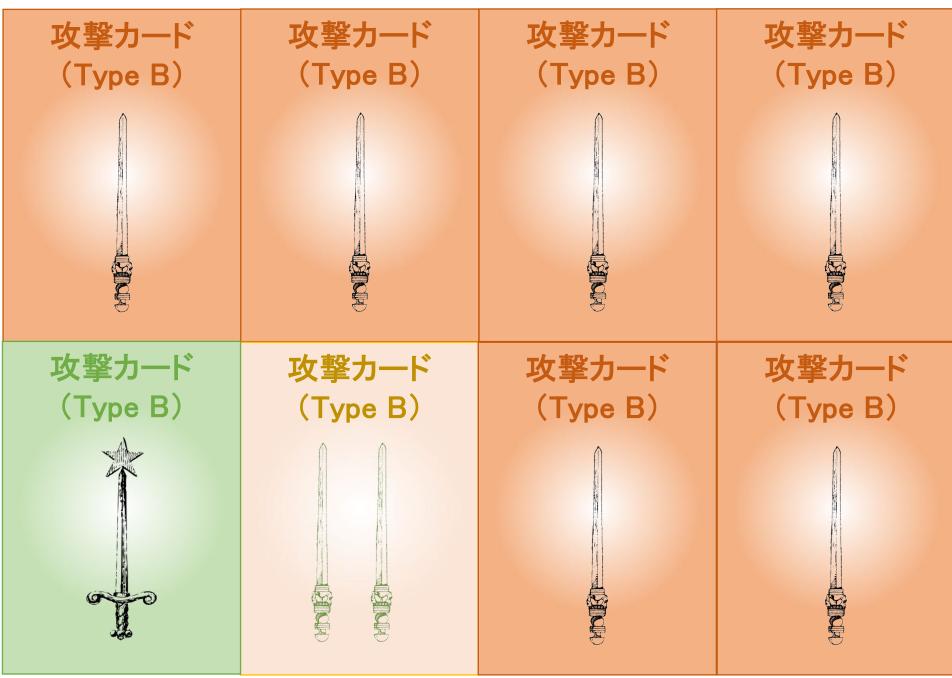
攻撃カード(表) 1.3 (-1)

1. 1 (-1) 初期偵察:発掘	1. <mark>2 (−1)</mark> 初期偵察∶傍受	1. 3 (-1) 初期偵察:フットプリン ティング	1. 4 (-1) 初期偵察:プロトコル分 析
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	システムにアクセス可能 な媒体を介してデータを 傍受	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	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	1. 6 (−1) 初期偵察:情報抽出	<mark>2. 1 (−1)</mark> ツール開発/取得	3. 1 (-1) 配送:コンテンツスプー フィング
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	ソーシャルエンジニアリリングにより, 標的組織及び個人に関する重要な情報を取得	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	フィッシングサイト等の 偽装コンテンツを表示



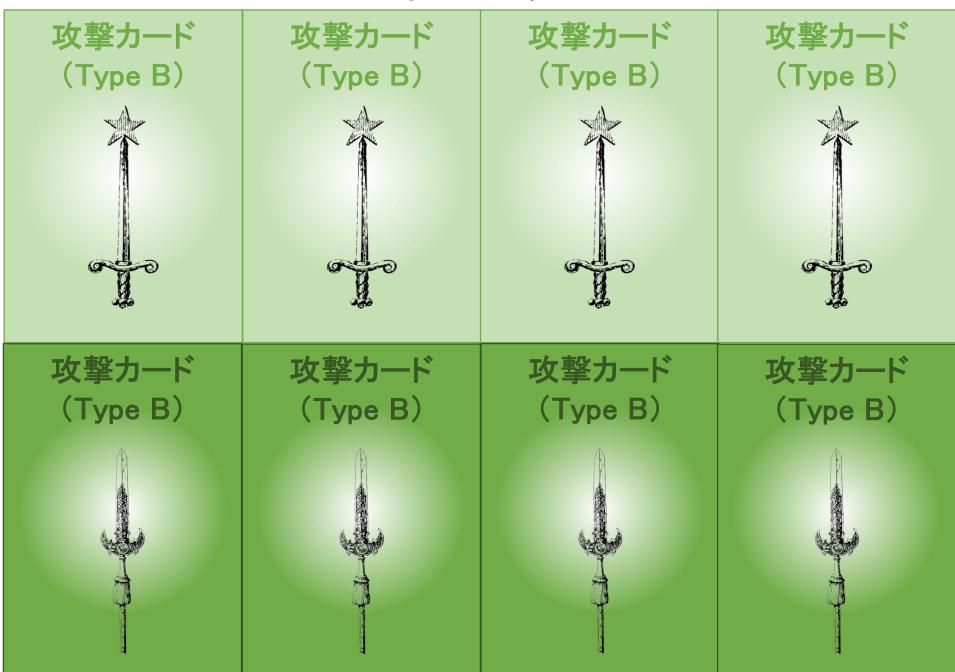
3. 4 (-1)

3. 3 (-1)

3. 5 (-1)

3. 2 (-1)

配送:アイデンティティス	配送:リソースロケー	配送:アクションスプー	配送:人間の行動を操作
プーフィング	ションスプーフィング	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	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	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	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)	4. 2 (-2)	4. 3 (-2)	4. 4 (-2)
初期侵害:防御回避	初期侵害:防御回避	初期侵害:防御回避	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	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	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	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



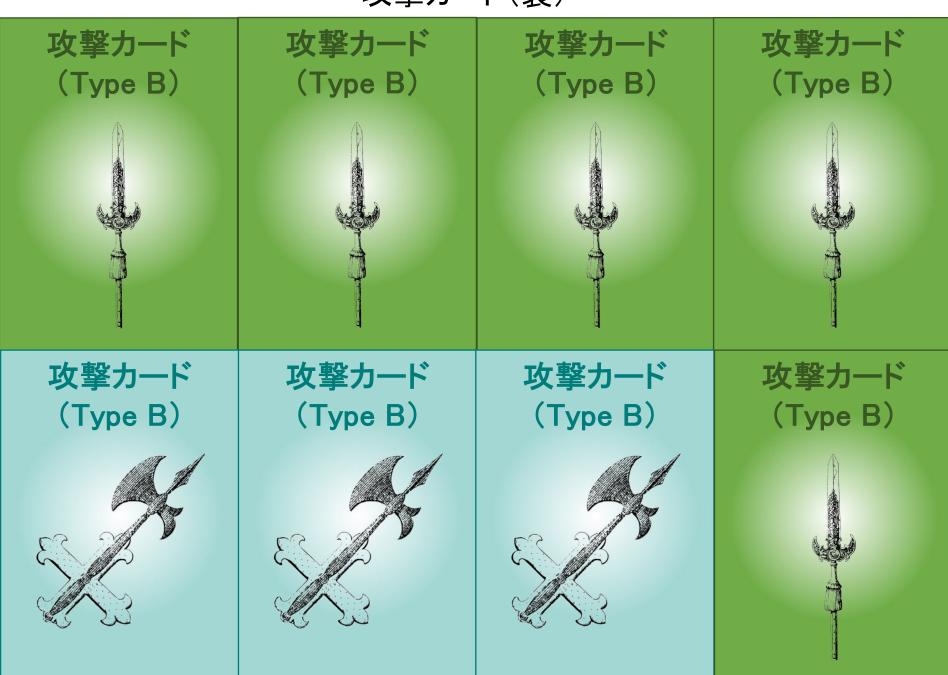
4. 7 (-2)

4. 8 (-2)

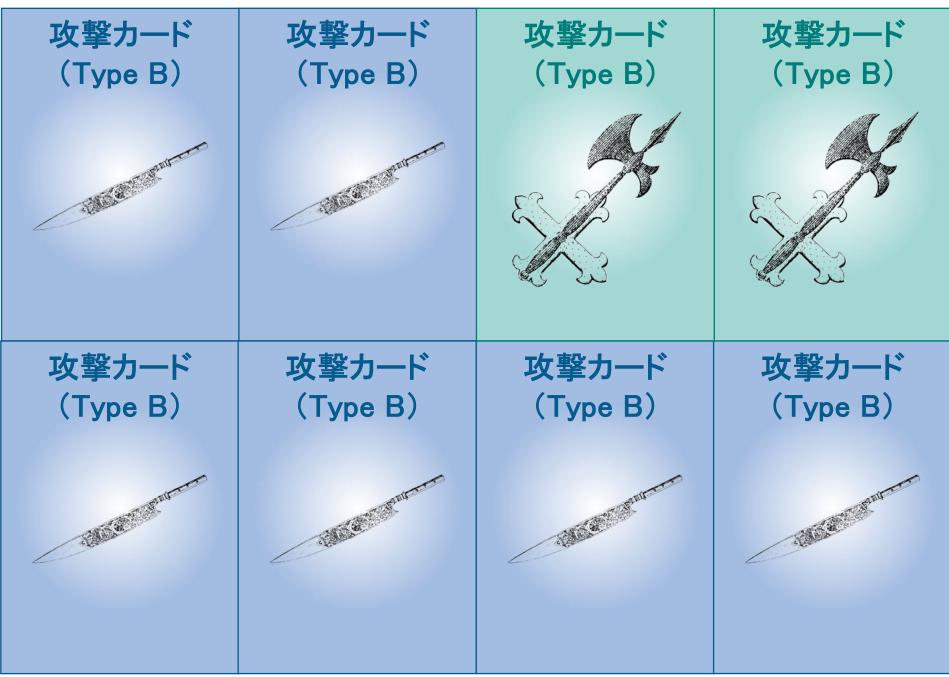
4. 6 (-2)

4. 5 (-2)

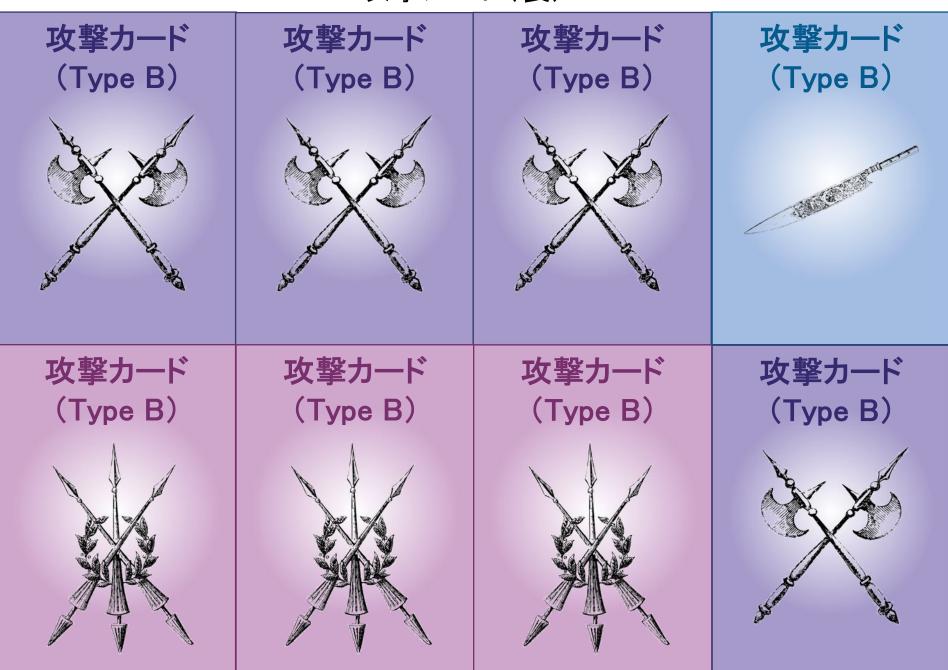
初期侵害:防御回避	初期侵害:防御回避	初期侵害:実行	初期侵害:実行
悪意のあるプログラム のタイムスタンプを改ざ んし, 分析から回避	セキュリティツールを無効化し、悪意のあるアク ティビティの検出を回避	ネットワーク管理目的で使用するサードパーティアプリケーションやソフトウェア開発システムを悪用し、制御コードを実行	開発, デバッグ, リバー スエンジニアリングを支 援するソフトウェア関連 ユーティリティを悪用し, 悪意のあるコードを実行
4. 9 (-2) 初期侵害:実行	5. 1 (-3) 誤用/特権昇格	5. 2 (-3) 誤用/特権昇格	5. 3 (-3) 誤用/特権昇格
標的が使用する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	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	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	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



5. 4 (-3) 誤用/特権昇格	5. 5 (-3) 誤用/特権昇格	6. 1 (-3) 内部偵察:資格情報ア クセス	6. 2 (-3) 内部偵察: 資格情報ア クセス
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	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	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	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	6. 4 (-3) 内部偵察: 資格情報ア クセス	6.5 (-3) 内部偵察:資格情報ア クセス	6. 6 (-3) 内部偵察:発見
アカウントへのアクセス のため, 総当たり攻撃を 使用	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	端末に保存されている 秘密鍵にアクセス	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



6. 7 (-3)	7. 1 (-4)	7. 2 (-4)	7.3 (-4)
内部偵察:発見	侵入拡大	侵入拡大	侵入拡大
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	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	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	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)	8. 1 (-4)	8. 2 (-4)	8.3 (-4)
侵入拡大	持続性確立	持続性確立	持続性確立
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	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	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	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



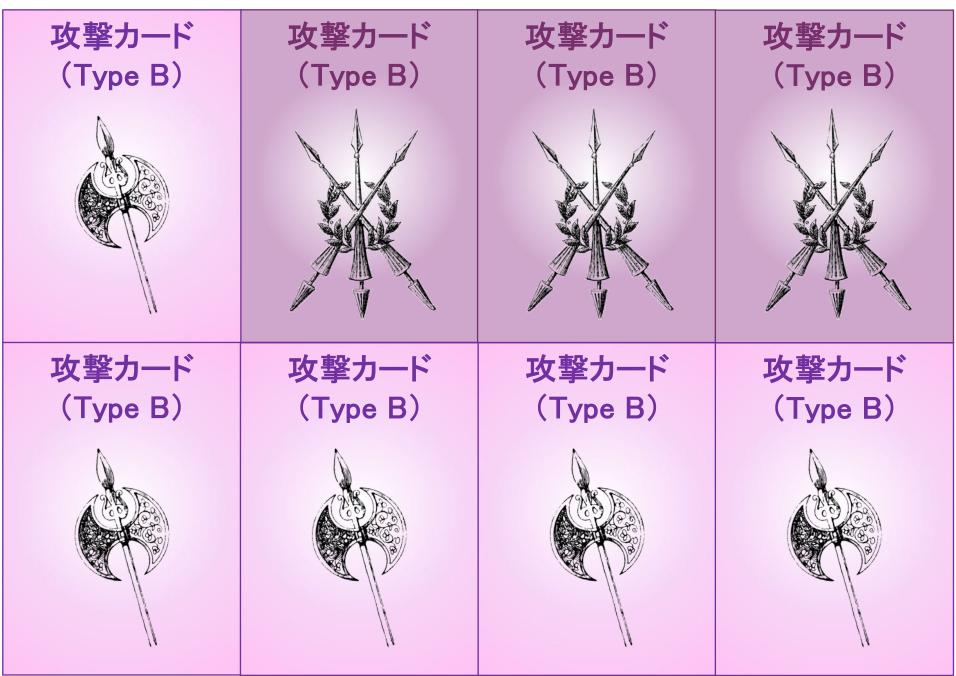
8. 5 (-4)

8. 4 (-4)

8. 6 (-4)

9. 1 (-5)

持続性確立	持続性確立	持続性確立	任務目的実行:収集
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	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	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	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	9.3 (-5) 任務目的実行:収集	9. 4 (-5) 任務目的実行:情報流出	9. 5 (-5) 任務目的実行:情報流出
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	標的内のローカルドライブ・リモートドライブ・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	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	任意の通信プロトコルを 使用し、情報を収集



		-	
9. 6 (-5) 任務目的実行:情報流出	9. 7 (-5) 任務目的実行:遠隔操作	9. 8 (-5) 任務目的実行:遠隔操作	9. 9 (-5) 任務目的実行:遠隔操作
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	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	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	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

