サイバーセキュリティ工学領域

研究室紹介

宮　地　充　子*

Cyber Security Engineering Area

Key Words：security, cryptology, privacy, cyber attack

1．はじめに

本研究室は2015年10月に電気電子情報工学専攻　情報通信工学部門通信システム工学の1講座として発足しました．情報セキュリティと暗号理論，ネットワークセキュリティが研究領域となります．我々を取り巻く情報社会では，多種多様なデータが収集され，その解析結果は医療，産業など様々な分野での利活用が期待されています．しかしながら，意図的に歪められたデータを用いると正しい解析結果を入手できませんし，解析結果も意図的に歪められる可能性もあります．情報セキュリティはデータの秘匿，完全性，可用性を実現し，情報社会に安心と信頼を与える技術です．

2021年現在，高野 祐輝特任准教授，奥村 伸也助教，Tian Yangguang 特任助教，博士後期課程学生7名，博士前期課程学生10名，学部学生11名，研究生2名で合計30名が本研究室に所属しています．本研究室で実施している研究テーマは下記となります．

・現在利用されている暗号や耐量子暗号の解読や効率的な実装方法などの暗号基盤研究
・暗号化したまま平均値や分散値などの統計処理や，ソート等のデータ処理を実現するなど，秘匿したディジタルデータの可用性を実現する情報セキュリティの研究
・ビットコインなどディジタルデータを用いた社会システムの実現や，IoT機器，クラウド等のセキュアアプリケーションを実現するセキュアプロトコルの研究
・NWに繋がるIoT機器の普及により，サイバー攻撃は企業や組織だけではなく，身近な脅威になってきました．サイバー攻撃に対する防御として，強固なネットワークの設計や，脆弱性を削減したソフトウェアを用いて高信頼なソフトウェアの設計に関する研究

本研究室では，数論と計算量理論，情報理論を駆使した暗号理論の研究から，新しい社会システムをモデル化し，それを実現するディジタルプロトコルの構築という応用，またそれらを実際にソフトウェア，あるいはネットワークで安全に活用するための技術，また暗号についてはFPGAのハード実装等，セキュリティ全般にまたがる研究を行っています．このため，学生一人一人の研究に必要な知識がかなり違います．そういう異なる知識・研究に触れ合うことで，論理的な思考能力，問題発見能力，そして解決能力を養っていきたいと考えています．

本稿では上記4つの研究分野から具体的な研究と

表1：学校の事故における分散データ管理事例（✓：データ有り、ー：データ無し）

	生徒名	遊具メーカ	救急搬送データ	傷害データ	後遺症データ
学校	✓	✓	―	―	―
消防署	✓	―	✓	―	―
病院	✓	―	―	✓	✓

* Atsuko MIYAJI
大阪大学理学部　前期課程修了
博士（理学）　学位取得（1997年）
現在、大阪大学大学院　工学研究科
電気電子情報通信工学専攻　教授
博士（理学）
TEL：06-6879-7715
FAX：06-6879-7715
E-mail：miyaji@comm.eng.osaka-u.ac.jp

して，以下の研究内容について説明させていただきます．

・プライバシを保護した分散多機関データ統合
(privacy-Preservind Data Integration(PDDI))

JST CREST プロジェクト『ビッグデータ統合利活用促進のためのセキュリティ基盤技術の体系化』での主要研究となります．

・欺瞞的防御システム

欺瞞的防御システムは，境界型防御技術では防ぐことが難しい標的型攻撃やゼロデイ攻撃からシステムを守る方法です．

2．プライバシを保護した分散多機関データ統合

我々を取り巻く情報社会では多種多様なデータが存在します．例えば，けがをした事例を考えます．このとき，事故が起こった遊具に関するデータは学校，病院への救急搬送データは消防署，傷害・後遺症に関するデータは病院に管理されます．このように，学校，消防署，病院がそれぞれ同じ事故で異なるデータを管理します．

学校における事故の予防安全の実現には，事故の統計的因果モデルの作成が重要です．これにはこのように異なる機関に分散した関連データの統合が必須です．つまり，異なる機関が独立に収集したデータから生徒の名前などの機微情報は洩れることなく，統合できることが重要です．関連データが複数の異なる機関で保管されるケースは医療においても頻繁に起こります．例えば，同じ患者が異なる病気になった場合，複数の病院に通うことが考えられます（図 1）．このように独立に 2 つの医療機関で管理された異なる病気は，それぞれ因果関係がある可能性があります．この時，同一の患者のデータを患者のプライバシを保護しつつ，必要な医療データのみ突合できると，異なる病気の因果関係の詳細なデータの収集が可能になります．

ここで，異なる機関がもつ医療データの突合方法とプライバシの関係について考えます．1 つの医療機関が全データを別の医療機関に渡せば，同じ患者を検索することで，データを突合することができます．しかし，この場合，本来もつはずでなかった患者の情報である名前，住所などの機微情報を別の医療機関が入手することになります．別の方法として，第 3 の機関（データ預託機関）にそれぞれの病院が医療情報を渡し，その第 3 の機関で突合することもできます．しかしこの場合には，第 3 の機関に患者の機微情報が移動することになります．これが名寄せシステムです（図 2-1）．つまり，単純な突合方法は突合に用いる情報が必要となるため，突合を実施する機関に機微情報が移動し，プライバシ保護を実現することが困難です．

本研究室で提案した PDDI は，機微情報を他の機関に移動することなく，データ突合を実現する方式です（図 2-2）．

本提案は以下の特徴を持ちます．

・秘匿計算機サーバには暗号化データのみが送付れるので，データは完全に秘匿されます．

・暗号化不可逆データを用いて，突合が実現されるので機微情報はどの機関にも移動しません．

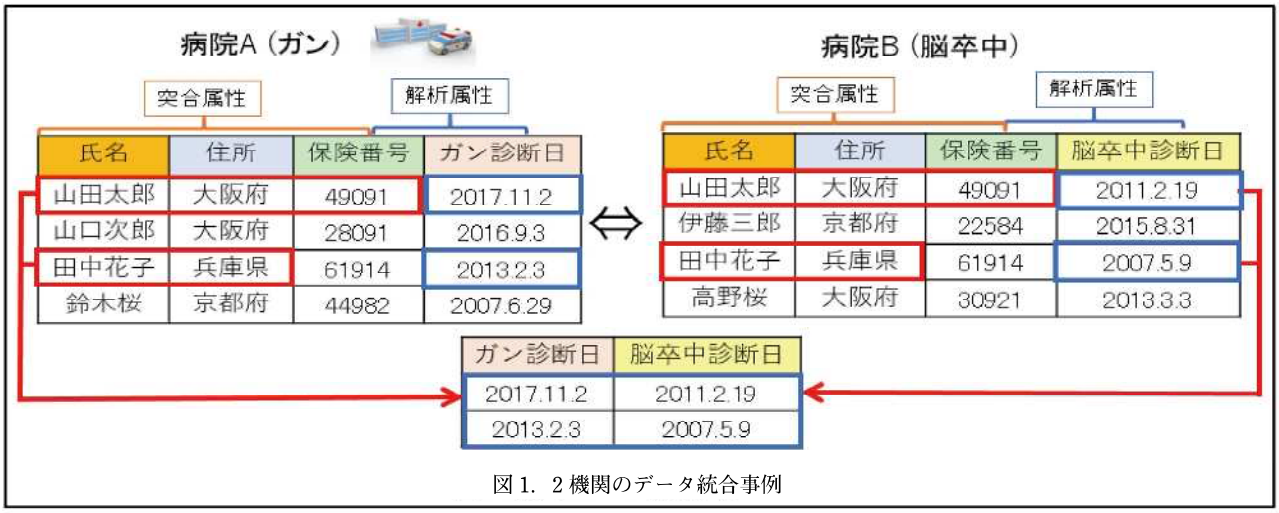


図 1．2 機関のデータ統合事例

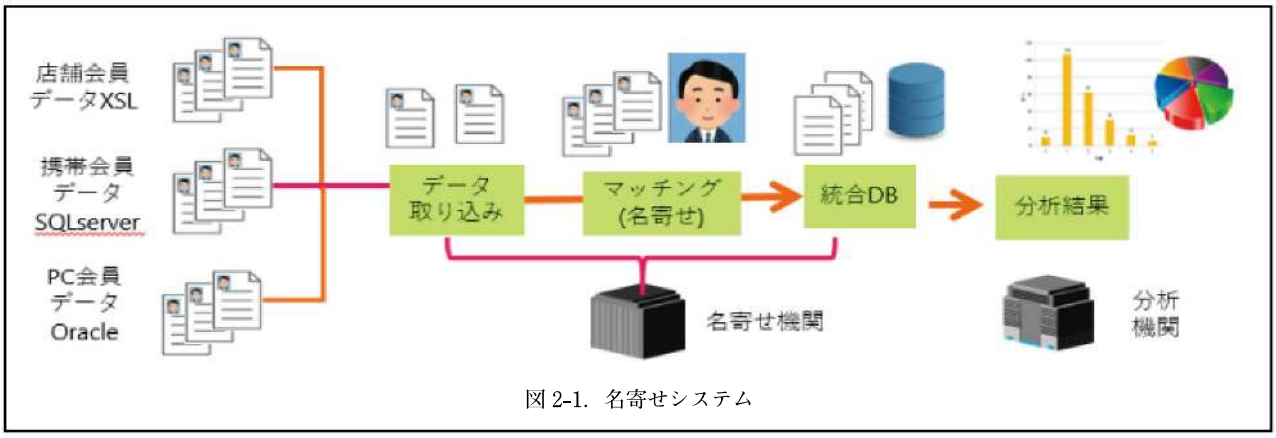


図 2-1.　名寄せシステム

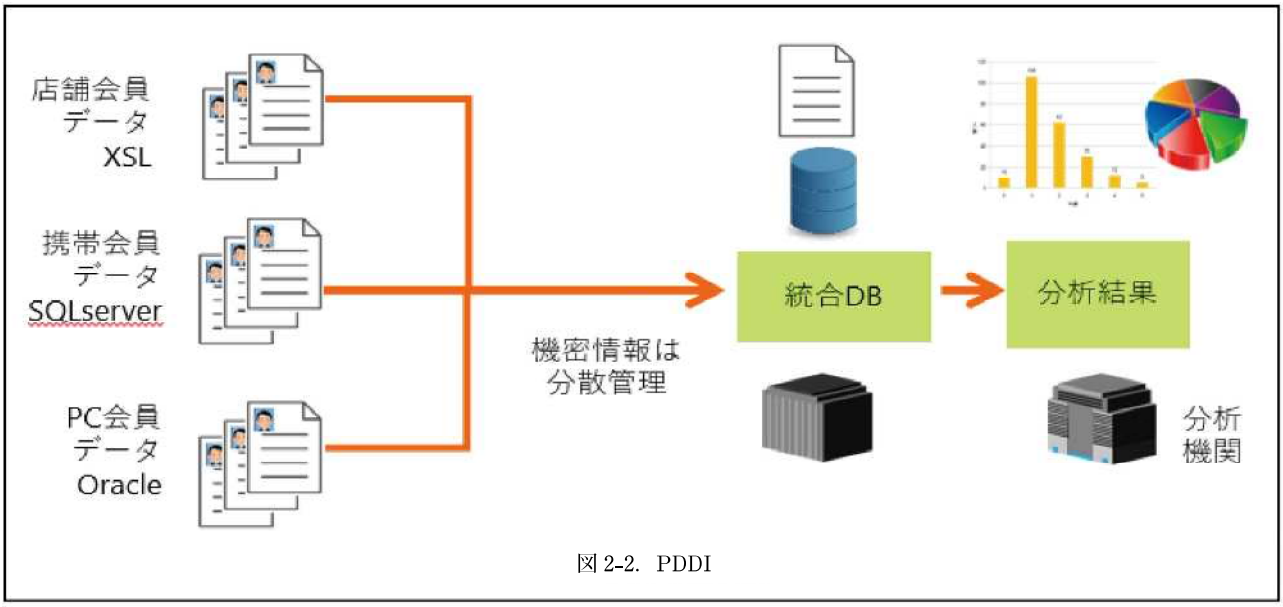


図 2-2.　PDDI

・各機関の処理時間は機関数に依存しません．

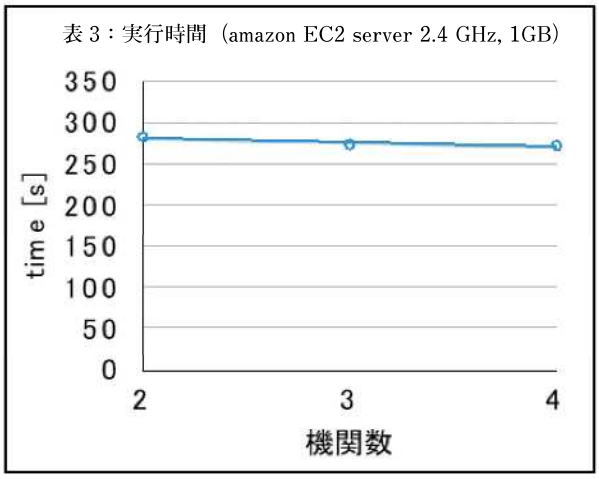
既存研究はデータサイズや機関数に依存する処理時間，通信量が大きな課題であるのみならず，図 1 のような複数の属性の統合方法がありませんでした．当研究室で考案された方式は，機関数に処理時間が依存せず，さらに複数の属性の統合を可能にします．表 2 に提案方式と既存方式の比較を記載します．

提案方式はデータ預託機関が不要で，各機関のデータ数の制限がなく，通信量，計算量を削減した方式となっています．既存方式 1 と提案方式の処理時間は表 3 に記載されています．機関数の二乗のオーダで処理時間が掛かる既存方式では，データ数が増えると非常に多くの処理時間がかかり，提案方式の優位性がわかると思われます．

表 2：提案方式と既存研究の比較

方式	既存方式 1 [1]	既存方式 2 [2]	既存方式 3 [3]
データ預託機関	不要	必要	不要
各機関の計算量 (機関数 n)	機関数 n の 2 乗の計算量	機関数に依存しない	機関数に依存しない
通信量	機関数 n の計算量	機関数 n の計算量	機関数 n の計算量
データ数の制限	全機関が同じデータ数	制限なし	制限なし
秘匿される情報	データ集合のみ	データ集合とその個数	データ集合とその個数

表3：実行時間（amazon EC2 server 2.4 GHz, 1GB）



3．欺瞞的防御 NW

様々なサイバー攻撃が世界中で問題となっています．またIoT機器の普及に伴い，身近な機器もサイバー攻撃の対象になりました．従来の固定機器間のネットワーク環境と異なり，IoT機器では無人状況で利用されることも多く，各種攻撃によりIoT機器が攻撃され，データが偽造，不正利用される危険性もあります．IoT機器の環境では，攻撃者は機器のデータのみならず鍵も入手し，さらに攻撃した機器を利用して，健全なIoT機器からの情報を入手することが考えられます．2016年10月21日に発生したIoT機器による大規模なDDoS攻撃では，Twitterなどのサービスが利用できなくなりました．このように，IoT機器の脆弱性は非常に大きく拡散する危険性が高いです．またDEF CONではIoT Villageが2015年から開始し，家庭用ルータ（ASUS），WiFi対応血圧モニター（Blicare社）などあらゆるIoT機器の脆弱性が指摘されており，IoT機器のセキュリティ向上は喫緊の課題といえます．

従来より利用されてきたネットワークの防御技術として，ファイアーウォール，IDS/IPS, Web Application Firewall（WAF）が挙げられます．ファイアーウォールは送信元，送信先のIPアドレスや接続ポートから通信の可否を決定します．IPS/IDSはファイアーウォールでは検知できない既存の攻撃の特徴を持つ攻撃を検知（IDS），破棄（IPS）します．WAFはWeb Applicationの脆弱性をついた攻撃を遮断します．このような防御手法は境界防御と呼ばれ，既知の攻撃に対する防御方法です．一方，標的型攻撃やゼロデイ攻撃などの未知の攻撃に対しては，従来の境界型防御と呼ばれる手法では防御が難しくなります．この結果，攻撃者は，設置された境界を突破して，ネットワーク内部で自由に行動が可能となります．欺瞞的防御システムとは，これら内部ネットワークに侵入できた攻撃者に対して，見せかけの偽のネットワークを構築することで，侵入した攻撃者からシステムを守る研究です（図3）．

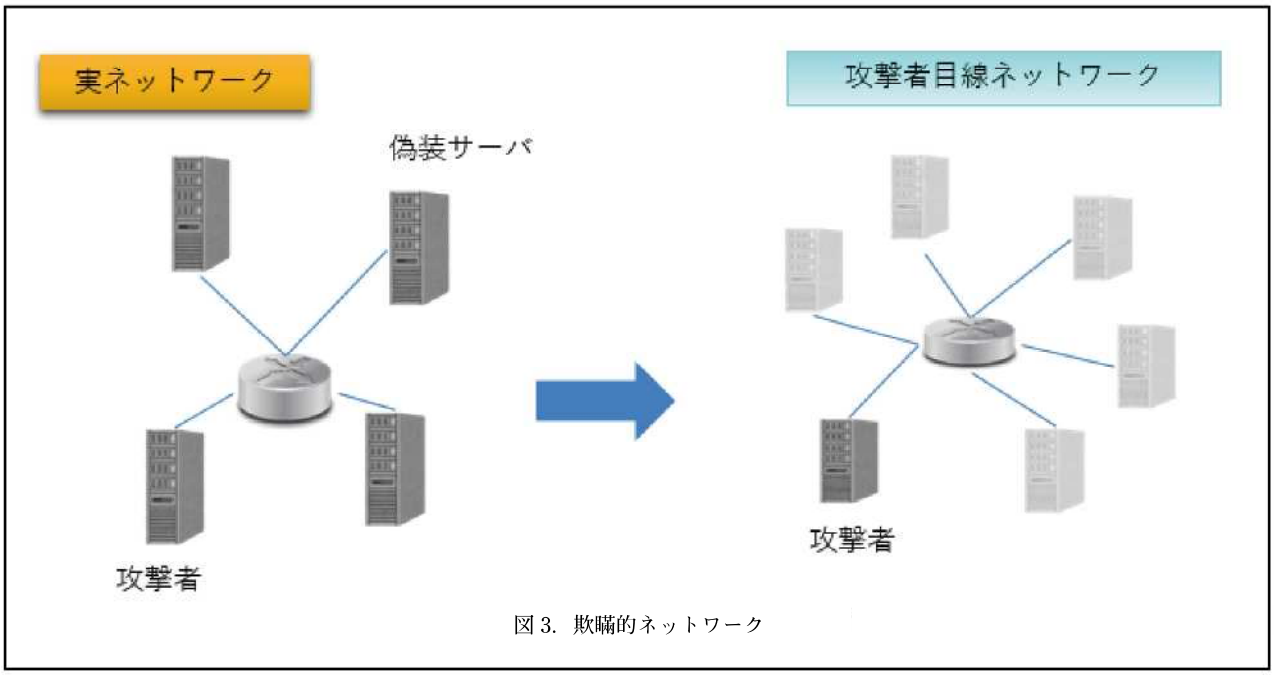


図3．欺瞞的ネットワーク

将来的には欺瞞的防御システムは通信量の多い企業の大規模なネットワークやIoTネットワークで有効に利用できることが望まれます．そのため，高速かつ効率的にパケットの応答が可能な欺瞞的防御システムの構築が必須です．当研究室では，Linuxに標準で用意されたeXpress Data Path（XDP）を用いて，高速なパケット処理を可能とする欺瞞的防御システムを設計と実装を提案しました[4].

４．セキュリティ人材教育

現代ではセキュリティ技術は情報インフラストラクチャーを支える必須の技術であるのみならず，医療，教育，公共サービスなど，様々な分野で活躍する人にとっても，切り離せない必須の知識ともいえます．このような背景のもと，文部科学省の学部生向けの高度IT人材を育成する教育プログラム，さらには，社会人向け情報技術人材育成プログラムが進められています．大阪大学工学部は学部に対しては「セキュリティ分野（Basic SecCap)」，社会人向けに対しては「enPiT Pro Security（ProSec)」を提供しています[5, 6]．社会人向けの教育は，講義は金曜の夜間（18：30以降）にオンラインと現地のハイブリッドで実施し，全国に講義配信されます．PBL（課題解決型）演習は，土日にハイブリッド開催（現地とオンライン参加）です．受講者は自宅や勤務先など，好きな場所でリアルタイムに受講できます．PBL演習もハイブリッド演習ですので，演習会場で対面の受講もできますし，自宅等で受講も可能です．コロナ期においても，これまでと変わらず，講義，演習とも実施しており，関西圏のみならず，名古屋圏，関東圏からも受講生が勉強しています．本セキュリティプログラムは，大学間連携による教育内容のダイバーシティと，産業界，あるいはセキュリティ関連団体との連携により，実践的人材育成の教育コースを開発していることも特徴です．また，講義，演習が，受講生達のコミュニケーションの場になっており，セキュリティで繋がる人的NWの構築にも貢献しています．

５．終わりに

本稿では，本研究室で実施している研究について紹介させていただきました．今後も，情報セキュリティに関する先進的な研究テーマに取り組んでいく所存です．

［参考文献］

[1] Kissner and Song, Privacy-Preserving Set Operations, CRYPTO 2005, LNCS 3621, Springer, pp. 241－257, 2005.

[2] Many, Burkhart, and Dimitropoulos. Fast private set operations with sepia. Technical Report, 345, 2012.

[3] Miyaji, Nakasho, and Nishida, "Privacy-Preserving Integration of Medical Data A Practical Multiparty Private Set Intersection", Journal of Medical Systems, Vol. 41 No. 3, pp. 1-10, (2017).

[4] 「多様なネットワークで利用可能な低レイテンシ欺瞞的防御システムの設計と実装」竹中 幹（大阪大学），高野 祐輝（大阪大学），宮地 充子（大阪大学），2021年暗号と情報セキュリティシンポジウム（SCIS2021）.

[5] https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/basic-seccap/index-jp.html

[6] https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/pro-sec/index-jp.html