6-4　セキュリティ SLA 構築のための記述手法とネゴシエーション技術

高橋健志

現在のオンラインサービスでは、サービスプロバイダが掲示したセキュリティレベルに対し、ユーザが合意する形になっている。そのため現時点では、そのセキュリティレベルに満足しないユーザはそのサービスを利用しない、もしくは我慢して利用することになるが、簡単なネゴシエーションを実現することにより、彼らの満足度は大幅に改善可能である。そこで本稿では、ユーザとサービスプロバイダの間でネゴシエーションを実施し、セキュリティ SLA を構築する方式を提案する。

1　まえがき

オンラインサービスは近年大幅に増加・発展を続けているが、それと並行してサイバー社会でのセキュリティとプライバシを脅かすインシデントも増加している。そのようなインシデントからユーザを保護する仕組みが求められおり、様々な対策技術が既に存在しているが、それらのすべてを実装することはコスト及びサービスの利便性の観点から望ましくない。そこでセキュリティと利便性のバランスを考慮する必要があるが、ユーザにより環境やセキュリティ要件が異なるため、そのバランスを一様に決定するのは非現実的である。そのバランスはユーザごとに、また、サービス利用の度に決定される必要があるが、それを実現するためには下記に代表される技術的課題が存在する。

a）ユーザのセキュリティ要件は、機械可読な形で記述されなければならず、構造化されたフォーマットが必要不可欠である。

b）技術的知識の少ない普通のユーザが、必要なセキュリティ技術を特定するのは非常に困難であるため、そのようなユーザがセキュリティ要件を特定できる技術が必要である。

c）サービスが満たすべきセキュリティポリシを構築するのに、自動ネゴシエーション手法が必要である。ユーザは現在、サービスプロバイダが掲示するセキュリティポリシに対して、同意するか拒否するかの 2 択しかなく、そのプロバイダと必要なセキュリティレベルや技術について交渉する手段を持たない。そして、もしプロバイダがユーザとネゴシエーションしたいと考えても、人手でのネゴシエーションはコストの観点から非現実的である。

d）ネゴシエーションの結果生成される合意事項は、非否認性を担保していなければならない。ユーザとプロバイダが満たすべきセキュリティポリシに合意しても、セキュリティインシデントが生じないわけではない。そのため、インシデント発生時にその原因が合意事項違反にある場合には、違反をされた側は違反をした側を訴えるべく、その合意事項を証拠として利用できる必要がある。

上記の問題に対応し、セキュリティと利便性のバランスを実現すべく、本稿では非否認性を担保したセキュリティ SLA（SSLA）を構築する手法を提案する。SSLA とは、ユーザとプロバイダ間で合意した、サービスが実現すべきセキュリティレベルである。提案方式は要素技術としてセキュリティ表現手法と ID 変換手法を提供する。

セキュリティ表現手法は、セキュリティ要件と対応能力（capability）を機械可読なフォーマットにて記述可能にする。その記述は複数の視点から行うことができ、その視点のことを次元と呼んでいる。ID 変換手法は異なる次元にて記述されたそれらの情報を任意の次元の情報に変換可能にし、それにより技術的知識の少ないユーザが技術用語を用いずにセキュリティ要件を記述し、自動的に技術用語へと変換することを可能とする。これにより、ユーザとサービスプロバイダは SSLA 構築に向けたネゴシエーションを実施することが可能になる。提案方式は、そのネゴシエーションの結果として、非否認性を担保した SSLA を構築する。その結果、従来プロバイダが掲示するセキュリティポリシに yes もしくは no のどちらかしか回答できなかったユーザが、お互いに合意できるセキュリティポリシを作り上げることができるようになる。

なお、本稿の内容は参考文献 [1] [2] の要約であり、詳細情報についてはこれらの文献を参照いただきたい。

2 アーキテクチャの概要

提案方式は、ユーザ（User）、サービスプロバイダ（SP）、知識ベース（KB）といった3つのロールを定義している。User はオンラインサービスを利用し、SP はユーザにそのサービスを提供する。KB はセキュリティに関する各種情報を保持しており、翻訳を実現するために必須となる辞書を保持している。

図1は、提案方式におけるプロセスの概要である。User は複数のセキュリティ要件を任意の次元で記述し、ID 変換手法を利用してそれらを単一の次元へ変換し集約する。その User のセキュリティ要件と SP の対応能力を突き合わせ、ネゴシエーションすることにより、サービスが満たすべきセキュリティレベル、すなわち SSLA を構築する。

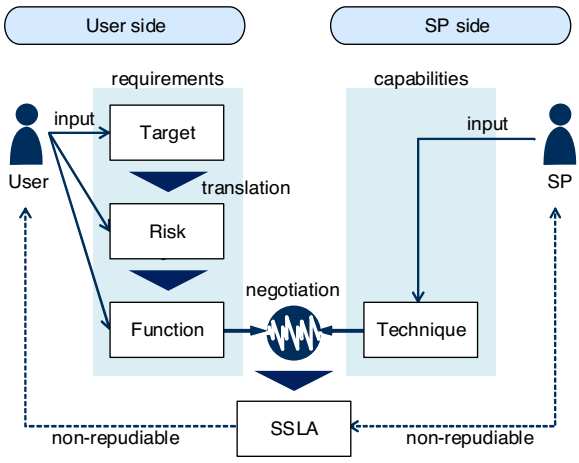

図1　プロセスの概要

3 セキュリティ表現手法

SSLA は User と SP の間で合意されたセキュリティレベルに関する情報である。SSLA の構築には、セキュリティ要件と対応能力が明示される必要がある。セキュリティ要件とは、どのようなセキュリティもしくはセキュリティ技術が必要かを記述した情報であり、対応能力とはどのような技術を持っているか、もしくは何を実現できるかを記述した情報である。これらの情報は KB 内に保存された辞書内の語彙を用いて記述される。提案方式は、機械による処理を実現すべく、自由記述を最小化することを目指しており、そのため、それらの各語彙に一意の識別子を付与している。本識別子は、Object Identifier（OID）[3] の形式で表現される。そして SSLA は、このセキュリティ要件と対応能力を User と SP の間で突き合わせることにより構築される。

様々なユーザが自由自在にセキュリティ要件と対応能力を記述できるようにすべく、提案方式は Target、Risk、Function、Technique の4つの次元を用意している。そしてそのそれぞれの次元ごとに、語彙とそれに対応する識別子を記載した辞書を用意している。Target 次元は守るべき対象を指定する。Target 辞書内に記載されている語彙から選んで記述するが、例えばユーザの「個人情報」などが存在する。Risk 次元は避けるべきリスク種別を指定する。Risk 辞書内に記載されている語彙から選んで記述するが、例えば「通信傍受」のリスクなどが存在する。Function 次元は実装すべき機能を指定する。Function 辞書内に記載されている語彙から選んで記述するが、例えば「ユーザデータの暗号化」や「ユーザの認証」などが存在する。

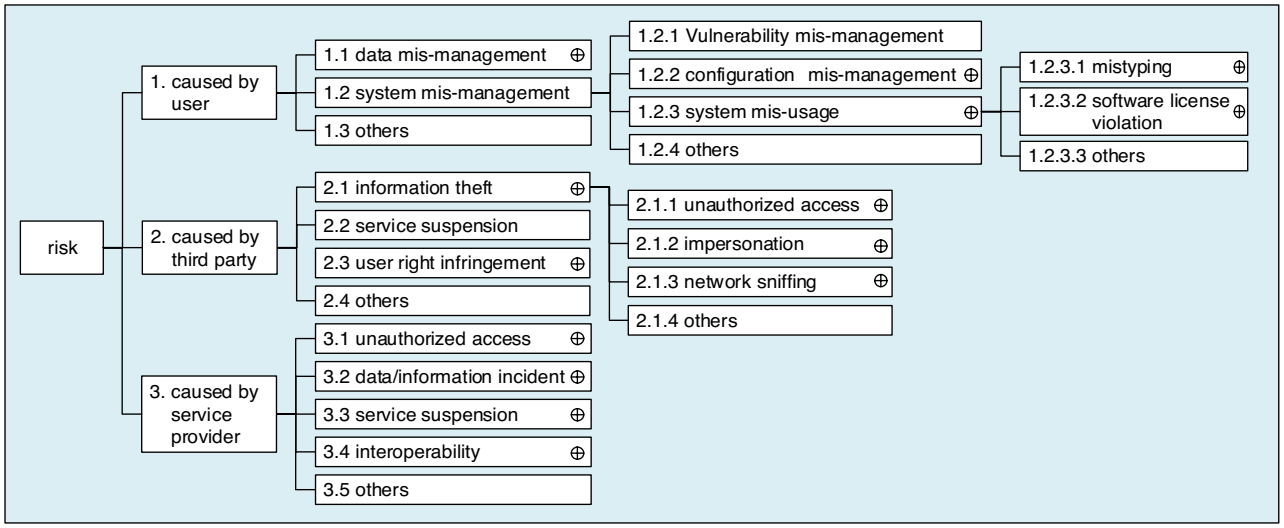

図2　Risk 辞書例（抜粋）

Technique 次元は実装すべきセキュリティ技術・ツールを指定する。Technique 辞書内に記載されている語彙から選んで記述するが、例えば「AES」や「SHA」などが存在する。

これらの語彙の識別子は、それぞれの次元ごとに TARGET、RISK、FUNCTION、TECHNIQUE のいずれかの OID arc から始まる。図 2 に Risk 辞書の一例を抜粋して示す。それぞれの辞書ごとに、TARGET、RISK、FUNCTION、TECHNIQUE の OID arc に続く形で、各項目の識別子が記述される。KB ごとに、独自の辞書を保持してもよい。User も SP も通常は複数のセキュリティ要件と対応能力を保持しているため、セキュリティ要件も対応能力も実際にはこれらの OID のリストとして表現される。

場合によっては、また、User によっては、複数の次元の語彙を使ってセキュリティを表現したいケースも存在する。その際には、コロンを使って複数の次元の語彙を掛け合わせて表記することができる。例えば、特定の Risk に対応する Function を指定した際には、Risk と Function の語彙をコロンを用いて接続することが可能であり、例えば "Risk.1.1.2 :Function.19.12.2." のように記述することができる。

4　ID 変換手法

セキュリティ要件の記述に複数の次元を用意することにより、User はセキュリティ要件を様々な視点から指定可能であり、結果として重要なセキュリティ要件を指定できないリスクを低減することができる。しかしながら次元の異なる情報をコンピュータで自動処理するためには、それらの情報を任意の次元に翻訳する手法が必要となる。

提案方式は、ある次元の OID が別の次元のどの OID に相当するかを紐づけた翻訳対応表を用意し、それを参照することにより翻訳を実現する。この対応表も KB 内に保存されており、[target, risk]、[risk, function]、[function, technique] の 3 種類の対応表に分かれて存在している。それらの対応表は 2 つのコラムで構成されており、一方のコラムの OID がもう一方のコラムの複数の OID に対応する形になっている。例えば、[risk, function] の対応表では、Risk を表す OID と、それに対応するひとつ以上の Function で構成されている。ひとつの Risk に対してひとつ以上の Function が紐づいているのは、実際、あるリスクに対応するために複数の機能を要するケースが存在するためである。

5　ネゴシエーションプロトコル

提案方式では、KB 参照と SSLA ネゴシエーションの 2 種類の通信を実施する。KB 参照は、様々な次元で表現されているセキュリティ要件と対応能力を翻訳する手続きであり、SSLA ネゴシエーションは、2 者間で合意可能な SSLA を構築する手続きである。

KB 参照は、クエリー送信者がセキュリティ要件と対応能力の情報を KB に送信するところから開始される。それを受け取った KB は、セキュリティ要件と対応能力について次元変換を実施し、その結果をクエリー送信者に返信する。

SSLA ネゴシエーションは SSLA-proposal と -confirmation メッセージを用い、SSLA を構築する。SSLA-proposal はセキュリティ要件と対応能力を保持しており、もし、そのメッセージの受信者が提案されたセキュリティ要件に合意した場合、SSLA-confirmation を送信する。内容に合意しない場合は、SSLA-confirmation を送る代わりに別のセキュリティ要件と対応能力情報を入れた新たな SSLA-proposal を返信する。どちらか一方が SSLA-confirmation を送信するか、ネゴシエーションを中止するまで、本手続きは継続される。

SSLA-confirmation メッセージが届くと、本ネゴシエーションは終了し、その際のセキュリティ要件のリストが SSLA となる。

上述のとおり、提案方式は複数回のメッセージ交換を許可しているが、議論を簡略化するため、図 3 に 1 ラウンドで終了するネゴシエーション手続きの例を示す。ここで、KB_U と KB_{SP} は User と SP がそれぞれ信頼している KB である。ネゴシエーション開始に先立ち、User は KB_U にコンタクトをし、様々な次元で記述したセキュリティ要件を Function 次元へと変換する。User は、その変換結果及び KB_U の URI を入れた SSLA-proposal メッセージを SP に送る。それを受領すると、SP は自身が提案されたセキュリティ要件を満たせるかどうかチェックし、また、セキュリティ要件を曖昧度の残る Function 次元ではなく、より具体化された Technique 次元にて合意し、責任範囲を限定したいと考える。そのため、KB_{SP} と通信し、User から受領したセキュリティ要件を満たす Technique 次元のセキュリティ要件のリストを問い合わせる。そして、その結果及び KB_{SP} の URI を入れた新たな SSLA-proposal メッセージを構築し、User へと送る。それを受領した User は、提案された Technique のリストで、自らが元々実現したかった Function 次元でのセキュリティ要件を満たせるかどうかを確認すべく、再度 KB_U に問い合わせる。User

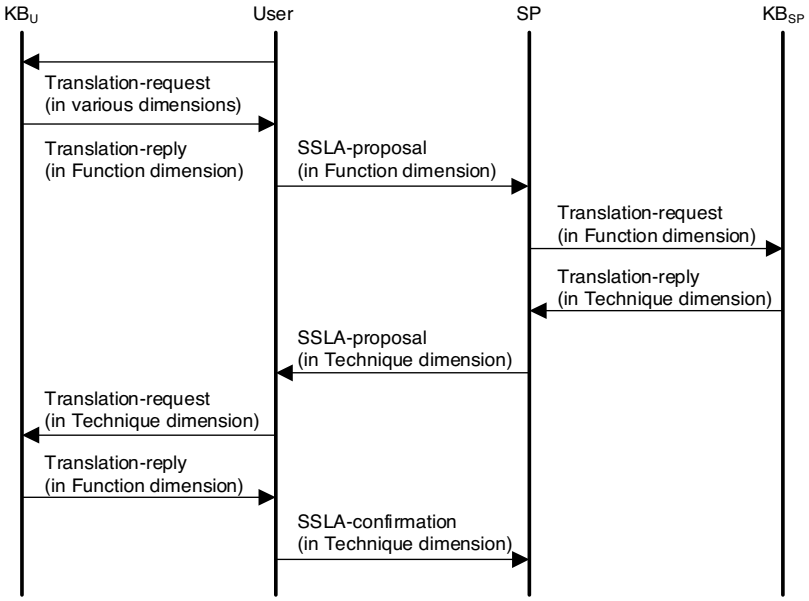

図 3　ネゴシエーション手続き例

は SP から受領した Technique 次元のセキュリティ要件のリストを KB$_U$ に送り、Function 次元へと変換されたセキュリティ要件のリストを受け取るので、それに基づき、元々の自身のセキュリティ要件が満たされるかどうかを確認することができるのである。問題ないことが確認できた後、User は SP に対し SSLA-confirmation メッセージを送り、最終的な SSLA が合意されるに至る。なお、本手続きの冒頭では User は Function 次元のセキュリティ要件を送っているが、最終的に合意されている SSLA は Technique 次元であることに留意されたい。

提案方式では、ネゴシエーション結果として生成される SSLA の非否認性を担保すべく、ネゴシエーションプロトコルのメッセージには暗号識別子とデジタル署名を利用しているが、その詳細については、文献 [2] を参照されたい。

6　結論

提案方式はセキュリティ表現手法、ID 変換手法、ネゴシエーションプロトコル、SSLA 決定アルゴリズムを用い、非否認性を担保した SSLA を構築可能にした。提案方式は実現可能性、非否認性、DoS 耐性の観点からその有効性が示されているものの（文献 [1] [2] 参照）、本稿で示した各種の手法は、今後更なる研究を経て、発展されていく必要がある。例えば、セキュリティ要件や対応能力の記述手法については、ユーザが自分で指定するのは、たとえ多数の次元が用意されていても、また、たとえ知識があっても、時間を要し、面倒になりがちである。そこで状況やユーザにかんがみて、自動的にセキュリティ要件や対応能力を記述してくれる手法が望まれる。特に、モバイル端末など、画面サイズが小さいものや、利便性が限定される場合には、その重要性はより高いものとなる。これらの研究を発展させていくことにより、今後、セキュリティと利便性のバランスをユーザごとに最適化できる世の中が到来することに期待したい。

謝辞

本研究の実施に際し、様々なご支援を頂いた中尾康二主管研究員及び平和昌研究所長に深く感謝する。

【参考文献】

1　T. Takahashi, J. Harju, J. Kannisto, B. Silverajan, J. Harju, S. Matsuo, “Tailored security: building nonrepudiable security service level agreements,” IEEE Vehicular Technology Magazine, 2013.
2　J. Kannisto, T. Takahashi, J. Harju, S. Heikkinen, M. Helenius, S. Matsuo, B. Silverajan, “A Non-repudiable Negotiation Protocol for Security Service Level Agreements,” International Journal of Communication Systems, 2015.
3　International Telecommunications Union, “ Information technology - Open Systems Interconnection - Procedures for the operation of Object Identifier Registration Authorities: General procedures and top arcs of the International Object Identifier tree,” ITU-T Recommendation X.660, 2011.

高橋健志　（たかはし　たけし）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究員
博士（国際情報通信学）
サイバーセキュリティ、通信プロトコル