サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2022 年 7 月～9 月]

2022 年 11 月 7 日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

サイバー情報共有イニシアティブ（J-CSIP）[1]について、2022 年 9 月末時点の運用体制、2022 年 7 月～9 月の運用状況を報告する。1 章、2 章は全体状況を、3 章以降は本四半期で把握、分析した特徴的な攻撃事例を解説する。

目次

[1] IPA が情報ハブ（集約点）となり、サイバー攻撃等に関する情報を参加組織間で共有する取り組み。
https://www.ipa.go.jp/security/J-CSIP/

1　運用体制

2022 年 7 月～9 月期（以下、本四半期）は、参加組織の増減はなく、全体で 13 業界 279 組織[2]＋2 情報連携体制（医療業界 4 団体およびその会員約 5,500 組織、水道関連事業者等 9 組織）の体制となっている（図 1）。

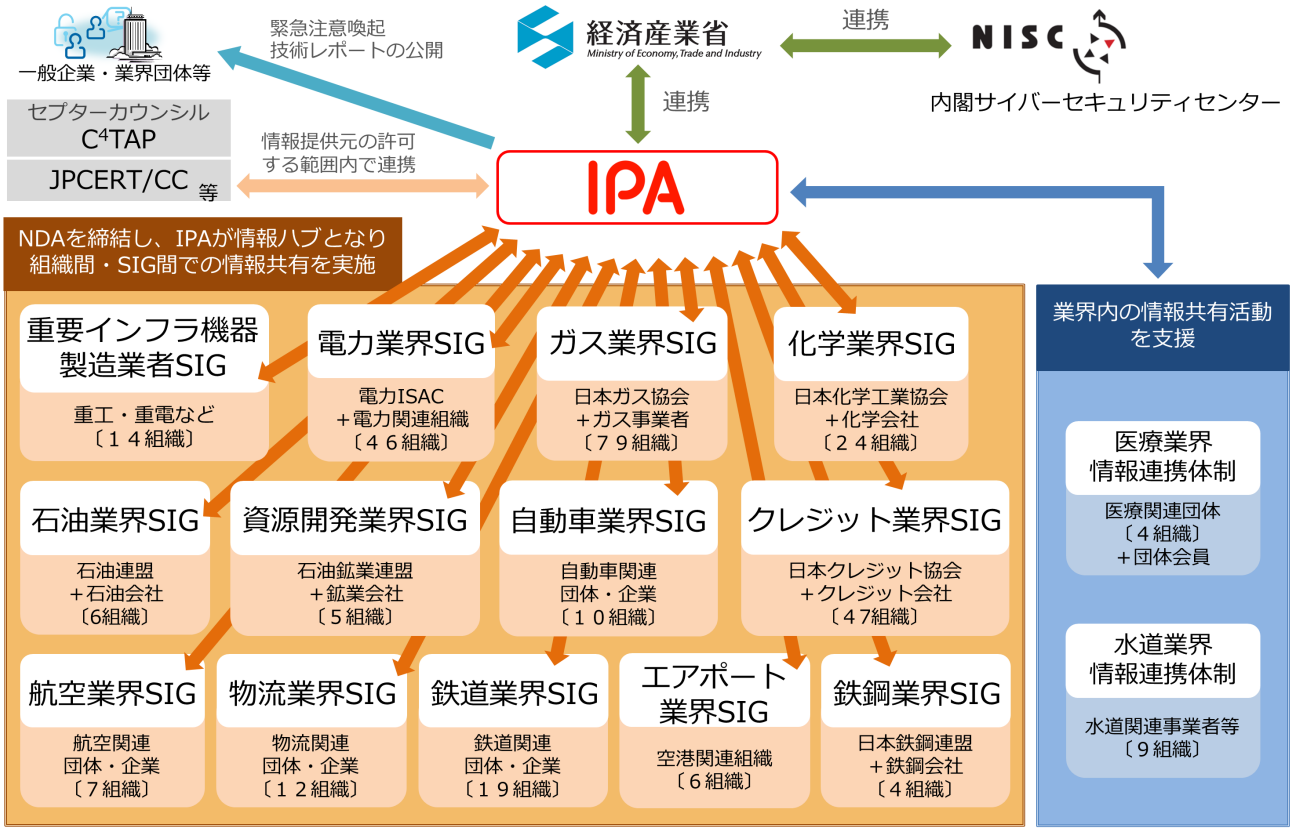

図 1 J-CSIP の体制図

[2] 複数業界に関係する組織が、複数の SIG に所属するケースも現れている。ここでは延べ数としている。

2　実施件数（2022 年 7 月～9 月）

2022 年 7 月～9 月に、J-CSIP 参加組織から IPA に対し、サイバー攻撃に関する情報（不審メール、不正通信、インシデント等）の情報提供が行われた件数と、それらの情報をもとに IPA から J-CSIP 参加組織へ情報共有を実施した件数（9 月末時点、13 の SIG、全 279 参加組織と、2 つの情報連携体制での合算）を、表 1 に示す。

表 1 情報提供および情報共有の状況

項番	項目	2021 年	2022 年		
		10 月～12 月	1 月～3 月	4 月～6 月	**7 月～9 月**
1	IPA への情報提供件数	77 件	51 件	134 件	**22 件**
2	参加組織への情報共有実施件数※1	28 件	29 件	35 件	**38 件※2**

※1 同等の攻撃情報（不審メール等）が複数情報提供された際に情報共有を 1 件に集約して配付することや、広く無差別にばらまかれたウイルスメール等、情報共有対象としない場合があるため、情報提供件数と情報共有実施件数には差が生じる。

※2 IPA が独自に入手した情報で、J-CSIP 参加組織へ情報共有を行ったもの **32 件**を含む。

本四半期は情報提供件数が **22 件**であり、うち標的型攻撃に関する情報（攻撃メールや検体等）とみなしたものは **2 件**であった。

そのうち、次にあげるような情報提供があり、情報共有を行った。

- 標的型攻撃の被害に関する情報提供があった。本件は、まず情報提供元のグループ企業が侵害され、その後同一ネットワーク内にあった情報提供元組織のシステムまで侵害範囲を拡大された。事案発覚の経緯や攻撃手口について 3 章で述べる。

- J-CSIP 参加組織の海外子会社にて、不正アクセスによる情報漏えいの被害を受けたという情報提供があった。本件は、VoIP ゲートウェイ装置から組織内ネットワークに侵入され、最終的に情報の窃取等が行われた。事案発覚の経緯や攻撃手口について 4 章で述べる。

このほか、情報提供に加え、次のような相談・報告事例があった（表 2）。

表 2 相談・報告事例

項番	相談・報告内容	件数
1	自組織のメールサービスを騙るフィッシングメールが複数着信し、フィッシングサイトでメールアドレスとパスワードを入力してしまった。	1 件
2	返信を装った、ウイルスへの感染を企図した攻撃メールを受信した。	1 件
3	組織内から外部のサイトへのアクセスをセキュリティ機器で検知した。	3 件

項番 1 は、自組織のメールサービスを騙る不審メールが複数着信し、職員が本文に記載されている URL リンクへアクセスし、メールアドレスとパスワードを入力してしまった、との情報提供を受けたものである。IPA で調査をしたところ、URL リンク先はウェブメールのログイン画面を模したフィッシングサイトであった。フィッシングサイトでメールアドレスやパスワードを入力してしまった場合、早急にメールアカウントのパスワードを変更するとともに、当該利用者のアカウントに不正アクセスされていないか、組織内で同様の事象が他に発生していないかを確認していただきたい。また、不審なメールの URL リンクを容易にクリックしないこと、正規のものか判断がつかないサイトでのメールアドレスやパスワード等の入力をしないことも周知徹底していただきたい。

項番 2 は、組織内に着信した不審メールについての情報提供を受けたものである。IPA で調査したところ、Qbot（別名：Qakbot）と呼ばれるウイルスへの感染を企図した攻撃メールであった。この攻撃メールは、正規のメールアカウントを悪用し、過去にやり取りをしたとみられるメールの引用とともに、返信を装う形で送信されていた。なお、メールの送信元アドレスと引用文に記載されているメールアドレスは別の組織のものであり、攻撃者は複数の組織からメールアカウントやメールの内容を窃取しているものと推測している。また、本件と同等の手口のメールを複数確認していることから、ある程度ばらまかれているメールと思われる。ばらまき型メールは、システムによる対策のほか、メール利用者ひとりひとりが不審なメールに注意し、関係者からの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かないといった対策を徹底し、多層的な防御を行っていくことが重要である。

項番 3 は、組織内のパソコンから外部サイトへのアクセスをセキュリティ機器で検知したというものである。IPA で調査をしたところ、いずれも検知されたサイトに不審な動作等はみられなかった。本件は特に問題がなかったものの、通常業務の中で意図せず不審なサイトを閲覧してしまうことは当然発生し得るリスクである。不審なサイトの閲覧による被害に遭わないよう、OS やブラウザ等のソフトウェアは最新の状態を保つことに加え、不審サイト・詐欺サイト・偽警告 [3]等に騙されないよう、従業員への教育を継続的に実施すべきであろう。

[3] 被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20170411.html

3　国内組織を狙う標的型攻撃の被害事例

本四半期、J-CSIP 参加組織より、標的型攻撃と思われる被害に関する情報提供があった。数ヵ月の調査により、被害の内容や攻撃の流れの全体像は判明したが、細かい点では不明な点が残った事例であった。

当該組織（情報提供元）によると、本件は標的型攻撃を行うグループによるものと推定しており、攻撃者は当該組織のグループ企業のサーバを侵害し、同一ネットワーク内にあった当該組織のシステムも続いて侵害したとのことであった。

本章では、可能な範囲で攻撃の発見経緯と攻撃手口について説明する。

本件の説明にあたり、図 2 にシステム構成の概略を示す。

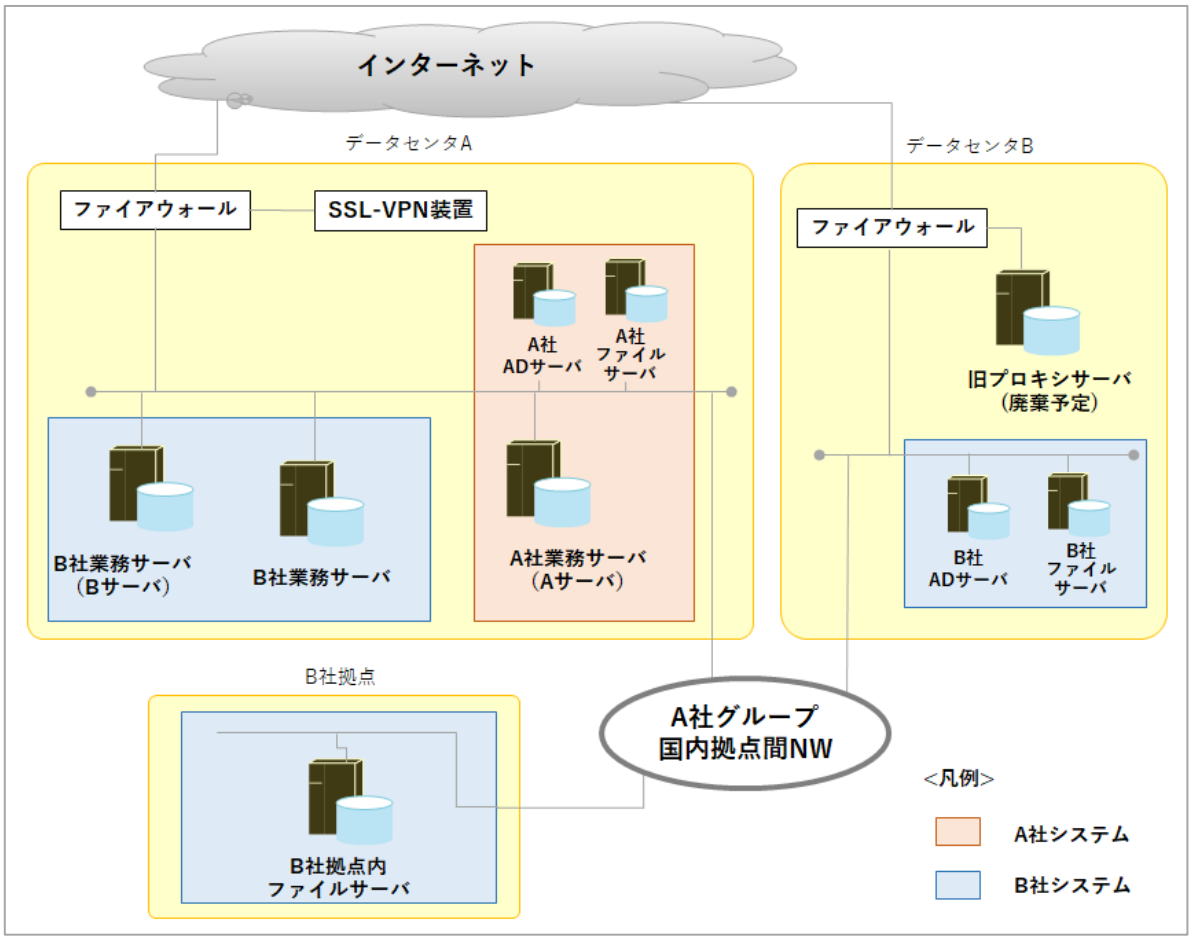

図 2 システム構成概略

説明のため、当該組織（情報提供元）を A 社、最初に侵害されたグループ企業を B 社とする。A 社グループでは、インターネットの接続口や拠点間ネットワーク、データセンタ、一部のシステムをグループ企業である B 社と共有している。なお、ActiveDirectory（AD）については、A 社と B 社で個別の管理をしている。

3.1 攻撃発見の経緯

本件は、A 社の業務サーバの一台（A サーバ）で、ディスク使用率の閾値超過のアラートが発生したことを契機として発覚した。A 社にてアラートの原因を調査したところ、不審なファイルが A サーバ上に存在しており、また特定の社員に紐づいた管理者 ID からの不審なアクセス履歴が見つかった。さらに調査を進めたところ、A サーバは同一ネットワーク内にあった B 社の業務サーバの一台（B サーバ）から不正に侵入されていたことが判明した。

3.2 攻撃手口

攻撃の流れと、攻撃で使用されたウイルスについて説明する。

図 3 は、初期侵入から侵害範囲の拡大を経て、攻撃が発覚するまでの全体の流れを示したものである。

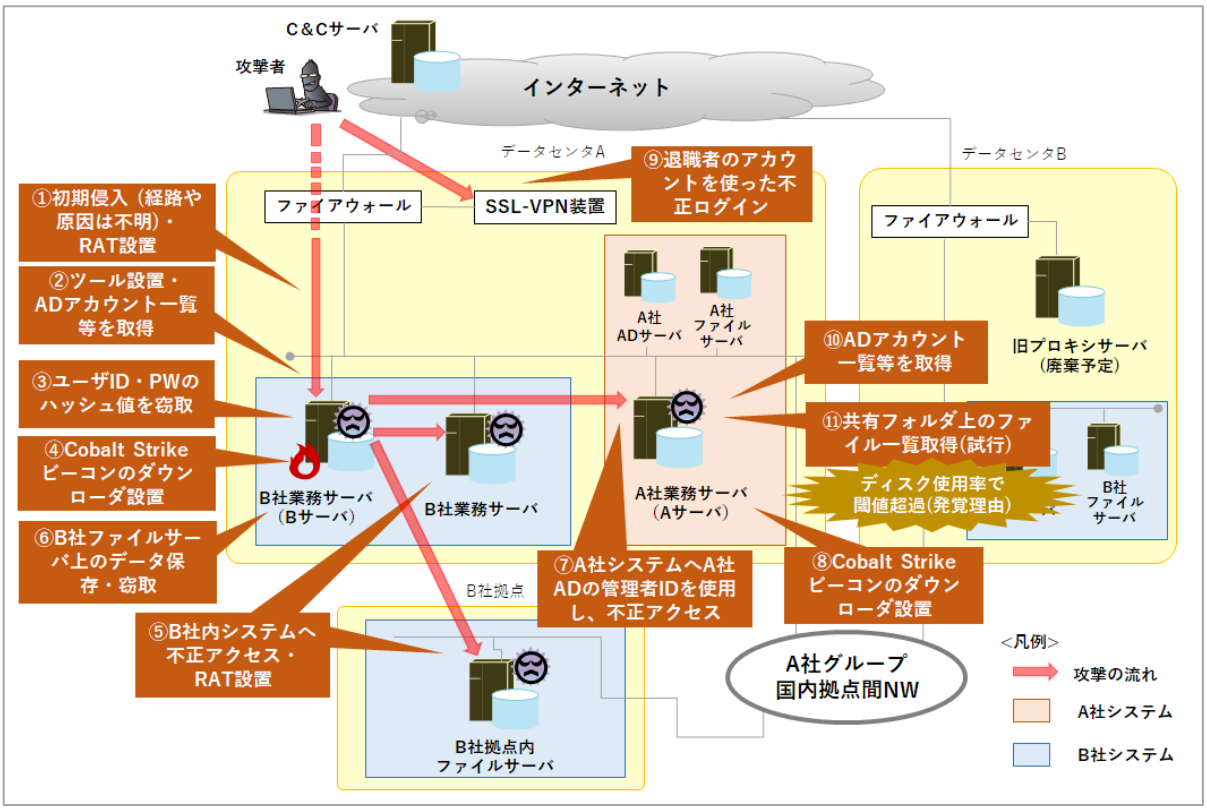

図 3 攻撃の流れ

3.2.1 初期侵入

本件では、始めに B サーバに侵入されたとみられるが、その侵入経路や原因については不明である。外部専門機関の調査によると、B サーバ上で確認された最も古い攻撃の痕跡として、事案発覚時点から 1 年半以上も前のものが確認された。攻撃者は B サーバに侵入後、ネットワーク内にあるシステムを探索したのち、当該サーバ内に遠隔操作プログラム（RAT）（3.2.3 にて後述）を設置したとのことである（図 3-①）。これにより、攻撃者はいつでも B サーバへアクセス可能な状態となっていたものと考えられる。

続いて、攻撃者はおよそ 1 年後、AD に含まれる情報の取得やファイル圧縮を行うツールを B サーバへ設置・実行し、B 社 AD ドメイン内のアカウント情報一覧やサーバ情報を取得した。これは、侵害範囲の拡大に向けた準備段階であったと考えられる（図 3-②）。

3.2.2 侵害範囲の拡大

攻撃者は準備段階を経て、更にその約半年後に、組織内ネットワークの侵害範囲の拡大を図っている。調査で判明した範囲で、攻撃者の行動を説明する。

ここで説明する図 3-③から図 3-⑪までの行動は、およそ 2 週間の間に行われた。

B 社システムでの侵害

- B サーバ上で、WindowsOS の正規プログラムを悪用し、LSASS というプロセスのダンプを行い、メモリ空間上に保存されていたユーザ ID やパスワードのハッシュ値を取得した（図 3-③）。
- B サーバに対し、商用のペネトレーションツールである「Cobalt Strike」のエージェントプログラム（ビーコン）のダウンローダ（3.2.3 にて後述）を設置した（図 3-④）。外部専門機関による調査によれば、当該ダウンローダが実行され、「Cobalt Strike」のエージェントプログラムを使って、ネットワーク調査・アカウント情報窃取・権限昇格・侵害範囲の拡大・情報窃取等が行われた可能性が高いとのことであった。
- B 社内の他の業務サーバや、別拠点に設置されたファイルサーバに不正アクセスし、遠隔操作プログラム（RAT）を設置した（図 3-⑤）。
- B 社ファイルサーバ上のデータを、パスワード付きの圧縮ファイルとして B サーバ上に保存した。その後、当該ファイルの外部送信（窃取）がされたと思われる状況であった（図 3-⑥）。

A 社システムへの侵害

- B サーバから A サーバに対して、A 社 AD の管理者 ID を使用し、不正にアクセスを行った（図 3-⑦）。当該管理者 ID のパスワードが平易なものであったため、攻撃者に推測されたものと A 社では判断している。
- A サーバに「Cobalt Strike」のエージェントプログラムのダウンローダを設置した（図 3-⑧）。ただし、外部専門機関の調査の結果、ダウンローダの実行や「Cobalt Strike」のエージェントプログラムの稼働は確認されておらず、何らかの理由で失敗したか、攻撃を中断した可能性が考えられる。

SSL-VPN からの再侵入

- 退職済みの協力会社社員の SSL-VPN 用アカウントを使って、外部から A 社および B 社のネットワークに接続した（図 3-⑨）。その後、ネットワーク内の共有フォルダや、リモートデスクトップ接続が可能な端末を探索した。

A サーバでの情報窃取の試行と発覚

- A サーバ上で、A 社 AD 上のアカウント情報の一覧や、サーバ情報を取得した（図 3-⑩）。
- A サーバから A 社ファイルサーバの共有フォルダにアクセスし、攻撃者の用意したバッチファイルを実行してファイル名一覧の取得を試行した（図 3-⑪）。このとき、ファイル名一覧を保存する際にディスク使用率の閾値超過が起こり、アラートが発生した。これに気づいた A 社が対応を開始したため、ファイル名一覧のデータ窃取は行われなかった。
  これを契機に、本件一連の攻撃が発覚した。

3.2.3　攻撃で使われたウイルス

A 社および B 社のサーバに存在していた 2 種類のウイルスを外部専門機関が解析したところ、攻撃者が指定したサーバからファイルのダウンロードを行うもの（ダウンローダ）と、攻撃者からの命令を受け取り、実行するもの（遠隔操作プログラム、RAT）があり、その通信先のサーバ（C&C サーバ）は標的型攻撃を行うグループの関与が疑われるものとのことであった（図 4-①）。

また、当該 2 種類のウイルスには、A 社グループで使っていた古いプロキシサーバの情報（IP アドレスとポート番号）がハードコードされており、A 社および B 社の環境と C&C サーバ間の通信時は当該プロキシサーバを経由していた（図 4-②）。攻撃者は侵入後にネットワーク内の環境を調査し、その環境に合わせてウイルスをカスタマイズしていたということである。

当該プロキシサーバは、システム移行により廃棄予定であり、事案発生当時、利用は停止していたが、稼働したままの状態であった（図 4-③）。

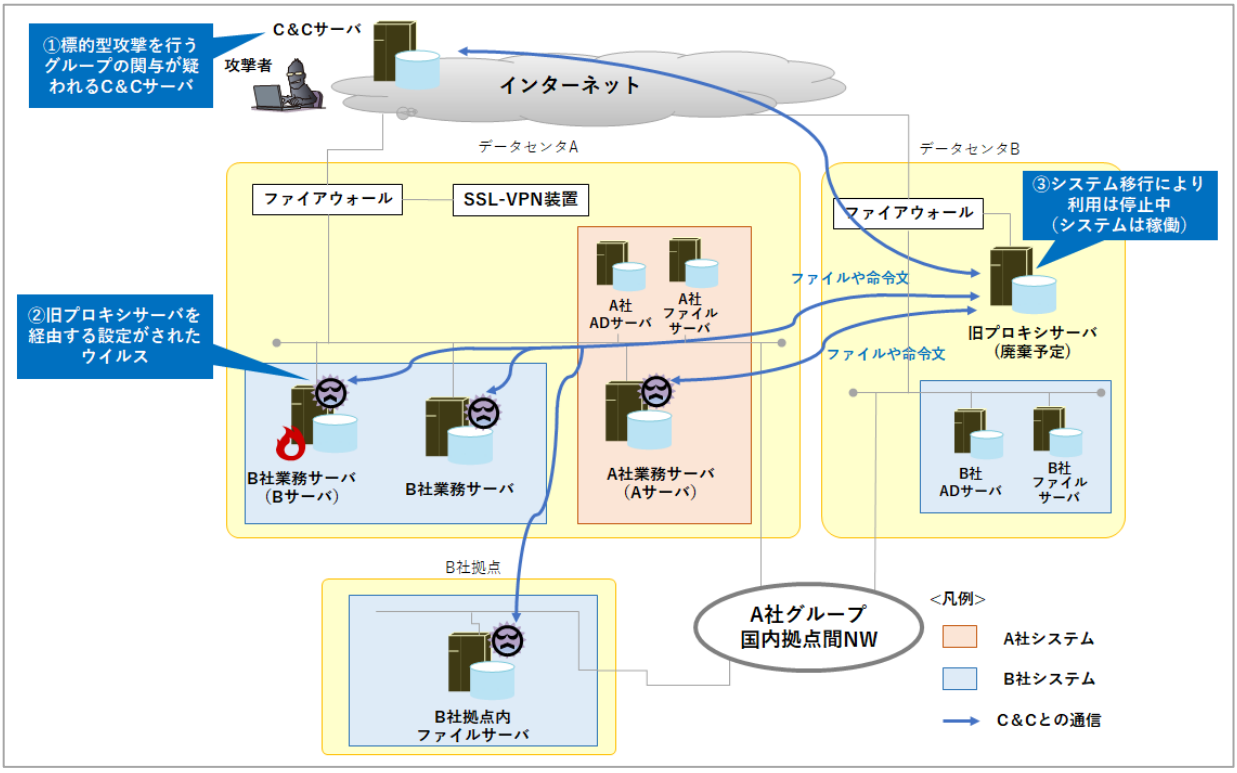

図 4 攻撃で使われたウイルス

3.3 まとめ

標的型攻撃は高度かつ巧妙と言われる一方、攻撃の中で使われる一つひとつの手口は、対策ができないような未知の攻撃手法であることは少ない。本件についても、パスワード管理やシステム管理、アクセス制御など、基本的なセキュリティ対策が徹底できていれば防げた可能性のある箇所が見受けられた。

標的型攻撃への対策の一つは、まず基本的なセキュリティ対策の徹底である。もちろん、組織内システムの全ての機器を漏れなく対策するというのは、実際には非常に困難である。しかしながら、管理者の想像を超えて、攻撃者が脆弱な点を探し出すということが、この事例でも顕著であった。標的型攻撃に限らず、あらゆる脅威に対して有効であるので、地道なセキュリティ対策の徹底を進めていただきたい。

また、本件では、攻撃者は事案発覚の 1 年半以上前に初期侵入に成功してから、理由は不明であるが、長期間潜伏していた。潜伏中に何があったのかも不明である。痕跡が示しているのは、侵害範囲を拡大する準備ののち、システムの脆弱な箇所を探索しながら、突然攻撃が進められたということであった。事案が発覚し、当該組織や外部専門機関による調査が行われたが、攻撃が長期に及びログ保存期間を超えていたこと、そもそも攻撃者の行動を示すログが不十分であったことなどから、結果、究明に至らない点もあった。

本事例に限らず、一般的な標的型攻撃の検知・調査の観点では、同じような状況が見られる。すなわち、検知できない、十分な記録が残らない、記録が消えている、といった原因により、攻撃者による長期的な侵入を許したり、インシデント対応での調査が難航するという問題が生じている。これらについては、基本的なセキュリティ対策から一歩進み、標的型のような攻撃を想定した対策、例えば、各種ログの確実かつ長期の保存や、EDR のような検知・記録ツールの活用等が必要だということであろう。

十分な対策のためには、十分なリソース（人員、機材、費用等）を要する。組織内ネットワークに攻撃者が侵入した場合の被害や対応工数は、経営の観点からも甚大になりうることを想定し、企業・組織の経営層の理解のもとで、着実に進めていく必要がある。

4　海外子会社への不正アクセスによる情報漏えいの被害事例

J-CSIP 参加組織より、不正アクセスによる情報漏えい被害を受けたとの情報提供があった。本件は、情報提供元組織の海外子会社にて、ランサムウェア攻撃グループとみられる攻撃者によって、廃棄予定であった VoIP ゲートウェイ装置から組織内ネットワークに侵入され、侵害範囲の拡大、ウイルスや不正なファイルの設置、情報の窃取、一部の工業機器制御用 PC のデータの改ざん、不審メールの送付等が行われたというものである。これらの攻撃により、当該組織（海外子会社）では、一時的に操業を停止した。なお、その後の調査により、データを暗号化されるという被害はなかったことが確認されている。

本章では、本件が発覚した経緯や攻撃手口について説明する。

4.1 攻撃発見の経緯

本件が発覚した契機は、次の 2 点である。

- 当該組織で導入していたセキュリティソフトが、攻撃者の侵害範囲拡大行為を検知した。
- 従業員へ送られた不審メールについて、従業員から通報があった。

4.2 攻撃手口

本件の攻撃の流れを、図 5 に示す。

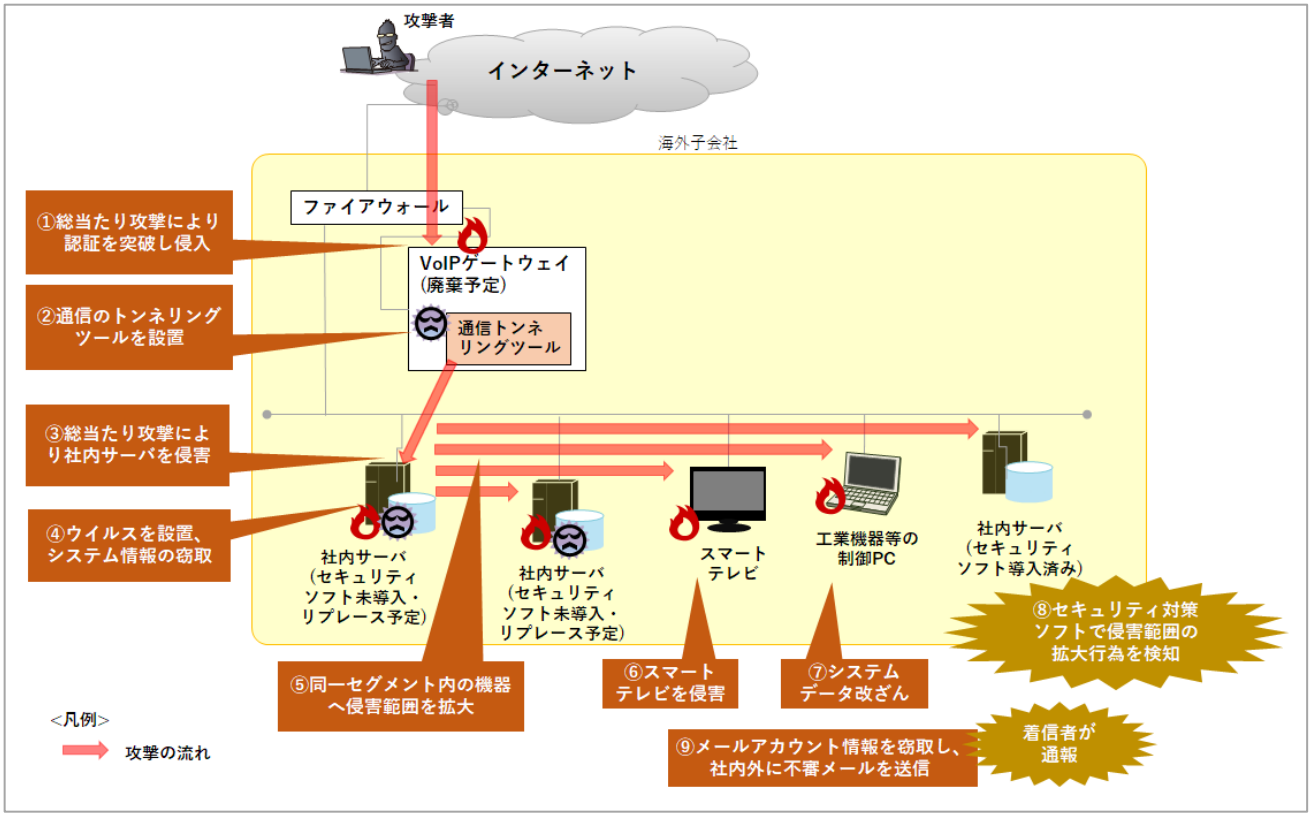

図 5 攻撃の流れ

4.2.1 初期侵入

本件では、組織内ネットワークとインターネットの境界に設置されていた VoIP ゲートウェイ装置を経由して、攻撃者が組織内ネットワークへ侵入した（図 5-①）。このとき、当該装置が次のような状態であったため、攻撃者による総当たり攻撃から認証を突破され、侵入されてしまったとのことである。なお、当該 VoIP ゲー

トウェイ装置は、攻撃を受けた 2 週間後には廃棄予定であった。

- 外部から VoIP ゲートウェイ装置へ SSH 接続が可能であった。
- 大量のログイン試行に対する対策がされていなかった。
- 管理者 ID と認証パスワードが装置にハードコードされており、変更できなかった。

攻撃者は VoIP ゲートウェイ装置に不正ログイン後、当該装置に「chisel」[4] と呼ばれる通信のトンネリングツールを設置した。これを悪用し社内ネットワークに侵入したとみられる（図 5-②）。

4.2.2 侵害範囲の拡大

攻撃者は、初期侵入の後、同一セグメント内にあった組織内のサーバやスマートテレビ、工業機器を制御する PC 等へ順次侵害範囲を拡大した。この時の攻撃者の行動を、次に示す。

(1) Windows 共有フォルダの探索等のネットワーク内の探索行為と、総当たり攻撃で認証を突破し、サーバを侵害した（図 5-③）。
この際、セキュリティソフトが導入されていないサーバが侵害されたため、不正アクセスを検知することができなかった。同サーバは、セキュリティソフトを導入できない OS バージョンであり、リプレース予定であった。

(2) 侵害したサーバに、正規ソフトウェア（音声管理ソフトやセキュリティソフト）のファイル名に偽造したウイルスを設置・実行し、システムの情報を窃取した（図 5-④）。

(3) リモートデスクトップ（RDP）による接続および PsExec コマンドの実行、「Impacket（SMBExec など）」[5]というツール群の悪用を行い、同一セグメント内の次の機器に対して、侵害範囲を拡大した（図 5-⑤）。
- セキュリティソフトが導入されていないサーバ
- デジタルサイネージ用途で使用していたスマートテレビ [6]（図 5-⑥）
スマートテレビは、その被害が事業に影響を及ぼすものではなく、情報提供元にて詳細な調査は不要と判断し、侵害を確認してすぐに処分したため、具体的な被害状況は不明である。
- 工業機器等を制御する PC（図 5-⑦）
工業機器等を制御する PC は、攻撃者によって侵害後にシステムデータが改ざんされ、動作不能となった。

(4) 上記と同じ手口にて、セキュリティソフトが導入されたサーバへ侵害範囲を拡大した際に、セキュリティソフトが検知し、本件が発覚した（図 5-⑧）。

---

[4] LAC 社「オープンソースのポート転送／トンネリングツールを悪用する標的型攻撃に注意」
https://www.lac.co.jp/lacwatch/people/20200212_002127.html

[5] トレンドマイクロ社「Python 製ペネトレーションテストツール「Impacket」、「Responder」の悪用手口を分析」
https://www.trendmicro.com/ja_jp/research/22/i/analyzing-penetration-testing-tools-that-threat-actors-use-to-br.html

[6] スマートテレビは、侵害を受けた社内サーバ等と同一セグメント内に設置（当該セグメントに割り当てられたアドレス帯で IP アドレスを付与）されており、攻撃者からはサーバや PC と同等の機器として見えていたものと推測される。

4.2.3 不審メールの送信

攻撃者は従業員のメールアカウント情報を窃取した上で、アカウントに不正ログインし、社内外へ複数の不審メールを送信した（図 5-⑨）。

当該組織では、認証に多要素認証を行う仕組みがあったが、利用は従業員の任意となっていた。この時、不正ログインされたアカウントは、多要素認証が設定されていないアカウントであった。

どのような不審メールが送信されたかについては、今回情報提供範囲外となっており、詳細は不明であるが、組織内外に対する、何らかの更なる攻撃が試みられたものと思われる。

4.3 まとめ

昨今の被害事例では、攻撃者の侵入経路に VPN 装置の脆弱性等を悪用するケースが多く報告されているところ、本件では VoIP ゲートウェイ装置が悪用された。VPN 装置に限らず、インターネットからアクセス可能な機器類は、攻撃者の侵入経路の起点として狙われることが多いため、十分な注意が必要である。

各組織おいては、第一に、自組織のネットワーク上にあるこれらの機器類をすべて把握してほしい。その上で、存在するすべての機器で、アクセス制御、堅牢な認証、脆弱性の解消などの基本的な管理を確実に行ってほしい。特に撤去予定の機器類は、把握漏れや十分な管理がされないことがあるので、注意が必要である。

また、業務都合や運用、利便性の兼ね合いから、セキュリティレベルを落とさざる得ない場合も考えられるが、その点も注意したい。本件で、セキュリティソフトの導入ができなかったサーバや、多要素認証を選択していなかった一部の従業員アカウントが攻撃者に悪用された点も、セキュリティの弱い部分を狙われた一例である。

このようにセキュリティレベルを落とした場合は、発生するリスクを想定し、それをカバーするようなセキュリティ施策を用意するなど、システム全体で組織が求めるセキュリティレベルを満たすことを考慮していただきたい。

関連情報のご提供のお願い

本書で紹介した事例について、J-CSIP では関連情報を求めています。
同様の事例を確認した場合など、下記窓口へ情報提供をいただけますと幸いです。

J-CSIP 事務局 ご連絡窓口 （IPA）
jcsip-info@ipa.go.jp

ウイルス・不正アクセス届出のお願い

IPA では、国内のコンピュータウイルスの感染被害や、コンピュータ不正アクセスによる被害の届出を受け付けています。被害等の実体把握や今後の防止に役立てるため、ぜひご協力をお願いします。

コンピュータウイルス・不正アクセスに関する届出 （IPA）
https://www.ipa.go.jp/security/outline/todokede-j.html

標的型サイバー攻撃特別相談窓口

IPA の「標的型サイバー攻撃特別相談窓口」では、標的型サイバー攻撃を受けた際の相談を受け付けています。お気づきの点があれば、ご相談ください。

標的型サイバー攻撃特別相談窓口 （IPA）
https://www.ipa.go.jp/security/tokubetsu/

以上