WHITE PAPER | 2014 年 10 月

高度なモデルを使用した 3D セキュアの本人認証

リスクに関するモデルと e コマースの動作ベースの本人認証によって、損失を削減できるだけでなく、摩擦のないチェックアウトと低リスクの取引が可能になります。

Paul Dulany
Hongrui Gong
Kannan Shah
CA Technologies、高度な分析およびデータ・サイエンス

ca technologies

目次

概要

課題

発行者は e コマースの決済処理を保護すると同時に、顧客がスムーズにチェックアウトできるようにする必要があります。最大の課題は、正規の顧客にシームレスなチェックアウトを提供することによって取引の放棄や異なる決済フォームの使用を防止しながら、違法な取引を防止することです。動作ベースの本人認証を使用する場合、追加の本人認証を顧客に求める取引を判断することは、顧客の不便を解消し、正規の取引をより正確に識別する上で重要です。リスクベースと動作ベースの認証を提供する場合、ルールは重要な構成要素になります。モデルを追加して、リスクベースのルールを効果的に適用できれば、不正な本人認証を大幅に抑制できるだけでなく、正規の顧客への影響の低減、カード所有者のエクスペリエンスの向上、発行者の損失減少などの利点があります。

ビジネス・チャンス

3D セキュアのチャネルは発行者にとって多くのチャンスをもたらします。e コマースで詐欺が大幅に増加し、法的義務も変化した現在、3D セキュアの本人認証は発行者にとって防御の第一線になっています。ただし、この防御の第一線を最大限に活用するには、適切に使用する必要があります。CA Risk Analytics では、本人認証詐欺検知システムには提供されない独自の情報を使用して、本人認証中に e コマースを検査できます。本人認証のリスク評価は、正規のカード所有者に中断のないチェックアウトを提供するためには必要不可欠です。CA Risk Analytics を使用すると、発行者は損失を低減しながら、顧客の不便を解消できます。

メリット

CA Risk Analytics を使用すると、発行者は 3D セキュアを導入している加盟店におけるオンライン・アクティビティのリスク・レベルを評価できます。このソリューションでは、正規のカード所有者以外による e コマースのリスクがリアルタイムでトランスペアレントに評価されます。また、正規の取引の大半が特定されるだけでなく、顧客には影響しないため、スムーズに購入を続けることができ、その間に不正な取引も特定されます。デバイスの ID、ジオロケーション、接続特性および履歴パターンを使用して、取引が試行されるたびにリスクを評価できます。

CA Risk Analytics の重要なメリットは、動作ベースのニューラル・ネットワーク・モデルなどの高度な Regional Model を使用して取引のリスク・レベルを評価し、試行された取引のリスクを示すスコアを提供できることです。また、CA Risk Analytics のルールを使用すると、モデルのスコアと他のビジネス要因を組み合わせて取引に対する適切な対応を判断できるため、ソリューションの効果が大幅に向上します。

セクション 1

3D セキュアが提供する e コマースの損失抑制の基盤

3D セキュアでは、発行者は 3D セキュア・チャネルの保護とメリットを活用できます。

3D セキュア・チャネルでは、e コマースの本人認証が実行されます。本人認証と権限認証は異なります。本人認証は、取引（または他のアクティビティ）を開始した個人が本来の正規のカード所有者であることを確認することを指します。権限認証は、（確認済みの）カード所有者が取引を行う権限があるかどうかを検証することを指します（ポリシー、利用可能残高、口座の状態などに基づく）。詐欺は本人認証でも権限認証でも発生し、検出されますが、この 2 つには大きな違いがあります。たとえば、本人認証は当時者の詐欺を直接防止するものではありません。しかし、詐欺のタイプによらず、取引を試行する個人の本人認証は、取引自体の有効性を確認する第一歩になります。

カードを提示する取引では、長年、実物のカードを持っていることが本人認証の重要な要素とされてきました。不正ユーザの巧妙化に合わせて、発行者はカードのセキュリティを強化して対応していました（磁気ストライプ、CVV/CVC/CID、スマート・カード）。そのデータまたはそのデータによる本人認証の結果は通常、権限認証リクエストを通して送信されます。

実物のカードを使用しない（CNP）取引では、実物のカードによる本人認証が不可能なため、一般的に加盟店がその義務を負います。しかし、e コマースの出現によって、e コマースで使用できる強力な本人認証の開発が必要になりました。権限認証リクエストに関するデータは取引の権限認証には十分ですが、e コマースの本人認証には不十分です。そのため、権限認証リクエストとは異なる情報を使用し、取引を行う個人の本人認証を目的とした 3D セキュアが開発されました。その処理には、基本的に権限認証とは異なる独自の考え方が必要です。ただし、本人認証の結果は権限認証システムに対しより適切なコンテキストを提供するため、権限認証のストリームで使用されます。

曖昧さを避けるため、この文書では「詐欺」という用語は、e コマースの 3D セキュアの取引における本人認証の詐欺を指します。

3D セキュアを使用すると、e コマースの本人認証が試行された段階で検査できます。また、権限認証の詐欺検出システムには提供されない独自の情報を使用するため、権限認証リクエストを作成する前に不正な取引を防止できます。CA Risk Analytics システムでは、この固有の情報には各デバイス固有の ID（デバイス ID）、取引のためにカード所有者がアクセスする URL（加盟店の URL）、デバイスの現在の IP アドレス、サードパーティのデータ・プロバイダからの補助的な情報（デバイスの場所、接続速度、アノニマイザ ID など）が含まれます。この情報によって、金額、通貨、加盟店の名前と ID、カード識別子などの従来の情報が大幅に増補されます（従来の情報に代わることはありません）。また、それによって、3D セキュアの本人認証モデルでは、従来の情報のみの本人認証モデルより多くのメリットが提供され、不正な本人認証の検知が強化されるだけでなく、正規の利用への影響が最小化されます。

3D セキュア・チャネルでは、本人認証の分析に必要な情報がリアルタイムで提供されるため、取引に使用されるカード、デバイスまたはその他の重要な要素に関する情報をリアルタイムで更新できます。そのため、その後の取引で本人認証を評価するときに、より多くの情報を活用できます。これは、クラウドの SaaS 環境で銀行のデータを確認するときには特に効果的です。

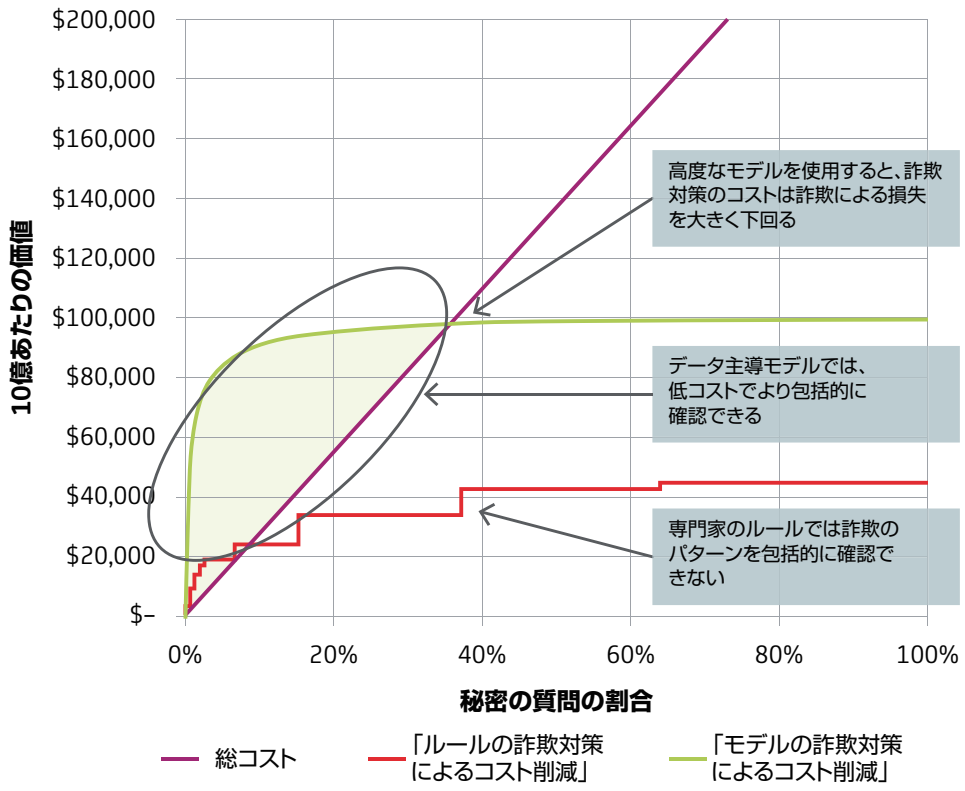
また、e コマースにおける摩擦の緩和にも役立ちます。初期の 3D セキュアでは、3D セキュアを利用する加盟店で買い物をすると、秘密の質問が表示されます。これは、ワンタイムパスワード（OTP）などの強化策を使用していれば効果的ですが、取引自体に必要な情報（有効期限や CVV2 など）を使用するなど、秘密のレベルが低ければ、損失の防止にはほとんど役立ちません。さらに、別の問題もあります。カード所有者に秘密の質問を表示することで取引に「摩擦」が起こり、取引を先に進めることに強い抵抗を感じさせたり、顧客エクスペリエンスに悪影響を及ぼします。

顧客エクスペリエンスに対する悪影響は質だけでなく、量にも及びます。そのために、取引の放棄や「擬似障害」が大幅に増えます。取引の放棄は、インターチェンジ・フィーが失われるだけでなく、クレジット・カードのリボルビングの残高の損失、または顧客の利用が減少するなど、より大きな影響があるため、特に、デビット・カードとクレジット・カードにとって深刻な問題です。これらは、マイナスの顧客エクスペリエンスによる発行者への影響を定量化して、取引の摩擦を減少させる強力な動機になります。極端な場合、すべての顧客に秘密の質問をすると、中断のコストが削減した損失を上回る可能性さえあります。そのため、取引のリスクを評価し、顧客の処理に干渉するのは十分正当化できる場合に限定することが重要です。これは、動作ベースの本人認証では特に効果的です。

次のページの図 1 では、詐欺検知の総コスト（取引放棄による機会喪失を含む）（紫色の線）、一般的なルール・システムによるコスト削減（赤色の線）および一般的な CA Risk Analytics Regional Model によるコスト削減（緑色の線）を示しています。秘密の質問の割合が増えると、システムの運用コストも増えます。ルール・システムでは一般的に、詐欺を包括的に確認することができないため、システムの運用コストはルールによって削減したコストをすぐに超えてしまいます。高度なデータ主導のモデルでは、低コストで詐欺を包括的に確認できます。緑色の影の部分には、ルールに対するモデルのメリットを示しています。

図 1:

詐欺検知の総コスト



セクション 2

動作ベースの本人認証

動作ベースの本人認証では、カード所有者、加盟店および支払い人のデバイスのアクティビティの通常のパターンから現在の取引を検査し、その情報だけで支払い人が間違いなくカード所有者であると強く確信できるかどうかを判断します。確信できると判断された場合、支払い人が取引の途中で煩わされることなく、スムーズに手続きを進められるため、摩擦と中断の可能性が大幅に減少し、カード所有者のエクスペリエンスも向上します[1]。また、本来のカード所有者ではないという強く確信された場合、取引は完全に拒否されるため、権限認証や決済のリクエストは不要になり、攻撃者に本人認証の情報を入手されても詐欺を防止できます。正規か不正か強く確信できない取引については、カード所有者に対して強力な本人認証を行います。動作ベースの本人認証の重要な目的は、動作のパターンを使用して、本人認証を試行する個人が正規のカード所有者であるかどうかに関する不確実性を低減すると同時に、(a) 二次的な本人認証が正規の取引に影響するのを防ぎ、(b) より多くの詐欺に二次的本人認証を行い、(c) より多くの詐欺を拒否することにあります。

動作ベースの本人認証としてのモデル

CA Risk Analytics Regional Model は、地域の発行者から許可および提供された「真のデータ」[2] を CA eCommerce Consortium で使用して構築されています。これらのデータには、クラジット・カードとデビット・カードの 3D セキュアの取引データが含まれます。

Regional Model には、異なるさまざまな要素が含まれます。まず、このモデルでは、現在の取引の情報が使用されます。これには、取引の本人認証が試行された日付と時間、金額、ユーザの場所（e コマースの場合はカード所有者のコンピュータまたはモバイル・デバイス）、加盟店名、ID および URL、デバイスの IP アドレス、接続特性、サードパーティのデータ・プロバイダからの補助情報などが含まれます。この情報は、モデルが現在の取引を把握するために使用されます。ただし、関係する動作を把握するには十分ではありません。

次に、カード、デバイスまたは加盟店など、現在の本人認証の試行の重要な要素に対する過去の動作に関する情報が使用されます。過去の動作の情報からは、動作パターンを検出するのに重要な要素が抽出されます。この情報には、過去に利用した加盟店、そのときの金額、場所およびデバイス、そのカードを使用したことのあるデバイスなどが含まれます。他の重要な要素についても類似のパターンが確認されます。かつて「重要な抽出物」と呼ばれていたこれらの情報は、取引に対する本人認証の試行が観察されるたびに更新されます。

3 番目に、ミニモデルなどの複雑な可変要素が使用されます。それによって、取引に関係する重要な要素の動作パターンが取り出され、現在の取引がこれらのパターンにどのように一致するか判断されます。これらの可変要素は、カードに対して初めて使用されるデバイスであるかを確認したり、カードやデバイスに対する消費の頻度を特定するような単純なものです。ただし、買い物の反復や同じ加盟店の訪問回数などのカード所有者の傾向を他のユーザの同じパターンと比較するような場合は複雑になります。

4 番目に、履歴データから作成された表が使用されます。これらの表では、トレンドやナイーブ・ベイズ・メトリクスなど、履歴データの正規の取引と詐欺の取引に関する過去の傾向の情報が提供されます。

最後に、これらの異なる要素のすべてが非線形の数値モデルに提供され、異常な動作や不正な試行のリスクに関する異なる予測が評価されます。このようなモデルでは非線形の動作、つまり、単純な線形の関係ではない詐欺の可能性と可変要素との間の重要な関係が取得されます。また、リスクのインジケータと緩和の要素が比較され（加盟店と金額は詐欺の可能性が高いが、ユーザはこのデバイスで以前に同種の取引をしているなど）、多くの異なる関係が確認されます。

これらの異なる要素をどのように評価するかは、学習アルゴリズムを過去の取引の膨大なデータセットと「真のデータ」に適用して判断されるため、このようなタイプのモデルは本質的に「データ主導」です。ルールでは簡単に収集できない重要な関係がモデルによって「検出」されるため、不正な取引の可能性についてより的確な予測が可能になります。

これらのモデルからは、本人認証の試行が**不正**である可能性の予測を示す番号が出力されます。これは、本人認証を行う取引の等級序列を認めるもので、複数のアクションのそれぞれの優先度とそれらのアクションの実行が許可されたことを示します。これによって、不正の可能性が低いことを示すデータの動作パターンに基づいて、カード所有者に影響しない取引の「サイレント認証」が可能になります。

フィードフォワード・ニュートラル・ネットワークを使用した非線形の数値モデル

さまざまな数値モデルのアプローチがありますが、フィードフォワード・ニューラル・ネットワーク（FFNN）ではパフォーマンス、柔軟性、実現可能性の理想的な組み合わせが提供されます。

FFNN は高度な柔軟性を備えているため、入力に対する構造上または分布上の仮定は必要ありません。万能関数アプロキシメータなので、非線形データの大半に対してさえ、最先端のパフォーマンスを示します。さらに、データのサイズや複雑さにかかわらず、線形時間の学習と定数時間のスコアによって、極端に大きなデータセットに対しても実用的です。

ニューラル・ネットワークの構造

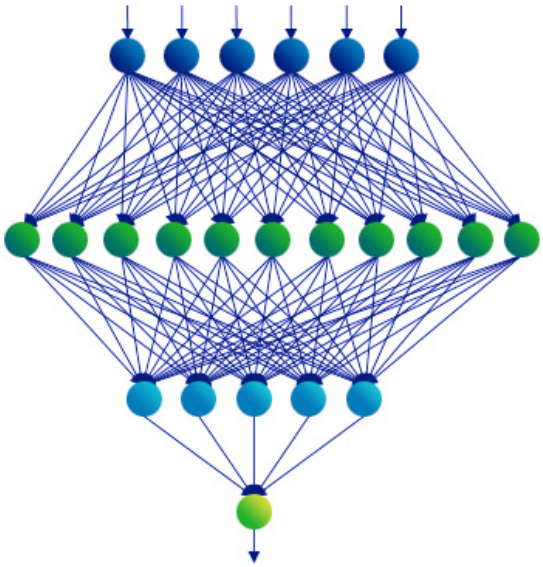
FFNN は必然的に有向非巡回非線形シグナルフロー・グラフになり、その入力は上記で説明した手法で収集した取引の数値表現であり、その出力はここでは、本人認証が詐欺である可能性の序数の評価として解釈されます（スコア）。

さらに説明するなら、FFNN は一連の「層」で構成されていると考えることができ、そのそれぞれは一組の「ニューロン」で構成されます（図 2 参照）。本人認証の入力の試行は最初の（入力）層に提供され、そこからネットワークに伝播されます。この伝播は内部の層（「隠れ層」）を通して続けられ、最終的に出力層に到達します。各層では入力に対して非線形の変形が行われ、その結果が後続の層に渡されます。各層のニューロンの数は任意ですが、ここでは、最終的な（出力）層のニューロンは 1 つになります（それによってスコアを生成）。

FFNN の表現力の高さはこれらの連続した非線形の変形にあります。これらが組み合わさって、FFNN はその入力の関数をモデル化することができます。

図 2:

フィードフォワード・ニューラル・ネットワーク（FFNN）の例



セクション 3

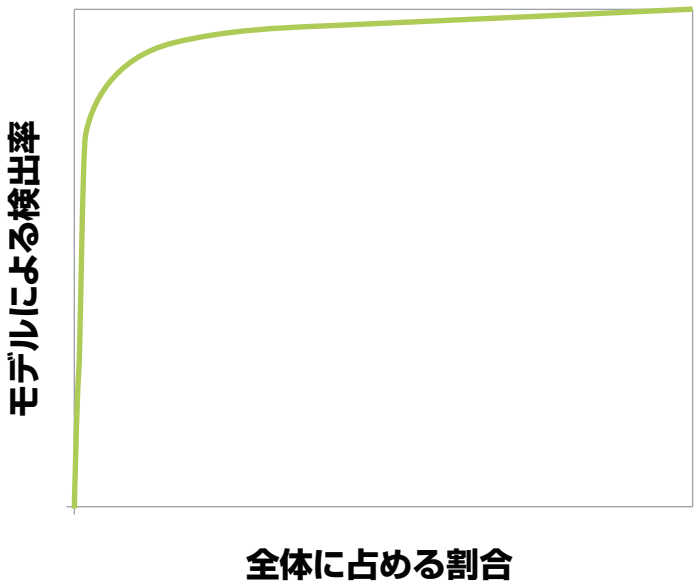
高度なモデルのメリット

モデルのパフォーマンス

CA Regional Model では、取引における詐欺の大半に対して拒否や本人認証の強化が可能になるだけでなく、正規の取引にはわずかな影響しかありません。一般的なパフォーマンスは図 3 に示しています。このモデルでは、詐欺の検出が最大化され、顧客への影響が最小化されます。このグラフではすべての曲線ではなく、曲線が大きく変化した領域を示しています。

図 3:

モデルによる詐欺の検出（すべての取引におけるモデルで検出された詐欺の割合）。このグラフではすべての曲線ではなく、曲線が大きく変化した領域を示しています。



モデルのスコアとルール

ルールは、詐欺のよく知られた正確なインジケータを対象にした場合は優れています。また、実装も理解も簡単です。しかし、データ主導ではないため、詐欺の可能な兆候については、ルール作成者の知識に制限されます。ルールでは複雑な動作を簡単に捉えることはできず、また、複数のリスクに対して 1 つの決定を行うことができません。また、取引に等級序列を付けて、拒否か二次的本人認証を行うことはできず、ケース・ボリュームを調整できません。

モデルでは高度な可変要素を使用して、複雑なパターンを取得できます。可変要素は現在の取引と重要な抽出物（過去の取引から抽出された取引における重要な識別子に関する主な情報）に基づきます。非線形と線形の両方の可変要素、および確立された学習手法を使用すると、モデルのデータ主導のアプローチによって異なる要因を評価して、詐欺の可能性に基づいて取引の等級序列を作成できます。ただし、モデルではアクションは自動で実行されないため、モデルを補完するルールが必要です。

ルールとモデルの組み合わせ

最良のアプローチは、強度の異なるモデルとルールを組み合わせて使用することです。まず、強力なモデルを使用して詐欺と詐欺でない取引を区別して、スコアを使用して取引の等級序列を付けます。次に、そのスコアを活用するためのルールを作成しますが、(i) 高いスコアは詐欺の可能性が高いことを示し、アクションの実行に使用しますが、スコアのしきい値を調整して組織に必要な詐欺の量と多様性に合わせ、(ii) 低いスコアは Flash による詐欺などの他のルールと共に使用し、詐欺でない可能性が高い取引をフィルタリングし、より豊富なデータをルールで操作できるようにします。最後にポリシー・ルールですが、これは、組織が実装した詐欺の可能性から独立しています。詐欺の可能性にかかわらず、新しいデバイスには二次的本人認証が必要になるでしょう。

セクション 4

まとめ

動作ベースの本人認証を使用して本人認証や拒否が影響する取引を判断することは、顧客への影響（摩擦）を低減し、正規の取引をより正確に判断するためには重要です。リスクベースと動作ベースの認証を提供する場合、ルールは重要な構成要素になります。ただし、ルールには多くの制限があります。高度な動作ベースのモデルを追加して、リスクベースのルールを効果的に適用できれば、不正な試行を大幅に抑制できるだけでなく、正規の顧客への影響の低減、カード所有者のエクスペリエンスの向上、発行者の損失減少などの利点があります。

セクション 5

著者について

Paul Dulany は高度な分析とデータ・サイエンスの分野では 14 年の経験があります。2013 年に CA Technologies に入社した後、CA データ・サイエンス・チームを統率して、分析モデル・インフラストラクチャと最初のモデルを開発しました。CA Technologies に入社する前は、SAS Institute に 8 年以上務め、SAS Enterprise Fraud Management ソリューションの最初のモデルを開発したチームに所属し、最初のデビット・カードのモデルをはじめ、数多くの新しい手法の開発を統率しました。SAS の前は、HNC と Fair Isaac に 5 年以上務め、Fraud Predictor のモデル作成チームのマネージャとして、多様な Falcon 決済カード・モデルなどの開発を手がけました。理論物理学の博士であり、HNC と SAS では特許を取得しています。

Hongrui Gong は高度な分析とデータ・サイエンスの分野で豊富な経験があります。2013 年 4 月に CA Technologies に入社し、モデル・インフラストラクチャの構築と 3D セキュア製品のモデル開発で重要な役割を務めました。CA に入社する前は、大手分析会社（SAS、FICO、HNC）に 15 年以上務め、クレジット・カード詐欺検出、保険詐欺検出、連邦政府と州政府のための税過少申告者の特定、マネー・ロンダリング対策、貸付損失の予測、委託証拠金貸付リスク管理、公共機関と民間企業のための信用リスク評価などの製品モデルを開発しました。計算流体力学の博士号を取得し、ロスアラモス国立研究所で乱流体の論理モデルとコンピュータ・シミュレーションの研究に携わっていました。これまでに多数の特許を取得しています。

Kannan Shah は高度な分析とデータ・サイエンスの分野では 6 年の経験があります。2013 年に CA Technologies に入社した当初は、CA データ・サイエンス・チームによる分析モデル・インフラストラクチャと最初のモデルの開発に携わりました。CA Technologies に入社する前は、SAS Institute でシニア・スタッフ・サイエンティストとして、SAS Enterprise Fraud Management ソリューションの統計モデルや手法を開発し、顧客サポートも経験しました。クレジット・カードの詐欺検出モデルのほか、米国、英国、メキシコ、アジア太平洋に向けた ACH/ 電信送金の詐欺検出モデルの開発チームにも参加しています。また、SAS 勤務時代に多数の特許を取得しています。フィラデルフィアのドレクセル大学で電気工学の分野で修士を取得しています。大学では、検出と評価、確率論的信号処理、人工知能、統計パターン認識、ニューラル・ネットワーク、情報理論、高次スペクトル解析、アルゴリズム設計と複雑性を研究していました。

1 カード所有者が 3D セキュアのインジケータについて十分な知識のある地域では、3D セキュアによって取引が保護されていることを示すポップアップ・ウィンドウを表示するとカード所有者は安心するかもしれません。

2 「真のデータ」という用語は、本人認証のプロセスを停止する必要のある取引を特定する取引レベルとカード・レベルの情報を指しています。

CS200_94860_1014