脅威の定義

類型	脅威	解説
T1	平文伝送	送受信データが通信路上を平文で伝送されているために、送受信データを盗聴することにより情報漏洩が起こる可能性がある。
T2	共有ﾊﾟｽﾜｰﾄﾞ	エンティティ認証に使用されるパスワードが平文で伝送されているため、送受信データを盗聴することによりパスワードを取得される可能性がある。その結果として、取得したパスワードを利用してサーバにログインされる危険性がある。
T3	辞書攻撃	「平文」と「暗号文」および「暗号文」と「ハッシュ関数」を取得している場合に、攻撃者は正しい応答をもたらす秘密鍵(パスワード)を発見するまで、(辞書ファイルのような)よくある単語リストから選択した文字列を秘密鍵の候補として試行する。その結果として、エンティティ間の認証に使用される秘密鍵が漏洩する可能性がある。
T4	推定攻撃	「平文」と「暗号文」および「暗号文」と「ハッシュ関数」を取得している場合に、攻撃者は正しい応答をもたらす秘密鍵(パスワード)を発見するまで、すべての共有された秘密鍵(パスワード)の候補を試行する。その結果として、エンティティ間の認証に使用される秘密鍵が漏洩する可能性がある。
T5	NIS,解読ﾂｰﾙの存在	「平文」と「暗号文」および「暗号文」と「ハッシュ関数」を取得している場合に、攻撃者は正しい応答をもたらす秘密鍵(パスワード)を発見するまで、すべての共有された秘密鍵(パスワード)の候補を試行を解読ツールを用いて実施する。解読ツールを用いることにより、秘密鍵を判別するために要する時間を短縮することができる。その結果として、エンティティ間の認証に使用される秘密鍵が漏洩する可能性がある。
T6	ﾄﾎﾟﾛｼﾞｰの破壊	攻撃者は、データを送受信するためにトポロジーを破壊して、攻撃者自身をパス上に配置します。その結果として、盗聴やIPヘッダの改ざん等のより多くの攻撃をしかけることが可能になるため、パス上を送受信されるデータが攻撃される危険性が増大する。
T7	同一ﾘﾝｸ上の判別	パス上の特殊ケースとして、攻撃者が同一リンク上ローカルネットワーク上に存在する場合がある。ローカルネットワーク上に位置するホストと、そうでないホストを区別できない場合に外部ネットワークからの攻撃を許してしまう可能性が増大する。
T8	常用ﾌﾟﾛﾄｺﾙでの攻撃	HTTP や SMTP, SOAP などの一般的にファイアウォールを通過するプロトコルにおける攻撃に対して暗号化ペイロードやメッセージ認証の対策で影響を軽減しない場合に、LANセキュリティの侵害を引き起こす危険性がある。
T9	内部の脅威	攻撃者が内部ネットワークに存在している場合には、通常、ネットワークを送受信されるいかなるデータを読むこと、変更すること、および削除することが可能となる。このような攻撃者からの盗聴、改ざん、削除などの攻撃に耐えうるよう対策すべきである。
T10	情報の不正ｺﾋﾟｰ	ウイルスには、特定の日になると、というような特定の条件のもとでのみ動作する「時限爆弾」があり、特定の関連したプログラムが動作しない限り、システム中に隠れているものも存在する。さらに常時動作しており、危害を加える期をうかがっているものもある。また巧妙なウイルスには、単にシステムの設定を変更したり、隠れてしまうものもある。
T11	ｾｯｼｮﾝ乗っ取り	エンティティ間の認証を行わないと、確立したセッションにおいて攻撃者が中間者が入り込むことが可能となる。攻撃者は、一方のエンティティから送信されたパケットを盗聴し、対象サーバに到達する前にパケットを挿入することで、中間者攻撃を成功させることが可能となる。
T12	ARP詐称(IPｱﾄﾞﾚｽ詐称)	攻撃者は LAN 上のホストの ARP テーブルの書き換えを行うことにより、送信者が意図した宛先ではなく攻撃者にパケットを送信させることができる。
T13	ｱｸｾｽの証明	否認防止とは、一般的に、送信者が送信事実を否定したり、受信者が受信事実を否定したりすることである。攻撃者がこれらの事実を否定することを防止することはできないが、通信が行われた記録を適切に収集・管理することにより、証拠を提出して、これらの事象が発生していることで対応することが可能となる。

脅威の定義

類型	脅威	解説
T14	TCP SYNﾊﾟｹｯﾄ挿入	メッセージ挿入攻撃において、攻撃者は、いくつかの選択された属性についてメッセージを偽装し、ネットワーク中に挿入する。攻撃者は、これらの挿入されたメッセージの応答を受け取る必要がないため、これらの攻撃は送信元アドレスを偽造されることがしばしばある。
T15	TLS RST偽装	トランスポート層のトラフィックセキュリティの対策を実施していない状況では、メッセージ挿入攻撃を実施することで TCP コネクションをリセットすることが可能となる。その結果として、TLS/SSL コネクションの切断が行われる可能性がある。
T16	ｼｰｹﾝｽ番号推測攻撃	攻撃者は標的に信頼されたホストの口を塞ぎ、標的に話しかける際に、信頼されたホストの IP アドレスを偽装して、次に最初に使われるシーケンス番号を推測することに基づく 3 ウェイハンドシェイクを完結させる。標的への通常のコネクションは シーケンス番号の状態の情報を集めるのに使用され、このシーケンス全体が、アドレスに基づく認証と組み合わされて、攻撃者が標的となるホスト上でコマンドを実行できるようになる可能性がある。
類型	**脅威**	**解説**
T17	MACﾁｪｯｸ未使用	メッセージ変更攻撃において、攻撃者は、回線からメッセージを削除し、それを変更し、ネットワーク中に再投入する。攻撃者がメッセージ中にデータを送ることを望むが、同時に、その一部を変更することを望む場合、この種の攻撃は特に有効となる。
T18	ﾎｽﾄtoﾎｽﾄSA	ホスト間での認証において暗号化されたメッセージのやり取りを実施していると、攻撃者が利用できるホストに到達した際に複号されたメッセージを、同一ホスト内の別のポートに転送することにより、暗号文を参照される可能性がある。
T19	ｳｲﾙｽ混入後の転送	ウイルスには、特定の日になると、というような特定の条件のもとでのみ動作する「時限爆弾」があり、特定の関連したプログラムが動作しない限り、システム中に隠れているものも存在する。さらに常時動作しており、危害を加える期をうかがっているものもある。また巧妙なウイルスには、単にシステムの設定を変更したり、隠れてしまうものもある。
T20	情報の破壊・書換え	ウイルスには、特定の日になると、というような特定の条件のもとでのみ動作する「時限爆弾」があり、特定の関連したプログラムが動作しない限り、システム中に隠れているものも存在する。さらに常時動作しており、危害を加える期をうかがっているものもある。また巧妙なウイルスには、単にシステムの設定を変更したり、隠れてしまうものもある。
T21	ﾒｯｾｰｼﾞ盗聴後再送	例えば、クレジットカードによる購入や株取引のように、何らかのサービスを要求するために S/MIME メッセージが使われる事例がある。攻撃者が被害者の邪魔をするだけの場合にはサービスを 2 回実行することを望むため、攻撃者はメッセージを補足し、たとえそれを理解できなくても、再送することにより結果的にトランザクションを2回実行させることが可能となる。
T22	自動発呼による再送	ISDN回線では，同一電話番号に連続して規定回数(3回)発呼しても接続できなかった場合，その電話番号への発呼を規定時間(3分間)抑止する必要があります。このため，何らかの要因によって発呼規制状態の通信相手への送信データが発生しても，ISDNへの発呼が行えない場合があります。なお，通信相手指定のshow peerコマンドによって，発呼規制状態にあるかどうかを確認できます。
T23	TCP SYNﾌﾗｯﾄﾞ攻撃	攻撃者がパケットを挿入することによって、被害者に膨大な資源(この場合はメモリ)を浪費させることができる。あわせて攻撃者は、この行為を被害者から全くデータを受け取らずに行うことができるため、攻撃を匿名で行うことができる。
T24	DDoS	DDoS において、攻撃者は、標的マシンを同時に攻撃するように、数多くのマシンを準備し、数多くのマシンに攻撃のリモートによる開始ができるプログラムをしかけることによって達成される。
T25	災害・物理的破壊	ネットワーク機器等に倒壊防止対策等の保護措置を施していない場合、災害や破壊行為などを受けることにより、機器が正常に動作せず提供中のサービスが停止してしまう可能性がある。

脅威の定義

類型	脅威	解説
T26	不正な用法	しばしばWeb サーバはあらゆるユーザにデータを提供しますが、ページを変更する権限を特定のユーザに限定している。一般公衆によるこのような変更が「不正な用法」である。
T27	不適切な用法	一般的に、ユーザは電子メールを送ることが許可されているが、一定の大きさ以上のファイルやウイルスに感染したファイルを送信することは禁止されている。このような行為は「不適切な用法」である。
T28	なりすまし	正規のユーザが使用する、IDや秘密鍵を使用して、エンティティ認証や権限の認可を行うため、攻撃を検知しにくい。証拠収集やアーカイビングしている証跡を確認することで検知することが可能である。
T29	ｻｰﾋﾞｽ中断による不正処理	通信中にネットワーク機器の故障やネットワーク回線が何らかの理由で切断された場合、処理途中でサービスが異常終了する可能性がある。異常終了した場合、それまでの入力データがどのように処理されるか想定できない危険性がある。
T30	改ざん	オブジェクトセキュリティにおけるデータインテグリティを侵害する行為。そのために、なりすましが行われることもある。
T31	過失・盗難・紛失	セキュリティインシデントは、故意または過失によって引き起こされる場合がある。後者は、誰かがドアをロックすることを忘れた場合、もしくは、ルータ中のアクセスリストを有効にし忘れた場合に引き起こされる。