IT業者さんへの確認票

ご担当の範囲について、3つの質問にお答えください。担当外・未確認の項目は、その旨と理由を書いてください。答えをいただくことは、安全の保証ではありません。直っていないことは、担当と期限を決めて対応します。

記入日	
回答した会社・担当者	
自社の取りまとめ担当	
この回答の対象の機器・サービス	
緊急の連絡先・受付時間・対応してもらえる範囲	
確認や対応の追加の費用（有無・見積もり）	

質問1　VPN機器・遠隔操作のソフト

VPN機器と遠隔操作のソフトの製品名、版、サポート期限、必要な修正の適用状況、管理の担当を教えてください。要らない入口はありませんか。つなげる人・端末・場所を絞っていますか。御社が保守でつなぐ入口も含めてください。

確かめられている答えの例　「VPN機器は○○社の△△、版は○○、サポート期限は○年○月です。○月○日に、メーカーが出している必要な修正の適用を確認しました。管理は当社の○○です。外からつなげるのは御社の○名と当社の保守用の1つのIDで、つなげる場所も限っています。遠隔操作のソフトは、保守の日だけ起動しています」

あいまいな答えの例　「大丈夫です」「自動で更新されています」「たぶん入っていません」

あいまいだったら　製品名・版・サポート期限・確認した日を、メールか書面でもらう。サポートが終わっている機器は、買い替えか廃棄を相談する。使っていない遠隔操作のソフトは、用途と業務への影響を確かめてから、止めるか消してもらう。

状態	確認済み　／　未確認　／　対象外　　理由：
確認した日・根拠の記録	
直っていないこと・直す担当・期限	
答え	

質問2　二段階認証（違う種類を組み合わせる多要素認証）

遠隔接続、メール、大事な管理画面（会計・予約・ホームページなど）のそれぞれで、社員と御社のアカウントに二段階認証がかかっていますか。方式（パスワードと認証アプリなど）も書いてください。かかっていないものはありますか。

確かめられている答えの例　「遠隔接続とメールは、パスワードと認証アプリの組み合わせで、全員にかかっていることを○月○日に設定画面で確認しました。予約の管理画面は二段階認証に対応していないため、つなげる場所を限っています。○月までに対応する仕組みに替える予定です。当社の担当者も1人ずつ別のアカウントです」

あいまいな答えの例　「主なアカウントにはかけています」「管理用は共有なので外しています」

あいまいだったら　かかっていないアカウントの一覧をもらう。対応していないものは、理由・代わりの守り方・変える期限を書いてもらう。辞めた人や契約の終わった業者のアカウントは、その時点で止めてもらう。

状態	確認済み　／　未確認　／　対象外　　理由：
確認した日・根拠の記録	
直っていないこと・直す担当・期限	
答え	

質問3　消されないバックアップと、戻した記録

普段の端末や管理者のIDが乗っ取られても消されないコピーがあり、必要な仕事を戻せますか。最後に戻したときは、何のデータを、いつの状態まで、何時間で戻しましたか。

確かめられている答えの例　「会計と予約のデータは、普段の端末や管理者のIDを奪われても、保存期間中は消したり書き換えたりできない保管先にも毎日コピーしています。保存期間は○日分で、この設定は○月○日に確認しました。○月○日に、会計のデータを前日の状態まで、本番を上書きしない場所に戻し、○時間かかりました」（保存期間と戻す時間は、業務によって決めます）

あいまいな答えの例　「取っています」「クラウドにあるので大丈夫です」「戻したことはありません」

あいまいだったら　業務のデータを上書きしない方法で、戻す練習を計画してもらう。何のデータを、いつの状態まで、何時間で戻せたかを書いてもらう。

状態	確認済み　／　未確認　／　対象外　　理由：
確認した日・根拠の記録	
直っていないこと・直す担当・期限	
答え	

この票は、年に1回の棚卸しと、業者さんの担当者が替わったときに、もう一度使います。重大な弱点の公表や設定の変更があったときは、その都度、業者さんと確かめます。

HaruIroAI ブログ「IT業者さんに、この3つを聞いてください」より
https://www.haruiroai.co/blog/security/vendor-security-3-questions/