不正送金対策向け金融サイバーキルチェーン

岡田 周平[†1]　森 滋男[†1]　後藤 厚宏[†1]

概要：近年，インターネットバンキングにおいて，フィッシングやトロイの木馬等による預金者を標的とした金銭的被害が相次いでおり，不正送金の脅威が顕在化している．ひとつのセキュリティ対策ですべての不正送金を狙う攻撃を防御することはできず，多層なセキュリティ対策を講ずることが望ましい．各ステークホルダがどのような対策をすることで，どのような不正送金の攻撃を，どの段階で防御できるのか，最適な防御に向けた分析が期待される．そこで，本稿では，サイバーキルチェーンを応用して，不正送金対策における攻撃の分析を行う．その後，分析結果を踏まえ，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として，「金融サイバーキルチェーン」を提案する．本提案は，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．本稿では複数の対策を事例に提案を分析し，考察した．

キーワード：サイバーキルチェーン，不正送金

Financial Cyber Kill Chain for countermeasures of financial fraud

Shuhei Okada[†1]　Shigeo Mori[†1]　Atsuhiro Goto[†1]

Abstract: In recent years, monetary damage that targets depositors has happened one after another by phishing and banking trojan in Internet banking, threats of financial fraud become obvious. It's not possible to defend against all of financial fraud threats in one of the security countermeasures. It's desirable to take defense in depth. Each stakeholder takes countermeasures, what kind of financial fraud threats do we defense, and how can defense at any stage. An analysis toward optimum defense is expected. In this paper, by applying the Cyber Kill Chain, we carry out an attack analysis of the financial fraud countermeasures. And based on the results of the analysis, we propose an analysis framework called "Financial Cyber Kill Chain". This framework clarifies the effects and limitations of individual countermeasures against financial fraud threats. This proposal expresses the attack phase and countermeasures by a tabular form as a starting point the behavior of attackers. We analyze and consider the usefulness of our approach with several case studies.

Keywords: Cyber Kill Chain, Financial Fraud

1. はじめに

金融分野では，インターネットを利用した金融サービスが普及する一方で，近年，銀行，信用金庫，信用組合等の預金取扱金融機関（以下「金融機関」）が提供するインターネットバンキングにおいて，フィッシングやトロイの木馬（以下「金融マルウェア」）等による預金者を標的とした不正送金の脅威が顕在化している．

金融機関は，不正送金を狙う攻撃に対して，これまでも乱数表，ワンタイムパスワード（以下「OTP」），抗ウイルスソフト（以下「AV」）の無償提供等，様々なセキュリティ対策を講じているが，不正送金を狙う攻撃の手口は高度化，巧妙化しており，インターネットバンキングの個々のセキュリティ対策を迂回したり，新たな攻撃を仕掛けたりしてくる．

不正送金対策は，ひとつのセキュリティ対策ですべての攻撃を防御することはできず，金融機関，預金者，警察当局その他のステークホルダにおいて複数の対策を組み合わせ，多層によるセキュリティ対策を講ずることが望ましい．各ステークホルダがどのような対策をすることで，どのような不正送金の攻撃を，どの段階で防御できるのか，最適な防御に向けた分析及びステークホルダ間における認識の共通化の改善が期待される．

そこで，本稿では，APT を対象とするサイバーキルチェーンを応用して，不正送金対策における攻撃の分析を行う．その後，分析結果を踏まえ，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として，「金融サイバーキルチェーン」を提案する．

本提案は，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ことにより，各ステークホルダの対策が攻撃のどの部分を阻止し，どの部分が阻止できないか，最適な防御の実施に向けた分析を行い，ステークホルダ間における認識を共通化する．具体的には，攻撃分析表及びふたつの対策表から構成され，攻撃分析表は，定義された攻撃フェーズに基づき，攻撃パターンを具体的に記述する．対策表は，攻撃者の行動を起点として，攻撃フェーズ及び対策を，対策主体別や効果分類別に記述する．

本稿の構成は次のとおりである．2 章において不正送金を狙う攻撃と攻撃の分析の要件や期待について述べる．3

†1 情報セキュリティ大学院大学
Institute of Information Security

章ではサイバーキルチェーンを用いた不正送金を狙う攻撃の分析を行い，4 章において提案手法である「金融サイバーキルチェーン」について説明する．最後に 5 章で本稿をまとめ，今後の課題を述べる．

なお, 本稿では, 預金者を狙う不正送金を研究対象とし，金融機関の情報システムを直接狙うサイバー攻撃は対象外である．

2. 不正送金の特徴と攻撃の分析

2.1 不正送金を狙う攻撃

不正送金を狙う攻撃として，主にフィッシング，Man-in-the-Middle（以下「MitM」）攻撃及び Man-in-the-Browser（以下「MitB」）攻撃が知られている．

フィッシングとは，実在する組織を騙って，ユーザネーム，パスワード，アカウント ID, ATM の暗証番号といった認証情報を詐取する攻撃である[1].

MitM 攻撃とは，預金者とインターネットバンキングサイトの二者間に割り込んで，通信を盗聴したり，通信内容に介入したりする攻撃である[2].

MitB 攻撃について，鈴木ら[3]は，ID 盗取型 MitB 攻撃，取引偽造型 MitB 攻撃及び取引改ざん型 MitB 攻撃の三つの手口に大別している．ID 盗取型 MitB 攻撃とは，預金者のログイン時に，金融マルウェアがなりすまし等の不正取引に必要となる情報を盗取する攻撃である. 取引偽造型 MitB 攻撃とは，インターネットバンキングにログインする際に偽画面を表示して，取引に必要な認証情報まで入力させた後，預金者の取引指示の有無にかかわらず裏で不正な取引指図を勝手に行う攻撃である．取引改ざん型 MitB 攻撃とは，金融系マルウェアが取引内容（振込先，金額）を預金者の PC 内でリアルタイムに改ざんする攻撃である．

2.2 不正送金を狙う攻撃の特徴

不正送金を狙う攻撃の特徴について，まず攻撃手法について，主にフィッシング，MitM 攻撃，MitB 攻撃により，なりすまし，取引偽造又は取引改ざんが行われ，不正送金が実行されるという特徴がある[1][2][3].

二点目の特徴として，不正送金を狙う攻撃は，複数の攻撃フェーズを経て, 目的行動を達成するという特徴がある. 例えば，ID 盗取型 MitB 攻撃の場合，まず攻撃者は，金融機関や預金者の情報収集を行う．次に，金融マルウェアや送信用の電子メールを準備し, 預金者に送信する. その後，預金者 PC を金融マルウェアに感染させ, C&C（以下「C2」）サーバと通信を行いながら, 認証情報を盗取する. 最後に，不正送金指示を行い，現金化するという一連のフェーズを辿る．なお，C2 サーバまでの通信は，預金者と攻撃者間の通信である．インターネットバンキングサーバに対して通信が発生するのは，不正送金指示を行うフェーズ以降である．

三点目の特徴として，不正送金を狙う攻撃において，攻撃者はまず，不特定多数の預金者を標的にするが，当該 PC は金融機関の管理下にないということが挙げられる. 即ち，金融機関は，自身のセキュリティ対策のみ強化すれば良いというものではない．

2.3 不正送金対策における攻撃の分析の要件

不正送金を狙う攻撃の特徴を踏まえ，当該攻撃の分析の要件について述べる．まず，不正送金を狙う攻撃の手口は高度化, 巧妙化しており, インターネットバンキングの個々のセキュリティ対策を迂回したり，新たな攻撃を仕掛けたりする．例えば，OTP は，真の預金者になりすました攻撃者が不正送金指示を行う際，OTP がなければ送金できないという点でなりすましに対して有効である．一方で，Web ブラウザに預金者が意図した送金額を表示しながら，インターネットバンキングサーバには改ざんされた送金額を指定する取引改ざん型 MitB 攻撃等の攻撃に対して，OTP では限界がある．また，トランザクション署名は，取引改ざん型 MitB 攻撃等の攻撃に対して有効であるが，預金者が網羅的に導入することは困難である．このように，個々の不正送金対策の有効性は，攻撃手法毎に異なるため，対策毎の効果と限界を明らかにする分析が求められる．

二点目として，不正送金を狙う攻撃は，複数の攻撃フェーズがチェーンのように連なっており，一連の攻撃を処理することにより，目的行動を達成するため，フェーズ毎に攻撃を阻止するため，多層によるセキュリティ対策を講ずる必要がある．

三点目として，不正送金対策は，金融機関のほか，預金者，セキュリティベンダ，インターネットサービスプロバイダ（以下「ISP」），警察当局をはじめとする各ステークホルダにおいて，それぞれの管理下において実施可能な対策を講じることが求められる．

2.4 不正送金対策における攻撃の分析への期待

不正送金対策における攻撃の分析の要件を踏まえ，まず各ステークホルダがどのような対策をすることで，どのような不正送金を狙う攻撃を，どの段階で防御できるのかを明らかにすることが期待される．これにより，各ステークホルダの役割を考慮した最適な防御に向けた分析が改善すると考える．

また，最適な防御に向けた分析について，どの主体がどの対策について対処すれば良いのか，ステークホルダ間において認識を共通化するための表現を明らかにすることが期待される．

3. 不正送金対策における攻撃の分析

本章では，不正送金対策において，サイバーキルチェーンを用いた攻撃の分析を実施する．

3.1 サイバーキルチェーンとは

標的型攻撃（APT）に関する攻撃の分析手法として，サ

イバーキルチェーンが提唱されている[4]．サイバーキルチェーンは，APT の攻撃フェーズを 7 段階に分解し，定義している（表 1）．

攻撃者は，APT において，標的毎にカスタマイズした手口を使う一方で，侵入を経済的に行うため，ツールやインフラを使い回す．組織は，侵入への深い理解やインテリジェンスのツール，インフラの活用によって，攻撃キャンペーンのパターンや振舞い，TTPs（戦略，技術，手順）を検知・分析することにより，攻撃者がどのように攻撃するかということを把握し，後続の攻撃手法の変更を余儀なくさせる．APT の被害規模は，攻撃フェーズの進展に応じて拡大するため，組織は当該攻撃を早期に検知する必要がある（図 1）．

表 1　サイバーキルチェーンが定義する攻撃フェーズ[4]

No.	フェーズ	攻撃者の行動
1	偵察	攻撃目標を調査，識別，選択する．メールアドレスや社会的関係，特定技術の情報を得るため，会議議事録やメーリングリスト等，Web サイトを巡回する．
2	武器化	脆弱性を悪用する RAT（Remote Access Trojan）に配送可能なペイロードを組み込むものであり，典型的には自動化ツールを用いる．Adobe PDF や Microsoft Office のようなクライアントアプリケーションの悪用が増加傾向である．
3	デリバリ	標的の環境に武器を配送する．Lockheed Martin 社によれば，2004 年から 2010 年の間，メール添付，Web サイト及び USB メモリが悪用されている．
4	エクスプロイト	武器を被害ホストへ配送した後，脆弱性を悪用し攻撃コードを実行する．アプリケーション又は OS の脆弱性を突くほか，利用者自身や OS の自動実行機能を利用することもある．
5	インストール	RAT のインストールや被害システムのバックドアは，攻撃者に対して，継続的に被害環境に対する維持を確保する．
6	C2	侵害されたホストは C2 サーバとの外部通信を行う．APT マルウェアは特に，自動化された指示よりむしろ，手動の指示を必要とする．
7	目的の行動	これまでの 6 つのフェーズを処理した後，攻撃者は所期の目的行動を達成する．典型的には情報漏えいであり，データの完全性や可用性に対する侵害のほか，踏み台が目的であることもある．

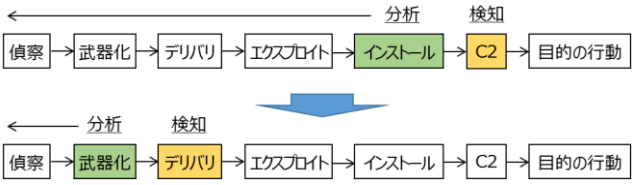

図 1　サイバーキルチェーンにおける検知のタイミング（[4]を基に筆者加工）

3.2　サイバーキルチェーンを用いた不正送金を狙う攻撃の分析

3.2.1 分析観点

不正送金対策における攻撃の分析の要件や期待を踏まえ，サイバーキルチェーンを用いた不正送金を狙う攻撃の分析を行う．分析観点を表 2 に示す．

表 2　分析観点

No.	観点
1	不正送金を狙う攻撃者の行動を，攻撃フェーズに分解し，定義ができるか．
2	不正送金を狙う攻撃の攻撃フェーズを基に，フィッシング，MitM 攻撃，MitB 攻撃をはじめとする攻撃パターンを具体的に記述できるか．
3	個々の対策を攻撃者の行動に紐付けできるか．
4	攻撃パターンが比較・分析できるか．
5	個々の対策を効果分類に紐付けできるか．

3.2.2 分析結果

サイバーキルチェーンを用いた不正送金を狙う攻撃の分析結果について，次に述べる．

観点 1：不正送金を狙う攻撃者の行動の定義

サイバーキルチェーンが行う攻撃フェーズの定義と同様に，不正送金を狙う攻撃者の行動を 8 つの攻撃フェーズに分解し，定義する（表 3）．

表 3　不正送金を狙う攻撃者の行動

No.	フェーズ	攻撃者の行動
1	偵察	攻撃目標を調査，識別し，選択する．攻撃目標は，不正送金を狙う攻撃の対象となる金融機関及び預金者である．
2	武器化	攻撃手法を選択し，偽インターネットバンキングサイトや金融マルウェア，配送する電子メールの準備を行う．主な攻撃パターンは，フィッシング，MitM 攻撃又は ID 盗取型 MitB 攻撃によるなりすましのほか，取引偽造や取引改ざんによる攻撃が想定される．
3	デリバリ	標的の環境に武器を配送する．配送方法は，ばら撒き型の電子メール及び Web 改ざんが想定される．
4	エクスプロイト	預金者は，配送された金融マルウェアを実行する．
5	インストール	預金者 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 を監視する．
6	C2	預金者 PC と C2 サーバの間で外部通信を行う．預金者は，正規又は偽インターネットバンキングサイトにアクセス，ログインし，認証情報の盗取，取引偽造又は取引改ざんを行い，これらの情報を C2 サーバに送信する．
7	不正送金指示	盗取した情報によるなりすまし，取引偽造又は取引改ざんにより，金融機関に対して不正送金指示を行う．金融機関は，送金指示に基づき，送金先へ送金を行う．
8	出金	送金先口座から現金化を行う．主な現金化手法は，出し子が現金出金，資金移動業者を介した国外送金，電子マネーへの換金を想定する[5]．

表 4　攻撃分析表

フェーズ	なりすまし型 ID 盗取型 MitB 攻撃		改ざん型 取引改ざん型 MitB 攻撃	
	攻撃者の行動	対策	攻撃者の行動	対策
偵察	①攻撃者は，金融機関や預金者を調査，識別，選択する等，情報収集		①同左	
武器化	②攻撃者は，預金者 PC を感染させる金融マルウェアや預金者に対して送信するメールを準備		②同左	
デリバリ	③攻撃者は預金者に対して，電子メールを送信		③同左	
エクスプロイト	④預金者は，配送された金融マルウェアを実行		④同左	
インストール	⑤預金者 PC は，金融マルウェアに感染 ⑥金融マルウェアは，預金者 PC の通信を継続的に監視		⑤同左 ⑥同左	
C2	⑦預金者 PC と C2 サーバの間で外部通信 ⑧預金者は，Web ブラウザを通じて正規のインターネットバンキングサイトへアクセス ⑨金融マルウェアは，アクセスを検知し，ログイン後，認証情報の入力を求める画面（偽画面）が表示されるような命令を追加する改ざんを行った上で，ブラウザに渡す ⑩預金者は，認証情報を入力 ⑪金融マルウェアは，預金者が入力した情報を盗取し，C2 サーバに送信	AV 預金者 PC に感染している金融マルウェアを駆除 C2 通信遮断 協力企業から提供された通信について遮断	⑦同左 ⑧同左 ⑨同左	AV 同左 C2 通信遮断 同左
不正送金指示	⑫攻撃者は，盗取した認証情報を利用し，正規のインターネットバンキングサイトになりすましてアクセス，ログインし，不正送金を指示 ⑬金融機関は，送金指示に基づき，送金先へ送金	OTP（HWT） 攻撃者は OTP を保有しておらず、送金指示できない	⑩預金者は，正規の画面において，取引内容を入力 ⑪金融マルウェアは，入力された取引内容を改ざんし，インターネットバンキングサーバに送信 ⑫インターネットバンキングサーバは，（改ざんされた）取引内容確認のために，受信した取引内容を預金者 PC に送信 ⑬金融マルウェアは，インターネットバンキングサーバから受信した取引内容を改ざんして，預金者がもともと入力した内容に戻してブラウザに渡す ⑭預金者は，ブラウザに表示された取引内容が意図したとおりの内容であることを確認し，「取引確定」ボタンを押す．「取引確定」がインターネットバンキングサーバに送信 ⑮金融機関は，送金指示に基づき，送金先へ送金	OTP（HWT） ブラウザに表示された取引内容が預金者の意図した内容になる一方で，インターネットバンキングサーバへ送信する内容が改ざんされる場合，預金者は OTP を入力してしまう
出金	⑭攻撃者は，振込先口座から出金		⑯同左	

サイバーキルチェーンの分析対象である APT と比較して，本攻撃特有の攻撃フェーズは，「不正送金指示フェーズ」及び「出金フェーズ」である．

「エクスプロイトフェーズ」及び「インストールフェーズ」において預金者 PC が金融マルウェアに感染し，「C2 フェーズ」及び「不正送金指示フェーズ」において認証情報の盗取，取引偽造又は取引改ざんによる不正送金指示が行われ，「出金フェーズ」において現金化が行われる．フェーズの進展に伴い，預金者の被害が拡大するため，より早い攻撃フェーズにおける対処が望ましいと考えられる．

観点 2：攻撃パターンの具体的記述

観点 1 において定義した不正送金を狙う攻撃の攻撃フェーズに基づき，攻撃者の行動をシナリオ化し，具体的に記述する．本稿では，MitB 攻撃のうち，ID 盗取型 MitB 攻撃及び取引改ざん型 MitB 攻撃を対象に分析する（表 4）．

攻撃パターンの記述内容は，表 4 のうち，「攻撃者の行動」の部分である．本表を活用することにより，攻撃者の行動を明らかにし，攻撃フェーズに着目した脅威を検出することが可能となる．

観点 3：攻撃者の行動と対策の紐付け

観点 2 において記述した攻撃パターンについて，不正送

表 5　対策表（効果分類別）

フェーズ	効果分類					
	検知 (Detect)	拒否 (Deny)	中断 (Disrupt)	減殺 (Degrade)	欺き (Deceive)	破壊 (Destroy)
偵察						
武器化						
デリバリ						
エクスプロイト						
インストール						
C2		C2 通信遮断	AV			
不正送金指示		OTP (HWT)				
出金						

金対策が攻撃者の行動のうち，どの部分で効果を発揮しているかを分析する（表 4）．

本稿では，個々の対策として，OTP（ハードウェアトークン方式）（以下「OTP（HWT 方式）」），AV 及び C2 通信遮断に関する対策を事例に分析する．

(1) OTP（HWT 方式）

OTP（HWT 方式）は，ハードウェアトークンを利用して，OTP を通知する一回限りで無効となる使い捨てのパスワードである．OTP（HWT 方式）は，ID 盗取型 MitB 攻撃のうち，不正送金指示フェーズにおいて，攻撃者が盗取した認証情報を利用し，真の預金者になりすまして不正送金を指示する際，OTP を求めることにより，当該送金指示を阻止する．他方，取引改ざん型 MitB 攻撃では，同フェーズにおいて，預金者はブラウザに表示された取引内容が預金者の意図した内容になる一方で，インターネットバンキングサーバへ送信する内容が改ざんされる場合，預金者が OTP を入力してしまうため，当該対策は有効ではなく，限界があると考えられる．

(2) AV

AV は，ID 盗取型 MitB 攻撃及び取引改ざん型 MitB 攻撃共に，C2 フェーズにおいて，預金者 PC に感染している金融マルウェアを駆除する．他方，預金者が AV を利用しない場合や振舞いで金融マルウェアが検知できない場合が想定される点で限界があると考えられる．

(3) C2 通信遮断

C2 通信遮断とは，ISP がセキュリティベンダをはじめとする協力企業からの提供リストを利用して，予め同意を得たインターネット利用者の端末が C2 サーバへアクセスしようとする場合，アクセスを遮断することでマルウェアによる被害を未然に防止するとともに，C2 サーバにアクセスする預金者に対して，注意喚起を行う取組である[6].

C2 通信遮断は，ID 盗取型 MitB 攻撃及び取引改ざん型 MitB 攻撃共に，C2 フェーズにおいて，預金者 PC と C2 サーバの間で外部通信を，協力企業から提供された情報に基づき遮断する．その一方で，提供されない通信は遮断されない点で限界があると考えられる．

観点 4：攻撃パターンの比較・分析

観点 2 及び 3 において記述した攻撃パターン及び対策の具体的な記述について，これらを並列に記述することにより，攻撃パターンを比較する分析が可能となる．

具体的には，表 4 において，ID 盗取型 MitB 攻撃と取引改ざん型 MitB 攻撃の「偵察フェーズ」から「インストールフェーズ」では，攻撃者の行動が共通化されている部分が確認できる．当該箇所では，対策も共通化できると考えられる．他方，「C2 フェーズ」及び「不正送金指示フェーズ」は，攻撃パターン毎に，攻撃者の行動が異なることが分かる．当該箇所では，攻撃の手口が異なるため，対策毎の効果と限界を明らかにする分析が必要であると考えられる．

観点 5：対策を効果分類に紐付け

個々の不正送金対策の効果は，表 4 を基に導出するが，これらの対策を効果分類に対応させる．サイバーキルチェーンにおいて，不正送金対策の効果分類は，検知，拒否，中断，減殺，欺き及び破壊が挙げられている（表 5）．

(1) OTP（HWT 方式）

OTP（HWT 方式）は，攻撃者が金融機関に対して，不正送金指示を行う際，OTP による認証ができない場合，当該通信を「拒否」する．

(2) AV

AV は，金融マルウェアが預金者 PC に感染している金融マルウェアの活動を「中断」する．

(3) C2 通信遮断

C2 通信遮断は，預金者 PC と C2 サーバの間で外部通信を行う際，当該通信を「拒否」する．

3.2.3 考察

サイバーキルチェーンを用いた不正送金対策における攻撃の分析は，攻撃者の行動を起点とした検討が可能であり，有用であると考えられる．

特に，フィッシング，MitM 攻撃及び MitB 攻撃をはじめとする複数の脅威パターンにおいて，共通の手口と独自の手口を区分する分析ができる点が有用であると考える．

一方で，個々の対策を対策実施主体に紐付けする分析は

行われておらず，各ステークホルダがどのような対策をすることで，どのような不正送金を狙う攻撃を，どの段階で防御できるのか，サイバーキルチェーンのみでは明らかにならない．不正送金対策では，ステークホルダが多岐に亘るため，これらの役割を考慮することにより，最適な防御に向けた分析が改善されると考える．

4. 金融サイバーキルチェーンの提案

不正送金対策について各ステークホルダの役割を考慮した最適な防御の実施に向け，サイバーキルチェーンを応用し，「金融サイバーキルチェーン」を提案する．

4.1 サイバーキルチェーンの金融系インシデントへの応用

不正送金対策の攻撃の分析では，ステークホルダが多岐に亘ることを踏まえ，サイバーキルチェーンによる分析に加え，各対策実施主体がどのような対策をすることで，どのような不正送金を狙う攻撃を，どの段階で防御できるのか，役割を考慮することにより，最適な防御に向けた分析が改善されると考える．

具体的には，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対策実施主体に紐付け，表形式により表現する（表 6）．

表 6　対策表（対策主体別）

フェーズ	対策主体		
	金融機関	預金者	…
…			
C2	AV の提供	AV の利用	
…			

また，サイバーキルチェーンを改善し，金融サイバーキルチェーンを活用することにより，「不正送金指示フェーズ」の水際対応や「出金フェーズ」における事後対応のみならず，「C2 フェーズ」以前の対応を含め，各ステークホルダの役割を考慮した最適な防御に向けた分析を行い，ステークホルダ間において各対策の利点と制約に関する認識の共通化ができると考える．

4.2 対策表（対策主体別）の分析

対策表（対策主体別）を用いた分析が可能か検証を実施する．なお，分析には，3.2 と同様に，個々の対策として，OTP（HWT 方式），AV 及び C2 通信遮断を対象とする（表 7）．

(1) OTP（HWT 方式）

OTP（HWT 方式）に関する対策者は，金融機関及び預金者である．金融機関が OTP をシステム整備するとともに，預金者に提供し，預金者は当該 OTP を利用する．

(2) AV

AV に関する対策者は，金融機関及び預金者である．金融機関が AV についてシステム整備するとともに，預金者に提供し，預金者は当該 AV を利用する．

(3) C2 通信遮断

C2 通信遮断に関する対策者は，ISP 及び協力企業である．協力企業は，本稿ではセキュリティベンダを想定する．セキュリティベンダが金融マルウェアを解析し，C2 通信先を把握する．セキュリティベンダは当該情報を ISP に提供する．

本対策表を活用することにより，個々の対策の実施主体が明らかになるとともに，いずれの攻撃フェーズにおける攻撃に対して対策が有効になるかが明確になり，金融機関，預金者をはじめとするステークホルダ間において各対策の利点と制約に関する認識の共通化ができると考える．

4.3 金融サイバーキルチェーンの全体像

(1) 概要

金融サイバーキルチェーンは，APT を対象とするサイバーキルチェーンを応用し，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ことにより，各ステークホルダの対策が攻撃のどの部分を阻止し，どの部分が阻止できないか，最適な防御の実施に向けた分析を行い，ステークホルダ間において認識を共通化する．本提案の概要を図 2 に示す．

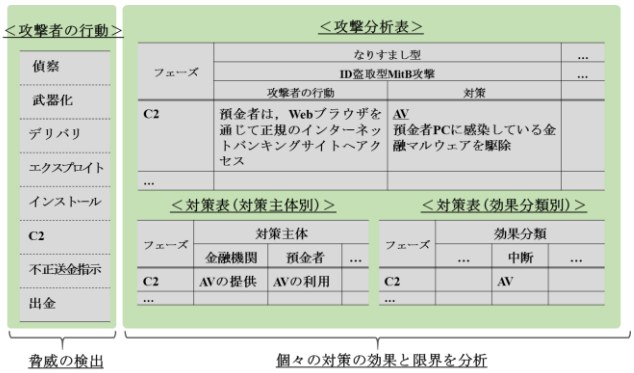

図 2　金融サイバーキルチェーンの概要

(2) 利用対象

本提案が想定する利用対象は，金融機関，ISP，セキュリティベンダ及び警察当局等，預金者を除く不正送金対策を講じるステークホルダである．

4.4 金融サイバーキルチェーンの構成

金融サイバーキルチェーンは，攻撃分析表，対策表（対策主体別）及び対策表（効果分類別）の三つの表から構成される．

攻撃分析表及び対策表（効果分類別）は，サイバーキルチェーンの考え方を活用する．攻撃分析表は，まず不正送

表 7　対策表（対策主体別）

フェーズ	対策主体					
	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
偵察						
武器化						
デリバリ						
エクスプロイト						
インストール						
C2	AV の提供	AV の利用		C2 通信遮断の実施	C2 通信遮断の提供	
不正送金指示	OTP (HWT)の提供	OTP (HWT)の利用				
出金						

金を狙う攻撃の攻撃フェーズに基づき，攻撃者の行動をシナリオ化する．その後，定義した攻撃フェーズを基に，フィッシング，MitM 攻撃，MitB 攻撃をはじめとする不正送金を狙う攻撃に関する攻撃パターンを具体的に記述する．攻撃分析表を活用することにより，例えば，「デリバリフェーズ」における標的の環境に武器を配送する部分は共通している等，複数の攻撃パターンにおいて，共通の手口と独自の手口を区分することができるなどの分析が可能になると考える．

対策表（効果分類別）は，攻撃者の行動を起点として，攻撃フェーズ及び対策を効果分類に紐付け，表形式により表現する．金融サイバーキルチェーンの効果分類についても，サイバーキルチェーンを引用し，検知，拒否，中断，減殺，欺き及び破壊を用いる．

対策表（対策主体別）は，本提案において新たに加えるものであり，4.1 で述べたとおり攻撃フェーズ及び対策を対策実施主体に紐付けるものである．

5. おわりに

本稿では，まず不正送金対策について，サイバーキルチェーンを活用した分析が有用であることを，複数の観点から検討した．次に，不正送金対策の攻撃の分析では，ステークホルダが多岐に亘るため，これらの役割を考慮することにより，最適な防御に向けた分析が改善されると考えられることを示した．その後，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として，金融サイバーキルチェーンを提案した．提案手法は，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ことにより，各ステークホルダの対策が攻撃のどの部分を阻止し，どの部分が阻止できないか，最適な防御の実施に向けた分析を行い，ステークホルダ間における認識を共通化するものである．金融サイバーキルチェーンの構成要素である攻撃分析表，対策表（対策主体別）及び対策表（効果分類別）を活用することにより，攻撃者の行動を基に脅威を検出し，各対策実施主体がどのような対策をすることで，どのような不正送金を狙う攻撃を，どの段階で阻止できるのか分析が可能になると考える．また，本稿では，金融サイバーキルチェーンにおいて新たに加えた対策表（対策主体別）について，OTP（HWT 方式），AV 及び C2 通信遮断に関する対策を事例に，各ステークホルダがどのような対策をすることで，どの段階で防御できるのか，分析を行った．

今後の課題は，攻撃パターン及び個々の対策に関する検証対象の拡充，有用性の更なる評価及び実際の活用に向けた検討を行う．

参考文献

[1] “フィッシング対策ガイドライン　2016 年度版”. https://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf,（参照 2016-08-02）

[2] “Man-in-the-Browser および Man-in-the-Middle 攻撃からオンライン顧客を保護”. http://www.ca.com/jp/~/media/ Files/ whitepapers/jpProtection_from_MITM_MITB_Attacks_White_Paper201104010.pdf,（参照 2016-08-02）

[3] 鈴木雅貴，中山靖司，古原和邦. インターネット・バンキングに対する Man-in-the-Browser 攻撃への対策「取引認証」の安全性評価．金融研究. 2013, vol. 32, no. 3 p. 51-76

[4] Eric Hutchins, Michael Cloppert, Rohan Amin：Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. 6th International Conference on Information Warfare and Security. 2011, p. 113-125

[5] “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 2016-08-02）

[6] “マルウェア被害未然防止活動について”. http://www.active.go.jp/active/damage_prevention.html,（参照 2016-08-02）