1ZA-5

偽造証明書を用いたファーミング攻撃の危険性について

平井 圭佑† 菊池 浩明†
†東海大学 情報通信学部 通信ネットワーク工学科

1 はじめに

近年，偽サイトへ誘導して ID などを盗聴するフィッシング攻撃や，事前に DNS や SSL 証明書を偽造した環境を用意するファーミング攻撃などの危険性が高まっている．フィッシングサイトの見分け方の一つとして SSL による公開鍵証明書 (証明書) があるが，自己署名された偽のルート証明書を用いて簡単にユーザとフラウザをだますことができる．Soghoian らは，政府による強制証明書偽造攻撃のリスクを指摘している [1]．それゆえ，フォームの送受信において SSL が利用されているからといって安易に信じることはできない．

そこで，本研究では偽造証明書を用いたファーミング攻撃の危険性について検証することを目的とする．本稿では，標的型メールで攻撃の評価，偽造証明書を用いた SSL 中間者攻撃，ルート証明書インポートの危険性について報告する．

2 実験

2.1 中間者攻撃

図 1 は，1 で DNS サーバにサイト *C* の IP アドレスを問い合わせ，2 で偽サーバ *B* の IP アドレスを返す．3 で *C* のつもりで偽サーバ *B* にアクセスし，*B* が入力された情報を抜き取る．*B* は 4 で正規サーバにアクセスし返ってきたデータを 6 でユーザ *A* に返す．

2.2 実験目的

1. 偽サーバにアクセスするよう書き換えた偽 DNS サーバと偽のルート証明をインポートした実験環境を実現し，ファーミング攻撃の実現可能性を検証する．

2. 証明書を偽造したフィッシングサイトが及ぼす危険性を，偽造証明書作成の容易さとインターネットカフェなどフィーミングが実現可能な環境における発見の困難性の観点から明らかにする．

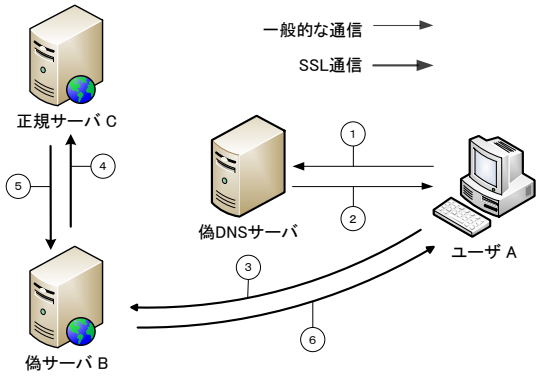

図 1: SSL 中間者攻撃

2.3 実験方法

実験環境を表 1 に示す．

表 1: 実験環境

OS	Ubuntu 11.10
メモリ	1GB
CPU	Intel Xeon E5620 2.4GHz
HTTP サーバ	Apache 2.2.20
証明書	OpenSSL 1.0.0e

OpenSSL を用いて東海大学授業支援システムの偽 Web ページの証明書を作成する．作成した証明書を Apache に適用した偽ウェブサーバを用意する．ファーミング環境として，事前に作成したルート証明書をインポートしたパソコンを用いて，判別の難しさ，危険性，インポート時の安全性について考察する．

実験 1 標的型メールでの検証

東海大学の 3 年，4 年次生を対象に教務課を装った評価用のフィッシングメールを送信し，アクセスした学生に対してアンケートを取る．期間は 8 月 1 日から 8 月 20 日の 20 日間である．

実験 2 偽造証明書を用いた SSL 中間者攻撃

図 1 に示す環境を用いて，正規サイト，DNS を変更しない状態のフィッシングサイト，DNS を変更したフィッ

On the risk of pharming attack using fake certificate.
†Keisuke HIRAI †Hiroaki KIKUCHI
†School of Information and Telecommunication Engineering, Tokai University

シングサイトの違いをブラウザから判定することの困難性について検証する．

実験 3　ルート証明書インポートの危険性の評価

ルート証明書のインポート開始手順とクリック数，ID やパスワードの入力の有無を OS , ブラウザ別に評価した．

2.4　実験 1 の結果

フィッシングサイトにアクセスした人は 32 名で，約 47%の 15 名が回答した．回答したうちの 7 割以上が本物のサイトと思いアクセスしている (表 2). 実際に気付いた人はごくわずかで，標的型攻撃はフィッシングに対し大きな脅威となることが裏付けられた．

表 2: アンケートの回答結果

回答内容 (選択式)	3 年	4 年	計	[%]
本物のサイトだと思った	1	10	11	34.4
URL があったからクリック	2	1	3	9.38
偽サイトだと思ったがアクセス	1	0	1	3.13
メール内容で気付いたがアクセス	1	0	1	3.13
無回答	8	9	17	53.1
合計	11	20	32	100

2.5　実験 2 の結果

図 2 に正規サイト A と DNS 変更前 B , 変更後 C の 3 つの URL の違いを示す．図 3 は，正規サイト A の証明書と偽サイト C の証明書の違いを示している．B の DNS 変更前は明らかに URL が違うため容易に見破り判断することができるが，DNS を変更すると元のサイト A と偽サーバのサイト C とが全く同じで判別ができない．

A と C の違いは，図 3 の証明書のパスのみである．サイトの正規性を検証するために証明書を確認しても，一見問題なく見える (図 3). ルート証明書をインストールしてあれば，C をアクセスしてもブラウザは警告しない．ルート証明書のインポート手順を表 3 に示す．

図 2: URL の違い

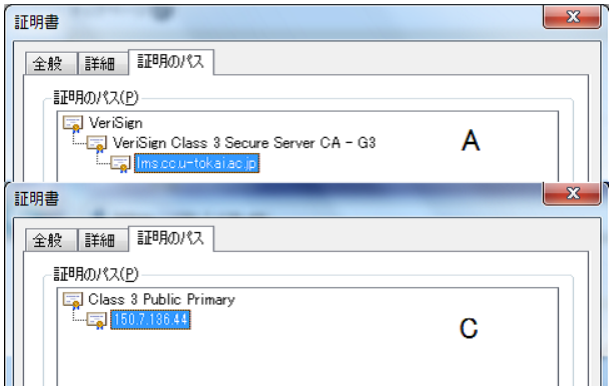

図 3: 正規サイトの証明書と偽の証明書のパスの違い

2.6　実験 3 の結果

Windows では，ID やパスワード入力などの認証もなく，インポート用の証明書をダブルクリックですることでインポートできてしまい，安全性は低い．これに対し，FireFox や Opera ではメニューから選択し，インポートすることから安全性は普通であり，MacOS はファイルから実行しインポートできるが，ID の入力とパスワードの入力が必要なことから安全性は高いとした．

表 3: 証明書インポート手順と安全性

	Version	開始場所	選択数	承認	安全性
Windows	XP	ファイル	10	無	低
	7				
Mac OS X	10.6.8		7	有	高
	10.7.2				
FireFox	8.01	メニュー	11	無	中
Opera	11.60		12		

3　おわりに

本研究では，ファーミング環境として，自己署名されたルート証明書がインポートされた PC を用いることで，発見困難なフィッシングサイトを容易に実現できることを示した．ルート証明書を強制インストールするケースは頻繁にあり，重大な脆弱性になり得る．本実験は特定のサイトで静的に中間者攻撃をしたが，動的に自動証明書偽造も可能である．これらの攻撃を防止するには，Windows において証明書のインポートのアクセス制御を改良するべきである．

参考文献

[1] C. Soghoian and S. Stamm, “Certified lies: Detecting and defeating government interception attacks against SSL”, In Proceedings of Financial Cryptography and Data Security(FC 2011), pp. 1-18, 2011.