

脅威と対策表(ネットワーク機器のobjセキュリティ)

脅威		対策		通信セキュリティ								否認防止	システムセキュリティ	
				エンティティ間の認証				守秘性	データインテグリティ	証拠収集とアーカイビング	不正な用法/不適切な用法		サービス妨害	
				ユーザ名/パスワード	ユーザ名/ワンタイム	ユーザ名/チャレンジ	IPSec + 自動鍵管理/鍵配布							
				共有鍵	証明書(公開鍵)	暗号ペイロード(ESP)	メッセージ認証	認証と認可	インGRESSフィルタリング					
盗聴	待ち伏せ攻撃	盗聴	T1. 平文伝送	×	-	-	-	-	◎	-	-	-	-	
		パスワード盗聴	T2. 共有パスワード	×	◎	◎	◎	◎	◎	△	△	△	△	
		オフラインでの暗号技術的攻撃	T3. 辞書攻撃	×	×	×	◎	◎	◎	◎	△	△	△	△
			T4. 推定攻撃	×	×	×	◎	◎	◎	◎	△	△	△	△
			T5. NIS、解読ツールの存在	×	×	×	◎	◎	◎	◎	△	△	△	△
	トポロジー	パス外からの攻撃	T6. トポロジーの破壊	△	△	△	◎	◎	◎	◎	△	△	△	△
			T7. 同一リンク上の判別	△	△	△	◎	◎	◎	◎	△	△	△	△
		ファイアウォール	T8. 常用プロトコルでの攻撃	△	△	△	◎	◎	◎	◎	◎	△	△	△
			T9. 内部の脅威	△	△	△	◎	◎	◎	◎	◎	△	△	△
不適切な用法	ウィルス	T10. 情報の不正コピー	△	◎	◎	◎	◎	◎	◎	△	△	△		
侵入	積極的な攻撃	中間者	T11. セッション乗取り	△	△	△	◎	◎	◎	◎	△	△	△	
		T12. ARP詐称(IPアドレス詐称)	△	◎	◎	◎	◎	◎	◎	◎	△	△	△	
	否認防止	T13. アクセスの証明	△	△	△	△	△	△	△	△	△	△	△	
改ざん	積極的な攻撃	メッセージ挿入	T14. TCP SYNパケット挿入	△	△	△	△	△	◎	◎	△	△	△	
			T15. TLS RST偽装	△	△	△	△	△	◎	◎	△	△	△	
		メッセージ削除 メッセージ変更	T16. シーケンス番号推測攻撃	△	△	△	◎	◎	◎	◎	△	△	△	
			T17. MACチェック未使用	△	△	△	△	△	◎	◎	△	△	△	
	不適切な用法	ウィルス	T18. ホストtoホストSA	△	△	△	△	△	◎	◎	△	△	△	
			T19. ウィルス混入後の転送	△	◎	◎	◎	◎	◎	◎	△	△	△	
妨害	積極的な攻撃	リプレイ攻撃	T20. 情報の破壊・書換え	△	◎	◎	◎	◎	◎	◎	△	△	△	
			T21. メッセージ盗聴後再送	△	△	△	◎	◎	◎	◎	△	△	△	
			T22. 自動発呼による再送	△	△	△	◎	◎	◎	◎	△	△	◎	
	妨害攻撃	Blind妨害	T23. TCPSYNフラッド攻撃	△	△	△	◎	◎	◎	◎	△	△	◎	
			T24. DDoS	△	△	△	◎	◎	◎	◎	◎	△	◎	
		分散型妨害	T25. 災害・物理的破壊	△	△	△	△	△	△	△	△	△	△	△
			T26. 不正な用法	△	◎	◎	◎	◎	◎	◎	◎	◎	◎	△
T27. 不適切な用法	△	◎	◎	◎	◎	◎	◎	◎	◎	◎	△			
T28. なりすまし	△	◎	◎	◎	◎	◎	◎	◎	◎	◎	△			
T29. サービス中断による不正処理	△	△	△	△	△	◎	◎	◎	△	△	△			
T30. 改ざん	△	◎	◎	◎	◎	◎	◎	◎	◎	◎	△			
T31. 過失・盗難・紛失	△	△	△	△	△	△	△	△	△	△	△			