攻撃カード（表）

No.1 （−3） 未保護の新規システムを継続的にスキャンし，脆弱性を悪用	No.2 （−3） パッチ処理が未完で，セキュリティ設定が不適切なクライアントソフトウェアの脆弱性を悪用	No.3 （−3） 継続的に脆弱性の高いソフトウェアをスキャンし，脆弱性を利用して対象マシンを侵害	No.4 （−3） マルウェア感染したマシンから他の脆弱なマシンを特定し，侵害
No.5 （−3） システムの脆弱なデフォルト設定を悪用	No.6 （−3） 継続的な脆弱性評価や修正が未実施で，重要パッチが未適用のシステムの脆弱性を悪用	No.7 （−3） 対策の有効性測定や継続的改善が未実施の標的を攻撃	No.8 （−3） 悪意あるコードにより対象マシンを侵害し，機密データを取得

攻撃カード（裏）

攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 
攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 

攻撃カード（表）

No.9 （−3） 業務に不必要なリモートアクセス可能なサービスを詳細にスキャンし，攻撃ルートを用意することでセキュリティを侵害	No.10 （−3） SQL インジェクション，クロスサイトスクリプティングなどにより脆弱なアプリケーションソフトウェアを悪用	No.11 （−3） 無線アクセスポイントや無線クライアントシステムの脆弱性を悪用し，内部ネットワークに侵入	No.12 （−3） ソーシャルエンジニアリングによりユーザやシステム管理者を欺瞞
No.13 （−3） 一時的に例外を認めたが修正されず，セキュリティ設定が脆弱なネットワークデバイスを悪用	No.14 （−3） フィッシングメールにより対象マシン上で悪意あるコードを管理者権限で実行	No.15 （−3） インターネットからアクセス可能なDMZ上のシステム経由で内部ネットワークの深部まで侵入	No.16 （−3） 未保護の接続，脆弱なフィルタリング設定などの不適切なネットワークアーキテクチャの設定を悪用

攻撃カード（裏）

攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 
攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 

攻撃カード（表）

No.17 （-3） ログ収集及びログレビューが未実施の標的システム上で，長時間，検知されることなく活動	No.18 （-3） 機密情報を適切に特定せず未保護な組織の機密文書にアクセス	No.19 （-3） 一時雇用者，請負業者，元従業員などが残した非アクティブアカウントを悪用	No.20 （-3） パスワード推測，パスワード解析，権限昇格の脆弱性を突く攻撃により管理者権限を取得し，他のマシンにも被害を拡大
No.21 （-3） システムの内部にアクセスし，検知されることなく機密情報を収集	No.22 （-3） システムを侵害し，重要データを改ざんすることで組織の信頼性を侵害	No.23 （-3） 効果的対応能力を持たない組織内で検知されずに活動を継続	No. （-3）

攻撃カード（裏）

攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 
攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A） 	攻撃カード（Type A）