情報セキュリティ市場分類区分定義表

2012 年度版

この情報セキュリティ市場分類区分定義表は、NPO 日本ネットワークセキュリティ協会が実施する情報セキュリティ市場調査において、市場を区分分類し、その規模を統計的に算出するに際して使用する定義表である。

同調査報告書を利用される際には、本表を参照の上、各市場区分の意味するところを理解し、どのような製品・サービスが対応するか確認されることをお勧めする。

また、JNSA が提供するソリューションガイドの利用に際しても、同ガイドの区分のベースとなっている本表を参照し、参考としていただければ利便が高まるものと思われる。

その他情報セキュリティ分野に属する各種製品やサービスについて調査研究等をされる際の参考となれば幸いである。

以下、表 1 には、表 2、表 3 で使用する用語･略号等の説明を載せている。

表 2、表 3 には、情報セキュリティ市場調査で用いた「情報セキュリティツール」「情報セキュリティサービス」の市場区分とその定義、もしくは説明･例示等の一覧表を掲げる。

また第 1 部、第 2 部に各市場分類の内容説明を掲載する。

表 1　用語説明

アプライアンス	ハードウェアとソフトウェアを一体として特定の機能を提供する販売形態をとる製品 1 台のコンピュータで複数の機能を提供するサーバ型コンピュータ。内部バスに複数の機能モジュールを接続して複数の機能を実現する形（いわゆるシャーシ型）を含む。ブレードサーバ形式で複数の機能サーバが並列して機能を実行し、全体として統括する OS が存在しない状態（いわゆるブレードサーバ型）は含まない。
ソフトウェア	パッケージ製品、ダウンロード製品、ライセンス販売製品等、定型化されたもの 一部カスタマイズの場合は対象に含め、完全な個別開発ソフトウェアは含まない
AV	Anti Virus アンチウイルス
FW	Firewall ファイアウォール
IDS	Intrusion Detection System 侵入検知システム
IPS	Intrusion Prevention System 侵入防止システム
PKI	Public Key Infrastructure 公開鍵暗号基盤
SSL	Secure Socket layer 暗号通信の一方式
URL	Unifie Resource Locator 統一資源位置指定子
VPN	Virtual Private Network 仮想私設通信網
PCI DSS	Payment Card Industry Data Security Standard　PCI データセキュリティ基準
QSA	Qualified Security Assessors 認定審査機関
ASV	Approved Scanning Vendors 認定スキャンベンダー

表 2　情報セキュリティツールの市場分類

大分類	中分類	定義、説明、例示　等
統合型アプライアンス		
「ネットワーク脅威対策製品」と「コンテンツセキュリティ対策製品」に分類される機能のいずれかまたは両方を備え、2つ以上の大分類カテゴリにまたがる複数の機能を1台（またはセット）で提供するアプライアンス製品。	統合型アプライアンス	アンチウイルス・アンチワームウイルス・不正プログラム対策（スパム対策・フィッシング対策機能を併設するものを含む）, FW, IDS／IPS, VPN のうち、少なくとも二つ以上の機能を装備したアプライアンス製品。（いわゆる「複合脅威対策」<Unified Threat Management =UTM=>製品でアプライアンス型であるもの） 二つ以上の大分類カテゴリにまたがる複数の機能を1台（またはセット）で提供するアプライアンス製品でUTM以外のもの。ただし、FWとVPNだけの組み合わせはファイアウォールアプライアンスに含める。
ネットワーク脅威対策製品		
主としてネットワークの境界付近に配置して通信のハンドリングまたはモニタリングを行い、設定に基づいてネットワーク通信の許可･不許可、アラート、ログ生成等、通信の制御と管理を行う製品。 通信パケットに暗号化を施し、組織外のネットワーク上でのパケット内容の盗聴・改ざんを防止する、いわゆるVPN(Virtual Private Network)製品を含む。 ファイアウォール、VPN製品、侵入検知･侵入防止製品(IDS／IPS)等を含む。	ファイアウォールアプライアンス／ソフトウェア	ネットワーク上の通信を解析し、送信元アドレス、送信先アドレス、プロトコルの種類、ポート番号、通信のステータス等の情報に基づき、あらかじめ設定されたルールまたはポリシーに従って、通信の許可、遮断、制御を行う製品。 VPN機能を併設するものを含む。 アプライアンス型製品、ソフトウェア型製品の双方を含む。
	VPNアプライアンス／ソフトウェア	ネットワーク上の通信に暗号化処理を施して、通信経路上で第三者からの盗み見、改ざん等を防止し、閉じたネットワークのような通信を可能にする機能（VPN= Virtual Private Network=機能）を提供する製品。SSL(Secure Socket Layer)-VPNを含む。 アプライアンス型、ソフトウェア型（サーバ=ゲートウェイ=型、クライアント型）の双方を含む。 ファイアウォールにVPN機能が付帯する場合はファイアウォールに分類。
	IDS／IPSアプライアンス／ソフトウェア	侵入検知（Intrusion Detection System =IDS=）・侵入防止（Intrusion Prevention System または Intrusion Protection System =IPS=）、すなわち、ネットワーク上の通信の内容や状態を一定の方法・技術に基づき解析し、侵入もしくは攻撃と判断される通信に対して報告･警告･遮断･阻止・監視･ログ記録等の対策を行う製品。 アプライアンス型製品、ソフトウェア型製品の双方を含む。
	アプリケーションファイアウォール	アプリケーションサーバへのネットワーク通信を監視･解析し、不正侵入その他の攻撃･悪用を目的とする通信に対して報告･警告･遮断･監視･ログ記録等の対策を行う製品。 アプライアンス型、ソフトウェア型の双方を含む。 典型的例として、Webアプリケーションファイアウォールがある。データベースサーバの保護を主目的とするものを含む。
	その他のネットワーク脅威対策製品	外部ネットワーク（インターネット等）から内部ネットワークに対して行われる、不正侵入、盗聴、不正プログラムの挿入などの攻撃に対して、検知、防御、抑止、警告などの防衛の機能を提供する製品で他の中分類に属さないもの。
コンテンツセキュリティ対策製品		
1. コンピュータウイルス、スパイウェア、ボット等の不正プログラム（マルウェア）などを、ファイル等の電子データや電	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	ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持ったソフトウェア（主として企業等向けにライセンス契約方式で提供されるもの）またはアプライアンス。プログラムや定義ファイル更新の年次参照権の販売を含む。

子メール送受信・Web閲覧等のコンピュータ通信の中から検出し、排除・無害化・警告等の対策を講じる機能を持つ製品群。 2. システム・業務・サービスの目的や適正な運営にとって有害な電子メール送受信やWeb閲覧等の通信を検査し、フィルタリング・警告・排除・ログ記録その他の対応を行う機能を持つ製品群。 3. 電子メール、電子ファイル等の内容（コンテンツ）について、ポリシー等あらかじめ設定された条件に基づいて、その送信・移送・受け渡し等の移動、複製・閲覧・編集・印刷等の加工その他の利用を阻止・防止もしくは制限し、または警告・報告・記録等を行う、情報保護のための製品群。		ゲートウェイ型、サーバ型、クライアント型の全てを含む。 付加機能としてFW、IDS、スパム対策、URLフィルタリング等の機能を併設するものを含む。
	ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）	ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持った、主として個人使用のクライアントパソコン向けソフトウェア。主としてパッケージ形式もしくはオンラインダウンロード形式で販売されるもの。プログラムや定義ファイル更新の年次参照権の販売を含む。 デスクトップFW、HIPS（ホストIPS）、スパム対策、URLフィルタリング等の機能を併設するものを含む。
	スパムメール対策ソフトウェア／アプライアンス	無差別・大量に送りつけられる、不要もしくは有害な内容を含む宣伝・勧誘目的等の電子メール（スパムメール）をフィルタリングし、マーキング、警告、分別、排除等を行うソフトウェアもしくはアプライアンス製品。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
	URLフィルタリングソフトウェア／アプライアンス	インターネット上のWebサイト（ホームページ）へのアクセスや閲覧につき、そのアドレスや内容が、所定の条件（有害、危険、不適格、Reputation Serviceによるリスト等）に合致（もしくは違反）する場合に処理（停止、警告、管理者への通報、ログ保存等）を行うソフトウェアもしくはアプライアンス製品。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
	メールフィルタリングソフトウェア／アプライアンス	送受信される電子メールにつき、そのアドレスや内容、添付ファイル等を検査し、所定の条件（有害、不適格、情報漏えい、Reputation Serviceによるリスト等）に合致（もしくは違反）する内容を含むものに対して処理（停止、隔離、警告、管理者への通報もしくは回送、ログ保存等。）を行うソフトウェアもしくはアプライアンス製品。単に全メールを無条件にアーカイブするだけのものを除く。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
	DLP製品・システム（情報漏えい対策製品・システム）	Data Loss/Leak/Leakage Protection/Preventionと呼ばれる製品またはシステム。 企業内システムやネットワークから外部に向かうデータの流れ（電子メールその他のネットワークトラフィック、別のストレージへの書き込み、外部記憶媒体への書き込み、印刷等）の中に特定の特徴を含むデータがある場合、その行為に対して阻止、警告、記録等の動作を行い、外部への情報・データの流出や紛失を防止する機能を提供するシステムまたは製品。
	その他のコンテンツセキュリティ対策製品	組織内（あるいは個人）と組織外の間でネットワーク通信その他の方法で受け渡しされる電子データに関して、主としてセキュリティの目的でフィルタリングその他の機能を提供する製品で、上記のいずれにも属さない、あるいは特定の中分類に仕分けできないもの。 いわゆるDigital Rights Management(DRM)製品やシステムを含む。 いわゆるフィッシング詐欺目的で送付される電子メールのフィルタリング、フィッシングサイトへのアクセスや閲覧に対する警告、Webサイトのフィッシングに関する安全性の確認等の機能を提供する、ソフトウェア、システムもしくはサービスを含む。 （ただし、一般的なサイト証明書の発行サービスは「運用・管理サービス」に分類する。）
アイデンティティ・アクセス管理製品		
ネットワーク資源、コンピューティング資源のユーザを電子的手段で特定	個人認証用デバイス及びその認証システム	ワンタイムパスワード、ICカード、USBキー、携帯電話等を用いて本人確認する機能を提供するデバイスおよびそのシステム（生体認証を除く）。

し、ユーザごとに定義されたアクセス権等に基づいて、ネットワーク資源・コンピュータ資源へのアクセスや利用の許可を行う機能を提供する製品群またはシステム。 本人特定（アイデンティファイ）と認証、アクセス権限の付与と管理、電子証明の発行と管理等の各機能を、個別にあるいは総合・連携して提供する。 いわゆるAuthentication, Authorization, Access Control の機能を提供する製品群。	個人認証用生体認証デバイス及びその認証システム	指紋、静脈等の生体の特長のみならず、声紋、筆跡等身体的特徴に着目して本人を特定する機能を提供するセンシングデバイスおよびその認証システム。
	アイデンティティ管理製品	システム並びにデータへのアクセス権について、システムの利用者に関してはその職務や権限に基づく定義のデータベースを、システム並びにアプリケーションに関してはそのアクセス許可ポリシーを管理する機能を提供する製品群。 利用者の異動に伴う変更管理や、システム間のアクセス権の情報連携や統合管理を実現し、情報資産の利用権の即時的一元的管理を可能にする。 プロビジョニング製品を含む。 フェデレーション製品（異システム・異組織間のID連携、プロビジョニング連携のための製品）を含む。
	ログオン管理／アクセス許可製品	ユーザがシステムにアクセスする際の承認・許可機能を提供する製品分類。 シングルサインオン(SSO)およびSSO間連携製品を含む。 但し、個人認証用および個人認証用生体認証デバイスと一体で機能するシステムは当該各デバイス及び認証システムに分類する。
	PKIシステム及びそのコンポーネント	電子証明書の発行、管理、証明サービスを提供するシステムおよびその構成要素。 但し、構築サービス(SI)は含まない。（サービス市場に分類する） なお、電子証明書の発行サービスはサービス市場に分類する。
	その他のアイデンティティ・アクセス管理製品	本人認証、アクセス権管理、ログオン管理等の機能を提供しまたはそれらに関連する機能・サービスを提供する製品で上記のいずれにも属さない製品。 ディレクトリサーバ（単独で製品化されているもの）を含む。

システムセキュリティ管理製品		
1．ネットワークトラフィックを監視・制御する装置等の状態やその発する情報を統合管理し、セキュリティについて分析し、表示・統計・警告・記録等を行う製品群。 2．ネットワークを構成する装置やサーバ等の設定やアプリケーションの脆弱性を検査し、結果を報告する製品群。 3．ネットワークやコンピュータを構成する機器やデバイスの情報を入手し、その状態や属性や設定や動作の監視・診断・制御・記録等の機能を持つ製品群。 4．ネットワークに接続するデバイスの設定状態等を確認し、接続の可否を制御・管理する機能を持つ製品群。 5．ファイル等の電子データの移動・複製・編集その他の処理を中心とし	セキュリティ情報管理システム／製品	FW等のセキュリティ監視・制御装置のログまたはサーバのイベントログ等の情報を統合・監視・分析し、ネットワークシステムのセキュリティ状態をリアルタイムで総合的に管理する機能を持つ製品およびシステム。 統合ネットワーク管理プラットフォームのうちセキュリティ管理モジュールの製品部分も統計対象とする。
	脆弱性検査製品	検査対象となるサーバ等に対し、スキャニングや擬似攻撃を行い、脆弱性や設定の不備等、危険事項を検査し報告する製品群。いわゆる脆弱性スキャナー（ネットワークベース、ホストベース）。
	ポリシー管理・設定管理・動作監視制御製品	1．OSやアプリケーションの設定、パッチ適用、バージョン等を監視・管理する製品群 2．クライアントマシン等におけるファイルのコピー・印刷その他の操作を監視・制限・制御等する製品群。 3．クライアントPC等の識別情報やインベントリ情報等を収集・分析・管理し、ポリシー等の設定された条件に合致しないアプリケーション等のインストール等の管理（警告・報告・禁止・削除等）を行う製品・システム。 4．その他個別のマシンの設定、状態、動作等に着目してセキュリティを管理する製品群。 5．クライアントPC等の識別情報やインベントリ情報等に基づきネットワーク接続を管理・制御する製品・システム。いわゆる「ネットワーク検疫システム」における機器認証サーバを含む。 原則として単体製品またはネットワーク制御装置等のオプションとして取引対象となる製品形態のものを対象とし、その機能がルータ等の一部にデフォルトとして組み込まれている場合は対象外とする。

	たコンピュータの動作について監視･制御･記録･警告等をする製品群。 6. その他、コンピュータとネットワークの状態や動作をセキュリティ面から管理する機能を持つ製品群。	その他のシステムセキュリティ管理製品	コンピュータネットワークシステムの、システムとしての状態を監視･解析･管理する機能を持った製品群のうち、上記セグメントのいずれにも分類されない製品群。 主としてセキュリティ、内部統制管理（ITガバナンス）等を目的としてログの収集、減量･圧縮、保管･アーカイブ、解析等を行う製品、ならびにいわゆるデジタルフォレンジック製品等を含む。 ただし、ログ収集･解析機能を提供する製品のうち、リアルタイム監視を主目的とする製品は「セキュリティ情報管理システム／製品」に分類し、当分類では主に傾向解析等スタティックな目的のものを対象とする。
暗号製品			
	データの暗号化を主たる機能とする製品群。 通信経路に対する防御を主目的に通信の暗号化を行う、いわゆるVPN製品は、「ネットワーク脅威対策製品」に分類する。	暗号製品	1. メール、ファイル、ディスク、記憶デバイス等のデータを暗号化することで権限外使用、覗き見、改ざん、漏えい等を防止することを主たる機能とする製品群。 2. ハードディスク、USBメモリ、磁気テープ装置等に組み込まれて書き込み･読み出しの際に暗号化･復号化を自動で行う機能部分を構成する暗号化モジュール。 3. 暗号ライブラリ、暗号化モジュール等の中間製品で、製品または部品として単独で取引されるもの。 4. 暗号化することでセキュリティの目的を満たすことを主たる機能とする製品で上記に属さないもの。 ただし、電子証明書発行システムは「アイデンティティ･アクセス管理」に、その関連サービスはサービス市場に分類する。

表 3　情報セキュリティサービスの市場分類

大分類	中分類	定義、説明、例示　等
情報セキュリティ･コンサルテーション		
1. 情報セキュリティについて、主として経営管理およびIT管理の領域において、管理のための政策、管理体系、運用体制等の構築、診断、監査に関する支援やコンサルティングを行うサービス。 2. これらに関連する規格認証枠組みに対応して認証取得を目指す場合の支援サービスおよび規格等の審査･認証サービス。 3. これらに類似または直接関連するコンサルティングサービス。	情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション	情報セキュリティの管理の体制や手順に関する総合的コンサルティングサービス。 情報セキュリティポリシーや管理･運用基準等の構築および見直しのサービスを含む。 情報セキュリティガバナンスの構築・取組支援サービス・コンサルテーションを含む。
	情報セキュリティ診断･監査サービス	情報セキュリティのポリシー、システム、管理体制、コンプライアンスの現状に対して診断または評価（一部では慣例的に「監査」とも呼ぶ）を行うサービス。ITシステムの弱点を擬似ネットワーク攻撃等で検査するサービスは「セキュリティ運用･管理サービス」の中に位置づける。ここでは管理体制等に対する総合的診断・評価を行うサービスを主体とするサービスを対象とする。 情報セキュリティ監査制度（経済産業省告示に基づく）における情報セキュリティ監査サービスは「情報セキュリティ関連認証・審査・監査機関（サービス）」に分類する。
	情報セキュリティ関連規格認証取得等支援サービス	情報セキュリティ監査の受審、情報セキュリティ格付けの取得、ISMS適合性認証の取得、プライバシーマーク適合認定、PCI DSS準拠認定の取得等を支援するサービス。
	情報セキュリティ関連認証・審査・監査機関（サービス）	情報セキュリティ監査（経済産業省告示に基づく「情報セキュリティ監査制度」における情報セキュリティ監査サービス）、情報セキュリティ格付け、ISMS適合性認証、プライバシーマーク適合認定等を行うサービス。 PCI DSS準拠認定を行うQSA(Qualified Security Assessors)を含む。ただし、ASV(Approved Scanning Vendors)は「セキュリティ運用･管理サービス」のうち「脆弱性検査サービス」に含める。
	その他の情報セキュリティコンサルテーション	その他の情報セキュリティ管理に関するコンサルティングサービス。 内部統制管理、事業継続管理、ITサービスマネジメント等に関連して、情報セキュリティに関わる強化・改善等を**主たる**目的として実施されるコンサルテーション等を含む。（情報セキュリティが従たるもしくは副次的目的の場合は「情報セキュリティコンサルテーション」としてはカウントしない。）
セキュアシステム構築サービス		
ITセキュリティシステム、またはITシステムのセキュリティについて、構築を支援するサービス。 ただし、セキュリティツールやそのプラットフォーム自体の価格は含めず、その導入や構築といった役務･サービス部分を集計対象とする。	ITセキュリティシステムの設計・仕様策定	ITシステムのセキュリティについて、その設計、仕様の定義、要求条件の設定等の全体の枠組み、あるいは特定機能の内容について策定するサービス。
	ITセキュリティシステムの導入・導入支援	ITセキュリティシステムまたはITシステムのセキュリティに関する、システムインテグレーションサービス。 原則として設計部分を除く導入部分のみとするが、両者が不可分の場合はこの分類に集計する。
	セキュリティ製品の選定・選定支援	顧客のポリシーや要求条件に基づいて、それに適したITセキュリティ対策製品を選定し、またはそのための情報提供等の支援を行うサービス。
	その他のセキュアシステム構築サービス	その他のITセキュリティシステム構築サービス。 ITセキュリティ製品の保守・サポート等のサービスを、メーカの製品付帯サービスの再販以外に、再販事業者やSI事業者が独自付加価値として提供する場合はこの区分で集計する。

セキュリティ運用･管理サービス			
	1. ITセキュリティシステム、またはITシステム上のセキュリティ対策機器等の運用や管理の支援を行い、状態の監視、安全対策に対する診断、インシデント等に際しての判断や対応の実施や支援を行うサービス。 2. ITシステムの運用等に関連する各種の情報･利便･機能等を提供するサービス。	セキュリティ総合監視･運用支援サービス	ネットワークシステムのセキュリティ状態を総合的に監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
		ファイアウォール監視･運用支援サービス	ファイアウォール等のモニタリング状況やアラート等を監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
		IDS／IPS監視･運用支援サービス	IDS／IPSシステム等のモニタリング状況やアラート等を監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
		ウイルス監視･ウイルス対策運用支援サービス	コンピュータウイルス等の不正プログラム等に対して監視や対策を行い、またその運用を支援するサービス。関連するログ解析サービスを含む。
		フィルタリングサービス	電子メールの送受信に際して、スパムメール等の有害メール対策や情報漏えい防止のためのフィルタリングもしくは監視を行うサービス。電子メールサーバ機能の提供と一体で提供されるサービスを含む。 インターネット上のWebアクセスに際して、ポリシーやリストに基づき警告、制限、遮断、報告、記録等の管理やフィルタリングを行うサービス。いわゆるレピュティションサービスを含む。
		脆弱性検査サービス	ITシステムの脆弱性やアプリケーションのセキュリティホールに対して、侵入検査等の擬似攻撃手法やコードの解析等によって検査･診断するサービス。
		セキュリティ情報提供サービス	インシデント、脆弱性、パッチその他のITセキュリティに関する情報を提供するサービス。 Web、メールニュース、レポート、出版等、媒体種類を問わない。
		電子認証サービス	電子証明書の発行･認証、無改竄保証、否認防止、タイムスタンプ証明等の電子的証明やそれに関連するサービス。
		インシデント対応関連サービス	情報セキュリティ･インシデントに際しての緊急対応や復旧に関する専門的スキルを提供するサービス、ならびにいわゆるデジタルフォレンジックに係る専門的スキルを提供するサービス。 ただし上記の各監視･運用支援サービスと一体のものとして提供される場合はその分類に集計する。
		その他の運用･管理サービス	その他の、情報セキュリティの運用･管理に関するサービス。 ITセキュリティ製品の保守･サポート等のサービスを、メーカの製品付帯サービスの再販以外に、監視･運用支援サービス提供事業者、SI事業者等の第三者が独自の付加価値として提供する場合はこの区分で集計する。
情報セキュリティ教育			
	情報セキュリティに関連する知識やスキルの習得、情報セキュリティポリシーやルールの組織内への周知徹底、および情報セキュリティ関連の資格取得のための教育、研修に関するサービス。 セキュリティコンサルテーションやセキュアシステム構築サービスの一環として社員や運用担当者等に実施する教育はそれらのサービスの一部ととらえ、「セキュリティ教育サービス」には	情報セキュリティ教育の提供およびe-ラーニングサービス	情報セキュリティ教育の提供･実施サービス。 講師が実施する集合教育･実地教育･演習等のサービス提供の形態、ならびにセキュリティ教育の内容または教材（いわゆるコンテンツ）の販売もしくはライセンス提供を行う形態の双方を含む。 情報セキュリティ教育のためのe-ラーニングのコンテンツの開発･提供およびe-ラーニングの実施サービスを含む。 セキュリティ資格関連のサービスは「セキュリティ資格認定及び教育サービス」に分類する。
		情報セキュリティ関連資格認定及び教育サービス	情報セキュリティ関連の資格の認定（継続･維持を含む）を行い、または資格認定のための教育研修の実施や受験準備のための講習等を行うサービス。
		その他の情報セキュリティ教育サービス	その他の情報セキュリティ教育に関するサービス。情報セキュリティ教育を直接の目的としたコンサルテーションやシステム構築サービスを含む。 情報セキュリティ製品の使用等に関して製品ベンダが行う教

	集計しない。		育のうち、製品取扱知識だけでなくネットワークセキュリティー般についての知識・技術習得を主たる目的とする教育（資格認定を伴うものを含む）サービスを含む。 システムのセキュリティを作り込む技術やセキュアプログラミング、安全なWebサイトの作り方など、セキュリティ技術の教育を主たる目的とする教育を含む。
情報セキュリティ保険			
	情報セキュリティならびにITセキュリティに関する損害を補償する保険。	情報セキュリティ保険	情報漏えい等の情報セキュリティインシデントならびにネットワークを中心としたITシステムのセキュリティインシデントに起因する損害を補償することを主たる機能とした保険。

第１部　情報セキュリティツール市場の定義に関する説明

「ツール」については、ハードウェア製品とソフトウェア製品の両方を含むものとし、製品・商品化されて販売されているものを対象とした。製品カテゴリとしては「統合型アプライアンス」、「ネットワーク脅威対策製品」、「コンテンツセキュリティ対策製品」、「アイデンティティ・アクセス管理製品」、「システムセキュリティ管理製品」、「暗号製品」の 6 区分（大分類）とした。

以下に各市場区分に関する概要解説を記述する。

1.　統合型アプライアンス

「統合型アプライアンス」は、ハードウェアとソフトウェアを一体化して一つの製品として販売する製品形態である「アプライアンス」製品の中で、二つ以上のカテゴリにまたがる機能を複数統合して一つのアプライアンス上に実現する製品と定義した。

ハードウェアの高機能･低価格化と入手の容易さが進むに連れて、ユーザの利便性や保守の簡便性から、アプライアンスへ向かう動きが全般的に強まっている。導入に際して、ハード、OS、ソフトを各々購入して組み合わせる手間や、仕様の整合性を確保するための煩雑さから解放される。アップデートに際してもハードとの整合性はベンダの責任でカバーされる。トラブル対策に際しては、原因の所在をユーザ側で切り分ける必要がない。このようにアプライアンスはユーザにとっての利便性が高く、販売店にとってもユーザ対応が単純化するメリットがあることから、様々なセキュリティ機能がアプライアンスによって提供されるようになっている。

このうち単一機能のアプライアンスは各々の機能別カテゴリに分類し、複数のカテゴリの機能を併せ持つタイプのものを「統合型アプライアンス」として独立カテゴリとした。市場分類定義表では、「『ネットワーク脅威対策製品』と『コンテンツセキュリティ対策製品』に分類される機能のいずれかまたは両方を備え、二つ以上の大分類カテゴリにまたがる複数の機能を 1 台（またはセット）で提供するアプライアンス製品」と定義している。各大分類区分を一言で表わすと次のようになる。

①ネットワーク脅威対策製品

ファイアウォール、IDS／IPS、VPN、フィルタリングといった、主にネットワークの境界付近に配置し通信のハンドリング、モニタリング、ロギング等を行う製品。

②コンテンツセキュリティ対策製品

アンチウイルス、アンチスパム、URL フィルタリングといった、ファイルや電子メールや Web アクセスに対する不正・迷惑・妨害行為を阻止・防止・予防する製品。

本調査の市場分類の原則では、機能に着目して、その装置等が提供する機能の種類ごとに市場区分を定義している。しかし、統合型アプライアンスは、複数の機能を有することがその定義のベースになっており、他のカテゴリのどこにも分類できないために、独立のカテゴリとして調査集計する。

従来からファイアウォールと VPN ゲートウェイを一体で実現する製品は多く見られたが、これに留まらず不正侵入監視やウイルス監視機能を併設し、1 台でほとんどの外部脅威防御機能を実現する製品が 2003 年頃に登場し、2006 年頃から普及期を迎えた。複数機能の統合と共に、コンパクトなハードと一体化して提供するという特徴も指摘できる。またこれらの製品を、UTM（Unified Threat Management =統合脅威管理=）と総称する呼び方も一般的になっている。これは米国のメーカや調査会社が、製品が登場した初期に使った呼び方が一般

に使われるようになった結果と考えられる。Unified Threat Management の訳語としては「統合脅威管理」が一般的だが、Management という言葉から連想する「管理」よりは対策機能が主体であることに留意し、本調査の市場区分定義では「複合脅威対策」という訳語を当てている。

UTM 以外では、帯域管理にプロキシ、パケットフィルタリング、URL フィルタリング、コンテンツフィルタリング等を組み合わせるようなものも登場している。また、内部ネットワークのスキャンと同時にウイルスやスパムのチェックを行うようなタイプの製品も見られる。認証機能や検疫システム機能といった、これまではソフトウェア製品で実現されていた機能がアプライアンス化される例も見られるようになった。

このように様々なバリエーションを持った複合機能のアプライアンスが登場しているが、ファイアウォールの発展型である UTM が主流であるところから、特に中分類では区分せず、「二つ以上の大分類カテゴリにまたがる複数の機能を 1 台で提供するアプライアンス製品」を「統合型アプライアンス」として、単一セグメントのカテゴリとして定義した。

2. ネットワーク脅威対策製品

「ネットワーク脅威対策製品」の機能は、内部ネットワークと外部ネットワーク（通常インターネット）の境界（Perimeter）やその近傍に配置されて、主として通信のハンドリングまたはモニタリングを行うことである。主たる製品として外部からの不正な侵入・アクセスを防ぐファイアウォール、VPN（Virtual Private Network 仮想私設通信網）、IDS／IPS（Intrusion Detection System 侵入検知システム、Intrusion Prevention System 侵入防御システム）の 3 種類の製品分類を含む。

ネットワーク脅威対策製品の分野では、当初はソフトウェアタイプが主流であったが、現在ではアプライアンス型製品が一般的になっている。本調査では、従来、中分類レベルにおいてソフトウェア製品とアプライアンス製品を分けて定義し集計していたが、2009 年度調査からその区分を廃止し統合している。また、個人向けパッケージ製品であるパーソナルファイアウォールも、そのほとんどがウイルス対策ソフトウェアと一体化して単体製品としては存続しなくなったので統合し、再編整理した。詳しくは 2009 年度の調査報告書を参照されたい。

その結果、2009 年度からは「ネットワーク脅威対策製品」は以下の 5 つの中分類市場に分けて市場規模推計を行っている。

①ファイアウォールアプライアンス／ソフトウェア

ファイアウォールは、ネットワーク上の通信パケットに対して、あらかじめ設定されたその組織の通信に関するルールに従って、通信の許可、遮断、制御を行うことで外部からの攻撃に対する防御や不正な通信の制限・遮断を行う製品である。アプライアンス型製品とソフトウェア製品がある。ファイアウォールが使われ出した初期のころはほとんどがソフトウェアタイプであったが、その後専用ハードウェアによってパフォーマンスとメンテナンス性を向上させたアプライアンスが主流となった。クラウドの浸透に伴い、仮想マシン上に実装するソフトウェアタイプが再び増加しつつある。ファイウォールの多くは VPN 通信を通過させる必要があるため、VPN ゲートウェイの機能を併設している。

ネットワーク上に配置するファイアウォールとは別に、サーバや端末 PC に実装する、パーソナルファイアウォールまたはデスクトップファイアウォールと呼ばれるソフトウ

ェア製品もある。過去には先進的な個人や一部企業で用いられていたが、ウイルス対策ソフトウェアがデスクトップファイアウォール機能を併設することが一般的になってからは、単体製品としてのデスクトップファイアウォールは限定的存在となっている。

②VPN アプライアンス／ソフトウェア

ネットワーク通信を暗号化して、オープンなネットワークでも専用線と同様な通信の安全を確保する機能（VPN= Virtual Private Network=機能）を提供する製品で、アプライアンス型のものとソフトウェアタイプの製品がある。ただし、ファイアウォールに VPN 機能が付帯する場合はファイアウォールに分類する。VPN に際しては、通常、外部から VPN 通信のためにアクセスしてきた相手が､通信を許可されている相手かの確認をする認証手続きを伴うが、その認証のための通信のハンドリングも、VPN 製品が行うことが一般的である。

アクセスを受ける LAN 側ゲートウェイはファイアウォールに併設される機能を用い、リモートアクセスする端末 PC にはソフトウェアタイプのクライアントを実装する形が一般的である。クライアントは、IC カードや USB メモリに実装して、VPN 通信を実現するタイプもある。その場合、同時に端末をシンクライアントとして使用する構成を実現する製品も登場している。ただし、シンクライアントは本調査の対象外としているので、シンクライアントに付属の VPN は集計対象外となる。

③IDS／IPS アプライアンス／ソフトウェア

通常ファイアウォールの後方（内側）に置かれ、ファイアウォールに許可された、あるいはフィルタリングされなかった通信に対して、その内容や状態を一定の方法・技術に基づき検査し、侵入もしくは攻撃と判断される通信に対して報告・警告・ログ記録等を行うのが IDS（侵入検知システム）であり、IPS（侵入防止システム）は更に遮断や阻止まで行う。ファイアウォールのポリシーでは許可される種類のパケットやポートを利用して悪意ある通信内容を仕込み、攻撃する手段に対する防御手法である。

アプライアンス型製品とソフトウェア型製品がある。ファイアウォールと同様に、初期のころはほとんどがソフトウェアタイプであったが、その後専用ハードウェアによってパフォーマンスとメンテナンス性を向上させたアプライアンスが主流となった。

また IDS／IPS には上記のネットワーク型のほかにホスト型と呼ばれる製品がある。これは、監視対象となるサーバ等の OS 上に常駐して、そのマシンが授受する通信パケットやシステムの動作を監視し、異常な動きを検知して報告・警告・ログ記録、遮断等を行うものであり、その性質上、ソフトウェアタイプの製品である。ホスト IDS／IPS を略称して HIDS／HIPS とも通称される。

④アプリケーションファイアウォール

アプリケーションファイアウォールとは、ネットワークトラフィック一般を対象とするファイアウォールとは異なり、特定の装置・用途・目的に限定して通信の監視や制御を行うファイアウォールである。主なものとして、ウェブアプリケーションファイアウォール[1]がある。Web サーバの前に配置して、ウェブアプリケーションに固有の攻撃からアプリケーションを保護する目的で使われる。データベースへの攻撃やその不正利用を防ぐ目的で使われるファイアウォール型の装置もある。本調査では、これらを総称してアプリケーションファイアウォールとしている。アプリケーションファイアウォールの利用は広がりつつある。

[1] WAF （Web Application Firewall）と略称する場合もある。

アプリケーションファイアウォールは、前項の IDS／IPS の一種とも言える。パケットの中身に対して特定の定義に基づき制御するという点で、機能的にはほぼ IDS／IPS の定義が該当するが、そのうち、ウェブアプリケーション等特定の防御対象に特化したものを、アプリケーションファイアウォールと称するようになっており、ひとつの市場セグメントを形成するまでに至っていると考えられる。

⑤その他のネットワーク脅威対策製品

外部ネットワーク（インターネット等）から内部ネットワークに対して行われる、不正侵入、盗聴、不正プログラムの挿入等の攻撃に対して、検知、防御、抑止、警告等の防衛の機能を提供する製品で上記のどのセグメントにも属さないものを集計している。

3. コンテンツセキュリティ対策製品

「コンテンツセキュリティ対策製品」とは、コンテンツ、すなわち、ファイルやデータの内容について、その危険性の有無や、内部規定・セキュリティポリシーに対する違反等の有無をチェックすることを主目的とした製品群である。本調査では、ネットワーク通信に関して、その通信目的をコントロールすることを主目的とするものを、前述の「ネットワーク脅威対策」と定義し、通信の中身について不都合の有無をチェックすることを主目的とするものを「コンテンツセキュリティ対策」と定義した。主として外部からの脅威への対策に用いられるが、情報漏えい対策にも用いられており、大きくは以下の３つの製品群に分かれる。

1．コンピュータウイルス、スパイウェア、ボット等の不正プログラム、マルウェア等を、ファイル等の電子データや電子メール送受信・Web 閲覧等のコンピュータ通信の中から検出し、排除･無害化･警告等の対策を講じる機能を持つ製品群。

2．システム･業務･サービスの目的や適正な運営にとって有害な電子メール送受信や Web 閲覧等の通信を検査し、フィルタリング・警告･排除・ログ記録その他の対応を行う機能を持つ製品群。

3．電子メール、電子ファイル等の内容（コンテンツ）について、内部規定（セキュリティポリシー）等あらかじめ定められた条件に基づいて送配信を制限し、ログ記録その他の対応を行う機能を持つ製品群。

つまり、ファイルやメールや通信の内容に対するチェックやコントロールを提供する製品のグループである。データそのものの保護については、暗号を利用することが一般的であるため「暗号製品」に分類している。

マルウェアは、出現当初はフロッピーディスク等の記憶媒体を介する感染が主流であり、電子メールの普及に伴って添付ファイルを装ったり、ファイルに付随するマクロを偽装するウイルスが猛威を振るった。電子メール添付ファイルに対する対策が進んだ結果、現在では、Web サイトにマルウェアを仕込み、そのサイトに誘導することで、ファイルのダウンロードや閲覧行為に便乗して感染するタイプが主流となっている。そして、USB メモリという記憶媒体を介するパターンも、OS の自動実行機能を悪用する形で復活している。

2009 年度の中分類市場区分からの変化として、「フィッシング対策ソフトウェア／システム」を「その他のコンテンツセキュリティ対策製品」に統合し、一方「その他のコンテンツセキュリティ対策製品」に含めていた「DLP 製品･システム（情報漏えい対策製品･システム）」を独立した市場区分とした。「フィッシング対策ソフトウェア／システム」は、フィッシングが新たな脅威として注目された 2004 年以降に専用対策製品やベンダが登場したが、その後脅威の複雑化と、それに対応する対策の複層化に伴って専用製品やシステムによる対応が限ら

れるようになっている。標的型脅威対策も含めて総合的対策が一般化していることから、独立の市場セグメントと位置づけることは不要になったと判断した。一方、DLP 製品はやはり 2000 年代前半に登場していたが、近年参入ベンダも増加し製品バリエーションも広がって、導入事例も増えてきたことから、独立のセグメントとして統計対象とすることとした。

当市場調査においては製品区分（市場区分）を次の 7 種類にセグメント分けする。

① 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

ウイルス、ワーム、スパイウェア、トロイの木馬、ボット等の不正プログラムを検知し、更に防御や排除する製品。クライアントパソコンやサーバに、ソフトウェアとしてインストールして使う形が一般的で、企業等向けにライセンス契約方式で提供される。また、内部ネットワークの入り口にゲートウェイ型で設置して通過するトラフィックをチェックする使い方もある。この場合はアプライアンス型製品が利用されるケースが多い。ウイルス対策製品の特徴として、不正プログラムを検知するための一種のリストである定義ファイルを常時更新する必要があり、ソフトウェア代金の他に、この定義ファイルの更新権は年間契約で支払う形が一般的だが、その更新料もこの市場を構成する金額としてカウントする。

一方、マルウェアの種類、特に亜種の発生量が桁違いに増加しており、定義ファイルの巨大化と更新頻度を上げる必要が生じている。それは端末とネットワークの負荷を著しくしく高めるため現実的でなくなってきている。そのため、基本的なフィルタリングは定義ファイルで行い、不振なファイルは挙動を見て判断する手法や、ウイルス対策ソフトベンダのサーバに都度問合わせて判断する方法を組合わせることが一般的になっている。後者の方法はサーバや判断機能がクラウドにあるのでクラウドサービス型アンチウイルスといった呼称も登場している。

この製品には、付加機能として、ファイアウォール、IDS、スパム対策、URL フィルタリング等の機能を併設するものが一般的であるが、最近は脅威の複雑化と深刻化から、それぞれ個別の対策製品を個別に導入する方向にあると見られる。

② ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）

ウイルスを始めとするマルウェア対策ソフトで、個人ユーザが自宅のパソコンで使うための製品である。製品形態としては、ソフトウェアパッケージとして家電店等の店頭やオンラインショップで販売される形が主流である。またネットワーク越しに製品をダウンロードしてインストールする、オンラインダウンロード販売も増加している。①同様、プログラムや定義ファイル更新の年次参照権の販売代金も含む。また、個人向けウイルス対策製品のほとんどが、デスクトップファイアウォール、HIPS（ホスト IPS)、スパム対策、URL フィルタリング等の機能を併せ持っている。

近年、スマートフォンやタブレット型 PC と呼ばれるスマートデバイスが急速に普及している。モバイルアクセスにおいては、PC に取って代わる勢いである。クラウドコンピューティングの広がりにより、端末でのアプリケーション稼動が不要になっていることも普及に拍車をかけている。同時に、スマートデバイス上で動作するマルウェアも急速に出回っており、その対策製品も各ベンダから登場している。スマートデバイス向けマルウェア対策製品もこのセグメントで集計している。

③ スパムメール対策ソフトウェア／アプライアンス

宣伝、勧誘等の目的で無差別・大量に送りつけられる、不要もしくは有害な内容を含むメール、いわゆるスパムメールに対する対策製品。フィルタリング、マーキング（タグ付け）、警告、隔離、排除（廃棄）等の対応をする。クライアント用、サーバ用、ゲートウェイ型のタイプがあり、製品形態もソフトウェアとアプライアンスがある。

なお、スパム対策は、メールフィルタリングと同様、ISP のサービスの一環として、あるいは SaaS 型の専門サービスとして提供される形も浸透している。これらはサービス市場で集計している。

④ URL フィルタリングソフトウェア／アプライアンス

アクセスしようとするインターネット上のウェブサイトが有害、危険、不適格等と判断される場合に、そのアクセスに対して停止、警告、ログ保存等を行うソフトウェアもしくはアプライアンス製品。判断は、自社の基準により禁止するサイトを指定するブラックリスト、キーワードによるフィルタリング、ツールベンダが提供するリスト等に基づく。近年はレピュティション（評判）ベースと称し、対象となるウェブサイトに関する情報やインシデントを世界中から収集蓄積して解析し、その評価に基づく判断を行う形が増えている。この場合はベンダのサーバに可否を問合せて判断する形が一般的となっており、クラウド型サービスという呼称も登場している。

企業向けと個人向けの両方がある。特に家庭において子供を有害サイトから守るための使われ方が関心を集めている。特にスマートフォン向けには、携帯販売会社に、年少者の利用に対して有害サイト遮断機能の紹介推奨が義務付けられており、利用は拡大していると見られる。

⑤ メールフィルタリングソフトウェア／アプライアンス

送受信される電子メールに対して、電子メールアドレスや内容、添付ファイル等を検査し、情報漏えい等の情報セキュリティ事故を防止するための製品。所定の条件（有害、不適格、情報漏えい、レピュティションサービス[2]によるリスト等）に合致（もしくは違反）する内容を含むものに対して処理（停止、隔離、警告、管理者への通報もしくは回送、ログ保存等）を行う。単に全メールを無条件にアーカイブするだけのものを除く。ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。

製品形態としてはソフトウェア製品とアプライアンス製品がある。また、スパム対策と同様に、ISP または専門事業者によるフィルタリングサービスも提供されている。このサービスについては情報セキュリティサービス市場で集計対象としている。

⑥ DLP 製品・システム（情報漏えい対策製品･システム）

情報漏えい対策手段として、データそのものの存在や移動を検知して警報、通知、阻止等を行う機能を有するソフトウェア、アプライアンスまたはシステムである。メールのコンテンツやファイルに対してフィルタリングやマーキングを行い、情報そのものの動きを直接追いかけて境界外への流出をコントロールする。DLP のうち D は data の頭文字であり、L は loss、leak または leakage を、P は prevention または protection を示す。D は一意だが、L と P はベンダによって用語の選択が違う。比較的多い用法は Data Leak Prevention または Data Loss Protection であろうか。

[2] Reputation Service ウェブサイトやメールの発信源等の URL について、過去の不正行為の事例や安全に通信された実績等の情報に基づき、ウイルス対策ツールベンダや専門事業者が安全度の評価をした結果のデータベースを Reputation（英語の元の意味は評判、評価）と呼び、アクセス制御やフィルタリングに際しての判断根拠として利用する技術およびそのサービス。

メールフィルタリングや端末における書き込み動作等だけでは防ぎきれない情報の外部流出を、ファイルやその中のデータの特性を把握することで抑止・防止しようとする考え方の製品である。

⑦ その他のコンテンツセキュリティ対策製品

メール等の電子データに関して、主として情報セキュリティの目的でフィルタリングその他の機能を提供する製品で、上記のいずれにも属さない、あるいは特定の中分類に仕分けできないもの。

いわゆる Digital Rights Management （DRM）[3]と呼ばれる製品群があり、このセグメントに含めた。DRM とは、コンテンツの利用の態様に対してコントロールをかけるもので、利用する人の属性、方法、時間、場所、回数等によってコントロールすることで、権利者の意図する範囲と方法での利用を担保する目的で使われる。これは内容の保護を同時に実現する場合も多いがそれが必然ではなく、暗号を伴わないケースもあることから、「その他のコンテンツセキュリティ対策製品」に含めて集計している。

4. アイデンティティ･アクセス管理製品

「アイデンティティ･アクセス管理製品」は、情報システムやネットワークに対してユーザがアクセスする際に、本人であることを認証し、そのユーザに与えられた権限の範囲内で情報資源にアクセスさせることを保証する一連の製品である。各種認証デバイス（装置・機器）並びにその認証システム、アイデンティティ管理システム、ログオン管理･アクセス許可システム、ディレクトリ管理システム、シングルサインオンシステム、PKI 関連システム等がこのカテゴリに含まれる。

このカテゴリの呼称については、従来「アクセス管理製品」としてきたが、2008 年度調査から「アイデンティティ管理システム」のセグメントを独立させ、カテゴリの名称を「アイデンティティ・アクセス管理製品」とした。本人認証だけでなく、認証されたユーザに対するリソースへのアクセス範囲と権限を、人事情報と連動させて管理することの重要性に対する認識が高まっている。その領域を管理するツールとして、アイデンティティ管理システムが注目され出したことに対応する変更である。

このカテゴリは、以下の 6 セグメントに区分定義している。

① 個人認証用デバイスおよびその認証システム

ワンタイムパスワード、IC カード、USB キー、携帯電話（個体識別番号含む）等を用いて本人確認する機能を提供するデバイス、およびそのシステム（生体認証を除く）等である。認証は、システムにアクセスするユーザを特定するための情報（ID）と、それ対応する認証情報（credential）を予め登録されている情報と照合することで行う。認証情報は、一般的に本人しか知らないものや本人しか持っていないものを用いる。両者の組合せによる、二要素認証を行うことも普及してきている。

IC カード、特に社員証を兼ねるものが最も普及していると推測される。より安全性が高いとされるワンタイムパスワード製品には、時刻同期方式、カウンタ同期方式、チャレンジレスポンス方式等のハードウェアタイプと、PC や携帯電話にソフトウェアをインストールするものや、Web ブラウザを利用し、位置情報やイメージ情報からワンタイムパスワードを生成するソフトウェアタイプの製品等がある。

[3] 一部のベンダは IRM （Information Rights Management）とも呼ぶ。

②個人認証用生体認証デバイスおよびその認証システム

認証情報として、本人の身体的特徴の情報を用いる考え方・技術があり、独立のセグメントとして集計している。身体的特徴として実用化されているものとしては、指紋、手や指の静脈パターン、虹彩や網膜のパターン、顔そのもの、更には行為や行動の癖や特徴、声といったものがある。これら情報の識別技術は、入退室管理に利用され物理セキュリティ対策製品としても利用が進んでいるが、本調査では、PC やサーバ、ネットワーク等のシステムへのアクセスにおけるユーザ認証デバイスおよびシステムを対象としている。

生体認証に使われる情報は ID・パスワードと違って、個人を特定する上で代替のきかない性格を持つため、セキュリティレベルを高くできる反面、一旦そのデジタルデータが漏えいした場合の影響は大きく、そのデータについてはシステム的に厳格な管理が求められる。また指紋の利用等については、運用面においてもユーザの心理面への配慮が求められる。

③アイデンティティ管理製品

システム並びにデータへのアクセス権について、システムの利用者に関してはその職務や権限に基づく定義のデータベースを、システム並びにアプリケーションに関してはそのアクセス許可ポリシーを管理する機能を提供する製品群で、利用者の異動に伴う変更管理や、システム間のアクセス権の情報連携や統合管理を実現し、情報資産の利用権の即時的一元的管理を可能にする。プロビジョニング製品（ユーザ別のシステム利用権限の定義）やフェデレーション製品（異システム・異組織間の ID 連携、プロビジョニング連携のための製品）を含む。

アプリケーションやサーバが増加する一方、社員の流動化や従業員構成の複雑化も進んでいる。従業員の所属と職務権限に対応したアクセス権を統合的に管理するために、物理的な一元化が困難な環境において、論理的に一元化できる仕組みを構築するためのツールとして、アイデンティティ管理ツールの重要性が増している。

④ログオン管理／アクセス許可製品

「ログオン管理／アクセス許可製品」は、保護対象となる情報処理資源に対してのアクセスをコントロール（管理・制御）する。自らに実装されたテーブルやアイデンティティ管理製品からの情報に基づき、どのようなユーザにどのようなアクション（システムやネットワークへのログオン、アプリケーションの実行、データベースの参照、ファイル操作等）を許可するのかを一元的に管理し、アクセスを制御する。保護対象となるのは、PC やサーバのみでなく、ファイルやディレクトリをはじめ、ポートやログインアプリケーション、マシン名、ネットワーク ID、メモリ等、多岐に渡る。また、大規模なトータルソリューションとなる場合も多い。

一方、昨今発生している主なセキュリティ事故や情報漏えいの多くが、特権アカウントと呼ばれる管理者権限（Windows の Administrator 権限、UNIX/Linux の root 権限、データベースの sysdba 等）の悪用によることから、より実効的なセキュリティ向上のために、システム本番環境や重要サーバに対する特権 ID のアクセス制御・管理に特化した製品も出ている。

ユーザの利便性と一元的なポリシー管理を両立させるシングルサインオン（1 回の認証で複数のシステムへのアクセスを可能にする管理システム）製品もこのカテゴリに含まれる。

⑤PKI システムおよびそのコンポーネント

公開鍵暗号の仕組みを応用して電子証明書や電子署名を作成し、第三者による保証と組み合わせて、ユーザの認証、文書等の真正性の証明、改ざん防止（無改ざんの確認）、否認防止等に利用する仕組みがある。Public Key Infrastructure、公開鍵基盤と呼ばれる。このセグメントには、そのような公開鍵基盤のための電子証明書の発行、管理、証明サービスを提供するシステムおよびその構成要素等の製品を含む。但し、構築サービス（SI）や電子認証サービスは情報セキュリティサービス市場に計上するものとし、このセグメントには含まない。

⑥その他のアクセス管理製品

このセグメントには、単独で製品化されるディレクトリサービス製品、ネットワーク統合管理製品におけるユーザ管理モジュール等が含まれる。また、本人認証の手法として、「リスクベース認証」という方法が登場しており、このセグメントに含めている。これはアクセスしてきたユーザの PC の識別記号、地理的場所、アクセス履歴や行動パターン、予め登録された質問と答えのセット（本人しか知り得ない情報による）等を取り合わせて、高い精度で本人確認を実現するという手法で、インターネットバンキング等、IT に不慣れな人でも特定できる技術である。何をどう取り合わせれば実用目的に耐える精度が得られるかのアルゴリズムが開発されて実用化が始まっている。

5. システムセキュリティ管理製品

「システムセキュリティ管理製品」とは、主にシステム全体のセキュリティ情報を監視して統合管理と統計処理を行い、その結果を統合表示したり、異常に対してアラート（警報・警告）を出したりする製品である。システム全体に関して、ある判断基準に従いチェックを行い、ポリシーへの準拠性を確認する製品（いわゆるコンプライアンス管理製品）や脆弱性検査製品（いわゆるスキャニングツール）等が含まれる。

監視機能としては管理対象となるネットワークやコンピュータから出力されるログ等を取得してリモートから統合的に状態を把握し、その結果を統合表示したり、異常に対してアラートを出したりする機能を持つ。管理機能としては管理対象となるネットワークやコンピュータの構成情報、設定ポリシー等を統合的に管理し、ポリシーへの準拠性を確認する機能がある。制御機能としては自動、手動にてネットワークの接続を拒否したり、アカウントをロックしたり、ファイル等の電子データの処理を停止したりする機能がある。

この市場区分には以下の 4 種類の中分類（セグメント）を設定している。

①セキュリティ情報管理システム／製品

「セキュリティ情報管理システム／製品」区分には、セキュリティ監視・制御装置、ネットワークシステムやサーバ機器やデータベース等様々な対象に対してセキュリティ状態を総合的に管理する機能を持つ製品およびシステムを集計する。ネットワークシステムやサーバから出力されるログを統合的に収集し管理する製品である SIM(Security Information Management:セキュリティ情報管理)製品、収集したログに重要度等の意味付けを行いセキュリティイベントとして管理しリアルタイムに相関関係を分析する SEM(Security Event Management:セキュリティイベント管理) 製品、あるいはそれらを統合した SIEM と呼ばれる製品等がある。ネットワークの統合管理プラットフォームの一部を構成する製品もある。

② 脆弱性検査製品

「脆弱性検査製品」は、ネットワーク機器やサーバ等に対して、ネットワーク越しにスキャニングや擬似攻撃を行うことにより、設定の不備やプログラムの不具合等の危険事項を調べ脆弱性が存在していないかを検査する製品群である。フリーウェアも含めて多くのソフトウェア製品が提供され、脆弱性スキャナーとも呼ばれている。一部にはアプライアンス製品もある。

また、同様の機能を持つモジュールを検査対象内にインストールして内部から脆弱性検査をするホストベーススキャナもある。

③ ポリシー設定管理・動作監視制御

「ポリシー管理・設定管理･動作監視制御製品」は、インベントリ管理（OS のバージョンやパッチ適用状況の情報、インストールされているアプリケーションの情報、CPU 使用率等ハードウェア情報等の収集・管理機能)、ポリシー管理（管理対象マシンにあらかじめ定められたポリシーに準拠した設定がされているかをモニタし報告する機能)、動作監視（管理対象マシンで行われたファイルの編集、更新、複写、印刷、外部記憶装置の使用等といった、情報漏えいにつながる動作や行為に対しての監視、抑制、警告、報告機能）等の管理機能を提供する製品群である。

クライアント PC 等の識別情報やインベントリ情報等に基づきネットワーク接続を管理･制御する、いわゆる「ネットワーク検疫システム」における機器認証サーバや認証エージェントをこのセグメントに含める。この機能は、ネットワークアクセス制御であり、「ネットワーク脅威対策製品」に分類する考え方もあるが、むしろ端末と位置付けられる各ユーザの PC のポリシー順守状況の管理が主眼で、それとネットワーク接続許可を連動させている構造なので、前者に注目して「ポリシー管理･設定管理･動作監視制御製品」に分類することとした。原則として単体製品またはネットワーク制御装置等のオプションとして取引対象となる製品形態のもののみを対象とし、その機能がルータ等の一部にデフォルトとして組み込まれている場合は含まない。

④ その他のシステムセキュリティ管理製品

「その他のシステムセキュリティ管理製品」は、システムセキュリティ管理製品の中で、上記セグメントのいずれにも分類されない製品の区分である。デジタルフォレンジックといわれる、セキュリティ事象や不正アクセスを追跡するために、電磁的記録の証拠保全および調査・分析を行う機能を有する製品や、セキュリティ・内部統制管理（IT ガバナンス）等を目的としてログの収集、減量・圧縮、保管･アーカイブ、解析等を行う製品等がこれに該当する。（但し、ログ収集・解析機能を有する製品の内、リアルタイム監視を主目的とする製品は「セキュリティ情報管理システム／製品」に分類しており、「その他のシステムセキュリティ管理製品」では主に傾向解析等スタティックな目的のものを対象としている。）

情報漏えい事故等インシデント[4]発生時の追跡や内部統制管理のための取引記録の追跡可能性確保のために、適切なログ取得や管理、改ざん防止対策が必要である。大量のログを統合し統計分析を行える機能や証拠保全のためのログの改ざん防止機能を提供している製品を用いることにより、監査証跡の信頼性を確保し、管理者の負担を

[4] 「インシデント」は出来事、事件のような意味。情報セキュリティに関してはウイルス感染、不正侵入、情報漏えい、秘密情報の紛失等の事件･事故･事案を総称して情報セキュリティインシデント又は単にインシデントと言う。

軽減することが可能となる。

6. 暗号製品

「暗号製品」とはデータ、ファイル、電子メール、ハードディスク等を暗号化する各種製品および半製品を指す。

暗号技術そのものは、PKI や VPN の基幹技術を構成する他、各種情報セキュリティ製品の内部処理等に広範に使われている。PKI、VPN はその使用目的から各々アイデンティティ・アクセス管理製品、ネットワーク脅威対策製品に分類しており、ここではデータの保護等を目的とする製品を中心に定義している。具体的にはメールやデータを暗号化するソフトウェア、および暗号化のためのライブラリやモジュール等が含まれる。

「暗号製品」は昨年度まで、「データ暗号化製品」、「暗号化ミドルウェア」、「その他暗号製品」の３つの中分類市場を区分定義していたが、今年度調査からセグメント分けはせず「暗号製品」全体を一つの区分として調査した。「暗号製品」とはハードディスク、文書ファイル、メール、外部記憶デバイス等を暗号化することを主たる機能とする製品群や、データベースの暗号化や組み込み用暗号モジュール等が該当する。

ハードディスク暗号化製品とはハードディスク全体を暗号化するため利用者が意識せず利用することができる。そのため導入後の運用負荷が低いので導入しやすい製品といえる。また、ＰＣを持ち出した際に、紛失・盗難等が発生した時の情報漏えい対策として有効なことから、大企業や大企業と取引を行う中小企業にも導入が進んでいる。

文書ファイルの暗号化製品とはパーティション、フォルダ、ファイル単位でユーザが任意に暗号化処理をすることにより、アクセスするユーザの権限に応じて参照・更新・削除等をコントロールすることができる製品である。これにより情報の重み付けや権限外のユーザによる覗き見や漏えい防止を実現する。実際に運用する際にはユーザ側に判断や操作を求める製品が多いため、暗号化ルールや情報の重み付けルール等導入の際にはある程度の運用設計を実施する必要がある。

メールの暗号化製品とはメール本文および添付ファイルの暗号化を実現するものと添付ファイルのみ暗号化するものとがある。メールは情報漏えいを発生させやすいポイントと考えられているため、企業のリスクと運用コストを比較し導入を検討する企業は多い。しかし既存のメールシステムの変更や運用の変更に対するコストは規模が大きいほど膨らむ傾向にあり、ニーズの強さほど市場は伸びていない。この仕組みをアプライアンス型で提供している製品や SaaS 型サービスとして提供しているものもある。後者は運用管理サービス市場に分類している。

記憶デバイスの暗号化製品は記憶デバイスを接続する端末側に組み込むものと USB メモリ等デバイス自体に暗号化の仕組みが組み込まれるものとがある。ハードディスク暗号化製品と同様、利用者への負担も軽く、外部に持ち出した際の紛失・盗難対策として有効な製品であるため、企業のニーズが高い。そのためリリースされている製品の種類も多い。

暗号化ミドルウェア、つまりは暗号化のためのライブラリやモジュールも市場の一部を形成している。通常の情報システムやネットワークを構成する機器に組み込む用途の他 OEM 提供されるビジネスモデルも多い。デジタル複合機[5]、ネットゲームや家電製品のネットワーク

[5] 複写機にファクス、スキャナー、プリンタの機能を付加したマルチ用途のものをデジタル複合機（MFP, Multi-Functional Printer）と呼びならわしている。複写機の基本構造はスキャナーで読み取ったイメージをプリンタで紙に出力するものであるが、それをデジタル処理にすることでコンピュータによるデータ処理と同等のプロセスとなり、ネットワーク機能とファクス機能、更にデータ蓄積機能を持つことで多彩な複写、印刷機能を提

接続に際して、一定の情報を内部に暗号化し、格納する必要があるので、組込み開発の現場でも暗号製品のニーズはあり、一定の需要が存在するものと考えられる。

上記以外に、暗号ライセンス、鍵管理システム周辺製品、電子割符や電子透かし等の暗号製品もある。

なお、情報漏えい対策、内部統制対策として用いられる事が多い DRM（Digital Rights Management）と呼ばれる製品群は、暗号技術を応用している場合がほとんどだが、本調査では「セキュアコンテンツ管理製品」と位置付けており、「暗号製品」には含めていない。

供するようになっている。蓄積機能とネットワーク機能、ネットワーク越しに離れた場所で紙に出力されたものの物理的管理の問題等から、新たな情報セキュリティのフロンティアとしても浮上している。

第 2 部　情報セキュリティサービス市場の定義に関する説明

「情報セキュリティサービス」市場には、情報セキュリティ対策を構築・実践し、情報セキュリティソリューションを実装し機能させ活用するために提供される、各種サービスが含まれる。

本調査では、国内で事業を行うサービスプロバイダ（サービス提供事業者）から、情報セキュリティサービスとして提供されているものを対象とした。カテゴリとしては、「情報セキュリティコンサルテーション」、「セキュアシステム構築サービス」、「セキュリティ運用・管理サービス」、「情報セキュリティ教育」、「情報セキュリティ保険」の 5 区分とした。

1. 情報セキュリティコンサルテーション

「情報セキュリティコンサルテーション」とは、情報セキュリティに関するポリシー、システム、運用体制の構築を支援するサービスである。情報セキュリティ対策は、情報資産のリスク管理を目的とするところから、単に IT システムへの脅威対策といった技術的領域にとどまらず、経営資源と位置付けられる情報資産に関する経営のリスクコントロールという視点に基づく必要がある。従い、経営管理と技術方針を包含する、専門性が高く、多様性を伴う分野である。

企業のコンプライアンス（法令・ルール遵守）重視の立場から、情報セキュリティマネジメントシステム認証制度等客観的な規格要件の認証取得を目指す企業が多い。それに対応して、その認証取得を支援するサービスも様々な事業者から提供されている。一方、こうした規格適合性を審査し、認証するサービスもまた、公的機関に限らず、民間事業者から提供されている。

「情報セキュリティコンサルテーション」市場は、大別すると、マネジメント系、診断･監査系、認証取得系に分けることができる。これを、以下の 5 つのセグメントに区分して調査集計している。

① 情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション

今年度調査から「情報セキュリティポリシー構築支援」と「情報セキュリティ管理全般のコンサルテーション」を統合して 1 セグメントとした。マネジメント系セグメントは当市場 1 つである。主に情報セキュリティポリシーの策定やコンプライアンス対応施策、情報保護対策全般がサービスの中心となる。

情報セキュリティポリシーの策定では、会社の基本方針や情報セキュリティ対策の基準、実際の運用ルールや処理手順等を体系的に整備することを支援する。更に、情報セキュリティ管理全般のコンサルテーションでは、推進組織や責任体制、IT も含めた情報セキュリティの基本枠組であるアーキテクチャの設計開発まで全般にわたって支援を提供する。

② 情報セキュリティ診断・監査サービス

診断・監査系サービスは当市場区分で集計している。

経済産業省告示により、情報セキュリティ監査制度が制定され、情報セキュリティ監査の枠組みを提供している。実際の運用と推進は NPO 日本セキュリティ監査協会に委ねられ、同協会が認定する公認情報セキュリティ監査人が中心となって監査を提供している。ISMS 認証取得企業の内部監査を外部のコンサルタントが実施あるいは支援を行うサービスもある。監査という枠組みによらず、自社の基準やサービス事業者の推奨基準に基づく情報セキュリティ診断を受けるケースも多い。また外部の第三者に

よる委託先に対する監査もある。更に、情報セキュリティ対策がどこまでできているかを絶対基準に基づき評価して評点をつける、情報セキュリティ格付けも行われている。

このような、情報セキュリティ管理に関する監査や診断を専門サービスとして提供するのが「情報セキュリティ診断・監査サービス」である。なお、同じ「診断」「監査」という語を用いても、もっぱらシステムの技術的脆弱性の診断・評価を行うサービスもある。これはマネジメントシステムに対する評価とは異質であり、プロフェッショナルサービスと位置付けて、本調査では、「セキュリティ運用・管理サービス」の１セグメントとして区別して集計している。

③ 情報セキュリティ関連規格認証取得等支援サービス

認証取得系については、企業が認証を取得するための支援を提供するサービスと、その審査・認証を実施し認証証を交付するサービスの両面がある。

当セグメントが対象とするのは、前者の規格適合性の認定、認証の取得を支援するサービスである。規格・基準の適合性認定には、一定のモデルもしくはパターンがあり、それに沿ったルールや書式や体制を構築し、審査に耐える運用、特に PDCA サイクルをうまく回すことが必要となる。その専門的ノウハウを提供し、企業の認証取得を支援するのがこのサービスである。マネジメントシステムの構築と PDCA サイクルの実施を支援し、審査のサポートや取得後の運用の支援等も行う。

④ 情報セキュリティ関連認証・審査・監査機関（サービス）

このセグメントは、認証を提供する側のサービスである。情報セキュリティ関係の認証の主なものとしては、ISMS（Information Security Management System、情報セキュリティマネジメントシステム）認証と、プライバシーマークの認定がある。各々、認定機関に認定された認証機関が審査し、認証する。ISMS は JISQ27001（国際規格である ISO/IEC27001 と同等）に基づいて適合性を認証する制度で、認証機関が審査する。認証機関を認定するのは、日本においては公益財団法人日本適合性認定協会（JAB）と一般財団法人日本情報経済社会推進協会（JIPDEC）がある。

プライバシーマークは、JIPDEC が直接審査し付与するケースの他に、業界団体等が JIPDEC の指定審査機関として審査し、その結果に基づいて JIPDEC が付与するケースがある。基準は JISQ15001 である。

関連する認証として、IT サービスマネジメントシステム（ITSMS）や事業継続マネジメントシステム（BCMS）の構築、認証も行われるようになっている。

⑤ その他の情報セキュリティコンサルテーション

この他、これらが複合した需要や個別ニーズに沿ったコンサルティング、企業独自のメニューや体系をパッケージ化したサービス等がある。また、内部統制管理、特に IT ガバナンスの主たる要素である情報セキュリティガバナンスに関する構築や診断、事業継続管理や IT サービスマネジメントに関連して情報セキュリティに関するコンサルテーションを提供するサービスがある。それらを「その他の情報セキュリティコンサルテーション」というセグメントで集計している。

2. セキュアシステム構築サービス

「セキュアシステム構築サービス」は、実際にセキュアなシステムを構築する段階で必要となるサービスであり、システム構築におけるセキュリティ面の設計や運用について、現状分析、

ポリシー、製品選定、情報更新等、専門的な見方から、ソリューションを提供する。IT セキュリティシステムの設計、仕様策定といった上流工程から、セキュリティソフトウェアの開発、カスタマイズ（個別対応改造）、セキュリティソフトウェアおよびハードウェアの選定、導入、設定等の現場に近いサービスまでが含まれる。主にネットワークインテグレータ、システムインテグレータによりサービス提供がおこなわれる。

このカテゴリは以下の４種類の中分類（セグメント）にて市場区分を行なった。

① IT セキュリティシステムの設計・仕様策定

「IT セキュリティシステムの設計・仕様策定」は、IT システムを構築するにあたりセキュリティに関しての設計、仕様の定義を実施するサービスである。システム設計時にセキュリティ対策についてセキュリティ専門家による支援を提供する。また、既存のシステムに対してセキュリティ面を付加するまたは向上させるための対策を設計するニーズもある。

② IT セキュリティシステムの導入・導入支援

「IT セキュリティシステムの導入・導入支援」は、システムのセキュリティに関する部分の構築に際して、セキュリティ製品等を導入し、システムを構築、あるいは、その支援をするサービスであり、セキュリティに関するインテグレーション・エンジニアリングサービスと言える。この市場もまた、情報セキュリティ対策の実施やセキュリティレベル向上という目的のためには、専門家によるセキュリティアーキテクチャの適用が必要だという認識が浸透することで、大きな需要を形成している。

③ セキュリティ製品の選定・選定支援

「セキュリティ製品の選定・選定支援」は、顧客のポリシーや要求に基づいて、それに適したセキュリティ対策製品の選定またはそのための情報提供等の支援を行うサービスである。セキュリティ対策は、システムの利用目的と設置･利用環境をにらんで必要な機能を適正に配置する必要がある。そのため、セキュリティ製品の導入に際して、セキュリティの専門家による製品選定や製品の比較評価のサービスを活用するニーズが存在する。

④ その他のセキュリティシステム構築サービス

上記 3 セグメントに当てはまらない IT セキュリティシステムの構築サービスを「その他のセキュアシステム構築サービス」とした。例えば SI 事業者が行うセキュリティ対策製品の設定や保守、診断等のサービスが含まれる。

3. セキュリティ運用・管理サービス

「セキュリティ運用・管理サービス」市場は、大別してマネージドセキュリティサービス、プロフェッショナルセキュリティサービス、電子認証サービスに分けられる。

マネージドセキュリティサービスは、IT セキュリティシステムまたは IT システム上のセキュリティ対策機器等の運用や管理の支援を行い、システム、サーバ、ネットワーク状態等の監視を行う、いわゆる運用支援サービスである。外部事業者が事業所内に常駐し、あるいは事業所外から遠隔操作によって代行する形態が中心で、その監視対象別に「セキュリティ総合監視･運用支援サービス」「ファイアウォール監視･運用支援サービス」「IDS／IPS 監視･運用支援サービス」「ウイルス監視･ウイルス対策運用支援サービス」の 4 セグメントを定義した。またスパム対策や有害ウェブフィルタリングをアウトソースサービスとして提供するビジネスモデルの拡大に対応して「フィルタリングサービス」を今年度から独立セグメントとした。この一

部は従来「ウイルス監視･フィルタリング・運用支援サービス」としてウイルス監視と同一セグメントに分類していた。

プロフェッショナルサービスには、ネットワークからの攻撃に対する弱点を検査する「脆弱性検査サービス」、セキュリティに関する脆弱性やインシデント、ネットワーク攻撃の傾向や趨勢等の予防的情報を提供し外部脅威に対するセキュリティ対策をサポートする「セキュリティ情報提供サービス」、何らかの事故等が発生した場合の対応を引き受けたり支援したりする専門家のサービスである「インシデント対応関連サービス」がある。

電子認証サービスは、個人の認証を第三者が発行する電子証明書によって行う PKI（公開鍵基盤）や、Web サーバの実在性・信頼性を保証する SSL[6]サーバ証明に用いられる電子証明書の発行を行うサービスである。文書の完全性・真正性の証明や否認防止、時刻の証明であるタイムスタンプ等にも用途が広がっている。

これに電子認証サービスと「その他」を加え、10 という大きな数のセグメント（中分類市場区分）を設定した。各セグメントの概要は以下の通りである。

① セキュリティ総合監視・運用支援サービス

企業はネットワークに対してファイアウォールや IDS／IPS を設置し、ネットワークシステム上で起こる異常を検知し対策に努めているが、サーバのログ等も含めて総合的に監視し判断をする必要がある。それにはネットワークの知識を十分に持ち、また攻撃や異常状態に関する経験や知識を必要とするが、一般企業ではそれだけの人材を確保したり配置したりすることは容易ではない。

そこで、セキュリティ専門企業がそのノウハウを生かして監視を行い、異常発生時には対応の支援も提供するサービスが提供されている。SIM／SEM や統合型ネットワークセンサを活用して総合的な監視を提供するものがセキュリティ総合監視・運用支援サービスである。

② ファイアウォール監視・運用支援サービス

①と同じサービスをファイアウォール専用に提供するサービスである。

③ IDS／IPS 監視・運用支援サービス

①と同じサービスを IDS／IPS 専用に提供するサービスである。

④ ウイルス監視･ウイルス対策運用支援サービス

①と同じサービスをウイルス・マルウェア対策製品専用に提供するサービスである。

⑤ フィルタリングサービス

電子メールを通じての情報漏えいの防止には、アウトバウンドの全てのメールをスクリーニングする必要があるが、企業が自ら実施するのはシステム面と管理負荷の面から現実的でない。インバウンドのメール対策としてはスパムメールの排除がセキュリティ面と事業効率面で必須だが、これも多大な負荷を強いる事態となっている。それらを専門家が専門システムを用いてサービスとして提供するモデルが普及している。本調査では、そのようなサービスをフィルタリングサービスとして調査集計対象としている。なお、このセグメントは 2008 年から独立させた。

⑥ 脆弱性検査サービス

ネットワークシステムやウェブサービスは、構築した側では発見しきれない、隠れた脆弱性を内蔵している可能性が強い。それに対して、ハッカーの視点とスキルを持って擬似攻撃を仕掛けることで脆弱性を発見し、対策を指導することで被害を未然に

[6] SSL: Secure Socket Layer　暗号通信の一方式。

防ぐ支援を提供するのが「脆弱性検査サービス」である。ペネトレーションテスト（侵入検査。更に縮めてペンテストとも言う。）とも呼ばれ、特定のスキルを持った専門家を擁する企業が専門サービスとして提供している。

また、ネットワーク越しに外から実施する、いわゆるブラックボックス検査のほかに、システム構成図やアプリケーションのソースコードを解析して隠れた弱点を発掘する、ホワイトボックス検査も提供されている。

プロフェッショナルサービスとしての脆弱性検査サービスはあくまで技術的な検査を集計対象としており、マネジメントシステムに対する監査・診断といった評価は、本調査では「情報セキュリティコンサルテーション」サービスの一部として取り扱っている。

⑦ セキュリティ情報提供サービス

「セキュリティ情報提供サービス」は世界中のネットワークの状態を監視、あるいは専門サイトを巡回して情報を収集し、それらを解析してネットワークからの攻撃の予報や警報、傾向分析と対策等を地域別、業種別、時期や時間帯別等きめ細かく提供するサービスで、IT が事業上極めて重要な企業等の組織に提供されている。

また OS やアプリケーションの脆弱性情報や他の場所で発生したインシデントの情報も、解説や推奨対策を付加して提供している。

⑧ 電子認証サービス

「電子証明サービス」は公開鍵暗号技術を応用して公開鍵と秘密鍵のペアで本人性、真正性、無改ざん等を証明するための電子証明書を発行するサービスである。電子証明書の仕組みは PKI（Public Key Infrastructure、公開鍵基盤）とも呼ばれる。

⑨ インシデント対応関連サービス

「インシデント対応関連サービス」はハッキングや情報漏えいといった情報セキュリティインシデントに際して、その対応や原因分析、事後対策等を専門家のノウハウを駆使して支援する専門サービスである。コンプライアンス対応や内部犯行事例の増加に伴い、電子的証拠の収集・解析・保全も必要度が高まっており、そのようなデジタルフォレンジック対応のサービスも提供されるようになってきた。

⑩ その他の運用･管理サービス

これらのセグメントのいずれにも属さない IT セキュリティに関する専門家による運用・管理サービスを「その他の運用･管理サービス」として集計する。SI 事業者が提供する製品の保守やサポート等が含まれる。また、PC 等の安全な廃棄や、逆に破損・焼損・浸水等したハードディスク等からのデータの復元サービス等も需要が増している。これらの特殊なサービスもこのセグメントで集計している。

4. 情報セキュリティ教育

情報セキュリティ対策部門、情報システム管理部門、システム開発部門、システム構築・運用部門等の部門は、情報セキュリティの専門知識・スキル・資格の習得が必要な部署である。ISMS 認証取得企業やプライバシーマーク認定取得企業は、全社員に対する情報セキュリティ教育の定期的・継続教育を実施しなければならない。金融商品取引法に基づく内部統制報告・監査制度（日本版 SOX 法）の施行に伴うコンプライアンス関連教育は欠かせないものとなっている。これらの教育は、それぞれ専門知識を必要とするために全てを自社内で対応することは不可能で、必然的に外部の専門サービスを利用することになる。特に、情報セキュリティ技

術は進化が激しく教育のために専門家の知識は不可欠となる。本調査では、これら情報セキュリティ専門家や専業ベンダより提供される教育サービス、e - ラーニングサービス、資格認定教育サービス等が集計の対象となる。

「情報セキュリティ教育」市場は、従来「情報セキュリティ教育の提供サービス」、「情報セキュリティの e - ラーニングサービス」、「情報セキュリティ関連資格認定および教育サービス」、「その他の情報セキュリティ教育サービス」の 4 つの中分類市場（セグメント）に分類していたが、今年度から「情報セキュリティ教育の提供サービス」に「情報セキュリティの e - ラーニングサービス」を統合し、3 区分とした。e-ラーニングが教育手段として一般に浸透したことと、外部サービスとしての提供は限定的範囲にとどまることによる。

各セグメントの概要は以下の通りである。

① 情報セキュリティ教育の提供サービス

「情報セキュリティ教育の提供サービス」は、教育コンテンツのみを提供して教育実施は客先社内で実施するケースと、教育実施まで一貫して提供するサービスの両方を含めている。情報セキュリティのコンテンツの開発・作成・提供のみを行うサービスは、教育の中身そのものをテキストやデジタルファイル等のコンテンツとして提供するサービスである。教育コンテンツ開発・作成から教育の実施まで一貫して行うサービスは、専業ベンダの教育施設に出向いて教育を受ける集合研修型の「通学授業」と講師が客先に出向いて教育を実施する集合研修型の「出張授業」がある。また、専業ベンダが開発したコンテンツに基づく情報セキュリティ技術分野別のカリキュラムと個別教育コースを標準的な公開講座として受講者を募集する「レディメイド」教育と、客先個々の教育ニーズに対してコンサルティング（教育目的、目標とそれを達成するための課題、問題点の抽出と解決策等の提供）を行い、受講者のレベルを考慮したコンテンツや育成プログラムの開発と実施を行う「テーラーメイド」教育のビジネスモデルがある。

外部の専業ベンダがコンテンツを Web ベースで提供する e - ラーニングサービスもある。インターネットに接続できる環境さえあれば、いつでもどこでも一定期間内の都合のよい時間に受講者が自分のスケジュールに合わせて受講が可能で、受講可能時間に合わせ途中で受講を止め、後日続きを再開することもできる。管理者も受講者全員の進捗を Web ブラウザ等を通してリアルタイムに把握（可視化）でき管理できる。また、集合研修より総合的に費用を抑えられるメリットも大きい。e-ラーニングのコンテンツ開発・提供サービス面では、紙芝居的なテキストベースの電子版型から、講師の講義の動画提供型や講師による講義のリアルタイム動画配信によるサービスもある。更に Web の特性を活かして遠隔の受講者との質疑応答ができる対話（インタラクティブ）型サービスも生まれ、e - ラーニングサービスの利用を促進する要因となっている。

② 情報セキュリティ関連資格認定および教育サービス

「情報セキュリティ関連資格認定および教育サービス」は、情報セキュリティに関連する各種資格認定と認定資格取得のための専門的な教育を提供するサービスである。特定の製品ベンダに偏らない世界標準の情報セキュリティ認定資格取得技術者の世界的な需要の高まりを受け、国内でもその必要性の認知が進んでいる。

③ その他の情報セキュリティ教育サービス

その他、以上に当てはまらない、教育コンテンツの開発・作成を伴わず、単に講師

を派遣するサービス等を「その他の情報セキュリティサービス」とした。また、特定の情報セキュリティ対策製品に関する解説や訓練を第三者が有料で実施する教育サービスもこのセグメントに含む。

5. 情報セキュリティ保険

ウイルスや不正アクセスによる被害並びに情報漏えい等による損害を賠償するタイプの損害保険商品が複数の保険事業者から提供されるようになった。需要側としても、リスク対策の一手段としてリスクの移転を採用する機運が高まっており、IT 保険、ネットワーク保険と共に、あるいはその一部として、情報セキュリティ保険が市場の認知を得ていると見られる。本調査では、これを情報セキュリティサービスの 1 カテゴリとして調査集計対象とした。

なお、本調査では、原則として、情報セキュリティを付保対象とする情報セキュリティ保険（コンピュータ保険等の一部である場合にはその部分のみ）を集計対象としている。情報セキュリティも、システムインテグレーションにおけるセキュリティの組み込みが一般的に所与の要件となり、その部分を特段計算したり分別集計したりする要素が減っているのと同様に、IT リスク全体の一部として IT システム保険商品に組み込まれたりオプション扱いになったりして、情報セキュリティに特化する形での市場形成という認知の度合いは弱まってきている。

以上