【FISC サイバーセキュリティ参考情報 No.1】

平成 27 年 10 月 30 日

公益財団法人　金融情報システムセンター

情報収集並びに攻撃発生時の相談先の例

Ⅰ 問合せ内容

サイバー攻撃に対応するために、事前の情報収集並びに攻撃発生時の相談先として、どのようなセキュリティ対応機関が利用できるか。

Ⅱ 関連する FISC 安全対策基準

基準番号	小項目	項番	解説
【運 113】	サイバー攻撃対応態勢を整備すること。	6	サイバー攻撃に対応するためには、事前の情報収集並びに攻撃発生時の相談先として、セキュリティ対応機関を利用することが望ましい。

Ⅲ 留意点及び参考情報

事前の情報収集並びに攻撃発生時の相談先として、表 1 に挙げた機関がございます。

表 1 では「1.『FISC 安全対策基準』に掲載されている機関」と、「2.『FISC 安全対策基準』に掲載されていない機関」の順に記載しております。

なお、これらの機関につきましては、当センターから利用を推奨するものではなく、金融機関等が利用できる機関の例でございます。利用に際しては、各機関に詳細をご確認の上、ご検討頂きますようお願い申し上げます。

【表１】

１．『FISC 安全対策基準』に掲載されている機関（順不同）

機関名	FISC 安全対策基準の掲載箇所			URL
	項番	小項目	記載内容	
独立行政法人 情報処理推進機構（IPA）	【運 103】	不正使用を防止すること。	(参考 3) 不正アクセス対策、Web アプリケーションの脆弱性、セキュアプログラミング等に関する WEB サイト 独立行政法人情報処理推進機構(IPA)セキュリティセンター	https://www.ipa.go.jp/
	【運 105-1】	顧客対応方法を明確にすること。	(参考 1) コンピュータウイルス等の不正プログラム対策やフィッシング対策等、利用者に周知すべき事項に関する情報に関する WEB サイト 独立行政法人情報処理推進機構(IPA)セキュリティセンター	
	【運 106】	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。	(参考 1) コンピュータウイルス等の不正プログラム対策やフィッシング対策等、利用者に周知すべき事項に関する情報に関する WEB サイト 独立行政法人情報処理推進機構(IPA)セキュリティセンター	
	【技 10】	プログラム作成段階での品質を確保すること。	(参考 1) Web システムの脆弱性対策の参考文献「安全なウェブサイトの作り方」 独立行政法人情報処理推進機構(IPA)セキュリティセンター	
	【技 29】	伝送データの漏洩防止策を講ずること。	(参考 2) 「安全なウェブサイトの作り方」 独立行政法人情報処理推進機構(IPA)セキュリティセンター	
	【技 43】	外部ネットワークからの不正侵入防止機能を設けること。	(参考 3) 標的型攻撃に関する参考の WEB サイト 独立行政法人情報処理推進機構(IPA)	
	【技 49】	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	(表 1) コンピュータウイルス対策の例 感染が発見された場合の届け出	
			(参考 3) スパイウェアに関する参考の WEB サイト 独立行政法人情報処理推進機構(IPA)セキュリティセンター	

機関名	FISC 安全対策基準の掲載箇所			URL
	項番	小項目	記載内容	
一般社団法人 JPCERT コーディネーションセンター （JPCERT/CC）	【運 105-1】	顧客対応方法を明確にすること。	(参考 2) フィッシングサイト閉鎖の協力を行う専門機関の例 JPCERT コーディネーションセンター(JPCERT/CC)	https://www.jpcert.or.jp/
	【運 106】	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。	(参考 2) フィッシングサイト閉鎖の協力を行う専門機関の例 JPCERT コーディネーションセンター(JPCERT/CC)	
	【技 43】	外部ネットワークからの不正侵入防止機能を設けること。	(参考 4) 組織内 CSIRT に関する参照 URL 一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)	
内閣官房 内閣サイバーセキュリティセンター（NISC）	【運 103】	不正使用を防止すること。	(参考 2) 重要インフラ防護のための政府のサイバーテロ対策 ・重要インフラの情報セキュリティ対策に係る行動計画	http://www.nisc.go.jp/
	【技 43】	外部ネットワークからの不正侵入防止機能を設けること。	(参考 3) 標的型攻撃に関する参照 URL 内閣サイバーセキュリティセンター(NISC)	
独立行政法人 産業技術総合研究所 （2015 年 4 月に国立研究開発法人産業技術総合研究所に改名）	【技 10】	プログラム作成段階での品質を確保すること。	(参考 1) Web システムの脆弱性対策の参考文献 「安全な Web サイト利用の鉄則」 独立行政法人産業技術総合研究所情報セキュリティ研究センター	https://www.rcis.aist.go.jp/index-ja.html
	【技 29】	伝送データの漏洩防止策を講ずること。	(参考 2) Web サイトの設計に関する参考文献「安全な Web サイト利用の鉄則」 独立行政法人産業技術総合研究所情報セキュリティ研究センター	
	【技 49】	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	(参考 2) フィッシング対策の参考文献「安全な Web サイト利用の鉄則」 独立行政法人産業技術総合研究所情報セキュリティ研究センター	

機関名	FISC 安全対策基準の掲載箇所			URL
	項番	小項目	記載内容	
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）	【技 49】	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	(参考 3) スパイウェアに関する参考の WEB サイト 日本ネットワークセキュリティ協会(JNSA)スパイウェア対策啓発 WG	http://www.jnsa.org/
一般社団法人 日本スマートフォンセキュリティ協会（JSSEC）	【運 50】	運用管理方法を明確にすること。	(参考 3) スマートデバイスのセキュリティ対策や利用者に周知すべき情報を公開しているガイドライン「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」	https://www.jssec.org/
日本コンピュータセキュリティインシデント対応チーム協議会 （日本シーサート協議会）	【技 43】	外部ネットワークからの不正侵入防止機能を設けること。	(参考 4) 組織内 CSIRT に関する参照 URL 日本コンピュータセキュリティインシデント対応チーム協議会(日本シーサート協議会)	http://www.nca.gr.jp/
フィッシング対策協議会	【運 103】	不正使用を防止すること。	(参考 4) フィッシング対策の参考文献「フィッシング対策ガイドライン」	https://www.antiphishing.jp/
	【技 10】	プログラム作成段階での品質を確保すること。	(参考 1) Web システムの脆弱性対策の参考文献「フィッシング対策ガイドライン」	
	【技 49】	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	(参考 2) フィッシング対策の参考文献「フィッシング対策ガイドライン」	

２．『FISC 安全対策基準』に掲載されていない機関（順不同）

機関名	URL
一般社団法人 金融 ISAC	http://www.f-isac.jp/
一般財団法人 日本サイバー犯罪対策センター（JC3）	https://www.jc3.or.jp/