【添付資料1】対策オブジェクトモデルに基づくIPA標的型攻撃の機能要素による表現

2013年6月7日

	IPA提唱の「新しいタイプの攻撃」への対策（出口対策）			WG検討結果		
通番	大区分	小区分	対策	機能	バリエーション	機能要素表現
1	対策の全体像（1）～入口対策～	(1) システムへの入口と経路での防御	□ ファイアウォール	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」）
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）
3			□ 最新のウイルス対策ソフト（ネットワーク、サーバー、クライアント）	ゲートウェイアンチウイルス		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
4				ゲートウェイアンチウイルス	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
5				ゲートウェイアンチウイルス	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
6				ゲートウェイアンチウイルス	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
7				ゲートウェイアンチウイルス	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
8				ゲートウェイアンチウイルス	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
9				ゲートウェイアンチウイルス	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
10					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）	
11			□ 侵入検知システム／防止システム	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）
12				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
13				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
14				アノマリ型IDS		異常検知による不正／異常パケットの検知機能
15				振る舞い検知型IDS		挙動判断による不正／異常パケットの検知機能
16				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
17			□ ネットワーク構造／設計（重要なサーバーに対するルート制御やネットからの隔離）	動的NATによるフィルタリング		ネットワークアドレス変換（NAT）機能
18		(2) 脆弱性対策	□ OSやサーバーソフトウェアの定期的な脆弱性診断	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
19				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
20			□ ウェブサイトで使用しているOSやサーバー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			
21				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
22			□ ウェブアプリケーションへの脆弱性の作り込みの回避			
23				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
24				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
25			□ ウェブアプリケーションファイアウォール（WAF）	アプリケーション（L7）ファイアウォール		アプリケーション単位での通信制御
26				アプリケーション（L7）ファイアウォール	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
27				ー	ー	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クラウドで遮断する機能
28		(3) 標的型攻撃ルートでの対策	□ スパムフィルター	スパムフィルタ		迷惑メールをフィルタリングする機能
29			□ URLフィルター	コンテンツフィルタ		URLベースでアクセスできるWebサイトの制限機能
30				コンテンツフィルタ	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
31			□ 外部メディア利用規則、強制利用抑止	PC外部メディア利用抑止		PCに接続される外部メディアの利用を抑止する機能
32				PC外部メディア利用抑止	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
33	対策の全体像（2）～出口対策、情報保護	(4) ウイルス活動の阻害および抑止（出口対策）	□ 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）			
34			□ 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	プロキシ		プロキシ機能
35				プロキシ	HTTPプロキシ	HTTPのプロキシ機能
36				プロキシ	SOCKSプロキシ	SOCKSによるプロキシ機能
37				プロキシ	認証プロキシ	認証プロキシ機能
38			□ 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）	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
39			□ 知財等のある重要なサーバーはインターネットから隠離	ファイアウォール		
40		(5) アクセス制御	□ ユーザ認証	ワンタイムパスワード		
41				パスワード認証	SSO認証	
42				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
43				カード認証		ICカードを利用した認証技術
44				カード認証	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
45				カード認証	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
46				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
47				電子証明書認証		電子証明書を利用する認証
48			□ アクセスするプログラムの特定（ホワイトリスト化）	起動可能プログラム制限機能		起動可能なプログラムを制限する機能
49		(6) 情報の暗号化	□ 通信路の暗号化（Virtual Private Networkなどの利用）	VPN		カプセリング技術によるパケットの暗号化機能
50				VPN	SSL-VPN	SSLによる伝送路暗号化機能
51				VPN	IPSec-VPN	IPSecによる伝送路暗号化機能
52				VPN	PPTP-VPN	PPTPによる伝送路暗号化機能
53				VPN	SoftEther-VPN	
54			□ ファイルの暗号化	ファイル暗号化機能		ファイルを暗号化する機能
55				ディスク暗号機能		HDDを暗号化する機能
56			□ 暗号鍵管理	暗号鍵管理機能		暗号鍵を管理する機能
57				暗号鍵管理機能	HSM	ハードウェアにより暗号鍵を管理する機能
58	対策の全体像（3）～監視、管理統制～	(7) システム監視、ログ分析	□ ネットワークログ取得・分析	（メソッドとして処理）		ネットワーク（LAN）上を流れるパケットをキャプチャすること
59			□ サーバログ取得・分析	（メソッドとして処理）		多種・多様なログを同一筐体にて管理し、、集積・検索・レポーティング等のログ運用を統合的に行うこと
60			□ アクセスログの監査（DB監査ツールなど含む）	（メソッドとして処理）		
61		(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）	□ セキュリティポリシー	（ルール）		
62			□ 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	（ルール）		
63			□ 危機対応体制の整備	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
64				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

オブジェクト指向の手法を使ったアクティビティ図