【付録】C.よくあるQ&A事例集

共通、標的型メール攻撃（Emotet）、ランサムウェアの3区分にてよくあるQ&Aをまとめています。詳細については、出典先の情報をご確認ください。

区分	No	Q	A	出典
共通	1	法令上「サイバーセキュリティ」はどのように定義されているのか？	サイバーセキュリティ基本法（平成26年法律第104号）第2条において、サイバーセキュリティが定義されています。保護すべき客体として情報、情報システム、情報通信ネットワークの3つを挙げており、外部からのサイバー攻撃への対応に限らないものとなっています。また、いわゆる情報のCIA（機密性、完全性、可用性）も定義の中に実質含まれています。	NISC：「サイバーセキュリティ関係法令Q&Aハンドブック」
	2	情報のCIA（機密性、完全性、可用性）とは何ですか？	JIS Q 27000では、以下の通り定義されています。 ・機密性 (Confidentiality): 情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること ・完全性 (Integrity): 情報が破壊、改ざん又は消去されていない状態を確保すること ・可用性 (Availability): 情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること	JIS Q 27000
	3	セキュリティ対策といってもまず、何からやればいいのか？	IPAが提示している「情報セキュリティ5か条」を参考に、できることから始めましょう。 ①OSやソフトウェアは常に最新の状態にしよう！ ②ウイルス対策ソフトを導入しよう！ ③パスワードを強化しよう！ ④共有設定を見直そう！ ⑤脅威や攻撃の手口を知ろう！	IPA：「中小企業の情報セキュリティ対策ガイドライン」
	4	会社が保有する情報の漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）によって会社又は第三者に損害が生じた場合、会社の役員（取締役・監査役）は、どのような責任を問われるか？	取締役（会）が決定したサイバーセキュリティ体制が、当該会社の規模や業務内容に鑑みて適切でなかったため、会社が保有する情報が漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）されたことにより会社に損害が生じた場合、体制の決定に関与した取締役は、会社に対して、任務懈怠（けたい）に基づく損害賠償責任（会社法第423条第1項）を問われ得ます。	NISC：「サイバーセキュリティ関係法令Q&Aハンドブック」
	5	インシデント発生時に対応含めてどの程度の費用がかかるのか？	インシデントにより直接的または漢籍的に発生しうる費用項目を洗い出し、それぞれの費用項目について対応を請け負う企業・組織へのアンケートやインタビュー調査、またはインターネット上の公開データを調査し集計した資料を参照ください。 https://www.jnsa.org/result/incidentdamage/2021.html	JNSA：「インシデント損害額調査レポート　2021年版」
標的型メール攻撃（Emotet）	6	外部からなりすましメールが届いたという報告があった場合どうすればよいですか？	以下のケースが考えられます。ケースの状況に応じて感染している可能性は異なりますので、詳細は、出典先の情報をご確認ください。 A）なりすましメールの送信者として表示されているアカウントの端末がEmotetに感染して、メール情報やアドレス帳の情報などが窃取された B) メールの送受信をしたことがある方（取引先やユーザなど）の端末がEmotetに感染して、アドレス帳を窃取された（連絡を受けた方はEmotetに感染していないが、メールアドレスがEmotetの送信先リストに加えられた）	JPCERT/CC：「マルウエアEmotetへの対応FAQ」 https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html
	7	Emotet の感染有無を確認するためにはどうすればよいですか?	EmoCheckによるEmotet感染有無の確認が可能です。ダウンロード手順や実行手順などの詳細は、出典先の情報をご確認ください。	
	8	EmotetはWindows OS以外に感染しますか?	Windows OS以外(Mac OS, Linux, iOS, Android等)での感染は確認されていません。（2020.1.23情報）	
	9	Emotet の感染を確認した場合どのように対処すればよいですか?	以下の対応が必要です。詳細は、出典先の情報をご確認ください。 ・感染端末の隔離、証拠保全、および被害範囲の調査 ・感染した端末が利用していたメールアカウントなどのパスワード変更 ・感染端末が接続していた組織内ネットワーク内の全端末の調査 ・ネットワークトラフィックログの調査 ・他のマルウェアの感染有無の確認 ・被害を受ける（攻撃者に窃取されたメールアドレス）可能性のある関係者への注意喚起 ・感染した端末の初期化	
	10	Emotetに感染しないためにはどのような対策が必要ですか?	対策については、以下のJPCERT/CCで公開している注意喚起をご参照ください。 JPCERT/CC: マルウエア Emotet の感染に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190044.html	
ランサムウェア	11	被害について相談したいがどうしたらいいか？	警察への通報や所管省庁などへの報告のほか、インシデント対応の初動段階での対応方法について相談したい場合、JPCERT/CCなどの専門機関の相談窓口への相談や、緊急対応を行うセキュリティ専門企業への調査依頼をご検討ください。詳細は、出典先の情報をご確認ください。	JPCERT/CC：「侵入型ランサムウェア攻撃を受けたら読むFAQ」 https://www.jpcert.or.jp/magazine/security/ransom-faq.html#q1-2
	12	被害にどのように対応すべきか？	JPCERT/CCでは、侵入型ランサムウェア攻撃の被害の初動対応相談に対して、次の3つの方針をお伝えしています。詳細は、出典先の情報をご確認ください。 (A) 攻撃の被害範囲を把握し、被害の最小化を図る (B) 攻撃の原因を解消するため、考えられる侵入経路を塞ぐ (C) 攻撃者の要求には応じず、バックアップから復旧する	
	13	被害を抑えるためにはどうすべきか？	被害を認知あるいは検知した後は、状況や攻撃の進行段階に応じて、以下のような、被害の拡大や攻撃の進行を防ぐための対応実施を検討します。詳細は、出典先の情報をご確認ください。 ・侵害を受けたシステムの切り離し ・侵害を受けたシステムやアカウントへの対応 ・予防的なアクセス制御や認証強化 ・被害を免れたバックアップの保護	
	14	攻撃者に身代金を支払うべきか？	JPCERT/CCは、次に挙げるような理由から身代金の支払いを選択するべきではないと考えます。 (a) 暗号化されたファイルが復元される保証がない (b) 被害原因や侵害による他の被害は未解消のまま (c) 支払い後に別の攻撃の被害や支払い要求を受ける恐れがある	
	15	被害公表前になぜ被害に関する情報が報じられているのか？	リークサイトに被害組織名が掲載されると、この情報が公に拡散するケースがあります。また、マルウェアの検体などをオンラインスキャンサービスにアップロードすると、検体によって特定の組織の被害が推測されるデータが含まれているような場合、同じく被害事実が推測されるケースがあります。また、被害により広範囲の業務影響が発生した場合に、対外サービスの停止や関係者によるSNSでの書き込みなどにより被害事実が推測されるケースもあります。	

【出典】JPCERT/CC：「マルウエアEmotetへの対応FAQ」https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html
JPCERT/CC：「侵入型ランサムウェア攻撃を受けたら読むFAQ」https://www.jpcert.or.jp/magazine/security/ransom-faq.html#q1-2
NISC：「サイバーセキュリティ関係法令Q&Aハンドブック」https://www.nisc.go.jp/security-site/law_handbook/index.html
JNSA：「インシデント損害額調査レポート　2021年版」https://www.jnsa.org/result/incidentdamage/2021.html