Secureworks®

インシデント対応で得られた教訓：2022年1月～3月

Secureworks® カウンター・スレット・ユニット™ リサーチチーム

目次

概要

2022年1月から3月にかけて当社が従事し、対応を完了した100件を超えるインシデント対応（IR）案件のデータを、当社カウンター・スレット・ユニット™（CTU）のリサーチャーが解析し、新たな脅威や最新動向に関する知見を取りまとめました。組織のリスク管理における意思決定や優先度分類の指針としてお役立てください。

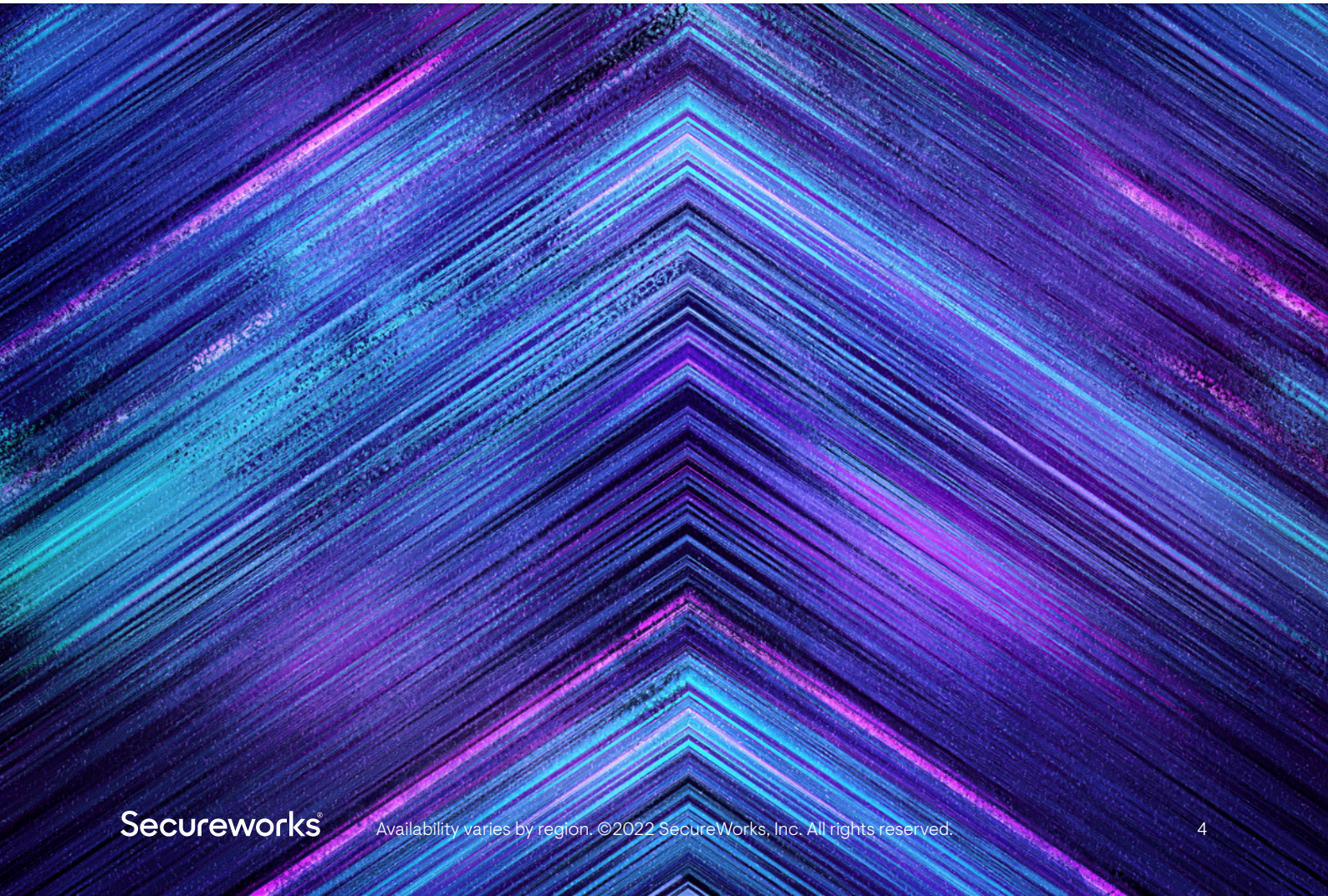
お客様が当社にインシデント対応（IR）案件を委託される経緯やその内容は様々です。たとえば、社内リソースの多寡やインシデントに関する報道を受けて、もしくは社内のセキュリティオペレーションに細心の注意を払うべき局面を迎えた、などのきっかけがあります。そのため、当社が観測した脅威の種類には、大局的な脅威動向が必ずしも反映されていない可能性があります。このような制限はあるものの、インシデント対応案件で得られたデータを解析することにより、「攻撃者がいかにしてネットワークを侵害するのか」、「攻撃者の活動が標的組織にどのような影響を及ぼすのか」、さらには「こうしたインシデントをどのようにすれば防げるのか」という点において有益な情報が得られます。

主なポイント：

単一要素認証ベースのソリューションを不正利用して標的組織のネットワークにアクセスするランサムウェア攻撃グループを複数確認

標的組織の内部で足掛かりを固めたい攻撃者にとって、インターネット接続デバイスの脆弱性は格好のターゲット

当社インシデント対応コンサルタントが介入し、お客様組織の機密データ大量損失・流出を回避した「内部脅威への対応案件」が前四半期の2倍以上に増加



観測された脅威動向

当社CTUリサーチャーが2022年第1四半期のインシデント対応案件を精査し、攻撃者、脅威の種類、初期アクセス取得に用いる攻撃手法（IAVs）の動向を以下のとおり取りまとめました。

脅威の種類

金銭目的の脅威は、これまでと変わらず観測された脅威の大半を占めています。その一例が、ランサムウェア、ビジネスメール詐欺（BEC）、仮想通貨マイニングです（図1）。サイバー犯罪者の活動は、企業規模や収益額を問わず、様々な組織に影響を及ぼしています。

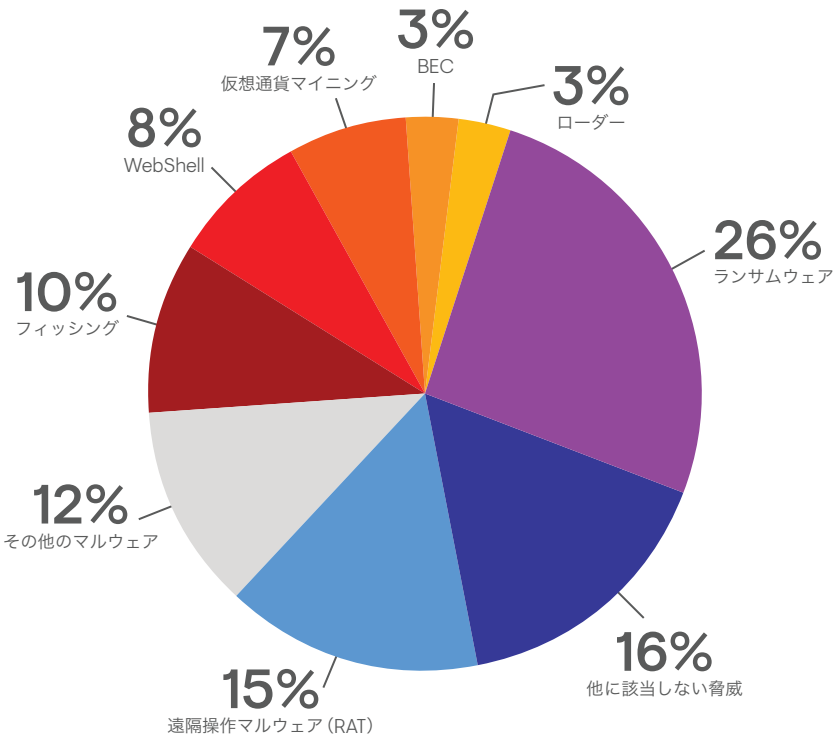


図1：2022年第1四半期の当社インシデント対応案件で観測された脅威（出典：Secureworks）

初期アクセス取得に用いる攻撃手法（IAVs）

前四半期の傾向と同様、最も多用されたIAVは、「インターネット接続デバイスの脆弱性の悪用」でした（図2）。サービス管理ソリューションManageEngineの認証バイパスに関する不具合など、新たに公表された脆弱性が悪用されています。さらに、パッチ未適用のまま放置されている既存の脆弱性（Microsoft Exchangeサーバーに影響を及ぼす脆弱性ProxyShellなど）も攻撃者に悪用されています。

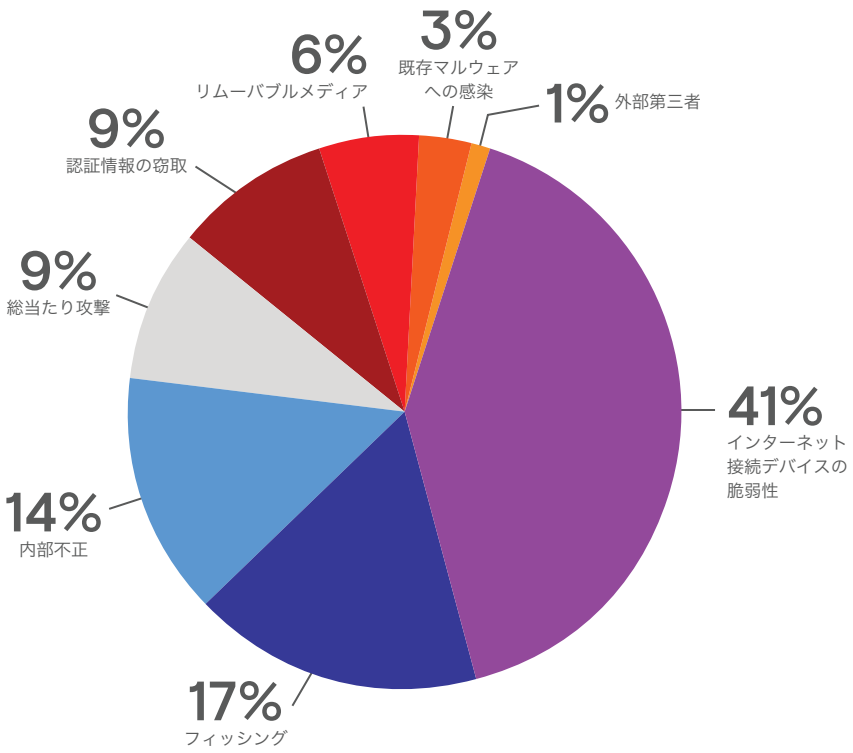


図2：2022年第1四半期に観測されたIAVの内訳（出典：Secureworks）

観測されたIAVおよび該当する MITRE ATT&CKカテゴリの対比表

下表は、前述のIAVをMITRE ATT&CK®の各カテゴリにマッピングしたものです。このナレッジベースの情報をもとに脅威インテリジェンスデータを整理・分類し、実際の業務にお役立てください。

初期アクセス取得に用いる攻撃手法（IAV）	MITRE ATT&CK MAPPING 該当するMITRE ATT&CKカテゴリ
インターネット接続デバイスの脆弱性	Exploitation of Remote Services リモートサービスの悪用 Exploit Public-Facing Application 外部公開されたアプリケーションの悪用
認証情報（総当たり攻撃、パスワードスプレー攻撃、認証情報の窃取）	Valid Accounts 正当なアカウント Brute Force 総当たり攻撃
悪質なメール	Phishing フィッシング Spearphishing Attachment 添付ファイル型スピアフィッシング Spearphishing Link リンク型スピアフィッシング Spearphishing via Service サービスを利用したスピアフィッシング
外部第三者によるアクセス	Supply Chain Compromise サプライチェーンの侵害 Trusted Relationship 信頼関係
既存マルウェアへの感染	Develop Capabilities 攻撃能力の開発

ケーススタディ

2022年第1四半期に当社が従事したインシデント対応案件のなかで、特に注目すべき事例を以下に掲載します。

ランサムウェア攻撃の足掛かりとなる単一要素認証

あるインシデント対応案件で、多要素認証（MFA）が実装されていない複数の仮想プライベートネットワーク（VPN）アカウントが攻撃者に侵害されたケースがありました。このお客様組織で稼働中のSonicWall製VPNアプライアンス（SMA-500V）にはSQLインジェクションの脆弱性（CVE-2021-20016）が存在していました。当該脆弱性を悪用した攻撃者により、VPNアカウントの詳細情報（ユーザー名、パスワード、セッション関連の情報）が窃取されました。

攻撃グループはその後、認証情報窃取ツール（Mimikatz）およびProcDumpツール（Sysinternals）を実行しました。ProcDumpは、Windows Local Security Authority Server Service（LSASS）プロセスのダンプ時によく使われるツールであり、出力情報が悪用されると認証情報が盗み取られる可能性があります。攻撃者は、侵害したアカウントのひとつにプロキシマルウェア（SystemBC）を展開し、アクセスをさらに確保したうえで、Cobalt Strikeを実行しました。

攻撃の過程では、上記以外にもPrintNightmareの脆弱性（CVE-2021-34527）悪用ツール（PowerShell）、ペネトレーションテストフレームワークのPowerSploit、SoftPerfect Network Scanner、FTP用のFileZilla、クラウドストレージデータ同期ツールのMegaSyncをはじめとする汎用ツールが使われていました。データの窃取にはMegaSyncが用いられたと見られます。情報を窃取した攻撃者の手によって、ランサムウェアLVが投下されました。

パッチ適用の遅れおよびソフトウェアの設定不備によるリスク

パッチ未適用の脆弱性やソフトウェアパッケージの設定不備に起因する複数の侵害事案において、当社のインシデント対応コンサルタントがお客様環境の修復を実施しました。攻撃者は通常、脆弱性実証用の攻撃コードが公開されると同時にインターネットをスキャンし、脆弱そうなシステムを探索します。自社環境で脆弱なシステムがある場合は可及的速やかにパッチを適用し、リスクを最小化しましょう。

2022年第1四半期は、ProxyShellに起因するセキュリティ侵害がWebShell、仮想通貨マイニングマルウェア、ランサムウェアなどの攻撃に発展したケースが複数見られました。原因となった一連の脆弱性（CVE-2021-34473、CVE-2021-34523、CVE-2021-31207）はMicrosoft Exchangeサーバーに影響を及ぼすものであり、2021年8月に公表されました。Microsoft社は4月から5月にかけてセキュリティ更新プログラムをリリースし、これらの問題に対処しましたが、パッチを迅速に適用しなかった、もしくはオペレーション上の理由であえてパッチを適用しなかった組織も見られました。脆弱なシステムは常に、攻撃者によるスキャンおよび攻撃の標的となります。

同様に、ManageEngineに関する重大な認証回避の脆弱性（CVE-2021-40539）が存在するシステムが広範囲にわたりスキャンされていることも当社CTUリサーチャーの調べで確認されています。攻撃者は当該脆弱性を悪用し、ユーザー環境へのアクセスを試みます。2021年9月に開発元が公表した勧告を受け、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）は当該脆弱性を悪用する攻撃に関する警告を発出し、対象ソフトウェアを利用中の組織に対し、ただちにパッチを適用するよう注意を呼びかけました。

2022年第1四半期、当社のインシデント対応コンサルタントは、パッチ適用の遅れにより脆弱性スキャンの被害を受けたお客様組織の支援にも従事しました。このほか、ManageEngineの環境設定に不備があり、デフォルトの管理者アカウントをそのまま使用していたため、攻撃者の標的となったお客様組織も見られました。

パッチ未適用の脆弱性を悪用する、またはデフォルト状態のアカウントを介して標的環境に侵入する攻撃者は通常、WebShellやバックドアの他、遠隔操作マルウェア（RAT）などを投下して接続状態を維持します。その後、権限昇格や、侵害された環境全体の横展開を試みます。

増加傾向にある内部脅威

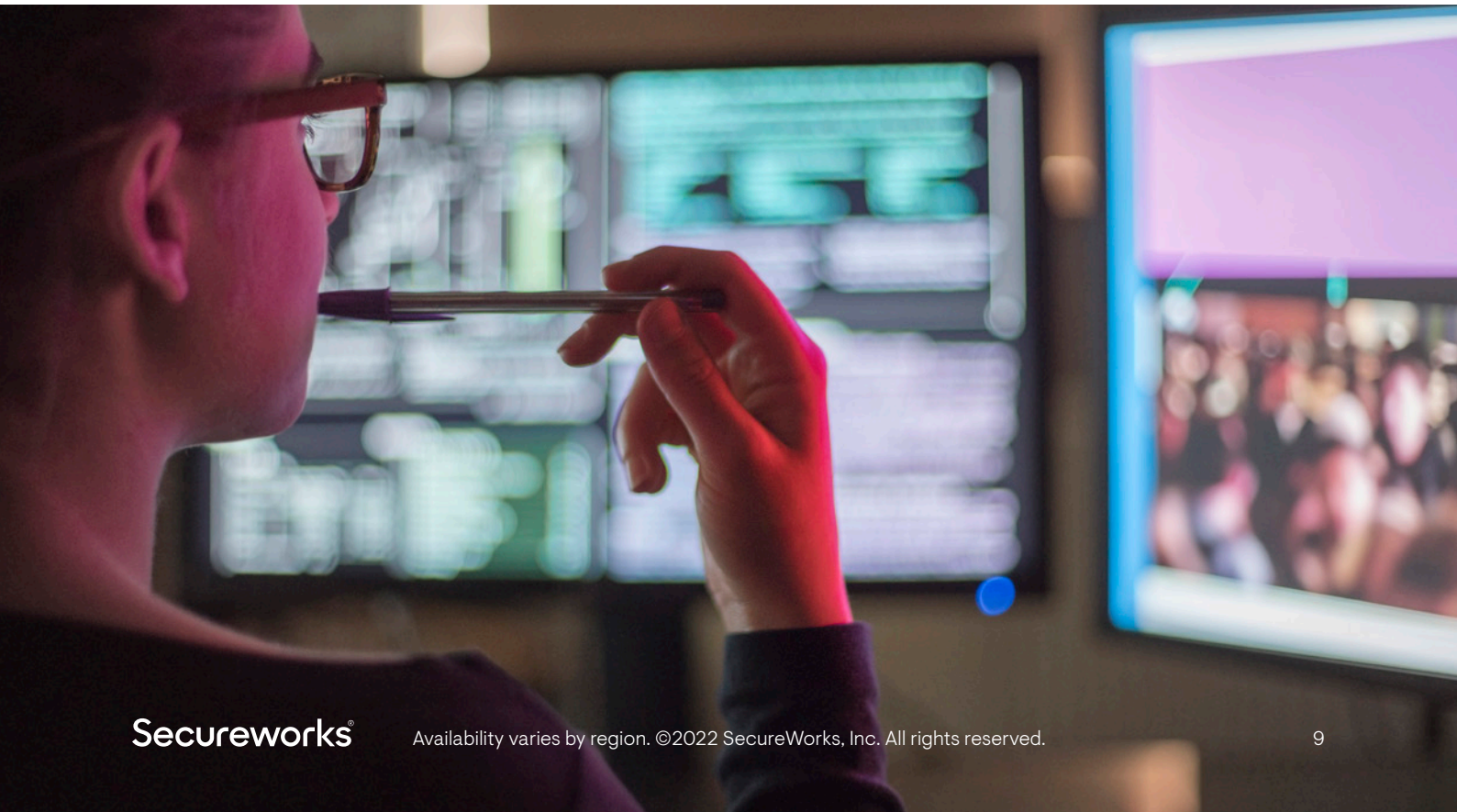
今四半期、当社のインシデント対応コンサルタントが調査した内部不正の事案は、前四半期の2倍以上に増えました。インシデントの約半数は過失によるもので、残り半数が故意によるもの（悪意をもつ内部犯行）でした。

あるインシデントでは、解雇された従業員が元勤務先の機密書類を自身の勤務先宛に送り付けていました。当該組織のデータ損失防止（DLP）システムからアラートが配信されたため、調査に至りました。

この内部犯行者は、セキュリティ対策を迂回するためにオフィス端末の個人用メールを使ったことが当社インシデント対応コンサルタントの調べで判明しました。また、犯行が検知されるまでに窃取された情報の量も判明しました。

内部犯行によるインシデント事例では、解雇されてネットワークアクセス権をはく奪されたリモート勤務社員が、自らの端末のローカルアクセス権限を1ヵ月以上にわたって保持していた、というケースもありました。この間、犯行者はローカル保存されているデータを大量に削除し、自らの犯行を隠蔽しようと試みていました。フォレンジック調査により、USBデバイスやネットワークストレージサービスを使ってデータを削除しようとしていた痕跡が判明しました。当該内部犯行者はさらに、OSファイルロックの迂回も試みていましたが、こちらは失敗に終わっています。

こうしたインシデントを振り返ると、正式な解雇プロセスを制定しておくことが自社の資産を保護する上でいかに重要なのかがわかります。また、データの損失・流出の可能性を検知可能なDLPソリューションの重要性も改めて浮き彫りになりました。



インシデント防止に向けた推奨策

図3は、2022年第1四半期のインシデント対応案件で当社コンサルタントがお客様組織に提言した推奨策の上位項目です。なかでも「多要素認証（MFA）の不備」により、正当な認証情報をもつ攻撃者にさらなる活動を許してしまったケースが多く見られました。また、標的組織内のシステムや環境への初期アクセスの格好の手段として「パッチ未適用のシステム」が悪用されていました。「ログ情報の欠落」も、インシデント対応の阻害要因となっていました。侵害の防止、検知、対応、修復措置の一助としてご参照いただければ幸いです。

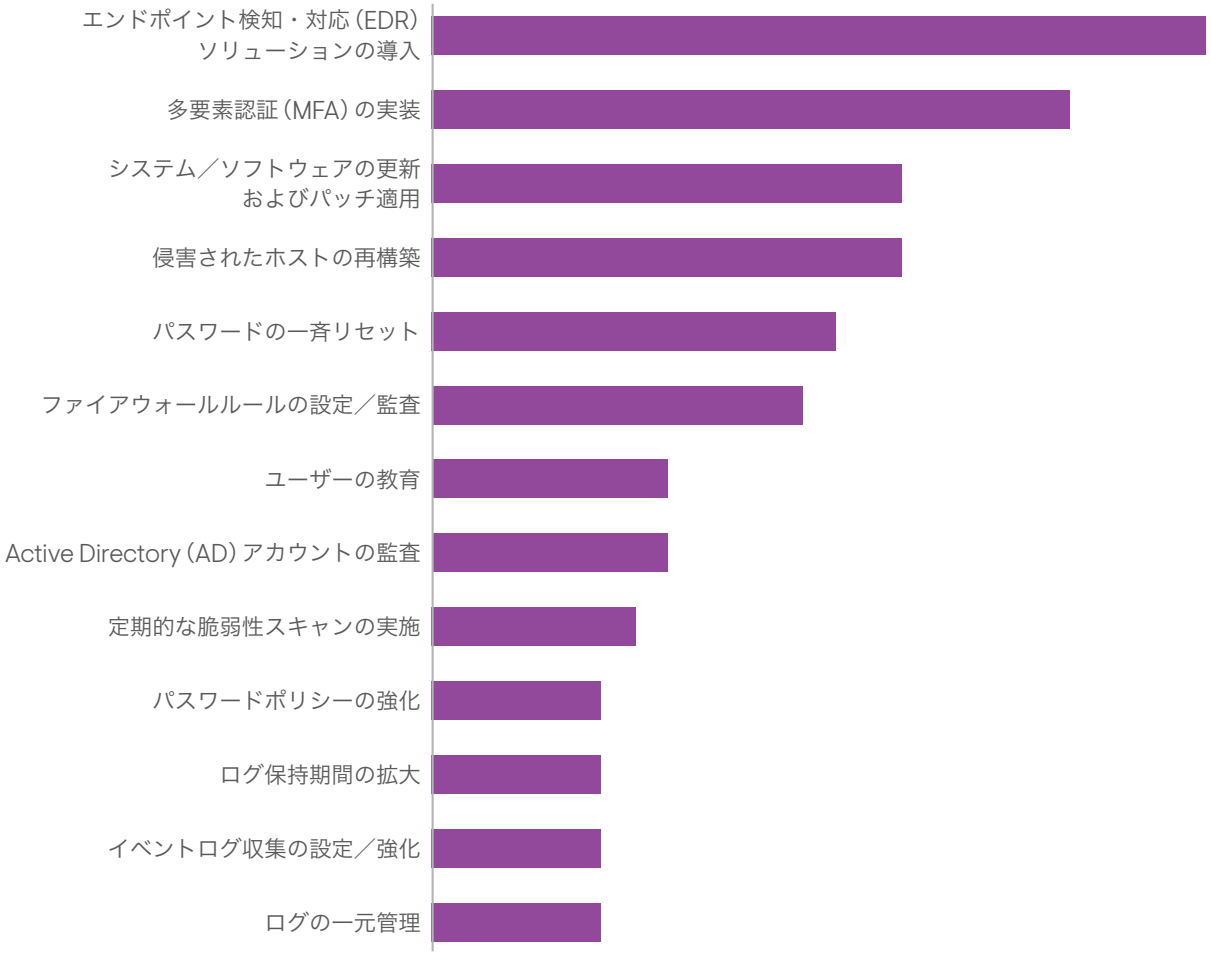


図3：2022年第1四半期のインシデント対応案件でお客様に提言した主な推奨策（出典：Secureworks）

まとめ

当社のCTUリサーチャーは、インシデント対応案件で明らかになった脅威および攻撃者の振る舞いを追跡し、様々な脅威の特性および発展動向の把握に役立てています。当社のCTUリサーチャーおよびインシデント対応コンサルタントは、脅威への対策プログラムの開発、定期的な脅威動向の分析、インシデント対応案件を通じて観測された攻撃活動に関するレポート（実務者向けに随時発行）を通じて、お客様組織を常に保護し、知見を提供すると共に、実際のインシデント対応経験にもとづくガイダンスを提供します。

Secureworks®

Secureworksのインシデント対応サービスについて

広範囲な専門知識、サイバー脅威に関するインテリジェンス、専用テクノロジーを擁するセキュアワークスのインシデント対応チームが、サイバーインシデントの予防対策および発生後の対応を支援します。当社のインシデント対応コンサルタント（コマンダー）が、オンサイト*またはリモート形式で皆様のインシデント対応を支援します（*コロナによる渡航制限の影響を受ける可能性あり）。緊急インシデント対応サービス、脅威ハンティングによるアセスメント、机上演習、その他様々なインシデント事前準備サービスを通じ、当社の専門家がお客様の社内チームと密接に協力します。これらはすべて、お客様組織におけるインシデント対応プログラムの策定、大規模インシデントの効果的・効率的な解決を目的としたサービスです。

Secureworksについて

Secureworks（NASDAQ：SCWX）は、20年以上にわたり実環境で蓄積された脅威インテリジェンスとリサーチに基づき構築されたクラウトネイティブのセキュリティ分析プラットフォームSecureworks®Taegis™により、高度な脅威の検知、合理化された協調モデルによる調査、また脅威に対する適切なアクションを自動的に実施する能力を強化し、お客様のビジネスを保護するサイバーセキュリティのグローバルリーダーです。

www.secureworks.com

出典

ManageEngine. “Security advisory - ADSelfService Plus authentication bypass vulnerability.” September 7, 2021.

Secureworks. “LV Ransomware.” June 22, 2021.

Tsai, Orange. “From Pwn2Own 2021: A New Attack Surface on Microsoft Exchange - ProxyShell!” Zero Day Initiative. August 18, 2021.

U.S. Cybersecurity & Infrastructure Security Agency. “APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus.” November 22, 2021.