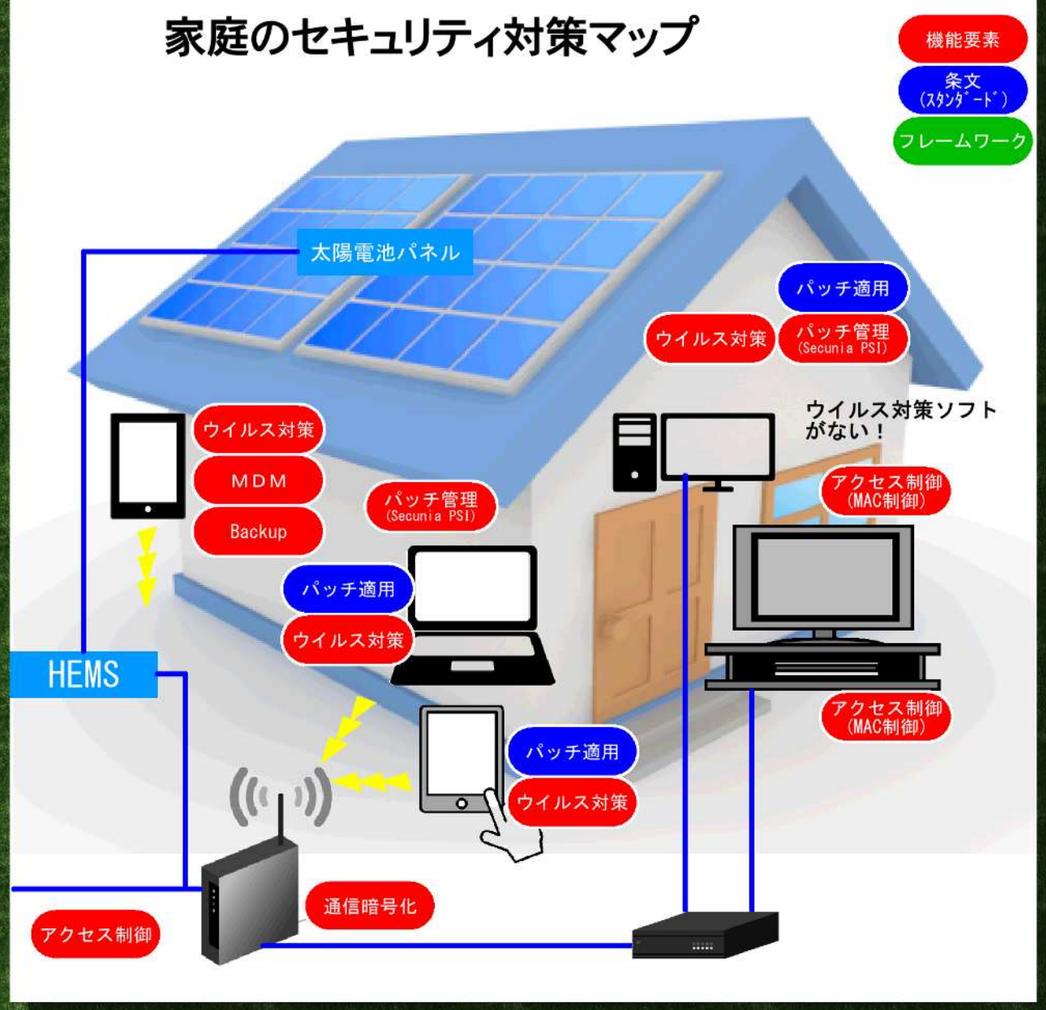
2013年度
情報セキュリティ対策マップ検討WG　活動報告書
別冊資料編

2014年6月10日

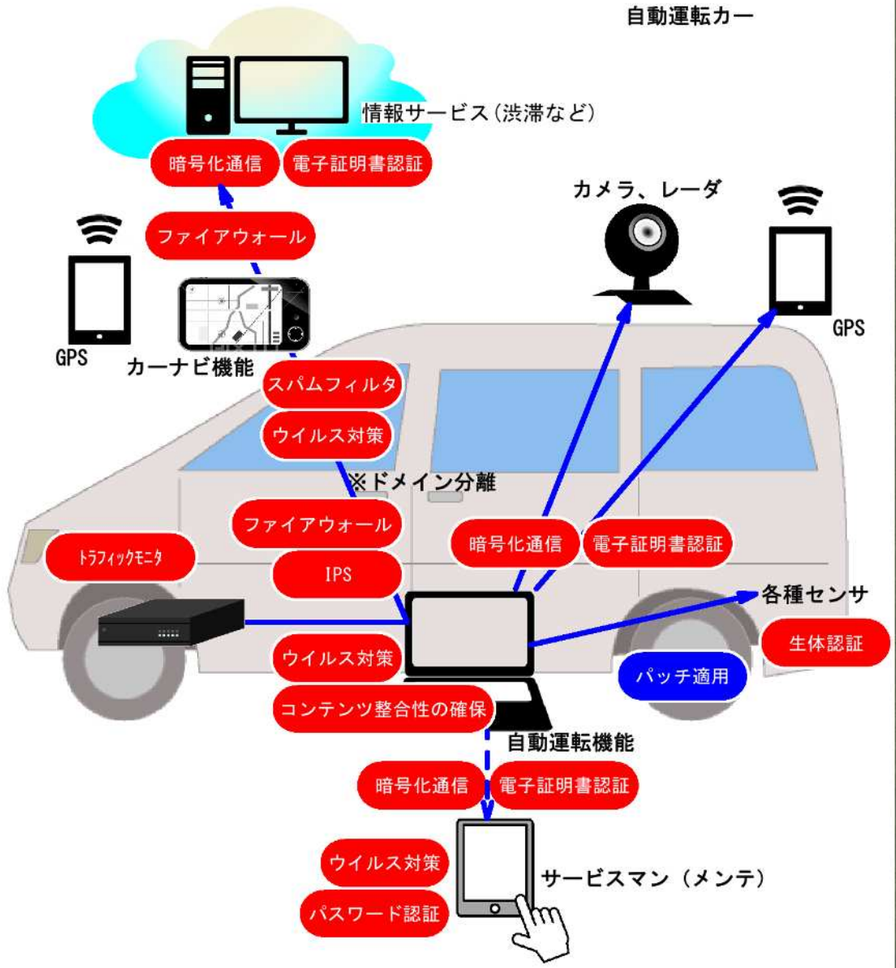
NPO 日本ネットワークセキュリティ協会
情報セキュリティ対策マップ検討ワーキンググループ

インデックス

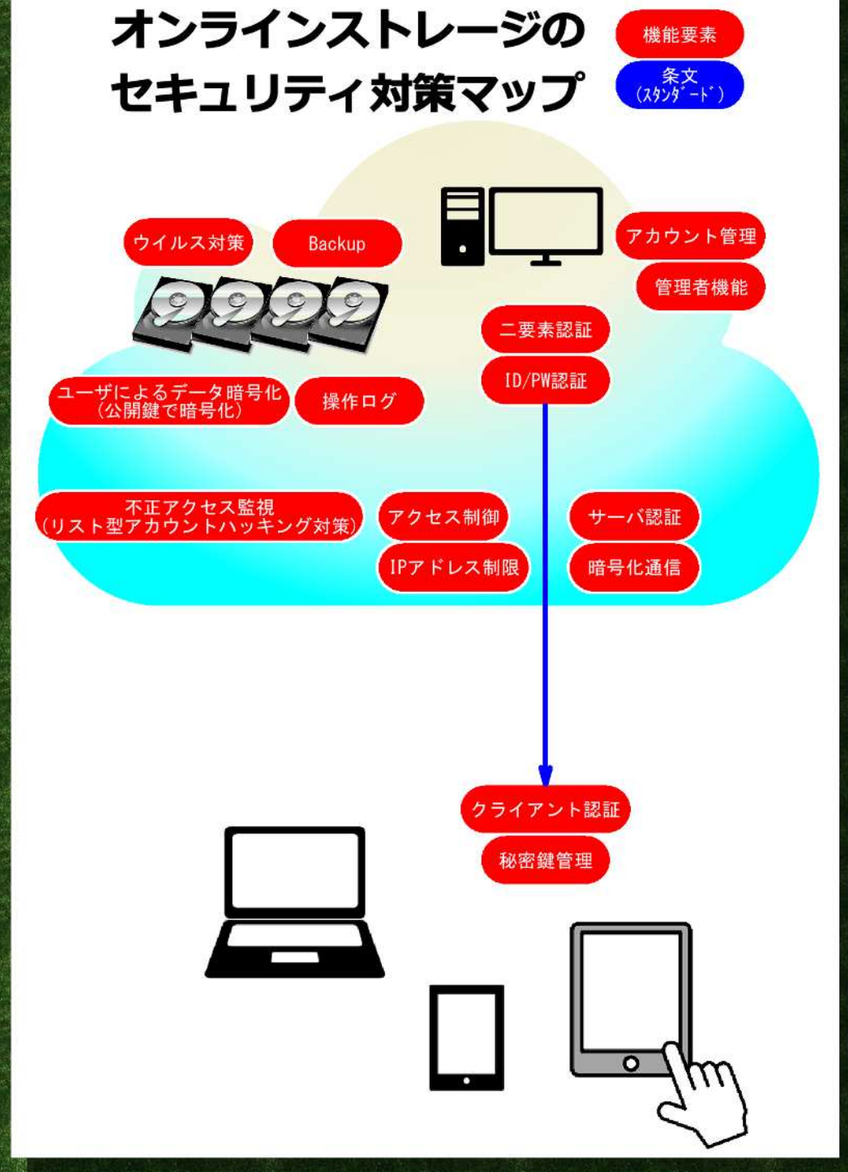
家庭のセキュリティ対策マップ



自動車のセキュリティ対策マップ

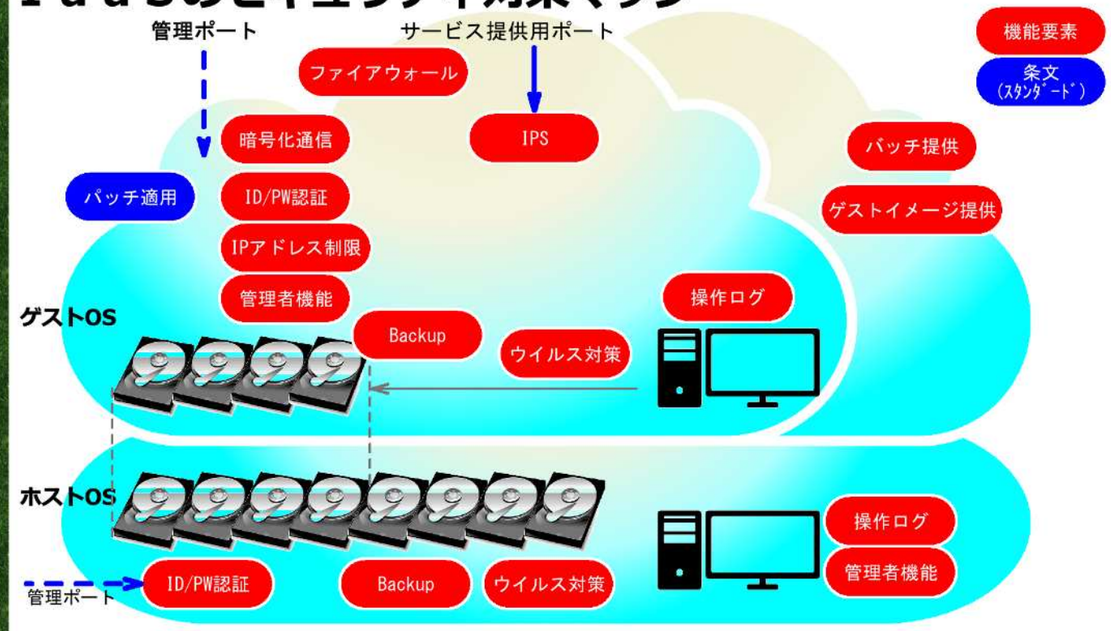


オンラインストレージのセキュリティ対策マップ

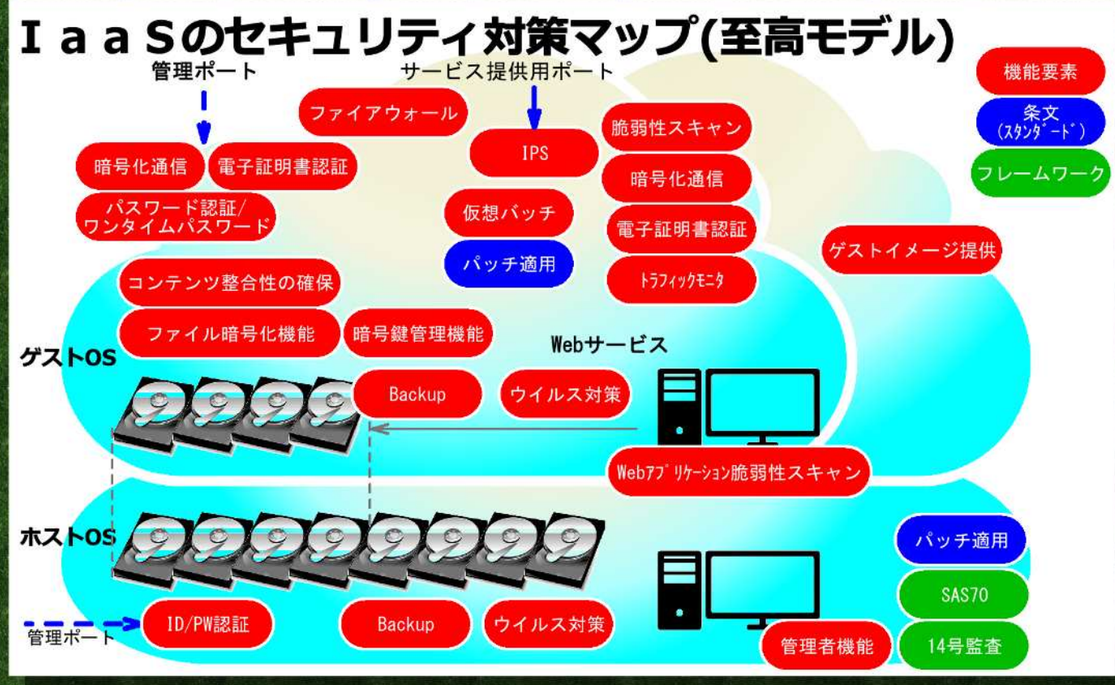


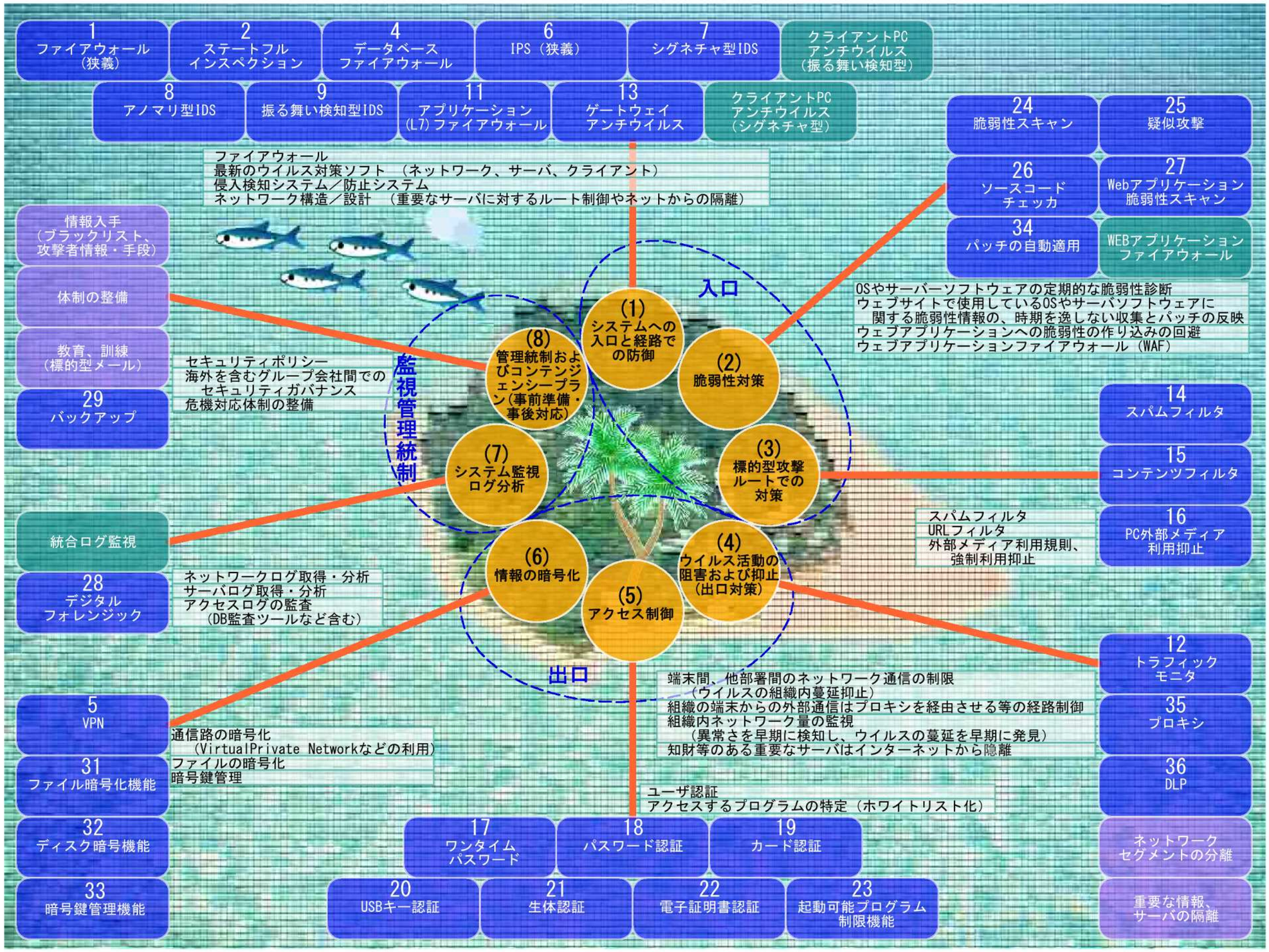
ＩａａＳのセキュリティ対策マップ

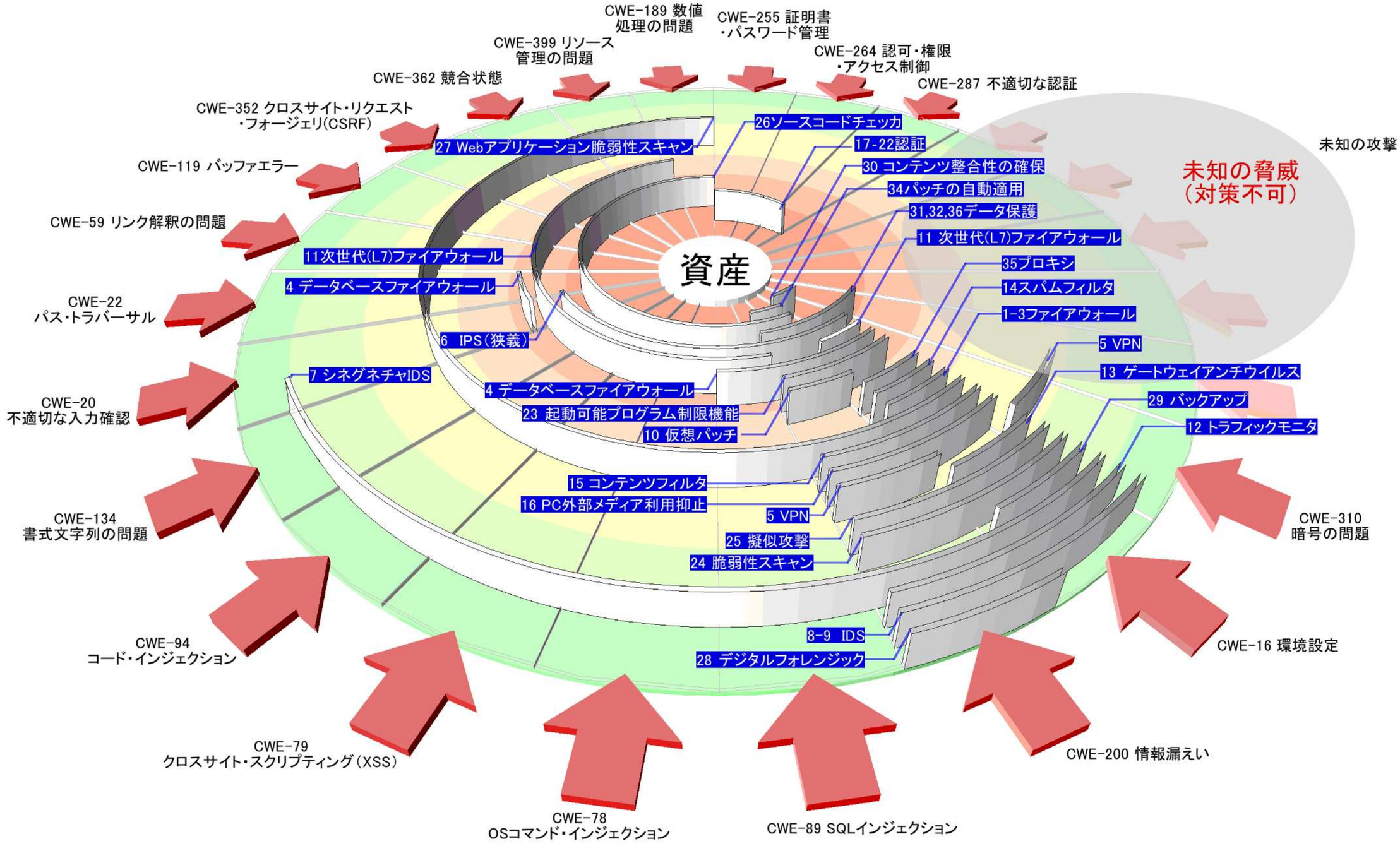
対策の必須・オプションはWG基準で決める



ＩａａＳのセキュリティ対策マップ(至高モデル)




1 ファイアウォール（狭義）
2 ステートフルインスペクション
4 データベースファイアウォール
6 IPS（狭義）
7 シグネチャ型IDS
クライアントPCアンチウイルス（振る舞い検知型）
8 アノマリ型IDS
9 振る舞い検知型IDS
11 アプリケーション(L7)ファイアウォール
13 ゲートウェイアンチウイルス
クライアントPCアンチウイルス（シグネチャ型）
ファイアウォール
最新のウイルス対策ソフト （ネットワーク、サーバ、クライアント）
侵入検知システム／防止システム
ネットワーク構造／設計 （重要なサーバに対するルート制御やネットからの隔離）
24 脆弱性スキャン
25 疑似攻撃
26 ソースコードチェッカ
27 Webアプリケーション脆弱性スキャン
34 パッチの自動適用
WEBアプリケーションファイアウォール
OSやサーバーソフトウェアの定期的な脆弱性診断
ウェブサイトで使用しているOSやサーバソフトウェアに
関する脆弱性情報の、時期を逸しない収集とパッチの反映
ウェブアプリケーションへの脆弱性の作り込みの回避
ウェブアプリケーションファイアウォール（WAF）
情報入手（ブラックリスト、攻撃者情報・手段）
体制の整備
教育、訓練（標的型メール）
29 バックアップ
セキュリティポリシー
海外を含むグループ会社間での
セキュリティガバナンス
危機対応体制の整備
監視管理統制
入口
(1) システムへの入口と経路での防御
(2) 脆弱性対策
(3) 標的型攻撃ルートでの対策
(4) ウイルス活動の阻害および抑止（出口対策）
(5) アクセス制御
(6) 情報の暗号化
(7) システム監視ログ分析
(8) 管理統制およびコンテンジェンシープラン(事前準備・事後対応)
出口
14 スパムフィルタ
15 コンテンツフィルタ
16 PC外部メディア利用抑止
スパムフィルタ
URLフィルタ
外部メディア利用規則、
強制利用抑止
統合ログ監視
28 デジタルフォレンジック
ネットワークログ取得・分析
サーバログ取得・分析
アクセスログの監査
（DB監査ツールなど含む）
12 トラフィックモニタ
35 プロキシ
36 DLP
ネットワークセグメントの分離
重要な情報、サーバの隔離
端末間、他部署間のネットワーク通信の制限
（ウイルスの組織内蔓延抑止）
組織の端末からの外部通信はプロキシを経由させる等の経路制御
組織内ネットワーク量の監視
（異常さを早期に検知し、ウイルスの蔓延を早期に発見）
知財等のある重要なサーバはインターネットから隠離
5 VPN
31 ファイル暗号化機能
32 ディスク暗号機能
33 暗号鍵管理機能
通信路の暗号化
（VirtualPrivate Networkなどの利用）
ファイルの暗号化
暗号鍵管理
ユーザ認証
アクセスするプログラムの特定（ホワイトリスト化）
17 ワンタイムパスワード
18 パスワード認証
19 カード認証
20 USBキー認証
21 生体認証
22 電子証明書認証
23 起動可能プログラム制限機能


CWE-189 数値
処理の問題
CWE-255 証明書
・パスワード管理
CWE-399 リソース
管理の問題
CWE-264 認可・権限
・アクセス制御
CWE-362 競合状態
CWE-287 不適切な認証
CWE-352 クロスサイト・リクエスト
・フォージェリ(CSRF)
CWE-119 バッファエラー
CWE-59 リンク解釈の問題
CWE-22
パス・トラバーサル
CWE-20
不適切な入力確認
CWE-134
書式文字列の問題
CWE-94
コード・インジェクション
CWE-79
クロスサイト・スクリプティング(XSS)
CWE-78
OSコマンド・インジェクション
CWE-89 SQLインジェクション
CWE-200 情報漏えい
CWE-16 環境設定
CWE-310
暗号の問題
未知の攻撃
未知の脅威
(対策不可)
資産
26ソースコードチェッカ
27 Webアプリケーション脆弱性スキャン
17-22認証
30 コンテンツ整合性の確保
34パッチの自動適用
31,32,36データ保護
11 次世代(L7)ファイアウォール
35プロキシ
14スパムフィルタ
1-3ファイアウォール
5 VPN
13 ゲートウェイアンチウイルス
29 バックアップ
12 トラフィックモニタ
11次世代(L7)ファイアウォール
4 データベースファイアウォール
6 IPS(狭義)
7 シネグネチャIDS
4 データベースファイアウォール
23 起動可能プログラム制限機能
10 仮想パッチ
15 コンテンツフィルタ
16 PC外部メディア利用抑止
5 VPN
25 擬似攻撃
24 脆弱性スキャン
8-9 IDS
28 デジタルフォレンジック

情報セキュリティ対策地図

マルウェア対策

三途の川図法 V0.4989

2011年 JNSA情報セキュリティ対策マップWG

目的界

手段界

0:マルウェアに対する［対策］を実施する。

1:マルウェアの被害発生のリスクを包括的に軽減するための［対策］を実施する。

2:［色々な場面において］マルウェアの被害発生を防止する［対策］を実施する。

3:マルウェアの被害拡大を防止する［対策］を実施する。

4:マルウェアの被害からの回復のための［対策］を実施する。

5:［感染時の経済的損害の補償］をする。

6:再発の防止のための事後対策を行う。

7:マルウェアが侵入しにくくする。

8:脆弱性をなくす。

9:マルウェアの拡散防止を行う。

10:［ツール］を利用して、［媒介物］を介して送り込まれた［悪意のコード］を検知する。

11:速やかな復旧・回復が行えるように事前の対策を行う。

12:駆除を行いマルウェアを根絶する。

13:［入手経路］から入手した許可されない［資産］の使用を禁止する。

14:組織内部のすべてのユーザに、［意識すべきこと］を意識させる。

15:事態収束後にマルウェアの感染について報告する。

16:再発防止のため、［振り返りの会議］を開催する。

17:ウェブ閲覧時にマルウェア感染防止のための［フィルタリング対策］をする。

18:［侵入防止］のため、ウイルス対策ソフトウェアを導入する。

19:［各種アプリケーション］のセキュリティ設定を適切に行う。

20:ホストの［強化措置］を行う。

21:［情報］に関する最新情報を入手する。

22:正しい情報とデマ情報を識別する。

23:［色々な対象］の脆弱性診断を実施する。

24:［色々な対象］の脆弱性を［適切に対処］する。

25:システムへの適切なアクセスを実現する［アクセス管理策］を導入する。

26:マルウェアの感染を報告する。

27:［検出］のため、ウイルス対策ソフトウェアを導入する。

28:ウイルス対策ソフトウェアを正しく設定する。

29:ウイルス対策ソフトウェアでスキャンする。

30:複数ベンダーが提供する、ウイルス対策ソフトを利用する。

31:ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを［最新に保つ］。

32:プログラムやデータのバックアップを取得する。

33:プログラムのオリジナルファイルにはライトプロテクトを施して保管する。

34:システムの変更管理を行う。

35:［駆除］のため、ウイルス対策ソフトウェアを導入する。

36:保険を適用する。

37:［IPフィルタリングデバイス］を導入する。

38:ウェブ閲覧時にマルウェア検出のための［スキャン対策］をする。

39:ウイルス対策ソフトウェアで定期的にスキャンする。

40:ウイルス対策ソフトウェアでリアルタイムにスキャンする。

41:ダウンロードファイルに対してマルウェア検出のための使用前スキャンをする。

42:すべての電子メールの添付ファイルをスキャンし、疑わしい電子メールの添付ファイルを特定し、［処理］する。

43:取り外し可能な［記録媒体］上のファイルに対する、マルウェア検出のための使用前スキャンをする。

44:ウイルス対策ソフトウェアでローカルファイルを定期的にスキャンする。

対策の実現例

フィルタリングソフト

ウイルス対策ソフト製品

セキュリティ情報サイト

セキュリティ情報提供サービス

脆弱性スキャナ製品

ファイアウォール製品

ウイルス対策ソフト製品

ウイルス対策ソフト製品

保険サービス

行番号	2012年度セキュリティ市場調査報告書P57 http://www.jnsa.org/re	大分類	中分類	仮№	機能	仮№	バリエーション	機能要素表現	一般化されたオブジェクト表現	機能オブジェクト表現	製品例	備考
1	情報セキュリティツール	ネットワーク脅威対策製品	ファイアウォールアプライアンス	1	ファイアウォール（狭義）			ルールに基づくパケットフィルタ機能（必要な通信のみ通す、「すべてを拒否」）	[メカニズムにより]ルールに基づきパケットをフィルタリングする。	[メカニズムにより]ルールに基づきパケットをフィルタリングする。		[参考] 昨今、FWの定義として、パケットフィルタのみではなく、UTMの要素も含まれる。 http://www.hitachi-solutions.co.jp/paloalto/sp/history/history1.html
2			同上	2	ステートフルインスペクション			動的パケットフィルタ機能（セッションと紐付け）	セッションと紐付けて動的にパケットをフィルタリングする。	セッションと紐付けて動的にパケットをフィルタリングする。	Cisco iMPERVA Juniper	
3			同上	3	NAT機能			NAT機能	NATする。	NATする。		既出
4			同上	4	データベースファイアウォール			Webサーバ、DBサーバ間において特定のルールに基づきDBMSへの通信を遮断する機能	Webサーバ、DBサーバ間において特定のルールに基づきDBMSへの通信を遮断する。	Webサーバ、DBサーバ間において特定のルールに基づきDBMSへの通信を遮断する。	Imperva SecureSphere Database Firewall Oracle Audit Vault and Database Firewall	
5			VPNアプライアンス／ソフトウェア	5	VPN	1		カプセリング技術によるパケットの暗号化機能	（なし）	伝送路を暗号化する。		
6			同上	5	VPN	2	SSL-VPN	SSLによる伝送路暗号化機能 [利点]IPSecより普及率が高い。様々なプロトコルにも対応。リモートアクセスだけに絞って考えると、特定のクライアントソフト等のインストールが必要なく、ファイアウォール越しでの接続性が高い為、IPsecよりも幅広い環境で利用可能。	（なし）	SSLにより伝送路を暗号化する。	IPCOM（富士通） SSLアクセラレータ（一般）	
7			同上	5	VPN	3	IPSec-VPN	IPSecによる伝送路暗号化機能 [利点]ハードウェア制御なので、トネリングではSSLより早い。企業間（専用線等）の暗号化通信のみでは、SSLより優れている。	（なし）	IPSecにより伝送路を暗号化する。	IPCOM（富士通）	
8			同上	5	VPN	4	PPTP-VPN	PPTPによる伝送路暗号化機能	（なし）	PPTPにより伝送路を暗号化する。	IPCOM（富士通）	ほぼWindows環境のみ
9			IDS/IPSアプライアンス／ソフトウェア	6	IPS（狭義）			シグネチャあるいは挙動判断による不正／異常パケットの遮断・防御機能（パケット破棄、アラート、リセットパケット送信によるコネクション切断）	（なし）	シグネチャあるいは挙動判断により不正／異常パケットを遮断する。	IPCOM（富士通） Proventia（IBM） Juniper	
10			同上	7	シグネチャ型IDS			シグネチャによる不正／異常パケットの検知機能	（なし）	シグネチャにより不正／異常パケットを検知する。	IDS/IPS製品一般	最近の傾向としては、両方の利点を活かした製品が多い。
11			同上	8	アノマリ型IDS			RFCに準拠しないパケットなど不正／異常パケットの検知機能	（なし）	パケットの異常な特性・性質により不正／異常パケットを検知する。	IDS/IPS製品一般	
12			同上	9	振る舞い検知型IDS			挙動判断による不正プログラムの検知機能	（なし）	挙動判断により不正プログラムを検知する。	FireEye	
13			IDS/IPSアプライアンス／ソフトウェア	10	仮想パッチ			IPS技術を利用して仮想的にセキュリティパッチを実現する機能	（なし）	IPS技術を利用して仮想的にセキュリティパッチを実現する。	Proventia（IBM）	
14			アプリケーションファイアウォール	11	アプリケーション（L7）ファイアウォール	1		アプリケーション単位での通信制御	（なし）	アプリケーション単位で通信制御する。	iMPERVA BARRACUDA Palo Alto Check Point Firewall Software Blade	
15			同上	11	アプリケーション（L7）ファイアウォール	2	Web アプリケーションファイアウォール	Web通信においてルールに基づきアプリケーションに有害な通信を遮断する機能	Webアプリケーションを攻撃から守る。	Web通信においてルールに基づきアプリケーションに有害な通信を遮断する。		
16			その他のネットワーク脅威対策製品	12	トラフィックモニター			ネットワークのトラフィック量をモニタリングする機能	ネットワークを監視して異常を検知する。	ネットワークのトラフィック量をモニタリングする。	WireShark	基本的にソフトウェア製品が多
17		コンテンツセキュリティ対策製品	ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス	13	ゲートウェイアンチウイルス	1		ネットワークトラフィックを監視し、シグネチャあるいは挙動判断によりウイルスやスパイウェアを検知、そして、または遮断する機能	ウイルスやスパイウェアに感染しないようにする。	ネットワークトラフィックを監視し、シグネチャあるいは挙動判断によりウイルスやスパイウェアを検知し遮断する。	McAffee、Symantec、Trendmicroなど Checkpoint	

行番号	2012年度セキュリティ市場調査報告書P57 http://www.jnsa.org/re	大分類	中分類	仮№	機能	仮№	バリエーション	機能要素表現	一般化されたオブジェクト表現	機能オブジェクト表現	製品例	備考
18			同上	13	ゲートウェイアンチウイルス	2	HTTPのマルウェアスキャン	Webサイトのコンテンツに含まれているマルウェアを検知し除去する機能		Webサイトのコンテンツに含まれているマルウェアを検知し除去する。	FireEye	
19			同上	13	ゲートウェイアンチウイルス	3	HTTPSのマルウェアスキャン	HTTPSの通信に含まれているマルウェアなどを検知し除去する機能		HTTPSの通信に含まれているマルウェアなどを検知し除去する。	McAffee、Paloalto	
20			同上	13	ゲートウェイアンチウイルス	4	POP3Sのマルウェアスキャン	POP3Sの通信に含まれているマルウェアなどを検知し除去する機能		POP3Sの通信に含まれているマルウェアなどを検知し除去する。	キヤノンESET	
21			同上	13	ゲートウェイアンチウイルス	5	IMAPSのマルウェアスキャン	IMAPSの通信に含まれているマルウェアなどを検知し除去する機能		IMAPSの通信に含まれているマルウェアなどを検知し除去する。	(要調査)	
22			同上	13	ゲートウェイアンチウイルス	6	SMTPSのマルウェアスキャン	SMTPSの通信に含まれているマルウェアなどを検知し除去する機能		SMTPSの通信に含まれているマルウェアなどを検知し除去する。	FireEye	
23			同上	13	ゲートウェイアンチウイルス	7	メールウイルスゲートウェイ	メールに添付されているマルウェアなどを検知し除去する機能(平文)		メールに添付されているマルウェアなどを検知し除去する。	アンチウィルスソフト、UTMなどに多数実装	
24			同上	13		8	アンチスパイウェア(上記全部に対してのバリエーション)				アンチウィルスソフト、UTMなどに多数実装	出口対策かもしれない。
25			スパムメール対策ソフトウェア／アプライアンス 及び メールフィルタリングソフトウェア／アプライアンス	14	スパムフィルタ			迷惑メールをフィルタリングする機能	迷惑メールを開封しないようにする。	迷惑メールをフィルタリングする。	Interscan Viruswall McAffeeなど サービスとしての実装例多い	
26			URLフィルタリングソフトウェア／アプライアンス	15	コンテンツフィルタ	1		URLベースでアクセスできるWebサイトの制限機能	不適切なWebサイトへのアクセスを禁止する。	URLベースでアクセスできるWebサイトを制限する。	i-Filter	
27			同上	15	コンテンツフィルタ	2	アンチフィッシング	レーティングに従い危険なサイトへのアクセスを防止する機能		レーティングに従い危険なサイトへのアクセスを防止する。	Phishwall	
28			DLP製品・システム(情報漏えい対策製品・システム)	16	PC外部メディア利用抑止	1		PCに接続される外部メディアの利用を抑止する機能	PCに接続される外部メディアの利用を抑止する。	PCに接続される外部メディアの利用を抑止する。	SeP CWAT 秘文 SkySea LanScope TotalSecurityFort(ファインアート) Systemwalker Desktop Patrol(富士通) MaLion(インターコム)	
29			同上	16	PC外部メディア利用抑止	2	記憶メディア	PCに接続される外部記憶メディアの利用を抑止する機能		PCに接続される外部記憶メディアの利用を抑止する。		
30		アイデンティティ・アクセス管理瀬品	個人認証用デバイス及びその認証システム	17	ワンタイムパスワード					使い捨ての一時的パスワードにより安全な認証を行う。	TheGRID(イーロックジャパン) VIP(シマンテック、旧ベリサイン)	対象によってさまざまな認証が想定できる。
31			同上	18	パスワード認証				利用者を認証する。	パスワードで認証する。	EnterpiseSSO(Evidian) SmartOn(ソリトン) GetAccess(RSA) L5ICEWall(HP) Tivoli(IBM)	
32			同上	19	カード認証	1		ICカードを利用した認証技術		ICカードを利用して認証する。	(詳細はバリエーション参	
33			同上	19	カード認証	2	接触型ICカード認証	情報の読み書きを金属端子などの物理的接触で行うICカードを利用した認証		情報の読み書きを金属端子などの物理的接触で行うICカードを利用して認証する。	SmartAccess(富士通)	
34			同上	19	カード認証	3	非接触型ICカード認証	カードの内部にアンテナを持ち、外部の端末が発信する弱い電波を利用してデータを送受信するICカードを利用した認証技術		カードの内部にアンテナを持ち、外部の端末が発信する弱い電波を利用してデータを送受信するICカードを利用して認証する。	EndopointSaver SmartOn Gemalto	
35			同上	20	USBキー認証			USBメモリ内にPINコードを保有し、OSログオンパスワードの代わりにPINコードを利用する認証方式		USBメモリ内にPINコードを保有し、OSログオンパスワードの代わりにPINコードを利用して認証する。	iKey Safety-DRSシリーズ	
36			個人認証用生体認証デバイス及びその認証システム	21	生体認証			人間の身体的特徴(生体器官)や行動的特徴(癖)の情報を用いて行う個人認証技術		人間の身体的特徴(生体器官)や行動的特徴(癖)の情報を用いて個人を認証する。	UBF(DDS) UBF(日立ソリューション) 静脈認証組込(日立製作所) 指紋認証(SecureFinger)(NEC) 指紋認証組込(富士通) SecureLoginBox(富士通)	生体認証、カード認証は、利用される局面として金融関連が多い。また、金融で普及率は高いものの、一般企業での採用率は極端に落ちる。
37			PKIシステム及びそのコンポーネント	22	電子証明書認証			電子証明書を利用する認証		電子証明書を利用して認証する。	シマンテック(旧ベリサイン)、GeoTrust	電子証明書認証を汎用的に利用するには、ICカードやUSB等に電子証明書を組み込んで、SSL認証を行うのが一般的である。

行番号	2012年度セキュリティ市場調査報告書P57 http://www.jnsa.org/re	大分類	中分類	仮№	機能	仮№	バリエーション	機能要素表現	一般化されたオブジェクト表現	機能オブジェクト表現	製品例	備考
			その他のアイデンティティ・アクセス管理製品	23	起動可能プログラム制限機能			起動可能なプログラム／プロセスを制限する機能	(なし)	起動可能なプログラム／プロセスを制限する。	SHieldWare (富士通)	詳細については要調査。
39			脆弱性検査製品	24	脆弱性スキャン			OSやサーバソフトウェアの脆弱性を検出する機能	OSやサーバの脆弱性の存在を検知する。	OSやサーバソフトウェアの脆弱性を検査し検出する。	QualysGuard nCircle 360 Retina Nessus	
40			同上	25	疑似攻撃			OSやサーバソフトウェアの脆弱性を疑似的に攻撃する機能	OSやサーバの脆弱性の重大性を把握する。	OSやサーバソフトウェアの脆弱性を疑似的に攻撃し脆弱性の重大度を評価する。	Metasploit SecureScout	
41			同上	26	ソースコードチェッカー			Webアプリケーションの脆弱性をソースコードから検出する機能	Webアプリケーションの脆弱性の存在を検知する。	Webアプリケーションの脆弱性をソースコードから検出する。	CxSuite, Fortify	
42			同上	27	Webアプリケーション脆弱性スキャン			Webアプリケーションの脆弱性を検出する機能		Webアプリケーションの脆弱性を検出する。	AppScan HackerSafe Scan Digest	
43			その他のシステムセキュリティ管理製品	28	デジタルフォレンジック			不正アクセスや機密情報漏洩などコンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称	機器やデータ、電子的記録を収集・分析し、その証拠性を明らかにする。	機器やデータ、電子的記録を収集・分析し、その証拠性を明らかにする。	スペクタープロ 7 Plus(AOSテクノロジー) EnCase FTK	将来分解する方針
44			同上	29	バックアップ			データやシステムのバックアップとは、複製（コピー）をあらかじめ作成し、たとえ問題が起きてもデータを復旧できるように備えておくこと。	データやシステムの複製（コピー）をあらかじめ作成し、たとえ問題が起きても復旧できるようにする。	データやシステムの複製（コピー）をあらかじめ作成し、たとえ問題が起きても復旧できるようにする。	ARCserve(富士通) Backup Exec Family(Symantec)	将来分解する方針
45			その他のシステムセキュリティ管理製品	30	コンテンツ整合性の確保			静的データが不正に改ざん・削除されないようコンテンツの整合性を確保する機能。	静的データが不正に改ざん・削除されないようコンテンツの整合性を検知し、必要に応じて回復する。	静的データが不正に改ざん・削除されないようコンテンツの整合性を検知し、必要に応じて回復する。	WebALARM(イーロックジャパン) Tripwire(トリップワイヤ)	
46		暗号化製品	暗号化製品	31	ファイル暗号化機能			ファイルを暗号化する機能	(なし)	ファイルを暗号化する。	Safeboot(Safenet) SOPHOS 秘文（日立製作所） EZ-SecurityFort	
47			同上	32	ディスク暗号機能			HDDを暗号化する機能	(なし)	HDDを暗号化する。	Safeboot(Safenet) Pointsec BitLocker Check Point Full Disk Encryption 秘文AEシリーズ(日立製作所)	(標的型攻撃対象外かも)
48			同上	33	暗号鍵管理機能	1		暗号鍵を管理する機能		暗号鍵を管理する。	KeyMeister(富士通) Safeboot(Safenet) CICLOCK II	
49			同上	33	暗号鍵管理機能	2	HSM	ハードウェアにより暗号鍵を管理する機能		ハードウェアにより暗号鍵を管理する機能	LUNA	
50				34	パッチの自動適用			サーバ・クライアントなどにセキュリティパッチを自動的に適用する機能	サーバ・クライアントなどにセキュリティパッチを適用する。	サーバ・クライアントなどにセキュリティパッチを自動的に適用する。	WSUS 各製品に個別に組み込まれているケースが多い（Adobeなど） FMV Lifebook (富士通)	
51			?	35	プロキシ	1		プロキシ機能	(なし)	内部ネットワークのコンピュータに代わって、「代理」としてインターネットとの接続を行う。		アプリケーションゲートウェイ（ソフトウェア型専用FW）の場合、プロキシ(Proxy)として、すべての通信を仲介。
52			?	35	プロキシ	2	HTTPプロキシ	HTTPのプロキシ機能	(なし)	HTTPに対してプロキシ機能を提供する。	Squid DigitalArts Secure Proxy Appliance(デジタルアーツ) Blue Coat ProxySG(マクニカネットワークス) IIJプロキシオプション BlackJumboDog	
53			?	35	プロキシ	3	SOCKSプロキシ	SOCKSによるプロキシ機能	(なし)	SOCKSによりプロキシ機能を提供する。	TOR Blue Coat ProxySG(マクニカネットワークス)	
54			?	35	プロキシ	4	認証プロキシ	認証プロキシ機能	(なし)	認証プロキシ機能を提供する。	TACACS+ (Cisco) Blue Coat ProxySG (Blue Coat Systems, inc)	
			?	36	DLP			機密情報をマーキングし、その漏えいを防止する機能	システムからの秘密情報の漏えいを防止する。	機密情報をマーキングし、その漏えいを防止する。	＊DLP	

脅威と対策の関係整理表

				脅威																		
				CWE-310 暗号の問題	CWE-16 環境設定	CWE-200 情報漏えい	CWE-89 SQL インジェクション	CWE-78 OSコマンド・インジェクション	CWE-79 クロスサイト・スクリプティング (XSS)	CWE-94 コード・インジェクション	CWE-134 書式文字列の問題	CWE-20 不適切な入力確認	CWE-22 パス・トラバーサル	CWE-59 リンク解釈の問題	CWE-119 バッファエラー	CWE-352 クロスサイト・リクエスト・フォージェリ (CSRF)	CWE-362 競合状態	CWE-399 リソース管理の問題	CWE-189 数値処理の問題	CWE-255 証明書・パスワード管理	CWE-264 認可・権限・アクセス制御	CWE-287 不適切な認証
28	デジタルフォレンジック	デジタルフォレンジック	3			●																
8	IDS	アノマリ型IDS	3		●	●																
9		振る舞い検知型IDS	3		●	●																
12	トラフィックモニター	トラフィックモニター	3		●	●																
7	シグネチャ型IDS	シグネチャ型IDS	3		●	●	●	●	●	●	●											
29	バックアップ	バックアップ	3		●																	
24	脆弱性スキャン	脆弱性スキャン	3		●	●																
25	疑似攻撃	疑似攻撃	3		●	●																
13	ゲートウェイアンチウイルス	ゲートウェイアンチウイルス	2		●																	
5	VPN	VPN	2	●		●																
16	PC外部メディア利用抑止	PC外部メディア利用抑止	2		●	●																
15	コンテンツフィルタ	コンテンツフィルタ	2		●	●																
27	Webアプリケーション脆弱性スキャン	Webアプリケーション脆弱性スキャン	2		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			
1	ファイアウォール	ファイアウォール (狭義)	2		●																	
2		ステートフルインスペクション	2		●																	
3		NAT機能	2		●																	
14	スパムフィルタ	スパムフィルタ	2		●																	
35	プロキシ	プロキシ	2		●																	
10	仮想パッチ	仮想パッチ	2			●																
23	起動可能プログラム制限機能	起動可能プログラム制限機能	2		●	●																
4	データベースファイアウォール	データベースファイアウォール	2		●	●	●					●										
11	次世代 (L7) ファイアウォール	次世代 (L7) ファイアウォール	2		●		●	●	●	●	●	●	●	●	●	●	●	●				
6	IPS (狭義)	IPS (狭義)	2		●	●	●	●	●	●	●											
31	データ保護	ファイル暗号化機能	1	●	●	●																
32		ディスク暗号機能	1	●	●	●																
36		DLP	1	●	●	●																
26	ソースコードチェッカー	ソースコードチェッカー	1			●	●	●	●	●	●	●	●	●	●	●	●	●	●			
34	パッチの自動適用	パッチの自動適用	1			●																
30	コンテンツ整合性の確保	コンテンツ整合性の確保	1		●																	
17	認証	ワンタイムパスワード	1																	●	●	●
18		パスワード認証	1																	●	●	●
19		カード認証	1																	●	●	●
20		USBキー認証	1																	●	●	●
21		生体認証	1																	●	●	●
22		電子証明書認証	1																	●	●	●