攻撃カード(表)

1．1 (−1)
初期偵察：発掘

システム情報の解明のため，対象から返答される未処理の例外やエラーメッセージを調査

1．2 (−1)
初期偵察：傍受

システムにアクセス可能な媒体を介してデータを傍受

1．3 (−1)
初期偵察：フットプリンティング

システムまたはアプリケーションが送信する識別可能な情報を調査

1．4 (−1)
初期偵察：プロトコル分析

システムが使用する通信プロトコルの情報を調査・解読

1．5 (−1)
初期偵察：フィンガープリント

標的からの出力と既知のインジケータを比較し，標的を特定

1．6 (−1)
初期偵察：情報抽出

ソーシャルエンジニアリングにより，標的組織及び個人に関する重要な情報を取得

2．1 (−1)
ツール開発/取得

攻撃の効率化を図るため，ツールを開発または取得し，使用

3．1 (−1)
配送：コンテンツスプーフィング

フィッシングサイト等の偽装コンテンツを表示

攻撃カード（裏）

攻撃カード（Type B） 	攻撃カード（Type B） 	攻撃カード（Type B） 	攻撃カード（Type B） 
攻撃カード（Type B） 	攻撃カード（Type B） 	攻撃カード（Type B） 	攻撃カード（Type B） 

攻撃カード(表)

3. 2 (-1) 配送:アイデンティティスプーフィング 窃取またはなりすました認証情報を使用し, メッセージや署名付きファイルを送付	3. 3 (-1) 配送:リソースロケーションスプーフィング ブラウザに偽のアドレスを表示する等により利用者が意図しない場所からリソースを取得	3. 4 (-1) 配送:アクションスプーフィング 第2の目に見えないインターフェースを利用して意図しない動作を実行	3. 5 (-1) 配送:人間の行動を操作 人間の心理につけこみ, 標的から情報を収集または標的を操作して利益を獲得
4. 1 (-2) 初期侵害:防御回避 シグネチャベースによる検出回避のため, バイナリパディングによりファイルハッシュを変更	4. 2 (-2) 初期侵害:防御回避 形跡を消すため, レジストリ・コマンドヒストリ・イベントファイル・マルウェア自身等を削除	4. 3 (-2) 初期侵害:防御回避 OSやアプリケーションの機能を利用し, セキュリティツールによる悪意のある動作の検出を防止	4. 4 (-2) 初期侵害:防御回避 悪意のあるコードを難読化・暗号化し, コードの分析から回避

攻撃カード（裏）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード（表）

4．5 （-2） 初期侵害：防御回避 悪意のあるプログラムのタイムスタンプを改ざんし，分析から回避	4．6 （-2） 初期侵害：防御回避 セキュリティツールを無効化し，悪意のあるアクティビティの検出を回避	4．7 （-2） 初期侵害：実行 ネットワーク管理目的で使用するサードパーティアプリケーションやソフトウェア開発システムを悪用し，制御コードを実行	4．8 （-2） 初期侵害：実行 開発，デバッグ，リバースエンジニアリングを支援するソフトウェア関連ユーティリティを悪用し，悪意のあるコードを実行
4．9 （-2） 初期侵害：実行 標的が使用するOSやアプリケーションの機能・仕組みを悪用し，標的を制御するコードを実行	5．1 （-3） 誤用/特権昇格 動的ライブラリの仕組みを利用し，他のプロセスに悪意のあるコードをロードさせ，実行	5．2 （-3） 誤用/特権昇格 不適切なファイルシステムのパーミッションを利用し，管理者権限で起動するプロセスをユーザ権限で改ざん	5．3 （-3） 誤用/特権昇格 不適切なレジストリのパーミッションを利用し，管理者権限で起動するプロセスを登録

攻撃カード（裏）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード(表)

5．4 （-3） 誤用/特権昇格 資格情報アクセス技術を使用して，特定アカウントの資格情報を窃取	5．5 （-3） 誤用/特権昇格 OSやアプリケーションの機能または脆弱性を悪用し，アカウントの権限を昇格	6．1 （-3） 内部偵察：資格情報アクセス アカウント情報が保存されているファイルや履歴を調査	6．2 （-3） 内部偵察：資格情報アクセス ネットワークスニファにより，非暗号化通信で送信される資格情報を収集
6．3 （-3） 内部偵察：資格情報アクセス アカウントへのアクセスのため，総当たり攻撃を使用	6．4 （-3） 内部偵察：資格情報アクセス アクセス権限を持った攻撃者が攻撃に使用するアカウントを作成	6．5 （-3） 内部偵察：資格情報アクセス 端末に保存されている秘密鍵にアクセス	6．6 （-3） 内部偵察：発見 レジストリにアクセスし，システム情報またはインストールされているソフトウェアの情報を発見

攻撃カード（裏）

攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 
攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 

攻撃カード（表）

6．7 （-3） 内部偵察：発見 追加攻撃またはシステム環境の詳細を知るため，端末に接続されている周辺機器を発見	7．1 （-4） 侵入拡大 システムの認証の仕組みを悪用し，ネットワーク上の別端末を侵害	7．2 （-4） 侵入拡大 リムーバブルメディアの自動実行機能を悪用し，クローズドシステム等にマルウェアを拡散	7．3 （-4） 侵入拡大 ソフトウェアの脆弱性を突きリモートシステム上でコマンドやバイナリを実行し，システム侵害を拡大
7．4 （-4） 侵入拡大 標的が使用するOSやアプリケーションの機能・仕組みを悪用し，システム侵害を拡大	8．1 （-4） 持続性確立 悪意のあるファイルに隠れファイル・ディレクトリ属性を付与し，利用者から隠蔽	8．2 （-4） 持続性確立 既存のファイルやレジストリ情報を変更し，悪意のあるプログラムやスクリプトを継続的に実行	8．3 （-4） 持続性確立 OSの起動時に動作するプロセス・スクリプト一覧に悪意のあるプログラム・スクリプトを追加

攻撃カード（裏）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード
（Type B）

攻撃カード（表）

8．4 （-4） 持続性確立 OSやアプリケーションの設定を変更し，システムアクセスへの永続性を確保	8．5 （-4） 持続性確立 OSの下層で動作するブートキットを悪用して，永続的にシステムにアクセス	8．6 （-4） 持続性確立 リモートサービスを使用して持続的にネットワークにアクセス	9．1 （-5） 任務目的実行：収集 標的で使用可能なAPIにより音声やクリップボード，スクリーンキャプチャなどの情報を収集
9．2 （-5） 任務目的実行：収集 標的の内部情報を効率よく収集するために自動化技術を活用	9．3 （-5） 任務目的実行：収集 標的内のローカルドライブ・リモートドライブ・リムーバブルメディアから情報を収集	9．4 （-5） 任務目的実行：情報流出 データの暗号化・圧縮・転送サイズ制限を行い，標的に気づかれないように情報を取得	9．5 （-5） 任務目的実行：情報流出 任意の通信プロトコルを使用し，情報を収集

攻撃カード（裏）

攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 
攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 

攻撃カード(表)

9．6 （−5） 任務目的実行：情報流出 外部デバイス，携帯電話，MP3プレイヤーなどを使用し，情報を収集	9．7 （−5） 任務目的実行：遠隔操作 リムーバブルメディアによりクローズネットワークのホストを侵害し，コマンド及び制御トラフィックを実行	9．8 （−5） 任務目的実行：遠隔操作 コンピュータ上の通信ポートを介して，コマンドおよび制御トラフィックを送信	9．9 （−5） 任務目的実行：遠隔操作 暗号プロトコルまたはアルゴリズムを使用して，コマンドおよび制御トラフィックを隠蔽

攻撃カード（裏）

攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 
攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B） 	攻撃カード （Type B）