英国　中小企業向けサイバーセキュリティ対策の手引き

資料4

○　本年３月、英国ビジネス・イノベーション・職業技能省（BIS）は、2014年において約6割の中小企業が情報漏洩・紛失を経験し、また、情報漏洩や紛失による最大の損害が平均で1,200万円から2,200万円であったことから、本年３月に中小企業向けセキュリティ対策の手引きを公表。

○　①基礎的対策、②リスク評価アプローチによる対策、③「サイバー・エッセンシャルズ」（英国政府による認証）の取得、と対策レベルの高度化を手引きしている。

手引きにおけるサイバーセキュリティ対策の３段階

基礎的対策

○　ソフトウェアアップデートの実施

○　強度の高いパスワードの利用

○　不審メールの削除

○　アンチウイルスソフトの利用

○　政府提供のフリーオンライントレーニングの受講

リスク評価アプローチ

○　計画
- 法令やガイドラインへの適合
- すべての機器のリスクの確認
- 従業員の教育
- 緊急時の支援機関等の確認
- サイバー保険の活用　　等

○　実装
- アンチウィルスソフト等によるマルウェアからの保護
- プロキシサーバ等によるネットワークセキュリティの確保

○　評価
- 定期的見直しやインシデント原因の特定　　等

「サイバー・エッセンシャルズ」の取得

○　2014年10月より、政府調達要件となったセキュリティ認証。

○　以下の項目を要求
- システムの境界対策
- ID・パス管理や不要なソフトの削除等のセキュアなコンフィグレーションの確保
- アクセスコントロール
- マルウェア対策
- パッチマネジメント

○　ペネトレーションテスト等による認証を受けた場合は、サイバーエッセンシャルズ・プラスの認証を受ける。

（英国ビジネス・イノベーション・職業技能省（BIS）資料に基づき経産省作成）

（参考） リスク評価アプローチによる対策項目

計画

〇自社が標的になるのか、リスクを知るために、サプライヤーや顧客が攻撃されたことがあるか確認
〇個人情報保護法やクレジットカード業界が定める基準等への遵守が必要がどうか確認
〇ビジネスに大きな影響のある金融・情報資産、ITサービス（Webサービスによる決済）を特定
〇個人所有の機器やモバイル端末を含む、すべてのIT機器の評価を行い、管理・保管状況を踏まえたリスクを理解
〇オンラインサービスにアクセスする職員、顧客や第三者のパスワード強度を評価
〇職員のトレーニング
〇セキュリティ制限や投資の判断のために専門家にアドバイスできるようにする
〇攻撃を受けてオンラインサービスが停止した際の復旧手順等を定める
〇サイバー攻撃被害によるビジネスへの影響から保護するためのサイバー保険導入の検討

対策の実装

〇マルウェアからの保護
・アンチウィルスソフト
・ソフトウェアとブラウザを最新に
・不適切なウェブサイトへの制限
・セキュリティアップデート適用ポリシー策定
〇ネットワークセキュリティ
・ファイアウォール
・プロキシサーバ
・アクセス制御リスト
※無線ネットワーク含む
〇安全な機器構成
・IT資産台帳管理
・セキュアな機器設定の特定
・デフォルトPWの変更
〇ユーザー権限管理
・機器・システム・情報へのアクセス人数の最少化
・物理的な（機器盗難防止）固定
〇在宅環境や私物端末管理
・許可されたアクセス時のデータ暗号化
〇可搬媒体管理
〇機器やシステムログを保管し、不正活動の監視

評価

〇IT機器やサービス・情報のリスクレベル変化に対応するための、セキュリティ管理の定期的見直し
〇不要な機器・ソフトウェアの排除と退職者のアクセス（権）管理
〇インシデント時にマルウェアを排除し、インシデント原因を理解し、可能であれば、インシデント原因となったセキュリティ管理の穴を確認する。
〇サイバー攻撃・オンライン詐欺等に被害にあった際の通報
〇データ消失した際の顧客やサプライヤーへの通知