8c-8.23.2　組織は、要員がアクセスすることが望ましい又は望ましくないウェブサイトの種類を特定する。

8c-8.23.3　組織は次の種類のウェブサイトへのアクセスを塞ぐことを考慮する。
- a）情報アップロード機能をもつウェブサイト。ただし、正当な業務上の理由のため許可されている場合を除く。
- b）悪意のある、又はその疑いのあるウェブサイト
- c）C＆Cサーバ
- d）脅威インテリジェンスで認識した悪意のあるウェブサイト
- e）違法なコンテンツを供給しているウェブサイト

8c-8.23.4　ウェブフィルタリングに関する管理策を導入する前に、組織は、望ましくない又は不適切なウェブサイト及びウェブベースのアプリケーションに対する制限を含め、オンライン資源を安全かつ適切に使用するための規則を確立する。

8c-8.23.5　オンライン資源を安全かつ適切に使用するための規則は最新の状態に保つ。

8c-8.23.6　ウェブへのアクセスを含む、オンライン資源のセキュリティを保った適切な使用について、要員を訓練する。

8c-8.23.7　オンライン資源のセキュリティを保った適切な使用についての訓練には、組織の規則、セキュリティ上の懸念を報告するための連絡先、及び制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合の例外プロセスを含める。

8c-8.23.8　ウェブサイトで、セキュリティが保たれないことを通知するブラウザアドバイザリを利用者が無効にしないことを確実にするように、要員を訓練する。

8c-8.24　暗号の利用

管理策：暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。

目的：　事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。

詳細管理策

【暗号の利用全般】

8c-8.24.1　暗号化を利用する場合、次の事項を考慮する。
- a）情報を保護する上での一般原則も含む、組織で定義した暗号に関するトピック固有の方針。暗号技術の利用の便益を最大化し、リスクを最小化し、不適切又は誤った利用を回避するには、暗号の利用に関するトピック固有の方針が必要である。
- b）要求された保護レベル及び情報の分類を特定し、その結果によって、要求される暗号アルゴリズムの種別、強度及び品質を確立する。
- c）持ち運び可能な利用者エンドポイント機器又は記憶媒体に保持され、ネットワークを通じてその機器又は記憶媒体に伝送される情報を保護するための暗号の利用
- d）鍵管理に対する取組。これには、暗号鍵の生成及び保護手法、並びに鍵が紛失した場合、危たい（殆）化した場合又は損傷した場合の暗号化された情報の復元手法を含む。
- e）次の事項に関する役割及び責任
  - 1）暗号を効果的に利用するための規則の実施
  - 2）鍵生成を含めた鍵管理
- f）採用する標準類、並びに組織での利用が承認又は要求されている暗号アルゴリズム、暗号強度、暗号ソリューション及び利用方法
- g）暗号化した情報を用いることの、コンテンツ検査に依存する管理策への影響

8c-8.24.2　暗号を効果的に利用するための組織の規則を実施するときには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を考慮する。

8c-8.24.3　暗号サービスの外部供給者とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供の応答時間を扱う。

【鍵管理】

8c-8.24.4　鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保った手法に基づくことを考慮する。
- a）種々の暗号システム及び種々のアプリケーションのために鍵を生成する。
- b）公開鍵証明書を発行し、入手する。
- c）意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にするか）も含む。
- d）鍵を保管する。これには、認可されている利用者がどのような方法で鍵にアクセスするかも含む。
- e）鍵を変更又は更新する。これには、鍵をいつ、どのような方法で変更するかの規則も含む。
- f）危たい（殆）化した鍵に対処する。
- g）鍵を無効にする。これには、鍵をどのような方法で取消し又は非活性化するかも含む。
- h）紛失した鍵又は破損した鍵を回復する。
- i）鍵をバックアップ又は保存する。
- j）鍵を破壊する。
- k）鍵管理に関連する活動を記録し、監査する。
- l）鍵管理に関する組織の規則に従って鍵を一定期間だけ利用できるように、鍵の活性化及び非活性化の日付を設定する。
- m）暗号鍵へのアクセスに関する法的要求の取扱い

（8c-8.24.4参考）　適切な鍵管理には、暗号鍵を生成、保管、保存、読出し、配布、利用停止及び破壊するための、セキュリティを保ったプロセスが必要となる。

8c-8.24.5　全ての暗号鍵は、改変及び紛失から保護する。

8c-8.24.6　秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護する。

8c-8.24.7　鍵の生成、保管及び保存のために用いる装置は、物理的に保護する。

8c-8.24.8　暗号鍵の完全性に加え、多くの事例では、公開鍵の真正性も考慮する。