富士通のセキュリティ人材を駆使し CSIRT の最適運用を全方位で支援

サイバー攻撃対策には、運用が欠かせない。その中心となるものが、CSIRT である。どのように技術が進んでも、やはり守るのは人だ。そこに、高度な技術が必要となる。しかし、人員や技術の不足、インシデント発生時の適切な対応方法など、CSIRT の運営に際して多くの悩みの声が寄せられている。富士通はこれらの課題に応えるため、企業の CSIRT 運営を支援するソリューションを提供。セキュリティに関する高度な技術と知見、そして数多くの経験を誇る富士通のアナリストが CSIRT の運営をトータルでサポートする。

万全のセキュリティ対策の推進には 組織的な対応力の強化が不可欠

ますます複雑化・巧妙化するサイバー攻撃の脅威に対抗するためには、ツールの導入だけでは不十分であり、セキュリティインシデントの発生に際して迅速かつ適切な対策を講じられる組織体制の整備が必須となる。その役割を担う組織が、CSIRT(Computer Security Incident Response Team）だ。

富士通は、コンサルサービスの１つとして、企業の CSIRT 運営を支援するソリューションを提供している(図 1)。これは富士通がお客様のセキュリティ対応組織に加わり、体制の確立をはじめとして、日々のセキュリティ運用の作業支援、プロダクトのセキュリティ品質向上の強化支援を実施するなど、現場のセキュリティ運用の“旗振り役”を担うものだ。お客様ごとに抱える固有のセキュリティニーズに応じてサービスチームを編成し、リモート対応でサービスを提供。セキュリティ専任チームが対応することで、人的リソースや対応スキルの不足を解消し、円滑なセキュリティ運用の推進をサポートしている。

富士通がこのソリューションを提供している背景には、CSIRT の運営に際して企業が様々な悩みや課題を抱えていることがある。企業の CSIRT の運営においてどのような課題が浮上しているのか、そして富士通の CSIRT 運営を支援するソリューション（以下、「CSIRT マネジメント」）を利用することで、どのような解決策がもたらされるのか。①セキュリティ組織運営、②インシデント＆レスポンス③セキュリティ対策の計画立案と実行、改善――の 3 つの視点に基づきながら解説していく。

人員とスキルの不足をカバーし 事業の円滑な CSIRT 運営を支援

CSIRT マネジメントのポイントの１つは、企業の CSIRT に富士通の CSIRT 運用のプロフェッショナルが参画し、組織運営の支援を行うことだ。企業における CSIRT の運営は、専任のスタッフによる専門部署を設置して行う場合と、社内の各部門から有識者を招聘し、既存業務との兼任によるバーチャルな組織を形成して行われるケースの 2 つに大別される。多くの企業では、後者の体制で運営されているのが実情であろう。その場合、本来の業務に従事しながら CSIRT 業務も行わなければならないため、慢性的な人材不足に悩む企業からは「CSIRT に十分な人員を確保できない」という声も多々寄せられている。

また、複雑化するセキュリティ脅威に伴い CSIRT に求められる対応も多方面へと拡大しており、CSIRT のスタッフには、より高度なセキュリティ知識や知見が求められるようになっている。さらに、インシデントの発生から対処までを、迅速かつ適切に遂行していくためのスキルも不可欠だ。例えば、セキュリティインシデントが発生した際の対応１つとっても、それが社内のユーザーから報告されたのか、外部に業務委託している SOC から連絡があったのか、多種多様な報告元からの連絡に基づいて、対処していなければならない。調査分析から対処策の検討、実際の対処の実施、関係部署への報告など、多岐にわたるタスクが要求される。

さらに CSIRT のスタッフは関係部署との円滑なコミュニケーションも図っていく必要があるため、高いコミュニケーションスキルの保有、あるいは、プロジェクトリーダーの経験を持っていることが望ましい。

これらのことから、セキュリティ技術に関連する知識以外にも、ビジネスインパクト分析や交渉スキルなどの経験が必要とされるが、そうした人材をチームに招き入れることは至難の業となる。

このような人員とスキル不足の課題を、富士通の CSIRT マネジメントは解決可能だ。セキュリティに関する高い知見と多くの経験を有した、専用の CSIRT チームが実際にお客様先に参画し、セキュリティ組織の運営に関して様々な支援を行う。特筆すべきポイントは助言だけではなく、CSIRT 業務の実務を行う

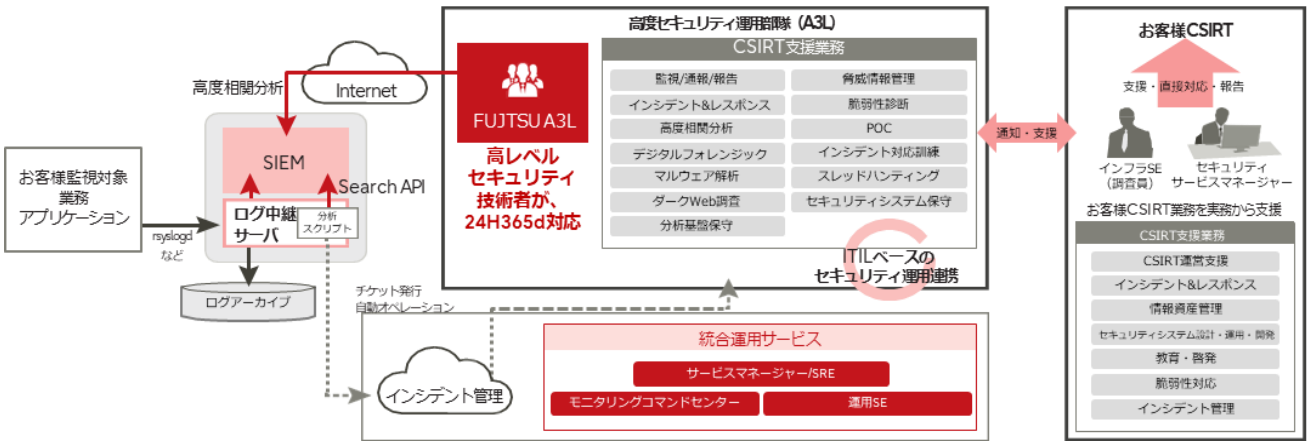

図 1 CSIRT マネジメントの概要

とだ。脅威情報の収集・分析・評価をはじめ、インシデント発生時の対応から、指揮命令や関連部署との連携などの取りまとめ、自組織内外の情報共有、対処後の報告や今後の方針策定といった、CSIRT に必要となる役割のほぼすべてを、お客様の “メンバーの一員”となって遂行する。そうしたことからセキュリティ対策に必要なアドバイスや、セキュリティプロセスの管理・改善支援、情報資産の現状分析とリスクアセスメント支援、セキュリティに関する教育・啓発もサービス提供範囲に含まれており、CSIRT 業務を効率化しながら全面的にセキュリティ強化を図れるようになる。

インシデントハンドラーとアナリストが連携し、広範囲にわたる対応を実施

2 つ目のインシデント＆レスポンスについて、CSIRT マネジメントは、富士通のセキュリティ運用サービスとの連携により、迅速かつ適切な対応を可能にする。

いざ、セキュリティインシデントが発生した際、CSIRT としてどのように対処すればよいのか不安に感じている企業は少なくない。サプライチェーンを経由したマルウェア感染などのセキュリティインシデントが発生した場合、その検知をはじめ感染経路の究明、自社への影響度の評価、そして関連部署への連絡や対処など、関係者には多くの決定と対応が求められる。事実、セキュリティインシデントの発生時には、その対応に経営判断が必要とされることもあり、“これが本当に正しい対応なのか、専門家のアドバイスがなければ判断できない”という声も多々、寄せられている。

こうした悩みに対しても、富士通の CSIRT マネジメントを活用することで、最適なインシデント＆レスポンスが可能となる。富士通のセキュリティ運用サービスとの連携により、日々、サイバー攻撃やセキュリティインシデントの情報を収集、攻撃パターンの分析と対処法の策定を行う一方、有事の際には、CSIRT マネジメントのメンバーが関連企業を含めて情報収集を行い、適切な決断ができるように対応する。

具体的には、実際にセキュリティインシデントが発生した場合、セキュリティシステムの運用設計や現場での対策実施を担う「セキュリティインシデントハンドラー」が関係部署、および富士通の SOC、アナリストと連携しながら、インシデント発生の連絡から原因の調査、対処、そして収束後の改善策の立案に至るまでの陣頭指揮を実施。一方、アナリストは、セキュリティインシデントハンドラーと連携しながら、インシデント発生時のログ確認をはじめ、マルウェア感染が発生した場合には感染経路の究明など、より高レベルの調査を行う。アナリストには、マルウェアに習熟した人員や、フォレンジック調査に精通した人員など、各分野における高い見識と、様々なプロジェクトでの豊富な実績を有したスタッフが在籍しており、有事の際にはこの両者が一体となり、迅速で適切なインシデント＆レスポンスが行える点が CSIRT マネジメントの大きな強みである。

セキュリティに関する課題を解決するための継続的な提案とサポートを提供

3 つ目のポイントとして、CSIRT マネジメントは CSIRT の運営支援だけでなく、セキュリティポリシーの策定や改善、展開をはじめとした、情報セキュリティ対策全般にわたる改善提案や支援も行う(図 2)。

これまで述べてきたように、セキュリティインシデントの発生時には多岐にわたる対処が必要となるほか、日々、高度化するサイバー攻撃に備えていくためには、事後対応力の強化を含めた、継続的な改善策を打ち立て、それを着実に実施していくことが不可欠だ。だが、現実として、自社にどのようなセキュリティに関する課題が生じているのか明確に把握できておらず、また、どのような手立てを講じれば、自社にとって最善となるセキュリティ対策の強化、改善を図っていけるのか、苦慮しているのが実情ではないだろうか。このほかにも、セキュリティポリシーや規定を定めたものの見直しができていない、社員へのセキュリティに関する啓発活動が進んでいないなど、セキュ

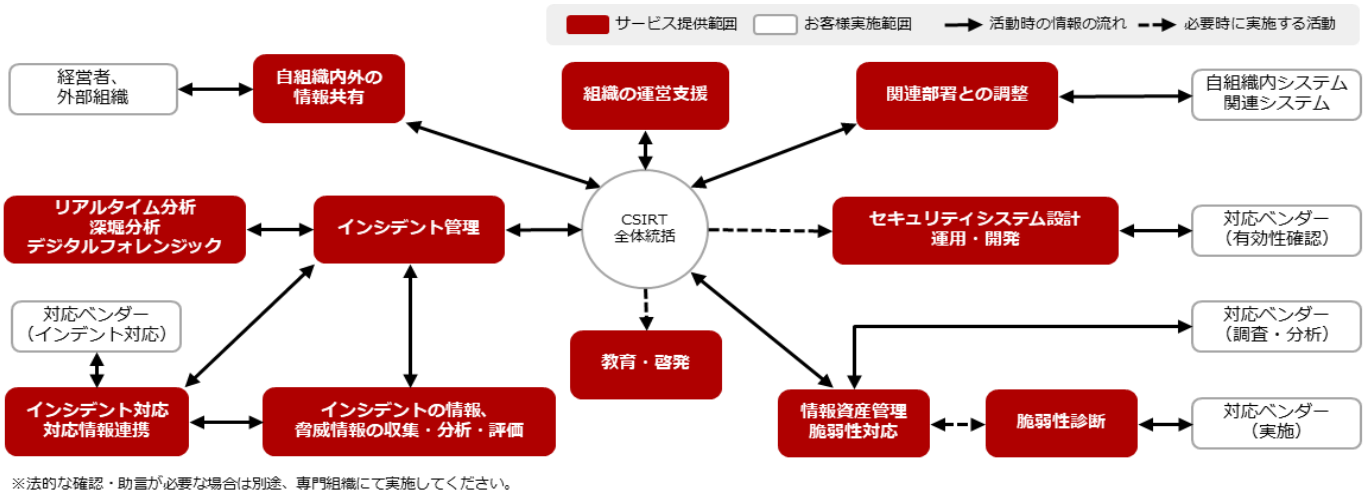

図 2 CSIRT マネジメントのサービス提供範囲

リティ運用における実行サイクルの強化も課題として挙げられるだろう。

CSIRT マネジメントは、CSIRT の構築・運用支援にとどまらず、将来にわたって様々なセキュリティ上の脅威に対応していけるよう、既存環境、新技術、組織、富士通の専門組織などを最大限に活用しながら、着実なセキュリティ対策の計画立案と実行、改善をサポートしている。具体的には、CSIRT マネジメントのスタッフがセキュリティプロセスの改善から顧客 CSIRT の組織強化、さらにはセキュリティガバナンスの改善までアドバイスや支援を実施し、継続的なセキュリティ対策の強化・改善を支援している。

富士通の総合力を活用し、お客様との“二人三脚”でセキュリティ強化に邁進

これまで説明してきた CSIRT マネジメントの提供を根底から支えているのが、富士通のセキュリティアナリストの存在である。個別のセキュリティインシデントや技術に対する知見はもちろんのこと、それらを統合し実際のセキュリティ対策の提案や実施に活かすことが可能な、数多くの経験値を積み上げている。

最近は標的型ランサムウェア攻撃や、サプライチェーン攻撃などに加え、テレワーク環境への攻撃も増えている。こうした脅威に対処していく上で、その先導を担う CSIRT の重要性はますます高まっており、参加メンバーに求められる知識や責任、そして負担もさらに大きなものとなっている。より高度な CSIRT の運営を効果的に行っていくためには、アウトソーシングサービスの利用は有効な手段の１つとなる。富士通の CSIRT マネジメントは、最高レベルのサイバーセキュリティ技術者がお客様の CSIRT 業務の運用を全面的に支援する。さらに、富士通がシステムインテグレーターとして長年培ってきた、多岐にわたる業種業界におけるシステム構築経験や業務に関する知識、そして他部門との連携によるトータルソリューションが提供できる点も大きな優位性の１つである。

多くの企業においてデジタル化に向けた取り組みが積極的に推進される中、そのための基盤を強固にしていくためには、あらゆるサイバーセキュリティの脅威に対応可能な体制を構築していかなければならない。そこで重要な施策の１つとなるものが、CSIRT の整備・強化であることは言うまでもない。CSIRT マネジメントは、お客様と富士通が“二人三脚”となって、社内のセキュリティを向上させていくためのサービスであり、企業が抱える固有の要件にも柔軟に対応が可能だ。

これからも富士通はセキュリティに関する最新の脅威動向や技術トレンドに全方位でアンテナを張り巡らせるとともに、お客様のシステム全体を支えるセキュリティの“プロフェッショナル”として安全安心な企業運営、社会の実現に向けて貢献していく。

[2021 年掲載]

お問い合わせ先

製品・サービスについてのお問い合わせはコチラ

富士通株式会社　〒211-8588　神奈川県川崎市中原区上小田中 4-1-1