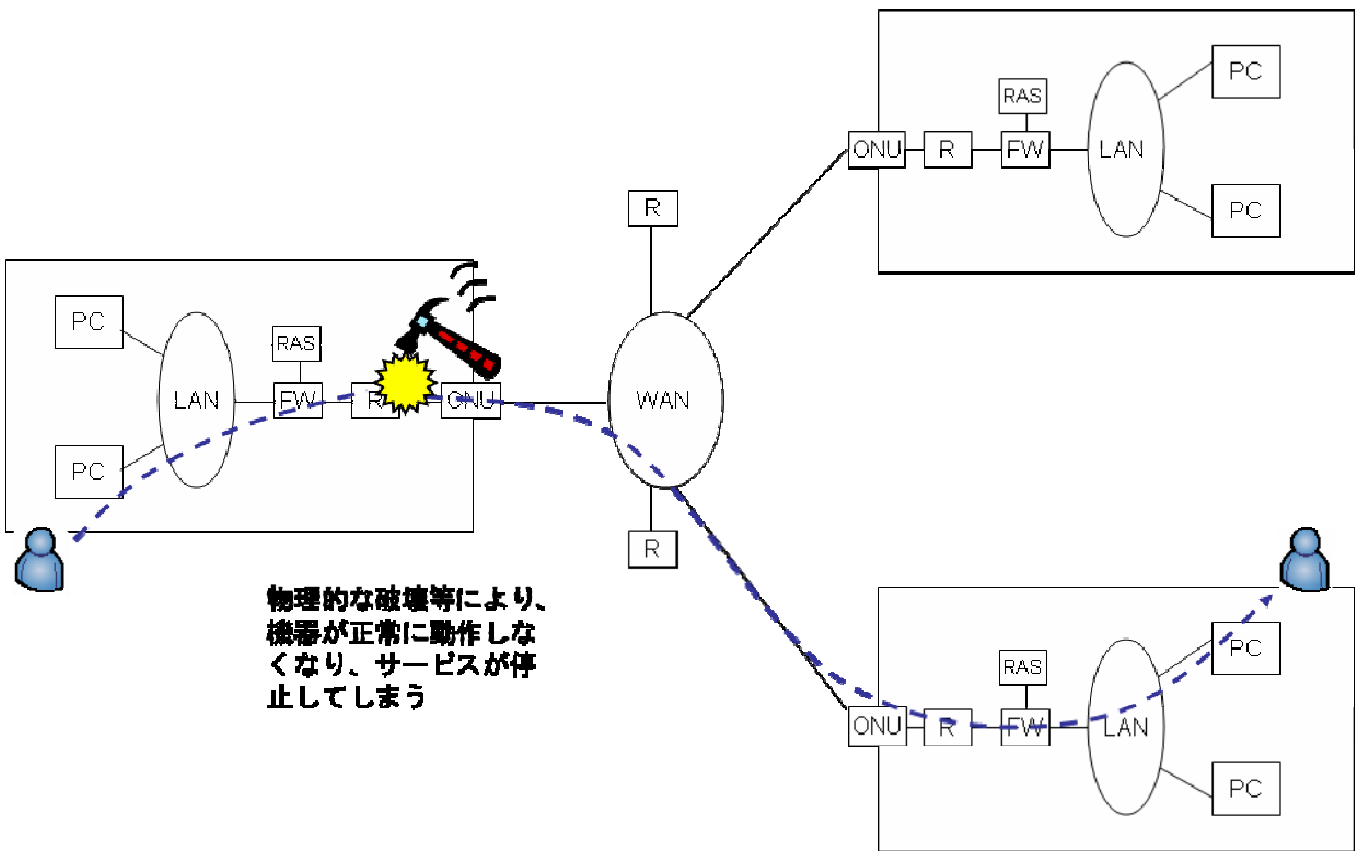
| 項番 | T25. 災害・物理的破壊 | 脅威の大区分 | 妨害 | 守るべき資産 | 提供されるサービス | 対象 | AP/NW |
|---|---|---|---|---|---|---|---|
| 解説 | ネットワーク機器等に倒壊防止対策等の保護措置を施していない場合、災害や破壊行為などを受けることにより、機器が正常に動作せず提供中のサービスが停止してしまう可能性がある。 | | | | | | |
| 対策の概要 | | | | | | | |

**脅威発生のイメージ**




＜対策の概要＞

機器等への物理的な脅威であり、オブジェクトセキュリティや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**

$ survivability（生存可能性）
(I) 不運な条件にかかわらず、運用を続行したり、あるいは、存続するシステムの能力。自然災害や偶発的行為と、システムにおける攻撃の両方を含む。
（availability, reliability 参照。）

b.「物理的破壊（Physical destruction）」:
システムの運用を中断または妨害するために、システムコンポーネントを故意に破壊すること。

e*「自然災害（Natural disaster）」:
システム機能またはデータの変更をもたらす、あらゆる「神のなせる業」

| 対策 | | | | リスク | |
|---|---|---|---|---|---|
| 対策の内容 | 参照文書 | 対策表との対比 方法 | 対策表との対比 有効度 | 頻度 | 影響度 |
| 4.4.8 改ざんや災害からの復旧 English<br>このサブコンポーネントは、改ざんや災害が起きた場合における通知と復旧の手続きに関する要件を記述します。下記の各状況が別々に対応 される必要があります。:<br><br>* コンピューティング資源、ソフトウェア、かつ／または、データが破壊された、もしくは、破壊されたことが疑われる場合に使用 される復旧手続き。これらの手続きは、どのようにセキュアな環境は再構築されるか、どの証明書が失効するか、主体の鍵は失効されるのか、どのように新しい主体の公開鍵はユーザに提供 されるのか、どのようにサブジェクトは再認証されるのか、を記述 します。<br><br>* 主体の公開鍵が失効された場合に使用される復旧手続き。これらの 手続きは、どのようにセキュアな環境は再構築されるか、どのよう に新しい主体の公開鍵はユーザに提供されるのか、どのように サブジェクトは再認証されるのか、を記述します。<br><br>* 主体の鍵が改ざんされた場合に使用される復旧手続き。これらの手続きは、どのようにセキュアな環境は再構築されるか、どのように新しい主体の公開鍵はユーザに提供されるのか、どのようにサブジェクトは再認証されるのか、を記述します。<br><br>* 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。 | RFC2527JA | | | | |
| 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 | | | | |
| 万一破壊がおこった場合に備えて、必要に応じて回復できる機能を備えること。 | 安全管理 | | | | |