d）情報処理施設・設備の周辺での飲食及び喫煙に関する指針を確立する。
e）情報処理施設・設備の運用に悪影響を与える可能性がある環境条件を監視する。
f）全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。
g）作業現場などの環境にある装置には、特別な保護方法の使用を考慮する。
h）電磁波の放射による情報漏えいのリスクを最小限にするため、秘密情報を処理する装置を保護する。
i）組織が管理する情報処理施設・設備を、組織が管理していない情報処理施設・設備から物理的に分離する。

7b-7.9　構外にある資産のセキュリティ

管理策：構外にある資産を保護する。

目的：　構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。

詳細管理策

（7b-7.9参考）　組織が所有する装置・機器、及び個人が所有し組織のために用いる機器［私物機器の業務利用（ＢＹＯＤ）］を含む、情報を保管又は処理する、組織の構外で使用する装置・機器は全て保護する必要がある。

7b-7.9.1　構外にある装置・機器の使用は、管理者によって認可される。

7b-7.9.2　組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。
a）構外に持ち出した装置・機器及び記憶媒体は、公共の場所で、かつ、セキュリティが保たれない場所に無人状態で放置しない。
b）装置・機器の保護に関する製造業者の指示を常に守る。
c）構外にある装置・機器を、複数の個人又は利害関係者の間で移動する場合には、その装置・機器の受渡記録を明記した記録（少なくとも、その装置・機器に対して責任を負う者の氏名及び組織を含むもの）を維持する。資産とともに移動する必要のない情報は、移動前にセキュリティを保って削除する。
d）必要かつ実施可能な場合には、組織の構内から装置・機器及び媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する。
e）公共交通機関において機器上の情報を見ること、及びのぞき見に関連するリスクに対して保護する。
f）機器の位置追跡及び遠隔データ消去機能を実装する。

（7b-7.9.2参考）　組織の構外に装置を恒久的に設置すると、損傷、盗難又は傍受のリスクが高くなる可能性がある。これらのリスクは、場所によってかなり異なる可能性がある。

7b-7.9.3　装置を恒久的に設置する構外のそれぞれの場所に応じた最も適切な対策の決定には、リスクを考慮する。

7b-7.9.4　装置を組織の構外に恒久的に設置する場合、次の事項を考慮する。
a）物理的セキュリティの監視
b）物理的及び環境的脅威からの保護
c）物理的アクセス制御及び不正防止（tamper proofing）の管理策
d）論理的アクセス制御

7b-7.10　記憶媒体

管理策：記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。

目的：　記憶媒体上の情報に対して認可された開示、変更、移動又は破棄だけがなされることを確実にするため。

詳細管理策

【取外し可能な記憶媒体】

7b-7.10.1　取外し可能な記憶媒体の管理において、次の事項を考慮する。
a）取外し可能な記憶媒体の管理に関するトピック固有の方針を確立し、取外し可能な記憶媒体を使用する又は取り扱う全ての人にトピック固有の方針を伝達する。
b）必要かつ実施可能な場合には、組織から記憶媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する。
c）全ての記憶媒体は、情報の分類に従って安全でセキュリティが保たれた環境に保管し、製造業者の仕様に従って、環境の脅威（熱、水分、湿度、電場、経年劣化など）から保護する。
d）情報の機密性又は完全性が重要な考慮事項である場合は、取外し可能な記憶媒体上の情報を保護するために、暗号技術を用いる。
e）保管した情報がまだ必要な間に記憶媒体が劣化するリスクを軽減するため、読み出せなくなる前に情報を新しい記憶媒体に移し替える。
f）価値の高い情報は、一斉に損傷又は消失するリスクをより低減するために、複数の複製を別の記憶媒体に保管する。
g）情報を失う危険性を小さくするために、取外し可能な記憶媒体の登録を検討する。
h）取外し可能な記憶媒体のポートは、組織にその利用について理由があるときにだけ有効とする。
i）取外し可能な記憶媒体を用いる必要がある場合、そのような記憶媒体への情報の転送を監視する。
j）情報は、物理的な輸送中、例えば、郵便サービス又は宅配便で記憶媒体を送る場合に、認可されていないアクセス、不正使用又は破損に関してぜい弱である可能性がある。

（7b-7.10.1参考）　この管理策では、媒体は紙の文書を含んでいる。物理的記憶媒体を輸送する場合には、5b-5.14のセキュリティ対策を適用する。

【セキュリティを保った再利用又は処分】

7b-7.10.2　認可されていない者に秘密情報が漏えいするリスクを最小化するために、記憶媒体のセキュリティを保った再利用又は処分の手順を確立する。

7b-7.10.3　秘密情報を格納した記憶媒体の、セキュリティを保った再利用又は処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとする。