2024年03月15日　技術情報

未来社会の脅威に対するサイバーレジリエンスの実装手法

#防災・レジリエンス　#セキュリティ　#デジタルソリューション

執筆者

米光 一也 (Yonemitsu Kazuya)

株式会社日立ソリューションズ セキュリティソリューション事業部 セキュリティサイバーレジリエンス本部 マネージドセキュリティサービス部 所属
現在，セキュリティコンサルティング業務，インシデントハンドリング業務などに従事

猪股 健一 (Inomata Kenichi)

株式会社日立ソリューションズ セキュリティソリューション事業部 セキュリティサイバーレジリエンス本部 マネージドセキュリティサービス部 所属
現在，マネージドセキュリティサービス事業，SIEM（Security Information and Event Management）事業，セキュリティ診断事業などに従事

清水 秀樹 (Shimizu Hideki)

株式会社日立ソリューションズ セキュリティソリューション事業部 セキュリティサイバーレジリエンス本部 セキュリティコンサルティング部 所属
現在，セキュリティコンサルティング業務に従事

ハイライト

世界的にサイバー攻撃の脅威が増大する中，近年，サイバーレジリエンスに注目が集まっている。サイバーレジリエンスとは，情報システムがサイバーを受けたとしても，それを予測し，抵抗し，素早く回復して適応する能力を備えることであり，それにより重要な事業の継続性を確保しようとするものである。

株式会社日立ソリューションズは，顧客企業のサイバーレジリエンス能力の向上に寄与するため，サイバーレジリエンスの能力を評価する具体的な手法を開発した。

本稿では，開発までのプロセス，および開発した手法の概要や，実証実験を通じて得たノウハウについてまとめる。

1. はじめに

世界的にサイバー攻撃の脅威が増大する中，サイバー攻撃による被害は，企業が想定すべき重大な経営リスクであるという認識が定着して久しい。これまで，多くの企業は，ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission） 27001認証の取得や，CSIRT（Computer Security Incident Response Team）の設立など，セキュリティインシデントへの対応能力の向上を図ることで被害に備えてきた。こうした中，近年，サイバーレジリエンスに注目が集まっている。サイバーレジリエンスとは，情報システムが，サイバー攻撃に対してそれを予測し，抵抗し，素早く回復して適応する能力を備えることである。このサイバーレジリエンス能力の向上により，企業は情報システムの可用性を維持し，重要な事業の継続性を高めることができる。

2. SP 800-160 Vol. 2 Rev. 1

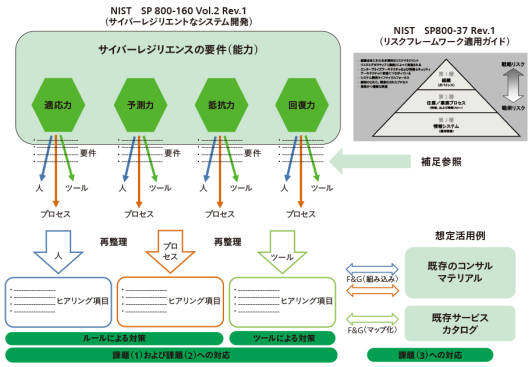
サイバーレジリエンスという言葉が世の中に広まるきっかけとして，SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach[1)] （以下，「SP800-160v2r1」と記す。）という文書の存在がある。SP800-160v2r1は，そのタイトルのとおり，サイバーレジリエントなシステムを開発するための，エンジニアリング観点でまとめられた文書であり，米国国立標準技術研究所が発行するSP800シリーズの一つである。SP800-160v2r1は，サイバーレジリエンスの能力の一面を「予測力」，「抵抗力」，「回復力」，「適応力」の四つと定義し，システムがそれぞれの能力を高めることを目的としたガイダンスであり，フレームワークの説明や，システムに対して求める具体的な要件が整理されている。

3. 企業によるSP800-160v2r1活用における課題

「情報システム」のサイバーレジリエンス能力を評価する際，SP800-160v2r1は，有力なリファレンスといえる。しかし，「企業」のサイバーレジリエンス能力を測るという目的で活用しようとすると，いくつかの課題に直面する。例えば，通常，企業内では多種多様な情報システムが複雑に連携しながら稼働しており，SP800-160v2r1で述べられているような特定システムの要件を当てはめようとすると，（1）企業内のどの範囲の情報システムに対して評価を実施すればよいのか判断が難しい，（2）SP800-160v2r1に記載された膨大なセキュリティ要件を評価する具体的手法を読み手が考えなければならないといった課題がある。さらに，仮にこれらの課題が解決できたとしても，（3）要件と現状とのギャップを埋める具体的手段は読み手の知識や経験に依存するという点も課題といえる。

そこで，株式会社日立ソリューションズは，SP800-160v2r1で述べられている内容を分析し，前述した課題を解決するような日立ソリューションズオリジナルの評価基準を作ることにした。具体的には，日立ソリューションズの事業継続計画を策定するコンサルティングサービスで用いるBIA（Business Impact Analysis）の手法を応用し，評価する対象システムを限定することで，（1）の課題を解決しようと考えた。次に，SP800-160v2r1に記載されている膨大な要件の再整理を行った。一般的に，セキュリティ要件を実現する手段は複数存在する。それらの実現手段を列挙し，人手による運用やルール化により実現するもの（以下，「ルールによる対策」と記す。），アプリケーションソフトウェアの機能およびその運用によって実現するもの（以下，「ツールによる対策」と記す。）の二つに分類した。現状の企業のサイバーレジリエンス能力に対し，ルールの整備状況およびセキュリティ対策ソフトウェアの導入状況の確認といった客観的な評価を実施できるようにすることで，（2）の課題が解決できると考えた。加えて，「ルールによる対策」や「ツールによる対策」が不十分だった際の対応策として，日立ソリューションズが持つ既存のさまざまなソリューションメニューをひも付け，それを示すソリューションマップを作成することで（3）の課題を解決しようと考えた。SP800-160v2r1から日立ソリューションズオリジナルの評価基準を作る流れを図1に示す。

図1｜SP800-160v2r1から日立オリジナルの評価基準をつくる流れ



注：略語説明　F&G（Fit and Gap），NIST（National Institute of Standards and Technology）

各課題の解決のための，日立オリジナルのサイバーレジリエンス評価基準を作成する。

4. 課題解決案の検討およびフィードバック

各課題の解決方針が定まったことから，これらを取り込みつつ，最終的には日立ソリューションズのコンサルティングサービスメニューに組み込めるようなアセスメントサービスとして仕立てることにした。以下にその検討の詳細について述べる。

4.1 アセスメントサービスの開発

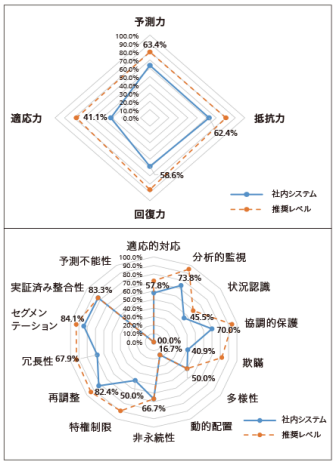
開発したアセスメントサービスは，コンサルタントのヒアリングを通じて，顧客企業のサイバーレジリエンス能力を分析し，強化すべきポイントを明確にしたうえで，報告書を提示するサービスである。アセスメントプロセスの全体像を図2に示す。

「対象の検討」は，既に日立ソリューションズがノウハウを持つBIAの手法を応用し，顧客企業において重要な事業・業務に関連するシステムを特定し，対象範囲を絞るプロセスである。「対象システムの把握」は，顧客から提出された資料を基に，対象システムの用途，利用者，ネットワーク構成などの環境面およびシステム運用やセキュリティ対策の概要を把握し，後続のプロセスを精度高く実施するためのプロセスである。「ヒアリング，現地調査」は，チェックリストを用い，顧客へのヒアリングを通じてサイバーレジリエンス能力の現状を把握，評価するプロセスである。ここで用いるチェックリストは，SP800-160v2r1で述べられている四つの能力および，それらをレジリエンシー手法として詳細化した，テクニックと呼ばれる14の分類で評価できるように独自の工夫を行った。「課題抽出，分析，対策案検討」および「報告書作成，報告会」は，これまでのプロセスで得た情報をインプットとし，視覚的に理解しやすい出力が得られるような分析手順を構築するものであり，顧客が現状の問題点を容易に把握できるように工夫した（図3参照）。

図2｜アセスメントプロセスの全体像

企業のサイバーレジリエンス能力を把握するための評価プロセスを整備し，各プロセスにおける作業概要，成果物を明確にした。

図3｜視覚的に理解しやすい出力



能力	評価値	推奨値
予測力	63.4%	79.5%
抵抗力	62.4%	80.1%
回復力	56.6%	86.6%
適応力	41.1%	77.4%

テクニック	リスク 高	中	低	評価値	推奨値
適応的対応		2	1	57.80%	71.90%
分析的監視				73.80%	95.00%
状況認識			1	45.50%	59.10%
協調的保護	1	2	1	70.00%	94.00%
欺瞞		1		40.90%	81.80%
多様性				50.00%	50.00%
動的配置				16.70%	16.70%
非永続性				66.70%	66.70%
特権制限	1	1		50.00%	89.70%
再調整			1	82.40%	94.10%
冗長性		1	1	67.90%	92.90%
セグメンテーション			1	84.10%	93.20%
実証済み整合性				83.30%	83.30%
予測不能性				0.00%	0.00%

報告書では，四つの能力および14のテクニックごとに，評価値とめざすべき推奨値を示し，現状のリスクを視覚的に分かりやすく表現している。

4.2 実証実験およびフィードバック

この新たに開発したアセスメントサービスにより，仮説どおり有効な評価を実施可能かどうかを確認するため，3社6システムを対象に実証実験を実施した。その結果，いくつかの改善すべき問題点を洗い出すことができた。例えば，実証実験では，コンサルタントがヒアリングに要した時間が，想定を大きく超過してしまうという問題が発生した。これは，コンサルタントと，被ヒアリング者との間でサイバーレジリエンスに関する知識差が大きく，ヒアリングの際に，なぜこの質問を実施しているのかの趣旨を伝えることに想定以上に時間を要したためである。

SP800-160v2r1に記載されている要件は，従来の情報セキュリティで求められていた要件と比較すると，かなりの部分で重複している。サイバーレジリエンスを切り口とした固有の要件もあるが，比較すれば数は少ない。すなわち，サイバーレジリエンスは従来のセキュリティ対策に対して新たな切り口を提供するものといえるが，この切り口を理解するには，従来の情報セキュリティの知識が前提となる。

例えば，感染を確認したマルウェアの不正通信をプロキシサーバで遮断するための設定変更を実施する際，従来の情報セキュリティにおいては，「遮断設定の標準化された運用」が求められていた。サイバーレジリエンスでは，この運用に加え，「情報システムを停止させずに設定変更を実施すること」が求められる。この「停止させずに」という部分が肝要である。被ヒアリング者の情報セキュリティに関する知識量によっては，こういった趣旨を理解してもらうためのオーバーヘッドに想定以上の時間を要した。

これに対し，ヒアリングの質問を工夫することで対処した。被ヒアリング者のサイバーレジリエンスへの理解を促し，回答を得る時間は最小限として，評価のためにコンサルタントが知りたい「ルールによる対策」ならびに「ツールによる対策」の実施状況を端的に聞くように変更した。前述の例では，「～の際，『情報システムを停止させずに』設定変更する運用ルールになっているか。」と，そのまま事例を問い，特にサイバーレジリエンスの要素に関係する文言を強調表記にする。これにより，ヒアリングに要する時間を当初の想定時間内に収めることができた。この対策に関しては，被ヒアリング者がサイバーレジリエンスの本質を理解せずに答弁する懸念もあったが，多くの場合，被ヒアリング者が答弁に困るような場合には趣旨確認のための質疑応答があり，評価精度が低下することはなかった。

4.3 ソリューションマップの作成

アセスメントサービスは，報告会で顧客に強化すべきポイントを提言する。この提言は，顧客がその後どのようなアクションをすべきかを明確にイメージできるようなものでなければならない。そこで，評価後に提言する可能性のある強化ポイントごとに，提示可能な日立ソリューションズの保有ソリューションをひも付けるソリューションマップを作成した。日立ソリューションズは，トータルセキュリティソリューションを掲げ，豊富なソリューションメニューを保有している。そのため，多くの強化ポイントで「ルールによる対策」の実装に向けたコンサルティングサービスソリューション，もしくは「ツールによる対策」の実装に向けたパッケージSI（System Integration）サービスソリューションをひも付けることができた。ひも付けができなかった強化ポイントについては，海外拠点が保有する商材との連携や，過去に参加したセキュリティカンファレンスなどで得られた海外商材の中から有望な製品を選定し，日立ソリューションズの既存ソリューションに組み込むなどの取り組みにより補完した。最終的にはすべての強化ポイントにおいて，提案可能なソリューションをそろえることができた。

5. おわりに

サイバーセキュリティ対策は攻撃者とのいたちごっこという側面があり，一度築き上げたセキュリティ対策も，継続的な見直し・改善が行われなければ，やがて綻びが生じてしまう。セキュリティ対策のトレンドや流行のキーワードは，こうした事態を防ぐための指針といえる。この先数年は，サイバーレジリエンスがその指針の主役となることが想定される。日立ソリューションズは，今後，顧客企業のサイバーレジリエンス能力の向上を通じて，Society 5.0に代表される未来社会の安心・安全に貢献していく。

参考文献など

1) SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach

日立評論

日立評論は、イノベーションを通じて社会課題に応える
日立グループの取り組みを紹介する技術情報メディアです。

日立評論Webサイトでは、日立の技術者・研究者自身の執筆による論文や、
対談やインタビューなどの企画記事、バックナンバーを掲載しています。ぜひご覧ください。

日立評論(日本語) Webサイト

https://www.hitachihyoron.com/jp/

Hitachi Review(英語) Webサイト

https://www.hitachihyoron.com/rev/

日立評論メールマガジン

Webサイトにてメールマガジンに登録いただきますと、
記事の公開をはじめ日立評論に関する最新情報をお届けします。