新たなプライバシ脅威「Silhouette」の発見と対策への取り組み

ユーザおよび事業者にとって，全く未知の脅威による被害を未然に防ぐためには，システムに潜在するセキュリティ上の問題を攻撃者より先に解明し，あらかじめ防御策を講じておくことが重要です．本稿では，こうした脅威実証研究の一環で発見した新たなプライバシ脅威「Silhouette」の仕組みと対策手法，および世界的なサービスやブラウザのセキュリティ機能を強化させるに至った取り組みについて紹介します．

わたなべ　たくや
渡邉　卓弥
NTTセキュアプラットフォーム研究所

Silhouetteがもたらすプライバシ脅威

SNSや動画共有サービスといった，人と人との相互コミュニケーションによってコンテンツが形成されるソーシャルウェブサービス（SWS）は，登場以来めざましい発展を続け，今日では私たちの生活に不可欠な存在となりました．インターネットユーザに対する調査[(1)]によれば，１人当り平均５種類以上のSWSのアカウントを保有していると報告されています．SWS上では，これらのアカウント名を基にユーザのプロフィールや投稿を参照できるため，氏名や顔写真，その人のアクティビティといった個人情報が各アカウントに紐付いているといえます．

NTTセキュアプラットフォーム研究所（SC研）が発見したプライバシ脅威「Silhouette（シルエット）」では，あるユーザが第三者のWebサイトにアクセスした際に，自身の所有するSWSアカウントを第三者から特定されてしまいます．例えば，検索エンジン経由や，一般的なWebサイトに含まれる広告，メールに含まれるリンクによって，本来SWSと全く関係のない悪意のあるWebサイトへアクセスしてしまうと，その悪意あるWebサイトはユーザが利用しているであろうSWSへの通信をユーザには分からないように裏で行い，収集した情報からアカウント名を特定します．

特定が成立してしまう条件は，PCやモバイル端末のWebブラウザにおいて，本脅威に対して脆弱なSWSへのログイン状態を保持しているユーザが，悪意ある第三者の設置したWebサイトを訪問するというものです．一般的なSWSでは，ログアウトを明示的に実施する等の操作によってブラウザのCookie*が削除されるまで，自動的にログイン状態を保持する仕組みになっています．したがって，過去に一度でも脅威の対象となるSWSを利用した経験のあるユーザは，特定の対象となってしまうおそれがあります．

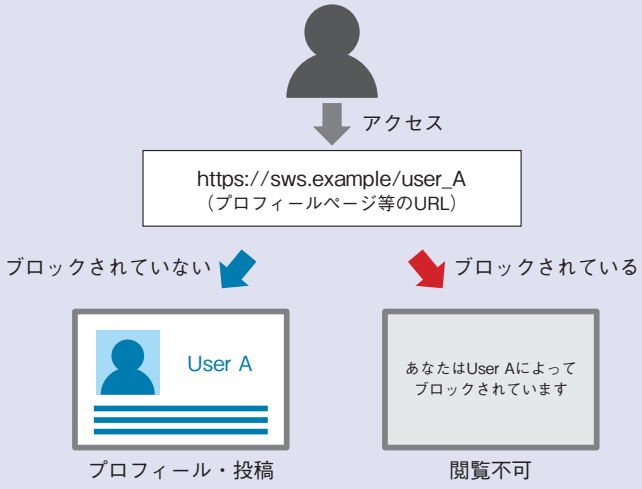


図１　ユーザブロック機能

脅威が成立する仕組み

本脅威を成立させるために，SWSに広く採用されている「ユーザブロック」という機能（**図１**）が悪用されま

＊ Cookie：ユーザ設定，ログイン状態，セッション等を管理するために，Webサービスが訪問ユーザのWebブラウザに情報を保存できる機能です．

す. ユーザブロックは本来, 正当なユーザが悪質なユーザに対して自身のページ閲覧可否をコントロールし，ハラスメントやスパム行為から身を守るための機能です．SC研は，悪質なユーザもまた正当なユーザに対してページの閲覧可否をコントロールできてしまうというユーザブロックの特性に，セキュリティ上の問題が潜在していることを突き止めました．

事前準備として，悪意ある第三者はSWS内に自らアカウント（特定補助アカウント）を作成します．特定補助アカウントを複数用意し，同一サービス上のユーザらを計画的にブロックすることで，さまざまな閲覧可・閲覧不可の組合せパターンを構築することができます．このパターンは，ユーザアカウントを一意に識別するための情報として利用されます（**図2**）．

特定実行時，すなわちアカウント名を特定するためのスクリプトが設置されたWebサイトに訪問したユーザに対しては，それぞれの特定補助アカウントのページへの通信を強制的に送信させます．このときの通信は，異なるサイト間のデータ漏洩を防ぐためにWebブラウザが採用しているSame-Origin Policyによって保護されているため，第三者は応答内容を直接的に取得することはできません（**図3**）．しかしながら，閲覧可能時と閲覧不可能時では通信の応答時間には統計的な差異が発生します．悪意ある第三者はこの差異を用いて，訪問ユーザがそれぞれの特定補助アカウントからブロックされているかどうかを推定することができます．推定結果を，あらかじめ構築したパターンと照合することで，当該ユーザのSWSにおけるアカウント名を特定します．

既存のサイバー攻撃のカテゴリに当てはめると，Silhouetteはクロスサイトリクエストフォージェリ（CSRF）およびサイドチャネル攻撃に分類され

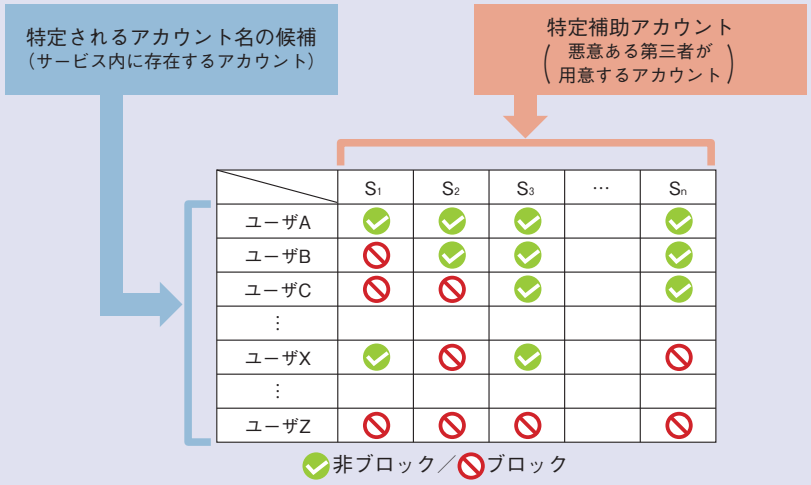


図2　閲覧可・閲覧不可のパターン例

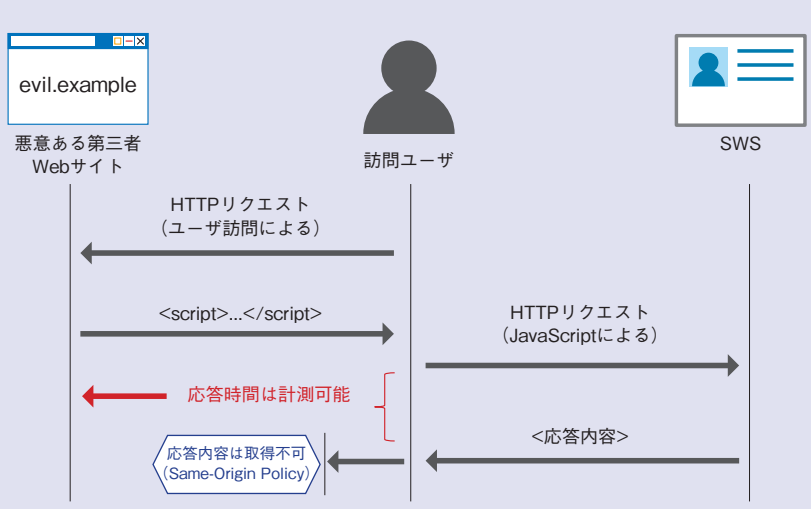


図3　Same-Origin Policyによる応答内容の保護

ます．CSRFとは，ユーザが意図しない異なるサイトへのリクエストを強制的に送信させることで，データの奪取や悪性コードの実行などを行うWeb系の攻撃です．また，サイドチャネル攻撃とは，応答時間や電力消費量といった物理空間の情報を活用し，センシティブな情報の推測を行う攻撃の総称です．本研究は，CSRFとサイドチャネル攻撃を組み合わせることで，SWSに広く採用されているユーザブロック機能を悪用し，正当なユーザのプライバシを脅かすことができてしまうという，サービス設計に潜在していたセキュリティ上の問題を明らかにしました．

対策手法

本脅威に対して，SWS事業者およびユーザが実施可能な対策手法をそれぞれ紹介します．前述したとおり，本脅威はCSRFとサイドチャネル攻撃を組み合わせた攻撃であるため，これらのいずれかを防御することで対策が実現します．サイドチャネル攻撃の対策[(2)]には，タイミング情報の特性を考慮した専門的な見地が必要とされますが，CSRFは，Webサービスのプログラム変更を伴う汎用的な対策が知られています．以下では，CSRFの対策に主眼を置いた対策手法を紹介します．

■前提条件

本脅威の対象となり得るSWSは，アカウント登録機能があり，なおかつユーザブロック機能などによって，あるユーザが他のユーザに対して，ユーザのコンテンツページ（プロフィールなど）の閲覧権限を強制的に変更できる機能を持っているサービスとなります．これらに該当しないサービスは本脅威の対象とはなりません．

■SWSによる対策

SWSが実施できる1番目の対策は，SameSite属性と呼ばれるCookieのオプションを用いたものです．SameSiteが付与されたCookieは，JavaScript等による異なるサイトへのリクエスト時に送信されなくなります．したがって，ログイン状態を管理するCookieにこの属性を指定することで，本脅威を含むCSRFを広く対策することが可能となります．ただし，本機能を利用するためには，ユーザの用いるWebブラウザがSameSiteに対応しているうえで，SWSがHTTPヘッダでSameSiteの利用を宣言する必要があります．後述するとおり，Silhouetteを対策するためのSC研の取り組みによって，世界中の主要なブラウザがSameSiteに対応するようになりました．

2番目の対策は，リクエスト検証と呼ばれるものです．CSRFでは，JavaScriptによってユーザおよびサービスが意図しないHTTPリクエストが発生します．このとき，SWSなどのサービス側で，リクエストの送信元となったWebサイトのURLを示すリファラや，CSRF対策のための特殊な文字列を含んだリクエストパラメータを検証することで，正当なリクエストであるかどうかを判別するという対策手法[(3)]が知られています．リクエスト検証は，Webサービスへの投稿等を行うPOSTメソッドを受け付けるページで採用されることが多いですが，ユーザプロフィールのようなGETメソッドを受け付けるページにおいても採用することができます．ただしこの場合，検索エンジンやブログ記事から直接リンクされた際に検証に失敗し，不正なリクエストとして棄却してしまう可能性があります．そこで，検証に失敗した際には，サービス側が実際のコンテンツを含まない中間ページを返した後，その中間ページのJavaScriptによって実際のコンテンツを取得するという手順を加えることで，ページを表示するまでのリクエスト数は増加するものの，直接リンクからのアクセスを阻害することなく対策できます．

■ユーザによる対策

ユーザが実施できる対策の1つに，ブラウザに搭載されているプライベートブラウジングモードが挙げられます．これはシークレットモード，プライベートウィンドウ，InPrivateなどとも呼ばれており，この機能を有効にしている間は，今までのCookie情報を引き継ぐことなく，また終了時には新たに保持したCookieを削除するようになります．プライベートブラウジングを有効にしてから第三者のWebサイトに訪問することで，本脅威によるアカウント名の特定を防ぐことがで

きます．

ユーザが実施できる2番目の対策は，SWSからログアウトすることです．本脅威では，ユーザがSWSにログインしているという状態に基づいて，アカウント名の特定が実現します．SWSにログインしてサービスを利用した際は，終了時に毎回ログアウト処理を行うなどの手段によって，本脅威によるアカウント名の特定を防ぐことができます．

脅威の成立を未然に防ぐための取り組み

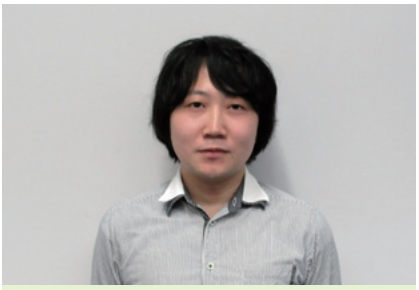
SC研では，Silhouetteに対してSWSが脆弱であるか評価する手法を確立し，NTTグループおよび世界的に著名な外部のSWSの調査を実施しました．その結果，影響力の大きな海外の著名サービスの一部において，実際にアカウント名が特定され得る状態にあることを解明し，事業者に対して脅威の詳細や対策方法の共有と，対策の有効性を検証する実験協力を行いました．この取り組みを受けて，TwitterなどのSWSが仕様変更によってセキュリティ機構を向上させ，アカウント名特定の脅威を未然に防ぐことができました．さらに，Microsoft Edge，Internet Explorer，Mozilla Firefoxといった主要ブラウザにおいて，本研究や類似手法によって発生し得る脅威を回避するため，CookieのSameSite属性が利用できるようになりました．この貢献による影響ユーザは現時点で6億人以上にのぼり，世界中で利用されている多くのSWSの安全性を大きく向上させただけでなく，今後NTTを含むあらゆる事業者がセキュアなWebサービスを設計するための高度な機能を活用できるようになったことを意味します．本研究の成果は，短期的・中長期的いずれの視点においても，世界中のユーザがより安全にインターネットを利用できる環境を実現したといえます．また，脅威の発見および実証と対策手法をまとめた論文[2]は，世界トップレベルの学術会議「IEEE European Symposium on Security and Privacy」に日本から初めて採択されるとともに，サイバーセキュリティ業界に大きな影響力を持つ国際会議「Black Hat Europe」に採択[4]されるなど，世界のWebセキュリティ向上のために極めて大きなインパクトを与えました．

今後の展開

SC研はサイバーセキュリティに関する研究開発の一環として，このたび発見した脅威「Silhouette」を含む新たな脅威を評価する手法の開発を実施するとともに，問題を発見した際には関係機関と協力して対策の実現に向けて取り組んできました．今後も潜在的な脅威の発見と対策の展開を継続することで，NTTが堅牢なサービスを提供できるよう努め，Webサービスや Webブラウザのセキュア化を推進し，インターネットの安心・安全な利用を促進します．

■参考文献

(1) https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/
(2) T. Watanabe, E. Shioji, M. Akiyama, K. Sasaoka, T. Yagi, and T. Mori：“User Blocking Considered Harmful? An Attacker-Controllable Side Channel to Identify Social Accounts,” Proc. of EuroS&P 2018, London, U.K., April 2018.
(3) https://www.ipa.go.jp/security/vuln/websecurity.html
(4) https://www.blackhat.com/eu-18/briefings/schedule/index.html#i-block-you-because-i-love-you-social-account-identification-attack-against-a-website-visitor-12912



渡邉　卓弥

どんなに堅牢なシステムを構築しても，攻撃者はときに物理空間の情報まで駆使し，迂回する方法を探します．本当の意味で脅威を未然に防ぐため，攻撃側の視点から彼らより先に脅威を発見し，対策を講じることをめざしています．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
サイバーセキュリティプロジェクト
TEL　0422-59-7466
FAX　0422-59-3844
E-mail　takuya.watanabe.yf@hco.ntt.co.jp