると、データストレージデバイス１０６の所定の領域へのアクセスが阻止されてもよい。ボタン、スイッチ、センサ、加速度計、バイオメトリックスキャナ、光学撮像素子、マイクロフォンなど、任意の適切なタイプの機械的及び／又は電気的コンポーネントが使用されてもよい。ある実施例では、独立コンポーネントによって検出されたアクションは、ホストコントローラ１０８によって脅威イベントと見なされてもよい。例えば、バイオメトリックスキャナは、登録されたユーザのバイオメトリクスが読み出されたときに、データストレージデバイス１０６の一部へのアクセスを制御するために使用されてもよいが、権限のないユーザがバイオメトリックスキャナを使用して認証を試みた場合に、脅威イベントが検出されてもよい。

【００５０】

ある実施形態では、ホストコントローラ１０８は、データストレージデバイス１０６がフラッシュメモリを使用するときに、追加の機能を実行するように構成されてもよい。フラッシュメモリの性質のために、データは、ウェアレベリング（wear leveling）・アルゴリズムを使用するフラッシュメモリの摩耗及び劣化のために、フラッシュメモリ内のブロック間で移動されることがある。伝統的に、摩耗したブロックは、そのブロックから別のブロックにデータを移動させるが、オリジナルのブロックは消去されず、したがって残されたデータが侵害の対象となる。ある実施形態では、ホストコントローラ１０８は、フラッシュメモリ１１２に対して実行されるウェアレベリング・プロセスの一部として、これらのオリジナルのブロックの完全消去を実行するように構成されてもよい。ホストコントローラ１０８は、ブロックの使用を監視してもよく、ブロックは、その中に記憶されたデータの状態及びフラッシュメモリ１１２内でのその使用に基づいて、アクティブ又はインアクティブとしてラベル付けされてもよい。ホストコントローラ１０８は、所定の期間に、インアクティブブロック内のデータの完全消去を実行して、その侵害を阻止し、データブロックの寿命を延ばすことができる。完全消去は、書き込みの繰り返し、データにおいてより小さな部分のアドレス指定、ブランク又は解読不可能なデータによるデータの上書き、及び古いブロック又はインアクティブなブロック内のデータを確実にクリアするために使用される他の技術を使用することによって達成されてもよい。ある実施例では、ホストコントローラ１０８は、使用するブロックのタイプ（例えば、インアクティブブロック、使い古されたブロック（worn blocks）など）又は消去プロセスのタイプを指定した、コンピューティングシステム１００のユーザによるコマンド入力に応答して、ブロックの完全消去を実行するように構成されてもよい。

【００５１】

ある実施形態では、ホストコントローラ１０８は、データストレージデバイス１０６に記憶されたデータファイルへのアクセスを制御するために２要素認証を使用するように構成されてもよい。２要素認証は、（ｉ）ユーザが何を知っているか（例：パスワード）と（ｉｉ）ユーザが何を持っているか（例：ドングル）とに依存する２つの異なるタイプの認証を要求することにより、認証ルーチンのセキュリティを高める方法である。ある場合には、ユーザは、バイオメトリックスキャナ、パスワード、第三者認証サービス、セキュリティドングル、スマートデバイスなど、いずれか又はすべてのタイプの認証を設定してもよい。ある実施例では、ユーザは、アクセスするために２要素認証が必要なデータファイルを選択してもよい。このような場合には、使用される２要素認証のタイプは、制御されるアクセスによって異なってもよい。例えば、ユーザは、データストレージデバイス１０６に記憶されたすべての画像にアクセスするために、パスワード及びセキュリティドングルから成る２要素認証を要求してもよく、特定のフォルダ内のファイルにアクセスするために、指紋スキャン及び異なるセキュリティドングルから成る２要素認証を要求してもよい。２要素認証は、特定のファイル又はフォルダ、ファイルの種類、特定の取得条件を満たすファイル又はフォルダなどに対して設定されてもよい。ある場合には、２要素認証が要求されるときの基準が、ユーザによって設定されてもよい。例えば、ユーザは、（例えば、特定の２要素認証の規則のセットについて）２要素認証が常に要求されること、２要素認証が所定の期間（例えば、午後５時から午前６時の間）にのみ要求されること、特

定のタイムフレーム（例えば、次の１時間、翌日、翌週など）に要求されること、或いはコンピューティングデバイス１００によって攻撃が検出された場合（例えば、直接的に検知した場合、又は外部システム又はデバイスによって通知された場合）又はコンピューティングデバイス１００が攻撃の危険にさらされている可能性があると判定された場合（例えば、上述のように識別された場合）にのみ２要素認証が要求されること、を指定してもよい。ユーザは、基準、保護タイプ、及び２要素認証タイプの任意の組合せを有してもよく、データストレージデバイス１０６に対してアクティブな複数の保護のセットを有してもよい。ある場合には、データストレージデバイスは、データストレージデバイス１０６がオペレーティングシステムから取り外された場合に（例えば、ホストコントローラ１０８がアクセスされることで、或いはオペレーティングシステムがホストコントローラの代わりに２要素認証を管理するために使用されることで）データへのアクセスを阻止するなどの、ユーザが２要素認証プロセスを終了できない限り、１つ以上のセクタへのアクセスを制限する、ファームウェア変更を有してもよい。

【００５２】

ある実施形態では、コンピューティングシステム１００は、例えば上述の２要素認証における要素のうちの１つとして、認証プロセスの一部に拡張現実を使用するように構成されてもよい。このような実施形態では、位置的、物理的、及び視覚的な入力の組合せが、コンピューティングシステム１００におけるユーザの認証に使用されてもよい。このような入力は、ジオロケーション、ローカル環境、ローカル位置、及びオブジェクトの入力を含んでもよい。ジオロケーション入力は、全地球測位システムの使用により提供されるような、地理的座標（例えば、緯度及び経度）を含んでもよい。ローカル環境入力は、（例えば、オフィス、自宅、特定のオフィス、野球場など）ユーザのすぐ周囲の環境を識別する広範な視覚的な手がかりを含んでもよい。ローカル位置入力は、（例えば、オフィスのコーナー、特定のオフィスの中央、野球場のファーストベース上など）ローカル環境におけるユーザの位置を識別するために、ローカル環境に関連付けられた、より具体的な環境特徴を含んでもよい。オブジェクト入力は、（例えば、取り付けられた写真、名刺、カウチのコーナー、壁金庫の裏、壁のステッカーなど）ユーザのローカル位置から見ることができるローカル環境における特定のオブジェクト又はその特徴に関するデータを含んでもよい。これらの入力のシリーズは、ユーザの認証に使用するための認証データのセットとして使用されてもよい。例えば、ユーザは、カメラを（例えば、スマートフォン、ウェアラブルコンピューティングデバイス、又は他の適切なデバイス上に）所有してもよく、カメラを使用して画像データをキャプチャし、画像がキャプチャされた地理的位置を特定して、コンピューティングシステム１００に送信してもよい。次に、コンピューティングシステム１００は、地理的位置を使用してユーザが登録されたジオロケーションにいるか否かを識別し、そして、画像データから、ユーザがローカル環境内の正しいローカル位置にいるか否かを判定し、ユーザが特定のオブジェクトを見ているか否かを判定してもよい。例えば、認証は、ユーザが自宅にいて、自宅のオフィスにいて、オフィスの特定の壁にある特定のステッカーを見ることを要求してもよい。

【００５３】

ある場合には、拡張現実の使用が２要素認証の一部として使用されてもよい。このような場合、指定されたジオロケーションの、指定された環境における、指定されたオブジェクトのユーザによる目視の認証は、オブジェクトの目視に加えて提供され認証されるパスワード又は他の情報のような、追加データの提供と組み合わされてもよい。ある実施例では、オブジェクトの目視は、認証の２番目の要素に使用されるデータを明らかにするために使用されてもよい。例えば、ユーザは、カメラ又は他の光学撮像装置を使用して、コンピューティングシステム１００に送信される画像データをキャプチャしてもよく、コンピューティングシステム１００は、カメラによってキャプチャされ、コンピューティングシステム１００に送信されるものを表示するスマートフォンなど、キャプチャされた光学画像のリアルタイム表示をユーザに提供する表示装置を含んでもよい。ユーザがコンピューティングシステム１００によって判定された正しいオブジェクトを見ている場合、コンピ

ューティングシステム１００は、パスワード又は他のデータを、標準的な拡張現実技術を使用して、正しいオブジェクトに重ねてデータを表示可能な、デバイスに送信してもよい。例えば、上記の例では、パスワードのリストがユーザの自宅のオフィスの特定のステッカーに表示され、ユーザは、リストから適切なパスワードを第２の認証要素として提供してもよい。したがって、ユーザが正しいパスワードを識別することができる唯一の方法は、正しい環境の正しい位置にいて、正しいオブジェクトを見ていることである（パスワードは、例えば、静的であってもよく、或いは、動的で、ユーザへの表示のために送信する前にコンピューティングシステム１００によって生成されてもよい）。

【００５４】

ある実施形態では、タイピングヒューリスティックが、コンピューティングシステム１００における認証要素として使用されてもよい。コンピューティングシステム１００は、そのユーザによって入力されたキーストロークを受け付けるために、コンピューティングシステム１００とインタフェース接続された入力装置として、キーボードを含んでもよく、或いは、コンピューティングシステム１００は、ユーザの認証要求の一部としてキーストローク情報を受信してもよい。キーストローク情報は、少なくとも、ユーザによってキーボード上で押下されたキーを含んでもよく、また、それぞれのキーストロークに関するタイムスタンプ情報を含んでもよく、（例えば、それぞれのキーを押下するために使用される）タイピング圧力、それぞれのキーストロークの押下及び／又は解放時間（例えば、ユーザがキーを押下し、或いは一旦押下されたキーを解放するのにどれだけの時間がかかるか）などの、任意の他の使用可能な情報を含んでもよい。コンピューティングシステム１００は、キーストローク情報を受信し、ユーザのタイピングパターンを識別してもよい（例えば、任意の適切なプロセスを通じてユーザを識別してもよい）。タイピングパターンは、タイピング速度、キーストローク速度、キーストローク圧力、キーストローク間の時間（例えば、一般的なキーストローク、及び／又は、ある特定の文字から別の文字へといった特定のキーストローク）、タイピング精度などの、ユーザのタイピングヒューリスティックの評価であってもよい。タイピングパターンは、ユーザの認証キーを生成するために使用されてもよく、認証キーは、タイピングヒューリスティックをハッシュ化することにより生成される値のような、タイピングパターンを示すデータ値であってもよい。認証キーは、コンピューティングシステム１００との後続の相互アクションにおいてユーザを認証するために使用されてもよい。例えば、一例では、タイピングヒューリスティックは、コンピューティングシステム１００のユーザ（或いは、例えば、認証のためにコンピューティングシステム１００を使用する他の外部デバイスのユーザ）が電子メールを書く任意の時点でキャプチャされてもよい。ユーザが電子メールメッセージのコンテンツをタイプすると、そのキーストロークがキャプチャされ、そのタイピングヒューリスティックが送信前にコンピューティングシステム１００によって評価されてもよい。コンピューティングシステム１００は、電子メールのタイピングパターンに基づいて新たなキーを生成し、登録プロセス中にユーザのために生成された認証キーと比較してもよい。比較が成功すると、電子メールをタイプしたユーザは、登録ユーザと判定され、電子メールが正常に送信されてもよい。比較が失敗すると、タイプパターンの違いにより他人が登録されたユーザであると主張していることを示すような、認証失敗を示すエラーメッセージが電子メールの代わりに（或いは、例えば、電子メールとともに）送信されてもよい。ある実施例では、タイピングヒューリスティックは、上述のユーザフィンガープリントと組み合わされてもよい。

【００５５】

＜例示的なホストコントローラプロセス＞

図３は、コンピューティングシステム１００におけるデータストレージデバイス１０６の動作に関して、データストレージデバイス１０６のホストコントローラ１０８によって実行されるプロセス３００を示す。図３に示すプロセス３００は一例であり、ホストコントローラ１０８がその動作中に追加及び／又は代替のプロセスを使用し得ることは、当業者には明らかであろう。

【００５６】
ステップ３０２において、ホストコントローラ１０８は、インタフェース（例えば、ファイルシステムコントローラ１２２、中継装置１１８などと通信するためのアプリケーションプログラミングインタフェース）のアクティベーション、記憶ブロック及びセクタの読み出し及びログへの記録、任意のベンダ機能のアクティベーション、コンピューティングシステム１００又はネットワーク内の他のコンポーネントとのセキュアチャネルの確立などを含む、プラットホームの初期化を実施してもよい。ステップ３０４において、データストレージデバイス１０６の動作のためのホストコントローラ１０８によるコマンドの標準的な処理を含む、コマンド処理ループが開始されてもよい。
【００５７】
ステップ３０６において、ホストコントローラ１０８は、ホストコントローラ１０８、中継装置１１８、又はデータをホストコントローラ１０８と通信する他のデバイスにより検出され得る脅威イベントなどの、セキュリティイベントが発生したか否かを判定してもよい。例えば、脅威イベントは、独立コンポーネントに関連付けられたコマンドの有無、データアクセスリミットへの到達、セキュアチャネルを使用して通信される他のコンピューティングデバイスによる脅威イベントの検出などであってもよい。セキュリティイベントが検出された場合、ステップ３０８において、ホストコントローラ１０８は、構成可能な応答テーブルに従って適切な応答を実行してもよい。構成可能な応答テーブルは、検出されたイベントに対する応答のリストを含んでもよく、応答は、例えば、データのバックアップ、データの暗号化、ＯＳアプリケーション１２０の復元、他のコンピューティングシステム１００への通知、データの消去、データへのアクセスの阻止、（例えば、０ｘ００ｓ、ランダムデータなどの）代替のデータの返送を含んでもよい。ホストコントローラ１０６により追跡されているイベントのプロンプトがある場合、適切な応答が実行されると、セキュリティイベントのプロンプトがリストから除去されてもよい。
【００５８】
脅威イベントではないイベントが発生した場合、ステップ３１０において、イベント（本明細書ではコマンドパケットとも称される）が解析される。コマンドパケットの解析は、図４に示されるプロセス４００を使用して実行されてもよい。ステップ４０２において、データの読み出し、データの変更、データの上書き、データの移動などのコマンドである、コマンドパケットが審査されてもよい。ステップ４０４において、ホストコントローラ１０８は、コマンドの要求者又はそれに関連付けられたアクションなどに基づいて、コマンドのコマンドタイプを判定してもよい。例えば、コマンドは、ファイルシステムコントローラ１２２から受信した標準読み出しコマンドであってもよく、或いは、データストレージデバイス１０６の一部としてベンダアクションから発行されたコマンドであってもよい。ステップ４０６において、ホストコントローラ１０８は、データストレージデバイス１０６に向かうデータ、データストレージデバイス１０６から出てくるデータ、或いは、データストレージデバイス１０６に出入りするデータなし、というように、コマンドの結果としてデータが流れる方向を判定してもよい。
【００５９】
コマンドパケットが解析されると、ステップ３１２において、ホストコントローラ１０８は、（例えば、ステップ４０４の解析に基づいて）コマンドパケットがベンダコマンドであるか否かを判定してもよい。コマンドパケットがベンダコマンドである場合、ステップ３１４において、図５に示されるプロセス５００が実行されてもよい。ステップ５０２において、ホストコントローラ１０８は、その動作が、ベンダコマンドに対応するベンダに関連付けられたモードにあるか否かを判定してもよい。そうではない場合、プロセス５００は終了してもよい。あるいは、ホストコントローラ１０８のモードが、それに応じて調整されてもよい。ホストコントローラ１０８がベンダモードにある場合、ステップ５０４において、ベンダコマンドがホストコントローラ１０８によって実行され、対応するアクションが実行されてもよい。
【００６０】

ステップ３１２において、コマンドパケットが非ベンダコマンドのものであるとホストコントローラ１０８が判定した場合、ステップ３１６において、ホストコントローラ１０８は、図６に示されるプロセス６００を実行してもよい。ステップ６０２において、コマンドの前に実行されるベンダに関連付けられた任意のプロセスが、ホストコントローラ１０８によって実行されてもよい。ステップ６０４において、（例えばコマンドパケットに示されるように）実行されるべきコマンドがパターンエンジンに追加されてもよい。ステップ６０６において、パターンエンジンは、（例えばコマンドの）パターンが正常であるか否か、及び、（署名、実行されるべきコマンドなどに基づいて）パターンが脅威イベントであることの何らかの兆候を示すか否かを判定するために照会されてもよい。ステップ６０８において、ホストコントローラ１０８は、パターンエンジンのチェックが失敗したか否か（例えば、脅威又は異常イベントが検出されたか否か）を判定する。チェックが失敗した場合、ステップ６１０において、ステップ３０８に記載されているように、構成可能な応答テーブルに示されるような適切な応答が実行されてもよい。ある場合には、プロセス６００は、応答が実行されると完了されてもよい。他の場合、又はチェックが合格した場合、ステップ６１２において、コマンドパケット内のコマンド（例えばデータ読み出し、書き込み、上書き、変更など）が実行されてもよい。コマンドの実行は、図８に示され、以下で詳細に説明されるプロセス８００を使用してもよい。

【００６１】

ステップ６１４において、コマンド後処理が実行されてもよい。ある場合には、コマンド後処理は、コマンドの実行の結果として生じるような脅威イベントの識別を含んでもよい。脅威イベントが発生した場合、脅威イベントは、適切な応答の実行のために（例えばステップ３０６で）ホストコントローラ１０８にフィードバックされてもよい。ステップ６１６において、コマンドの実行に関するメトリクスがキャプチャされ、後続のイテレーションにおけるステップ６０６で行われる将来の判定に使用されるためにパターンエンジンにフィードバックされてもよい。

【００６２】

コマンドが処理されると、ステップ３１８において、ホストコントローラ１０８は、プロセス３００がアイドルであるか否かを判定してもよい。この判定は、例えば、実行を待っている受信されたコマンドのプロンプトリストに基づいてもよく、ホストコントローラ１０８は、ホストコントローラ１０８による処理を現在待っているコマンドパケットがない場合にはアイドルであってもよい。ホストコントローラ１０８がアイドルではない場合、ステップ３２２において、プロセス３００は、ステップ３０４に戻り、次のコマンドパケットを処理してもよい。

【００６３】

ホストコントローラ１０８がアイドルである場合、ステップ３２０において、ホストコントローラ１０８は、図７に示されるような、アイドルプロセス７００を実行してもよい。アイドルプロセスでは、ステップ７０２において、ホストコントローラ１０８は、何らかの実行されるべき処理が（例えば古いデータのクリア、データセクタの切り替えなどのために）データストレージデバイス１０６に記憶されたデータを変更するか否かを判定してもよい。変更が行われる場合、ステップ７０４において、ホストコントローラ１０８は、独立コンポーネントのステータス、該当する規則の遵守などに基づいて、このような変更が許可されるか否かを判定してもよい。変更が許可されないが、コマンドに必要である場合、プロセス７００は、コマンドを実行せずに完了してもよい。変更が許可される場合、又は変更が必要ではない場合、ステップ７０６において、ホストコントローラ１０８は、アイドル処理コマンドを実行してもよい。アイドル処理コマンドは、例えば、ガーベッジコレクション、古い又はインアクティブなブロックのクリア、パターンエンジンの更新、及び当業者には明らかな他のアクションを含んでもよい。

【００６４】

ホストコントローラ１０８によるコマンドの実行は、図８に示されるプロセス８００を使用してもよい。ステップ８０２において、ホストコントローラ１０８は、（例えばステ

ップ４０６で判定されるように）コマンドが読み出しコマンドであるか否かを判定する。コマンドが読み出しコマンドである場合、ステップ８０４において、ホストコントローラ１０８は、ユーザ制限、ユーザパーミッション、独立コンポーネント状態などに基づいて、データの読み出しが現在許可されるか否かを判定してもよい。読み出しが許可されない場合、ステップ８０６において、ホストコントローラ１０８は、試みられた読み出しアクセスがログに記録されるべきか否かを判定してもよい。このような判定は、コンピューティングシステム１００のオペレータ、データストレージデバイス１０６の製造者、コマンドの性質などにより行われる、ホストコントローラ１０８の設定に基づいてもよい。アクセスがログに記録されるべきではない場合、プロセス８００は完了されてもよい。アクセスがログに記録されるべきである場合、ステップ８０８において、試みられた読み出しコマンドは、ホストコントローラ１０８において（或いは、例えば中継装置１１８のＳＡＴＡドライブ２１０などの他の適切なコンポーネントにおいて）ログに記録されてもよい。

【００６５】

ステップ８０４において、読み出しが許可されるとホストコントローラ１０８が判定した場合、ステップ８１０において、ホストコントローラ１０８は、アクションの実行がログに記録されるべきか否かを判定してもよい。そうであれば、ステップ８１２において、ホストコントローラ１０８は（或いは、例えば他の適切なコンポーネントは）、コマンドの実行をログに記録してもよい。ステップ８１４において、ホストコントローラ１０８は、読み出されるデータが（例えば、コマンドパケットに示されるなどにより）返される前に変更されるべきか否かを判定してもよい。データが変更される場合、ステップ８１６において、データはそれに応じて変更されてもよい。データが変更された場合、或いは、変更が行われなかった場合、ステップ８１８において、データは、ファイルシステムコントローラ１２２又はコマンドパケットに示される他の該当するコンポーネントに返され、プロセス８００が完了してもよい。

【００６６】

ステップ８０２において、コマンドパケットがデータの読み出しに関するものではないとホストコントローラ１０８が判定した場合、ステップ８２０において、ホストコントローラ１０８は、コマンドパケットがデータの書き込みに関するものであるか否かを判定してもよい。コマンドパケットがデータの読み出し又は書き込みを行わないコマンドに関するものである場合、ステップ８２２において、ホストコントローラ１０８によって、データなし（non-data）コマンドが実行されてもよい。コマンドがデータの書き込みを伴う場合、ステップ８２４において、ホストコントローラ１０８は、上述のように、対応するデータへの変更が許可される否かを判定してもよい。変更が許可されない場合、ステップ８２６及び８２８において、ホストコントローラ１０８は、試みられた変更がログに記録されるべきか否かを判定し、それに応じて処理を進めてもよい。

【００６７】

変更が許可される場合、ステップ８３０において、ホストコントローラ１０８は、変更がログに記録されるべきか否かを判定してもよく、そうであれば、ステップ８３２において、実行される変更をログに記録してもよい。ステップ８３４において、ホストコントローラ１０８は、変更されるデータが変更前にバックアップされるべきか否かを判定してもよい。このような判定は、コマンドのタイプ、ホストコントローラ１０８で設定されたポリシー、脅威イベントとしてのコマンドパケットの検出などに基づいてもよい。バックアップが実行される場合、ステップ８３６において、ホストコントローラ１０８は、データをデータストレージデバイス１０６内の所定のブロック及び／又はセクタにコピーすることなどにより、変更されるデータをバックアップしてもよい。バックアップが完了した場合、又はバックアップが実行されない場合、ステップ８３８において、ホストコントローラ１０８は、対応するデータブロック又はセクタへの変更を実行して、コマンドパケットに示されるとおりに、データの書き込みを達成してもよい。

【００６８】

＜コンピュータシステムアーキテクチャ＞

図９は、本開示の実施形態又はその一部がコンピュータ可読コードとして実装され得るコンピュータシステム９００を示す。例えば、図１のコンピューティングシステム１００は、ハードウェア、ソフトウェア、ファームウェア、命令を記憶した非一時的コンピュータ可読媒体、又はそれらの組み合わせを使用してコンピュータシステム９００に実装されてもよく、１つ以上のコンピュータシステム又は他の処理システムに実装されてもよい。ハードウェア、ソフトウェア、又はそれらの任意の組合せにより、図３～図８の方法を実施するために使用されるモジュール及びコンポーネントが具現化されてもよい。

【００６９】

プログラマブルロジックが使用される場合、このようなロジックは、専用のコンピュータ又は専用のデバイスとなるように、実行可能なソフトウェアコードによって構成された市販の処理プラットホーム上（例えばプログラマブルロジックアレイ、特定用途向け集積回路など）で実行されてもよい。開示された主題の実施形態が、マルチコアマルチプロセッサシステム、ミニコンピュータ、メインフレームコンピュータ、分散機能を用いてリンク又はクラスタ化されたコンピュータ、並びに、実質的に任意のデバイスに組み込まれ得るパーベイシブ又はミニチュアコンピュータを含む、様々なコンピュータシステム構成で実施され得ることは、当業者であれば理解されよう。例えば、少なくとも１つのプロセッサデバイス及びメモリを使用して、上述の実施形態が実装されてもよい。

【００７０】

本明細書で説明されるプロセッサユニット又はデバイスは、単一のプロセッサ、複数のプロセッサ、又はそれらの組み合わせとされてもよい。プロセッサデバイスは、１つ以上のプロセッサ「コア」を有してもよい。本明細書で論じられる「コンピュータプログラム媒体」、「非一時的コンピュータ可読媒体」、及び「コンピュータ使用可能媒体」という用語は、一般に、リムーバブルストレージユニット９１８、リムーバブルストレージユニット９２２、及びハードディスクドライブ９１２に設置されるハードディスクのような、有形媒体を指すために使用される。

【００７１】

本開示の様々な実施形態は、この例示的なコンピュータシステム９００に関連付けて説明されている。本説明を読んだ後、他のコンピュータシステム及び／又はコンピュータアーキテクチャを使用して、どのように本開示を実装するかは、当業者には明らかになるであろう。動作は連続的なプロセスとして記述されてもよいが、動作のいくつかは実際には並列、同時、及び／又は分散環境において実行されてもよく、シングル又はマルチプロセッサマシンによるアクセスのためにローカル又はリモートに記憶されたプログラムコードを用いて実行されてもよい。さらに、ある実施形態では、動作の順序は、開示された主題の趣旨から逸脱することなく再構成されてもよい。

【００７２】

プロセッサデバイス９０４は、本明細書で説明される機能を実行するように特に構成された、専用又は汎用プロセッサデバイスであってもよい。プロセッサデバイス９０４は、バス、メッセージキュー、ネットワーク、マルチコアメッセージパッシングスキームなどの、通信インフラストラクチャ９０６に接続されてもよい。ネットワークは、本明細書で開示されるような機能を実行するのに適した任意のネットワークであってもよく、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、ワイヤレスネットワーク（例えば、ＷｉＦｉ）、移動体通信網、衛星ネットワーク、インターネット、光ファイバ、同軸ケーブル、赤外線、無線周波数（ＲＦ）、又はそれらの任意の組合せを含んでもよい。他の適切なネットワークのタイプ及び構成は、当業者には明らかであろう。コンピュータシステム９００は、メインメモリ９０８（例えば、ランダムアクセスメモリ、リードオンリーメモリなど）を含んでもよく、セカンダリメモリ９１０を含んでもよい。セカンダリメモリ９１０は、ハードディスクドライブ９１２と、フロッピーディスクドライブ、磁気テープドライブ、光ディスクドライブ、フラッシュメモリなどのリムーバブルストレージドライブ９１４と、を含んでもよい。

【００７３】

リムーバブルストレージドライブ９１４は、周知の方法で、リムーバブルストレージユニット９１８への読み出し及び／又は書き込みを実施可能であってもよい。リムーバブルストレージユニット９１８は、リムーバブルストレージドライブ９１４によって読み出し及び書き込みされ得る、取り外し可能な記憶媒体を含んでもよい。例えば、リムーバブルストレージデバイス９１４がフロッピーディスクドライブ又はユニバーサルシリアルバスポートである場合、リムーバブルストレージユニット９１８は、それぞれフロッピーディスク又はポータブルフラッシュドライブであってもよい。一実施形態では、リムーバブルストレージユニット９１８は、非一時的コンピュータ可読記録媒体であってもよい。

【００７４】

ある実施形態では、セカンダリメモリ９１０は、例えばリムーバブルストレージユニット９２２及びインタフェース９２０など、コンピュータプログラム又は他の命令をコンピュータシステム９００にロードすることを可能にする代替手段を含んでもよい。このような手段の例は、当業者には明らかなように、（例えばビデオゲームシステムに見られるような）プログラムカートリッジ及びカートリッジインタフェース、（例えばＥＥＰＲＯＭ、ＰＲＯＭなどの）リムーバブルメモリチップ及び関連付けられたソケット、並びに他のリムーバブルストレージユニット９２２及びインタフェース９２０を含んでもよい。

【００７５】

コンピュータシステム９００に（例えば、メインメモリ９０８及び／又はセカンダリメモリ９１０に）記憶されるデータは、光学ストレージ（例えば、コンパクトディスク、デジタルバーサタイルディスク、ブルーレイディスク等）又は磁気テープストレージ（例えば、ハードディスクドライブ）のような、任意のタイプの適切なコンピュータ可読媒体に記憶されてもよい。データは、リレーショナルデータベース、ストラクチャードクエリランゲージ（ＳＱＬ）データベース、分散データベース、オブジェクトデータベースなど、任意のタイプの適切なデータベース構成で構成されてもよい。好適な構成及びストレージタイプは、当業者には明らかであろう。

【００７６】

コンピュータシステム９００は、通信インタフェース９２４を含んでもよい。通信インタフェース９２４は、コンピュータシステム９００と外部デバイスとの間でソフトウェア及びデータを転送可能にするように構成されてもよい。例示的な通信インタフェース９２４は、モデム、ネットワークインタフェース（例えば、イーサネットカード）、通信ポート、ＰＣＭＣＩＡスロット及びカードなどを含んでもよい。通信インタフェース９２４を介して転送されるソフトウェア及びデータは、当業者には明らかなように、電子的、電磁気的、光学的、又は他の信号などの、信号の形態であってもよい。信号は、信号を伝送するように構成され、ワイヤ、ケーブル、光ファイバ、電話回線、携帯電話リンク、無線周波数リンクなどを使用して実施され得る、通信パス９２６を介して移動してもよい。

【００７７】

コンピュータシステム９００は、表示インタフェース９０２を更に含んでもよい。表示インタフェース９０２は、コンピュータシステム９００と外部ディスプレイ９３０との間でデータを転送可能にするように構成されてもよい。例示的なディスプレイインタフェース９０２は、高精細度マルチメディアインタフェース（ＨＤＭＩ）、デジタルビジュアルインタフェース（ＤＶＩ）、ビデオグラフィックスアレイ（ＶＧＡ）などを含んでもよい。ディスプレイ９３０は、陰極線管（ＣＲＴ）ディスプレイ、液晶ディスプレイ（ＬＣＤ）、発光ダイオード（ＬＥＤ）ディスプレイ、静電容量タッチディスプレイ、薄膜トランジスタ（ＴＦＴ）ディスプレイなどを含む、コンピュータシステム９００の表示インタフェース９０２を介して送信されるデータを表示するための任意の適切なタイプのディスプレイであってもよい。

【００７８】

コンピュータプログラム媒体及びコンピュータ使用可能媒体は、メモリ半導体（例えばＤＲＡＭなど）であり得る、メインメモリ９０８及びセカンダリメモリ９１０などのメモリを指してもよい。これらのコンピュータプログラム製品は、コンピュータシステム９０

０にソフトウェアを提供するために手段である。コンピュータプログラム（例えば、コンピュータ制御ロジック）は、メインメモリ９０８及び／又はセカンダリメモリ９１０に記憶されてもよい。コンピュータプログラムは、通信インタフェース９２４を介して受信されてもよい。このようなコンピュータプログラムは、実行されると、コンピュータシステム９００が本明細書で論じられる本方法を実施できるようにしてもよい。具体的には、コンピュータプログラムは、実行されると、本明細書で説明すされるように、プロセッサデバイス９０４が図３～図８に示される方法を実施できるようにしてもよい。したがって、このようなコンピュータプログラムは、コンピュータシステム９００のコントローラを表してもよい。本開示がソフトウェアを使用して実装される場合、ソフトウェアは、コンピュータプログラム製品に記憶され、リムーバブルストレージドライブ９１４、インタフェース９２０、及びハードディスクドライブ９１２、又は通信インタフェース９２４を使用して、コンピュータシステム９００にロードされてもよい。

【００７９】

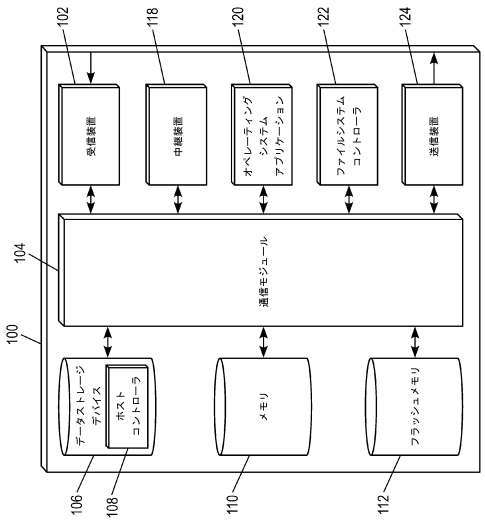
プロセッサデバイス９０４は、コンピュータシステム９００の機能を実行するように構成された１つ以上のモジュール又はエンジンを備えてもよい。モジュール又はエンジンのそれぞれは、ハードウェアを使用して実装されてもよく、ある実施例では、メインメモリ９０８又はセカンダリメモリ９１０に記憶されたプログラムコード及び／又はプログラムに対応するようなソフトウェアを使用してもよい。このような場合、プログラムコードは、コンピュータシステム９００のハードウェアによる実行の前に、プロセッサデバイス９０４（例えばコンパイルモジュール又はエンジン）によってコンパイルされてもよい。例えば、プログラムコードは、プロセッサデバイス９０４及び／又はコンピュータシステム９００の任意の追加のハードウェアコンポーネントによる実行のために、アセンブリ言語又はマシンコードのような下位言語（lower level language）に翻訳されるプログラミング言語で書かれたソースコードであってもよい。コンパイルのプロセスは、語彙分析、前処理、構文解析、意味解析、構文指向翻訳、コード生成、コード最適化、及び本明細書に開示される機能を実行するためにコンピュータシステム９００を制御するのに適した下位言語へのプログラムコードの翻訳に適している他の任意の技術の使用を含んでもよい。このようなプロセスの結果、コンピュータシステム９００が、上述の機能を実行するように一意にプログラムされた、特別に構成されたコンピュータシステム９００になることは、当業者には明らかであろう。

【００８０】

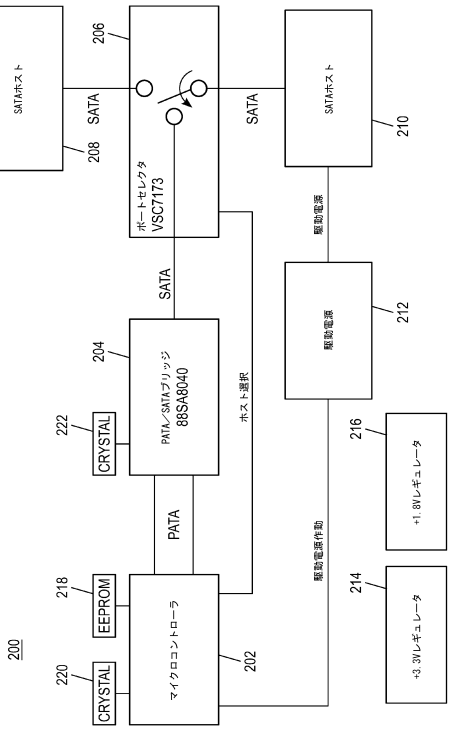
本開示と整合性のある技術は、特に、データアクセスの監視及び制御のシステム及び方法を提供する。開示されたデバイス及び方法の様々な例示的な実施形態が上述されたが、限定ではなく、単に例示の目的のために提示されたことを理解されるべきである。これは網羅的ではなく、開示された厳密な形態に限定するものではない。上記の教示に照らして、変更及び変形が可能であり、あるいは、本開示の実施から、その範囲又はスコープから逸脱することなく、変更及び変形を得ることができる。

【図面】

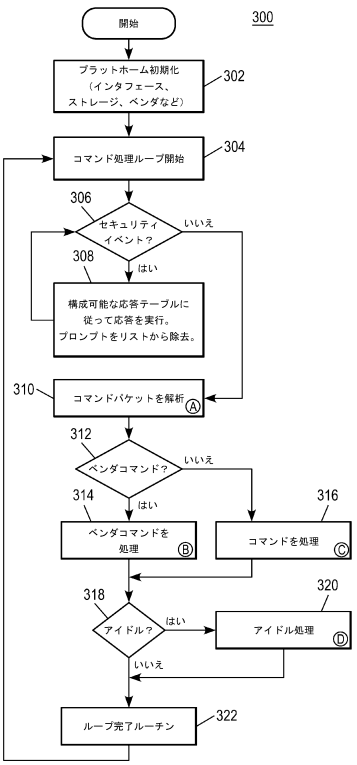
【図１】


102
118
120
122
124
受信装置
中継装置
オペレーティングシステム アプリケーション
ファイルシステム コントローラ
送信装置
104
通信モジュール
100
データストレージデバイス
ホストコントローラ
メモリ
フラッシュメモリ
106
108
110
112

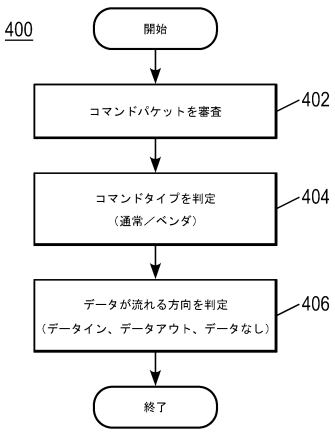
【図２】


SATAホスト
206
SATA
208
ポートセレクタ VSC7173
SATA
SATAホスト
210
駆動電源
SATA
212
204
PATA／SATAブリッジ 88SA8040
ホスト選択
222
CRYSTAL
216
+1.8Vレギュレータ
PATA
218
EEPROM
214
+3.3Vレギュレータ
駆動電源作動
220
CRYSTAL
マイクロコントローラ
202
200

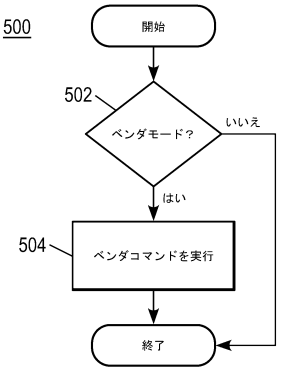
【図３】


開始
300
プラットホーム初期化（インタフェース、ストレージ、ベンダなど）
302
コマンド処理ループ開始
304
306
セキュリティイベント？
いいえ
はい
308
構成可能な応答テーブルに従って応答を実行。プロンプトをリストから除去。
310
コマンドパケットを解析 Ⓐ
312
ベンダコマンド？
いいえ
はい
314
ベンダコマンドを処理 Ⓑ
316
コマンドを処理 Ⓒ
318
アイドル？
はい
320
アイドル処理 Ⓓ
いいえ
ループ完了ルーチン
322

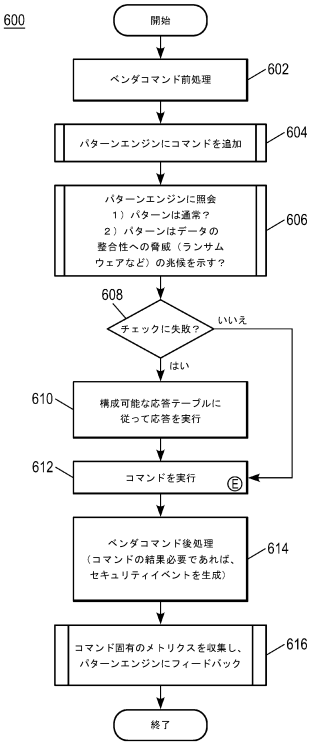
【図４】


400
開始
コマンドパケットを審査
402
コマンドタイプを判定（通常／ベンダ）
404
データが流れる方向を判定（データイン、データアウト、データなし）
406
終了

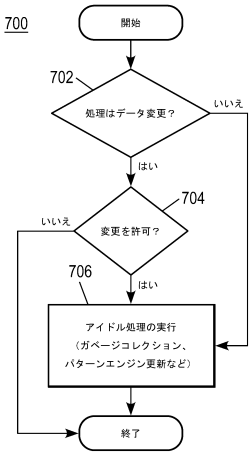
【図５】


500
開始
502
ベンダモード？
いいえ
はい
504
ベンダコマンドを実行
終了

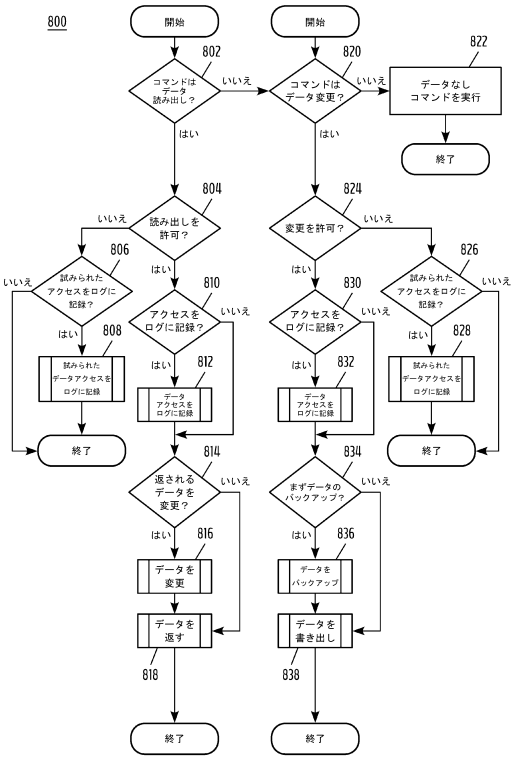
【図６】


600
開始
ベンダコマンド前処理
602
パターンエンジンにコマンドを追加
604
パターンエンジンに照会
1）パターンは通常？
2）パターンはデータの
整合性への脅威（ランサム
ウェアなど）の兆候を示す？
606
608
チェックに失敗？
いいえ
はい
610
構成可能な応答テーブルに
従って応答を実行
612
コマンドを実行
Ⓔ
ベンダコマンド後処理
（コマンドの結果必要であれば、
セキュリティイベントを生成）
614
コマンド固有のメトリクスを収集し、
パターンエンジンにフィードバック
616
終了

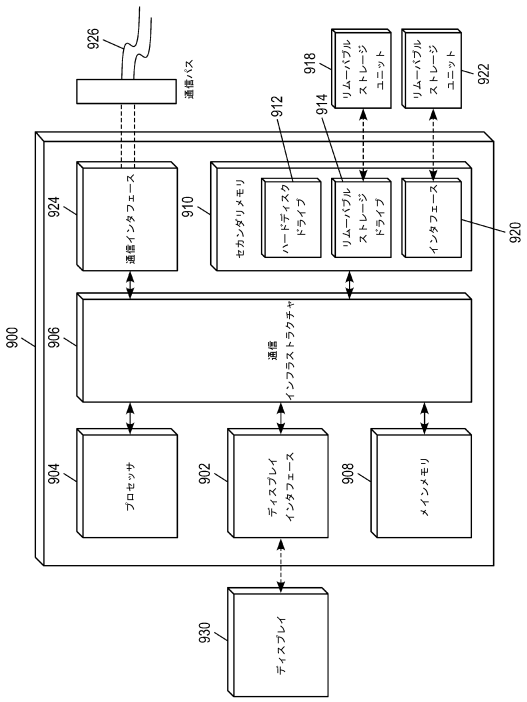
【図７】


700
開始
702
処理はデータ変更？
いいえ
はい
704
変更を許可？
いいえ
はい
706
アイドル処理の実行
（ガベージコレクション、
パターンエンジン更新など）
終了

【図８】


800
開始
802
コマンドは
データ
読み出し？
いいえ
はい
804
読み出しを
許可？
いいえ
はい
806
試みられた
アクセスをログに
記録？
いいえ
はい
808
試みられた
データアクセスを
ログに記録
終了
810
アクセスを
ログに記録？
いいえ
はい
812
データ
アクセスを
ログに記録
814
返される
データを
変更？
いいえ
はい
816
データを
変更
データを
返す
818
終了
開始
820
コマンドは
データ変更？
いいえ
はい
822
データなし
コマンドを実行
終了
824
変更を許可？
いいえ
はい
826
試みられた
アクセスをログに
記録？
いいえ
はい
828
試みられた
データアクセスを
ログに記録
終了
830
アクセスを
ログに記録？
いいえ
はい
832
データ
アクセスを
ログに記録
834
まずデータの
バックアップ？
いいえ
はい
836
データを
バックアップ
データを
書き出し
838
終了

【図９】


926
通信バス
918
リムーバブル
ストレージ
ユニット
922
912
914
924
通信インタフェース
910
セカンダリメモリ
ハードディスク
ドライブ
リムーバブル
ストレージ
ドライブ
インタフェース
920
900
906
通信
インフラストラクチャ
904
プロセッサ
902
ディスプレイ
インタフェース
908
メインメモリ
930
ディスプレイ

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
前置審査
アメリカ合衆国 フロリダ州 ３３９０７ フォート マイヤーズ シマリング レイク コート １４０１６
審査官 岸野 徹
(56)参考文献 特開２０１７－０９８６５８（ＪＰ，Ａ）
米国特許第０８３１２０６４（ＵＳ，Ｂ１）
特表２００９－５１２９４７（ＪＰ，Ａ）
国際公開第２０１３／１５４９３６（WO，Ａ１）
米国特許出願公開第２００６／０２４２１５９（ＵＳ，Ａ１）
特開２０１３－０４５２９２（ＪＰ，Ａ）
国際公開第２００９／０９６０８９（WO，Ａ１）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ ２１／３１