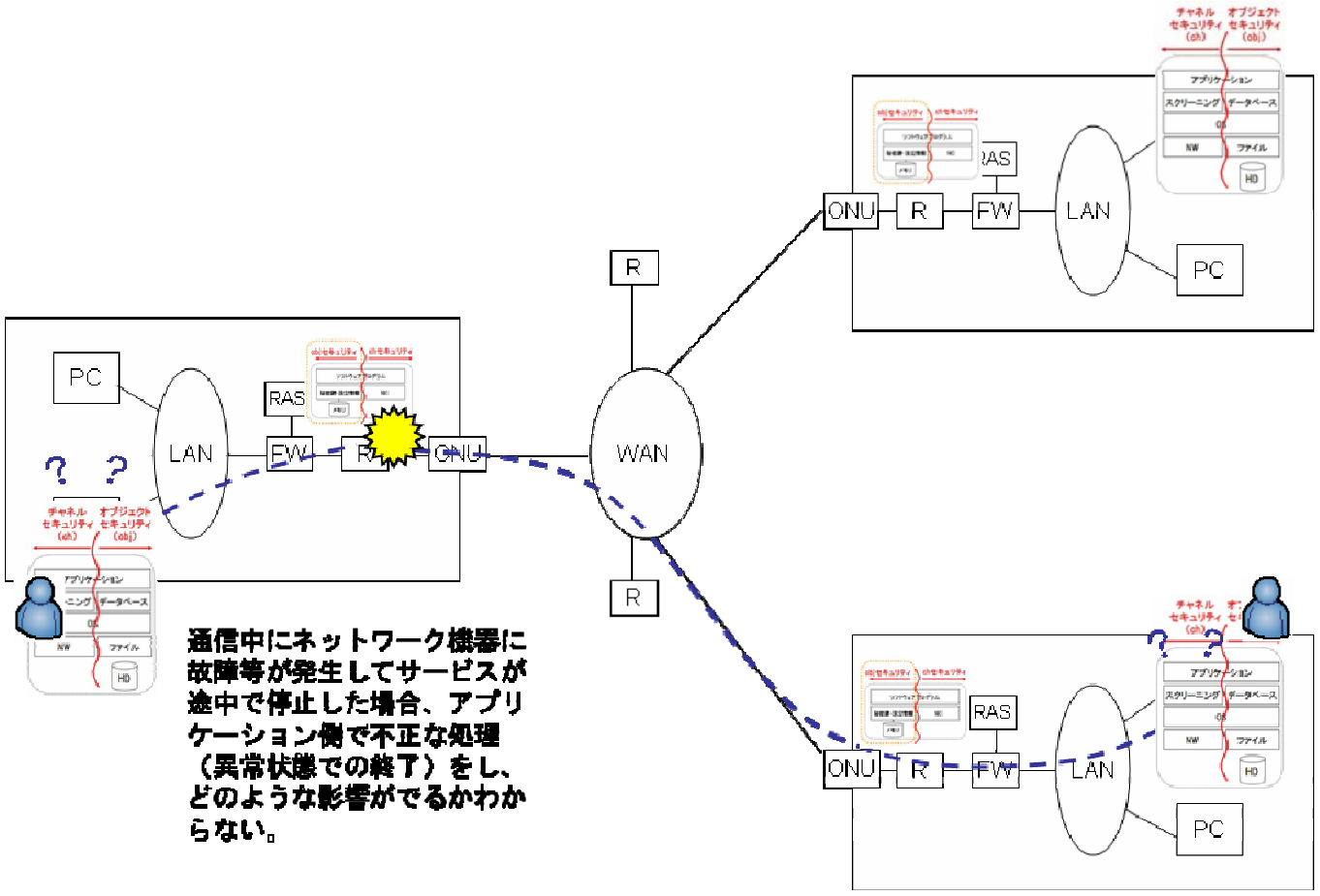
項番	T29. サービス中断による不正処理	脅威の大区分		守るべき資産	システムの処理（オブジェクトセキュリティ）	対象	AP/NW
解説	通信中にネットワーク機器の故障やネットワーク回線が何らかの理由で切断された場合、処理途中でサービスが異常終了する可能性がある。異常終了した場合、それまでの入力データがどのように処理されるか想定できない危険性がある。						
対策の概要							

脅威発生のイメージ



＜対策の概要＞

オブジェクトセキュリティの侵害行為であり、チャネルセキュリティでの対策だけでは不十分である。
アプリケーション側でロールバックやロールフォワード等、異常終了した場合の対策が必要である。

加えて、ネットワーク機器のオブジェクトセキュリティでの対策としても検討すべきである。

脅威の内容	ネットワーク回線の切断、ネットワーク機器の故障等

対策				リスク	
対策の内容	参照文書	対策表との対比		頻度	影響度
		方法	有効度		
(6) 伝送の完全性の確保 システムは、ネットワーク回線の切断、ネットワーク機器の故障等の不測の事態にでも対処できる機能を有すること	レセプト				
あなたのホームコンピュータにウイルスがあるとか、悪意を持ったプログラムが動作したとか、システムが侵入されたといった懸念がある場合、最も賢明な行動は、まずそのシステムをすべてのネットワークから切断することです。入手可能であれば、ウイルス検出ソフトウェア、またはシステム監査ソフトウェアを使用する必要があります。	RFC2504				
あなたのモデムが完全にコールを切断することをチェックしてください。ユーザがアクセスサーバーからログアウトするときに、そのサーバーが電話回線を正しくハングアップさせるかを検証してください。そのサーバーが、ユーザが予期せずハングアップしたときに、どこからのセッションが活動状態にあったか、ログ アウトを監視することも同等に重要です。	RFC2196				
ダイアルインサーバーには、コールバック機能を提供するものがあります。（つまり、ユーザがダイアルインして認証されると、そのシステムはそのコールを切断し、特定の番号でコールバックします。）この機能は注意して使う必要があります。	RFC2196				