



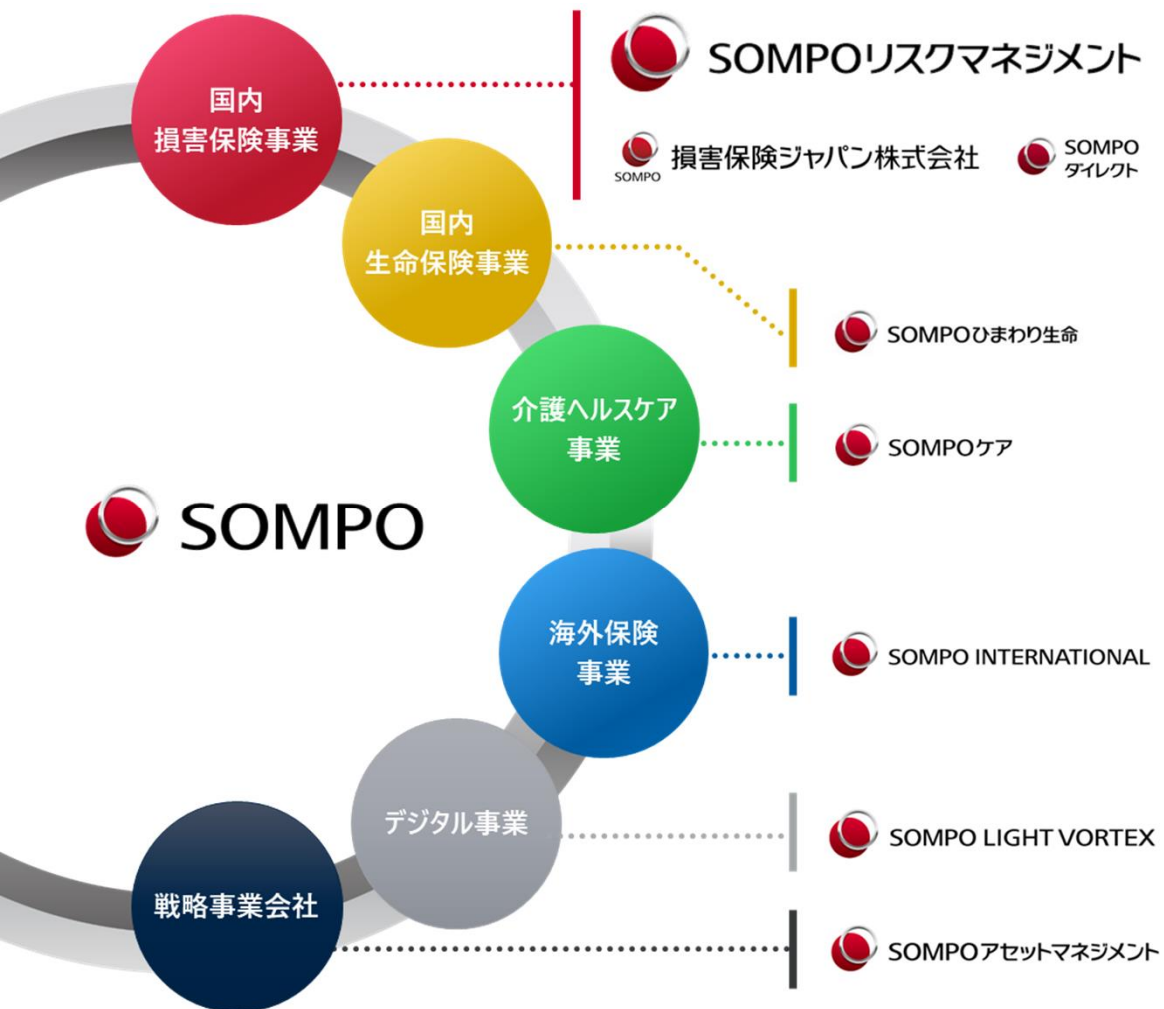
「JNX会員専用サイバー事故相談窓口」の開設について

SOMPOリスクマネジメント株式会社
サイバーセキュリティ・コンサルティング部



会社案内

会社概要



社名	SOMPO リスクマネジメント株式会社 (英文表記：Sompo Risk Management Inc.)
設立年月日	1997年11月19日
本社所在地	〒160-0023 東京都新宿区西新宿1-24-1 エステック情報ビル 27階
事業内容	・デジタル事業 ・リスクマネジメント事業 ・サイバーセキュリティ事業
拠点	東京・名古屋・大阪・福岡
従業員数	519名 (2024.4時点)
資本金	3,000万円
株主	SOMPO ホールディングス株式会社 (100%)

SOMPOサイバーセキュリティ事業のご紹介（サービス全体像）



SOMPO CYBER SECURITY

平時のセキュリティサービス

ー ロスプリベンション: 損害を事前に防止 ー

サイバーリスク
アセスメント

ネットワーク
セキュリティ

体制整備
コンサルティング

エンドポイント
セキュリティ

セキュリティ診断
侵入テスト

教育・メール訓練・
危機演習

脆弱性管理

サプライチェーン
リスク評価

一体での
ご提案

有事のセキュリティサービス

ー ロスコントロール: 損害の波及・拡大を防止・軽減 ー

SOMPOサイバーインシデントサポートデスク
(24時間/365日対応)

インシデント
ハンドリング

緊急時広報対応・
コールセンター

デジタルフォレンジック
・侵害調査

信頼回復・
GDPR対応

データリカバリ

恒久対策

保険×サービスの一体化

シームレス対応

サイバー保険

ー ロスファイナンス: 金銭的な損失に対する資金の手当て ー

賠償責任


「サイバーリスク」に起因して他人に損害を
与えた場合の賠償責任・訴訟費用の補償

事故発生時の各種対応費用

「サイバーリスク」の発生に起因して生じる
「事故の調査」から「解決/再発防止」までの
諸費用の補償

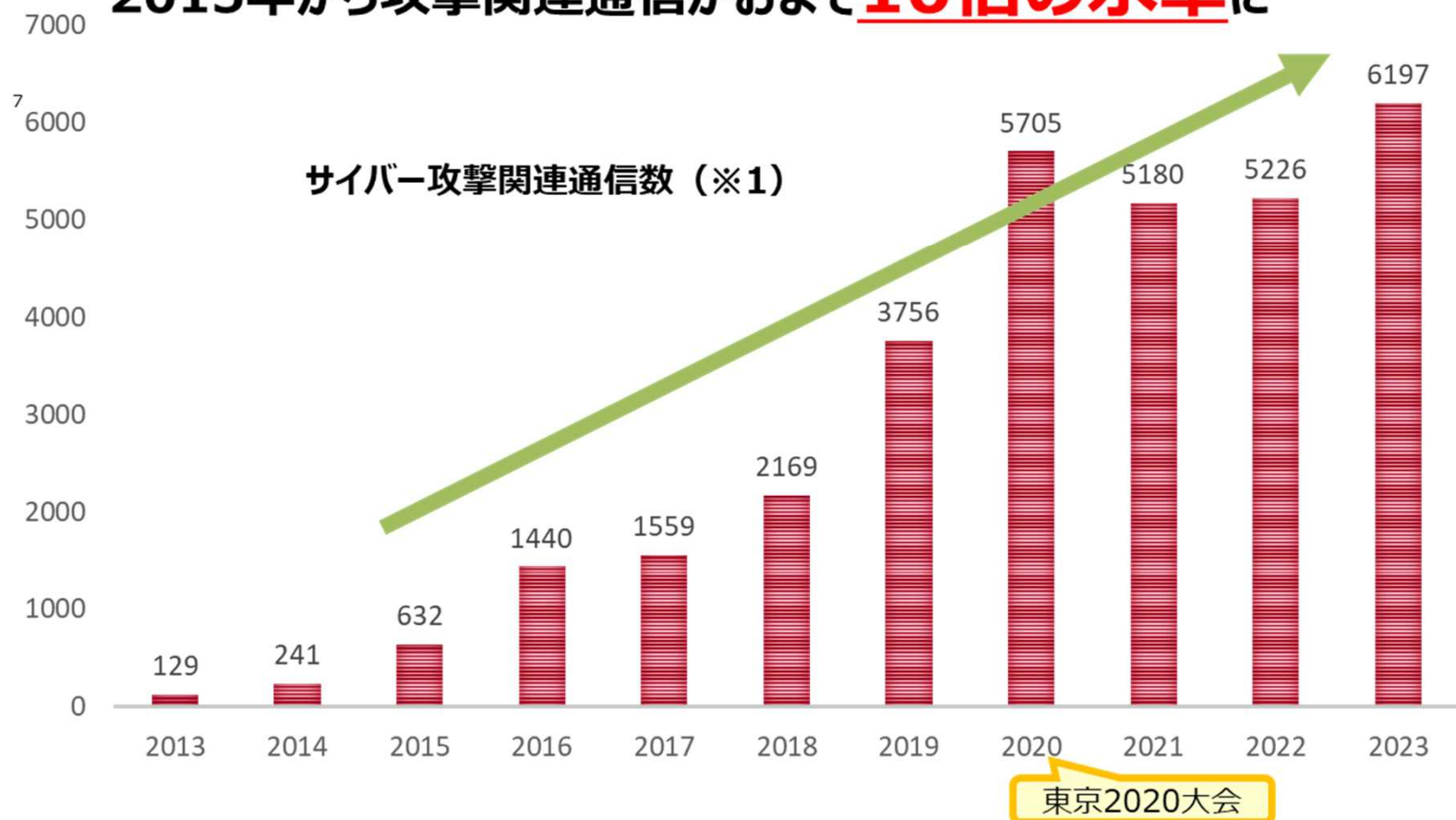
利益・営業継続費用

システムの中断に起因して生じた逸失利益
や営業継続のための費用の補償



国内のサイバー事故発生状況

2015年から攻撃関連通信がおよそ10倍の水準に

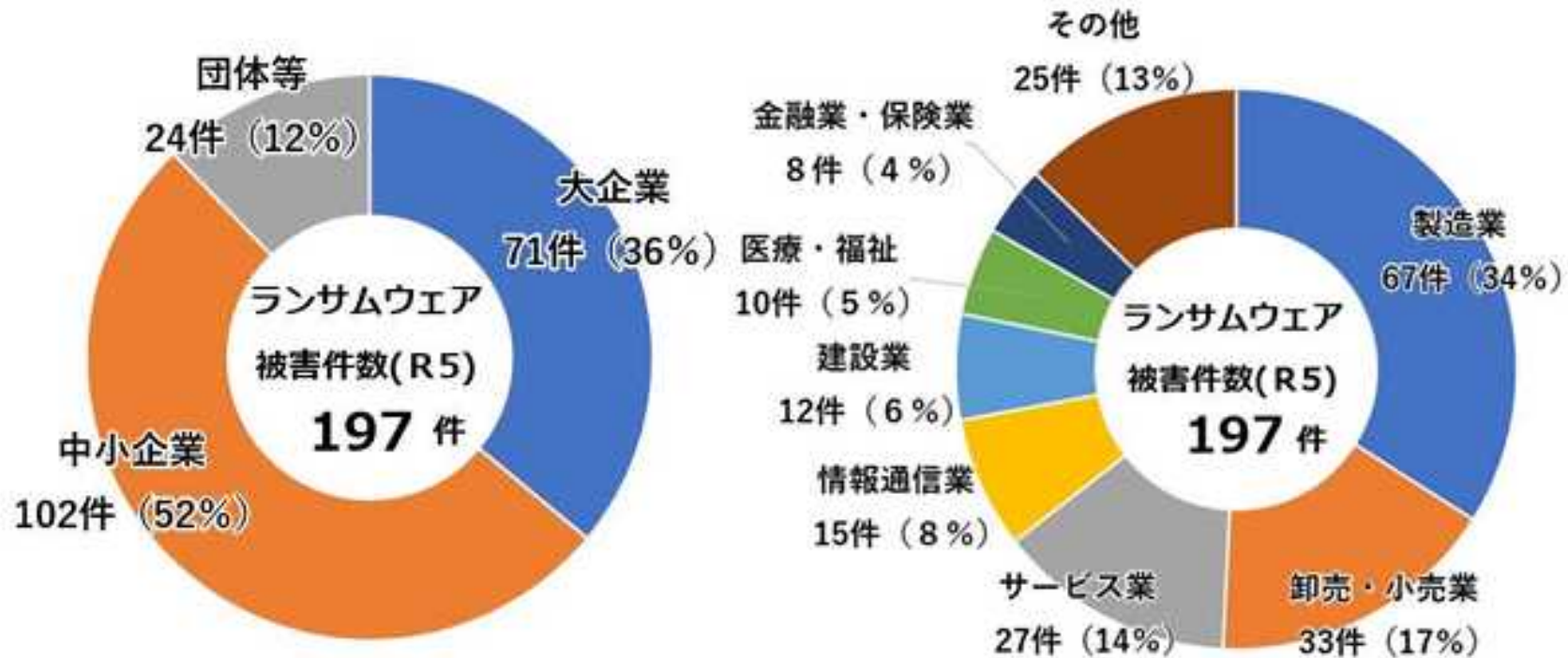


(※1) 図表は国立研究開発法人・情報通信研究機構「NICTER観測レポート2023」より当社作成

規模別・業種別のサイバー事故発生状況

- 企業・団体等におけるランサムウェア（※）被害の警察庁への報告件数は令和4年上半期以降高い水準を維持
- **中小企業の占める割合が過半数を超え、業種を問わず被害が発生**

※ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラム



警視庁「（令和6年3月14日）令和5年におけるサイバー空間をめぐる脅威の情勢等について」より抜粋

サイバー攻撃による主な影響

サイバー攻撃では、同業の他組織が通常営業の中、「システム作動停止」と「情報窃取・不正操作」が単一組織内で同時期に併発する事態に陥ることも想定され、集積する損害による事業への影響が懸念されます。

1. システム作動停止（直接的な事業中断のおそれ）

- ・停止したシステムへの依存度が大きな事業が重大な打撃を受け、主要な事業オペレーションの停止の結果、売上の喪失、ビジネスパートナーおよびその他の第三者との関係の悪化、既存顧客離れや新規顧客減少等による損害

2. 情報窃取・不正操作（間接的な事業中断のおそれ）

- ・不正なアクセスで窃取された情報の漏えい、改変、破壊あるいは悪用された個人情報の本人や機密情報の所有者に対するお詫び・補償等の諸費用
- ・調査のために停止させたシステムへの依存度が大きい事業のオペレーションが停止した結果、売上の喪失、ビジネスパートナーおよびその他の第三者との関係の悪化、既存顧客離れや新規顧客減少等による損害
- ・知的財産を含む専有競争力の低下にともなう売上の喪失、既存顧客離れや新規顧客減少等による損害

3. 被害者等との折衝や係争

- ・上記1. 2. のそれぞれに係る自社調査および訴訟・規制当局による調査や規制措置を含む法的措置、付帯的な対処費用や将来的な調停、判決、罰金等の諸費用


4. 事故対応

- ・設備やネットワーク、情報システムのセキュリティ強化や修繕・置換え等にかかる諸費用
- ・上記1. ～3. および4. への対応人員や代替オペレーション等に向けた新たな人員の配置、外部専門家の利用、従業員の教育、被害を受けていない顧客への説明や問い合わせ対応等の諸費用

サイバー攻撃による対応コスト（例）

以下対応事例は実際に発生した複数のサイバー事故(ランサムウェア他)をもとに当社で設定

主な対応事項	主な対応内容	費用の小計
インシデントハンドリング	■インシデント発生企業の伴走支援（状況把握・初動対応・原因調査・復旧対応・再発防止策/対策強化等のアドバイス）	約 500万円
デジタルフォレンジック調査	■サーバ・クライアントPC等のログ調査（侵入経路・アクセス状況・不審プログラムの有無・情報流出有無・他端末への影響有無・・・等）	約 1,100万円
謝罪、報告、社外公表等の広報対応	■ 被害者への謝罪、関係機関への報告、社外公表文書、緊急記者会見用の報道発表資料・想定Q&Aの作成助言・レビュー、緊急記者会見の手順等のコンサルティングなど各種の広報対応のサポート	約 300万円
専用コールセンターの設置・運営	■コールセンターに専用のコール受発信ブース設置、3週間の照会対応実施	約 700万円
再発防止策の実施	■EDRの導入や脆弱性診断の実施など	約 800万円
弁護士等への相談	■ 公表文書のレビュー、訴訟への対応等	約 200万円
その他の費用	■被害者へのお詫び金品、その他取引先への通信・連絡費用など ■ネットワーク再構築費用、その他業務継続のために緊急に要する対応費用など	+ a
費用の総合計		約 3,700万円 + a



JNX会員専用サイバー事故相談窓口について

サイバー事故発生時の対応について

緊急時に何をすべきか分からない

誰に相談したらいいか分からない

対応できる要員やノウハウがない

緊急対応の規定はあるが、手順が明確になっていない

原因究明は、どのようにやるのか



監督官庁への報告などはどうすればいいのか

JNX会員専用サイバー事故相談窓口にご相談いただければ、そのお悩み解決できます！

情報漏えい・不審なメール・ウイルス感染など、今すぐご相談されたい方は「JNX会員専用サイバー事故相談窓口」へご連絡ください！



データが
暗号化された

脅迫メッセージが表示され
PCがロックされた



情報が漏洩
している

取引先など外部から
通達があった



ホームページが勝手に
書き換えられた

ホームページの不具合を
攻撃された



自社を騙るメールが
送られている

怪しいメールの添付ファイル
を開いてしまった

情報漏えい・不審メール・ウイルス感染など、今すぐ相談されたい方はこちら
JNX会員専用サイバー事故相談窓口

サイバー事故の相談と初動のアドバイスを無料でサポート

まもる さいばー

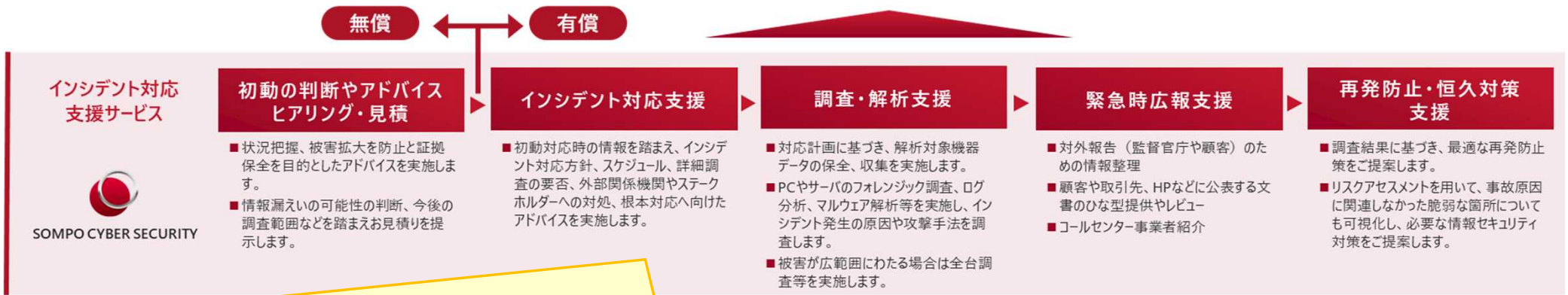
0120-066-318

24時間・365日対応（年中無休）

本サービスご利用にあたってのご注意

ご連絡が平日17：00以降、翌9:00までもしくは休日の場合などにつきましては、
当社のサービス提供開始が翌営業日9時以降になる場合があります。あらかじめご了承ください。
サービスの詳細につきましては「利用規約」および「よくあるご質問」をご確認ください。

インシデント対応の流れ／当社サービス範囲



サイバー保険に加入している場合、上記「インシデント対応支援」「調査・解析支援」「緊急時広報支援」など有償サービスの多くが保険会社による保険金支払いの検討対象となります。ただし、不要や過剰な調査であった場合には保険金のお支払い対象とならなかったり、再発防止に係る費用など保険金のお支払い対象になりづらいサービスもありますので、詳細は保険会社までお問合せください。

(参考) 各種サポートメニュー〔調査・データ復旧等〕

原因究明に必要な調査やデータ復旧などの対処にご利用いただけるサポートメニューです。主に専門会社を手配の上、サービスを提供します。

デジタル フォレンジック

原因調査に必要不可欠

インシデント発生時の証拠保全、ログデータ等の解析による感染源と感染ルートの特定を実施し、調査結果を報告書で提出します。

データリカバリ

貴重なデータを復旧・復号

対象となるコンピューターやデジタル記録媒体等の機器など改ざん・破壊・暗号化されているデータ・ファイル等をお預かりし、復旧・復号を実施します。

エンドポイント 侵害調査

全台調査による被害状況確認

過去の攻撃追跡や現在の侵害状況を全端末のフォレンジック調査（EDR検知）で、調査します。全台調査を行って、安全性を確認したい場合に最適です。

情報漏えい チェック (マルウェア感染)

収束宣言前にチェック！

通信のトラフィックデータ収集機器を設置し、一定期間のデータを解析することで、マルウェア感染したパソコンの通信を見つけ出し、情報漏えいのリスクを確認します。

ダークウェブ 情報えい調査

情報が闇サイトに流れていないか確認

ダークウェブを含むサイバー空間内に、お客さまに関連する機微情報・脅威情報が漏えいしていないかを調査し、レポート報告します。

マルウェア 通信調査

お客さまに負荷をかけずに外部から調査

マルウェア感染端末が、サイバー攻撃者と不正な通信を行っていないかを、お客さまの環境に手を加えることなく、『外部から』調査します。

(参考) 各種サポートメニュー [恒久対策支援]

再発防止に向けてお客さまのセキュリティ強化に貢献すべく、対策内容や方向性の検討段階から支援させていただくコンサルティングサービスです。

- セキュリティ対策をどこから着手するべきか知りたい
- 導入済対策の実効性を評価してほしい
- 自社の課題、弱点を分析・評価してほしい

- セキュリティ施策の計画・推進にあたり、専門家に色々と相談したい。

サイバーリスクアセスメントサービス

専門のコンサルタントによる複数回のヒアリングとディスカッションを通じて、貴社を取り巻く脅威に対し、対策が有効に実施されているかを分析・評価します。セキュリティ上の課題と潜在リスクを可視化するとともに、把握された課題の改善に向けてとるべき対策のロードマップ・実施計画（費用感含む）を提示します。（「標準プラン」と「簡易プラン」の2種類がございます）

成果物

- アセスメント報告書
（エグゼクティブサマリ、境界俯瞰図、対策の方向感、 など）

情報セキュリティアドバイザー

情報セキュリティアドバイザーサービスは、企業を取り巻く脅威に対して適切かつ効果的なセキュリティ対策を実現するための相談サービスです。情報セキュリティコンサルティングの経験豊富なコンサルタントが、貴社 CISO・情報システム担当者のセキュリティ施策に関する悩みについて、適切なアドバイスを行います。

活用例

- 社内情報セキュリティ運用体制に関するご相談
- 情報セキュリティ文書の策定・改定に関するご相談 など

(参考) 各種サポートメニュー〔恒久対策支援〕

サイバーリスクアセスメントサービスやアドバイザリーその他、各種コンサルティングサービスを提供しています。

No	コンサルティングメニュー	概要
1	セキュリティポリシー策定支援	<ul style="list-style-type: none">■ ポリシー策定支援（方針・規程・基準の策定支援）
2	セキュリティガイドライン策定支援	<ul style="list-style-type: none">■ 手順・要領書を利用したガイドライン策定支援
3	インシデント対応関連サービス	<ul style="list-style-type: none">■ CSIRT体制整備支援■ 各種規程および手順書の整備とオーソライズ■ インシデント対応態勢構築■ インシデント対応フロー策定■ インシデント対応マニュアル策定■ インシデント対応訓練サービス■ CSIRT演習
4	ISO/IEC27001認証取得支援	<ul style="list-style-type: none">■ ISO27001取得支援
5	ISO/IEC27001運用支援	<ul style="list-style-type: none">■ 資格取得後のフォロー支援
6	Pマーク取得支援	<ul style="list-style-type: none">■ Pマーク取得支援
7	Pマーク運用支援	<ul style="list-style-type: none">■ 資格取得後のフォロー支援
8	セキュリティ教育サービス	<ul style="list-style-type: none">■ 標的型攻撃メール訓練サービス■ セキュリティ教育コンテンツ作成支援■ eラーニングサービス■ セミナー型研修
9	情報セキュリティアドバイザリー	<ul style="list-style-type: none">■ お客さまの課題・ご要望事項に関して、定例会を中心に対応

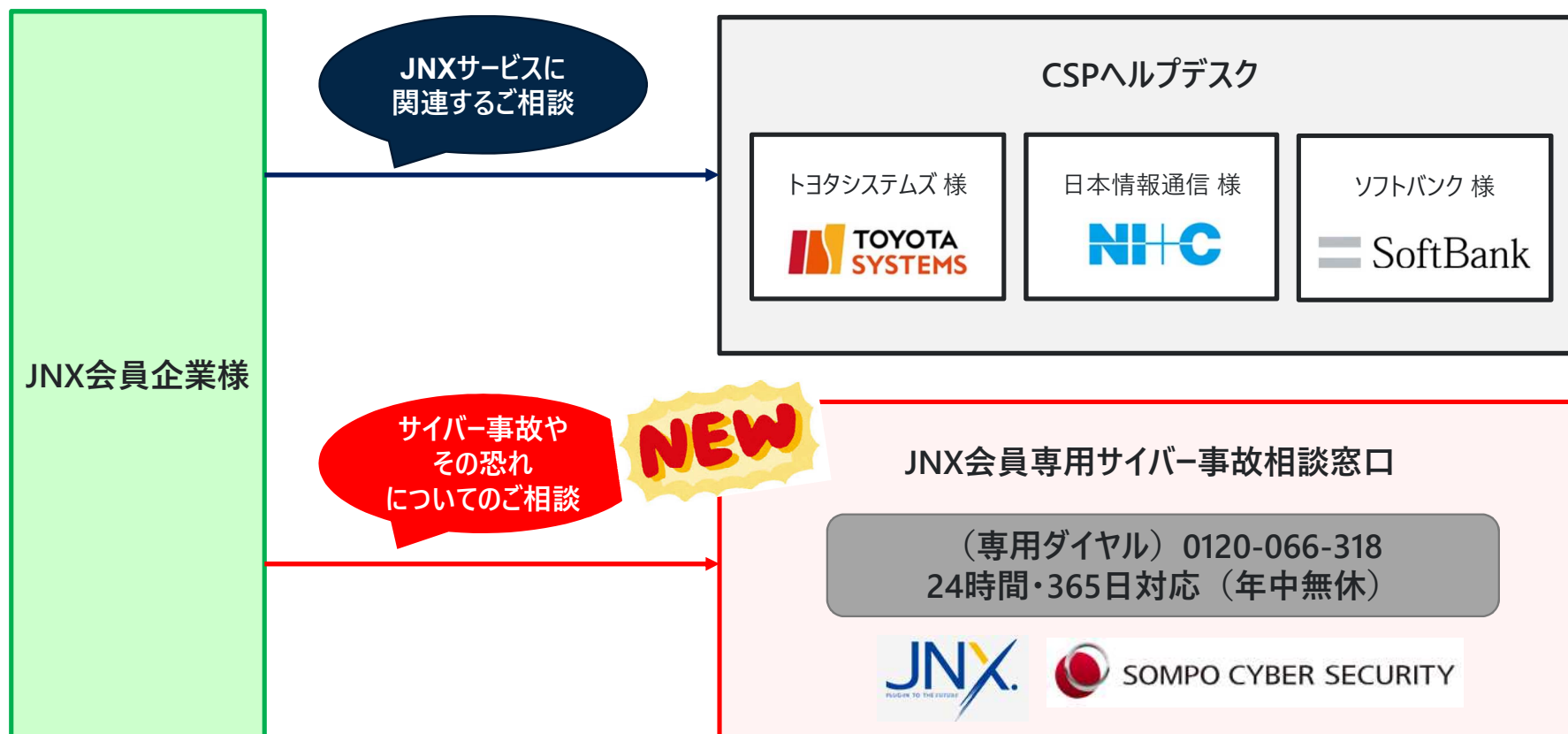
(参考) 各種サポートメニュー〔恒久対策(技術的対策)〕

コンサルティングサービス以外に、各種技術対策のご支援も可能です。

No	ジャンル	サービス名	概要
1	 エンドポイント対策	<ul style="list-style-type: none"> ■ 次世代型AIアンチウイルスソフト Deep Instinct 	<ul style="list-style-type: none"> ● 未知マルウェアやランサムウェア防御として深層学習 AI による検知機能を搭載した次世代エンドポイント製品です
		<ul style="list-style-type: none"> ■ エンドポイント監視検知プラットフォーム CybereasonEDR 	<ul style="list-style-type: none"> ● パソコンやサーバーへの標的型サイバー攻撃を、機械学習 AI によりリアルタイムに検知・可視化し、攻撃の拡大を阻止するEDR製品です
2	 WEB サイト対策	<ul style="list-style-type: none"> ■ WEB サイトへの攻撃防御 WAF 攻撃遮断くん 	<ul style="list-style-type: none"> ● お客様の Web サイトを守るセキュリティサービスで、外部からのサイバー攻撃を遮断し、個人情報の漏洩や Web サイトの改ざん、サービス停止などを防ぎます
3	 脆弱性対策	<ul style="list-style-type: none"> ■ 脆弱性診断サービス (WEB アプリ、ネットワーク、クラウドセキュリティ) 	<ul style="list-style-type: none"> ● 公開している Web アプリケーションや、リモートアクセス可能なサーバやNW機器を対象として、悪用が想定されるシステム上の脆弱性の有無を技術的視点で検証します
		<ul style="list-style-type: none"> ■ ペネトレーションテスト 	<ul style="list-style-type: none"> ● お客様環境に合わせて疑似シナリオを作成し、シナリオに基づいて侵入テストを実施し、情報漏えいリスクなどを評価・検証し報告します
4	 ログ分析対策	<ul style="list-style-type: none"> ■ ネットワーク監視サービス SOMPO SOC 	<ul style="list-style-type: none"> ● UTMのアラートログを24時間リアルタイムで分析・分類した上で、インシデントの疑いがある場合には初期対応方法とともに通知する監視サービスです
5	 ログ集積対策	<ul style="list-style-type: none"> ■ 統合ログ管理ツール Logstorage 	<ul style="list-style-type: none"> ● ログの暗号化、改ざん検出、アーカイブ化などで監査証拠を安全に長期保持し、あらゆるログを収集・保管・分析・監視できるシステムです
6	 フィッシング攻撃対策	<ul style="list-style-type: none"> ■ セキュリティ意識向上トレーニングプラットフォーム KnowBe4 	<ul style="list-style-type: none"> ● セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界が認める統合型プラットフォームです
7	 脆弱性管理・SBOM 対策	<ul style="list-style-type: none"> ■ LANSCOPE Endpoint Manager 	<ul style="list-style-type: none"> ● お客様環境のIT資産管理／内部不正対策／外部脅威対策を統合管理する事で、シンプルで効率的なITマネジメントの実現を支援します
		<ul style="list-style-type: none"> ■ 脆弱性管理サービス yamory 	<ul style="list-style-type: none"> ● 企業内 IT システム基盤のソフトウェアの脆弱性を可視化する脆弱性管理サービスで、OSS ライセンス管理や SBOM 対応にも準拠できます
8	 クラウドサービス対策	<ul style="list-style-type: none"> ■ クラウドリスク評価サービス Assured 	<ul style="list-style-type: none"> ● クラウドサービス (SaaS) のセキュリティリスク評価を Assured 社がリサーチャーとなり調査しデータとして提供する WEB サービスです
9	 グループ会社・委託先対策	<ul style="list-style-type: none"> ■ サプライチェーンリスク評価サービス Panorays 	<ul style="list-style-type: none"> ● ドメイン情報から調査する外部評価と、調査票 (アンケート) による内部評価にて一元的に管理するサービスで、サードパーティのセキュリティ対策状況を幅広く可視化することが可能になります

「JNX会員専用サイバー事故相談窓口」ご利用の流れ

「JNX会員専用サイバー事故相談窓口」は、会員企業様においてサイバー事故やその恐れが発生した場合に、以下の通り会員企業様から直接相談窓口にご連絡いただくことを想定しています。





SOMPO CYBER SECURITY