サーバからの漏洩・盗聴を防ぐ暗号ビジネスチャット

ビジネス向けチャットアプリケーションにおいて，政府やサービス提供者による盗聴・漏洩を防ぐためのエンド・ツー・エンド暗号化技術の導入が望まれています．NTTセキュアプラットフォーム研究所では，端末にデータを残さないことで端末からの漏洩を防ぐだけでなく，サーバに対して秘匿したままメッセージの送受信と検索を可能にする，セキュアなビジネスチャットの試作を行っています．本稿では，その試作システムに使われている暗号技術を紹介します．

よしだ れお おかの ゆうき
吉田 麗生 /岡野 裕樹
おくやま ひろのぶ こばやし てつたろう
奥山 浩伸 /小林 鉄太郎
NTTセキュアプラットフォーム研究所

チャットのセキュリティ動向

著名なコンシューマ向けチャットアプリケーションには，日本やアジアではLINEやWeChat，欧米ではFacebook MessengerやWhatsAppがあり，各社の公式アナウンスによれば，それぞれ億単位のユーザを抱えています．これらのチャットアプリケーションでは近年，元CIA職員であるエドワード・スノーデン氏[(1)]やWikiLeaks[(2)]による告発などをきっかけとする通信に対する不安から，政府やチャット事業者によるチャット内容の盗聴・漏洩疑惑が浮上しています．さらに電子フロンティア財団による代表的なチャットアプリケーションに対する安全性評価[(3)]によって，各アプリケーションが達成している具体的な安全性とその実装方法について，ユーザの関心が大きく高まりました．この関心の高まりを受け，LINE，Facebook MessengerやWhatsAppでは，事業者にもチャット内容が盗聴できないことを保証するために，ユーザの端末でメッセージの暗号化・復号を実施し，事業者はチャットメッセージの配送だけを行うエンド・ツー・エンド暗号化技術などを導入し，チャットアプリケーションの安全性を高め始めています．

一方，ビジネス向けのチャットアプリケーション（ビジネスチャット）には，日本ではChatworkやTopicRoom，欧米ではSkype for BusinessやSlackがあります．コンシューマ向けとは違い，チャットデータは企業のものであるため，多くのアプリケーションでは端末にチャットデータは残さず，ログインごとにクラウドなどのサーバにアクセスしチャットデータを取得することで，端末の紛失や盗難時のデータの漏洩を防止するセキュリティ対策が実施されています．

ビジネスチャットのエンド・ツー・エンド機密性面の課題

ビジネスチャットでは，端末の紛失や盗難時にチャットデータの漏洩を防止するために，クラウドなどのサーバ上にデータを保存しています．しかし，ビジネス向けでは，多人数で利用することが前提です．また，その前提のために，人事異動，入社や退職に伴いチャットルームやトーク内のメンバが頻繁に変更になります．したがって，サーバにデータを保存しながら，エンド・ツー・エンドの暗号化を実現することは従来の暗号方式を用いるだけでは技術的に困難で，実際，実現できているアプリケーションはありません．また，チャットメッセージの全文検索は，処理速度向上を目的に，サーバサイドで実現するアプリケーションが多いですが，サーバに秘匿したままメッセージを検索することも技術的に困難で，こちらも実現できているアプリケーションがないのが現状です．

以上をまとめると，ビジネスチャットにおける機密性面の課題は以下の3点になります．

- 多人数でのエンド・ツー・エンド暗号化チャットを実現できること
- 暗号化チャットデータはサーバに保存され，チャットルームのメンバの変更・更新に伴い，閲覧メンバを変更・更新できること
- サーバにチャット情報を機密にしたまま，サーバ上でメッセージの全文検索ができること

NTTセキュアプラットフォーム研究所のめざす方向性

NTTセキュアプラットフォーム研究所では，長年培ってきた暗号技術を用いて，前述の課題を解決し，サーバからのチャット内容の盗聴・漏洩を防

止する安全なビジネスチャットを実現しようと取り組んでいます．そこで今回，次の３つの技術を開発しました．

・多者間鍵共有技術[3]
・代理人再暗号
・検索可能暗号

上記技術が適用されたビジネスチャットシステム概要を**図１**に示します．

安全なビジネスチャットを実現する３つの技術

■多者間鍵共有技術

盗聴される可能性のある安全でない通信路上で，情報のやり取りを行い，クライアント端末間でメッセージ暗号化・復号に用いられる鍵（共有鍵）を共有するプロトコルを鍵共有プロトコルといいます．共有鍵は，その後の通信を秘匿するために用いられます．２者間で行う鍵共有プロトコルとして，例えばDiffie-Hellman鍵共有プロトコルがあり，多くの既存のビジネスチャットで利用されています．しかし多者間で鍵を共有する場合，２者間鍵共有プロトコルを繰り返し実行する必要があるため非効率であり，また参加人数が限られるなど，多者間での鍵共有には技術的な課題があります．

NTTの多者間鍵共有技術では，中央に鍵仲介サーバを置き，このサーバを介して複数のユーザ間で鍵を共有します（**図２**）．これは直接ユーザ間で鍵を共有するよりもずっと効率的です．なお，共有鍵は各ユーザと鍵仲介サーバの持つ秘密情報から高度な計算を行うことで生成されるため，ユーザと鍵仲介サーバとの間で共有鍵そのものが流れることはなく，鍵仲介サーバには共有鍵を知られることはありません．さらに，ユーザの追加・削除が可能であり，またそのイベントに伴って鍵を更新する仕組みになっています．これにより「その時点で通信にかかわるユーザ（任意の人数可）のみによる，サーバからも秘匿された通信」が実現されます．

■代理人再暗号

代理人再暗号は，ある鍵K1で復号可能な暗号文を復号することなく，再暗号化鍵と呼ばれる鍵RKを用いて，別の鍵K2で復号できるように暗号文を変換する技術です．これにより，例

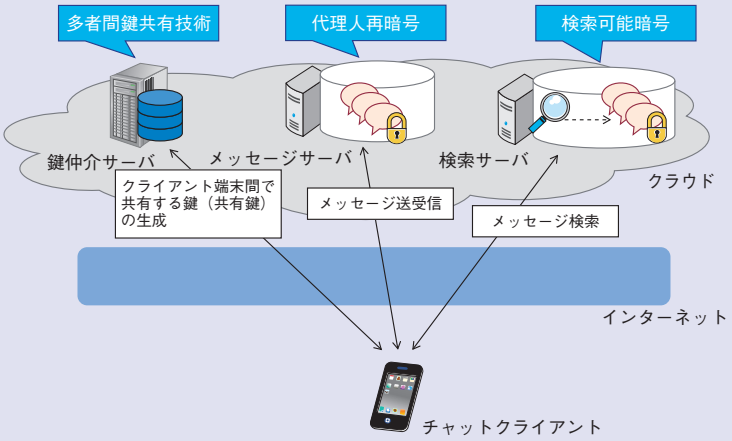


図１　暗号ビジネスチャットのシステム概要と開発技術

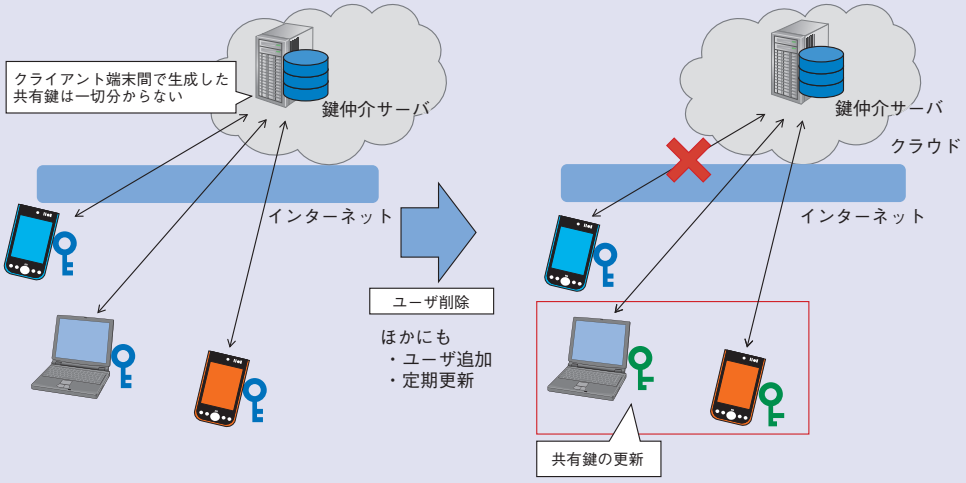


図２　多者間鍵共有技術

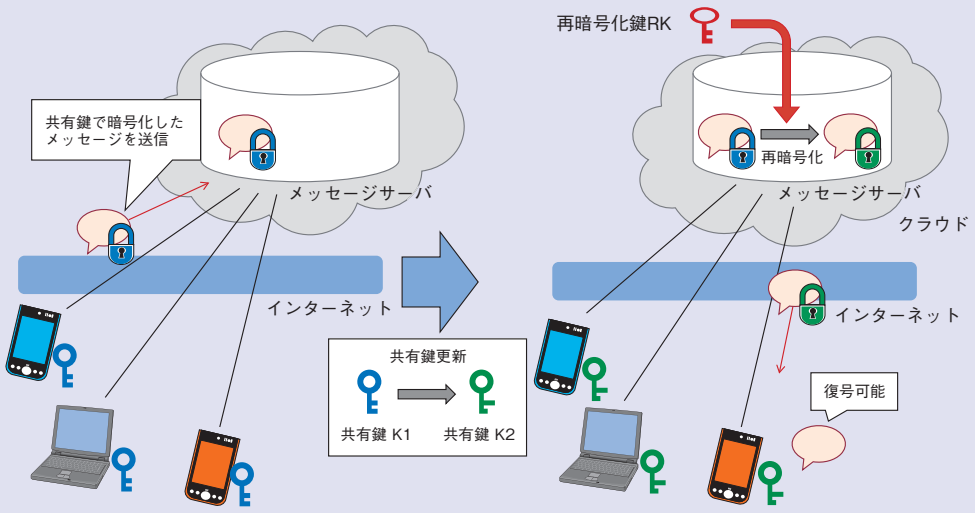


図 3　代理人再暗号

えばメッセージサーバSに置いたAさん宛の暗号文を，サーバSが再暗号化鍵を用いてBさんが復号できるように変換（再暗号化）することが可能です．サーバSに元の平文を知られることはありません．

本稿で紹介するビジネスチャットでは，組織改変・人事異動などでルームメンバが変更されると，多者間鍵共有技術により共有鍵が更新されます．その際，メッセージサーバに保存されたデータは更新された共有鍵で復号できなければなりません．NTTの代理人再暗号技術によって，サーバ側でメッセージを復号することなく，更新された共有鍵で復号できるよう再暗号化されます（**図3**）．これにより，ルームメンバ変更イベントが発生しても，サーバに秘匿したまま現在の参加メンバのみがメッセージを復号することができます．また，従来の代理人再暗号技術は暗号化されたデータ全体に対し再暗号処理を行うため処理速度は遅く，ビジネスチャットに適していませんでした．NTTの代理人再暗号技術では，安全性を保ちつつ必要な部分のみへの処理に限定することで，従来の代理人再暗号技術と比べて効率的な再暗号処理を実現しています．

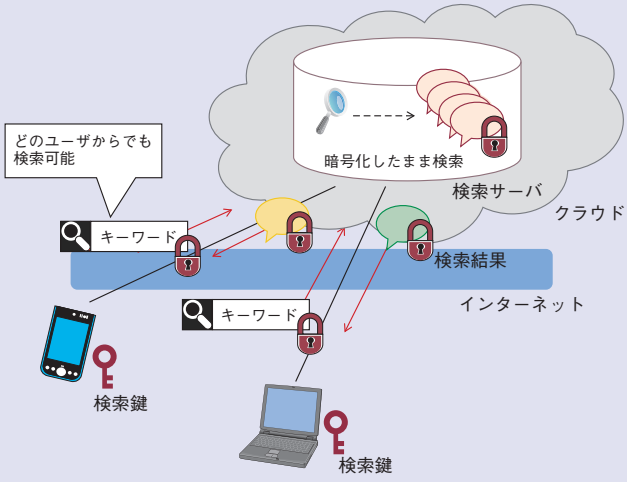


図 4　検索可能暗号

■検索可能暗号

検索可能暗号とは，検索対象のデータとキーワードを暗号化したまま，キーワードを含むデータを検索できる暗号技術です．共通鍵ベースの検索可能暗号では，ユーザは鍵（検索鍵）を生成し，検索鍵を用いて，検索サーバから秘匿しておくデータに対するインデックスを秘匿化します．サーバは，ユーザによって秘匿化されたインデックスを，暗号化されたデータとともに検索サーバに保存します．検索鍵を用いて秘匿化されたクエリをユーザが送信すると，サーバは秘匿化されたクエリと秘匿化されたインデックスから，該当するデータを暗号化されたまま検索し，その結果をユーザに送付します（**図4**）．ビジネスチャットシステムのキーワード検索では，過去のメッ

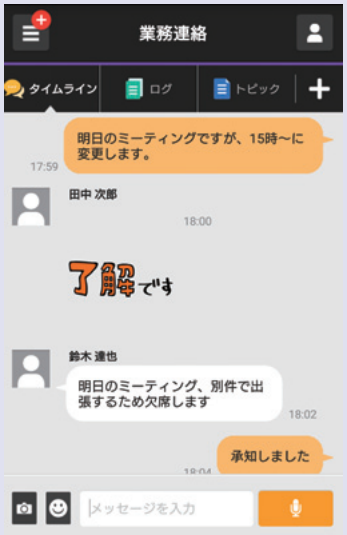


図５　３つの技術を適用したTopicRoom使用画面例

セージから必要な情報を素早く得られることが必要です．NTTの検索可能暗号技術は，リアルタイム性が求められるビジネスチャットシステムに適した，高速な秘匿検索を実現しています．また，ユーザが追加された場合でも，そのユーザは暗号化したキーワードを生成し，検索することが可能です．

評　価

前述の技術をTopicRoomに適用し，その評価を行いました．TopicRoomとは，NTTソフトウェアが販売する，クラウドベースのビジネス向けグループチャットです．クライアントアプリのUI（User Interface）はそのままにしつつ，上記暗号技術適用のため，鍵配送サーバと検索サーバを新規追加し，メッセージサーバに再暗号化機能を追加しました．クライアントアプリの動作と，メッセージサーバ・検索サーバに保存されているデータを解析したところ，以下の機能が正しく行われていることを確認しました（**図５**）．

表　TopicRoomの処理時間の比較

項目	通常の処理時間	３つの技術を適用した処理時間
トークルーム入室	平均３～４秒	平均３～４秒
メッセージ送受信	平均１秒以内	平均１～２秒
キーワード検索	平均１秒以内	平均１秒以内

・ユーザ追加・削除に伴う，共有鍵の更新（多者間鍵共有技術）
・共有鍵の更新に伴うメッセージの再暗号化（代理人再暗号）
・インデックスの秘匿化と秘匿キーワード検索（検索可能暗号）

また，通常のTopicRoomと上記３つの技術を適用したTopicRoomにおけるログインやメッセージ送受信，キーワード検索における処理時間の比較を**表**に示します．

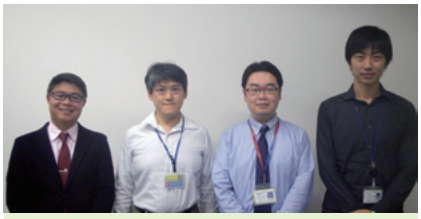
今後の展開

サーバからの盗聴・漏洩を防止する安全なビジネスチャットを実現する暗号方式を考案しました．また，それらの方式を実装した試作ビジネスチャットを開発し，その動作を確かめた結果，実用に耐える性能を実現できたと確認しました．

このビジネスチャットシステムについては今後商品化をめざしていきます．また，今回用いた暗号方式は学会・論文発表を行っていきます．さらに，その方式をVPN（Virtual Private Network）やメールなどビジネスチャット以外のアプリケーションにも応用できると考えており，実現に向けて取り組んでいきます．

■参考文献

(1) G. Greenwald：“No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,” Picador USA, 2015.
(2) https://wikileaks.org/nsa-japan/
(3) https://www.eff.org/secure-messaging-scorecard
(4) K. Yoneyama, R. Yoshida, Y. Kawahara, T. Kobayashi, H. Fuji, and T. Yamamoto: “Multi-cast Key Distribution: Scalable, Dynamic and Provably Secure Construction,” Proc. of ProvSec 2016, pp.207-226, Nanjing, China, Nov. 2016.



（左から）吉田　麗生/ 小林　鉄太郎/ 奥山　浩伸/ 岡野　裕樹

NTTセキュアプラットフォーム研究所では暗号技術を活用し，安心・安全かつ実用的なサービス提供の実現をめざします．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
企画担当
TEL　0422-59-3212
FAX　0422-59-2971
E-mail　scpflab@lab.ntt.co.jp