出典：サイバーレスキュー隊（J-CRAT）技術レポート2017（IPA 独立行政法人情報処理機構 セキュリティセンター

別紙：表 1.2-1 標的型攻撃の調査の全体像

フェーズ	調査目的	調査	調査対象	調査の観点	関連する調査目的 A	B	C	D	E	F	G
攻撃嫌疑	A. 攻撃メールかどうか	メール調査	PC	・送信元のFQDN/IPアドレスに攻撃インフラの可能性があるかどうか ・添付ファイルがマルウェア等の攻撃であるかどうか ・リンクが正規のものかどうか	○			△			
		不審ファイル調査	PC	・添付ファイルが不審な挙動をしないか ・外部通信が発生する場合、FQDN/IPアドレスに攻撃インフラの可能性があるかどうか	○			△			
感染嫌疑	B. 感染しているかどうか	PC永続化設定調査	PC	・不審な永続化設定がないか（初動調査）		○					
		PC実行痕跡調査	PC	・不審ファイルを実行したかどうか ・ブラウザ等のキャッシュにリンク先が記録されていないか ・不審な通信先への名前解決をおこなっていないか（初動調査）		○	△				
		PC感染頻出箇所調査	PC	・不審ファイルが配置されていないか（初動調査）		○					
		プロキシサーバ調査	SV	・不審ファイルを実行した結果、外部へ通信をおこなっていないか ・リンクをたどって、外部へ通信をおこなっていないか ・FQDN/IPアドレスに攻撃インフラの可能性があるか		○	△		△		
		Firewall調査	NW	・不審ファイルを実行した結果、外部へ通信をおこなっていないか ・リンクをたどって、外部へ通信をおこなっていないか ・FQDN/IPアドレスに攻撃インフラの可能性があるか		○	△		△		
被害の把握	被害の範囲を知りたい C.通信先 D.侵入元 E.被害の範囲 F.情報漏えい	メールサーバ調査	SV	・同時に他メールアドレスあてに受信していないか ・同送信元（サーバ、メールアドレス）から受信記録がないか				△	○		
		プロキシサーバ調査	SV	・同通信先への通信はいつからはじまっているか ・同通信先に組織内の別PCから通信が発生していないか		△	△		○		
		DNSサーバ調査	SV	・同FQDNのクエリがいつからはじまっているか ・同FQDNのクエリが組織内の別PCから発生していないか		△	△		○		
		Firewall調査	NW	・同通信先への通信はいつからはじまっているか ・同通信先に組織内の別PCから通信が発生していないか		△	△		○		
		同一セグメントPC調査	PC	・PC永続化設定・実行痕跡・感染頻出箇所調査をおこなう ・感染PCと同じネットワークアドレスのPCに不審なリモートデスクトップ接続や管理共有への接続などがおこなわれていないか					○		
		組織内PC/サーバ調査	PC SV	・PC永続化設定・実行痕跡・感染頻出箇所調査をおこなう ・感染PCが到達可能なネットワークアドレスのPCに、不審なリモートデスクトップ接続や管理共有への接続などがおこなわれていないか					○		
		ActiveDirecoryサーバ侵害調査	SV	・永続化・実行痕跡・不審ファイル調査をおこなう ・共有フォルダへのアクセス、また、不審なリモートデスクトップ接続や管理共有への接続などがおこなわれていないか ・感染PCからのアクセスについては特に、利用時間、頻度など分析をおこなう					○	△	
		ファイルサーバ侵害調査	SV	・永続化・実行痕跡・不審ファイル調査をおこなう ・共有フォルダへのアクセス、また、不審なリモートデスクトップ接続や管理共有への接続などがおこなわれていないか ・感染PCからのアクセスについては特に、利用時間、頻度など分析をおこなう					○	△	
		初期感染の特定	PC SV NW	・組織内感染がどこからはじまったかを特定する ・メールによる攻撃が疑われる場合は、メールサーバ調査、不審メール調査など ・外部公開サーバからの侵入が疑われる場合は、外部公開サーバ調査、Firewall調査など				○	△		
		感染PC/サーバ詳細調査	PC SV	・状況に応じて感染PCフォレンジックと並行、またはどちらかを実施する ・イベントログ、不審ファイルの各種情報を調査し、感染日、感染方法、感染後の挙動を調査する				△	○	△	
		感染PC/サーバフォレンジック	PC SV	・状況に応じて感染PC詳細調査と並行、またはどちらかを実施する ・イベントログ、不審ファイル、ファイルシステム、レジストリ等の各種情報を調査し、感染日、感染方法、感染後の挙動を調査する				△	○	△	
対策の有効性	G.実施した対策が有効なことを知りたい	プロキシサーバ調査	SV	・同通信先への通信が発生していないか ・同通信先に組織内の別PCから通信が発生していないか					△		○
		DNSサーバ調査	SV	・同FQDNのクエリが発生していないか ・同FQDNのクエリが組織内の別PCから発生していないか					△		○
		Firewall調査	NW	・同通信先への通信が発生していないか ・同通信先に組織内の別PCから通信が発生していないか					△		○

○：直接的な効果　△：間接的な効果