防御カード一覧

	カード内容			
	No.	(PT)	タイトル	本文
1	CSC1.1		許可，無許可のデバイスのインベントリ	自動化された資産インベントリ検出ツールを適用し，ネットワークに接続された資産インベントリを作成
2	CSC1.2		許可，無許可のデバイスのインベントリ	DHCPサーバのロギング機能により，資産インベントリを改善し不明デバイスを検出
3	CSC1.3		許可，無許可のデバイスのインベントリ	機器の新規取得に伴い資産インベントリを更新し，承認デバイスのネットワーク接続を確認
4	CSC1.4		許可，無許可のデバイスのインベントリ	ネットワークアドレスなどの情報を記録し，接続したシステムおよびデバイスの資産インベントリを保守
5	CSC1.5		許可，無許可のデバイスのインベントリ	ネットワークに接続可能なデバイスを制限するために，802.1x によるネットワークレベル認証を適用
6	CSC2.1		許可，無許可のソフトウェアのインベントリ	許可されているソフトウェアの変更を検証するファイル完全性チェックツールによるモニタ
7	CSC2.2		許可，無許可のソフトウェアのインベントリ	アプリケーションのホワイトリストテクノロジーを適用
8	CSC2.3		許可，無許可のソフトウェアのインベントリ	使用中の各OSタイプに対応したソフトウェアインベントリツールを組織全体に適用
9	CSC3.1		ハードウェア，ソフトウェアのセキュアな設定	使用中のOSおよびソフトウェアの標準的なセキュア設定を確立し，この設定を使用
10	CSC3.2		ハードウェア，ソフトウェアのセキュアな設定	厳密な設定管理に従い新規システムを構築するために使用するセキュアなイメージをビルド
11	CSC3.3		ハードウェア，ソフトウェアのセキュアな設定	安全に設定されたサーバにマスターイメージを格納
12	CSC3.4		ハードウェア，ソフトウェアのセキュアな設定	サーバ，ホスト，ネットワークデバイスなどのリモート管理はセキュアなチャネルを介して実施
13	CSC3.5		ハードウェア，ソフトウェアのセキュアな設定	ファイル完全性チェックツールを使用し重要システムファイルの変更の有無を確認
14	CSC3.6		ハードウェア，ソフトウェアのセキュアな設定	リモートテストで測定可能なセキュアな設定を確認し，無許可な設定変更時にアラートを出力
15	CSC3.7		ハードウェア，ソフトウェアのセキュアな設定	定期的な構成設定を自動的に実施・再適用するシステム設定管理ツールを適用
16	CSC4.1		継続的な脆弱性診断及び修復	ネットワーク上の全システムに対し，毎週よりも高頻度で自動化された脆弱性スキャンを実行
17	CSC4.2		継続的な脆弱性診断及び修復	イベントログと脆弱性スキャン情報との関連付けを実施
18	CSC4.3		継続的な脆弱性診断及び修復	セキュリティ構成の分析に各マシンのローカルで実行されているエージェントなどを使用
19	CSC4.4		継続的な脆弱性診断及び修復	脆弱性情報提供サービスに登録し，取得した情報を脆弱性スキャンアクティビティに毎月更新
20	CSC4.5		継続的な脆弱性診断及び修復	OSやソフトウェアの自動化パッチ管理・更新ツールを安全に使用可能な全システムに適用
21	CSC4.6		継続的な脆弱性診断及び修復	スキャンアクティビティと権限付きアカウントを介した関連アクセスが正当な時間枠でのみ実行されていることを確認
22	CSC4.7		継続的な脆弱性診断及び修復	脆弱性スキャンの結果を比較し，パッチの適用などにより脆弱性が対処されたことを確認
23	CSC4.8		継続的な脆弱性診断及び修復	脆弱性の悪用可能性と潜在的影響からリスク評価のプロセスを確立し，適切な資産グループに基づき分割
24	CSC5.1		管理者権限のコントロールされた使用	管理権限を最小限に抑え，必要な場合にのみ管理アカウントを使用
25	CSC5.2		管理者権限のコントロールされた使用	自動化ツールを使用し，管理アカウントインベントリから管理権限ユーザの上級管理者による承認を確認
26	CSC5.3		管理者権限のコントロールされた使用	ネットワークに新規デバイスを適用する前にデフォルトパスワードを管理者アカウントレベルの値に変更
27	CSC5.4		管理者権限のコントロールされた使用	ドメイン管理者グループへのアカウント追加・削除時にログエントリを発行し，アラートを送信
28	CSC5.5		管理者権限のコントロールされた使用	管理者アカウントへのログイン失敗時にログエントリを発行し，アラートを送信
29	CSC5.6		管理者権限のコントロールされた使用	すべての管理者アクセスに対して多要素認証を使用
30	CSC5.7		管理者権限のコントロールされた使用	管理者アクセスに多要素認証を使用していない場合，ユーザアカウントには長いパスワードを使用

31	CSC5.8		管理者権限のコントロールされた使用	システムアクセス時に完全にログが記録される非管理者アカウントの使用を管理者に対し，義務付け
32	CSC6.1		監査ログの保守，監視，分析	ログ内のタイムスタンプを整合するため，デバイスが定期的に時刻同期する時刻ソースを2つ以上組み込む
33	CSC6.2		監査ログの保守，監視，分析	各種監査ログ設定を検証し，タイムスタンプ，ソースアドレスなど有用な要素が含まれていることを確認
34	CSC6.3		監査ログの保守，監視，分析	十分なストレージスペースがあることを定期的に確認し，ログ循環間隔内でログの容量超過を防止
35	CSC6.4		監査ログの保守，監視，分析	セキュリティ担当者やシステム管理者がログの異常を特定するため隔週のレポートを作成
36	CSC6.5		監査ログの保守，監視，分析	ネットワーク境界デバイスがすべてのトラフィックを詳細に記録するよう構成
37	CSC6.6		監査ログの保守，監視，分析	複数のマシンからのログの集約，統合，関連付け，分析のため，SIEMツールまたはログ分析ツールを適用
38	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
39	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
40	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不必要なスクリプト言語の使用を制限
41	CSC7.4		電子メールとWebブラウザの保護	オンサイト・モバイルデバイス問わず，組織の各システムからのすべてのURLリクエストのログを取得
42	CSC7.5		電子メールとWebブラウザの保護	各システムに2つの別個のブラウザ設定を適用
43	CSC7.6		電子メールとWebブラウザの保護	組織から未承認のWeb サイトへの接続を制限するネットワークベースの URL フィルタを維持・適用
44	CSC7.7		電子メールとWebブラウザの保護	電子メールメッセージがスプーフされる可能性を減らすため，Sender Policy Framework（SPF）を実装
45	CSC7.8		電子メールとWebブラウザの保護	全電子メールをスキャンし，悪意のあるコードや不要なファイルタイプを含むメールをブロック
46	CSC8.1		マルウェア対策	自動化ツールを利用し，アンチウイルス，ホスト IPSなどの機能を持つデバイスを継続的にモニタ
47	CSC8.2		マルウェア対策	レピュテーション機能または管理者が手動でシグネチャ更新可能なアンチマルウェアソフトを採用
48	CSC8.3		マルウェア対策	外部デバイスの利用を承認・文書化された業務要件に限定
49	CSC8.4		マルウェア対策	データ実行防止（DEP），アドレス空間配置ランダム化（ASLR）などを有効化
50	CSC8.5		マルウェア対策	DNSクエリのロギングを有効にし，悪意のある C2ドメインを検索するホストを検知
51	CSC9.1		サービス等の制限，コントロール	検証済みの業務要件に対応したポート，プロトコル，サービスのみが稼働していることを確認
52	CSC9.2		サービス等の制限，コントロール	許可された通信以外をドロップする拒否ルールを持つホストベースファイアウォールなどをホストに適用
53	CSC9.3		サービス等の制限，コントロール	重要なサーバに対して自動化されたポートスキャンを定期的に実行し，既知の有効なベースラインと比較
54	CSC9.4		サービス等の制限，コントロール	インターネットアクセスできるサーバをすべて確認し，業務目的で必要ない場合は内部 VLANに移動
55	CSC10.1		データ復旧能力	毎週自動的にバックアップすること，機密情報が格納するシステムではより頻繁に実施することを確認
56	CSC10.2		データ復旧能力	データ復旧プロセスを実行してバックアップメディアのデータをテストする作業を定期的に実施
57	CSC10.3		データ復旧能力	バックアップの保管およびネットワーク上で移動時，物理セキュリティまたは暗号化により保護
58	CSC10.4		データ復旧能力	主要システムは1つ以上のバックアップ先を持ち，OS呼び出しで継続的アドレス指定が不可能なことを確認
59	CSC11.1		ネットワーク機器のセキュアな設定	組織で使用中の各種ネットワーク機器用に定義された標準のセキュアな設定と機器の設定とを比較
60	CSC11.2		ネットワーク機器のセキュアな設定	トラフィックの通過を許可する設定を標準設定に追加する際は，構成管理システムに文書化して記録
61	CSC11.3		ネットワーク機器のセキュアな設定	自動化ツールを使用して標準の機器設定を検証し，変更を検知
62	CSC11.4		ネットワーク機器のセキュアな設定	二要素認証および暗号化されたセッションを使用してネットワーク機器を管理
63	CSC11.5		ネットワーク機器のセキュアな設定	ネットワーク機器にセキュリティ関連の更新を実施する際は，最新の安定したバージョンをインストール

64	CSC11.6	ネットワーク機器のセキュアな設定	ネットワークインフラの構成管理は，業務ネットワークとは異なる管理用のセグメントを通じて実施
65	CSC12.1	境界防御	既知の悪意のある IP アドレスとの通信を拒否するか，信頼できるサイトのみにアクセスを制限
66	CSC12.2	境界防御	DMZにモニタシステムを構成し，少なくともパケットヘッダ情報を記録
67	CSC12.3	境界防御	ネットワーク境界上に，システムへの侵害を検知するネットワークベース IDS センサーを導入
68	CSC12.4	境界防御	ネットワークベースの IPS デバイスにより既知の不正な攻撃の動作をブロックし，IDS を補完
69	CSC12.5	境界防御	インターネットへの全通信がDMZの1つ以上のプロキシを通過するようにネットワーク境界を設計
70	CSC12.6	境界防御	すべてのリモートログインアクセスで二要素認証を使用
71	CSC12.7	境界防御	異常なアクティビティを検知するため，NetFlow収集および分析機能をDMZネットワークフローに適用
72	CSC13.1	データ保護	データのアセスメントにより暗号化および完全性コントロールを適用する必要がある機密情報を特定
73	CSC13.2	データ保護	機密データを保持するデバイスとシステムに認可されたハードドライブ暗号化ソフトウェアを適用
74	CSC14.1	Need-to-Knowによるアクセスコントロール	サーバ上に保管されている情報のラベルや重要度に応じてネットワークを分割
75	CSC14.2	Need-to-Knowによるアクセスコントロール	信頼性の低いネットワークを介した機密情報の通信は，すべて暗号化通信を使用
76	CSC14.3	Need-to-Knowによるアクセスコントロール	ネットワークにPrivate Virtual Area Networks (VLANs)を有効化
77	CSC14.4	Need-to-Knowによるアクセスコントロール	システム上に保管されているすべての情報をファイルシステム，ネットワーク共有，アクセスコントロールリスト等を使用して防御
78	CSC14.5	Need-to-Knowによるアクセスコントロール	非公開データへのアクセスに関する詳細な監査ロギングと機密データに対する特殊な認証を実装
79	CSC14.6	Need-to-Knowによるアクセスコントロール	定期的にアクセスしないアーカイブデータやシステムは組織のネットワークから分離
80	CSC15.1	無線アクセスコントロール	ネットワークに接続中の各無線デバイスが許可されたセキュリティプロファイルに一致することを確認
81	CSC15.2	無線アクセスコントロール	脆弱性スキャンツールにより有線ネットワークに接続されている無線アクセスポイントを検知
82	CSC15.3	無線アクセスコントロール	すべての無線トラフィックが，AES以上の暗号化とWPA2以上の保護の両方に対応していることを確認
83	CSC15.4	無線アクセスコントロール	無線ネットワークで認証情報の保護と相互認証を提供するEAP／TLSなどの認証プロトコルの使用を確認
84	CSC15.5	無線アクセスコントロール	無線クライアントのピアツーピア無線ネットワーク機能を無効化
85	CSC15.6	無線アクセスコントロール	Bluetooth のようなデバイスの無線周辺アクセスは文書化された業務要件で必要な場合を除き，無効化
86	CSC15.7	無線アクセスコントロール	BYOD システムなどの信頼できないデバイス向けに別の仮想ローカルエリアネットワークを構築
87	CSC16.1	アカウントの監視，コントロール	全アカウントを見直し，ビジネスプロセスと所有者に関連付けできないアカウントをすべて無効化
88	CSC16.2	アカウントの監視，コントロール	全アカウントに有効期限が設定されていることを確認し，一般ユーザが変更できないようにする
89	CSC16.3	アカウントの監視，コントロール	従業員の退職時などにアカウントを即時に無効化し，システムアクセスを失効するプロセスを確立
90	CSC16.4	アカウントの監視，コントロール	全アカウントの使用を定期的にモニタし，標準の未使用期間経過後にユーザを自動的にログオフ
91	CSC16.5	アカウントの監視，コントロール	無人のワークステーションへのアクセスを制限するため，システムのスクリーンロックを設定
92	CSC16.6	アカウントの監視，コントロール	アカウントの使用状況モニタにより休止アカウントを判別し，ユーザまたはユーザの上司に通知
93	CSC16.7	アカウントの監視，コントロール	設定したログイン失敗回数に達した場合，アカウントが標準の期間，ロックされるように設定
94	CSC16.8	アカウントの監視，コントロール	監査ログによって存在しないアカウントへのアクセスの試行をモニタ
95	CSC16.9	アカウントの監視，コントロール	全アカウントのアクセスが集中型認証ポイント（AD等）を経由するように設定
96	CSC16.10	アカウントの監視，コントロール	機密データへのアクセス権限があるすべてのユーザアカウントに多要素認証を義務付け

97	CSC16.11	アカウントの監視，コントロール	機密データへのアクセス権限があるアカウントに多要素認証を使用しない場合，長いパスワードを使用
98	CSC16.12	アカウントの監視，コントロール	ネットワーク上でユーザ名と認証情報を送信する際，暗号化チャネルを利用
99	CSC16.13	アカウントの監視，コントロール	全パスワードファイルが暗号化され，管理者権限なしではアクセスできないことを確認
100	CSC17.1	セキュリティスキル評価，適切な訓練	全従業員を対象としたベースライントレーニングと意識向上のためのロードマップを策定
101	CSC17.2	セキュリティスキル評価，適切な訓練	スキルギャップを解決するためのトレーニングを提供
102	CSC17.3	セキュリティスキル評価，適切な訓練	セキュリティ意識向上プログラムを実施
103	CSC17.4	セキュリティスキル評価，適切な訓練	電子メール内不審リンクのクリックや電話で適切な認証なしに機密情報の提供をしないか確認テストを定期的に実施
104	CSC18.1	アプリケーションソフトウェアセキュリティ	取得したすべてのソフトウェアのバージョンがサポートされているか確認し，必要に応じ更新
105	CSC18.2	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よる全トラフィックを検査する WAFを導入し，保護
106	CSC18.3	アプリケーションソフトウェアセキュリティ	自社開発ソフトウェアの場合，全入力に関する明示的なエラーチェックを実行し，文書化
107	CSC18.4	アプリケーションソフトウェアセキュリティ	Webアプリケーションリリース前及び定期的に，スキャナによりテストし，脆弱性の有無を確認
108	CSC18.5	アプリケーションソフトウェアセキュリティ	エンドユーザに対してシステムエラーメッセージを表示しないようにする
109	CSC18.6	アプリケーションソフトウェアセキュリティ	本番環境と非本番環境を別個の環境で維持し，監視下にない状況で開発者に本番環境へアクセスさせない
110	CSC18.7	アプリケーションソフトウェアセキュリティ	データベースを使用するアプリケーションについては，標準の強化設定テンプレートを使用
111	CSC18.8	アプリケーションソフトウェアセキュリティ	ソフトウェア開発担当者は全員，特定の開発環境向けのセキュアなコードを書くトレーニングを受講
112	CSC18.9	アプリケーションソフトウェアセキュリティ	自社開発のアプリケーションの場合，開発成果物が本番環境からアクセスできないことを確認
113	CSC19.1	インシデントレスポンスと管理	インシデントに対応する担当者の役割を含んだインシデントレスポンス手順を策定し，文書化
114	CSC19.2	インシデントレスポンスと管理	セキュリティインシデントを処理するための役職と職務を特定の個人に割り当て
115	CSC19.3	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プロセスをサポートする管理担当者を定義
116	CSC19.4	インシデントレスポンスと管理	インシデント通知に含める情報の種類に関する組織全体の標準を作成
117	CSC19.5	インシデントレスポンスと管理	セキュリティインシデントの報告に使用する第3者機関の連絡先に関する情報を収集，保持
118	CSC19.6	インシデントレスポンスと管理	全担当者にコンピュータ異常とインシデントの報告に関する情報を公開
119	CSC19.7	インシデントレスポンスと管理	担当者を対象にインシデントシナリオセッションを定期的に実施し，責務の理解度を確認
120	CSC20.1	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・内部ペネトレーションテストを実施し，悪用可能な脆弱性と攻撃経路を特定
121	CSC20.2	ペネトレーションテスト，レッドチーム訓練	ペネトレーションテストで使用するユーザアカウントなどがテスト終了後に除去されているか確認
122	CSC20.3	ペネトレーションテスト，レッドチーム訓練	定期的にレッドチームの訓練を実施し，組織の準備状況をテスト
123	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未保護のシステム情報や成果物の存在を確認するためのテスト
124	CSC20.5	ペネトレーションテスト，レッドチーム訓練	複合型の攻撃を念頭に置き，標的の資産を特定し，ペネトレーションテスト自体の明確な目標を策定
125	CSC20.6	ペネトレーションテスト，レッドチーム訓練	脆弱性スキャンの評価結果に基づいて，ペネトレーションテストを実施