

令和7年度春期応用情報技術者試験：サイバー攻撃インシデント復習・分析レポート

1. はじめに：サプライチェーン攻撃の戦略的脅威

本レポートは、令和7年度春期応用情報技術者試験の出題事例に基づき、企業のサイバーセキュリティにおける「サプライチェーン攻撃」の脅威を構造的に分析したものです。現代のビジネス環境において、企業は独立した存在ではなく、パートナー企業との密接なネットワーク接続（広域イーサネット等）の上に成り立っています。今回のケースでは、中古車販売会社であるC社と、業務提携先であるP社の関係が攻撃の起点となりました。特筆すべきは、P社がC社の販売管理システムを共同利用しており、P社従業員がPC-Rを通じて直接C社のDBサーバーへデータを登録する「常時接続のブリッジ」が存在した点です。一社のセキュリティ脆弱性が、この構造的な信頼関係を逆手に取られ、結果としてC社の基幹システムの停止とデータ暗号化を招きました。サプライチェーン上の「最も弱い環」が、提携する全企業のレジリエンス（回復力）を左右するという戦略的リスクを深く認識する必要があります。

2. ネットワーク構成とインシデントの発生状況

防御側として、まずシステムの全体像と攻撃の影響範囲を整理します。

ネットワーク構成の可視化

SOURCE_IMAGE_1および本文に基づき、C社の構成を整理します。特に、自社店舗用のPC-Cと、P社からの接続を受け入れるPC-Rの役割の違いに注目してください。

セグメント	主な役割	主要サーバ・PC
DMZセグメント	外部公開サービスの提供	Webサーバ
業務セグメント	業務遂行・提携先接続・管理	APサーバ、DBサーバ、PC-C（C社販売店用）、PC-S（システム管理用）、PC-R（P社接続受入用）
バックアップセグメント	データの保護	NAS（バックアップ用ストレージ）

P社からは、自宅PCや社内PC-PからSSL-VPNおよび広域イーサネットを経由し、C社のPC-Rへリモートデスクトップ（RDP）接続を行う運用となっていました。

事象のタイムライン

- **月曜日 午前9時頃：** C社販売店よりシステム利用不能の報告。C社各サーバのデータ暗号化が発覚。
- **初動対応：** 外部調査機関（U社）へ調査依頼。
- **証拠保全：** U社の要請により、インターネットおよび広域イーサネットを遮断。これは、攻撃の拡大防止に加え、**揮発性データの破壊を防ぐ「証拠保全」**を目的としたデジタルフォレンジックの重要な初動です。

3. 攻撃ベクターの多角的分析：侵入から発病まで

本事例では、技術的脆弱性と運用の隙を突いた複数の攻撃フェーズが確認されています。

攻撃ステップの解体

1. **初期侵入：** P社のVPNルータに存在する脆弱性を悪用し、認証情報を取得。その後、管理用PC-Pに対し「administrator」IDで約1万回のログイン試行（総当たりの推測）を行い失敗。その後「admin」IDに切り替え、辞書にあるパスワードで試行を重ね、151回目でログインに成功（**辞書攻撃**の成立）。
2. **横移動（ラテラルムーブ）：** 攻撃者は、PC-PとPC-Rで「同一のID・パスワード」が流用されていることを悪用。広域イーサネットを経由し、FW2/FW3で許可されていた**TCP/3389（RDP）**を利用してPC-Rへ侵入。さらにPC-Sに対し、一つのパスワードを複数のIDに試す「リバースブルートフォース攻撃」を展開しました。
3. **権限昇格：** PC-S上のAPソフトウェアにあるメモリ脆弱性を悪用。管理者がログインした際に残る「特権ID」の情報をメモリ上から奪取し、サーバ全体の支配権を確立しました。
4. **目的遂行：** 奪取した特権IDを用い、まず **マルウェア対策ソフトウェアのプロセスを強制終了**。その後、ランサムウェアを実行してデータを暗号化しました。特権奪取からサービス停止へと至る、極めて合理的な攻撃シーケンスです。

デジタルフォレンジックの定義

この一連の手口を解明したのが **デジタルフォレンジック** です。これは、不正アクセス等が発生した際に、電磁的記録の証拠保全、調査、分析を行う手続きを指します。本事例では、上書きされる前のログやメモリ上の残存情報を分析することで、侵入経路の特定に成功しました。

4. セキュリティ上の課題と技術的・運用的評価

インシデントの根本原因は、単一のミスではなく多層防御の欠如にあります。

課題の構造化

- **ログ管理の不備：** ログが最大値に達すると古いものから上書きされる設定（下線④）であったため、大量の攻撃試行が行われた際に、初期侵入時の重要な証拠ログが消失するリスクがありました。
- **バックアップの脆さ：** NASには最大7日分（1世代分）のデータしかなく、月曜日に暗号化されたデータが「正常な差分」として上書き（下線③）されれば、復旧が不可能になる極めて深刻な状況でした。

認証設定とリバースブルートフォースの脅威

PC-Pで辞書攻撃を防げなかったのは、PC-Rでは有効だった「失敗5回でのロックアウト」設定が適切になされていなかったためです。しかし、より教育的なポイントは「リバースブルートフォース攻撃」への脆弱性です。****「同一のIDに対して2回以上ログイン試行しない（一つのパスワードで異なるIDを順に狙う）」****という攻撃手法に対し、ID単位のロックア

ウトしきい値設定は無力です。これが、C社の設定でも攻撃を防げなかった論理的理由です。

5. 再発防止策とレジリエンスの強化

教訓を活かし、将来の耐性を高めるための対策が講じられました。

具体的対策の要約

- **技術的対策：** VPNルータ・APソフトへのパッチ適用。特権ID使用時のみ管理者が許可し、その都度「ワンタイムパスワード」を発行する運用の導入。
- **運用的対策：** P社からのRDP接続を「事前申請・許可制」とし、常時開放の橋を廃止。P社への機器管理ルール策定の要請。
- **ログ管理の強化：** ログサーバを新設し、各機器からログを集約。上書きを防止し、長期保存と集中管理を実現。

最新ストレージ技術の適用

バックアップの安全性を担保するため、**イミュータブルバックアップ** の導入が決定されました。これは「変更不可」な状態でデータを保存する技術で、ランサムウェアによるデータの改ざんや削除を物理的に防ぎます。これを **3世代分保存** する運用により、不測の事態でも確実にクリーンなデータから復元できるレジリエンスを確保しました。

6. まとめ：応用情報技術者試験に向けた重要知識の整理

本事例は、技術的な脆弱性管理と、パスワード・ログ運用といった管理面の両輪がいかに重要であるかを問う良問です。

設問解答キーポイント表

本問題の核となる解答要素を整理します。

設問番号	解答	重要な技術キーワード・概念
設問1	デジタルフォレンジックス	証拠保全・調査・分析の一連の手続き
設問2	aオ（辞書） bウ（RDP）	攻撃手法の識別とプロトコル(TCP/3389)
設問3	ロックアウトのしきい値	同一パスワードで異なるIDを狙う攻撃への理解
設問4(1)	暗号化されたデータで上書きされている	バックアップの世代管理と整合性リスク
設問4(2)	古い記録のログが上書きされるから	ログ保存期間と容量設計の重要性
設問5	ア（イミュータブル）	変更不可ストレージによるデータ保護

学習アドバイス

応用情報技術者試験では、「なぜその対策で不十分なのか（例：ロックアウト設定がリバースブルートフォースに効かない理由）」という論理的帰結が問われます。単なる用語暗記に

留まらず、攻撃者の視点で防御の「穴」を探し、技術（パッチ、OTP、イミュータブル）と運用（ログ管理、承認制）の双方からその穴を埋める思考を養ってください。