



社内説明資料 | 取引先からの情報漏えいへの備え

取引先で漏えいがあったとき、 迷わず動ける体制をつくります

「起きない」ではなく「いつか起きる」前提で、
窓口・判断者・連絡先を先に決めておく提案です

[部署名] [氏名] [日付]

お願いしたいこと

起きる前に、3つだけ決めておきたいです

1

窓口

取引先からの連絡を最初に受ける人

2

判断者

国への報告や取引の停止を決める人

3

連絡先一覧

取引先ごとの事故時の連絡先と、渡している情報

前提

取引先で起きても、報告するのは当社です

個人情報保護委員会のガイドライン

個人データの取扱いを委託している場合、委託元と委託先の双方が報告義務を負います。委託先が委託元に通知すれば、委託先の義務は免除され、委託元が報告します。

期限の起点は、当社のいずれかの部署が通知を受けた時点です。

IPA「情報セキュリティ10大脅威 2026」
組織編

2位

サプライチェーンや委託先を狙った攻撃
(8年連続)

期限

連絡を受けた瞬間から、時計が動き始めます

0日目

取引先から通知を受けた。
ここが起点

3～5日

速報:分かっている範囲で
国へ報告(目安)

速やかに

本人への通知(状況に
応じて)

30日

確報:全項目を報告。
不正の目的のおそれ
があれば60日

取引先の調査が終わるのを待っていると、速報の目安を過ぎてしまいます。

起きたとき

最初の1時間にやることは、7つに決めておきます

1 記録を始める(受けた時刻が起点)

2 判断者に第一報(分かっていることだけ)

3 取引先に確認依頼(報告に要る9項目)

4 つながりを止める(共有フォルダ・ID・VPN)

5 渡した情報を洗い出す(何を何件)

6 報告が必要かを見立てる(4つの事態)

7 次の連絡時刻を約束する(取引先と)

国への報告が必要なのは、4つの事態です

No	事態	例
1	要配慮個人情報の漏えい等	健康診断の結果、病歴
2	財産的被害のおそれがある漏えい等	カード番号、ID・パスワード
3	不正の目的のおそれがある漏えい等	不正アクセス、ランサムウェア
4	本人の数が1,000人を超える漏えい等	顧客名簿の流出

「おそれ」の段階で対象になります。迷うときは、該当するものとして準備を進めます。

漏れる前提で、4つの準備をしておきます

準備	変わること	SCS
取引先ごとに、渡している情報の一覧を作る	当日に影響範囲が分かる	★3 2-1-1
契約で、事故時の役割と連絡期限を決める	連絡が遅れない	★3 2-1-4
社内の窓口・判断者・連絡先を決める	第一報が1時間で回る	★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減る	★3 3-1-4

取引先の対策状況は、同じ基準のチェックシートで確認できます。

決めていただきたいこと

この5点を決めれば、準備は動き出します

項目	案
窓口	[部署名・氏名](不在時:[氏名])
判断者	[役職・氏名](不在時:[役職・氏名])
連絡先一覧の作成	[月日]までに[部署名]が作成
契約の見直し	次の更新から、事故時の連絡期限を追加
見直しの頻度	年1回([月])