f）輸送する記憶媒体内の情報の分類レベルに応じて、開封を明らかにする又は開封を防止する管理策の使用
g）運送業者の識別情報を検証する手順
h）情報の分類に応じた、輸送又は運送業者のサービスを提供する第三者の承認された一覧
i）記憶媒体の内容及び適用した保護方法を特定するためのログを保持し、認可された受領者のリスト、輸送の責任窓口への発送時刻、及び宛先での受領時刻を記録すること

【口頭での伝達】

5b-5.14.7　情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを留意させる。
a）公共の場所又は安全でない通信チャネルを通じた口頭での秘密会話は、認可されていない者に聞かれる可能性があるので行わない。
b）秘密情報を含んだメッセージを留守番電話又は音声メッセージに残さない。留守番電話又は音声メッセージに残したメッセージは、認可されていない者が再生する可能性、共有システムに保管される可能性、又は誤ダイアルの結果、間違って保管される可能性があるからである。
c）会話を聞く際は、適切なレベルで音を遮断する。
d）適切な部屋の管理策が実施されることを確実にする。
e）取扱いに慎重を要する会話においては、始めに注意事項を説明し、出席者に、これから伝える情報の分類レベル及び取扱いの要求事項を知らせる。

5c　アクセス権管理

5c-5.15　アクセス制御

管理策：情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。

目的：　情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。

詳細管理策

5c-5.15.1　情報及びその他の関連資産の管理責任者は、アクセス制御に関連する情報セキュリティ及び事業上の要求事項を決定する。

5c-5.15.2　情報セキュリティ及び事業上の要求事項を考慮したアクセス制御に関するトピック固有の方針を定め、関連する全ての利害関係者に伝達する。

5c-5.15.3　情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。
a）どのエンティティが、情報及びその他の関連資産にどの種類のアクセスを必要とするかの決定
b）アプリケーションセキュリティ
c）物理的アクセス。これは適切な物理的入退管理策によって支援する必要がある。
d）情報の配布及び認可、並びに情報のセキュリティ水準及び情報の分類
e）特権的アクセスの制限
f）職務の分離
g）データ又はサービスへのアクセスの制限に関連する法令、規制及び契約上の義務
h）アクセス制御機能の分離
i）アクセス要求の正式な認可
j）アクセス権の管理
k）ログ取得

5c-5.15.4　アクセス制御規則は、関連するエンティティに対して、適切なアクセス権及び制限を定義し、対応付けすることによって実施する。

（5c-5.15.4参考）　エンティティは、人間の利用者だけでなく、技術的又は論理的なアイテムの場合もある。アクセス制御の管理を簡潔にするために、役割をエンティティのグループに割り当てることが可能である。

5c-5.15.5　アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。
a）アクセス権と情報分類との整合性
b）アクセス権と物理的境界のセキュリティのニーズ及び要求事項との整合性
c）エンティティに、使用が認められているネットワーク及びネットワークサービスを含む、情報及びその他の関連資産へのアクセスだけを提供するために、分散環境で利用可能な全ての種類の接続を考慮すること
d）動的アクセス制御に関連する要素又は要因をどのように反映できるかを検討すること

5c-5.16　識別情報の管理

管理策：識別情報のライフサイクル全体を管理する。

目的：　組織の情報及びその他の関連資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。

詳細管理策

5c-5.16.1　識別情報の管理におけるプロセスは、次の事項を確実にする。
a）個人に割り当てられる識別情報の場合、特定の識別情報を使って実行した処理に関してその個人にアカウンタビリティを負わせることができるように、一つの識別情報は一人の個人にだけひも（紐）付ける。
b）複数の人に割り当てられる識別情報は、業務上又は運用上の理由で必要であり、そのための承認及び文書化をする場合にだけ許可する。
c）人間以外のエンティティに割り当てられる識別情報は、適切に権限を分離した承認及び独立した継続的な監視の対象とする。
d）識別情報が不要になった場合、識別情報を時機を失せずに無効化又は削除する。
e）特定の領域では、一つだけの識別情報を一つのエンティティに対応付ける。
f）利用者識別情報及び認証情報の使用及び管理に関する全ての重要な事象の記録を保持する。