ランサムウェア・インシデント発生時の組織向けガイダンス

序文/ステートメント：

1. カウンターランサムウェア・イニシアティブ[1]のメンバーは、保険機関[2]と連携して、ランサムウェア攻撃を受けている組織とその被害組織を支援するパートナー組織向けのガイダンスを発出する。

2. ランサムウェアによる金銭支払い要求に応じることはランサムウェアのビジネスモデルを拡大させ、2023 年には、全世界のランサムウェアの金銭支払いが過去最大となった（Chainalysis[3]）。

3. ランサムウェアは国境を越えた複雑な問題であり、対処するためには強力な国際連携が必要である。2023 年に開催された第 3 回 CRI サミットでは、CRI[4]はランサムウェアの要求に対し金銭支払を避けることを強く勧める共同声明を発出した。この声明はランサムウェアの実行者への身代金の支払いについて、次のように認識している。

    - インシデントの終息や、貴方のシステムから悪意のあるソフトウェアの削除を保証しない。
    - 犯罪者に対して、彼らの活動を継続・拡大させるインセンティブを与える。
    - 犯罪者が不正活動のために使用できる資金を提供する。
    - 貴方がデータを取り戻すことを保証しない。

4. **このガイダンスに拘束力はなく、CRI メンバーの法的管轄下で適用される特定の法令に優先するものではない。**

5. ランサムウェア攻撃を受けた組織にとって、身代金を支払うかどうかの判断は簡単ではない。CRI は、

---

[1] アルバニア、アルゼンチン、オーストラリア、バーレーン、ベルギー、カナダ、チャド、コロンビア、コスタリカ、デンマーク、ECOWAS 委員会、フランス、ドイツ、ギリシャ、アイルランド、イスラエル、日本、ケニア、リトアニア、メキシコ、モルドバ共和国、オランダ、ニュージーランド、ナイジェリア、フィリピン、韓国、ルーマニア、ルワンダ、シエラレオネ、シンガポール、スロバキア、スロベニア、スペイン、スイス、アラブ首長国連邦、英国、米国、ウルグアイ、バヌアツ、ベトナム

[2] 米国損害保険協会、英国保険会社協会、英国保険ブローカー協会、オランダ保険会社協会、オーストラリア保険評議会、ニュージーランド保険評議会、国際保険引受協会、スイス保険協会

[3] ランサムウェア被害額は 2023 年に 10 億ドルに達した（chainalysis.com）

[4] ランサムウェア不払声明 - GOV.UK (www.gov.uk)

ランサムウェア・インシデント発生時の組織向けガイダンスをとりまとめた。このガイダンスは、ランサムウェア犯罪者への支払いを検討する前に、組織が講じるべき手順の全体的な概要を提供しており、ランサムウェア犯罪者への支払いがもたらす悪影響の検討も含まれる。

6. このガイダンスは、ランサムウェア・インシデントが組織に及ぼす影響全体を最小限に抑え、かつ、
    - 業務の妨害とコスト
    - ランサムウェア被害組織による身代金の支払件数
    - ランサムウェア被害組織による身代金の支払額

   の軽減を目的とする。

7. サイバー保険は重要なリスク管理手法となり得る。CRI メンバーは、サイバー保険が保険契約企業の防御対策の改善を支援することなどを通じて、サイバー攻撃に対する強靭性の構築に重要な役割を果たしていることを認識している。CRI メンバーと民間サイバー保険機関は、ランサムウェアに対する組織の強靭性を強化し支援する民間サイバー保険機関の重要な役割をさらに深めることで協力する。

8. CRI メンバーと民間サイバー保険機関は、被害にあった組織が最終的にサイバー犯罪グループに身代金を支払うか否かを検討する前に、次のガイダンスを参照することを推奨する。

ランサムウェア・インシデント発生時の組織向けガイダンス:

1. 組織は、事業継続計画の一環として、ランサムウェア・インシデントに備えるため、前もって対応方針、手順、フレームワーク、コミュニケーション計画を策定し、実施しておくことを推奨する。

身代金支払いに関する正しい法規制の環境を考慮する

2. 組織が身代金を支払う前に法規制上考慮すべきことがあり、専門家がアドバイスを提供することができる。民間サイバー保険機関は、被害組織にアドバイスを提供できる弁護士を紹介することもできる。

3. 例えば、制裁対象になっている組織に身代金を支払う場合など、特定の状況下では支払いが合法でない場合がある。

当局へランサムウェア・インシデントを報告する

4. できるだけ早い機会に当局にインシデントを報告することは、被害組織への支援に繋がる。インシデントを報告することにより、当局は被害組織に必要な助言や支援を提供できるようになり、ひいては被害組織の強靭性を強化して、将来のランサムウェア・インシデントを防げるようになる。また、攻撃を受けた場合や支払いを行った場合のタイムリーな報告は、法執行機関等の当局が効果的な捜査を行い、ランサムウェア実行者の活動を将来的に阻止するための証拠を収集し、当局がランサムウェア犯罪行為について全体的に理解を深めて、将来の被害組織をより適切に支援し、場合によっては攻撃者の逮捕や起訴、攻撃者が使用するインフラやサービスの押収や妨害等を通じて将来の攻撃を阻止するためにも必要である。

すべての選択肢を評価する

5. ランサムウェア攻撃を受けた直後は、圧倒されるように感じるかもしれない。ランサムウェアの実行者は、組織に迅速な決断を迫る戦術を知っており、それを駆使している。しかし、利用可能な選択肢を慎重に検討することで、意思決定が改善され、より良い結果が得られる可能性がある。

6. デューデリジェンス、すなわち合理的な情報収集と潜在的な損害の分析は、あらゆる組織のインシデント対応と復旧計画の構成要素とするべきである。デューデリジェンスには次のような利点がある。

    - 重要な情報又は証拠を見逃さないという保証
    - 決定の裏付けとなる、データに基づいた明確な根拠

- インシデント報告など、国内関連法の要件を満たす能力

可能であれば専門家に相談する

7. 保険会社、国の技術担当当局、法執行機関、又はランサムウェア・インシデントに精通したサイバーインシデントレスポンス（CIR）会社など外部の専門家は、意思決定の質を向上させることができる。保険会社が組織を支援するCIR会社を推奨することはよくある。組織がサイバー保険に加入している場合は、保険契約の報告規定に従うべきである。

身代金支払いの代替案を検討する

8. 一般的な対応として、2023 年の第３回 CRI サミットで発出された共同声明[5]に従い、組織は金銭支払を避けることを強く勧める。

9. CRI の声明では、組織は金銭支払を避けることを強く勧めるが、現地の法規制に従い、被害組織が最終的に身代金の支払いを検討する場合もある。

10. 支払いに関する決定は、可能な限り、インシデントの影響と支払いによりその結果が変わるかどうかを総合的に判断した上で通知される必要がある。身代金の支払いにはマイナス面があるにもかかわらず、サイバー犯罪者は支払うことが唯一の復旧方法であると被害組織を説得しようとする。

影響と法的義務を評価するための関連情報の収集

11. 我々は、組織が以下のことを検討することを推奨する：

12. 組織はバックアップの利用可能性、復号鍵の代替入手先、復号鍵取得後の機能復旧にかかる時間の見積もりなど、技術的な状況について慎重に検討する。これらのツールのいくつかは、サイバーセキュリティ企業、法執行機関、又は市販のツールやオープンソースのツールから入手できる場合がある。

13. 業務妨害に対応する次善策を講じ、これらの次善策を維持する期間を決めておく。また組織への影響を検討する際は、システム機能性、業務運営への影響、顧客や従業員への影響（該当する場合はサプライ・チェーンへの間接的な影響を含む）、更なるデータ流出の可能性を評価する必要がある。

---

[5] ランサムウェア不払声明 - GOV.UK (www.gov.uk)

インシデントの影響を評価する

14. インシデントの影響を評価するための措置を講じることで、組織はより良い準備を整え、保険適用範囲を検討することができる。情報が最終的に漏洩するかどうかに関係なく、ランサムウェア・インシデント時のデータ流出の結果として、影響を受けた個人への通知、データ保護に関連する規制上の罰金など、既に何らかのコストが発生している可能性があることに留意することが重要である。そのため、これらのコストの影響は、身代金を支払うかどうかの決定とは別に考慮する必要がある。考慮事項には次のものが含まれる。

    - 加入している保険の補償範囲の調査。
    - 業務の中断、セキュリティ改善作業、スタッフの残業、訴訟費用又は規制上の罰金による収益損失の見積もり。
    - 盗まれた可能性があるデータや知的財産の特定、及び盗まれたデータが流出した場合には組織、顧客、該当する場合はクライアントに及ぶ可能性がある損害の推定。

15. 最後に、多くのランサムウェア・インシデントにおいて、サイバー犯罪者はデータも盗むようになっている。したがって、被害組織は身代金を支払えば盗まれたデータを削除するという約束を信用してはならない。組織が、盗まれたデータの特定とその機密性を判断するための評価を実施することは優れた取組みである。法的助言は、法規制の遵守、関連当局への報告や支援の要請に役立つ。また、データが公開された場合、生命、個人データ、又は国家安全保障へのリスクも評価する必要がある。盗まれたデータの性質と量に関する主張が真実であることを確認することを推奨する。

意思決定を記録する

16. インシデントへの対応、下した決定、実行した措置、回収した（又は欠落した）データを入念に記録しておくことは、インシデント後の検証、学んだ教訓、又は規制当局への証拠の提示のため重要である。インシデント時は、意思決定をオフラインで、又はインシデントの影響を受けないシステムで意思決定を記録することが賢明である。

17. このプロセスの目標は、意思決定に関する監査可能な証跡を生成し、意思決定に関する簡潔な説明を作成することにより、再度このような攻撃が成功する可能性を減らすことである。

18. このような取組は、規制プロセス、法制度、内部組織要件など、法的管轄区域によって異なる場合がある。

技術スタッフや上級意思決定者など、組織全体にわたって必要な関係者を意思決定に参加させる

19. 身代金を支払うかどうかの決定ほど迅速に上級経営者や意思決定者を関与させるシナリオは他にない。ただし、組織は選択肢の提示が時期尚早とならないこと、また、可能な限り強固な根拠に基づくようにすることに留意する必要がある。

身代金の支払いをしてもデバイスやデータへのアクセスが保証されるわけではないことに注意する

20. 復号鍵を入手できたとしても、すぐに通常の業務に戻れる可能性は高くない。複雑なネットワーク上での復号鍵の実行には時間がかかる。被害組織がバックアップにも復号ツールにもアクセスできる場合は、バックアップを使用する方が早いかもしれない。

21. 支払いを行って復号鍵を取得しても、インシデントの終息が保証されるわけではないことに留意することが重要である。被害組織は、侵害されたシステムがバックアップコピー又は復号鍵を使用して復元されたとしても安全であると推定すべきではない。バックアップコピーも侵害されている可能性があり、悪意ある行為者は、暗号鍵から復元されたシステムを将来の攻撃に対して脆弱なままにしている可能性がある。

22. また、悪意ある行為者が盗まれたデータを削除するという約束を履行しない可能性があること、悪意ある行為者が実際に盗まれたデータを削除したかどうかを確認する手段がない可能性が高いことも考慮する必要がある。

インシデント後の評価：インシデントの根本原因を調査し、再発防止に必要な準備を行う

23. 侵害元を明らかにしないで支払いを行うと、その後に適切な緩和措置を講じても、組織は更なるインシデントリスクに晒される。組織は、侵害がどのように発生したかを独自に検証し、欠陥があれば修復するよう努めるべきである。

24. 組織は、最初の侵入とそれに関連した脆弱性が修復されたかどうかも評価する必要がある。セキュリティ侵害の発生経緯を評価することは、将来のランサムウェア攻撃に対する防御力の強化に役立つ。これには、認証情報の管理、ネットワークの分離と区分化、オフライン/未接続のバックアップなどの予防策とリスク軽減策の実施が含まれる。