安全な暮らしを支えるセキュリティ技術の研究開発

サイバー攻撃が日々激化、巧妙化を続け企業システムの安全が脅かされています。一方で、マイナンバーの民間利用を見据えた、厳格な本人確認による新しいサービスが検討され始め、パーソナル情報を保護しつつ、確実に本人確認が行える技術が求められています。これらの課題の解決のために、富士通研究所では、最先端の技術開発に取り組んでいます。本報告書では、巧妙なサイバー攻撃をAI（人工知能）の活用により効率的に抽出する技術と、生体情報を安全に暗号鍵にする技術をご紹介します。

AIのサイバー攻撃検知への適用技術

背景

サイバー攻撃は激化の一途をたどり、政府や企業などのネットワークは様々な攻撃にさらされています。特に近年では、脆弱性スキャンやDoS攻撃（Denial of Service Attack）といった大量の既知の攻撃に紛れて、標的型攻撃などの巧妙な攻撃も行われています。こうした巧妙な攻撃を見つけるには、ネットワーク機器などから出力されるログを監視・分析する手段が有効だといわれています。しかし、巧妙な攻撃は攻撃頻度が低いため、膨大なログを人手により分析し、攻撃を発見することは困難な状況です。

富士通研究所では、AI技術を活用し人手では見つけることが困難な脅威を可視化するセキュリティログ分析技術を開発しました。この技術により、ログの分析者は、大量の既知攻撃に隠れた巧妙な攻撃を効率的に抽出することが可能になります。

開発した技術

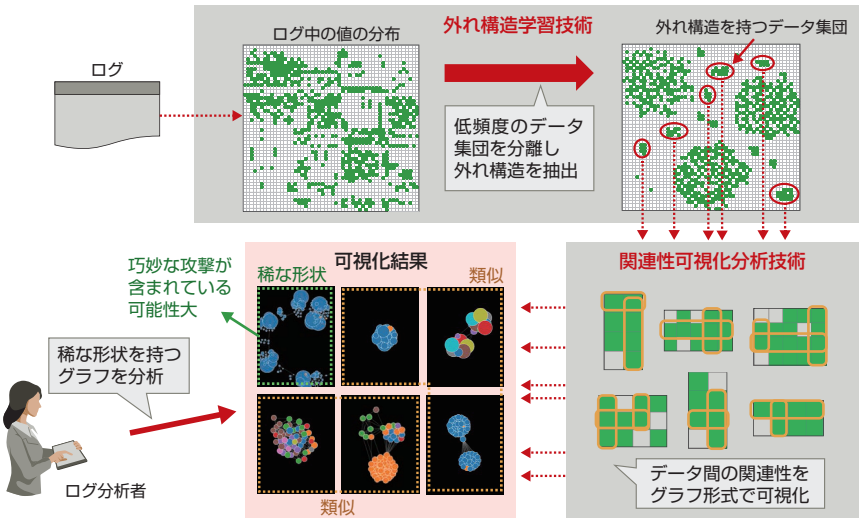
巧妙な攻撃抽出のために、富士通研究所では「外れ構造学習技術」と「関連性可視化分析技術」の2つの技術を開発しました。

外れ構造学習技術では、膨大なログを分析し「外れ構造」という稀な特徴を持つ小規模のデータ集団を抽出します。巧妙な攻撃は攻撃頻度が低いため、この外れ構造に含まれる可能性が高くなります。

関連性可視化分析技術では、外れ構造を持つデータ集団の可視化を行います。可視化したデータ集団は、攻撃の種類によりグラフ形状に特徴が出ます。この特徴を利用して、外れ構造を持つデータ集団を攻撃の種類ごとに分類します。

ログ分析者は可視化結果を分析することで、データ集団から巧妙な攻撃を効率的に抽出できます。

AI技術を活用したセキュリティログ分析技術：処理の流れ



1. 外れ構造学習技術

外れ構造学習技術では、ログに出現するデータの特徴の出現頻度に着目し、ログの中で稀な特徴を持つ小規模のデータ集団を抽出します。従来の学習技術では、ログ内で頻出する特徴にのみ着目してログを分類・抽出していました。そのため、大量に発生した攻撃は抽出できたとしても、それらに紛れて発生した小規模の特異な攻撃を抽出することは困難でした。

そこで外れ構造学習技術では、稀な頻度でログに含まれる特徴にも着目し、頻度の低い特徴を共有するデータ集団の分離と、頻度の低い特徴が分断された複数のデータ集団の統合を繰り返します。これにより、ログの中で稀な特徴を共有する「外れ構造」と呼ばれる小規模のデータ集団を抽出できます。

2. 関連性可視化分析技術

次に、外れ構造を持つデータ集団に対し、データ間の関連性をグラフ形式で可視化します。

外れ構造を持つデータ集団の中にも、発生頻度が低い既知の攻撃が数多く含まれます。それらの攻撃を可視化すると、そのグラフ形状が類似することが判明しました。そこでこの特徴に着目し、ログ分析者は、稀な形状を持つグラフを抽出します。稀なグラフ形状を持つデータ集団は、ほかとは異なる特徴を持つ攻撃に該当するため、巧妙な攻撃を抽出する可能性をより高めることができます。

このように、関連性可視化分析技術では、可視化結果を比較し、稀なグラフ形状を持つデータ集団を抽出します。これにより、巧妙な攻撃である可能性が高いデータ集団を絞り込むことが可能となり、ログ分析者は巧妙な攻撃を効率的に抽出できます。

実環境ログでの検証

開発した技術を実環境より得られたログに適用し、検証を行いました。ログから外れ構造を持つデータ集団を抽出し、可視化結果を比較した結果、2〜3の稀なグラフ形状を持つデータ集団を抽出することができました。これらのデータ集団を詳細に分析したところ、ある巧妙な攻撃が含まれていました。この攻撃は、以前研究所が約3か月かけて抽出した攻撃であり、開発した技術では約1日の分析により抽出することができました。このことから、開発した技術はログから巧妙な攻撃を効率的に抽出可能であることが検証できました。

今後の取り組み

現在、本技術は富士通クラウドサービスの監視で試験運用を実施しています。今後は、分析精度を高め、富士通クラウドサービスの安全な運用・管理に貢献します。

自身の生体情報を暗号鍵にする技術

背景

インターネットサービスの普及に伴い、IDやパスワードなどをはじめとする個人の秘密にしたい情報（以下、秘密情報と記す）が増えています。それらの秘密情報をすべて覚えきることは困難であり、現状では標準の暗号化技術であるAESなどで暗号化して管理されることが多くなっています。利用者は暗号化したデータを復号するための「暗号鍵」をICカードに格納したり、パスワード認証でガードを掛けたりするなどして安全に管理する必要がありました。そのため、身一つで本人認証ができる生体情報を本人固有の鍵として個人の秘密情報を暗号化し、安全に管理する技術が求められています。

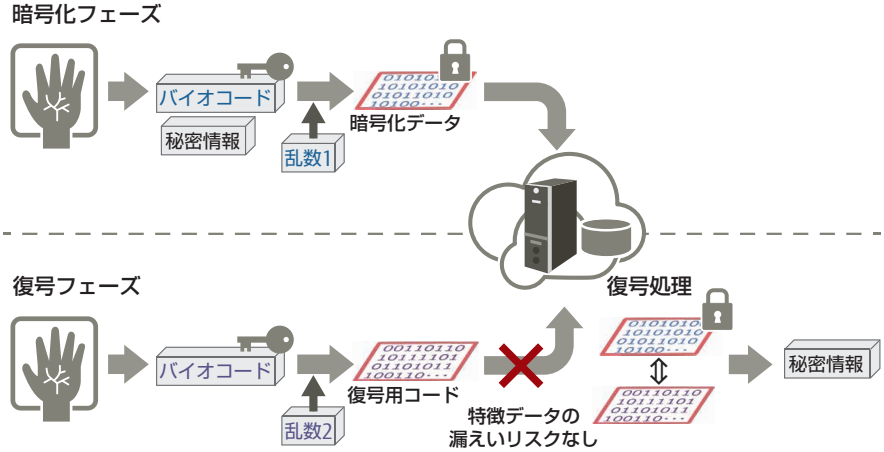
一方で、「生体情報を暗号鍵に利用する技術」の従来方式では、生体情報から抽出した特徴データ※1を暗号鍵に用いるため、復号時には特徴データをそのまま利用することが一般的でした。クラウド上などのオープンなネットワークを経由して使用するには、万一の生体情報の漏えいを防ぐために、より安全に復号させる技術が必要でした。

富士通研究所は、手のひら静脈画像から特徴データを2048bitのコードとして抽出するバイオコード技術※2を応用し、秘密情報をバイオコードで変換して暗号化する技術を開発しました。暗号鍵に利用するバイオコードをも乱数で変換して保護するため、オープンなネットワークを経由するクラウドサービスでの利用に拡大できます。

〔※1〕特徴データ：人の生体的な特徴がデータ化されたもの。

〔※2〕バイオコード技術：富士通研究所の独自技術で、手のひら静脈画像から抽出した2048bitで表されるコード。本技術の概要は、「富士通グループ情報セキュリティ報告書2014」に掲載。

バイオコードを用いた暗号化・復号の流れ



開発した技術

今回、「乱数により生体情報を保護する技術」と「誤り訂正符号を用いて秘密情報を復元する技術」の2つの技術を開発し、手のひら静脈を用いたバイオコード技術に適用しました。

1. 乱数により生体情報を保護する技術

暗号化フェーズでは、乱数で変換したバイオコードを秘密情報に加えることで「暗号化データ」を生成し、これをサーバに登録します。

復号フェーズでは、暗号化データを復号するときに用いる鍵として復号用コードを用い、端末側で安全なデータに変換したうえでサーバに送信します。復号用コードは、バイオコードを乱数で変換して生成します。乱数は暗号化と復号のそれぞれでシステムが無作為に決定できるため、毎回異なる安全な復号用コードが生成されます。

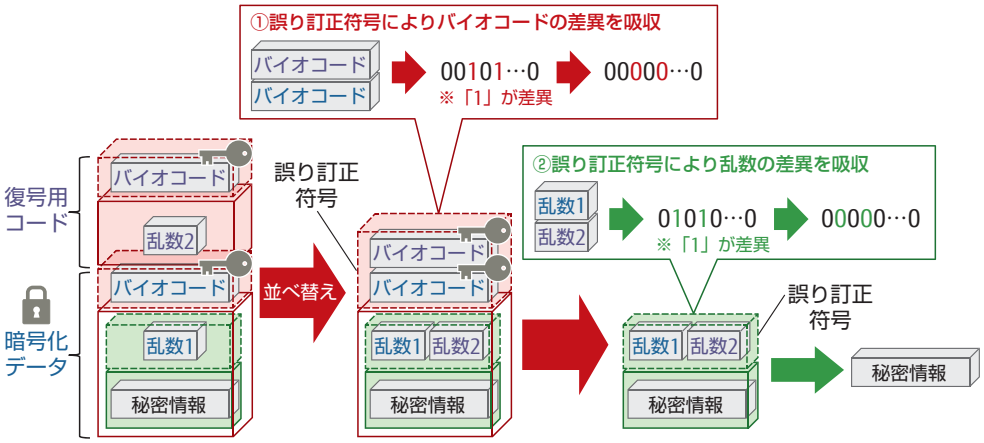
2. 誤り訂正符号を用いて秘密情報を復元する技術

生体情報を入力する際の動作や姿勢の変化により生じる微妙な差異や、毎回異なる乱数を加えたことによる差異を吸収するため、誤り訂正符号を暗号化方式に応用しました。誤り訂正符号は伝送路で発生するデータの損失を補償する技術として広く用いられています。

誤り訂正符号を用いた復号処理では、ステップ①で暗号化用のバイオコードに復号用のバイオコードを演算して得られる差異を訂正します。ステップ②では暗号化の際に加えた乱数に復号で利用した乱数を演算することで得られる差異も同様に訂正し、秘密情報を復元します。

このように、本人であれば暗号化と復号のそれぞれで入力した生体情報が類似しているため、誤り訂正の技術を用いて暗号化データから秘密情報を正しく取り出すことができます。

誤り訂正符号を用いた秘密情報の復元



効果

生体情報のみで暗号化・復号処理が可能であるため、既存の暗号化技術で必要とされてきた「暗号鍵の管理」が不要になります。すなわち、暗号化データを格納するサーバ上に暗号鍵が同時に保持されることはないため、運用がより安全になります。また、暗号化や復号の際に利用する生体情報は乱数で変換されるため、変換前の生体情報がネットワークに流れることはありません。これにより、生体情報を用いた暗号化技術を、クラウドサービスでの利用に拡大できます。

今後の取り組み

復号処理の高速化や暗号化できる秘密情報の種類の拡充などを進めると共に、暗号化した本人しか復号できない特徴を活かして、マイナンバーの管理など様々な利用シーンへの適用を検討し、本技術の実用化を目指します。また、バイオコードの開発も併せて検討し、指紋など利用可能な生体情報の種類も拡充していきます。