

明 細 書

発明の名称：

解析システム、解析装置、解析方法、及び、解析プログラムが記録された記憶媒体

技術分野

[0001] 本発明は、情報通信装置等において実行される暗号通信を解析する技術に関する。

背景技術

[0002] 近年、通信ネットワークに接続された、コンピュータ等の情報処理装置（以下、単に「情報通信装置」と称する場合がある）において実行される通信処理を解析する技術が求められている。

[0003] そのような通信処理の解析は、例えば、情報通信装置の開発及び運用段階における挙動の解析、あるいは、情報通信装置において実行される通信処理プログラムの挙動の解析等に用いられる。

[0004] 特に、近年では、情報通信装置において実行されるウィルス等の不正なコンピュータ・プログラム（コンピュータ・プログラムには、各種ソフトウェア・プログラムが含まれる。以下単に「プログラム」と称する場合がある）に起因する、不正な通信処理の内容を解析する技術が求められている。

[0005] 係る不正なプログラム（以下「マルウェア」と称する場合がある）が、例えば、公開鍵暗号等の高度な暗号方式を採用して各種通信処理を実行する場合、通信記録（通信データ）の解読（復号）が極めて困難である。

[0006] 例えば、解析対象の情報通信装置が、特定の暗号通信プロトコルを採用している場合（即ち、解析対象の情報通信装置の間で、当該特定の暗号通信プロトコルにより暗号化された通信路が確立される場合）を想定する。この場合、当該暗号通信プロトコルに関する暗号鍵及び認証情報等は、通信装置の間で安全に交換される。上記特定の暗号通信プロトコルとして、例えば、以下のような暗号通信プロトコルが用いられ得る。

[0007] ・SSL (Secure Sockets Layer) / TLS (Transport Layer Security)、
 ・IPSec (Security Architecture for Internet Protocol) におけるIKE (Internet Key Exchange)、
 ・SSH (Secure Shell)。

[0008] 通常、このような暗号通信プロトコルに基づいて送受信される暗号化された通信データを解読することは容易ではない。このため、当該暗号通信を実行する情報通信装置（当該情報通信装置において実行される各種ソフトウェア・プログラムを含む）を解析することにより、係る暗号通信に関する情報を収集する技術が検討されている。

[0009] このような情報通信装置を解析する技術として、例えば、情報通信装置において特定のプログラム（例えば、マルウェア等）を実行させたまま、当該プログラムの挙動を解析する手法（以下「ライブフォレンジック手法」と称する場合がある）が知られている。係るライブフォレンジック手法は、ある装置（あるいはシステム）が稼働した状態において、当該装置に関する各種情報を収集することにより、当該装置の挙動に関する各種調査や分析を実行する。係るライブフォレンジック手法は、例えば、情報処理装置の稼働時における、揮発性の記憶装置（メモリ等）に記憶されるデータや、実行されるプログラム等を調査可能である。

[0010] 上記したような、通信処理を含む情報処理装置の挙動を解析する技術に関連して、例えば以下のような文献が開示されている。

[0011] 即ち、特許文献1（特表2014-514651号公報）は、マルウェア解析に関する技術を開示する。特許文献1に開示された技術は、仮想マシン（バーチャルマシン）により構成された情報処理装置からの各種リクエストを、仮想マシンモニタがインターセプト（取得）し、その情報をセキュリティエージェントに転送する。セキュリティエージェントは、取得した情報に基づいて、係るリクエストを実行したプログラムがマルウェアか否かを判定

する。仮想マシンモニタは、仮想マシンよりも低レイヤに存在するので、仮想マシンにおいて実行される全てのリクエストを取得可能である。

[0012] 特許文献2（特開2013-114637号公報）は、マルウェア解析に関する技術を開示する。特許文献2に開示された技術は、マルウェアを実行した際のトレース及び実行過程において参照されるデータを解析することにより、マルウェアを実行した装置におけるメモリ空間から、マルウェアが使用する暗号鍵を抽出する。また、特許文献2に開示された技術は、当該抽出した暗号鍵を用いてマルウェアによる暗号化通信を解読する。

[0013] 特許文献3（特表2012-511847号公報）は、マルウェア等による暗号通信を分類する技術を開示する。特許文献3に開示された技術は、解析対象装置において実行される暗号化通信と、予め登録した承認済みの暗号化通信とを比較することにより、未承認の暗号通信を検出する。また、特許文献3に開示された技術は、未承認の暗号通信を検出した場合、係る暗号通信をブロック（停止）する。

[0014] 特許文献4（特開2009-037545号公報）は、マルウェアの類似性に基づいて、マルウェアを分類及び識別する技術を開示する。特許文献4に開示された技術は、マルウェアの実行コード自体を解析するミクロ分析と、マルウェアに関連する通信を解析するマクロ分析との間の相関関係に基づいて、マルウェアを分類及び識別する。特許文献4に開示された技術は、ミクロ分析において、所定のタイミングにおいてダンプした解析対象マシンのメモリから、マルウェアの実行コードを抽出して逆アセンブルする構成を開示する。

[0015] 特許文献5（特開2006-279938号公報）は、2つの通信装置の間に介在し、通信装置間の暗号通信を解析する暗号通信復号装置に関する技術を開示する。特許文献5に開示された暗号通信復号装置は、2つの通信装置間における通信データを解析し、暗号通信（IPSec）の鍵交換が実行されるタイミングにて、それぞれの通信装置との間で暗号鍵を交換する。即ち、特許文献5に開示された暗号通信復号装置は、2つの通信装置の間に中

間者として介在し、一方の通信装置との間で暗号鍵を交換すると共に、他方の通信装置との間でも暗号鍵を交換する。これにより、特許文献5に開示された装置は、2つの通信装置の間で実行される暗号通信に介在し、一方の通信装置から送信される暗号通信データを復号して監視装置に送信すると共に、当該データを再度暗号化して他方の通信装置に送信する。

[0016] 特許文献6（特表2013-508823号公報）は、コンピュータにおけるリンクファイルの生成を監視することにより、マルウェアを検出する技術を開示する。特許文献6に開示された技術は、コンピュータの内外に存在する各種リソースに対するリンクを作成するプロセスに関する情報と、当該作成されたリンクの参照先の情報とを解析する。特許文献6に開示された技術は、その解析結果に基づいて、マルウェアに対する対策プロセスの実行や、リンクへのアクセスを抑制する。特許文献6に開示された技術は、作成されたリンクファイルを削除、編集、移動することが可能である。

[0017] 特許文献7（特表2013-507722号公報）は、情報処理装置において実行される特定のファイルの挙動に基づいて、マルウェアを検出する技術を開示する。特許文献7に開示された技術は、特定のファイルの普及率（実際のネットワーク環境にどの程度分布しているか）に基づいて、当該ファイルの攻撃性レベルを調整する。特許文献7に開示された技術は、特定のファイルに対する攻撃性のレベルを用いて、当該ファイルの挙動がマルウェアに該当するか否かを判定する。

[0018] 特許文献8（特開2011-154727号公報）は、マルウェアを仮想ネットワークにアクセスさせ、当該マルウェアの動作及び通信に関する情報を取得する技術を開示する。特許文献8に開示された技術は、仮想ネットワーク部に接続されたマルウェア実行環境においてマルウェアを実行する。仮想ネットワーク部は、マルウェア実行環境からの通信を受信して通信プロトコルを解析し、当該プロトコルに応じた適切な応答を生成してマルウェア実行環境に送信する。また、特許文献8に開示された技術は、マルウェア実行環境からの通信の内容に応じて、係る通信を実際のインターネット環境に接

続する。

[0019] 特定のタイミングあるいは日時においてのみ活動するプログラムを解析するために、係るプログラムの実行環境における時間経過速度を調整する技術が、特許文献9（特開2013-105366号公報）に開示されている。

[0020] また、暗号化されたデータを復号する技術に関連して、以下のような文献が存在する。

[0021] 特許文献10（特開2007-116752号公報）は、暗号文を復号した復号データの正しさを確認する技術を開示する。特許文献10に開示された技術は、疑似乱数を用いて暗号化されたデータを復号した際に、当該復号されたデータのエントロピーと特定の基準値とを比較することにより、当該復号されたデータの正しさを判定する。

先行技術文献

特許文献

- [0022] 特許文献1：特表2014-514651号公報
特許文献2：特開2013-114637号公報
特許文献3：特表2012-511847号公報
特許文献4：特開2009-037545号公報
特許文献5：特開2006-279938号公報
特許文献6：特表2013-508823号公報
特許文献7：特表2013-507722号公報
特許文献8：特開2011-154727号公報
特許文献9：特開2013-105366号公報
特許文献10：特開2007-116752号公報

発明の概要

発明が解決しようとする課題

[0023] 上記したように、情報処理装置においてマルウェア等により実行される暗号通信を解析する場合、暗号化された通信データを復号可能な情報（鍵等）

を取得する必要がある。

[0024] 例えば、上記したライブフォレンジック手法は、特定のタイミングにおける情報通信装置のメモリ空間の内容（メモリ空間に保持されるデータ）を取得可能であることが期待される。このため、当該取得したメモリ空間の情報を解析することにより、メモリ空間に存在する鍵を抽出することが考えられる。

[0025] しかしながら、例えば、メモリ空間に存在する鍵を抽出するために、調査対象の情報通信装置において各種監視プログラム等（以下「エージェント」と称する場合がある）を実行すると、それらのプログラムの実行をマルウェアに検知されてしまう可能性がある。エージェントの実行を検知したマルウェアは、当該マルウェア自体の活動を休止したり、当該マルウェア自体を含む、活動の痕跡を消去したりする。上記のように、マルウェアの解析を阻止する回避策が実行された場合、当該マルウェア自体、あるいは、当該マルウェアが実行する暗号通信の解析が困難になる。以上より、調査対象の情報通信装置においてエージェントを実行しない、エージェントレス方式の解析技術が必要とされている。

[0026] また、マルウェアによる暗号通信を停止（遮断）してしまうと、当該通信の遮断を検知したマルウェアは、自己の解析を阻止する回避策を実行する可能性がある。しかしながら、マルウェアによる暗号化通信を遮断せずに継続した場合、当該マルウェアの実行に伴う実体的な被害が拡大する可能性がある。

[0027] このため、マルウェアによる暗号通信自体は継続させつつ、当該暗号通信により発生する実体的な被害を低減可能な技術が必要とされている。即ち、マルウェアによる暗号通信の内容を解析した結果に基づいて、当該暗号通信により発生する実体的な被害を低減可能な技術が必要とされている。

[0028] これに対して、特許文献1、特許文献2、特許文献4、特許文献6、特許文献7、及び、特許文献8に開示された各技術は、情報通信装置に監視手段や実行トレース手段等（エージェント）を導入することによりマルウェアを

解析する。このため、当該マルウェアが、係るエージェントによる解析処理を検知して、自己の解析を阻止する回避策を実行する可能性がある。具体的には、特許文献2に開示された技術は、マルウェアの実行過程を解析することにより暗号鍵を抽出していることから、当該マルウェアが自己の解析を阻止する回避策を実行した場合、暗号鍵を抽出することが困難である。

[0029] また、特許文献3に開示された技術は、マルウェア等による暗号通信を解読しない。このため、係る技術をマルウェアが実行する暗号通信の解析に適用することは困難である。

[0030] また、特許文献4、特許文献6、特許文献7に開示された各技術は、マルウェアの挙動自体を解析する技術であり、マルウェアによる暗号化通信の解析については十分考慮していない。

[0031] また、特許文献5に開示された技術は、暗号化通信において使用される暗号鍵を事前に共有可能であることを前提としていることから、暗号鍵が不明なマルウェアによる暗号化通信を解析することが困難である。

[0032] また、特許文献8に開示された技術は、マルウェアが暗号化通信を実行する場合について十分考慮していない。

[0033] また、特許文献10に開示された技術は、暗号文の復号結果の成否を判定するのみであり、係る暗号文の解読に必要な暗号鍵の抽出に関しては十分考慮していない。

[0034] 以上より、上記各特許文献に開示された技術を採用した場合、例えば、マルウェア自体に検知される可能性を低減しつつ、当該マルウェアが実行する暗号通信を適切に検査することが困難である。

[0035] 本発明は、上記のような事情を鑑みてなされたものである。

[0036] 即ち、本発明は、解析対象である情報通信装置と、通信ネットワークとの間に介在し、当該情報通信装置と通信ネットワークとの間で送受信される暗号化された通信データを解読した結果に応じて特定の処理を実行する、解析システム等を提供することを主たる目的とする。

課題を解決するための手段

[0037] 上記の目的を達成すべく、本発明の一態様に係る解析システムは、以下の構成を備える。即ち、本発明の一態様に係る解析システムは、演算部とメモリ部とを有する情報通信装置から、上記メモリ部に保持されたデータの少なくとも一部を取得するメモリ取得部と、上記情報通信装置と、通信ネットワークとの間で暗号通信プロトコルに従って送受信される通信データに基づいて、当該暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データが上記メモリ部に保持されていると判定した場合に、上記メモリ取得部に対して上記メモリ部に保持されたデータの取得を指示する通信処理部と、上記鍵データの特徴を表すデータに基づいて、上記メモリ取得部が取得した上記メモリ部に保持されたデータから、上記鍵データの候補である1以上の鍵データ候補を抽出し、上記情報通信装置と上記通信ネットワークとの間で送受信される暗号化された上記通信データを、当該抽出した上記鍵データ候補を用いて解読した結果に基づいて、1以上の上記鍵データ候補の中から、暗号化された上記通信データを正しく解読可能な正しい鍵データを抽出する、暗号解析部と、を備え、上記通信処理部は、上記暗号解析部により解読された上記通信データに応じた特定の処理を実行する。

[0038] また、本発明の一態様に係る解析方法は、以下の構成を備える。即ち、本発明の一態様に係る解析方法は、情報処理装置が、演算部とメモリ部とを有する情報通信装置と、通信ネットワークとの間で暗号通信プロトコルに従って送受信される通信データに基づいて、当該暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データが上記メモリ部に存在すると判定した場合に、上記メモリに記憶されたデータの少なくとも一部を取得し、上記鍵データの特徴を表すデータに基づいて、当該取得した上記メモリに記憶されたデータから、上記鍵データの候補である1以上の鍵データ候補を抽出し、上記情報通信装置と上記通信ネットワークとの間で送受信される暗号化された上記通信データを、当該抽出した上記鍵データ候補を用いて解読した結果に基づいて、上記1以上の鍵データ候補の中から、暗号化された上記通信データを正しく解読可能な正しい鍵データを抽出し、上記解読された上記

通信データに基づいて、特定の処理を実行する。

[0039] また、同目的は、上記構成を有する解析システム、並びに対応する解析方法を、コンピュータによって実現するコンピュータ・プログラム、及び、そのコンピュータ・プログラムが格納されている、コンピュータ読み取り可能な記憶媒体等によっても達成される。

発明の効果

[0040] 本発明によれば、解析対象である情報通信装置と、通信ネットワークとの間で送受信される暗号化された通信データを解読した結果に応じて特定の処理を実行する解析システム等を提供可能である。

図面の簡単な説明

[0041] [図1]図1は、本願発明の第1の実施形態における解析システム及び解析対象装置等の機能的な構成を例示するブロック図である。

[図2]図2は、本願発明の第1の実施形態における解析対象装置及びメモリ取得部を実現可能な第1の構成例を例示する図である。

[図3]図3は、本願発明の第1の実施形態における解析対象装置及びメモリ取得部を実現可能な第2の構成例を例示する図である。

[図4]図4は、本願発明の第1の実施形態における鍵データ取得ポリシーの具体例を示す図である。

[図5]図5は、本願発明の第1の実施形態における通信データ記録ポリシーの具体例を示す図である。

[図6]図6は、本願発明の第1の実施形態における通信データ保持部の具体例を説明する図である。

[図7]図7は、本願発明の第1の実施形態における鍵候補判定情報の具体例を示す図である。

[図8]図8は、本願発明の第1の実施形態における鍵候補保持部の具体例を説明する図である。

[図9]図9は、本願発明の第1の実施形態における解析結果判定情報の具体例を示す図である。

[図10]図10は、本願発明の第1の実施形態における解析結果保持部の具体例を説明する図である。

[図11]図11は、本願発明の第1の実施形態における解析システムの動作の概要を例示する、フローチャートである。

[図12A]図12Aは、本願発明の第1の実施形態において、解析対象装置と通信ネットワークとの間で実行される暗号通信に用いられる暗号鍵を取得する動作を例示するフローチャートである。

[図12B]図12Bは、本願発明の第1の実施形態において、解析対象装置と通信ネットワークとの間で実行される暗号通信に用いられる暗号鍵を取得する動作を例示するフローチャートである。

[図13]図13は、SSLプロトコルにおける、暗号鍵の共有手順を例示するシーケンス図である。

[図14]図14は、本願発明の第1の実施形態における通信処理部（特には、通信データ記録部）の動作を例示するフローチャートである。

[図15]図15は、本願発明の第1の実施形態における暗号解析部（特には、鍵候補抽出部）の動作を例示するフローチャートである。

[図16]図16は、本願発明の第1の実施形態における暗号解析部（特には、暗号解読部）の動作を例示するフローチャートである。

[図17]図17は、本願発明の第2の実施形態における解析システム及び解析対象装置等の機能的な構成を例示するブロック図である。

[図18]図18は、本願発明の第2の実施形態における通信データ改変ポリシーの具体例を示す図である。

[図19]図19は、本願発明の第2の実施形態において、解析対象装置と通信ネットワークとの間の暗号通信に用いられる暗号鍵を取得し、通信データを改変する動作を例示するフローチャートである。

[図20]図20は、本願発明の第2の実施形態における通信データを改変する処理の具体例を示すフローチャートである。

[図21]図21は、本願発明の第3の実施形態における解析システム及び解析

対象装置等の機能的な構成を例示するブロック図である。

[図22]図 22 は、本願発明の各実施形態における解析システム、あるいは、当該解析システムの構成要素を実現可能な情報処理装置のハードウェア構成を例示したブロック図である。

発明を実施するための形態

[0042] 次に、本発明を実施する形態について図面を参照して詳細に説明する。以下の実施の形態に記載されている構成は単なる例示であり、本願発明の技術範囲はそれらには限定されない。

[0043] なお、各実施形態において説明する解析システムは、当該システムの 1 以上の構成要素が複数の物理的あるいは論理的に離間した装置（物理的な情報処理装置や、仮想的な情報処理装置等）を用いて実現されたシステムとして構成されてもよい。この場合、係る複数の装置の間は、有線又は無線又はそれらを組み合わせた任意の通信ネットワークを用いて通信可能に接続されてもよい。また、係る複数の装置が仮想的な情報処理装置等により構成される場合、上記通信ネットワークは、仮想的な通信ネットワークであってもよい。

[0044] また、各実施形態において説明する解析システムは、当該システムの全ての構成要素が 1 つの装置（物理的な情報処理装置や、仮想的な情報処理装置等）を用いて実現されたシステムとして構成されてもよい。

[0045] <第 1 の実施形態>

以下、本発明の第 1 の実施形態について説明する。まず、図 1 乃至図 3 を参照して、本実施形態における解析システムについて説明する。図 1 は、本実施形態における解析システム 100 の機能的な構成を例示するブロック図である。図 2 及び図 3 は、本実施形態における解析対象装置 101 及びメモリ取得部 102 を実現可能な構成例を例示する図である。

[0046] まず、解析対象装置 101 について説明する。解析対象装置 101 は、本実施形態における解析システム 100 により解析される解析対象の装置である。

- [0047] 図1に例示するように、本実施形態における解析対象装置101は、少なくとも演算部101a及びメモリ部101bを有し、通信路106を介して通信ネットワーク105と通信可能に接続された、任意の情報通信装置である。
- [0048] 解析対象装置101は、例えば、物理的なハードウェアにより構成されたコンピュータ等の情報通信装置であってもよい。また、解析対象装置101は、情報処理装置等の各種ハードウェアを仮想化可能な所定の仮想化基盤において提供される、仮想的なコンピュータ（VM: Virtual Machine）等であってもよい。
- [0049] 係る仮想化基盤は、例えば、通信ネットワークにより相互に接続された複数の情報処理装置により構築された環境（クラウドコンピューティング環境等）において提供されてもよく、1台の情報処理装置により構築された環境において提供されてもよい。
- [0050] 係る仮想化基盤は、例えば、特定のホストOS（Operating System）において実行されるソフトウェア・プログラムとして提供されてもよく、情報処理装置のハードウェアと、OSとの間に介在するソフトウェア・プログラムとして提供されてもよい。
- [0051] また、係る仮想化基盤は、物理的なハードウェアデバイスの機能を用いて提供されてもよく、ハードウェアデバイスの機能（例えば、CPU（Central Processing Unit）における各種仮想化支援機能等）と、ソフトウェア・プログラムとの組合せを用いて提供されてもよい。
- [0052] 例えば、係る仮想化基盤としてMicrosoft（登録商標）社製のHyper-Vを採用することが可能であるが、係る仮想化基盤は、これには限定されない。
- [0053] なお、解析対象装置101は、各種コンピュータ等に限定されず、例えば、携帯電話（スマートフォンを含む）、PDA（Personal Digital Assistant）、ゲーム機器、タブレット型情報機器、プリンタ、デジタル複合機、各種ネットワーク機器（スイッチ、ルータ、アク

セスポイント)等、通信ネットワークに接続可能な任意の機器であってもよい。

[0054] 演算部101aは、例えば、メモリ部101bに記憶された各種データ及びプログラム(コンピュータ・プログラム)を読み出して、当該プログラムに実装された各種演算処理を実行するCPU(Central Processing Unit)や、MPU(Microprocessing Unit)等の演算装置である。演算部101aは、特定のハードウェア(集積回路)を用いて構成される、物理的な演算装置であってもよい。演算部101aは、また、図3に例示するように、当該ハードウェアを仮想化した仮想化基盤における、仮想的な演算装置(仮想CPU)であってもよい。

[0055] メモリ部101bは、例えば、解析対象装置101におけるメインメモリとして機能し、演算部101aにおいて処理される各種プログラム及びデータ等を保持する。係るメモリ部101bは、特定のハードウェア(集積回路等)により構成された物理的なメモリ装置(例えば、DIMM(Dual Inline Memory Module)により構成されたDRAM(Dynamic Random Access Memory))であってもよい。また、メモリ部101bは、上記した所定の仮想化基盤において提供される、仮想的なメモリ装置であってもよい。

[0056] 本実施形態におけるメモリ部101bについては、当該メモリ部101bに保持(記憶)される記憶データ(以下、「メモリ領域データ」と称する場合がある)を、メモリ部101bの外部から取得(ダンプ)することができる。メモリをダンプする具体的な方法は、周知の技術を適宜選択してよい。例えば、係る方法として、OS(Operating System)の休止状態(ハイバネーション)機能を用いて不揮発性記憶装置に保存されたメモリ領域データを取得する方法や、OSが提供する仮想記憶においてページアウトされたメモリ領域データを取得する方法が採用されてもよい。

[0057] 上記に限らず、例えば、メモリ部101bを物理的なハードウェアにより構成した場合、メモリ領域データは、上記演算部101aと、メモリ部10

1 bとを接続する通信バス等において送受信されるデータを取得することにより取得されてもよい。また、メモリ領域データは、特定のタイミングにおいて、メモリ部101bの記憶領域を全て出力（メモリダンプ）することにより取得されてもよい。この場合、例えば、メモリ部101bに対するデータの読み込み、書き込み、アクセス等を制御するメモリコントローラ（不図示）の機能を用いて、メモリ領域データを取得することが可能である。

[0058] メモリ部101bを仮想的なメモリ装置として構成した場合、仮想化基盤が提供する機能（例えば、特定のAPI（Application Programming Interface）等）や、仮想化基盤が提供するデータ（例えば、仮想的なメモリ部に記憶されたデータの保存領域を特定可能な情報等）を介して、当該メモリ部101bに記憶されるデータを取得可能である。係る処理の具体的な実現方法は、仮想化基盤の具体的な構成に応じて周知の技術を適宜採用してよいので、詳細な説明は省略する。

[0059] 本実施形態における解析対象装置101は、通信路106を介して、通信ネットワーク105との間で、暗号通信を実行する。より具体的には、解析対象装置101は、通信ネットワーク105を介して通信可能に接続された他の情報通信装置107との間で、暗号通信を実行する。

[0060] この場合、解析対象装置101において実行されるプログラムが、他の情報通信装置107との間で暗号通信を実現してもよい。係るプログラムは、解析対象装置101において実行される正規のプログラムに限られない。係るプログラムには、上記説明したマルウェアが含まれ得る。

[0061] 解析対象装置101と、通信ネットワーク105（他の情報通信装置107）との間の通信路を暗号化する暗号通信プロトコルとしては、例えば、SSL、SSH、あるいはIPSec等の暗号通信プロトコル等が採用可能である。本実施形態を含め、以下に説明する各実施形態においては、係る暗号通信プロトコルとしてSSLが用いられる場合の具体例を説明する。なお、本実施形態における解析システム100は、SSLに限定されず、他の暗号通信プロトコルにも適用可能である。

[0062] 通信ネットワーク１０５は、有線、無線、又はこれらの任意の組合せにより構成され、任意の通信プロトコルを用いて通信路を確立可能な通信ネットワークである。係る通信ネットワーク１０５は、例えばInternet等の広域通信網であってもよく、LAN (Local Area Network) 等の構内通信網であってもよく、これらの組合せであってもよい。

[0063] また、通信ネットワーク１０５において用いられる通信プロトコルは、例えば、TCP/IP (Transmission Control Protocol / Internet Protocol) 等の周知の通信プロトコルであってよい。また、当該通信ネットワーク１０５は、例えば、上記説明した各種暗号通信プロトコルにより暗号化された通信路を、解析対象装置１０１に対して提供可能である。このような通信ネットワーク１０５は、周知の技術あるいはその組合せにより構成可能であるので、詳細な説明は省略する。

[0064] 他の情報通信装置１０７は、通信ネットワーク１０５を介して、解析対象装置１０１と通信可能に接続される。他の情報通信装置１０７は、例えば、物理的なハードウェアにより構成されたコンピュータ等の情報通信装置であってもよい。また、他の情報通信装置１０７は、所定の仮想化基盤において提供される、仮想的なコンピュータ等であってもよい。

[0065] 他の情報通信装置１０７は、例えば、各種コンピュータ等に限定されず、携帯電話（スマートフォンを含む）、PDA、ゲーム機器、タブレット型情報機器、プリンタ、デジタル複合機、各種ネットワーク機器、通信ネットワークに接続可能な任意の機器であってもよい。

[0066] 他の情報通信装置１０７は、例えば、上記例示したような暗号通信プロトコルを用いて、解析対象装置１０１との間で暗号通信を実行する。このような他の情報通信装置１０７は、周知の技術あるいはその組合せにより構成可能であるので、詳細な説明は省略する。

[0067] (解析システム１００の構成)

次に、本実施形態における解析システム１００の構成要素について説明す

る。

[0068] 本実施形態における解析システム１００は、メモリ取得部１０２、暗号解析部１０４、及び、通信処理部１０３を主たる構成要素として備える（以下、メモリ取得部１０２、暗号解析部１０４、通信処理部１０３、及びそれらを構成する構成要素を、単に「解析システム１００の構成要素」と称する場合がある）。

[0069] 本実施形態における解析システム１００は、これらの構成要素を用いて、解析対象装置１０１と、通信ネットワーク１０５を介して接続された他の情報通信装置１０７との間で実行される暗号通信を解析する。そして、本実施形態における解析システム１００は、当該解析結果に基づいて、特定の処理を実行する。

[0070] 解析システム１００の各構成要素は、それぞれ物理的なコンピュータ等の情報処理装置を用いて実現されてもよく、あるいは、仮想化基盤において提供されるＶＭを用いて実現されてもよい。解析システム１００の各構成要素の間は、無線、有線、あるいはそれらを組み合わせた任意の通信回線により、通信可能に接続されている。係る通信回線は、周知の技術を採用してよいので、詳細な説明は省略する。以下、解析システム１００の各構成要素について説明する。

[0071] （メモリ取得部１０２の構成）

まず、本実施形態におけるメモリ取得部１０２について説明する。本実施形態におけるメモリ取得部１０２は、解析対象装置１０１と通信可能に接続される。メモリ取得部１０２は、解析対象装置１０１のメモリ部１０１ｂに保持されるメモリ領域データを取得する。メモリ取得部１０２は、取得したメモリ領域データを保持するメモリダンプ保持部１０２ａを有する。

[0072] 解析対象装置１０１を物理的なコンピュータ等の情報通信装置により実現する場合、メモリ取得部１０２は、例えば、図２に例示するように、メモリ部１０１ｂに各種通信バス等を介して接続される拡張ハードウェア装置として実現されてもよい。また、メモリ取得部１０２は、メモリ部１０１ｂに対

するデータの読み込み、書き込み、アクセス等を制御するメモリコントローラ（不図示）に接続されてもよい。この場合、メモリ取得部102は、例えば、メモリ部101bに対するデータの読み書きを制御するメモリコントローラ（不図示）を介して、メモリ部101bに保持されているデータを取得してもよい。なお、PCI（Peripheral Components Interconnect）バスに接続した拡張ハードウェアにより、コンピュータに実装されたメモリ装置（SDRAM：Synchronous Dynamic Random Access Memory）の内容を取得する技術が、下記参考文献1に開示されている。

[0073] （参考文献1）

Brian D. Carrier、Joe Grand、「A hardware-based memory acquisition procedure for digital investigations」、Digital Investigation Volume 1、Issue 1、February 2004、p. p. 50-60

解析対象装置101が仮想化基盤により提供されるVM等を用いて実現される場合を想定する。この場合、メモリ取得部102は、例えば、図3に例示するように、仮想化基盤において提供される、VMの動作を制御可能なソフトウェアであるVMM（Virtual Machine Monitor）300の機能を用いて実現されてもよい。より具体的には、メモリ取得部102は、VMM300の機能を利用したソフトウェア（ソフトウェア・プログラム）あるいは仮想的なデバイスにより実現されてもよい。

[0074] この場合、メモリ取得部102は、上記したように、VMMが提供する機能（例えば、特定のAPI等）や、データ（例えば、仮想的なメモリ部101bに記憶されたデータの保存領域を特定可能な情報等）を介して、当該メモリ部101bに記憶されるデータを取得（ダンプ）可能である。なお、メモリ領域データを取得する具体的な方法は、メモリ部101bの構成等に応じて周知の技術を適宜採用してよい。

[0075] また、上記図2及び図3に限らず、メモリ取得部102は、例えば、解析対象装置101自体にハードウェアもしくはソフトウェアもしくはハードウェアとソフトウェアの組合せによるメモリダンプ機能を組み込むことにより、実現されてもよい。この場合、メモリ取得部102は、例えば、解析対象装置において実行される任意のソフトウェアとして実現されてもよい。なお、メモリ取得部102自身はマルウェアあるいはマルウェアによる通信の解析処理を実行しないことから、マルウェアにより検知される危険性は比較的低い。

[0076] メモリ取得部102は、例えば、後述する通信処理部103（特には、暗号通信検査部103b）から、メモリ部101bに保持されたメモリ領域データの取得を指示するダンプ指示を受け付ける。メモリ取得部102は、当該ダンプ指示を受け付けたタイミングにおいて、メモリ部101bに保持されていたメモリ領域データをダンプする。

[0077] メモリ取得部102は、メモリ部101bに保持された全てのメモリ領域データ（即ち、メモリ部101bの全メモリ領域に保持されたデータ）をダンプしてもよい。また、メモリ取得部102は、メモリ部101bに保持されたデータの内、少なくとも一部のメモリ領域データをダンプしてもよい。

[0078] メモリ取得部102は、ダンプしたメモリ領域データを、後述するメモリダンプ保持部102aに保存（登録）する。

[0079] メモリ取得部102は、メモリ部101bからメモリ領域データをダンプする処理が完了した際、後述する通信処理部103（特には、暗号通信検査部103b）に、当該処理の完了を通知してもよい。

[0080] メモリダンプ保持部102aは、メモリ取得部102が取得したメモリ領域データを保持する。なお、メモリダンプ保持部102aは、メモリ部101bから取得したメモリ領域データと、当該メモリ領域データを取得したタイミングを表す情報とを、関連付けて保持してもよい。

[0081] （通信処理部103の構成）

次に、本実施形態における通信処理部103について説明する。まず、本

実施形態における通信処理部１０３の概要について説明する。

[0082] 通信処理部１０３は、解析対象装置１０１と、通信ネットワーク１０５との間に介在し、通信路１０６を介してそれぞれと通信可能に接続される。通信処理部１０３は、解析対象装置１０１と、通信ネットワーク１０５との間で送受信される通信データを解析した結果に基づいて、解析対象装置１０１と、通信ネットワーク１０５との間で通信データを中継する。特に、本実施形態における通信処理部１０３は、解析対象装置１０１と、通信ネットワーク１０５との間で実行される所定の暗号通信プロトコルを用いた暗号通信に関する通信データを中継可能である。

[0083] また、通信処理部１０３は、上記通信データを解析した結果に基づいて、メモリ取得部１０２に対して、解析対象装置１０１のメモリ部１０１ｂに保存されたメモリ領域データの取得を指示する。この際、通信処理部１０３は、解析対象装置１０１と、通信ネットワーク１０５との間の通信の一時的な停止及び再開を制御してもよい。

[0084] また、通信処理部１０３は、上記通信データを解析した結果に基づいて、当該通信データを保存する。

[0085] 通信処理部１０３は、例えば、複数の通信路１０６に接続された通信インタフェースを有するルータ、スイッチ、又は、アクセスポイント等のネットワーク機器であってもよい。また、通信処理部１０３は、それらの機能を実現可能なコンピュータ等の情報処理装置であってもよい。なお、係る通信処理部１０３は、物理的な装置としてのネットワーク機器や情報処理装置として実現されてもよい。また、係る通信処理部１０３は、特定の仮想化基盤においてネットワーク機器や情報処理装置を仮想化した仮想デバイスとして実現されてもよい。

[0086] 以下、通信処理部１０３の具体的な構成について説明する。

[0087] 通信処理部１０３は、図１に例示するように、通信制御部１０３ａ、暗号通信検査部１０３ｂを有する。通信処理部１０３は、通信データ記録部１０３ｄを有してもよい。なお、通信制御部１０３ａと、暗号通信検査部１０３

bと、通信データ記録部103dとの間は、それぞれ通信可能に接続されている。

[0088] 以下、通信処理部103の各構成要素について説明する。

[0089] 通信制御部103aは、上述したように、解析対象装置101と、通信ネットワーク105との間の通信を中継する。より具体的には、通信制御部103aは、解析対象装置101と、通信ネットワーク105を介して接続された他の情報通信装置107との間の通信を中継する。以下、解析対象装置101と、通信ネットワーク105との間の通信は、解析対象装置101と、通信ネットワーク105を介して接続された他の情報通信装置107との間の通信を含むことを想定する。解析対象装置101と、通信ネットワーク105との間の通信は、特定の暗号通信プロトコル（例えば、SSL等）により暗号化されていてもよい。

[0090] 通信制御部103aは、解析対象装置101から送信される通信データをキャプチャして、その通信データが表す通信内容（宛先情報、あるいは、通信プロトコルに関する情報等）を解析する。また、通信制御部103aは、通信ネットワーク105から受信した通信データをキャプチャしてその内容（宛先情報、あるいは、通信プロトコルに関する情報等）を解析する。通信制御部103aは、それらを解析した結果に基づいて、各通信データを、通信ネットワーク105と、解析対象装置101との間で転送する。

[0091] 例えば、通信ネットワーク105がインターネット等のIP（Internet Protocol）プロトコルを採用したネットワーク（IPネットワーク）である場合を想定する。この場合、通信制御部103aは、通信データを構成するIPパケットを解析することにより、当該通信データを、通信ネットワーク105と、解析対象装置101との間で転送可能である。なお、係る通信データの転送制御は、例えば、ルータやスイッチ等の周知のネットワーク機器と同様の技術を採用してよいので、詳細な説明は省略する。

[0092] 通信制御部103aは、解析対象装置101と、通信ネットワーク105

との間の通信を一時停止し、また、停止した当該通信を再開可能である。より具体的には、通信制御部 103a は、解析対象装置 101 と、通信ネットワーク 105 を介して接続された他の情報通信装置 107 との間の通信の停止及び再開を制御可能である。

[0093] 通信制御部 103a は、例えば、通信ネットワーク 105 又は解析対象装置 101 との間の通信路 106 が接続された図示しないネットワークインタフェースに対する通信データの書き込み（又は読み込み）の停止、あるいは、再開を制御する。これにより、通信制御部 103a は、解析対象装置 101 と、通信ネットワーク 105 との間の通信を制御可能である。ネットワークインタフェースに対する通信データの書き込み（又は読み込み）の制御は、当該ネットワークインタフェースあるいは通信処理部 103 の具体的構成に応じて周知の技術を適宜採用してよいので、詳細な説明は省略する。

[0094] 通信制御部 103a は、後述する暗号通信検査部 103b からの要求に基づいて、解析対象装置 101 と、通信ネットワーク 105 との間の通信を一時停止してもよい。同様に、通信制御部 103a は、後述する暗号通信検査部 103b からの要求に基づいて、当該停止した通信を再開してもよい。

[0095] 通信制御部 103a は、上記キャプチャした通信データを、後述する暗号通信検査部 103b に伝達（受け渡し）する。同様に、通信制御部 103a は、上記キャプチャした通信データを、後述する通信データ記録部 103d に伝達（受け渡し）してもよい。

[0096] 次に、暗号通信検査部 103b について説明する。

[0097] 暗号通信検査部 103b は、上記通信制御部 103a から受け付けた通信データを解析する。暗号通信検査部 103b は、当該解析結果と、後述する鍵データ取得ポリシ 103c とに基づいて、上記暗号通信プロトコルにおける通信路の暗号化に用いられる秘密情報を含むデータが、解析対象装置 101 におけるメモリ部 101b に存在するタイミングを判定する。

[0098] 係る秘密情報を含むデータは、一般的に、通信路の暗号化に用いられる鍵（以下、「暗号鍵」と称する場合がある）を含むデータ（以下「鍵データ」

と称する場合がある）である。係る暗号鍵は、暗号化された通信路において送受信される通信データを暗号化、あるいは、復号（解読）可能な鍵である。

[0099] 換言すると、暗号通信検査部 103b は、特定の暗号通信プロトコルに基づいて送受信される通信データを解析することにより、暗号鍵を含む鍵データが解析対象装置 101 のメモリ部 101b に存在するか否かを判定する。より具体的には、暗号通信検査部 103b は、上記通信データを解析することにより、上記鍵データが、解析対象装置 101 におけるメモリ部 101b に存在するタイミングを判定してもよい。

[0100] 例えば、SSL/TLS 等の暗号通信プロトコルにおいて、通信路の暗号化に用いる暗号鍵を交換する処理手順の進行状況は、通信データを解析することにより確認可能である。

[0101] 具体的には、SSL/TLS 等の暗号通信プロトコルにおいて、2 以上の通信端末において交換される暗号鍵自体（あるいは暗号鍵を導出可能な情報自体）は、PKI（public key infrastructure）等の技術を用いて保護（暗号化）される。このため、第三者が、暗号鍵自体（あるいは暗号鍵を導出可能な情報自体）を、通信路を介して取得することは困難である。

[0102] しかしながら、暗号通信検査部 103b は、通信データにおいて暗号化されていない部分を解析することにより、当該暗号通信プロトコルにおける暗号鍵の交換手順の進行状況を表す情報を確認可能である。例えば、暗号通信プロトコルが SSL であることを想定すると、通信データにおいて、Record プロトコルのヘッダ（Record ヘッダ）、及び、handshake プロトコルにおける一部のメッセージは暗号化されていない。このため、暗号通信検査部 103b は、例えば、通信データにおける当該部分を解析することにより、SSL プロトコルにおける暗号鍵を交換する処理手順の進行状況を確認可能である。

[0103] 例えば、SSL プロトコルにおいては、所定の手順が実行された際（具体

的には、ChangeCipherSpecメッセージが送受信された際）、通信路を暗号化する暗号鍵が、2つの通信端末において共有される。即ち、係る暗号鍵が共有されたタイミングにおいて、当該通信端末（例えば、解析対象装置101）のメモリ部には、係る暗号鍵を含む鍵データが保持されている可能性が高い。以上より、暗号通信検査部103bは、特定の暗号通信プロトコルに基づいて送受信される通信データを解析することにより、暗号鍵を含む鍵データが解析対象装置101のメモリ部101bに存在するタイミングを判定可能である。

[0104] また、暗号通信検査部103bは、通信データを解析することにより、上記暗号通信プロトコルにおける通信路の暗号化処理に用いられる各種情報（以下「暗号スイート」と称する場合がある）を取得してもよい。係る暗号スイートには、例えば、暗号アルゴリズム、暗号鍵の鍵長、暗号利用モード（後述）、通信データに対するメッセージ認証方式等を表す情報が含まれる。例えば、上記暗号通信プロトコルがSSLプロトコルである場合、暗号通信検査部103bは、ClientHelloメッセージ及びServerHelloメッセージを解析することにより、通信路の暗号化に用いられる暗号アルゴリズム等を特定可能である。

[0105] なお、SSLプロトコルにおいて用いられるRecordプロトコル、handshakeプロトコル、及び、各種メッセージ等は、周知の技術であることから、詳細な説明は省略する。

[0106] 暗号通信検査部103bは、上記したように、解析対象装置101と、他の情報通信装置107との間で暗号鍵を交換する処理手順の進行状況を確認する。これにより、暗号通信検査部103bは、当該暗号鍵を含む鍵データが解析対象装置101のメモリ部101bに存在するタイミングを判定する。より具体的には、暗号通信検査部103bは、鍵データ取得ポリシ103cに設定された情報を用いて、暗号鍵を含む鍵データが解析対象装置101のメモリ部101bに存在するタイミングを判定する。

[0107] 鍵データ取得ポリシ103cには、図4に例示するように、特定の暗号通

信プロトコル（図４における４０１）の種別と、鍵データ取得基準（図４における４０２）とが含まれる。なお、暗号通信プロトコル４０１に対して、鍵データ取得基準４０２が関連付けられる。上記鍵データ取得基準４０２は、少なくとも上記鍵データが解析対象装置１０１のメモリ部１０１ｂに存在するタイミングを判定可能な基準を表す情報である。

[0108] また、鍵データ取得ポリシ１０３ｃには更に、暗号通信検査部１０３ｂが実行する処理の内容（図４における４０３）が、含まれてもよい。処理内容４０３は、暗号通信プロトコル４０１に関連付けられる。処理内容４０３は、鍵データ取得基準４０２に基づいて上記鍵データが解析対象装置１０１のメモリ部１０１ｂに存在すると判定された場合に、暗号通信検査部１０３ｂが実行する処理の内容を表す情報である。

[0109] 暗号通信プロトコル４０１には、例えば、具体的な暗号通信プロトコルごとに、当該暗号通信プロトコルを識別可能な識別符号（ID: Identifier）が設定されてもよい。

[0110] 鍵データ取得基準４０２には、例えば、情報処理装置（コンピュータ）等による機械解釈が可能な任意の形式（書式）に基づいて表現された、上記特定のタイミングを判定可能な情報が登録されてもよい。なお、機械解釈可能な形式は任意に定めてよく、例えば、特定の符号の組合せや、構造化言語による表現等であってもよい。

[0111] 処理内容４０３には、例えば、機械解釈が可能な任意の形式（書式）に基づいて表現された、暗号通信検査部１０３ｂが実行する処理の内容を表す情報が登録されてもよい。

[0112] 例えば、図４に例示するように、暗号通信プロトコルが「SSL/TLS」である場合、鍵データ取得基準４０２に、「（SSL/TLSサーバからChangeCipherSpecが送信された後）、かつ、（Application Dataの送受信が開始する前）」というタイミングに関する情報が設定される。暗号通信検査部１０３ｂは、通信データを解析した結果、上記鍵データ取得基準４０２を満たすと判定した場合には、処理内容４

０３に登録された処理を実行する。

[0113] 鍵データ取得基準４０２には、例えば、暗号通信プロトコルにおいて、暗号鍵に関する特定の条件が成立するタイミングに関する情報が設定されてもよい。より具体的には、鍵データ取得基準４０２には、特定の暗号通信プロトコル４０１において、解析対象装置１０１と、他の情報通信装置１０７との間で暗号鍵が共有されるタイミングに関する情報が設定されてもよい。また、鍵データ取得基準４０２には、特定の暗号通信プロトコル４０１において、解析対象装置１０１と、他の情報通信装置１０７との間で、暗号鍵の共有に関する特定の手順が実行されたタイミングに関する情報が設定されてもよい。

[0114] 上記説明した鍵データ取得ポリシー１０３ｃは、任意の手法により暗号通信検査部１０３ｂに予め設定されていてもよい。

[0115] 暗号通信検査部１０３ｂは、鍵データ取得ポリシー１０３ｃ（特には鍵データ取得基準４０２）を参照して、解析対象装置１０１のメモリ部１０１ｂに暗号鍵を含む鍵データが存在するか否かを判定する。暗号通信検査部１０３ｂは、メモリ部１０１ｂに暗号鍵を含む鍵データが存在すると判定した場合には、上記説明したメモリ取得部１０２に対して、メモリ領域データの取得を指示することができる。

[0116] 即ち、暗号通信検査部１０３ｂは、通信データを解析し、鍵データ取得ポリシー１０３ｃに基づいて、解析対象装置１０１のメモリ部１０１ｂに暗号鍵を含む鍵データが存在するタイミングを判定する。当該タイミングにおいて、暗号鍵がメモリ部１０１ｂに存在する可能性が高い。このため、暗号通信検査部１０３ｂは、当該タイミングにおいて、メモリ取得部１０２に対してメモリ領域データの取得を指示する。この場合、メモリ取得部１０２が取得したメモリ領域データには、当該暗号鍵が含まれる可能性が高い。

[0117] また、暗号通信検査部１０３ｂは、解析対象装置１０１のメモリ部１０１ｂに上記鍵データが存在すると判定した場合には、上記説明した通信制御部１０３ａに対して、解析対象装置１０１と、通信ネットワーク１０５との間

の通信を（少なくとも一時的に）停止するよう指示することが可能である。

[0118] 仮に解析対象装置 101 と、通信ネットワーク 105 との間の通信が停止されずに続行された場合を想定する。この場合、上記鍵データが解析対象装置 101 のメモリ部 101b から失われてしまう可能性がある。また、当該通信が停止されずに続行された場合、通信プロトコルによっては、通信路の暗号化に用いられる暗号鍵が変更されてしまう可能性がある。

[0119] このため、暗号通信検査部 103b は、メモリ部 101b に上記鍵データが存在すると判定したタイミングにおいて、解析対象装置 101 と、通信ネットワーク 105 との間の通信の一時停止を通信制御部 103a に指示する。上記通信が停止されている間、メモリ部 101b に上記暗号鍵が保持されていることが期待される。よって、メモリ取得部 102 がこの間に取得したメモリ領域データには、上記鍵データが含まれることが期待される。

[0120] 換言すると、暗号通信検査部 103b は、上記暗号鍵がメモリ部 101b に保持される期間（時間）が延びるように、係る通信を一時停止してもよい。メモリ部 101b に上記鍵データが存在するタイミングにおいて、解析対象装置 101 と、通信ネットワーク 105 との間の通信を一時停止してからメモリ領域データを取得することにより、上記鍵データが含まれる可能性が高いメモリ領域データを取得することが可能である。

[0121] 暗号通信検査部 103b は、メモリ取得部 102 からメモリ領域データを取得する処理の完了を通知された際、解析対象装置 101 と、通信ネットワーク 105 との間の通信が停止している場合には、当該通信を再開するよう上記通信制御部 103a に指示してもよい。

[0122] なお、暗号通信検査部 103b は、解析対象装置 101 と、通信ネットワーク 105 との間の通信を再開するタイミングを適宜選択してよい。即ち、暗号通信検査部 103b は、メモリ取得部 102 から、メモリ領域データの取得完了を通知された際、上記通信を再開してもよい。また、暗号通信検査部 103b は、例えば、通信データの解読完了を暗号解析部 104（後述）から通知された際に、上記通信を再開してもよい。暗号通信検査部 103b

は、上記のように通信の再開タイミングを制御することにより、上記通信が停止される時間（期間）を必要最小限度に留めることが可能である。

[0123] 例えば、上記通信が停止される期間が長引いた場合、解析対象装置において通信処理を実行するプログラムにおいて通信エラー等として扱われ、係るプログラムによる処理が異常終了してしまう可能性がある。特に、係るプログラムがマルウェアである場合、当該マルウェアによる処理が終了してしまうと、その挙動を解析することが困難になる。これに対して、上記通信が停止される時間（期間）を必要最小限度に留めることで、例えばマルウェアによる処理を続行させつつ、その挙動を解析することが可能である。

[0124] 暗号通信検査部 103b は、上記通信制御部 103a に対して解析対象装置 101 と、通信ネットワーク 105 との間の通信の停止を指示してから特定の時間（例えば 30 秒等）が経過した際に、解析対象装置 101 と、通信ネットワーク 105 との間の通信の再開を指示してもよい。暗号通信検査部 103b は、上記特定の時間として適切な値を適宜選択してよい。例えば、メモリ取得部 102 がメモリ部 101b からメモリ領域データを取得するのに必要な時間を、事前実験や模擬実験を通じて予め算出することにより、暗号通信検査部 103b は、上記特定の時間として必要最小限の値を選択可能である。

[0125] 更に、暗号通信検査部 103b は、メモリ取得部 102 からメモリ領域データを取得する処理の完了を通知された際、後述する暗号解析部 104 に対して、後述する通信データ記録部 103d により保存された通信データの解読を指示してもよい。また、その際、暗号通信検査部 103b は、上記暗号通信プロトコルにおいて用いられる暗号アルゴリズムに関する情報を暗号解析部 104 に通知してもよい。通信データの解読に関する詳細な処理については、後述する。

[0126] 暗号通信検査部 103b は、後述する暗号解析部 104（特には暗号解読部 104d）から、通信データの解読処理が完了したことを表す通知を受け付けてもよい。その際、暗号通信検査部 103b は、解析対象装置 101 と

、通信ネットワーク１０５との間の通信が停止している場合には、当該通信を再開するよう上記通信制御部１０３ａに指示してもよい。

[0127] 暗号通信検査部１０３ｂは、暗号解析部１０４により解読された通信データを検査（解析）し、当該解析の結果に基づいて、特定の処理を実行する。暗号通信検査部１０３ｂは、係る特定の処理を適宜選択してよい。

[0128] 暗号通信検査部１０３ｂは、例えば、係る特定の処理として、解析対象装置１０１と通信ネットワーク１０５との間の通信の停止を通信制御部１０３ａに指示してもよい。また、暗号通信検査部１０３ｂは、例えば、係る特定の処理として、解析対象装置１０１と通信ネットワーク１０５との間で送受信されるデータを改変してもよい。また、暗号通信検査部１０３ｂは、例えば、マルウェア等に感知されないように、解析対象装置１０１と通信ネットワーク１０５との間の通信をそのまま続行させてもよい。なお、係る特定の処理は、解読された通信データに応じて、予め定められていてもよい。

[0129] 次に、通信データ記録部１０３ｄについて説明する。

[0130] 通信データ記録部１０３ｄは、通信制御部１０３ａにおいてキャプチャされた上記通信データを、通信データ記録ポリシー１０３ｅに基づいて、通信データ保持部１０３ｆに保存（登録）する。

[0131] 通信データ記録ポリシー１０３ｅは、通信制御部１０３ａにおいてキャプチャされた通信データの保存要否の判定に用いられる情報である。

[0132] より具体的には、通信データ記録ポリシー１０３ｅには、図５に例示するように、特定の暗号通信プロトコル（図５における５０１）の種別と、通信データ記録基準（図５における５０２）とが含まれる。なお、暗号通信プロトコル５０１に対して、通信データ記録基準５０２が関連付けられる。通信データ記録基準５０２は、暗号通信プロトコル５０１を用いて送受信される通信データの保存（記録）の要否を判定可能な基準（情報）である。

[0133] また、通信データ記録ポリシー１０３ｅには更に、通信データ記録部１０３ｄが実行する処理の内容（図５における５０３）が含まれてもよい。係る処理内容５０３は、暗号通信プロトコル５０１に対して関連付けされる。処理

内容 5 0 3 は、上記通信データ記録基準 5 0 2 を満たすと判定された場合に、通信データ記録部 1 0 3 d が実行する処理の内容を表す情報である。

[0134] 暗号通信プロトコル 5 0 1 には、例えば、具体的な暗号通信プロトコルごとに、当該暗号通信プロトコルを識別可能な識別符号（ID）が設定されてもよい。

[0135] 通信データ記録基準 5 0 2 には、例えば、機械解釈が可能な任意の形式（書式）に基づいて表現された、通信データの保存（記録）の可否を判定可能な情報が登録されてもよい。より具体的には、通信データ記録基準 5 0 2 には、例えば、通信データを保存する条件の成否、あるいは、通信データを保存するタイミングを判定可能な情報が登録されてもよい。

[0136] 処理内容 5 0 3 には、例えば、機械解釈が可能な任意の形式（書式）に基づいて表現された、通信データ記録部 1 0 3 d が実行する処理の内容を表す情報が登録されてもよい。

[0137] 例えば、図 5 に例示するように、暗号通信プロトコルが「SSL/TLS」である場合、通信データ記録基準 5 0 2 には「（Application Data の送受信が開始された後）」という情報が設定される。通信データ記録部 1 0 3 d は、通信データを解析した結果、上記通信データ記録基準 5 0 2 を満たすと判定した場合には、処理内容 5 0 3 に登録された処理を実行する。

[0138] なお、通信データ記録基準 5 0 2 には、例えば、暗号通信プロトコル 5 0 1 によって暗号化された通信路において最初の（暗号化された）通信データが送受信されるタイミング以降のデータを記録することを表す条件が設定されてもよい。

[0139] 上記したように、暗号通信プロトコルによっては、通信路の暗号化に用いる上記暗号鍵が所定のタイミングで変更される可能性がある。即ち、暗号化された通信路において最初の通信データと、2 回目以降の通信データとでは、通信路を暗号化する暗号鍵が異なる可能性がある。また、通信路が暗号化された後、最初の通信データにおいて機密度が高い情報（重要度が高い情報

）が送受信される可能性がある。このため、後述する暗号解析部 104 が全ての暗号通信のデータを解読できるように、通信路が暗号化された際、最初の通信データが送受信されるタイミングで当該通信データを保存することが有効である。

[0140] なお、通信データ記録基準 502 には、上記に限定されず、任意のタイミングを判断可能な情報が設定されてよい。

[0141] 上記説明した通信データ記録ポリシ 103 e は、任意の手法により通信データ記録部 103 d に予め設定されていてもよい。

[0142] 通信データ記録部 103 d は、上記説明した上記通信データ記録基準 502 を満たすと判定した通信データを、通信データ保持部 103 f に登録する。

[0143] 通信データ保持部 103 f は、例えば、図 6 に例示するように、各通信データについて、当該通信データの発信元に関する情報（図 6 の 601）、暗号通信プロトコルを表す識別情報（図 6 の 602）、及び、記録される通信データを表す記録データ（図 6 の 603）を関連付けて保持する。なお、記録データ 603 には、当該通信データをキャプチャした時刻等のタイミングを表す情報と、当該通信データの内容とが登録されてもよい。

[0144] （暗号解析部 104 の構成）

次に、本実施形態における暗号解析部 104 について説明する。まず、本実施形態における暗号解析部 104 の概要について説明する。

[0145] 暗号解析部 104 は、上記メモリ取得部 102 が取得したメモリ領域データを解析し、鍵データの特徴を表す情報（後述）に基づいて、当該メモリ領域データに含まれる上記暗号鍵の候補を抽出する。

[0146] 暗号解析部 104 は、上記通信データ記録部 103 d により保存された暗号化された通信データを、上記抽出した暗号鍵の候補を用いて復号した結果に基づいて、当該暗号鍵の候補の中から、正しい暗号鍵を抽出する。この場合、正しい暗号鍵は、暗号化された通信データを正しく復号可能な鍵である。なお、この際、暗号解析部 104 は、上記暗号通信プロトコルにおいて用

いられる暗号方式（暗号アルゴリズム）を特定してもよい。

[0147] 以下、暗号解析部 104 の具体的な構成について説明する。

[0148] 暗号解析部 104 は、鍵候補抽出部 104 a、及び、暗号解読部 104 d を有する。暗号解析部 104 を構成するこれらの構成要素の間は、それぞれ通信可能に接続されている。

[0149] まず、本実施形態における鍵候補抽出部 104 a について説明する。鍵候補抽出部 104 a は、鍵候補判定情報 104 b と、鍵候補保持部 104 c とを有する。

[0150] 鍵候補抽出部 104 a は、上記メモリダンプ保持部 102 a に登録されたメモリ領域データを参照し、鍵候補判定情報 104 b に基づいて、当該メモリ領域データから上記暗号鍵の候補を抽出する。即ち、鍵候補抽出部 104 a は、鍵候補判定情報 104 b に基づいて、メモリ領域データから、解析対象装置 101 と、通信ネットワーク 105 との間の暗号通信に用いられる暗号鍵の候補を含む鍵データの候補を抽出する。以下、係る鍵データの候補を、「鍵データ候補」と称する場合がある。なお、鍵候補抽出部 104 a は、鍵データ候補を抽出した際、当該処理の完了を、後述する暗号解読部 104 d に通知してもよい。

[0151] まず、鍵候補抽出部 104 a による、上記メモリ領域データにおける上記暗号鍵の探索について説明する。

[0152] 上記したように、メモリ領域データは、特定のタイミングにおいて解析対象装置 101 のメモリ部 101 b に保持されているデータである。即ち、メモリ取得部 102 がメモリ部 101 b から上記メモリ領域データを取得するタイミングにより、メモリ領域データの内容は変わる。このため、当該メモリ領域データの中で上記暗号鍵を含む鍵データを予め特定することは困難である。

[0153] また、解析対象装置 101 におけるメモリ部 101 b の記憶容量（メモリ空間のサイズ）が大きい場合、メモリ領域データも大きくなる。即ち、鍵候補抽出部 104 a は、巨大なサイズのデータの中から、暗号鍵を探索する必

要がある。仮に、1GB（単位：G i g a B y t e s）のメモリ領域データから、128ビット（単位：b i t）の暗号鍵を全探索する場合、その候補の数が膨大になることから、鍵データ候補を抽出する効率的な手法が必要とされる。

[0154] 上記暗号鍵を含む鍵データは、上記メモリ領域データに含まれるデータの中で、特有の特徴を示すことが多い。係る鍵データの特徴は、例えば、鍵データ自体の属性（例えば、データ自体のランダム性等）、あるいは、係る鍵データの上記メモリ領域データにおける配置パターン（配置される位置や、配置されるデータの並び）等を表す。

[0155] 上記鍵データの特徴は、暗号通信の実行に関する各種条件に応じて異なる。係る条件には、例えば、上記暗号通信プロトコルにおいて用いられる暗号方式（暗号アルゴリズム）、当該暗号方式に用いられる暗号パラメータ（後述）、あるいは、解析対象装置101における当該暗号方式に関する処理の実行環境（後述）等が含まれる。具体例として、例えば、特定の暗号アルゴリズムにおいて用いられる暗号鍵の鍵長が異なる場合、上記鍵データの特徴が異なる場合がある。また、例えば、各暗号アルゴリズムにおいて用いられる暗号利用モードによって、上記暗号鍵を含む暗号化処理に必要な情報が異なることから、上記鍵データの特徴が異なる場合がある。なお、暗号利用モードは、暗号アルゴリズムとしてブロック暗号を採用した場合に、ブロック長よりも長い平文を暗号化する場合の処理方法である。

[0156] 鍵候補抽出部104aは、上記メモリ領域データから、特定の鍵データの特徴に合致するデータを鍵データ候補として抽出する。これにより、鍵候補抽出部104aは、上記暗号鍵の候補を抽出可能である。

[0157] 例えば、暗号アルゴリズムに関する事前知識、あるいは、事前実験等に基づいて、上記各種条件の組合せごとに、予め上記鍵データの特徴を表す情報（データ）を収集することが可能である。そして、当該収集した上記鍵データの特徴を表すデータをパターン化することにより、メモリ領域データの中から上記鍵データ候補を抽出可能な判定情報を設けることが可能である。

[0158] 上記鍵データの特徴を表すデータを収集する具体的な方法は、適宜選択可能である。例えば、解析システムのユーザ、開発者、あるいは管理者等（以下、「ユーザ等」と称する）が、解析対象装置１０１において、暗号鍵を出力可能な実験用の暗号通信プログラムを実行する。そして、当該ユーザ等は、例えば、メモリ取得部１０２を用いて、当該実験用の通信プログラムが実行されている特定のタイミングにおいて、解析対象装置１０１のメモリ領域データを取得する。当該ユーザ等は、当該取得したメモリ領域データにおいて、実験プログラムから出力された（正しい）暗号鍵を探索する。このような実験を繰り返すことにより、暗号鍵が配置された領域に共通する特徴を抽出することが可能である。また、当該ユーザ等は、例えば、暗号方式に関する一般的な事前知識（例えば、暗号鍵の鍵長や、暗号鍵のランダム性等）に基づいて、記鍵データに特有の特徴を抽出することが可能である。

[0159] また、例えば、当該ユーザ等は、解析対象装置１０１において上記実験プログラムを実行した際に、解析対象装置１０１における暗号通信に用いられるＡＰＩをフックしてもよい。当該ユーザ等は、フックしたＡＰＩに渡される引数を解析することにより、暗号鍵を入手し、当該暗号鍵を表す鍵データの特徴を解析する。また、当該暗号鍵を表すデータが、解析対象装置におけるメモリ部１０１ｂのどこに配置されているかを調査する。当該ユーザ等は、そうして得られた調査結果を、上記鍵データの特徴を表すデータとして収集する。なお、ＡＰＩをフックする方法は、周知の技術であることから、詳細な説明を省略する。

[0160] なお、上記鍵データの特徴を表すデータを収集する方法は、上記具体例に限定されず、任意の方法を採用してよい。

[0161] 上記説明したように、上記各種条件に応じて、鍵データの特徴を表すデータを予め収集してパターン化することにより、メモリ領域データの中から上記鍵データ候補を抽出可能な判定情報を設けることが可能である。係る判定情報には、例えば、メモリ領域データにおいて鍵データ候補を探索（抽出）する位置（場所）や、特定のデータが鍵データか否かを判定可能な判定基準

等が設定されてもよい。

[0162] 本実施形態における鍵候補抽出部 104 a は、係る判定情報を用いてメモリ領域データから上記暗号鍵を含む鍵データ候補を抽出する。より具体的には、鍵候補抽出部 104 a は、上記暗号鍵を含む鍵データ候補を抽出可能な判定情報を有する鍵候補判定情報 104 b を用いて、鍵データ候補を抽出する。

[0163] 鍵候補判定情報 104 b は、図 7 に例示するように、暗号方式（暗号アルゴリズム）の種別を表す情報（図 7 における 701）と、鍵候補判定基準（図 7 における 704）とを有する。鍵候補判定基準 704 は、暗号アルゴリズム 701 に関連付けられる。係る鍵候補判定基準 704 は、メモリ領域データに含まれる特定のデータが、上記暗号鍵を含む鍵データに該当するか否かを判定可能な基準を表す情報である。換言すると、鍵候補判定基準 704 は、鍵データの特徴を表すデータに基づいて、メモリ領域データに含まれる特定のデータが、上記暗号鍵を含む鍵データに該当するか否かを判定可能な基準である。

[0164] また、鍵候補判定情報 104 b は、暗号アルゴリズム 701 に関連付けられた、当該暗号アルゴリズムに関する暗号パラメータ（図 7 の 702）と、解析対象装置 101 において暗号アルゴリズム 701 に関する暗号処理の実行環境を表す情報（図 7 の 703）と、を更に含んでもよい。

[0165] 暗号アルゴリズム 701 には、例えば、具体的な暗号アルゴリズムを識別可能な識別符号（ID）が設定されてもよい。

[0166] 鍵候補判定基準 704 には、例えば、機械解釈が可能な任意の形式（書式）に基づいて表現された情報が登録されてもよい。

[0167] 暗号パラメータ 702 は、図 7 に例示するように、暗号アルゴリズム 701 において用いられる鍵の長さ（鍵長）と、暗号利用モードに関する情報とを含んでもよい。暗号利用モードは、上記したように、暗号アルゴリズム 701 としてブロック暗号を採用した場合に、ブロック長よりも長い平文を暗号化する際の処理方法である。係る暗号モードとして、例えば、CBC（C

ipher Block Chaining) モードや、GCM (Galois/Counter Mode) 等が知られている。

[0168] 実行環境情報 703 は、例えば、解析対象装置 101 において、暗号アルゴリズム 701 に関する処理が実装されたライブラリに関する情報、及び、解析対象装置 101 の実行環境に関する情報等が設定される。より具体的には、実行環境情報 703 は、例えば、解析対象装置 101 の OS (例えば、Windows (登録商標)、Linux (登録商標) 等)、及び、暗号処理実装 (CGN (Cryptography Next Generation) API、OpenSSL 等) を特定可能な情報であってもよい。

[0169] 上記説明した鍵候補判定情報 104 b は、任意の手法により鍵候補抽出部 104 a に予め設定されていてもよい。

[0170] 上記のような鍵候補判定情報 104 b (特には鍵候補判定基準 704) に基づいて、鍵候補抽出部 104 a は、メモリ領域データに含まれる特定のデータ領域を、鍵候補として抽出するか否かを判定する。

[0171] 以下、鍵候補抽出部 104 a による、上記鍵データ候補の抽出処理について、図 7 に示す具体例を用いて説明する。

[0172] 例えば、図 7 に例示するように、暗号アルゴリズム 701 が「AES」、暗号パラメータ 702 の鍵長が「128ビット」又は「256ビット」、暗号利用モードが「CBC」の場合を仮定する。

[0173] この場合、鍵候補抽出部 104 a は、上記暗号アルゴリズム 701 及び暗号パラメータ 702 に関連付けされた鍵候補判定基準 704 を参照する。そして、鍵候補抽出部 104 a は、メモリダンプ保持部 102 a に保持されたメモリ領域データから、エントロピーが特定の基準値以上である連続した 16 バイト又は 32 バイトのデータ領域を抽出する。

[0174] 一般的に、あるデータ領域に含まれるデータが表す値のエントロピー (以下、「データのエントロピー」と称する場合がある) が大きいほど、そのデータ領域に含まれるデータが表す値のばらつきが大きい。また、暗号鍵は (規則性を見いだせない) 乱数値であることが多いことから、暗号鍵を含む鍵

データの値は、ばらつきが大きいと想定される。このため、図7に例示するような判定基準に基づいて、鍵候補抽出部104aは、ばらつきが大きい値を有するデータを含むデータ領域を、鍵データ候補として抽出可能である。

[0175] なお、係るバラつきの大きさは、既知の種々の計算方法を用いて算出可能である。具体的な一例として、鍵候補抽出部104aは、例えば、鍵データ候補の標準偏差（又は分散）を係るバラつきの大きさとして算出してもよい。標準偏差（又は分散）の算出方法は、周知の技術であることから、詳細な説明を省略する。

[0176] また、例えば、図7に例示するように、暗号アルゴリズム701が「AES」、暗号パラメータ702の鍵長が「128ビット（単位：bit）」、暗号利用モードが「GCM」の場合を仮定する。

[0177] この場合、鍵候補抽出部104aは、上記暗号アルゴリズム701及び暗号パラメータ702に関連付けされた鍵候補判定基準704を参照し、メモリ領域データから、「0x30、0x02、0x00、0x00、0x4b、0x53、0x53、0x4Dから開始する連続した560バイト（単位：byte）のデータ」に該当すると判定したデータを抽出する。例えば、解析対象装置101における特定の実行環境において、暗号鍵を含む鍵データは、特定の配置パターンを有する場合がある。図7に例示するように、このような配置パターンを鍵候補判定基準704として登録することにより、鍵候補抽出部104aは、係る配置パターンに合致するデータを、鍵データ候補として抽出可能である。

[0178] 鍵候補抽出部104aは、例えば、メモリ領域データの特定の位置（例えば先頭）から、順次特定のサイズ（例えば1バイト）ずつシフトしながら、特定のサイズのデータを抽出し、鍵候補判定基準704に基づいて、当該データが鍵候補に該当するか否かを判定してもよい。

[0179] 暗号通信検査部103bが、ある暗号通信に関する通信データを解析した結果から、暗号スイートに関する情報を取得可能である場合を想定する。この場合、当該暗号通信に関する暗号アルゴリズム701及び暗号パラメータ

702の情報は、通信データから判明する既知の情報として扱うことができる。また、解析対象装置101に関する実行環境情報703は、暗号解析部104に予め設定する等の方法により、既知の情報として扱うことができる。

[0180] なお、暗号アルゴリズム701及び暗号パラメータ702が不明である場合、鍵候補抽出部104aは、鍵候補判定情報104bに登録された全ての鍵候補判定基準704を用いて、それぞれの基準に適合する鍵データ候補を抽出してもよい。この場合、後述する暗号解読部104dが、暗号化された通信データを、上記抽出した鍵データ候補を用いて解読した結果に基づいて、当該通信データの暗号化に用いられる暗号鍵を含む鍵データ、暗号アルゴリズム、及び、暗号パラメータを特定することが可能である。

[0181] また、鍵候補抽出部104aは、鍵データ候補を抽出すると共に、特定の暗号通信プロトコルにおいて通信データを暗号化あるいは復号する処理に用いられるその他の必要な情報（以下、「暗号処理データ」と称する場合がある）を取得してもよい。

[0182] 係る暗号処理データには、例えば、以下のようなデータが含まれてもよい。即ち、係る暗号処理データには、暗号アルゴリズムとしてブロック暗号が用いられる場合の初期化ベクタ（`IV: Initialization Vector`）が含まれてもよい。また、係る暗号処理データには、特定の暗号利用モードにおいて用いられる各種パラメータ（例えば、カウンタモードにおけるカウンタ、`nonce (number used once: 一度のみ使用される使い捨ての値)`等）が含まれてもよい。また、係る暗号処理データには、暗号化された通信データに付与される認証情報等が含まれてもよい。なお、係る暗号処理データには、上記に限定されず、暗号アルゴリズムや暗号パラメータ等に応じて必要となる任意のデータが含まれてもよい。

[0183] 鍵候補抽出部104aは、例えば、暗号通信検査部103bあるいは通信制御部103aから通信データを取得し、当該通信データを解析することにより、係る暗号処理データを取得してもよい。また、鍵候補抽出部104a

は、例えば、上記鍵データ候補と同様、特定の判断基準に基づいて、メモリダンプ保持部 102a に保持されたメモリ領域データの中から、暗号処理データを取得してもよい。

[0184] 鍵候補抽出部 104a は、メモリ領域データから抽出した鍵データ候補を、鍵候補保持部 104c に保存（登録）する。また、鍵候補抽出部 104a は、当該鍵データ候補に関連する暗号処理データを、鍵候補保持部 104c に保存（登録）してもよい。

[0185] 鍵候補保持部 104c は、図 8 に例示するように、暗号アルゴリズム 801 ごとに、抽出した鍵データ候補 803 を関連付けて保持する。なお、鍵候補保持部 104c は、暗号アルゴリズム 801 ごとに、当該暗号アルゴリズムにおいて用いられる暗号パラメータ 802 を関連付けて保持してもよい。また、鍵候補保持部 104c は、鍵データ候補 803 の一部に、上記暗号処理データを併せて保持してもよい。なお、上記に限らず、鍵候補保持部 104c は、鍵データ候補 803 とは別の、図示しない領域に、上記暗号処理データを保持してもよい。

[0186] 鍵候補保持部 104c は、図 8 に例示するように、特定の暗号アルゴリズム（例えば「AES」）に関する鍵データ候補を、複数保持してもよい。なお、図 8 に例示された構成は 1 つの具体例であり、本実施形態における鍵候補保持部 104c はこの構成には限定されない。

[0187] 次に、本実施形態における暗号解読部 104d について説明する。

[0188] 暗号解読部 104d は、図 1 に例示するように、解析結果判定情報 104e、及び、解析結果保持部 104f を有する。

[0189] 暗号解読部 104d は、鍵候補抽出部 104a において鍵データ候補が抽出された際、当該鍵データ候補を用いて、通信データ保持部 103f に保存された（暗号化された）通信データを解読（復号）する。

[0190] 暗号解読部 104d は、通信データ保持部 103f に保存された（暗号化された）通信データを参照し、鍵候補保持部 104c に保存された鍵データ候補を用いて、当該暗号化された通信データを解読（復号）する。即ち、暗

号解読部 104 d は、鍵候補保持部 104 c に保存された鍵データ候補を用いて、解析対象装置 101 と、通信ネットワーク 105 との間の暗号通信において送受信される通信データを解読（復号）する。なお、暗号解読部 104 d は、必要に応じて、鍵データ候補と、鍵候補抽出部 104 a が取得した暗号処理データとを用いて、通信データを解読（復号）してもよい。以下においては、解読（復号）された通信データを、「解読済み通信データ」と称する場合がある。

[0191] 暗号解読部 104 d は、解読済み通信データの特徴を表すデータに基づいて、当該解読済み通信データが正しく解読（復号）されたか否かを判定する。係る解読済み通信データの特徴を表すデータは、例えば、当該解読済み通信データ自体の属性（例えば、データ自体のランダム性）、あるいは、当該解読済み通信データのデータフォーマット等を表す。

[0192] 具体的には、暗号解読部 104 d は、解析結果判定情報 104 e に基づいて、特定の鍵データ候補による通信データの解読結果の成否を判定する。そして、暗号解読部 104 d は、通信データの解読に成功した場合、当該解読に用いた鍵データを、解析結果保持部 104 f に保存（登録）する。また、暗号解読部 104 d は、当該鍵データと共に、解読に使用した暗号処理データを解析結果保持部 104 f に保存（登録）してもよい。

[0193] なお、以下においては、解析結果判定情報 104 e に基づいて、通信データの解読に成功したと判定された鍵データを、「正しい鍵データ」と称する場合がある。

[0194] 解析結果判定情報 104 e は、図 9 に示すように、解析結果判定基準 901 と、判定結果 902 とを含む。

[0195] 解析結果判定基準 901 には、解読済み通信データの特徴を表すデータに基づいて、当該解読済み通信データが正しく解読（復号）されたか否かを判定可能な基準を表す情報が設定される。この場合、解析結果判定基準 901 に設定される情報は、例えば、機械解釈が可能な任意の形式（書式）に基づいて表現されてもよい。

- [0196] 判定結果 902 には、暗号解読部 104d が特定の通信データを解読した結果が、解析結果判定基準 901 を満たした場合の判定結果（解読成功か否か）が設定される。この場合、判定結果 902 には、係る判定結果を表す符号等が登録されてもよい。
- [0197] 上記のような解析結果判定基準 901 に基づいて、暗号解読部 104d は、通信データの復号が成功したか否かを判定する。以下、暗号解読部 104d による通信データの解読成否の判定について、図 9 に示す具体例を用いて説明する。
- [0198] 図 9 に示す具体例においては、暗号解読部 104d は、例えば、解読済み通信データのエントロピーが特定の基準値以下である場合に、当該解読済み通信データが正しく復号されたと判定する。
- [0199] また、上記とは逆に、例えば、解読済み通信データのエントロピーが特定の基準値より大きい場合、暗号解読部 104d は、当該通信データの解読に失敗したと判定する。
- [0200] 上記したように、一般的にデータのエントロピーが大きいほど、データ領域に含まれるデータが表す値のばらつきが大きい。即ち、解読済み通信データのエントロピーが特定の基準値以下の場合、解読済み通信データに含まれるデータが表す値のばらつきがある程度小さいことから、解読に成功した可能性が高い。逆に、解読済み通信データのエントロピーが特定の基準値よりも大きい場合、解読済み通信データに含まれるデータが表す値のばらつきが大きい（即ち、ランダム性が高い）ことから、解読に失敗した可能性が高い。なぜならば、一般的に暗号化されたデータ（通信データ）は、（規則性を見いだせない）乱数値であることが多く、そのようなデータが表す値は、ばらつきが大きいからである。
- [0201] なお、上記説明した、データのばらつき程度（エントロピー）の大小を判定する特定の基準値は、通信データ自体の一般的な特性（ランダム性）に関する知識、あるいは、事前実験等により適宜選択してよい。
- [0202] 例えば、係るデータのばらつき度合いを表す基準として、標準偏差 σ を用

いることが可能である。データのばらつきが正規分布に従うと仮定すると、データの平均値を「 m 」として「 $m \pm \sigma$ 」の範囲に全体の約 68.2%、「 $m \pm 2\sigma$ 」の範囲に、全体の約 95.4%のデータが含まれる。即ち、この σ の値が大きい場合、解読済み通信データは、極めてばらつきが大きい（ランダム性が高い）。この場合、暗号解読部 104 d は、解読済み通信データのばらつきがある程度小さい場合に解読が成功したと判定するよう、係る σ の値を適宜選択してよい。

[0203] また、例えば、図 9 に例示するように、解読済み通信データが特定のデータを含むか否かを、当該解読済み通信データの解読の成否を判定する基準としてもよい。解読済み通信データが既知のデータや、特定のパターンを含む場合、当該解読済み通信データは正しく解読されている可能性が高いからである。

[0204] また、上記以外にも、例えば、解読済み通信データが特定のデータフォーマット（各種データを表現可能な表現形式）に適合するか否かを、当該解読済み通信データの解読の成否を判定する基準としてもよい。係るデータフォーマットは、例えば、各種の音声、静止画像、動画、ドキュメント（文書）等を表すデータフォーマットであってもよい。また、係るデータフォーマットは、例えば特定のファイルシステムにおけるファイルフォーマットであってもよい。なお、図 9 に示す具体例は一つの例示であり、本実施形態はこれには限定されない。

[0205] 上記説明した解析結果判定情報 104 e は、任意の手法により暗号解読部 104 d に予め設定されていてもよい。

[0206] 暗号解読部 104 d は、例えば、鍵候補保持部 104 c に保存された全ての鍵データ候補を用いて通信データの解読処理を行い、その結果を上記解析結果判定情報 104 e に基づいて判定する。これにより、暗号解読部 104 d は、正しい鍵データを抽出可能である。暗号解読部 104 d は、通信データ保持部 103 f に保存されている全ての通信データに対して、上記説明した暗号解読処理を実行してもよい。

[0207] 暗号解読部 104 d は、解析結果判定情報 104 e に基づいて通信データを解読した結果から、正しい鍵データと、当該正しい鍵データにより解読された解読済み通信データとを、解析結果保持部 104 f に保存（登録）する。なお、暗号解読部 104 d は、暗号通信検査部 103 b に、上記説明した通信データの解読処理の完了を通知してもよい。

[0208] 解析結果保持部 104 f は、図 10 に例示するように、暗号アルゴリズムを特定可能な情報（図 10 の暗号アルゴリズム 1001）と、正しい鍵データ（図 10 の鍵データ 1002）と、解読済み通信データ（図 10 の解読結果 1003）とを関連付けて保持する。なお、図 10 に例示された構成は 1 つの具体例であり、本実施形態における解析結果保持部 104 f は、これには限定されない。例えば、解析結果保持部 104 f は、正しい鍵データのみ、あるいは、解読済み通信データのみを保持してもよく、これらを別々に保持してもよい。また、解析結果保持部 104 f は、鍵データ 1002 の一部として、上記正しい鍵データと共に通信データの解読に用いた暗号処理データを保持してもよい。なお、解析結果保持部 104 f は、鍵データ 1002 とは別の図示しない領域に、当該暗号処理データを保持してもよい。

[0209] （解析システム 100 の動作）

次に、上記のように構成された解析システム 100 の動作について説明する。なお、以下の説明においては、具体例として、解析対象装置 101 と、通信ネットワーク 105 との間の暗号通信プロトコルが、SSL であることを想定する。

[0210] 図 11 を参照して、解析システム 100 の動作の概要について説明する。

[0211] まず、通信処理部 103 が、解析対象装置 101 と、通信ネットワーク 105 との間で送受信される通信データをキャプチャする（ステップ S1101）。

[0212] 次に、通信処理部 103 が、上記キャプチャした通信データを解析し、鍵データが解析対象装置 101 におけるメモリ部 101 b に存在するタイミングを判定する（ステップ S1102）。

- [0213] ステップS 1 1 0 2において、当該タイミングが到来したと判定された場合（ステップS 1 1 0 3においてY E S）、メモリ取得部 1 0 2は、解析対象装置 1 0 1におけるメモリ部 1 0 1 bが保持するメモリ領域データを取得する（ステップS 1 1 0 4）。なお、ステップS 1 1 0 3における判定結果がN Oの場合、ステップS 1 1 0 1に戻って、通信処理部 1 0 3が処理を続行する。
- [0214] 次に、暗号解析部 1 0 4が、ステップS 1 1 0 4において取得されたメモリ領域データを特定の基準に基づいて解析し、鍵データ候補を抽出する（ステップS 1 1 0 5）。
- [0215] 次に、暗号解析部 1 0 4が、ステップS 1 1 0 5において抽出した鍵データ候補を用いて通信データを解読した結果に基づいて、正しい鍵データ及び解読された通信データを得る（ステップS 1 1 0 6）。
- [0216] 次に、通信処理部 1 0 3（特には暗号通信検査部 1 0 3 b）は、上記ステップS 1 1 0 6にておいて得られた、解読済み通信データの内容を解析し、特定の処理を実行する（ステップS 1 1 0 7）。通信処理部 1 0 3（特には暗号通信検査部 1 0 3 b）は、上記説明したように、係る特定の処理を適宜選択してよい。
- [0217] なお、ステップS 1 1 0 1において通信データをキャプチャした通信処理部 1 0 3は、当該通信データの保存要否を判定し、当該判定結果に基づいて通信データを保存する（ステップS 1 1 0 8）。ステップS 1 1 0 8における処理は、ステップS 1 1 0 2乃至ステップS 1 1 0 5における処理と並行して実行されてもよい。
- [0218] 次に、上記説明した解析システム 1 0 0の動作の詳細について説明する。
- [0219] まず、図 1 2 A及び図 1 2 Bに例示するフローチャートを参照して、メモリ取得部 1 0 2、及び、通信処理部 1 0 3の動作について説明する。以下、図 1 2 Aに例示するフローチャートについて説明する。図 1 2 Bは、後述するステップS 1 2 0 9 B及びステップS 1 2 1 0 Bを除いて、図 1 2 Aと同様のフローチャートであるため、相違点のみ説明する。なお、以下のステッ

プS 1 2 0 1乃至S 1 2 0 8に例示する処理は、図 1 1に例示するステップ S 1 1 0 1乃至S 1 1 0 5に相当する。

[0220] まず、通信制御部 1 0 3 aが、解析対象装置 1 0 1と、通信ネットワーク 1 0 5との間で送受信される通信データをキャプチャする（ステップS 1 2 0 1）。

[0221] この場合、上記説明したように、通信制御部 1 0 3 aは、解析対象装置 1 0 1から通信ネットワーク 1 0 5に向けて送信される通信データ、及び、通信ネットワーク 1 0 5から解析対象装置 1 0 1宛てに送信された通信データの両方をキャプチャ可能である。

[0222] 次に、暗号通信検査部 1 0 3 bが、上記ステップS 1 2 0 1においてキャプチャした通信データを解析し、鍵データ取得ポリシー 1 0 3 cに基づいて、メモリ部 1 0 1 bに記憶されているメモリ領域データを取得するか否かを判定する（ステップS 1 2 0 2）。

[0223] より具体的には、暗号通信検査部 1 0 3 bは、鍵データ取得ポリシー 1 0 3 cを参照して、解析対象装置 1 0 1のメモリ部 1 0 1 bに鍵データが存在するタイミングを判定する。

[0224] 暗号通信プロトコルとしてSSLが採用されている場合、暗号通信検査部 1 0 3 bは、例えば、図 1 3に示すSSLプロトコルの処理シーケンスにおいて、解析対象装置 1 0 1が、SSLサーバ側（他の情報通信装置 1 0 7側）からChangeCipherSpecメッセージを受信した際（図 1 3に例示する「停止タイミングT 1」）、係るタイミングが到来したと判定してもよい。

[0225] なお、暗号通信検査部 1 0 3 bは、解析対象装置 1 0 1が、SSLサーバ側（他の情報通信装置 1 0 7側）からFinishedメッセージを受信した際（図 1 3に例示する「停止タイミングT 2」）、係るタイミングが到来したと判定してもよい。

[0226] 上記ステップS 1 2 0 2において、暗号通信検査部 1 0 3 bが、当該タイミングが到来したと判定した場合（ステップS 1 2 0 3においてYES）、

暗号通信検査部 103b は、通信制御部 103a に対して、解析対象装置 101 と、通信ネットワーク 105 との間の通信を停止するよう指示する（ステップ S1204）。

[0227] この場合、当該指示を受け付けた通信制御部 103a は、解析対象装置 101 と、通信ネットワーク 105 との間の通信を一時停止する。係る通信を停止する具体的な方法は、適宜選択してよい。

[0228] なお、上記ステップ S1203 において NO の場合、ステップ S1201 に戻って、通信制御部 103a が処理を続行する。

[0229] 次に、暗号通信検査部 103b は、メモリ取得部 102 に対して、解析対象装置 101 のメモリ部 101b に記憶（保持）されたメモリ領域データの取得を指示する（ステップ S1205）。

[0230] 係る指示を受け付けたメモリ取得部 102 は、解析対象装置 101 のメモリ部 101b に記憶（保持）されたメモリ領域データをダンプする（ステップ S1206）。メモリ部 101b に保持されたデータの具体的なダンプ方法は、上記説明した通り、解析対象装置 101 の構成に応じて適宜選択してよい。

[0231] 次に、メモリ取得部 102 は、上記取得したメモリ領域データを、メモリダンプ保持部 102a に保存（登録）する（ステップ S1207）。

[0232] 次に、メモリ取得部 102 は、暗号通信検査部 103b に対して、メモリ領域データの取得が完了したことを通知する（ステップ S1208）。

[0233] 次に、上記ステップ S1208 における通知を受け付けた暗号通信検査部 103b は、通信制御部 103a に対して、一時停止している通信の再開を指示する。そして、通信制御部 103a が、当該通信を再開する（ステップ S1209）。

[0234] なお、上記ステップ S1208 が実行されない場合、暗号通信検査部 103b は、上記ステップ S1204 において通信の停止を指示してから特定の時間が経過した際に、通信制御部 103a に対して、一時停止している通信の再開を指示してもよい。

- [0235] 上記ステップS 1 2 0 9における処理の後、暗号通信検査部 1 0 3 bは、暗号解析部 1 0 4 に対して、通信データ記録部 1 0 3 dにより保存された通信データの解読と、暗号鍵の抽出とを指示してもよい（ステップS 1 2 1 0）。この際、通信データを解析した結果から、暗号通信プロトコルにおいて用いられる暗号アルゴリズム等が判明している場合、暗号通信検査部 1 0 3 bは、暗号解析部 1 0 4 に対して、当該暗号アルゴリズムに関する情報を提供してもよい。
- [0236] なお、上記説明した図 1 2 AにおけるステップS 1 2 0 9、及びステップS 1 2 1 0の処理順序は逆であってもよい。即ち、図 1 2 Bに例示するように、上記ステップS 1 2 0 8における通知を受け付けた暗号通信検査部 1 0 3 bは、暗号解析部 1 0 4 に対して、通信データ記録部 1 0 3 dにより保存された通信データの解読と、暗号鍵の抽出とを指示してもよい（ステップS 1 2 0 9 B）。そして、暗号通信検査部 1 0 3 bは、暗号解析部 1 0 4 から、通信データの解読処理の完了を通知された際に、通信制御部 1 0 3 a に対して、一時停止している通信の再開を指示してもよい（ステップS 1 2 1 0 B）。
- [0237] 次に、通信処理部 1 0 3（特に、通信データ記録部 1 0 3 d）の処理について、図 1 4 に例示するフローチャートを参照して説明する。なお、以下のステップS 1 4 0 1 乃至ステップS 1 4 0 4 は、上記図 1 1 に例示したステップS 1 1 0 8 に相当する。
- [0238] まず、図 1 4 に示すステップS 1 2 0 1 において、通信制御部 1 0 3 a が、通信データをキャプチャする。係る処理は、図 1 2 A 及び図 1 2 B に例示するステップS 1 2 0 1 と同様としてよい。
- [0239] 次に、通信制御部 1 0 3 a は、キャプチャした通信データを、通信データ記録部 1 0 3 d に伝達（通知）する（ステップS 1 4 0 1）。
- [0240] 通信データ記録部 1 0 3 d は、通信データ記録ポリシー 1 0 3 e に基づいて、ステップS 1 2 0 1 においてキャプチャされた通信データを保存するか否かを判定する（ステップS 1 4 0 2）。

- [0241] 通信プロトコルとしてSSLが採用された場合、通信データ記録ポリシー103e（特には通信データ記録基準502）には、例えば、図13に例示する最初のApplicationDataメッセージが送信されるタイミングである「T3」以降の通信データを保存（記録）することを表す条件が設定されてもよい。なお、通信データ記録ポリシー103e（特には通信データ記録基準502）には、例えば、図13に例示する「停止タイミングT1」、あるいは、「停止タイミングT2」以降の通信データを保存（記録）することを表す条件が設定されてもよい。
- [0242] ステップS1402における判定の結果、通信データを保存する場合（ステップS1403においてYES）、通信データ記録部103dは、当該通信データを通信データ保持部103fに登録（保存）する（ステップS1404）。
- [0243] なお、ステップS1403においてNOの場合、通信データ記録部103dは、当該通信データを保存しなくともよい。
- [0244] 上記ステップS1401乃至S1404の処理によって、通信データが必要に応じて通信データ保持部103fに保存される。
- [0245] 次に、暗号解析部104の処理について、図15及び図16に例示するフローチャートを参照して説明する。なお、図15及び図16に例示するフローチャートは、図11におけるステップS1105乃至S1106に相当する。
- [0246] まず、図15に例示するフローチャートを参照して、鍵候補抽出部104aの動作について説明する。
- [0247] 上記したように、例えば、暗号通信検査部103bからの指示（ステップS1210）に応じて、暗号解析部104は、暗号化された通信データの解読処理を開始する。
- [0248] まず、鍵候補抽出部104aは、メモリダンプ保持部102aに登録（保存）されたメモリ領域データを参照する（ステップS1501）。この場合、鍵候補抽出部104aは、メモリダンプ保持部102aから、当該メモリ

領域データを取得してもよい。

[0249] 次に、鍵候補抽出部 104 a は、鍵候補判定情報 104 b に基づいて、ステップ S 1501 において参照（取得）したメモリ領域データから暗号鍵の候補を抽出する（ステップ S 1502）。

[0250] 上記説明したように、暗号通信検査部 103 b から、暗号アルゴリズムに関する情報が提供された場合、鍵候補抽出部 104 a は、当該暗号アルゴリズムに関連付けされた鍵候補判定基準 704 を用いて、メモリ領域データから鍵データ候補を抽出する。

[0251] 暗号アルゴリズムが不明である場合には、鍵候補判定情報 104 b に登録された全ての暗号アルゴリズム 701 について、鍵候補判定基準 704 に基づいて鍵データ候補を抽出する。

[0252] また、この際、鍵候補抽出部 104 a は、鍵データ候補に関連付された暗号アルゴリズムに関する情報（例えば、暗号アルゴリズム 701、及び、暗号パラメータ 702）を抽出してもよい。

[0253] 次に、鍵候補抽出部 104 a は、ステップ S 1502 において抽出した鍵候補、及び、暗号アルゴリズムに関する情報を、鍵候補保持部 104 c に登録（保存）する（ステップ S 1503）。

[0254] ステップ S 1503 の後、鍵候補抽出部 104 a は、暗号解読部 104 d に対して鍵候補の抽出処理が完了したことを通知してもよい（ステップ S 1504）。

[0255] 次に、暗号解読部 104 d は、上記ステップ S 1501 乃至 S 1503 において抽出された鍵データ候補を用いて、暗号化された通信データを解読する処理を実行する（ステップ S 1505）。

[0256] 以下、ステップ S 1505 における処理の詳細について、図 16 に例示するフローチャートを参照して説明する。

[0257] まず、暗号解読部 104 d は、鍵候補保持部 104 c に登録された鍵データ候補（図 8 の 803）を取得する（ステップ S 1601）。なお、この際、暗号解読部 104 d は、当該鍵候補と関連付けされた暗号アルゴリズムに

関する情報（図8の801及び802）を取得してもよい。また、暗号解読部104dは、当該鍵候補に関連付けされた暗号処理データを取得してもよい。

[0258] 次に暗号解読部104dは、通信データ保持部103fに登録（保存）された、暗号化された通信データを参照する。この場合、暗号解読部104dは、当該通信データを、通信データ保持部103fから取得してもよい。

[0259] そして、暗号解読部104dは、上記ステップS1601において参照（取得）した鍵データ候補及び暗号アルゴリズムに関する情報を用いて、当該取得した通信データを解読（復号）する（ステップS1602）。

[0260] 次に、暗号解読部104dは、ステップS1602において通信データを解読（復号）した結果である解読済通信データが、正しく解読（復号）されたか否かを、解析結果判定情報104eに基づいて判定する（ステップS1603）。

[0261] 上記説明したように、暗号解読部104dは、例えば、解読済み通信データのエントロピーの値、あるいは、解読済み通信データが特定のデータフォーマットに合致するか否か、等に基づいて、解読済通信データが、正しく解読されたか否かを判定してもよい。

[0262] 解読済通信データが正しく解読されたと判定した場合（ステップS1604においてYES）、暗号解読部104dは、正しい鍵データと、解読済み通信データとを、解析結果保持部104fに登録する（ステップS1606）。

[0263] 解読済通信データが正しく解読されなかったと判定した場合（ステップS1604においてNO）、暗号解読部104dは、鍵候補保持部104cに他の鍵データ候補が登録されているか確認する（ステップS1605）。

[0264] 他の鍵データ候補が登録されている場合（ステップS1607においてYES）、暗号解読部104dは、ステップS1601から処理を続行し、当該他の鍵データ候補を鍵候補保持部104cから取り出す。

[0265] 上記ステップS1601乃至S1607の処理により、通信データを解読

可能な暗号鍵を含む鍵データと、解読された通信データとが得られる。

[0266] なお、暗号解読部 104 d は、上記説明した通信データの解読処理の完了を、暗号通信検査部 103 b に通知してもよい（ステップ S 1608）。

[0267] 上記ステップ S 1608 における通知を受け付けた暗号通信検査部 103 b は、上記説明したステップ S 1107 から処理を続行する。この場合、暗号通信検査部 103 b は、解読された通信データを解析した結果に基づいて、特定の処理を実行可能である。

[0268] 以上のように構成された本実施形態における解析システム 100 においては、まず、通信処理部 103 が、解析対象装置 101 と、通信ネットワーク 105 との間で特定の暗号通信プロトコルに基づいて送受信される通信データを解析する。そして、通信処理部 103 は、係る解析の結果に基づいて、解析対象装置 101 と、通信ネットワーク 105 との間の通信路を暗号化する暗号鍵が、解析対象装置 101 のメモリ部 101 b に存在するタイミングを特定する。

[0269] 通信処理部 103 は、当該タイミングにおいて、メモリ部 101 b に記憶されたメモリ領域データの取得を、メモリ取得部 102 に対して指示する。

[0270] 以上より、本実施形態における解析システム 100 によれば、メモリ取得部 102 は、解析対象装置 101 と、通信ネットワーク 105 との間の通信路を暗号化する暗号鍵を含むメモリ領域データを、解析対象装置 101 のメモリ部 101 b から取得可能である。

[0271] また、通信処理部 103（特には暗号通信検査部 103 b）は、上記特定のタイミングにおいて、通信制御部 103 a に対して、解析対象装置 101 と、通信ネットワーク 105 との間の通信を一時的に停止するよう指示可能である。これにより、本実施形態における通信処理部 103 は、上記暗号鍵がメモリ部 101 b に保持される期間を延ばすことが可能である。なぜならば、解析対象装置 101 と、通信ネットワーク 105 との間の通信が一時停止されることにより、通信処理の進行に伴う暗号鍵の消失や変更等が発生せず、メモリ部 101 b に上記暗号鍵が保持されていることが期待されるから

である。このため、本実施形態における解析システム１００によれば、当該暗号鍵を含む可能性が高いメモリ領域データを取得することが可能である。

[0272] また、本実施形態における解析システム１００においては、暗号解析部１０４が、上記取得したメモリ領域データの中から、暗号鍵を含む鍵データの特徴を表すデータ（鍵候補判定情報１０４ｂ）に基づいて、暗号鍵の候補（鍵データ候補）を抽出する。そして、暗号解析部１０４は、解析結果判定情報１０４ｅに基づいて、上記抽出した鍵データ候補を用いて通信データを解読（復号）した結果の成否を判定する。暗号解析部１０４は、係る判定結果に基づいて、正しい暗号鍵を含む鍵データと、解読された通信データを取得可能である。

[0273] 以上より、本実施形態における解析システム１００は、メモリ領域データの中から、効率よく鍵データ候補を抽出可能である。なぜならば、暗号解析部１０４が、メモリ領域データの中から鍵データの特徴を表すデータ（鍵候補判定情報１０４ｂ）に基づいて鍵データ候補を抽出することから、鍵データの特徴に合致しないデータを、鍵データ候補から排除可能であるからである。また、複数の鍵データ候補の中に含まれる正しい鍵データを判定可能であることから、本実施形態における解析システム１００は、メモリ領域データから、正しい鍵データを、効率的に探索可能である。

[0274] また、本実施形態における解析システム１００においては、上記抽出した正しい鍵データを用いて、暗号解析部１０４が、暗号化された通信データを解読可能である。

[0275] また、本実施形態における解析システム１００によれば、通信処理部１０３は、暗号解析部１０４により解読された通信データを用いて、解析対象装置１０１と、通信ネットワーク１０５との間で送受信される通信データの内容を解析可能である。通信処理部１０３は、当該解析結果に応じて、例えば、上記説明したような特定の処理を実行することが可能である。

[0276] 以上より、本実施形態における解析システム１００は、解析対象装置１０１と、通信ネットワーク１０５との間で送受信される暗号化された通信デー

タの少なくとも一部を解析可能である。また、本実施形態における解析システム100は、上記解析の結果に応じて、特定の処理を実行することが可能である。具体的には、本実施形態における解析システム100は、例えば、解析対象装置101において実行されるマルウェア等の任意のソフトウェア・プログラムによる暗号通信の内容を解析可能である。特に、本実施形態における解析システム100は、当該ソフトウェア・プログラムや、解析対象装置101に対して非侵襲的な手法により、暗号通信の内容を解析可能であり、当該解析結果に基づいて、任意の処理を実行可能である。

[0277] <第1の実施形態の変形例>

以下、上記説明した第1の実施形態の変形例について説明する。

[0278] 上記第1の実施形態においては、鍵候補抽出部104aは、メモリ取得部102において取得されたメモリ領域データから、鍵候補判定情報104bに基づいて、鍵データ候補を抽出する。

[0279] 本変形例における鍵候補抽出部104aは、上記説明した暗号処理データの候補と、上記暗号鍵を生成する基になるデータである鍵素材データの候補との少なくとも一方を、メモリ領域データから抽出するよう、上記第1の実施形態における鍵候補抽出部104aを拡張する。係る鍵素材データの候補は、例えば、SSLにおけるpre__master__secretや、master__secret等であってもよい。

[0280] 係る暗号処理データ、及び、鍵素材データは、上記説明した鍵データと同様に、上記メモリ領域データに含まれるデータの中で、特有の特徴を示す場合がある。これらのデータの特徴は、例えば、係るデータ自体の属性（例えば、データ自体のランダム性等）、あるいは、係るデータの上記メモリ領域データにおける配置パターン（配置される位置や、配置されるデータの並び）等を表す。

[0281] また、暗号処理データ、及び、鍵素材データの特徴は、上記鍵データの特徴と同様に、暗号通信の実行に関する各種条件に応じて異なる場合がある。具体的には、例えば、上記暗号通信プロトコルにおいて用いられる暗号アル

ゴリズム、あるいは、解析対象装置 101 における当該暗号方式に関する処理の実行環境等に応じて、係るデータの特徴が異なる場合がある。

[0282] 例えば、特定の暗号アルゴリズムが暗号利用モードとして GCM が採用された場合と、CBC モードが採用された場合とでは、暗号処理データとして必要となるデータの種類が異なり、そのデータ自体の特性も異なる。例えば、ランダム性が高いデータもあれば、所定の値に設定されるデータもある。また、解析対象装置 101 における、暗号処理の実行環境に応じて、メモリ領域データにおける暗号処理データの配置位置が異なる場合がある。

[0283] 上記鍵データの特徴と同様、これらのデータの特徴を表すデータを予め収集してパターン化することにより、メモリ領域データの中からこれらのデータの候補を抽出可能な判定基準を設けることが可能である。本変形例における鍵候補抽出部 104a は、当該判定基準に基づいて、メモリ領域データからこれらのデータ候補を抽出する。当該判定基準には、例えば、これらのデータの候補を探索（抽出）する位置（場所）が設定されていてもよい。あるいは、当該判定基準には、例えば、特定のデータがこれらのデータに該当するか否かを判定するための判定方法等が設定されていてもよい。

[0284] なお、係る判定基準は、上記第 1 の実施形態における鍵候補判定情報 104b に追加されてもよい。また、係る判定基準は、新たな構成要素（不図示）として、鍵候補抽出部 104a に追加されてもよい。

[0285] 本変形例における暗号解読部 104d は、上記鍵素材データの候補を抽出した場合には、当該鍵素材データの候補から、上記鍵データ候補を生成してもよい。一般的に、鍵素材データから、暗号鍵を生成する方法は、暗号通信プロトコル（あるいは、当該暗号通信プロトコルにおいて用いられる暗号アルゴリズム）ごとに規定されている。例えば、SSL プロトコルの場合、`pre_master_secret` から、`master_secret` を生成する方法、及び、`master_secret` から暗号通信に用いる鍵等を生成する方法は、SSL プロトコルの仕様として規定されている。

[0286] 本変形例における暗号解読部 104d は、上記第 1 の実施形態と同様、鍵

データ候補と、暗号処理データの候補とを用いて通信データを解読する。本変形例における暗号解読部 104 d は、上記第 1 の実施形態と同様、解析結果判定情報 104 e に基づいて当該解読結果の成否を判定する。

[0287] 本変形例における暗号解読部 104 d は、通信データの解読が成功した場合に、正しい鍵データと、解読済み通信データと、暗号処理データとを、解析結果保持部 104 f に保存（登録）してもよい。

[0288] 上記のように構成された本変形例における解析システム 100 は、所定の判定基準に基づいて、暗号処理データの候補、及び、鍵素材データの候補の少なくとも何れかを抽出可能である。また、本変形例における解析システム 100 は、上記第 1 の実施形態と同様、それらのデータを用いて通信データを解読した結果に基づいて、正しい鍵データと、解読済み通信データとを取得可能である。

[0289] また、本変形例における解析システム 100 は、上記第 1 の実施形態における解析システム 100 と同様の構成を有するので、上記第 1 の実施形態と同様の効果を奏する。

[0290] <第 2 の実施形態>

次に、上述した第 1 の実施形態に係る解析システムを基本とする、本発明の第 2 の実施形態について説明する。以下の説明においては、本実施形態に係る特徴的な部分を中心に説明すると共に、上述した第 1 の実施形態と同様な構成についての重複する説明は省略する。

[0291] 図 17 に例示するように、本実施形態における解析システム 1700 は、通信データ改変部 1701 を有する点において、上記第 1 の実施形態における解析システム 100 と相違する。以下においては、係る相違点を中心に説明する。

[0292] まず、本実施形態における解析システム 1700 の概要について説明する。

[0293] 解析システム 1700 は、通信データ改変部 1701 を除いて、上記第 1 の実施形態における解析システム 100 と同様の構成を有する。このため、

解析システム１７００は、第１の実施形態における解析システム１００と同様、解析対象装置１０１と、通信ネットワーク１０５（具体的には、通信ネットワーク１０５を介して接続された他の情報通信装置１０７）との間の暗号通信を解析可能である。また、解析システム１７００（特には、通信処理部１０３）は、当該暗号通信を解析した結果に基づいて、特定の処理を実行可能である（図１１に例示するステップＳ１１０７）。

[0294] ここで、通信処理部１０３が当該暗号通信を解析した結果、解析対象装置１０１あるいは通信ネットワーク１０５に対して望ましくない事象が生じる危険性があると判定した場合を想定する。この場合、通信処理部１０３は、係る危険性を低減可能な、適切な処理を実行可能であることが望ましい。

[0295] これに対して、例えば、解析対象装置１０１と、通信ネットワーク１０５との間の暗号通信を遮断することにより、通信処理部１０３は、係る危険性を低減可能である。しかしながら、当該暗号通信が解析対象装置１０１において活動するマルウェアにより実行されている場合、当該暗号通信が遮断されることにより、当該マルウェアは、自身の攻撃が失敗したことを認識することが可能である。この場合、当該マルウェアは、マルウェアの本来の活動とは異なる別の行動（例えば、攻撃手段の選択、あるいは、消滅や活動停止等）を選択する可能性がある。例えば、マルウェアが活動を休止した場合、係るマルウェアの挙動を解析することが困難となる。

[0296] 本実施形態における通信処理部１０３は、解析対象装置１０１と、通信ネットワーク１０５との間の暗号通信を遮断することなく、当該暗号通信による危険性を低減する。すなわち、本実施形態における通信処理部１０３は、通信データ改変部１７０１を用いて、解析対象装置１０１と、通信ネットワーク１０５との間で送受信される（暗号化された）通信データを改変することにより、当該暗号通信による危険性を低減する。

[0297] （通信データ改変部１７０１の構成）

以下、通信データ改変部１７０１の構成について説明する。

[0298] 通信データ改変部１７０１は、通信処理部１０３、及び、暗号解析部１０

4と、それぞれ通信可能に接続されている。通信データ改変部1701は、通信データ改変ポリシ1701aを有する。

[0299] 通信データ改変部1701は、暗号解析部104により解読された通信データを解析する。係る解析の結果、当該通信データの改変が必要であると判定した場合には、通信データ改変部1701は、当該特定の通信データにおいて改変を要する箇所の内容を改変する。

[0300] より具体的には、通信データ改変部1701は、解析対象装置101と、通信ネットワーク105との間で暗号化された通信データを送受信する通信処理の種別を特定する。係る通信処理の種別（以下、「通信処理種別」と称する場合がある）は、特定の通信データを送受信する通信処理を、その目的に従って分類可能な情報であってもよい。

[0301] 通信データ改変部1701は、例えば、特定した通信処理種別に基づいて、特定の通信データに対する改変が必要か否かを判定する。そして、通信データ改変部1701は、特定の通信データに対する改変が必要であると判定した場合には、当該特定の通信データにおいて改変を要する箇所の内容を改変する。

[0302] 本実施形態において、通信データ改変部1701は、通信データ改変ポリシ1701aに基づいて、特定の通信データに対する通信処理種別を特定し、当該特定の通信データにおいて改変を要する箇所の内容を改変する。

[0303] 通信データ改変ポリシ1701aは、図18に例示するように、通信処理種別1801と、判定基準1804と、改変情報1805と、を含む。通信処理種別1801に対して、判定基準1804と、改変情報1805とが関連付けられる。また、通信データ改変ポリシ1701aは、通信処理種別1801ごとに、通信元（通信データの送信元）1802と、通信先（通信データの送信先）1803とを更に含んでもよい。

[0304] 通信処理種別1801には、上記したように、特定の通信データを送受信する通信処理を分類する情報が設定される。

[0305] 判定基準1804には、特定の通信データを解析した結果に基づいて、当

該通信データを送受信する通信処理が、通信処理種別 1801 に該当するかどうかを判定可能な情報が設定される。

[0306] 改変情報 1805 には、特定の通信データにおいて改変が必要な箇所を特定するとともに、当該部分の内容を変更可能な情報が設定される。

[0307] なお、通信処理種別 1801、判定基準 1804、及び、改変情報 1805 に設定される各情報は機械解釈が可能な任意の形式に基づいて表現される。

[0308] 通信データ改変部 1701 の処理について、図 18 に示す具体例を用いて説明する。通信データ改変部 1701 は、特定の通信データを解析した結果、判定基準 1804 を満たすと判定した場合、当該通信データに関する通信処理種別 1801 を、「マルウェア X による認証処理」とであると判定する。図 18 に示す具体例においては、通信データ改変部 1701 は、例えば、当該通信データの送信先アドレスが” a a a . b b b . c c c . d d d ” であり、当該通信データの先頭 N バイト（N：自然数）に文字列” G E T / l o g i n . c g i ” が含まれる場合、判定基準 1804 を満たすと判定する。

[0309] そして、通信データ改変部 1701 は、当該特定の通信データを改変情報 1805 に基づいて改変する。この場合、通信データ改変部 1701 は、通信データに含まれるユーザ ID 部分を無害な文字列（例えば、” A A A A ”）に改変する。また、通信データ改変部 1701 は、通信データに含まれる認証情報部分を無害な文字列（例えば、” B B B B ”）に変更する。

[0310] なお、上記説明した具体例における判定基準 1804 には、通信データに含まれる値に基づいて、当該通信データを送受信する通信処理に関する通信処理種別 1801 を判定可能な情報が設定される。本実施形態はこれには限定されず、判定基準 1804 には、通信データの属性（例えば、データのサイズやデータフォーマット等）等の任意の情報に基づいて、通信処理種別 1801 を判定可能な情報が設定されてよい。

[0311] 以上のように、通信データ改変部 1701 は、通信データ改変ポリシー 17

01aに基づいて通信データを改変することにより、暗号通信を遮断することなく、当該暗号通信による危険性を低減可能である。

[0312] (解析システム1700の動作)

以下、上記のように構成された解析システム1700の動作について、図19乃至図20に例示するフローチャートを参照して説明する。

[0313] まず、図19に例示するフローチャートに従って、解析システム1700の各構成要素（特に、通信処理部103及び、通信データ改変部1701）の動作について説明する。なお、図19に例示するステップS1201乃至ステップS1209Bは、上記図12A、図12Bに例示したフローチャートと同様としてよいので、説明を省略する。

[0314] 図19に例示するステップS1209Bにおいて、暗号解読部104dから通信データの解読処理の完了を通知（上記図16におけるステップS1608）された際、暗号通信検査部103bは、通信データ改変部1701に対して、通信データの改変を指示する。そして、通信データ改変部1701が、必要に応じて、通信データを改変する（ステップS1901）。

[0315] 以下、ステップS1901における処理の具体的な内容について、図20に例示するフローチャートを参照して説明する。

[0316] まず、暗号通信検査部103bは、通信データ改変部1701に対して、通信データの改変を指示する（ステップS2001）。

[0317] 係る指示を受け付けた通信データ改変部1701は、解析結果保持部104fに保存（登録）された解読済み通信データを参照する（ステップS2002）。この際、通信データ改変部1701は、当該解読済み通信データを取得してもよい。

[0318] 次に、通信データ改変部1701は、通信データ改変ポリシー1701aに基づいて、上記参照（取得）した解読済み通信データを送受信する通信処理に対する、通信処理種別1801を特定する（ステップS2003）。

[0319] より具体的には、通信データ改変部1701は、上記ステップS2002において取得した解読済み通信データが、特定の判定基準1804を満たす

か否かを判定する。通信データ改変部 1701 は、通信データ改変ポリシー 1701a に登録された全ての判定基準 1804 に対して上記判定を行ってもよい。

[0320] 通信データ改変部 1701 は、上記解読済み通信データが特定の判定基準 1804 を満たす場合、当該特定の判定基準 1804 が関連付けされた通信処理種別 1801 を、上記解読済み通信データを送受信する通信処理に対する通信処理種別として特定する。

[0321] ステップ S2003 における処理の結果、通信処理種別 1801 が特定された場合（ステップ S2004 において YES）、通信データ改変部 1701 は、通信データ改変ポリシー 1701a に基づいて上記解読済み通信データを改変する。

[0322] より具体的には、通信データ改変部 1701 は、改変情報 1805 に基づいて、上記解読済み通信データにおいて改変を要する箇所を特定し、当該改変箇所のデータを編集する。この場合、通信データ改変部 1701 は、例えば、当該改変箇所のデータを他のデータを用いて置換してもよく、あるいは、削除してもよい。

[0323] 次に、通信データ改変部 1701 は、上記ステップ S2005 において改変した解読済み通信データを、再度暗号化する（ステップ S2006）。より具体的には、通信データ改変部 1701 は、解析結果保持部 104f を参照し、正しい鍵データ 1002 を用いて、解読済み通信データを暗号化する。この際、通信データ改変部 1701 は、上記正しい鍵データと共に、解析結果保持部 104f に登録されている暗号処理データを用いて、解読済み通信データを暗号化してもよい。

[0324] 次に、通信データ改変部 1701 は、通信データの改変処理が完了したことを、暗号通信検査部 103b に通知する（ステップ S2007）。

[0325] なお、ステップ S2004 において NO の場合（通信処理種別が特定されない場合）、通信データ改変部 1701 は、ステップ S2007 において、通信データが改変されなかったことを、暗号通信検査部 103b に通知して

もよい。

[0326] 再び図 19 を参照して、暗号通信検査部 103b は、ステップ S1901 における処理が完了した後、ステップ S1204 において一時停止した通信処理を再開する。そして、暗号通信検査部 103b は、改変された通信データを、解析対象装置 101、又は、通信ネットワーク 105 に宛てて送信する（ステップ S1902）。

[0327] より具体的には、暗号通信検査部 103b は、通信制御部 103a に対して、解析対象装置 101 と、通信ネットワーク 105 との間の通信を再開するように指示する。そして、暗号通信検査部 103b は、通信制御部 103a に対して、通信データ改変部により改変された（再暗号化済の）通信データを、解析対象装置 101、又は、通信ネットワーク 105 に対して送信するように指示する。

[0328] 以上のような動作により、本実施形態における解析システム 1700 は、解析対象装置 101 と、通信ネットワーク 105 との間で送受信される（暗号化された）通信データを改変することにより、当該暗号通信による危険性を低減可能である。

[0329] なお、上記説明したフローチャートにおいては、通信データ改変部 1701 が、改変された通信データを暗号化しているが、本実施形態はこれには限定されない。例えば、暗号通信検査部 103b が、通信データ改変部 1701 により改変された解読済み通信データを再度暗号化してもよい。

[0330] 上記のように構成された本実施形態における解析システム 1700 においては、上記第 1 の実施形態における解析システムと同様、暗号解析部 104 が、解析対象装置 101 と、通信ネットワーク 105 との間で送受信される暗号化された通信データを解読する。これにより、通信処理部 103 は、解析対象装置 101 と、通信ネットワーク 105 との間で送受信される通信データの内容を解析可能である。

[0331] 更に、上記のように構成された本実施形態における解析システム 1700 においては、通信処理部 103 の指示により、通信データ改変部 1701 が

、通信データ改変ポリシ１７０１aに基づいて、（必要に応じて）通信データを改変する。そして、通信データ改変部１７０１は、当該改変したデータを再暗号化する。通信処理部１０３は、当該改変された通信データを、解析対象装置１０１、又は、通信ネットワーク１０５に宛てて送信する。これにより、通信処理部１０３は、解析対象装置１０１と、通信ネットワーク１０５との間で送受信される通信データの内容を改変可能である。

[0332] 以上より、本実施形態における解析システム１７００は、解析対象装置１０１と、通信ネットワーク１０５との間の暗号通信を遮断することなく、当該暗号通信による危険性を低減可能である。すなわち、本実施形態における通信処理部１０３は、通信データ改変部１７０１を用いて、解析対象装置１０１と、通信ネットワーク１０５との間で送受信される（暗号化された）通信データを改変することにより、当該暗号通信による危険性を低減可能である。

[0333] 具体的には、本実施形態における解析システム１７００は、例えば、解析対象装置１０１において実行されるマルウェア等の任意のソフトウェア・プログラムによる暗号通信を遮断することなく、その通信内容を解析することが可能である。また、本実施形態における解析システム１７００は、その解析結果に基づいて通信データを改変することが可能である。

[0334] 特に、本実施形態における解析システム１７００は、解析対象装置１０１におけるソフトウェア・プログラムや、解析対象装置１０１自体に対して非侵襲的な手法により、暗号通信の内容を解析（検査）可能であり、当該解析結果に基づいて、当該暗号通信の内容を改変可能である。

[0335] <第３の実施形態>

次に、本発明における第３の実施形態について、図２１を参照して説明する。図２１は、本実施形態における解析システム２１００の機能的な構成を例示するブロック図である。

[0336] 本実施形態における解析システム２１００は、情報通信装置２１０１と、通信ネットワーク２１０５との間で実行される暗号通信を解析する。そして

、本実施形態における解析システム 2100 は、当該解析結果に基づいて、特定の処理を実行する。

[0337] 情報通信装置 2101 は、少なくとも演算部 2101a 及びメモリ部 2101b を有し、通信ネットワーク 2105 に対して通信可能に接続された、コンピュータ等の任意の情報通信装置である。

[0338] 係る情報通信装置 2101 は、例えば、物理的なハードウェアにより構成されたコンピュータ等の情報通信装置であってもよい。また、情報通信装置 2101 は、情報処理装置等の各種ハードウェアを仮想化可能な所定の仮想化基盤において提供される、仮想的なコンピュータ（VM）であってもよい。

[0339] 情報通信装置 2101 における演算部 2101a は、上記各実施形態における演算部 101a と同様、メモリ部 2101b に記憶された各種データ及びプログラムを読み出して、当該プログラムに実装された各種演算処理を実行する CPU や、MPU 等の演算装置である。

[0340] 情報通信装置 2101 におけるメモリ部 2101b は、上記各実施形態におけるメモリ部 101b と同様、情報通信装置 2101 におけるメインメモリとして機能し、演算部 2101a において処理される各種プログラム及びデータ等を保持する。また、メモリ部 2101b に保持（記憶）されたデータは、外部から取得（ダンプ）可能である。

[0341] このような情報通信装置 2101 は、上記説明した各実施形態における解析対象装置 101 と同様としてよい。

[0342] 通信ネットワーク 2105 は、有線、無線、又はこれらの任意の組合せにより構成され、任意の通信プロトコルを用いて通信路を確立可能な通信ネットワークである。また、通信ネットワーク 2105 は、例えば、上記各実施形態において説明した各種暗号通信プロトコルにより暗号化された通信路を、情報通信装置 2101 に対して提供可能である。係る通信ネットワーク 2105 は、上記各実施形態における通信ネットワーク 105 と同様としてよいので、詳細な説明は省略する。

- [0343] 次に、解析システム 2100 の構成について説明する。
- [0344] 本実施形態における解析システム 2100 は、メモリ取得部 2102 と、通信処理部 2103 と、暗号解析部 2104 とを備える。
- [0345] なお、解析システム 2100 の各構成要素は、それぞれ物理的なコンピュータ等の情報処理装置を用いて実現されてもよく、あるいは、仮想化基盤において提供される VM を用いて実現されてもよい。また、解析システム 2100 の各構成要素の間は、無線、有線、あるいはそれらを組み合わせた任意の通信回線により、通信可能に接続されている。係る通信回線は、周知の技術を採用してよいので、詳細な説明は省略する。以下、解析システム 2100 の各構成要素について説明する。
- [0346] メモリ取得部 2102 は、上記情報通信装置 2101 から、メモリ部 2101b に保持されたデータの少なくとも一部を取得する。メモリ部 2101b に保持（記憶）されたデータを取得する具体的な方法は、情報通信装置 2101 の具体的な構成に応じて適宜選択可能である。係るメモリ取得部 2102 は、例えば、上記各実施形態におけるメモリ取得部 102 と同様としてもよい。
- [0347] 通信処理部 2103 は、情報通信装置 2101 と、通信ネットワーク 2105 との間で特定の暗号通信プロトコルに従って送受信される通信データに基づいて、以下の処理を実行する。即ち、通信処理部 2103 は、上記通信データに基づいて、上記暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データが、メモリ部 2101b に保持されているか否かを判定する。通信処理部 2103 は、上記鍵データが、メモリ部 2101b に保持されていると判定した場合、メモリ取得部 2102 に対して、メモリ部 2101b に保持されたデータの取得を指示する。係る通信処理部 2103 は、例えば、上記各実施形態における通信処理部 103 と同様としてもよい。
- [0348] 通信処理部 2103 は、例えば、上記通信データを解析することにより、特定の暗号通信プロトコルにおいて上記暗号鍵に関する特定の条件が成立したタイミング（例えば、暗号鍵の交換が成立したタイミング等）を判定して

もよい。そして、通信処理部 2103 は、当該タイミングにおいて、メモリ取得部 2102 に対して、メモリ部 2101b に保持されたデータの取得を指示してもよい。

[0349] 暗号解析部 2104 は、上記鍵データの特徴に基づいて、上記メモリ取得部 2102 が取得したメモリ部 2101b に保持されたデータから、鍵データの候補である 1 以上の鍵データ候補を抽出する。暗号解析部 2104 は、情報通信装置 2101 と通信ネットワーク 2105 との間で送受信される暗号化された通信データを、当該抽出した鍵データ候補を用いて解読する。そして、暗号解析部 2104 は、当該解読した結果に基づいて、1 以上の鍵データ候補の中から、暗号化された通信データを正しく解読可能な正しい鍵データを抽出する。係る暗号解析部 2104 は、例えば、上記各実施形態における暗号解析部 104 と同様としてもよい。

[0350] 具体的には、暗号解析部 2104 は、例えば、特定の基準に基づいて、特定の鍵データ候補により、上記通信データを正しく解読できたと判定した場合、当該特定の鍵データを正しい鍵データとしてもよい。

[0351] 上記のように構成された解析システム 2100 において、通信処理部 2103 は、暗号解析部 2104 により解読された通信データに基づいて、所定の処理を実行する。通信処理部 2103 は、例えば、当該解読された通信データを解析し、その内容の一部を改変してもよい。

[0352] 以上のように構成された解析システム 2100（特にはメモリ取得部 2102）は、情報通信装置 2101 と、通信ネットワーク 2105 との間の通信路を暗号化する暗号鍵を含むメモリ領域データを、情報通信装置 2101 のメモリ部 2101b から取得可能である。なぜならば、通信処理部 2103 が、当該暗号鍵を含む鍵データがメモリ部 2101b に保持されていると判定した場合に、メモリ取得部 2102 に対してメモリ部 2101b に保持されたデータの取得を指示するからである。

[0353] また、本実施形態における解析システム 2100（特には、暗号解析部 2104）は、メモリ領域データの中から、効率よく正しい鍵データを抽出可

能である。なぜならば、暗号解析部 2104 が、鍵データの特徴に基づいて鍵データ候補を抽出可能であるからである。また、解析システム 2100（特には、暗号解析部 2104）は、当該抽出した鍵データ候補を用いて、通信データを解読した結果に基づいて、正しい鍵データを抽出可能であるからである。

[0354] また、本実施形態における解析システム 2100 においては、暗号解析部 2104 が、暗号化された通信データを、上記抽出した正しい鍵データを用いて解読することができる。これにより、通信処理部 2103 は、情報通信装置 2101 と、通信ネットワーク 2105 との間で送受信される通信データの内容を解析可能である。

[0355] 以上より、本実施形態における解析システム 2100 は、情報通信装置 2101 と、通信ネットワーク 2105 との間で送受信される暗号化された通信データの少なくとも一部を解析可能である。また、これにより、本実施形態における解析システム 2100 によれば、当該解析の結果に応じて、特定の処理を実行することが可能である

＜ハードウェア及びソフトウェア・プログラム（コンピュータ・プログラム）の構成＞

以下、上記説明した各実施形態を実現可能なハードウェア構成について説明する。

[0356] 以下の説明において、上記各実施形態において説明した解析システム（符号 100、符号 1700、符号 2100）をまとめて、単に「解析システム」と称する場合がある。また、当該解析システムの各構成要素（例えば、メモリ取得部（符号 102、符号 2102）、通信処理部（符号 103、符号 2103）、暗号解析部（符号 104、符号 2104）、通信データ改変部（符号 1701）等）をまとめて、単に「解析システムの構成要素」と称する場合がある。

[0357] 上記したように、上記各実施形態において説明した解析システムは、単体の装置（例えば、物理的な情報処理装置や、仮想的な情報処理装置等）によ

り実現されてもよい。また、上記各実施形態において説明した解析システムは、物理的あるいは論理的に離間した複数の装置（物理的な情報処理装置や、仮想的な情報処理装置）等を組み合わせることにより実現されてもよい。

[0358] より具体的には、上記各実施形態において説明した解析システムは、専用のハードウェア装置を用いて構成されてもよい。その場合、上記各図に示した各構成要素は、一部又は全部を統合したハードウェア（処理ロジックを実装した集積回路等）として実現されてもよい。

[0359] 例えば、各構成要素をハードウェアにより実現する場合、各構成要素は、それぞれの機能を提供可能な集積回路をSoC（System-on-a-chip）等により実装されてもよい。この場合、例えば、各構成要素が保持するデータは、SoCとして統合されたRAM領域やフラッシュメモリ領域に記憶されてもよい。

[0360] また、この場合、各構成要素を接続する通信回線としては、周知の通信バスを採用してもよい。また、各構成要素を接続する通信回線はバス接続に限らず、それぞれの構成要素間をピアツーピアで接続してもよい。

[0361] また、上述した解析システム、あるいは、当解析システムの構成要素は、図22に例示するようなハードウェアと、係るハードウェアによって実行される各種ソフトウェア・プログラム（コンピュータ・プログラム）とによって構成されてもよい。

[0362] 図22における演算装置2201は、汎用のCPU（Central Processing Unit）やマイクロプロセッサ等の演算処理装置である。演算装置2201は、例えば後述する不揮発性記憶装置2203に記憶された各種ソフトウェア・プログラムを記憶装置2202に読み出し、係るソフトウェア・プログラムに従って処理を実行してもよい。

[0363] 記憶装置2202は、演算装置2201から参照可能な、RAM（Random Access Memory）等のメモリ装置であり、ソフトウェア・プログラムや各種データ等を記憶する。なお、記憶装置2202は、揮発性のメモリ装置であってもよい。

- [0364] 不揮発性記憶装置 2203 は、例えば磁気ディスクドライブや、フラッシュメモリによる半導体記憶装置のような、不揮発性の記憶装置である。不揮発性記憶装置 2203 は、各種ソフトウェア・プログラムやデータ等を記憶可能である。
- [0365] ネットワークインタフェース 2206 は、通信ネットワークに接続するインタフェース装置であり、例えば有線及び無線の LAN (Local Area Network) 接続用インタフェース装置等を採用してもよい。
- [0366] 例えば、上記各実施形態における解析システムあるいは解析システムの構成要素は、解析対象装置 101、情報通信装置 2101、及び、通信ネットワーク (105、2105) と、当該ネットワークインタフェース 2206 を用いて、通信可能に接続されている。
- [0367] なお、上記各実施形態における解析システムあるいは解析システムの構成要素 (特に、通信処理部 (103、2103)) は、ネットワークインタフェース 2206 を複数備えてもよい。この場合、例えば、特定のネットワークインタフェース 2206 が解析対象装置 101、あるいは、情報通信装置 2101 と接続され、他のネットワークインタフェース 2206 が通信ネットワーク (105、2105) と接続されてもよい。
- [0368] ドライブ装置 2204 は、例えば、後述する記憶媒体 2205 に対するデータの読み込みや書き込みを処理する装置である。
- [0369] 記憶媒体 2205 は、例えば光ディスク、光磁気ディスク、半導体フラッシュメモリ等、データを記録可能な任意の記録媒体である。
- [0370] 入出力インタフェース 2207 は、外部装置との間の入出力を制御する装置である。例えば、解析システムのユーザあるいは管理者は、当該入出力インタフェースを介して接続された各種入出力装置 (例えば、キーボード、マウス、ディスプレイ装置、プリンタ等) を用いて、解析システムに対して各種操作の指示等を入力してもよい。
- [0371] 上述した各実施形態を例に説明した本発明においては、例えば、図 22 に例示したハードウェア装置により解析システム又はその構成要素が構成され

てもよい。そして、本発明においては、係るハードウェア装置に対して、上記各実施形態において説明した機能を実現可能なソフトウェア・プログラムが供給されてもよい。この場合、係る装置に対して供給したソフトウェア・プログラムを、演算装置 2201 が実行することによって、本願発明が実現されてもよい。

[0372] 上述した各実施形態において、上記各図（例えば、図 1、図 17、図 21 等）に示した各部は、上述したハードウェアにより実行されるソフトウェア・プログラムの機能（処理）単位である、ソフトウェアモジュールとして実現することができる。但し、これらの図面に示した各ソフトウェアモジュールの区分けは、説明の便宜上の構成であり、実装に際しては、様々な構成が想定され得る。

[0373] 例えば、図 1、図 17、及び、図 21 に例示した各部をソフトウェアモジュールとして実現する場合、これらのソフトウェアモジュールを不揮発性記憶装置 2203 に記憶しておき、演算装置 2201 がそれぞれの処理を実行する際に、これらのソフトウェアモジュールを記憶装置 2202 に読み出すよう構成してもよい。

[0374] また、これらのソフトウェアモジュール間は、共有メモリやプロセス間通信等の適宜の方法により、相互に各種データを伝達できるように構成してもよい。このような構成により、これらのソフトウェアモジュール間は、相互に通信可能に接続可能である。

[0375] 更に、上記各ソフトウェア・プログラムは記憶媒体 2205 に記録されてもよい。この場合、上記通信装置等の出荷段階、あるいは運用段階等において、適宜ドライブ装置 2204 を通じて当該ソフトウェア・プログラムが不揮発性記憶装置 2203 に格納されるよう構成されてもよい。

[0376] また、上記解析システムの構成要素をソフトウェア・プログラムとして実現する場合、上記各実施形態において説明した、以下の各構成要素に関する各種データは、適切なファイルシステムや、データベース等を用いて、不揮発性記憶装置 2203 に記憶されてもよい。係る構成要素には、メモリダン

プ保持部 102 a、鍵データ取得ポリシ 103 c、通信データ記録ポリシ 103 e、通信データ保持部 103 f、鍵候補判定情報 104 b、鍵候補保持部 104 c、解析結果判定情報 104 e、解析結果保持部 104 f 等が含まれる。

[0377] なお、上記の場合において、上記解析システムへの各種ソフトウェア・プログラムの供給方法は、出荷前の製造段階、あるいは出荷後のメンテナンス段階等において、適当な治具を利用して当該装置内にインストールする方法を採用してもよい。また、各種ソフトウェア・プログラムの供給方法は、インターネット等の通信回線を介して外部からダウンロードする方法等のように、現在では一般的な手順を採用してもよい。

[0378] そして、このような場合において、本発明は、係るソフトウェア・プログラムを構成するコード、あるいは係るコードが記録されたところの、コンピュータ読み取り可能な記憶媒体によって構成されたと捉えることができる。

[0379] また、上述した解析システム、あるいは、当解析システムの構成要素は、図 22 に例示するハードウェア装置を仮想化した仮想化環境と、当該仮想化環境において実行される各種ソフトウェア・プログラム（コンピュータ・プログラム）とによって構成されてもよい。この場合、図 22 に例示するハードウェア装置の構成要素は、当該仮想化環境における仮想デバイスとして提供される。なお、この場合も、図 22 に例示するハードウェア装置を物理的な装置として構成した場合と同様の構成にて、本発明を実現可能である。

[0380] 以上、本発明を、上述した模範的な実施形態に適用した例として説明した。しかしながら、本発明の技術的範囲は、上述した各実施形態に記載した範囲には限定されない。当業者には、係る実施形態に対して多様な変更又は改良を加えることが可能であることは明らかである。即ち、本発明は、本発明のスコープ内において、当業者が理解し得る様々な態様を適用することができる。そのような場合、係る変更又は改良を加えた新たな実施形態も、本発明の技術的範囲に含まれ得る。また、係る実施形態の組み合わせも、本発明の技術的範囲に含まれる。そしてこのことは、請求の範囲に記載した事項か

ら明らかである。

[0381] 本発明は、例えば、情報通信装置の開発及び運用段階における通信処理の解析や、情報通信装置において実行される各種プログラムの通信処理の解析等に適用可能である。より具体的には、本発明は、例えば、情報通信装置において各種プログラムが実行する不正な通信処理を検査し、通信処理の内容に応じて適切な処理を実行する、検査システム等に適用可能である。

[0382] この出願は、2014年9月25日に提出された日本出願特願2014-195178を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

- [0383]
- 100 解析システム
 - 101 解析対象装置
 - 102 メモリ取得部
 - 103 通信処理部
 - 104 暗号解析部
 - 105 通信ネットワーク
 - 106 通信路
 - 107 他の情報通信装置
 - 1701 通信データ改変部
 - 2100 解析システム
 - 2101 情報通信装置
 - 2102 メモリ取得部
 - 2103 通信処理部
 - 2104 暗号解析部
 - 2105 通信ネットワーク
 - 2201 演算装置
 - 2202 記憶装置
 - 2203 不揮発性記憶装置

- 2 2 0 4 ドライブ装置
- 2 2 0 5 記憶媒体
- 2 2 0 6 ネットワークインタフェース
- 2 2 0 7 入出力インタフェース

請求の範囲

[請求項1] 演算部とメモリ部とを有する情報通信装置における前記メモリ部に保持されたデータの少なくとも一部を取得可能なメモリ取得手段と、
前記情報通信装置と、通信ネットワークとの間で暗号通信プロトコルに従って送受信される通信データに基づいて、当該暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データが前記メモリ部に保持されていると判定した場合に、前記メモリ取得手段に対して前記メモリ部に保持されたデータの取得を指示する通信処理手段と、

前記鍵データの特徴を表すデータに基づいて、前記メモリ取得手段が取得した前記メモリ部に保持されたデータから、前記鍵データの候補である1以上の鍵データ候補を抽出し、

前記情報通信装置と前記通信ネットワークとの間で送受信される暗号化された前記通信データを、当該抽出した前記鍵データ候補を用いて解読した結果に基づいて、1以上の前記鍵データ候補の中から、暗号化された前記通信データを正しく解読可能な正しい鍵データを抽出する、

暗号解析手段と、を備え、

前記通信処理手段は、前記暗号解析手段により解読された前記通信データに応じた特定の処理を実行する、
解析システム。

[請求項2] 前記暗号解析手段により解読された前記通信データを解析した結果に基づいて、前記通信データに対する改変が必要であると判定した場合に、前記通信データの少なくとも一部を改変可能な通信データ改変手段を更に備え、

前記通信処理手段は、前記特定の処理として、前記通信データ改変手段により改変された前記通信データを、前記情報通信装置及び前記通信ネットワークの少なくとも一方に送信する、

請求項 1 に記載の解析システム。

[請求項3]

前記通信処理手段は、

前記通信データに関する暗号処理に用いられる暗号鍵を含む鍵データが前記情報通信装置のメモリ空間に存在すると判定した場合に、前記情報通信装置と、前記通信ネットワークとの間の通信を停止し、

前記特定の処理として、前記通信データ改変手段により改変された前記通信データを、前記情報通信装置及び前記通信ネットワークの少なくとも一方に送信する際に、当該停止した通信処理を再開する、請求項 2 に記載の解析システム。

[請求項4]

前記通信処理手段は、

前記通信データに関する暗号処理に用いられる暗号鍵を含む鍵データが前記情報通信装置のメモリ空間に存在すると判定した場合に、前記情報通信装置と、前記通信ネットワークとの間の通信を停止し、

前記メモリ取得手段による、前記メモリ部に保持されたデータを取得する処理が完了した際、前記情報通信装置と、前記通信ネットワークとの間の通信を再開し、

前記再開された通信において、最初の暗号化された前記通信データが前記情報通信装置と、前記通信ネットワークとの間で送受信されるタイミングにおいて、前記情報通信装置と、前記通信ネットワークとの間の通信を停止し、

前記特定の処理として、前記通信データ改変手段により改変された前記通信データを、前記情報通信装置及び前記通信ネットワークの少なくとも一方に送信する際に、当該停止した通信処理を再開する、請求項 3 に記載の解析システム。

[請求項5]

前記通信データ改変手段は、

前記通信データに対する改変の要否を判定可能な情報である改変判定基準と、前記通信データにおいて改変対象となる部分を特定可能な改変情報とを関連付けて保持する通信データ改変ポリシーを有し、

当該通信データ改変ポリシーに基づいて、前記通信データにおいて改変対象となる部分を改変する、

請求項 2 乃至請求項 4 の何れかに記載の解析システム。

[請求項6]

前記改変判定基準は、前記通信データを送受信する通信処理の種別を識別可能な情報であり、

前記通信データ改変手段は、

前記改変判定基準に基づいて、前記通信データを送受信する通信処理の種別を識別し、

当該識別した通信処理の種別に基づいて、前記通信データに対する改変の要否を判定する、

請求項 5 に記載の解析システム。

[請求項7]

前記改変判定基準は、前記暗号解析手段により解読された前記通信データの少なくとも一部の値と、当該データの属性との少なくとも何れかに基づいて、前記通信データを送受信する通信処理の種別を識別可能な情報である、

請求項 6 に記載の解析システム。

[請求項8]

前記通信データ改変手段は、

前記改変した通信データを前記抽出した正しい鍵データを用いて暗号化し、

前記通信処理手段は、前記通信データ改変手段により暗号化された前記通信データを、前記情報通信装置及び前記通信ネットワークの少なくとも一方に送信する、

請求項 2 に記載の解析システム。

[請求項9]

演算部とメモリ部とを有する情報通信装置と、通信ネットワークとの間で暗号化された通信路を確立可能な暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データの特徴を表すデータに基づいて前記メモリ部に保持されたデータから抽出された当該鍵データを用いて解読された、前記通信路において送受信される通信データを

解析し、

当該解析した結果に基づいて、前記通信データに対する改変が必要と判定した場合に、前記通信データの少なくとも一部を改変する解析装置。

[請求項10] 前記通信データに対する改変の要否を判定可能な情報である改変判定基準と、前記通信データにおいて改変対象となる部分を特定可能な改変情報とを関連付けて保持する通信データ改変ポリシーを有し、

当該通信データ改変ポリシーに基づいて、前記通信データにおいて改変対象となる部分を改変する、

請求項9に記載の解析装置。

[請求項11] 前記改変した通信データを前記抽出された鍵データを用いて暗号化する

請求項9又は請求項10に記載の解析装置。

[請求項12] 情報処理装置が、

演算部とメモリ部とを有する情報通信装置と、通信ネットワークとの間で暗号通信プロトコルに従って送受信される通信データに基づいて、当該暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データが前記メモリ部に存在すると判定した場合に、前記メモリに記憶されたデータの少なくとも一部を取得し、

前記鍵データの特徴を表すデータに基づいて、当該取得した前記メモリに記憶されたデータから、上記鍵データの候補である1以上の鍵データ候補を抽出し、

前記情報通信装置と前記通信ネットワークとの間で送受信される暗号化された前記通信データを、当該抽出した前記鍵データ候補を用いて解読した結果に基づいて、前記1以上の鍵データ候補の中から、暗号化された前記通信データを正しく解読可能な正しい鍵データを抽出し、

前記解読された前記通信データに基づいて、特定の処理を実行する

、
解析方法。

[請求項13]

演算部とメモリ部とを有する情報通信装置と、通信ネットワークとの間で暗号通信プロトコルに従って送受信される通信データに基づいて、当該暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データが前記メモリ部に存在すると判定した場合に、前記メモリ部に記憶されたデータの少なくとも一部を取得する処理と、

前記鍵データの特徴を表すデータに基づいて、当該取得した前記メモリ部に記憶されたデータから、上記鍵データの候補である1以上の鍵データ候補を抽出する処理と、

前記情報通信装置と前記通信ネットワークとの間で送受信される暗号化された前記通信データを、当該抽出した前記鍵データ候補を用いて解読した結果に基づいて、前記1以上の鍵データ候補の中から、暗号化された前記通信データを正しく解読可能な正しい鍵データを抽出する処理と、

前記解読された前記通信データに基づいて特定の処理を実行する処理と、をコンピュータに実行させる
コンピュータ・プログラムが記録された記憶媒体。

[請求項14]

請求項1乃至請求項8の何れかに記載の解析システムを、単体の装置として提供する解析装置。

[請求項15]

演算部とメモリ部とを有する情報通信装置から、当該情報通信装置と、通信ネットワークとの間で実行される暗号通信に用いられる暗号鍵を含む、前記メモリ部に保持されたデータを取得するメモリ取得手段と、

前記メモリ取得手段が取得したデータから、前記暗号鍵を含む鍵データの候補である1以上の鍵データ候補を抽出し、前記暗号通信により送受信された通信データを当該抽出した前記鍵データ候補を用いて解読した結果に基づいて、当該通信データを正しく解読可能な正しい

鍵データを抽出する、暗号解析手段と、

前記暗号解析手段により解読された前記通信データに応じて、前記暗号通信に関する特定の処理を実行する、通信処理手段と、を備える解析システム。