ランサムウェアに対するサプライチェーンレジリエンスを構築するため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・イニシアティブのメンバー国・機関[1]及びその民間セクターアドバイザリーパネル[2]は相互に連携して、ランサムウェアの脅威に対するサプライチェーンのレジリエンスを構築することに関する組織向けガイダンスを発出する。

2. **このガイダンスの目的は、組織がランサムウェア・インシデントによって重大な影響を受ける可能性を、**以下の方法で**低減することである**：

a. 組織のサプライチェーン全体でランサムウェアの脅威に対する意識を高める
b. サプライチェーンを保護するための適切なサイバー衛生（サイバーハイジーン）を推進する
c. サプライチェーンの脆弱性が、組織のリスク評価や意思決定（調達に関するものを含む）に確実に織り込まれるようにする

3. 各組織は、以下のガイダンスを参照し、既存及び将来のサプライチェーン運用者と協力して、推奨事項の実施を検討することが望ましい。**本ガイダンスの目的は、組織がランサムウェア攻撃に対するサプライチェーンの脆弱性を放置しないようにすることである。**

4. あらゆるインシデントに備えておくことが極めて重要であり、発生時の影響を軽減するうえでも有効である。2024 年に CRI は保険団体と連携して、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発表した[3]。本ガイダンスはこの 2024 年版文書に基づいており、特に組織とそのサプライチェーンを対象としている。

---

[1] アルバニア、アルゼンチン、アルメニア、オーストラリア、オーストリア、バーレーン、ベルギー、ブラジル、ブルガリア、カメルーン、カナダ、チャド、コロンビア、コスタリカ、欧州評議会（CE）、クロアチア、キプロス、チェコ共和国、デンマーク、ドミニカ共和国、西アフリカ諸国経済共同体、エジプト、エストニア、フィンランド、フランス、ドイツ、サイバー専門的知識に関するグローバルフォーラム（GFCE）、ギリシャ、ハンガリー、国際刑事警察機構（INTERPOL）、アイルランド、イスラエル、日本、ヨルダン、ケニア、ラトビア、リトアニア、メキシコ、モルドバ共和国、モロッコ、オランダ、ニュージーランド、ナイジェリア、ノルウェー、米州機構（OAS）、パプアニューギニア、フィリピン、ポーランド、大韓民国、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、南アフリカ、スペイン、スリランカ、スウェーデン、スイス、ウクライナ、アラブ首長国連邦、英国、ウルグアイ、バヌアツ、ベトナム、世界銀行

[2] パネルのメンバーは、Arctic Wolf、BlackBerry、CyberCX、Ensign Infosecurity、Institute of Science and Technology、Microsoft、英国王立防衛安全保障研究所から構成される。

[3] CRI「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」- GOV.UK、またはCyber Security Agency of Singapore「Singapore Contributes to Ransomware Guidance for Organisations（シンガポールが組織向けランサムウェア・ガイダンスに貢献）」を参照。

5.　　このガイダンスに拘束力はなく、CRI メンバー国・機関の法的管轄下で適用される特定の法令や国レベルのサイバーセキュリティ・ガイダンスに優先するものでもない。

主なガイダンス

ランサムウェアの脅威について

1. ランサムウェアは、規模が大きく、国際的な連携を要する課題であり、事業の運営や必要不可欠なサービスに重大な混乱を生じさせて我々の日常生活に影響を与える能力を持っいるので、世界中の組織にとって深刻な脅威となっている。

2. ランサムウェアの影響による混乱とは別に、ランサムウェア攻撃の被害者に生じる直接的なコストは莫大なものになる可能性がある。IBMの「2025年データ侵害のコストに関する調査レポート」によると、ランサムウェア攻撃1件の世界平均コストは444万米ドル [4] であった。間接的なコストも大きくなる。例えば、ランサムウェアの実行者が被害者を脅して身代金を支払わせようと試み、盗み出したデータをデータ漏洩ウェブサイトに公開し、結果として風評被害を招いたり、機密情報や個人識別用情報（PII）が流出して個人情報保護法違反とみなされたりする可能性がある。またランサムウェアの被害者は、二次的または三次的な恐喝の脅威に直面する可能性もある。

3. ランサムウェアの実行者は、その作戦の効果を最大化しようとしてサプライチェーンを標的にすることが確認されている。攻撃者は被害者のサプライヤーやパートナーの弱点を悪用し、侵害された1つのベンダーが入口となって、攻撃者がサプライチェーンの上流や下流へ横展開する可能性がある。

4. 例えば 2024 年 6 月、あるサイバー犯罪グループが英国の主要な NHS トラストの病理学サプライヤーである Synnovis 社にランサムウェア攻撃を実行し、複数の病院に大きな混乱をもたらした。このインシデントの被害を最も大きく受けた２つの病院トラストでは、インシデント後 4 か月で 10,152 件の急性期外来予約と 1,710 件の選択的手術に影響が及んだ [5]。

サプライチェーンのリスクとは？

5. 組織とサプライヤー間のやり取りに伴い、サイバーセキュリティリスクが生じる可能性がある。ランサムウェアの観点から見ると、サプライヤーにとっての主なリスクは、インシデントによってサービスが提供不能になること、及びデータの損失である。

6. より広範なサプライチェーンリスクが生じる可能性があるのは、次の場合である：

   a. **サードパーティのサービス：**マネージド・サービス・プロバイダー（MSP）が侵害されると、顧客が標的になる。

[4] 2025 年 データ侵害のコスト｜IBM

[5] NHS England - London » Update on cyber incident（サイバーインシデントの最新情報）: Clinical impact in south east London（ロンドン南東部における医療への影響）—2024 年 9 月 26 日（木）

b. **相互接続システム：**組織によっては、サプライヤーとの間で相互接続されたシステムや信頼された接続が存在し、サプライヤーに特権的なアクセスを与えている場合もある。また、組織のシステムアーキテクチャがリスクに対して十分に保護されていない可能性もある。
c. **特権データ**：組織は、適切な管理体制を整備することなく、サプライヤーに機密データを提供している場合がある。

7. このようなリスクは、以下の要因によって増幅する可能性がある：

a. **高い集中度／依存度のリスク：**
少数のサプライヤーからのサービス提供に対する依存度が高い／不均衡であると、リスクが増幅する可能性があり、ランサムウェア・インシデントの影響が複雑化する可能性がある。状況に応じてサプライチェーンを多様化することで、こうしたリスクを軽減できる。
b. **サプライチェーンの可視性が低い場合**：組織は、自分たちが認識できないものを守ることはできない。
c. **不十分な保証メカニズム：**契約時及び契約期間を通じてサプライヤーのセキュリティ適格性を検査しない組織は、安全でないサプライチェーンのリスクを負うことになる。

サプライチェーン・セキュリティへの取り組み

8. このガイダンスでは、組織がランサムウェアのリスクに対応し、サプライチェーン・セキュリティ態勢を改善する方針を策定する際の指針となる原則を示す：

ステップ1：
サプライチェーンのセキュリティが重要である理由を理解する（*「なぜ？」*）

a. グローバルなデジタル経済において、企業の事業運営はこれまで以上にサプライチェーンに依存している。このような相互依存関係により、サプライチェーンはサイバー攻撃者の格好の標的にもなっている。このため、組織が業務の混乱を防ぎ、機密情報を保護し、業務効率を維持するには、サプライチェーンを保護することが重要である。
特に契約上の要件を通じて、サプライチェーンに強固なサイバーセキュリティを確実に組み込むようにすると、個々の組織や相互接続されたサプライチェーンの脆弱性を減らし、重要インフラやその他の重要なシステムに対するリスクを軽減することができる。

ステップ2：主要なサプライチェーン・パートナーとそのアクセスレベルを特定する（*「誰が？」*）

a. サプライヤーの一覧を作成し、契約の一環として当該サプライヤーが保有することになる情報／資産の機密性と価値を理解し、サプライヤーについて以下の評価を行う：

- サイバーセキュリティの成熟度（多要素認証、パッチ管理、バックアップの慣行、認定などの有無）
- 過去のデータ漏洩
- 下請業者の利用
- インシデント対応／復旧計画
- 保険契約

b. サプライヤーがアクセスできる、あるいは特権的な役割を持つネットワークやシステムについて詳しく把握する必要がある。これにより、自らの組織が置かれているデジタル環境の状況認識が向上し、インシデントの封じ込めと復旧を迅速に行うことができる。

ステップ3：
サプライチェーン・セキュリティの戦略と実施計画を策定する（*「何を？」*）

a. 契約の一環としてサプライヤーが提供する製品やサービスだけでなく、自社の資産や情報について、サプライヤーに求めるべき保護レベルを明確にしておくことが極めて重要である。

(I) サプライヤーが関与する業務活動のリスクレベルに応じて、必要なサイバーセキュリティ管理を踏まえ、サプライヤーを選定する。

a. 調達オプションに関する貴組織の評価に基づき、サプライヤーが実施することになる業務活動に伴うリスクに見合った、必要なサイバーセキュリティ管理体制を有するサプライヤーを選択する。

b. サプライチェーン・セキュリティにリスクベースの手法を採用することを検討できる。具体的には、リスクの高い活動に関与するサプライチェーン・パートナーにはより厳格な管理を求める一方、リスクの低い活動に関与するパートナーには、比較的緩やかなサイバー衛生レベルで活動を進められる場合もある。

c. ランサムウェア攻撃によく見られる攻撃ベクトルを分析した結果、組織のシステム全体に以下の5つの管理策を一貫して導入すると、サイバー攻撃成功のリスクを大幅に低減できることが分かっている。すなわち、

- ネットワークの細分化と保護（ファイアウォールなど）
- 安全な構成設定（使用されていないソフトウェアの削除など）
- セキュリティ更新管理
  （例：すべてのソフトウェアとシステムに定期的にパッチを当て、更新する）
- ユーザーアクセス制御（多要素認証 [MFA] など）
- マルウェア対策（アンチウイルス、エンドポイント検出・対応ツールなど）

d.
これらは基本的なサイバー衛生を達成するうえで最低限必要なものと考えられており、学術研究、保険データ、さまざまな事例によって裏付けられている。　さらに、重要なデータをバックアップし、本番環境とは別にそれを保管すると、組織が影響を受けた場合の復旧に役立つ。

e.　例えば、（直接的に同等ではないが）英国の Cyber Essentials スキーム、シンガポールの Cyber Essentials スキーム、CyberFundamentals フレームワーク、ドイツのトップ 10 ランサムウェア対策は、サプライヤーが基本的な技術的管理を実施済みであることを顧客に対して担保する手段となり得る。

f.　よりリスクの高い業務活動に携わるサプライヤーのサイバーセキュリティ態勢は、サイバー衛生を超越して、リスクに見合うより高度な基準を採用するべきである。リスクに基づく手法を採用している国家基準の例としては、シンガポールのサイバートラストがあり、5 段階のレベルに分けられている。加えて、ISO/IEC 27001 のような国際標準やプロセスもある。

(II) セキュリティに関する期待事項をサプライヤーに伝える：

a.　ランサムウェアの予防と復旧に関する貴組織の最低基準を明確に説明する。

(III) 契約締結プロセスにセキュリティを組み込む

a.　次の事柄を考慮できる：

- 商品やサービスの提供を支えるすべてのシステムが、一般的なランサムウェア脆弱性に対する回復力を備えているという保証。その証拠となり得るものは、関連する証明書、事業復旧計画、及びそのような計画が一定間隔で実施されていることの検証である。
- 監査権条項
- ランサムウェア・インシデントの通知義務
- コンプライアンス違反に対する罰則

(IV)適切な措置が既に講じられているという保証をサプライヤーから得ること。

a.　これを達成する手段としては、独立した監査、テスト、または（国のサイバー技術当局が提供する認定を含む）外部認定が考えられる。

(V) サイバー保険

a.　サイバー保険は重要なリスク管理手法となり得る。CRI メンバー国・機関は、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レジリエンス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。

b. 組織は、サプライチェーンにサイバー保険への加入を奨励できる。また、サプライヤーがアクセスできるデータに関するサプライヤーの保険適用範囲を理解しておく必要がある。しかし、サイバー保険に加入したからといって、組織がランサムウェア攻撃から身を守るためのサイバー衛生対策を実施する必要性に取って代わるわけではない。

ステップ4：取り組みの見直しと改良

a. ランサムウェアの手口は急速に進化しており、サプライチェーンのセキュリティもそれに対応し続ける必要がある。組織とそのサプライヤーは共同で、以下を行うことができる：

- インシデントやニアミスを検証し、教訓を得る
- 対応計画を定期的に演習する
- 脅威インテリジェンスとベストプラクティスを共有する
- 契約やポリシーを更新して、新たな脅威を反映させる

b. また、（同業種などの）類似する組織とともにサプライヤー・サイバーセキュリティのフォーラムやワーキンググループを設立し、対話と協調を推進することもできる。

結論

9. **いかなる組織もサプライチェーンのリスクから完全に逃れることはできないが、事前の対策を講じることで、ランサムウェア・インシデントの可能性とその影響を大幅に低減できる。**組織とそのサプライチェーンは、「理解する」、「特定する」、「策定する」、「見直す」という 4 つのステップを踏むことで、組織自体の業務運営の中だけでなく、より広いエコシステム全体でレジリエンスを構築することができる。