サプライチェーンのサイバーリスクリスクアセスメント

近年、大企業から中小企業までを含む一連の商流（サプライチェーン）上の弱点を狙って攻撃対象への侵入を図るサイバー攻撃が顕在化・高度化しています。

背景：組織の攻撃可能領域の増加

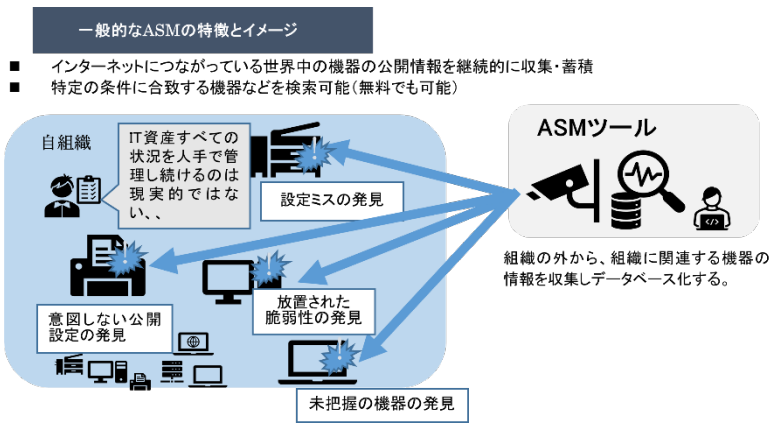
順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位

出典：「情報セキュリティ10大脅威 2023」解説書
https://www.ipa.go.jp/security/10threats/10threats2023.html

IPA（情報処理推進機構）が公開した「情報セキュリティ10大脅威 2023」によれば、サプライチェーンの弱点を悪用した攻撃が昨年３位から２位へ脅威度がアップしております。実際に組織のサプライチェーンに含まれる子会社・取引先等の関連組織がランサムウェア攻撃の被害に遭い、自組織にも被害が出てしまう事例の発生も確認されています。こうした背景には組織のIT環境の近代化によるデジタル資産の増加やクラウド利用の拡大によりサイバー攻撃の起点が増加しているという現状があります。昨今では自組織のサイバーセキュリティ対策だけではなく、関連組織も含めたサプライチェーン全体への対策が重要になってきています。

ガイドライン：経済産業省によるASM導入ガイダンス

経済産業省は攻撃となりうるポイントを把握するためにASM（Attack Surface Management：攻撃可能領域の管理）を活用するよう推奨しております。ASMを利用することでサプライチェーンに存在する脆弱性などの弱点を攻撃者目線で特定し、対策を行うことでサイバー攻撃のリスクを低減する効果が期待されています。



出典：経済産業省
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

株式会社 アイサン情報システム
〒103-0016　東京都中央区日本橋小網町6番1号　山万ビル12階
Tel: 03-5614-5177　| E-mail: cyber@aisan-is.jp

ソリューションのご紹介（SLING）

SLING

SLINGはサプライチェーンの攻撃対象領域を監視します。

◆サプライチェーンやグループ企業全体のサイバー防衛の強度を定量的にスコアリングし，強化のための情報を提供
◆ダークネット脅威インテリジェンスにある攻撃者のTPPと脆弱性を関連付け
◆デジタル資産ごとのリスク評価とプライオリティ付けを実施
◆独自のスコアリングアルゴリズムと検証済みの脅威検出
◆修復に必要な情報も提供

攻撃者目線での調査の重要性

攻撃者から何が見える?

脆弱性と侵入機会はある?

既に狙われているか?

サプライチェーン全体でのサイバーセキュリティ脅威対策をご検討ください
ご相談は cyber@aisan-is.jp まで

株式会社 アイサン情報システム
AISAN
〒103-0016 東京都中央区日本橋小網町6番1号 山万ビル12階
Tel: 03-5614-5177 | E-mail: cyber@aisan-is.jp