情報管理・労務リスク 実務セミナー

社労士・人事のための情報管理実務

最新裁判例に学ぶ 情報漏えい・内部不正への実務対応

～ 平時の「備え」と有事の「初動」 ～

講師　**杜若経営法律事務所　弁護士　佐藤 浩樹**

開催日時　2026年　7月　28日（火）　13：00　～　14：00

講師紹介

弁護士 佐藤 浩樹 さとう ひろき

杜若経営法律事務所 ｜ 第一東京弁護士会（75期） ｜ 経営法曹会議会員

使用者（企業）側の労務問題を専門に、問題社員対応・ハラスメント・団体交渉など、経営の現場で起こる労使トラブルの解決と予防を支援。

略歴

青山学院大学法学部 卒業／慶應義塾大学法科大学院 修了

令和3年 司法試験合格、令和4年 弁護士登録・杜若経営法律事務所 入所

著作

『就業規則の法律相談Ⅰ・Ⅱ』（共著・青林書院）

講演

第65回全日本病院学会「医療介護求人サイト・人材紹介会社からの違約金請求トラブルに巻き込まれないために」 ほか

労務ネット ｜ 使用者側労務問題ひとすじ・50年の実績を持つ専門事務所

AGENDA

本日のテーマ

01

退職者による情報持ち出しと懲戒処分

「持って行かれた」後で会社は何ができるか

02

内部通報・社内調査と秘密保持

調査の秘密保持と公益通報者保護のはざま

03

メール・PCのモニタリングとプライバシー

どこまで「見てよい」のか、その線引き

04

情報漏えい・サイバー事故の初動と委託先管理

有事の対応費用は億単位になりうる

INTRODUCTION

なぜ今「情報管理」が労務の問題なのか

働き方の変化

テレワークとクラウド利用が定着。会社の情報は社外端末・私物デバイスからもアクセスされる時代に。

内部不正の増加

退職者による情報の持ち出しが、組織の重大な脅威の上位を占め続けている。

サイバー攻撃

ランサムウェア等による被害が拡大。委託先経由の漏えいも後を絶たない。

労務管理の問題でもある

情報の管理・持ち出し・漏えいへの対応は、就業規則・規程・誓約書という「人」のルールづくりが出発点。

情報を守る取り組みは、IT の問題であると同時に「労務管理」の問題でもある。

OVERVIEW

関係する法律と「秘密情報・営業秘密」の関係

「秘密情報」は広い概念

秘密情報

会社が事業上保有し、社外への漏えい・業務外の利用を禁ずる情報（法律用語ではない）

営業秘密

不競法上の保護（3要件を満たす狭い範囲）

個人情報保護法

漏えい等の際、個人情報保護委員会への報告と本人通知が義務（令和4年4月〜）。

不正競争防止法

「営業秘密」の侵害に差止め・損害賠償・刑事罰。ただし“秘密管理”が前提。

労働法（就業規則）

懲戒・秘密保持・モニタリング・退職金不支給などの根拠。会社の備えの中心。

POINT　「営業秘密」として守れなくても、就業規則・規程違反として懲戒できる。両輪で備える。

THEME 1

退職者による情報持ち出しと懲戒処分

競合への転職予定者が大量データを持ち出した ― 会社はどこまで処分できるか

架空事例

CASE

大手商社A社の総合職Xは、競合他社への転職が内定（退職予定は約2か月半後）。退職を申し出た後、**わずか2日間で**、業務用クラウド（Box）から **約1万1,000件・24GB** の業務ファイルを個人のGoogleドライブへフォルダごと一括アップロード。中には **約90か国分の投資判断基準や経営会議の付議資料** も含まれ、競合に勤める婚約者へも社外秘を5回送信していた。A社はXを **懲戒解雇・退職金不支給** とした。

この事例の「問題点」

Q1 持ち出された情報は「営業秘密」と認められるか（社内の秘密管理が不十分なのでは？）

Q2 退職を決めた従業員を、そもそもどこまで懲戒できるのか

Q3 懲戒解雇・退職金不支給は重すぎて、後から「無効」と争われないか

Q4 情報はすでに社外へ。損害賠償だけで本当に取り戻せるのか

実際の裁判例：伊藤忠商事事件

東京地判 令和5年11月27日（退職予定者が業務データを個人クラウドへ持ち出した事案）

事案の概要（重要な事実）

- 退職予定の総合職が、わずか2日間で 1万1,320個・約24GB を個人のGoogleドライブへフォルダごと複製
- 約90か国分のハードルレート（投資判断基準）や経営会議（HMC）の付議資料を含む
- 競合商社に勤める婚約者へ機密情報を5回メール送信
- 社内ログ監視で当日検知 → 18日後に懲戒解雇・退職金不支給

裁判所の結論

- **懲戒解雇は有効**
- **退職金の全額不支給も適法**
- 金銭的損害の立証がなくても、処分は重くてよい

注目　**持ち出した情報は「営業秘密」とは認められなかった（→次頁）。それでも就業規則違反として重い処分が認められた。**

ここがポイント

1 「漏えい」でなくても懲戒できる

個人クラウドへの保存は、社外への「漏えい」とは認められなかった。

しかし、機密情報の 目的外利用・公私混同・情報管理規程違反 として懲戒事由に該当。

→ 「外に出ていないから大丈夫」は通用しない。

2 「営業秘密」の壁＝秘密管理性

情報の多くは「営業秘密」と認められなかった。
理由は秘密管理性の不足：

- 旧部署の約50名が、担当外の案件にもアクセスできた
- 「課長の許可を得る」運用は書式も申請実績もなく形骸化
- 過去のレストラン一覧まで混在し、「極秘」表示もなかった

→ 不競法で守れなくても、就業規則違反としては問える。

懲戒処分の「有効・無効」を分けるもの

情報持ち出しの「特殊性」　一度流出すると回収困難・損害立証も困難。事後の損害賠償では実効性に乏しいため、金銭的損害がなくても懲戒解雇が比較的広く認められる。

有効に働く事情

- 機密情報の目的外利用・公私混同にあたる
- 信頼関係を破壊する重大な非違行為である
- 就業規則に懲戒事由の根拠規定がある
- 金銭的損害の立証がなくても処分できる

無効となる場合（労契法15条）

- 懲戒事由の根拠規定がない（労基法89条9号）
- 情報の性質・悪質性に照らし処分が過度（相当性を欠く）
- 弁明の機会など手続的な相当性を欠く

会社の守り方は「二段構え」— 不競法 と 就業規則

① 不正競争防止法で守る

- 合意がなくても差止め・損害賠償・刑事罰
- ただし「営業秘密」3要件を満たすことが前提
- **ハードルは高い（特に秘密管理性）**

② 就業規則・誓約書で守る

- 目的外利用・私的保存の禁止を懲戒事由に
- 必要なのは「合意」と「合理性」（判断は緩やか）
- **営業秘密でなくても処分できる**

営業秘密の3要件

秘密管理性	秘密として管理
有用性	事業に有用な情報
非公知性	公然と知られていない

両輪で備える

「一切漏らさない」式の包括的合意は無効も（東京地判H20.11.26）。対象を具体的に特定することが有効性のカギ。

退職後も秘密を守らせる – 「有効」と「無効」の境界

前提　退職後の秘密保持義務は、就業規則・誓約書など明文の根拠（合意）が必要。その合意は「合理性」が認められる場合に限り有効（情報の性質・範囲・価値、退職前の地位で判断）。

有効となる場合

- 秘密情報を具体的に特定・例示（顧客名簿・取引内容／製造過程・価格 等）
- 従業員がその情報を熟知する地位にあった
- 代償措置（退職金の上乗せ等）がある

無効となる場合

- 「一切漏らさない」式で対象が不明確（定義・例示がない）
- 対象が広範・抽象的に過ぎる（職業選択の自由を不当に制限）
- 代償措置がない

有効例　ダイオーズサービシーズ事件（東京地判 H14.8.30）　**無効例**　包括的合意を無効とした事案（東京地判 H20.11.26）

平時の「5つの対策」と社労士の実務ポイント

情報漏えい対策の5つの目的（経産省ハンドブック）

1. **接近の制御**　アクセス権を必要な人に限定
2. **持出し困難化**　私物USB・私用メール送信を制限
3. **視認性の確保**　アクセスログを記録・確認
4. **認識向上**　「マル秘」表示で秘密と気づかせる
5. **信頼関係の維持**　適正な評価・処遇で動機を抑える

社労士の先生の実務ポイント

- 「営業秘密」該当性に頼り切らない。目的外利用・私的保存を就業規則で懲戒事由に。
- 秘密管理性を平時から確保：アクセス制限・マル秘表示・秘密の特定（明文化）。
- 退職金規程に不支給・減額条項を整備。根拠規定があってこそ不支給は正当化できる。
- 退職の申し出を受けたら、アクセス権の見直しとログ確認をルール化。

規定例：就業規則の条項 と 秘密情報管理規程

就業規則の条項例

〔秘密保持〕
社員は、在職中・退職後を問わず、会社の秘密情報を業務上必要な目的以外で使用し、又は会社の許可なく第三者に開示・提供してはならない。

〔懲戒事由〕
前項に違反し、又は違反しようとしたときは、第○条の懲戒処分を行う。

〔誓約書提出〕
会社が必要と認めるときは、在職中・退職後の秘密保持につき誓約書を提出する。

秘密情報管理規程の骨子

1. 適用範囲（役員含む）
2. 秘密情報の定義
3. 情報の区分（極秘・マル秘等）
4. 管理責任者の設置・権限
5. 漏えいの禁止
6. 目的外使用の禁止
7. 誓約書の提出義務

ポイント　就業規則は概括的に／変わりやすい詳細は管理規程で（労契法12条：誓約書は就業規則より不利にしない）。

書式例：秘密保持誓約書（入社時／退職時）

入社時の誓約書

- 就業規則・情報管理規程を遵守すること
- 秘匿情報の例示（製品技術／原価・価格／顧客名簿・販売資料 等）に同意
- 在職中・退職後の開示・目的外使用の禁止
- 退職時・要求時の返還・消去
- 異動・PJ参加・退職時に改めて誓約書を提出

退職時の誓約書

- 貸与機器・データを全て返還し、私物端末・クラウドに複製を残さない／消去したこと
- 在職中に知り得た秘密情報を退職後も漏えい・利用しないこと
- 秘密情報の範囲は別紙のとおり（具体的に特定）
- 違反時は損害賠償・退職金不支給の対象

最も有効　退職時は対象を具体的に特定でき有効性が高い。代償措置（退職金の上乗せ等）でさらに有効性UP。

THEME 2

内部通報・社内調査と秘密保持

ハラスメント申告者が秘密保持に反して経営陣へ大量メール ― 処分できるか

02

架空事例

CASE

外資系企業B社の従業員Yは、上司からハラスメントを受けたとして人事部へ申告。会社は調査の結果、**「ハラスメントとは認められない」**と判断した。これに納得しないYは、**“調査内容を口外しない”との誓約と業務命令に反し**、CEOを含む経営陣や多数の管理職に対して、上司を強い言葉で非難するメールを繰り返し送信した。会社はYを**譴責処分とし、その後普通解雇**した。

この事例の「問題点」

Q1 調査の秘密保持を従業員に課し、その違反を理由に処分できるか

Q2 「内部通報」なら公益通報者保護法で守られ、処分できないのではないか

Q3 申告した内容が真実と認められない場合、どう扱うべきか

Q4 経営陣への大量メール送信という「手段」は許されるのか

実際の裁判例：モルガン・スタンレー事件

東京地判 令和6年6月27日（ハラスメント申告者の譴責処分・普通解雇の事案）

事案の概要（重要な事実）

- 韓国籍のED（年収約1億円）が、上司のハラスメントと国籍差別を申告
- 会社は調査の結果「ハラスメントとは認められない」と判断
- 守秘の誓約・度重なる業務命令に反し、約4か月でCEO・経営幹部へ15件超のメール
- 「応じねばMD30名に送る」と予告し、会社を「北朝鮮」になぞらえ非難

裁判所の結論

- **秘密保持・業務命令は有効**
- **譴責処分・普通解雇も有効**
- 不正目的は否定も、真実性・手段相当性を欠き保護されず

整理　国籍差別など「通報対象事実」に当たる部分は懲戒不可。ただしハラスメント申告自体は直ちには通報対象事実でない。

申告・公表が「保護される」3つの要件

1

真実性／誤信相当性

申告内容が真実、または真実と信じる相当な理由があること。

2

不正の目的でないこと

私的な報復など、不当な目的でないこと。

3

手段の相当性

伝える相手・方法・態様が、目的に照らして相当であること。

保護される場合／されない場合

公益通報に当たる場合 → その通報を理由とする懲戒はできない。　**当たらない場合 →** 上の3要件で判断。本件は、①発言は8年で5回・口調も概ね穏やかで加害者は5年連続で原告をMD推薦＝真実性を欠き、③経営幹部への大量送信や「北朝鮮」になぞらえる非難＝手段も相当でない。よって保護されず、譴責・普通解雇は有効とされた。

実務への活かし方（内部通報・調査）

社労士の先生のポイント

- 申告・通報は正面から受け止めつつ、調査で知った情報の「伝達範囲」を事前にルール化する。
- 通報を理由とする不利益取扱いの禁止と、調査協力・秘密保持義務を、規程と書面の両方で定める。
- 「真実か」「手段は相当か」を意識して、対応記録を残す。

△ 改善を要する例

口頭で「内密に」と伝えるだけ。調査協力や守秘の根拠規定がない。

◎ 理想の規定例

調査時の秘密保持・伝達範囲・通報者保護を規程化し、関係者から守秘の確認書を取得する。

THEME 3

メール・PCのモニタリングとプライバシー

上司が部下の私用メールを監視 — どこまでが許されるのか

架空事例

CASE

C社の事業部長Zは、部下Wが私用メールに書いた自分への悪口を、**Wが誤ってZ本人へ送信した**ことから、その後**Wの社内メールを継続的にチェック**するようになった。社内メールはアドレスが公開され、パスワードも氏名のままという環境だった。これを知ったWは、**「プライバシーの侵害だ」**として、会社と上司Zに損害賠償を求めて訴えた。

この事例の「問題点」

Q1 会社は、従業員のメールやPCをどこまで監視できるのか

Q2 監視が「プライバシー侵害」になる線引きはどこにあるのか

Q3 規程やルールがないまま、上司の判断で監視を始めてよいのか

メール監視 –「適法」と「違法」の境界

東京地判 平成13年12月3日（F社Z事業部事件）

本件はアドレスが社内公開・パスワードも氏名のままで、上司が容易に閲読できた環境。社内メールのプライバシー保護は環境に応じ低減し、目的・手段・態様が「相当な範囲」を逸脱したかで違法性を判断する。

適法（相当な範囲内）

- 監視する権限のある者が行う
- 情報漏えい防止など合理的な必要性がある
- 目的に照らし相当な手段・態様にとどまる

違法（プライバシー侵害）

- 監視する権限のない者が監視した
- 必要性がなく、個人的な好奇心から監視した
- 第三者に秘密にして恣意的な手段で監視した

本件
Zは事業部の最高責任者で監視の必要性があり、相当な範囲を逸脱しないとして、プライバシー侵害は否定された。

規定例：モニタリング規程に定める5項目

1. **目的** 業務上の必要性・情報漏えい防止 等を明示
2. **対象範囲** 社内メール・PC・ログ等／私物端末は本人同意
3. **方法** 閲覧範囲・手段を特定し、必要最小限に
4. **実施主体** 中立・公正な責任部署が実施（上司に委ねない）
5. **事前周知** 従業員へ事前に周知し予測可能性を確保

△ ルールなし

上司の判断でその都度メールを閲覧している。

◎ 規程化＋事前周知

目的を明示し、責任部署が必要最小限の範囲で実施する。

事前周知が「適法性のカギ」

THEME 4

情報漏えい・サイバー事故の初動と委託先管理

委託先の設定不備で大量の個人情報が流出 — 責任・費用・初動を学ぶ

架空事例

CASE

D市は、教育情報ネットワーク（MENET）の運用をIT企業Eに委託していた。ところが、Eの **ファイアウォール設定不備（DMZから内部へ全通信を許可＝設計と正反対）** が一因で外部から不正アクセスを受け、児童・生徒 **約4万8千人分の個人情報（アレルギー・既往症や口座情報を含む）が流出のおそれ** 。D市は原因調査・本人通知などの対応に追われ、その費用をEに請求できるかが問題となった。

この事例の「問題点」

Q1 委託先のミスによる漏えいで、誰がどのような責任を負うのか

Q2 漏えい時、会社は「何を」「いつまでに」しなければならないのか

Q3 原因調査や通知などの対応に、どれだけの費用がかかるのか

Q4 発生した費用を、委託先にどこまで求償できるのか

実際の裁判例：前橋市MENET事件

前橋地判 令和5年2月17日（児童・生徒 約4.8万人分の個人情報が流出のおそれ）

委託先に約1億4,298万円の損害賠償を命じた事案。賠償上限（契約金額）を超える認容となった。

本来的な義務だった

ファイアウォールを適切に設定する義務は“付随的”ではなく契約の本来的な義務 → 委託先の債務不履行が成立。

因果関係あり

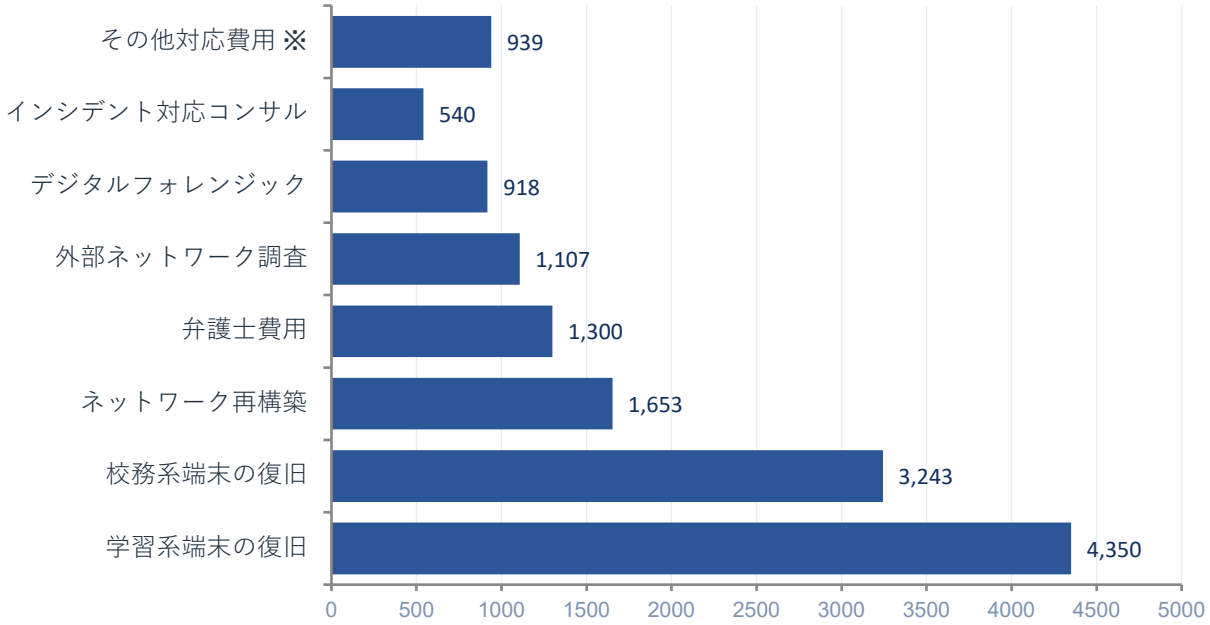
設定不備とバックドアが相まって被害が発生。設定不備がなければ不正アクセスは起きなかった。

責任限定条項も不適用

「賠償は契約金額を限度」とする条項も、設計書で複数回確認しながら放置した重過失ゆえ不適用。

求償できる場合 → 本来的義務違反＋因果関係あり（重過失なら責任限定条項も不適用）。
限定される場合 → 軽過失にとどまり、有効な責任限定条項があるとき。

漏えい対応にかかった費用（認容額）



¥

総　額

約1.4億円

（認容額の合計）

※「その他」＝時間外勤務手当・通知の郵送料・第三者委員会報酬 等　／　端末復旧は学習系3,822台＋校務系1,892台＝計5,714台

ベネッセ事件：賠償責任と事業ダメージ

① 何が起きたか

再々委託先の派遣SEが約4,858万人分を名簿業者へ売却（500社超に拡散）。USB接続スマホのMTP通信という当時の“盲点”を突いた手口。

② 裁判所の判断 – 誰が・いくら

委託元ベネッセ → 責任なし（過失も使用者責任も否定）

委託先シンフォーム → 末端の派遣SEの“故意”の漏えいに使用者責任（民法715条）

支払いはシンフォームのみ：1人 3,300円（慰謝料3,000円＋弁護士費用300円）

③ ベネッセHDの事業ダメージ

賠償命令とは別に会社が負った打撃

約260億円

対策・お詫び等の特別損失

▲82.2%

純利益が前年同期比で減少

約4,200→3,580億円

株式時価総額が約2か月で下落

教訓　法的な賠償責任を免れても、事業上の打撃は甚大。だからこそ委託元は、委託先の選定・監督を徹底する。

漏えいが起きたら：初動対応の流れ

1

個人情報保護委員会へ報告

速報：速やかに（目安3〜5日以内）／確報：原則30日以内（不正アクセス等は60日以内）

2

本人への通知

対象となる本人へ通知。問い合わせ窓口を設ける。

3

原因調査・フォレンジック

侵入経路・影響範囲を特定。ログ等の証拠を保全する。

4

二次被害の防止・公表検討

隔離・パスワード変更等。公表の要否とタイミングを判断。

実務への活かし方（委託先管理）

社労士の先生のポイント

- 委託契約に、安全管理措置・再委託の制限・報告義務・監査権・損害賠償を具体的に盛り込む。
- 委託先の「選定基準」を設け、契約後も定期的に点検・確認する。
- インシデント対応規程と報告フローを整え、有事に“誰が何をするか”を明確にする。

△ 改善を要する例

契約に「個人情報を適切に管理する」とだけ記載している。

◎ 理想の規定例

安全管理措置を具体化し、再委託の事前承認・報告・監査・賠償の各条項を明記する。

SUMMARY

平時の備え：場面別の規程・書式一覧

採用時	前職の秘密を持ち込まない旨の誓約書 ／ 秘密保持誓約書（秘匿情報を例示）
在職時	就業規則（懲戒・秘密保持）／ 秘密情報管理規程 ／ モニタリング規程 ／ BYOD・SNS利用ガイドライン
退職時	秘密保持・情報返還の誓約書（対象を特定）／ 競業避止に関する取り決め ／ アクセス権の見直し・ログ確認
有事	インシデント対応規程 ／ 報告・連絡フロー（社内・委託先・監督官庁）

SUMMARY

有事対応チェックリスト（初動）

- 事実確認・影響範囲の特定（ログを保全する）
- フォレンジック・第三者委員会の要否を判断
- 二次被害の防止（隔離・パスワード変更 等）
- 委託先がある場合、契約に基づき報告を求める
- 個人情報保護委員会への報告（速報 → 確報）
- 委託先への求償の検討
- 本人への通知／問い合わせ窓口の設置
- 公表・広報対応の方針決定