## 攻撃カード(表)

No.3 (-3)

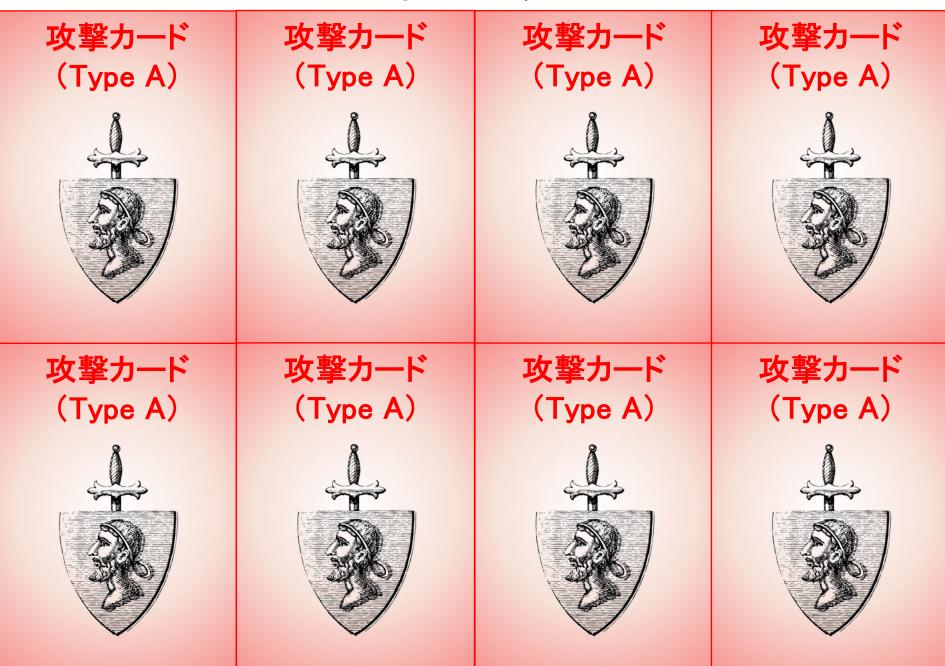
No.4 (-3)

No.2 (-3)

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	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	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	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)	No.6 (-3)	No.7 (-3)	No.8 (-3)
システムの脆弱なデフォ ルト設定を悪用	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	対策の有効性測定や継 続的改善が未実施の標 的を攻撃	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(表)

No.11 (-3)

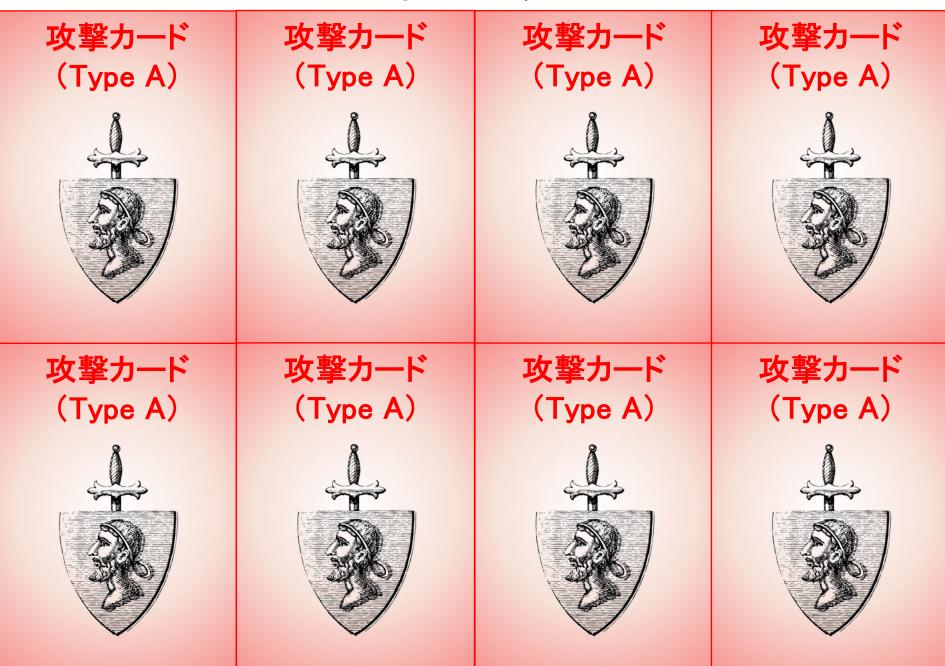
No.12 (-3)

No.10 (-3)

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	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	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	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)	No.14 (-3)	No.15 (-3)	No.16 (-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	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	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	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(表)

No.19 (-3)

No.20 (-3)

No.18 (-3)

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	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	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	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)	No.22 (-3)	No.23 ( <del>-3</del> )	No. ( <del>-3</del> )
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	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	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	

#### 攻撃カード(裏)

