サイバーセキュリティと個人情報保護†

畠中　伸敏*

After analyzing the cases of cyberattacks on medical institutions from the ITIL perspective in recent years, the necessaries for pro-active and re-active from the analysis results are derived, and the recurrence of cyberattacks will be removed with looped corrective action is proposed. Furthermore, as system vulnerabilities were induced from lack in checking at the upper design phase, rather than loading the user, vulnerability checks in design phase should be held before delivering software products to recipients. In order to decrease system vulnerabilities from software products, OWASP ZAP, Burp suite professional are useful tools which are illustrated. Additionally, reviewing information systems with the awareness that cyberattacks will be realized to us in the futue is an urgent matter, as learning the lesson of case studies from medical institutions or Asahi GHD.

1．はじめに

日本の個人情報保護法第20条に，安全管理措置が定められている．

（個人情報保護法第20条）

個人情報取扱事業者は，その取り扱う個人データの漏えい，滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない．

この訴訟例としては，2015 年 1 月に，インテリア商材の通信販売を営む会社とシステム開発の会社との間で，SQL　インジェクション脆弱性が原因でクレジットカード情報が漏洩した事件につき，ショップ側が開発会社を相手取り損害賠償請求の裁判を起こし，「SQLインジェクション対策もれの責任」を開発会社に問い，ショップ側が勝訴した．

その他に，個人情報保護法を適用した主務所の事例は，2005年4月，金融庁が「勧告」した「M地方銀行CD-ROM（128万件預金者情報を格納）紛失」の事例のみで，個人情報の有用性に配慮しつつ，個人情報の保護の条文の理念が生きている．

しかし，個人情報保護法は，EUと日本の相互認証の条件として，EUの法律のレベルまで追いつくことが求められ，オプトイン（最初に同意していれば，NOと言わない限り，収集した個人情報を再同意なく，使い続ける）の規制はやや緩め，罰則を厳しくすべく改訂が進められている．

昨今は，大手ビール会社，医療機器通販大手会社とサイバー攻撃に個人情報の漏えいが相次いでいることから，インシデント発生から，是正処置までの過程を，マネジメントのノウハウを整理したITIL（Information Technology Infrastructure Library）のプロセスから一部流用する形で，国内の病院事例を分析し，予防的処置，事後的処置の必要性を提示する．

2．病院へのサイバー攻撃事例の分析[1]

国内病院の電子カルテをねらった一連のランサムウェアによる攻撃に対して，どの程度の影響があり，各病院がどのように障害からの回復を行ったかを，障害が発生した場合の障害処理のマネジメントのノウハ

†令和8年5月5日　受付

*一般社団法人リスク戦略総合研究所
連絡先：〒261-0023　千葉県千葉市美浜区中瀬1丁目6
m BAY POINT 幕張低層棟2F（勤務先）
E-mail：nhatanaka@risk-strategy.jp

ウを整理したITIL（Information Technology Infrastructure Library）のプロセスから一部流用する形で，**表・1**に整理した．

時系列的にみると，最初の2件のA,Bの大学付属病院の大病院で，サイバー攻撃を試みるが，横展開も権限上昇も確認できない．大きな病院の情報システムは，ネットワークトラフィック全体をリアルタイムで監視・分析し，社内ネットワークに侵入した脅威を早期に発見するためのNDR（Network Detection and Response）の仕組みや，ネットワークを細かく分割（セグメント化）し，セグメントごとにアクセス制御を行い，内部からの攻撃や情報漏洩を防ぐマイクロセグメンテーションの仕組みができていたものと思われ，被害は小さい．次に攻撃者は，より規模の小さい病院に目標を定め，E医療センター，F町立病院，G地域病院を狙っている．いずれも，権限上昇と横展開が認められ，取得していたバックアップまで，ラムサムウェア攻撃の被害に遭い，暗号化されている．バックアップの使用に情報システムを復元できないF町立病院は復旧に2カ月を要し，G地域病院は復旧に4カ月を要している．

この二つの病院事例ではネットワークを細かく分割（セグメント化）や，ネットワークトラフィック全体をリアルタイムで監視・分析の効果が認められない．

次の二つのI地域病院，J地域病院では，時系列的に，あとの方で発生していることから，発生した過去の事例の教訓が生き，対策の準備が整っていたと考えられる．I地域病院は，予備のデータを用いて診療を継続し，J地域病院はシステムダウンの間，医療業務を一時停止していたが，バックアップにより情報システムを復旧している．I地域病院は患者の待ち時間が長くなる程度で復旧し，J地域病院はシステムの回復まで，診療業務を停止する程度で復旧している．

いずれの病院も，懸念されるインシデントが現実化した対応は，汚染された区域を情報システムから分離するで，対応には問題があるとはいえない．しかし，公表された事実のみから判断する限り，問題が発生した場合の不適合の解消は，現物処置に終わり，ITILが要求する是正処置のループは回っていない．攻撃者に再度，狙われる可能性がある．

3．予防的処置と事後的処置

3.1　予防的処置の例

予防的処置の例として，脆弱性診断サービスとペネトレーションの例を挙げる．

ところで，脆弱性診断サービスとペネトレーションをおなじものとする者がいるが，別物である．脆弱性診断サービスには，「脆弱性には“対象の網羅性”と“脆弱性の網羅性”の2つが含まれる」[2]と定義され，2つの意味合いで脆弱性診断を実施する．また，同様に，ペネトレーションとは「対象のシステムやアプリケーションに潜む“脅威に到達可能な経路を見つけだすこと”を目的として実施する．またクライアントからのヒアリングを基に“クライアントが想定している攻撃者”と“クライアントが懸念している脅威（シナリオゴール）”の2つを慎重に定義し，定義したシナリオゴールを目指してテストを開始する」[2]と定義する．

3.1.1　脆弱性診断サービスの大きな流れ

国際ウェブセキュリティ標準機構（OWASP：The Open Web Application Security Project）と1999年に発足した非営利組織のMITRE（マイター）がある．

世界中に数百の支部と数万名の会員から，脆弱性の情報を収集し，脆弱性の致命度の上位10項目をOWASP TOP 10として発表し，日本にもその支部が存在する．MITRE（マイター）はアメリカ政府の出先機関で，会員にはNIST，ISACAが含まれ，民間企業と連携し，国家安全保障，公共安全，ヘルスケア，サイバーセキュリティを扱う．また，個別製品中の脆弱性を対象として，共通脆弱性識別子（CVE：Common Vulnerabilities and Exposures）の採番を行い，ソフトウェアにおけるセキュリティ上の弱点を識別するための共通脆弱性タイプ一覧（CWE：Common Weakness Enumeration）の共通基準を定めている．脆弱性の重要度のスコアリング方法としては，2004年に発足したFIRST（Forum of Incident Response and Security Teams）が提示する，共通脆弱性評価システム（CVSS：Common Vulnerability Scoring System）がある．

3.1.2　OWASP TOP 10（2021年から2025年の変化）

OWASP TOP 10で注目すべき点は，ほとんどの項目の順位は変化していないが，A03：2025-ソフトウェアサプライチェーンの失敗が順位3位に割り込んでいる．これは，ソフトウェアサプライチェーンの構成要素の依存関係に内在するリスクのことで，Javaベースのロギングユーティリティの Apache Log4j の攻撃事例がある．Log4jの更新時に，リモートで実行可能な悪意のあるコード（ミュタント）が埋め込まれ，多くのシステムに影響が出た．その他の例として，SolarWindsの攻撃事例がある．悪意のあるコードは，

表・1　病院のランサムウェア被害

病院名	情報資産	付け入った脆弱性	被害の程度	攻撃の到達度				対策		
				侵入	権限上昇	横展開	バックアップに到達	封じ込め・ドロップ（破棄	バックアップから復元	分離（セグメンテーション）
1. A 大学付属病院	患者の CT	PC の持ち込み	検査装置が使用できない	小	—	小	—	×	—	○
2. B 大学付属病院	患者の治療情報	PC の持ち込み	実害なし	—	—	—	—	○	—	—
3. C 市立病院	電子カルテ	サーバ，端末	医療費補助の償還遅れ	有	—	有	—	×	—	×
4. D 医療センター	患者の個人情報	メールの添付ファイル	医師の PC が使用できない	有	—	有	—	×	—	—
5. E 医療センター	患者の CT や MRI 画像	ソフトの脆弱性	相当時間後に復旧	有	有	大	有	×	×	×
6. F 町立病院	電子カルテ	明確でない（APT 攻撃？）	復旧に 2 ヵ月	有	有	大	有	×	×	×
7. G 地域病院	電子カルテ	VPN の脆弱性	復旧に 4 ヵ月	有	有	大	有	×	×	×
8. H 大学付属病院	電子カルテ，会計情報	記憶媒体の持ち込み	一時停止	有	—	大	—	×	—	×
9. I 地域病院	電子カルテ	明確でない	患者の待ち時間増大	有	—	—	—	×	○予備データ	×
10. J 地域病院	電子カルテ	明確でない	診療業務の一時停止	有	有	有	—	×	◎	×

個人情報

ウイルス（ホストファイルを起点とした感染する悪意のあるプログラム），ワーム（ネットワークを介して感染する悪意のあるプログラム），ミュタント（感染性はないが，悪意のあるプログラム）は区別して，用語を用いるが，使用者が信用するユーティリティの中にボットが仕組まれた事例である．

3.1.3　IPA の情報セキュリティ 10 大脅威 2025

日本の IPA も，OWASP と同様に，毎年，情報セキュリティ 10 大脅威を発表している．「サプライチェーンや委託先を狙った攻撃」が 2 位に浮上している．内容は，第 2 章で紹介したように，情報セキュリティの弱い組織を狙って，攻撃を仕掛けられたように，委託先が狙われることを，注意喚起している．

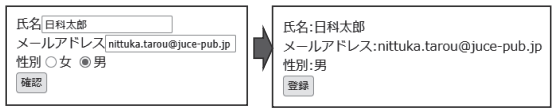
3.1.4　脆弱性診断サービスの診断ツール

自動実行のツールの知名度が高いのは，OWASP の OWASP ZAP で，手動実行ツールとしては，PortSwigger Ltd. の Burp Suite Professional がある．両方とも無料版があり，Burp Suite Professional の有料版と無料版の違いは，脆弱性診断サービスのツールを実行させたときに，記録が取得されるかの違いで，認証チェックで，画面間を跨って，脆弱性をチェックする場合は，Burp Suite Professional が優れている．

図・1，**図・2**，は，クロスサイトスクリプティングの例である．図・1 の画面で，日科太郎，メールアドレス，ラジオボタンで男性を選択し，登録するプログラムを作成したものを，脆弱性のツールに掛けた結果が，図・2 に示される．

図・2 で，REQUEST は，画面にペイロード（各通信階層の送信情報からヘッダー部分を取り除いた部分）を入力した場合のサーバに送信されるヘッダーとペイロードが示される．ペイロードの値は，日科太郎，メールアドレス，男性である．RESPONSE は，サーバ側の実行結果を示す．HTTP/1.1 200 OK がでているので，問題なくプログラムが終了したことを示している．

一見，何も問題が無いように思えるが，注目すべきは中央部に出力された脆弱性の警告である．一行目の「Content Security Policy（CSP）ヘッダーが設定されていない」は「Content Security Policy（CSP）は，クロスサイトスクリプティング（XSS）やコードインジェクション攻撃などの特定の攻撃を検出・軽減するための追加セキュリティ機構で，これらの攻撃はデータ窃取，サイト改ざん，マルウェア配布など様々な悪意のある活動に利用される．CSP は Web サイト管理者がブラウザに対してページ上で読み込み許可するリ



図・1　画面への入力と出力結果

ソースの信頼できるソースを宣言するための標準 HTTP ヘッダー群を提供し，制御対象には，JavaScript，CSS，フレーム，フォント，画像，メディアファイルなどの各種リソースが含まれる」の警告が出力され，警告レベルは high であることが示される．

ログイン時に，サーバから発行される認証キーが奪われ，不正ログインされることを言っている．

3.1.5　ソフトウェア製品の最終検査試験と受入検査

バグは，ソフトウェアの設計の瑕疵事項として認識されているが，システムの脆弱性となると，ソフトウェアのバグ，設定ミス，設計のチェック漏れであることを認識する者は少ない．ソフトウェア開発モデルのスパイラルモデルでは，一画面ずつ，脆弱性のチェックが行え，ウォータフォールモデルでは，要求定義，機能設計段階で，脆弱性の有無のデザインレビューやウォークスルーにより，脆弱性チェックの漏れを無くすことができ，設計の後半の検証段階では，レッドチームを編成し，脆弱性診断を実施すべきである．

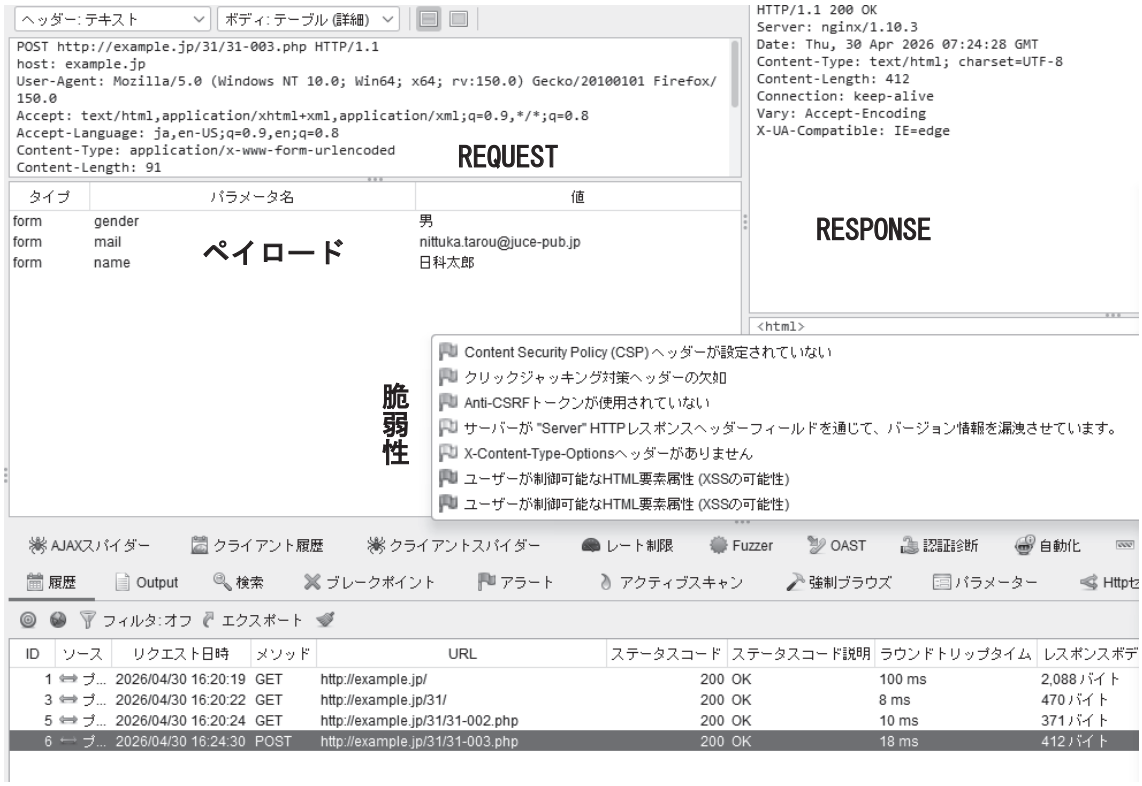
このように，すべての活動が終了し，最終検査・試験に合格して，ソフトウェア製品の受取手側に引渡すことができる．一方，受取手側は，受入検査に，脆弱性診断を検査の項目として入れ，受入れの可否を判定する．

バグがソフトウェアの設計の瑕疵事項であるのと，同様に，システムの脆弱性は，運用段階の設定不備を除いて，設計のチェック漏れである．

3.1.6　脆弱性の品質管理特性

品質管理特性とは品質の悪さを表現し，それをコントロールすることにより，品質を良くするものである．ソフトウェア開発の従事者はバグについて，試験や，市場での使用を通して，バグを検出し，対策を取って，残存バグの推定値を徐々に低減してきた．死滅曲線の ETGM，GTGM モデルの漸近線を推定全バグとし，指標は，残存バグ数や MTTF で表現される．残存バグ 5% では MTTF 100 時間，残存バグ 1% で 1,000 時間の指標を作り出し，出荷基準としている所も多い．

脆弱性についても，同様に，適切な品質管理特性を選定し，市場に負担を掛けるのではなく，自己の設計行為の中で，十分に脆弱性のチェックを行って，次の



図・2　OWASP ZAP の画面

設計プロセスに引き渡す責任がある．

3.2　事後的処置の例

ファイアウォールと一体化して動作するプロキシの設定である．ファイアウォールの機能には，IP アドレスとポート番号に基づいて，通信を制御する機能と，通信のふるまいを見て，侵入や攻撃を検知し，防御（ブロック）する機能がある．プロキシには，ブラックリスト，ホワイトリスト，シグネチャの情報を蓄える機能があり，ブラックリストは悪意があると見なされた許可されないリストの集まりで，ホワイトリストは，サーバ等へのアクセスを許可するリストの集まりである．シグネチャは攻撃のパターンを集めたもので，攻撃の兆候を見逃さないことで，悪意のあるアクセスはドロップ（破棄）し，侵入された場合には，封じ込めを行う．

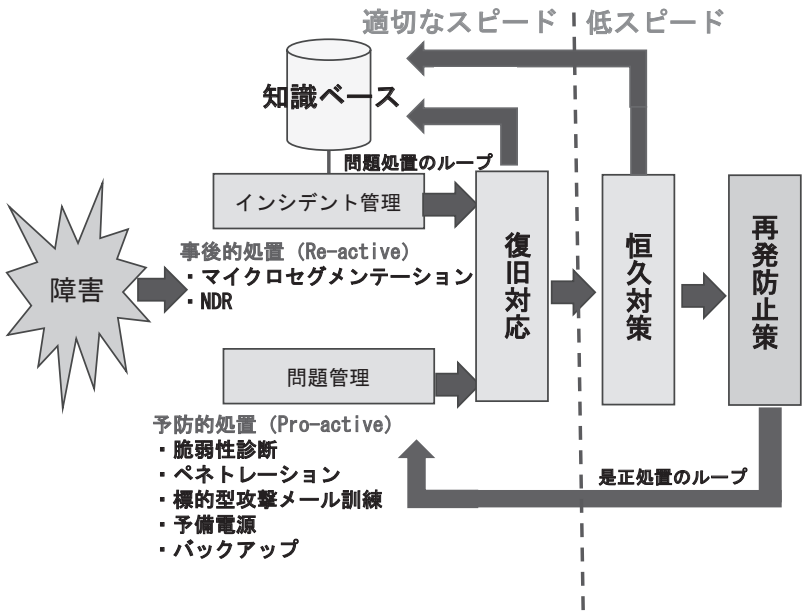
3.3　是正処置のループ

図・3 の内側のループは問題処置のループで，是正処置のループは外側のループである．第 2 章の病院の事例では手術待ちの患者や，救急で運ばれる患者を想定すると，病院の機能が停止することは社会的影響が大きい．内側の問題処置のループは速く回し，外側のループは時間を掛けても，原因を掴んで，再発防止策を打たなければ，同じ攻撃の手口で，サイバー攻撃を受ける可能性がある．

4．アサヒ GHD の事例

アサヒ GHD は，「2025 年 9 月 29 日午前 7 時頃，発生したシステム障害に対する調査で暗号化ファイルを確認し，9 月 29 日午前 11 時にネットワーク遮断，データセンターを隔離措置した．侵入経路については，システム障害発生の約 10 日前に，グループ内の拠点にあるネットワーク機器を経由（通過）し，アサヒグループのネットワークに侵入したことが判明．その後，アサヒグループの主要なデータセンターに侵入した．

内部活動としては，パスワードの脆弱性を悪用し，管理者権限を奪取した．奪取した管理者アカウントを不正利用してネットワーク内を探索し，主に業務時間外に複数のサーバへの侵入と偵察を繰り返した．



図・3　問題処置のループと是正処置のループ

情報漏えいが発生またはそのおそれがある個人情報は，アサヒビール株式会社・アサヒ飲料株式会社・アサヒグループ食品株式会社各社のお客様相談室に問い合せした人の個人情報が，152.5 万件（氏名，性別，住所，電話番号，メールアドレス），祝電や弔電などの慶弔対応を実施した社外の関係先の個人情報が，11.4 万件（氏名，住所，電話番号），従業員情報（退職者を含む）が，10.7 万件（氏名，生年月日，性別，住所，電話番号，メールアドレスなど），従業員（退職者を含む）の家族の個人情報が，16.8 万件（氏名，生年月日，性別）」と発表した[3].

しかし，横展開されていることから，認証（身元調査）のみでなく，認可（権限の付与）も攻撃されていると考えられ，これを管理する AD（Active Directory）には脆弱性があり，ゼロディ攻撃を仕掛けられた可能性がある.

5．結論

システムの脆弱性は上流工程である設計行為のチェック漏れにより生じ，市場に負担を掛けるのではなく，十分に設計のチェックを行って，ソフトウェア製品の受取手に引き渡すべきである.

また，医療機関の分析事例，アサヒ GHD の事例を傍観するのではなく，明日は我が身と，情報システムを見直すことが緊急の課題である.

次の三つの要点を結論とする.

・システムの脆弱性は，設計のチェック漏れ
・是正処置のループを回し，再発を防止する.
・予防的処置，事後的処置により，防御を強固にする.

参考文献

［1］畠中伸敏(2025)：「サイバーセキュリティと個人情報保護」，日科技連出版社.
［2］川田柾浩(2024)：「ペネトレーションの教科書」，DATAHOUSE.
［3］アサヒグループホールディングス株式会社(2025.11.27)：“サイバー攻撃による情報漏えいに関する調査結果と今後の対応について”，アサヒグループホールディングス株式会社.
(https://asahigroup-holdings-ir-umb.azurewebsites.net/media/5tejpt3z/20251127j3)