特集 第三部

新型コロナウイルスの感染症拡大を踏まえて、改めてISO/IEC 27001を考える

新型コロナウイルス感染症の流行により、企業の状況や利害関係者のニーズなどに変化が生じている。情報セキュリティ分野においては、テレワーキングの新規導入や、従来はテレワーキングの対象外だった従業員への導入拡大が、最も影響が大きいところといえるだろう。コロナ禍での情報セキュリティマネジメントシステムの審査のポイントについて、審査事業センター 情報審査部 部長の宮下 卓士に聞いた。

審査事業センター
情報審査部 部長
宮下 卓士

審査で注目するポイント

箇条4　組織の状況

東京では、オリンピック時の出勤抑制を意識して、テレワーキングの導入・準備をしていた企業もあり、テレワーキングに対応したマネジメントシステムの構築をすでに進めていましたが、これまでテレワーキングに未対応であった企業や業務においても、急遽対応せざるを得なくなったことがコロナ禍での2020年度の特徴です。

◎審査の視点とチェックポイント

テレワーキングの導入等により業務プロセス自体が変化すれば、リスクも変化し、マネジメント対象も変わります。コロナ禍においてマネジメントシステムを変更した企業も多く、ISO/IEC 27001の審査に際しては、企業の状況を含め実情に応じてマネジメントシステムが変更され新たなリスクが定義されているか、リスクに対応する方策が確実に実施されているかどうかが、確認のポイントとなります。

それらの点は利害関係者が企業に期待するところであり、企業が外部変化に対応してリスク対策を講じていくことは、企業として利害関係者のニーズを監視している証左にもなります。

ただし、コロナ禍は突然起きたことであり、企業は細かいリスク分析をしてマニュアルの書き換えを行うより先に、目の前に起きている課題に対応しながらリスクをまとめテレワーキングの体制をつくるなど、事業継続の方策を実現化する必要がありました。そのため、リスク分析が不十分なところがあると考えられます。箇条4に限ったことではありませんが、一年近くが経過してテレワーキングの運用体制が多少落ち着いたところで当時構築したシステムを今一度見直し、リスクなどを整理し直すことが必要です。ISO/IEC 27001では、テレワーキングに伴う情報セキュリティの管理策について、取引先とデータをやりとりする場合なども含め、あらかじめ規定されています。テレワーキング導入に伴うマネジメントシステムの変更や、手順書に新規項目を追加する場合は、本規格を参照することで網羅的に管理できるようになっています。

なお、マニュアルの書き換えについては、早急に行ったかよりも、現状の手順の内容が全員に伝わっていることが重要です。テレワーキングを導入

し、順守されるべき規則を新規につくった場合、それがWebポータルなどに明示されて周知されているか、縦系列で漏れなく伝達されているかなどは、注意するポイントとなります。認識が共有され、ガバナンスが働いている状態であれば、文書への反映に多少のタイムラグがあっても大きな問題とはなりません。

箇条4.3　情報セキュリティマネジメントシステムの適用範囲の決定

箇条4.3（情報セキュリティマネジメントシステムの適用範囲の決定）では、適用範囲を定義するために、外部と内部の課題、利害関係者のニーズ、外部組織で実施する活動とのインターフェースと依存関係を考慮して、境界と適用可能性を決定することが規定されています。テレワーキングの導入により、ネットワークを含む情報システムに対して変化が発生していることが考えられます。

◎審査の視点とチェックポイント

テレワーキング等により企業の人員が会社外から企業の情報システムにアクセスする場合でも、企業の内部にいる人員が企業の情報システムにアクセスすることと同等にマネジメントされた状況にあると考えられる限りは、テレワーキングの実施場所に関する適用範囲を大きく変更する必要はないと考えます。

Web会議を使用する場合も、その仮想空間を企業の拠点として考えることができます。ただし、他社の提供するクラウド上のサーバや、各種のクラウドサービスなどを利用することを、適用範囲に含めて考慮しておく必要があります。

企業の情報システムに外部のネットワーク経由でアクセスする場合は、適用範囲を定義し直し、VPN、アクセス権の付与、各端末の認証、自宅の通信環境の確認等のセキュリティ対策を講じている必要があります。

登録活動範囲については、企業、業務内容、場所、論理的なネットワーク構成が現状に即した内容となっているかを確認します。

箇条5　リーダーシップ

コロナ禍でのテレワーキングの整備は、必ずトップマネジメントのコミットメントに基づいています。トップマネジメントがどのような過程で方針変更を決定し指示を出したか、情報セキュリティについても経営層の了解を得ているか、ということを確認します。

非常時であり、トップマネジメントの意思決定がWeb会議システム上などで行われたこともあると考えられます。審査においては、定型的なマネジメントレビューでなくとも、方針変更を決定した役員会、経営会議等がマネジメントレビューに当たると考えます。方針決定に至る時系列の流れについては、審査時に確認しています。

附属書A.6　情報セキュリティのための組織

コロナ禍においては、ISO/IEC 27001 の箇条6.1（リ

スク及び機会に対処する活動）や箇条6.1.2（情報セキュリティリスクアセスメント）、附属書A.6.2（モバイル機器及びテレワーキング）に関する部分が特に大きく変化しました。これまで附属書A.6.2（モバイル機器及びテレワーキング）を不採用だった企業も採用するようになっています。

附属書A.6.2（モバイル機器及びテレワーキング）はモバイル機器とテレワーキングに関するセキュリティを確実にする目的で定められたもので、在宅で勤務しテレワーキングの場所から会社のサーバなどの情報にアクセスして業務を行う場合に加え、社内のネットワークだけではなく外部のインターネットを経由して会社のネットワークに入る場合も扱っています。

附属書A.6.2.1（モバイル機器の方針）では、モバイル機器を用いることで生じるリスクを管理するために、方針およびその方針を支援するセキュリティ対策を採用することが推奨されています。この方針は附属書A.5.1.1（情報セキュリティのための方針群）に示された実施の手順を参考に策定します。

また、附属書A.6.2.2（テレワーキング）では、テレワーキングの場所でアクセス、処理、保存される情報を保護するために、方針およびその方針を支援するセキュリティ対策を実施することを求めています。

◎審査の視点とチェックポイント

自宅から会社のサーバなどの情報にアクセスして業務を行ったり、インターネットから会社のネットワークに入るケースが激増しています。テレワーキング導入に関しては、附属書A.6.2.1（モバイル機器の方針）に示されるとおり、モバイル機器の使用に伴うリスクに関する管理方針を立て、その方針に則ったセキュリティ対策が採用されているかに着目して審査します。

特に、会社から貸与された装置ではなく、個人のパソコンを使って会社のネットワークにアクセスする場合、個人のパソコンであっても会社のルールや機能を確実に履行することが求められます。これに関するモラル教育は、ISO/IEC 27001の箇条7（支援）、箇条7.2（力量）、箇条7.3（認識）、箇条7.4（コミュニケーション）を参照してください。

テレワーキングの場所でアクセス、処理、保存される情報の保護については、附属書A.6.2.2（テレワーキング）で示すように情報保護の方針を立て、その方針を実現するセキュリティ対策が実施されているかを確認します。また、在宅勤務をする上での操作マニュアルが整備されているかも確認します。

箇条9　パフォーマンス評価

箇条9.1（監視、測定、分析及び評価）では業務が滞りなく効率的に回る体制がとられていることを求めていますが、運用が変われば監視項目や測定方法も変更されます。例えば、テレワーキングが基本となった場合の出退勤管理やEラーニングについて、Webサイト上で報告・集計できるシステムを構築するなど、変化に応じた監視、測定、評価システムを整備することも必要になる場合があります。

機械的に測定できるものは良いのですが、テレワーキングの実施場所、作業中のPC画面や出力したドキュメントが第三者に見られない対策の実施状況などは、自己申告になる可能性が高くなり、確認が難しいためできる範囲での対応にならざるを得ないと考えます。

また、社内のネットワークに比べて自宅の通信環境は整備されておらず、サーバにアクセスする場合の応答率の悪化も見られました。インタビューでは、次に同様の事態が発生したときのために、どこまで、どのように投資をしてリスク対応をしていくのかを確認する場合があります。

内部監査も、開催時期の延長、Web会議での開催など、テレワーキングによりフェイス・トゥー・フェイスの実施が難しいこともあります。Web会議システムで実施する場合、電子化された記録の閲覧は容易ですが、紙での記録、現場の状況などは難しくなります。Webカメラを使って現場や紙記録を確認する、今回の重

点監査ポイントを確認可能な内容に限定する、など内部監査計画の見直しも必要となります。

箇条10　改善

今回、テレワーキングを導入された企業は、環境の変化が発生しています。企業に影響を及ぼすリスクや機会の変化の可能性もあり、新たなリスクや機会に対して対処することが必要となるでしょう。また、情報資産の洗い出し、情報セキュリティリスクアセスメント、情報セキュリティリスク対応も実施することが必要です。

箇条4（組織の状況）でも述べましたが、テレワーキングが導入されたことにより、適用された管理策の内容が適切なのか、確認して見直すことも必要です。

附属書A.11　物理的及び環境的セキュリティ

テレワーキングの実施にあたっては、会社のモバイル機器を自宅に持ち帰るケースも多く見られました。これについては附属書A.11.2.5（資産の移動）および附属書A.11.2.6（構外にある装置及び資産のセキュリティ）を参照します。

附属書A.11.2.5（資産の移動）では管理策として、装置や情報またはソフトウェアは事前の許可なしで構外に持ち出さないことが記されています。管理策の実施にあたっては、持ち出しを許可された従業員や外部利用者を特定すること、持ち出し期限を設定して返却が設定どおりであったかを検証すること、持ち出しと返却を記録すること、そして、資産を扱う者や利用する者については識別情報や役割、所属を文書化し、資産の返却時に文書も返却することを要求しています。

附属書A.11.2.6（構外にある装置及び資産のセキュリティ）では、構外にある資産の管理策として、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れてセキュリティを適用することが求められています。

◎審査の視点とチェックポイント

会社のモバイル端末を自宅で使用する場合には、附属書A.6（情報セキュリティのための組織）で規定している情報の保護に関するリスクや、附属書A.13（通信のセキュリティ）に記載のある外部ネットワークを使用することに伴うリスクに加え、紛失等のリスクについても考慮しておく必要があります。審査においては、これらの項目について従来は記載する必要がなかった企業も、必要に応じて本箇条を追加して資産に対するリスクの把握に努めているか、また、それらのリスクに対する対策を講じて、それを周知し実践しているかを確認します。

構外にある装置および資産には、会社から貸与しているIDカードも含まれます。毎日通勤している状況であれば、もし紛失してもすぐに気づくことができますが、長期間、自宅でのテレワーキングが続き、IDカードを使用する機会がないままであると、紛失しても気がつかず、対処が遅れる可能性があります。審査ではそういったリスクを想定し、常駐している契約先社員への貸与分も含め、IDカードの保管状況を定期的に確認するなど、紛失時に早期発見できる仕組みができているかにも着目します。

附属書A.12　運用のセキュリティ

情報処理設備の運用における管理目的と管理策を定める附属書A.12（運用のセキュリティ）では、操作手順書、変更管理、容量・能力の管理、開発環境・試験環境・運用環境の分離についての指針を示し、これらに則ってセキュリティを保った運用を行うことを求めています。

◎審査の視点とチェックポイント

社内においてはセキュリティと可用性を適切なバランスで保つことが可能ですが、テレワーキングで自宅から接続する場合には、当初規定していたとおりに運用できるとは限りません。在宅勤務が増え、セキュリティ強度を多少下げても可用性を優先した企業もあると思いますが、審査では、その際にセキュリティリスクアセスメントをどのように行い、トップマネジメントの許可を得て構築したのかというプロセスを確認します。

緊急事態宣言を受けてのセキュリティリスクアセスメントは、短時間での実施にならざるを得なかったと思われますが、運用から一年近くが経っていますので、妥当性はあるか、機密性に問題はないかなどを、再度確認してください。

また、在宅勤務中のセキュリティをどこまで要求するのかも考えるべき課題です。家族が同じ空間にいるとき、あるいはシェアオフィスなどを利用して業務を行う状況ではセキュリティ面への影響が大きく、自宅内に独立した空間を確保できない場合、どのようにセキュリティ対策を講じているかが重要です。

プリントアウトした書類の扱いについても同様です。本来は自宅での出力を不可能にするシステムが必要ですが、コストもかかります。やむを得ず出力した場合、シュレッダーで処理する、溶解処理するなど、従来の会社のルールの適用がどのようになされているかは確認すべき点だと考えています。

附属書A.13　通信のセキュリティ

附属書A.13.1.1（ネットワーク管理策）では、システムおよびアプリケーション内の情報を保護するためにネットワークの管理と制御を行うことを求めており、考慮すべきことの一つとして、公衆ネットワークまたは無線ネットワークを通過するデータの機密性・完全性や、

ネットワークを介して接続したシステムおよびアプリケーションを保護するために、特別な管理策を確立することを求めています。

◎審査の視点とチェックポイント

テレワーキングではWeb会議システムが頻繁に使われますが、公衆ネットワークまたは無線ネットワークを経由して会社のネットワークにアクセスする場合は、附属書A.13.1.1（ネットワーク管理策）に記されている内容を考慮する必要があります。ここでは公衆ネットワークまたは無線ネットワークを通過するデータの機密性・完全性や、ネットワークを介して接続したシステムおよびアプリケーションを保護するための特別な管理策を確立しているかが問われており、それらが適切に実施されているかが審査のポイントとなります。

また、細かい点ですが、例えば自宅でWi-Fiを使って無線LANに接続する場合、パソコンとルーター間の暗号化の機能が脆弱であると、第三者に見られてしまう危険性があります。そのような点も含め、ネットワーク管理策に変更があった場合、マネジメントシステムも実情に応じた変更をしているかどうかを確認します。

また、2020年4月の緊急事態宣言発出直後には、テレワーキングの増加の影響で通信会社の

ネットワーク負荷が高まり、通信スピードが著しく悪くなることがありました。また、マンションなどは、在宅勤務者が多くなり、共有の通信設備の負荷が高まったことで通信スピードの問題が発生したこともあります。この件に関しては、企業側で対応できることは限られていますが、可用性を確保するために、業務方法の変更（例:通信時間を減らす、データをまとめて夜間帯に取得しておく）などが必要と思われます。

附属書A.15　供給者関係

附属書A.15（供給者関係）では、外部のサプライヤーがアクセスできる企業の資産、情報を保護するために、サプライチェーンにおける情報セキュリティの管理目的および管理策を定め、サプライヤーと合意しておくことを求めています。

◎審査の視点とチェックポイント

テレワーキングを導入しているのはサプライヤー、協力会社も同様です。自社に関しては情報セキュリティマネジメントシステムを構築していても、協力会社の対策状況まで確認していない企業が多く、取引先調査でテレワーキングに関する調査項目を設けていない例も見受けられます。附属書A.15.1（供給者関係における情報セキュリティ）で求めているように、協力会社でテレワーキングを行っている場合は、協力会社の通信・運用のセキュリティ管理策についても確認し、リスクの状況に応じた対応をすることが必要です。

附属書A.17　事業継続マネジメントにおける情報セキュリティの側面

附属書A.17（事業継続マネジメントにおける情報セキュリティの側面）では、情報セキュリティ継続を企業の事業継続マネジメントシステムに組み込むことを求めています。コロナ禍においては、特に附属書A.17.1.1（情報セキュリティ継続の計画）および、附属書A.17.1.2（情報セキュリティ継続の実施）に関して、必要に応じた見直しに取り組んだ企業が多く見られます。

◎審査の視点とチェックポイント

事業継続を意図して緊急的にマネジメントシステムを変更した場合、情報セキュリティもそれに対応して変更されています。審査においては、変更の方針やプロセス、具体的な内容について明文化されていない場合でも、インタビューをして確認します。

附属書A.12（運用のセキュリティ）で述べたセキュリティと可用性の兼ね合いの問題も、事業継続という視点から、アクセシビリティの確保をどこまでのレベルとするかを検討しておく必要があります。

コロナ禍の審査方法

ISO/IEC 27001の場合、可能な限り現場審査を実施したいと考えています。
これは、入退管理装置のログ記録、その装置の利用者登録状況、日々の記録は現場でないと確認が難しいことや、現場で室内の状況など幅広く確認することで、大きなリスクとなり得るぜい弱な箇所の発見につながるためです。
その反面、審査の実施に際しては、企業の方々と審査員の接触を極力減らすことにより、罹患リスクを下げることが重要です。
接触を少なくするための取り組みとして、JQAでは、企業の希望に基づき、手書き記録や管理システムは現場で確認しつつ、それ以外の要員へのインタビューや電子記録の確認などはWeb会議システムを利用して行うことが可能です。
また、審査員が企業には一切訪問せず、Web会議システムのみで審査を実施することも可能です。ただし、この場合には、企業側にて現場をカメラで映していただくことや手書き記録などはその場で撮影いただくなどの対応が必要となります。
新型コロナウイルス感染症の収束に関して、先行き不透明な状況ではありますが、早期に通常どおりの現場審査を実施できることを願っています。

■

Column

ISO/IEC 27001内部監査のポイント

テレワーキングが常態化している企業では、内部監査や審査をリモートで行うケースも増えています。
内部監査で業務環境等の確認を行う場合、相手の自宅の状況を見ることはできないため、口頭で聞くしかありません。Web会議システムで実施する場合には、画面共有機能などを活用し、デスクトップのウイルス対策ソフトやWindowsのアップデート、アクセス権などのアクティブディレクトリを確認することは可能です。しかし、核となる画面構成はWeb会議システムでは提示しづらいため、出社してチェックする方がよい場合があります。
また、記録されている対策や成果は画面共有でも確認できますが、実際の業務の非効率な点などは記録ではなかなか把握できません。そのためリモート監査であっても、やはりインタビューが重要となります。
リモートでインタビューを行う場合、対面でのインタビューとは異なる視点が加わることで、従来以上に経営面の本質に迫る課題が洗い出される可能性もあります。情報機器についても、従来と異なる使い方がされるようになったことで、情報セキュリティに関わるインシデントにつながる情報が拾える場合もあります。
内部監査の結果はトップマネジメントに報告されるため、内部監査員が得た気づきは、改善の種になります。そういった気づきを通して、可用性と機密性のバランスを整えていくことが重要です。

■ 参考1　ISO/IEC 27001:2013の構成

まえがき
0 序文
　0.1 概要
　0.2 他のマネジメントシステム規格との両立性
1 適用範囲
2 引用規格
3 用語及び定義
4 組織の状況
　4.1 組織及びその状況の理解
　4.2 利害関係者のニーズ及び期待の理解
　4.3 情報セキュリティマネジメントシステムの適用範囲の決定
　4.4 情報セキュリティマネジメントシステム
5 リーダーシップ
　5.1 リーダーシップ及びコミットメント
　5.2 方針
　5.3 組織の役割、責任及び権限
6 計画
　6.1 リスク及び機会に対処する活動
　　6.1.1 一般
　　6.1.2 情報セキュリティリスクアセスメント
　　6.1.3 情報セキュリティリスク対応
　6.2 情報セキュリティ目的及びそれを達成するための計画策定
7 支援
　7.1 資源
　7.2 力量
　7.3 認識
　7.4 コミュニケーション
　7.5 文書化した情報
8 運用
　8.1 運用の計画及び管理
　8.2 情報セキュリティリスクアセスメント
　8.3 情報セキュリティリスク対応
9 パフォーマンス評価
　9.1 監視、測定、分析及び評価
　9.2 内部監査
　9.3 マネジメントレビュー
10 改善
　10.1 不適合と是正処置
　10.2 継続的改善
附属書A（規定）管理目的及び管理策

■ 参考2　ISO/IEC 27001:2013 附属書A（規定）管理目的及び管理策の構成

A5. 情報セキュリティのための方針群
　A.5.1 情報セキュリティのための経営陣の方向性
　　A.5.1.1 情報セキュリティのための方針群
　　A.5.1.2 情報セキュリティのための方針群のレビュー
A6. 情報セキュリティのための組織
　A.6.1 内部組織
　　A.6.1.1 情報セキュリティの役割及び責任
　　A.6.1.2 職務の分離
　　A.6.1.3 関係当局との連絡
　　A.6.1.4 専門組織との連絡
　　A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ
　A.6.2 モバイル機器及びテレワーキング
　　A.6.2.1 モバイル機器の方針
　　A.6.2.2 テレワーキング
A.7 人的資源のセキュリティ
　A.7.1 雇用前
　　A.7.1.1 選考
　　A.7.1.2 雇用条件
　A.7.2 雇用期間中
　　A.7.2.1 経営陣の責任
　　A.7.2.2 情報セキュリティの意識向上、教育及び訓練
　　A.7.2.3 懲戒手続
　A.7.3 雇用の終了及び変更
　　A.7.3.1 雇用の終了又は変更に関する責任
A.8 資産の管理
　A.8.1 資産に対する責任
　　A.8.1.1 資産目録
　　A.8.1.2 資産の管理責任
　　A.8.1.3 資産利用の許容範囲
　　A.8.1.4 資産の返却
　A.8.2 情報分類
　　A.8.2.1 情報の分類
　　A.8.2.2 情報のラベル付け
　　A.8.2.3 資産の取扱い
　A.8.3 媒体の取扱い
　　A.8.3.1 取外し可能な媒体の管理
　　A.8.3.2 媒体の処分
　　A.8.3.3 物理的媒体の輸送
A.9 アクセス制御
　A9.1 アクセス制御に対する業務上の要求事項
　　A.9.1.1 アクセス制御方針
　　A.9.1.2 ネットワーク及びネットワークサービスへのアクセス
　A.9.2 利用者アクセスの管理
　　A.9.2.1 利用者登録及び登録削除
　　A.9.2.2 利用者アクセスの提供
　　A.9.2.3 特権的アクセス権の管理
　　A.9.2.4 利用者の秘密認証情報の管理
　　A.9.2.5 利用者アクセス権のレビュー
　　A.9.2.6 アクセス権の削除又は修正
　A.9.3 利用者の責任
　　A.9.3.1 秘密認証情報の利用
　A.9.4 システム及びアプリケーションのアクセス制御
　　A.9.4.1 情報へのアクセス制限
　　A.9.4.2 セキュリティに配慮したログオン手順
　　A.9.4.3 パスワード管理システム
　　A.9.4.4 特権的なユーティリティプログラムの使用
　　A.9.4.5 プログラムソースコードへのアクセス制御
A.10 暗号
　A.10.1 暗号による管理策
　　A.10.1.1 暗号による管理策の利用方針
　　A.10.1.2 鍵管理
A.11 物理的及び環境的セキュリティ
　A.11.1 セキュリティを保つべき領域
　　A.11.1.1 物理的セキュリティ境界
　　A.11.1.2 物理的入退管理策
　　A.11.1.3 オフィス、部屋及び施設のセキュリティ
　　A.11.1.4 外部及び環境の脅威からの保護
　　A.11.1.5 セキュリティを保つべき領域での作業
　　A.11.1.6 受渡場所
　A.11.2 装置
　　A.11.2.1 装置の設置及び保護
　　A.11.2.2 サポートユーティリティ
　　A.11.2.3 ケーブル配線のセキュリティ
　　A.11.2.4 装置の保守
　　A.11.2.5 資産の移動
　　A.11.2.6 構外にある装置及び資産のセキュリティ

- A.11.2.7 装置のセキュリティを保った処分又は再利用
- A.11.2.8 無人状態にある利用者装置
- A.11.2.9 クリアデスク・クリアスクリーン方針

A.12 運用のセキュリティ
- A.12.1 運用の手順及び責任
  - A.12.1.1 操作手順書
  - A.12.1.2 変更管理
  - A.12.1.3 容量・能力の管理
  - A.12.1.4 開発環境、試験環境及び運用環境の分離
- A.12.2 マルウェアからの保護
  - A.12.2.1 マルウェアに対する管理策
- A.12.3 バックアップ
  - A.12.3.1 情報のバックアップ
- A.12.4 ログ取得及び監視
  - A.12.4.1 イベントログ取得
  - A.12.4.2 ログ情報の保護
  - A.12.4.3 実務管理者及び運用担当者の作業ログ
  - A.12.4.4 クロックの同期
- A.12.5 運用ソフトウェアの管理
  - A.12.5.1 運用システムに関わるソフトウェアの導入
- A.12.6 技術的ぜい弱性管理
  - A.12.6.1 技術的ぜい弱性の管理
  - A.12.6.2 ソフトウェアのインストールの制限
- A.12.7 情報システムの監査に対する考慮事項
  - A.12.7.1 情報システムの監査に対する管理策

A.13 通信のセキュリティ
- A.13.1 ネットワークセキュリティ管理
  - A.13.1.1 ネットワーク管理策
  - A.13.1.2 ネットワークサービスのセキュリティ
  - A.13.1.3 ネットワークの分離
- A.13.2 情報の転送
  - A.13.2.1 情報転送の方針及び手順
  - A.13.2.2 情報転送に関する合意
  - A.13.2.3 電子的メッセージ通信
  - A.13.2.4 秘密保持契約又は守秘義務契約

A.14 システムの取得、開発及び保守
- A.14.1 情報システムのセキュリティ要求事項
  - A.14.1.1 情報セキュリティ要求事項の分析及び仕様化
  - A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティ考慮
  - A.14.1.3 アプリケーションサービスのトランザクションの保護
- A.14.2 開発及びサポートプロセスにおけるセキュリティ
  - A.14.2.1 セキュリティに配慮した開発のための方針
  - A.14.2.2 システムの変更管理手順
  - A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
  - A.14.2.4 パッケージソフトウェアの変更に対する制限
  - A.14.2.5 セキュリティに配慮したシステム構築の原則
  - A.14.2.6 セキュリティに配慮した開発環境
  - A.14.2.7 外部委託による開発
  - A.14.2.8 システムセキュリティの試験
  - A.14.2.9 システムの受入れ試験
- A.14.3 試験データ
  - A.14.3.1 試験データの保護

A.15 供給者関係
- A.15.1 供給者関係における情報セキュリティ
  - A.15.1.1 供給者関係のための情報セキュリティの方針
  - A.15.1.2 供給者との合意におけるセキュリティの取扱い
  - A.15.1.3 ICTサプライチェーン
- A.15.2 供給者のサービス提供の管理
  - A.15.2.1 供給者のサービス提供の監視及びレビュー
  - A.15.2.2 供給者のサービス提供の変更に対する管理

A.16 情報セキュリティインシデント管理
- A.16.1 情報セキュリティインシデント管理及びその改善
  - A.16.1.1 責任及び手順
  - A.16.1.2 情報セキュリティ事象の報告
  - A.16.1.3 情報セキュリティ弱点の報告
  - A.16.1.4 情報セキュリティ事象の評価及び決定
  - A.16.1.5 情報セキュリティインシデントへの対応
  - A.16.1.6 情報セキュリティインシデントからの学習
  - A.16.1.7 証拠の収集

A.17 事業継続マネジメントにおける情報セキュリティの側面
- A.17.1 情報セキュリティ継続
  - A.17.1.1 情報セキュリティ継続の計画
  - A.17.1.2 情報セキュリティ継続の実施
  - A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価
- A.17.2 冗長性
  - A.17.2.1 情報処理施設の可用性

A.18 順守
- A.18.1 法令及び契約上の要求事項の順守
  - A.18.1.1 適用法令及び契約上の要求事項の特定
  - A.18.1.2 知的財産権
  - A.18.1.3 記録の保護
  - A.18.1.4 プライバシー及び個人を特定できる情報(PII)の保護
  - A.18.1.5 暗号化機能に対する規制
- A.18.2 情報セキュリティのレビュー
  - A.18.2.1 情報セキュリティの独立したレビュー
  - A.18.2.2 情報セキュリティのための方針群及び標準の順守
  - A.18.2.3 技術的順守のレビュー