寄稿記事

〈コロナ禍での CSIRT 活動〉リモート時代のセキュリティ活動

I. リモート環境でのセキュリティ活動

阿部恭一（あべ　きょういち）
ANA システムズ株式会社　品質・セキュリティ管理部

1. ブレークスルーをもたらした 2020 年

2020 年，新型ウィルスの全国的かつ急速な蔓延を防ぐために緊急事態宣言が発出され，企業においてもリモートワークが推奨された．

これまでも働き方改革などにより，社会全体として緩やかにリモートワークに移行しつつあったが，これを機会に半ば強制的に働き方が変わることになった．

昨今，サイバー空間を利用した犯罪が激増し，セキュリティ活動の重要性がさらに増す中，今回の緊急事態宣言により，CSIRT（Computer Security Incident Response Team）の活動舞台も実環境からリモート環境に移行した．この流れは緊急事態宣言が解除されたあとも後戻りするとは考えにくく，新しい，リモート時代の働き方として定着していくと思われる．

本連載ではこれから 4 回にわたってリモート時代のセキュリティ活動について何が変わったのか，どのような点に注意しなければならないのかをセキュリティ活動の変化，事故時の対応，情報共有，経営面という切り口で解説していきたい．

今回はまず，CSIRT で行うセキュリティ活動の内容とそれがリモート環境でどのように変化したのかを述べることとする．

2. リモート環境で影響を受けるセキュリティ活動

セキュリティの活動は大きく平常時の活動と事故時（以下インシデント対応時）の活動に分けられる．平常時はセキュリティ観測装置から発出される警告の分析や他組織などからの情報共有により，利用している機器類の不具合などに対する手当などを行い，インシデントが発生しないように活動を行っている．一方，インシデント対応時には侵害されている状況を把握し，リスクが最小限になるように被害範囲を隔離し，対応，復旧，再発防止までを行う．

これらの活動の主たる手段は機器類の警告の分析については機器が排出する電子的記録（以下ログ）を端末から確認したり，情報共有に関してはメールや Web で確認したり，インシデント対応については調査すべき機器に対してのログの確認など，もともとその現場に行かなくてもリモートで確認できる作業が多い．

ただし，ここでいうリモートとは社内であることが多く，いざとなったら顔を付き合わせて会議ができる環境である．

今回のリモートの定義は社内ではなく，在宅勤務のように実際に仲間と顔を合わせられない環境としている．

セキュリティ活動の大きな要素のひとつとして，対 CSIRT, 対社内，対他組織などとの情報共有やコミュニケーションの正確さがある．

この部分の変化としては電子会議やメール連絡，情報共有基盤などが今まで以上に用いられるようになってきているが，反面，コミュニケーションの精度が低下していると考えられる．

情報の伝達方法としてメールのような文字のみで伝達する場合には，発信側の文章作成能力，受信側の文章読解能力によって正確性や効率が極端に変化する．情報伝達については対面であれば話す人の表情や受け手の表情によって正しく理解できたのか，何を補足すればよいのか，がわかることもあるが，メールや情報共有基盤のみでは今まで以上の文書作成・読解能力が求められる．電子会議にて顔を画面

に映し出すことができれば，ある程度は精度があがるが，依然として，温度感や雰囲気などは対面よりも劣っている．

逆に電子会議の利用方法によっては，今まで対面以外では行えなかった各地域どうしでのコミュニケーションが即時で行えるため，移動時間や宿泊などのコスト・時間が圧倒的に削減でき，短時間の開催が可能である，頻繁に情報が交換できるという大きなメリットがある．この詳細については第3回にて説明する．

もうひとつのセキュリティ活動の大きな要素として，インシデント対応時に侵害された，もしくは疑わしい機器を押収して現物を精密検査することが必要となることがある．

この場合についても，もちろん電子的にデータを転送してリモートで行うことも可能ではあるが，現物を調査する，ということもまだまだ多い．手段としては現物の引き渡しが発生し，リモートでは不可能な作業となる．また，精密検査に必要なソフトウェアについても社外に持ち出せないケースもあり，出社対応にならざるを得ない場合がある．これについては，安全に出社してどのように現物を引き渡すのか，出社はどのように人的ローテーションを行うのかの課題があるが，詳細については第2回にて説明する．

これらのリモート時代のセキュリティ活動に完全移行するためにはコミュニケーションの正確性の向上や従業員の安全確保のための設備の準備，完全在宅勤務による勤務形態の変更など，経営としても考えなければならないことが多くある．これらについては法的な面も含め，詳細については第4回にて説明する．

今回はこれらのインシデント対応や情報共有以外のセキュリティ活動について，何が変わったのか，どうすべきなのかを説明する．

3. リモート環境でのメリット・工夫が必要なこと

セキュリティ活動の平常時の主な活動内容として，資産管理（リスク管理含む），リリースする製品に対しての脆弱性診断，役職員への教育，経営者への定期報告がある．

資産管理については定期的な棚卸しによって最新の状態を維持することが行われる．手法としては，チェックリストなどによる自己点検の他にセキュリティ担当者のヒアリングによる実地確認という手法がある．チェックリストについてはリモート環境でも環境の変化はないが，この実地確認という手法については工夫が必要となる．実地確認のメリットとしてはセキュリティ担当者が確認部門を訪問することにより，ヒアリング相手の表情や雰囲気による回答の正当性，職場の散らかり具合，監視カメラやドア施錠の状況など，総合的にリスクを判断できることである．施錠管理されているはずのロッカーが開いたままだったり，パスワードを付箋紙で貼ってあったり，サーバーにUSBメモリが挿しっぱなしになっていたり，現地調査ならではの気づきが得られる．この部分については訪問なしのリモートでは確認が難しく，できればドローンなどを飛ばしてリアルタイムでチェックするなどの代替案が欲しいところである．ヒアリングについても重要な資産についてはチェックリストについての誤解を防ぐために念のために電子会議で記載内容の確認を行いたい．この部分については現場へ行く時間もコストも短縮できるため，多少雰囲気を感じる精度は落ちるが，リモート時代のメリットであろう．

リリースする製品に対しての脆弱性診断やガイドライン通りに作られているかの確認については，従来からオンラインで審査を行っているところが多いと思われるため，リモート時代でも変化はない．しかし，同じように重要な箇所は電子会議にて確認すべきである．これについても，隙間時間を利用して短時間で行えるため，リモート環境のほうが効率的である．役職員への教育については，対面教育とE-ラーニングの2手法で行っているところが大部分であると思われる．E-ラーニングについてはリモートでも今までと変わらない．

対面教育の良さとしては講義中に受講者の顔色を見て理解度が把握でき，講義内容をその場でアレンジできることである．電子会議では受講者の顔は写せるが，現場よりは雰囲気がつかみにくい．電子会議の性格として，同時に複数人から発言すると聞き取れなくなるため，ワイガヤの会議がしづらく，自然と発言が減る傾向がある．また，現場よりも集中力が切れやすいため，短時間のコマをセットで組む

ようなカリキュラムの工夫も必要である．ただし，教育についても各地域からの従業員の参加しやすさ，隙間時間にカリキュラムが組めるという点では大きなメリットがある．

経営者への報告については少人数であれば，電子会議でも変化はないが，大人数になった場合には役職員への教育と同様にメリット，デメリットがある．

なお，リモート時代の報告では電子的なコミュニケーション能力の問題は大きくなり，正しく，簡潔に，相手のレベルに合わせてわかりやすく書く，ということが一層重要なスキルとなる．

平常時の活動について，リモート時代ではこのような変化への対応と改善が求められる．では，インシデントが発生した時の対応はどうなるのだろうか．

実際にインシデント対応で行う活動について，リモートで行える行為，現地でなければ行えない行為，その場合の注意点などを次回説明する．

略歴

阿部恭一（あべ　きょういち）
汎用機から AI の応用まで急発展する時代を開発者として活躍．2004 年以降セキュリティに従事し，ASY-CSIRT として ANA グループ全体のセキュリティ向上を図る．書籍：『CSIRT―構築から運用まで』（共著）NTT 出版．『CSIRT 小説―側線』ITmedia エンタープライズ．