サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023 年 1 月～3 月]

2023 年 5 月 11 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、2023 年 3 月末時点の運用体制と、2023 年 1 月～3 月期（以下、本四半期）の運用状況を報告する。1 章、2 章では本四半期の全体状況を、3 章では 2022 年度の活動状況、4 章以降では本四半期で把握・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/about.html

1　運用体制

本四半期では、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）。

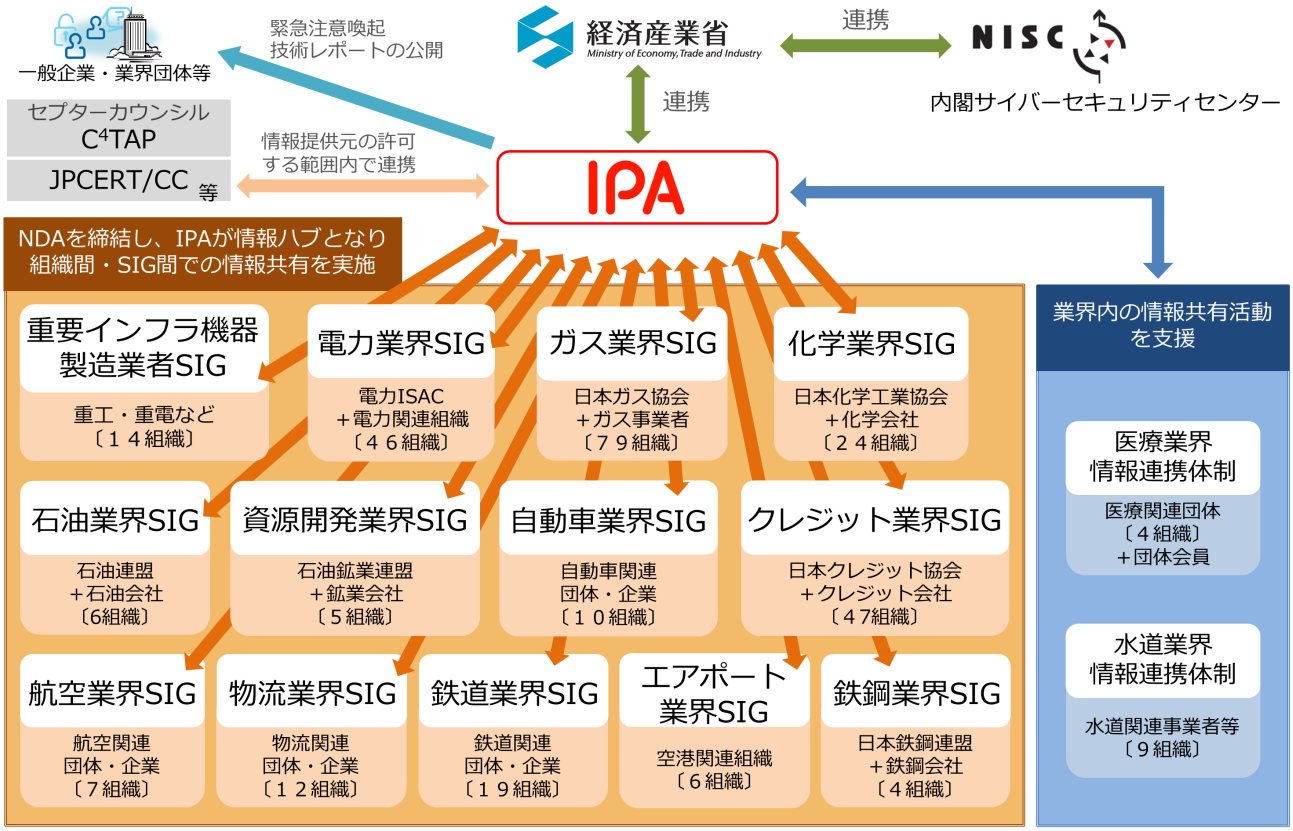

図 1 J-CSIP の体制図

[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ある。ここでは延べ数としている。

2　運用状況（2023 年 1 月～3 月）

2023 年 1 月～3 月の運用状況について、2.1 節で情報提供・情報共有の実施件数を、2.2 節と 2.3 節で参加組織から提供された情報や IPA が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

2023 年 1 月～3 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（3 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			2023 年
		4 月～6 月	7 月～9 月	10 月～12 月	1 月～3 月
1	IPA への情報提供件数	134 件	22 件	26 件	**59 件**
2	参加組織への情報共有実施件数 ※1	35 件	38 件	25 件	**22 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 **59 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 **1 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 へ提供された。

- 標的型攻撃の被害に関する情報提供があった。情報提供元の海外グループ企業が管理するシステムの脆弱な箇所から侵入され、その後、国内側のシステムまで侵害範囲を拡大されたという内容であった。事案発覚の経緯や攻撃手口について、4 章で述べる。

- 情報提供元の取引先を装った不審なメールに関する情報提供があった。この不審メールには、詐称用ドメインの使用や、過去にやり取りした正規のメールの引用がなされており、明らかに悪意のあるものであった。一方で、ウイルスの感染やフィッシングサイトへの誘導を目的としたファイルの添付や URL リンク等はなく、本文には受信者の身に覚えのない用件が記載されていた。攻撃者の意図は不明ではあるものの、このメールに返信した場合、何らかの攻撃に発展するものと考えられる。不審メールの内容について、5 章で述べる。

- 情報提供元の管理しているサーバにおいて、ウイルス感染の被害を受けたという情報提供があった。外部から SMB プロトコルを使用して侵入されたとみられるが、攻撃手口の詳細は不明である。また、侵入後、侵害を受けたサーバ上でウイルスのダウンロードや実行が行われ、そのサーバを起点として、ネットワーク上の複数台のサーバに対して RDP 等を使った不正なログインおよびウイルスへの感染が

行われた。使われたウイルスの特徴から、暗号資産のマイニングを目的とした攻撃と考えられるものであった。
インターネットからアクセス可能なサーバや機器においては、不必要なポートの閉塞、既知の脆弱性の有無の確認など、防御策の徹底が不可欠である。

- 情報提供元の海外関係会社において、EDR で不正プログラムを検知したという情報提供があった。不正プログラムは USB メモリに保存されており、OA 端末に接続したタイミングで検知し発覚した。当該 USB メモリは、FA（Factory Automation）系機器と OA 端末間のデータ転送用に従業員が持ち込んだもので、海外関係会社としては認知していないものであった。USB メモリにウイルスが混入した経緯は不明であるものの、ウイルスの特徴から、すでにウイルスに感染していた端末に USB メモリを接続した際、書き込まれたことも考えられた。
  USB メモリの接続を制御するシステムの利用や従業員への教育など、管理の徹底を目指していながらも、海外関連会社などへの徹底が及ばないという事例は過去にも多く、今後とも継続的な課題であろう。

- 2023 年 3 月、Emotet の攻撃活動が再開し、新しい攻撃手口を観測した。攻撃メールにファイルサイズが 500MB を超える Word ファイルが ZIP ファイルとして圧縮され添付されているものや、OneNote 形式のファイルを悪用したものがあった。これに関連して、J-CSIP 参加組織からも、Emotet 感染を企図した攻撃メールの情報提供が複数件あった。情報提供のあったいくつかの組織においては、メール受信時のセキュリティ対策システムをすり抜け、従業員まで Emotet の攻撃メールが届いていたものもあった。
  攻撃者は、セキュリティ対策のシステムを回避するため、巧妙に攻撃手口を変えてくる。組織においては、最新の攻撃動向に気をくばり、システム的な対策のほか、必要に応じて利用者へ攻撃手口を注意喚起してほしい。

2.3 IPA が収集し共有した情報

IPA では公開情報を含め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。本四半期に IPA が収集し共有を行った情報について、その一部を報告する。

- 2023 年 1 月、Microsoft Office のソフトウェアの一つである OneNote 形式のファイル（拡張子 .one）を悪用し、ウイルスに感染させる攻撃メールの情報を入手した。攻撃メールには、悪意のある OneNote 形式のファイルが添付されている。このファイルを開き、ファイル内に書かれた偽の指示に従って操作をすると、当該ファイル内に隠されている悪意のある VBS ファイルが実行され、ウイルスに感染することを確認している。この攻撃手口については、これまで多く観測されている Word や Excel のマクロ機能を悪用した添付ファイルへの対策（マクロの無効化や保護ビューでの閲覧）では防ぐことができない。VBS ファイル実行前には警告メッセージが表示されるが、この種の警告メッセージはユーザ側で無視し「OK」ボタンを押してしまうことが多いため、注意が必要である。
  J-CSIP では参加組織に対して、この手口や注意点を周知し、被害を発生させないようにするべく、情報共有を実施した。
  なお、2023 年 3 月には、本攻撃と同様の手口を使い、Emotet への感染を狙うメールについても観測されている。また、JPCERT/CC の記事 [3]によると、Emotet などのばらまき型のウイルス以外の攻撃にも、この手口が使われていることを観測しており、深刻な被害をうけるケースもありうるので注意してほしい。

  この攻撃手口と注意点をまとめた一般利用者向けの資料を、本書の参考資料とした。必要に応じ活用していただきたい。また、本手口の技術的な対策として、Microsoft Office のグループポリシーを設定するという方法もある [4]。グループポリシーの設定を行う場合、業務影響などを検討しつつ対策を行ってほしい。

---

[3] JPCERT/CC Eyes「暗号資産交換業者を標的とする Parallax RAT 感染を狙った活動」
https://blogs.jpcert.or.jp/ja/2023/04/parallax-rat.html

[4] How to prevent Microsoft OneNote files from infecting Windows with malware (BLEEPINGCOMPUTER)
https://www.bleepingcomputer.com/news/security/how-to-prevent-microsoft-onenote-files-from-infecting-windows-with-malware/

3　2022 年度の状況

3.1　2022 年度の取り扱い件数と年度毎の推移状況

J-CSIP における取り扱い件数（情報提供件数、標的型攻撃（メール、検体等）と見なした件数、情報共有実施件数）と参加組織数について、J-CSIP を運用開始した 2012 年度から 2022 年度までの推移状況を次に示す（表 2、図 2）。

表 2 年間の取り扱い件数と参加組織数

項目	IPA への情報提供件数	標的型攻撃（メール、検体等）と見なした件数	参加組織への情報共有実施件数	参加組織数
2012 年度	246	201	160	5 業界 39 組織
2013 年度	385	233	180	5 業界 46 組織
2014 年度	626	505	195	6 業界 59 組織
2015 年度	1,092	97	133	7 業界 72 組織
2016 年度	2,505	177	96	7 業界 86 組織
2017 年度	3,456	274	242	11 業界 228 組織
2018 年度	2,020	213	195	13 業界 249 組織 ＋ 2 情報連携体制 13 組織
2019 年度	2,303	401	225	13 業界 249 組織 ＋ 2 情報連携体制 13 組織
2020 年度	6,202	125	147	13 業界 262 組織 ＋ 2 情報連携体制 13 組織
2021 年度	843	35	118	13 業界 279 組織 ＋ 2 情報連携体制 13 組織
2022 年度	241	13	120	13 業界 279 組織 ＋ 2 情報連携体制 13 組織

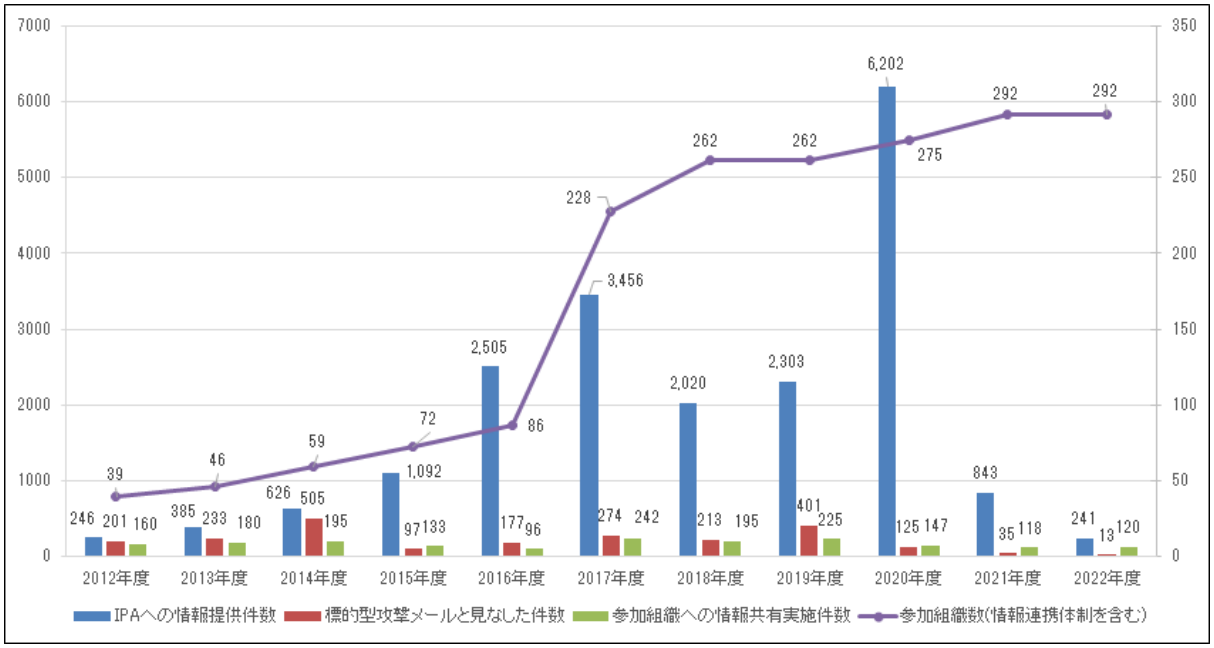

図 2 年間の取り扱い件数と参加組織数の推移

3.2 2022 年度の活動

2022 年度、J-CSIP の参加組織数については増減なしであった。

情報提供数について、2022 年度は 241 件となり、2021 年度に比べると数を減らしている。情報提供の中には、組織に着信したすべての不審なメールを提供いただく場合があり、内容を IPA で確認した結果、正規であると判断されるメールや、広くばらまかれているフィッシングメールと判断するケースについては、参加組織への共有は行わない場合がある。2022 年度については、その種の情報提供数が減少している。こうした背景には、J-CSIP 参加組織側で、不審な通信やメールを分析する調査対応力向上が進み、より有益な情報共有に向けて、情報提供要否の判断が高度化してきたことが推測される。

2022 年度にあった情報提供のうち、日本国内の特定の業界や組織を狙う標的型攻撃について、J-CSIP 参加組織内のネットワークに侵入されたという重要な事案が 2 件あった。いずれも海外拠点やグループ会社などの脆弱な箇所から侵入されたというものであった。標的型攻撃の情報提供は減少傾向にあるものの、依然として標的型攻撃自体は継続している状況であると考えられ、引き続き警戒していただきたい。

また、実際に被害は発生しなかったものの、組織内のアカウント情報を窃取することが目的と思われるフィッシングメールの情報提供が複数あった。組織のアカウント情報を狙うフィッシングメールについては、これまでも毎年継続して確認されているが、添付ファイルやアクセス先のウェブサイトに受信した組織の企業ロゴや役員名を掲載しているものや、組織内メールを装うためにメール本文に企業ロゴを張り付けるなど巧妙に細工がされたものがあり、引き続き組織のアカウントは攻撃者に狙われるものと考えられる。Microsoft アカウントなどの組織で利用している認証情報が窃取されると、メール情報の盗み見や、外部から侵入、侵入後の横展開（侵害範囲の拡大）に悪用される可能性がある。基本的なメールのセキュリティ対策に加え、アカウント管理の徹底や従業員教育も必要である。

J-CSIP では標的型攻撃に限らず、サイバー攻撃全般の情報共有を今後も進めていく予定である。

3.3 ビジネスメール詐欺（BEC）対策特設ページを公開（2022 年 9 月）

J-CSIP では 2022 年度も引き続きビジネスメール詐欺（BEC）について情報提供を受けている。IPA では、BEC についてはこれまで過去に 3 回の注意喚起を行ってきたが、J-CSIP のみならず IPA の安心相談窓口でも BEC について継続して相談を受けている状況であることから、IPA 内の BEC に関する情報を一か所に集約し、より一般の方へ注意を促すべく「ビジネスメール詐欺（BEC）対策特設ページ [5]」を 2022 年 9 月に公開した。

当該ページには、BEC に関して、その特徴や対策をまとめたレポートや動画、実際に被害に遭ってしまった場合の対応や、FAQ など多数の情報を掲載している。あわせて J-CSIP や安心相談窓口に実際に報告された被害事例も複数掲載している。

自組織の教育や BEC への対策の検討、事案発生時の対応方法など、参考にしてほしい。

---

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

4　海外拠点を侵入経路とした標的型攻撃の被害事例

J-CSIP 参加組織より、標的型攻撃と思われる事案に関する情報提供があった。情報提供元（以下、A 社）によると、攻撃者は当該組織の海外グループ企業（以下、B 社）のサーバを侵害した後、A 社のシステムを侵害した。また、A 社の PC では、Microsoft 社の正規のサーバを C＆C サーバとして悪用する遠隔操作プログラム（RAT）が発見された。

A 社は、本件で使用されたウイルスの作りや内部侵害の手口などから、標的型攻撃を行うグループによる攻撃と推定している。なお、この攻撃による A 社からの機密情報等の漏えいや改ざん被害は確認されていない。

本章では、公開可能な範囲で、発見の経緯と攻撃手口、および発見後の対応について説明する。

4.1 攻撃発見の経緯

A 社が管理する PC で、不審な挙動が発生したことをセキュリティソフト（EDR）が検知した。検知原因を調査したところ、次の 2 点が判明した。

- A 社の PC に RAT を含む不審なファイルが複数設置されていた。
- RAT を含む不審なファイルは、A 社の Active Directory サーバ（AD サーバ）から不正アクセスされ、設置されていた。

このため、A 社はさらに調査を継続したところ、AD サーバは、B 社のサーバから不正アクセスされていたことが判明した。

4.2 攻撃手口

本件の攻撃の流れと発見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。

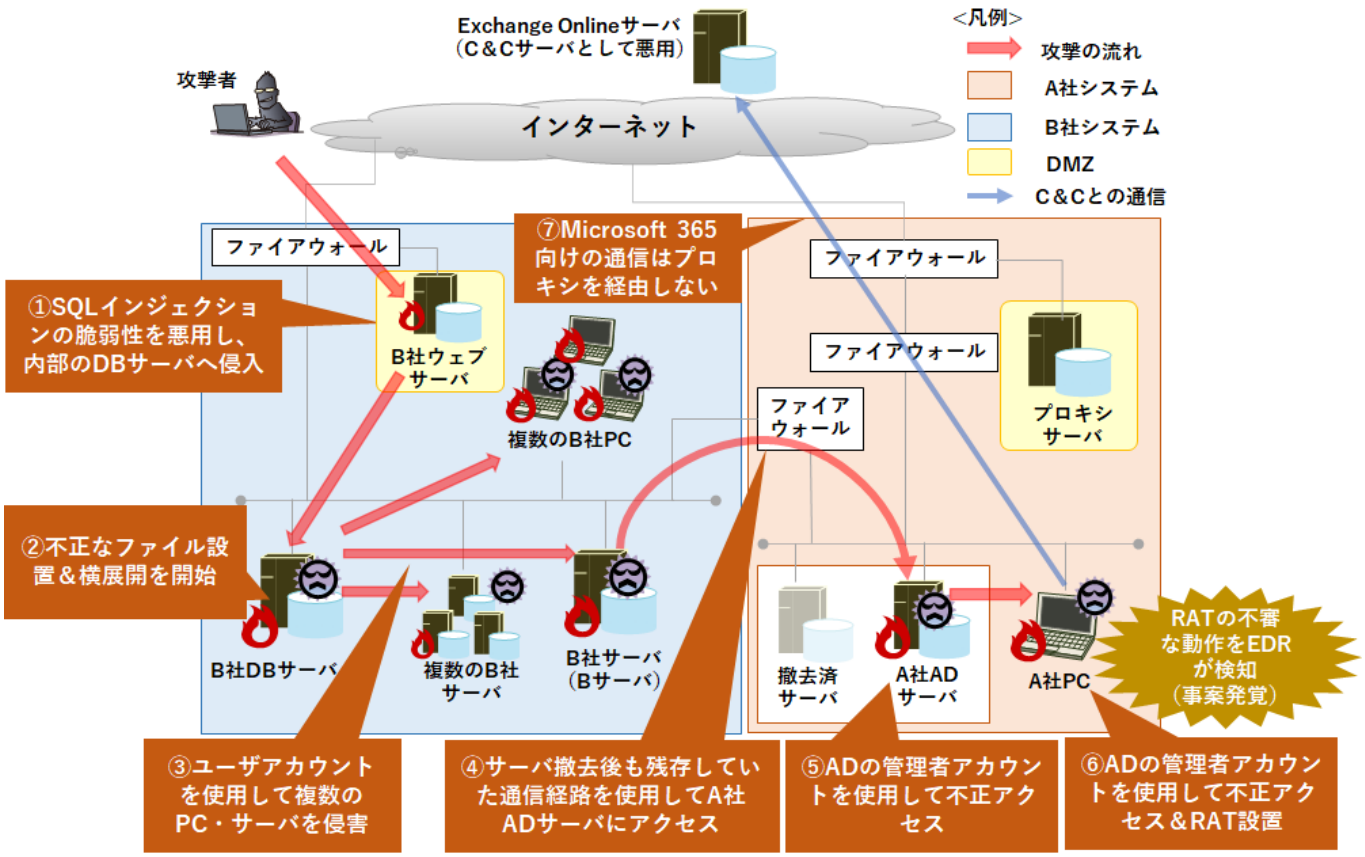

図 3 攻撃の流れ

4.2.1 初期侵入

本件では、B 社ウェブサーバに存在していた SQL インジェクションの脆弱性を悪用し、B 社 DB サーバに侵入したと考えられる（図 3-①）。DB サーバには、ウェブアプリケーションを経由して、PowerShell の起動などのコマンドが実行された形跡が残っていた。また、B 社 DB サーバは次に示す通り脆弱な状態であり、攻撃者との通信経路の確立やその後の侵害範囲拡大に悪用された可能性がある。

- セキュリティ更新プログラムが適切に適用されておらず、リモートでコード実行可能な脆弱性が複数存在していた。
- DB サーバの匿名ユーザが有効であり、B 社の AD ユーザが DB サーバの C ドライブに対する書き込み権限を持っている状況であった。

なお、DB サーバにはいくつかの不正なファイルが設置されていたが、これらのファイルが実行された痕跡は見つからなかった（図 3-②）。

4.2.2 侵害範囲拡大

B 社への侵入後から A 社での攻撃発覚までの攻撃者の動きを説明する。攻撃者は、B 社に侵入後、A 社への侵入経路を探索しつつ、侵害範囲を拡大していった。最初の侵入（図 3-①）から A 社 PC への不正なファイルの設置（図 3-⑤）までは、数週間の間に行われた。

B 社システムでの侵害範囲拡大

- DB サーバを起点に、他のサーバへの探索行為を行った。その後、匿名アカウントや、何らかの方法で入手した複数のユーザアカウントによるログインを試行したのち、複数のサーバへ不正にログインし侵害範囲を拡大した（図 3-③）。不正にログインされた痕跡はあったが、ウイルスの設置等の具体的な侵害行為が確認されていないサーバもあり、攻撃者は A 社への侵入を目的に特化した行動をしていた可能性がある。
- 侵害された手口や経路は不明であるが、A 社サーバの侵入元となるサーバ（以下、B サーバ）に侵入した。
- B サーバには、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を起動するためのファイルなどが不正に設置されていた。後の調査により、B サーバから不正な通信が発生していることが判明しており、詳細は不明ながら、当該のプログラムを使用してアカウント情報窃取や侵害範囲の拡大等の活動を試みた可能性がある。

A 社システムへの侵害範囲拡大

- B サーバから A 社 AD サーバへ、A 社と B 社を結ぶネットワーク回線を介して、不正ログインを行った。A 社のネットワーク接続口にはファイアウォールが設置されていたが、B サーバから A 社 AD サーバへのアクセスは、意図しない設定により、通信可能な状態であった（図 3-④）。この設定は、過去に A 社内に設置されていたサーバ（撤去済サーバ）の通信要件として設定されていたものであり、当該サーバ撤去後は不要な設定であったが、残存したままになっていた。またその設定内容も、ネットワークセグメント単位での設定となっており、A 社 AD サーバを含め、当該ネットワークセグメント上のサーバにアクセス可能な状態であった。
- B サーバから A 社 AD サーバへの不正ログインには、AD の管理者 ID が使用されていた。（図 3-⑤）。当該管理者 ID は、退職済みの外部業者に付与していたもので、当該 ID とパスワードが悪用された原因は不明であった。
- A社 AD サーバから A 社 PC 複数台へ、先述した管理者IDを使用しログインを試みた形跡があった。うち 1 台に、Microsoft の Exchange Online サーバを C＆C サーバとして悪用する遠隔操作プログラム（RAT、詳細は後述）を設置した（図 3-⑥）

4.2.3 攻撃に使われたウイルス

A 社 PC を調査したところ、4 種類の不審なファイルが発見された。当該ファイルを外部専門機関が解析したところ、Microsoft の Exchange Online サーバを C＆C サーバとして悪用する遠隔操作プログラム（RAT）を動作させるためのファイル群であることが判明した。

本件で確認された RAT は、PC の再起動等を行っても活動を継続できるよう永続化されていた。また、RAT は正規ファイルの悪用や、不正なプログラム部分の高度な難読化が行われており、セキュリティソフト等による検知を逃れようとする意図があったと思われる。

発見されたファイル

(1) 正規の実行ファイル
(2) 正規の実行ファイルが読み込む悪性の DLL ファイル
(3) 悪意ある実行コードが書かれた遠隔操作プログラム（RAT）
(4) Exchange Online サーバとの接続に使用される正規の DLL ファイル

上記ファイルを使った RAT の実行の流れを、図 4 に示す。

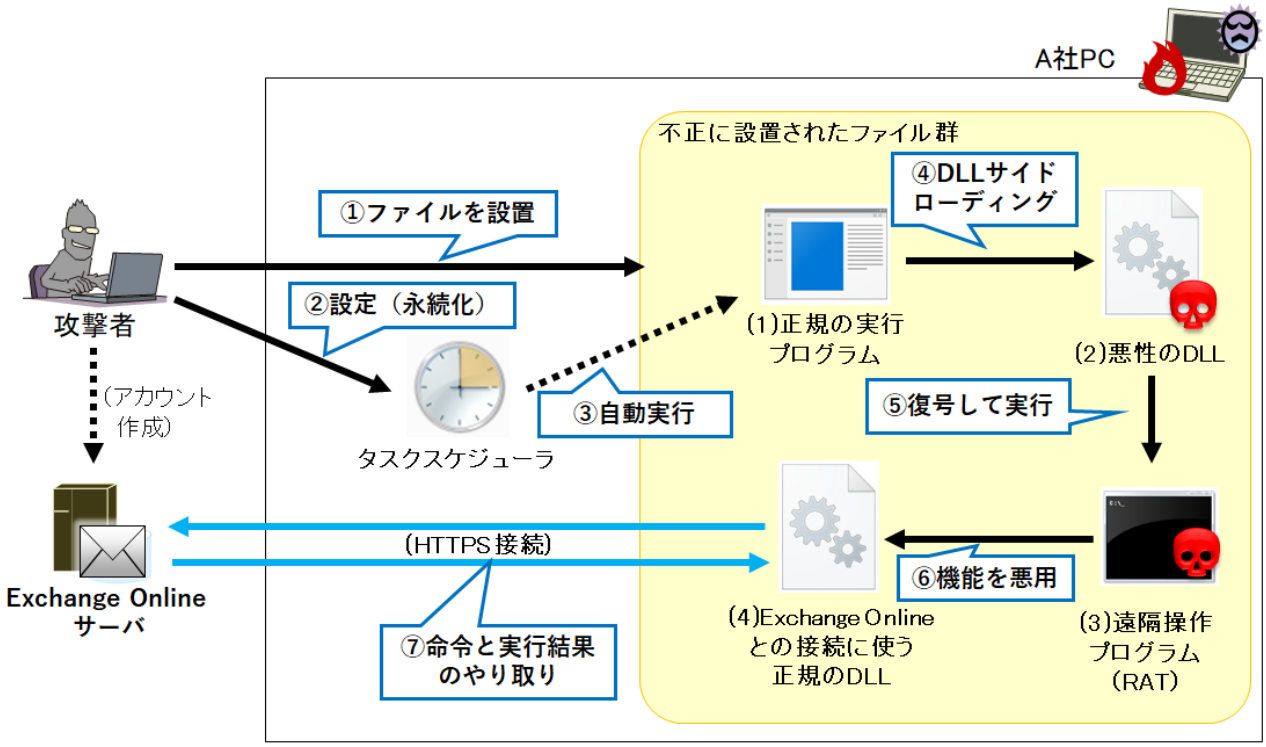

図 4 RAT 実行の流れ

RAT の実行方法

- 窃取済みの管理者 ID を使用して A 社 PC に侵入し、(1)～(4)のファイルを設置する(図 4-①)。
- (1)のファイルをタスクスケジューラで自動実行するように設定し、感染を永続化させる(図 4-②、③)。
- (1)が実行されると、DLL サイドローディング [6]により、(2)の悪性 DLL が読み込まれる(図 4-④)。
- (2)は(3)を復号し、遠隔操作プログラム(RAT)を実行する(図 4-⑤)。
- RAT は、(4)の正規 DLL ファイルの機能を悪用して(図 4-⑥)、Exchange Online サーバとの正規の通信を装い、命令と実行結果のやり取りを行う(図 4-⑦)。

続いて、Exchange Online サーバとの命令のやりとりの流れを図 5 に示す。RAT は、情報の取得やファイル操作、認証情報の窃取などの機能を有していた。命令の内容や実行結果は暗号化された状態で Exchange Online サーバ上に格納される仕組みであった。

[6] 正規の実行ファイルに存在する脆弱性を悪用し、本来読み込まれる DLL とは別の DLL を読み込ませることにより、悪意あるコードを実行させる手法

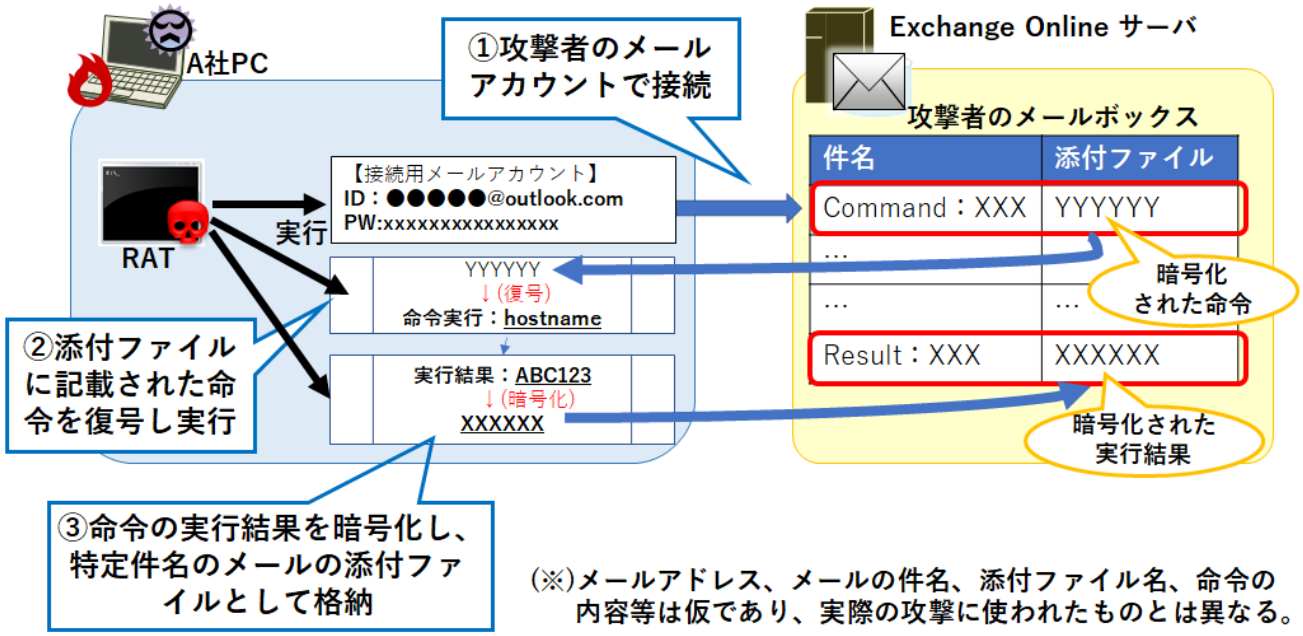

図 5 Exchange Online サーバとの命令と実行結果のやり取り

命令のやり取りの方法

- 攻撃者が作成したメールアカウントを用いて、Exchange Online サーバに接続する(図 5-①)。
- 特定件名のメールアイテムの添付ファイルに記載された、暗号化された命令を読み取り、感染したコンピュータ上で復号し実行する(図 5-②)。
- 命令の実行結果を暗号化し、特定件名のメールアイテムの添付ファイルに格納する(図 5-③)。

この攻撃手口では、命令のやり取りを正規の Exchange Online サーバとの正規の通信内容に見せかけることで、攻撃の検知を困難なものにしていた。

また、Exchange Online サーバをはじめとした Microsoft 365 関連のサーバへの通信は、ネットワークへの負荷を避けるため、プロキシサーバを経由しない設定とすることが推奨されている [7]。情報提供元も、同様の設定としていた。この結果、攻撃者が意図したかは不明ながら、プロキシログに通信の痕跡が残っていない状況であった(図 3-⑦)。

4.3 事案発覚後の対応

本件発覚後、A 社と B 社はフォレンジックを含めた調査を実施し、侵入元や侵害されたコンピュータを特定した。その後、侵害拡大を防止する対策として、侵入元からのアクセスの遮断や EDR ソフトウェアのインストール等を講じた。

4.3.1 A 社の対応

本件発覚から翌日までの間に、侵入経路、および侵害された PC とサーバを特定しネットワークから隔離

[7] Microsoft 365 エンドポイントの管理(Microsoft 社)
https://learn.microsoft.com/ja-jp/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide

した。並行して、B 社サーバからの侵入であったことを特定し、B 社からのアクセスを遮断した。

その後、未使用のサーバの停止、稼働中サーバへの EDR ソフトウェアのインストールを行い、監視を継続した。以降、B 社から A 社への侵入は確認されていない。

調査の結果、A 社から機密情報等の漏えいは確認されなかった。

4.3.2 B 社の対応

A 社から連絡を受け、調査・対応に着手した。対応の過程で B サーバへ EDR ソフトウェアをインストールしたところ、外部との不正な通信を検知したため、当該経路の通信を遮断した。さらに調査を進めたところ、ウェブサーバを経由して B 社内に侵入している可能性があることが判明した。最終的に、A 社が攻撃を発見してから数週間後、当該経路からの通信を遮断した。

通信を遮断してからおよそ 1 週間後、侵害されたサーバを再構築し、主要業務に必要な機能の提供を再開した。

4.4 まとめ

本件では、正規のサーバやサービスを悪用した RAT の使用など、非常に巧妙で発見が難しい攻撃手口が用いられていた。一方で、SQL インジェクションの脆弱性の存在や、脆弱性修正プログラムの未適用、アカウント管理の不備などが初期侵入や侵害範囲拡大の原因と考えられている。すなわち、ウェブサイトのセキュリティ診断や脆弱性修正プログラムの適用、不要な権限の削除などの基本的な対策を徹底していれば、侵入や侵害範囲の拡大を防げた可能性がある。A 社においても、使用されなくなった B 社からの通信許可設定を適切なタイミングで削除していれば、B 社からの不正アクセスを防げた可能性がある。

また、A 社では EDR の導入等の対策により、本件を速やかに検知し対応できた一方で、B 社は A 社からの連絡を受けてからの対応となるなど、A 社と B 社との間で、セキュリティ対策のレベルに差があった。

標的型攻撃は、標的となる組織に直接侵入することが難しくとも、相対的にセキュリティ対策が脆弱な海外グループ企業などを経由して侵入を試みようとする場合がある。このため、自組織のみならず、グループ企業全体でセキュリティ対策の水準を高く維持する必要がある。特に、本件のような被害を防止するためには、会社間のシステムやネットワークの境界に設置されている機器の情報を正確に把握し、脆弱性対策や接続に使用する特権 ID の棚卸、使用状況の監視を確実に行ってほしい。あわせて、機器やネットワーク接続が不要になった際には、速やかに機器の撤去や通信許可設定の見直しを行っていただきたい。

本件の攻撃発見・インシデント対応には EDR が活用された。EDR は、通常とは異なる挙動を監視することで、従来のパターンマッチング型と言われるセキュリティソフトでは検知できないウイルス等を検知できると言われている。EDR が万能ということではないが、適切に使用・運用することにより、成果が得られたことが分かる事例であった。

5　取引先を装った不審なメールが着信した事例

J-CSIP 参加組織より、取引先を装った不審なメールに関する情報提供があった。不審メールの送信元アドレスには、取引先の正規ドメインに似せた詐称用ドメインが使われていた。また、本文には過去にやり取りした正規のメールが引用されているなど、明らかに悪意のあるものであった。一方、メールには、ウイルスへの感染を企図するような不審なファイルの添付や、フィッシングサイトへ誘導するような URL リンクはなかった。受信者はこの不審メールに返信はせず、組織内の管理部署に連絡したため、特段の被害は発生していない。

本章では、不審なメールの詳細について説明する。

5.1 不審なメールについて

本件で受信した不審メールの特徴を次に示す。

(1) 受信したメールの宛先と通数

不審メールの連絡を受けた組織の管理部門が調査したところ、十数名の従業員が当該メールを受信していることが判明した。受信したメールの通数は人により異なるが、多い人では 13～14 通を受信していた。

また、受信した従業員は、件名に書かれた商品・商材の関係者であった。

(2) 送信元アドレス

送信元アドレスには、取引先の正規ドメインに似せた詐称用ドメインが使われていた。詐称用ドメインは複数あり、次のようなパターンで正規のドメインに似せていた。

■ドメイン詐称の例
正規ドメイン　　：company■■■abc.com.sg
詐称用ドメイン1：company■■■abc-com.ga
（差異）「.com」を「-com」に変更
トップレベルドメインを「ga」に変更
詐称用ドメイン2：company■■■abcc-com.ga
（差異）詐称用ドメイン1にさらに1文字追加

図 6 取引先のドメインに似せた詐称用ドメイン

(3) 件名

件名は、次のようなもので、ある月の取引の請求に関連した内容を思わせるようなものであった。また、返信を装う「RE:」がつけられていた。

■メール件名
RE: [INVOICE] [redacted] (Sales of [redacted] for the month of November 2022)
請求書の番号　　商品・商材

図 7 メールの件名

(4) 本文

メール本文は、返信を装うため、引用文がつけられていた。この引用文は、過去にやりとした本物の

メールであったことから、関係者（情報提供元組織、または取引先組織）のメールが盗み見られていたと思われる。
また、引用部分以外の本文は、引用とは関係なく、受信者には身に覚えのない内容であった。その一例を次に示す。

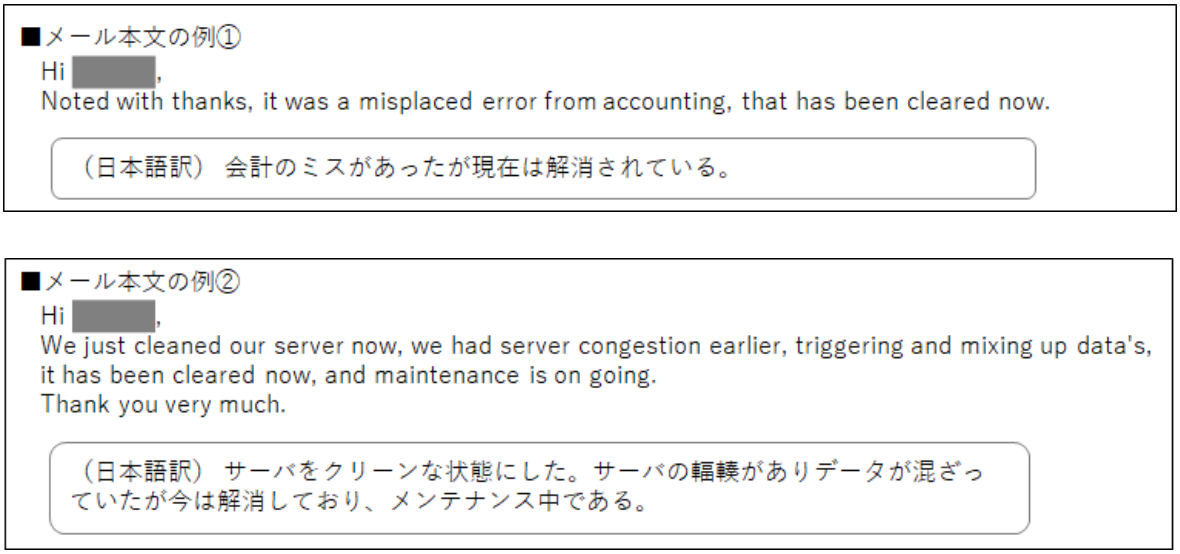

図 8 メールの本文

意図は不明ながら、攻撃者は、受信者からの返信を誘っていたものと思われる。これらのメールに返信した場合、何らか別の攻撃に発展するものと考えらえる。

不審な添付ファイルやURLリンクがないメールであっても、内容に心当たりがなければ、不用意に返信せずに、組織の情報セキュリティ部門などに報告するようにしてほしい。また、組織の情報セキュリティ部門では、報告を受けた不審メールの確保と調査を実施し、必要に応じて組織内への注意喚起を行うことで、同件や類似した不審メールによる被害を防止してほしい。

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/todokede/crack-virus/about.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/todokede/tokubetsu.html

以上