サイバー攻撃（標的型攻撃）対策
防御モデルの解説

付録2 システムログ一覧（IOC）

攻撃経路	1. ドライブバイダウンロード

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避した外部への送信 非信頼ドメイン経由	検知回避した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	ファイアウォール（FW）	—	日時	○	－	○	○				○					○		○				○			○					○		○	○	○
				ファイアウォールホスト名	○	－	－	－																											
				ファイアウォールルール名及び番号	○	－	－	－																											
				インバウンドインタフェース	○	－	－	－																											
				アウトバウンドインタフェース	○	－	－	－																											
				MACアドレス	○	－	－	－																											
				パケットサイズ	○	転送バイト数	○	○				○					○		○				○			○					○		○	○	○
				IPパケット優先度（TOS,PREC）	○	－	－	－																											
				IPパケット生存期間（TTL）	○	－	－	－																											
				IPフラグメントパケット識別子（ID）	○	－	－	－																											
				IPフラグメンテーション情報（DFビット）	○	－	－	－																											
				ソースIPアドレス	○	接続元IPアドレス	○	○				○					○		○				○			○					○		○	○	○
				ソースポート番号	○	接続元ポート番号	○	○				○					○		○				○			○					○		○	○	○
				宛先IPアドレス	○	接続先IPアドレス	○	○				○					○		○				○			○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○				○					○		○				○			○					○		○	○	○
				プロトコル	○	－	－	－																											
				TCPウインドウサイズ（WINDOW）	○	－	－	－																											
				TCPフラグ	○	－	－	－																											
		ネットワーク型IPS/IDS	—	日時	○	－	○	○				○					○		○				○			○					○		○	○	○
				送信元アドレス	○	－	○	○				○					○		○				○			○					○		○	○	○
				送信元ポート番号	○	－	○	○				○					○		○				○			○					○		○	○	○
				宛先アドレス	○	－	○	○				○					○		○				○			○					○		○	○	○
				宛先ポート番号	○	－	○	○				○					○		○				○			○					○		○	○	○
				同一セッションの送受信バイト数	○	－	○	○				○					○		○				○			○					○		○	○	○
				同一セッションの送受信パケット数	○	－	○	○				○					○		○				○			○					○		○	○	○
				プロトコル	○	－	○	○				○					○		○				○			○					○		○	○	○
				セッション継続時間	○	－	○	○				○					○		○				○			○					○		○	○	○
				セッションのユーザ名	○	－	○	○				○					○		○				○			○					○		○	○	○
				URL	○	－	○	○				○					○		○				○			○					○		○	○	○
				ファイル名	○	－	○	○				○					○		○				○			○					○		○	○	○
				脅威情報	○	－	○	○				○					○		○				○			○					○		○	○	○
		Webサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				クライアントの識別子	○	－	－	－																											
				認証されたユーザー名	○	ログインユーザ名	－	○																									○	○	○
				日時	○	－	－	○																									○	○	○
				リクエストの最初の行の値	○	接続先URL	－	○																									○	○	○
				最後のレスポンスのステータス	○	ステータスコード	－	○																									○	○	○
				送信されたバイト数（ヘッダーは含まず）	○	転送バイト数	－	○																									○	○	○
				リクエストに含まれるRefererの値	○	リファラ	－	○																									○	○	○
				リクエストに含まれるUser-Agentの値（ブラウザ情報）	○	ユーザエージェント	－	○																									○	○	○
			エラーログ	日時	○	－	－	○																									○	○	○
				エラーの重要度	○	－	－	－																											
				アクセスしたクライアントのIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				メッセージ	○	－	－	－																											
			SSLログ	日時		－	－	－																											
				リモートホスト名		－	－	－																											
				SSLプロトコルバージョン		－	－	－																											
				SSL暗号		－	－	－																											
				リクエストの最初の行の値		－	－	－																											
				送信されたバイト数(ヘッダーは含まず)		－	－	－																											
		APサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				認証されたユーザー名	○	ログインユーザ名	－	○																									○	○	○
				日時	○	－	－	○																									○	○	○
				メソッドとURL	○	接続先URL	－	○																									○	○	○
				HTTPステータスコード	○	ステータスコード	－	○																									○	○	○
				レスポンスサイズ	○	－	－	－																											
			APログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
			ホストログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
		DBサーバ	—	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
		プロキシサーバ	アクセスログ	UTCの時間	○	日時	○	○				○					○		○							○					○				
				継続時間	○	セッション継続時間	○	○				○					○		○							○					○				
				クライアントのIPアドレス	○	接続元IPアドレス	○	○				○					○		○							○					○				
				リザルトコード（結果コード）	○	ステータスコード	○	○				○					○		○							○					○				
				転送バイト数	○	転送バイト数	○	○				○					○		○							○					○				
				リクエストメソッド	○	リクエストメソッド	○	○				○					○		○							○					○				
				URL	○	接続先URL	○	○				○					○		○							○					○				

攻撃経路	1. ドライブバイダウンロード

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	プロキスサーバ	アクセスログ	階層コード	○	接続先IPアドレス	○	○				○					○		○							○					○				
				HTTPヘッダにリプライされてきたオブジェクトのコンテンツタイプ	○	ファイル形式	○	○				○					○		○							○					○				
				User-Agent		ユーザエージェント	○	○				○					○		○							○					○				
			動作ログ（エラーログ・デバッグログ・キャッシュ）	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
			デバッグログ	日時	○	－	－	－																											
				メッセージ（エラーやデバックメッセージ）	○	－	－	－																											
		DNSサーバ	－	日時		－	○	○				○					○		○							○		○			○				
				ログカテゴリ		－	－	－																											
				クライアントのIPアドレスとポート番号		接続元IPアドレス	○	○				○					○		○							○		○			○				
				ファシリティ（ログの分類）		－	－	－																											
				ゾーン情報		リクエストドメイン名	○	○				○					○		○							○		○			○				
						DNSリクエストレコードタイプ	○	○				○					○		○							○		○			○				
		メールサーバ	－	日時	○	－	－	○																○	○						○				
				サーバホスト名	○	－	－	－																											
				プロセスの情報（プロセスの所有者とプロセスID）	○	－	－	－																											
				メッセージID（Sendmailによって送信されたメッセージに割り当てられたID）	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	－	○																○	○						○				
				メッセージサイズ	○	転送バイト数	－	○																○	○						○				
				メッセージ優先度	○	－	－	－																											
				メッセージ受信者数	○	メッセージ受信者数	－	○																○	○						○				
				メッセージ識別番号	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				サーバデーモン名	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	－	○																○	○						○				
				ステータス	○	－	－	－																											
				添付ファイル名		添付ファイル名	－	○																○	○						○				
	内部セグメント	スイッチ/ルータ	－	日時		－	○	○				○					○		○			○	○	○	○	○		○			○				
				送信元アドレス	○	接続元IPアドレス	○	○				○					○		○			○	○	○	○	○		○			○				
				送信元ポート番号	○	接続元ポート番号	○	○				○					○		○			○	○	○	○	○		○			○				
				宛先アドレス	○	接続先IPアドレス	○	○				○					○		○			○	○	○	○	○		○			○				
				宛先ポート番号	○	接続先ポート番号	○	○				○					○		○			○	○	○	○	○		○			○				
				同一フローの送受信バイト数		転送バイト数	○	○				○					○		○			○	○	○	○	○		○			○				
				同一フローの送受信パケット数		転送バイト数	○	○				○					○		○			○	○	○	○	○		○			○				
		ドメインコントローラー	－	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	○														○	○	○	○										
				イベントID	○	エラーコード	－	○														○	○	○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	－	○														○	○	○	○										
				ユーザー	○	アカウント名	－	○														○	○	○	○										
				コンピュータ	○	ワークステーション名	－	○														○	○	○	○										
				オペコード	○	－	－	－																											
		DHCPサーバ	－	日時		－	－	－																											
				ホスト名またはIPアドレス		－	－	－																											
				MACアドレス		－	－	－																											
				状態		－	－	－																											
		DNSサーバ（内部DNS）	－	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	－																											
				イベントID	○	－	－	－																											
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	－	－	－																											
				ユーザー	○	－	－	－																											
				コンピュータ	○	－	－	－																											
				オペコード	○	－	－	－																											

攻撃経路	1. ドライブバイダウンロード

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	ファイルサーバ	ー	ログの名前	○	–	–	–																										
				ソース	○	–	–	–																										
				日時	○	–	–	○															○	○										
				イベントID	○	エラーコード	–	○															○	○										
				タスクのカテゴリ	○	–	–	–																										
				レベル	○	–	–	–																										
				キーワード	○	イベント名	–	○															○	○										
				ユーザー	○	アカウント名	–	○															○	○										
				コンピュータ	○	ワークステーション名	–	○															○	○										
				オペコード	○	–	–	–																										
		エンドポイント(Windows)	イベントログ	ログの名前	○	–	–	–																										
				ソース	○	–	–	–																										
				日時	○	–	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○				
				イベントID	○	エラーコード	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○				
				タスクのカテゴリ	○	–	–	–																										
				レベル	○	–	–	–																										
				キーワード	○	イベント名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○				
				ユーザー	○	アカウント名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○				
				コンピュータ	○	ワークステーション名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○				
				オペコード	○	–	–	–																										
			プリフェッチ	日時	○	–	○	○			○					○					○	○					○	○		○				
				ファイル名	○	ファイル名	○	○			○					○					○	○					○	○		○				
			レジストリ	自動起動のファイル名		ファイル名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				接続したUSBメモリ等の情報		接続デバイス名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			スクリーンセーバー	起動するスクリーンセーバー		–	–	–																										
			タスクスケジューラ	ログの名前	○	–	–	–																										
				ソース	○	–	–	–																										
				日時	○	–	○	○									○	○																		
				イベントID	○	エラーコード	○	○									○	○																		
				タスクのカテゴリ	○	–	–	–																										
				レベル	○	–	–	–																										
				キーワード	○	イベント名	○	○									○	○																		
				ユーザー	○	アカウント名	○	○									○	○																		
				コンピュータ	○	ワークステーション名	○	○									○	○																		
				オペコード	○	–	–	–																										
			ファイルの履歴	以前のバージョン情報		–	–	–																										
			プロセスログ	日時		–	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		–	–	–																										
				タイプ		–	–	–																										
				ファイル名		プロセス名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
		エンドポイント(Linux)	メッセージログ	日時	○	–	–	–																										
				ログを出力したホスト名	○	–	–	–																										
				メッセージの出力元	○	–	–	–																										
				メッセージ	○	–	–	–																										
			cronログ	日時	○	–	–	–																										
				ログを出力したホスト名	○	–	–	–																										
				メッセージの出力元	○	–	–	–																										
				メッセージ	○	–	–	–																										
			カーネルログ	日時	○	–	–	–																										
				ログを出力したホスト名	○	ワークステーション名	–	–																										
				メッセージの出力元	○	–	–	–																										
				メッセージ	○	接続デバイス名	–	–																										
			セキュリティログ	日時	○	–	–	○														○									○	○	○
				ログを出力したホスト名	○	–	–	–																										
				メッセージの出力元	○	–	–	–																										
				メッセージ	○	接続元IPアドレス	–	○														○									○	○	○
						ログインユーザ名	–	○														○									○	○	○
						認証成否結果	–	○														○									○	○	○
		エンドポイント(OS)	システムコールログ ファイル操作ログ	日時		–	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		–	–	–																										
				プロセス名		プロセス名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				ファイルパス		ファイルパス	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ プロセス操作ログ	日時		–	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				親プロセスID		–	–	–																										
				プロセスID		–	–	–																										
				プロセス名		プロセス名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				コマンドライン		ファイルパス	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ レジストリ操作ログ	日時		–	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		–	–	–																										
				キー		レジストリキー	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				値		レジストリ値	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				データ		–	–	–																										
			システムコールログ API操作ログ	日時		–	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		–	–	–																										
				API名		API名	○	○			○					○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				APIの引数		–	–	–																										
				APIの戻り値		–	–	–																										

攻撃経路	1. ドライブバイダウンロード

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																															
									攻撃侵入フェーズ検知ログカテゴリ											拡散フェーズ検知ログカテゴリ														目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み								③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行												
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織にさない人間ち人が持ち込む機）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	エンドポイント（ブラウザ）	_	日時	○	-	○	○				○																											
				URL	○	接続先URL	○	○				○																											
		エンドポイント（AntiVirus）	_	スキャン日時	○	-	○	○				○						○								○	○											
				プロセスID	○	-	○	○				○						○								○	○											
				プロセス名	○	-	○	○				○						○								○	○											
				スキャン結果	○	-	○	○				○						○								○	○											

攻撃経路	1. ドライブバイダウンロード

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	L7FW (NGFW,APFW)	―	日時	○	-	○	○				○					○		○							○					○		○	○	○
				送信元アドレス	○	接続元IPアドレス	○	○				○					○		○							○					○		○	○	○
				送信元ポート番号	○	接続元ポート番号	○	○				○					○		○							○					○		○	○	○
				宛先アドレス	○	接続先IPアドレス	○	○				○					○		○							○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○				○					○		○							○					○		○	○	○
				同一セッションの送受信バイト数	○	転送バイト数	○	○				○					○		○							○					○		○	○	○
				同一セッションの送受信パケット数	○	転送バイト数	○	○				○					○		○							○					○		○	○	○
				プロトコル	○	通信アプリケーション名	○	○				○					○		○							○					○		○	○	○
				セッション継続時間	○	セッション継続時間	○	○				○					○		○							○					○		○	○	○
				セッションのユーザ名	○	アカウント名	○	○				○					○		○							○					○		○	○	○
				URL	○	接続先URL	○	○				○					○		○							○					○		○	○	○
				ファイル名	○	ファイル名	○	○				○					○		○							○					○		○	○	○
				脅威情報	○	-	-	-																											
		DLP (Data Loss Prevention)		日時	○	-	-	○																							○				
				送信元アドレス	○	接続元IPアドレス	-	○																							○				
				送信元ポート番号	○	接続元ポート番号	-	○																							○				
				宛先アドレス	○	接続先IPアドレス	-	○																							○				
				宛先ポート番号	○	接続先ポート番号	-	○																							○				
				プロトコル		通信アプリケーション名	-	○																							○				
				URL		接続先URL	-	○																							○				
				検知キーワード	○	検知キーワード	-	○																							○				
				検知ファイル名	○	ファイル名	-	○																							○				
		Mailゲートウェイ		日時	○	-	-	○																○	○										
				サーバホスト名	○	-	-	-																											
				メッセージID	○	-	-	-																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	-	○																○	○										
				メッセージサイズ	○	-	-	-																											
				メッセージ受信者数	○	-	-	-																											
				プロトコル情報	○	-	-	-																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	-	○																○	○										
				ステータス		-	-	-																											
				件名	○	件名	-	○																○	○										
				検知名	○	-	-	-																											
				検知ファイル名	○	-	-	-																											
				検知URL	○	-	-	-																											
		WAF		日時	○	-	-	○																									○	○	○
				ログID	○	-	-	-																											
				送信元アドレス	○	接続元IPアドレス	-	○																									○	○	○
				送信元ポート番号	○	接続元ポート番号	-	○																									○	○	○
				宛先アドレス	○	接続先IPアドレス	-	○																									○	○	○
				宛先ポート番号	○	接続先ポート番号	-	○																									○	○	○
				検知タイプ	○	-	-	-																											
				優先度	○	-	-	-																											
				アラートメッセージID	○	-	-	-																											
				アラートメッセージIDに紐づく検知項目（URL含む）	○	-	-	-																											
		サンドボックス		日時	○	-	○	○				○					○																		
				ログID	○	-	-	-																											
				送信元アドレス	○	接続元IPアドレス	○	○				○					○																		
				送信元ポート番号	○	接続元ポート番号	○	○				○					○																		
				宛先アドレス	○	接続先IPアドレス	○	○				○					○																		
				宛先ポート番号	○	接続先ポート番号	○	○				○					○																		
				プロトコル	○	-	-	-																											
				URL	○	接続先URL	○	○				○					○																		
				ファイル名	○	ファイル名	○	○				○					○																		
				ファイルタイプ	○	ファイル形式	○	○				○					○																		
				ファイルサイズ	○	ファイルサイズ	○	○				○					○																		
				ファイルハッシュ値	○	ファイルハッシュ値	○	○				○					○																		
				悪性判定結果	○	-	-	-																											
				マルウェアのファイル操作ログ	○	-	-	-																											
				マルウェアのプロセス操作ログ	○	-	-	-																											
				マルウェアのレジストリ操作ログ	○	-	-	-																											
				マルウェアのAPI呼出し	○	-	-	-																											
				マルウェアの通信先アドレス/ポート番号	○	-	-	-																											
		改ざん検知		日時	○	-	-	○																○	○										
				ログID	○	-	-	-																											
				改ざん内容(ファイルサイズ変化：旧、新)	○	ファイルサイズ変化	-	○																○	○										
				検知ルール名(追加/削除/編集)	○	イベント名	-	○																○	○										
				検知ファイル名	○	ファイル名	-	○																○	○										
				ユーザ名（検知した操作を行ったOSのアカウント名）	○	アカウント名	-	○																○	○										

攻撃経路	1. ドライブバイダウンロード

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	ホスト型IPS/IDS		日時	○	－	○	○				○					○		○					○	○	○		○			○		○	○	○
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	○	○				○					○		○					○	○	○		○			○		○	○	○
				ホスト名	○	－	－	－																											
				検知ルール	○	－	○	○				○					○		○					○	○	○		○			○		○	○	○
				検知したファイル操作	○	－	○	○				○					○		○					○	○	○		○			○		○	○	○
				検知したプロセス操作	○	－	○	○				○					○		○					○	○	○		○			○		○	○	○
				検知したレジストリ操作	○	－	○	○				○					○		○					○	○	○		○			○		○	○	○
				検知したAPI呼出し	○	－	○	○				○					○		○					○	○	○		○			○		○	○	○
	内部セグメント			日時	○	－	－	○																○	○										
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	－	○																○	○										
				ホスト名	○	－	－	－																											
				検知ルール	○	－	－	○																○	○										
				検知したファイル操作	○	－	－	○																○	○										
				検知したプロセス操作	○	－	－	○																○	○										
				検知したレジストリ操作	○	－	－	○																○	○										
				検知したAPI呼出し	○	－	－	○																○	○										

攻撃経路	2. 標的組織の公開サービス・ホスト

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	ファイアウォール(FW)	—	日時	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				ファイアウォールホスト名	○	－	－	－																											
				ファイアウォールルール名及び番号	○	－	－	－																											
				インバウンドインタフェース	○	－	－	－																											
				アウトバウンドインタフェース	○	－	－	－																											
				MACアドレス	○	－	－	－																											
				パケットサイズ	○	転送バイト数	○	○		○					○		○		○				○			○					○		○	○	○
				IPパケット優先度（TOS,PREC）	○	－	－	－																											
				IPパケット生存期間（TTL）	○	－	－	－																											
				IPフラグメントパケット識別子（ID）	○	－	－	－																											
				IPフラグメンテーション情報（DFビット）	○	－	－	－																											
				ソースIPアドレス	○	接続元IPアドレス	○	○		○					○		○		○				○			○					○		○	○	○
				ソースポート番号	○	接続元ポート番号	○	○		○					○		○		○				○			○					○		○	○	○
				宛先IPアドレス	○	接続先IPアドレス	○	○		○					○		○		○				○			○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○		○					○		○		○				○			○					○		○	○	○
				プロトコル	○	－	－	－																											
				TCPウインドウサイズ（WINDOW）	○	－	－	－																											
				TCPフラグ	○	－	－	－																											
		ネットワーク型IPS/IDS	—	日時	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				送信元アドレス	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				送信元ポート番号	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				宛先アドレス	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				宛先ポート番号	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				同一セッションの送受信バイト数	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				同一セッションの送受信パケット数	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				プロトコル	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				セッション継続時間	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				セッションのユーザ名	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				URL	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				ファイル名	○	－	○	○		○					○		○		○				○			○					○		○	○	○
				脅威情報	○	－	○	○		○					○		○		○				○			○					○		○	○	○
		Webサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	○	○							○																		○	○	○
				クライアントの識別子	○	－	－	－																											
				認証されたユーザー名	○	ログインユーザ名	○	○							○																		○	○	○
				日時	○	－	○	○							○																		○	○	○
				リクエストの最初の行の値	○	接続先URL	○	○							○																		○	○	○
				最後のレスポンスのステータス	○	ステータスコード	○	○							○																		○	○	○
				送信されたバイト数（ヘッダーは含まず）	○	転送バイト数	○	○							○																		○	○	○
				リクエストに含まれるRefererの値	○	リファラ	○	○							○																		○	○	○
				リクエストに含まれるUser-Agentの値（ブラウザ情報）	○	ユーザエージェント	○	○							○																		○	○	○
			エラーログ	日時	○	－	○	○							○																		○	○	○
				エラーの重要度	○	－	－	－																											
				アクセスしたクライアントのIPアドレス	○	接続元IPアドレス	○	○							○																		○	○	○
				メッセージ	○	－	－	－																											
			SSLログ	日時		－	－	－																											
				リモートホスト名		－	－	－																											
				SSLプロトコルバージョン		－	－	－																											
				SSL暗号		－	－	－																											
				リクエストの最初の行の値		－	－	－																											
				送信されたバイト数(ヘッダーは含まず)		－	－	－																											
		APサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	○	○							○																		○	○	○
				認証されたユーザー名	○	ログインユーザ名	○	○							○																		○	○	○
				日時	○	－	○	○							○																		○	○	○
				メソッドとURL	○	接続先URL	○	○							○																		○	○	○
				HTTPステータスコード	○	ステータスコード	○	○							○																		○	○	○
				レスポンスサイズ	○	－	－	－																											
			APログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
			ホストログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
		DBサーバ	—	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
		プロキシサーバ	アクセスログ	UTCの時間	○	日時	○	○									○		○							○					○				
				継続時間	○	セッション継続時間	○	○									○		○							○					○				
				クライアントのIPアドレス	○	接続元IPアドレス	○	○									○		○							○					○				
				リザルトコード（結果コード）	○	ステータスコード	○	○									○		○							○					○				
				転送バイト数	○	転送バイト数	○	○									○		○							○					○				
				リクエストメソッド	○	リクエストメソッド	○	○									○		○							○					○				
				URL	○	接続先URL	○	○									○		○							○					○				

攻撃経路	2. 標的組織の公開サービス・ホスト

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ											拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	プロキシサーバ	アクセスログ	階層コード	○	接続先IPアドレス	○	○									○		○							○					○				
				HTTPヘッダにリプライされてきたオブジェクトのコンテンツタイプ	○	ファイル形式	○	○									○		○							○					○				
				User-Agent		ユーザエージェント	○	○									○		○							○					○				
			動作ログ（エラーログ・デバッグログ・キャッシュ）	日時	○	–	–	–																											
				メッセージ	○	–	–	–																											
			デバッグログ	日時	○	–	–	–																											
				メッセージ（エラーやデバックメッセージ）	○	–	–	–																											
		DNSサーバ	–	日時		–	○	○									○		○							○		○			○				
				ログカテゴリ		–	–	–																											
				クライアントのIPアドレスとポート番号		接続元IPアドレス	○	○									○		○							○		○			○				
				ファシリティ（ログの分類）		–	–	–																											
				ゾーン情報		リクエストドメイン名	○	○									○		○							○		○			○				
						DNSリクエストレコードタイプ	○	○									○		○							○		○			○				
		メールサーバ	–	日時	○	–	○	○		○														○	○						○				
				サーバホスト名	○	–	–	–																											
				プロセスの情報（プロセスの所有者とプロセスID）	○	–	–	–																											
				メッセージID（Sendmailによって送信されたメッセージに割り当てられたID）	○	–	–	–																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	○	○		○														○	○						○				
				メッセージサイズ	○	転送バイト数	○	○		○														○	○						○				
				メッセージ優先度	○	–	–	–																											
				メッセージ受信者数	○	メッセージ受信者数	○	○		○														○	○						○				
				メッセージ識別番号	○	–	–	–																											
				プロトコル情報	○	–	–	–																											
				サーバデーモン名	○	–	–	–																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	○	○		○														○	○						○				
				ステータス	○	–	–	–																											
				添付ファイル名		添付ファイル名	○	○		○														○	○						○				
	内部セグメント	スイッチ/ルータ	–	日時		–	○	○									○		○			○	○	○	○	○		○			○				
				送信元アドレス	○	接続元IPアドレス	○	○									○		○			○	○	○	○	○		○			○				
				送信元ポート番号	○	接続元ポート番号	○	○									○		○			○	○	○	○	○		○			○				
				宛先アドレス	○	接続先IPアドレス	○	○									○		○			○	○	○	○	○		○			○				
				宛先ポート番号	○	接続先ポート番号	○	○									○		○			○	○	○	○	○		○			○				
				同一フローの送受信バイト数		転送バイト数	○	○									○		○			○	○	○	○	○		○			○				
				同一フローの送受信パケット数		転送バイト数	○	○									○		○			○	○	○	○	○		○			○				
		ドメインコントローラー	–	ログの名前	○	–	–	–																											
				ソース	○	–	–	–																											
				日時	○	–	–	○														○	○	○	○										
				イベントID	○	エラーコード	–	○														○	○	○	○										
				タスクのカテゴリ	○	–	–	–																											
				レベル	○	–	–	–																											
				キーワード	○	イベント名	–	○														○	○	○	○										
				ユーザー	○	アカウント名	–	○														○	○	○	○										
				コンピュータ	○	ワークステーション名	–	○														○	○	○	○										
				オペコード	○	–	–	–																											
		DHCPサーバ	–	日時		–	–	–																											
				ホスト名またはIPアドレス		–	–	–																											
				MACアドレス		–	–	–																											
				状態		–	–	–																											
		DNSサーバ（内部DNS）	–	ログの名前	○	–	–	–																											
				ソース	○	–	–	–																											
				日時	○	–	–	–																											
				イベントID	○	–	–	–																											
				タスクのカテゴリ	○	–	–	–																											
				レベル	○	–	–	–																											
				キーワード	○	–	–	–																											
				ユーザー	○	–	–	–																											
				コンピュータ	○	–	–	–																											
				オペコード	○	–	–	–																											

攻撃経路	2. 標的組織の公開サービス・ホスト

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ												目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	ファイルサーバ	－	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	○																○	○										
				イベントID	○	エラーコード	－	○																○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	－	○																○	○										
				ユーザー	○	アカウント名	－	○																○	○										
				コンピュータ	○	ワークステーション名	－	○																○	○										
				オペコード	○	－	－	－																											
		エンドポイント(Windows)	イベントログ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○									○	○	○		○	○	○	○	○	○		○	○		○				
				イベントID	○	エラーコード	○	○									○	○	○		○	○	○	○	○	○		○	○		○				
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○									○	○	○		○	○	○	○	○	○		○	○		○				
				ユーザー	○	アカウント名	○	○									○	○	○		○	○	○	○	○	○		○	○		○				
				コンピュータ	○	ワークステーション名	○	○									○	○	○		○	○	○	○	○	○		○	○		○				
				オペコード	○	－	－	－																											
			プリフェッチ	日時	○	－	○	○		○							○					○	○					○	○		○				
				ファイル名	○	ファイル名	○	○		○							○					○	○					○	○		○				
			レジストリ	自動起動のファイル名		ファイル名	○	○							○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				接続したUSBメモリ等の情報		接続デバイス名	○	○							○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			スクリーンセーバー	起動するスクリーンセーバー		－	－	－																											
			タスクスケジューラ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○									○	○																	
				イベントID	○	エラーコード	○	○									○	○																	
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○									○	○																	
				ユーザー	○	アカウント名	○	○									○	○																	
				コンピュータ	○	ワークステーション名	○	○									○	○																	
				オペコード	○	－	－	－																											
			ファイルの履歴	以前のバージョン情報		－	－	－																											
			プロセスログ	日時		－	○	○							○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				タイプ		－	－	－																											
				ファイル名		プロセス名	○	○							○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
		エンドポイント(Linux)	メッセージログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			cronログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			カーネルログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	ワークステーション名	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続デバイス名	－	－																											
			セキュリティログ	日時	○	－	○	○							○								○										○	○	○
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続元IPアドレス	○	○							○								○										○	○	○
						ログインユーザ名	○	○							○								○										○	○	○
						認証成否結果	○	○							○								○										○	○	○
		エンドポイント(OS)	システムコールログ / ファイル操作ログ	日時		－	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				ファイルパス		ファイルパス	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ / プロセス操作ログ	日時		－	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				親プロセスID		－	－	－																											
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				コマンドライン		ファイルパス	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ / レジストリ操作ログ	日時		－	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				キー		レジストリキー	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				値		レジストリ値	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				データ		－	－	－																											
			システムコールログ / API操作ログ	日時		－	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				API名		API名	○	○		○					○		○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				APIの引数		－	－	－																											
				APIの戻り値		－	－	－																											

攻撃経路	2. 標的組織の公開サービス・ホスト

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	エンドポイント（ブラウザ）	–	日時	○	–	–	–																											
				URL	○	接続先URL	–	–																											
		エンドポイント（AntiVirus）	–	スキャン日時	○	–	○	○		○					○		○							○	○										
				プロセスID	○	–	○	○		○					○		○							○	○										
				プロセス名	○	–	○	○		○					○		○							○	○										
				スキャン結果	○	–	○	○		○					○		○							○	○										

攻撃経路	2. 標的組織の公開サービス・ホスト

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	L7FW (NGFW,APFW)	－	日時	○	－	○	○							○		○		○							○					○		○	○	○
				送信元アドレス	○	接続元IPアドレス	○	○							○		○		○							○					○		○	○	○
				送信元ポート番号	○	接続元ポート番号	○	○							○		○		○							○					○		○	○	○
				宛先アドレス	○	接続先IPアドレス	○	○							○		○		○							○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○							○		○		○							○					○		○	○	○
				同一セッションの送受信バイト数	○	転送バイト数	○	○							○		○		○							○					○		○	○	○
				同一セッションの送受信パケット数	○	転送バイト数	○	○							○		○		○							○					○		○	○	○
				プロトコル	○	通信アプリケーション名	○	○							○		○		○							○					○		○	○	○
				セッション継続時間	○	セッション継続時間	○	○							○		○		○							○					○		○	○	○
				セッションのユーザ名	○	アカウント名	○	○							○		○		○							○					○		○	○	○
				URL	○	接続先URL	○	○							○		○		○							○					○		○	○	○
				ファイル名	○	ファイル名	○	○							○		○		○							○					○		○	○	○
				脅威情報	○	－	－	－																											
		DLP (Data Loss Prevention)		日時	○	－	－	○																							○				
				送信元アドレス	○	接続元IPアドレス	－	○																							○				
				送信元ポート番号	○	接続元ポート番号	－	○																							○				
				宛先アドレス	○	接続先IPアドレス	－	○																							○				
				宛先ポート番号	○	接続先ポート番号	－	○																							○				
				プロトコル		通信アプリケーション名	－	○																							○				
				URL		接続先URL	－	○																							○				
				検知キーワード	○	検知キーワード	－	○																							○				
				検知ファイル名	○	ファイル名	－	○																							○				
		Mailゲートウェイ		日時	○	－	○	○		○														○	○										
				サーバホスト名	○	－	－	－																											
				メッセージID	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	○	○		○														○	○										
				メッセージサイズ	○	－	－	－																											
				メッセージ受信者数	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	○	○		○														○	○										
				ステータス		－	－	－																											
				件名	○	件名	○	○		○														○	○										
				検知名	○	－	－	－																											
				検知ファイル名	○	－	－	－																											
				検知URL	○	－	－	－																											
		WAF		日時	○	－	○	○							○																		○	○	○
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	○	○							○																		○	○	○
				送信元ポート番号	○	接続元ポート番号	○	○							○																		○	○	○
				宛先アドレス	○	接続先IPアドレス	○	○							○																		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○							○																		○	○	○
				検知タイプ	○	－	－	－																											
				優先度	○	－	－	－																											
				アラートメッセージID	○	－	－	－																											
				アラートメッセージIDに紐づく検知項目（URL含む）	○	－	－	－																											
		サンドボックス		日時	○	－	○	○		○					○		○																		
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	○	○		○					○		○																		
				送信元ポート番号	○	接続元ポート番号	○	○		○					○		○																		
				宛先アドレス	○	接続先IPアドレス	○	○		○					○		○																		
				宛先ポート番号	○	接続先ポート番号	○	○		○					○		○																		
				プロトコル	○	－	－	－																											
				URL	○	接続先URL	○	○		○					○		○																		
				ファイル名	○	ファイル名	○	○		○					○		○																		
				ファイルタイプ	○	ファイル形式	○	○		○					○		○																		
				ファイルサイズ	○	ファイルサイズ	○	○		○					○		○																		
				ファイルハッシュ値	○	ファイルハッシュ値	○	○		○					○		○																		
				悪性判定結果	○	－	－	－																											
				マルウェアのファイル操作ログ	○	－	－	－																											
				マルウェアのプロセス操作ログ	○	－	－	－																											
				マルウェアのレジストリ操作ログ	○	－	－	－																											
				マルウェアのAPI呼出し	○	－	－	－																											
				マルウェアの通信先アドレス/ポート番号	○	－	－	－																											
		改ざん検知		日時	○	－	○	○							○									○	○										
				ログID	○	－	－	－																											
				改ざん内容(ファイルサイズ変化：旧、新)	○	ファイルサイズ変化	○	○							○									○	○										
				検知ルール名(追加/削除/編集)	○	イベント名	○	○							○									○	○										
				検知ファイル名	○	ファイル名	○	○							○									○	○										
				ユーザ名（検知した操作を行ったOSのアカウント名）	○	アカウント名	○	○							○									○	○										

攻撃経路	2. 標的組織の公開サービス・ホスト

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	ホスト型IPS/IDS		日時	○	－	○	○		○					○		○		○					○	○	○		○			○		○	○	○
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	○	○		○					○		○		○					○	○	○		○			○		○	○	○
				ホスト名	○	－	－	－																											
				検知ルール	○	－	○	○		○					○		○		○					○	○	○		○			○		○	○	○
				検知したファイル操作	○	－	○	○		○					○		○		○					○	○	○		○			○		○	○	○
				検知したプロセス操作	○	－	○	○		○					○		○		○					○	○	○		○			○		○	○	○
				検知したレジストリ操作	○	－	○	○		○					○		○		○					○	○	○		○			○		○	○	○
				検知したAPI呼出し	○	－	○	○		○					○		○		○					○	○	○		○			○		○	○	○
	内部セグメント			日時	○	－	－	○																○	○										
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	－	○																○	○										
				ホスト名	○	－	－	－																											
				検知ルール	○	－	－	○																○	○										
				検知したファイル操作	○	－	－	○																○	○										
				検知したプロセス操作	○	－	－	○																○	○										
				検知したレジストリ操作	○	－	－	○																○	○										
				検知したAPI呼出し	○	－	－	○																○	○										

攻撃経路	3.USB等の外部記憶媒体

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	ファイアウォール(FW)	―	日時	○	－	○	○									○		○				○			○					○		○	○	○
				ファイアウォールホスト名	○	－	－	－																											
				ファイアウォールルール名及び番号	○	－	－	－																											
				インバウンドインタフェース	○	－	－	－																											
				アウトバウンドインタフェース	○	－	－	－																											
				MACアドレス	○	－	－	－																											
				パケットサイズ	○	転送バイト数	○	○									○		○				○			○					○		○	○	○
				IPパケット優先度（TOS,PREC）	○	－	－	－																											
				IPパケット生存期間（TTL）	○	－	－	－																											
				IPフラグメントパケット識別子（ID）	○	－	－	－																											
				IPフラグメンテーション情報（DFビット）	○	－	－	－																											
				ソースIPアドレス	○	接続元IPアドレス	○	○									○		○				○			○					○		○	○	○
				ソースポート番号	○	接続元ポート番号	○	○									○		○				○			○					○		○	○	○
				宛先IPアドレス	○	接続先IPアドレス	○	○									○		○				○			○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○									○		○				○			○					○		○	○	○
				プロトコル	○	－	－	－																											
				TCPウインドウサイズ（WINDOW）	○	－	－	－																											
				TCPフラグ	○	－	－	－																											
		ネットワーク型IPS/IDS	―	日時	○	－	○	○									○		○				○			○					○		○	○	○
				送信元アドレス	○	－	○	○									○		○				○			○					○		○	○	○
				送信元ポート番号	○	－	○	○									○		○				○			○					○		○	○	○
				宛先アドレス	○	－	○	○									○		○				○			○					○		○	○	○
				宛先ポート番号	○	－	○	○									○		○				○			○					○		○	○	○
				同一セッションの送受信バイト数	○	－	○	○									○		○				○			○					○		○	○	○
				同一セッションの送受信パケット数	○	－	○	○									○		○				○			○					○		○	○	○
				プロトコル	○	－	○	○									○		○				○			○					○		○	○	○
				セッション継続時間	○	－	○	○									○		○				○			○					○		○	○	○
				セッションのユーザ名	○	－	○	○									○		○				○			○					○		○	○	○
				URL	○	－	○	○									○		○				○			○					○		○	○	○
				ファイル名	○	－	○	○									○		○				○			○					○		○	○	○
				脅威情報	○	－	○	○									○		○				○			○					○		○	○	○
		Webサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																								○	○	○
				クライアントの識別子	○	－	－	－																											
				認証されたユーザー名	○	ログインユーザ名	－	○																								○	○	○
				日時	○	－	－	○																								○	○	○
				リクエストの最初の行の値	○	接続先URL	－	○																								○	○	○
				最後のレスポンスのステータス	○	ステータスコード	－	○																								○	○	○
				送信されたバイト数（ヘッダーは含まず）	○	転送バイト数	－	○																								○	○	○
				リクエストに含まれるRefererの値	○	リファラ	－	○																								○	○	○
				リクエストに含まれるUser-Agentの値（ブラウザ情報）	○	ユーザエージェント	－	○																								○	○	○
			エラーログ	日時	○	－	－	○																								○	○	○
				エラーの重要度	○	－	－	－																											
				アクセスしたクライアントのIPアドレス	○	接続元IPアドレス	－	○																								○	○	○
				メッセージ	○	－	－	－																											
			SSLログ	日時		－	－	－																											
				リモートホスト名		－	－	－																											
				SSLプロトコルバージョン		－	－	－																											
				SSL暗号		－	－	－																											
				リクエストの最初の行の値		－	－	－																											
				送信されたバイト数(ヘッダーは含まず)		－	－	－																											
		APサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																								○	○	○
				認証されたユーザー名	○	ログインユーザ名	－	○																								○	○	○
				日時	○	－	－	○																								○	○	○
				メソッドとURL	○	接続先URL	－	○																								○	○	○
				HTTPステータスコード	○	ステータスコード	－	○																								○	○	○
				レスポンスサイズ	○	－	－	－																											
			APログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
			ホストログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
		DBサーバ	―	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
		プロキシサーバ	アクセスログ	UTCの時間	○	日時	○	○									○		○							○					○				
				継続時間	○	セッション継続時間	○	○									○		○							○					○				
				クライアントのIPアドレス	○	接続元IPアドレス	○	○									○		○							○					○				
				リザルトコード（結果コード）	○	ステータスコード	○	○									○		○							○					○				
				転送バイト数	○	転送バイト数	○	○									○		○							○					○				
				リクエストメソッド	○	リクエストメソッド	○	○									○		○							○					○				
				URL	○	接続先URL	○	○									○		○							○					○				

攻撃経路	3.USB等の外部記憶媒体

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
									①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）		標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	プロキスサーバ	アクセスログ	階層コード	○	接続先IPアドレス	○	○									○		○							○					○				
				HTTPヘッダにリプライされてきたオブジェクトのコンテンツタイプ	○	ファイル形式	○	○									○		○							○					○				
				User-Agent		ユーザエージェント	○	○									○		○							○					○				
			動作ログ（エラーログ・デバッグログ・キャッシュ）	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
			デバッグログ	日時	○	－	－	－																											
				メッセージ（エラーやデバックメッセージ）	○	－	－	－																											
		DNSサーバ	―	日時		－	○	○									○		○							○		○			○				
				ログカテゴリ		－	－	－																											
				クライアントのIPアドレスとポート番号		接続元IPアドレス	○	○									○		○							○		○			○				
				ファシリティ（ログの分類）		－	－	－																											
				ゾーン情報		リクエストドメイン名	○	○									○		○							○		○			○				
						DNSリクエストレコードタイプ	○	○									○		○							○		○			○				
		メールサーバ	―	日時	○	－	－	○																○	○						○				
				サーバホスト名	○	－	－	－																											
				プロセスの情報（プロセスの所有者とプロセスID）	○	－	－	－																											
				メッセージID（Sendmailによって送信されたメッセージに割り当てられたID）	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	－	○																○	○						○				
				メッセージサイズ	○	転送バイト数	－	○																○	○						○				
				メッセージ優先度	○	－	－	－																											
				メッセージ受信者数	○	メッセージ受信者数	－	○																○	○						○				
				メッセージ識別番号	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				サーバデーモン名	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	－	○																○	○						○				
				ステータス	○	－	－	－																											
				添付ファイル名		添付ファイル名	－	○																○	○						○				
	内部セグメント	スイッチ/ルータ	―	日時		－	○	○									○		○			○	○	○	○	○		○			○				
				送信元アドレス	○	接続元IPアドレス	○	○									○		○			○	○	○	○	○		○			○				
				送信元ポート番号	○	接続元ポート番号	○	○									○		○			○	○	○	○	○		○			○				
				宛先アドレス	○	接続先IPアドレス	○	○									○		○			○	○	○	○	○		○			○				
				宛先ポート番号	○	接続先ポート番号	○	○									○		○			○	○	○	○	○		○			○				
				同一フローの送受信バイト数		転送バイト数	○	○									○		○			○	○	○	○	○		○			○				
				同一フローの送受信パケット数		転送バイト数	○	○									○		○			○	○	○	○	○		○			○				
		ドメインコントローラー	―	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	○														○	○	○	○										
				イベントID	○	エラーコード	－	○														○	○	○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	－	○														○	○	○	○										
				ユーザー	○	アカウント名	－	○														○	○	○	○										
				コンピュータ	○	ワークステーション名	－	○														○	○	○	○										
				オペコード	○	－	－	－																											
		DHCPサーバ	―	日時		－	－	－																											
				ホスト名またはIPアドレス		－	－	－																											
				MACアドレス		－	－	－																											
				状態		－	－	－																											
		DNSサーバ（内部DNS）	―	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	－																											
				イベントID	○	－	－	－																											
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	－	－	－																											
				ユーザー	○	－	－	－																											
				コンピュータ	○	－	－	－																											
				オペコード	○	－	－	－																											

攻撃経路	3.USB等の外部記憶媒体

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	ファイルサーバ	―	ログの名前	○	－	－	－																										
				ソース	○	－	－	－																										
				日時	○	－	－	○																○	○										
				イベントID	○	エラーコード	－	○																○	○										
				タスクのカテゴリ	○	－	－	－																										
				レベル	○	－	－	－																										
				キーワード	○	イベント名	－	○																○	○										
				ユーザー	○	アカウント名	－	○																○	○										
				コンピュータ	○	ワークステーション名	－	○																○	○										
				オペコード	○	－	－	－																										
		エンドポイント(Windows)	イベントログ	ログの名前	○	－	－	－																										
				ソース	○	－	－	－																										
				日時	○	－	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○				
				イベントID	○	エラーコード	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○				
				タスクのカテゴリ	○	－	－	－																										
				レベル	○	－	－	－																										
				キーワード	○	イベント名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○				
				ユーザー	○	アカウント名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○				
				コンピュータ	○	ワークステーション名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○				
				オペコード	○	－	－	－																										
			プリフェッチ	日時	○	－	○	○			○						○					○	○					○	○		○				
				ファイル名	○	ファイル名	○	○			○						○					○	○					○	○		○				
			レジストリ	自動起動のファイル名		ファイル名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				接続したUSBメモリ等の情報		接続デバイス名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			スクリーンセーバー	起動するスクリーンセーバー		－	－	－																										
			タスクスケジューラ	ログの名前	○	－	－	－																										
				ソース	○	－	－	－																										
				日時	○	－	○	○									○	○																	
				イベントID	○	エラーコード	○	○									○	○																	
				タスクのカテゴリ	○	－	－	－																										
				レベル	○	－	－	－																										
				キーワード	○	イベント名	○	○									○	○																	
				ユーザー	○	アカウント名	○	○									○	○																	
				コンピュータ	○	ワークステーション名	○	○									○	○																	
				オペコード	○	－	－	－																										
			ファイルの履歴	以前のバージョン情報		－	－	－																										
			プロセスログ	日時		－	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																										
				タイプ		－	－	－																										
				ファイル名		プロセス名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
		エンドポイント(Linux)	メッセージログ	日時	○	－	－	－																										
				ログを出力したホスト名	○	－	－	－																										
				メッセージの出力元	○	－	－	－																										
				メッセージ	○	－	－	－																										
			cronログ	日時	○	－	－	－																										
				ログを出力したホスト名	○	－	－	－																										
				メッセージの出力元	○	－	－	－																										
				メッセージ	○	－	－	－																										
			カーネルログ	日時	○	－	○	○			○																								
				ログを出力したホスト名	○	ワークステーション名	○	○			○																								
				メッセージの出力元	○	－	－	－																										
				メッセージ	○	接続デバイス名	○	○			○																								
			セキュリティログ	日時	○	－	－	○															○										○	○	○
				ログを出力したホスト名	○	－	－	－																										
				メッセージの出力元	○	－	－	－																										
				メッセージ	○	接続元IPアドレス	－	○															○										○	○	○
						ログインユーザ名	－	○															○										○	○	○
						認証成否結果	－	○															○										○	○	○
		エンドポイント(OS)	システムコールログ：ファイル操作ログ	日時		－	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																										
				プロセス名		プロセス名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				ファイルパス		ファイルパス	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ：プロセス操作ログ	日時		－	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				親プロセスID		－	－	－																										
				プロセスID		－	－	－																										
				プロセス名		プロセス名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				コマンドライン		ファイルパス	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ：レジストリ操作ログ	日時		－	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																										
				キー		レジストリキー	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				値		レジストリ値	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				データ		－	－	－																										
			システムコールログ：API操作ログ	日時		－	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																										
				API名		API名	○	○			○						○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				APIの引数		－	－	－																										
				APIの戻り値		－	－	－																										

攻撃経路	3.USB等の外部記憶媒体

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																									
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ					
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行					
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	エンドポイント（ブラウザ）	–	日時	○	–	–	–																										
				URL	○	接続先URL	–	–																										
		エンドポイント（AntiVirus）	–	スキャン日時	○	–	○	○			○						○							○	○									
				プロセスID	○	–	○	○			○						○							○	○									
				プロセス名	○	–	○	○			○						○							○	○									
				スキャン結果	○	–	○	○			○						○							○	○									

攻撃経路	3.USB等の外部記憶媒体

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	L7FW (NGFW,APFW)	－	日時	○	－	○	○									○		○							○					○		○	○	○
				送信元アドレス	○	接続元IPアドレス	○	○									○		○							○					○		○	○	○
				送信元ポート番号	○	接続元ポート番号	○	○									○		○							○					○		○	○	○
				宛先アドレス	○	接続先IPアドレス	○	○									○		○							○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○									○		○							○					○		○	○	○
				同一セッションの送受信バイト数	○	転送バイト数	○	○									○		○							○					○		○	○	○
				同一セッションの送受信パケット数	○	転送バイト数	○	○									○		○							○					○		○	○	○
				プロトコル	○	通信アプリケーション名	○	○									○		○							○					○		○	○	○
				セッション継続時間	○	セッション継続時間	○	○									○		○							○					○		○	○	○
				セッションのユーザ名	○	アカウント名	○	○									○		○							○					○		○	○	○
				URL	○	接続先URL	○	○									○		○							○					○		○	○	○
				ファイル名	○	ファイル名	○	○									○		○							○					○		○	○	○
				脅威情報	○	－	－	－																											
		DLP (Data Loss Prevention)		日時	○	－	－	○																							○				
				送信元アドレス	○	接続元IPアドレス	－	○																							○				
				送信元ポート番号	○	接続元ポート番号	－	○																							○				
				宛先アドレス	○	接続先IPアドレス	－	○																							○				
				宛先ポート番号	○	接続先ポート番号	－	○																							○				
				プロトコル		通信アプリケーション名	－	○																							○				
				URL		接続先URL	－	○																							○				
				検知キーワード	○	検知キーワード	－	○																							○				
				検知ファイル名	○	ファイル名	－	○																							○				
		Mailゲートウェイ		日時	○	－	－	○																○	○										
				サーバホスト名	○	－	－	－																											
				メッセージID	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	－	○																○	○										
				メッセージサイズ	○	－	－	－																											
				メッセージ受信者数	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	－	○																○	○										
				ステータス		－	－	－																											
				件名	○	件名	－	○																○	○										
				検知名	○	－	－	－																											
				検知ファイル名	○	－	－	－																											
				検知URL	○	－	－	－																											
		WAF		日時	○	－	－	○																									○	○	○
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	－	○																									○	○	○
				送信元ポート番号	○	接続元ポート番号	－	○																									○	○	○
				宛先アドレス	○	接続先IPアドレス	－	○																									○	○	○
				宛先ポート番号	○	接続先ポート番号	－	○																									○	○	○
				検知タイプ	○	－	－	－																											
				優先度	○	－	－	－																											
				アラートメッセージID	○	－	－	－																											
				アラートメッセージIDに紐づく検知項目（URL含む）	○	－	－	－																											
		サンドボックス		日時	○	－	○	○									○																		
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	○	○									○																		
				送信元ポート番号	○	接続元ポート番号	○	○									○																		
				宛先アドレス	○	接続先IPアドレス	○	○									○																		
				宛先ポート番号	○	接続先ポート番号	○	○									○																		
				プロトコル	○	－	－	－																											
				URL	○	接続先URL	○	○									○																		
				ファイル名	○	ファイル名	○	○									○																		
				ファイルタイプ	○	ファイル形式	○	○									○																		
				ファイルサイズ	○	ファイルサイズ	○	○									○																		
				ファイルハッシュ値	○	ファイルハッシュ値	○	○									○																		
				悪性判定結果	○	－	－	－																											
				マルウェアのファイル操作ログ	○	－	－	－																											
				マルウェアのプロセス操作ログ	○	－	－	－																											
				マルウェアのレジストリ操作ログ	○	－	－	－																											
				マルウェアのAPI呼出し	○	－	－	－																											
				マルウェアの通信先アドレス/ポート番号	○	－	－	－																											
		改ざん検知		日時	○	－	－	○																○	○										
				ログID	○	－	－	－																											
				改ざん内容(ファイルサイズ変化：旧、新)	○	ファイルサイズ変化	－	○																○	○										
				検知ルール名(追加/削除/編集)	○	イベント名	－	○																○	○										
				検知ファイル名	○	ファイル名	－	○																○	○										
				ユーザ名（検知した操作を行ったOSのアカウント名）	○	アカウント名	－	○																○	○										

攻撃経路	3.USB等の外部記憶媒体

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ											拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	ホスト型IPS/IDS		日時	○	－	○	○									○		○					○	○	○		○			○		○	○	○
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	○	○									○		○					○	○	○		○			○		○	○	○
				ホスト名	○	－	－	－																											
				検知ルール	○	－	○	○									○		○					○	○	○		○			○		○	○	○
				検知したファイル操作	○	－	○	○									○		○					○	○	○		○			○		○	○	○
				検知したプロセス操作	○	－	○	○									○		○					○	○	○		○			○		○	○	○
				検知したレジストリ操作	○	－	○	○									○		○					○	○	○		○			○		○	○	○
				検知したAPI呼出し	○	－	○	○									○		○					○	○	○		○			○		○	○	○
	内部セグメント			日時	○	－	－	○																○	○										
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	－	○																○	○										
				ホスト名	○	－	－	－																											
				検知ルール	○	－	－	○																○	○										
				検知したファイル操作	○	－	－	○																○	○										
				検知したプロセス操作	○	－	－	○																○	○										
				検知したレジストリ操作	○	－	－	○																○	○										
				検知したAPI呼出し	○	－	－	○																○	○										

攻撃経路	4.不正コード混入ソフトウェア

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																															
									攻撃侵入フェーズ検知ログカテゴリ											拡散フェーズ検知ログカテゴリ														目的遂行フェーズ検知ログカテゴリ					
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備								⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行											
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的的が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的的が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	ファイアウォール(FW)	_	日時	○	-	○	○						○			○			○				○					○				○			○		○
				ファイアウォールホスト名	○	-	-	-																																
				ファイアウォールルール名及び番号	○	-	-	-																																
				インバウンドインタフェース	○	-	-	-																																
				アウトバウンドインタフェース	○	-	-	-																																
				MACアドレス	○	-	-	-																																
				パケットサイズ	○	転送バイト数	○	○						○			○			○				○					○				○			○		○
				IPパケット優先度（TOS,PREC）	○	-	-	-																																
				IPパケット生存期間（TTL）	○	-	-	-																																
				IPフラグメントパケット識別子（ID）	○	-	-	-																																
				IPフラグメンテーション情報（DFビット）	○	-	-	-																																
				ソースIPアドレス	○	接続元IPアドレス	○	○						○			○			○				○					○				○			○		○
				ソースポート番号	○	接続元ポート番号	○	○						○			○			○				○					○				○			○		○
				宛先IPアドレス	○	接続先IPアドレス	○	○						○			○			○				○					○				○			○		○
				宛先ポート番号	○	接続先ポート番号	○	○						○			○			○				○					○				○			○		○
				プロトコル	○	-	-	-																																
				TCPウインドウサイズ（WINDOW）	○	-	-	-																																
				TCPフラグ	○	-	-	-																																
		ネットワーク型IPS/IDS	_	日時	○	-	○	○						○			○			○				○					○				○			○		○
				送信元アドレス	○	-	○	○						○			○			○				○					○				○			○		○
				送信元ポート番号	○	-	○	○						○			○			○				○					○				○			○		○
				宛先アドレス	○	-	○	○						○			○			○				○					○				○			○		○
				宛先ポート番号	○	-	○	○						○			○			○				○					○				○			○		○
				同一セッションの送受信バイト数	○	-	○	○						○			○			○				○					○				○			○		○
				同一セッションの送受信パケット数	○	-	○	○						○			○			○				○					○				○			○		○
				プロトコル	○	-	○	○						○			○			○				○					○				○			○		○
				セッション継続時間	○	-	○	○						○			○			○				○					○				○			○		○
				セッションのユーザ名	○	-	○	○						○			○			○				○					○				○			○		○
				URL	○	-	○	○						○			○			○				○					○				○			○		○
				ファイル名	○	-	○	○						○			○			○				○					○				○			○		○
				脅威情報	○	-	○	○						○			○			○				○					○				○			○		○
		Webサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	-	○																												○	○	○
				クライアントの識別子	○	-	-	-																																
				認証されたユーザー名	○	ログインユーザ名	-	○																												○	○	○
				日時	○	-	-	○																												○	○	○
				リクエストの最初の行の値	○	接続先URL	-	○																												○	○	○
				最後のレスポンスのステータス	○	ステータスコード	-	○																												○	○	○
				送信されたバイト数（ヘッダーは含まず）	○	転送バイト数	-	○																												○	○	○
				リクエストに含まれるRefererの値	○	リファラ	-	○																												○	○	○
				リクエストに含まれるUser-Agentの値（ブラウザ情報）	○	ユーザエージェント	-	○																												○	○	○
			エラーログ	日時	○	-	-	○																												○	○	○
				エラーの重要度	○	-	-	-																																
				アクセスしたクライアントのIPアドレス	○	接続元IPアドレス	-	○																												○	○	○
				メッセージ	○	-	-	-																																
			SSLログ	日時		-	-	-																																
				リモートホスト名		-	-	-																																
				SSLプロトコルバージョン		-	-	-																																
				SSL暗号		-	-	-																																
				リクエストの最初の行の値		-	-	-																																
				送信されたバイト数(ヘッダーは含まず)		-	-	-																																
		APサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	-	○																												○	○	○
				認証されたユーザー名	○	ログインユーザ名	-	○																												○	○	○
				日時	○	-	-	○																												○	○	○
				メソッドとURL	○	接続先URL	-	○																												○	○	○
				HTTPステータスコード	○	ステータスコード	-	○																												○	○	○
				レスポンスサイズ	○	-	-	-																																
			APログ	日時	○	-	-	-																																
				ログを生成したスレッド	○	-	-	-																																
				ログレベル	○	-	-	-																																
				カテゴリー名	○	-	-	-																																
				メッセージ	○	-	-	-																																
			ホストログ	日時	○	-	-	-																																
				ログを生成したスレッド	○	-	-	-																																
				ログレベル	○	-	-	-																																
				カテゴリー名	○	-	-	-																																
				メッセージ	○	-	-	-																																
		DBサーバ	ー	日時	○	-	-	-																																
				メッセージ	○	-	-	-																																
		プロキシサーバ	アクセスログ	UTCの時間	○	日時	○	○						○			○			○				○					○				○			○		○
				継続時間	○	セッション継続時間	○	○						○			○			○				○					○				○			○		○
				クライアントのIPアドレス	○	接続元IPアドレス	○	○						○			○			○				○					○				○			○		○
				リザルトコード（結果コード）	○	ステータスコード	○	○						○			○			○				○					○				○			○		○
				転送バイト数	○	転送バイト数	○	○						○			○			○				○					○				○			○		○
				リクエストメソッド	○	リクエストメソッド	○	○						○			○			○				○					○				○			○		○
				URL	○	接続先URL	○	○						○			○			○				○					○				○			○		○

攻撃経路	4.不正コード混入ソフトウェア

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																									
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	プロキスサーバ	アクセスログ	階層コード	○	接続先IPアドレス	○	○						○			○		○							○					○			
				HTTPヘッダにリプライされてきたオブジェクトのコンテンツタイプ	○	ファイル形式	○	○						○			○		○							○					○			
				User-Agent		ユーザエージェント	○	○						○			○		○							○					○			
			動作ログ（エラーログ・デバッグログ・キャッシュ）	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
			デバッグログ	日時	○	－	－	－																											
				メッセージ（エラーやデバックメッセージ）	○	－	－	－																											
		DNSサーバ	—	日時		－	○	○						○			○		○							○		○			○			
				ログカテゴリ		－	－	－																											
				クライアントのIPアドレスとポート番号		接続元IPアドレス	○	○						○			○		○							○		○			○			
				ファシリティ（ログの分類）		－	－	－																											
				ゾーン情報		リクエストドメイン名	○	○						○			○		○							○		○			○			
						DNSリクエストレコードタイプ	○	○						○			○		○							○		○			○			
		メールサーバ	—	日時	○	－	－	○																○	○						○			
				サーバホスト名	○	－	－	－																											
				プロセスの情報（プロセスの所有者とプロセスID）	○	－	－	－																											
				メッセージID（Sendmailによって送信されたメッセージに割り当てられたID）	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	－	○																○	○						○			
				メッセージサイズ	○	転送バイト数	－	○																○	○						○			
				メッセージ優先度	○	－	－	－																											
				メッセージ受信者数	○	メッセージ受信者数	－	○																○	○						○			
				メッセージ識別番号	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				サーバデーモン名	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	－	○																○	○						○			
				ステータス	○	－	－	－																											
				添付ファイル名		添付ファイル名	－	○																○	○						○			
	内部セグメント	スイッチ/ルータ	—	日時		－	○	○						○			○		○			○	○	○	○	○		○			○			
				送信元アドレス	○	接続元IPアドレス	○	○						○			○		○			○	○	○	○	○		○			○			
				送信元ポート番号	○	接続元ポート番号	○	○						○			○		○			○	○	○	○	○		○			○			
				宛先アドレス	○	接続先IPアドレス	○	○						○			○		○			○	○	○	○	○		○			○			
				宛先ポート番号	○	接続先ポート番号	○	○						○			○		○			○	○	○	○	○		○			○			
				同一フローの送受信バイト数		転送バイト数	○	○						○			○		○			○	○	○	○	○		○			○			
				同一フローの送受信パケット数		転送バイト数	○	○						○			○		○			○	○	○	○	○		○			○			
		ドメインコントローラー	—	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	○														○	○	○	○										
				イベントID	○	エラーコード	－	○														○	○	○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	－	○														○	○	○	○										
				ユーザー	○	アカウント名	－	○														○	○	○	○										
				コンピュータ	○	ワークステーション名	－	○														○	○	○	○										
				オペコード	○	－	－	－																											
		DHCPサーバ	—	日時		－	－	－																											
				ホスト名またはIPアドレス		－	－	－																											
				MACアドレス		－	－	－																											
				状態		－	－	－																											
		DNSサーバ（内部DNS）	—	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	－																											
				イベントID	○	－	－	－																											
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	－	－	－																											
				ユーザー	○	－	－	－																											
				コンピュータ	○	－	－	－																											
				オペコード	○	－	－	－																											

攻撃経路	4.不正コード混入ソフトウェア

区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名）検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ（基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ（拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み 標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	③感染したコンピュータシステムにおける足場固め マルウェア初期活動	再起動時の実行設定による常駐化	④他のコンピュータシステムへの展開準備 バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	⑤C2ホストとの積極的な通信 検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	⑥本格的な攻撃実行 取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	ファイルサーバ	－	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	○																○	○										
				イベントID	○	エラーコード	－	○																○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	－	○																○	○										
				ユーザー	○	アカウント名	－	○																○	○										
				コンピュータ	○	ワークステーション名	－	○																○	○										
				オペコード	○	－	－	－																											
		エンドポイント(Windows)	イベントログ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○				
				イベントID	○	エラーコード	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○				
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○				
				ユーザー	○	アカウント名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○				
				コンピュータ	○	ワークステーション名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○				
				オペコード	○	－	－	－																											
			プリフェッチ	日時	○	－	○	○						○			○						○	○					○	○		○				
				ファイル名	○	ファイル名	○	○						○			○						○	○					○	○		○				
			レジストリ	自動起動のファイル名		ファイル名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				接続したUSBメモリ等の情報		接続デバイス名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			スクリーンセーバー	起動するスクリーンセーバー		－	－	－																											
			タスクスケジューラ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○									○	○																	
				イベントID	○	エラーコード	○	○									○	○																	
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○									○	○																	
				ユーザー	○	アカウント名	○	○									○	○																	
				コンピュータ	○	ワークステーション名	○	○									○	○																	
				オペコード	○	－	－	－																											
			ファイルの履歴	以前のバージョン情報		－	－	－																											
			プロセスログ	日時		－	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				タイプ		－	－	－																											
				ファイル名		プロセス名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
		エンドポイント(Linux)	メッセージログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			cronログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			カーネルログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	ワークステーション名	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続デバイス名	－	－																											
			セキュリティログ	日時	○	－	－	○															○											○	○	○
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続元IPアドレス	－	○															○											○	○	○
						ログインユーザ名	－	○															○											○	○	○
						認証成否結果	－	○															○											○	○	○
		エンドポイント(OS)	システムコールログ ファイル操作ログ	日時		－	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				ファイルパス		ファイルパス	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ プロセス操作ログ	日時		－	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				親プロセスID		－	－	－																											
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				コマンドライン		ファイルパス	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ レジストリ操作ログ	日時		－	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				キー		レジストリキー	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				値		レジストリ値	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				データ		－	－	－																											
			システムコールログ API操作ログ	日時		－	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				API名		API名	○	○						○			○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				APIの引数		－	－	－																											
				APIの戻り値		－	－	－																											

攻撃経路	4. 不正コード混入ソフトウェア

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																															
									攻撃侵入フェーズ検知ログカテゴリ												拡散フェーズ検知ログカテゴリ												目的遂行フェーズ検知ログカテゴリ							
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み								③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行													
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的的組織に属さない人間持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他のコンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した報改ん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	エンドポイント（ブラウザ）	_	日時	○	-	○	○						○																									
				URL	○	接続先URL	○	○						○																									
		エンドポイント（AntiVirus）	_	スキャン日時	○	-	○	○						○				○									○	○											
				プロセスID	○	-	○	○						○				○									○	○											
				プロセス名	○	-	○	○						○				○									○	○											
				スキャン結果	○	-	○	○						○				○									○	○											

攻撃経路	4.不正コード混入ソフトウェア

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ											拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ							
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行							
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	L7FW (NGFW,APFW)	－	日時	○	－	○	○						○			○		○							○					○		○	○	○
				送信元アドレス	○	接続元IPアドレス	○	○						○			○		○							○					○		○	○	○
				送信元ポート番号	○	接続元ポート番号	○	○						○			○		○							○					○		○	○	○
				宛先アドレス	○	接続先IPアドレス	○	○						○			○		○							○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○						○			○		○							○					○		○	○	○
				同一セッションの送受信バイト数	○	転送バイト数	○	○						○			○		○							○					○		○	○	○
				同一セッションの送受信パケット数	○	転送バイト数	○	○						○			○		○							○					○		○	○	○
				プロトコル	○	通信アプリケーション名	○	○						○			○		○							○					○		○	○	○
				セッション継続時間	○	セッション継続時間	○	○						○			○		○							○					○		○	○	○
				セッションのユーザ名	○	アカウント名	○	○						○			○		○							○					○		○	○	○
				URL	○	接続先URL	○	○						○			○		○							○					○		○	○	○
				ファイル名	○	ファイル名	○	○						○			○		○							○					○		○	○	○
				脅威情報	○	－	－	－																											
		DLP (Data Loss Prevention)		日時	○	－	－	○																							○				
				送信元アドレス	○	接続元IPアドレス	－	○																							○				
				送信元ポート番号	○	接続元ポート番号	－	○																							○				
				宛先アドレス	○	接続先IPアドレス	－	○																							○				
				宛先ポート番号	○	接続先ポート番号	－	○																							○				
				プロトコル		通信アプリケーション名	－	○																							○				
				URL		接続先URL	－	○																							○				
				検知キーワード	○	検知キーワード	－	○																							○				
				検知ファイル名	○	ファイル名	－	○																							○				
		Mailゲートウェイ		日時	○	－	－	○																○	○										
				サーバホスト名	○	－	－	－																											
				メッセージID	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	－	○																○	○										
				メッセージサイズ	○	－	－	－																											
				メッセージ受信者数	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	－	○																○	○										
				ステータス		－	－	－																											
				件名	○	件名	－	○																○	○										
				検知名	○	－	－	－																											
				検知ファイル名	○	－	－	－																											
				検知URL	○	－	－	－																											
		WAF		日時	○	－	－	○																									○	○	○
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	－	○																									○	○	○
				送信元ポート番号	○	接続元ポート番号	－	○																									○	○	○
				宛先アドレス	○	接続先IPアドレス	－	○																									○	○	○
				宛先ポート番号	○	接続先ポート番号	－	○																									○	○	○
				検知タイプ	○	－	－	－																											
				優先度	○	－	－	－																											
				アラートメッセージID	○	－	－	－																											
				アラートメッセージIDに紐づく検知項目（URL含む）	○	－	－	－																											
		サンドボックス		日時	○	－	○	○						○			○																		
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	○	○						○			○																		
				送信元ポート番号	○	接続元ポート番号	○	○						○			○																		
				宛先アドレス	○	接続先IPアドレス	○	○						○			○																		
				宛先ポート番号	○	接続先ポート番号	○	○						○			○																		
				プロトコル	○	－	－	－																											
				URL	○	接続先URL	○	○						○			○																		
				ファイル名	○	ファイル名	○	○						○			○																		
				ファイルタイプ	○	ファイル形式	○	○						○			○																		
				ファイルサイズ	○	ファイルサイズ	○	○						○			○																		
				ファイルハッシュ値	○	ファイルハッシュ値	○	○						○			○																		
				悪性判定結果	○	－	－	－																											
				マルウェアのファイル操作ログ	○	－	－	－																											
				マルウェアのプロセス操作ログ	○	－	－	－																											
				マルウェアのレジストリ操作ログ	○	－	－	－																											
				マルウェアのAPI呼出し	○	－	－	－																											
				マルウェアの通信先アドレス/ポート番号	○	－	－	－																											
		改ざん検知		日時	○	－	－	○																○	○										
				ログID	○	－	－	－																											
				改ざん内容(ファイルサイズ変化：旧、新)	○	ファイルサイズ変化	－	○																○	○										
				検知ルール名(追加/削除/編集)	○	イベント名	－	○																○	○										
				検知ファイル名	○	ファイル名	－	○																○	○										
				ユーザ名（検知した操作を行ったOSのアカウント名）	○	アカウント名	－	○																○	○										

攻撃経路	4. 不正コード混入ソフトウェア

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ											拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	ホスト型IPS/IDS		日時	○	－	○	○						○			○		○					○	○	○		○			○		○	○	○
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	○	○						○			○		○					○	○	○		○			○		○	○	○
				ホスト名	○	－	－	－																											
				検知ルール	○	－	○	○						○			○		○					○	○	○		○			○		○	○	○
				検知したファイル操作	○	－	○	○						○			○		○					○	○	○		○			○		○	○	○
				検知したプロセス操作	○	－	○	○						○			○		○					○	○	○		○			○		○	○	○
				検知したレジストリ操作	○	－	○	○						○			○		○					○	○	○		○			○		○	○	○
				検知したAPI呼出し	○	－	○	○						○			○		○					○	○	○		○			○		○	○	○
	内部セグメント			日時	○	－	－	○																○	○										
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	－	○																○	○										
				ホスト名	○	－	－	－																											
				検知ルール	○	－	－	○																○	○										
				検知したファイル操作	○	－	－	○																○	○										
				検知したプロセス操作	○	－	－	○																○	○										
				検知したレジストリ操作	○	－	－	○																○	○										
				検知したAPI呼出し	○	－	－	○																○	○										

攻撃経路	5.クラウドサービス

区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名）	検知に使用する基本ログ	検知に使用する基本ログ＋拡張ログ	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
						検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	（基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	（拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）		②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
標準構成機器	DMZ	ファイアウォール（FW）	－	日時	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				ファイアウォールホスト名	○	－	－	－																											
				ファイアウォールルール名及び番号	○	－	－	－																											
				インバウンドインタフェース	○	－	－	－																											
				アウトバウンドインタフェース	○	－	－	－																											
				MACアドレス	○	－	－	－																											
				パケットサイズ	○	転送バイト数	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				IPパケット優先度（TOS,PREC）	○	－	－	－																											
				IPパケット生存期間（TTL）	○	－	－	－																											
				IPフラグメントパケット識別子（ID）	○	－	－	－																											
				IPフラグメンテーション情報（DFビット）	○	－	－	－																											
				ソースIPアドレス	○	接続元IPアドレス	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				ソースポート番号	○	接続元ポート番号	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				宛先IPアドレス	○	接続先IPアドレス	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				プロトコル	○	－	－	－																											
				TCPウインドウサイズ（WINDOW）	○	－	－	－																											
				TCPフラグ	○	－	－	－																											
		ネットワーク型IPS/IDS	－	日時	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				送信元アドレス	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				送信元ポート番号	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				宛先アドレス	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				宛先ポート番号	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				同一セッションの送受信バイト数	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				同一セッションの送受信パケット数	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				プロトコル	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				セッション継続時間	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				セッションのユーザ名	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				URL	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				ファイル名	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
				脅威情報	○	－	○	○					○				○		○	○			○			○	○				○	○	○	○	○
		Webサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				クライアントの識別子	○	－	－	－																											
				認証されたユーザー名	○	ログインユーザ名	－	○																									○	○	○
				日時	○	－	－	○																									○	○	○
				リクエストの最初の行の値	○	接続先URL	－	○																									○	○	○
				最後のレスポンスのステータス	○	ステータスコード	－	○																									○	○	○
				送信されたバイト数（ヘッダーは含まず）	○	転送バイト数	－	○																									○	○	○
				リクエストに含まれるRefererの値	○	リファラ	－	○																									○	○	○
				リクエストに含まれるUser-Agentの値（ブラウザ情報）	○	ユーザエージェント	－	○																									○	○	○
			エラーログ	日時	○	－	－	○																									○	○	○
				エラーの重要度	○	－	－	－																											
				アクセスしたクライアントのIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				メッセージ	○	－	－	－																											
			SSLログ	日時		－	－	－																											
				リモートホスト名		－	－	－																											
				SSLプロトコルバージョン		－	－	－																											
				SSL暗号		－	－	－																											
				リクエストの最初の行の値		－	－	－																											
				送信されたバイト数(ヘッダーは含まず)		－	－	－																											
		APサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				認証されたユーザー名	○	ログインユーザ名	－	○																									○	○	○
				日時	○		－	○																									○	○	○
				メソッドとURL	○	接続先URL	－	○																									○	○	○
				HTTPステータスコード	○	ステータスコード	－	○																									○	○	○
				レスポンスサイズ	○	－	－	－																											
			APログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
			ホストログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
		DBサーバ	－	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
		プロキシサーバ	アクセスログ	UTCの時間	○	日時	○	○					○				○		○	○						○	○				○	○			
				継続時間	○	セッション継続時間	○	○					○				○		○	○						○	○				○	○			
				クライアントのIPアドレス	○	接続元IPアドレス	○	○					○				○		○	○						○	○				○	○			
				リザルトコード（結果コード）	○	ステータスコード	○	○					○				○		○	○						○	○				○	○			
				転送バイト数	○	転送バイト数	○	○					○				○		○	○						○	○				○	○			
				リクエストメソッド	○	リクエストメソッド	○	○					○				○		○	○						○	○				○	○			
				URL	○	接続先URL	○	○					○				○		○	○						○	○				○	○			

攻撃経路	5.クラウドサービス

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																																
									攻撃侵入フェーズ検知ログカテゴリ											拡散フェーズ検知ログカテゴリ											目的遂行フェーズ検知ログカテゴリ										
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行											
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	プロキシサーバ	アクセスログ	階層コード	○	接続先IPアドレス	○	○					○				○		○	○					○	○				○	○						
				HTTPヘッダにリプライされてきたオブジェクトのコンテンツタイプ	○	ファイル形式	○	○					○				○		○	○					○	○				○	○						
				User-Agent		ユーザエージェント	○	○					○				○		○	○					○	○				○	○						
			動作ログ（エラーログ・デバッグログ・キャッシュ）	日時	○	－	－	－																													
				メッセージ	○	－	－	－																													
			デバッグログ	日時	○	－	－	－																													
				メッセージ（エラーやデバックメッセージ）	○	－	－	－																													
		DNSサーバ	－	日時		－	○	○					○				○		○	○					○	○	○			○	○						
				ログカテゴリ		－	－	－																													
				クライアントのIPアドレスとポート番号		接続元IPアドレス	○	○					○				○		○	○					○	○	○			○	○						
				ファシリティ（ログの分類）		－	－	－																													
				ゾーン情報		リクエストドメイン名	○	○					○				○		○	○					○	○	○			○	○						
						DNSリクエストレコードタイプ	○	○					○				○		○	○					○	○	○			○	○						
		メールサーバ	－	日時	○	－	－	○																		○	○				○	○						
				サーバホスト名	○	－	－	－																													
				プロセスの情報（プロセスの所有者とプロセスID）	○	－	－	－																													
				メッセージID（Sendmailによって送信されたメッセージに割り当てられたID）	○	－	－	－																													
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	－	○																		○	○				○	○						
				メッセージサイズ	○	転送バイト数	－	○																		○	○				○	○						
				メッセージ優先度	○	－	－	－																													
				メッセージ受信者数	○	メッセージ受信者数	－	○																		○	○				○	○						
				メッセージ識別番号	○	－	－	－																													
				プロトコル情報	○	－	－	－																													
				サーバデーモン名	○	－	－	－																													
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	－	○																		○	○				○	○						
				ステータス	○	－	－	－																													
				添付ファイル名		添付ファイル名	－	○																		○	○				○	○						
	内部セグメント	スイッチ/ルータ	－	日時		－	○	○				○					○		○	○		○	○	○	○	○	○	○			○	○						
				送信元アドレス	○	接続元IPアドレス	○	○				○					○		○	○		○	○	○	○	○	○	○			○	○						
				送信元ポート番号	○	接続元ポート番号	○	○				○					○		○	○		○	○	○	○	○	○	○			○	○						
				宛先アドレス	○	接続先IPアドレス	○	○				○					○		○	○		○	○	○	○	○	○	○			○	○						
				宛先ポート番号	○	接続先ポート番号	○	○				○					○		○	○		○	○	○	○	○	○	○			○	○						
				同一フローの送受信バイト数		転送バイト数	○	○				○					○		○	○		○	○	○	○	○	○	○			○	○						
				同一フローの送受信パケット数		転送バイト数	○	○				○					○		○	○		○	○	○	○	○	○	○			○	○						
		ドメインコントローラー	－	ログの名前	○	－	－	－																													
				ソース	○	－	－	－																													
				日時	○	－	－	○																		○	○	○	○									
				イベントID	○	エラーコード	－	○																		○	○	○	○									
				タスクのカテゴリ	○	－	－	－																													
				レベル	○	－	－	－																													
				キーワード	○	イベント名	－	○																		○	○	○	○									
				ユーザー	○	アカウント名	－	○																		○	○	○	○									
				コンピュータ	○	ワークステーション名	－	○																		○	○	○	○									
				オペコード	○	－	－	－																													
		DHCPサーバ	－	日時		－	－	－																													
				ホスト名またはIPアドレス		－	－	－																													
				MACアドレス		－	－	－																													
				状態		－	－	－																													
		DNSサーバ（内部DNS）	－	ログの名前	○	－	－	－																													
				ソース	○	－	－	－																													
				日時	○	－	－	－																													
				イベントID	○	－	－	－																													
				タスクのカテゴリ	○	－	－	－																													
				レベル	○	－	－	－																													
				キーワード	○	－	－	－																													
				ユーザー	○	－	－	－																													
				コンピュータ	○	－	－	－																													
				オペコード	○	－	－	－																													

攻撃経路	5.クラウドサービス

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	ファイルサーバ	－	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	○																○	○										
				イベントID	○	エラーコード	－	○																○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	－	○																○	○										
				ユーザー	○	アカウント名	－	○																○	○										
				コンピュータ	○	ワークステーション名	－	○																○	○										
				オペコード	○	－	－	－																											
		エンドポイント(Windows)	イベントログ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○			
				イベントID	○	エラーコード	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○			
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○			
				ユーザー	○	アカウント名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○			
				コンピュータ	○	ワークステーション名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○			
				オペコード	○	－	－	－																											
			プリフェッチ	日時	○	－	○	○					○				○					○	○					○	○		○	○			
				ファイル名	○	ファイル名	○	○					○				○					○	○					○	○		○	○			
			レジストリ	自動起動のファイル名		ファイル名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				接続したUSBメモリ等の情報		接続デバイス名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
			スクリーンセーバー	起動するスクリーンセーバー		－	－	－																											
			タスクスケジューラ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○									○	○																	
				イベントID	○	エラーコード	○	○									○	○																	
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○									○	○																	
				ユーザー	○	アカウント名	○	○									○	○																	
				コンピュータ	○	ワークステーション名	○	○									○	○																	
				オペコード	○	－	－	－																											
			ファイルの履歴	以前のバージョン情報		－	－	－																											
			プロセスログ	日時		－	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				プロセスID		－	－	－																											
				タイプ		－	－	－																											
				ファイル名		プロセス名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
		エンドポイント(Linux)	メッセージログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			cronログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			カーネルログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	ワークステーション名	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続デバイス名	－	－																											
			セキュリティログ	日時	○	－	－	○															○										○	○	○
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続元IPアドレス	－	○															○										○	○	○
						ログインユーザ名	－	○															○										○	○	○
						認証成否結果	－	○															○										○	○	○
		エンドポイント(OS)	システムコールログ ファイル操作ログ	日時		－	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				ファイルパス		ファイルパス	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
			システムコールログ プロセス操作ログ	日時		－	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				親プロセスID		－	－	－																											
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				コマンドライン		ファイルパス	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
			システムコールログ レジストリ操作ログ	日時		－	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				プロセスID		－	－	－																											
				キー		レジストリキー	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				値		レジストリ値	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				データ		－	－	－																											
			システムコールログ API操作ログ	日時		－	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				プロセスID		－	－	－																											
				API名		API名	○	○					○				○	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○
				APIの引数		－	－	－																											
				APIの戻り値		－	－	－																											

攻撃経路	5.クラウドサービス

ログとして扱うことができる情報						IOC	検知に使用するログ変更	
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）
標準構成機器	内部セグメント	エンドポイント(ブラウザ)	－	日時	○	－	○	○
				URL	○	接続先URL	○	○
		エンドポイント(AntiVirus)	－	スキャン日時	○	－	○	○
				プロセスID	○	－	○	○
				プロセス名	○	－	○	○
				スキャン結果	○	－	○	○

［検知］標的型攻撃関連事象の痕跡

ログ項目	攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
		標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
日時					○																						
URL					○																						
スキャン日時					○				○							○	○										
プロセスID					○				○							○	○										
プロセス名					○				○							○	○										
スキャン結果					○				○							○	○										

攻撃経路	5.クラウドサービス

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	L7FW (NGFW,APFW)	―	日時	○	－	○	○					○				○		○	○						○	○				○	○	○	○	○
				送信元アドレス	○	接続元IPアドレス	○	○					○				○		○	○						○	○				○	○	○	○	○
				送信元ポート番号	○	接続元ポート番号	○	○					○				○		○	○						○	○				○	○	○	○	○
				宛先アドレス	○	接続先IPアドレス	○	○					○				○		○	○						○	○				○	○	○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○					○				○		○	○						○	○				○	○	○	○	○
				同一セッションの送受信バイト数	○	転送バイト数	○	○					○				○		○	○						○	○				○	○	○	○	○
				同一セッションの送受信パケット数	○	転送バイト数	○	○					○				○		○	○						○	○				○	○	○	○	○
				プロトコル	○	通信アプリケーション名	○	○					○				○		○	○						○	○				○	○	○	○	○
				セッション継続時間	○	セッション継続時間	○	○					○				○		○	○						○	○				○	○	○	○	○
				セッションのユーザ名	○	アカウント名	○	○					○				○		○	○						○	○				○	○	○	○	○
				URL	○	接続先URL	○	○					○				○		○	○						○	○				○	○	○	○	○
				ファイル名	○	ファイル名	○	○					○				○		○	○						○	○				○	○	○	○	○
				脅威情報	○	－	－	－																											
		DLP (Data Loss Prevention)		日時	○	－	－	○																							○	○			
				送信元アドレス	○	接続元IPアドレス	－	○																							○	○			
				送信元ポート番号	○	接続元ポート番号	－	○																							○	○			
				宛先アドレス	○	接続先IPアドレス	－	○																							○	○			
				宛先ポート番号	○	接続先ポート番号	－	○																							○	○			
				プロトコル		通信アプリケーション名	－	○																							○	○			
				URL		接続先URL	－	○																							○	○			
				検知キーワード	○	検知キーワード	－	○																							○	○			
				検知ファイル名	○	ファイル名	－	○																							○	○			
		Mailゲートウェイ		日時	○	－	－	○																○	○										
				サーバホスト名	○	－	－	－																											
				メッセージID	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	－	○																○	○										
				メッセージサイズ	○	－	－	－																											
				メッセージ受信者数	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	－	○																○	○										
				ステータス		－	－	－																											
				件名	○	件名	－	○																○	○										
				検知名	○	－	－	－																											
				検知ファイル名	○	－	－	－																											
				検知URL	○	－	－	－																											
		WAF		日時	○	－	－	○																									○	○	○
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	－	○																									○	○	○
				送信元ポート番号	○	接続元ポート番号	－	○																									○	○	○
				宛先アドレス	○	接続先IPアドレス	－	○																									○	○	○
				宛先ポート番号	○	接続先ポート番号	－	○																									○	○	○
				検知タイプ	○	－	－	－																											
				優先度	○	－	－	－																											
				アラートメッセージID	○	－	－	－																											
				アラートメッセージIDに紐づく検知項目（URL含む）	○	－	－	－																											
	DMZ	サンドボックス		日時	○	－	○	○					○				○																		
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	○	○					○				○																		
				送信元ポート番号	○	接続元ポート番号	○	○					○				○																		
				宛先アドレス	○	接続先IPアドレス	○	○					○				○																		
				宛先ポート番号	○	接続先ポート番号	○	○					○				○																		
				プロトコル	○	－	－	－																											
				URL	○	接続先URL	○	○					○				○																		
				ファイル名	○	ファイル名	○	○					○				○																		
				ファイルタイプ	○	ファイル形式	○	○					○				○																		
				ファイルサイズ	○	ファイルサイズ	○	○					○				○																		
				ファイルハッシュ値	○	ファイルハッシュ値	○	○					○				○																		
				悪性判定結果	○	－	－	－																											
				マルウェアのファイル操作ログ	○	－	－	－																											
				マルウェアのプロセス操作ログ	○	－	－	－																											
				マルウェアのレジストリ操作ログ	○	－	－	－																											
				マルウェアのAPI呼出し	○	－	－	－																											
				マルウェアの通信先アドレス/ポート番号	○	－	－	－																											
		改ざん検知		日時	○	－	－	○																○	○										
				ログID	○	－	－	－																											
				改ざん内容(ファイルサイズ変化：旧、新)	○	ファイルサイズ変化	－	○																○	○										
				検知ルール名(追加/削除/編集)	○	イベント名	－	○																○	○										
				検知ファイル名	○	ファイル名	－	○																○	○										
				ユーザ名（検知した操作を行ったOSのアカウント名）	○	アカウント名	－	○																○	○										

攻撃経路	5. クラウドサービス

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																															
									攻撃侵入フェーズ検知ログカテゴリ												拡散フェーズ検知ログカテゴリ												目的遂行フェーズ検知ログカテゴリ							
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名）	検知に使用する基本ログ	検知に使用する基本＋拡張ログ	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み								③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備								⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行											
						検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	（基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	（拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）		標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的が組織利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的が組織利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的が組織利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的が組織利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	ホスト型IPS/IDS		日時	○	－	○	○					○				○		○	○				○	○	○	○	○			○	○	○	○	○				
				ログID	○	－	－	－																																	
				ホストIPアドレス	○	－	○	○					○				○		○	○				○	○	○	○	○			○	○	○	○	○				
				ホスト名	○	－	－	－																																	
				検知ルール	○	－	○	○					○				○		○	○				○	○	○	○	○			○	○	○	○	○				
				検知したファイル操作	○	－	○	○					○				○		○	○				○	○	○	○	○			○	○	○	○	○				
				検知したプロセス操作	○	－	○	○					○				○		○	○				○	○	○	○	○			○	○	○	○	○				
				検知したレジストリ操作	○	－	○	○					○				○		○	○				○	○	○	○	○			○	○	○	○	○				
				検知したAPI呼出し	○	－	○	○					○				○		○	○				○	○	○	○	○			○	○	○	○	○				
	内部セグメント			日時	○	－	－	○																		○	○													
				ログID	○	－	－	－																																	
				ホストIPアドレス	○	－	－	○																		○	○													
				ホスト名	○	－	－	－																																	
				検知ルール	○	－	－	○																		○	○													
				検知したファイル操作	○	－	－	○																		○	○													
				検知したプロセス操作	○	－	－	○																		○	○													
				検知したレジストリ操作	○	－	－	○																		○	○													
				検知したAPI呼出し	○	－	－	○																		○	○													

攻撃経路	6. 保守業者持込機器

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	ファイアウォール（FW）	－	日時	○	－	○	○								○	○		○				○			○					○		○	○	○
				ファイアウォールホスト名	○	－	－	－																											
				ファイアウォールルール名及び番号	○	－	－	－																											
				インバウンドインタフェース	○	－	－	－																											
				アウトバウンドインタフェース	○	－	－	－																											
				MACアドレス	○	－	－	－																											
				パケットサイズ	○	転送バイト数	○	○								○	○		○				○			○					○		○	○	○
				IPパケット優先度（TOS, PREC）	○	－	－	－																											
				IPパケット生存期間（TTL）	○	－	－	－																											
				IPフラグメントパケット識別子（ID）	○	－	－	－																											
				IPフラグメンテーション情報（DFビット）	○	－	－	－																											
				ソースIPアドレス	○	接続元IPアドレス	○	○								○	○		○				○			○					○		○	○	○
				ソースポート番号	○	接続元ポート番号	○	○								○	○		○				○			○					○		○	○	○
				宛先IPアドレス	○	接続先IPアドレス	○	○								○	○		○				○			○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○								○	○		○				○			○					○		○	○	○
				プロトコル	○	－	－	－																											
				TCPウインドウサイズ（WINDOW）	○	－	－	－																											
				TCPフラグ	○	－	－	－																											
		ネットワーク型IPS/IDS	－	日時	○	－	○	○								○	○		○				○			○					○		○	○	○
				送信元アドレス	○	－	○	○								○	○		○				○			○					○		○	○	○
				送信元ポート番号	○	－	○	○								○	○		○				○			○					○		○	○	○
				宛先アドレス	○	－	○	○								○	○		○				○			○					○		○	○	○
				宛先ポート番号	○	－	○	○								○	○		○				○			○					○		○	○	○
				同一セッションの送受信バイト数	○	－	○	○								○	○		○				○			○					○		○	○	○
				同一セッションの送受信パケット数	○	－	○	○								○	○		○				○			○					○		○	○	○
				プロトコル	○	－	○	○								○	○		○				○			○					○		○	○	○
				セッション継続時間	○	－	○	○								○	○		○				○			○					○		○	○	○
				セッションのユーザ名	○	－	○	○								○	○		○				○			○					○		○	○	○
				URL	○	－	○	○								○	○		○				○			○					○		○	○	○
				ファイル名	○	－	○	○								○	○		○				○			○					○		○	○	○
				脅威情報	○	－	○	○								○	○		○				○			○					○		○	○	○
		Webサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				クライアントの識別子	○	－	－	－																											
				認証されたユーザー名	○	ログインユーザ名	－	○																									○	○	○
				日時	○	－	－	○																									○	○	○
				リクエストの最初の行の値	○	接続先URL	－	○																									○	○	○
				最後のレスポンスのステータス	○	ステータスコード	－	○																									○	○	○
				送信されたバイト数（ヘッダーは含まず）	○	転送バイト数	－	○																									○	○	○
				リクエストに含まれるRefererの値	○	リファラ	－	○																									○	○	○
				リクエストに含まれるUser-Agentの値（ブラウザ情報）	○	ユーザエージェント	－	○																									○	○	○
			エラーログ	日時	○	－	－	○																									○	○	○
				エラーの重要度	○	－	－	－																											
				アクセスしたクライアントのIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				メッセージ	○	－	－	－																											
			SSLログ	日時		－	－	－																											
				リモートホスト名		－	－	－																											
				SSLプロトコルバージョン		－	－	－																											
				SSL暗号		－	－	－																											
				リクエストの最初の行の値		－	－	－																											
				送信されたバイト数(ヘッダーは含まず)		－	－	－																											
		APサーバ	アクセスログ	リモートホスト名またはIPアドレス	○	接続元IPアドレス	－	○																									○	○	○
				認証されたユーザー名	○	ログインユーザ名	－	○																									○	○	○
				日時	○	－	－	○																									○	○	○
				メソッドとURL	○	接続先URL	－	○																									○	○	○
				HTTPステータスコード	○	ステータスコード	－	○																									○	○	○
				レスポンスサイズ	○	－	－	－																											
			APログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
			ホストログ	日時	○	－	－	－																											
				ログを生成したスレッド	○	－	－	－																											
				ログレベル	○	－	－	－																											
				カテゴリー名	○	－	－	－																											
				メッセージ	○	－	－	－																											
		DBサーバ	－	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
		プロキシサーバ	アクセスログ	UTCの時間	○	日時	○	○									○		○							○					○				
				継続時間	○	セッション継続時間	○	○									○		○							○					○				
				クライアントのIPアドレス	○	接続元IPアドレス	○	○									○		○							○					○				
				リザルトコード（結果コード）	○	ステータスコード	○	○									○		○							○					○				
				転送バイト数	○	転送バイト数	○	○									○		○							○					○				
				リクエストメソッド	○	リクエストメソッド	○	○									○		○							○					○				
				URL	○	接続先URL	○	○									○		○							○					○				

攻撃経路	6. 保守業者持込機器

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	DMZ	プロキスサーバ	アクセスログ	階層コード	○	接続先IPアドレス	○	○									○		○							○					○				
				HTTPヘッダにリプライされてきたオブジェクトのコンテンツタイプ	○	ファイル形式	○	○									○		○							○					○				
				User-Agent		ユーザエージェント	○	○									○		○							○					○				
			動作ログ（エラーログ・デバッグログ・キャッシュ）	日時	○	－	－	－																											
				メッセージ	○	－	－	－																											
			デバッグログ	日時	○	－	－	－																											
				メッセージ（エラーやデバックメッセージ）	○	－	－	－																											
		DNSサーバ	―	日時		－	○	○									○		○							○		○			○				
				ログカテゴリ		－	－	－																											
				クライアントのIPアドレスとポート番号		接続元IPアドレス	○	○									○		○							○		○			○				
				ファシリティ（ログの分類）		－	－	－																											
				ゾーン情報		リクエストドメイン名	○	○									○		○							○		○			○				
						DNSリクエストレコードタイプ	○	○									○		○							○		○			○				
		メールサーバ	―	日時	○	－	○	○								○								○	○						○				
				サーバホスト名	○	－	－	－																											
				プロセスの情報（プロセスの所有者とプロセスID）	○	－	－	－																											
				メッセージID（Sendmailによって送信されたメッセージに割り当てられたID）	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	○	○								○								○	○						○				
				メッセージサイズ	○	転送バイト数	○	○								○								○	○						○				
				メッセージ優先度	○	－	－	－																											
				メッセージ受信者数	○	メッセージ受信者数	○	○								○								○	○						○				
				メッセージ識別番号	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				サーバデーモン名	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	○	○								○								○	○						○				
				ステータス	○	－	－	－																											
				添付ファイル名		添付ファイル名	○	○								○								○	○						○				
	内部セグメント	スイッチ/ルータ	―	日時		－	○	○								○	○		○			○	○	○	○	○		○			○				
				送信元アドレス	○	接続元IPアドレス	○	○								○	○		○			○	○	○	○	○		○			○				
				送信元ポート番号	○	接続元ポート番号	○	○								○	○		○			○	○	○	○	○		○			○				
				宛先アドレス	○	接続先IPアドレス	○	○								○	○		○			○	○	○	○	○		○			○				
				宛先ポート番号	○	接続先ポート番号	○	○								○	○		○			○	○	○	○	○		○			○				
				同一フローの送受信バイト数		転送バイト数	○	○								○	○		○			○	○	○	○	○		○			○				
				同一フローの送受信パケット数		転送バイト数	○	○								○	○		○			○	○	○	○	○		○			○				
		ドメインコントローラー	―	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○								○						○	○	○	○										
				イベントID	○	エラーコード	○	○								○						○	○	○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○								○						○	○	○	○										
				ユーザー	○	アカウント名	○	○								○						○	○	○	○										
				コンピュータ	○	ワークステーション名	○	○								○						○	○	○	○										
				オペコード	○	－	－	－																											
		DHCPサーバ	―	日時		－	－	－																											
				ホスト名またはIPアドレス		－	－	－																											
				MACアドレス		－	－	－																											
				状態		－	－	－																											
		DNSサーバ（内部DNS）	―	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	－	－																											
				イベントID	○	－	－	－																											
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	－	－	－																											
				ユーザー	○	－	－	－																											
				コンピュータ	○	－	－	－																											
				オペコード	○	－	－	－																											

攻撃経路	6. 保守業者持込機器

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	ファイルサーバ	ー	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○								○								○	○										
				イベントID	○	エラーコード	○	○								○								○	○										
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○								○								○	○										
				ユーザー	○	アカウント名	○	○								○								○	○										
				コンピュータ	○	ワークステーション名	○	○								○								○	○										
				オペコード	○	－	－	－																											
		エンドポイント(Windows)	イベントログ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○				
				イベントID	○	エラーコード	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○				
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○				
				ユーザー	○	アカウント名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○				
				コンピュータ	○	ワークステーション名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○				
				オペコード	○	－	－	－																											
			プリフェッチ	日時	○	－	○	○									○					○	○					○	○		○				
				ファイル名	○	ファイル名	○	○									○					○	○					○	○		○				
			レジストリ	自動起動のファイル名		ファイル名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				接続したUSBメモリ等の情報		接続デバイス名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			スクリーンセーバー	起動するスクリーンセーバー		－	－	－																											
			タスクスケジューラ	ログの名前	○	－	－	－																											
				ソース	○	－	－	－																											
				日時	○	－	○	○									○	○																	
				イベントID	○	エラーコード	○	○									○	○																	
				タスクのカテゴリ	○	－	－	－																											
				レベル	○	－	－	－																											
				キーワード	○	イベント名	○	○									○	○																	
				ユーザー	○	アカウント名	○	○									○	○																	
				コンピュータ	○	ワークステーション名	○	○									○	○																	
				オペコード	○	－	－	－																											
			ファイルの履歴	以前のバージョン情報		－	－	－																											
			プロセスログ	日時		－	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				タイプ		－	－	－																											
				ファイル名		プロセス名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
		エンドポイント(Linux)	メッセージログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			cronログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	－	－	－																											
			カーネルログ	日時	○	－	－	－																											
				ログを出力したホスト名	○	ワークステーション名	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続デバイス名	－	－																											
			セキュリティログ	日時	○	－	○	○								○							○										○	○	○
				ログを出力したホスト名	○	－	－	－																											
				メッセージの出力元	○	－	－	－																											
				メッセージ	○	接続元IPアドレス	○	○								○							○										○	○	○
						ログインユーザ名	○	○								○							○										○	○	○
						認証成否結果	○	○								○							○										○	○	○
		エンドポイント(OS)	システムコールログ ファイル操作ログ	日時		－	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				ファイルパス		ファイルパス	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ プロセス操作ログ	日時		－	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				親プロセスID		－	－	－																											
				プロセスID		－	－	－																											
				プロセス名		プロセス名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				コマンドライン		ファイルパス	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
			システムコールログ レジストリ操作ログ	日時		－	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				キー		レジストリキー	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				値		レジストリ値	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				データ		－	－	－																											
			システムコールログ API操作ログ	日時		－	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				プロセスID		－	－	－																											
				API名		API名	○	○								○	○	○	○		○	○	○	○	○	○		○	○		○		○	○	○
				APIの引数		－	－	－																											
				APIの戻り値		－	－	－																											

攻撃経路	6. 保守業者持込機器

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
標準構成機器	内部セグメント	エンドポイント(ブラウザ)	－	日時	○	－	－	－																											
				URL	○	接続先URL	－	－																											
		エンドポイント(AntiVirus)	－	スキャン日時	○	－	○	○								○	○							○	○										
				プロセスID	○	－	○	○								○	○							○	○										
				プロセス名	○	－	○	○								○	○							○	○										
				スキャン結果	○	－	○	○								○	○							○	○										

攻撃経路	6. 保守業者持込機器

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																									
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ										目的遂行フェーズ検知ログカテゴリ						
									①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ （基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ （拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）		標的型メール送付	USBによる感染	ドライブバイダウンロード 非信頼ドメイン	ドライブバイダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	L7FW (NGFW,APFW)	―	日時	○	－	○	○									○		○							○					○		○	○	○
				送信元アドレス	○	接続元IPアドレス	○	○									○		○							○					○		○	○	○
				送信元ポート番号	○	接続元ポート番号	○	○									○		○							○					○		○	○	○
				宛先アドレス	○	接続先IPアドレス	○	○									○		○							○					○		○	○	○
				宛先ポート番号	○	接続先ポート番号	○	○									○		○							○					○		○	○	○
				同一セッションの送受信バイト数	○	転送バイト数	○	○									○		○							○					○		○	○	○
				同一セッションの送受信パケット数	○	転送バイト数	○	○									○		○							○					○		○	○	○
				プロトコル	○	通信アプリケーション名	○	○									○		○							○					○		○	○	○
				セッション継続時間	○	セッション継続時間	○	○									○		○							○					○		○	○	○
				セッションのユーザ名	○	アカウント名	○	○									○		○							○					○		○	○	○
				URL	○	接続先URL	○	○									○		○							○					○		○	○	○
				ファイル名	○	ファイル名	○	○									○		○							○					○		○	○	○
				脅威情報	○	－	－	－																											
		DLP (Data Loss Prevention)		日時	○	－	－	○																							○				
				送信元アドレス	○	接続元IPアドレス	－	○																							○				
				送信元ポート番号	○	接続元ポート番号	－	○																							○				
				宛先アドレス	○	接続先IPアドレス	－	○																							○				
				宛先ポート番号	○	接続先ポート番号	－	○																							○				
				プロトコル		通信アプリケーション名	－	○																							○				
				URL		接続先URL	－	○																							○				
				検知キーワード	○	検知キーワード	－	○																							○				
				検知ファイル名	○	ファイル名	－	○																							○				
		Mailゲートウェイ		日時	○	－	○	○								○								○	○										
				サーバホスト名	○	－	－	－																											
				メッセージID	○	－	－	－																											
				メッセージの受信者または送信者	○	送信元/送信先メールアドレス/ドメイン	○	○								○								○	○										
				メッセージサイズ	○	－	－	－																											
				メッセージ受信者数	○	－	－	－																											
				プロトコル情報	○	－	－	－																											
				メッセージ送信サーバとIPアドレス	○	接続元IPアドレス	○	○								○								○	○										
				ステータス		－	－	－																											
				件名	○	件名	○	○								○								○	○										
				検知名	○	－	－	－																											
				検知ファイル名	○	－	－	－																											
				検知URL	○	－	－	－																											
		WAF		日時	○	－	－	○																									○	○	○
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	－	○																									○	○	○
				送信元ポート番号	○	接続元ポート番号	－	○																									○	○	○
				宛先アドレス	○	接続先IPアドレス	－	○																									○	○	○
				宛先ポート番号	○	接続先ポート番号	－	○																									○	○	○
				検知タイプ	○	－	－	－																											
				優先度	○	－	－	－																											
				アラートメッセージID	○	－	－	－																											
				アラートメッセージIDに紐づく検知項目（URL含む）	○	－	－	－																											
		サンドボックス		日時	○	－	○	○									○																		
				ログID	○	－	－	－																											
				送信元アドレス	○	接続元IPアドレス	○	○									○																		
				送信元ポート番号	○	接続元ポート番号	○	○									○																		
				宛先アドレス	○	接続先IPアドレス	○	○									○																		
				宛先ポート番号	○	接続先ポート番号	○	○									○																		
				プロトコル	○	－	－	－																											
				URL	○	接続先URL	○	○									○																		
				ファイル名	○	ファイル名	○	○									○																		
				ファイルタイプ	○	ファイル形式	○	○									○																		
				ファイルサイズ	○	ファイルサイズ	○	○									○																		
				ファイルハッシュ値	○	ファイルハッシュ値	○	○									○																		
				悪性判定結果	○	－	－	－																											
				マルウェアのファイル操作ログ	○	－	－	－																											
				マルウェアのプロセス操作ログ	○	－	－	－																											
				マルウェアのレジストリ操作ログ	○	－	－	－																											
				マルウェアのAPI呼出し	○	－	－	－																											
				マルウェアの通信先アドレス/ポート番号	○	－	－	－																											
		改ざん検知		日時	○	－	○	○								○								○	○										
				ログID	○	－	－	－																											
				改ざん内容(ファイルサイズ変化：旧、新)	○	ファイルサイズ変化	○	○								○								○	○										
				検知ルール名(追加/削除/編集)	○	イベント名	○	○								○								○	○										
				検知ファイル名	○	ファイル名	○	○								○								○	○										
				ユーザ名（検知した操作を行ったOSのアカウント名）	○	アカウント名	○	○								○								○	○										

攻撃経路	6. 保守業者持込機器

ログとして扱うことができる情報						IOC	検知に使用するログ変更		[検知]標的型攻撃関連事象の痕跡																										
									攻撃侵入フェーズ検知ログカテゴリ										拡散フェーズ検知ログカテゴリ											目的遂行フェーズ検知ログカテゴリ							
区分	機器設置場所	機器	種別	ログ項目	デフォルトの設定で出力される項目	痕跡名（IOC名） 検知に使用する痕跡のみを記載（セキュリティ機器による検知結果・被害分析に使用する痕跡については除外）	検知に使用する基本ログ（基本ログは、攻撃の侵入フェーズを広く捉えるため取得が推奨されるログ）	検知に使用する基本ログ＋拡張ログ（拡張ログは、攻撃の拡散フェーズ及び目的遂行フェーズを広く捉えるため取得が推奨されるログ）	①公開情報あるいは別の攻撃から得たと考えられるターゲットの情報収集	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み							③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備							⑤C2ホストとの積極的な通信			⑥本格的な攻撃実行						
										標的型メール送付	USBによる感染	ドライブダウンロード 非信頼ドメイン	ドライブダウンロード 信頼ドメイン（標的組織が利用する外部サービス）	不正コード混入ソフトウェアの実行	外部にオープンなサービス・ホストの脆弱性	持ち込み機器（標的組織に属さない人間が持ち込む機器）を介した侵入	マルウェア初期活動	再起動時の実行設定による常駐化	バックドア通信経路確保 非信頼ドメイン経由	バックドア通信経路確保 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した権限昇格	他者認証情報取得	内部ネットワーク調査	他コンピュータに配置するマルウェアの設置	他のコンピュータ・システムへの展開活動	検知回避を施したC2通信確立とビーコン通信 非信頼ドメイン経由	検知回避を施したC2通信確立とビーコン通信 信頼ドメイン（標的組織が利用する外部サービス）経由	内部のコンピュータシステムの挙動監視	取得情報のパッケージ化と暗号化 標的組織内ホストの情報窃取	取得情報のパッケージ化と暗号化 クラウドサービスからの情報窃取	検知回避を施した外部への送信 非信頼ドメイン経由	検知回避を施した外部への送信 信頼ドメイン（標的組織が利用する外部サービス）経由	脆弱性を悪用した情報窃取	脆弱性を悪用した情報改ざん	脆弱性を悪用したサービス停止
対策強化機器	DMZ	ホスト型IPS/IDS		日時	○	－	○	○								○	○		○					○	○	○		○			○		○	○	○
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	○	○								○	○		○					○	○	○		○			○		○	○	○
				ホスト名	○	－	－	－																											
				検知ルール	○	－	○	○								○	○		○					○	○	○		○			○		○	○	○
				検知したファイル操作	○	－	○	○								○	○		○					○	○	○		○			○		○	○	○
				検知したプロセス操作	○	－	○	○								○	○		○					○	○	○		○			○		○	○	○
				検知したレジストリ操作	○	－	○	○								○	○		○					○	○	○		○			○		○	○	○
				検知したAPI呼出し	○	－	○	○								○	○		○					○	○	○		○			○		○	○	○
	内部セグメント			日時	○	－	○	○								○								○	○										
				ログID	○	－	－	－																											
				ホストIPアドレス	○	－	○	○								○								○	○										
				ホスト名	○	－	－	－																											
				検知ルール	○	－	○	○								○								○	○										
				検知したファイル操作	○	－	○	○								○								○	○										
				検知したプロセス操作	○	－	○	○								○								○	○										
				検知したレジストリ操作	○	－	○	○								○								○	○										
				検知したAPI呼出し	○	－	○	○								○								○	○										