5W-06

不正送金対策向け金融サイバーキルチェーンの検証

岡田　周平†　　森　滋男†　　後藤　厚宏†

情報セキュリティ大学院大学†

概要

不正送金を狙う攻撃には，複数の手口があり，いずれも複数の攻撃フェーズから構成される．また，対策を講じる者（以下「対策主体」）は，口座保有金融機関，預金者，他の金融機関，ISP，セキュリティベンダ，警察当局等多岐に亘る．対策には，どの対策主体が，どのような手口を，いずれの攻撃フェーズで防御するものなのかという属性があり，各対策主体は，これらを明らかにした上で，自身が実施すべき対策を理解，合意し，履行することが不可欠である．以上を踏まえ，不正送金を狙う攻撃に対して，最適な防御に向けた分析及び対策主体間における認識の共通化を改善し，対策全体の強化を行うことを目的に，「金融サイバーキルチェーン」を提案した[1]．本稿では，不正送金を狙う攻撃事例を基にケーススタディを実施し，提案手法の有効性を検証した結果について報告する．

１．提案手法

提案手法は，不正送金を狙う攻撃に対する個々の対策の効果と限界を明確にする分析フレームワークである．不正送金を狙う攻撃者の行動を起点として，攻撃フェーズ及び対策を表形式で表現する．具体的には，攻撃分析表，対策表（対策主体別）及び対策表（効果分類別）の 3 つの表から構成される．想定する利用対象は，預金者を除く対策主体である．

２．ケーススタディ

2.1　目的と実施内容

ケーススタディの目的は，不正送金を狙う攻撃事例を基に，個々の対策の有効性や更なる対策の検討，対策主体の分類を行うことである．実施対象は，提案手法のうち，攻撃分析表及び対策表（対策主体別）とする．

実施フローは次のとおりである．まず，利用者は，攻撃事例を収集する．また，検証対象金融機関である X 銀行及びその他の対策主体の対策事例を収集する．次に，時系列に記述した攻撃事例に対して，対策事例が効果を発揮する箇所を追記する．併せて，各対策事例の対策主体を記述する．以上により，攻撃分析表及び対策表を生成する．これらの表を基に，個々の対策の有効性や更なる対策の検討，対策主体の分類を行う．

2.2　攻撃事例及び対策事例の収集

ケーススタディで利用する攻撃事例は，調査対象の 33 金融機関が Web サイトにおいて公表している情報及び記事を中心に収集した．収集対象期間は 2013 年 1 月から 2016 年 12 月の 4 年間である．上記収集の結果，ケーススタディは 6 個の公表事例を基に実施する（表 1）．

表 1　攻撃事例の概要

	手口の概要
事例 1	検索連動型広告　→　フィッシング
事例 2	電子メール　→　フィッシング
事例 3	SMS　→　フィッシング
事例 4	電子メール　→　マルウェア感染 →　Web インジェクト　→　スパイウェア
事例 5	不正な Web サイト　→　マルウェア感染 →　取引偽造送金
事例 6	不正な Web サイト　→　マルウェア感染 →　ファーミング　→　フィッシング

事例 6 のうち，手口が公表されているエクスプロイト，インストール，C2 及び資金移動指示フェーズについてケーススタディを行った結果を，表 2 に示す．

2.3　検証

2.2 で行った事例 6 に対するケーススタディと同様に，収集した 6 個の事例すべてについてケーススタディを行った検証結果は，次のとおりである．

(1) 攻撃者の行動及び対策の分類

X 銀行及びその他の対策主体は，20 を超える対策を講じており，個々の対策がどの手口を，いずれの攻撃フェーズで防御できるのかを分類できた．

(2) 分類結果の分析

①攻撃者の行動に着目した分析

偵察及び武器化フェーズでは対策が見られない．本フェーズにおいて攻撃を阻止するには，攻撃者がフィッシングサイトや不正プログラム配布サイトを構築した段階で，構築した事実を検知する技術の導入が考えられる．

次に，デリバリ，エクスプロイト及びインストールフェーズでは，預金者を中心に対策を講じている．本フェーズにおいて攻撃を阻止するには，預金者における対策の普及が求められる．また，3 個の事例（事例 4，5，6）において，金融マルウェアが利用されている．この点を踏まえ，投資効果を考慮しつつ，より早い段階で攻撃を阻止するため，不正プログラム配布サイト閉鎖サービスの導入が考えられる．

C2 フェーズでは，金融機関，預金者，ISP 及びセキュリティベンダが対策を講じている．本フェーズにおいて攻撃を阻止するには，金融機関において導入している EV SSL 証明書の確認や不正送金対策向け AV の利用徹底が求められる．

資金移動指示フェーズは資金移動を行う水際であり，金融機関，預金者及びその他の金融機関が対策を講じている．5 個の事例（事例 1，2，3，4，6）において，フィッシングや金融マルウェアにより認証情報が盗取され，なりすましが行われている．不正送金の被害は，OTP を利用していないことに伴い発生していることが多い[2]．預金者における対策の普及を進める一方で，利用者に頼らない対策を同時に進める必要があると考える．具体的には，リスクベース認証の導入が考えられる．ま

Verification of Financial Cyber Kill Chain for countermeasures against financial fraud

Shuhei OKADA†, Shigeo MORI†, Atsuhiro GOTO†

†Institute of Information Security

表2　事例6に関するケーススタディの結果

No.	発生事象	攻撃者	防御者					
		攻撃フェーズ	金融機関	預金者	他の金融機関	ISP	セキュリティベンダ	警察当局
1	攻撃者は Adobe Flash Player の脆弱性を突いて，インターネット利用者の PC の Web ブラウザ上で攻撃コードを実行した.	エクスプロイト						
2	当該インターネット利用者は，【OS 等の最新化】を行っておらず，攻撃コードが実行された.	↑		✔				
3	当該インターネット利用者の PC は，金融マルウェアに感染し，金融マルウェアは，継続的に当該 PC を監視した.	インストール						
4	【抗ウイルスソフト（以下「AV」）】は金融マルウェアを駆除できなかった，又は，駆除できたが，本対策を導入していなかった.	↑		✔				
5	2016 年 7 月以降，当該預金者が感染 PC で Google にアクセスすると，金融監督庁を騙った不審なポップアップが表示された.	C2						
6	ポップアップには 8 金融機関が表示されており，本銀行の部分をクリックすると，偽サイトに誘導された.	↑						
7	【EV SSL 証明書】が正規のサイトに導入されていたが、一部の預金者は気付かなかった.	↑	✔	✔				
8	【不正送金対策向け AV】は金融マルウェアを駆除できなかった，又は，駆除できたが，本対策を導入していなかった.	↑	✔	✔				
9	預金者は、偽サイトに誘導されたことに気付かず，認証情報を入力した.	↑						
10	攻撃者は，何らかの手法により，偽サイトに保存された預金者が入力した認証情報を盗取したと推測される.	↑						
11	本ケースはキー入力を盗聴するものではなく，【ソフトウェアキーボード】は有効でなかった.	↑	✔	✔				
12	金融マルウェアの C&C（以下「C2」通信について，【C2 通信遮断】を行うことにより，一部の攻撃が阻止できた可能性がある.	↑				✔	✔	
13	資金移動指示には認証情報が必要であったが，攻撃者は当該情報も入手していたため，指示を行った可能性がある.	資金移動指示						
14	攻撃者はログインパスワードを含む認証情報を盗取しており，【複数回のログイン試行の失敗によるサービス利用停止】は有効でなかった.	↑	✔					
15	攻撃者は乱数表を含む認証情報を盗取しているため，【乱数表】及び【複数 PW による認証】は有効でなかった.	↑	✔	✔				
16	【ワンタイムパスワード（以下「OTP」）（ハードウェアトークン，ソフトウェアトークン）】について，攻撃者は当該情報を盗取できず，有効であったと推測される．しかしながら，一部の預金者は，本対策を導入していなかった.	↑	✔	✔				
17	攻撃者はログインパスワードを含む認証情報を盗取しているため，【自動タイムアウト】は有効でなかった.	↑	✔					
18	【IP 等情報共有】は資金移動指示を遮断できるため，一部の攻撃が阻止できた可能性がある.	↑	✔		✔			

た，2 個の事例（事例 4，5）において，OTP が有効でない可能性がある．この点を踏まえ，投資効果を考慮しつつ，トランザクション署名，二経路認証の導入が考えられる.

最後に，出金フェーズでは，攻撃者が用意した口座への資金移動が行われており，金融機関，預金者及び警察当局が対策主体となり，被害の軽減に関する対策や，犯人逮捕等の対策を講じている．本フェーズにおいて攻撃を阻止するには，攻撃者が現金化を行うより前に，資金移動が行われている事実を検知する対策の導入が考えられる.

②対策主体に着目した分析

デリバリフェーズ以降，各攻撃フェーズにおいて一貫して対策を講じているのは，預金者である．また，攻撃の初期段階で対策を講じられるのも預金者である．佐野ら[3]は，「対策の提供と利用者に対して説明・教育、知らない人・意識の薄い人に対しては周知をするという 3 つを行うことが必要であると感じる」と論じているが，本分析の結果からも，対策の導入，教育及び周知の必要性が裏付けられている.

3．まとめ

本稿では，提案手法について，6 個の不正送金を狙う攻撃事例を基にケーススタディを実施し，その有効性を検証した．提案手法は，対策の検討を行うに当たって，議論の整理に役立つとともに，複数の対策主体における認識の共通化に資すると考える．今後の課題は，攻撃事例及び対策主体の拡充である.

参考文献

[1] 岡田 周平，森 滋男，後藤 厚宏. 不正送金対策向け金融サイバーキルチェーン. コンピュータセキュリティシンポジウム 2016 3E2-3

[2] “平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について”. https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf, (参照 2017-01-05).

[3] 佐野 宏明，田中 英彦. インターネットバンキングの不正送金対策. 情報処理学会第 77 回全国大会 4E-08