欧米の金融機関事例を踏まえたリモートワークにおける内部不正対策

国内では新型コロナウイルス感染症（COVID-19）の拡大を契機に金融機関におけるリモートワークの導入率が大幅に増加し、今後もニューノーマル（新常態）社会においてさらなる活用が予想されますが、その一方で、リモートワークに起因する内部不正などのリスクが高まることが懸念されています。本稿では、長年にわたりリモートワークを活用している欧米の金融機関の対策事例を踏まえ、リモートワークにおける内部不正リスクへの効果的な対策について考察します。

1. リモートワークにおける内部不正の近年の状況

2020年4月に、政府の方針を踏まえて金融庁から金融機関に対して「出勤率7割削減」が要請され、その対応として各金融機関でリモートワークの導入が推進されました。現在はリモートワークにおけるコミュニケーション・従業員管理の難しさなどから、オフィス回帰の動きも出てきています。しかし今後、COVID-19の拡大を経て形成されるニューノーマル社会においては、場所に捉われない働き方としてリモートワークは新たな生活環境の一軸に位置けられ、恒常的に活用する姿が「当たり前」となっていくことが予想されます。リモートワークを導入することで、従業員の通勤時間の削減や生産性・効率性の向上などのメリットがある一方、新たなリスクも発生します。オフィスでの作業とは異なり衆人環視がないため、内部不正を助長しかねないこともその1つです。

独立行政法人情報処理推進機構（IPA）が発行した『情報セキュリティ10大脅威 2020』[1]によると「内部不正による情報漏えい」はすでに企業における脅威のなかで第2位となっています。リモートワークの拡大により従来以上に内部不正リスクが高まることが懸念されるなかで、金融ビジネスの安全・安定の確保に対し、より厳格かつ効果的な内部不正対策が求められます。

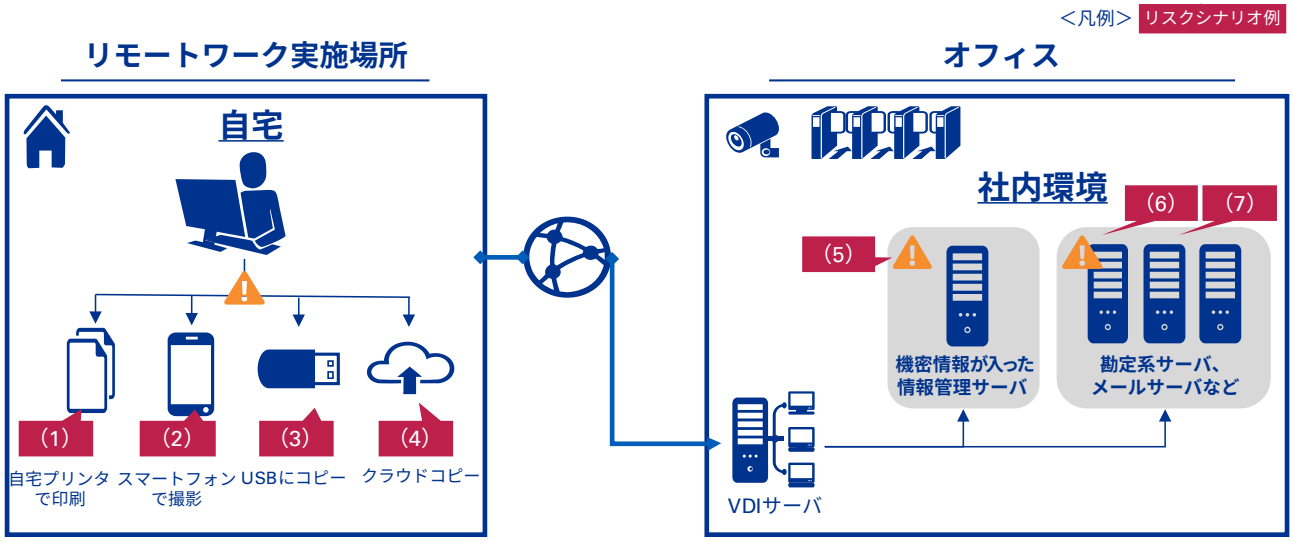
[1] 『情報セキュリティ10大脅威 2020』（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/vuln/10threats2020.html

2. リモートワークに起因する内部不正のリスクシナリオ

リモートワークは衆人環視があるオフィス作業時と異なり、不正に対する心理的なハードルが下がり、不正の機会が生じやすい環境と言えます。「時間的制約がない」「個人所有端末を利用しやすい」などの要因により、重要データへの不正アクセスや不正持ち出しリスクを増大させる懸念があります。リモートワークの特徴から、「時間をかけて重要データを検索し不正にアクセスされる」「USBメモリや自宅のプリンタを利用して重要データを不正持ち出しされる」「私用スマートフォンなどにより端末画面をカメラ撮影される」などの内部不正に関するリスクシナリオが想定されます（図表1参照）。

リモートワークの実施方式により想定されるリスクシナリオが異なるため、自組織のリモートワークの特徴を理解したうえでリスクシナリオの洗い出し・評価を実施する必要があります。

【図表1　リモートワークにおける内部不正のリスクシナリオ例】



リスクシナリオ例
(1) リモートワーク端末から自宅プリンタに接続し、機密情報を印刷され外部に流出・悪用される。
(2) 私用スマートフォンなどのカメラを使い、機密情報が映っているパソコン画面を撮影され外部に流出・悪用される。
(3) リモートワーク端末にUSBメモリなどの外部媒体を接続し、機密情報をコピーされ外部に流出・悪用される。
(4) 利用未承認のクラウドストレージに機密情報が持ち出され、外部に流出・悪用される。
(5) 時間をかけて機密情報を検索し、情報管理サーバに不正にアクセスされる。
(6) 勘定系サーバやメールサーバなどに不正にアクセスされ、情報が改ざんされる。
(7) 勘定系サーバやメールサーバなどへの不正アクセスにより、システムパフォーマンスの低下やシステムダウンが発生する。

3. 欧米の金融機関における内部不正の対策傾向

多くの国内金融機関は増加するセキュリティリスクへの対策を模索している状態であり、情報漏洩などの懸念から、リモートワーク実施者の絞り込みや重要情報へのアクセス制限など、リモートワーク利用を限定せざるを得ない状況が発生しています。

一方、欧米においては、長年にわたりICT（情報通信技術）を活用して経済成長と雇用を促すためにリモートワークを推進してきた実績と、ジョブ型を中心とした雇用形態により個人ごとにデータへのアクセス権を厳密に設定していることから、リモートワークにおいてもオフィス勤務時と同レベルの業務が遂行可能な環境を整備できている金融機関が多数存在します。コロナ禍においても大手金融機関では高い割合でリモートワークを実施しており、中には98%のリモートワーク実施率を実現している企業もあります。

内部不正へのリスクシナリオに対する基礎的な情報セキュリティ対策の徹底には、欧米と国内の金融機関との間に大きな違いはありません。「ログによる従業員の行動監視」「DLP（Data Loss Prevention）」「誓約書の提出による従業員責任の明確化」の3点は複数の欧米金融機関が注力している取組みであり、リモートワークにおけるキーコントロールと認識しています（図表2参照）。
これら3つの対策について、実施傾向と論点を解説します。

【図表2　3つの対策によるリモートワークにおける内部不正リスクへの統制状況】

リモートワークにおける内部不正のリスクシナリオ例		3つの対策による統制状況		
		I. ログによる行動監視	II. DLP	III. 誓約書の提出
(1)	リモートワーク端末から自宅プリンタに接続し、機密情報を印刷され外部に流出・悪用される。	○	○	○
(2)	私用スマートフォンなどのカメラを使い、機密情報が映っているパソコン画面を撮影され外部に流出・悪用される。	—	—	○
(3)	リモートワーク端末にUSBメモリなどの外部媒体を接続し、機密情報をコピーされ外部に流出・悪用される。	○	○	○
(4)	利用未承認のクラウドストレージに機密情報が持ち出され、外部に流出・悪用される。	○	○	○
(5)	時間をかけて機密情報を検索し、情報管理サーバに不正にアクセスされる。	○	○	○
(6)	勘定系サーバやメールサーバなどに不正にアクセスされ、情報が改ざんされる。	○	○	○
(7)	勘定系サーバやメールサーバなどへの不正アクセスにより、システムパフォーマンスの低下やシステムダウンが発生する。	○	—	○

I.　ログによる従業員の行動監視

リモートワークでは、管理者目視による従業員の行動確認が難しく、オフィス勤務時と比較して、相対的に不正行動を把握することが困難です。欧米金融機関では、従業員の不正行動を端末ログベースで監視する文化が根付いていることから、働き方の変化についてもリモートワーク移行へと迅速に対応することができています。

ログ監視を導入することで、明らかに怪しい行動を即座に把握・対処できるとともに、相関的に不審な行動を炙り出すことが可能になります。また、行動監視していること自体が、従業員の不正に対する抑止力となることが期待できます（図表3参照）。

一方で、リモートワークにより働き方が多様化することに対して、不正行動かどうかを識別する監視ロジックの適宜見直しを行うことが不可欠です。ログ監視の有効性を維持・確保するためには、導入後のメンテナンススキルを持った人員と運用リソースの確保が重要になります。

【図表3　異常行動の監視対象例】

監視対象例
• 機密ファイルへの過剰なアクセス • 異常な量のデータアップロードまたはダウンロード • 通常と異なる時間帯、休暇中のアプリケーションまたはデスクトップの使用 • 端末画面のスクリーンショット • ファイルまたはフォルダの過剰な削除 • 危険なウェブサイトへのアクセス • 未承認のクラウドサービスまたはファイル共有サービスへのアクセス • 個人アカウントへのメール送信・メール転送 • 未許可のデータコピー（端末側へのコピー、リムーバブルメディアへのコピー） • 内部ネットワークの探索（PINGコマンドの投入など）

II.　DLP（Data Loss Prevention）

これまでも情報漏洩に対する出口対策として認知されていたDLPですが、リモートワーク環境においても有効な対策となります。

DLPは、データの移送を制限・制御することで機密情報の流出・改ざんを防止するツールであり、国内でも「メールでのファイル送信」や「クラウドサービスへのファイルアップロード」の制御などに使用されています。
欧米金融機関においては、データ自体に着目した統制を模索しており、DLPを活用して、重要データに対する一段高いコントロールを実現するケースが見られます。

事前に重要データの仕分けをすることで、インターネット空間上でのビジネスの柔軟性を維持したまま、重大なインシデントに繋がるデータのみ厳しく制御することができます。一方で、すべての情報を仕分ける必要があるため、準備・運用負荷を考慮してDLPの活用方法を決めることが重要です。

III.　誓約書の提出による従業員責任の明確化

リモートワークにより、組織が統制可能な範囲を超えて多くの脅威にさらされる可能性があります。たとえば、個人所有スマートフォンで端末画面を撮影する行為は端末やサーバ上に痕跡が残らないため、技術的対策によるリスク低減が困難です。

これらのリスクに対して、欧米金融機関でも国内金融機関と同様に、「情報セキュリティポリシー遵守に係る誓約書」を従業員に提出させることで、リスク低減が図られています。誓約書を提出する行為自体が従業員自身に責任を意識するきっかけを与えることとなり、また、違反した場合の罰則規定を明確にすることで内部不正全般に対する抑止効果が期待できます。

技術的な対策の導入には費用や期間を要することから、暫定処置として誓約書による統制強化を行ったうえで、並行して技術的対策の導入を進めることも有効です。

4. おわりに

リモートワークにおける内部不正に対するセキュリティ対策は、仕組みの導入だけでなく、導入した後の運用も十分に考慮する必要があります。たとえば「ログによる行動監視」を導入する場合は、「適切なツールの選定」「既存システムへの影響確認」「ログの取得可否・監視シナリオの管理実効性確認」といった対応だけでなく、常時監視による従業員のモチベーションへの影響についても検討する必要があります。

また、ツール導入などの技術的な対策とともに、リモートワークに関する情報セキュリティポリシーやルール・ガイドラインを整備し、教育・啓発活動などにより社内へ浸透させることでガバナンスを強化することも必要です。各金融機関においては、自組織のリモートワーク環境におけるリスクの洗い出し・評価を実施し、脆弱性を特定して対策を講じていくことが重要です。

KPMGコンサルティング株式会社
シニアマネジャー　門野 仁
シニアコンサルタント　大内 諭

KPMGコンサルティング株式会社

03-3548-5111
kc@jp.kpmg.com

home.kpmg/jp/kc