サイバーセキュリティ対策の見える化と継続的な取り組み環境の整備

ジスインフォテクノ株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

相澤　雅典

2003 年　ゼオン情報システム（株）入社
2005 年　ジスインフォテクノ（株）社名変更
2007 年　全社ネットワーク(LAN/WAN)担当
2014 年　セキュリティワーキンググループ
　　立ち上げ
2018 年　現在 システム運用部運用チーム
　　サブリーダー

■ 論文要旨 ■

大企業での情報漏洩事件などサイバーセキュリティの脅威が増大する中、当社の顧客(日本ゼオン)においても、インシデントが多数発生するようになっており、喫緊の問題となっていた。その問題解決のために、過去の情報セキュリティ対策を振り返り、自社業務に合うセキュリティ対策評価フレームワークの選定を行い、現状を評価した。その結果 20 の診断項目のうち、継続的な脆弱性診断と改善、境界防御など６項目のコントロールに課題があることが判明した。洗い出された課題を元に、定期的な脆弱性診断や外部からの侵入防止の仕組みの導入などの対策を行った。さらにこれらの活動を継続的に行うための組織を発足し、PDCA サイクルが回るような工夫を行った。これらの取り組みの結果、検討開始から２年で、６項目のコントロール課題を 2018 年度中に解決する見通しが立つと共に、事後対応ではなく事前対応型のセキュリティ対策を実行できる体制が整った。

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要

当社の顧客である日本ゼオンは、合成ゴム/高機能樹脂などを製造販売する化学メーカーである。従業員は 3,328 人（連結：2018 年３月末）であり、日本国内のみならず、欧米、アジアにも拠点がある。

ジスインフォテクノ（ZIFTEC）は、日本ゼオンの IT（基幹業務、社内 Web システム、メールなどのコミュニケーションインフラ）を開発/保守運用を一貫して行っている。元は日本ゼオン電算部として設立され、1994 年にゼオン情報システムとして分社化し、2005 年に富士通より 51%の出資を受けた、戦略的アウトソーシングの IT 会社である。

私はジスインフォテクノのシステム運用部システム運用チームに所属し、ネットワークインフラ（LAN/WAN）を主に担当している。

2014 年初頭、大企業での情報漏洩事件などを契機に、サイバーセキュリティに重要性が叫ばれる中、お客様内でもセキュリティインシデントが発生するようになり、その対応に追われるようになっていた。そこで、ジスインフォテクノではサイバーセキュリティを総合的に検討する企画を立ち上げ、私が担当することとなった。

２．取り組み開始の状況と振り返り

２．１　それまでの日本ゼオンの情報セキュリティに関する取り組み

ジスインフォテクノが IT サービスを提供する日本ゼオン内での情報セキュリティに関する取り組み自体は、2002 年から始まっており、情報セキュリティ規程の整備や、情報セキュリティ教育を進めていた。

その２年後の 2004 年は個人情報保護法/不正競争防止法の施行もあり、より情報セキュリティの重要性が認識される状況となった。経営をはじめ関連部署（法務/人事総務/情

報システム）で ISO/IEC17799 に基づくトータルセキュリティコンサルティングを受け、現状評価と活動の具体化を行った。情報システム部が主管となって取り組むべき課題（主にサイバーセキュリティ）については日本ゼオン情報システム部とジスインフォテクノが連携し、対応を行った。

【表１】ISO17799 で定義された情報セキュリティ領域と情報システム部門の役割表

NO	セキュリティ領域	情報システム部	ジスインフォテクノ
1	情報セキュリティ基本方針	○	－
2	組織の情報セキュリティ	－	－
3	資産の分類および管理	－	－
4	人的情報セキュリティ	－	－
5	物理的及び環境的セキュリティ	○	－
6	通信及び運用管理	○	○
7	アクセス制御	○	○
8	システムの開発及び保守	○	○
9	事業継続管理	－	－
10	適合性	－	－

３．発生した問題と課題

３．１　発生した問題

2013 年頃から、不審な E メールが従来のウィルス対策を潜り抜けて、お客様のパソコンがウィルス感染する事故がたびたび発生するようになった。主な攻撃手法はパターンマッチングでは検知できない未知の Word マクロウィルスを添付する方法であった。この攻撃は、プログラムの振る舞いを検知するシステム（IDS/IPS）があれば防ぐことができたと考えられる事象でもあった。しかし、その当時のメンバーは、IDS/IPS がないことのリスクを認識していたわけでもなく、明確に受容していたわけでもなかったのである。

システムの利用環境にも大きな変化があり、モバイル端末の増大、海外関連会社とのネットワーク相互接続など、利便性の向上と比例する形で、セキュリティリスクが増大し、これまでの運用/対策の延長では対応しきれない状況になりつつあった。これらの問題が本取り組みのきっかけとなった。

３．２　見えてきた課題

取り組みを始めた 2014 年のジスインフォテクノのサイバーセキュリティ対策の状況は、2004 年頃に定義された取り組みを個々に継続する（IT 機器については老朽化更新）にとどまっていた。そのため、当時の対策だけでは対応できない攻撃によってシステムが破壊される、情報漏洩が発生するリスクがあった。私たちは”なぜこのような状況であるのか”を分析した。方法としてサイバーセキュリティを検討するワーキンググループを立ち上げ、運用/開発関係者にヒアリングする形式で行った。その結果、大きな課題が以下の 3 点にあるのではないかと仮定した。

（1）事象発生前に先手の対応ができていない。
サイバーセキュリティ対策は、リスクが顕在化してから対応という後手後手の状態であった。従来から運用していたファイヤーウォールやアンチウィルスの対策も、きっかけは 2000 年代前半に発生した大規模ワームウィルス（Nimda（ニムダ）、Blaster（MS ブラスト））の流行があっての対応であり、ジスインフォテクノとして提供すべきサービス（対策）はなにかを明確にできていなかった。

（2）最新セキュリティ情報の収集
サイバーセキュリティのトレンドの変化（外部からのサイバー攻撃の激化、巧妙化）に気づけていなかった。情報セキュリティの対策は日本ゼオンからの指示待ちであり、主体的にセキュリティの情報を収集できていなかった。

（3）システム全体を見通したセキュリティ対策の立案
サイバーセキュリティ対策で実行したファイヤーウォール等の評価/見直しは個別対策ごとの見直しにとどまっており、全体としての評価/見直しは行っていなかった。

見えてきた課題を解消するべく、ワーキンググループは活動を始めた。

４．課題に対する取り組み

４．１　施策に取り組むときに満たすべき条件

改めて、サイバーセキュリティ対策を考えるにあたり、満たすべき条件としたことは２点である。

ひとつめは「定量的な評価を元にサイバーセキュリティ対策を見える化し、顧客である日本ゼオン情報システム部の納得感を得る」ことである。今までの”リスクが顕在化してから対策”であれば、対策の納得感自体ははすぐ得られる。しかし、予防措置として先手先手で対策する場合は、すぐに何かの役に立つわけではない。よって、客観性があり、だれが聞いても対策に納得感があるように提案しなければならないと考えたからである。

ふたつめは「ジスインフォテクノとして、一過性ではなく継続的に改善できる仕組みにする」ことである。継続的な改善の仕組みにするという目標は、過去の反省から、絶えず PDCA サイクルを回さなければ、検討したことも忘れ去られてしまうと考えたからである。

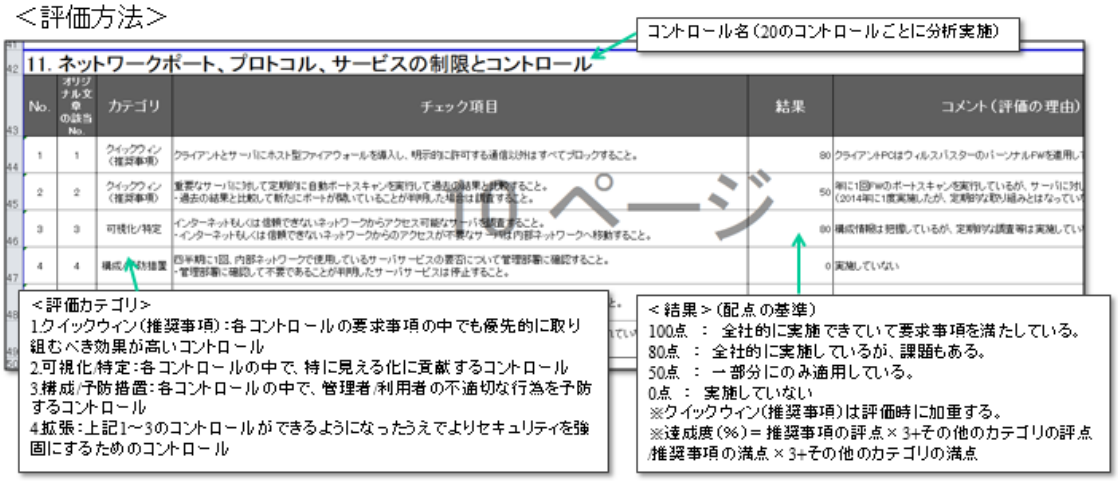
４．２　フレームワーク利用による評価

顧客情報システム部の納得感を得るために取り組んだことは、システム/運用/人など様々な角度から現状を評価することである。評価は外部の信頼できる客観的な基準を基とした分析をすることが有用と考えた。これは自分たちの立てた仮説（課題）の認識があっているのかを確かめたいとも考えたからである[参考文献１]。

セキュリティ対策評価のために用いたフレームワークは Critical Security Controls

（CSC20）［参考文献２］であった。様々なフレームワークや評価基準がある中、選定した理由としてはセキュリティは日進月歩であるので“比較的最近発表されたしくみのほうがよい”ということと、システム運用業務をベースに項目が設定されており、自身の業務（システム運用）にあっていると考えたからである。よって、CSC20 をベースに評価を行うことにした。CSC20 を読み込み、要求項目を１問１答のチェックシート形式に変換した（図１）。加えてインタビュアーによって、結果に差異が出ないよう配点の基準を作成した。

＜評価方法＞

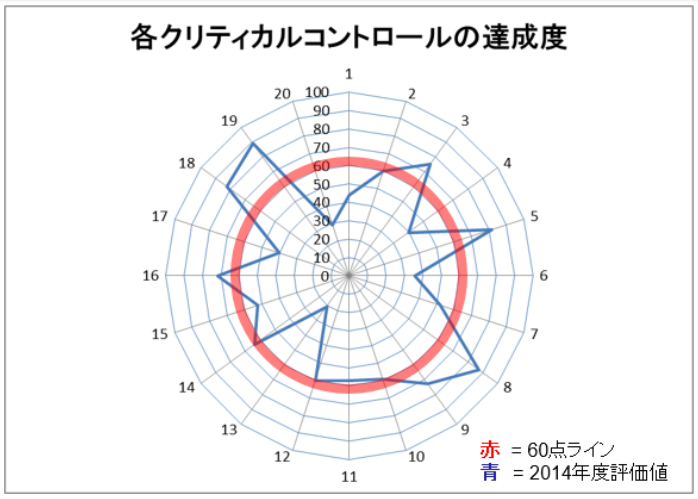


【図１】Critical Security Controls(CSC20)に基づく評価

評価を行うにあたり、どこまでできていれば合格とするかという基準の設定にも留意した。CSC20 のフレームワークはアメリカ政府（公官庁系）/重要インフラ/金融系企業の提案が採用されているためか、要求レベルが非常に高いものであった。そのため、推奨する対策/体制をすべて整えることは現実的ではないと考えた。外部セキュリティベンダーの意見も参考に“グローバルで活動する化学系メーカーであれば、短/中期的に達成しておきたいセキュリティレベル”（≒60 点）を満たすことを最低ラインとして設定した。

自社内の各部門（開発/運用/ヘルプデスク）と日本ゼオンの情報システム部にそれぞれインタビューする形式で現状を評価した。CSC20 で定義されている 20 項目（クリティカルコントロール）すべてに対して評価を行った（図２）。その結果、設定した基準を満たしていない６項目があった（表２）。

＜評価が低かったコントロール＞
1. 許可された機器と無許可の機器のインベントリ
4. 継続的な脆弱性診断と改善
6. アプリケーションソフトウェアのセキュリティ
13. 境界防御
17. DLP（Data Loss Prevention/情報漏えい対策）
20. ペネトレーションテストおよびレッドチームの訓練



＜コントロール一覧＞
1. 許可された機器と無許可の機器のインベントリ
2. 許可されたソフトウェアと無許可のソフトウェアのインベントリ
3. ラップトップ、ワークステーション、およびサーバでのハードウェアおよびソフトウェアのためのセキュアな構成
4. 継続的な脆弱性診断と改善
5. マルウェアの防御
6. アプリケーションソフトウェアのセキュリティ
7. 無線機器のコントロール
8. データ復旧能力
9. 不足を補うためのセキュリティスキル診断および適切なトレーニング
10. ファイアウォール、ルーター、およびスイッチなどのネットワーク機器のためのセキュアな構成
11. ネットワークポート、プロトコル、サービスの制限とコントロール
12. 管理権限のコントロールされた使用
13. 境界防御
14. 監査ログの保守、モニタリング、および分析
15. 知る必要性に基づいたコントロールされたアクセス
16. アカウントのモニタリングおよびコントロール
17. DLP（Data Loss Prevention、情報漏えい対策）
18. インシデントレスポンス能力
19. セキュアなネットワークエンジニアリング
20. ペネトレーションテストおよびレッドチームの訓練

【図２】各クリティカルコントロールの達成度

【表２】評価が低かったクリティカルコントロールと改善目標

No	評価の低かったクリティカルコントロール	主な改善目標
1	許可された機器と無許可の機器のインベントリ	資産管理ツールと管理台帳が自動連動していること。
2	継続的な脆弱性診断と改善	セキュリティパッチ、ウィルスパターンファイルの自動配信に関し、その効果を定期的に確かめる仕組みがあること。
3	アプリケーションソフトウェアのセキュリティ	Web アプリケーションセキュリティ監査をインターネットに接続するシステムについて行っているのみならず、内部にも悪意がある前提で対策すること。
4	境界防御	パターンマッチングでは検知できないマルウェア対策を実施すること。
5	DLP（Data Loss Prevention/情報漏えい対策）	大量のデータ送受信、機密情報への定期的なアクセス、異常なプロトコルとポートの使用等を即座に検知できる仕組みを実装すること。
6	ペネトレーションテストおよびレッドチームの訓練	実際の攻撃者の手段を模した攻撃、およびそれに対応する訓練を行うこと。

４．３　自己評価に基づく対応方針の決定

評価の結果を元に点数が低かったクリティカルコントロールから改善することとした。セキュリティは桶に入る水の絵に象徴されるように、低いところから溢れる（攻撃される、情報漏洩する）とされているからである。また設定した基準を満たすために各クリティカルコントロールの要求事項の中でも改善目標との関連が高く、優先して対応すべき推奨事項（クイックウィン）から対応することとした（表３）。ただし、”ペネトレーションテストおよびレッドチームの訓練”コントロールは、攻撃者の手段を模した攻撃に

対応する訓練のため、各サイバーセキュリティ対策が完了してから最後に実行することにした。このように客観的かつ/定量的に評価することで、顧客に納得していただいたうえで、各種施策を提案し、実行までつなげることができた。

【表３】評価が低かったクリティカルコントロールに対する推奨事項(クイックウィン)

No	評価の低かったクリティカル コントロール	推奨事項（クイックウィン）の具体例
1	許可された機器と無許可の機器のインベントリ	資産管理ツールを使用して組織内ネットワークに接続された機器の管理表を自動的に作成する仕組みの導入
2	継続的な脆弱性診断と改善	定期的にシステムに対して脆弱性スキャンツールを自動化して実行すること。
3	アプリケーションソフトウェアのセキュリティ	WAF（Web アプリケーションファイヤーウォール）の導入
4	境界防御	・ネットワーク型 IPS を導入して、不正な通信をブロックすること。 ・キャプチャデータをイベント情報管理（SIEM）に送信して、他の機器からの情報/ログなどと共に相関分析を行うこと。 ・アドレス詐称されたメールを受信しないためにメールサーバで SPF を導入すること。
5	DLP（Data Loss Prevention/情報漏えい対策）	・持ち運び可能なクライアント、モバイルマシンのハードディスクを暗号化すること。 ・持ち運び可能なストレージメディアは、データ書き込みと同時に自動的に暗号化されるよう構成すること。
6	ペネトレーションテストおよびレッドチームの訓練	定期的に、外部ネットワーク及び内部ネットワークから社内システムに対してペネトレーションテストを実行すること。

本論文では、「継続的な脆弱性診断と改善」と「境界防御」の取り組みを一例として紹介する。

４．３．１　対策例①継続的な脆弱性診断と改善

サイバーセキュリティシステムの導入・対策・体制の整備が完了後、そのセキュリティ対策に問題がないか、診断を年１回行うように運用を開始した（表４）。診断の結果、発見された脆弱性は、ジスインフォテクノの各チームのシステム担当にフィードバックを実施し、診断担当者は少なくとも１年以内に問題点を解消するように依頼した。対策が確実に行われているかどうかモニタリングし、必要に応じて助言も行った。

【表４】継続的な脆弱性診断の内容

年度	実施内容
2014	・アタックテスト（認証基盤/情報共有基盤/グループウェア等主要サービス） ・Web セキュリティ診断（外部公開 Web システム）
2015	アタックテスト（海外業務委託サーバ、ベンダー主体の構築サーバ等）
2017	標的型攻撃診断（標的型攻撃の手法を用いた模擬攻撃試験）

※2016 年度は IT 基盤の大幅な変更を行ったため、見送り

４．３．２　対策例②境界防御

インターネットと社内 LAN の接続点を見直し、従来のアンチウィルスパターンによらない不正通信を捕捉し、検知/遮断できるような仕組みを導入した。従来型のファイヤーウォール等の対策に加え、通信の振る舞いで脅威を検出する IPS/IDS と、メールの添付ファイルや改ざんされたサイトからの脅威を検出するサンドボックスを組み合わせて、不正なファイルが利用者の端末まで届かないような形に改善した。

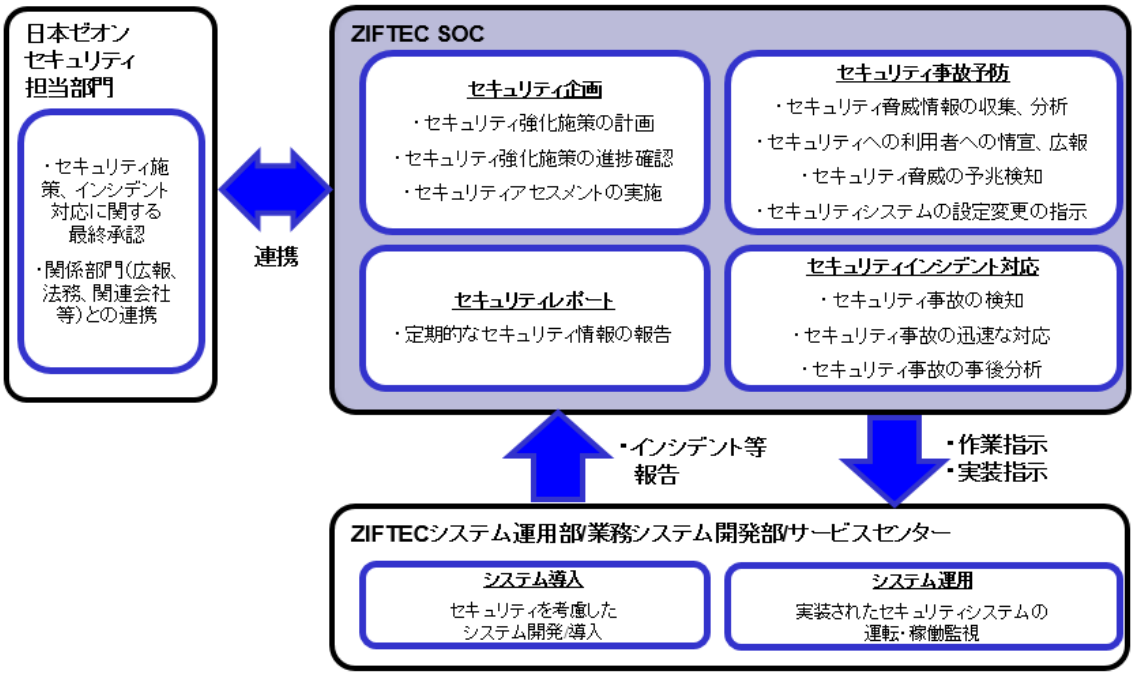
４．４　継続的な取り組みのための仕掛け

サイバーセキュリティ対策が継続的に機能/改善を続けるために、必要なことは自社と情報システム部だけの検討にとどめず、日本ゼオングループ全体の取り組みにする必要があると考えた。そのためには、本活動を日本ゼオンの情報システム部だけではなく、企業の危機管理全般を取り扱う部門にも認知してもらおうと取り組んだ。具体的には“重大なサイバーインシデントの発生時の対応フローの定義“を行い、自社の動きに加え、情報システム部および関連部門の動きも定義した。作成したフローは全関係者でレビューをし、認識を共有するという活動を行った。

一般利用者向けには活動を認知してもらうための定期的な広報/レポートを発行することにした。四半期ごとにサイバーセキュリティレポートを発行すること、セキュリティ事故が発生しやすいとされる長期休暇前や、重要インシデント発生時に利用者目線での注意喚起情報を発信することとした。

これらの役割を継続的に行えるように、ワーキンググループの検討内容を引き継ぐ組織を社内に常設することにした。組織作成のポイントは役割と既存チームとの関係性を明確に定義することであった。JPCERT/CC の CSIRT ガイド[参考文献３]などを参照し、どのような組織にするかをワーキンググループ内で議論した。一般的には親会社内に CSIRT を結成し、ジスインフォテクノのようなシステム子会社は SOC（セキュリティオペレーションセンター）のような役割を担うのが一般的である。しかし、それでは従来の主従関係を打開できず、指示待ちの組織になってしまうのではないかと考えた。そして CSIRT の主な役割であるインシデントのハンドリングや SOC の異常検知の機能だけではなく、広く予防的な企画活動も実施したいという思いがあった。

そこで新しい組織の役割を“企画”、“事故予防”、“レポート”、“インシデント対応”と PDCA のサイクルをすべて担い（図３）、日本ゼオンの関係部署とジスインフォテクノ内の既存の組織をつなぎ、サイバーセキュリティを広く統括することを目標とする組織にした。組織の名称は ZIFTEC CSC（サイバーセキュリティセンター）とした。

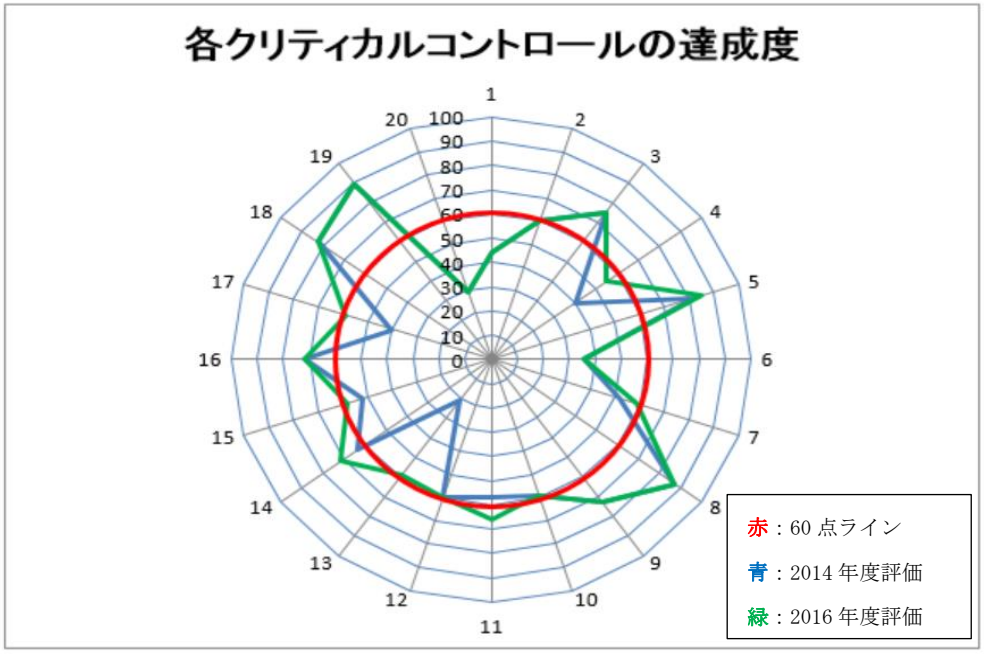


【図３】ZIFTEC CSC（サイバーセキュリティセンター）機能定義図

５．取り組みの成果

５．１　現在の状況

活動開始から、２年が過ぎた 2016 年終了時に、CSC20 に基づき再評価を行った。その結果、取り組み開始時に比べ各要素のレベルが上がってきた（図４）。2017 年以降も資産管理の改善等の取り組みを行い、検討の最後に行うとしたペネトレーションテストの実行を計画するフェーズにまで来ている。2014 年に描いた“60 点の円“は 2018 年度中に達成される見込みである。



【図４】2014 年度と 2016 年度終了時の達成度比較図

ZIFTEC CSCも定期的に活動を行い、社内外にその活動が認知され、利用者の意識も徐々に向上している。2018 年初に標的型メール攻撃訓練を行った際に行ったアンケートでは、事前の啓もうや教育で気づくことができたという意見を多数いただいた。サイバーセキュリティの必要性が、経営層や、情報セキュリティの関係者、一般利用者まで広く認知されてきている。[参考文献４]

６．今後の展望

６．１　重要機密情報保護の取り組み

サイバーセキュリティ対策で、最終的に守らなければいけないものはシステムそのものではなく、そこで扱う機密情報であると考えられる。現在までの取り組みは、世間動向などを調査し、ある一定レベルでのインターネットからの攻撃や一般従業員の不正から広くシステムを守るという観点で進めてきている。今後は、例えば情報資産の管理方法や物理セキュリティなどに、サイバーセキュリテイの考え方も取り入れていき、機密情報保護にも効果的なセキュリティ対策を提案していきたい。

６．２　IoT など新しい要素技術への対応

IoT など従来インターネットに接続することのなかった機器の活用が企業で進んでいる。そしてIoTを狙ったサイバー攻撃も多数発生している現状がある。日本ゼオンでも今後のビジネス拡大のためにIoT活用を進めている。IoT活用にあたり、サイバーセキュリティが足かせにならなず、安心して活用できるようにしていきたい。今回構築した仕組みを愚直に運用し、定期的に外部からの情報収集等を行い、迅速に対応できるようにしたい。

６．３　最後に

2014年度から取り組んできたサイバーセキュリティへの取り組みは、2018年度には当初の目標にかなり近づける状況まで進んできている。しかし、サイバーセキュリティ対策は完了形はなく、常に最新の動向とお客様の状況を把握しながら、対策し続けなければならない。そうしなければ、たちまちレベルが下がり、重大な問題が発生してしまう恐れがある。道はまだまだ半ばであると考えている。今後も引き続きサイバーセキュリテイの品質の維持・向上に勤めていきたい。

以上

参考文献

［１］経済産業省：情報セキュリティ管理基準
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf
［２］米国CIS（Center For Internet Security）：効果的なサイバー防御のためのCIS クリティカルセキュリティコントロール（翻訳：NRIセキュアテクノロジーズ）
https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-CSC_v6.1_Japanese_Final_r1.pdf
［３］JPCERT/CC：CSIRT ガイド
https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf
［４］経済産業省：サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/mng_guide.html