２０２４年５月２日

三井住友海上火災保険株式会社
あいおいニッセイ同和損害保険株式会社
ＭＳ＆ＡＤインターリスク総研株式会社

～サプライチェーン全体のサイバー攻撃対策を後押し～

# 「ＭＳ＆ＡＤサイバーリスクファインダー 取引先診断サービス」の提供開始

ＭＳ＆ＡＤインシュアランス グループの三井住友海上火災保険株式会社（代表取締役社長：舩曳 真一郎）、あいおいニッセイ同和損害保険株式会社（代表取締役社長：新納 啓介）、およびＭＳ＆ＡＤインターリスク総研株式会社（代表取締役社長：一本木 真史）は、大企業の関係会社や取引先などに潜むサイバーリスクを一括診断できる「ＭＳ＆ＡＤサイバーリスクファインダー 取引先診断サービス」を開発しました。

３社は、本サービスの提供を通じて、危険性が高まるサプライチェーン攻撃に対する企業の対策強化を図るとともに、リスクソリューションのプラットフォーマーとして提供価値を変革していきます。

## １．背景

企業や組織を狙うサイバー攻撃が社会問題となる中、対策が手薄とされる大企業の関係会社や取引先の中小企業を狙った攻撃による被害が相次いでいます。経済産業省・独立行政法人情報処理推進機構（ＩＰＡ）は、２０２３年３月にサイバーセキュリティ経営ガイドラインを改訂するなど、サプライチェーン全体での対策を求めています。一方で、多くの関係会社や取引先を含むサプライチェーン全体のサイバーリスク管理は、手間がかかる上、リスクを客観的に把握しにくい実態がありました。このような中、３社が中小企業向けに提供するサイバーリスク診断サービス※1の技術を応用することで、関係会社や取引先のサイバーリスクを一括で診断し、サプライチェーン全体の傾向把握や継続的なモニタリング、緊急時の脆弱性を通知する大企業向けのサービスを開発しました。

※１：「ＭＳ＆ＡＤサイバーリスクファインダー」の提供開始（２０２３年９月２８日ニュースリリース）

## ２．サービス概要

（１）特長

・米国立標準技術研究所（ＮＩＳＴ）の民間パートナーとしても知られる米サイバー保険会社Coalition※2と共同開発したアタックサーフェスマネジメント（ＡＳＭ）※3を活用することで、数十～数百社にのぼる大企業の関係会社や取引先を一括で診断し、サイバーリスクを客観的に可視化します。
・月次や四半期ごとの頻度で対象企業を診断し、全体の傾向値や過去の推移を含めた診断結果を提供します。
・対策が難しいとされる「ゼロデイ攻撃※4」につながるシステムの欠陥を検知・都度通知することで、緊急性の高いシステムの欠陥を適時適切に把握できます。

※２：ＳＭＥ向けサイバーセキュリティ・ソリューションを共同開発（２０２３年１月６日ニュースリリース）
※３：「攻撃者視点」で攻撃対象領域（アタックサーフェス）を把握し、セキュリティを強化する技術
※４：ＯＳやアプリケーションの脆弱性に対応するパッチがソフトウェアの開発企業等から提供される前に、その脆弱性を悪用して行われる攻撃の総称

（２）サービス提供開始日等

| | 三井住友海上 | あいおいニッセイ同和損保 |
|---|---|---|
| 提供開始日 | ２０２４年３月１８日より | ２０２４年５月２日（本日）より |
| 対象となるお客さま | 主に大企業（関係会社、海外現地法人、業務委託先、取引先のサイバーセキュリティ対策の強化を目指す企業）　※保険契約の有無にかかわらず利用可能です | |
| 費　　用 | 以下の要素により、個別にお見積りします<br>・診断頻度<br>・診断企業数（診断ドメイン数）<br>・診断方法（詳細診断・簡易診断） | |
| 申込方法 | 以下、オフィシャルＷｅｂサイトよりお問い合わせください<br>【ＭＳ＆ＡＤサイバーリスクファインダー取引先診断サービス】 | |

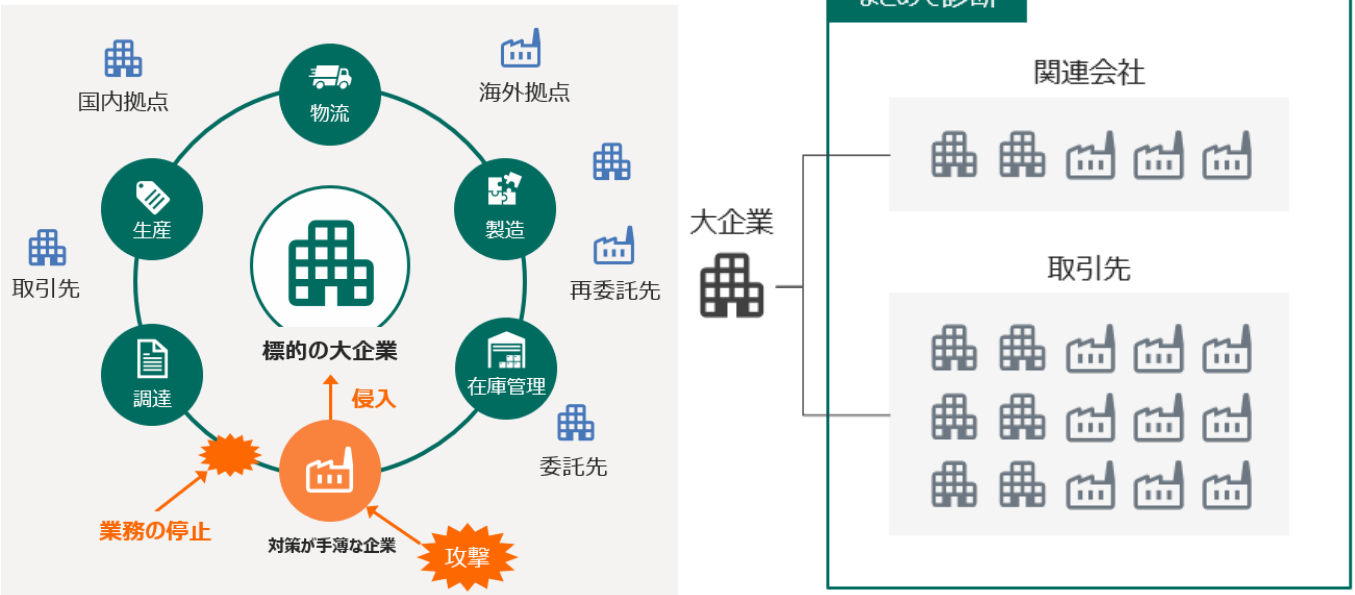
## ３．今後の展開

３社は、サプライチェーン全体のサイバーセキュリティ向上に貢献するとともに、本サービスと中小企業向けサービスを組み合わせることで、企業が優先して対策を取るべきリスクに対して適切なソリューションを提供していきます。

さらに、三井住友海上やあいおいニッセイ同和損保のパートナーである保険代理店のセキュリティ状況の確認にも、本サービスの活用を予定しています。

＜参考＞

・サプライチェーン攻撃と本サービスのイメージ

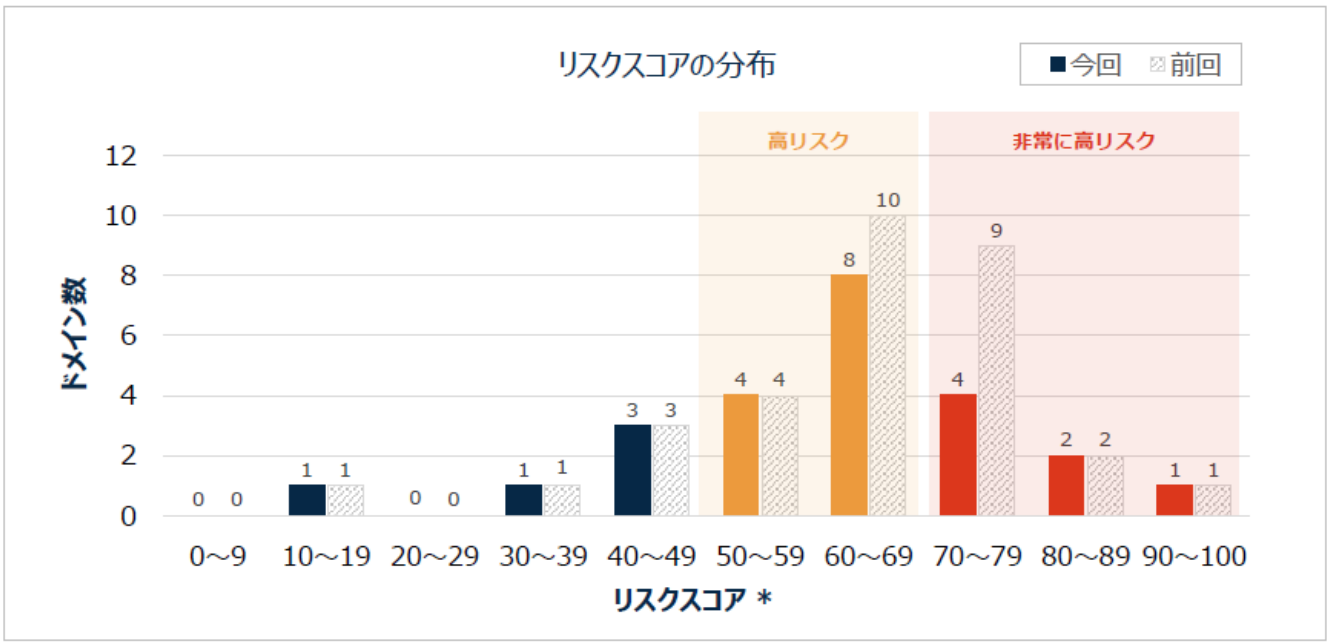



・サイバーリスク診断結果のサマリー

### 診断対象

| | |
|---|---|
| **診断企業数** | **24** 社 |
| **診断ドメイン数** | **24** 個 |
| 簡易診断 | 24 個 |
| 詳細診断 | 0 個 |

### 診断結果




*参考：米国のサイバー保険大手Coalitionは、スコア50以上の企業に対してはサイバー保険の引き受けを見合わせています

*リスクスコア50～69：高リスク。危険度Highが1件以上存在し、未解決の場合攻撃を受ける可能性がある状態です

*リスクスコア70～：非常に高リスク。危険度Criticalが1件以上存在し、未解決の場合攻撃を受ける可能性が高い状態です

・関係会社・取引先ごとの診断結果

## 診断結果の詳細

参考：項目の説明・考えられる原因・対策方法

| No. | 企業名 | ドメイン | 診断プラン | リスクスコア | | セキュリティ上の課題（件） | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | CRITICAL | | HIGH | | MEDIUM | | LOW | |
| | | | | 今回 | 前回比 | 今回 | 前回比 | 今回 | 前回比 | 今回 | 前回比 | 今回 | 前回比 |
| 1 | サンプル株式会社 | sample1.com | 簡易診断 | 9 | △ 2 | 14 | △ 10 | 0 | ▲ 8 | 21 | △ 7 | 34 | ▲ 3 |
| 2 | サンプル2株式会社 | sample2.com | 簡易診断 | 22 | ▲ 9 | 17 | ▲ 10 | 3 | △ 8 | 17 | △ 7 | 23 | △ 10 |
| 3 | サンプル3株式会社 | sample3.com | 簡易診断 | 82 | ▲ 10 | 15 | ▲ 7 | 5 | ▲ 3 | 37 | △ 1 | 28 | △ 8 |

## 課題の詳細と推奨アクション

診断したすべての企業のセキュリティ上の課題一覧です。危険度Critical・Highのみ掲載していますが、
Medium・Lowを含めた一覧もご入用の場合は担当者までご連絡ください。

| No. | 企業名 | ドメイン | 危険度 | 対象のアセット | セキュリティ上の課題 |
|---|---|---|---|---|---|
| 1 | サンプル株式会社 | sample1.com | HIGH | 192.192.192.192, 252.252.252.252 | Plesk Obsidian Panel Exposed |
| 2 | サンプル2株式会社 | sample2.com | CRITICAL | 192.192.192.192 | Exim version prior to 4.92.2 |
| 3 | サンプル3株式会社 | sample3.com | HIGH | 192.192.192.192 | CVE-2023-42115: Exim mail transfer agent (MTA) allows Remote Code Execution |
| 4 | サンプル4株式会社 | sample4.com | CRITICAL | 192.192.192.192 | End-of-life IIS Software |
| 5 | サンプル5株式会社 | sample5.com | CRITICAL | 192.192.192.192 | CVE-2019-10149: Exim mail transfer agent (MTA) allows Remote Code Execution for some non-default server configurations |

以　上