情報セキュリティヒント集

この資料はダウンロードしてお使いください。

ケース1　電子メールによるサイバー攻撃

No	質問	回答（O・×）	対策のヒント
1	メールシステムは、ウイルスや迷惑メールを駆除する機能を有する製品を利用していますか。		セキュリティ機能を有するメールシステムを利用することで攻撃メールを検知・対処することができ、メールを悪用したサイバー攻撃の被害を抑えることができます。
2	不審なメールの受信情報やその見分け方等を社内共有する仕組みを構築していますか。		「身に覚えのないメールの添付ファイルは開かない・本文中のURLリンクはクリックしない」「自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない」ことを従業員に周知してください。
3	マクロの自動実行を無効化していますか。		Officeファイルのマクロ機能を悪用したサイバー攻撃が観測されています。マクロの自動実行を無効化するとともに、安易にマクロを有効化しないよう従業員に周知してください。また、マクロの有無が判別できない旧形式「.doc」「.xls」の利用は推奨できません。
4	OSやアプリケーション、セキュリティソフトは常に最新の状態にできていますか。		OSやアプリケーション、セキュリティソフトの更新は、従業員任せにせず集中管理することが推奨されます。また、高度化するサイバー攻撃に対応するために、EDR等の高機能なセキュリティソフトを導入すると効果的です。
5	端末やブラウザに認証情報を保存していませんか。		ウイルスが端末やブラウザに保存したID・パスワード等の認証情報を窃取する恐れがあります。また、端末を不正利用された場合に悪用される恐れがあるため、保存は推奨できません。
6	メールの監査ログを有効化していますか。		ウイルスに感染すると、攻撃者が感染端末を悪用し、大量の攻撃メールを外部へ送信する恐れがあります。事後調査を行うために、事前に監査ログを有効化しておく必要があります。
7	重要情報は定期的にバックアップを取得し、オフラインで保管していますか。		Emotet経由でランサムウェアに感染してファイルが暗号化された場合、バックアップデータから復旧する必要があります。ランサムウェアはネットワーク経由で感染拡大する恐れがあるため、オフラインの保管が推奨されます。
8	ウイルス等の感染が疑われる場合は、直ちにネットワークから切り離して管理者に報告することを従業員に周知していますか。		セキュリティ事故が発生した際は被害を最小限に抑えるために、速やかに対処する必要があります。ウイルスの感染拡大を抑えるためにパソコンをネットワークから切り離す、管理者に報告して速やかに対処する等、予め対応体制や手順を定めておく必要があります。

参考　○IPA　「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
　　https://www.ipa.go.jp/security/announce/20191202.html
　　○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
　　○JPCERT/CC　マルウェア Emotet の感染拡大および新たな攻撃手法について
　　https://www.jpcert.or.jp/newsflash/2020090401.html

ケース2　不正ログイン

No	チェックリスト	回答（O・×）	対策のヒント
9	パスワードは「長く」「複雑」にして「使い回さない」設定をさせていますか。		安易なパスワードを設定すると推測・解析される恐れがあるため、「長く」「複雑」にする必要があります。また、サービス毎に異なるキーワードを追加する等して「使い回さない」工夫が必要です。可能な限り「多要素認証」があるサービスの利用を推奨します。
10	社用メールアドレスの私的利用を制限していますか。		漏えいしたID・パスワードを悪用して、別のサービスへ不正ログインを試みるサイバー攻撃（パスワードリスト攻撃）が観測されています。業務と関係ないサービス等のID登録には社用メールアドレスを利用させないことを推奨します。
11	ID・パスワード等の流出を検知するサービス等を利用していますか。		ID・パスワード等が流出すると闇サイトで取引されて悪用される恐れがあります。ID・パスワード等の流出を検知・調査したい場合、流出を検知し、通知するサービス等を活用することが効果的です。
12	不正ログインを受けた場合の対処方法を決めて、周知していますか。		不正ログインに早期に気づくために、利用しているサービスのログイン履歴や利用履歴を定期的に確認することが推奨されます。不正ログインの被害を受けた場合は、速やかにパスワードの変更やアカウントの一時停止が推奨されます。

参考　○IPA　不正ログイン対策特集ページ
　　https://www.ipa.go.jp/security/anshin/account_security.html

ケース3　インターネットに接続されているサーバへの不正アクセス

No	質問	回答（O・×）	対策のヒント
13	発注者や関係先から受領したデータを、業務完了後、サーバ及びパソコン等から完全に消去していますか。		業務完了後は、図面等の工事情報を、速やかにかつ確実に返却または消去する必要があります。企業として台帳等で管理し、返却漏れや消去漏れがないか確認することが推奨されます。
14	システムメンテナンスの手順等を定めていますか。		システムメンテナンスにあたっては、あらかじめ作業手順等を定めて実施する必要があります。また、設定ミス等に気付くためにチェックリスト等を作成し、作業終了後に確認することが推奨されます。
15	システムの脆弱性診断を定期的に行っていますか。		システムの脆弱性を突くサイバー攻撃を防ぐために、システムリリース時だけでなく、定期的な脆弱性診断の実施が推奨されます。また、自社に専門的な知識をもった人材がいない場合は、外部の専門サービス等を活用することが推奨されます。
16	社外とメール以外で大容量のデータを交換する場合、会社が認める安全なファイル転送サービスを利用していますか。		適切なクラウドサービスを利用すれば、管理の手間無く、安全にデータ交換を行うことができます。FTP サーバはセキュリティ面での脆弱性が指摘されているため、利用は推奨しません。

参考　○IPA　情報セキュリティサービス基準適合サービスリスト
　　https://www.ipa.go.jp/security/it-service/service_list.html
　　○IPA　クラウドサービス安全利用の手引き
　　https://www.ipa.go.jp/files/000072150.pdf

ケース4　廃棄情報機器からの情報漏えい

No	質問	回答（O・×）	対策のヒント
17	重要な情報を保管する場合は、データの暗号化をしていますか。		重要な情報には暗号化やパスワード設定等を実施する必要があります。暗号化設定漏れを防止するために、ファイルの保存時に自動で暗号化するツールを導入すると効果的です。
18	発注者や関係先から受領したデータを、業務完了後、サーバ及びパソコン等から完全に消去していますか。		業務完了後は、図面等の工事情報を、速やかにかつ確実に返却または消去する必要があります。企業として台帳等で管理し、返却漏れや消去漏れがないか確認することが推奨されます。
19	業務完了後も必要となるデータを保管する場合は、発注者や取引先の許可を受けていますか。		業務完了後も一定期間保管する場合は、発注者や取引先の許可を受ける必要があります。また、別の記録媒体に保管し、漏えい事故が発生しないよう日常的に厳重管理し、定期的に保管された情報の棚卸を行うことが推奨されます。
20	業務完了後も必要となるデータを保管する場合は、データは安全なサーバ室や社外のデータセンターに保管していますか。		業務完了後も保管するデータは、紛失・盗難・ウイルス感染等による情報漏えいリスクや機器の故障によるデータ消失のリスクを避けるため、セキュリティ等の完備したサーバ室や社外のデータセンターのファイルサーバに保管してください。
21	委託先・サービスを選定する際はセキュリティ対策も含めて信頼できる企業を選定していますか。		ファイルサーバの保管、移送、データ消去等について、監視・警備やトレーサビリティ、情報漏えい対策等、十分な安全管理対策を行っている、信頼できる会社を選定する必要があります。また、契約書を交わし、実施状況を監督する必要があります。

ケース1～4　共通

No	質問	回答（O・×）	対策のヒント
22	情報セキュリティに関する責任者や担当者を任命し、組織的な運用を図っていますか。		情報セキュリティ対策は従業員任せにせず、組織的に取組む必要があります。また、自社に専門的な知識をもった人材がいない場合は、外部の専門サービス等を活用することが推奨されます。
23	No.1～21に関する社内規定やルール等を整備し、情報セキュリティ対策の内容を明確にしていますか。		従業員が自らルールに従って行動ができるようにするために「情報セキュリティに関するルール」を明文化し、従業員がいつでも確認できるようにする必要があります。
24	従業員に対して情報セキュリティ教育を定期的に実施し、意識付けや注意喚起を行っていますか。		情報セキュリティ教育を定期的に実施し、意識付けや適時の注意喚起を行う必要があります。情報セキュリティ教育には日本建設業連合会が提供する教育資料集の活用が推奨されます。
25	情報セキュリティ監査等によりNo.23で定めた対策などが守られていることを定期的に確認していますか。		「情報セキュリティに関するルール」は決めただけで終わりではありません。ルール通りに実行し、その状況を定期的（１回/年以上）に確認する必要があります。

参考　○一般財団法人日本建設業連合会　各種ガイドライン・教育資料集
　　https://www.nikkenren.com/kenchiku/ict/security/guideline.html
　　○IPA　中小企業の情報セキュリティ対策ガイドライン
　　https://www.ipa.go.jp/security/keihatsu/sme/guideline/