防御カード一覧

	カード内容			
	No.	（PT）	タイトル	本文
1	CSC1.1		ハードウェア資産のインベントリと管理	アクティブな検出ツールを使用して、組織のネットワークに接続されているデバイスを識別し、ハードウェア資産のインベントリを更新
2	CSC1.2		ハードウェア資産のインベントリと管理	パッシブな検出ツールを使用して、組織のネットワークに接続されているデバイスを識別し、ハードウェア資産のインベントリを更新
3	CSC1.3		ハードウェア資産のインベントリと管理	ハードウェア資産のインベントリを更新するため、DHCPサーバまたはIPアドレス管理ツールでDHCPのログを活用
4	CSC1.4		ハードウェア資産のインベントリと管理	情報を保存または処理する可能性のあるすべての資産の正確かつ最新の詳細なインベントリを更新
5	CSC1.5		ハードウェア資産のインベントリと管理	インベントリ更新に資産のネットワークアドレス、ハードウェアアドレス、マシン名、データ資産所有者、部門、資産のネットワーク接続の承認の有無を記録
6	CSC1.6		ハードウェア資産のインベントリと管理	許可されていない資産をネットワークから隔離、またはインベントリを適時に更新
7	CSC1.7		ハードウェア資産のインベントリと管理	802.1x規格に準拠したポートレベルのアクセス制御を使用して、ネットワークで認証できるデバイスを管理
8	CSC1.8		ハードウェア資産のインベントリと管理	クライアント証明書を使用して、組織の信頼されたネットワークに接続するハードウェア資産を認証
9	CSC2.1		ソフトウェア資産のインベントリ管理	ビジネス目的達成のために必要なすべての認可されたソフトウェアの最新リストを維持
10	CSC2.2		ソフトウェア資産のインベントリ管理	ベンダーが現在サポートしているアプリケーションまたはOSのみが、組織の許可されたソフトウェアインベントリに含まれていることを確認
11	CSC2.3		ソフトウェア資産のインベントリ管理	システム上の全ソフトウェアの一覧の取得を自動化するため、組織全体のソフトウェアインベントリツールを活用
12	CSC2.4		ソフトウェア資産のインベントリ管理	ソフトウェアインベントリシステムで組織が認可したOSを含む、すべてのソフトウェアの名前、バージョン、発行元、およびインストール日を追跡
13	CSC2.5		ソフトウェア資産のインベントリ管理	ソフトウェアインベントリシステムとハードウェア資産インベントリの統合ため、すべてのデバイスと関連するソフトウェアを単一の場所から追跡
14	CSC2.6		ソフトウェア資産のインベントリ管理	承認されていないソフトウェアの削除、またはインベントリの適時、更新
15	CSC2.7		ソフトウェア資産のインベントリ管理	承認されたソフトウェアのみが実行され、未承認のソフトウェアは実行されないようにアプリケーションのホワイトリスト技術をすべての資産に活用
16	CSC2.8		ソフトウェア資産のインベントリ管理	アプリケーションホワイトリストソフトウェアで承認されたソフトウェアライブラリ（＊.dll、＊.ocx、＊.so等）のみがシステムプロセスにロードされることを保証
17	CSC2.9		ソフトウェア資産のインベントリ管理	アプリケーションホワイトリストソフトウェアでデジタル署名された許可されたスクリプト（*.ps1、*.py、マクロ等）のみがシステム上で実行されることを許可
18	CSC2.10		ソフトウェア資産のインベントリ管理	物理的または論理的に分離されたシステムを使用して、業務に必要な組織へのリスクが大きいソフトウェアを切り離して実行
19	CSC3.1		継続的な脆弱性管理	最新のSCAP準拠の脆弱性スキャンツールを使用し、週単位以上の頻度でネットワーク上の全システムを自動的にスキャンし、潜在的な脆弱性を特定
20	CSC3.2		継続的な脆弱性管理	各システムのローカルで起動中のエージェント、または権限の昇格が設定されたリモートスキャナで認証された脆弱性スキャンを実行
21	CSC3.3		継続的な脆弱性管理	認証された脆弱性スキャンに使用する専用アカウントを他の管理者操作には使用せず、アカウントを特定のIPアドレスの特定のマシンに関連付ける
22	CSC3.4		継続的な脆弱性管理	OSがベンダーが提供する最新のセキュリティ更新プログラムを実行していることを確認するため、自動ソフトウェア更新ツールを展開
23	CSC3.5		継続的な脆弱性管理	サードパーティ製ソフトウェアがベンダーが提供する最新セキュリティ更新プログラムの実行を確認するため、自動化ソフトウェア更新ツールを展開
24	CSC3.6		継続的な脆弱性管理	繰り返し実施した脆弱性スキャンの結果を定期的に比較して、脆弱性が適時に修正されたことを確認
25	CSC3.7		継続的な脆弱性管理	リスク評価プロセスを利用して、発見された脆弱性の修復に優先順位を付け
26	CSC4.1		管理者特権の管理された使用	自動化されたツールを使用し、ドメインおよびローカルアカウントを含むすべての管理者アカウントを棚卸し
27	CSC4.2		管理者特権の管理された使用	新しい資産を展開する前に、すべてのデフォルトパスワードを管理者レベルのアカウントと一致する値に変更
28	CSC4.3		管理者特権の管理された使用	管理者アカウントの権限を持つすべてのユーザが昇格されたアクティビティに専用のアカウントまたはセカンダリアカウントを使用していることを確認
29	CSC4.4		管理者特権の管理された使用	多要素認証がサポートされていない場合（ローカル管理者、ルート、サービスアカウントなど）、アカウントはそのシステム固有の強力なパスワードを使用
30	CSC4.5		管理者特権の管理された使用	すべての管理者アカウントアクセスにマルチファクタ認証と暗号化されたチャネルを使用

31	CSC4.6	★	管理者特権の管理された使用	管理者はすべての管理タスクまたは管理アクセスを必要とするすべてのタスクに専用マシンを使用
32	CSC4.7	★	管理者特権の管理された使用	スクリプティングツール（Microsoft PowerShellやPythonなど）へのアクセスをこれらの機能にアクセスする必要がある管理者または開発ユーザに制限
33	CSC4.8	★	管理者特権の管理された使用	管理者権限が割り当てられたグループに追加または削除があった場合にログエントリと警告を発するようにシステムを設定
34	CSC4.9	★	管理者特権の管理された使用	管理者アカウントへのログイン失敗時にログエントリと警告を発するようにシステムを構成
35	CSC5.1	★	ハードウェアとソフトウェアのセキュアな構成	すべての認可されたオペレーティングシステムおよびソフトウェアに関する標準化したセキュリティ構成基準を文書化し、維持
36	CSC5.2	★	ハードウェアとソフトウェアのセキュアな構成	組織の承認済みの構成基準に基づいて、企業内のすべてのシステムのセキュアなイメージまたはテンプレートを維持
37	CSC5.3	★	ハードウェアとソフトウェアのセキュアな構成	イメージの許可された変更のみを確認するため、整合性を監視するツールで検証済みのセキュアなサーバにマスターイメージとテンプレートを格納
38	CSC5.4	★	ハードウェアとソフトウェアのセキュアな構成	スケジュールされた定期的な間隔で自動的にシステムに構成設定を強制し、再適用するシステム構成管理ツールを展開
39	CSC5.5	★	ハードウェアとソフトウェアのセキュアな構成	すべてのセキュリティ構成要素、承認された例外一覧、無許可の変更が発生したときの警告を検証するため、SCAP準拠の構成監視システムを使用
40	CSC6.1	★	監査ログの保守，監視，分析	全サーバーとネットワークデバイスが定期的に時刻情報を取得し、ログのタイムスタンプが一致するように、少なくとも3つの同期した時刻ソースを使用
41	CSC6.2	★	監査ログの保守，監視，分析	すべてのシステムとネットワークデバイスでローカルロギングが有効になっていることを確認
42	CSC6.3	★	監査ログの保守，監視，分析	イベントの情報源、日付、ユーザ、タイムスタンプ、送信元アドレス、宛先アドレス、その他の有用な要素など、詳細な情報をシステムログに記録
43	CSC6.4	★	監査ログの保守，監視，分析	ログを格納するすべてのシステムに、生成されるログ用の十分な記憶領域があることを確認
44	CSC6.5	★	監査ログの保守，監視，分析	分析とレビューのために、適切なログが中央ログ管理システムに集約されていることを確認
45	CSC6.6	★	監査ログの保守，監視，分析	ログ相関と分析のためにSIEMまたはログ解析ツールを導入
46	CSC6.7	★	監査ログの保守，監視，分析	定期的にログをレビューし、異常なふるまいや異常なイベントを特定
47	CSC6.8	★	監査ログの保守，監視，分析	使用可能なイベントをよりよく識別し、イベントノイズを減らすために、SIEMシステムを定期的に調整
48	CSC7.1		電子メールとWebブラウザの保護	完全にサポートされているWebブラウザと電子メールクライアントのみ組織内で実行可能なことを確認
49	CSC7.2		電子メールとWebブラウザの保護	ブラウザや電子メールクライアントの未許可なプラグイン，アドオンをアンインストールまたは無効化
50	CSC7.3		電子メールとWebブラウザの保護	すべての Web ブラウザと電子メールクライアントにおいて承認されたスクリプト言語のみに使用を制限
51	CSC7.4		電子メールとWebブラウザの保護	未承認Webサイトに接続するシステムの機能を制限するネットワークベースのURLフィルタを適用
52	CSC7.5		電子メールとWebブラウザの保護	URL分類サービスを用いて、利用可能な最新のWebサイトカテゴリ定義が最新であることを確認し、未分類のサイトはデフォルトでブロック
53	CSC7.6		電子メールとWebブラウザの保護	インシデントハンドラが侵害システムを特定するのを支援するため、オンサイト・モバイルデバイスに関わらず組織の各システムからの全URL要求を記録
54	CSC7.7		電子メールとWebブラウザの保護	DNSフィルタリングサービスを使用し、既知の悪意のあるドメインへのアクセスをブロック
55	CSC7.8		電子メールとWebブラウザの保護	有効なドメインを偽装または改ざんした電子メールの機会を減らすため、SPFおよびDKIM標準に基づくDMARCポリシーおよび検証を実装
56	CSC7.9		電子メールとWebブラウザの保護	ファイルの種類が組織のビジネスにとって不要な場合、組織の電子メールゲートウェイを通るすべての電子メールの添付ファイルをブロック
57	CSC7.10		電子メールとWebブラウザの保護	サンドボックスを使用して、悪意のある行為を伴うインバウンド電子メールの添付ファイルを分析およびブロック
58	CSC8.1		マルウェア対策	集中管理されたマルウェア対策ソフトウェアを使用して、組織のワークステーションおよびサーバのそれぞれを継続的に監視および防御
59	CSC8.2		マルウェア対策	マルウェア対策ソフトウェアのスキャンエンジン及びシグネチャデータベースを定期的に更新
60	CSC8.3		マルウェア対策	OSで利用可能なDEPやASLRなどの不正使用防止機能を有効にするか、広範なアプリケーション等の保護が可能な適切なツールキットを展開
61	CSC8.4		マルウェア対策	挿入または接続時にリムーバブルメディアのマルウェア対策スキャンを自動的に実行するようにデバイスを設定
62	CSC8.5		マルウェア対策	リムーバブルメディアからコンテンツを自動実行しないようにデバイスを設定

63	CSC8.6	マルウェア対策	分析およびアラート通知のため、エンタープライズマルウェア対策管理ツールおよびイベントログサーバにすべてのマルウェア検出イベントを送信
64	CSC8.7	マルウェア対策	既知の悪意のあるドメインにおけるホスト名のアクセスを検出するためにDNSクエリのログを有効化
65	CSC8.8	マルウェア対策	Microsoft PowershellやBashなどのコマンドシェルのコマンドライン監査ログを有効化
66	CSC9.1	サービス等の制限と管理	アクティブなポート、サービス、およびプロトコルを資産インベントリ内のハードウェア資産に関連付け
67	CSC9.2	サービス等の制限と管理	検証されたビジネスニーズがあるネットワークポート、プロトコル、およびサービスのみが各システムで実行されていることを確認
68	CSC9.3	サービス等の制限と管理	すべてのシステムに対して定期的に自動化されたポートスキャンを実行し、システム上で不正なポートの起動を検出した場合に警告
69	CSC9.4	サービス等の制限と管理	システムにホストベースのファイアウォールやポートフィルタリングツールを使用し、未許可のサービスやポートの全トラフィックを拒否するルールを適用
70	CSC9.5	サービス等の制限と管理	サーバに送信されるトラフィックを検証し、正当性を確認するため重要なサーバの前にアプリケーションファイアウォールを配置
71	CSC10.1	データ復旧機能	すべてのシステムデータが定期的に自動バックアップされることを確認
72	CSC10.2	データ復旧機能	システム全体を迅速に復旧できるように、主要なシステムのイメージングなどのプロセスを通じて完全なシステムとしてのバックアップを作成
73	CSC10.3	データ復旧機能	データの復元プロセスを実行してバックアップが正常に動作していることを確認し、定期的にバックアップメディアのデータ整合性をテスト
74	CSC10.4	データ復旧機能	バックアップの格納時及びネットワーク経由による移動時、物理セキュリティまたは暗号化によってバックアップが適切に保護されていることを確認
75	CSC10.5	データ復旧機能	全バックアップは少なくとも1つのバックアップ先があり、オペレーティングシステムの呼び出しによって継続してアドレス指定できないようにする
76	CSC11.1	ネットワーク機器のセキュアな設定	認可されたすべてのネットワークデバイスに標準の文書化されたセキュリティ構成基準を維持
77	CSC11.2	ネットワーク機器のセキュアな設定	トラフィックのネットワーク機器の通過を許可する全設定ルールは業務上の理由、業務の担当名、必要な期間とともに構成管理システムに文書化
78	CSC11.3	ネットワーク機器のセキュアな設定	使用中のネットワーク機器ごとに定義されている承認されたセキュリティ構成と全ネットワークデバイス構成を比較し、変更が検出された場合，警告
79	CSC11.4	ネットワーク機器のセキュアな設定	すべてのネットワークデバイスに最新の安定版のセキュリティ関連アップデートをインストール
80	CSC11.5	ネットワーク機器のセキュアな設定	マルチファクタ認証と暗号化されたセッションを使用して、すべてのネットワークデバイスを管理
81	CSC11.6	ネットワーク機器のセキュアな設定	ネットワークエンジニアがアクセスを必要とするすべての管理者タスクまたは権限昇格が必要なタスクに専用のマシンを使用
82	CSC11.7	ネットワーク機器のセキュアな設定	ネットワーク機器の管理セッションに別々のVLAN、別の物理接続を用い、ビジネス使用とは別のネットワーク接続を介してネットワークインフラを管理
83	CSC12.1	境界防御	組織のすべてのネットワーク境界の最新インベントリを保持
84	CSC12.2	境界防御	信頼できる各ネットワーク境界の外側から定期的にスキャンを実行し、境界を越えてアクセス可能な不正な接続を検出
85	CSC12.3	境界防御	既知の悪意あるまたは未使用のインターネットIPアドレスとの通信を拒否し、各ネットワーク境界で信頼されたIPアドレス範囲にのみアクセスを制限
86	CSC12.4	境界防御	許可されていないTCPまたはUDPポートまたはアプリケーショントラフィックに対する通信を拒否
87	CSC12.5	境界防御	各組織のネットワーク境界を通過するネットワークパケットを記録するように監視システムを構成
88	CSC12.6	境界防御	ネットワークベースのIDSセンサーを導入することで、組織の各ネットワーク境界で異常な攻撃メカニズムを探索し、システムの侵害を検出
89	CSC12.7	境界防御	ネットワークベースの侵入防御システム（IPS）を展開して、各組織のネットワーク境界で悪意のあるネットワークトラフィックをブロック
90	CSC12.8	境界防御	すべてのネットワーク境界デバイスでNetFlowおよびロギングデータを収集できるようにする
91	CSC12.9	境界防御	インターネットとの間の全ネットワークトラフィックが、未許可の接続をフィルタする認証済みのアプリケーション層プロキシを通過することを確認
92	CSC12.10	境界防御	境界プロキシで暗号化されたすべてのネットワークトラフィックを復号してから、コンテンツを分析
93	CSC12.11	境界防御	組織のネットワークへアクセスするためのすべてのリモートログインアクセスは転送データを暗号化し、マルチファクタ認証を使用
94	CSC12.12	境界防御	組織のセキュリティポリシーの強制を確認するため、ネットワークにアクセスする前にリモートログインを試みる全社内デバイスをスキャン
95	CSC13.1	データ保護	オンサイトまたはリモートサービスプロバイダーに存在する情報を含む、システムによって保管、処理、送信される全機密情報のインベントリを管理

96	CSC13.2	データ保護	組織から定期的にアクセスされない機密データやシステムをネットワークから削除
97	CSC13.3	データ保護	機密情報の不正な転送を監視・転送を遮断・情報セキュリティの専門家に警告するネットワーク周辺機器に自動化ツールを導入
98	CSC13.4	データ保護	許可されたクラウドストレージまたは電子メールプロバイダにのみアクセスを許可
99	CSC13.5	データ保護	組織から出て行くすべてのトラフィックを監視し、暗号化の不正使用を検出
100	CSC13.6	データ保護	承認された全ディスク暗号化ソフトウェアを使用して、すべてのモバイルデバイスのハードディスクドライブを暗号化
101	CSC13.7	データ保護	USBストレージデバイスが必要な場合は、特定のデバイスを使用できるようにシステムを構成できるエンタープライズソフトウェアを使用
102	CSC13.8	データ保護	外部のリムーバブルメディアをサポートするビジネス上の必要性がない場合、データを書き込まないようにシステムを設定
103	CSC13.9	データ保護	USBストレージデバイスが必要な場合は、そのデバイスに保存されているすべてのデータをセキュアに暗号化
104	CSC14.1	知る必要性に基づくアクセスコントロール	サーバに保存されている情報のラベルまたは分類レベルに基づいてネットワークを分割し、分離されたVLAN上にすべての機密情報を保存
105	CSC14.2	知る必要性に基づくアクセスコントロール	特定の目的のため、許可システムだけが必要とする他システムと通信できることを保証するため、VLAN間のファイアウォールフィルタリングを有効化
106	CSC14.3	知る必要性に基づくアクセスコントロール	隣接システムへ侵入拡大する攻撃者を制限するため、プライベートVLANやマイクロセグメンテーション等によりワークステーションの相互通信を無効化
107	CSC14.4	知る必要性に基づくアクセスコントロール	転送中のすべての機密情報を暗号化
108	CSC14.5	知る必要性に基づくアクセスコントロール	オンサイトやサービスプロバイダの情報を含む組織のシステムが保存、処理、送信する全機密情報をアクティブ検出ツールで識別、インベントリを更新
109	CSC14.6	知る必要性に基づくアクセスコントロール	ファイルシステム、ネットワーク共有、アプリケーション、データベース固有のアクセス制御リストを用いてシステムに保存されている全情報を保護
110	CSC14.7	知る必要性に基づくアクセスコントロール	ホストベースData Loss Prevention（DLP）等の自動ツールを使用し、データがシステムからコピーされてもコピーされたデータへのアクセス制御を強制
111	CSC14.8	知る必要性に基づくアクセスコントロール	情報にアクセスするためにOSに統合されていない二段階認証メカニズムを必要とするツールを使用して、すべての機密情報を保存時に暗号化
112	CSC14.9	知る必要性に基づくアクセスコントロール	機密データへのアクセスや機密データへの変更（ファイルの整合性監視、セキュリティ情報、イベント監視等のツールを使用）の詳細な監査ログを適用
113	CSC15.1	無線アクセスコントロール	有線ネットワークに接続されている許可された無線アクセスポイントのインベントリを管理
114	CSC15.2	無線アクセスコントロール	有線ネットワークに接続されている不正なワイヤレスアクセスポイントを検出してアラートを発するようにネットワーク脆弱性スキャンツールを構成
115	CSC15.3	無線アクセスコントロール	ワイヤレス侵入検知システム（WIDS）を使用して、ネットワークに接続されている不正なワイヤレスアクセスポイントを検出し、警告
116	CSC15.4	無線アクセスコントロール	ワイヤレスアクセスのビジネス目的がないデバイスにおいて、ワイヤレスアクセスを無効化
117	CSC15.5	無線アクセスコントロール	ビジネス上必要なマシンに無線アクセスを設定し、承認済の無線ネットワークへのアクセスのみを許可し、他無線ネットワークへのアクセスを制限
118	CSC15.6	無線アクセスコントロール	ワイヤレスクライアントでピアツーピア（アドホック）ワイヤレスネットワーク機能を無効化
119	CSC15.7	無線アクセスコントロール	Advanced Encryption Standard（AES）を活用して、転送中のワイヤレスデータを暗号化
120	CSC15.8	無線アクセスコントロール	ワイヤレスネットワークが相互認証、マルチファクタ認証を必要とするEAP/TLSなどの認証プロトコルを使用
121	CSC15.9	無線アクセスコントロール	ビジネス目的で必要とされる場合を除き、デバイスのワイヤレス周辺機器へのアクセス（BluetoothやNFCなど）を無効化
122	CSC15.10	無線アクセスコントロール	個人用または信頼できないデバイス用に個別のワイヤレスネットワークを作成
123	CSC16.1	アカウントの監視，管理	オンサイトまたはリモートサービスプロバイダに存在するものを含む、組織の認証システムのそれぞれのインベントリを管理
124	CSC16.2	アカウントの監視，管理	ネットワーク、セキュリティ、クラウドシステムを含むすべてのアカウントのアクセスを、可能な限り中央集中型の認証ポイントで構成
125	CSC16.3	アカウントの監視，管理	オンサイトでの管理、サードパーティのプロバイダでの管理に依らず、すべてのシステム上の全ユーザアカウントに対してマルチファクタ認証を適用
126	CSC16.4	アカウントの監視，管理	保存時にすべての認証資格情報を暗号化またはハッシュ化
127	CSC16.5	アカウントの監視，管理	すべてのアカウントのユーザ名と認証資格情報が、暗号化されたチャネルを使用してネットワーク経由で送信されていることを確認
128	CSC16.6	アカウントの監視，管理	認証システムによってまとめられたすべてのアカウントのインベントリを管理

129	CSC16.7	アカウントの監視，管理	従業員または請負業者の解雇または変更時に即座にアカウントを無効化しシステムアクセス権を取り消すための自動化されたプロセスを確立
130	CSC16.8	アカウントの監視，管理	ビジネスプロセスやビジネスオーナーに関連付けられないアカウントをすべて無効化
131	CSC16.9	アカウントの監視，管理	一定期間休止している休止状態のアカウントは自動的に無効化
132	CSC16.10	アカウントの監視，管理	すべてのアカウントに監視および強制される有効期限があることを確認
133	CSC16.11	アカウントの監視，管理	一定期間使用しないとワークステーションのセッションを自動的にロック
134	CSC16.12	アカウントの監視，管理	監査ログを使用して非アクティブ化されたアカウントにアクセスしようとする試みを監視
135	CSC16.13	アカウントの監視，管理	時刻、ワークステーションの場所、ログイン間隔など、ユーザーが通常のログイン動作から逸脱した場合に警告
136	CSC17.1	セキュリティ意識啓発プログラムの実施	スキルギャップ分析を実施して、従業員が遵守していないスキルや行動を把握し、この情報を基にしてベースラインの教育ロードマップを構築
137	CSC17.2	セキュリティ意識啓発プログラムの実施	従業員のセキュリティ行動に積極的に影響を与えるため、特定されたスキルギャップに対処するための訓練を提供
138	CSC17.3	セキュリティ意識啓発プログラムの実施	組織のセキュリティを確保するために必要な行動やスキルを理解し、発揮できるように、定期的に全従業員のセキュリティ意識向上プログラムを作成
139	CSC17.4	セキュリティ意識啓発プログラムの実施	新しい技術、脅威、標準、ビジネス要件に対応するために、組織のセキュリティ意識向上プログラムが頻繁に更新
140	CSC17.5	セキュリティ意識啓発プログラムの実施	セキュアな認証を有効にして利用することの重要性について、従業員を訓練
141	CSC17.6	セキュリティ意識啓発プログラムの実施	フィッシング、電話詐欺、偽装電話などのさまざまな形態のソーシャルエンジニアリング攻撃を特定する方法について、従業員を訓練
142	CSC17.7	セキュリティ意識啓発プログラムの実施	機密情報を特定し、適切に保管、譲渡、保管、破棄する方法について、従業員を訓練
143	CSC17.8	セキュリティ意識啓発プログラムの実施	モバイルデバイスの紛失や電子メールのオートコンプリートによる電子メール誤送信等、意図しないデータ漏洩の原因を認識するために従業員を訓練
144	CSC17.9	セキュリティ意識啓発プログラムの実施	従業員が最も一般的なインシデントのインジケータを特定し、インシデントを報告できるように従業員を訓練
145	CSC18.1	アプリケーションソフトウェアセキュリティ	使用されているプログラミング言語および開発環境に適した安全なコーディングの履行を確立
146	CSC18.2	アプリケーションソフトウェアセキュリティ	社内で開発したソフトウェアはサイズ・データタイプ・許容範囲・フォーマット等、全入力に対してエラーチェックが実行され、文書化されていることを確認
147	CSC18.3	アプリケーションソフトウェアセキュリティ	外部から取得した全ソフトウェアのバージョンがサポートされていること、または開発者のセキュリティ推奨事項に基づき適切に強化されていることを確認
148	CSC18.4	アプリケーションソフトウェアセキュリティ	組織が開発したソフトウェアには、最新の信頼できる第三者コンポーネントのみを使用
149	CSC18.5	アプリケーションソフトウェアセキュリティ	標準化され広範にレビューされた暗号化アルゴリズムのみを使用
150	CSC18.6	アプリケーションソフトウェアセキュリティ	すべてのソフトウェア開発担当者が、特定の開発環境と責任のために安全なコードを書くトレーニングを受けていることを確認
151	CSC18.7	アプリケーションソフトウェアセキュリティ	静的および動的分析ツールを適用して、内部開発されたソフトウェアのセキュリティ保護されたコーディング手法が遵守されていることを確認
152	CSC18.8	アプリケーションソフトウェアセキュリティ	セキュリティグループに連絡するための手段を提供するなど、ソフトウェア脆弱性の報告を受け入れて対処するプロセスを確立
153	CSC18.9	アプリケーションソフトウェアセキュリティ	生産システムと非生産システムのための別々の環境を管理し、開発者に本番環境への監視されていないアクセス権を付与しないようにする
154	CSC18.10	アプリケーションソフトウェアセキュリティ	一般的なWebアプリケーション攻撃に備えWebアプリケーションに流れるすべてのトラフィックを検査するWAFを実装して、Webアプリケーションを保護
155	CSC18.11	アプリケーションソフトウェアセキュリティ	データベースに依存するアプリケーションの場合は、標準のハードニング構成されたテンプレートを使用
156	CSC19.1	インシデントレスポンスと管理	人の役割とインシデントのハンドリング/管理のフェーズを定義するインシデント対応計画書が作成されていることを確認
157	CSC19.2	インシデントレスポンスと管理	特定個人にコンピュータとネットワークインシデントを処理するための職位と職務を割り当て、インシデント解決までの事案の追跡と文書化を実施
158	CSC19.3	インシデントレスポンスと管理	重要な意思決定の役割を果たすことによりインシデント対応プロセスをサポートする管理担当者とその代行者を指定
159	CSC19.4	インシデントレスポンスと管理	システム管理者や他の従業員が異常なイベントを対応チームに報告可能な時間帯、報告の仕組み、通知に含める情報について組織全体の基準の作成
160	CSC19.5	インシデントレスポンスと管理	法執行機関、関連する政府機関、ベンダー、ISACパートナー等のセキュリティ問題を報告する必要がある第3者連絡先情報に関する情報を集め、管理
161	CSC19.6	インシデントレスポンスと管理	インシデントハンドリングチームに報告すべきコンピュータの異常やインシデントの関連する情報を全従業員に公開

162	CSC19.7	インシデントレスポンスと管理	現実の脅威に対応するための意識と緩和を維持するため、インシデント対応に携わる人員の日常的なインシデント対応演習とシナリオを計画し、実施
163	CSC19.8	インシデントレスポンスと管理	組織への既知または潜在的な影響に基づいて、インシデントスコアリングおよび優先順位付けスキーマを作成
164	CSC20.1	ペネトレーションテスト，レッドチーム訓練	ワイヤレス、クライアントベース、Webアプリケーションの攻撃など、あらゆる種類の複合型攻撃を含む侵入テストのプログラムを確立
165	CSC20.2	ペネトレーションテスト，レッドチーム訓練	定期的な外部および内部からの侵入テストを実施して、エンタープライズシステムの悪用可能な脆弱性および攻撃経路を特定
166	CSC20.3	ペネトレーションテスト，レッドチーム訓練	組織の準備状況をテストすることに加えて、迅速かつ効果的な攻撃の特定・阻止や対応のため、定期的なレッドチームの演習を実施
167	CSC20.4	ペネトレーションテスト，レッドチーム訓練	攻撃者にとって有用な保護されていないシステム情報と成果物（ネットワーク構成図、設定ファイル、パスワード等）の存在を発見するためのテストを実施
168	CSC20.5	ペネトレーションテスト，レッドチーム訓練	特定の侵入テストのための実稼働環境を模擬したテストベッドを作成し、通常では実働環境でテストできない要素にレッドチームによる攻撃を実施
169	CSC20.6	ペネトレーションテスト，レッドチーム訓練	脆弱性スキャンと侵入テストツールを連携して使用
170	CSC20.7	ペネトレーションテスト，レッドチーム訓練	可能な限り、レッドチーム演習の結果は、コンピュータで読み取り可能なオープンな標準（SCAPなど）を使用して文書化されていることを確認
171	CSC20.8	ペネトレーションテスト，レッドチーム訓練	侵入テストのために使用されるユーザまたはシステムアカウントが、承認された目的でのみ使用されていることを確認し、テストの終了後には削除