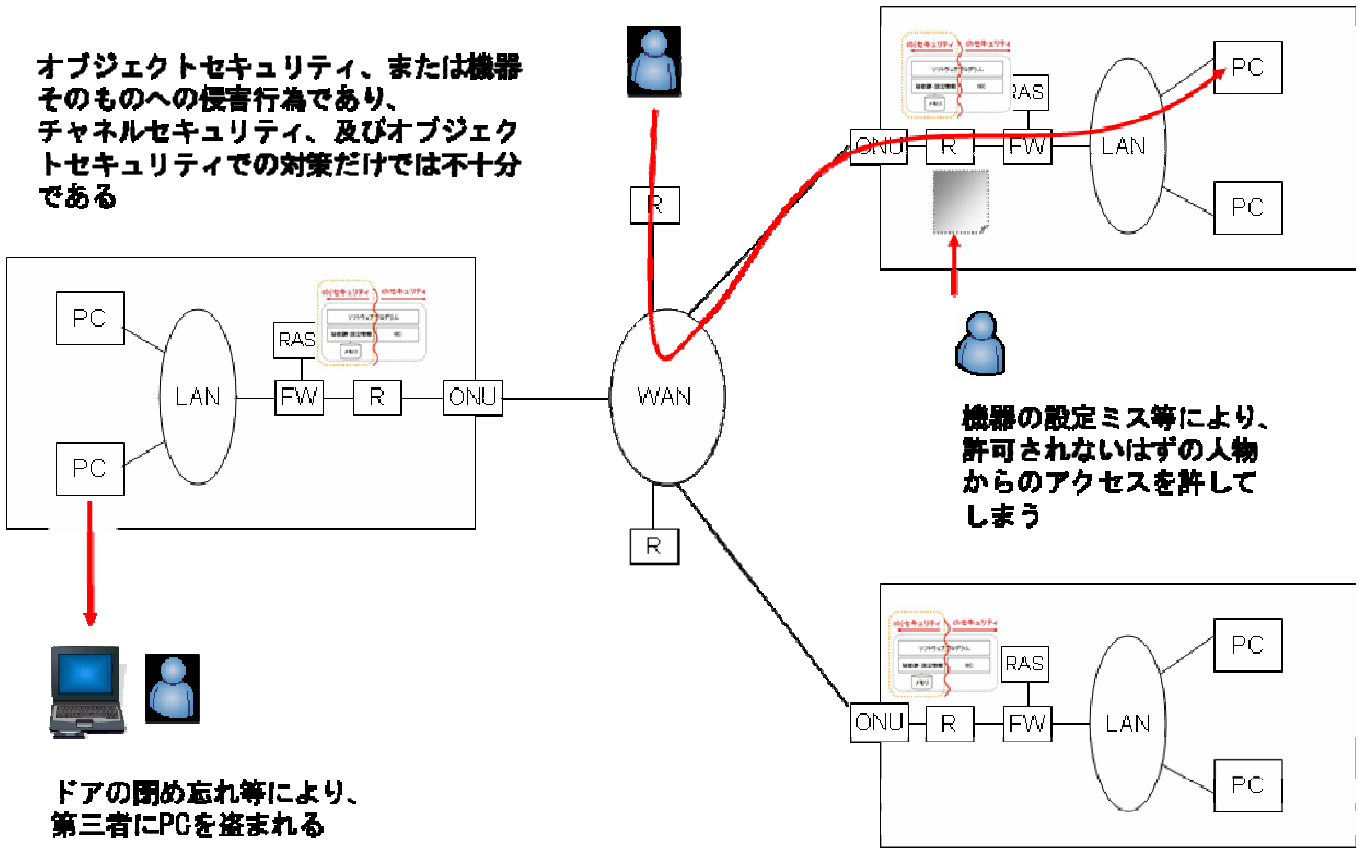
項番	T31. 過失・盗難・紛失	脅威の大区分		守るべき資産	システム（オブジェクトセキュリティ）	対象	AP/NW
解説	セキュリティインシデントは、故意または過失によって引き起こされる場合がある。後者は、誰かがドアをロックすることを忘れた場合、もしくは、ルータ中のアクセスリストを有効にし忘れた場合に引き起こされる。（RFC3067）						
対策の概要							

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。

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	

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		
アプリケーションによっては、長期間有効なチケットが必要な場合があります。しかし、チケットが長期間有効だと、信任状はその期間中、盗難の危険性にさらされることになります。盗まれた信任状も、有効期限が切れるまで有効 であるからです。	RFC1510				
有効期限の短いチケットを使い、新しいチケットを定期的に取得するには、クライアントが秘密鍵に長期間アクセスできる必要がありますが、これではさらにリスクが大きくなります。そこで、更新可能なチケットを使用すること により、盗難の危険性を減らすことができます。更新可能なチケットには、2 つの「満了時刻」があります。	RFC1510				
各更新時に、KDC はホットリストを参照して、最後に更新が行われてから盗難が報告されているか否かを判断できます。KDC は盗まれたチケットを更新することはしないので、盗まれたチケットの有効期限が短縮されます。	RFC1510				
オリジナルとバックアップのデータのコピーとプログラムを安全に保管してください。それらをバックアップ目的で良い保管状態に保つこととは別に、それらは盗難から守られている必要があります。ダメージ（破壊）についての考慮ばかりでなく、盗難防止のためにも、 バックアップを、オリジナルとは別の場所に保存することが重要です。	RFC2196				
7.4.4. 物理的セキュリティと環境的セキュリティ － 各コントロールは、情報や情報処理設備の侵害もしくは盗難を避けるために実施されるものとします。 － 物理的セキュリティコントロールおよび環境的セキュリティコントロールは、システム資源を設置する施設、そのシステム資源自体、および、それらの運用をサポートするために使われる施設を防護するために実施されるものとします。TSA のタイムスタンピング管理に関するシステムについての物理的セキュリティポリシーと環境的セキュリティポリシーは、最低限、物理的アクセスコントロール、自然災害からの防護、火災安全の要素、公共インフラのサービス（例： 電力、電信電話）の失敗、建造物の崩壊、配管の漏洩、盗難からの防護、破って入ること、および災害復旧に対応するものとします 。	RFC3628				
c) TSA の信用に値するシステムにおいて使われるメディアは、メディアを被害、盗難、認可されていないアクセス、および、老朽化から防ぐために、セキュアに取り扱われるものとします。	RFC3628				
天災、もしくは他の災害後、かつ、セキュアな環境が、元のサイト、または遠隔のホットサイトのいずれかで再構築される前の期間に、CA が、そのファシリティをセキュアにする手続き。例えば、地震で被害を受けたサイトからの、取り扱いに注意を要する資材の盗難を防護する手続き。	RFC2527				
秘密鍵の保護は、セキュリティを維持するうえで非常に重要です。ユーザーが自分の秘密鍵を守ることができなければ、攻撃者がユーザーの名をかたったりユーザーの情報を解読したりできることになります。	RFC2459				
IC カードの輸送に伴う盗難、改ざんを防ぐための対策を施したほうがよい。（運用要件・オプション）	RFC2459				
また、CA の秘密の署名鍵が改ざんされた場合にはその影響ははかり知れない程大きなものとなります。	RFC2459				
攻撃者が気づかれずに秘密鍵を手に入れたとしたら、攻撃者は偽の証明書と CRL を発行できることになります。偽の証明書と CRL が出回ると、システム全体の信用が無くなります。	RFC2459				
RA は、自分に属するエンドエンティティに代わって署名済みの失効リクエストを発行することができますが、エンドエンティティ自身にはそれができないこともあります 。（もしその鍵ペアが完全に紛失した場合）	RFC2510				
6.2.3. レコード送受信中の保護 English 暗号化と MAC 関数は、TLSCompressed 構造体を、TLSCiphertext 構造体へ変換する。復号関数は、逆の処理を行う。また、レコードの MAC はシーケンス番号を含んでいるため、紛失、超過、繰り返しメッセージを検出することができる。	RFC2246				
アプリケーション プロトコルが、紛失したメッセージを再送信せずにそれらを黙認する場合、タイムスタンプの使用は適切なリプレイ検出メカニズムとして機能します。タイムスタンプの使用は、ある ユーザが所有するすべてのピアが共通のサブセッション鍵を共有するが、いくつかのメッセージはピアのサブセットに送信されるマルチキャスト プロトコルにとっても適切なメカニズムです。	RFC1510				
単一の鍵ペアを署名とそれ以外の目的の両方に使用することは極力避けてください。署名用と鍵管理用に別々の鍵ペアを使用することで、ユーザーはいくつかの利点が得られます。署名用の鍵と鍵管理用の鍵では、紛失または漏洩により起こる派生問題が異なります。署名用と鍵管理用に別々の鍵ペアを使用することで、安定した柔軟性のある応答が保証されます。同様に、アプリケーション環境によっては、鍵ペアごとに異なる有効期限あるいは鍵の長さを割り当てた方がよい場合があります。残念なことに、従来のアプリケーション(たとえば SSL)によっては単一の鍵ペアが署名用と鍵管理用の両方に使用されています。	RFC2459				
CA の秘密の署名鍵が紛失しても問題が生じます。CA は CRL を発行できなくなったり、通常の鍵ロールオーバーを実行できなくなります。CA は署名用の鍵を安全な方法でバックアップしておくことが推奨されます。鍵のバックアップ手順がセキュアであるかどうかが、鍵の悪用を防止するうえで非常に重要です。	RFC2459				

④ 情報の破壊に対する保護機能や復旧の機能を備えること 故意または過失による情報の破壊がおこらないよう、情報保護機能を備えること	安全管理			
可搬型媒体の遺失や他の搬送物との混同について、注意する必要がある	安全管理			
診療録等の劣化、損傷、紛失、窃盗等を防止するために、適切な保存環境・条件を構築・維持しなくてはならない。	安全管理			