使えるねっと株式会社
株式会社アクシス
株式会社ネットブレインズ

ISPP（Information Security Platform for Partner）設立のお知らせ

参加企業の協業パートナを対象にした、企業向け包括的な情報セキュリティ対策「プラットフォーム」を効果的に中小・中堅企業向けに提供するコンソーシアムを立ち上げ

■ISSP とは？

ISPP は、協業パートナが情報セキュリティ対策をサイバーセキュリティキルチェーン（※1）にの考え方に基づき「点ではなく面」として、中小中堅企業（エンドユーザ）に効果的かつ効率的に提供するために設立された、個別プラットフォーム（セキュリティサービス基盤 ※2）を提供するプラットフォーマー（セキュリティサービス基盤提供事業者）の相互協業を目的とした共同事業体です。

※1：サイバーセキュリティキルチェーン

昨今の段階を踏んで行われるサイバー攻撃を構造化したもの。アメリカのロッキード・マーチン社によって、2009 年に提唱される。元々軍事用語であったものを標的型攻撃に適用し、攻撃者の動きを 7 つのフェーズに分類。これを活用し、攻撃者の行動パターンを知ることで、攻撃抑止に繋げることが期待される。

※2：プラットフォーム（セキュリティサービス基盤）

製品のみではなく、最適な導入、運用含め継続的にエンドユーザに活用いただくための一体的な「サービス基盤」を指す。ISPP 参画企業はこの「サービス基盤」を提供する事業者。

■中小・中堅企業における情報セキュリティ対策の現状

現在企業活動に欠かせないインフラである、「インターネット基盤」を悪用し、企業の情報資産の奪取、不正利用を行う各種犯罪行為が増加、手法の多様化、高度化等により、これらの脅威が大企業のみならず、中小企業自身の経営継続性を直接的に脅かす要因になっております。

この現状を鑑み、政策実施機関として情報セキュリティ、ソフトウェア高信頼化、IT 人材育成等の施策の展開を実施している IPA（独立行政法人 情報処理推進機構）からもさまざまな警鐘が発表されております。

その一例として

・ 「中小企業の情報セキュリティガイドライン」より

- 「経営課題」としての情報セキュリティ対策を推奨。そのための「経営者」自身の積極的関与、リーダーシップが必要になることを理解。

・ 「情報セキュリティ 10 台脅威　2020」より

- 「サプライチェーンの弱点を悪用した攻撃」は一企業組織の対策のみならず、企業間のつながり（IT サプライチェーン）の中でそれぞれが対策していないと、いずれかの組織（つながりのある中小企業など）が攻撃の足掛かりとなる。企業規模に関わらず、つながり全体の対策の必要性を警鐘
- 「ビジネスメール詐欺による金銭被害」による、巧妙になりすました性悪が判別しにくい内容のメールを送付することで、金銭送付、情報奪取などの入り口とする手口。ばらまき型手法により、企業規模に関係なく被害が増加。「わかりにくさ」の増加、専門家の知見が対策には必要

また、顧客情報、特許情報、会計情報など、企業の「情報資産」の価値が増大する中で、予期せぬ IT 基盤の障害や業務停止に伴う、「情報資産の毀損」による直接的な経営リスクも顕在化しております。

このような状況の中で、今後中小含めたすべての企業に「常識」としてセキュリティ対策の実施が、市場からの要請になることは必然です。情報セキュリティ対策は、比較的従来より実施されていた脅威を水際でより高度の技術を利用して実施する検知する「予防措置」のみならず、未知の脅威の増加により必要となる「感染後措置」も意識した、網羅的な対策を実施することが要求されております。

■中小・中堅企業における情報セキュリティ対策の課題

「感染前～感染後」のそれぞれの攻撃段階に応じた網羅的対策が求められており、そのリスク対応に関する「企業の自己責任」を前提とした法律等社会的状況の変化にもかかわらず、特に中小、中堅企業においてはこれらの対策が遅れているのが現状です。

その理由として以下の課題にあるものと、ISPP 参画企業は考えております。

1. 「製品」ありきの提供形態

・ セキュリティ対策は、目的に適した製品導入はもちろんですが、その活用及び運用がさらに重要です。しかしながら、セキュリティキルチェーン（対策全体）を理解無視した、かつ製品を導入することが目的化した対策により脅威の進化に追随できず、製品機能の陳腐化、その活用及び利用の最大化がないがしろになる企業の事例が数多く見受けられます。

2. 「企業へ提供を行う側」の課題

・ セキュリティ対策が、「製品＋活用＋運用」かる一連の網羅的な対策に重点が置かれる中、それを提供する側に必要とされる網羅的なスキルや体制を自前で有することが難しく、その結果として、企業（エンドユーザ）に提供されるセキュリティ対策が製品よりかつ偏りのあるものになりがちな状況となっております。

3. 「製品事業者」の課題

・ 製品（プロダクト）ベンダーは、本来セキュリティキルチェーンを構成する「パーツ」であるにもかかわらず、企業（エンドユーザ）との直接的な関りが薄いことにより、そのつながりを把握できない傾向があります。

・ 「パーツ（部品)」のメーカという位置づけ上、そのパーツを企業（エンドユーザ）それぞれに適した形で活用及び運用を促すための機能を持ち合わせていません。

■ISPP のミッション

1. プラットフォーマー（セキュリティサービス基盤提供事業者）による相互協業

・ ISPP 参画企業は、「製品＋活用＋運用」を一体的に提供する事業者となります。

・ 従来の「製品のみ」の提供ではない、企業（エンドユーザ）にとって最適かつ効果の高いセキュリティ対策を継続的に提供します。

2. プラットフォームの提供先を ISPP 参画企業の「パートナ（企業に提供する側)」に特化

・ ISPP 参画企業のセキュリティサービス基盤は、それぞれの ISPP 参画企業が有するパートナを経由して企業（エンドユーザ）に提供する形式となります。

・ この提供形式により、現在喫緊でセキュリティ対策が必要な企業（エンドユーザ）に最短で効果的、効率的なセキュリティ対策の提供を実現します。

3. 「商壁」を排除したパートナ施策（提供イメージは、下記図参照ください）

・ ISPP 参画の各企業は、それぞれが現在有するパートナを相互に紹介、それ以降の商流、直接的な支援は、該当するセキュリティサービスを有する ISPP 参画企業とパートナの直接行為となります。

・ ISPP のセキュリティサービス基盤を、ISPP の各参画企業がパートナに対し直接的に支援、提供を実施することで、パートナはこれらのセキュリティサービスを、自社サービスとして容易にかつ効果的に取り込むことができます。それにより、サイバーセキュリティキルチェーンの網羅性をもつ一貫した網羅的セキュリティサービスを、有効的かつ低コストに各パートナの有する企業（エンドユーザ）に実効性の高い網羅的な「セキュリティサービス」を提供することが可能となります。

【参考】サービス提供イメージ