TLP:WHITE

EthicsfIRST
インシデント対応およびセキュリティチームのための倫理規範

インシデント対応およびセキュリティチーム（以降「チーム」と略）のメンバーは多くのデジタルシステムや情報源にアクセスすることができる。彼らの行動は世界を変えることもある。この専門職に従事する者として、チームメンバーは自分のコンスティチュエンシー[1]や他のセキュリティ専門家、さらにはより広く社会に対する責任を認識しなければならない。また、一人ひとりが自分自身の幸福に対する責任も認識しなければならない。

EthicsfIRST はチームメンバー全員の倫理的な行動を奨励し、またその手引きとなるように設計されており、対象には現在および将来の実務者や指導者、学生、インフルエンサーなど、コンピューター技術を影響力のある方法で使用するいかなる人も含まれている。このフレームワークには、公共の利益が常に第一に考慮されるとの理解に基づいて、責任の表明として策定された原則が含まれている。各原則はガイドラインによって補足されており、コンピューター関係の専門家が原則を理解し適用するにあたり手助けとなる説明がなされている。

複数の義務が以下に紹介されているが、これらは重要度の順ではない。これらの義務は絶対的な要件とみなすべきではなく、どちらかと言えばIETF RFC2119における「SHOULD」の定義として記載されているものである。

> 「この語句もしくは「推奨される（RECOMMENDED）」という形容表現は、特定の状況下では、特定の項目を無視する正当な理由が存在するかもしれませんが、異なる選択をする前に、当該項目の示唆するところを十分に理解し、慎重に重要性を判断しなければならない、ということを意味します。」[2]

起こりうるジレンマへの対処法については付録 A を参照のこと。

信頼性の義務

信頼はチーム間の多くの関係の基礎であり、有意義な情報交換が行われる前に必要とされることが多い。FIRST のコミュニティはこの信頼関係の上に成り立っており、チーム間に妥当なレベルの信頼関係があるからこそ、このように機能し続けることができるのである。

信頼性とはチームメンバーが 1) 守れる約束をする、2) 他のチームに対して予測可能な行動を取る（例：TLP 基準を尊重する）、3) 他のチームとの信頼関係を維持する、といったことを意味する。

---

[1] 訳注：constituency - CSIRT がサービスを提供する対象、守る対象である人やシステムなど。

[2] 訳注：RFC2119 日本語訳 https://www.ipa.go.jp/security/rfc/RFC2119JA.html より。

信頼関係は仮定から始まり、推移的に醸成されるべきである。すなわち、Trust on First Use（TOFU）[3]であり、他のチームから信頼されているチームに対する信頼を可能にする。

協調的な脆弱性開示の義務

脆弱性を認知したチームメンバーは、利害関係者と協力してセキュリティ脆弱性を修正し、開示に伴う損害を最小限に抑えることで、協調的な脆弱性開示（Coordinated Vulnerability Disclosure）に従うべきである。利害関係者には脆弱性の報告者、影響を受けるベンダー、コーディネーター、ディフェンダー[4]、およびダウンストリームの顧客[5]、パートナー、ユーザーが含まれるが、これらに限定されない。

チームメンバーは適切な利害関係者と調整して、情報公開の明確なスケジュールと期待される結果に合意し、ユーザーがリスクを評価して実行可能な防御策をとれるような十分な詳細情報を提供すべきである。

機密保持の義務

チームメンバーには必要に応じて機密性を保持する義務がある。特定の情報を機密にしておきたいという要求は、Traffic Light Protocol（TLP）などで明示されることがある。チームメンバーは可能な限りそのような要求を尊重すべきである。しかし、例えば現地の法律や契約、通知義務などの要件と矛盾するために情報を機密にしておくことができない場合、チームメンバーは情報の所有者にこの矛盾について直ちに知らせるべきである。

守秘義務の中には法律、規則、慣習に基づくものもある。インシデント対応中に一部の当事者がそのような考慮事項に基づいて守秘義務に拘束されたり、守秘義務を期待したりする場合には、これらの期待を事前に明示するように最善を尽くすべきである。そして、可能な限り情報を機密にしておくようにとの明示的な要求を維持するために、すべての当事者は上記の期待に従うべきである。

受領確認を返信する義務

チームは、研究者、顧客、他のチーム、政府機関など、さまざまなソースから情報を受け取る。チームメンバーは、たとえリクエストを受け取ったことを確認するだけであっても、問い合わせに対してタイムリーに返答すべきである。可能であれば、チームメンバーは次の情報更新の見込みを設定すべきである。

認可についての義務[6]

チームメンバーには自分の責任範囲を理解し、アクセスを許可されたシステムでのみ行動

[3] 訳注：本来は、未知またはまだ信頼されていないエンドポイントとの信頼関係を確立する必要があるクライアントソフトウェアが使用する認証スキームのことである。
[4] 訳注：攻撃などに対する「防御側」の意味。
[5] 訳注：「ダウンストリーム（川下）」は顧客との契約関係を川の流れに喩えたもの。
[6] 訳注：厳密には「認可された範囲で行動する義務」である。

する正当な必要性と権利がある。チームメンバーは自分たちの行動がコンスティチュエンシーにどのような影響を与えるかを認識し、職務の遂行中にさらなる損害を与えないようにする必要がある。可能であれば、コンスティチュエンシーのシステムに変更を加える前に、コンスティチュエンシーに意見を聞くべきである。

情報を提供する義務

チームメンバーは現在のセキュリティ上の脅威やリスクについてコンスティチュエンシーに情報を提供し続けることを義務と考えるべきである。チームメンバーは安全性やセキュリティに悪影響を与える、または改善する可能性のある情報を持っている場合、守秘義務、プライバシーに関する法律や規則、その他の義務を正しく考慮しながら、適切な努力をもって関係者や協力してくれる人々に知らせる義務がある。

人権を尊重する義務

チームメンバーは、情報共有や潜在的な偏見、財産権の侵害を通じて、自分たちの行動が他者の人権に影響を与える可能性があることを認識すべきである。チームメンバーはインシデントに対処する過程で広範囲の個人情報、機密情報、および秘密情報にアクセスすることになる。これらの情報は、人権を守る方法で取り扱われるべきである。

インシデント対応中に、対応者は偏った行動をとってはならず、対応者が行う場合もアルゴリズムに組み込まれている場合も、プロセスや意思決定から偏りを排除するために最大限の努力をすべきである。

この原則においては、「財産（property）」の概念（国連の世界人権宣言[7]第17条）には、法的に保護されているかどうか（特許取得の有無など）にかかわらず、知的財産などの無形財産、およびアイデアやコンセプト全般が含まれている。

チームの健康に対する義務

チームにはコンスティチュエンシーに約束したサービスを継続して提供する責任がある。この責任にはチームの身体的・精神的な健康も含まれる。

チームを構成するメンバーを個人として尊重し、かつ適切なレベルのサービスの維持を長期的に実行可能にするために、チームは（すべての）メンバーの身体的・精神的な健康を支える、健康的で安全かつ前向きな職場環境を維持するよう努めるべきである。危機に対応するためには、「通常」の業務で精神的な健康とストレスの軽減をサポートする必要がある。

チームの能力に対する義務

インシデント管理はチームメンバーが継続して研究すべき発展的課題である。チームはメ

[7] 訳注：「世界人権宣言」全文の日本語訳
https://www.amnesty.or.jp/human-rights/what_is_human_rights/udhr.html

ンバーが自らの責任範囲内で技術的かつ科学的知識を学び、適用し、そして発展させるためのリソースを提供すべきである。トレーニングまたは教育のための CPE[8]/CEU[9]クレジット[10]は一助となるかもしれないが、単なるコンプライアンス演習ではこの義務を果たすには不十分である。チームはそのサービスを可能にするために十分な技術的インフラを維持すべきであり、これには外部による干渉からそのインフラを保護するための適切な手段をとることも含まれる。

責任ある収集の義務

データ収集はインシデント対応に必要だが、インシデント対応の目的とデータの利害関係者を尊重することとの間でバランスを取るべきである。

調査中に、収集が必要な情報の量が変わることがある。インシデントへの対応を進める一方で、チームメンバーは必要性の変化に応じて収集する対象を調整すべきである。インシデントとその復旧に直接関係のないデータは報告から除外すべきである。

収集および抽出したデータは、適用される法律に従い、ユーザーのプライバシーを尊重して取り扱わなければならない。データ所有者の管理下にあるデータを収集および処理する際には事前に許可を得るべきである。データの取り扱いにおいて適用される法律および規則を順守すべきである。

他のインシデントに関連して他の対応チームの活動に役立つかもしれないデータは、場合によっては編集された形で、その対応チームに提供すべきである。機密情報および所有権のある情報の提供は、適切な保護措置が講じられている場合に限るべきである。

インシデントの被害軽減のために第三者とデータを共有する際には、事前にリスクと利益を比較検討すべきである。データの共有は利益がリスクを明らかに上回る場合に限るべきである。機密データはインシデントがクローズした後に容易に破棄できる方法で保存すべきである。収集したデータはデータ保持ポリシーに則って安全に破棄すべきである。

管轄区域の境界を認識する義務

チームメンバーはインシデント対応に関連する活動に関与する当事者の管轄区域の境界、法的権利、規則、および権限を認識し、かつ尊重すべきである。

プライバシー保護やデータ侵害の通知に関連するものなど、法律、規則、その他の法的問題は、関係する管轄区域によって異なる場合がある。管轄区域の境界は、関係者の国や居住地などの物理的な場所や、関係者に関するその他の要因によって決定される場合がある。一つの国の中であっても、政治的な地域間（例：米国の各州間）や、国内の異なるビジネス、産業、セクター間（例：ヘルスケア、金融サービス、政府機関）で、法律や規則が異

[8] 訳注：Continuing Professional Education（継続的専門研修）
[9] 訳注：Continuing Education Units（継続教育ユニット）
[10] 訳注：「CPE/CEU クレジット」は継続教育を登録する単位である。

なる場合がある。ナショナル CSIRT[11]は、自らの管轄区域内のコンスティチュエンシーが関与する活動に対して指定された責任や権限を有する場合があり、また境界を越えた管轄区域に対して権限を有する他の組織と協力したり、その組織に情報や活動を「引き渡し」たりする場合もある。

チームメンバーは、プライバシー規則やデータ侵害通知の要件をはじめ、関係する管轄区域に影響を与える重要な問題を認識しておくべきである。サイバーセキュリティやプライバシーに関する法律や規則は世界中で進化し、かつ更新され続けているため、複数の管轄区域の境界に関わる問題が発生した場合には十分な知識を持った弁護士に相談して指針を得ることが望ましい。

根拠のある推論の義務

チームは検証可能な事実に基づいて活動すべきである。侵害の指標（indicators of compromise：IOC）やインシデントの説明などの情報を共有する場合、チームメンバーは根拠とスコープを透明性のある形で提供すべきである。それが不可能な場合は、その根拠とスコープを共有しない理由を情報とともに提供すべきである。

チームメンバーは、噂を広めたり共有したりすることを控えるべきである。いかなる仮説もそれが仮説であることを明確に示すべきである。

透明性のある根拠と推論のプロセスは、例えば大量の情報を自動的に共有するような場合でも重要である。この場合、データマイニングプロセスの説明は分かりやすいレベルの詳しさで伝えるべきである。

付録 A

ジレンマへの対処

チームメンバーは倫理原則の全てを満たすような行動が何もない状況に陥ることがよくある。そのような状況では、どの原則を優先すべきかを選択しなければならない。この状況において、インシデントハンドラーには、自分たちの行動によってどの利害関係者がどのような影響を受けるかについて、できれば同僚との話し合いの中で検討することが望まれる。原則として、この倫理規範のフレームワークに反するものを最小限に抑える解決策を選択すべきである。時には、外部からの圧力などによって、それが不可能な場合もあるかもしれない。そのような状況では、倫理的ジレンマに注意しながら、不承不承でも前に進めることが推奨される。

[11] 訳注：National CSIRT - 国や地域の国際的な窓口としての役割を担う CSIRT のこと。