JPCERT-ED-2009-0001

JPCERT/CC

技術メモ ー クリックジャッキング対策

～ X-FRAME-OPTIONS について ～

第二版：2009-03-04 (Ver. 2.0)

初　版：2009-03-03 (Ver. 1.0)

執筆者：常見 敦史、小宮山 功一朗

本文書の掲載 URL：http://www.jpcert.or.jp/ed/2009/ed090001.pdf

本文書は、Web サイト制作者及び運営者を対象に、クリックジャッキング攻撃の概要とその対策の一つとして X-FRAME-OPTIONS の概要、記述方法、設定値による挙動の違いについて解説します。

改訂履歴

	変更内容	日付
初版		2009 年 3 月 3 日
二版	● 章番号を追加しました。 ● 4 ページ「1. はじめに」の 6 行目から 8 行目において、原因に関する記述を修正しました。	2009 年 3 月 4 日

目次

1 はじめに

クリックジャッキングは、Robert Hansen 氏、Jeremiah Grossman 氏が報告した Web 利用者を標的とした攻撃手法です。2008 年 9 月 27 日に OWASP NYC AppSec 2008 カンファレンスにおいて詳細を発表する予定が、ベンダーからの要請により直前にキャンセルされたことが報道されるなど IT 関連のマスコミが大きく取り上げました。

両氏の発表とその後のセキュリティ研究者等の調査により、主要な Web ブラウザ利用者すべてがこの脅威の影響を受けることが明らかになったものの、原因が HTML や Flash などのコンテンツを透過表示できる仕組みそのものに関わるため、対策が難しいと考えられていました。

近日リリース予定の Microsoft Internet Explorer 8（以降、IE8）ではクリックジャッキングの解決を目的とした機能の追加が予定されています。詳細な技術的解説は次章以降で触れますが、IE8 に追加されるクリックジャッキング対策機能は、Web サイト側がこの機能に対応することではじめて効果が期待されるものであり、単に利用者が IE8 を導入しただけでは対策となりえません。よって、Web サイトの制作者及び運営者は利用者を守るためにこの新機能を正しく理解し、適切な設定を行うことが必要です。

本技術メモではクリックジャッキングの概要と IE8 で導入が予定されているクリックジャッキング対策機能がどのようなものかを紹介し、その概要及び設定方法について記述します。

なお、本技術メモは執筆時点における最新の IE8 RC1 を使用して検証を行っております。

2 クリックジャッキングとは

2.1 クリックジャッキングの概要

現在までに公開されている情報を総合すると、クリックジャッキングとは、図 1 に示すように透過指定された iframe 等の要素に標的サイトのコンテンツを読み込み、これを攻撃者サイトの他の要素より上に配置することで Web ブラウザの画面上には攻撃者サイトの要素だけを表示させ、その上で利用者が行うクリックを攻撃者サイトへのクリックから標的サイトへのクリックに置き換える手法です。

クリックジャッキングには、JavaScript を無効にしていても影響を受ける、標的サイト上の任意の要素に対し画面遷移を含む複数回のクリックをさせることが可能などの特徴があります。

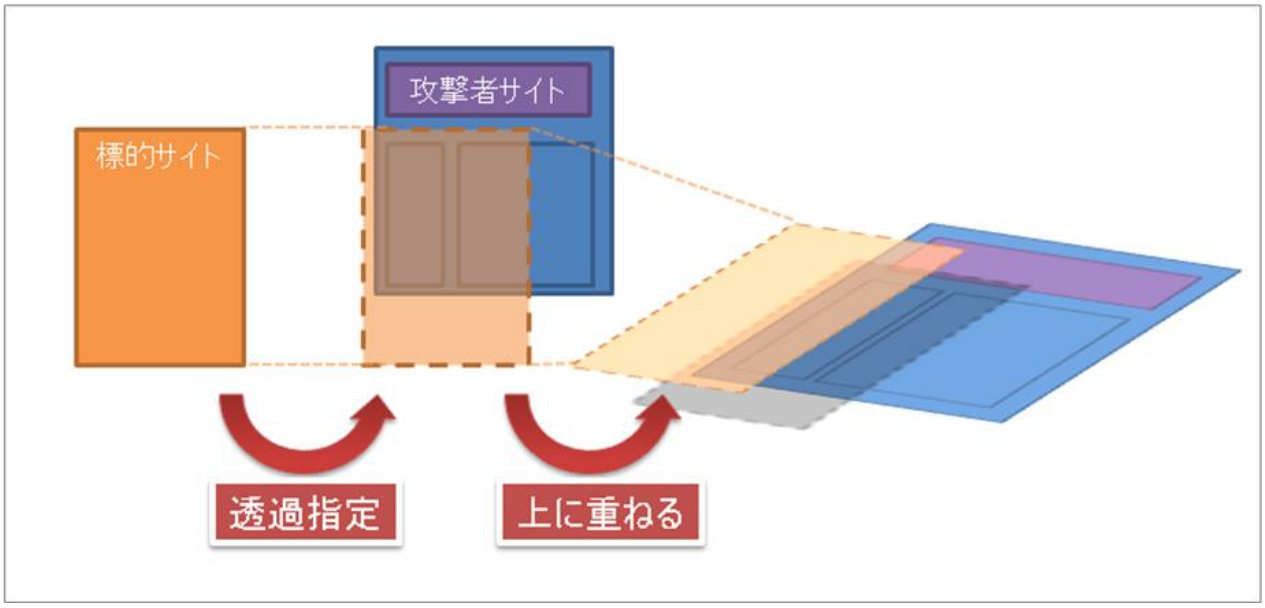

図 1・標的サイトを透過指定し、他の html コンテンツの上に配置する概念図

この手法を攻撃者が悪用することにより、悪意ある Web サイトに誘導された利用者が、気付かない間に標的サイト上で不正操作（ショッピングカートの操作、メールの送信、広告のクリック、会員サービスからの退会など）を引き起こすクリックをさせられる可能性があります。攻撃事例はまだ少ないものの、2009 年 2 月には Twitter において利用者の意図しない投稿をさせられてしまう事件が発生しました。

2.2 クリックジャッキング対策

この新たな脅威に対しては様々な対策手法が模索されている段階です。以下に実装が進んでいる、いくつかの例について紹介します。

■JavaScript を使った描画制御

一例としては JavaScript の Window オブジェクトを使用するというアプローチがあります。JavaScript の Window オブジェクトには window.top と window.self というプロパティがあります。window.top は「最上位のフレーム」を、window.self は「スクリプトが記載されているフレーム自身」を表します。コンテンツが他のフレームなどから読み込まれている場合(window.top と window.self の値が違う場合)にはダミーのコンテンツを表示させるなどの手法をとることでクリックジャッキング対策が実現できます。この手法は Web サイト制作者が手軽に導入できるというメリットがある反面、利用者のブラウザで JavaScript の実行が許可されていないと効果を発揮しないデメリットがあります。

■ブラウザ側での対策

ユーザが行える対策として、クリックジャッキング攻撃の多くに見られる、フレームの不透明度を細工する(opacity)、表示の前後位置を細工する(z-index)といった特徴を持つコンテンツの表示を避けるという方法が考えられます。Firefox のアドオンである”NoScript”はこの観点から隠されている領域の不透明度の設定を変更し可視化する「Opacize」や、透明な iframe 上でのクリックをブロックする「ClearClick」といった対策技術を導入しています。これらの方法のデメリットは iframe を使用した正当なサイトのコンテンツを攻撃と誤って認識する可能性が高いことや、柔軟性に乏しく新たな攻撃パターンが登場する都度対策を改める必要があるという点です。

またこれ以外にも Flash Player のバージョンアップなどによって対策がされる例もありますが、ここでは割愛します。

次章では、これらの対策のデメリットを補完する新たな手法と、その手法の実現を図り IE8 でサポートされる「X-FRAME-OPTIONS」について説明します。

3　クリックジャッキング対策機能「X-FRAME-OPTIONS」について

クリックジャッキングは、自分の管理する Web ページが悪意のある Web サイト上のフレームに表示されることで発生します。よって、

1) Web サーバ側で、外部サイト上のフレームに表示されることの可否を宣言する
2) Web ブラウザは受け取った Web サーバからの宣言に従い、表示が許可されていない
　場合はそのコンテンツを外部サイト上のフレームに読み込まない

といった取り決めをすることで対策が実現できます。

IE8 では、新たにサポートされる「X-FRAME-OPTIONS」という HTTP レスポンスヘッダーによって、こうした対策の実現を図っています。Web サーバ管理者は、Web サーバが送信する HTTP レスポンスヘッダーに「X-FRAME-OPTIONS」を加えるよう設定を行うことで、IE8 に対し、外部サイト上のフレームに自分の管理する Web ページが表示されることの可否を宣言することができます。「X-FRAME-OPTIONS」を含む HTTP レスポンスヘッダーを受け取った IE8 は、図 2 に示すように Web ページをフレーム上に表示することの可否を判断し、描画を変えます。

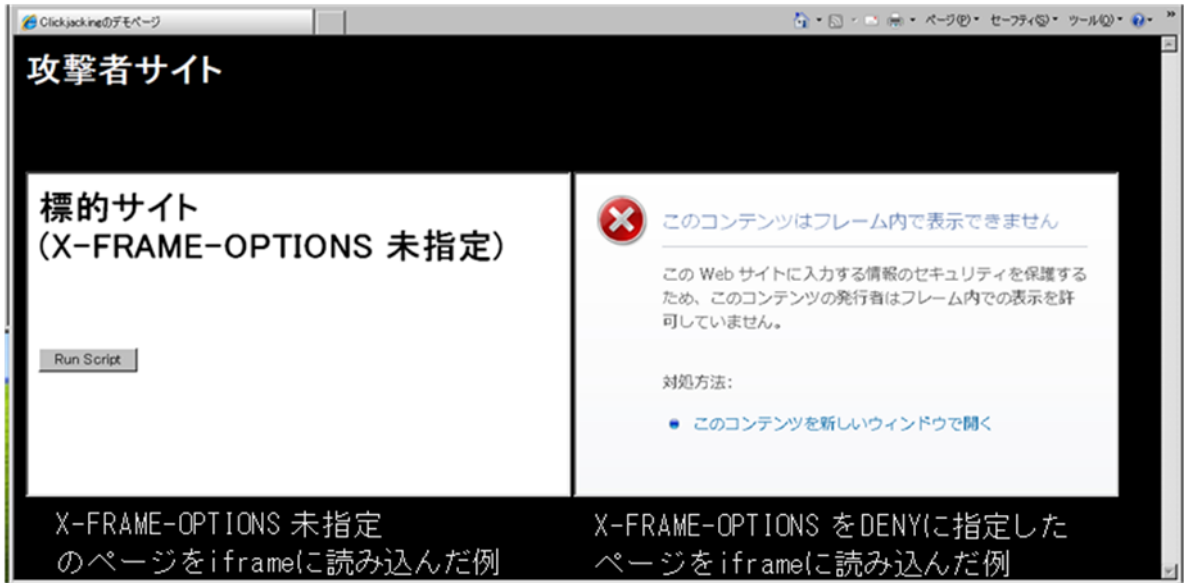

図 2 X-FRAME-OPTIONS 指定の有無による挙動の違い

3.1 X-FRAME-OPTIONS の設定値と効果

「X-FRAME-OPTIONS」には設定値として”DENY”と”SAMEORIGIN”が存在します。以下にそれぞれの設定値と効果について説明します。

設定値	効果
DENY	他の Web ページ上の frame 及び iframe 上での表示を拒否します。
SAMEORIGIN	Top-level-browsing-context が一致した場合のみ、他の Web ページ上の frame 及び iframe 上での表示を許可します。一致しない場合は表示を拒否します。

4 X-FRAME-OPTIONS の記述方法

「X-FRAME-OPTIONS」を送信するには、以下の 2 種類の方法が考えられます。Web サーバ管理者は主に 4.1 の内容を、Web サイト制作者は主に 4.2 の内容をそれぞれ参考にしてください。なお、本項では設定値を”DENY”にする場合を記述しています。SAMEORIGIN を指定する場合は”DENY”を”SAMEORIGIN”に読み替えてください。

なお、JPCERT/CC の評価環境においてこのヘッダーを追加することによる不具合は現在確認されておりませんが、導入に際しては構成システム上でよく動作確認をされることをお勧めします。

4.1 Web サーバに記述する

Web サーバの設定ファイルを書き換えることでヘッダーを追加する方法です。個別の html ファイルに対する変更作業が生じないため、管理する Web サーバに X-FRAME-OPTIONS を一括して設定したい場合はこの方法が便利です。

以下、一例として Debian 上の Apache2 と、Windows Server 2003 R2 上の IIS6.0 における設定例を記述します。いずれも JPCERT/CC の評価環境における導入テストに基づいた内容ですので、お使いの環境と照らし合わせて参考にしてください。

■Apache2 の場合

apache2.conf に以下の記述を追加して、プロセスを再起動します。

```
<IfModule mod_headers.c>
   Header append X-FRAME-OPTIONS “DENY”
</IfModule>
```

■IIS6.0 の場合

インターネット インフォメーション サービス マネージャを起動し、ツリーから既定の Web サイト(設定対象を限定する場合は任意の Web サーバ) を右クリックし、プロパティを表示します。HTTP ヘッダー タブを選択し、カスタム HTTP ヘッダーの 追加 をクリックします。

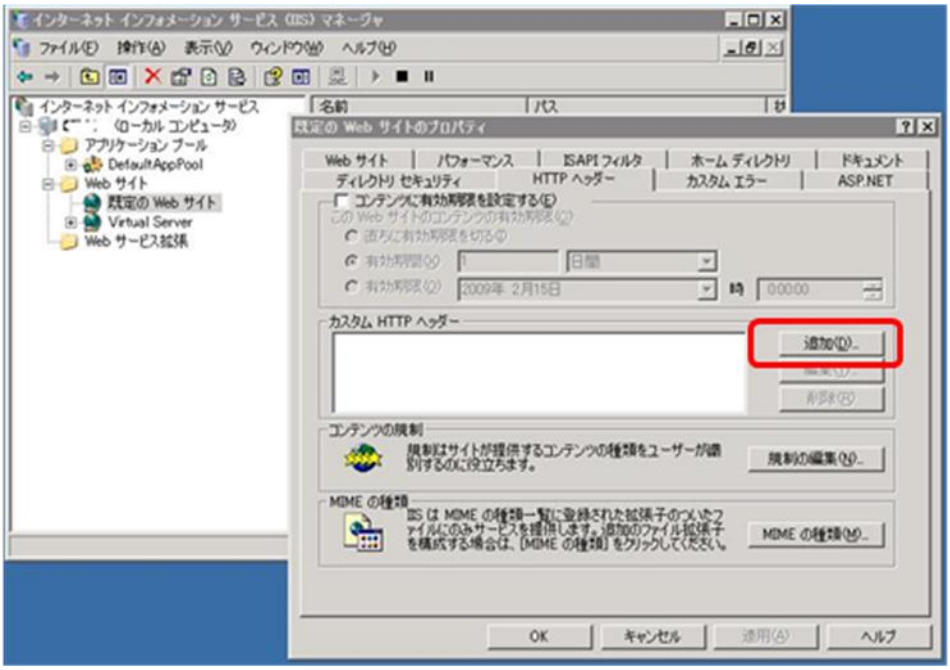

図 3 IIS6.0 におけるカスタム HTTP ヘッダーの追加方法（1）

カスタム ヘッダー名に ″ X-FRAME-OPTIONS ″、カスタム ヘッダー値に ″DENY″を追加し OK を押下します。適用または OK を押下し、マネージャを閉じます。

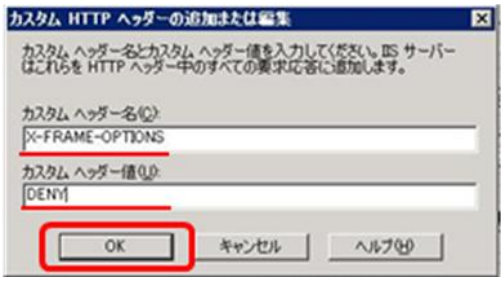

図 3 IIS6.0 におけるカスタム HTTP ヘッダーの追加方法（2）

4.2 HTML ファイルに記述する

Web サーバ全体の設定を変更できない、あるいはコンテンツやサービスごとにオプションの値や記述の有無を変えたい場合などは、http-equiv を使用して、HTML ファイルに直接記述することが可能です。

HTML ファイルの<head>タグ内に

```
<meta http-equiv="X-FRAME-OPTIONS" content="DENY" />
```

を追加し、保存します。

5 まとめ

「X-FRAME-OPTIONS」は、Web サイトの制作者及び運営者が実行可能なクリックジャッキング対策として有望な手法と言えます。特にクリックジャッキングによる脅威が大きいと考えられるショッピングサイトやオンラインバンキングサイトでは、脅威からの利用者保護を目的として本ヘッダーの導入を検討してください。

現在のところ、標準で「X-FRAME-OPTIONS」を元にレンダリングの挙動が変わるブラウザは IE8 のみ（Firefox 用のアドオンである NoScript はこのヘッダーに対応しています）であり、他のブラウザベンダーが対応を行うかどうかは現時点では不明です。

「X-FRAME-OPTIONS」が効力を発揮するには、これに対応したブラウザが一般ユーザに行き渡るとともに、クリックジャッキング対策が必要なすべての Web サイトがこのヘッダーを送出することが条件になります。

その間にも、新たなクリックジャッキングの手法が出現することが予想されるため、「X-FRAME-OPTIONS」への対応、それ以外のクリックジャッキング対策の検討、そしてそれらの対策に向けた攻撃手法の分析を並行して継続的に進めることが必要です。

6 参考資料

IE8 Security Part VII: ClickJacking Defenses –IEBlog

http://blogs.msdn.com/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx

Birth of a Security Feature: ClickJacking Defense –IEBlog

http://blogs.msdn.com/ie/archive/2009/02/02/birth-of-a-security-feature-clickjacking-defense.aspx

IE8's clickjacking fix not much help, security researchers say

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9000189&taxonomyId=17&pageNumber=2

IETF:RFC 2616 – Hypertext Transfer Protocol -- HTTP/1.1

http://www.ietf.org/rfc/rfc2616.txt

NoScript – JavaScript/Java/Flash blocker for a safer Firefox experience!

http://noscript.net/

＜お願い＞

引用の際は、引用元名、資料名、URL を明示してください。

なお、引用の際は引用先文書、時期、内容等の情報を JPCERT/CC 広報（office@jpcert.or.jp）までメールにてお知らせください。今後、より良い情報を提供するため、どこで、どのような方に、どのような場面で、お使いいただけているのかを把握し検討するため、ご協力をお願いいたします。