IDC TECHNOLOGY SPOTLIGHT

IBM が提供するサイバー・レジリエンシー・サービス：サイバーレジリエンシー向上による事業継続の実現

June 2019

登坂 恒夫

『*2019 年 国内情報セキュリティユーザー調査：企業における対策の現状*（IDC #JPJ44004519、2019 年 6 月発行）』を基に作成

Sponsored by 日本アイ・ビー・エム

マルウェアに感染したコンピューター内にあるファイルを暗号化して IT システムを人質に取り、身代金を要求するランサムウェアの出現によって、情報セキュリティ被害は、IT システムの停止や破壊といった深刻な事態にまで拡大し、サイバーセキュリティリスクが高まっている。またサイバー攻撃は、人をだます巧妙な手口によって IT システムに侵入し、機密情報の搾取や重要システムの乗っ取りなどの目的を果たすまで長期に渡って継続的に諜報活動を行う標的型攻撃へと変化している。このような状況下では、セキュリティ被害を最小限に留め早期の復旧が行えるリスク管理プロセスに応じた体制が求められる。そのためには、リスクベースの考え方に基づいたサイバーセキュリティフレームワークを活用したセキュリティ侵害の対応プロセスを可視化し、対処する必要がある。

本調査レポートでは、IDC が 2019 年 4 月に実施した「国内ユーザー企業におけるセキュリティの現状」の調査を基にサイバーセキュリティフレームワークの採用状況および事業継続性を考慮したセキュリティ対策の状況を分析し、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）のリスクベースの考え方に基づいたサイバーセキュリティフレームワーク（CSF：Cyber Security Framework）の活用によるセキュリティ対策、事業継続対策の有効性を検証する。

上記の IDC 調査では、企業と官公庁組織から 829 の有効回答を得ており、産業分野については官公庁を含む 14 業種、企業規模については従業員数 9 人以下の小規模企業／組織から 3,000 人以上の大規模企業／組織までを 8 セグメントに分けている。回答者は情報システム部門およびセキュリティ関連の役職者が中心である。

サイバーレジリエンシーとサイバーセキュリティフレームワーク

サイバーレジリエンシーとは

2013 年 2 月に米国で公布された大統領政策指令第 21 号の「重要インフラのセキュリティおよびレジリエンシー」において、「レジリエンシー（レジリエンス）」とは、「変化する状況に備え、それに適応し、混乱に耐えて迅速に回復する能力を意味する。レジリエンシーには、意図的な攻撃、事故、あるいは自然に発生する脅威や事件に耐え、回復する能力が含まれる」と定義している。サイバー攻撃は、標的対象の組織や個人を特定し執拗かつ継続的に偵察活動を行って機密情報の搾取などの目的を遂行する APT（Advanced Persistent Threat）攻撃など高度化しており、完全に排除するのは困難な状況になっている。高度化するサイバー攻撃へのセキュリティ対策では、自然災害と同様に、不測の事態が発生した場合でも、迅速に回復することが求められる。

サイバーセキュリティフレームワーク

セキュリティフレームワークとしては、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）の国際規格の ISO/IEC27001、NIST CSF、米国 CIS（Center for Internet Security）が公開した CIS Controls（旧称 SANS Top20 Critical Security Controls）などがあ

る。IDC が 2019 年 4 月に実施したユーザー調査では、従業員規模 1,000 人以上の企業においては、ISO/IEC27001 を採用している企業が 52.3%と最も多く、2014 年 2 月に NIST が発表した CSF を採用している企業は 36.2%に留まっていることが分かった。ISO/IEC27001 のセキュリティフレームワークは、情報資産の保護に重点を置き、「機密性」「完全性」「可用性」の 3 つの要素で情報資産の重要性を定義し、重要度に応じて対策を講じるため、こうした情報資産の保護に重点を置く国内企業で採用が浸透した。

一方、NIST CSF は、プライバシーリスクを含めたサイバーセキュリティリスクを管理するためのリスクベースのアプローチであり、「フレームワークコア」と「フレームワークインプリメンテーションティア」「フレームワークプロファイル」の 3 つの要素で構成される。フレームワークコアは、「特定（Identify）」「防御（Protect）」「検知（Detect）」「対応（Respond）」「復旧（Recover）」の 5 つの機能で構成される。フレームワークインプリメンテーションティアは、フレームワークコアと、組織のサイバーセキュリティリスク管理がどの程度実践されているかを 4 段階で示すものである。そしてフレームワークプロファイルは、フレームワークコアが示す基準、ガイドライン、プラクティスについてビジネスニーズ別の期待される成果を示すものである。2018 年 4 月にバージョン 1.1 が公開され、サプライチェーンに対するサイバーセキュリティリスク管理の要求事項が明記された。

NIST CSF 採用の必要性

米国では、政府調達に関わる政府以外の企業や組織に対して、2010 年 11 月の大統領令（Executive Order 13556）によって定義された管理すべき重要情報（CUI：Controlled Unclassified Information）を管理するシステムを構築するためのガイドライン「NIST SP800-171」が、2015 年 6 月に策定された。NIST SP800-171 は NIST CSF に準拠しており、サプライチェーンに対する適用も求められているため、米国政府調達関連企業と取り引きのある日本企業でも NIST CSF 基準に沿った対応が求められる。また、2011 年 12 月に発表された米国連邦政府共通のクラウドサービス調達のためのセキュリティ基準の認証管理プログラム「FedRAMP（Federal Risk and Authorization Management Program）」についても、クラウドサービスプロバイダーに対する認証管理プログラムであり、NIST CSF に準拠した対応が求められている。

EU 圏においては、2016 年 8 月にネットワークおよび情報システム指令（NIS 指令）が発効され、2018 年 5 月に GDPR 施行と共に国内法制化が始まった。NIS 指令は、重要インフラとクラウドサービスプロバイダーに対して、セキュリティレベルおよびレジリエンシー（回復力）の向上を求めており、NIST CSF と同じ考えを示している。

このように欧米においては、リスクの特定から防御／検知／対応／復旧までサイバーセキュリティリスク管理プロセスを示したセキュリティフレームワークを採用しており、これに準拠する NIST CSF が国際標準になりつつある。

国内では、経済産業省が策定した「サイバーセキュリティ経営ガイドライン Ver 2.0」（2017 年 11 月に発表された改訂版）において、セキュリティ侵害を最小限に抑えたレジリエンシー（回復力）の向上が求められている。今後国内企業においても、NIST CSF への準拠を求められるケースが多くなるとみられ、NIST CSF 採用の必要性が高まると考える。

セキュリティ被害の現状

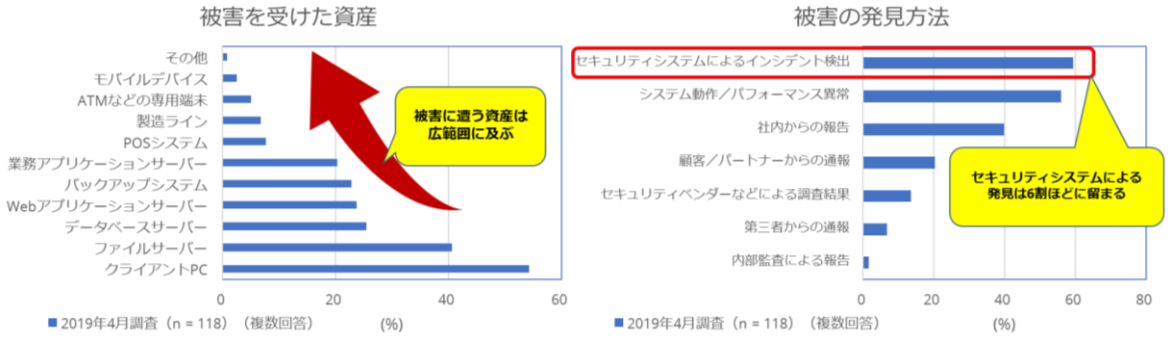
セキュリティ被害状況

IDC が 2019 年 4 月に実施したユーザー調査のセキュリティ被害に関する調査結果を Figure 1 に示す。セキュリティ被害を受けた資産については、PC やサーバーばかりでなく、POS（Point of Sale）や ATM（現金自動預払機）などの産業専用機器、製造ラインにも及んでいる。また、セキュリティシステムによる被害の発見率は 6 割ほどに留まっており、社内の報告や顧客／パートナーからの通報などによってセキュリティ被害が表面化した時点で発覚するケースも 2〜4 割程度ある。

サイバー攻撃によるセキュリティ被害は、PC やサーバーといった IT 資産から産業用機器や製造ラインまで広範囲に及んでおり、被害が重大化する恐れがある。また、本調査レポートでは詳細な結果については掲載していないが、セキュリティ被害を受けた企業の 2 割でバックアップシステムが被害を受けており、事業継続という観点からセキュリティ対策の見直しが必要であることを示している。さらに、多層防御のマルウェア検出技術を備えたセキュリティシステムが一般的に活用されている状況ではあっても、セキュリティシステムですべての被害を発見することは難しく、被害が表面化した時点でいかに迅速に対処し、復旧させるかが、より重要となっている。

Figure 1

セキュリティ被害状況



Note: 『*2019 年 国内情報セキュリティユーザー調査：企業における対策の現状*（IDC #JPJ44004519、2019 年 6 月発行）』を基に作成

Source: IDC Japan, June 2019

高度化するサイバー攻撃への対策

国境を越えて行われる高度なサイバー攻撃は、人間の心理的な隙や盲点を突く高度なソーシャルエンジニアリングを活用し、標的とする組織を攻撃する。高度なサイバー攻撃で使われるマルウェアは、身代金要求型のランサムウェアや実行ファイルを持たないファイルレスマルウェアなどの登場で巧妙化している。特にランサムウェアは、システム全体のファイルを暗号化するなどして、システムを使用不能な状態にして身代金を要求するため、事業継続に深刻な影響を及ぼす。

IDC が 2019 年 4 月に実施したユーザー調査のセキュリティ被害に関する調査によると、国内では、この 1 年間でセキュリティ被害に遭った国内企業の 56.8%がランサムウェア攻撃の被害に遭っている。そして、ランサムウェア攻撃の被害を受けた企業の 46.2%はバックアップファイルからの復旧またはシステムの再インストールで復旧している。

海外では、2018 年 3 月に米アトランタ市で大規模なランサムウェア攻撃が発生し、行政サービスに深刻な被害を与えた。この攻撃でアトランタ市の基幹システムを支えるソフトウェアの 3 分の 1 が被害を受け、被害からの復旧は難航し、最終的な被害総額は身代金の要求額（5 万 1,000 米ドル）を大幅に超える 1,700 万米ドルにも上ると報告されている。

アトランタ市の攻撃で使われたランサムウェア「SamSam」は、標的型攻撃を仕掛ける攻撃者がシステムに侵入後、偵察活動を行った上で、ランサムウェアを配備し最終段階で実行されるため、暗号化が広範囲に及び、甚大な被害となる。SamSam の攻撃は、サーバーの脆弱性を突いたり、RDP（Remote Desktop Protocol）に対する総当たり攻撃などでシステムに侵入し、ハッキングツールなどでドメイン管理者の権限を取得し、システムにアクセスしてランサムウェアを配備する。このような標的型ランサムウェア攻撃を完全に排除することは困難なため、以下のようなリスクを低減させるための対策を行う必要がある。

- **リスクの特定**：現状の情報資産と脆弱性を把握し、デバイスや OS、アプリケーションソフトに対する早期のパッチ適用を行う。また、RDP へのアクセス制限などシステム設定で脆弱な点を見直す。

- **マルウェア侵入を早期に検知し対処する最新テクノロジーの導入**：アクセスユーザー、アプリケーション、通信などの挙動を分析し、マルウェアによる不正な振る舞いを検知、対処する、シグネチャレス型のマルウェア検出テクノロジーを採用した製品を導入する。

- **システムのバックアップおよびリカバリー**：被害を受けた OS やアプリケーション、データを迅速に復旧させるために、バックアップからのリカバリーが有効である。

NIST CSF に基づいた新たな事業継続体制

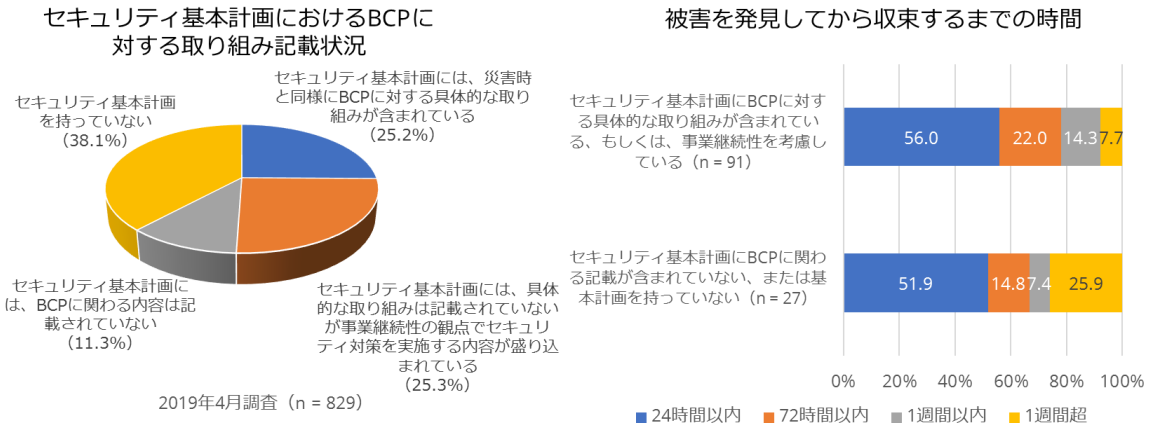
IDC が 2019 年 4 月に実施したユーザー調査で明らかになったセキュリティ基本計画における事業継続計画（BCP：Business Continuity Planning）の記載状況と被害の収束時間の関係についての調査結果を Figure 2 に示す。セキュリティ基本計画に、復旧までの目標日数など BCP に対する具体的な取り組みが含まれている企業は 25.2%に留まる。具体的な取り組みは記載していないが、事業継続性の観点からセキュリティ対策を実施する内容を盛り込んでいる企業を含めると、半数の企業では、事業継続性を考慮したセキュリティ基本計画が策定されている。しかし、残りの半数の企業は、事業継続性を考慮したセキュリティ基本計画を持っておらず、リスク管理が不十分である。

また、セキュリティ基本計画における BCP の記載状況を採用しているセキュリティフレームワーク別で分析すると、事業継続性を考慮したセキュリティ基本計画を策定している企業の割合が最も高かったのは、NIST CSF を採用している企業で 94.5%であった。次いで ISO/IEC27001 を採用している企業で 89.0%である。また、被害を発見してからの収束時間との相関を分析すると、事業継続性を考慮したセキュリティ基本計画を策定している企業の 78.0%が 72 時間以内に収束させているが、事業継続性を考慮した基本計画を持っていない企業では 66.7%である。また、収束時間が 1 週間超と長期間に渡った企業の割合は、事業継続性を考慮したセキュリティ基本計画を策定している企業で 7.7%であり、事業継続性を考慮した基本計画を持っていない企業の 25.9%と比較すると非常に少ない。

この分析から、事業継続性を考慮したセキュリティ基本計画を策定している企業は、セキュリティ被害に遭っても迅速に対処、復旧できており、NIST CSF に基づいた事業継続体制を整えることが有効な手段であると考えられる。

Figure 2

セキュリティ基本計画における BCP の記載状況と被害の収束時間の関係



Note: 『*2019 年 国内情報セキュリティユーザー調査：企業における対策の現状*（IDC #JPJ44004519、2019 年 6 月発行）』を基に作成

Source: IDC Japan, June 2019

IBM サイバー・レジリエンシー・ソリューション

IBM のサイバー・レジリエンシー戦略

IBM が考える「サイバー・レジリエンシー」は、NIST CSF に基づいたサイバーセキュリティとサイバーレジリエンシーの融合である。サイバーセキュリティは、システム、ネットワーク、データをサイバー犯罪から守り、不測の事態に備えて初動対応を行えるように技術、プロセス、対応を検討、実装し、サイバー攻撃のリスクを軽減し、企業／組織／個人を保護することを目的とするものである。また、サイバー・レジリエンシーは、サイバーセキュリティの実装に加え、レジリエンシーの観点からビジネスの継続に視野を広げ、企業が考えるべき BCP におけるリスクの想定にサイバーリスクも考慮し、ビジネスに対するインパクトの把握、復旧目標の設定と対策の立案、実装、定期的な検証を行うことを目標とするものである。同社は、サイバー・レジリエンシーを実現するために、セキュリティ対策に加え、リカバリー対策も取り入れて、現状の正しい把握からレジリエントなシステムの実装までの支援を提供している。

IBM サイバー・レジリエンシー・ソリューション

IBM サイバー・レジリエンシー・ソリューションは、NIST CSF に基づき、NIST CSF で定義している「Identify（立案する）」「Protect（防御する）」「Detect（検知する）」「Respond（対応する）」「Recover（復旧する）」の 5 つの各局面で、サイバーセキュリティにレジリエンシーの要素を補い、局面ごとに自組織の状況を正しく理解、改善することを支援する。このソリューションは、有事の際の迅速／確実な復旧につながるものである。

同ソリューションは、「ビジネス・レジリエンシー・ソリューション」と、「セキュリティ・アセスメント」を含む「セキュリティソリューション」で構成される。

「ビジネス・レジリエンシー・ソリューション」には、以下のソリューションが含まれる。

- **IBM レジリエンシー：コンサルティング**：「サイバー・レジリエンシー・成熟度診断」を含む、サイバー・レジリエンシーの実装支援コンサルティング
  - **サイバー・レジリエンシー・成熟度診断**：NIST CSF に関するフレームワークの 23 分野 108 項目に基づき、ユーザーの状況と将来目指すべき姿を 5 段階評価で客観的に分析する。
- **IBM レジリエンシー・オーケストレーション**：サイバー攻撃向け機能としては、「プラットフォーム構成用の サイバー・インシデント・リカバリー」（ネットワーク機器やサーバーの設定が変更されることを検知し、元の構成情報に戻す機能）と「データ用のサイバー・インシデント・リカバリー」（バックアップデータも攻撃の対象となり、削除、変更されることがないように追記不可の環境にデータを退避し、復旧させる機能）がある。
  - **プラットフォーム構成用のサイバー・インシデント・リカバリー**：サーバーやデバイス構成データのマスターコピーデータである「ゴールデン・コピー」を、「クラウド・オブジェクト・ストレージ」または「IBM データ・センター」にエアギャップで保護された「イミュータブル・ストレージ」（不変ストレージ）に複製することで、短時間でサービス回復を行う。本番稼働デバイスは検証され、構成データに加えられた変更が検出される。システムは変更を分析し、 その変更が適切なものであるかどうかを判別し、構成データに疑わしい変更が検出されるとアラートを出す。
  - **データ用のサイバー・インシデント・リカバリー**：エアギャップによる保護および「イミュータブル・ストレージ」（不変ストレージ）を使用することでデータを保護しながら、適切なデータを用いてユーザーの DR サイト（代替サイト）で迅速に復旧する。これによってデータそのものを破壊するサイバー攻撃に対し、信頼性の高い、短時間での復旧を実現する。
- **IBM Resiliency as a Service**：クラウドによるシステムリカバリーとデータバックアップ

「プラットフォーム構成用のサイバー・インシデント・リカバリー」と「データ用のサイバー・インシデント・リカバリー」といった「サイバー・インシデント・リカバリー」は、「コピー・

データ管理テクノロジー」を採用し、データの増分ポイント・イン・タイム（PIT）コピーを作成して保持する。クラウド・オブジェクト・ストレージまたはWORM（write only, read many）ストレージなどの「イミュータブル・ストレージ」（不変ストレージ）に保持されるこれらのコピーは、変更ができない「永久」コピーであり、コピー・データ管理ソフトウェアは、データをDRサイトに複製し、ポイント・イン・タイム（PIT）コピーを作成する。またオプションで、ポイント・イン・タイム（PIT）コピーを本番サイトに保管することで、迅速な復旧もできる。

IBMが提供する「サイバー・レジリエンシー・ソリューション」は、これらの「サイバー・インシデント・リカバリー」によって、サイバー攻撃から短時間で復旧を可能にする、信頼性が高く拡張が容易なソリューションである。この「サイバー・インシデント・リカバリー」の復旧機能によって、データおよびITプラットフォームを保護し、サイバー・レジリエンシー向上による事業継続の実現を可能にする。

IBMの課題

2019年4月にIDCが実施したユーザー調査では、従業員規模1,000人以上の企業の半数以上が防御対策を主体とするISMSのISO/IEC27001のセキュリティフレームワークを採用しており、リスク管理プロセスを通じて優先順位を付けてサイバーセキュリティ対策が行えるNIST CSFの採用は3割超に留まる。こうした国内企業の現状に対して、高度化するサイバー攻撃の新たな対策として、従来の防御中心のセキュリティ対策に加え、事後対応から復旧に至るまで事業継続性を考慮したサイバーセキュリティフレームワークの国際標準化が進んでいる。これを踏まえると、IBMは国内の企業や組織に向けて、事業継続を考慮したサイバーセキュリティ対策の重要性を明示し、IBMサイバー・レジリエンシー・ソリューションが万一の不測の事態にも継続してビジネスを支援するために有効であることを、事例を含めて訴求する必要がある。

結論

「SamSam」のような標的型ランサムウェア攻撃は、攻撃者がシステムに侵入後、偵察活動を行った上で、ランサムウェアを配備し最終段階で実行するため、暗号化されるシステムが広範囲に及び、復号化できなければ膨大な量のデータを破棄しなければならず、バックアップシステムからの復元もしくはアプリケーションやOSを含めたシステムの再構築が必要となる。欧米では、このような高度なサイバー攻撃に備え、自然災害と同様に事業継続性を考慮し、被害発生後の迅速な対応や復旧をリスク管理プロセスによって行える、リスクベースのアプローチによるセキュリティフレームワークの導入が進んでいる。デジタルトランスフォーメーション（DX）が進展する社会において、データの流通は経済活動の重要な柱となっている。欧米とのビジネス交流を進める上で、サイバーセキュリティリスク管理への取り組みは必須である。

ユーザー企業や組織は、高度化するサイバー攻撃への備えとDXを進めるために、事後対応から復旧に至るまで事業継続性を考慮したリスクベースのアプローチによるセキュリティフレームワークの導入が重要であり、それを実現するためにNIST CSFを導入すべきである。

ただし、国内ではNIST CSFはまだ十分浸透していない。IBMの「サイバー・レジリエンシー・ソリューション」は、NIST CSFに則ったセキュリティソリューションであり、国内の企業や組織でNIST CSFの導入を浸透させる有効なソリューションの選択肢の一つとなり得るため、IBMにとっては、市場機会が大きいと考える。