4.5　セキュリティ対策研究会

「セキュリティ対策研究会」2020 年度活動報告

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、働き方改革の取り組みが進み、政府のテレワーク推進で企業規模にかかわらず在宅勤務やサテライトオフィスの活用など私たちのワークスタイルもどんどん変わってきている。この様な環境変化を踏まえると、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、『守る』だけでなく、変化を『支える』取り組みも必要になるのではないか？と考えられる。

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ゆく。そこにおいてはこれまでの様に「囲って守る」という考え方では無い取り組み方が求められる。今の変革の流れから取り残されてしまわないよう、そして情報資産を保全してゆけるよう、セキュリティ関係のアドバイザーにも入っていただき、どう自社の変革を進めてゆくのか、それを踏まえてどういう対策を進めてゆけば良いのか、を参加の皆さんと考えることが出来た。この内容を自社での対応にて中心に成って取り組んで頂きたいと願っている。

ここで確認されたことは、急激なリモートワークへの切り替えが進んだ結果、通常業務は遂行出来ているもののそこには大きなセキュリティ上の弱点が生じてしまっており、実際この１年の間にセキュリティ関連の大きな事故も発生している、という点であった。

この現在進行形の内容に対し、”ゼロトラスト“という大きな方向性はあるものの、直ぐに移行できる内容では無く、５年単位の時間を要するものと考える。勿論、そこに向けて変革していかなくてはならないもののそれが出来上がるまで何もしなくて居ても良いのかと言えばそれは違う。これに応える内容は、リモート作業者一人ひとりへの意識付けと事故対応体制の確認、というのが今回の結論である。

つまり、職場にいて何かあれば直ぐに周りに相談できた環境には無いのであり、リモートワーク者自身が「管理責任者である」という責任をもって業務遂行していく必要がある、ということである。そしてもし、何らかの異常が発生した場合、これまでの様に上司に報告して、という流れではなく、直ちにセキュリティ責任者へ報告し指示を仰がなくてはならない、という事である。リモート環境は社内の様に安全確保された環境には無いので、作業者は万全の注意を払わなくてはならず、異常を感じたら対応スピードが被害最小化のポイントであることを踏まえ、責任者と直接コンタクトして対処してゆくことが重要であることから、直ぐ行うべきセキュリティ対処としてこの点を挙げたものである。

今後、“ゼロトラスト”の実現に向けどう行動していくのか？を議論してゆきたいと考えている。更に、工場系のセキュリティ課題についても、一歩踏み込んだ議論に進めてゆければと考えている。

2. 参加企業名　　ご参加者　7名

味の素株式会社
味の素食品株式会社
サトーホールディングス株式会社
システムズ・デザイン株式会社
トライビュー・イノベーション株式会社
日本デェイブレイク株式会社
株式会社フロンテス

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 7 月 16 日(木) 15:00～17:30　Zoom 会議

概要:①参加各者、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出された。
・ISMS 取得取り組みの中、規定などのカタチの面について関心がある。
・リモートワークが中心と成る中におけるセキュリティについて、VPN の割り当て問題、Zero トラスト、エンドの保護、といった点に関心がある。
・ISMS 遵守の中、クラウド利用の是非、テレワークにおけるエンドポイントのセキュリティ(個人ネットワークの利用や Wi-Fi ルータの使用)の考え方について関心がある。
・社内 Proj 業務を遂行する中、いろいろなクラウドのツール（メール、チャット、タスクスケジュールなど）を活用しているが、果たしてこれで良いのだろうか?という疑問も感じる。テレワークとの兼ね合いであり、個人の意識の持ち方に関心がある。
・テレワークに関する内容について関心がある。

◇第2回

日時:　2020 年 9 月 17 日(木) 15:00～17:30　Zoom 会議

概要:①ISMS の意義
ISMS を運用していくメリットとして、保持している情報資産に対する脅威と脆弱性を発見し、適切なリスク対策を検討できる機会を得ることができる、という点にある。
ISMS では手順を定めることが先ず求められている。そこでそれが社内ルールとして定められているのであれば、そのやり方が良い悪いという話ではなく、「ルールに基づいている」ので OK で

良い筈である(審査員への反論の仕方に気を付ける必要はあろう)。 その後のインシデントの発生などを踏まえ、より良くしていく取り組みは求められる。

横浜市のハードディスクの問題においても、ISMS での要求対応はできている。しかしそれが事故の起きないことを保証するものではない。

しかし逆から見ると、企業の担当者のレベルで組織のレベルが決まる、ということにもつながる。

②『ホンダにおけるサイバー攻撃』 報道を踏まえての議論

起因としては、未だ推定の範囲であるが、持ち出した PC が起点になり、事前にサーバーにランサムウェアをばらまくソフトがセットされてしまっていたようである。この影響により、国内4工場、海外9工場が生産停止に追い込まれた。

緊急対応として全社員のPCを使用禁止にしたので、再開までの間は携帯で出来る程度の仕事しか出来なくなった。

どうしてこのように広がったのかを考えてみると、WAN のコントロールは拠点毎に任されており、そこでは入って来る内容に対しては厳しいものの、出てゆく内容についてはほとんど管理していなかったのではないか？また、生産系も情報系にはつながっていない、とされていたが、実はつながっていた(現場任せになっていてこれが分かっていなかった)。これらが相まって工場にまで影響が及んでしまったと思われる。

つまり、本部から指示は出していたが、実態が分かっていなかった、と言えよう。何故かは分からないが、明らかに狙われた攻撃でもあった。

この例から学ぶとすると、コロナ対応でテレワークせざるを得なくなり、PC を持ち出して使っている現況において、セキュリティ確保の為には通信経路の制御が必要なのだが、そこまで手が回っておらず、後追いになっているのではないか？一方、攻撃者は弱いところを狙ってくる。生産系への影響を防止する為には論理的にネットワークを分離する、限定した通信のみに制限する、という対応を取らなくてはならない。

③新状況への対応の仕方

総務省から「テレワークセキュリティガイドライン」が出ているが、会社でのルールが先ず出来ているという前提に立っての内容である。コロナ対応でテレワークを認めざるを得ない状況にあるのであり、ルールが追いついていないのが現況であろう。

これまでのアプローチは、規定・ルール⇒体制⇒教育・ブラシュアップ、という流れであったが、現況を踏まえて、現状の棚卸し⇒規定化⇒ポリシー整備、という進め方が良いのではないかと考えている。

ネットワーク的に現況を見てみると、これまでは総て社内から外部のクラウドへと繋がっていた。しかし今、リモートワークに成ると外部から社内に入り、社内を経由してクラウドに繋がなくてはならなくなる。しかしそうするとネットワークのキャパオーバーが起きたり、ライセンス数を越えたりといった問題が発生し、緊急対応として社内ネットワークを経由せずに直にクラウドに接続することを認めざるを得なくなっている例がある。しかしこの時、認証が大丈夫か?という疑問が残る。セキュリティ観点からは、この各端末を守る、という取り組み方に変わる必要があるのであり、デバイス認証、本人認証、データアクセス管理などで正しく使われていることを

担保することが急がれるのではないだろうか？
そしてこれは、社内だけではなく、提携パートナーとの間でのデータ共有においても同様であろう。

④dペイ問題 （野口）
会社の施策がセキュリティに優先してしまったことにより、結果、トラブルが起きてしまったと言えよう。セキュリティ担当がしっかりこの様な流れを止めなくてはならない。

◇第3回
日時： 2020 年 10 月 22 日(木) 15:00～17:30 Zoom 会議
概要：①【JNSA 緊急事態宣言解除後のセキュリティ・チェックリスト】を行ってみたことを踏まえての議論
・コミュニケーションツールの有効性がこの間に確認されてきた。
例えば Teams でプロジェクトを作れば、ご送信に心配は無く、チャットも出来、ファイルサーバー共有も出来るなど使い勝手が良い。
・コロナ対応が長く成り、会社に行かなくても仕事は出来る事に皆気がついた。
・リモート中心の働き方として、例えば、朝・13 時・16 時に毎日ミーティングを持ち、その日に「何をやるか」「どれくらいの時間をかけるか」「助けることがあるか」を話し、デイリーレポートも作成している。すべての情報をお互いに確認できるので、言ってることとやっている事の違いがあればすぐに分ってしまう。この様にしてリモートで皆働いているが、全く問題無く業務対応してきている。
・常駐先でのルールにも従う、という環境では、“ルール”も複雑になる。

②テレワーク環境とセキュリティ
・コロナ対応として、外部から社内ネットワークに入り、そこから外部など含めて処理する、というやり方を取ったが、直ぐにネットワークのキャパシティ問題が発生し、直接接続を認める、個人デバイスの使用を認める、こととなった。総て性善説に基づいた運用になっている。そこで今一度、何が OK で何が NG なのか、ポリシーに立ち返ってハッキリさせていく必要が生じている。
・そこで、ポリシーの確立⇒星取表（OK/NG の明確化、重要情報の明確化、など）⇒具体的なサービス設計、と進める取り組みに各社取り掛かりつつある。
・この様な状況を踏まえると、昨年まで検討していた“階層俯瞰図”にてグレーにした階層は、現状では意味が無くなっている。そして改めて重要なのは、デバイス・本人認証・アクセス通信経路であり、インシデントレスポンスの考え方・行い方の見直しであり、6つの方針を決めなくてはならない。
・ゼロトラストは、理想として目指すべき方向ではあるが、実際は、その途中段階にて実行されていくこととなるであろう。その実際レベルを見定める意味でも、ここまで述べたような取り組みを進める必要があろう。

③トピックス デジタル庁について （野口）
・これ以外にも東証のシステムダウン問題などの問題が発生している。原因から学び事前の対応を取っていくことが重要である。

◇第4回

日時:　2020 年 11 月 19 日(木) 15:00～17:30　Zoom 会議

概要:①「クラウドの活用状況、シャドーIT」の調査を行ってみた上での懸念点

・以前はコミュニケーションツールというとメールしか無かったと思うが、今はこれがどう変わってきているのか？

	メール	Box など	チャット	
社内	4	2	2	
社外	5	2	1	(複数回答あり)

例えばストーンビートセキュリティ社では、漏洩を防ぐためにメールで機密情報を流すことはしない。添付文書を暗号化しても同じ様にメールでパスワードを流していたのではセキュリティ確保には成らない。守るべきは対象となるのは“情報”であり、新しいツールを活用していくのが良いと考える。

・調査にあたって直接尋ねたりされたようだが、情報を収集するツール(例えば、CASB、SkySee など)があるので、これを活用するのも監視という面では有効であると考える。特に CASB では、使用するサービスをブロックして使えないようにする事も出来る。各人が引き出したデータを何処に格納したのかといった行き先が懸念されるのであり、夜間に大量のデータを引き出しているなどの行動は疑わしい行動として検知が重要である。

②クラウドサービスの利用に際して

・クラウドサービスの利用にあたっては、ポリシーを定めるておく必要がある。これはクラウド利用におけるセキュリティ脅威の2点目にある様な「ルール未整備」に対処していく為のサービスである。盲点になる内容として、個人のスマホのデータは、所有者の同意が無いと中味を確認したり消去したりできない、という点である。クラウド利用のポイントとなる可用性・機密性・完全性を踏まえながら、利便性と安全性とを確保していかねばならず、ポリシーを定めるのは中々大変な内容と成る。

③トピックス 「カプコン」

・大きな影響の出た内容であるが、まだその原因は分かっていない。ただやはり“プロの集団”に狙われるとソフトを生業にしている会社であっても事故が起こるという事でもあろう。原因が共有化されると、大きな学びがあると思われる。先にクラウドサービスの利用ポリシー策定の紹介があったが、この様なルールがある事も必要である。

◇第5回「何にどう取り組んで行く事で、自社のセキュリティ対策を充実させて行くのか？」

日時:　2020 年 12 月 17日(木) 15:00～17:30　Zoom 会議

概要:　①IPA 情報 (内田)

2020年度の10大脅威が公表された。

＜情報セキュリティ 10 大脅威 2020「個人」および「組織」向けの脅威の順位＞

「個人」向け脅威 順位	順位	「組織」向け脅威
スマホ決済の不正利用	1	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2	内部不正による情報漏えい
クレジットカード情報の不正利用	3	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	4	サプライチェーンの弱点を悪用した攻撃
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	5	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6	予期せぬ IT 基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい
インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9	IoT 機器の不正利用
インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止

・標的型攻撃、ビジネスメール詐欺、ランサムウェア被害、など新聞報道されている内容が上位に上がっている。2位には内部不正が上がっている点も見逃せない内容である。

②アフターコロナの新状況を踏まえ、セキュリティポリシーなどの見直し必要点はあるか？テレワーク規定はあるか？新たに導入したツールは？を調べてみた結果を踏まえた議論

・アフターコロナの環境を受け、各社テレワーク規定の充実が図られている。しかしその内容を見てみると、人事勤務規程を補足する様な内容と成っていてセキュリティについてちゃんと見直し出来ていないケースが多々見られる。テレワークでのセキュリティ確保についてちゃんと見直し、ルールを決め、それを守っていくよう進めて頂きたい。

・コミュニケーションツールも TV・Web 会議に切り替わり、まだ社内限定が多いかも知れないが、チャット利用も増えてきている状況にある。

・個人認証／アクセス経路／端末管理がセキュリティ確保上重要となる点、以前、説明したとおりだが、それらの具体的ツールとして、特に Okta や Zscaler が良く検討されている様である。

・テレワーク規定に関連して、議論にあった様に作業環境やデバイスについて規定していくことが大切である。ただ、その規定を作るのに手間をかけてしまっては時間の使い方として勿体ない。例えば、「やってはいけないことリスト」を作って、これを皆に周知するだけでも早期に効果が期待できる。

一つ重要な事は、インシデント発生時の連絡先をしっかり周知しておくことであり、それは上司では無い。インシデントを集中管理している部署・人でなくてはならない。その後、上司に連絡する、という具合にすべきである。

もう一点、「責任者は自分自身」という点がある。テレワークで働く人は、この様な意識

を持って取り組んでもらうことが重要だと考える。
何れにしても、「利用者が適切に判断できないことはやらせない」という点が重要である。

③トピックス「アフターコロナのセキュリティ対策」
本来守るべきものは何か？を明確化し、それに対するアクセス制御を行いしっかり守ると共に、一元化・標準化したプロセスでインシデント管理を行っていくことがアスターコロナの状況におけるセキュリティ管理として重要となる。

◇第6回
日時：　2021年1月28日(木)　15:00～17:30　Zoom 会議
概要：
【上位者、或いは経営陣に対して、この IT 活用の変化した新状況において何を行うべきか、セキュリティ対応提言をまとめる】
① 何が新状況において変化したのか？それはれまでのセキュリティ対策では何が(どこが)足りないか、どんな影響があるのか？
② これに対応する為に、セキュリティ対策として新たにどの様な観点の手を打たなくてはならないと考えるか？(概念レベルの内容をまとめる)
③ そうした中、ご自分はどういう優先順位で何を行う必要があると考えるか？
という点について、参加者各位の考えを述べ合い、議論を行った。
主な内容は以下の通り。
① 境界防御から端末・個人・クラウド毎の認証への移行を進める。
宅内の通信環境が十分に整っていない人をどの様に支援するか。
クラウド利用に際して利用部門は自らの責任においてセキュリティを確保する必要がある。
工場の制御系ネット―ワーク(インフラ)に対しても、リモートでの監視・操作したいニーズが高まっている。
②従業員・役員の、一層の IT リテラシー向上
インシデント管理や対応強化、根本原因の究明
エンドポイントでのセキュリティ対策、端末・個人・クラウド毎の認証への移行
工場とクラウドがつながるのを前提にルールや設計を組みなおす。
③ 組織的対策として規定類、手順等の整備、CSIRT、SOC の検討、リモートワークのポリシー・マニュアルの作成
従来の e－ラニングに加えて、標的型攻撃に対する訓練内容を改訂する。
自社およびグループ各社でどの様なインシデントが起きているのか、グローバルに把握する体制を構築する。
コミュニケーションツールの利用を運用で厳格化する。
“乗っ取り”などが起きた時、復旧出来るようにしておく。
工場のセキュリティ責任者・担当者の選任(人員の確保)

◇参加者の方からは、以下のような感想を頂いた。

・現場の立場に立っているので、会社全体の観点から見てみたいという期待を持って参加した。忙しいと中々課題をまとめられなかった点もあったが、情報を得ることが出来た。

・階層防衛図など勉強になった。誰も正解が分からない中、一歩一歩進んできたと思うし、自分なりに考えることが出来たと感じる。急激な変化の中、もっと学びたいと思う。

・“事故”が起きてからでは遅いのに、まだ起きていないので重視されていない。米国では社長がクビに成る事もあるという話もあったが、事例を使ってアピールしていきたい。

・振り返ると自分自身のレベルが低かったが、セキュリティの考え方、ゼロトラストなど多くを学び、高まったと感じると共に、セキュリティについて考えるきっかけを得られたと感じる。

・セキュリティの新担当となったタイミングであったので、研究会内容を活かすことが出来た。これまでの研究会の内容は、社内の活動に活かされてきていると思っている。

以上