大規模仮想化サーバ環境における情報セキュリティ対策技術の研究開発

基本計画書

１．目　的

大規模仮想化サーバ環境を利活用した ICT サービスの提供が進展し、国民生活や社会経済活動を支える基盤インフラとなりつつある。一方、大規模仮想化サーバ環境には情報漏えい等の情報セキュリティ上の課題が残されていることから、利用者にとって安心・安全な ICT 利活用環境を実現するため、新たな情報セキュリティ対策技術を開発する。

２．政策的位置付け

第２次情報セキュリティ基本計画(平成21年２月　情報セキュリティ政策会議決定)では、情報セキュリティ基盤の強化及び発展のため、民間や大学における自主的な研究開発を促すとともに、産学官は適切な役割分担を行いつつ連携していくこととされている。

また、「セキュアジャパン 2009」（平成 21 年 6 月情報セキュリティ政策会議決定）では、総務省が「クラウドコンピューティングのような新技術が普及していく中で、情報漏えい等の情報セキュリティ脅威の拡がりにより新技術の普及が阻害されることがないよう、技術開発や人材育成等のセキュリティ対策を検討する。」とされている。

３．目　標

（１）政策目標

近年、仮想化技術を活用し、サーバ環境の大規模化・集約化が各国で進展しており、巨大なインフラに成長しつつある。これら環境下での情報資産の保存・処理等が拡大しているが、情報漏えい等の事故が懸念されること、また、多数の利用者のデータが共同処理され、さらに、世界中の複数のサーバに分散的に処理されており、利用者にとってセキュリティレベルが不明な環境に情報資産を預託することに繋がっている。このため、大規模仮想化サーバ環境における情報セキュリティ対策技術を新たに開発することで、前記の第２次情報セキュリティ基本計画等が掲げる目標の達成に大きく寄与し、安心・安全なインターネット環境を実現するとともに、技術仕様の国際標準化等を通じて、本分野における国際競争力強化を図る。

（２）研究開発目標

本研究開発では、通信回線から仮想化サーバまで一貫してデータを秘匿化して送受・処理する技術とともに、情報提供者側での情報の秘匿化を可能とする技術を確立

する「プライバシー保護型処理技術」、大量のデータ処理を行う大規模仮想化サーバ環境におけるセキュリティレベルを判断し、利用者に対してセキュリティレベルを可視化する技術とともに、利用者情報の価値に基づいてデータの重要度を判断し可視化する技術を確立する「セキュリティレベル可視化技術」の研究開発を行い、利用者が安心して個人情報等を預託できる大規模仮想化サーバ環境を実現するとともに、安心・安全な ICT 利活用環境に必要な基盤技術の確立を目標とする。

４．研究開発内容

（１）プライバシー保護型処理技術

①　概要

暗号化などにより秘匿した状態で収集した情報を、秘匿したままの状態でデータ処理を行うことによって情報漏えいにも耐性を持たせる、プライバシー保護型のデータ処理技術の研究開発を実施する。また、情報提供者が安全に情報提供を行えるように、低コスト装置でも実現可能なデータ秘匿向け演算方式の研究開発、及び情報提供者の個人情報を保護しつつ、データ処理の目的に沿った適切な対象者から正当なデータ収集を可能にする、情報提供者の属性管理技術の研究開発を実施する。

②　技術課題

ア）情報漏えい耐性のあるデータ処理技術

大規模仮想化環境においても情報提供者のプライバシーを保護した安全なデータ処理を可能にするため、データを秘匿したままで処理可能なデータ処理技術の研究開発を行う。理論的には、いかなるデータ処理も秘匿したままのデータに対して行うことが可能であることは知られているが、現在のところ汎用的なデータ処理技術は非常に効率が悪く、現実的な時間で実行できない状況である。そこで、検索や統計処理など特定のアプリケーションに特化したいくつかの効率的なデータ処理技術を検討し、現実的な時間で処理が行える方式の開発を行う。大規模仮想化環境におけるデータ処理は、その利用シーンから、以下の二つに大別される。

A)　情報提供者本人が処理結果を利用するタイプのデータ処理

B)　情報提供者以外が処理結果を利用するタイプのデータ処理

本研究開発では、A)，B)双方のタイプのデータ処理に関して、元データを秘匿したままでのデータ処理を実現する基盤技術の研究開発を行う。

具体的には、A)については、メールサーバでのメール検索や顧客データの該当者検索などに利用可能な方式として、情報提供者が自身の鍵でデータベース全体と、検索キーワードを暗号化し、大規模仮想化サーバ管理者が管理者側の計算資源を用いて検索処理のみを行い、該当箇所の報告を情報提供者に行うことをデータベースの内容や検索キーワードを知られることなく、かつ現実的な時間内で実行できる方式の研究開発を行う。B)については、情報提供者から提供された情報の統計量計算やデータの分布計算、複数の企業が管理するデータのマッチング処理な

ど、多くのシステムで汎用的に利用されるデータ処理を、元のデータを秘匿したまま現実的な時間内で計算する方式の研究開発を行う。

イ）安全な情報提供技術

多くの個人から提供される情報を大規模仮想化環境に集約し、個人情報に基づいた緻密なデータを分析することによって、社会や個人に有用な情報をより広く還元するサービスが検討されている。このようなサービスでは、大規模仮想化環境側の安全なデータ処理技術のみならず、情報提供側の安全な情報提供技術が必要になる。特に、低コスト情報提供端末への対応及び提供者個人の属性情報の扱いが課題となる。

大規模仮想化環境において漏えいの可能性を最小限にするために、情報提供者がデータを提供する時点において暗号化などの秘匿処理がなされていることが望ましい。この場合、情報提供者側で秘匿処理が必要である。そこで、多くの利用者に負担を強いずに情報提供できる環境を構築するために、多様な機器での情報提供を可能とするデータ秘匿向け演算方式の研究開発を行う。具体的には、ＰＣだけではなく、一般に広く普及している低コストの機器でも情報提供が可能になるように、演算ハードウェアを用いた情報提供技術の研究開発を行う。

また、大規模仮想化環境において個人情報に基づくサービスを実現する際には、個人利用者のプライバシーを保護しつつ、正当な個人が情報提供を行っていることの確認も重要となる。例えば、特定の属性を有する人の統計情報を計算しようとするサービスにおいて、計算される統計情報の信頼性を担保するためには、情報提供者がその属性を有することの確認が必要となる。しかし情報提供者の氏名など、データ提供に際して開示したくない情報もある。また、情報提供を複数回行い、いくつかの属性を開示した場合でも、名寄せによって本人が特定されたり、提供した複数の情報が同一の提供者から提供された情報であることが明らかになったりすることも防がなければならない。そこで、提供するデータを秘匿するだけではなく、情報提供者の開示属性を必要最小限にでき、また複数回の情報提供が行われた場合でも、その関連性を検知することが困難であるような属性管理が必要となる。本研究開発では、個人のプライバシーを保護しつつ、情報が所望の属性を持つ情報提供者から提供されていることを保証する安全な属性管理技術の研究開発を行う。

③　到達目標

ア）情報漏えい耐性のあるデータ処理技術

「A) データを拠出した本人が利用するタイプのデータ処理」に関しては、サーバ用途で一般的に使われている PC に相当する計算資源を利用可能な仮想化サーバ上で、1 万件規模のデータベースの検索を 30 秒以内の処理時間で実現可能とすることを目標とする。初年度は、基本アルゴリズムを複数方式検討し、それぞれの安全性や効率性についての基本評価を実施する。次年度以降は、初年度検討した方式のうち有望なものを数種類選択し処理性能の評価などを行い、実用的なア

プリケーションを定めたうえで、最終年度に、仮想化環境上で実現する基盤を試作する。

「B) データを拠出した人以外が利用するタイプのデータ処理」に関しては、サーバ用途で一般的に使われている PC に相当する計算資源を利用可能な仮想化サーバ上で、1 万人規模のデータの特徴量抽出を 10 分以内で実現可能とすることを目標とする。初年度は、複数の情報提供者のデータから得られる統計量などの特徴量を抽出する基本アルゴリズムを複数方式検討し、有望なアプリケーションを一つ定める。次年度以降は、複数組織・複数仮想化環境にまたがるデータベースを連携させてデータ処理を行うアプリケーションを定めたうえで、最終年度に、連携したデータ処理を仮想化環境上で実現する基盤を試作する。

イ）安全な情報提供技術

データ秘匿向け演算方式に関しては、最新のスマートフォンや携帯電話においてソフトウェアで 1 秒以内、演算ハードウェアを用いて 0.5 秒以内で実現することを目標とする。初年度は、携帯端末上でソフトウェアの基本アルゴリズム設計と、演算ハードウェアの基本設計を行う。次年度以降は初年度に設計した方式の処理性能の評価及び改良を行うとともに、演算ハードウェアを適切なインタフェースの下で携帯機器に接続する。

属性管理技術に関しては、情報提供者の 2 つ以上の属性を扱うことが可能な効率的な属性管理技術を確立し、2.5GHz 程度のマルチコアＣＰＵを搭載した最新のＰＣ上で 200ms 程度、演算ハードウェアを用いて携帯端末において 1 秒以内で実現することを目標する。初年度は属性の発行、変更、無効化のライフサイクルを検討し、基本方式を開発する。次年度以降は、ＰＣ上の属性認証と、演算ハードウェアを用いた携帯端末上の属性認証を試作する。

（2）セキュリティレベル可視化技術

① 概要

大規模仮想化環境では、システムを構成する機器がダイナミックに変化するため、セキュリティインシデントが発生しているかどうかを判別することが困難となってしまう。

そこで、処理サーバ群のセキュリティ状態に関わる情報を収集・分析し、仮想化サーバ環境及び扱うデータ自身の情報セキュリティ対策状況を把握し、サービスあるいは利用者が要求するセキュリティレベルに応じた処理を実行できるようにする技術を確立する。

② 技術課題

大規模仮想化環境では、システムを構成する機器がダイナミックに変化するため、これまでのセキュリティ対策のように固定的なシステム構成を前提とした脅威分析に基づくセキュリティ対策状況の確認は利用できない。このため、本課題では、大規模仮想化環境においてセキュリティ状態に関わる情報を効率的に収集するために設定す

る多面的（仮想化サーバ環境、実行サーバ、ネットワーク、等）な観測ポイントを明らかにするとともに、観測ポイントで監視／収集した情報に統計処理を施し、セキュリティに関係するデータを抽出し、セキュリティポリシーに対する相関関係等からセキュリティ状態をリアルタイムに決定して、利用者に対策状況を可視化する技術を研究開発する。

また、大規模仮想化環境で処理されるデータには、データを組み合わせることによってより大きな価値を持つ情報が含まれる場合が存在する。このようなデータは、より高いセキュリティ状態の仮想化環境で管理したり、大規模仮想化環境内で分散して管理したりすることにより、利便性を低下することなく、セキュリティを向上させることが求められる。このため、本課題では、大規模仮想化環境で処理されるデータの重要度を判断する技術、セキュリティ状態とデータの重要度に基づいて、利用者が要求したセキュリティレベルが担保されるように制御サーバに制御命令を発行し、処理を要求する仮想化サーバ環境を選択することを可能とする技術を開発する。特に、データの中に個人の特定が可能となる機微情報が含まれる場合には、プライバシー保護の観点から特に取り扱いに注意する必要があるため、課題１で研究するプライバシー保護機能を備えた仮想化サーバを優先的に選択し、利用者のプライバシーを保護するように制御を行う。また、データの重要度を判断する場合には、判断の対象となっているデータだけではなく、過去に大規模仮想化環境に提供したデータ等も考慮した判断を可能とする。

③　到達目標

大規模仮想化サーバ環境において、セキュリティ状態を判定するために効率的に情報を収集するための観測ポイントを明らかにするとともに、100 程度の観測ポイントから得られる毎秒１万件程度のイベント情報に基づいてセキュリティインシデントの発生・データの保管状態等のセキュリティレベルを 200ms 以内に判定して、4 段階程度に分類してユーザに適切に表示する。

また、過去に大規模仮想化環境に提供したデータも考慮した上で、新たに提供するデータの持つ価値を定量的に分析する手法を確立するとともに、確立した手法を使用してデータの重要度を判定し、ユーザが要求するセキュリティレベルを満足するように、適切なデータ保護を施した上で処理の振り分けを制御できることを目標とする。このとき、100 件のデータを受信した場合に 1 秒以内で各々のデータの重要度を判定すること、要求される所与のセキュリティレベルを満足するためのセキュリティポリシーの生成処理を 500ms 以内に実現することを目標とする。

そのため、初年度は、複数のネットワークに跨って実現されている、既存の仮想化システム環境を調査・検討し、様々な基準（認証・完全性・機密性・可用性等）に基づくセキュリティ状態を判定するための観測ポイントの設置場所および観測内容を明らかにする。また、観測ポイントから得られる情報に統計処理を行い、各基準でのセキュリティ状態を判定する基本アルゴリズムを設計する。さらには、複数のデータから構成されたテーブルに対して、セキュリティポリシーに基づいてデータの価値を定量的に評価する手法を検討し、自動評価を行うモジュールを設計･評価するとともに、

セキュリティ状態とデータの重要度に基づいて仮想化環境を選択する制御サーバを設計する。また、課題(1)で研究する機能を備えた仮想化サーバと連携するためのインタフェースを含む、データ保護フレームワーク、およびデータ保護ポリシー生成方式の基本設計を行う。

２年目以降は、初年度の結果に従い、観測ポイントから得られる情報に基づいてセキュリティ状態やデータ重要度を可視化・判定して仮想化環境を選択するシステムを試作して有効性を検証するとともに、最終年度に向けてセキュリティ状態を総合判定するアルゴリズムの開発、試作システムの高速化等を行い、最終目標を達成する。

５．実施期間

平成２２年度から平成２４年度までの３年間

６．その他　特記事項

本研究開発で確立した技術の普及啓発活動を実施すると共に実用に向けて必要と思われる研究開発課題への取り組みも実施し、その活動計画・方策については具体的に提案書に記載すること。