# 「セキュリティ対策研究会」2019 年度活動報告

「セキュリティ対策研究会」2019 年度活動報告サマリー

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、巧妙になってきています。どうしてもこれを防ぐことに目は行ってしまいますが、実はセキュリティインシデント発生後の対応体制を準備しておくことの方が、外部者からみると重要な内容です。

そこで本研究会では、企業において情報セキュリティ対策をどう進めてゆけばよいのか、CSIRT に学びながら最低限の対応体制の準備について全 6 回の研究会にて検討してきました。

本研究会におきましては、セキュリティ関係のアドバイザーにも入っていただき、どう自社の弱点を見つけてゆくのか、それを踏まえてどう対策を進めてゆけば良いのか、各社の実情も鑑みながら専門家の意見も踏まえ、皆で意見交換しながら検討し、そしてセキュリティ対応の主担当者に育って頂くことを目指しました。

具体的には、各研究会で扱ったテーマや得られた知識を基に「どう TOP にセキュリティ対策推進について意見具申するのか？」というテーマで各人の意見を出しながら、それが上位者に訴える意見に成っているだろうか？周りの人に理解してもらえる内容に成っているだろうか？本当に安全を守っていけるだろうか？といった検討を行ってきました。

この様な研究会を通し、どう訴えかけるかというポイントの理解であり、IT 利用において全員が安全な行動を取っていく為の訓練の大切さについて理解を深めて頂くことができたと思っております。

2. ご参加者　7名

◇アドバイザー、部会長

・部会長　内田昌宏 （LAC）

・アドバイザー　野口　勝 （株イフェクト）

大島　耕二 （ストーンビートセキュリティ㈱）

3. 各研究会でのテーマ

◇第1回 ①研究会の狙い ②参加各者、及び部会長・アドバイザーの自己紹介 ③階層防御俯瞰図の説明 ④最近のトピックス

◇第2回 ①階層防御俯瞰図を使った各社の現状と世間水準レベルとの比較発表 ②講師陣からのアドバイス ③最近のトピックス

◇第3回 ①経営への提言 ②最近のトピックス

◇第4回 ①「PC 乗っ取り」の実演と解説 ②DSS（Data Security Standard）アセスメント・シート説明

◇第5回 ①事故対応シミュレーション

◇第6回 ①会社への提言 ②講師からのアドバイス ③最近のトピックス

以上

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、巧妙になってきています。どうしてもこれを防ぐことに目が行ってしまいますが、実はセキュリティインシデント発生後の対応体制を準備しておくことの方が、外部者からみると重要な内容です。

そこで本研究会では、企業において情報セキュリティ対策をどう進めてゆけばよいのか、CSIRT に学びながら最低限の対応体制の準備について全 6 回の研究会にて検討してきました。

本研究会におきましては、セキュリティ関係のアドバイザーにも入っていただき、どう自社の弱点を見つけてゆくのか、それを踏まえてどう対策を進めてゆけば良いのか、各社の実情も鑑みながら専門家の意見も踏まえ、皆で意見交換しながら検討し、そしてセキュリティ対応の主担当者に育って頂くことを目指しました。

具体的には、各研究会で扱ったテーマや得られた知識を基に「どう TOP にセキュリティ対策推進について意見具申するのか？」というテーマで各人の意見を出しながら、それが上位者に訴える意見に成っているだろうか？周りの人に理解してもらえる内容に成っているだろうか？本当に安全を守っていけるだろうか？といった検討を行ってきました。

この様な研究会を通し、どう訴えかけるかというポイントの理解であり、IT 利用において全員が安全な行動を取っていく為の訓練の大切さについて理解を深めて頂くことができたと思っております。

2. 参加企業名　　ご参加者　7名

アイエックス・ナレッジ株式会社
株式会社　オカムラ
サトーホールディングス株式会社
株式会社　ソフトロード
トライビュー・イノベーション株式会社
日鉄日立システムエンジニアリング株式会社
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 （株イフェクト）
大島　耕二（ストーンビートセキュリティ㈱）

各研究会でのテーマ

◇第1回 ①研究会の狙い ②参加各者、及び部会長・アドバイザーの自己紹介 ③階層防御俯瞰図の説明 ④最近のトピックス

◇第2回 ①階層防御俯瞰図を使った各社の現状と世間水準レベルとの比較発表 ②講師陣からのアドバイス ③最近のトピックス

◇第3回　①経営への提言　　②最近のトピックス
◇第4回　①「PC 乗っ取り」の実演と解説　②DSS(Data Security Standard)アセスメント・シート説明
◇第5回　①事故対応シミュレーション
◇第6回　①会社への提言　②講師からのアドバイス　③最近のトピックス

3. 開催実績と検討テーマ

◇第1回

日時:　2019 年　7 月 18 日(木)　15:00～18:00
場所:　アイオス五反田(本館)2 階会議室にて
概要:①研究会の狙い

セキュリティの状況説明の為にまとめる資料は余り変わりません。
本研究会でこれについての知識を深めると共に、その様なまとめツールを使って『どう経営陣に説明するか？』を検討し、各社の目指す姿に近づいてゆくための一助となる事を目指します。

②参加各者、及び部会長・アドバイザーの自己紹介
③階層防御俯瞰図の説明
第 2 回に向けての資料のまとめかたの説明。
④最近のトピックス
セブンペイ　不正アクセス事件

◇第2回

日時:　2019 年　9 月 19 日(木)　15:00～18:00
場所:　アイオス五反田(本館)2 階会議室にて
概要:①階層防御俯瞰図を使った各社の現状と世間水準レベルとの比較発表

階層防御俯瞰図に従い、自社のセキュリティレベルを出来ていない／一部出来ている／出来ているの三段階にて評価し、その内容を世間一般レベルと比較することで自社のセキュリティレベルが一般的水準は満足しているかどうかを比較し、今後どの様な対策を打つ必要があると考えられるかを検討した。

②講師陣からのアドバイス
経営陣は、
・(結局のところ)当社は大丈夫なのか？
・他社と比べてどうか？
・これまでの投資は有効だったのか？
・(そのうえで)当社の弱いところはどこか？
・必要な対策は？　なぜその対策(方法)なのか？
・必要な金額は？　なぜその金額なのか？
という点を確認したいと思っているので、これに答えてゆくべく
1)当社におけるセキュリティ脅威は〇〇であり…

アセスメント結果を視覚的に
当社で発生した事故の実際（事象と件数）も
2)その脅威を放置すると…
セキュリティ脅威が当社事業に与えるインパクトは
組織としての責任、経営としての責任追及も
3)だからリスクを低減させる対策が必要で…
対策優先順位の判断材料
高リスク／投資対効果／他社比較
4)そのために必要な金額は…
当社のビジネス規模、これまでの投資額を参考に
という順にて説明を試めすのが良い、とのまとめを行った。
③最近のトピックス
セブンペイ　不正アクセス事件　　直近の報道を踏まえて

◇第3回「企業の抱える情報資産とは何か？　情報システムと情報資産との関係」
日時：　2019 年 10 月 17 日（木）　15：00～18：00
場所：　アイオス五反田（本館）2 階会議室にて
概要：①経営への提言
経済産業省発行の『サイバーセキュリティ経営ガイドライン』にある「サイバーセキュリティ経営チェックシート」に経営者目線で答え、その解答結果を基に自社におけるセキュリティ対策提言をまとめ、その内容を参加者で比較検討した。
②最近のトピックス
南アフリカ　ヨハネスブルグ市がハッキングされ、身代金を要求されたという事例も発生しており、この様な攻撃が大規模に起きていることを共有化した。

◇第4回
日時：　2019 年11月20日（木）　15：00～18：00
場所：　アイオス五反田（本館）2 階会議室にて
概要：①「PC 乗っ取り」の実演と解説
実演にて、如何に PC が乗っ取られるかを紹介し、解説をおこなった。
攻撃に使われるツールは、脆弱性テスト用に公開されているツールを使用して簡単に実施できてしまう実態を見て、驚かされる内容であった。
そしてこの防止には、一般に推奨されている様に確実に PC にて利用しているツールの最新版へのアップデートを行っておくことであり、緊急用に備えられていて使っていない PC などが盲点になり、攻撃を受けるセキュリティーホールと成りがちである点など実際的な解説がされた。
②会社全体としてのセキュリティ対応状況をリスクベースでまとめてゆける DSS（Data Security Standard）アセスメント・シートを説明し、内容を理解して貰う為に数項目を取り上げて、実際に

記入してもらい、使い方を学んでもらった。

③質疑応答、ディスカッション

④フリートーク

情報漏洩リスクに関する損保会社の講演内容の紹介、その様なリスクに対しての保険の掛け金に関する情報が話題と成った。

◇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1月16日（木）　15:00～18:00

場所：　アイオス五反田（本館）2 階会議室にて

概要：①事故対応シミュレーション

あるセキュリティ事故発生の想定の下、参加者を事故対応側とインシデント発生指示サイドとに分けて、事故対応を行ってゆくシミュレーションを実施した。

頭では理解している内容も、単なる技術的側面だけではない、例えばマスコミ対応や状況公表の行い方など、分担して対応を進めようとするとどう進めたら良いのか、混乱する場面もあり、そういう意味で参加者へは大変意義深い内容となった。

改めてセキュリティ対応は広い範囲で対処してゆく必要がある内容であり、CSIRT のように全社的な組織を準備しておかなくてはならないという実感を得ることができた。

◇第6回

日時：　2020 年2月20日（木）　15:00～18:00

場所：　アイオス五反田（本館）2 階会議室にて

概要：①会社への提言

第5回でおこなった事故対応のシミュレーションを振り返り、この仮想の会社においてはこれからどのような取り組みを行うべきか、自分がこの仮想会社の”情報担当責任者“であると仮定して提言をまとめ、各人に発表頂いた。

第3回でも提言まとめを行っているが、その内容に比べ広い視野からの提言内容となっていた。

②講師からのアドバイス

以下のような観点から提言を考えると良い、というアドバイスが行われた。

システム重要度基準例；　基準の持ち方の参考として説明

CSIRT構築事例　；　各社がどれくらいの陣容で構築しているかの参考情報

事故対応フロー例　；　事故対応の事前準備の例

クライシスコミュニケーション　；　どう外部とコミュニケートすると良いか、の参考資料として。

広報では分かっているであろうが、ポジションペーパーの準備が必要であり、「べからず集」など参考にして頂きたい。

③最近のトピックス

経営層の IT 部門に対する評価において、リード役という評価をしているのは 10%程度しかない。どうやってこの評価を高めてゆくかが大切な取り組みポイントであり、「経理目標、事業目標に直結する施策を達成」に貢献できていることを数字も使って見せていかなくてはならない。

④今回の研究会では議論できなかったが、今度取り上げて欲しいテーマ

参加者の方々より以下の様な希望を頂いた。

・AI 時代のセキュリティはどうあるべきか？

・セキュリティツールの詳細研究

・セキュリティ担当者のモチベーションアップ策

・セキュリティレベルと人材レベルの因果関係、意識改革（マネジメント側、ユーザ側）

・人をどう動かす、人の意識を変えるには

・エンドユーザへの浸透と協力をどのように得ればよいか、セキュリティをどのように自分事にするか

以上