

取引先で情報漏えいが起きたら

委託先・取引先からの漏えいは「起きない」ではなく「いつか起きる」前提で備えるものです。連絡を受けてから30日のあいだに、誰が何をするかを1冊にまとめました。

担当者のあなたにとって

連絡を受けたときに困ること	このガイドがあると
何から手を付ければいいか分からない	最初の1時間にやる7つが、順番どおりに並んでいます
法律上の期限を自分で調べる時間がない	個人情報保護委員会のガイドラインどおりの期限を、時間軸で示しています
上司への第一報をどう書くか迷う	そのまま使える第一報の型があります
取引先に何を聞けばいいか分からない	報告に必要な項目を、取引先への確認依頼の文面にしてあります
判断を一人で背負わされる	平时に「誰が判断するか」を決めておくための社内説明スライドが付いています

まず知っておくこと：委託元にも報告の義務がある

個人データの取扱いを委託している場合、漏えいが委託先で起きても、委託元と委託先の双方が報告義務を負うのが原則です。委託先が委託元に通知すれば、委託先の報告義務は免除され、委託元が個人情報保護委員会に報告します。

期限の起点は、委託元が委託先から通知を受けた時点です。社内のいずれかの部署が知った時点で数え始めます。

0日目 委託先から連絡を受けた。 ここが起点	概ね3～5日以内 速報：分かっている範囲で 個人情報保護委員会へ	速やかに 本人への通知(状況に 応じて)	30日以内 確報：全項目を報告(不正の 目的のおそれがある場合は 60日以内)
-------------------------------------	---	-----------------------------------	---

報告が必要なのは、次の4つのどれかに当たる場合です(規則第7条)。

No	報告が必要な事態	例
1	要配慮個人情報が含まれる個人データの漏えい等(おそれを含む)	健康診断の結果、病歴など
2	不正に使われると財産的被害が出るおそれがある個人データの漏えい等	クレジットカード番号、ネットバンキングのID・パスワードなど
3	不正の目的で行われたおそれがある漏えい等	不正アクセス、ランサムウェア、従業員による持ち出しなど
4	本人の数が1,000人を超える漏えい等	顧客名簿の誤送信・流出など

不正アクセスやランサムウェアによる漏えいは、3に当たることがあります。判断に迷うときは、該当するものとして準備を進めます。

最初の1時間にやること

1. 記録を始める: 連絡を受けた日時・相手・内容をそのまま書き残す(この時刻が期限の起点になります)
2. 上司と責任者に第一報: 下の「第一報の型」で、分かっていることだけを伝える
3. 取引先に確認依頼を送る: 下の文面で、報告に必要な項目を聞く
4. つながり止める: 取引先との共有フォルダ・アカウント・VPNなど、自社につながる経路の一時停止を情シスと判断する
5. 渡している情報を洗い出す: その取引先に、何の情報を、何件、いつから渡しているか
6. 報告が必要かの見立て: 上の4つに当たりそうかを、責任者と確認する
7. 次の連絡時刻を決める: 取引先と「次はいつ、何を報告するか」を約束する

第一報の型（上司・責任者へ）

件名:【第一報】取引先【会社名】で情報漏えいの可能性(【月日 時刻】受領)

■何が起きたか

【会社名】から【月日 時刻】に連絡あり。【概要を1～2行】。

■当社への影響(現時点)

- ・当社が渡している情報:【例:顧客名簿 約〇件】
- ・漏えいの確認状況:【確定／可能性あり／不明】

■これからやること

- ・取引先に詳細の確認を依頼済み。次の報告は【月日 時刻】
- ・当社と取引先をつなぐ経路の停止を情シスと検討中

■判断をお願いしたいこと

- ・個人情報保護委員会への報告の要否(速報の目安は受領から概ね3～5日以内)

【氏名】

取引先への確認依頼（そのまま送れる文面）

件名:ご連絡いただいた件の確認のお願い

【取引先の会社名】

【ご担当者名】様

【自社名】の【氏名】です。ご連絡ありがとうございます。
当社でも法令に基づく報告の要否を判断するため、
現時点で分かっている範囲で、次の点をお知らせください。
分からない項目は「確認中」で構いません。

■お知らせいただきたいこと

- ・発生日時と、気づいた日時
- ・何が起きたか(概要)
- ・漏えいした、またはそのおそれがある情報の項目
- ・その件数(当社分の本人の数)
- ・原因(分かっている範囲で)
- ・二次被害やそのおそれの有無
- ・現在とっている対応(封じ込め・調査の状況)
- ・公表の予定
- ・再発防止のための措置

次のご報告は【月日 時刻】ごろにいただけると助かります。
どうぞよろしくお願いいたします。

【署名】

項目は、個人情報保護委員会への報告事項(規則第8条第1項)に合わせています。

個人情報ではない情報が漏れたとき

図面・価格・技術情報など個人情報ではない情報は、個人情報保護委員会への報告の対象外です。対応は契約(秘密保持契約など)に沿って取引先と進め、必要に応じて自社の顧客・取引先へ説明します。このため、平時に契約で「事故のときの連絡先と期限」を決めておくことが効きます。

平时にやっておくこと（漏えいする前提の備え）

備え	これで変わること	SCS
取引先ごとに、何の情報を何件渡しているかの一覧を作る	連絡を受けた日に影響範囲が分かる	★3 2-1-1
契約で、機密情報の扱いと事故時の役割・連絡期限を決める	連絡が遅れない。役割で揉めない	★3 2-1-2 ★3 2-1-4
社内で、事故の窓口・判断者・連絡先一覧を決める	第一報が1時間以内に回る	★3 6-1-1
渡す情報を必要な分だけにする	漏れたときの件数が小さくなる	★3 3-1-4

契約終了時に、情報とアクセス権の回収・廃棄を確認する	使っていない経路から漏れない	★4 2-1-5
----------------------------	----------------	----------

取引先の現状は、同じ基準で作った「委託先セキュリティ対策状況チェックシート」で確認できます。

相談先

相談先	こんなとき
個人情報保護委員会 (漏えい等報告フォーム)	報告対象に当たるとき。速報は分かっている範囲で出せます
警察(都道府県警察の サイバー犯罪相談窓口)	不正アクセス・ランサムウェアなど犯罪の可能性があるとき
IPA 情報セキュリティ安心相談窓口	技術的な対処の相談をしたいとき
Moshiru(moshiru.com/ info@moshiru.com)	何から手を付けるか一緒に整理したいとき。取引先への確認・社内報告・報告書の文面づくりを、打合せなし・テキストで支援します。初動の相談は無料です

このガイドについて

- ・ 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン(通則編)」(2026年6月一部改正)の3-5(漏えい等の報告等)に沿って作成しています。法的な判断が必要なときは、弁護士や個人情報保護委員会に確認してください
- ・ 2026年に改正個人情報保護法(令和8年法律第56号)が成立し、委託先から委託元への報告義務や速報の扱いなどの政令・規則が検討されています(個人情報保護委員会事務局、2026年10月1日資料)。規則が決まったら本ガイドを見直します
- ・ 出典:個人情報保護委員会 通則編ガイドライン https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/ / 政令・規則の整備に向けた基本的な考え方について② https://www.ppc.go.jp/files/pdf/261001_kihonntekinakanngaekatanitsuite_2.pdf / IPA SCS評価制度 要求事項・評価基準(2026年3月27日版)
- ・ 作成:Moshiru(岡崎悠太)。無料で使えます。社内で自由に改変・配布して構いません。Moshiruは、同じ取引について発注側と委託先の両方からの依頼は受けません