第１１７回 維持管理研究会 議事録

１．開催日時 ： ２０２１年 ４月 15 日（木）１６：００～１７：４０

２．場　　所 ： Zoom リモート開催

３．出席者（敬称略） １９名＋10 名＝29 名

小田、相原、石綿、井上、大島、葛西、木村、久保、澤田、清水、守護、菅谷、高野、高橋、橋川
柳本、柳谷、山下、中谷（記）
（ゲスト参加）地域勉強会：奥野、神田、西川、近藤、武田
IT タスクフォース他：細坪、堀、松尾、上倉、中村

４．研究テーマ

今回は、最近のテレワーク増加等の影響もあり、昨年度から多くのサイバー攻撃が発生しており、多数の企業が被害を被っており、経営や事業継続にとって大きなインパクトを与えていると想定されております。
そこで、サイバーセキュリティ専門家に講義を依頼し、最近のセキュリティインシデントとセキュリティ対策の現状について講義して頂きました。

（講師） 株式会社ラック サイバーセキュリティ統括部
サイバー救急センター 竹内正典 氏
（議題） 昨今のセキュリティインシデントと おすすめするセキュリティ対策

リモート開催にも関わらず、多くのメンバーが参加され多方面からの多くの質問もあり、サイバーセキュリティ攻撃に対する疑問もかなり解消されたのではないかと推察しております。
また、参加メンバーも様々な立場の方がおり、ＩＴにかなり詳しい専門家の方から全く分からない方まで千差万別であり、講演者も苦労されたのではと思っておりますが、大変盛況な研究会となりました。
なお参加者には、ＡＰＴチェックリストを配布していますので、組織のセキュリティレベルを評価し、ＩＴ安全度を確認して、ＢＣ能力の向上を図って下さい。
これを機会に今回の講義内容を多くの方に広めて安全性向上に努めて下さい。

＜次回開催予定＞
2021 年 5月２０日（木）１６：００～１８：００
Zoom によるリモートで実施

以上

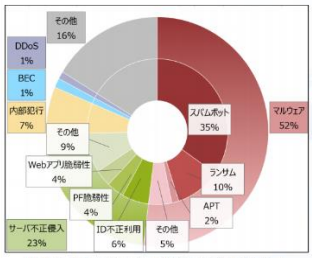
＜講義資料　抜粋＞

昨今のセキュリティインシデントと おすすめするセキュリティ対策

2021年4月15日

株式会社ラック
サイバー救急センター
竹内 正典

2020年の出動傾向



- マルウェア関連の相談が50%強
- 3割強がEmotet関連
  （左図のスパムボットのほぼ全てがEmotet）
- サーバ不正侵入、内部犯行、BEC等も件数としては例年よりも増加

「サイバー救急センターレポート 第10号（2020年出動傾向）」

10

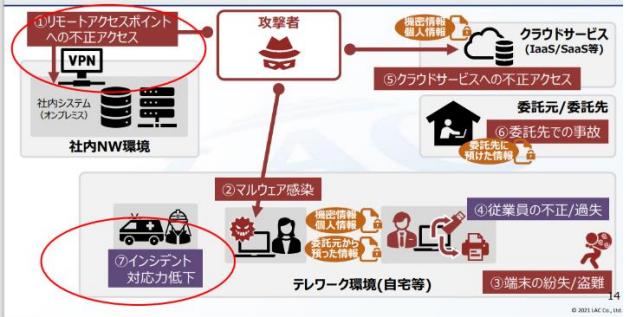
情報セキュリティ10大脅威2021

順位	内容	昨年順位
1	ランサムウェアによる被害	5
2	標的型攻撃による機密情報の窃取	1
3	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
4	サプライチェーンの弱点を悪用した攻撃	4
5	ビジネスメール詐欺による金銭被害	3
6	内部不正による情報漏えい	2
7	予期せぬIT基盤の障害に伴う業務停止	6
8	インターネット上のサービスへの不正ログイン	16
9	不注意による情報漏えい等の被害	7
10	脆弱性対策情報の公開に伴う悪用増加	14

IPA 情報セキュリティ10大脅威 2021

13

テレワークに伴うリスク発生ポイント



14

おすすめする3つの事

- リスクアセスメントの実施
- システム（セキュリティ）構成管理状況の確認
- CSIRTの確認

27

リスクアセスメントの実施

テレワークの導入・利用範囲拡大に伴ってリスクは確実に増加

テレワークを止める・抑制する方向に向かうのは間違い
テレワークは逃げられない課題

現時点で目に見えているリスクが必ずしも組織にとって優先度の高いリスクとは限らない
場当たり的な対策をするのではなく、リスクを可視化することが大切

28

テレワーク環境セキュリティ対策簡易チェック

総務省の『テレワークに関するガイドライン』と、ラック独自のセキュリティ基準を基に、ラックのセキュリティ専門家が作成した設問に答えていくだけで、自社のテレワーク環境セキュリティ対策の現状と改善点の把握、対処方法などをレポート

【テレワーク環境セキュリティ対策簡易チェック】https://www.lac.co.jp/telework/security_check.html

CSIRTの確認（インシデントレスポンスのポイント）

準備	• 「APTチェックリスト」を用いたチェック • インターネット全遮断の可否、URLホワイトリストの事前準備 • セキュリティログの収集
検知・分析	• EDR（Endpoint Detection and Response）の導入 ✓ ただし攻撃全てを検知できるわけではない
封じ込め・根絶	• 封じ込めも重要だが、根絶はもっと重要（119リピーターは意外と多い）
復旧	• 完全なクリーン状態に戻すのは難しい可能性が多いため（特にAPTの場合）継続監視を行いながら徐々に復旧させる • 喉元すぎてここが軽視されがち⇒再発のケースも少なくない

33