2.21 システムに利用期限のある機器／ソフトを組み込む際の教訓（G21）

教訓 G21　サーバ証明書等の有効期限の確認方法を工夫せよ

問題

A社では全社向け基幹業務システムを構築し、同システムを使用して来訪する自社顧客向けのサービスを全事業所で提供している。サービスの提供は平日日中から夜間までだけでなく、一部の事業所では休日も実施している。業務システムは2年前に構築したものであり、システム保守はシステム構築を委託した先の事業者が継続して担当し、システム運用はA社が自ら実施している。A社の基幹業務システムは端末側アプリを仮想化し、サーバと仮想端末が通信する構成にしていた。

A社基幹業務システムの構成を図2.21－1に示す。

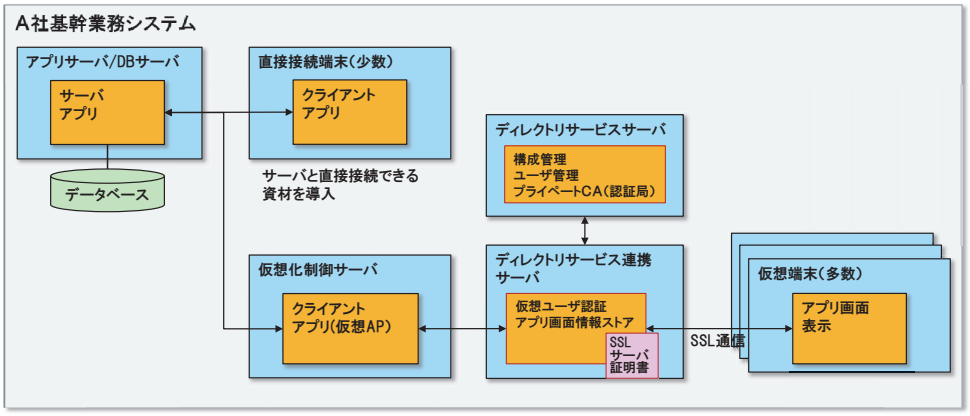

図2.21－1　A社基幹業務システムの構成

ある休日の朝、サービス利用の現場で、仮想端末上で基幹業務が起動しないという現象が発生した。仮想端末を起動すると「ディレクトリサービス連携サーバとの接続ができない」とのメッセージが表示されるだけであり、仮想端末上で動作するアプリケーションが全く使用できない状態になっていた。この現象は特定の端末によらず、すべての仮想端末で発生していた。表示されるメッセージから原因が端末の仮想化技術に関係するとの報告を保守委託先から受けたA社のシステム運用責任者は、休日にサービスを提供する事業所内に少数ながらも直接アプリサーバと接続する端末（以下、直接接続端末）が用意されていたことから、トラブルが収束するまでの間、直接接続端末だけを利用することを利用の現場に連絡して、当日の業務を開始した。

しかしながら、直接接続端末は数量が限定されており処理の順番待ちが多数発生したことから、一部の顧客が自分の順番を待ちきれずに帰るという事態に陥った。

原因

仮想端末に表示されるメッセージから、基幹業務システムが仮想端末で起動しなかった原因はディレクトリサービス連携サーバと仮想端末の通信途絶であることは明白であった。通信途絶が発生した直接の原因は、サーバのハードウェア故障等によるものではなく、ディレクトリサービス連携サーバの SSL サーバ証明書（以下、サーバ証明書と記す）の有効期限がトラブル発生前日までで切れ、当日以降は有効でなくなったことにより、サーバと仮想端末が SSL 通信できなくなったことであった。

トラブル発生時の状況を図 2.21－2 に示す。

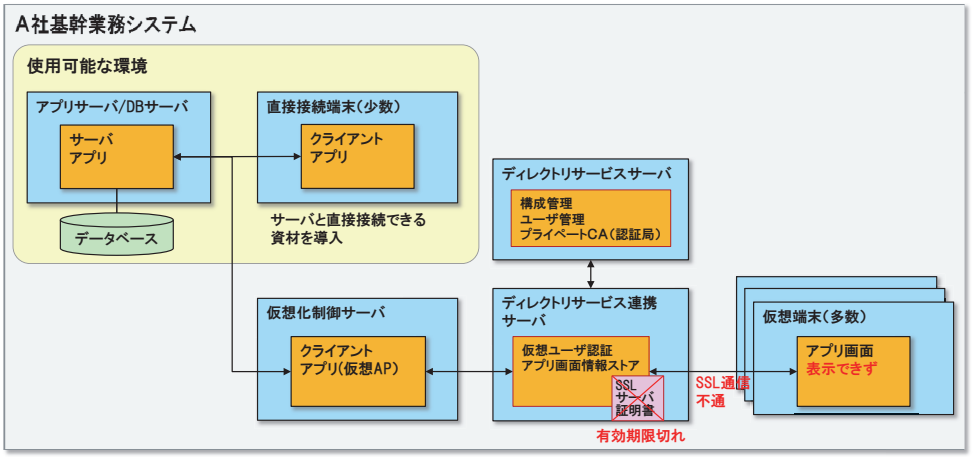

図 2.21－2　トラブル発生時の状況

そして、業務運用中にサーバ証明書の有効期限切れを発生させたシステム運用管理上の原因は、ディレクトリサービス連携サーバにサーバ証明書が組み込まれており、2 年ごとに更新する必要があったこと、さらにその期限がトラブル発生前日までであったことを A 社もシステム開発保守委託先の保守担当者も認識していなかったことであった。

幸い発生したのが休日であったため平日に比べればサービス利用者への影響は小規模で済んだが、少数ながらもサービスの提供が滞ったことにより一部の顧客がサービスを受けられなかったことを重く受け止めた A 社は、再発防止に向け、根本原因の分析を開始した。

対策

トラブル発生の原因が上記であることが判明し、A 社は直接の対応として以下の処置を実施した。

- ディレクトリサービス連携サーバのサーバ証明書を作成し、ディレクトリサービスサーバに登録
- 上記対応が完了し、システムを復旧するまで直接接続端末を増設

次いで A 社ではこのトラブルの再発防止のため、自社および開発・保守委託先会社の両当事者を

集めて根本原因の分析と採り得る再発防止策の選択を実施した。

再発防止策を検討する際には、単にサーバ証明書発行の期限切れの再発防止だけでなく、システム運用において定期的に実施する必要のある管理上の作業全般を対象とした再発防止（他個所の点検への水平展開）の観点で、実施すべきこと及び優先度の洗い出しを行った。検討の結果を以下に示す。

表 2.21－1　根本原因の分析および再発防止策の検討結果

原因			対策案（*斜体は水平展開*）	対応要否
仮想アプリが動作するサーバの SSL 認証が運用中に期限切れになった				
第一階層の原因	誰も期限を監視していなかった		サーバ証明書を毎年定期的に更新して期限切れを防止するよう運用変更	要 すぐ
			他のサーバ証明書やパッケージライセンスの監視に漏れはないか確認 *すべてのサーバ証明書の有効期限、管理担当者等を台帳管理し、定期的に確認する*	*要* *すぐ*
	第二階層の原因	仮想環境上で SSL 通信を使用すること、それには構築時のサーバ証明書発行と運用開始後の定期的な更新が必要になることをA社では認識していなかった	構築会社と同レベルの仮想化環境構築技術を内部留保	不要 現実的でない
		サーバ証明書の期限の管理者が曖昧 （開発委託先の意識は、証明は認証サーバが行うもの、認証サーバの管理はA社の担当）	サーバ証明書の定期更新を保守委託先の作業として契約時の仕様書に明示	要 次年度
			他に管理者が曖昧になっているハード、ソフトはないか確認	*要* *すぐ*
			管理すべき対象がA社側でもすべて認識できているか確認	*要* *時期調整*
		サーバ証明書の定期的な更新が必要であることが環境構築時に開発委託先からA社に伝達されていない	*他に同様の対処を必要とする案件がないか確認する*	*要* *すぐ*
		第三階層の原因：サーバ構築時の設定手順書にはサーバ認証に関する記載がなかったが、構築担当者は仮想化に詳しくサーバ証明書を登録できた それがA社にも開発保守委託先の保守担当者にも引き継がれていない	*サーバ証明書を組み込んでシステムを構築する際には、開発委託先に対してA社側からも引継ぎ事項の有無を確認する、* *引継ぎ事項チェックリストに確認事項として提示し、調査結果を相互確認することにより漏れを抑止する。* *（開発保守委託先における引継ぎ漏れ防止への自律改善策は別途実施する）*	*要* *次のシステム構築契約時*

効果

A 社では以前からオフィス等のソフトウェアのライセンスの保有状況や有効期限の管理を実施していたが、それに加えて表 2.21－1 に記載された各対策を実施することにより、今回トラブルが発生したサーバの証明書の有効期限にとどまらず、電子的な証明書を利用する他のシステムを把握し、それらの証明書の有効期限と更新作業者、保守委託契約書の記載を調査し、定期的な更新が漏れないよう管理監督することにより、運用中に不測の期限切れが再発することを防止できている。

また、保守委託先とは契約の不備を見直し、委託した業務においても同様に再発を防止する取り組みを行っている。今後のシステム開発や運用環境構築時の構築会社とのサーバ証明書などの組込み有無の確認については、次期システム構築までの見直し検討課題としている。

教訓

この事例では、運用中のサーバの証明書の期限切れを事例として、そこから根本原因を分析して広範囲の再発防止を検討した過程を説明した。サーバ証明書の期限の管理は、それが原因で大規模なシステム運用障害を引き起こした事例もあり、単純なようで意外に見落としやすい監視対象である。

ここでは、サーバ証明書の管理ができなかった原因をさ様々に考察し、それぞれに適した対策を検討した。その中で、証明書の期限が近いことをA社がトラブルになる前に認識できていなかった根本原因として特記すべき事項は、構築や保守を担当した委託先も、システムの保有者であり運用の最終責任者である A 社も、それがシステムに組み込まれているかどうかを運用開始時に確認できていなかったことである。

一般に、システム開発や運用環境の構築を委託する側に委託先と同レベルの技術が留保されていることは、大規模システムを自社で開発運用する組織以外には期待できない。今回の A 社の事例に限らず、大多数のシステム構築においては、システムを開発した側から運用を担当する側への情報伝達の漏れをなくすことが、このようなトラブルの発生を防止する最も有効な対策になる。しかしながら、構築時と保守時で委託先や再委託先が異なることや同じ委託先であっても担当 SE の変更が生ずることがままあり、その引継ぎの際に技術やノウハウの連携漏れが生ずるケースは少なくない。情報連携の漏れ防止は、システム構築や運用を受託する側の技術レベルの向上や内部チェックの強化が最も効果的な施策であるが、委託する側の自己防衛策は、以下の二点である。

- サーバ証明書の更新など運用継続に必要な作業が漏れなく報告されているかどうかを、運用引継ぎチェックリストに確認結果の記載を依頼する等により依頼元から積極的に確認することにより、システム構築委託元が知らないうちに証明書が組み込まれているというような事態の発生を抑止する
- サーバ証明書の有効期限のチェックや更新を漏れなく実施する（年間運用スケジュールに明示する）

この事例から教訓として伝えることは、「システム開発や環境構築を委託した際には、SSL サーバ証明書の有効期限の更新などのシステム運用開始後に定期的に実施すべき運用管理上のイベントの有無やその内容が漏れなく報告されているかどうかを、運用開始前に委託元から自主的に委託先に確認することを怠らない工夫をすること」とした。