付録Ｂ－２　技術対策の例（注：これらは現時点における対策の例示であり、環境の変化や各企業の状況により、変更されるものである）
以下に、『サイバーセキュリティ経営ガイドライン 付録Ｂ』で列記した技術対策項目の詳細例を記載する。

経営ガイドラインの各項目	項目の実現に有効な技術的対策項目	技術的対策の例
（３）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	**防御対象の特定とリスクの把握**	IT ベンダが納品するネットワーク構成図や資産管理台帳のみに頼らず、よりサイバー攻撃対策に特化した以下の観点にて点検・資料整備を行う。 □　組織システムの出入り口を全て洗い出したネットワーク図を作成する。また、社内で保有している、守るべき資産がどこに保管されているかをネットワーク図にマッピングする。 ※（システムを独自に管理・運用する事業部門を含む各部門が独自に導入したネットワークの構成についても確認する） □　法令上、安全管理措置を義務づけられている情報や業務継続上必要不可欠な情報が保存されているサーバや端末が特定され、また限定されており、当該端末緊急時にネットワークからの切り離しが速やかに実施可能か確認し、手順を整備する。
	多層防御措置の実施	「攻撃（感染など）の発覚＝攻撃の終了」ではなく、攻撃を発見し対応を始めた後も攻撃が継続している可能性があるため、予め侵入・被害拡大防止ために下記、多層防御の対策が必要である。 **〇マルウェア感染リスクの低減**　※クライアント、サーバそれぞれについて実施する必要がある。 □　OS やアプリケーションソフトウェアなどのタイムリーな更新（自動更新または強制的な更新）の徹底。 □　マルウェア対策ソフトの導入のみならず、組織内で使用されているすべての対策ソフトが最新版に維持されるよう更新管理を徹底する。 □　外部記憶媒体の接続を制限する。 □　業務に必要のないソフトウェアのインストールを禁止又は制限する。 **〇重要業務を行う端末やネットワークの分離** □　Ｌ３スイッチなどのネットワーク機器の設定により、部署など業務単位でのネットワーク分離を行い、感染時の拡大防止（局所化）を行う。 **〇重要情報が保存されているサーバの保護** □　重要情報を保存しているサーバについては、ネットワークの分離（別セグメント化）や、ファイアウォール（FW）設置、重要データ（データベースおよびファイル）への高度な暗号化、アクセス制限、アクセスログ収集を行う。 **〇出口対策とログの定期的なチェック** ※「ログの適切な保存」については（９）の実施にも影響。付録Ｂ本体記載の参考文献も参照のこと。 □　ネットワーク出入り口に設置される FW やプロキシサーバにおいて少なくとも自組織内から外部へ出ていく通信ログは最低でも半年分以上保存することが必要であり、１年以上保存することが望ましい。 □　FW では、IP アドレスやポート番号しかわからないため、より高度な分析が可能なプロキシサーバを導入することが望ましい。　※高性能な FW ではパケットの中身も確認可能。 □　サーバや端末の操作ログ、セキュリティログについても適切な期間保管すること。特に重要情報を保管しているサーバや認証サーバ については確実に保管されるよう設定を確認すること。 □　例えばシステムの運用をベンダなどに外注している場合、記録・保管しているログについては定期的（例えば１ヶ月に１回）に分析 を依頼し、結果は定期的なミーティング時に共有すること。 **＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＜標的型攻撃に対するより強固な対策＞＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊** **〇感染リスクの更なる低減策** □　標的型攻撃メールでよく用いられる実行形式ファイルが添付されたメールは受信拒否する。 □　WEB フィルタリングソフトやサービスの導入により業務上不要な WEB サイトへのアクセスを禁止する。また、業務上、インターネットへの広範囲な接続が必要でない端末においては、ホワイトリスト方式により閲覧可能な WEB サイトを最小限に限定する。 **〇感染した場合に備えた侵入拡大防止策** □　プロキシサーバを導入し、利用者認証を受けない不正通信をブロックする。 □　C&C サーバおよび不正 Web サイトへのインターネットアクセスをブロックする仕組みを導入し、セキュリティ専門企業および（８）情報共有活動で入手した情報を活用し、ブロック対象をタイムリーに更新する。 □　感染した端末から組織内の別の端末へ感染が拡大しないよう、例えば、ユーザー端末間のファイル共有機能を停止するなど、端末から端末への直接のアクセスを制限する。 □　一般の端末にシステムの管理権限は持たせず、システム管理に必要な端末は通常業務に使う端末とは別に設け、ネットワークセグメントの分離、ウェブサイトの閲覧や電子メールの利用を制限するなどして、システム管理端末が特に侵入を受けないよう保護する。

		□AD サーバなどの利用者権限の認証サーバへの管理者権限でのアクセスを最小限に限定し、アクセスログを定期的にチェックする。 □一般の端末は、攻撃者が夜間活動できないよう、かならず帰宅時に電源断を行うことを徹底する。
（４）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示	**PDCA サイクルの実施と改善**	※ISMS、CSMS の導入にあたっては各種ガイドライン等参考文献や制度を参照のこと。
	各種セキュリティ診断の実施	**〇各種脆弱性診断等の実施** IT システムで利用される OS やサーバでは、セキュリティ上の欠陥である脆弱性が定期的に発見され、対処するためのセキュリティパッチが公開されている。IT システムの運用者はセキュリティパッチをその都度適用する必要があるが、IT システムの規模が大きくなると、脆弱性の対策漏れが発生してしまう可能性がある。そのため、脆弱性診断やペネトレーションテスト等の検査を定期的に実施して脆弱性への対処状況や脆弱性を悪用して侵入された場合の影響度を把握し、対策を実施する必要がある。 組織内部でのセキュリティパッチの適用状況確認のほか、セキュリティ専門企業による、Web アプリケーションの脆弱性診断やプラットフォーム診断サービスを受けることを検討する。
（７）IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	**自組織で対応できる対策項目とできない項目の整理**	**〇対応可能作業の整理** ログの定期的なチェックや監視、インシデント対応のプロセスを漏れなく整理し、各対策項目が自組織の要員または、システム運用の委託先のみで対応できるか、できないか整理する。 **〇リスクマネーの確保** インシデント対応等、緊急の作業外注が必要な場合に備えて、あらかじめ必要な費用の検討を行い、予算等をリスクマネーとして確保しておく。
（８）情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備	**情報共有活動や公的機関などからの提供情報の活用**	**〇情報共有活動への参加** 各種公的機関が実施するものや業界団体等で実施している情報共有活動に参加することで、日々の他社・他組織に対する脅威情報の状況を参照し、同じ攻撃が自組織に向けられていないかチェックするとともに、今後同様の攻撃が自組織へ向けられる事態に備え、各種フィルタ（メール、Web アクセス、C&C サーバ通信）の設定を行う。 **〇注意喚起情報の入手と情報提供** IPA や JPCERT/CC、警察庁、セキュリティ専門企業等が公表する注意喚起情報や脆弱性情報を入手できるよう、メールニュース配信への登録や定期的な情報サイトのチェックを行う。 また、日頃よりマルウェアや不審メール、インシデントに係る情報提供を各種届出窓口へ行うなど、情報共有活動を支える各組織への情報提供を積極的に行う。
（９）緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施	**緊急時のための「体制整備」と「被害特定のための準備」**	**〇不審通信の洗い出しや感染原因特定のために各種ログや感染端末の確保等、証拠保全の実施** ※前述の項目（３）記載「出口対策とログの定期的なチェック」も参照のこと セキュリティ専門企業等に調査を依頼するとともに、IPA、JPCERT/CC などの外部機関から寄せられる情報の活用により、感染端末と感染原因となったマルウェアを特定する。マルウェア等の解析により判明した不正通信先情報により、通信ログを調査し、他に感染端末がないか点検する。マルウェア対策ソフトだけでは検知・除去しきれない場合が多いので、以下の方法により不審な動きをする端末を洗い出す。 **〇端末における不審ファイル等の確認** □　スタートアップフォルダに不審なプログラムが登録されていないか □　タスクスケジューラに不審なファイルが登録されていないか。 **〇システム内における感染端末のあぶり出し** □　FW・プロキシサーバのログ上に不正通信先との通信記録がないか確認し、ほかに不正通信を発している感染端末がないかあぶり出す。 □　標的型攻撃においては、攻撃者が侵入後に AD サーバなどの認証サーバの管理者アカウントを窃取し、組織内の感染を拡大させる手口が用いられるため、AD サーバなどの認証サーバが侵害を受けていないか、また、管理者アカウントが不正に利用されていないか確認する。
	定期的な職員への訓練実施	**〇標的型メールの職員訓練・注意喚起** 職員に対し、不定期に教育・訓練を行うことによって可能な限りリスクを小さくするとともに、標的型メールを受信した場合は必ず組織内の不審メール届出窓口に届けさせ、届出部門は、組織内告知にて件名や文面、添付ファイル名などを明示し、類似メールの着信がないか注意喚起を行う。 ※標的型攻撃においては 1 人でも感染すれば侵入を許してしまうことから、標的型メール訓練の効果としては、あくまで開いてしまう機会が減るだけであるが、前述の注意喚起と組み合わせ、機器による検知をすり抜けたメールを職員の“眼”で発見できる確率を少しでも向上する必要がある。また、セキュリティ担当部署へ情報が確実に集約されるよう、連絡体制等を点検する必要もある。