2020年4月10日
IPA

2019年度版セキュリティ技術・サービス重要分野マップ

■「セキュリティ技術・サービス重要分野マップ」とは？
有識者会議で重要分野を選定するために作成。日本発の製品・サービスが強みを持っているか、日本固有のニーズがあるか等の観点から選定した重要分野をセキュリティ対策全体の中にマッピング。
今後、このマップをベースに重要分野の見直し、追加等を行う。

■セキュリティ技術・サービス重要分野マップの見方
組織に対するサイバーセキュリティ上の脅威について、対策が必要なプロセスに「○」をつけ(一つの脅威で5個まで)、セキュリティ対策の全体像を俯瞰したマップを作成した。作成したマップ上に、下記の重要分野が対応する部分を色分けで示した。

＜重要分野＞
①脅威の可視化
説明：通信状況のふるまいなどからサイバー攻撃を検知する製品・サービス。
日本固有の攻撃は海外製品では検知できないこともあり、 日本発の製品・サービスの提供が望まれる。
SIP(戦略的イノベーションプログラム)第1期において類似の研究開発が行われており、今後の社会実装が期待される。
②脆弱性の可視化
説明：ソフトウェアに内在する脆弱性を調査し、脆弱性の一覧表示や対策状況の管理などの機能を提供する製品・サービス。
複数の日本発製品・サービスが既に存在しており、日本が得意とする分野。
利用が拡大しているOSSへの対応を強化する、日本固有のユーザーニーズに対応するなど、海外競合製品との差別化が求められる。
③IT資産管理
説明：サーバ、PCなどのハードウェア、搭載されているソフトウェアやそのライセンスなどIT関連の資産の情報を収集し、一元管理する製品・サービス。
日本発の製品ベンダーが得意としており、国内市場でシェアも獲得できている分野。
増加するIoT機器の管理、クラウド化の進展などIT利用環境の変化への対応が必要。
④脅威インテリジェンスの整理・管理
説明：日々報告される脅威インテリジェンスから、対策すべき脅威にプライオリティをつけて、具体的な対策内容を提示し、対策状況を管理する製品・サービス。
脅威インテリジェンスをどう活かせば良いか多くのユーザーが困っているのが現状。大量の脅威インテリジェンスの収集・統合、自社の状況に合わせた優先度付け、対策の選定等。
脅威インテリジェンス管理の自動化を掲げた海外製品が既に存在しており、日本固有の脅威インテリジェンスに対応した製品・サービスの登場が期待される。
⑤マルウェア感染/発症の重篤度判定
説明：マルウェアに感染しただけか、発症しているのかを検知し、マルウェアの被害分布を把握する製品・サービス。
マルウェアに感染しただけであればリスクを許容することも可能。重篤度が分かることでインシデントレスポンスの対応が変わるため、潜在ニーズがある分野。
海外でも製品化されておらず、海外に先駆けて日本発の製品化が望まれる。
⑥教育・トレーニング
説明：従業員等へのセキュリティ教育・訓練のためのコンテンツを提供する製品・サービス。
日本では自社内にサイバーセキュリティの専門家を有していない企業が多いため、従業員等へのセキュリティ教育・訓練の実施が依然として課題となっている。
日本のユーザーニーズに沿った製品・サービスの開発・提供が求められる。
⑦ハイレベルセキュリティ検証
説明：IoT機器等の未知の脆弱性やバックドアを発見するためのセキュリティ検証技術・サービス。
日本国内に複数の検証サービス事業者が存在し、優秀な技術者が活躍している分野。高品質を追求する日本が得意とする領域。

組織に対するサイバーセキュリティ脅威(*) ＼ 対策が必要なプロセス		資産管理		リスク管理			防御		監視・検知				対応・復旧				教育・訓練
		IT資産管理	ID/アクセス管理	脆弱性管理	テスト(ペネトレーションテスト等)	リスクアセスメント	境界防御	データ保護(暗号化)	クラウド/サーバ	ネットワーク	エンドポイント	リアルタイム検知	インシデントレスポンス	分析(フォレンジック)	復旧	サイバー保険	
継続的に存在する脅威	標的型攻撃による機密情報の窃取			○		④		○			○		○				○
	内部不正による情報漏えい		○	②				○	○	①	○		④	○			⑥
	ビジネスメール詐欺による金銭被害					○					○	⑤	○			○	○
	ランサムウェアによる被害										○	○	○			○	○
	予期せぬIT基盤(クラウド、データセンター)の障害に伴う業務停止	③													○	○	○
	不注意による情報漏えい	○						○			○						○
	Web上サービスからの個人情報窃取			○		○		○	○				○				
	DDoS攻撃によるサービス停止					○	○		○	○					○		
新たに顕在化した脅威	サプライチェーンの弱点を悪用した攻撃による情報漏えい	○		○	⑦	○			○							○	
	IoT機器のBot化などの不正利用、情報漏えい	○		○	○	○						○					
	制御系システムへの攻撃による製造ライン停止			○	○	○					○	○					
	シャドーITによる不正アクセス、情報漏えい	○	○			○			○			○					
	利用しているオープンソースソフトウェアの脆弱性による不正アクセス、情報漏えい	○		○		○						○	○				

(*)：IPAが2020年1月29日に公開した「情報セキュリティ10大脅威 2020(https://www.ipa.go.jp/security/vuln/10threats2020.html)」の組織編に上げられた脅威に、制御システムへのサイバー攻撃など組織として対策すべき事項を付け加えた