8c-8.21　ネットワークサービスのセキュリティ

管理策：ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。

目的：　ネットワークサービスの利用におけるセキュリティを確実にするため。

詳細管理策

8c-8.21.1　それぞれのネットワークサービスに必要なセキュリティ対策を、内部又は外部のネットワークサービス提供者が特定し、実装する。

8c-8.21.2　組織は、ネットワークサービス提供者による、ネットワークサービスに必要なセキュリティの対策の実施を確実にする。

8c-8.21.3　合意したサービスをセキュリティを保って管理できる、ネットワークサービス提供者の能力を定め、定常的に監視する。

8c-8.21.4　監査の権利について組織と提供者との間で合意する。

8c-8.21.5　組織は、サービス提供者が適切なセキュリティ対策を維持していることを実証するために、サービス提供者が提示する第三者認証も考慮する。

8c-8.21.6　ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。

a）アクセスが許可されているネットワーク及びネットワークサービス

b）様々なネットワークサービスにアクセスするための認証の要求事項

c）誰にどのネットワーク及びネットワークサービスにアクセスすることを許すかを決定する認可手順

d）ネットワーク接続及びネットワークサービスへのアクセスを保護するためのネットワーク管理並びに技術的管理策及び手順

e）ネットワーク及びネットワークサービスにアクセスするために利用する手段

f）アクセス時の利用者の時刻、場所及びその他の属性

g）ネットワークサービスの利用の監視

8c-8.21.7　ネットワークサービスは次のセキュリティ機能を考慮する。

a）ネットワークサービスのセキュリティに適用する技術

b）セキュリティ規則及びネットワーク接続規則に従った、ネットワークサービスへのセキュリティを確保した接続のために要求される技術的パラメータ

c）利用者が性能、可用性及び機密性の要求事項に従ってキャッシングの利用を選択できる、キャッシング及びそのパラメータ

d）必要な場合、ネットワークサービス又はアプリケーションへのアクセスを制限するための、ネットワークサービス利用の手順

8c-8.22　ネットワークの分離

管理策：情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離する。

目的：　業務のニーズに基づいて、ネットワークをセキュリティ境界で分割し、それらの間のトラフィックを管理するため。

詳細管理策

8c-8.22.1　組織は、大規模なネットワークを幾つかのネットワーク領域に分離し、公衆ネットワーク（すなわち、インターネット）から分離することによって、大規模なネットワークのセキュリティを管理する。

8c-8.22.2　ネットワーク領域は、可能であれば組織の単位又は特定の組合せに従い、信頼性、重要性及び取扱いに慎重を要する度合いに基づいて選択する。

8c-8.22.3　ネットワークの分離は、可能であれば物理的に異なるネットワーク又は論理的に異なるネットワークを用いて行う。

8c-8.22.4　それぞれのネットワーク領域の境界は、明確に定める。

8c-8.22.5　ネットワーク領域間のアクセスを認める場合､アクセスは境界にゲートウェイを設けて制御する。

8c-8.22.6　ネットワーク領域を分離する際の基準及びゲートウェイを通じて認められるアクセスの基準は、それぞれの領域のセキュリティ要求事項のアセスメントに基づく。

8c-8.22.7　それぞれのネットワーク領域のセキュリティ要求事項のアセスメントでは、次の事項を評価する。

a）アクセス制御に関するトピック固有の方針、アクセス要求事項、並びに処理する情報の価値及び分類に従っているか。

b）適切なゲートウェイ技術を組み込むための費用対効果を考慮しているか。

8c-8.22.8　無線ネットワークの分離のために、電波の届く範囲の調整を考慮する。

（8c-8.22.8参考）　無線ネットワークは、ネットワークの境界が十分に定められていないため、特別な取扱いを要する。

8c-8.22.9　取扱いに慎重を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離するように配慮する。

8c-8.22.10　要員が組織のトピック固有の方針に適合する管理された利用者エンドポイント機器だけを使用する場合、ゲスト用の無線アクセスネットワークを要員用の無線アクセスネットワークから分離する。

8c-8.22.11　ゲスト用のWiFiは、要員によるゲストWiFiの利用を防ぐために、少なくとも要員用のWiFiと同じ制限をもつ。

8c-8.23　ウェブフィルタリング

管理策：悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理する。

目的：　システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。

詳細管理策

8c-8.23.1　組織は、違法な情報があるウェブサイト、又はウイルス若しくはフィッシングの材料があることが知られているウェブサイトに組織の要員がアクセスするリスクを減らす。

（8c-8.23.1参考）　リスクを減らす手法として、関係するウェブサイトのＩＰアドレス又はドメインへのアクセスを阻止することがある。一部のブラウザ及びマルウェア対策技術は、アクセスすることが望ましくないウェブサイトへのアクセスを自動的に阻止、又は阻止するように構成することが可能である。