システム開発工程へのサイバーレジリエンス視点組み込みの提言

Recommendations for Incorporating Cyber Resilience Perspectives into the System Development Process

伊 藤 直 行

要 約 日本国内でランサムウエアによる被害は拡大しており，一部の事例ではサプライチェーンをも巻き込んだ事業停止を引き起こしている．情報システムにおけるセキュリティ品質を担保することの重要性は日を追って高まっている．2022年に発生したランサムウエアによるセキュリティインシデントでは，基幹業務システムが利用不能となったことで全面的な業務停止に陥り，復旧には数カ月を要した．このような被害を防ぐには「サイバーレジリエンス」の視点が重要である．「サイバーレジリエンス」とは，サイバーセキュリティ攻撃の影響を最小限に抑えつつ，迅速に元の状態に回復する能力を指す．情報システムの開発工程でサイバーレジリエンスの視点を組み込むことの重要性は，今後さらに増していく．

Abstract The damage caused by ransomware is increasing in Japan, with some incidents involving the supply chain leading to business interruptions. The importance of security quality in information systems is growing day by day. In a security incident involving ransomware that occurred at a customer site in 2022, the core business system became unavailable, resulting in a complete halt of operations, and the recovery took several months. In order to prevent such damage, the perspective of “Cyber Resilience” is essential. “Cyber Resilience” refers to the ability to minimize the impact of cyber security attacks while quickly recovering to the original state. This paper demonstrates the importance of incorporating a cyber resilience perspective into the information system development process through case studies of recovery from ransomware-related security incidents.

1. はじめに

日本国内においてランサムウエアによる被害は拡大しており，一部の事例ではサプライチェーンをも巻き込んだ連鎖的な事業停止を引き起こしている．

2022年に，BIPROGY株式会社（以下，BIPROGY）が担当する顧客（以下，Z社）の基幹業務システム（以下，基幹システム）にて，ランサムウエアによるセキュリティインシデントが発生した．基幹システム基盤が利用不能となったことで，Z社は全面的な業務停止の状態となり，業務が全面復旧するまでに数カ月を要した．さらに，復旧作業にかかるコストや手作業での業務運用にかかるコストなど，Z社のコスト負担は膨大なものとなった．

このインシデントではバックアップサーバーも被害に遭ったため，システムおよび業務の復旧に多くの時間を要した．業務アプリケーションソフトウエアやそれらに関する構成ファイルは被害を免れた開発環境から復旧できたものの，基幹システムを構成するサーバーやそこで管理されていた業務データは早期の復旧が不可能となり，最終的にシステム基盤上の全サーバーを初期化したうえで再構築することとなった．インシデント発生を前提として，早期復旧に向けて準備しておく「サイバーレジリエンス」の視点の重要性を強く感じさせられた．

「サイバーレジリエンス」とは，「サイバーセキュリティ攻撃の影響を最小限に留めつつ，迅速に元の状態に回復，復元すること」[1]を指す．本稿では，ランサムウエアによるセキュリティインシデントの復旧対応の事例をケーススタディとして，システム開発工程における「サイバーレジリエンス」の視点の組み込みの重要性を提言する．2章で今回の事例の概要と初期対応を時系列に沿って説明し，3章で復旧作業の概要と並行して実施したセキュリティ強化策について説明する．4章で今回のインシデントに関連する非機能要件について整理し，5章でサイバーレジリエンスの視点を組み込むことの重要性について説明する．

2. セキュリティインシデントの概要と初期対応

本章では，インシデントが発生したシステム構成およびインシデントによる被害の概要と，その後の復旧作業への足掛かりとなる初期対応について説明する．

2.1 システム構成および侵入経路の概要

Z社では，データセンター（以下，DC）にてサーバーやディスクストレージ装置（以下，ディスク）などのシステム基盤を構築している．そのうち，基幹システムを含む全社業務システムの基盤と，DCや社内拠点の一部の内部ネットワーク（以下，NW）をBIPROGYが構築し，インターネットなど外部NWの境界をBIPROGYグループ以外のNWベンダが構築した．構築後の運用管理はZ社が実施している．

NWの論理構成を図1に示し，今回のインシデントにおける侵入者の侵入経路を破線にて表す．今回のインシデントでは，このNWの境界領域に配置したNW機器のVPN接続機能の脆弱性を突かれ，外部からの侵入を許した．社内NWへの侵入後，侵入者は攻撃ツールを使用して，次々と基幹系システムを構成するサーバーに管理者権限でアクセスし，ファイルの暗号化を実行した．

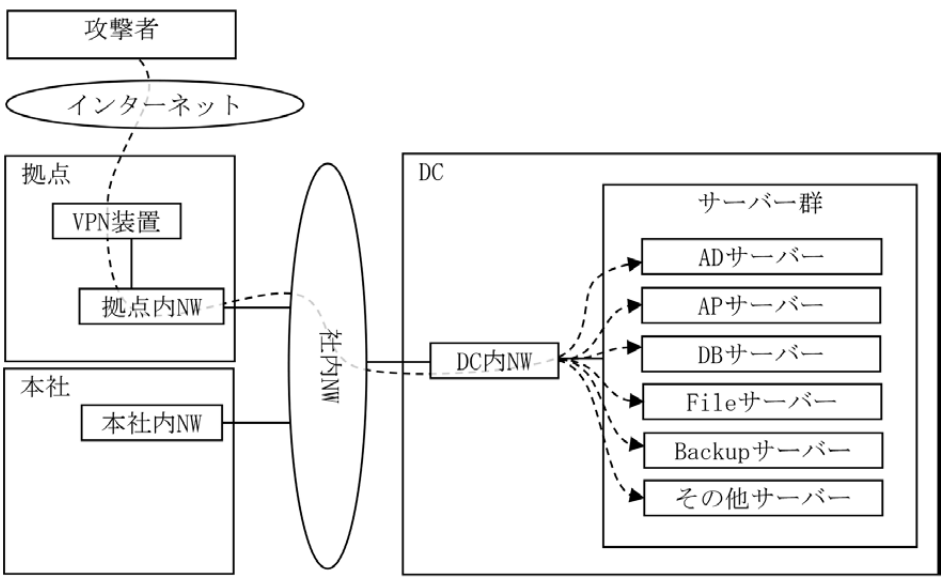

図1　NW論理構成と侵入経路

2.2　インシデントによる被害の概要

ファイル改ざんの痕跡と検体から，使用されたランサムウエアは「LockBit3.0」[2]だと特定された．このことから，侵入者は，侵入，探索，アカウント窃取，ファイル改ざんなどを組織的に高度化して実行する RaaS（Ransomware-as-a-Service）[*1] 組織であると想定される．

初期対応で行った被害調査では，DC の基盤に構築した物理サーバーと仮想サーバーのうち，60％近くが被害に遭ったことが分かった．さらに，被害に遭ったサーバーにおいては，最初にシステムの異常が検知されてから数時間のうちに攻撃が完了していたことも分かった．

また，基幹システムでは，Active Directory（以下，AD）による統合的なアカウント管理をシステム基盤全体のポリシーとして，AD ドメイン[*2]，サーバー，およびエンドユーザの権限管理が行われていた．後の調査で，この AD ドメイン全体を管理する管理者アカウントのパスワードが窃取されていたことが分かった．このパスワードは辞書攻撃[*3] などにより窃取されたものと推察している．管理者権限で操作できるアカウントで侵入されたため，AD ドメイン内に構築されたサーバーに対して，侵入者は容易に攻撃することができた．

ファイル改ざん動作の詳細は割愛するが，被害にあったサーバーでは多くのファイルが暗号化されていた．これにより，業務アプリケーションだけでなく，データベースなどのミドルウエアを含むほとんどのソフトウエアの機能が停止した．また，ファイルサーバーなどに格納される業務データも使用不能となった．結果として，基幹システム全体が使用不能となり，Z 社は業務停止に陥った．

2.3　初期対応

インシデント発生後，最初の二日間の初期対応タイムラインを表 1 に示す．まず，発生一日目の早朝にシステムの異常を知らせる障害発報が発生した．これはディスク容量の圧迫を示すものであった．この障害について Z 社による調査が始まり，基幹システムが使用できないことが判明した．

この段階で，Z 社からの連絡を受け，Z 社の承認のもと BIPROGY が対応作業の支援を開始した．まず外部 NW 遮断を実施した後，緊急 CSIRT[*4] の立ち上げ，対応作業の優先順位付け，検体確認などの初期対応を実施した．並行して，Z 社のニュースリリースや当局連携などの外部広報を支援し，PMO 業務の後方支援チームも組織した．おおよその復旧態勢とその指揮系統を，Z 社と BIPROGY が協同して 3 営業日内で構築した．

表 1　初期対応タイムライン

対応日	時刻	状　況
一日目	3:23	最初の監視イベント通知．ディスク容量圧迫のイベント確認
	7:56	Z 社情報システム部メンバーが DC に到着，調査開始．基幹システムが利用不能であることが判明．仮想サーバー管理画面からサーバーに接続しランサムウエアへの感染メッセージを確認
	10:00	BIPROGY グループの DC 常駐メンバーが Z 社の支援を開始
	10:13	インターネット接続 NW と社内閉域 NW を抜線
	11:58	AD サーバー，バックアップサーバーにてランサムウエア実行の痕跡があることを確認

対応日	時刻	状　況
	13:10	Z 社がサーバー群の感染状況を調査開始
	17:30	BIPROGY の担当 SE が DC に到着
	19:50	全サーバーのうち 60%が感染していることを確認
	21:30	Z 社・BIPROGY グループメンバーによる対策会議を実施．この時点で，復旧の目途立たずという状況を報告
	22:00	Z 社内部にて CEO 含めた報告会実施．翌朝，Z 社内部にて全役員含む対策会議開催にて方針決定を決議
	22:30	Z 社・BIPROGY グループメンバーが DC 退館
二日目	9:00	Z 社内部にて対策会議実施．BIPROGY へニュースリリース準備支援から始まり，業務システム影響調査と復旧に関する全面的な支援要請あり
	10:00	復旧・調査会議実施．調査チーム，復旧チームを編成．BIPROGY-CSIRT チームが Z 社本社に向けて移動開始
	13:00	定時進捗会議を実施．被害調査および復旧対象ファイルの確認状況を報告
	13:50	BIPROGY-CSIRT チームが Z 社本社到着．詳細状況確認および対応内容，体制検討したうえで対応作業継続
	17:00	定時進捗会議を実施．調査状況を共有．Z 社にて業務システム再構築を全体方針とすることを決議
	18:00	Z 社内部にて全社報告会実施．CEO から全社員向けに全体方針メッセージ発出
	18:30	BIPROGY-CSIRT チームメンバーが DC に入り，検体取得し AD サーバーを調査
	21:00	定時進捗会議を実施．検体の詳細調査結果にもとづき，ランサムウエアに間違いないことを共有

なお，インシデント発生翌日に実施した全社報告会において，Z 社 CEO が「過去を振り返らず，復旧最優先で新しく作り直していく」として大方針を表明したことにより，復旧に向けての意志を統一することができた．業務復旧に向けた対応作業の中では，サプライチェーンの川上と川下両面にわたる取引先への緊急連絡や，各拠点および各部署での人手作業の差配など，Z 社のシステム部と各業務部門が協力して復旧に向けた緊急態勢と業務プロセスを構築していった．CEO からの明確なメッセージ発出によって復旧態勢が構築され，業務システムが使用不能な状態の中でも，工夫しながら業務を継続することができた．

3.　復旧作業とセキュリティ強化の概要

本章では，システム復旧のプロセスを説明した後に，実施したセキュリティ強化の概要を示す．特に，システム復旧を行いながら同時にセキュリティ強化を行うとよい場合など，戦略的に復旧作業を計画することの重要性について説明する．

3.1　復旧作業の大方針

本節では，復旧作業の概要を示すとともに，復旧作業を計画し実施するにあたっての留意点について述べる．今回の事例では，最初に「どのようにシステム基盤を復旧するのか？」という大方針を決断した．また，感染したサーバーの画面上に表示されていた身代金要求メッセージに対しては，警察当局と BIPROGY-CSIRT の助言により「RaaS 組織に身代金は支払わない」

ことを決定した．なお，身代金支払いの是非については，経済産業省から「金銭の支払いは厳に慎むべきものである」との指針が出ている[3]．

その後，RaaS 組織との交渉による解決をしないという決定と，バックアップサーバーも被害に遭いバックアップデータが使用不能となっている状況を考慮したうえで，調査と復旧のどちらを優先するかを検討した．個々のサーバーの詳細なフォレンジック調査[*5]を行うには時間がかかること，業務システム全体が使用不能となり事業停止となっている状態を早期に復旧しなければならないこと，さらには被害にあったサーバー内のウイルス残置の可能性を排除しなければならないことなどから，今回は復旧を優先し，システム基盤を構成するサーバーとディスクを初期化して再構築するという判断に至った．

3.2　復旧計画の策定

本節では，全体復旧計画の策定と，日々の計画および実行の管理について述べる．全領域の業務システムの復旧を完了するには時間を要するため，今回は業務領域ごとに優先度をつけて各業務システムの復旧時期を設定した．最初に復旧すべき業務領域には，Z 社にとっての取引先である発注者への業務影響がもっとも大きい領域を選定した．その後に，Z 社が製造委託を行う発注先に関連する業務，最後にバックオフィス系の業務を復旧する方針とした．

こうして，業務領域の復旧優先度を考慮した業務システムごとの復旧期日を設定し，それらをマイルストーンとした全体復旧計画を策定した．復旧作業にあたっては，サーバーやソフトウエアなどの復旧を行う基盤復旧チームと，データやプログラムなど業務システム視点での復旧を行う業務復旧チームを両輪として実行体制を構築し，この体制に対応する作業をマッピングして中日程を策定した後，詳細な作業計画である作業パッケージを WBS として詳細化した．意思決定の場としては，Z 社システム部メンバーと BIPROGY グループメンバーの共同で朝会を定時開催し，実施状況の確認とスケジュール調整および課題管理を行いながら復旧作業を進めていった．

3.3　復旧作業の概要と経緯

復旧作業の概要を表 2 に示す．各種 NW 機器のログ調査により，今回の被害範囲は DC 内のサーバー基盤にとどまり，各拠点のクライアント PC や各種 NW 機器には被害がおよばなかったことが分かった．特に本社内情報システム部署に配置している開発環境にはテスト用途のプログラムやデータベースが保管されており，これを使用して業務アプリケーションや一部の業務データを復旧することができた．さらに，設計書などのドキュメント類について，システム基盤設計情報は BIPROGY でも保管することで合意していたため，Z 社が運用管理しているアカウントや EDI 取引先通信などの各種管理台帳と合わせて，基盤構築およびその後の各種設定作業を進めることができた．もし，電子化したシステム基盤設計情報がファイルサーバーのみに保管されていたら，暗号化の被害を受けて復旧は困難となっていた．また，暗号化されていなかったとしても，ネットワークを遮断している環境下では，ファイルへのアクセスに時間を要する．システム基盤および業務システムの設計書の構成管理の重要性があらためて認識された．

表 2　復旧作業の概要

No	対　象	復旧作業
1	サーバー基盤	・サーバー基盤を構成する物理サーバー，ディスクを初期化し仮想サーバーを初期構築する． ・OS を含むソフトウエアを新規で導入・設計し，サーバー間の通信を行うための設定を行う． ・古いバージョンやサポート停止のソフトウエアがある場合，原則新しいバージョンを適用する．
2	業務アプリケーション	・開発環境で保管していたソースプログラムから新しくビルドして配置する． ・サーバー上のソフトウエアのバージョンアップに依存する非互換が発生する場合は，原則作り直して非互換に対応させる．
3	業務データ	・開発環境に残っていた検証用データベースをもとに，業務データベースを新しく構築したうえで，業務アプリケーションを稼働させるためのマスタデータを再登録する． ・取引先管理台帳をもとに EDI 取引先接続のための接続定義を新規設定する．

全システム復旧までの経緯を表 3 に示す．インシデント発生の翌月には，一部取引先に関連する業務を再開した．Z 社によるマスタデータ整備も進み，2 カ月後以降は順に各業務を再開し，4 カ月後には月次バッチ処理の確認により基幹業務が全面再開となった．インシデント発生から 5 カ月後にはその他システムの復旧も完了し，全システムが再開した．

表 3　復旧の経緯

No	時　期	復旧経緯
1	某月中旬	セキュリティインシデント発生
2	某月下旬	侵入箇所含む外部接続 NW 機器への脆弱性パッチ適用
3	某月下旬	サーバー，ディスク初期化
4	翌月上旬	一部取引先に関連する業務を再開，順次取引先を拡大
5	翌月中旬	取引先に関連する業務の再開範囲を拡大
6	2 カ月後	取引先に関連する業務の全面再開
7	3 カ月後	発注先に関連する業務の全面再開
8	4 カ月後	月次処理，基幹業務システムの全面再開
9	5 カ月後	会計システムを含む全システムの全面再開

3. 4　セキュリティ強化要件

仮に，すべてのサーバーをこれまでの基盤設計書通りに再構築したとしても，インシデント以前の状態に戻るだけでセキュリティ強化にはならない．今回は復旧作業と並行して，侵入時および侵入後のランサムウエア実行までの被害を防ぐ対策を，Z 社とともに網羅的に確認していった．さらに，再度被害に遭った場合の復旧要件も含めて，Z 社と相互認識しながら，具備すべきセキュリティ強化要件を整備してきた．

今回実装したセキュリティ強化要件の一部について，詳細を表 4 に示す．この要件は，初期対応時に CSIRT メンバーが起案した要件を整理し，Z 社情報システム部門の上位管理者との協議を経て環境に合わせてブラッシュアップしたものである．

表 4　セキュリティ強化要件

No	要　件	対応方式
1	外部不正アクセス防止	・ログイン認証およびクライアント証明書認証による多要素認証 ・ビルトイン管理者アカウント Administrator の無効化
2	パスワード窃取防止	・サーバー，NW 機器の管理者パスワードの複雑化 ・不正パスワード投入時のロックアウト設定
3	不正侵入・不正操作の検知・分析・遮断	・サーバー，クライアント PC などへのふるまい検知機能を持つ EDR 製品[*6] 導入 ・ログ監視による不正侵入検知サービス利用
4	SOC サービス利用	・外部 SOC[*7] の利用によるセキュリティ運用体制構築
5	セキュリティ診断利用	・セキュリティ診断の定期的な実施によるリスク可視化
6	システム保守におけるサーバーアクセス強化	・サーバーへの直接アクセスの多要素認証化 ・アクセス可能な PC からの通信制御強化
7	セグメント分離によるアクセス制御強化	・取り扱うデータの機密度により機密セグメントと一般セグメントに分離することで通信制御を強化 ・NW 機器だけでなくサーバー OS レベルでのアクセス制御強化
8	バックアップ複数方式適用	・「バックアップの 3-2-1 ルール」[*8] の具備 ・ディスク製品のスナップショット機能[*9] の利用

復旧作業においては，これらの要件を効果的に実装するため，サーバーの初期設定などの初期構築時に実施すべき作業と復旧後に実施すべき作業を区分けして対応を進めた．

システム基盤の復旧作業と同時に実施したセキュリティ強化策は，「外部不正アクセス防止」，「パスワード窃取防止」，「セグメント分離によるアクセス強化」など，サーバーやディスクの初期構築時に実施すると効果のあるものを選定した．システム基盤の復旧作業が完了した後，業務の復旧と並行して，「不正侵入・不正操作の検知・分析・遮断」，「SOC サービス利用」，「セキュリティ診断利用」，「システム保守におけるサーバーアクセス強化」，「バックアップ複数方式適用」といったセキュリティ強化要件を実装することとした．すぐに実装できないものは次年度予算化を行うなど配慮し，そのうえでセキュリティ強化要件（表 4）をできる限り網羅するよう，優先度と実装順序を決定した．

最終的に実装したセキュリティ強化要件には，BIPROGY 以外のベンダによるものや Z 社自ら実装したものも含まれている．復旧作業においても，Z 社がコストとスケジュールを勘案しながら網羅的に実装することを優先した結果である．

4.　インシデント発生の要因分析と重要な非機能要件の整理

本章では，インシデント発生の背景にある要因を分析するとともに，セキュリティ強化において重要な非機能要件について説明する．

4.1　システム障害に対する非機能要件

被害に遭ったシステム基盤のなかで，最も業務への影響が大きかったのは Z 社の業務領域の全体を網羅する基幹システムである．

今回のインシデントに関連するシステム障害の重要な非機能要件を表 5 に示す．今回の基幹

システムは，単一障害点 SPOF（Single Point Of Failure）[*10] を冗長構成方式で回避する設計としていた．そのため，障害点が単一箇所であれば，稼働率 99.99％を担保できるように基盤方式設計，サイジング設計，およびシステム運用設計を実施していた．

表 5　インシデントに関連する重要非機能要件

No	非機能要件項目	内　　容
1	システム内部とシステム外部の境界の侵害の前提	・境界 NW のファイアウォールの機能により，システム基盤に対する侵入は防御できることを前提とする．
2	障害発生箇所の前提	・通常のシステム利用の範囲においては，同時に複数箇所で障害が発生することが無いという前提で，SPOF を回避する設計とする．
3	バックアップ方針	・基幹システムなどの最重要システムが早急に復旧できるよう，システムイメージ（OS，ミドルウエア），アプリケーション，データをバックアップサーバーに保管し，最新トランザクションまで復旧できるように設計する．

4. 2　セキュリティインシデントを想定した非機能要件の必要性

システムの内部と外部の境界にある NW 構成は，BIPROGY グループ以外の NW ベンダにより構築されていた．今回のインシデントは，Z 社の NW 担当要員が脆弱性パッチ[*11] の情報を得て，適用作業の段取りを考慮していた時に発生した．このように，事前に脆弱性に対する準備をしていたとしても，いつでも発生しうるのがランサムウエア被害の特徴である．

また，今回のインシデントでは，障害発生箇所の前提要件にもとづき SPOF 観点から可用性の設計を行っていたにもかかわらず，同時に複数のサーバーが被害に遭い機能停止に陥った．これは，通常使用時での障害ポイントの要件だけでなく，セキュリティインシデントや災害時復旧を想定した全損状態となるインシデントを強く意識する必要性を示している．

さらに，復旧時に使用するバックアップデータについては，システム基盤が全損状態となった場合でも「使用できる状態」で保管されていなければならない．今回のインシデントでは，バックアップサーバー上のデータも暗号化されて使用できなかった．こういった事態を防ぐためにも，バックアップデータはセキュアかつ分散されたサイトに保管することが望ましい．「常に三つのデータコピーを作成し，それらを二つの異なる媒体に保管し，一つはオフライン環境に保管する」という「バックアップの 3-2-1 ルール」[*8] に準拠することがより強く求められる．

このように，非機能要件については「万一重大インシデントが発生した場合，システム基盤を復旧できるか？」という視点で十分に検討すべきであり，これらの重要な要件が欠落することがないように考慮しなければならない．

4. 3　当該プロジェクトにおける重要な非機能要件設計の盲点

プロジェクトを進める中で，システムへの要求や要件とコストはトレードオフの関係となる．コスト削減を優先する場合，一部の要件事項を削除するか，もしくは性能品質を抑制しなければならないこともある．また，企業の基幹システムは，内部 NW の領域に構築されることが多い．こうしたシステム基盤の外部 NW と内部 NW の接続境界において，セキュリティ観点での見直しが十分でないケースも多い．

非機能要件は非常に広い領域を対象としており，通信方式や冗長化方式など詳細な方式の規定，性能の担保なども網羅する．加えて，非機能要件の検討では，ディザスタリカバリなど事業継続計画にもとづく災害対策の高い視点で事項を整理しなければならない．

情報システムおよびシステム基盤の構築に掛けられる予算は限られている．そんな中でも，企画段階で考慮すべき非機能要件を定義する際の重要なポイントとして，以下が挙げられる．

- 顧客が統括してマルチベンダにてシステム基盤を構築する場合，複数の基盤構築ベンダ間での包括的なセキュリティ視点が重要である．特に，外部 NW と内部 NW の双方についてセキュリティ要件を確認することは重要である．
- インターネットを含む外部 NW 接続境界でのインシデントが発生する場合は，被害が広範囲におよぶことに留意すべきである．
- システム基盤の更改時点など構成を見直す際に，セキュリティ要件をチェックしそれに見合った対策を実施することが重要である．
- ランサムウエアなどによる外部からの攻撃が発生することを前提として非機能要件を設計すべきである．

5. サイバーレジリエンス視点の組み込みの提言

本章では，セキュリティ対策においてサイバーレジリエンスの視点を組み込むことの重要性について説明する．

5.1 サイバーレジリエンスの考え方の理解

デジタル庁が作成した「政府情報システムにおける セキュリティ・バイ・デザインガイドライン」[4]に次の記述がある．

「企画から運用まで一貫したセキュリティ対策を実施する「セキュリティ・バイ・デザイン」の必要性が高まっている．」

また，同じくデジタル庁が作成した「政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート」[1]に次の記述がある．

「サイバー攻撃に対して「防御」を中心とした従来のセキュリティ態勢の構築が未だに続いている．しかしながら，昨今の高度化・複雑化するサイバー攻撃に対して，「防御」中心のサイバーセキュリティ対策だけでは，対処することが困難になってきている．そのため，サイバー攻撃は完全に防ぐことはできないという前提のもと，「防御」の対策だけではなく，サイバー攻撃を速やかに「検知」するとともに「対応」し，被害が発生した際には「復旧」するといったサイバーレジリエンスに関する対策にも注力すべきである．」

なお，同文献は「サイバーレジリエンス」を以下のように定義している．

「サイバーセキュリティ攻撃の影響を最小限に留めつつ，迅速に元の状態に回復，復元すること」

すなわち，企画・設計・開発・導入・運用・廃棄というシステムのライフサイクルの全ての段階において，一貫したセキュリティ対策をとることが重要である．さらに識別・防御・検知・対応・復旧の五つのセキュリティ機能の中でも，とりわけ検知・対応・復旧の対応策に注力すべきである．ここまで述べてきたように，「セキュリティインシデントは必ず発生する」という意識が重要であり，被害を受けた場合でも，すぐにインシデントの発生を検知しシステムを

復旧させる機能を，システム基盤構築の初期段階からセキュリティ設計の一部として組み込むべきである．

このように，システムのセキュリティ対策を設計するにあたっては「セキュリティを担保するために，いつ，誰が，何をすべきか？また，セキュリティ対策導入の目的をどのように考えるべきか？」という包括的かつ文脈的にも理解しやすい視点を常に持つことが重要である．

5.2　サイバーレジリエンス視点組み込みの提言

セキュリティインシデントがいつ発生してもおかしくない状況では，復旧機能の視点が重要である．「政府情報システムにおける セキュリティ・バイ・デザインガイドライン」[4]では，セキュリティ設計の項に「重要なセキュリティ対策の考え方」として「アタックサーフェス（攻撃対象領域）の管理，防御」，「管理者アカウントの保護」，「サイバーレジリエントな設計の実施」の３項目が定義されている．

識別・防御・検知・対応・復旧の五つのセキュリティ機能の中で，防御，検知の機能領域に該当する「アタックサーフェス（攻撃対象領域）の管理，防御」の項目を以下に引用する．

- セキュリティ設計においては，攻撃対象となるアタックサーフェス（攻撃対象領域）を極力減らす設計を行い，防御することが重要となる．
- システムにおけるアタックサーフェス（攻撃対象領域）を把握するため，システムで使用する資材の資産管理を実施し，最新な状態を維持する．
- システムで使用するハードウェアやソフトウェア等の資産に関して，脆弱性管理可能な仕組みを導入する．
- 攻撃者による悪用を防止するため，システムにおいて不要な機能やサービスは実装しない．プラットフォームに初期設定でインストールされているような機能，サービスも使用しない．
- 外部 I/F への入力に関しては，信頼せず，必ず入力値検証を実施する．

次に，防御，検知の機能領域に該当する「管理者アカウントの保護」の項目を以下に引用する．

- 権限管理に起因するインシデント被害を極小化するため，ユーザアカウント，管理者アカウントに対して過剰なアクセス権限は付与しない．
- とりわけ，管理者アカウントの悪用は被害が大きくなるため，管理者権限の利用者は必要最小限にとどめ，管理者アカウントによるアクセスには多要素認証等を用いて十分に保護する．
- 管理者アカウントの利用者を特定可能な仕組みを導入し，追跡可能な状態にする．

最後に，検知・対応・復旧の機能領域に該当し，本稿の主旨である「サイバーレジリエントな設計の実施」の項目を以下に引用する．

- サイバー攻撃の大規模化，高度化に伴い，攻撃は成功し，インシデントは発生する前提にたち，防御力だけでなく回復力（サイバーレジリエンス）を高める設計が重要となる．
- システムアーキテクチャの設計においても，NW 分離やアクセス権の必要最小権限付与，ゼロトラストセキュリティの考えに基づく対策の導入等，インシデント発生時のシステムへの被害を極小化するための設計が求められる．
- 必要な機器やソフトウェアのログ，セキュリティ製品のアラート等を収集/分析し，イ

ンシデント等異常な状態を速やかに検知するため，独立した監視環境を用意することが，セキュリティ運用上重要となる．

- インシデント検知をした際は，速やかなインシデント対応やサービス復旧を可能とする，運用体制や運用プロセスの整備が求められる．速やかなサービス復旧を行うため，重要データのバックアップやリストア手順を事前に準備する．

このように，セキュリティに関する設計項目を文脈形式で認識しておくことで，セキュリティ・バイ・デザインの必要性，特にサイバーレジリエント設計の必要性を理解でき，大まかな実装方式をとらえやすくなる．このような項目を，すべての開発工程のチェックリストに明示的に加えることが有効である．復旧作業と同時に実施したセキュリティ強化対応の要件（3.4節の表4）も，本節に記した設計項目と多くの事項が合致する．実際に行ったセキュリティ強化対応では，この要件一覧を常に見返すことで，どのような要件を実装しているかを意識しながら作業を進めた．

5.3　情報処理安全確保支援士として今後の活動への適用

今回のセキュリティインシデントの発生とほぼ同時に，筆者はセキュリティスペシャリストの国家資格である情報処理安全確保支援士（以下，支援士）の資格を取得していた．支援士の業務と役割を以下に引用する[5]．

1) 情報セキュリティ方針及び情報セキュリティ諸規程（事業継続計画に関する規程を含む組織内諸規程）の策定，情報セキュリティリスクアセスメント及びリスク対応などを推進又は支援する．
2) システム調達（製品・サービスのセキュアな導入を含む），システム開発（セキュリティ機能の実装を含む）を，セキュリティの観点から推進又は支援する．
3) 暗号利用，マルウェア対策，脆弱性への対応など，情報及び情報システムの利用におけるセキュリティ対策の適用を推進又は支援する．
4) 情報セキュリティインシデントの管理体制の構築，情報セキュリティインシデントへの対応などを推進又は支援する．

今回のインシデント対応における調査・復旧作業とセキュリティ強化対応作業を通して従事した業務は，支援士としての業務と役割とも合致する．セキュリティ強化対応策を案出することは，1)の「情報セキュリティの方針と規定を策定し，推進すること」である．システム基盤に対する2)の「セキュリティ機能の調達，開発」は，セキュリティ強化の実装作業そのものである．パスワードの強化などは，3)の「暗号利用などの情報システム利用上の，基本的なセキュリティ対策」と合致する．最後に，4)の「セキュリティインシデントへの対応と，複数のセキュリティ強化対策」については，優先順位とコスト計画を考慮した実施計画とすることで，Z社の要求に沿った実装を実現したことと合致する．

顧客のコスト制約などを考慮してプロジェクト管理を推進するプロジェクトマネージャのような「スコープ，予算，工程，品質などの管理」に対する責任は，支援士の役割には含まれていない．しかし，急激なコスト負担を考慮した対応が求められる場面もある．今回のセキュリティ強化対応策の実装においては，要求されるコストが度々変化する中「どの対策にどのくらいのコストを掛けることができるか？」といったコスト配分と実装の優先度を，Z社と調整し

ながら作業を実施した．

サイバーレジリエンスの観点に立ったセキュリティ・バイ・デザイン設計の提案・構築を指向した上で，対応優先順位とコスト負担のトレードオフを考慮しながらプロジェクトを推進することの必要性を強く感じている．同時に，支援士のような資格やスキルを持つ人材を自社で育成することや外部から調達することは，今後さらに重要視されることになる．

6. お わ り に

ランサムウエアなどによる近年のセキュリティインシデントでは，攻撃の高度化により甚大な被害が発生している．場合によっては，自社のみならずサプライチェーン上の関連企業をも巻き込んだ業務停止を引き起こすことがある．「セキュリティインシデントなど発生しないだろう」といった希望的観測を抱くのではなく，「いつかは必ず発生する」ということを前提とした準備をしておくべきである．そのためには，システム構築の構想段階からサイバーレジリエンス，セキュリティ・バイ・デザインの視点を盛り込むことが重要である．

2021 年に，BIPROGY は「Vision2030」として「デジタルコモンズを誰もが幸せに暮らせる社会づくりを推進するしくみに育てていく」ことを掲げた．デジタルコモンズは，社会的価値と経済的な価値の共創の場を構築し，その中で創発的な対話と実践を促して，共有財を広く利活用していくことを目指すコミュニティであり，その根幹として「安全・安心」の要素は欠かせない．デジタルコモンズを持続可能な共創基盤とするためにも，BIPROGY はサイバーレジリエンスやセキュリティ・バイ・デザインの視点を念頭に置いて，顧客業務システムの構築に取り組んでいく所存である．

最後に本稿執筆にあたり，ご協力およびご指導いただいたすべての皆様に深く感謝し，お礼申し上げる．なにより大きな被害に遭いながらも，前向きに復旧に取り組まれた Z 社の皆様，特に前線で踏ん張り続けた情報システム部の皆様に最大限の敬意を表する．

本稿が読者の関係する情報システムのセキュリティ強化の一助となれば幸いである．

＊ 1　ランサムウエアをサービスとして提供する形態や組織を指す．このような組織やサービスを利用することで，ランサムウエアを容易に利用し攻撃できる．

＊ 2　Active Directory のドメインのことを指す．Active Directory は，Microsoft が提供する Windows ネットワークにおけるディレクトリサービスで，ユーザー，コンピューター，その他のリソースを集中管理する仕組みである．

＊ 3　サイバー攻撃の一種．攻撃者が特定のシステムやサービスへのログイン認証を突破するために，パスワード候補となる文字列をリスト化し順番に試していく攻撃手法．

＊ 4　Computer Security Incident Response Team の略．企業や組織のコンピューターやネットワークが何らかのセキュリティインシデントに遭った場合，その対応を行う専門チームを指す．

＊ 5　セキュリティインシデント発生時の事実関係や経緯を詳細に分析・把握するための鑑識調査．具体的な調査内容としては，不正行為の調査，情報漏えいの調査，サイバー攻撃の解析などがある．

＊ 6　Endpoint Detection and Response の略．パソコンやサーバーなどのエンドポイントデバイスにおける不審な挙動や攻撃を検知し，迅速に対応するためのセキュリティソリューション．侵入後の脅威に対応するだけでなく，攻撃の被害を最小限に抑えることを目的とする．

＊ 7　Security Operation Center の略．サイバー攻撃の検知，分析，対策を講じる専門組織である．企業や組織の情報システムを監視し，サイバー攻撃の脅威から保護する役割を担う．

＊ 8　データのコピーを三つ作成し，それを二種類の異なるメディアで保存し，一つは別の場所（オフサイト）に保管するという，データのバックアップを徹底するためのガイドラインである．

＊ 9　ある時点でのディスクストレージ内のデータ状態を正確に記録し保存する機能．まるで写真を撮るようにその瞬間を切り取って記録し，後からその状態に戻すことができる．

＊10　システムの中でその部分が故障するとシステム全体が停止してしまうような，非常に重要なポイントのことを指す．SPOF を回避するためには，冗長化（二重化や多重化）が有効である．

＊11　脆弱性パッチとは，ソフトウエアのセキュリティ上の脆弱性を修正するためのプログラム．OS やアプリケーションなどのソフトウエアに脆弱性が発見された場合，開発者やベンダがこの脆弱性を修正するためのパッチを作成しユーザーに提供する．パッチ適用により攻撃者が脆弱性を悪用することを防ぎ，情報漏えいなどの被害を未然に防ぐ．

参考文献

［1］ 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート，デジタル庁，2023 年 3 月，
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf

［2］ LockBit3.0 とは何者か？，サイカルジャーナル，NHK，2022 年 11 月，
https://www3.nhk.or.jp/news/special/sci_cul/2022/11/special/lockbit-cyber-11/

［3］ 最近のサイバー攻撃の状況を踏まえた経営者への注意喚起，経済産業省，2022 年 12 月，
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/001_07_00.pdf

［4］ 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン，デジタル庁，2022 年 4 月，
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/2a169f83/20220630_resources_standard_guidelines_guidelines_01.pdf

［5］ 情報処理安全確保支援士試験，独立行政法人情報処理推進機構，2023 年 6 月，
https://www.ipa.go.jp/shiken/kubun/sc.html

※　上記参考文献に含まれる URL のリンク先は，2025 年 7 月 8 日時点での存在を確認．

執筆者紹介　伊　藤　直　行（Naoyuki Itoh）

1989 年日本ユニシス(株)入社後，一貫して顧客業務システム構築に従事．情報処理安全確保支援士（登録番号第 024056 号），IT ストラテジスト．