OPTiM 情報漏洩・サイバーセキュリティ対策ナビ

情報漏洩対策チェックリスト

自社で「塞がれていない漏洩ルート」を見つける30項目

会社名・部署：　　記入者：　　記入日：　　年　　月　　日

使い方：できているものに✓を入れてください。✓が付かなかった項目が、自社で塞がれていない漏洩ルートです。グループごとに「できている数」を書くと、弱い分野がわかります。

A. 外部からの攻撃への備え

8項目　できている数：＿＿／8

1	☐	社員が使うクラウドサービス（メール・ファイル共有など）に、多要素認証を設定している
2	☐	社内で利用しているSaaSを一覧で把握している
3	☐	パスワードの使い回し禁止など、パスワードのルールを決めてシステムで強制している
4	☐	PC・スマホのOSやソフトウェアを、最新の状態に保てているか確認できる
5	☐	VPN機器やサーバーなどの脆弱性情報を確認し、更新している
6	☐	全端末にウイルス対策ソフト（またはEDR）が入り、動いていることを確認できる
7	☐	不審なメールを開いたときの報告先・対応手順を社員が知っている
8	☐	主な委託先・取引先のセキュリティ対策状況を確認している

B. 紛失・盗難への備え

9項目　できている数：＿＿／9

9	☐	会社が貸与しているPC・スマホを、台帳で「誰が・どの端末を」持っているか把握している
10	☐	端末をなくしたとき、遠隔でロックできる
11	☐	端末をなくしたとき、遠隔でデータを消去できる
12	☐	PCのストレージを暗号化している（BitLocker・FileVaultなど）
13	☐	すべての端末に画面ロック・パスコードを強制している
14	☐	USBメモリなど外部記録媒体の利用を制限している
15	☐	紛失したときの連絡先と、24時間以内の対応手順が決まっている
16	☐	機密書類の施錠保管・シュレッダー処理のルールがある
17	☐	使わなくなった端末・記録媒体を、データを消去してから廃棄している

C. 人のミス・内部への備え　9項目　できている数：＿＿／9

- 18 ☐ 退職・異動した人のアカウントを、当日中に削除・変更している
- 19 ☐ 社員ごとのアクセス権限を、業務に必要な範囲に絞っている
- 20 ☐ メール誤送信対策（送信保留・宛先確認など）を導入している
- 21 ☐ ファイル共有リンクの公開範囲を定期的に点検している
- 22 ☐ 会社が許可していないアプリ・SaaSの利用を把握・制限できる
- 23 ☐ 私物端末を業務に使う場合のルールがある（または禁止している）
- 24 ☐ 生成AIに入力してよい情報・いけない情報のルールがある
- 25 ☐ 重要なデータへのアクセスや操作のログを記録している
- 26 ☐ 年1回以上、情報セキュリティの研修や訓練を行っている

D. 体制・ルール　4項目　できている数：＿＿／4

- 27 ☐ 自社のどこに、どんな重要情報があるかを把握している
- 28 ☐ 情報セキュリティの責任者が決まっている
- 29 ☐ 情報漏洩が起きたときの報告先（個人情報保護委員会・取引先など）と手順を決めている
- 30 ☐ 重要データのバックアップを取り、復元できることを確認している

チェック結果

できている数（合計）：＿＿＿＿＿ ／30

チェック数	状態	次にやること
26〜30個	主なルートは塞がれています	運用が形だけになっていないか、年1回は点検しましょう
16〜25個	一部のルートが開いています	チェックが付かなかったグループ（A〜D）から優先的に対策しましょう
15個以下	多くのルートが開いています	まず「多要素認証」「端末の一元管理」「退職者アカウントの削除」の3つから始めましょう

まず優先したい3つ：①多要素認証（クラウドへの不正アクセスを大きく減らせる）　②端末の一元管理（MDM・暗号化・リモートロック／ワイプ）　③退職者アカウントの削除を含むID管理

各項目の解説は「【徹底解説】情報漏洩の仕組みとその対策」をご覧ください。
https://www.optim.co.jp/optim-biz-premium/cybersecurity-navi/articles/info-leak-mechanism-countermeasures.html