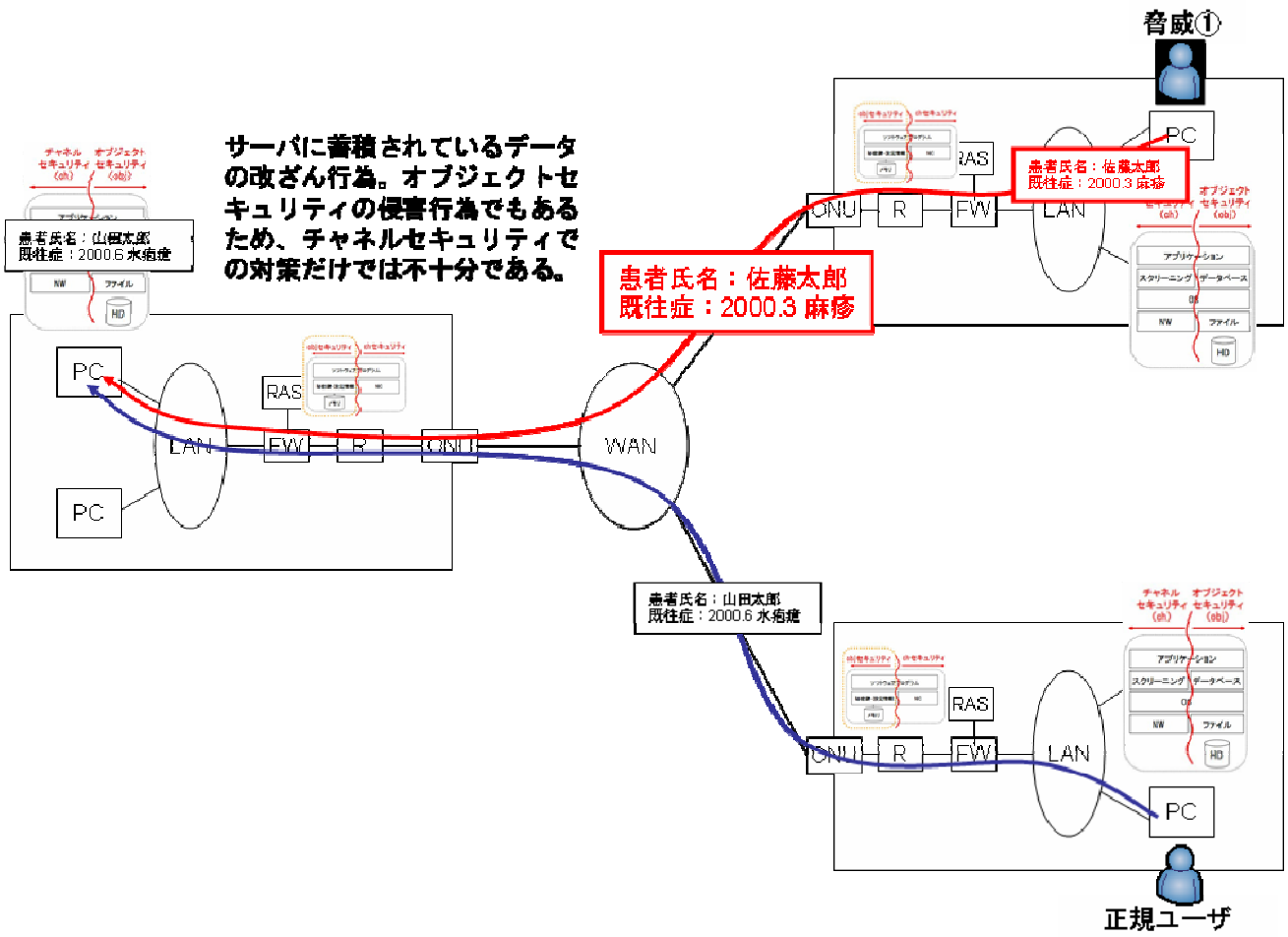
項番	T30. 改ざん	脅威の大区分		守るべき資産	データの完全性(オブジェクトセキュリティ)	対象	AP/NW
解説	オブジェクトセキュリティにおけるデータインテグリティを侵害する行為。そのために、なりすましが行われることもある。						
対策の概要							

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

$ data integrity（データインテグリティ、データの完全性）
(I) データが、認可されていない、または、偶発的な作法によって、変更されていない、破壊されていない、または、失われていないという属性。（data integrity service 参照。）

(O)「『情報が 認可されていない作法で変更／破壊されていない』という特性。」[I7498 Part 2]

(C) 値が表す情報ではなく、データ値の一貫性と信頼性を扱う(correctness integrity 参照)、または値のソースの信頼性。(source integrity 参照。)

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		
セキュリティは、情報のプライバシーの保護、不正な変更(改ざん)に対する情報の保護、サービス妨害に対するシステムの保護および不正アクセスに対するシステムの保護を含むものと解します。	RFC1281				
あなたのファイルが改ざんされたことに気がついた場合、もしくは、何らかの方法であなたの承諾なしにアカウントが使用されていたことを突き止めた場合、ただちにあなたのセキュリティ連絡先に通知する必要があります。	RFC2504				
一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。	安全管理				
4. アクセスログの記録を残し、そのログが改ざんされない対策を講じ、万が一、記録情報の改ざん・削除が起こった場合にはその事実を検証可能とすること。	安全管理				
認証や改ざん検知の機能をソフトウェアで行っている場合には、関連する暗号鍵が盗まれたり、認証や改ざん検知の機構そのものが破壊されたりするおそれもある。	安全管理				
・一定期間とは改ざんの機会が生じない程度の期間で、通常は遅滞なくスキャンを行なわなければならない	安全管理				
1度だけ書き込めるデバイス上に監査データを収集することは、単なるファイルの方法よりも設定に少し労力を要しますが、これには、大きくセキュリティを強化する明らかな利点があります。それは、侵入者が、侵入が起きたことを示すデータを改ざんすることができないからです。この方法の欠点は、保存メディアを用意し続ける必要性があることと、そのメディアの費用です。	RFC2196				
DNSsec [RFC 2065] DNS を防御することにおいてのみ重要であるのではありません。(能動的な攻撃をしかけるのに、キャッシュの改ざんが、最も容易なやり方です。)IPsec が使われている多くの場合においても要求されるものです。	RFC2316				
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)	NICSS運用GL				
カード保有者に渡る前にカードが紛失・改ざんされる可能性がある場合は、カード保有者以外の者がカードへアクセスできないような対策を施したほうがよい。(運用要件・オプション	NICSS運用GL				
R 4.4.0.14 カード発行者は、カードを輸送する際の輸送途中におけるカード改ざん防止、盗難後の偽造防止のために、カード供給者がカードに埋め込んだ輸送鍵あるいはPIN情報を、カード供給者から安全に入手しなければならない。(運用要件・必須)	NICSS要件書				