

参考資料 1

情報漏えい対策一覧

第3章3－4で紹介した情報漏えい対策の一覧表を作成しました。
講ずる対策を検討する際等にご活用下さい。

1. 従業員等に向けた対策

①「接近の制御」

ページ

a. ルールに基づく適切なアクセス権の付与・管理	26
b. 情報システムにおけるアクセス権者のID登録	27
c. 分離保管による秘密情報へのアクセス制限	29
d. ペーパーレス化	33
e. 秘密情報の復元が困難な廃棄・消去方法の選択	33

②「持出し困難化」

【書類、記録媒体、物自体等の持出しを困難にする措置】

a. 秘密情報が記された会議資料等の適切な回収	35
b. 秘密情報の社外持出しを物理的に阻止する措置	35
c. 電子データの暗号化による閲覧制限等	35
d. 遠隔操作によるデータ消去機能を有するPC・電子データの利用	36

【電子データの外部送信による持出しを困難にする措置】

e. 社外へのメール送信・Webアクセスの制限	36
f. 電子データの暗号化による閲覧制限等（再掲）	36
g. 遠隔操作によるデータ消去機能を有するPC・電子データの利用（再掲）	36

【秘密情報の複製を困難にする措置】

h. コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管	37
i. コピー機の使用制限	37
j. 私物のUSBメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限	37

【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】

k. 秘密情報の消去・返還	39
---------------	----

③「視認性の確保」

【管理の行き届いた職場環境を整える対策】

a. 職場の整理整頓（不要な書類等の廃棄、書棚の整理等）	40
b. 秘密情報の管理に関する責任の分担	40
c. 「写真撮影禁止」、「関係者以外立入り禁止」の表示	41

【目につきやすい状況を作り出す対策】

d. 職場の座席配置・レイアウトの設定、業務体制の構築	41
e. 従業員等の名札着用の徹底	41
f. 防犯カメラの設置等	41
g. 秘密情報が記録された廃棄予定の書類等の保管	42

h. 外部へ送信するメールのチェック	42
i. 内部通報窓口の設置	43

【事後的に検知されやすい状況を作り出す対策】

j. 秘密情報が記録された媒体の管理等	43
k. コピー機やプリンター等における利用者記録・枚数管理機能の導入	44
l. 印刷者の氏名等の「透かし」が印字される設定の導入	44
m. 秘密情報の保管区域等への入退室の記録・保存とその周知	44
n. 不自然なデータアクセス状況の通知	44
o. PCやネットワーク等の情報システムにおけるログの記録・保存とその周知	44
p. 秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査	45

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 秘密情報の取扱い方法等に関するルールの周知	46
b. 秘密保持契約等（誓約書を含む）の締結	48
c. 秘密情報であることの表示	50

⑤「信頼関係の維持・向上等」

【秘密情報の管理に関する従業員等の意識向上】

a. 秘密情報の管理の実践例の周知	52
b. 情報漏えいの事例の周知	52
c. 情報漏えい事案に対する社内処分の周知	52

【企業への帰属意識の醸成・従業員等の仕事へのモチベーション向上】

d. 働きやすい職場環境の整備	53
e. 透明性が高く公平な人事評価制度の構築・周知	53

2. 退職者等に向けた対策

①「接近の制御」

a. 適切なタイミングでのアクセス権の制限	56
-----------------------	----

②「持出し困難化」

【退職予定者に対する特有の措置】

k. 社内貸与の記録媒体、情報機器等の返却	57
-----------------------	----

【従業員等に向けた対策（再掲）】

（書類、記録媒体、物自体等の持出しを困難にする措置）

a. 秘密情報が記された会議資料等の適切な回収	35
b. 秘密情報の社外持出しを物理的に阻止する措置	35
c. 電子データの暗号化による閲覧制限等	35
d. 遠隔操作によるデータ消去機能を有するPC・電子データの利用	36

（電子データの外部送信による持出しを困難にする措置）

e. 社外へのメール送信・Webアクセスの制限	36
f. 電子データの暗号化による閲覧制限等（再掲）	36
g. 遠隔操作によるデータ消去機能を有するPC・電子データの利用（再掲）	36

（秘密情報の複製を困難にする措置）

h. コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管	37
i. コピー機の使用制限	37
j. 私物のUSBメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限	37

③「視認性の確保」

【退職予定者に対する特有の措置】

q. 退職をきっかけとした対策の厳格化とその旨の周知	58
r. OB会の開催等	59

【従業員等に向けた対策（再掲）】

（管理の行き届いた職場環境を整える対策）

a. 職場の整理整頓（不要な書類等の廃棄、書棚の整理等）	40
b. 秘密情報の管理に関する責任の分担	40
c. 「写真撮影禁止」、「関係者以外立入り禁止」の表示	41

（目につきやすい状況を作り出す対策）

d. 職場の座席配置・レイアウトの設定、業務体制の構築	41
e. 従業員等の名札着用の徹底	41
f. 防犯カメラの設置等	41

g. 秘密情報が記録された廃棄予定の書類等の保管	42
h. 外部へ送信するメールのチェック	42
i. 内部通報窓口の設置	43

(事後的に検知されやすい状況を作り出す対策)

j. 秘密情報が記録された媒体の管理等	43
k. コピー機やプリンター等における利用者記録・枚数管理機能の導入	44
l. 印刷者の氏名等の「透かし」が印字される設定の導入	44
m. 秘密情報の保管区域等への入退室の記録・保存とその周知	44
n. 不自然なデータアクセス状況の通知	44
o. PCやネットワーク等の情報システムにおけるログの記録・保存とその周知	44
p. 秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査	45

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 秘密保持契約等の締結	60
b. 競業避止義務契約の締結	60
c. 秘密情報を返還・消去すべき義務が生ずる場合の明確化等	61

⑤「信頼関係の維持・向上等」

a. 適切な退職金支払い	62
b. 退職金の減額などの社内処分の実施	62

3. 取引先に向けた対策

①「接近の制御」

a. 取引先に開示する情報の厳選	66
b. 取引先での秘密情報の取扱者の限定	67

②「持出し困難化」

a. 秘密情報の消去・返還と複製できない媒体での開示	68
b. 遠隔操作によるデータ消去機能を有するP C・電子データの利用	68

③「視認性の確保」

a. 秘密情報の管理に係る報告の確認、定期・不定期での監査の実施	69
b. 取引先に自社サーバーを使用させてログの保全・確認を実施	69

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 取引先に対する秘密保持義務条項	70
b. 秘密情報であることの表示	71
c. 具体的な秘密情報の取扱い等についての確認	71
d. 取引先に対する秘密情報の管理方法に関する研修等	71
e. 取引先とのやりとりの議事録等の保存	72

⑤「信頼関係の維持・向上等」

a. 適正な対価の支払い等	73
b. 契約書等における損害賠償や法的措置の記載	73

4. 外部者に向けた対策

①「接近の制御」

a. 秘密情報を保管する建物や部屋の入場制限、書棚や媒体等のアクセス制限	76
b. 外部者の構内ルートの制限	77
c. ペーパーレス化	77
d. 秘密情報の復元が困難な廃棄・消去方法の選択	78
e. 外部ネットワークにつながらない機器に秘密情報を保存する	78
f. ファイアーウォール、アンチウィルスソフトの導入、ソフトウェアのアップデート	78
g. ネットワークの分離（複数のLANを構築）	81

②「持出し困難化」

a. 外部者の保有する情報端末、記録媒体の持込み・使用等の制限	82
b. PCのシンクライアント化	82
c. 秘密情報が記載された電子データの暗号化	82
d. 遠隔操作によるデータ消去機能を有するPC・電子データの利用	82

③「視認性の確保」

a. 「関係者以外立入り禁止」や「写真撮影禁止」の張り紙等	84
b. 秘密情報を保管する建物・区域の監視	84
c. 来訪者カードの記入、来訪者バッジ等の着用	86

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 「関係者以外立入り禁止」や「写真撮影禁止」の張り紙等（再掲）	87
b. 秘密情報であることの表示	87
c. 契約等による秘密保持義務条項	87