IPA Technical Watch

知らぬ間にプライバシー情報の非公開設定を公開設定に変更されてしまうなどの「クリックジャッキング」に関するレポート

～クリックジャッキング攻撃の対策が行われていたのは、56 サイトの内 3 サイト～

独立行政法人情報処理推進機構
技術本部 セキュリティセンター

目次

はじめに

SNS サイトは趣味や近況等を公開し、新たな人間関係を築く場所として多くの人が利用している。しかし、SNS 等のサービスでは、ユーザ情報の一部の情報のみを公開したり、信頼している人以外へは全体を非公開に設定したりする機能があるが、無関係なウェブサイトを閲覧している最中に、この設定が知らぬ間に変更されてしまい、全ての人へ公開する状態にさせられてしまうというような事故が発生することがある。このようなことになってしまう原因は複数考えられるが、その一つにクリックジャッキングという攻撃が挙げられる。

クリックジャッキング攻撃への対策は公開されてから時間が経過しているにも関わらず、この攻撃によると思われる事件が複数発生している。そこで、IPA では 2013 年 2 月から 3 月にかけて、クリックジャッキング攻撃への対策がどの程度普及しているか、ウェブサイトを 56 サイト抽出し、X-FRAME-OPTIONS と呼ばれる仕組みによるクリックジャッキング攻撃への対策が実際にどれだけのウェブサイトで行われているかで調査を行った。その結果、X-FRAME-OPTIONS による対策が行われているウェブサイトは 3 サイトのみで、残りの 53 サイトは未対策[1]であった。このことを受け、クリックジャッキング攻撃への対策を行っていないサイトが多数存在する可能性があると推測した。このため、クリックジャッキング攻撃の認識およびその対策の普及が必要であると考えて本レポートを作成、公表した。

本レポートでは、クリックジャッキングの仕組みを説明した上で、ウェブサイト運営者の対策方法について紹介する。本書が、クリックジャッキングの仕組みとその対策を必要とするウェブサイトの把握・対策方針の参考となれば幸いである。

本書の対象読者

本書の対象読者は、ウェブサイトの構築や運営に携わる技術者の方を想定している。

[1] IPA では未対策のウェブサイト運営者に連絡を行っている。

1. クリックジャッキング攻撃とは

クリックジャッキング攻撃とは、ユーザを視覚的にだまして正常に見えるウェブページ上のコンテンツをクリックさせ、別のウェブページのコンテンツをクリックさせる攻撃のことである。その結果、ユーザが公開するつもりのないプライバシー情報を公開させられたり、意図しない情報を登録させられたりするなどの被害を受ける可能性がある。

本章では、クリックジャッキングの攻撃の流れを確認した後、具体的な仕組みと脅威について解説する。

1.1. クリックジャッキング攻撃の例

クリックジャッキング攻撃では、例えば次のような流れで攻撃が行われる(図 1)。サイト A はクリックジャッキング攻撃への対策をしていないサイト、悪意あるウェブサーバはユーザに細工したウェブページを送信するサーバとする。

① ユーザがサイト A にログインする
② ユーザがサイト A にログインした状態で、悪意あるウェブページを閲覧する
　ユーザのブラウザ上には、ページ上の特定箇所のクリックを促す内容が表示される
③ ユーザが悪意あるウェブページのコンテンツをクリックする（実際には、サイト A のコンテンツをクリックしている）
④ その結果、意図せずサイト A の設定を変更してしまう。

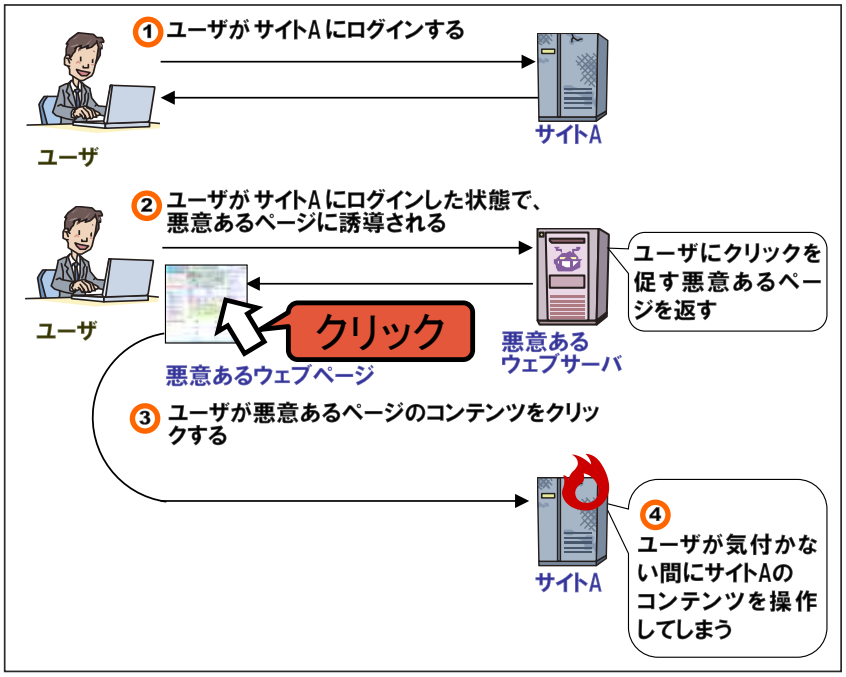

図 1　クリックジャッキング攻撃の流れの例

では、何故このような攻撃が成立してしまうのか、その仕組みについて説明する。

1.2. クリックジャッキング攻撃が成立する仕組み

クリックジャッキング攻撃を成立させるために、攻撃者はユーザを視覚的にだまし、意図した箇所をクリックさせる必要がある。例えば、攻撃者は図 1 の「悪意あるウェブページ」のような細工したページをユーザに閲覧させる。この悪意あるページは、2 つの”部品”により構成されている。

- ユーザのウェブブラウザ上で表示される悪意あるページ
- 表示形式が透明になるように細工されたサイト A のページ

■ 部品 1:ユーザのウェブブラウザ上で表示される悪意あるページ

一つは、ユーザがクリックしたいと思わせるためのページである。

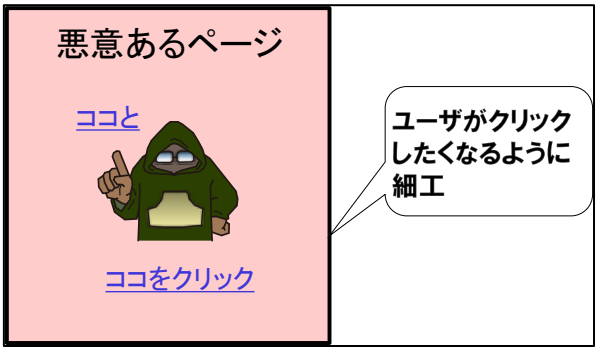

図 2　ユーザのウェブブラウザ上で表示される悪意あるページ

■ 部品 2:表示形式が透明になるように細工されたサイト A のページ

もう一つは、サイト A のウェブページを透明になるように細工したものである。この細工は、悪意あるウェブページ上で行われる。

具体的には、悪意あるページが、iframe 要素等によってサイト A のページを読み込み、そのページを CSS (Cascading Style Sheets)の opacity プロパティ[2]を使用するといった方法で透明にする。

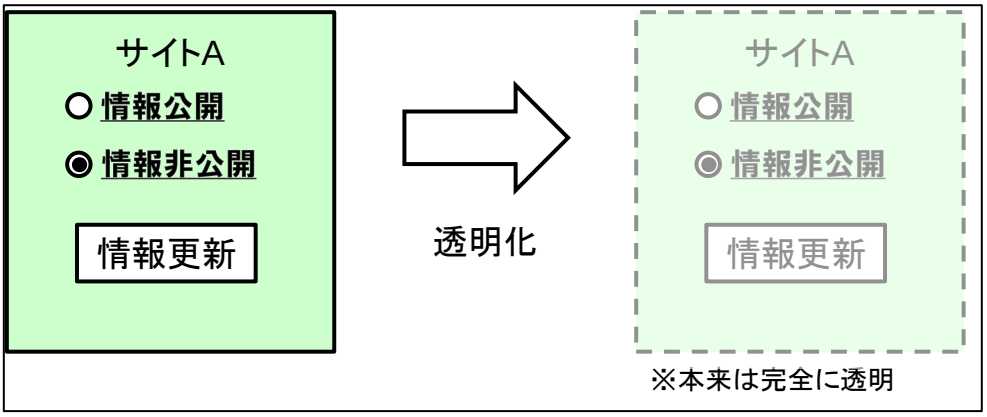

図 3　表示形式が透明になるように細工されたサイト A のページ

[2] CSS/Properties/opacity
http://www.w3.org/wiki/CSS/Properties/opacity

■　2 つの部品を組み合わせる

これらの 2 つの部品を以下のように配置させることで細工した「悪意あるウェブページ」ができる。

- 透明化したサイト A のページを前面に、悪意あるページを後面に配置
- 悪意あるページでサイト A のクリックさせたい位置を合わせる

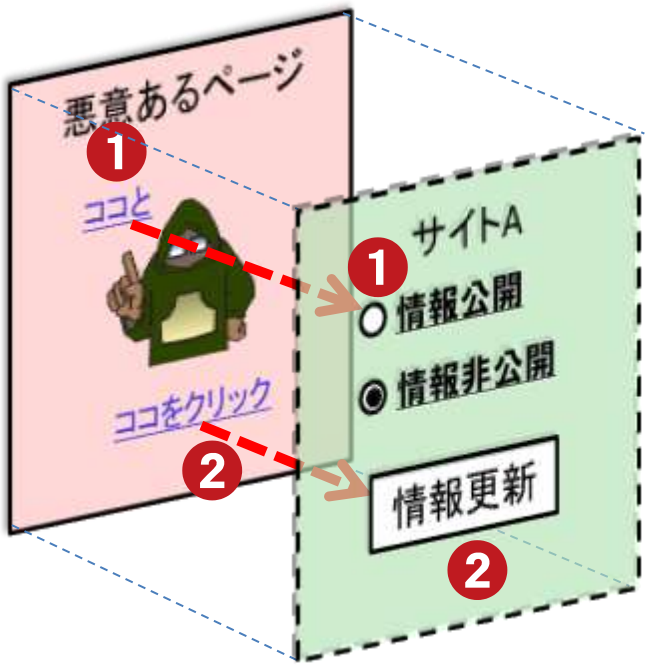

図 4　2 つの部品を重ねるイメージ

サイト A にログインしている状態のユーザは、悪意あるページの指示に従い①と②を順にクリックすると、結果的に自分自身でサイト A の設定を変更してしまうことになる。

1.3. クリックジャッキング攻撃によって想定される脅威

クリックジャッキング攻撃が成立することにより想定される脅威は以下が挙げられる。

- ログインしたユーザのみが利用可能なサービスの悪用
  - 意図しないコンテンツ等を自分が共有したものとしてウェブサイト上で共有させられてしまう。
  - 非公開にしていたはずのプライバシーの情報を公開に変更されてしまう。
  - 退会した覚えのないにも関わらず退会してしまう。
  - サイトの日記等のコンテンツにおいて、覚えのない投稿をしてしまう。

2. クリックジャッキング攻撃に関する対策状況の調査

本章では、クリックジャッキング攻撃の対策状況を調査するに至った背景とその調査結果を説明する。クリックジャッキング攻撃の対策が実際にどの程度行われているか見てみよう。

2.1. クリックジャッキング攻撃への対策状況の調査背景

クリックジャッキングは 2008 年に OWASP[3]で[4]Robert Hansen 氏と Jeremiah Grossman 氏により公表された[5]。この公表を受け、JavaScript による対策と、X-FRAME-OPTINS という仕組みによる対策が提案された。

X-FRAME-OPTIONS による対策は、Microsoft によって提唱[6]されたもので、ウェブブラウザとウェブサイトの双方で対策を実施することで有効になるものであった。その後、主要なウェブブラウザにおいては、X-FRAME-OPTIONS の対応が進み(2.3 章参照)、一般的な対策として認知されるようになってきた。

しかし、一方でクリックジャッキングの攻撃によると思われる事件が複数発生していたり、IPA へのウェブサイトの脆弱性としても少数ながら届出られたり、ウェブサイトでの対策が進んでいないのではないか、と思われる事象が散見された。

そのため、IPA では 2013 年 2 月にウェブサイトで X-FRAME-OPTIONS による対策が進んでいるかの調査を行った。

2.2. ウェブサイトにおける X-FRAME-OPTIONS への対策状況の調査

■ 調査方法

調査内容は、「クリックジャッキング攻撃への対策をしたほうがよいと思われるウェブページ」を表示した際に、サーバからのレスポンスにあるサーバヘッダに X-FRAME-OPTIONS ヘッダが出力されているか否かで判定した。

「X-FRAME-OPTIONS ヘッダを出力したほうがよいと思われるページ」は、次のような特徴を持つウェブサービスの該当設定変更ページである。

- ユーザの情報を登録し、その情報を公開するか非公開にするかを選択することができる
- インターネット上の情報を自分から共有することができる
- 日記やつぶやき等で自身の情報として投稿ができる。
- ユーザがクリックのみで登録しているサイトを退会できる

IPA の調査ではこれらのいずれかの特徴を持つ、日本人向けにサービスを展開していると思われるウェブサイトを抽出して調査を行った。

[3] Open Web Application Security Project
[4] https://www.owasp.org/index.php/OWASP_NYC_AppSec_2008_Conference
[5] http://www.sectheory.com/clickjacking.htm
[6] http://blogs.msdn.com/b/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx

■　**調査結果**

X-FRAME-OPTIONS によるクリックジャッキング攻撃への対策が実施されているかどうかのウェブサイトの調査は、2013 年 2 月から 3 月の期間で実施した(図 5)。その結果、クリックジャッキング攻撃への対策として X-FRAME-OPTIONS ヘッダが付与されていたウェブサイトは 56 サイトの内 3 サイトのみであった。

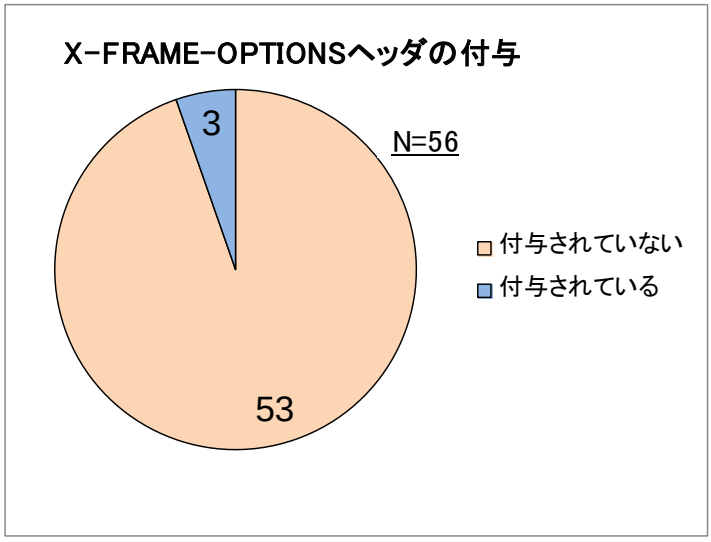

図 5　X-FRAME-OPTIONS によるクリックジャッキング攻撃の対策状況

この結果から、対策が必要と考えられる多くのウェブサイトで X-FRAME-OPTIONS ヘッダを付与していないことから、クリックジャッキング攻撃への対策が普及していない可能性が高いと推察する。

ただし、X-FRAME-OPTIONS ヘッダがサーバヘッダに含まれていないことだけでは、クリックジャッキング攻撃に対して無防備であるとは言えない。例えば、外部のウェブサイトへウェブページの素材（「ブログパーツ」や「いいね！ボタン」等）を埋め込むものを提供する場合等は、X-FRAME-OPTIONS を使用することができず、その他の対策で代替している可能性がある。

なお、X-FRAME-OPTIONS ヘッダが付与されていなかったウェブサイトに対してはクリックジャッキング攻撃への対策が行われていない可能性があったため、脆弱性関連情報の届出制度に則り、ウェブサイト運営者に連絡を行っている。

2.3. 主要ブラウザの X-FRAME-OPTIONS の対策状況について

X-FRAME-OPTIONS の対応は、下記の表 1 に示すように Internet Explorer、Safari、Firefox、Google Chrome、Opera といった主要ブラウザで採用され、既に時間が経過している。それにも関わらず、実際に対策が行われていたウェブサイトは図 5 の通りほとんどなかった。

表 1 ブラウザの X-FRAME-OPTIONS 対策状況

ブラウザ	対応バージョン
Internet Explorer	8.0 以上
Safari	4.0 以上
Firefox	3.6.9 以上
Google Chrome	4.1.249.1042 以上
Opera	10.5 以上

3. クリックジャッキング攻撃への対策

本章では、クリックジャッキング攻撃への対策方法と、対策を検討すべきウェブサイトについて述べる。

3.1. 対策を検討すべきウェブサイト

クリックジャッキング攻撃への対策の実施を検討すべきウェブサイトは、以下の 2 つの項目が該当するようなウェブサイトである。

1. 登録制のウェブサイト(ログイン機能のあるウェブサイト)であること
2. ウェブサイト上でユーザの情報を追加・編集・投稿・削除できること

該当するウェブサイトの中でも X-FRAME-OPTIONS ヘッダを出力すべきページの具体的な例として次のようなページが挙げられる。

- ユーザの情報（特に公開・非公開）の設定を行うページ
- ユーザが投稿を行うページ
- ユーザが退会等を行うページ

3.2. X-FRAME-OPTIONS による対策

（1） X-FRAME-OPTIONS とは

X-FRAME-OPTIONS は frame 要素または iframe 要素でウェブページを表示させることを許可するか否かを指定することができる仕組みである。X-FRAME-OPTIONS を使用することで、他のサイトで frame 要素や iframe 要素上で読み込ませたいページを除外することができる。

X-FRAME-OPTIONS は、HTTP レスポンスヘッダに出力し、DENY、SAMEORIGIN の設定値をとる。それぞれの設定値の違いは表 2 の通りである。

表 2 X-FRAME-OPTIONS の設定値

設定値	frame 要素および iframe 要素により表示できる範囲
DENY	すべてのウェブページにおいて表示を禁止
SAMEORIGIN	アドレスバーに表示されたドメインと同じウェブページのみ表示を許可

DENY を選択する場合は、自身のサイトを含めたすべてのサイトにおいて表示を禁止するため、自身のサイトでは全く frame 要素や iframe 要素を使用しない場合に選択する(図 6)。
SAMEORIGIN を選択する場合は、自身のサイトのみで frame 要素や iframe 要素で表示を許可する場合に選択する(図 7)。SAMEORIGIN を選択する場合で注意しなければならないのは、同一ドメインのみである点だ。

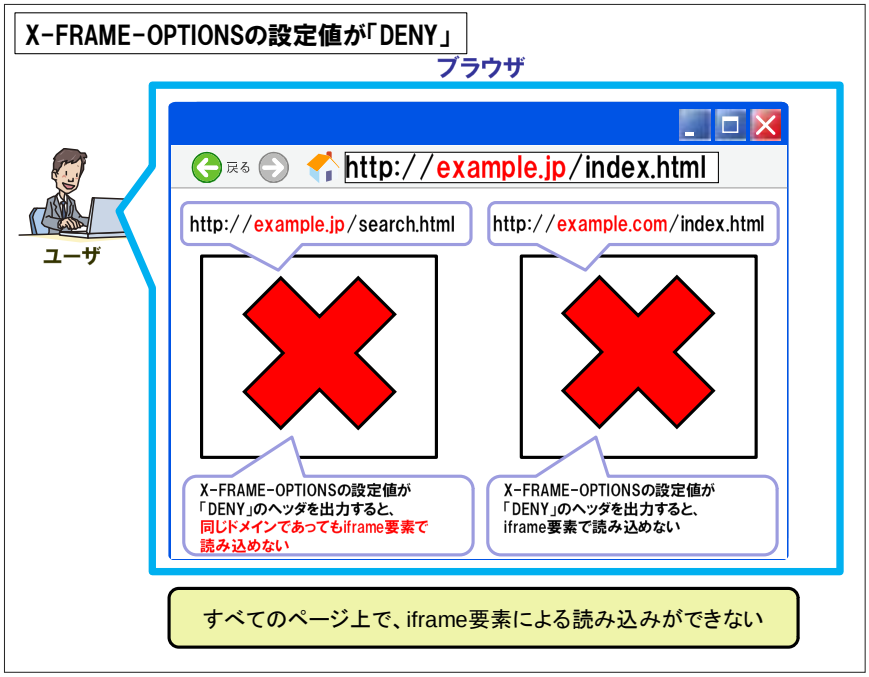

図 6　X-FRAME-OPTIONS の設定値が「DENY」の場合の iframe 要素の読み込み

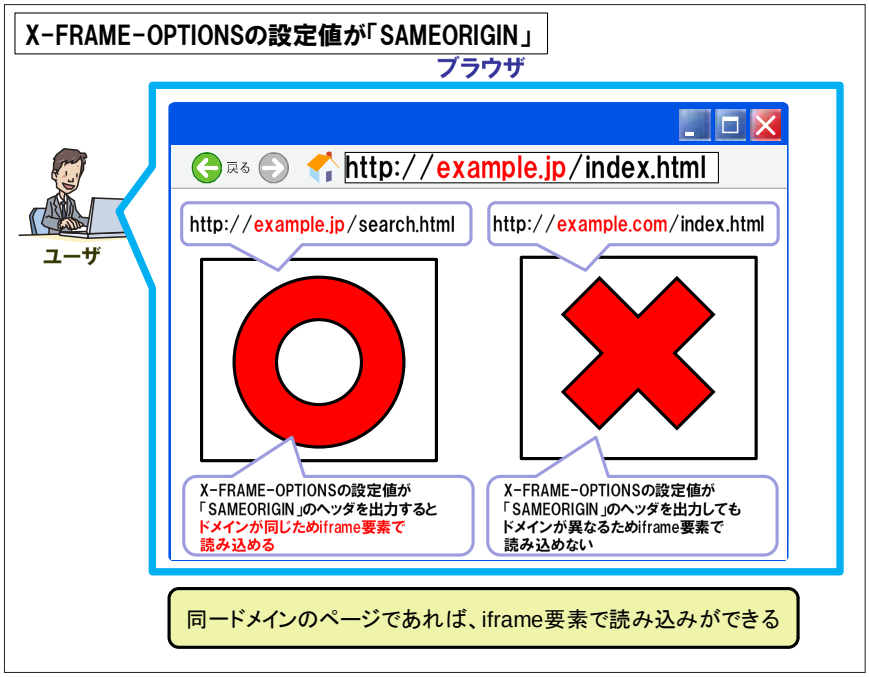

図 7　X-FRAME-OPTIONS の設定値が「SAMEORIGIN」の場合の iframe 要素の読み込み

なお、X-FRAME-OPTIONS には、上記 2 つの設定以外に、「ALLOW-FROM *origin*」を指定することができる。*origin* に指定したドメインのウェブページのみ frame 要素および iframe 要素による表示を許可することができる設定項目である。[7]

ただし、ALLOW-FROM については、2013 年 2 月現在対応していないブラウザもあり、この設定項目を選択しても、意図通りに動作しない可能性がある。なお、ALLOW-FROM の設定項目については、IPA が 2013 年 2 月に確認した対応状況を記載する(表 3)。

[7] Combating ClickJacking With X-Frame-Options
http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

表 3 ブラウザの X-FRAME-OPTIONS の ALLOW-FROM の対応状況

ブラウザ	ALLOW-FROM 対応	IPA が確認したバージョン
Internet Explorer	対応済	8, 9
Safari	未対応	5.1.7
Firefox	対応済	19.0
Google Chrome	未対応	25.0.1364.172 m
Opera	未対応	12.12

（2） X-FRAME-OPTIONS の設定例

■ウェブサーバ全体に対策を設定する場合：

ウェブサイト全体で X-FRAME-OPTIONS ヘッダを出力させたい場合、ウェブサーバの設定で実施する方法がある。そのウェブサーバの設定ファイルの記述例として、CentOS 上の Apache2 における設定ファイル httpd.conf の記述例を以下に記す。[8]

●httpd.conf の記述例

```
Header always append X-FRAME-OPTIONS "DENY"
```

上記の記述例では、X-FRAME-OPTIONS の設定値として DENY を指定し、ウェブサーバが管理しているすべてのウェブページにおいて frame 要素および iframe 要素による表示を禁止している。

■ウェブページ毎に対策を設定する場合：

本来はウェブサイト全体ではなく、対策を必要とするページのみで X-FRAME-OPTIONS ヘッダを出力したい場合が多いと考えられる。対策を必要とするページのみで出力する方法はいくつか考えられるが、ここではその方法を一つ紹介する。

- ページを作成するプログラムで、X-FRAME-OPTIONS ヘッダを出力する様な処理を加える。

  例えば、ウェブページの構成上、iframe 要素内でユーザの情報の設定を行うことがないのであれば、このページのみで X-FRAME-OPTIONS ヘッダの DENY を出力させれば対策ができる。frame 要素や iframe 要素を指定するページと同じドメインのユーザの情報の設定を行うページであれば、このページのみで X-FRAME-OPTIONS ヘッダの SAMEORIGIN を出力させれば対策ができる。

（3） X-FRAME-OPTIONS の注意点

X-FRAME-OPTIONS には次の注意点がある。

① 複数ドメインに対して X-FRAME-OPTIONS の設定が複雑

② HTML ファイル内に meta 要素で X-FRAME-OPTIONS を設定することができない

[8] mod_headers モジュールが有効になっている必要がある。

◆ （3）-① 複数ドメインに対して X-FRAME-OPTIONS の設定が複雑

特に複数のドメインを使い分けているウェブサイトの場合、X-FRAME-OPTIONS をどのように設定するかが複雑になる。該当のページのみでX-FRAME-OPTIONSヘッダを出力するだけでは、自身のサイト上でも正当なコンテンツが表示されなくなってしまう事態が考えられる。

ウェブサイトによっては、不特定多数のウェブサイト向けに素材を iframe 要素で埋め込むように提供している場合がある（例：Facebook における「いいね！ボタン」等）。このような場合、その素材を提供するページでは、X-FRAME-OPTIONS を設定できない。

その場合は次のような対策を検討していただきたい。

＜操作の過程の一部を別ウィンドウで行わせる＞

クリックジャッキング攻撃は、視覚的にユーザが見えない状態を悪用する。したがって、操作の過程の一部を、視覚的に見える形の部分を用意することで、ユーザに気づかせることができれば、攻撃の成功率を下げることができる。

例えば**「素材を押すと、その処理の確認画面を別のウィンドウで行わせる」**ことが挙げられる。素材をユーザがクリックすることにより、自身のサイト上で投稿したり、サイトを評価したりする場合、素材を押すと、「投稿の確認画面」や「サイトを評価する」を別のウィンドウで行わせる。このようにすることで、攻撃者のページの影響を受けない形で確認画面が視覚的に見えるようになる。

＜一連の操作をクリックだけで完了させない＞

クリックジャッキング攻撃は、クリックのみで一連の操作が完了する点を悪用する。そのため、**「ユーザの設定の変更時には必ずパスワードの入力後に完了させる」**ような仕組みを用意することで、クリックジャッキング攻撃の影響を防ぐことができる。

なお、この方法は例えば次のような注意点がある。この点も併せて考慮してほしい。

- ユーザに入力をしてもらう文字列は、攻撃者が容易に指定できないように工夫する必要がある。外部から容易に推測ができる文字列で、GET リクエストで指定できる仕組みでは対策にはならない。
- 設定変更のたびにパスワード等を入力させる仕組みは、ユーザの利便性を下げる可能性がある。

◆ （3）-② HTML ファイル内に meta 要素で X-FRAME-OPTIONS を設定することができない

HTML ファイル内に meta 要素を使用して X-FRAME-OPTIONS を指定することで、HTTP レスポンスヘッダに出力できるが、Microsoft のページ[9]にも記載されているように、HTML ファイル内に meta 要素で X-FRAME-OPTIONS を設定しても有効にならないため、注意してほしい。

[9] http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

コラム：X-FRAME-OPTIONS 以外の対策方法

本コラムでは、X-FRAME-OPTIONS 以外の対策を 2 点紹介する。これらの対策は、「対策の実装が行われていないブラウザがある」、「対策の回避方法がある」等の事情があるものだ。そのため、対策の導入に当たっては、2013 年 2 月現在では推奨しないものである。

■ Content Security Policy を使用した対策

（1） Content Security Policy とは

Content Security Policy は W3C[10]で勧告されている規格である。Content Security Policy はクリックジャッキング攻撃だけではなく、クロスサイト・スクリプティングや盗聴による情報漏えいの被害を軽減するための仕組みである。

Content Security Policy を利用することで、例えば自身のウェブサイト上で動作してもよいスクリプトを指定することができる。これにより、仮にウェブサイトにクロスサイト・スクリプティングの脆弱性があったとしても、指定された URL 以外からのスクリプトは実行されないため、外部サイト上にある JavaScript が実行されず、クロスサイト・スクリプティングによってできる攻撃範囲を限定することが可能になる。

Content Security Policy でのクリックジャッキング攻撃への対策は X-FRAME-OPTIONS とほぼ同様で、指定したサイト以外に iframe 要素や frame 要素から読み込ませない効果がある。Content Security Policy は、読み込ませてもよいサイトについて、複数のサイトを指定できる等、X-FRAME-OPTIONS に比べてより細かい設定を行えることが特徴である。

Content Security Policy におけるクリックジャッキング攻撃の対策例を以下に示す。

● Content Security Policy の設定例

```
X-Content-Security-Policy: allow 'self'; frame-ancestors *.ipa.go.jp *.meti.go.jp
```

上記の例は、基本的なセキュリティのポリシーとしては、スクリプトや画像ファイルの表示等は自身のサイトで用意しているもののみに限定し、frame 要素や iframe 要素で読み込んでよいサイトを、自身のサイト以外に、ipa.go.jp ドメインのサイトおよび meti.go.jp ドメインのサイトに限定する設定である。

Content Security Policy の詳細な説明については、次のサイトを参考にしていただきたい。

Content Security Policy 1.0
http://www.w3.org/TR/CSP/

[10] World Wide Web Consortium：ウェブサイトを実現するための様々な技術の標準化を推進する非営利団体。

（2） 注意点

Content Security Policy を導入する際における注意点を次に挙げる。

- 2013 年 3 月現在、調査した範囲では Firefox のみ Content Security Policy によるクリックジャッキング攻撃の対策が有効に機能する[11]。
- クリックジャッキング攻撃専用の対策ではないため、自身のサイトのセキュリティポリシーを総合的に判断し、最低限動作しなければならない機能が何かを見極めて設定しなければならない。

[11] How Mozilla Does Web Security　Brandon Sterne OWASP AppSec 2010 – DC
https://www.owasp.org/images/3/37/Mozilla_OWASP_AppSec_2010_DC.pdf

■ JavaScript の Window オブジェクトを使用した対策

主要ブラウザに X-FRAME-OPTIONS が実装される前は、X-FRAME-OPTIONS 以外の対策も検討されていた。その一つに JavaScript の Window オブジェクトを使用した対策がある。

（1） 記述例

JavaScript の Window オブジェクトを使用した対策は、window.top プロパティにより、表示されるウェブページの最上位の位置を取得し、window.self プロパティにより、JavaScript が記載されているウェブページの位置を取得するものがある。

クリックジャッキング攻撃で、iframe 要素等によってウェブページを表示させようとした場合、window.top と window.self の値が異なるため、それを基に表示するウェブページを変更する対策だ。

- JavaScript を使用した対策の記述例

```
<script type="text/javascript">
        if(window.top !== window.self){
                window.top.location = window.self.location
        }
</script>
```

この記載例では、if (window.top !== window.self)で iframe 要素等により表示させられているかを判断し、iframe 要素等で表示されていれば、読み込み元のウェブページを代わりに表示させる。

（2） 注意点

この対策は回避方法も研究[12]されている。回避方法は複数の方法が存在するため、JavaScript を使ったクリックジャッキング攻撃への対策については、回避策等を全て加味したウェブページを作成しなければならないこととなり、複雑な対策を要することになる。

[12] http://seclab.stanford.edu/websec/framebusting/framebust.pdf

コラム：クリックジャッキング攻撃と共に対策する脆弱性

本コラムでは、クリックジャッキング攻撃と共に対策すべき脆弱性について述べる。クリックジャッキング攻撃といくつかの類似点を持つクロスサイト・リクエスト・フォージェリ(以降 CSRF と呼ぶ)がその脆弱性である。

CSRF とは、ユーザが登録制のウェブサイトにログインしている状態で、罠サイトのリンク等をクリックすることでユーザが意図していないようなリクエストを送信してしまい予期しない処理を実行させられてしまう脆弱性である。

下記の表で CSRF がクリックジャッキング攻撃と同じようなページで対策を必要とすることがわかる。ただし、それぞれへの対策は異なるため、一方の対策を行っていても他方の対策が漏れていた場合は同じ脅威が存在し続けてしまう。クリックジャッキング攻撃への対策を必要とするウェブサイトは CSRF への対策も必要とする可能性が高いため、漏れなく対策することが重要だ。

クリックジャッキング攻撃と CSRF 攻撃の類似点

攻撃	類似点
クリックジャッキング攻撃	**[脅威]** ・意図しない投稿 ・意図しない設定の変更
	[対策を必要とするページ] ・クリック操作でユーザの情報の設定、退会を行うページ ・クリック操作でユーザが投稿を行うページ
CSRF[13]	**[脅威]** ・意図しない投稿 ・意図しない設定の変更
	[対策を必要とするページ] ・ユーザの情報の設定、退会を行うページ ・ユーザが投稿を行うページ

[13] http://www.ipa.go.jp/security/vuln/documents/website_security.pdf

おわりに

今回の IPA の調査で、X-FRAME-OPTIONS によるクリックジャッキング攻撃への対策が必要と考えられる多くのウェブサイトで行われていないことがわかった。X-FRAME-OPTIONS のウェブサイト側での普及はまだまだ進んでいないと考えられる。

本書等を参考にウェブサイト運営者は、クリックジャッキング攻撃への対策を推進することが望まれる。

IPA テクニカルウォッチ

知らぬ間にプライバシー情報の非公開設定を公開設定に変更されてしまうなどの「クリックジャッキング」に関するレポート

［発　　行］2013 年 3 月 26 日

［著作・制作］独立行政法人情報処理推進機構 セキュリティセンター

編集責任　　小林 偉昭

執筆者　　関口 竜也　　相馬 基邦
協力者　　徳丸 浩（非常勤研究員）