

リモート環境でのデジタル技術によるシステム保守の可能性

サイバーリスクや境界型防御の限界が指摘されるなか、システム保守が追い付いていない。特に金融セクターは、多くの物理的・技術的設備要件を遵守するため対策難易度が高い。リモート環境で活用されたデジタル技術をシステム保守に適用していくべきである。

性善説のシステム保守のリスク対策の限界

システム保守において高度な統制要件やセキュリティ対策を求められる操作は、各企業の拠点に設置された高度な統制とセキュリティ対策を備えた「本番端末室」や「専用作業室」の内部で行われることが一般的である。

中でも金融セクターでは、業界団体や省庁から示されている様々なガイドライン¹⁾があり、本番端末室等について様々な規定がある。IDカードや生体認証による入退室、防犯カメラの設置、記録保管等々が定められている。

これは境界型防御²⁾と呼ばれるセキュリティモデルであり、特定の施設や論理環境（ネットワーク）内部の人・デバイスを信頼することで成り立っている。

しかし、システムはパブリッククラウド活用やサーバー利用型に変遷し、境界自体が外部へ広がったことで、従来の自社内だけを対象にしたシステム保守には限界が生じる可能性がある。また、過去の事故例からも労働市場の流動化により人材管理がさらに難しくなりつつあることも認めざるをえない状況である。身内だから安全だといった性善説にたったシステム保守では対応が困難になってきたことを金融機関は認識すべきだろう。

システムへの攻撃の手法も内部関係者になりすましてのランサムウェア攻撃³⁾など内部侵入型に変わっており、人をそのまま信頼することが大きなリスクとなることが次第に明らかになっている。

また、これは別の視点からだが、大規模災害のリスクも高まり、従来の本番端末室でのシステム操作を前提とした境界型防御の仕組みが、システム保守の足かせになりつつあることも認識すべき点である。

デジタル技術によるシステム保守レジリエンス向上

こうした従来の境界型防御ではないシステム保守として、コロナ禍をきっかけに急成長したリモート環境でのシステム保守の活用が考えられる。以下、テレワーク時代の組織運営とデジタル技術を活用し、リモート環境特有の脅威・リスクを対策により、どの程度、システム保守レジリエンスが向上するのかを示したい。

留意すべき本番端末室とリモート環境の違いについて、まず整理しておく。本番端末室は、入退室管理、防犯カメラ等により作業者の悪意に対する牽制機能を複数有している。リモート環境は、特別な対策をしない限りそれらは存在しない。そのため、リモート環境でのシステム保守は、悪意ある行動に対する心理的ハードルが下がりがやすく、性悪説にたった対策検討が重要といえる。

システム保守時に留意すべきリスク観点である「脅威の発生源（第三者、悪意のある作業員、悪意のない作業員）」、「悪用の場（物理空間、デバイス、通信経路）」を組み合わせることで「想定される脅威・リスク」を整理した（図表左部）。

リモートアクセス特有のリスク例として、作業場所の安全性がある。従来の本番端末室では入室者を厳密に制限し、第三者の侵入を防ぐ仕組みとなっているが、リモート環境では、本番作業員の家族や第三者などによる画面の覗き見リスクがある。さらに作業員本人に悪意がある場合、作業画面を手持ちのスマートフォン等で撮影することで、映像として本番データを持ち出せる危険性がある。この対策として、ヘッドマウント型ディスプレイやスマートグラスの活用が考えられる。作業員自身が

NOTE

- 1) 「金融分野における個人情報保護に関するガイドライン」、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」、「金融機関等コンピュータシステムの安全対策基準・解説書」等を指す。
- ガイドラインには以下のような本番端末室等についての記載例がある。
- ・システムの本番端末室には、IDカードや生体認証を用いて事前に認められた人物のみが入退室できるように制限すること
 - ・インシデント発生時に当時の状況を確認できるように、本番端末室内に防犯カメラを設置し、記録を一定期間保管すること
 - また、下記のような作業者、監督者への分担を含めた相互牽制に関する記載例もある。
 - ・システムの本番作業は、「作業者」と「監督者」による複眼チェックを行えるように2名体制で行うこと
 - ・システムに保管されている個人情報、機密情報を含む本番データなどを無断で持ち出しができないように技術的な対策を講じること
- 2) 境界型防御とは、信用する領域（内部）と信用しない領域（外部）に境界を設け、境界外部からの脅威を境界上で検証することで、外部からの攻撃や不正アクセスを防ぐセキュリティモデルのことを指す。
- 3) ランサムウェア攻撃とは、PCやシステムのハードディスクドライブに保存されているファイルを、「人質」として暗号化し、復号のために被害者に金銭（ランサム＝身代金）を要求するマルウェア攻撃のことを指す。
- 4) 超小型カメラ等を利用した本番端末室盗撮によるデータ持出しリスクに対し、ヘッドマウント型ディスプレイ採用による盗撮・データ持出し防止などが一例として考えられる。

図表 想定される脅威・リスクと本番端末室、リモート環境での対策

セキュリティリスク			本番端末室		リモート環境	
脅威の発生源	悪用の場	想定される脅威・リスク	防止	追跡	防止	追跡
第三者	物理空間	画面の盗撮・覗き見	○ 第三者の入室不可	○ 防犯カメラによる記録	○ 物理的な画面遮蔽	○ 外観カメラによる記録
	デバイス・通信経路	ログイン済み端末/セッションの奪取・窃取	○ 第三者の入室不可	○ 防犯カメラによる記録	○ 再鑑者による監視、アクセス制御	○ 外観カメラによる記録
	デバイス・通信経路	ログの削除、改竄	○ 第三者の操作不可	○ システムの作業ログ	○ アクセスチェックの改竄不可	○ アクセスチェックの作業ログ
	物理空間・デバイス・通信経路	作業者・再鑑者のなりすまし	○ 生体認証	○ 防犯カメラによる記録	○ 生体認証+再鑑者による監視、アクセス制御	○ 外観カメラによる記録
悪意のある作業者・再鑑者	物理空間	データ持出し・画面記録、外部出力	○ 再鑑者による監視、牽制	○ 防犯カメラによる記録	○ 再鑑者による監視、アクセス制御	○ 外観カメラによる記録
	デバイス	データ持出し・手書き、音声による出力	○ 再鑑者による監視、牽制	○ 防犯カメラによる記録	○ 再鑑者による監視、アクセス制御	○ 外観カメラによる記録
	デバイス	ログイン済み端末の貸与	○ 端末入室、アクセスチェックの事前承認	○ 防犯カメラによる記録	○ 再鑑者による監視、アクセス制御	○ アクセスログ・作業ログ
	デバイス・通信経路	本番システムに対する不正アクセス・操作	○ 再鑑者による監視、牽制	○ アクセスログ・作業ログ	○ 再鑑者による監視、アクセス制御	○ アクセスログ・作業ログ
悪意のない作業者	デバイス・通信経路	誤操作・作業ミス	○ 再鑑者による複眼チェック	○ アクセスログ・作業ログ	○ 再鑑者による複眼チェック	○ アクセスログ・作業ログ

(出所) 野村総合研究所

頭部に装着し、虹彩認証を用いたデバイスのロック解除と物理的な視野を外部から遮蔽することで、“認証した本人以外からは物理的に覗き見ることができない”状態を作り出せる。また脱着時には当該デバイスを自動ロックすることで、装着時の虹彩認証を強制し、作業者のなりすましや不正な貸与ができないようになる。

GPSやWi-Fiを用いた位置情報により作業場所を把握することも安全性を確保する技術的対策の1つとして有効と考えられる。

また、本番端末室との大きな違いとして、リモートでは作業者に対して監督者からの物理的な牽制や作業中断を強制することができない。この場合、アクセス管理やリモート接続ソリューションを導入することで、作業者と監督者がお互いにリモートアクセス準備が整ったことを確認し、監督者からアクセスを許可する。作業を中断させたいときには、本番アクセスのセッションを強制的

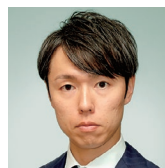
に切断する機能を利用することも考えられる。

上記も踏まえ、想定される脅威・リスクへの対策可能性について「防止」「追跡」の観点で整理したのが図表右部だが、デジタル技術の活用により、リモート環境でも本番端末室同等のリスク対策は可能と考える。

これらリモート特有の対策は、従来の本番端末室運用に潜在的に存在するリスクも解消⁴⁾する可能性があることを指摘しておきたい。想定を超えたリスクが起きる可能性も見据えて、時代にあった安全なシステム運用を考えていく時期に來ていると、筆者は強く思う。

(執筆協力：MDC運用サービス事業二部 恵良 雄太)

Writer's Profile



中川 直樹 Naoki Nakagawa
プラットフォームサービス開発一部
エキスパートシステムコンサルタント
専門は生産性向上、DevOps
focus@nri.co.jp