

2004年10月15日

## 不正アクセス事件に関する当社の対応について

ファーストサーバ株式会社  
代表取締役社長 岡田 良介

2003年11月上旬頃、当社のお客様である社団法人コンピュータソフトウェア著作権協会様(以下、「ACCS様」)の管理するサイト「ASK ACCS」(<http://www.askaccs.ne.jp/>)において不正なアクセスが行われ、2004年2月4日、その容疑者が逮捕されるという事件が発生しました。

本件に関しましては、刑事裁判が進行中である関係から、これまでは情報公開を極力控えて参りました。しかしながら、裁判に影響を及ぼさない範囲で事実関係を公表することが、当社をご利用頂いている2万社のお客様、さらにはインターネットをビジネス活用されているすべての方々の利益に資すると判断いたしました。そこで以下の通り、当社が調査した事実関係及び当社の行った措置について、ご報告させていただきます。

### 1. 事実関係について

2002年12月

当社が提供していたお客様の向けのCGI(以下「旧標準CGI」という)の一部に、不正なアクセスの原因となる脆弱性が存在していることを、社内のサニタライジング(プログラム脆弱性チェックおよび除去)作業の過程で発見する。直ちに、想定される攻撃に対して対抗可能なCGIを準備し、旧標準CGIを上書きする。

ただし、旧標準CGIはソースコードを公開しており、一部お客様が自らプログラムソースを書き換えたCGI(以下「カスタマイズCGI」という)が存在していた。これらのCGIは修正すると正常な動作を保証できないため、強制的に上書きすることができなかった。

この時、「CGIのソースコードをお客様に提供するサービス方法に」内在する危険性が認識され、問題の根本的な解決を図るため、新たなCGI提供方式の開発に着手する。

2003年3月

新型CGIが完成し、お客様に提供を開始する(以下「新標準CGI」という)。新標準CGIは、お客様によるプログラムソースの改変ができない仕組みとすることにより、CGIの同一性を保持し当社がセキュリティ対策を漏れなく施せるといふ、新しい提供方式を採用している。

新標準CGIの提供開始と同時に、プログラムソース公開型の旧標準CGIを当社のサポー

ト外とすることをお客様に予告する。以降、継続的に新標準 CGI への移行をお客様に推奨案内する。

なお、お客様の新標準 CGI への移行が完了する前に脆弱性を公開してしまうと、お客様に大きなリスクを発生させることとなるため、これを行わないこととした。

2003 年 8 月

新標準 CGI への移行準備期間として 5 ヶ月をおいた後、旧標準 CGI を当社のサポート外とした。

2003 年 11 月

ACCS 様の事件が発生する。

当社では、2003 年 11 月 9 日に、不正なアクセスが行われた疑いがあると認知し、独自に原因の調査を開始する。

また事件が公になると、約 2 万社におよぶ当社のお客様の運営サイトへ攻撃が行われることが危惧されるため、直ちにお客様のサイトを防衛する措置を施す。旧標準 CGI をサーバ上に復活させたり、残存させたりしているお客様に危険性を通知し、セキュリティ対策を施した旧標準 CGI で問題のある CGI を上書きした。

加えて、カスタマイズ CGI についても、2002 年 12 月当時は強制的な上書きを行えなかったが、事態が緊急を要したため、当社でプログラムソースの書き換え支援を行うなどして、脆弱性を除去する作業を実施する。一方、お客様には、「新標準 CGI」への移行を強く推奨する。

2004 年 2 月

カスタマイズ CGI の脆弱性除去作業を完了。

## 2 . ACCS 様サイト「ASKACCS」に残存した CGI について

当社は、2004 年 1 月、捜査当局より、事件発生当時に ACCS 様サイト「ASKACCS」のサーバ内で動いていた CGI の提示を受けました。その結果、当該 CGI が旧標準 CGI であることを確認いたしました。

社内調査を行ったところ、ACCS 様のサイト「ASKACCS」に旧標準 CGI が残存していた原因は、2002 年 12 月の CGI 上書き作業の際、当社が、当該 CGI が旧標準 CGI であるにもかかわらず、カスタマイズ CGI と誤認し、上書きを実施していなかったことにあると判明いたしました。

また今回の事件ではサーバ内に蓄積されていたログファイルが不正なアクセスの対象となりました。このログファイルは旧標準 CGI が個人情報や質問等の送信を受けたときに自動的に生成するものです。しかしながら当社は、旧標準 CGI がこのような機能を有して

いることを、お客様には説明しておりませんでした。

今回の事件につきましては、旧標準 CGI がサポート対象外となって以降に発生したものとはいえ、当社が提供した CGI をご信頼の上ご利用いただいていた ACCS 様に多大なご迷惑をおかけいたしました。心よりお詫び申し上げます。

### 3. 当社ポリシーについて

当社におきましては、自らセキュリティ対策を施せるお客様が必ずしも多くなく、脆弱性情報の公開がお客様の二次被害につながる恐れがあることに鑑み、脆弱性情報を原則として非公開とすることをポリシーとしております。しかしながら今回の事件を受け、当社のポリシーが必ずしも最善の策とはならないことを認識致しました。当社においてセキュリティ対策を施すことのできる新標準 CGI の頒布が進んでいることも考え合わせ、今後は適宜、情報の公開を致す所存であります。

もっとも、お客様の管理下におかれるサーバ領域のセキュリティ確保については、当社の努力のみでは十分ではありません。お客様ご自身のセキュリティ意識の向上が、何よりも重要となります。お客様におかれましても、今後ともセキュリティ確保の為の施策を御実施頂きますよう、御協力お願い申し上げます。

以 上