サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2022 年 10 月～12 月]

2023 年 2 月 9 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 12 月末時点の運用体制、2022 年 10 月～12 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 10 月～12 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）。

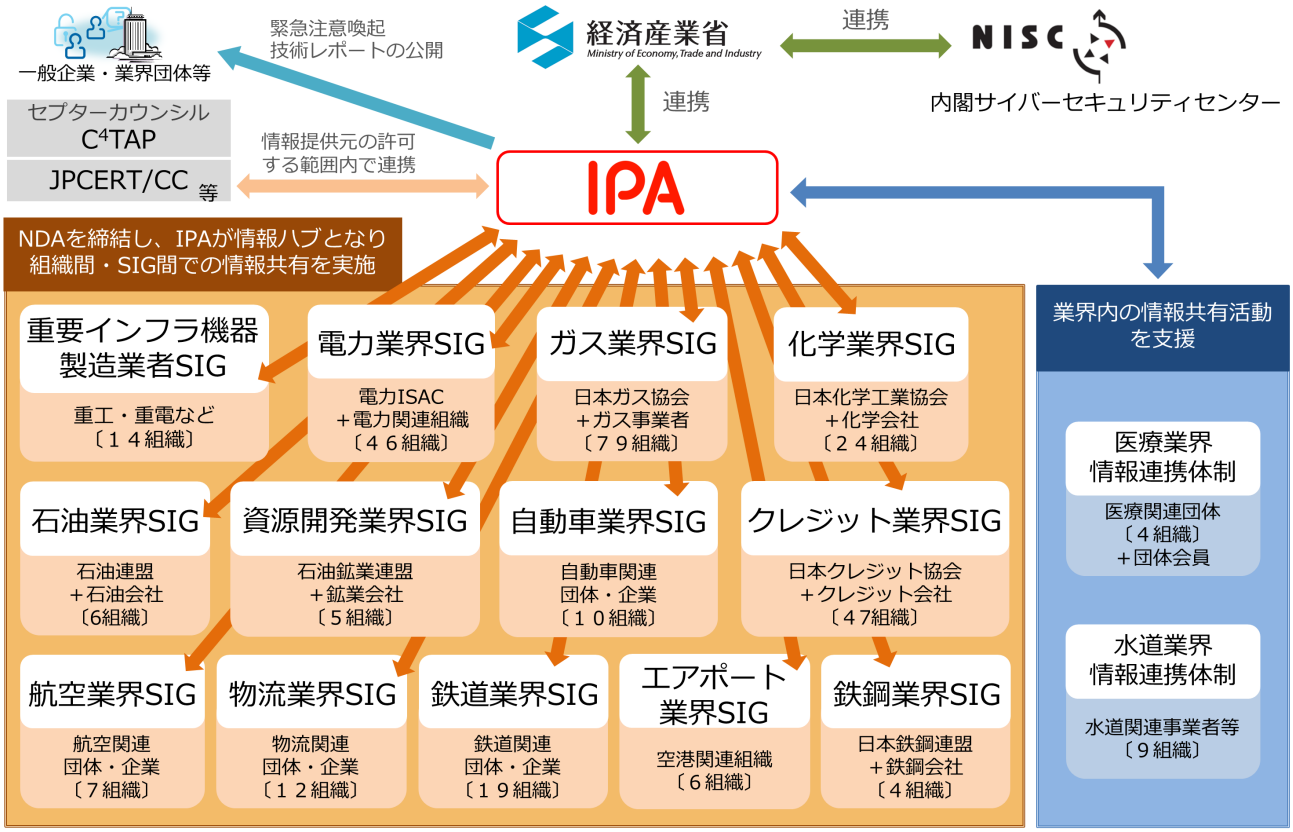


図 1 J-CSIP の体制図

[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　運用状況（2022 年 10 月～12 月）

2022 年 10 月～12 月の運用状況について、2.1 で情報提供・情報共有の実施件数を、2.2 と 2.3 で参加組織から提供された情報や IPA が独自で収集し共有した情報を報告する。

2.1 情報提供・情報共有の実施件数

2022 年 10 月～12 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（12 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	2022 年			
		1 月～3 月	4 月～6 月	7 月～9 月	**10 月～12 月**
1	IPA への情報提供件数	51 件	134 件	22 件	**26 件**
2	参加組織への情報共有実施件数※1	29 件	35 件	38 件	**25 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 **20 件**を含む。

本四半期は情報提供件数が **26 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 **6 件**であった。

2.2 参加組織から提供された情報

参加組織からは、次にあげるような情報が IPA へ提供されている。

- 参加組織に着信したビジネスメール詐欺について情報提供が 3 件あった。これら 3 件のビジネスメール詐欺は、いずれも経営者等になりすますもので、2 件が 2020 年 4 月に IPA が行ったビジネスメール詐欺に関する注意喚起 [3]に掲載した事例と類似したメール、残りの 1 件が「サイバー情報共有イニシアティブ（J-CSIP） 運用状況［2019 年 10 月～12 月］」[4]の 3.3 章「複数組織へ行われた CEO を詐称する一連の攻撃」に掲載した事例と類似したメールであった。
  本四半期でも過去に観測していたビジネスメール詐欺と同等の攻撃が続いており、引き続き注意が必要である。また、IPA では 2022 年 9 月末に「ビジネスメール詐欺（BEC）対策特設ページ」[5]を開設した。本ページには、ビジネスメール詐欺の手口や被害事例、対策などを掲載しているので、参考にしてほしい。

---

[3] 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（第三報） （IPA）
https://www.ipa.go.jp/security/announce/2020-bec.html

[4] サイバー情報共有イニシアティブ（J-CSIP） 運用状況 ［2019 年 10 月～12 月］ （IPA）
https://www.ipa.go.jp/files/000080133.pdf

[5] ビジネスメール詐欺（BEC）対策特設ページ （IPA）
https://www.ipa.go.jp/security/bec/index.html

- 人事部門からの通知を装った不審なメールが送られてきたという情報提供があった。IPA で確認したところ、フィッシングメールとみられた。当該メールには受信者にその組織の内部メールと思わせるため、組織のロゴを外部のウェブサイトから読み込み、本文中に表示するような仕掛けがあり、また、メール本文中に記載されたフィッシングサイトの URL は、メールのフィルタリング製品等による検知を避ける目的で細工がなされていた。
  これについて 3 章で述べる。

- グループ会社へのランサムウェア攻撃の被害に関する情報提供があった。本件は、攻撃者から不正アクセスを受け、組織内のネットワークへ侵入された後、Active Directory が侵害され、約 7 割のサーバと、約 2 割の業務用パソコンが暗号化の被害を受けた。
  これについて 4 章で述べる。

- 参加組織のグループ会社や同社の取り扱い製品のウェブサイトに対して、探索行為とみられる大量の不正通信や、大量の問い合わせフォームへの書き込みが発生したという情報提供があった。当該内容を整理し、J-CSIP 参加組織へ情報共有を行ったところ、別の参加組織においても同様の攻撃が見つかった。
  これについて 5 章で述べる。

- 参加組織の関係会社において、従業員が外部のサイトを閲覧した際に偽の警告（ポップアップ）が表示されたという情報提供があった。当該サイトを IPA で確認をしたところ、ブラウザの通知機能を悪用し、ウイルス対策ソフトウェアのライセンス切れを示す偽の警告を表示させ、さらに別の不審サイトへ誘導するというものであった。
  外部サイトを閲覧する際には、安易に通知等を許可しない、また何等かの警告が表示されても騙されないよう、従業員に教育を実施すべきであろう。

- 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情報提供があった。IPA で確認をしたところ、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、セキュリティ対策システムや URL フィルタリングシステム等でアクセス制限を行うことに加え、不審サイト・詐欺サイト・偽警告 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。

2.3 IPA が収集し共有した情報

IPA では公開情報を含め独自にサイバー攻撃の情報を収集し、必要に応じてこれらの情報を参加組織へ情報共有するといった活動を行っている。本四半期、IPA が独自に収集し共有を行った情報について、その一部を報告する。

- J-CSIP では、2017 年 10 月以降、継続してプラント等の設備や部品のサプライヤーに対し、実在すると思われる開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽のメールを送り付け、添付ファイル（ウイルス）を開かせようとする攻撃を多数観測してきた。本四半期も、「サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2019 年 10 月～12 月]」[6]の 4 章「プラント関連事業者を狙う一連の攻撃（続報）」に掲載したものと類似した英文の攻撃メールを観測した。
  J-CSIP では、プラントに関わる事業者が多く参加しており、3 年以上前から行われている攻撃メールが現時点でも観測されていることから今後も本攻撃の動向を注視していく。

[6] サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2019 年 10 月～12 月] （IPA）
https://www.ipa.go.jp/files/000080133.pdf

3　URL リンクが細工されたフィッシングメール

本四半期、J-CSIP の参加組織（A 社）より、A 社人事部門からの通知を装った不審なメールが組織内に 2 通送られてきたという情報提供があった。IPA で当該メールを確認したところ、アカウント情報の詐取を目的としたフィッシングメールと考えられるものであった。

当該フィッシングメールには複数の攻撃手口が確認された。本章では、実際に送られてきたフィッシングメールとともに攻撃手口の詳細について説明する。

3.1 フィッシングメールと細工された URL リンク

A 社の人事部門からの通知を装って送られた実際のフィッシングメールを図 2 に示す。

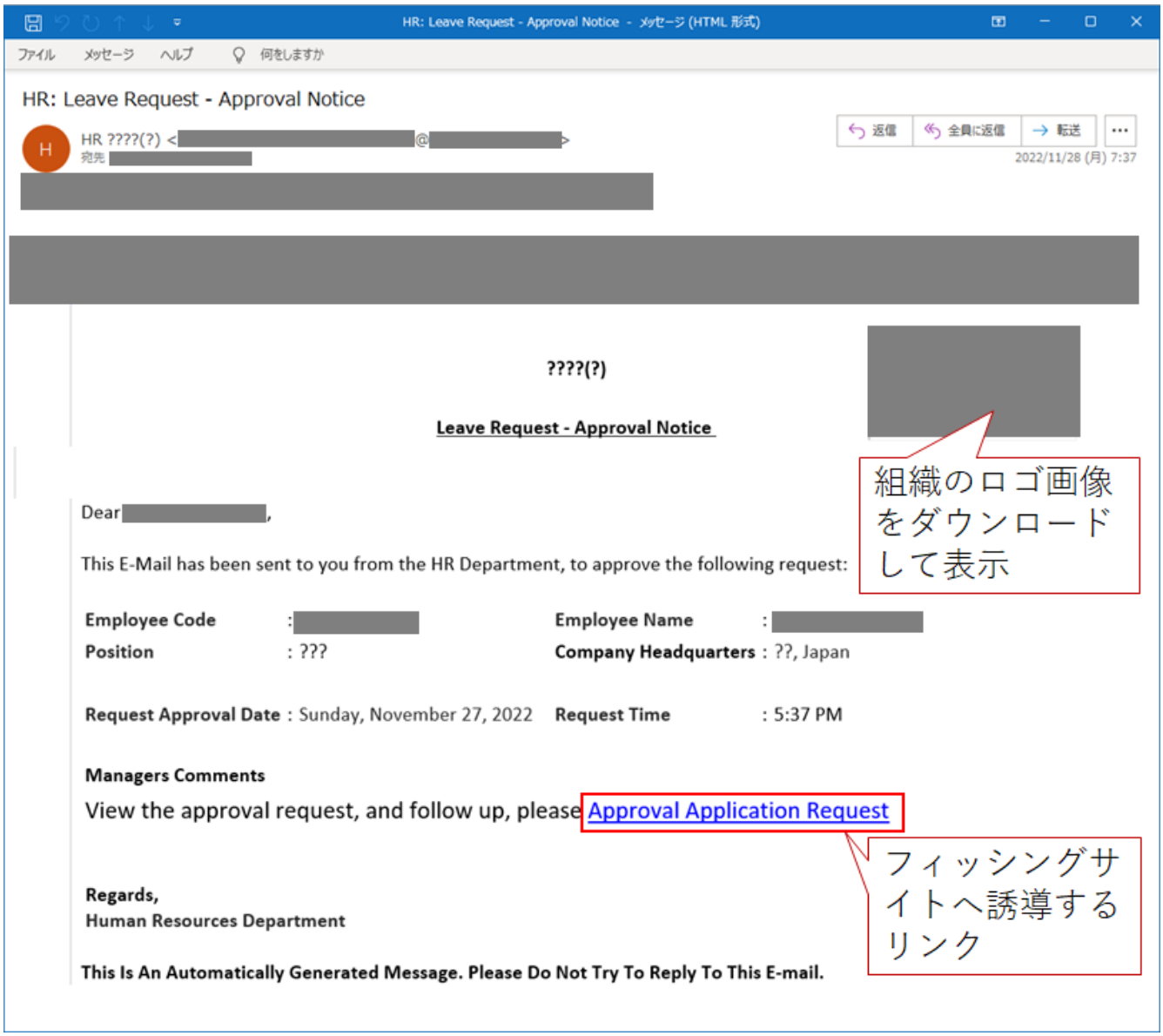


図 2 実際に送られてきたフィッシングメール

このメールは、人事システムからの休暇申請に関する通知メールを装っており、内容を確認させることで、フィッシングサイトへのリンクを開かせようとするものであった。送信元のメールアドレスは、ローカル部に A 社名や受信者の氏名を示す文字列が含まれており、ドメイン部には A 社ではなく別の企業のドメインに似せ

たものが使用されていた。 Reply-To ヘッダのメールアドレスも送信元メールアドレスと同じドメインが使用されており、返信すると攻撃者にメールが届く可能性がある。なお、メールの表示名や本文で「??」となっている部分は攻撃者が送信する際に漢字が文字化けしたものであり、本来は組織名や役職、住所などが入ると考えられる。

本フィッシングメールに記載された URL リンクは、図 3 で示す通り、海外のセキュリティベンダ（B 社）の URL を検査するサービスを経由してからフィッシングサイトにアクセスするように細工されていた。なお、フィッシングサイトの URL リンクには、組織のドメインや氏名等、受信者を識別できる情報が Base64 でエンコードされた状態で含まれていた。

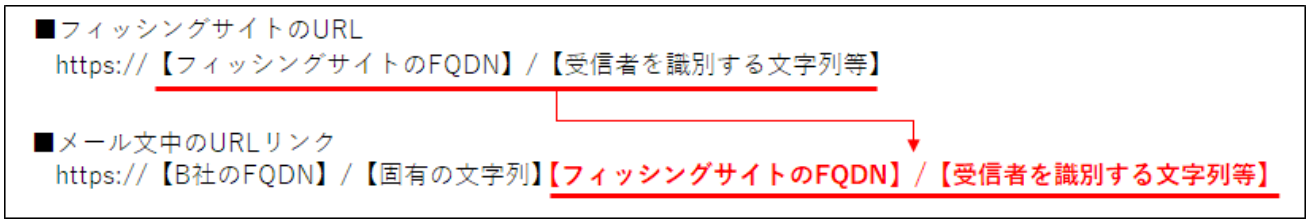


図 3 細工された URL リンク

細工された URL リンクにアクセスすると、まずは B 社のサーバにアクセスし、B 社のサービスが検査対象（フィッシングサイト）の URL を不審なサイトかどうか検査し、安全であると判定した場合のみ、フィッシングサイトに遷移する状態となっていた。通常は、メールが B 社のメールセキュリティ製品を導入したサーバを経由した際に、メール文中の URL リンクが図 3 のように置き換えられるものと考えられる。しかし、A 社は、B 社の製品を使用していないとのことであった。

また、公開情報でも類似の内容の攻撃メールを発見しており、同様に URL リンクが細工されていることを確認している。

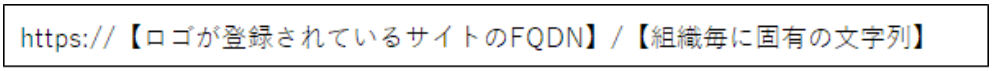
組織が導入するメールフィルタリング製品には、メール文中に含まれるフィッシングサイトの URL を検知する機能を持つものがある。攻撃者は、フィッシングサイトの URL を B 社のサービスを経由する URL に細工することで、メールフィルタリング製品による検知を回避しようとした可能性がある。

なお、本件の情報提供時点（2022 年 12 月時点）では、本文中の細工された URL リンクをクリックすることでフィッシングサイトの URL に遷移したものの、フィッシングサイトは表示されなかった。しかし、細工前の URL を公開情報にて確認したところ、同一サーバ上で別の FQDN で稼働するフィッシングサイトが存在していたため、アカウント情報を詐取する目的のフィッシングサイトが設置されていたものと推定している。

3.2 ロゴの表示

本フィッシングメールを HTML メールとして開くと、外部の URL から、A 社のロゴとみられる画像ファイルがダウンロードされ、メールの右上に表示されるようになっていた。攻撃者は、標的とする者が所属する組織内のメールに装うため、その組織のロゴを表示させようとしたと考えられる。

なお、画像ファイルの読み込み先のウェブサイトには、複数の企業や組織のロゴが登録されており、URL 中の固有の文字列を変えることで、対象の組織のロゴを表示できる仕組みとなっていた。



3.3 SNS 上に公開されている情報の悪用

本フィッシングメールの本文中には、受信者の氏名や所属する組織名のほか、本社所在地（Company Headquarters）や役職（Position）の情報が含まれていた。本フィッシングメールおよび複数の類似のメールにおいて、それらの情報を公開情報で確認したところ、全て LinkedIn に登録されている情報と一致していた。なお、メールで文字化けしていた情報は、LinkedIn 上では漢字で登録されていたものであった。

以上のことから、攻撃者は LinkedIn 等の公開情報に登録されている情報を悪用し、攻撃メールを送信している可能性が考えられる。

3.4 まとめ

企業・組織がセキュリティ対策を講じる一方で、攻撃者はその対策をかいくぐろうと画策してくる。フィッシングメールによるアカウント情報詐取の被害に遭わないためには、利用者一人ひとりが騙しの手口を知ることが重要である。その上で、不審なメールの添付ファイルは開かない、URL リンクはクリックしない、正規のものか判断がつかないサイトで ID やパスワードを入力しないといったことを徹底してほしい。

また、本事例のように、フィッシングメールを HTML 形式で送信することで、リンク先表示の隠蔽や受信者の組織を装うための画像表示などを行う場合がある。そのため、社外からのメールをテキスト形式で表示するように設定することで、フィッシングメールを見極めやすくなる可能性がある。最終的には利便性との兼ね合いとなるが、必要に応じて設定を検討してほしい。

あわせて、SNS 等で公開している個人情報は、ビジネスや交流等に活用されるだけではなく、本事例のように攻撃に悪用される可能性がある点も認識すべきである。ビジネス等で必要な情報の公開はやむを得ないが、SNS 上で公開する情報の必要性や公開範囲について、あらためて見直すことを勧める。

4　不正アクセスによるランサムウェア攻撃の被害事例

J-CSIP 参加組織より、グループ会社でランサムウェアに感染する事案が発生し、ファイルサーバやバックアップサーバ、業務用パソコンのデータが暗号化されたという情報提供があった。本件では、VPN 装置から組織内ネットワークに侵入され、その後 Active Directory（以下、AD）の侵害から、最終的に組織内のサーバやパソコンのデータが暗号化された。

本章では、攻撃の手口の詳細について説明する。

4.1 攻撃手口

本件の攻撃の流れを図 4 に示す。攻撃者の初期侵入から暗号化までは 3 日間程で行われていた。

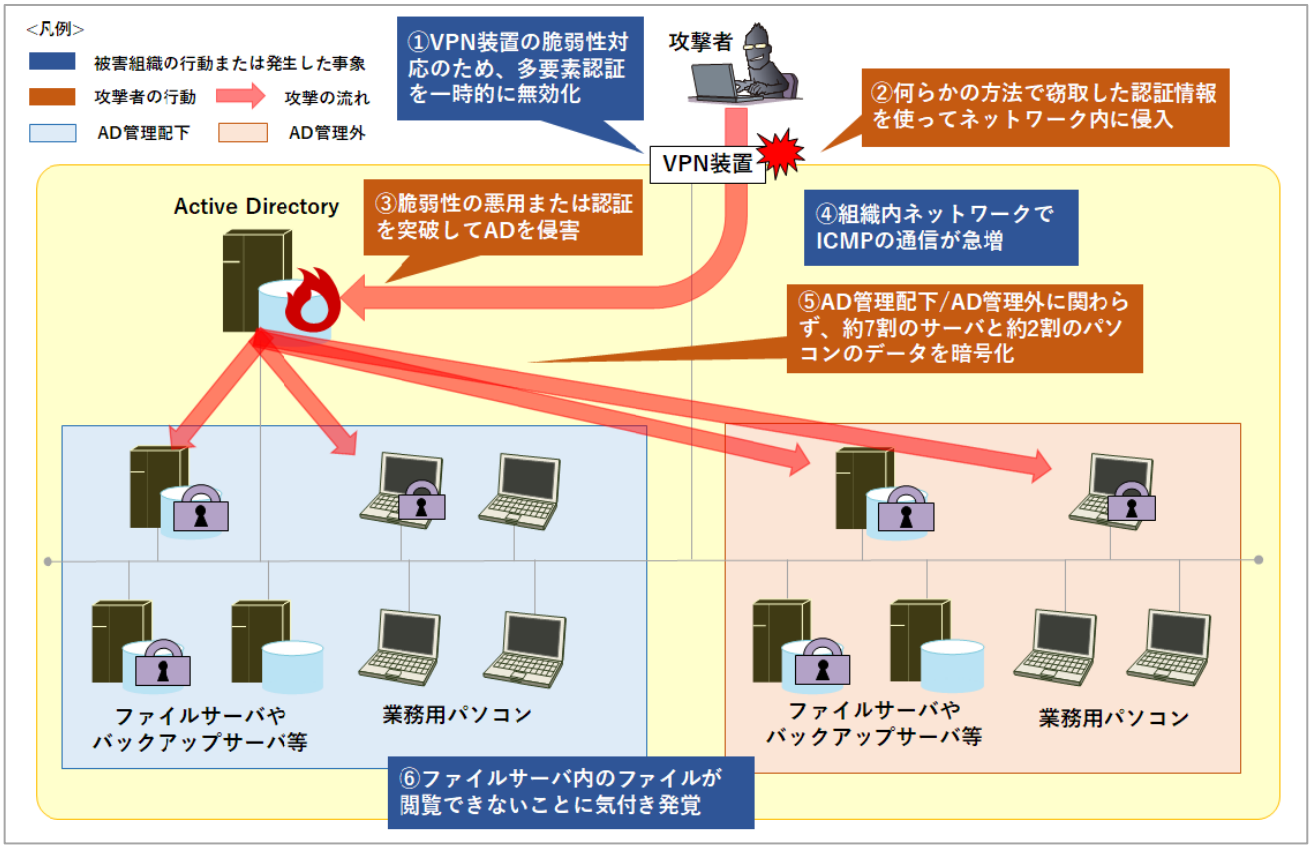


図 4 攻撃の流れ

4.1.1 初期侵入

当該組織では、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た VPN 装置の認証に多要素認証を導入していたが、脆弱性対応のために多要素認証を一時的に無効化していた（図 4-①）。なお、多要素認証を無効化しないと脆弱性対応ができなかった要因については情報提供外のため不明である。多要素認証を無効化していたのは 1 週間程度で、このタイミングで攻撃者は、VPN 装置から組織内ネットワークに侵入した（図 4-②）。何らかの方法で窃取された認証情報が使われて VPN 接続され、ネットワーク内に侵入されたとみられている。

4.1.2 侵害範囲拡大と暗号化

攻撃者は初期侵入後に、AD を侵害した（図 4-③）。当該組織によるフォレンジック調査の結果、AD の

Zerologon（CVE-2020-1472）と呼ばれる脆弱性が悪用された痕跡が確認されたとのことである。しかし、Zerologon が悪用された痕跡以前にも、AD への不審なログインが確認された。また、AD の管理者のパスワードの強度が低かったことも判明しているため、情報提供元の組織では、AD が侵害された原因は、脆弱性の悪用もしくは総当たり攻撃による認証の突破と推測している。

その後、組織内ネットワークで ICMP（ping）の通信が急増した（図 4-④）。この通信は、攻撃者が後に行う暗号化のためにネットワーク内のサーバやパソコンの稼働状況を確認する目的で行ったものと思われる。

最終的に、サーバやパソコンに対して、PsExec によりランサムウェアが実行され、約 7 割のサーバと、約 2 割の業務用パソコンが暗号化の被害を受けた（図 4-⑤）。被害を受けたサーバやパソコンは AD の管理配下のものもあれば、管理外のものもあった。攻撃者は稼働していたサーバやパソコンを手当たり次第に暗号化したものとみられる。当該組織では、社外に公開する用途のサーバをクラウド上に設置していたが、本件で侵害されたネットワーク（すべてオンプレミス環境）とクラウド環境は接続していなかったため、クラウド上のサーバは被害に遭わなかった。

その後、従業員がファイルサーバ内のファイルが閲覧できないことを社内で問い合わせし、被害が発覚した（図 4-⑥）。

暗号化の被害を受けたサーバには、バックアップサーバも含まれており、サーバやパソコンはバックアップから復旧することができず、初期化し、再構築することになった。

4.2 まとめ

本件ではバックアップサーバを含む大量のサーバやパソコンが被害に遭い、インシデント発生から暫定復旧までに約 2 か月の対応を強いられることとなった。また、フォレンジック調査や対策のために約 2,000 万円の費用がかかった。ランサムウェア攻撃は長時間の事業停止等、事業継続に影響を脅かすものであるということを認識し、必要に応じて組織の BCP の見直しの検討や、万が一ランサムウェア攻撃の被害に遭った場合でもバックアップから復旧できるよう、バックアップ先は複数用意する、バックアップに使用する機器はバックアップ時のみ対象機器と接続するといった対策の検討をしてほしい。

また、本件では初期侵入で VPN 装置が狙われた。当該組織では、多要素認証を導入していたが、脆弱性対応を行うために、多要素認証を無効化したところ、そのタイミングで攻撃者に侵入されていた。業務の都合上、一時的にセキュリティレベルを落として対応する場合もあるかもしれないが、攻撃者はそのタイミングで攻撃を行ってくる場合があることを認識し、セキュリティレベルを落とす場合でも安全に運用できるよう回避策を用意することを検討してほしい。

5　企業のウェブサイトへの不正通信の被害事例

本四半期、J-CSIP 参加組織（A 社）より、A 社のグループ会社や同社の取り扱い製品のウェブサイトに対して、探索行為とみられる大量の不正通信や問い合わせフォームへの書き込みが発生したとの情報提供があった。当該内容を整理し、J-CSIP 参加組織へ情報共有を行ったところ、別の参加組織（B 社）においても同様の不正通信が見つかった。

本章では、A 社と B 社で確認された不正通信の内容や、当該組織が行った対応について説明する。

5.1 A 社で確認された不正通信の内容と対応

情報提供元である A 社のグループ会社や同社の取り扱い製品のウェブサイトで、4 つの IP アドレスから、1 週間で 1,000 万件弱の大量の不正通信を受信した。確認された不正通信は、大きく分けると、探索行為とみられる大量のアクセスと、問い合わせフォームへの書き込みであった。

探索行為について、一部のログの情報提供があり、IPA で確認したところ、ウェブサイト上のコンテンツの取得や、ディレクトリトラバーサル、WordPress 等の脆弱性を悪用した設定ファイルやパスワードファイルの取得を試みるものであった。また、問い合わせフォームに書き込まれていた内容の一例としては、数字 3 桁が記載されているだけといった、意味がなく簡単な内容のものであった。問い合わせフォームの動作の調査や、大量のリクエストを投げシステムを停止するといった目的があったと考えられる。

A 社では、本インシデントの発生を確認したのち、問い合わせフォームの一時閉鎖と、WAF（Web Application Firewall）で攻撃元とみられる IP アドレスを遮断した。遮断後にも別の IP アドレスからの探索行為とみられる不正通信が確認されており、問い合わせフォームについては、1 か月強の期間、停止を行ったとのことだった。

5.2 B 社で確認された不正通信の内容と対応

A 社から情報提供のあった内容を整理し、複数の攻撃元 IP アドレスを含めて参加組織に情報共有を行ったところ、B 社でも、一部の攻撃元 IP アドレスから同様のものとみられる不正通信が確認されたという情報提供を受けた。こちらは 1 週間ほどで、60 万件を超える大量のアクセスであり、当該不正通信は、A 社とほぼ同時期に確認されていた。

B 社でも、攻撃元 IP アドレスをファイアウォールで遮断したところ、約 10 分後には不正通信を受信しなくなったとのことだった。

5.3 攻撃元 IP アドレスの所有者情報

A社によると、本件で確認された複数の攻撃元 IP アドレスの所有者情報には、同一の企業（X 社）が登録されているとのことだった。IPA 側でも公開情報を確認したところ、X 社はインターネット上のネットワークの構成単位である AS（Autonomous System）が割り与えられたホスティング会社とみられた。また、セキュリティベンダの解析記事によると、ある攻撃者グループが攻撃の際に利用するインフラとして、X 社の AS がリストアップされていた。加えて、信憑性は不確かであるが、ある攻撃者と X 社との関連性を紐づけていた解析記事も確認している。

このような情報をもとに A 社ではその後、上記の AS のネットワークアドレス全体を遮断した。また他のネットワークアドレスから同様の不正通信が発生しないか引き続き監視するとのことだった。

5.4 まとめ

本件で情報提供をいただいた A 社では、日頃から不正通信を監視し、不審なものがあれば調査や遮断を行うという仕組みや運用体制を持っていた。このため、今回のケースでも、不正通信の攻撃元 IP アドレス

を遮断したことで、甚大な被害は発生しなかったとみられる。また IPA より情報の共有を受けた B 社では、同様の通信の発生状況を調査し、迅速に遮断を行うことができた。

公開サーバ等、インターネット上からの脅威を受けやすいシステムについては、大量のアクセスなど、通常とは異なる通信を日頃から監視し、不審なものがあれば遮断する仕組みや体制を整備されていることが望ましい。

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