退職者による
セキュリティ事故が増加中――
テレワーク環境における内部不正対策

コロナ禍によりテレワークの導入が急速に進んだが、併せて様々な課題が浮上している。退職者によるセキュリティ事故・情報漏えいの報告が増加傾向にあり、注意が呼びかけられている。特に、テレワーク下にあった社員の退職には十分な対応が必要だ。これまで「始め方」ばかりがフォーカスされてきたテレワークだが、適切な「終り方」についても、今このタイミングで知っておこう。

本ホワイトペーパーは、内部不正対策についての基礎知識をまとめたものだ。また、テレワークやBYODとの関わりにおいて、考え方や手順も具体的に紹介している。テレワークやセキュリティの担当者には、ぜひ、ご一読いただきたい。

INDEX

【調査結果】「中途退職者」による情報漏えいが 36.3% に増加　「誤操作・誤認など」を抜き過去最多に

IPA の「企業における営業秘密管理に関する実態調査 2020 調査実施報告書」は、退職者による情報漏えいが増加傾向であることを報告している。2016 年の調査時に１位だった「誤操作、誤認」などが 21.2% とほぼ半減したのに対し、「中途退職者」によるものは最多で 36.3%。前回調査（28.6%）よりも大きく増加している。（図 1）

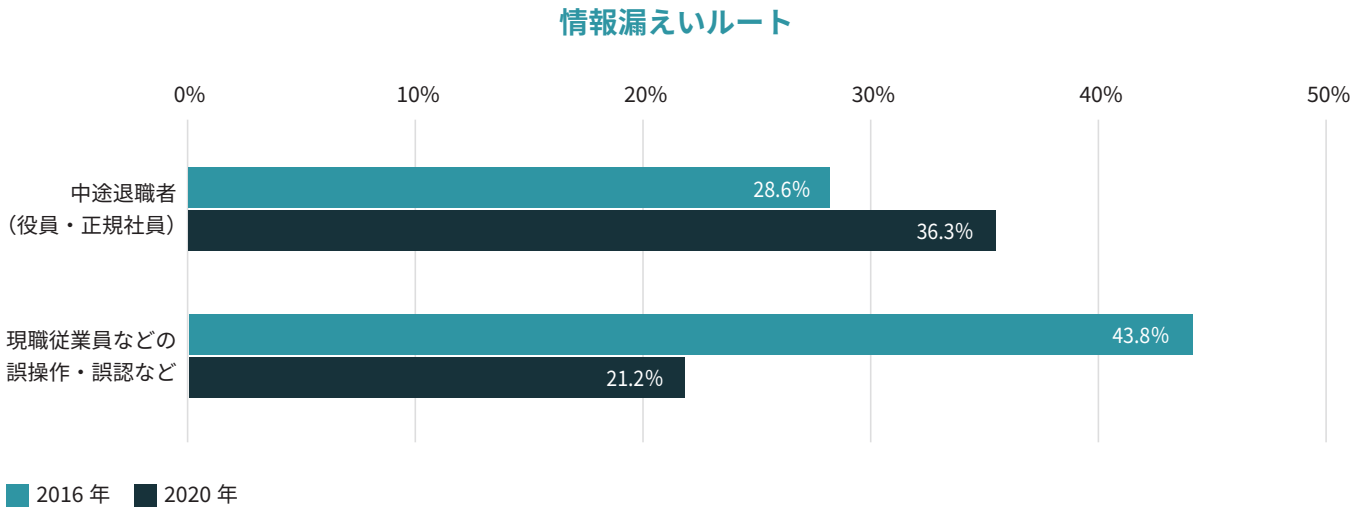
2021 年 1 月に明らかになった通信業大手 A 社 での技術情報漏えい事件も記憶に新しい。同ケースは、退職者がアクセス権のある社内サーバにログインし、メール添付で自分宛に送信するという、極めて安易な方法でデータが持ち出された点で耳目を集めた。
相次ぐ事件・事故の報告を受け、内部不正による持ち出し対策を講じる企業も増えているようだ。前述の IPA の調査によれば、従業員と秘密保持契約を締結する企業は過半数の 56.6% となっている。

日本における企業の情報漏えい対策の現状としては、不注意・管理不備などによる事故の対策は進んでいると見てよいだろう。しかし、内部不正については、まだまだ検討の余地がある。

一方、米国では、コロナ禍のテレワークを背景にした「大量離職時代（Great Resignation）」が取り沙汰されている。同国における離職者数は 2021 年 11 月だけで約 450 万人と、過去最大数を記録した。ここでも懸念されているのが、退職時の情報の持ち出しだ。
ちなみに日本では、2020 年の段階では、現在の米国に見るような大量離職現象は見て取れなかった。しかし、より新しい各種調査・報道などによると、転職者の数は増加に転じているようだ。テレワークにより、意図せず転職活動がしやすい環境が整ったことも一因だろう。
今後も、人材の流動性が高まっていくことを視野に入れれば、退職者によるセキュリティリスクの軽減は、早急に取り組むべき重要な課題である。

※1　出典：IPA「企業における営業秘密管理に関する実態調査 2020 調査実施報告書」2020 年 3 月 18 日
https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html

※2　出典：U.S. BUREAU OF LABOR STATISTICS「Job Openings and Labor Turnover Survey News Release」（2022 年 1 月 4 日）
https://www.bls.gov/news.release/archives/jolts_01042022.htm



出典：IPA「企業における営業秘密管理に関する実態調査 2020 調査実施報告書」2020 年 3 月 18 日（抜粋）

テレワーク環境は、内部不正の温床に！？
注目したいのは、その「終り方」と「BYOD」

ここでは、内部不正の増加と切っても切れない関係にある、テレワークについて掘り下げておこう。
2019 年 4 月より順次施行されている働き方改革関連法案。それ以前からもワークスタイルは多様化しており、テレワークは定着の途上にあった。その導入には、環境構築に加えて、セキュリティ対策が重要だ。多くの企業では、これら新しい環境への適応は、数年程度の期間をもって計画されていた。しかし、コロナ禍により計画を前倒す必要に迫られ、不十分な内容での導入となったというケースも多数見られる 。
オフィスと比較して、周囲の目が届かないテレワーク環境は、不正に対する心理的なハードルを下げやすい。内部不正対策については退職時の対応が特に重要だが、中には導入方法ばかりで、離職のことは考えていなかったという担当者も。テレワークを導入するなら、同時に安全な「終り方」について、必ず対応を決めておこう。その方向性は大きく次の 2 つだ。

- ✓ 退職者 ID の把握と確実な削除
- ✓ 退職者の手元にデータを残さない

退職者 ID の把握と確実な削除

まずは退職者の利用していたシステムを洗い出し、そのシステムにおいてどのような権限を付与されていたかを即時に把握することが必要になる。そこから、必要に応じて ID の削除、権限変更などを適用する。手動での作業は負荷が高いという場合には、ID 管理ツールなどの導入が望ましい。
権限管理については、在職時から適切に行うことが前提だ。管理者が常に状況を把握できる状態になっていれば、急な退職があってもあわてることはないだろう。

退職者の手元にデータを残さない

テレワークの場合は、特に、「退職者の手元にデータを残さない」点 に注意したい。ここでは、データを管理外の端末に保存させないこと、社員のローカル環境に保存させないことが重要だ。
さらに、BYOD（Bring your own device）についても注目したい。テレワーク用の社給端末を用意するコストを考えれば、BYOD は極めて現実的な選択だ。社員は使い慣れた端末を業務に利用でき、生産性向上・効率アップが期待できるなどメリットは多い。テレワーク開始とともに BYOD も始めたという企業は多いだろう。
内部不正対策の観点からは、BYOD の端末にデータを残さないアクセス方式を準備することが重要になる。

内部不正 のリスクを軽減するために、システム管理者がすべきこと

ここでは、内部不正のリスクを軽減するためにすべきことを、次の 3 つの項目から説明しよう。

1．ガバナンスの強化

企業のセキュリティ対策を行う際、重要なのが情報セキュリティの内部統制を強化することだ。まずは、事業目的に合致した戦略を立てること。企業として、どのような方針で情報セキュリティと向き合うのかを策定することが求められる。

また、リスク強化委員会など、セキュリティ対策部門の設置は必須だ。その上で、外部指標による客観的評価を採用する。ISMS（情報セキュリティマネジメントシステム）などの管理の仕組みの導入、そのほか、個人情報に特化したものなら、P マークもその代表的な指標となっている。

- ✔ セキュリティ対策部門の設立
- ✔ 外部評価を利用する

2．リスク評価

全体の方針が定まったら、実際に業務を遂行する上で必要になるルールの策定などに着手する。例えば、何を機密情報とするか、といった定義を行うことや、リスクになるもの・ならないものの棚卸を行うなどだ。これらをしっかり切り分けることで課題が洗い出され、存在するリスクを認識できるようになる。

さらに、社外とは、どのようなツールを使ってデータをやり取りするのか、従業員の端末のインターフェースはどうするのか、細部にわたるルール作りを行う。

- ✔ 機密情報の定義
- ✔ リスクの棚卸
- ✔ 細部にわたるルール作り

3．システムに対するセキュリティ強化

内部不正のリスクをなくすために、どのようなツールが効果的に利用できるのか、具体的に挙げておこう。

メールセキュリティ

不適切なメール転送など、セキュリティポリシー違反をシステムでチェック。メール上長承認やログ監査で情報漏えいを未然に防ぐ。

セキュアストレージ

アクセスログ管理やダウンロード制限などの機能を付帯したセキュアな法人向けストレージならば、安全にデータのやり取りが行える。

特権 ID 管理

必要な時に必要な人に正しい権限を付与する仕組みをシステム化することで、異動・退職後の ID の不正利用を防止する。

MAM（モバイルアプリケーション管理）

モバイル端末を利用するなら、管理ツールが必要だ。デバイスを OS レベルで一括管理する MDM（モバイルデバイス管理）と比較して、MAM はアプリケーション単位で管理できるのが特長だ。各種機能の提供により、セキュリティ対策、公私の切り分けなどを可能にする。

DLP（Data Loss Prevention）

機密情報の利用制御、監視、操作のトレース（追跡）を行う。ユーザーではなく「データそのもの」を監視し、持ち出しなどの危険を察知した際にアラートを出す。

テレワークを安全・快適に「moconavi」によるモバイルアプリケーション管理

「moconavi」は、端末や通信経路に一切データを残さずに、社内システムやクラウドサービスとのセキュアな連携を実現する、クラウド MAM の代表的な製品だ。業務で利用するデータを一切手元の端末に残さない仕組みになっており、過失・故意にかかわらず、情報漏えいのリスクを元から断つことができる。

「moconavi」を起動し、ログインすると、セキュアコンテナ（仮想環境）上から、API 連携する業務アプリやクラウドサービスへ全にアクセスできるようになる。

対応 OS：iOS・iPadOS、Android、Windows
対応業務アプリ：認証＆セキュリティ、情報共有、UC＆コミュニケーション、顧客管理・ワークフロー　ほか

なお、「moconavi」はデータをローカルにダウンロードできないだけではなく、管理下にあるアプリのスクリーンショットを禁止することや、強固な認証に対応するなどの機能も有しており、テレワークや BYOD に最適な MAM となっている。

また、モバイル導入に際しては、デバイス管理 も検討に上がることが多い。しかし、BYOD を視野に入れているなら、MAM を選択するのが賢明だろう。デバイス管理はその性質上、端末を OS レベルでまるごと管理するのが特長であり、強みである端末初期化などの機能は BYOD とは相性が悪い。個人用の端末に強制的に一括制御を行うわけにはいかないからだ。しかし、資産管理の観点からはデバイス管理は、非常に優れたツールでもある。シーンやニーズに合わせて使い分けることが肝要であり、併用を視野に入れてもいいだろう。

情報漏えいを予防するために社員教育を行っても、成果にはばらつきが出てしまう。内部不正のような悪意あるケースでは、教育では太刀打ちできない。だからこそ、セキュリティの責任を社員個人に負わせるのではなく、システムで例外なくカバーすることが必要だ。

「moconavi」についてさらに詳しく知りたい方はこちら ❯

recomot

recomot Inc.