いま、セキュリティ強化に求められる回復力 ――事業継続を意識した「サイバーレジリエンス」向上のカギ

佐　藤　重　之

要　約　多くの企業がサイバー攻撃へのセキュリティ対策を実施する一方で、攻撃者側はそれらの対策を回避するために攻撃を進化させている。企業は、攻撃を防ぐことが困難であることを認識し、攻撃を受けることを前提とした回復力（レジリエンス）を向上すべきである。サイバー攻撃に対するレジリエンスを向上するための対策として、サイバーレジリエンスが注目されている。サイバーレジリエンスの向上には、予測力、抵抗力、回復力、適応力をそれぞれ向上させていくことが重要であり、それぞれの能力強化がサイバーレジリエンス向上のカギになる。BIPROGY グループは様々なセキュリティソリューションおよびサービスを提供することで、顧客のサイバーレジリエンス向上を支援する。

1. はじめに

サイバー攻撃によるセキュリティインシデントのニュースを、今では日常的に目にするようになった。これまでセキュリティインシデント関連のニュースは、主にセキュリティ情報を取り扱うニュースサイトに掲載されてきたが、最近ではマスコミで報道されることが増加し、一般紙や各検索ページのトップで記事として取り上げられることが一般的になってきた。

こういった状況から、多くの企業がサイバー攻撃を脅威と認識し、何らかの対策を実施している。しかし、サイバー攻撃による被害が日々報道されているように、その脅威は衰えていない。原因は、サイバー攻撃を仕掛ける攻撃者側が、企業の対策を超える進化した攻撃を仕掛けてきていることである。だからこそ、企業はサイバー攻撃を完全に防ぐことはできないと認識し、被害を受ける前提での準備や対策を実施することが必要不可欠である。

本稿では、サイバー攻撃の中でランサム攻撃に焦点を当て、攻撃者側の進化を解説した上で、被害を受けることを前提とする回復力（サイバーレジリエンス）の考え方を、BIPROGY グループが提供しているソリューションと共に紹介する。2 章でサイバー攻撃の最新動向を示し、3 章で攻撃を受けた企業のセキュリティ対策の実態を解説する。4 章でいま求められる回復力であるサイバーレジリエンスの必要性や考え方を紹介したうえで、5 章で BIPROGY グループが提供するソリューションがサイバーレジリエンスのどのような領域で活用できるかを述べる。

2. サイバー攻撃の最新動向

本章では、独立行政法人情報処理推進機構から公開されている「情報セキュリティ 10 大脅威」[1]と警察庁サイバー警察局が発行している「サイバー空間をめぐる脅威の情勢等について」[2]を用いて、サイバー攻撃およびランサム攻撃の最新動向を解説すると共に、それぞれの脅威の捉え方を考察する。

2.1　情報セキュリティ 10 大脅威　2025

独立行政法人情報処理推進機構から毎年公開されている情報セキュリティ 10 大脅威は、セキュリティ対策を検討する上で、多くの企業に情報源として利用されている。表 1 は、2025 年 1 月 30 日に公開された組織向けの情報セキュリティ 10 大脅威に対して、2023 年からの順位の変遷を追記したものである。

表 1　情報セキュリティ 10 大脅威 2025［組織］

順位	「組織」向け脅威	2024 順位	2023 順位
1 位	ランサム攻撃による被害	1 位	1 位
2 位	サプライチェーンや委託先を狙った攻撃	2 位	2 位
3 位	システムの脆弱性を突いた攻撃	5 位	6 位
4 位	内部不正による情報漏えい等	3 位	4 位
5 位	機密情報等を狙った標的型攻撃	4 位	3 位
6 位	リモートワーク等の環境や仕組みを狙った攻撃	9 位	5 位
7 位	地政学的リスクに起因するサイバー攻撃	未選出	未選出
8 位	分散型サービス妨害攻撃（DDoS 攻撃）	圏外	圏外
9 位	ビジネスメール詐欺	8 位	7 位
10 位	不注意による情報漏えい等	6 位	9 位

2025 年の情報セキュリティ 10 大脅威は、2024 年のものと比べて、大きく二つの変化があった。一つ目の変化は、新たな脅威の出現である。7 位の「地政学的リスクに起因するサイバー攻撃」が初めて選出された。国家関連の団体や施設などに対して多くの攻撃があったことが、選出の理由と考えられる。また、8 位の「分散型サービス妨害攻撃（DDoS 攻撃）」が 5 年ぶりに 10 位以内にランクインした。大手企業のシステムが攻撃を受け、交通や通信、金融システムなどが利用不能な状態に陥ったことにより、多くの利用者に影響が出たことに起因しているものと想定する。なお、本稿ではランサム攻撃に焦点を当てて解説するため、それぞれの攻撃に関する詳細説明は割愛する。詳しくは情報セキュリティ 10 大脅威の解説書[3]を参照してほしい。

二つ目の変化は、脅威の表現が変更されていることである。1 位のランサム攻撃は、これまでランサムウエア攻撃と表現されていた。身代金を要求する攻撃が、ランサムウエアを使った攻撃だけでなく、ノーウエアランサム攻撃と呼ばれるランサムウエアを使わない攻撃や、DDoS 攻撃を組み合わせて脅迫する攻撃手法などが用いられるようになったことから、身代金を要求する攻撃手法全体を表す表現に変更したものと考えられる。また、2021 年から 2024 年まで使われていたニューノーマルな働き方を狙った攻撃という表現が無くなったことも、表現の変化の一つとして挙げられる。2020 年に発生した新型コロナウイルス感染症（COVID-19）によって大きく変容した働き方が、以前の働き方に戻るか、もしくは完全にリモートワークに移行したことで、新しい常識（ニューノーマル）とはいえなくなったためと推測される。

このように、情報セキュリティ 10 大脅威 2025［組織］には変化もあったが、1 位から 5 位の脅威は、2024 年と比べて順位は入れ替わっているものの、選出されている脅威に変更はない。1 位のランサム攻撃による被害は、2016 年の情報セキュリティ 10 大脅威［組織］から 10 年連

続ランクインしており、5年連続で1位に選出されている。ランサム攻撃は長年にわたり多くの企業に対して影響を与えており、企業側でも対策を実施しているものの、攻撃者側が企業のセキュリティ対策を理解し、その対策を回避するために攻撃手法を進化させていることが、ランクインの理由と考えられる。

2.1.1　ランサムウエア（Ransomware）攻撃とは

ランサム攻撃の進化を解説する前に、まずはランサムウエア攻撃の定義について記述する。ランサムウエアとは、身代金を意味する「Ransom（ランサム）」と「Software（ソフトウエア）」を組み合わせた造語であり、マルウエアの一種である。

ランサムウエア攻撃は、マルウエアを攻撃対象のパソコンやサーバーに感染させ、データやファイルを暗号化することで利用不能な状態とし、その暗号化したファイルを元に戻すことと引き換えに金銭（身代金）を要求する攻撃である（図1）。

図1　ランサムウエア攻撃

2.1.2　ランサム攻撃の進化

前項の通り、ランサムウエア攻撃はマルウエアを使ったランサム攻撃である。企業側は対策として、ランサムウエアの駆除や検知を行える高度なマルウエア対策ソフト（Next Generation Anti-Virus（NGAV）や Endpoint Detection and Response（EDR））を導入したり、仮に感染してデータやファイルが暗号化されてしまっても、バックアップによる復旧で身代金を払わずに済むように、バックアップ運用を強固にしたりするなどして、システム側の強化を推進してきた。しかし、そういった対策をかいくぐるために攻撃手法も進化しており、マルウエアでの攻撃だけでなく、次のような攻撃手法が用いられることも多くなっている。

1）二重脅迫型ランサム攻撃

従来のランサムウエアを使ったランサム攻撃を仕掛ける前に、対象となる組織のネットワークに不正侵入し、データを窃取して保存、その後ランサムウエアを実行する手法である。これにより、従来の「データを使えるようにしたければ金銭を払え」という要求に加えて、「窃取されたデータをインターネット上に公開されたくなければ金銭を払え」という、二重の脅迫をする（図2）。

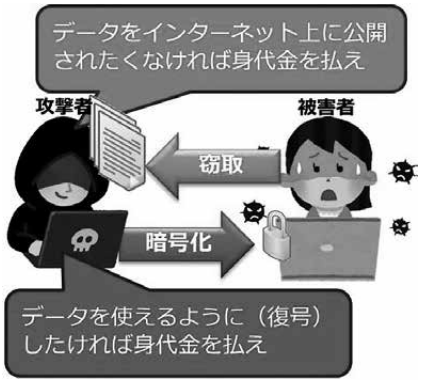

図 2　二重脅迫型ランサム攻撃

2）ノーウエアランサム攻撃

その名称の通りマルウエアを使わないランサム攻撃であり、不正侵入してデータを窃取することに特化した攻撃である。マルウエアを使わないことで、高度なマルウエア対策ソフトにも攻撃が検知されないばかりか、バックアップの有無も関係なく攻撃できる（図 3)。

図 3　ノーウエアランサム攻撃

このように、攻撃者は、攻撃先となる企業が導入したセキュリティ対策の状況を認識したうえで、対策不足の箇所や新たなシステムの脆弱性を突くよう攻撃手法を進化させて、次々と新しい仕組みの攻撃を仕掛けてくる。

2. 2　ランサム攻撃の被害状況

本節では、警察庁サイバー警察局が発行している「令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について」から情報を引用して、ランサム攻撃の被害状況を解説する。図 4 は、企業や団体がランサム被害にあった際の都道府県警察に届け出た件数を表している。2021 年以降件数は増加しており、2022 年以降は半期で 100 件以上の届け出があることから、多くの被害が発生していることが分かる。なお、2023 年以降の被害報告件数のうち、75％程度が 2 章で紹介した二重脅迫型のランサム攻撃手法になっているという報告もあり、多くの組織がネットワークへの不正侵入を許している状況と考えられる。また、2023 年上期からは、ノー

ウエアランサム被害も報告され始めている。ノーウエアランサム攻撃の場合、システム停止などの実害が無いため、企業が気づいていない場合も考えられることから、実際の被害数はさらに多い可能性がある。攻撃手法の進化により、実際の被害はより増加しているものと考えざるを得ない。

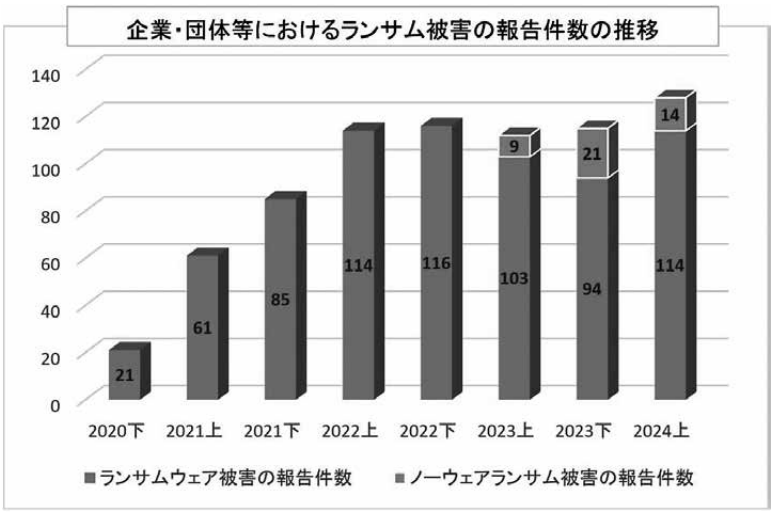

図 4　ランサム被害の報告件数の推移

2. 3　ランサム被害の対象企業

次に、ランサム被害を受けた企業について解説する。図 5 は、2024 年上半期にランサム被害の報告をした 114 件の業種別報告件数を表したグラフである。最も多くの被害報告を行った業種は製造業であり、次いで卸売・小売業となっている。これまで脅威とされてきた標的型攻撃や不正侵入による情報窃取においては、窃取した情報を転売することで攻撃者が金銭を得ていたため、大量の個人情報や国家機密などの重要情報を持った企業が狙われることが多かった。それに対して、ランサム攻撃は、操業停止による身代金により金銭を得る攻撃手法であることから、業種を問わず脆弱性を持った企業が攻撃対象となる。企業間の取引が中心の製造業は個人情報をあまり保持しておらず、これまで比較的狙われにくい業種であり、セキュリティ対策が不十分だったところを、ランサム攻撃に狙われたものと考えられる。

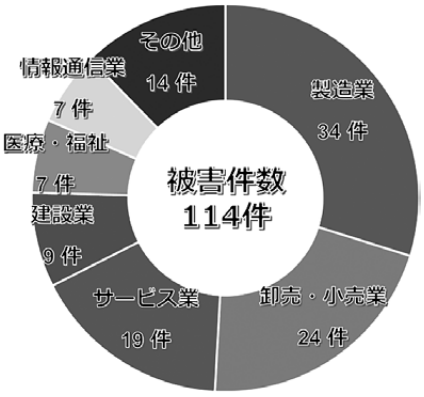

図 5　被害業種別報告件数

さらに、図 6 の被害企業規模別報告件数から、被害の多くが中小企業で発生していることが分かる。過去の脅威動向では、価値の高い情報を持つ大手企業が狙われるケースが多かったが、ランサム攻撃では、短期間の操業停止でも廃業の危機に陥るほど規模が小さい企業など、中小規模の企業にまで攻撃対象が広がっている。

このことから、ランサム攻撃を仕掛けてくる攻撃者は、要求した身代金を支払う能力があり、かつ攻撃できるような脆弱性を持っていると判断した企業を攻撃対象として選定していると推測される。そのため、ランサム攻撃は、業種や規模に関係なく、どの企業も攻撃対象になり得る脅威である。

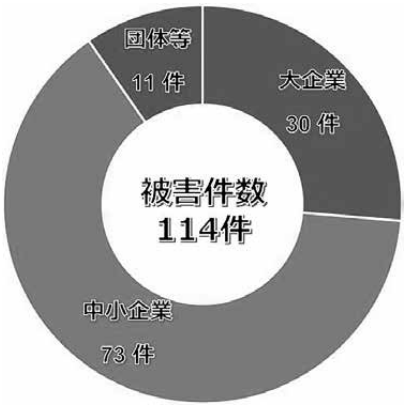

図 6　被害企業規模別件数

2. 4　ランサムウエアの感染経路

本節では、前項までに解説してきたランサムウエア攻撃がどのような経路で攻撃されているかを、統計情報から解説する。図 7 は、2024 年上半期にランサムウエア被害の報告をした 114 件のうち、感染経路について回答が得られた 47 件のグラフである。ランサムウエア感染は、公開サーバーや VPN 装置などのインターネットと接続している機器を通じて不正接続されるケースが多い。図 7 の通り、被害を受けた企業の多くは、インターネットに接続している VPN 装置やリモートデスクトップ接続から侵入されたことが確認されている。VPN 装置に認

証回避を許してしまう脆弱性があった、簡単なユーザ ID とパスワードで認証を突破できる状態だったなど、運用上で不備があったことがこれらの被害の原因である。

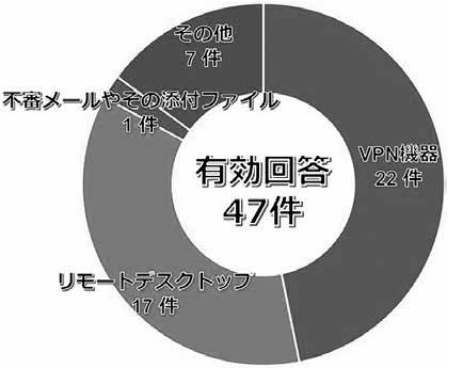

図 7　ランサムウエア感染経路

しかし、被害を受けた企業がセキュリティ対策を実施していなかったわけではない。次章で、被害企業の実態として、各企業のセキュリティ対策の状況と、被害要因を考察する。

3.　被害企業の実態

本章では、2 章でも紹介した「サイバー空間をめぐる脅威の情勢等について」にて公開されている被害企業の統計情報を用いて、被害企業の実態を考察する。

3. 1　被害企業のセキュリティ対策状況

2 章で、多くの被害が発生していることを解説してきたが、被害を受けた企業がセキュリティ対策を実施していなかったわけではない。

ランサムウエアの感染経路は、VPN 装置からの不正侵入が多かった。一方で、図 8 のグラフの通り、被害を受けた企業の半数が、侵入経路とされる機器に最新のセキュリティパッチを適用していることが分かる。

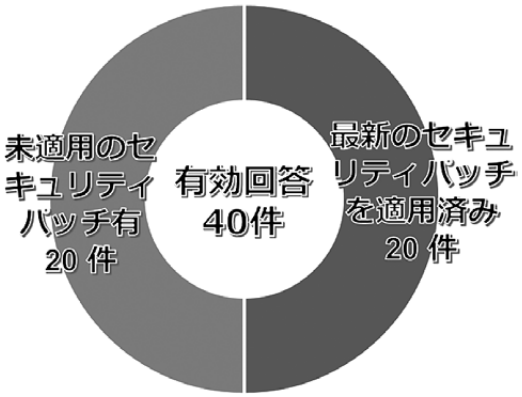

図 8　侵入経路とされる機器のセキュリティパッチ適用状況

また、図9の通り、ほとんどの企業でウイルス対策ソフトを導入しているという回答もある。多くの企業は、それぞれできる範囲でセキュリティ対策を実施していると考えられる。

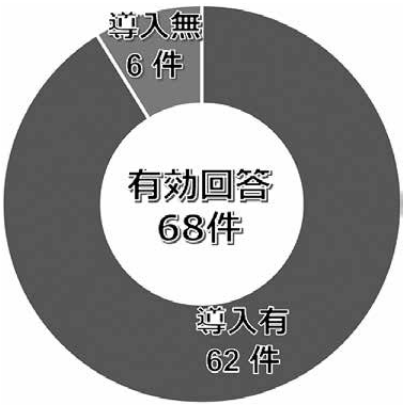

図9　ウイルス対策ソフト等の導入

ランサムウエア攻撃を仕掛けてくる攻撃者は、攻撃手法を進化させ、企業が実施するセキュリティ対策を回避する新たな手法や脆弱性を見つけて攻撃してきている。企業は被害を防ぐことの難しさを認識しなければならない。

3. 2　バックアップの取得とその効果

続いて、ランサムウエア攻撃への代表的な対策と考えられている、バックアップの実態を考察する。図10は、2024年上半期にランサムウエア被害の報告をした114件のうち、バックアップの取得有無について回答が得られた69件のグラフである。この結果から、約90%の企業で、バックアップが取得されていることが分かる。システムに対する被害はサイバー攻撃だけでなく故障もあり得る。その対策という意味も含めて、多くの企業が、バックアップを重要で必要不可欠なものと認識していると考えられる。

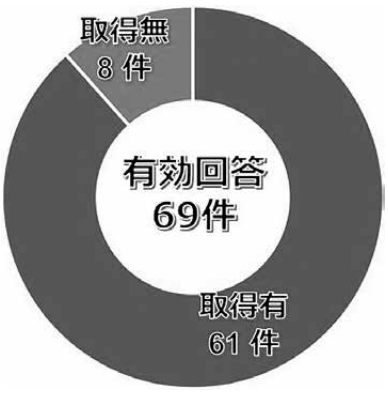

図10　バックアップの取得有無

一方で、図11の通り、ランサムウエア被害からの復旧に関しては、復旧できなかったと回

答する企業が75%となっており、半数以上が復旧できていない。復旧できなかった理由としては、ランサムウエアによってバックアップも暗号化されてしまったという回答が多い。ランサムウエア攻撃を仕掛ける攻撃者にとっては、バックアップからデータを復元されてしまっては身代金が得られない。そのため、攻撃者は最初にバックアップデータやバックアップシステムを攻撃する。

次に多い回答は、バックアップの運用不備である。過去のランサムウエア被害企業のインシデント対応支援のケースのうちいくつかで、バックアップは取得されていたものの、復旧手順資料が古いままで使い物にならなかったり、そもそも復旧の方法が分からなかったりすることがあった。さらに、バックアップデータでの復旧手順はわかっていても、取得したバックアップがデータ部分の差分バックアップのみで、ランサムウエア攻撃の被害を受けた後、システムをゼロから作り直す復旧プランが検討されていなかった例もある。

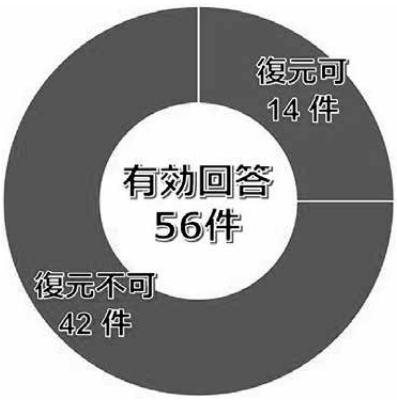

図 11　バックアップからの復旧結果

このように、多くの企業がバックアップの必要性を認識し、バックアップを取得しているものの、ランサムウエア攻撃への対策としては不十分な結果となっている。これは、ランサムウエア攻撃を受けるという前提でバックアップの設計や復旧プランの検討を実施していないためと考えられる。企業は、取得しているシステムのバックアップが、ランサムウエア攻撃の被害にあった際に復旧できるものとなっているか確認すべきである。

4.　サイバーレジリエンスの必要性

2章および3章で、ランサム攻撃の動向と企業の対策状況を解説してきた。このように攻撃が防げない状況に対して、いま、企業に求められるセキュリティ対策の考え方が、「攻撃を受けることを前提とした回復力」である。本章では、この回復力を考察すると共に、サイバーレジリエンスの定義とその強化策について解説する。

4. 1　回復力とは

回復力とは、一般的に「傷などを治し健康を取り戻す力」を指す。回復力という言葉の意味だけを考えれば、ランサムウエア攻撃における回復力はランサムウエア攻撃の被害を受けたシステムを正常な状態に戻すことであり、バックアップから復旧することという意味に取れる。

しかし、ランサムウエア攻撃の被害を受けた企業が本当に求めているのは、システムを回復させることではなく、事業を正常な状態に戻すことである。つまり、被害を受けたシステムをバックアップから復旧させることだけが回復力の目的ではない。一方でレジリエンスは、端的に言えば「回復力」を英語にした単語である。進化するサイバー攻撃に対応する対策として、サイバーレジリエンスという言葉が注目されている。

4. 2　サイバーレジリエンスとは

サイバーレジリエンスとは、サイバー攻撃やシステム障害などのリスクに対して、組織が迅速に回復し、事業活動を継続する対策を指す。セキュリティにおいて 100％安全な状態ということは実現不可能なため、セキュリティ対策をすり抜けて攻撃を受ける前提での対応策が企業には求められる。これまで多くの企業で実践されてきたサイバーセキュリティが、サイバー攻撃に対してどのようにシステムを守るのかという予防的な措置に主眼を置いた対策であったのに対して、サイバーレジリエンスは、万が一のサイバー攻撃や障害後に迅速に復旧し、事業を継続することに重点を置いた対策である。

サイバーレジリエンスに関して、米国国立標準技術研究所、通称 NIST（ニスト：National Institute of Standards and Technology）が発行している SP800-160 Vol.2, Rev.1 サイバーレジリエントなシステムの開発：システムセキュリティエンジニアリングアプローチ[4]というガイドラインがある。このガイドラインは、政府や民間組織が IT セキュリティ対策を行う際の参考になる。次節でこの SP800-160 Vol.2, Rev.1 について解説する。

4. 3　NIST SP800-160 Vol.2, Rev.1 によるサイバーレジリエンスの定義

本ガイドラインによると、サイバーレジリエンスとは、「サイバー資源を有するシステムが、困難な状況下、ストレス下、攻撃下にある、もしくは侵害されている状態に陥ったとしても、それを予測し、それに耐えて（抵抗）、そこから回復し、それに適応できる能力」と定義されている。この定義にあるように、予測、抵抗、回復、適応の各能力を向上することが、サイバーレジリエンス向上のカギになる。本節ではそれぞれの能力について解説する。

4. 3. 1　予測力

予測力とは、セキュリティインシデントを予測し備える能力である。セキュリティインシデントの発生を予測するだけではなく、インシデントがシステムに与える影響やリスクを評価し、適切な対策を準備することを指す。予測力を向上するためには、主に以下のような作業が求められる。

1）情報資産の整理
守るべき対象となる情報資産（データ、パソコンやサーバーなどのシステム、ネットワーク機器、セキュリティ装置など）を洗い出す。

2）情報資産に対する脆弱性やリスクの可視化
脆弱性診断やリスクアセスメントを実施し、守るべき対象となる情報資産が持つ脆弱性を洗い出し、対策を検討する。

3）脅威インテリジェンスやアタックサーフェスマネジメント（ASM）の活用
攻撃者の動向や攻撃手法、脆弱性に関する情報を収集する。また、ASM を活用することで、組織のネットワーク、システム、アプリケーション、デバイスなど、脆弱な領域（アタックサーフェス）を把握する。

4）対応計画の策定
インシデントが発生することを想定した、事業継続計画（BCP：ビジネスコンティニュティプラン）や、緊急時対応計画（コンティンジェンシープラン）を策定する。

5）対応体制の整備
対応計画を実行するための体制を整備する。具体的には、情報セキュリティ委員会、リスク対策委員会、CSIRT（Computer Security Incident Response Team）、SOC（Security Operations Center）などを構築する。

4. 3. 2　抵抗力

抵抗力とは、攻撃の防御もしくは被害を局所化して事業を継続する能力である。セキュリティソリューションの導入や、システムの堅牢化による防御力の強化や、インシデントの早期検知の仕組みがこれに該当する。抵抗力を向上するためには、主に以下のような作業が求められる。

1）セキュリティソリューションの導入
次世代型エンドポイントソリューション（NGAV：Next Generation Anti-Virus, EDR：Endpoint Detection and Response など）の導入やネットワークセキュリティソリューションとの相関分析である XDR（Extended Detection and Response）などによって、サイバー攻撃の早期検知や防御を強化する。

2）ネットワークの堅牢化
ネットワークゾーニングやマイクロセグメンテーションの組み合わせにより、セグメントをできる限り分割し、必要最小限のアクセスのみ許可することで、攻撃を受けた際に被害の範囲を局所化する。

3）サーバーやパソコンの堅牢化
定期的なパッチ適用、不要なサービスの無効化、必要最小限のアクセス制限、多要素認証による強固なアカウント管理などの対策を実施する。

4. 3. 3　回復力

回復力とは、迅速なシステムの復旧、業務機能を回復させて事業を再開する能力である。単にバックアップから復旧（リストア）するというだけでなく、サイバー攻撃の原因を特定し、それを封じ込める対応も含まれる。これは、封じ込めをしないままリストアしたとしても、再度同じ攻撃を受ける可能性が残っている場合、回復したとは言い難いためである。回復力を向上するためには、主に以下のような作業が求められる。

1）インシデントの原因特定および封じ込め手法の整備
インシデントの発生原因を特定する方法を確立する。システムやネットワーク機器、セキュリティソリューションのログ分析手法の整備や、関係者からヒアリングするためのポイントを事前に整理しておく。インシデント発生時は、その原因を取り除くことで、再発を防止する。原因を取り除く方法として、ネットワークの遮断や分離、パッチ適用による脆弱性の修正、パスワードの変更やアカウントの停止などが挙げられる。

2）バックアップからのリストアやシステムの再構築の準備
システムのバックアップを用いて、システムをリストアするための手順を準備する。ただし、ランサムウエア攻撃によってバックアップファイルが暗号化されてしまう可能性を考慮し、ランサムウエア対策となるバックアップ設計や専用ツールの選定が求められる。また、バックアップからの復旧が困難であることも考慮し、システムの再構築手順も準備すべきである。

4. 3. 4　適応力

適応力とは、インシデントの再発防止、予測される脅威の変化に応じた業務機能を改善する能力である。利用期間の経過とともに、システムには新たな脆弱性が発見され、ハードウエアの劣化やサポート切れも発生する。各能力は、インシデントの予測に連動して強化していくことになるが、強化した能力は継続的に維持、改善していかなければならない。適応力を向上するためには、主に以下のような作業が求められる。

1）インシデント原因の根絶
インシデントの発生を想定して、劣化したシステムの入れ替えや、脆弱性を持つ古い機器を廃止するなどの措置を取る。

2）セキュリティポリシーや対応手順の見直し
内外の環境変化やサイバー攻撃の進化に応じた、セキュリティ対応ルール（ポリシー）や対応手順を定期的に見直し、改善する。

3）役職員のセキュリティ教育とセキュリティ人材の育成
役職員の役割に応じたセキュリティ教育を実施する。セキュリティ教育は、一般的なセキュリティ知識の習得や標的型攻撃訓練によるリテラシーの向上だけでなく、組織のセキュリティポリシーの理解度の確認をするも重要となる。また、すべてのセキュリティ対策を実行していくための人材を育成していくことも求められる。

4. 4　サイバーレジリエンス向上の考え方

前節でサイバーレジリエンスの定義と各能力向上のポイントを解説してきたが、実際にはリソースやコストに限りがあるため、すべての能力を均等に強化することは難しい。そのため、優先順位をつけて対応しなければならない。対応の優先順位の決め方に関しては、組織の方針や環境、内外からの要求事項など、様々な検討要素があるものの、基本的な考え方として、事

業への影響が大きいシステムへの強化を優先するべきである。セキュリティ強化、サイバーレジリエンスの向上はあくまで手段であり、目的は組織の運営や事業の継続性を確保することである。だからこそ、サイバー攻撃などでシステムが停止した場合、事業を継続する上で一番影響が大きいシステムから優先的に対策を実施していくべきである。また、システムを活用すること自体が組織運営や顧客とのやり取りを効率的に実現するための手段であるということも認識すべきである。事業への影響を最小限にするためには、システムが停止している状況においても、事業を継続できるよう準備をしておくということも、サイバーレジリエンスの能力である予測力の強化手法の一つである。

対策を実施した後の準備の過不足についても、いくつかの手法が考えられる。その一つに、ランサムウエア被害が発生したことを仮定して、机上で逆算してみる方法がある。対策を実施したシステムに対してランサムウエア被害が発生した際、まずは被害の拡大を防止するために、ネットワークの遮断などによる初期封じ込めが求められるが、その手法が確立されているか、そして、そのシステムに対しての侵入経路を特定するために、ネットワーク図やシステム構成図、システムログが見られる状況であるかといったように、事前にシミュレーションすることで課題を発見できる。この時に特に注意すべきなのは、ランサムウエア被害を受けた場合、パソコンやファイルサーバーが使えない可能性があるということである。ペーパーレスの時代ではあるが、ネットワーク図やシステム構成図に関しては、印刷してファイリングしておくことも、サイバーレジリエンスの向上策になる。

5. BIPROGY グループが提供するセキュリティソリューション

本章では、前章で解説したサイバーレジリエンスの各能力を向上するために、BIPROGY グループが提供するセキュリティソリューションおよびサービスを紹介する。

5.1 サイバーセキュリティソリューション

BIPROGY グループはマルチベンダーを強みとして、製品の縛りなく様々なセキュリティソリューションを提供している。本節では、BIPROGY グループのソリューション提供の考え方を紹介する。図 12 で示すように、サイバーセキュリティにおける対策領域を構造化し、顧客環境のセキュリティ強化のための様々なセキュリティソリューションを、最適な組み合わせで、導入後の運用面のサービスも含めて提案している。

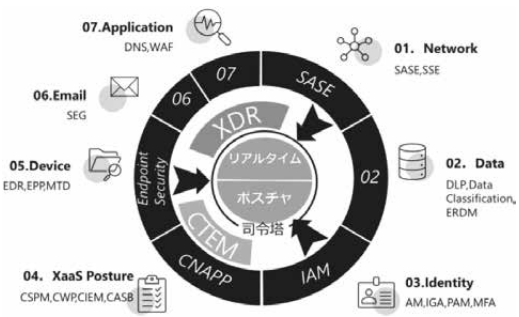

図 12　サイバーセキュリティー・メッシュ・アーキテクチャ

5. 2　サイバーセキュリティサービス

続いて、BIPROGY グループが提供するサイバーセキュリティサービスを紹介する。図 13 で示したアセスメント、インシデント対応態勢強化支援、情報セキュリティポリシー策定支援、脆弱性診断は、iSECURE サイバーセキュリティサービスの中での主要なサービスである。さらに、顧客の要望に応じて、個別のコンサルティングサービスも提供している。なお、iSECURE（アイセキュア）は、BIPROGY グループのセキュリティサービスブランドである。

アセスメントや脆弱性診断によって、予測力に求められる組織やシステムに対するリスクの評価、課題の可視化、対策不足の箇所を洗い出せる。インシデント対応態勢強化支援では、サイバーレジリエンス向上の要となるインシデント対応組織、所謂 CSIRT の構築をすることで、回復力強化を支援する。情報セキュリティポリシー策定支援では、ポリシーの見直しや適合性をチェックし、適応力の強化を支援する。

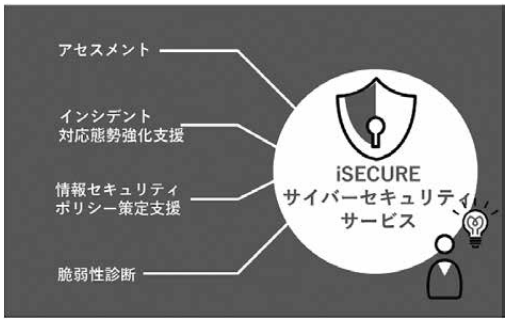

図 13　iSECURE サイバーセキュリティサービス

5. 3　マネージドセキュリティーサービス（CloudPas MSS）

BIPROGY グループでは、CloudPas MSS という名称で、マネージドセキュリティーサービス（MSS）を提供している。CloudPas MSS は、図 14 の通り、幅広いサービスを提供しており、サイバーレジリエンスにおける、すべての能力向上に貢献する。

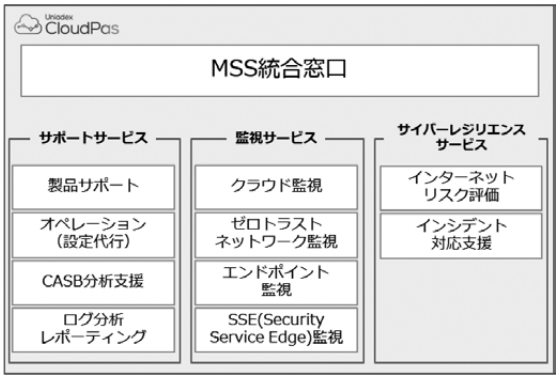

図 14　CloudPas MSS サービスメニュー

表 2 に各サービスメニューの概要を示す。CloudPas MSS は、様々なセキュリティソリュー

ションのサポートや監視を提供するだけでなく、継続的なセキュリティ対策の評価やインシデント発生時の初動対応を支援するサイバーレジリエンスサービスもオプションとして提供している。これら複数のメニューを MSS 統合窓口でワンストップに対応することも CloudPas MSS の特徴であり、顧客のセキュリティ運用の煩雑さを軽減できる。

表 2　CloudPas MSS　サービス概要

カテゴリ	概　　要
サポートサービス	セキュリティ商材の技術的な支援・設定代行、障害発生時の支援および定期的なログのレポーティングなどを行うサービス。
監視サービス	クラウド、エンドポイント、ゼロトラストネットワークの監視を行いアラートの通知と対策の提示および監視状況の定期レポーティングなどを行うサービス。
サイバーレジリエンスサービス	監視サービスのオプションサービス。セキュリティ対策状況の確認と評価およびインシデント対応計画の作成支援、およびインシデント発生時の初動対応などを実施するサービス。

6. お　わ　り　に

本稿は、2024 年 6 月に開催された BIPROGY FORUM 2024 セミナー「いま、セキュリティ強化に求められる回復力　～事業継続性を意識した『サイバーレジリエンス』向上のカギ～」で講演した内容をベースとして、最新のセキュリティ被害状況を再整理し、事業継続を意識した「サイバーレジリエンス向上」をキーワードとして記述したものである。サイバー攻撃は、基本的に攻撃者が優位であり、セキュリティインシデントを完全に防ぐことが困難であるという認識を持ち、サイバーレジリエンス向上をサイバー攻撃への対策方針として取り入れる一助になれば幸いである。

参考文献
［1］ 情報セキュリティ 10 大脅威 2025［組織編］，独立行政法人情報処理推進機構，2025 年 1 月 30 日，
https://www.ipa.go.jp/security/10threats/10threats2025.html
［2］ 令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について，警察庁，2024 年 9 月 19 日，
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf
［3］ 情報セキュリティ 10 大脅威 2025［組織編］解説書，独立行政法人情報処理推進機構，2025 年 2 月 28 日，
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf
［4］ NIST SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach，米国国立標準技術研究所，2021 年 12 月，
https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

※　上記参考文献に含まれる URL のリンク先は、2025 年 4 月 17 日時点での存在を確認。

執筆者紹介　佐　藤　重　之（Shigeyuki Sato）

2016年日本ユニシス(株)入社。前職のシステムインテグレータでは、主にネットワークセキュリティ製品の提案・設計・構築・運用支援対応に従事。2024年度よりユニアデックスに出向。現職は主にセキュリティコンサルティングサービスに従事。BIPROGYグループCSIRT（セキュリティインシデント対応チーム）メンバー。CISSP。情報処理安全確保支援士（登録番号第001924号）。