プレスリリース
2019 年 12 月 12 日

国立研究開発法人情報通信研究機構
高知県・高知市病院企業団立高知医療センター
高知県公立大学法人高知工科大学
株式会社 Zenmu Tech
学校法人芝浦工業大学
株式会社 SBS 情報システム
スカパーJSAT 株式会社
日本電気株式会社
ISARA Corporation
ダルムシュタット工科大学

秘密分散と秘匿通信技術を用いた電子カルテ保管・交換システムを開発

～南海トラフ地震等の災害想定実験において、医療データを迅速に復元～

【ポイント】

- 秘密分散と秘匿通信技術により、災害に強くセキュアな電子カルテ保管・交換システムを開発
- 南海トラフ地震等の災害想定実験で、衛星経由で検索から 9 秒以内で医療データの復元に成功
- 医療機関間で相互参照可能な電子カルテのデータ交換標準規格に準拠し、医療への貢献に期待

国立研究開発法人情報通信研究機構（NICT、理事長: 徳田 英幸）と高知県・高知市病院企業団立高知医療センター（病院長: 島田 安博）及び連携協力機関から成るチームは、秘密分散技術[*1] と秘匿通信技術[*2] を組み合わせることにより、電子カルテデータのセキュアなバックアップと医療機関間での相互参照、災害時の迅速なデータ復元を可能とするシステムを開発しました。

このシステムを用いた実証実験では、800 km 圏のネットワークで結ぶ高知医療センターと大阪、名古屋、大手町、小金井にあるデータサーバに、1 万人分の電子カルテの模擬データを分散保管しました。次に、南海トラフ地震等により四国エリアが被災したというシナリオの下、それぞれのデータサーバから処方履歴、アレルギー情報などの災害時医療に必要とされるデータ項目を小金井のサーバ上に復元し、衛星回線経由で高知医療センターの端末に伝送しました。その結果、高知医療センターの端末で患者検索してから 9 秒以内で医療データを復元することに成功しました。これは、救急時の猶予時間といわれる 15 秒程度の要求に応えるものです。

今回の結果により、災害時に必要な医療データを迅速に届けることが可能になり、災害医療に大いに役立つことが期待されます。また、地上網が使える平時においては、医療機関の間で電子カルテデータを相互参照することが可能になります。なお、本成果について、京都で開催される日米欧量子技術国際シンポジウム（EU-USA-Japan International Symposium on Quantum Technology）にて、12 月 16 日（月）に発表します。

【背景】

2011 年の東日本大震災では、海岸沿いの医療機関の多くが倒壊し、電子カルテもサーバごと流されてしまいました。電子カルテなどの重要な医療データは、遠隔地にバックアップを取っておく必要があります。いざ災害時には多くの方を早く診療、治療する必要があるため、患者の氏名、住所、生年月日とプロファイリングに必要な投薬、アレルギー情報など必要最小限の項目だけを迅速に復元することが求められます。

一方、電子カルテのバックアップデータは、究極の個人情報であり、適切な暗号技術を用いて安全にバックアップする必要があります。さらに、共通のデータ交換規格を活

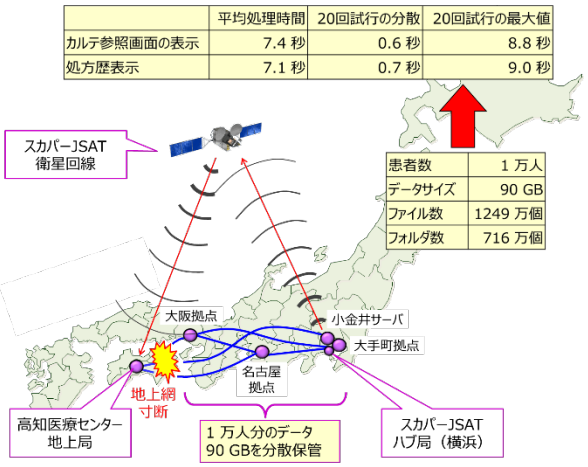

図 1 実証実験に用いたネットワーク接続図と性能評価結果

用すれば、異なる医療機関の間でも医療情報を安全に相互参照できるため、検査・投薬の重複防止や新しい医療技術の開発などにつながります。

しかし、これまで、電子カルテデータのセキュアなバックアップと医療機関間での相互参照、災害時に必要な医療データ項目の迅速な復元、という要件を全て満たすシステムは存在していませんでした。

【今回の成果】

我々は、秘密分散技術と秘匿通信技術を組み合わせることにより、電子カルテデータのセキュアなバックアップと医療機関間での相互参照、災害時を想定した場合に必要とされる医療データ項目の迅速な復元が可能な、保健医療用の長期セキュアデータ保管・交換システム（H-LINCOS: Healthcare long-term integrity and confidentiality protection system）を開発しました。

H-LINCOS は、高知医療センターとNICT のテストベッド JGN 上の大阪、名古屋、大手町、小金井のアクセスポイントを結ぶ 800 km 圏のネットワーク上に実装されています（図 1 参照）。また、H-LINCOS へのアクセス管理には、耐量子ー公開鍵認証方式という新しい技術が用いられており、医師や救急救命士といった保健医療分野 26 種の国家資格に基づいた高セキュアな認証機能が利用されています（補足資料参照 1（2）アクセス管理について 参照）。

このシステムを用いた実証実験では、1 万人分の電子カルテの模擬データ（計 90 GB）を用意し、データ交換標準規格*3 に準拠した保管用データ（SS-MIX データ）に変換して分散保管しました。次に、南海トラフ地震等の災害で四国エリアの光ファイバー網が寸断されているというシナリオの下、大阪、名古屋、大手町のデータサーバのうち 2 つのデータサーバから処方履歴、アレルギー情報などの項目を小金井のサーバ上に復元し、衛星回線経由で高知医療センターの端末まで伝送するという操作を行いました。

想定被災地にある端末で、患者の処方履歴やアレルギー情報などの医療データ項目を検索した結果、患者検索から 9 秒以内で端末上に復元することに成功しました。救急処置に必要な情報を入手する時間的猶予は 15 秒程度といわれており、今回の結果はその要求に応えるものです。これによって、災害時に必要な医療データを迅速に復元することが可能になり、災害医療に大いに役立つことが期待されます。

また、地上網が使える平時においては、SS-MIX データとして保管することにより、医療機関の間で電子カルテデータを相互参照することが可能になります。

【今後の展望】

今後、扱うデータサイズや接続する端末数を増やしながら、通信遅延や輻輳についての解析を進め、H-LINCOS の実用性を更に高めるための研究開発や実環境での運用方法についての検討を進めていきます。また、災害時の保健医療活動の効率化に向けて、H-LINCOS と災害時保健医療福祉活動支援システム（D24H）*4 の連携方法についても検討を進めていきます。

＜発表情報＞

・日米欧量子技術国際シンポジウム（EU-USA-Japan International Symposium on Quantum Technology）
・発表日時: 2019 年 12 月 16 日（月） 16:55～17:25
・発表セッション: 量子通信セッション
・講演タイトル: Quantum enhanced communication and cryptography
・演者: Masahide Sasaki（NICT）
・URL: https://www.jst.go.jp/kisoken/crest/isqt2019/index.html

各機関の役割分担

- NICT: H-LINCOS の開発、基本設計と実装、実証実験の取りまとめ
- 高知医療センター: H-LINCOS の要件定義と電子カルテ模擬データの提供
- 高知工科大学: H-LINCOS の要件定義と秘密分散方式の設計
- ZenmuTech: 高速秘密分散ドライバーソフトウェアの開発
- 芝浦工業大学: D24H との連動による H-LINCOS の災害医療への適用に向けた最適化
- SBS 情報システム: 電子カルテビューアの開発
- スカパーJSAT: 衛星通信回線の提供
- 日本電気: 高知医療センターと NICT 小金井間での秘匿通信回線の構築
- ISARA Corporation: 保健医療分野のための耐量子ー公開鍵認証方式の開発
- ダルムシュタット工科大学: セキュアなアクセス管理と改ざん防止法の開発

＜用語解説＞

***1 秘密分散技術**

原本データを無意味化された複数（n 個）のデータ（シェア）に分割し、異なるデータサーバに分散保管する技術。危殆化するデータサーバの数は、ある閾値（k 個）未満であり、かつ、データサーバ間は完全秘匿回線で結ばれていると仮定した場合、どんな計算機でも破れない機密性を実現できる。n-k 個以下のサーバが棄損しても、残った k 個のサーバからシェアを集めることで、原本データを復元できる。一方、k 個以上のシェアがそろわないと原本データは復元できない。

***2 秘匿通信技術**

通信路を盗聴された場合でも伝送されるデータの機密性が保たれるように、適切な暗号技術を用いてセキュアに通信する技術。現在主に使われているのは、共通鍵暗号を用いる秘匿通信であるが、計算機が高度化すると解読される危険性がある。近年、量子暗号も用いられるようになってきた。量子暗号は、どんな計算機でも解読できない暗号技術である。

***3 電子カルテデータのデータ交換標準規格**

2006 年度から始まった「厚生労働省電子的診療情報交換推進事業」（SS-MIX: Standardized Structured Medical Information eXchange）により策定された、医療機関を対象とした医療情報の交換・共有のための規約。医療機関の既存の情報通信インフラから各種情報を取得でき、標準的な形式の情報出力を可能にすることを特徴とする。電子カルテデータの標準化ストレージ構造として、患者 ID に基づく階層構造を持ったフォルダファイルの形式が定められている。

***4 災害時保健医療福祉活動支援システム**（D24H: Disaster/Digital information system for Health and well-being）

府省庁連携防災情報共有システム（SIP4D）及び被災地で支援活動を行う保健・医療・福祉チーム（DMAT、DPAT、DHEAT、日赤等）のそれぞれの独自システムと連携し、災害時の保健医療福祉支援活動に必要な情報を収集、整理統合、加工分析し、支援活動の意思決定判断に必要な情報を提供するシステム

研究支援

なお、本研究の一部は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「光・量子を活用した Society5.0 実現化技術」 https://www.qst.go.jp/site/collaboration/20660.html （管理法人: 国立研究開発法人量子科学技術研究開発機構）並びに「国家レジリエンス（防災・減災）の強化」（管理法人: 国立研究開発法人防災科学技術研究所）によって実施されました。

戦略的イノベーション創造プログラム（SIP） https://www8.cao.go.jp/cstp/gaiyo/sip/

補足資料

1. 今回開発した H-LINCOS の構成と機能

H-LINCOS は、電子カルテデータのセキュアなバックアップ、医療機関間での電子カルテデータの相互参照及び災害時等に必要な医療データ項目の迅速な復元を実現するシステムです。さらに、個人情報を扱うということから、セキュアなアクセス管理も行っています。

(1)セキュアなバックアップと相互参照について

H-LINCOS では、まず、電子カルテデータを SS-MIX データに変換します。次に、SS-MIX データの原本を無意味化された複数の分散データに変換し、最後に分散データを遠隔地のデータサーバへ秘匿通信し分散保管します(秘密分散)(図 2 参照)。

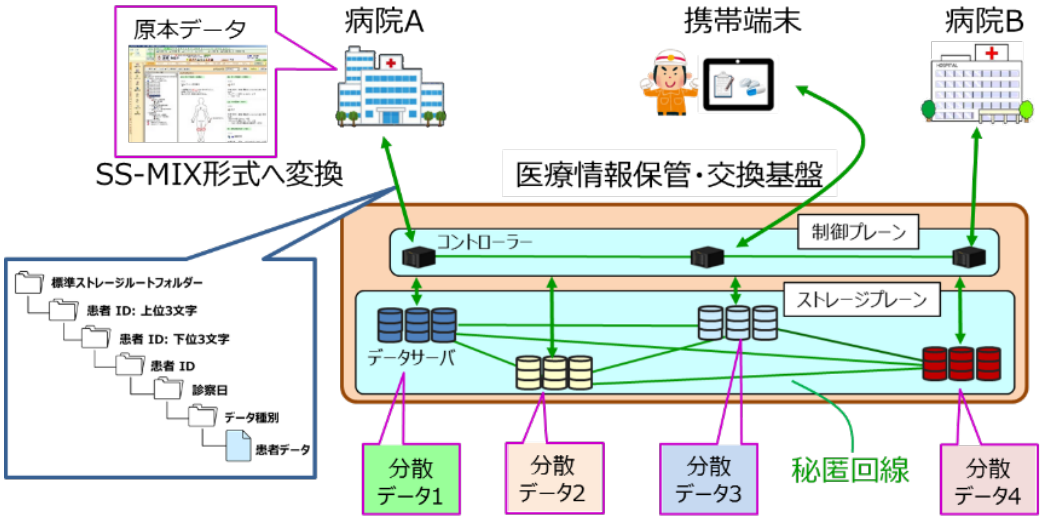

図 2 保健医療用の長期セキュアデータ保管・交換システムの概要

この方式では、一部のサーバが棄損しても、残ったサーバから原本データを復元できます。一方、一定数の分散データがそろわないと原本データは復元できないため、データの機密性を高めることができます。これにより、「セキュアなバックアップ」を実現できます。

実際の実装では、高知医療センターから提供された SS-MIX データを、JGN 上の小金井アクセスポイントまで 800 km にわたり秘匿通信し、そこで分散データに変換してから、大阪、名古屋、大手町の各拠点にあるデータサーバまで秘匿通信し、分散保管します。

秘匿通信回線は、事前に手渡しで配布した物理乱数を種鍵とする共通鍵暗号により構成されています。その安全性は、量子コンピュータでも解読が困難とされる「耐量子性」になっています。高知医療センターと小金井アクセスポイントには、日本電気の回線暗号の送受信装置が設置され、データリンク層で高速の暗号化を行えるようになっています。また、大手町と小金井を含む東京 100 km 圏では、これとは別に、さらに、量子暗号ネットワークで秘密分散保管が行えるようになっており、このシステムでは、どんな計算機でも解読できない「情報理論的安全性」を保証することができます。

また、電子カルテデータをデータ交換標準規格に準拠した SS-MIX に変換することで、「電子カルテデータの相互参照」が可能になります。さらに、高速検索のためのデータアクセス技術(高速秘密分散ドライバ)を開発し、「災害時に必要な医療データ項目の迅速な復元」を実現しました。

(2)アクセス管理について

H-LINCOS へのアクセス制御は、医師や看護師、薬剤師、救急救命士といった保健医療分野 26 種の国家資格に基づく権限管理と高セキュアなユーザ認証を用いて行われます。具体的には、現在、厚生労働省が推奨している保健医療用の公開鍵認証基盤(H-PKI: Healthcare Public Key Infrastructure)を踏襲し、さらに、次世代の耐量子ー公開鍵認証方式を新たに組み込んで、認証の安全性を量子コンピュータでも解読困難なレベルまで上げています。このいわゆる耐量子 H-PKI の概要を図 3 に示します。

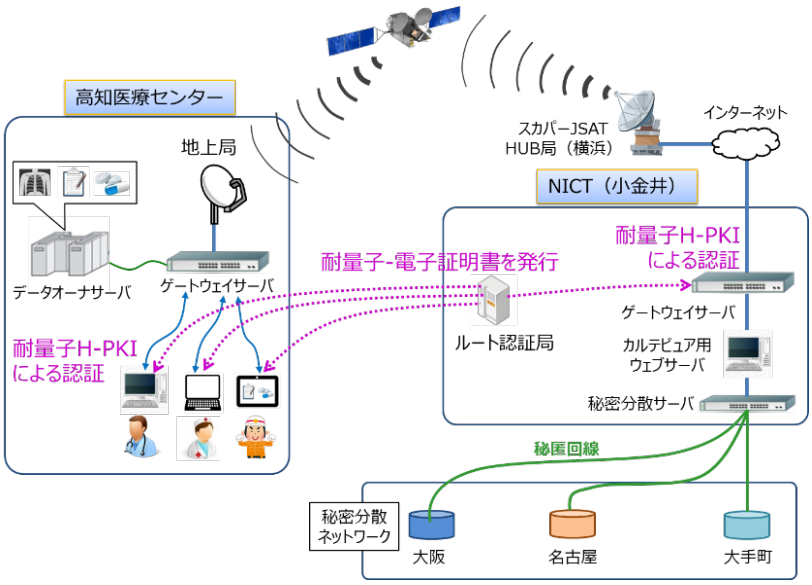

図 3 耐量子ー公開鍵認証基盤によるアクセス管理システム概要

耐量子ー公開鍵認証方式としては、現在、アメリカ国立標準技術研究所（NIST）が進めている標準化プロセスの中で有望と期待されている 7 つの方式を選択しました。具体的には、ルート証明書を発行するための 2 方式、鍵交換のための 2 方式、電子署名のための 3 方式を組み合わせ、全部で 12 種類の暗号ツールセット（いわゆる暗号スウィート）を用意し、これらをインターネット標準であるトランスポートレイヤセキュリティ（TLS）に準拠する形で実装しました。そして、全ての暗号スウィートが処理時間 100~250 ms 程度で正常動作することを確認しました。この処理時間は、既存の TLS 方式の約 10 倍程度となっているものの、十分に実用的な性能になっています。今回の SS-MIX データ復元実験では、最も高速で動作する暗号スウィートをアクセス認証に用いています。

2. 実証実験の結果について

	平均処理時間	20回試行の分散	20回試行の最大値
カルテ参照画面の表示	7.4 秒	0.6 秒	8.8 秒
処方歴表示	7.1 秒	0.7 秒	9.0 秒

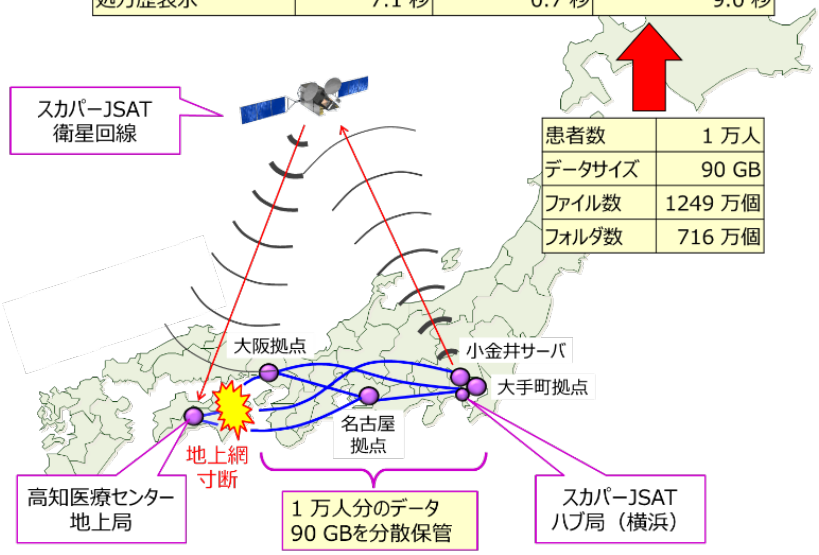

図 1 実証実験に用いたネットワーク接続図と性能評価結果（再掲）

災害時を想定した SS-MIX データの復元では、大阪、名古屋、大手町のデータサーバのうち 2 つのデータサーバを選択して、そこから処方履歴、アレルギー情報などの項目を小金井のサーバ上に一旦復元しました。次に、そのデータをインターネット上の秘匿通信回線で、横浜にあるスカパーJSAT の地上局まで伝送し、そこから衛星回線経由で高知医療センターの端末まで伝送して復元しました。

20 回の復元実験を行った結果、想定被災地にある端末で、患者 ID を入力して検索してから電子カルテ参照画面が表示されるまでの時間は、平均で 7.4 秒、最大で 8.8 秒でした。また、処方歴の選択ボタンを押してから表示までの時間は、平均で 7.1 秒、最大で 9.0 秒でした（図 1 参照）。

この結果は、本システムを用いることで、災害時に必要となる医療データの迅速な復元が可能であることを示しています。