2021年度　セキュリティ対策研究会　活動報告

1. 研究会開催の趣旨とその結果

不正アクセスなどのサイバー攻撃は、より高度に巧妙になってきており、ここまでやれば良いという目安がわからなくなっている。一方、コロナ対応として急激にテレワーク化が進み、これは今後も引き続き活用されていくと考えられる。併せて各種クラウドサービスの活用も次第に進んできている。これは今までの“社内”という境界線がなくなることであり、会社支給 PC に限らないスマートフォンなどを含めた多様な機器活用の要望も含め、『統制』と『いつでもどこでも』という働きやすさとのバランスを常に求められることとなっている。

この様な環境変化の中、企業経営にも重大な影響を及ぼすようになったセキュリティに関する取り組みも、変わっていく環境に対応するダイナミックな取り組みに変わらなくてはならない。つまり、デジタル化・デジタル活用の流れはますます勢いを増していくのであり、そこにおいては今までのように「囲って守る」という考え方ではない取り組み方が求められる。現在、変革の流れから取り残されてしまわぬよう、そして情報資産を保全できるよう、どう自社の変革を進めるのか、それを踏まえてどのような対策を進めるべきかをご参加の皆さんと検討した。

それぞれの状況であり、IT 環境も異なる中、共通的に重要な対策として、認証基盤の充実であり、利用者全員のリテラシー向上であろうという方向性が見出された。そして経営トップの方々の理解やリスクマネジメントの一環として情報セキュリティに取り組むよう努力というポイントも確認された。

今回ご参加頂いた皆様には、自社での対応の中心となり、これらの内容の実現に向けて取り組んで頂きたいと願っています。

2. 参加企業名　　ご参加者　5社　5名

アドバイザー ・ 部会長紹介

・部会長　　内田昌宏 （LAC）

・アドバイザー　野口　勝 （㈱イフェクト）

橋本（ストーンビートセキュリティ㈱）

3. 開催実績と検討テーマ

◇第1回

日時:　2020 年 6 月 17 日(木) 15:00～17:00　Zoom 会議

テーマ:参加各者、及び部会長・アドバイザーの自己紹介

近況及び問題意識の共有

以下のような関心ポイントが参加者より挙げられた。

・どのようにしてクラウドサービスを選定するのか、そのセキュリティ対策はどうなっているのか？

・リモートワークが中心の現在、セキュリティについてどう社員のレベルアップを図るのか？

どのようなセキュリティルールを備えるべきか？・またどう運営するのか？

・これまで対象とされていなかった工場系のセキュリティについて、どう進めるのか？
・これらについての世間動向であり、他社情報や有識者の意見を聞きたいとの要望有、これに応える研究会とする。

◇第2回

日時:　2021 年 7 月 29 日(木) 15:00～17:00　Zoom 会議

テーマ:「テレワークでの課題と対策」　工場、老朽機器

・これまでは「外部と遮断する」ことでセキュリティを確保すると考えていたが、工場機器もメンテナンスの為に外部ネットワーク接続が行われるように変化しており、遮断出来なくなった。
・工場設備の場合、機械設備と一体で動いており、ソフトウェア単体ではない。その為にソフトウェアの最新版へのアップデートは、単純なソフトウェアのバージョンアップではなく、そのハードであり、機械設備との関連があるので、“設備全体の更新”という内容になってしまう。だがそれは投資金額が嵩み実際的ではない。
・このような機器を扱う人達のリテラシー課題もある。これまでは遮断しており、気にしなくていいとしてきた為、教育など足りていない。
・理想的には情報系/共用系/制御系としっかり分けたいと考えるが、投資嵩む。今はDMZ(DeMilitarized Zone)レベルで分離しているのが現状である。対象設備としてのプリント機器であるので、大きなリスクはないと考えている。
・事例としても、FW や UTM を置いて制御系を分離し、スタンドアロンとして扱えるようにする事が多い。ただ最近はむしろ、セキュリティレベルが低い制御系から情報系をこのようにして守るという考え方に変わっているように感じる。中継サーバーを経由させ、通信ポイントを限定するというやり方もある。
・改めて工場のセキュリティ診断した事例では、机上点検にて情報系との接続以外に・リモートメンテナンス用の外部との接続口・他工場とのネットワーク接続・工場内他工程と接続など、“外”は必ずしも“外部”だけを意味するものではない“接続”があった。この場合、更に実システムの脆弱性チェックも行ったところ、UTM のソフトウェアバージョンが古いため、そこを攻撃される恐れがあることも判明した。
・「外部から遮断すること」は事実上出来ない状況だが、どう安全に接続するかを考えるべきだ。ただ工場設備の場合、ここから情報漏洩が起こる訳ではないので、『例えウィルス感染しようともちゃんと動けば良い』という考え方もある。
・『どこで、どのような事が起きると、どうなる』というシナリオを描くことがセキュリティ検討の始まりであり、これが重要である。例えば、中継サーバーがウィルス感染すると何が起きるのか、これを受けてどうするのか、ということである。どのくらいの頻度で、どのような接続が行われているのかという実態を踏まえて検討すべきであろう。

◇第3回

日時:　2020 年 9 月 16 日(木) 15:00～17:00　Zoom 会議

テーマ:「クラウドの活用」　クラウドのセキュリティはどうなっている？

・社内外からアクセスできるようになる点がクラウド活用の大きなメリットであるが、セキュリティ面ではオンプレと変わらないと言えよう。“お守り”とのトレードオフと言える。

・現在、クラウドサーバーを構成していくところである。広くアクセスできる点は良いが、社員情報などへのアクセスをどのようにコントロールするのかに悩んだ。結果、VPN 接続にて事務所経由で接続することとした。今のところ利用者が限られているため出来る対応方法であり、社員全員がユーザーとなると負荷対応の問題が生じる。それも含め、社内サーバーが守られているから出来る点も多く、パッチ対応やアップデートなどの手間対応についてサービス内容を精査する必要がある。

・経営陣からは、アセットを持たないという意味で活用を推進するようにと言われている。

・クラウド活用について全社システムでない内容は情報部門を経由せず、各事業部の管理で使用可能としている。故に情報部門での全体把握はできていない。あるいはクラウドの選定基準として、チェックシートを用意している例もある。
ただ開発受託をしていると、相手先企業の要請に合わせていろいろなクラウドツールを使用せざるを得ず、自社でコントロールすることは出来ない。

・例えば WS の場合、個別のサービス自体はそんなに高価ではないが、セキュリティ対策などの付加内容をまとめていくと、そんなに安価でない経験もある。
CIS(Center of Internet Security)にて利用に際してのガイドラインが公開されている。英文ではあるが興味があれば参照願いたい。

・クラウド化により資料で言われていた物理的境界はなくなる。今後、“認証”がポイントになり、更にアクセス制御・アクセスログ管理も重要となる。

◇第4回

日時:　2020 年 11 月 18 日(木) 15:00～17:00　Zoom 会議

テーマ:「個人を守る」

・自社においては各個人のソフトを管理できていない。それは客先の要請であり、各人の好きな開発環境を整えようとしているからである。管理に対する現場の反発もある。
また、個人 PC に対する制限もかけていない。そのため Slack を個人 PC に入れている例もあり、制限出来ていない。会社のネットワークに個人携帯をつなげるなども含め、BYOD をどうしたものか、悩んでいるところである。

・一方、個人用 PC や携帯は使用禁止という例もあった。それについて、ローカルにデータを落とすことの制御はしておらず、ログを取ることでそのような事実の確認をできるようにしている。また、VPN 接続においては機器認証をしているが、クラウドに対しては行っていない。

・ゼロトラストをベースにおいて、社内・社外の関係はなくなる。その実現に向けての技術論に加え、運用管理という面もあるが、そこの負担が増えることを懸念している。
例えば本人認証・デバイス認証・EDR 認証などあるが、認証が出来ないと運営に連絡が入り、な

ぜ認証できないのか調べなくてはならなくなる。その様な手段の用意が運営管理に大きな負担となるのであろう。何か仕組みに問題があるのか・単なる操作ミスなのか、分からなければならない。これまでは社内であり、ルートが絞られていたため楽だったが、これからはそうはいかない。またこれに対処することに情報部門だけでなく、ユーザー自身の力をつけることで対応ができるのではないだろうか？

・BYOD 使用を積極的に認めている会社はある。例えば、グーグルを利用しているケースなど。
本人かどうか、使用している端末は OK か、通信経路は OK かなどチェックがあるが、やはり大前提は利用者のリテラシーではないのか。リテラシーの高さが高ければ認めていいし、低くければと仕組みで縛らなくてはならない。

・日本企業は製造業を中心のチームワークであり、企業は人なりと言ってきた。ここに評価制度が入って来て歪んできたように思う。風土は変えずに仕組みだけを変えた歪みではないだろうか。一企業で一生勤め上げる時代ではなくなっており、企業もサポートできる関係になれると良い。

・会社に与える損害の規模も含めたリスクアセスが出来ていないこともポイントとなる。ISO のマネジメントレビュー最初の質問は、リスクの把握である。そしてリスクの被害金額規模と発生頻度を聞かれる。この準備を怠ってはならない。

◇第5回

日時：　2022 年 1 月 20 日(木) 15:00～17:00　Zoom 会議

テーマ:「会社を守るツールの変化」

・セキュリティについて、現場レベルではあまり考えていない。これに対して IT 部門はリスク認識し、経営に対して必要な投資を求め、啓発に努めようとしている。
中長期のロードマップをベースにゼロ・トラストや ISMS27002 も考慮しながら、端末制御と ID 管理としての統合認証基盤を構築するよう取り組んでいる。

・働き方が変化しており、クラウド活用によるメリットを事業部などは享受している。しかしクラウド活用に伴い、新たなセキュリティが必要となり、IT 部門の費用追加のみで判断されるべきではない。事業部などが得ているメリットとのプラス/マイナスの中で議論すべきと考えられるが、実際はそのように議論出来ていない。セキュリティはコストを上げると経営陣には認識されている。

・やはり企業では Windows がベースにあるので、Office365を活かしながら構築を考えることが多いようである。

・またログ管理について“サシー SASE”の導入などもあろう。ネットワークでは SWT・エンドポイントについては SIEM や SOAR などもある。ただ全部を網羅できるものはなく、選定には時間がかかる。プロセスマイニングの流れの中に PC ログの活用アイデアがあるが、各人の PC ログを取得できるのであれば、各クラウドのログを取るよりも簡単である。実際、米国では社用 PC にログソフトがセットされるのは当たり前のようだ。

◇第6回

日時:　2021年 3 月 17 日(木)　15:00～17:00　Zoom 会議

テーマ:「人材育成」

・新入社員向けに定型内容＋αで準備している。内容としては、社会人としての自覚(他人事でないという意識の持ち方)・やってはいけない事について若干脅迫(例えば不審メールを開いてしまうとどうなるかなど) も含めている。

・セキュリティの人的側面について、ルール作りを進めてきた。その内容を国内から海外へと展開させている。やはり海外には IT 人材がいないところもあり、単純には展開できない。社員へは階層別に教育しており、教育内容については LMS を導入している。
また、やはり専任者が必要と考え任命している。

・ISMS・プライバシーマークを持っているが、やはり当初は取得することが目的だった。効果を発揮できるよう活用していく必要がある。

・後継者については、一度怖い目にあうのが良いのではと思う。知識ではなく、感覚的な理解が重要ではないだろうか。専門家が情報収集しても読まれない。また、常に意識し続けることは専任者でも大変である。

・クラウドや DX と IT の領域が拡大する一方、社内人材は不足しており、今後の定年者の発生やローテーションも難しいことから、ユーザーとシステムの間に立つキーマンを育成しようと考えている。そのキーマンについて、ユーザースキル標準をベースにスキル定義し、目標設定し、e-ラーニングやベンダとの協働のカリキュラムに取り組んでもらっている。いろいろな取り組みからスタートし、ノウハウを修得することで、人材の数を増やし、DX 対応に繋げていきたい。

・マネジメントの理解は必要不可欠だが、危機感をどう伝えるかがポイントとなる。セキュリティの重要性を実態に合わせて説明しなくてはならない上に、リスクの認識もしてもらわなくてはならない。その為には同業他社との比較や、投資・人員のかけ方などを示すことが効果がある。

・IT・セキュリティはもはや特殊な内容ではなく、社会人として必須内容となっている。社員全員が身に付けなくてはならないスキルである。

◇その他

テーマの検討だけでなく、その時の話題となった以下のような内容について議論している。

・2021年1月の情報漏えい事件・事故

・経産省サイバーセキュリティ経営ガイドライン Ver2.0

・サイバー攻撃／ランサムウェア攻撃の近況　カセヤへの攻撃/ランサムウェア(身代金)近況

・米国　セキュリティ対策/ビジネスメール詐欺/多重要素認証

・改正個人情報保護法　2022 年 4 月 1 日に全面施行

・トヨタ、サイバー攻撃

◇参加者の方からは、以下のような感想を頂きました。

・＜平均評価点　1～5で評価＞　4．4

コメントご紹介

・他社のセキュリティに対する考え方や取り組みが知れたことがよかったと思います。

・実際の現場での困りごとや解決の方法を聞けた。

・まとめた資料をご提供頂ける。

・雰囲気よく話ができた。

・Web での集まりのみとなり、コミュニケーションを深めることが出来なかった。

・例えば、感染した後の対応などもご紹介できると良いのではと思います。

ご意見を踏まえ、最新状況を踏まえながら、対応方法であり、事故フォローであり、活発に議論を進めていきたく考えております。

以上