〈コロナ禍でのCSIRT活動〉リモート時代のセキュリティ活動

II. コロナ禍におけるCSIRT活動の考慮事項

小村誠一（こむら　せいいち）
NTTアドバンステクノロジ株式会社

1. はじめに

CSIRT（Computer Security Incident Response Team）は，不測の事態に備え，それ自体の事業継続に関する対策を用意することが求められる．しかし，2020年のコロナ禍では，従来では想定できない事態が発生し，CSIRT自体の事業継続計画がなく，コロナ禍で発生した状況に十分に対応できなかったチームが発生した．本稿ではコロナ禍におけるCSIRT活動について，その事業継続性とメンバの安全性に関する課題や対策について紹介する．

2. CSIRTのリスクマネジメント

端末のマルウェア解析やOAネットワークへの不正侵入などの情報セキュリティインシデントに対応するCSIRT（Computer Security Incident Response Team）は，一刻を争う緊急時にも活動することが求められる．そのため，メールや電話，他のコミュニケーションなど，複数の連絡手段を用意するとともに，チームによっては，夜間や休日も連絡を受け付ける体制を構築し，システムの状況把握やセキュリティパッチ適用の相談をいざというときに各部署と相談できるよう，連絡体制を整備しているチームが多い．また，CSIRTだけでは対処できない案件が発生した場合に備え，経営層や法務部門などへのエスカレーションを行う方法も整備している．更に，自組織のシステムのセキュリティホールや関連情報の漏えいなどを通知してくれる外部組織からの連絡について，GWや年末年始の時期でも受け付けられるように体制を準備している場合がある．このようにCSIRTは組織内外といつでも連携し，活動できる仕組みを持つことが重要である．筆者も，2011年の東日本大震災の後，当時所属していた組織のCSIRTのオペレーションルームが非常電源装置から電力を供給するように変更するなど，自然災害の被災後にも活動が継続できるよう改善をした．CSIRTのリスクマネジメントについては，自然災害への対処以外のものもある．ヨーロッパで開発され，世界のCSIRTコミュニティでも活用されているSIM3（Security Incident Management Maturity Model）は，CSIRTが組織や社会の変化に追随し，組織として安定して活動するために検討・整理すべき項目をまとめたCSIRT成熟度モデルである．その中にコミュニケーション手段の冗長性や経営層へのエスカレーションなどのリスクマネジメントに関する項目が含まれている．このように，柔軟に対応できることを重視するCSIRTは，今までも運用体制や環境などについて，活動を継続させるための改善が行われていた．

しかしながら，昨年2020年4月の緊急事態宣言が出た際には，従来の事業継続プランでは，カバーしきれない状況が発生した．テレワーク環境は従来から整備し使用していた企業が少なくなかったが，オフィスなどの職場を中心に，一部のメンバが一時的に使用するという前提でテレワーク環境や業務を設計・整備していたため，想定以上の社員がテレワークを実施する状況となり，一部の業務に混乱が発生した．また，従来の自然災害は一部地域で事業継続が困難になる，そして他の地域は通常の業務が行える場合が多かったが，今回は日本全国，世界の多くの地域で同時に活動制限が発生したため，活動拠点を移動させて事業を継続するという手段は選択できなかった．CSIRT活動も同様で，業務を行うオペレーションルームや事務スペースを前提に運用の設計・構築を行っていたチームが多かった．出社制

限により通常の業務が行えない状況が発生したケースや，逆に業務を継続するために出社を続けていたケースなど，事業継続と社員の安全性確保が充分に両立できない状況が発生した．また，マルウェア感染した端末を使用していた社員がコロナに感染していたことが確認できた場合，マルウェア対応を行う際に，その端末のキーボードやマウスをどのように操作するか，インシデント対応を行うCSIRTメンバの安全性をどのように守るかなど，健康被害を防ぐための対策を検討・整理するがある．このように新たな観点でのメンバの物理的安全性を検討・整理する必要があった．

これら新たな課題や対策検討の資料をまとめておくことは，さまざまなCSIRTや関連組織に対し，また将来のCSIRT関係者に有意義であると考えた．そこで有志を募り，コロナ禍におけるCSIRTを取り巻く状況や課題，対応事例を収集・整理することとした．そして，広くさまざまなコロナ禍におけるCSIRT活動の課題を早く認識し，対策に取り組みはじめること，対策事例を参考に自組織の取り組みを検討整理していただくことを目的に，「新型ウイルス感染リスク禍におけるCSIRT活動で考慮すべきこと」[1]を公開した．本文書は，CSIRTにおける事業継続やメンバの物理的安全確保の課題や対策の事例として，昨年度，日本シーサート協議会（以下，NCA）で整理，公開したものであり，以降で，その内容を紹介する．

3. コロナ禍でのCSIRT活動における課題

コロナ禍による活動制限やテレワークの推進により，今までの方法で連絡が行えないことや，一部の業務が行えない状況が発生した．その状況は自組織内だけではなく，他社や他組織も同様で，従来ならば速やかにできた連絡や一次調査が長引く状況が発生した．今回のコロナ禍がCSIRTに与えた特徴を以下に列挙する．

- 従来の自然災害は特定の地域が被災し，他の地域は業務継続が可能であったが，今回は日本全国や世界の広範囲で同時に発生した
- 活動制限などの感染予防策が社会全体で急速に実施されたため，テレワークを主体とする業務の整備が，CSIRTを含む多くの部署で十分に整備できないまま，実施する状況になった
- リモート接続が許可できない特殊なツールの操作や，会社のコンピュータで発生したインシデントの対応など，CSIRT業務ではどうしても現地対応が残る場合がある．その際の物理的安全対策を整理する必要があった

[1]では，2020年5～6月の時期にCSIRT活動を継続するうえでの課題を収集した．収集した課題の一部を以下に列挙する．

- 監視ルームや作業場所でコロナウイルス感染が発生
- 稼働が確保できないため，通常時のCSIRT業務が実施できない
- CSIRTメンバ間でコミュニケーションができない，相談できない，連絡つかない可能性
- テレワークで各種ツール類の利用ができない（私用PCに会社資産ツールをインストールできない，CSIRTで使用するツールをテレワーク環境経由でアクセスできない）
- インシデント対応活動によるコロナウイルスへの感染
- （メンバの不足やリモート作業，協力会社の稼働縮小による）インシデント対応の遅延
- テレワーク体制による連絡網の不整備や不整合による連絡の遅延

上記の課題は大きく，CSIRTの事業継続とメンバの物理的な安全確保に分けられる．そのため，CSIRTの活動ごとに，事業継続とメンバの物理的安全確保の観点から対策の収集・整理を行った．

4. コロナ禍でのCSIRT活動の課題への対応

CSIRTメンバをはじめ，従業員や関係者の安全確保を最優先として，以下を対策方針とすることとした．

- 各組織の状況に応じて，可能な限りテレワークに移行
- テレワークの移行が難しい業務については，感染防止などの対策実施や出社日のローテーション化を実施
- 関係会社・協力会社や感染症安全管理部門などの連絡体制の整備
- テレワーク環境のセキュリティ確保，利便性向上

表 1　CSIRT の各活動における課題と対策の枠組み

項目		解説
想定される課題		業務を行う上で想定される懸念や課題
想定される副次的な課題		想定される課題の具体例
活動場所	リモート	業務をリモート（遠隔）で行える場合
	現地	オフィスや発災（インシデント発生）場所で業務を行う必要がある場合
解決の方向性		想定される課題への対策方針や考え方
実施手段例		具体的な対策方法の例
組織としての備え		CSIRT としてではなく，会社や大学，団体など組織全体として実施すべき対策

表 2 「インシデント対応」で考慮すべきこと　実施手段例：安全性の観点

リモートでの対応	現地での対応
●リモートアクセスツールについては，権限設定や不正操作が調査できる仕組みを構築 ●アクセスポイントは上記の仕組みで一元管理し，個別のアクセスを許可しないように設定 ●特定の場所ではなく，テレワークにてインシデント受付・対応ができる仕組みを構築 ●リモートにてディスクイメージを取得し，大容量回線を使ってデータ転送する環境 ●大容量ストレージを利用する（接続 PC には電子証明書などのセキュリティ対策を実施） ●24 時間電源 ON はリスクがあるため，リモートで電源 ON/OFF できる BIOS の端末を利用	●毎日検温し，一定以上の高い体温が継続する場合，医師などに相談するとともに，上司に連絡 ●熱が高い場合や喉の痛みがあるなど，健康が優れない場合は出社しない ●出社しての作業場所では，入口に消毒液を設置，マスク着用，換気，空気清浄などを実施 ●作業場所の過密な状態を避けるためのローテーション制の整備 ●インシデント対応で現地に向かう前に，担当する CSIRT メンバの体調を確認し，状況によって担当者を変更 ●インシデント対応で発災当該者や周りの人の体調を確認し，感染防止備品の使用など安全性の確保 ●CSIRT として，マスク，フェイスガード，ビニール手袋など，消毒備品や感染防止備品を用意 ●感染者使用機器の一定期間の隔離手順を整備 ●発災組織や現地に向かう前に，インシデント対応する CSIRT メンバと発災組織側の担当者の体調を確認

のための ICT 環境・ルールの整備

上記に則り，CSIRT の活動ごとに表 1 の枠組みを用いて課題や対策事例を整理した．収集した CSIRT 活動の課題への対応については，CSIRT メンバが業務する場所がリモートか現地かを基に，事業継続と物理的安全性の観点から整理した．

リモートの場合

●事業継続性

リモートで作業する CSIRT 活動の選定，業務上使用するツールの使用可否確認，対象のシステムや従業員（コンスティチュエンシ）のリモート環境の再確認，連絡網の構築，など

●安全性

リモート作業環境のセキュリティ確保

現地作業の場合

●事業継続性

保有スキルを考慮したローテーション設定，継続する CSIRT 活動の選定や対応時間の見直しなど

●安全性

出社時やオペレーションルーム入室時の除菌，インシデント対応時の体調不良従業員を発見した際のエスカレーションルール制定など

上記の観点から対策の方向性を検討し，収集した例と併せて整理した．表 2 に，インシデント対応における，対策例をあげる．議論や収集した対策の中には，CSIRT が実施すべき項目以外に，会社や大学など，組織全体として整理，実施した方がよい項目があったため，それらを「組織としての備え」という分類でまとめた．「組織としての備え」は，以下の 5 つに分類している．

●従業員に関する対策

●技術・システムに関する対策

●物理・ファシリティに関する対策

表3 「インシデント対応」で考慮すべきこと　組織としての備え

リモートでの対応	現地での対応
従業員に関する対策 ●感染時，強制隔離時に従業員の休暇取得や事業継続を行う体制の確保	**従業員に関する対策** ●感染時，強制隔離時に従業員の休暇取得や事業継続を行う体制の確保 ●時差通勤など，安全性に配慮した勤務時間の設定
技術・システムに関する対策 ●大容量回線の確保（一時的にでも） ●安全なテレワークの仕組みの用意	**技術・システムに関する対策** ●システム的に可能なリモート作業の切り出しを検討 ●社内作業においても必要時以外は密閉空間でない職場で勤務するための工夫
物理・ファシリティに関する対策 ●テレワーク実施場所での安全な環境の確保 ●留守電メッセージの音声データの転送システム	**物理・ファシリティに関する対策** ●出社し作業する場合でも密集空間や密閉空間での作業を避けるための工夫 ●機器を発送・受け取りに関する消毒や防備備品の確保，使用 ●会社作業場所に出社した人の感染を確認した際の連絡や消毒手順，立入制限・解除方法の整備
プロセスに関する対策 ●オンラインフォレンジックの手続き，要領書の準備 ●事後承認，承認者の拡大規程の策定	**プロセスに関する対策** ●業務ごとのリモート作業の可否の整理とリモート作業不可部分についての対応方針の整理と決定 ●感染者使用端末を操作したメンバなど，接触者の一定期間隔離や健康状態管理手順の策定
法制度面に関する対策 ●証拠保全（特にデジタルコピーや伝送データの証拠能力）に関する事前シミュレーションおよび関係各所との取り交わし ●トラブル発生時に報告期限が法律や契約で定められている案件や業務の抽出，対応計画策定	**法制度面に関する対策** ●トラブル発生時に報告期限が法律や契約で定められている案件や業務の抽出，対応計画策定 ●自社業務により派遣社員が感染した場合の対応の整備

●プロセスに関する対策
●法制度面に関する対策
表3に，インシデント対応に関する，組織としての備えの例をあげる．

これら対策例は2020年5～7月時点のものであり，現在からみると不十分なものや，過剰な対策などもあるかもしれない．ただ，それらを精査するよりも事例を収集し，少しでも早く共有することを優先した．課題についても現時点では対応され，考慮する必要がなくなったものもあるかもしれない．しかしながら，それらも含め，本ドキュメントとしてまとめたことにより，将来，別の事業継続や安全性を考慮する必要が生じた際，良い点や悪い点も含め，参考になると考えている．

また，本ドキュメントの内容は，2021年6月に開催された世界のCSIRTコミュニティ：FIRSTの，33rd Annual Conferenceでも発表した．CSIRTの事業継続性や物理的安全性を検討・整備する点については，同意するコメントを何人かからいただいた．これからも日本発のCSIRT関連の成果を共有し，世界のセキュリティ向上に寄与したいと思う．

次回は，コロナ禍におけるCSIRTのコミュニティ活動について紹介する．

参考文献

[1] 新型ウイルス感染リスク禍におけるCSIRT活動で考慮すべきこと―CSIRT対応プラクティス集（ver. 1.0）―，日本シーサート協議会，https://www.nca.gr.jp/activity/evaluation_model.html

略歴

小村誠一（こむら　せいいち）
経営情報学会会員，情報処理学会会員，日本セキュリティマネジメント学会会員．形式的仕様記述などの研究開発に従事した後，情報セキュリティ統括業務やCSIRTにおいてインシデント対応や機能強化の業務に従事．NTTアドバンステクノロジに勤務の後はCSIRT関連の活動に加え，CISSPやセキュリティ研修業務も担当．書籍：『CSIRT―構築から運用まで』（共著）NTT出版．『CISSP公式問題集』（共同翻訳）NTT-AT.