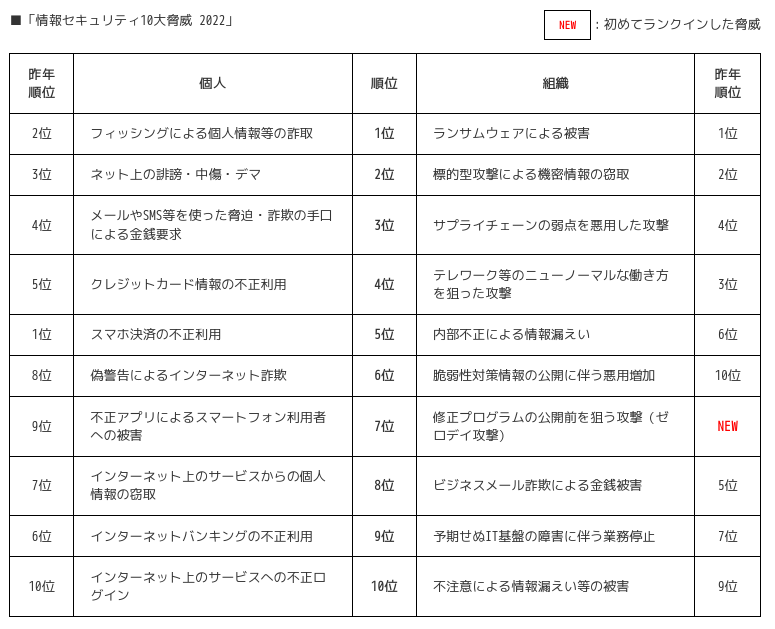
2022 Q1セキュリティ脅威動向まとめ

## まえがき

2022も5ヶ月を過ぎ、既に2022Q1でのセキュリティ上の脅威や脆弱性、また悪用されたインシデントが各社・各メディアから報告されています。本レポートでは各社の情報から代表的なものを抜粋し、2022Q1で世界的にどの様なセキュリティ上の問題が起きていたのか・またどの様な攻撃がトレンドでどの様に対策をしていけばよいかを纏めています。

## 当初予想されていた2022の脅威動向

IPAでは、2021の時点で2022に予想される脅威動向を「10大脅威」として発表していました。



（参考： IPA [情報セキュリティ10大脅威 2022](https://www.ipa.go.jp/security/vuln/10threats2022.html)）

こちらによると、2022年に発生し得るであろう脅威動向としては

1. 2021年末のLog4jの脆弱性（log4shell）から注目を集めるようになった、修正プログラム公開前を狙う悪用増加
2. 2021年に起きたPulseSecure VPNの脆弱性／Windows PrintSpoolerの脆弱性（PrintNightmare）等に代表されるゼロデイ攻撃
3. サプライチェーンの弱い箇所を利用した攻撃
4. ランサムウェア攻撃

などが重大脅威として注目を浴びることになるだろうと予想されていました。

## 2022Q1の脅威動向概略

2022Q1は、当初予想していなかったロシア・ウクライナの紛争が始まったことにより、セキュリティ関係でもロシア・ウクライナに起因した攻撃のニュースが大半を占める状態となっています。

一方で、IPAが予想していたとおりの攻撃も増えてきており、

* サプライチェーンを狙った攻撃
* ランサムウェアを使った攻撃
* 脆弱性公開直後を狙った攻撃

などが発生しています。

以降、

1. 2022Q1でのロシア・ウクライナ紛争に起因する攻撃
2. 2022Q1で発生した代表的なインシデント
3. 2022Q1に公開された脆弱性の推移と、重大な脆弱性

に分けて順番に見ていきたいと思います。

## 2022Q1でのロシア・ウクライナ紛争に起因する攻撃

2022Q1ではロシア・ウクライナ紛争に関連したサイバー攻撃が増加しました。

### I. SNS上での攻撃（Meta 2022Q1情報）

SNS上では虚偽情報を用いた世論誘導やヘイト行為などの攻撃が見受けられました。

* ウクライナ対象にした虚偽の情報 & ロシアを対象にした虚偽の情報
* ウクライナ紛争の情報を偽って、経済活動（動画再生数や広告収入・商品購入）への誘導を試みるSPAM
* ロシア／ウクライナへのヘイト行為を目的としたアカウント乗っ取り

### II. DDoS攻撃（Kaspersky 2022Q1情報）

通常DDoS攻撃は、動機が経済的なもの（企業への攻撃や脅迫等）であればすぐにDoSのセッションを切る傾向にあります。

しかし2022Q1では、長期的にDoSセッションを繋ぎっぱなしにする傾向がみられました。このことから、2022Q1のDDoS攻撃の多くが経済的な動機ではなかったことが伺えます。

DDoS攻撃の中では、直接的にロシア・ウクライナ双方の重要インフラや官公庁をターゲットとした攻撃も行われました。また、それらの攻撃に便乗して経済活動やユーザの個人情報取得を行うような活動も行われています。

* ウクライナに対するDDoS攻撃は最大100GB/s
  + 2021年のネット上での観測最大値は1TB/sの為、それに比べると意外に少ない
  + ウクライナ国防省のWebサイト、OschadbankとPrivatBankのオンラインサービス、ホスティングプロバイダーのMirohostに影響を及ぼした（パニックを起こす為）
  + DanaBot/MaaSによる国防省メールサーバへの攻撃（3月）
* ロシアへのDDoS攻撃
  + Anonymousによる攻撃
  + ロシア国営企業（[Rostec）のWebサイトがDDoS攻撃のためダウン](https://www.bleepingcomputer.com/news/security/russian-defense-firm-rostec-shuts-down-website-after-ddos-attack/)
  + 攻撃をゲーム化することで攻撃の敷居を下げる
    - [ロシアに対するウクライナからのサイバー攻撃キャンペーンを装った攻撃（不正な情報の取得）](https://www.bleepingcomputer.com/news/security/malware-disguised-as-security-tool-targets-ukraines-it-army/)

以下、Kaspersky社による2022Q1のDDoSの特徴になります。

1. KasperskyDDoSインテリジェンスシステムは91,052のDDoS攻撃を検出しました。
2. 攻撃の44.34％は、全ターゲットの45.02％を占める米国にあるターゲットに向けられました。
3. DDoS攻撃の最大数（16.35％）は、日曜日に発生します。
4. ほとんどの攻撃（94.95％）は4時間未満続きましたが、最長の攻撃は549時間（約23日）続きました。
5. 攻撃の53.64％はUDPフラッドでした。
6. C＆Cサーバーの55.53％は米国にありました。
7. 中国は、SSHハニーポットを攻撃するボットの20.41％、Telnetトラップを攻撃するボットの41.21％を占めています。

また、2022Q1では、一つのパケットを40億倍に増幅する、DDoS攻撃に使用できる脆弱性が見つかりました。この脆弱性が攻撃に使われていた可能性もあります。

1. 2022年3月に見つかった「TP240 電話機」の脆弱性(CVE-2022-26143)は、一つの通信を4,294,967,296(約40億)倍に増幅させることが出来、金融／ロジスティクス相手のDDoS攻撃として使用された（[アカマイのブログ](https://www.akamai.com/blog/security/phone-home-ddos-attack-vector)）

### III. 改ざんその他（各種ニュースサイト情報）

* ウクライナ省庁の改ざん（1月）
* [ウクライナの慈善活動団体・援助団体へのマルウェア攻撃](https://www.bleepingcomputer.com/news/security/amazon-charities-aid-orgs-in-ukraine-attacked-with-malware/)（３月）
* [ロシア政府のサイトがサプライチェーン攻撃のためダウン](https://www.bleepingcomputer.com/news/security/russian-government-sites-hacked-in-supply-chain-attack/)

参考情報)

[Meta Quarterly Adversary](https://about.fb.com/news/2022/04/metas-adversarial-threat-report-q1-2022/)

[Kaspersky DDoSレポート](https://securelist.com/ddos-attacks-in-q1-2022/106358/)

## 2022Q1に発生したインシデント

2022Q1に発生したインシデントは幾つかあります。代表的なものを取り上げてみましょう。

1. サプライチェーン攻撃
   1. TOYOTAへのサプライチェーン攻撃と思われるもの
      1. [TOYOTA](https://www.bleepingcomputer.com/news/security/toyota-halts-production-after-reported-cyberattack-on-supplier/)のサプライチェーン「小島プレス工業」への[攻撃](https://www.nhk.or.jp/politics/articles/lastweek/79950.html)（2022年2月）
      2. [ブリジストン・アメリカへのランサムウェア(Lockbit)攻撃](https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/) （2022年2月）
      3. [DENSO(ドイツ)のランサムウェア(Pandora)攻撃](https://www.bleepingcomputer.com/news/security/automotive-giant-denso-hit-by-new-pandora-ransomware-gang/)（2022年3月）
2. ランサムウエア攻撃
   1. [Taiwan Apple/Teslaへのランサムウェア](https://www.bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/)(Conti)攻撃 (2022年1月)
   2. Monclerへの[ランサムウェア（ ALPHV/BlackCat）攻撃](https://www.bleepingcomputer.com/news/security/fashion-giant-moncler-confirms-data-breach-after-ransomware-attack/) (2022年1月)
   3. [BlackByteランサムウェアグループ](https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/)によるUS政府への攻撃 (2022年2月)
   4. [Mizunoに対するランサムウェア(不明)攻撃](https://www.bleepingcomputer.com/news/security/sports-brand-mizuno-hit-with-ransomware-attack-delaying-orders/) (2022年2月)
   5. [KPスナックへのConti](https://www.bleepingcomputer.com/news/security/kp-snacks-giant-hit-by-conti-ransomware-deliveries-disrupted/)ランサムウェア攻撃 (2022年2月)
   6. コカ・コーラへのランサムウェア攻撃（Stormous Ransomware Group）（2022年4月）による情報流出
3. 情報流出
   1. アクセス管理システム会社[OKTA に対するLapsus$からの攻撃によるクレデンシャル流出](https://www.bleepingcomputer.com/news/security/okta-confirms-25-percent-customers-impacted-by-hack-in-january/) (2022年1月)
   2. Samsungに対するLapsus$からの攻撃[（190GB、Galaxyのソースコードも含まれる盗難）](https://www.bleepingcomputer.com/news/security/samsung-confirms-hackers-stole-galaxy-devices-source-code/)。[こちらも](https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/)参照。 (2022年3月)
   3. [Adafruit](https://www.bleepingcomputer.com/news/security/adafruit-discloses-data-leak-from-ex-employees-github-repo/)からのGithub経由のコード流出 (2022年3月)
   4. NVIDIAに対するLapsus$からの攻撃での[クレデンシャル](https://www.bleepingcomputer.com/news/security/nvidia-data-breach-exposed-credentials-of-over-71-000-employees/)流出 (2022年3月)
   5. [British Council](https://www.bleepingcomputer.com/news/security/british-council-exposed-more-than-100-000-files-with-student-records/)からのデータ漏洩 (2022年2月)
4. その他
   1. 赤十字への攻撃[（Zohoのバグ）](https://www.bleepingcomputer.com/news/security/red-cross-state-hackers-breached-our-network-using-zoho-bug/)(2022年2月)
   2. Vodaphoneポルトガルへの[サイバー攻撃](https://www.bleepingcomputer.com/news/security/vodafone-portugal-4g-and-5g-services-down-after-cyberattack/) (2022年1月)
   3. [Windows11への更新サイトを偽装](https://jp.ext.hp.com/blog/security/product/redline-stealer-disguised-as-a-windows-11-upgrade/)しマルウェアRedLine Stealerを仕込む (2022年1月)
   4. 東映への[不正アクセスによるシステム障害（**業務利用するソフトのダウンロード先の改ざん）**](https://www.bleepingcomputer.com/news/security/new-one-piece-anime-episodes-delayed-after-toei-cyberattack/) (2022年4月)

上述は代表的なインシデントであり、その他にも多くのインシデントが発生しています。これらからわかるところでは

* サプライチェーンを対象とした攻撃（ここではTOYOTAに関連したサプライチェーン）が目立つ。
* クレデンシャル流出が目立っており、OKTAやNVIDIA製品を使用しているユーザサイトへの二次被害も懸念される。この中で中心的に動いている攻撃者は「Lapsus$」というグループになっている。
* サプライチェーンを狙った攻撃を含めて、ランサムウェアを用いた攻撃が目立っている。特にConti/LockBit/ALPHVが目立っている。

となっています。

それぞれのカットで見てみましょう。

#### I. TOYOTAに関連したサプライチェーン攻撃の状況

TOYOTAに関連したサプライチェーン攻撃は2022Q1だけでも

1. 小島プレス工業
2. ブリジストン
3. DENSO

が対象となっています。それぞれのインシデントの概略は下記になります。

1. 小島プレス工業

2022年02月26日夜、社内サーバーの障害を検知し、ウイルス感染と脅迫メッセージを確認した。同２７日、再攻撃を防ぐため、外部とのネットワークを遮断。トヨタと部品の受発注などをやりとりするシステムも停止したため、納入業務が滞ったという。

[同社プレスによる経緯説明](https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E9%9A%9C%E5%AE%B3%E8%AA%BF%E6%9F%BB%E5%A0%B1%E5%91%8A%E6%9B%B8%EF%BC%88%E7%AC%AC1%E5%A0%B1%EF%BC%89.pdf)としては「子会社が独自に特定外部企業との専用通信に利用していたリモート接続機器に脆弱性があり、そのことがきっかけとなり不正アクセスを受けました。攻撃者はそのリモート接続機器から子会社内のネットワークに侵入し、さらに当社（小島プレス社）内ネットワークへ侵入して、 2月26日20時過ぎにサーバやパソコン端末へ攻撃を受けた」としている。本件に付随した情報漏えいは現在の所確認されていない。

1. ブリヂストン・アメリカ

2022年03月11日、ブリヂストン・アメリカは02/27の朝に「潜在的な脅威インシデント」が検出され調査を行っていることを明らかにした。

これは同日にLockBitランサムウェアの攻撃者が「攻撃と情報漏えいが行われたこと」をダークウェブ上で公開した為である。

ブリジストン・アメリカによると、アクセンチュアセキュリティと協力して調査を行い、連邦政府にも報告を行っているということである。この調査の結果、実際にLockBitランサムウェアによる攻撃と情報漏えいが行われていたことを確認している。実際にどれだけのデータが盗み出されたのかなどは明らかにされていない。

1. DENSO

2022年03月14日、自動車技術、システム・製品を提供するDENSO社は、3/10にDENSO ドイツ支社にPandoraランサムウェアによる攻撃が発生した事、感染システムはすぐにネットワークより遮断したため影響はないとの発表を行った。

一方で、Pandoraランサムウェアを用いたグループにより、DENSO社から発注書／技術回路図／非開示契約書などを含む1.4TBのデータを盗み出したこと、またこれを03/16に公開するとの声明が出された。

DENSO社は、当該1.4TBのデータがDENSOドイツ支社から盗み出されたデータかどうかを、2022/06/23現在確認している。

Pandoraランサムウェアは2021年に確認されたRookランサムウェアに酷似しており、このRookランサムウェアのリブランディングがPandoraランサムウェアではないかと推測されている。また、Rookランサムウェアは2021年に活動を停止しビルダーが公開されたBabukランサムウェア（Babuk Locker, Babyk Locker, Babyk Ransomware）を使用しているのではないかと推測されるため、PandoraランサムウェアもBabukランサムウェアが基になっていると推測されている。

参考情報)

[小島プレスシステム障害調査報告書（第1報）](https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E9%9A%9C%E5%AE%B3%E8%AA%BF%E6%9F%BB%E5%A0%B1%E5%91%8A%E6%9B%B8%EF%BC%88%E7%AC%AC1%E5%A0%B1%EF%BC%89.pdf)

[Bridgestone Americas confirms ransomware attack, LockBit leaks data](https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/?_x_tr_sl&_x_tr_tl&_x_tr_hl)

[Automotive giant DENSO hit by new Pandora ransomware gang](https://www.bleepingcomputer.com/news/security/automotive-giant-denso-hit-by-new-pandora-ransomware-gang/)

#### II. Lapsus$が中心となったクレデンシャル流出

Lapsus$ Group (別名：DEV-0537, UNC3661)は、2021年12月以来、ポルトガルとブラジルの組織を積極的に標的にしており、2022年に入ってからは世界中を標的にしています。

標的となった主なものは以下になります

* Microsoft
  + 従業員１名のアカウントを侵害し、そこから侵入。[盗み出した37GBのソースコードを公開](https://www.bleepingcomputer.com/news/microsoft/lapsus-hackers-leak-37gb-of-microsofts-alleged-source-code/)
* NVIDIA
  + [クレデンシャルを含む1TBのデータを盗み出したとして公開](https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/)
* Samsung
  + [190GBのデータを盗み出したとして公開](https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/)
* Okta
  + [サポートエンジニア1名のラップトップを侵害し、そこから侵入](https://www.bleepingcomputer.com/news/security/okta-confirms-25-percent-customers-impacted-by-hack-in-january/)
* T-Mobile
  + [以前に漏洩していたアカウントの情報、またソーシャルエンジニアリングを用いてアカウントを突破し侵入](https://www.securitymagazine.com/articles/97492-t-mobile-is-latest-lapsus-breach-victim)

等になります。これらの例からわかるとおり、彼らは主にソーシャルエンジニアリングを用いて攻撃を行っています。

種々のセキュリティベンダーの調査により、Lapsus$に関しては以下の情報がわかっています。

* Lapsus$グループは専門的なランサムウェアギャングではなく、金銭的な動機からデータの恐喝を専門とする低レベルの脅威グループ（所謂スクリプトキディ）であると考えられます。
* Lapsus$グループの管理者は、現在英国（UK）に住んでいる16歳のアルバニア人男性でハンドルネーム「White」氏だと特定されています。
* Palo-Altoの調査によると、Lapsus$グループは侵入された被害環境ではマルウェアを使用せず、データを暗号化することもありません。ほとんどの場合、実際に恐喝を行うこともありません。
* Lapsus$の興味はもっぱら、窃取した認証情報(クレデンシャル)とソーシャルエンジニアリングを組み合わせ、被害組織へのアクセスを得ることにあります。

Lapsus$グループに関与したとして、3月には首謀者の「White」氏を含む7名のティーンエイジャーが逮捕されています。

彼らはスクリプトキディとして活動していたため直接的な被害があまり見られない様に見えますが、リークされた情報はクレデンシャル等を含んでいたため二次的な被害がかなり出ています。例えば、既に彼らからリークされた[NVIDIAのコード署名証明書を用いたマルウェアも出現](https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/)しています（これは署名上正常なNVIDIAドライバの様に見えるため、Windowsにインストールされてしまいます）。

これら一連の攻撃から判明したことは、どんなにセキュリティを強化したとしても、一番弱い箇所は人間であり、ソーシャルエンジニアリングを用いて破られてしまうということです。そのため、人間に対してのセキュリティ教育を高めると共に、ログイン等に関しては少なくともMFA（多要素認証）を使用して、クレデンシャルが流出したとしても被害を最小限にすることが必要となります。

参考情報)

[Lapsus$: The script kiddies are alright](https://therecord.media/lapsus-the-script-kiddies-are-alright/)

[脅威に関する情報: Lapsus$グループ](https://unit42.paloaltonetworks.jp/lapsus-group/)

[10代の若者が中心の国際的ハッカー集団「LAPSUS$」が通信大手・T-Mobileのソースコードを盗んだと判明](https://gigazine.net/news/20220426-lapsus-stole-t-mobile-source-code/)

[Lapsus$ hackers leak 37GB of Microsoft's alleged source code](https://www.bleepingcomputer.com/news/microsoft/lapsus-hackers-leak-37gb-of-microsofts-alleged-source-code/)

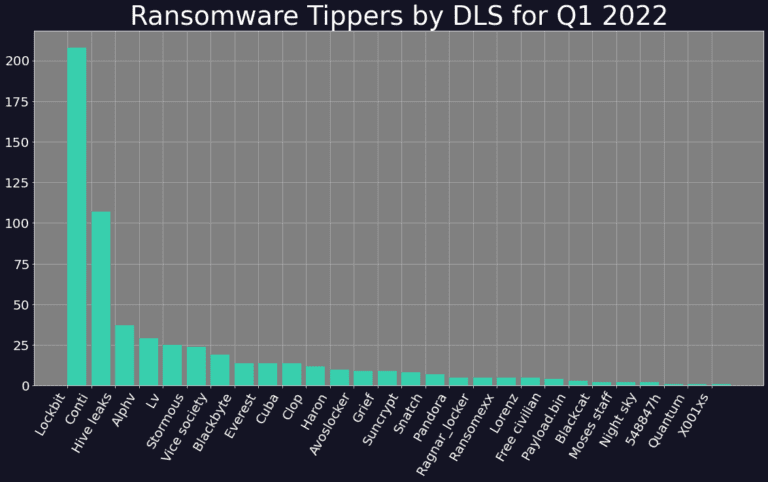
[Okta confirms 2.5% customers impacted by hack in January](https://www.bleepingcomputer.com/news/security/okta-confirms-25-percent-customers-impacted-by-hack-in-january/)

#### III. ランサムウェアによる攻撃（暗号化、情報流出）

2022Q1でも攻撃にはランサムウェアが広く使われています。特に2022Q1では

* Conti (Contiグループが背後にいます)
* LockBit 2.0 (LockBitグループが背後にいます)

が目立っています。[Digital Shadows](https://www.digitalshadows.com/blog-and-research/q1-2022-ransomware-roundup/)により、2022Q1では「LockBit 2.0」と「Conti」合わせてインシデント全体の58％を占めていたとの分析結果が出ています。

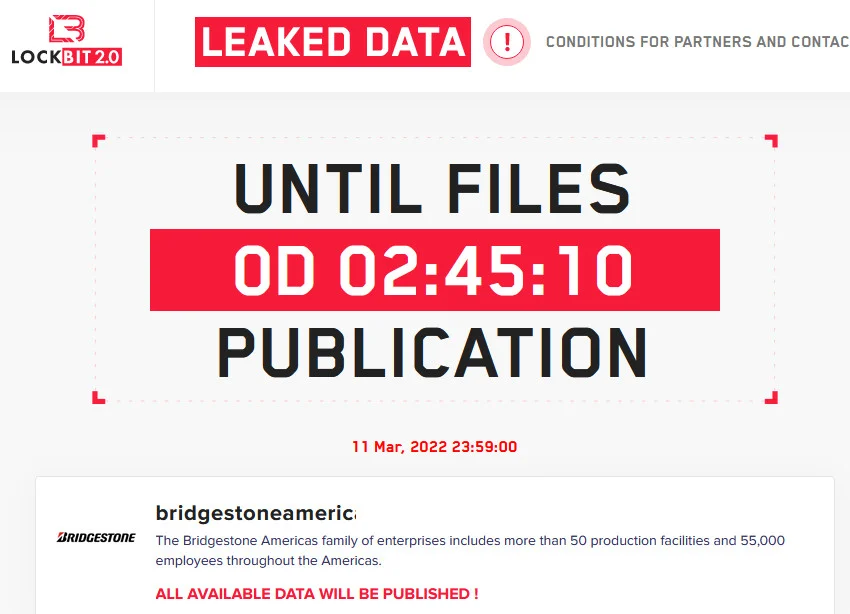


(画像：Digital Shadows [Q1 2022 Ransomware Roundup](https://www.digitalshadows.com/blog-and-research/q1-2022-ransomware-roundup/)より引用)

これらのランサムウェアは「二重脅迫型ランサムウェア（double extortion ransomware）」と呼ばれるものになります。つまり

* 「復号化に対する身代金」を要求する
* 「身代金支払いが遅れた場合には少しずつデータを漏洩させる」として、実際に少しずつ漏洩させていく

というものになり、単に暗号化されたデータの復号化が問題になるだけでなく、データの漏洩も問題になっていくため、対処する企業側としては頭の痛い状態になっています。



(参考：[BridgeStone Americaを標的にしたLockBit 2.0の「公開脅迫」画像](https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/)。)

1. Conti

Contiランサムウェアは2020年5月に初めて確認されたもので

Ransomware-as-a-Service（RaaS）を利用して作られたものになります。

Contiランサムウェアの開発グループは、様々なセキュリティ製品の無償アカウントを取得して迂回する方法を探していたようです。[2020年5月には有償製品のライセンスを購入しようとしてウクライナのキエフにあるDocSoftという会社をでっち上げています](https://news.sophos.com/ja-jp/2022/03/04/countermeasures-and-observability-key-to-defending-against-attackers-trying-to-buy-security-products-jp/)（購入には失敗したようです）。

2022/02/25にConti は、ロシアのウクライナ侵攻の支持を宣言しました。その後 2022/02/27にウクライナの研究者と思われる人物が、Conti のメンバー間で交わされたグループ内のやり取りをTwitter アカウント「ContiLeaks」を使ってリークしました。

Contiランサムウェアの内部構造に関しては、こちら[の三井物産セキュアディレクション(MBSD)のブログ「Contiランサムウェアの内部構造を紐解く」](https://www.mbsd.jp/research/20210413/conti-ransomware/)で詳しくかつわかりやすく説明されています。

また、前述の流出したチャットを分析することにより、内部でのやり取りや構造の説明が「[KELAインテリジェンスレポート](https://ke-la.com/wp-content/uploads/2022/05/KELA-Intelligence-Report-ContiLeaks-JA-1.pdf)」から見ることが出来ます。

1. LockBit(2.0)

LockBitは、2020年1月前後にロシアのアンダーグラウンドフォーラム上に登場したことが確認されています。LockBitグループは2021年6月、彼らのランサムウェアサービス（RaaS）を「LockBit 2.0」に更新し新たな宣伝活動を始めました。

「LockBit2.0」はリークサイトを持つ暴露型ランサムウェアです。LockBit2.0のリークサイト上では、いきなり盗取データが暴露されるのではなく、「被害組織名」とともに「暴露までの残り時間」をリアルタイムでカウントし、被害組織に圧力をかけます。そのためリークサイトに掲載された時点においては、被害組織と攻撃者間で交渉の前段階か実際に交渉が行われている段階かだと考えられています。

LockBit 2.0の攻撃には、VMWareの仮想化ソフトウェアである「ESXi」の脆弱性が利用されており、最近では「Windows」PCだけでなくLinuxサーバーも標的にされています。すでに、Accentureや、フランス司法省などがこのランサムウェアの被害に遭ったとみられています。FBIもLockBit 2.0に対して[注意を呼びかけています。](https://www.ic3.gov/Media/News/2022/220204.pdf)

LockBit 2.0の背後にいるLockBitグループは、「グループはロシア人やウクライナ人が多数を占めるが、米国や中国、カナダ、スイスなどにもメンバーがいる。私たちは皆、単純で平和な地球人」などとして、[どんな状況においても国際紛争には加担しない方針を示しています](https://www.itmedia.co.jp/news/articles/2202/28/news175.html)。

LockBitランサムウェアの内部構造に関しては、こちら[の三井物産セキュアディレクション(MBSD)のブログ「LockBitランサムウェアの内部構造を紐解く」](https://www.mbsd.jp/research/20211019/blog/)で詳しくかつわかりやすく説明されています。

参考情報)

[Q1 2022 Ransomware Roundup](https://www.digitalshadows.com/blog-and-research/q1-2022-ransomware-roundup/)

[Contiランサムウェアの内部構造を紐解く](https://www.mbsd.jp/research/20210413/conti-ransomware/)

[KELAインテリジェンスレポート](https://ke-la.com/wp-content/uploads/2022/05/KELA-Intelligence-Report-ContiLeaks-JA-1.pdf)

[Conti グループのチャットから、セキュリティ製品を購入・分析しようとする試みが明らかに](https://news.sophos.com/ja-jp/2022/03/04/countermeasures-and-observability-key-to-defending-against-attackers-trying-to-buy-security-products-jp/)

[「LockBit 2.0」のランサムウェア攻撃が拡大中。日本にも被害を及ぼす攻撃活動を解説](https://blog.trendmicro.co.jp/archives/28572)

[ランサムウェア「LockBit 2.0」、FBIが注意喚起--推奨されるリスク軽減策など提示](https://japan.zdnet.com/article/35183221/)

[Indicators of Compromise Associated with LockBit 2.0](https://www.ic3.gov/Media/News/2022/220204.pdf)

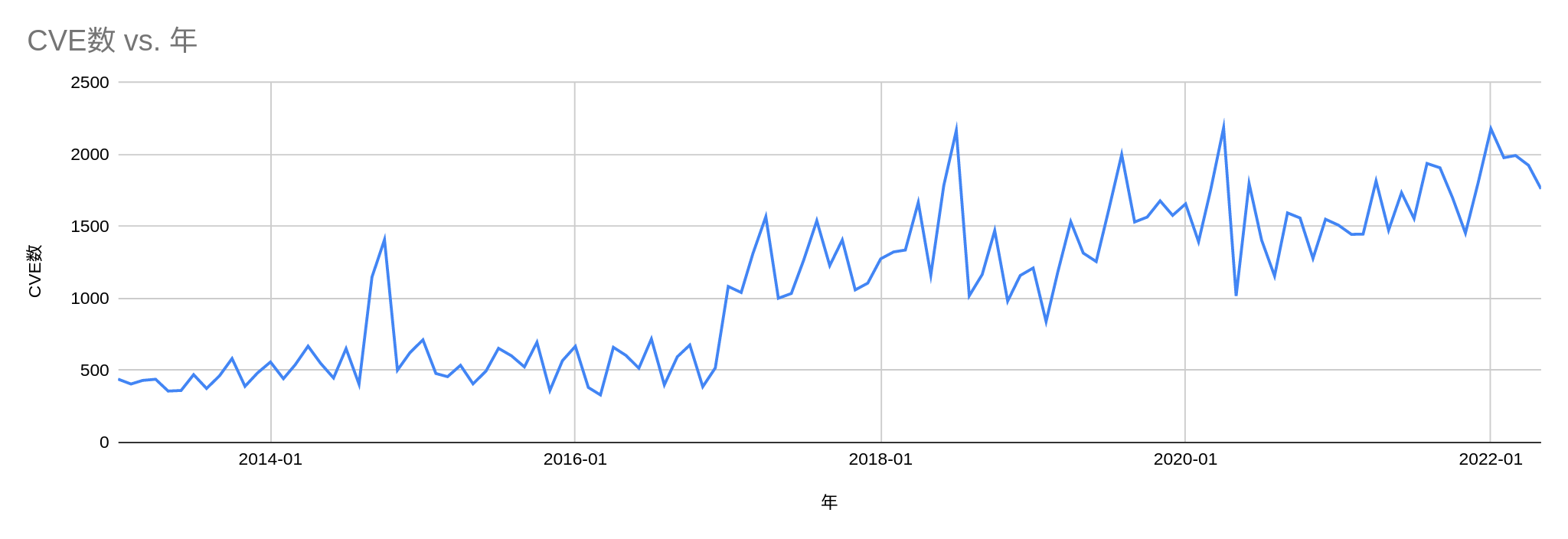
[ランサムウェア集団「Lockbit 2.0」、ロシアのウクライナ侵攻に関与しないと声明　「無害な仕事から得る金銭にしか興味がない」](https://www.itmedia.co.jp/news/articles/2202/28/news175.html)

## 2022Q1に公開された脆弱性（CVE）の推移と、重大な脆弱性一覧

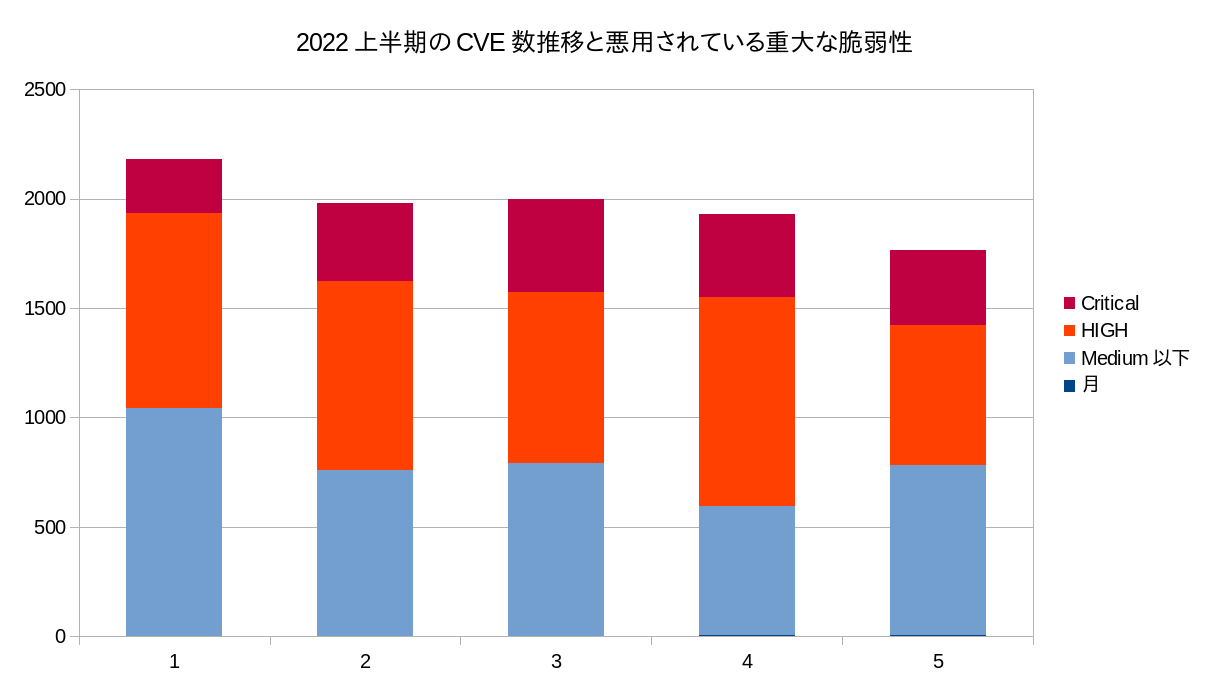
2022Q1も様々な危険な脆弱性が公開されています。ここではCVEの推移と重大な脆弱性、また悪用の度合いを見てみたいと思います。

### I. 2022Q1でのCVE数の推移

まず全体的なトレンドを見てみましょう。2014年からの発行・公開されたCVE数の推移をグラフにしています。月ごとに発行されるCVE数は全体的なトレンドとして右肩上がりになっていることがわかります。

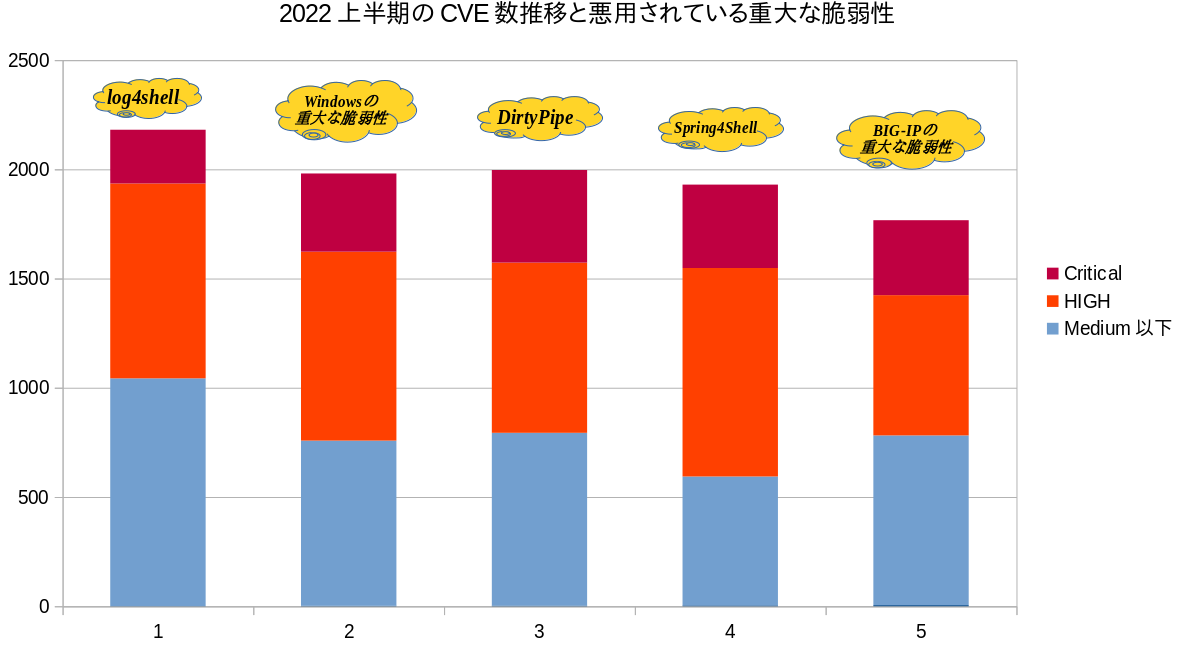


更に2022の1月〜5月に掛けて公開されたCVE数の推移と、その中でも(NISTのスコアリングで)HIGH/Criticalにされたものの数を下の図で見てみます。



2022は毎月約2000件近くのCVEが公開されていることがわかり、その中でもHigh/Criticalの脆弱性が半数近くを締めていることがわかります。

この図に、更に直近で公開された危険な脆弱性を重ね合わせてみます。

この様に2022Q1では毎月重大な（一部のものは既に悪用されている）脆弱性が公開されていることがわかります。

### II. 2022Q1での重大な脆弱性

#### Spring4Shell

* 1. 脆弱性内容 ([SIOSセキュリティブログより](https://security.sios.com/vulnerability/spring4shell-vulnerability-20220401.html))

03/31/2022にSpring Frameworkの脆弱性(Spring4Shell / SpringShell : CVE-2022-22965)が公開されました。PoCも同時に公開されており、2021年末に発生したLog4Shellの脆弱性と比較されている方も多く見られ、情報も錯綜しました。今回は、こちらで脆弱性の情報等を纏めて取り上げていきます。

JDK 9以上で動いているSpring MVC又はSpring WebFluxアプリケーションにリモートコード実行(RCE)の脆弱性となっています。エクスプロイトが動くには、アプリケーションがTomcat上でWARデプロイメントで動作している必要があります。アプリケーションがSpring Bootで実行可能なjarファイル（こちらがデフォルトです）で動いている場合には、エクスプロイトによる攻撃は出来ません。

SIOSによるPoC動画は[こちら](https://youtu.be/1iEe4E4FVF8)になります。

log4shellの時と同じく、環境に利用されているケースも多いため、有効な対策としては「使用しているパッケージをきちんと把握し」「アップデートをきちんと行う」事になります。

* 1. TrendMicroによると、Miraiマルウェア（IoTを標的に攻撃を行い、Miraiボットネットを形成する）にSpring4Shellを利用していることが[報告されて](https://news.mynavi.jp/techplus/article/20220411-2319243/)います。構築されたボットネットはさらなる侵害に利用されたり、暗号通貨マイニングに利用されたりします。
  2. Microsoftによると、[Spring4Shell攻撃がAzure上で観測](https://www.bleepingcomputer.com/news/security/microsoft-detects-spring4shell-attacks-across-its-cloud-services/#.Yk2fJQvQ2EA.twitter)されているとのことです。
  3. こうした状況を受け、CISAでは米連邦政府や行政機関に対して拘束力を持ち、2週間以内の対応が必要となる「悪用が確認された脆弱性カタログ（KEV）」にも同脆弱性を追加しました。

#### Dirty Pipe

* 1. 脆弱性内容 ([SIOSセキュリティブログより](https://security.sios.com/vulnerability/kernel-security-vulnerability-20220309.html))

3/08/2022にLinux Kernelの脆弱性(Important: CVE-2022-0847 (Dirty Pipe))が公開されました。「[Dirty Cow](https://security.sios.com/vulnerability/selinux-security-20161028.html)と同じような脆弱性」ということで、「Dirty Pipe」と名前が付けられており、脆弱性公開とほぼ同時にPoCも公開されました。

Linux Kernelで、新しいパイプバッファー構造体の「flag」メンバーがcopy\_page\_to\_iter\_pipe()とpush\_pipe()関数で不完全な初期化をされており、古い値が残ったままになっている可能性があるという問題が見つかりました。

これを利用して、ローカルの攻撃者がページキャッシュ中のページに書き込みを行うことでRead Onlyのファイルに書き込みを行い、特権を昇格することが可能です。

SIOSによるPoC動画は[こちらに公開](https://youtu.be/s6TucbcMVq0)しています。

* 1. Dirty Pipeですが、既に悪用が現実味を帯びています（ただし、実際に悪用されたというニュースは現在の所入っていません）。

Android上で管理者権限を奪う動画が[公開されています](https://arstechnica.com/information-technology/2022/03/researcher-uses-dirty-pipe-exploit-to-fully-root-a-pixel-6-pro-and-samsung-s22/)。

QNAP社のNASも悪用される可能性があることから[警告とファームウェアをリリースしました](https://www.bleepingcomputer.com/news/security/qnap-warns-severe-linux-bug-affects-most-of-its-nas-devices/)。

* 1. こうした状況を受け、CISAでは米連邦政府や行政機関に対して拘束力を持ち、2週間以内の対応が必要となる「悪用が確認された脆弱性カタログ」にも同脆弱性を追加しました。

#### BIG-IP(F5)の脆弱性(CVE-2022-1388)

* 1. F5は2022年5月4日、CVE番号CVE-2022-1388でトラッキングされるBIG-IP製品のiControlRESTコンポーネントにおけるリモートコード実行の脆弱性についてのセキュリティアドバイザリを公開しました。脅威アクターがこの脆弱性を悪用すると、パッチ未適用のシステムで認証を回避して任意のコードを実行可能です。この脆弱性はCVSSスコア9.8となっており緊急の対応が必要です。
  2. パロアルトネットワークスによると、当該アドバイザリの公開以降、パッチ未適用のシステムを探して大量のスキャン活動が行われ、実際の悪用も始まっています。

5/10にパロアルトネットワークスはF5 BIG-IP 認証バイパス脆弱性（92570）に対する脅威防御シグネチャを公開しましたが、わずか10時間のあいだに、脆弱性スキャンとアクティブな悪用試みによるシグネチャのトリガーが2,552回発生しています。

* 1. [coinminerボットがBIG-IPのRCEをターゲットにしています](https://twitter.com/0xrb/status/1523964137776496641)（coinminerを実行させています）
  2. こうした状況を受け、CISAでは米連邦政府や行政機関に対して拘束力を持ち、2週間以内の対応が必要となる「悪用が確認された脆弱性カタログ（KEV）」にも同脆弱性を追加しました。

#### Log4Shellの悪用

* 1. 厳密に言えばこちらは2021末のインシデントですが、2022年になってLog4Shellの悪用が幾つか報告されているので取り上げます。
  2. BlackBerry社によりVMWare Horizonに対するlog4j脆弱性を悪用した攻撃の[IoCが公開されています。](https://blogs.blackberry.com/ja/jp/2022/02/log4u-shell4me)
  3. log4j2の脆弱性を利用した攻撃を[ベルギー国防省が確認しています。](https://www.zdnet.com/article/belgian-defense-ministry-confirms-cyberattack-through-log4j-exploitation/)
  4. log4shellの脆弱性ですが、2022Q1では実際に[DDoSやcryptominerに使用されている](https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/)という報告が上がっています。

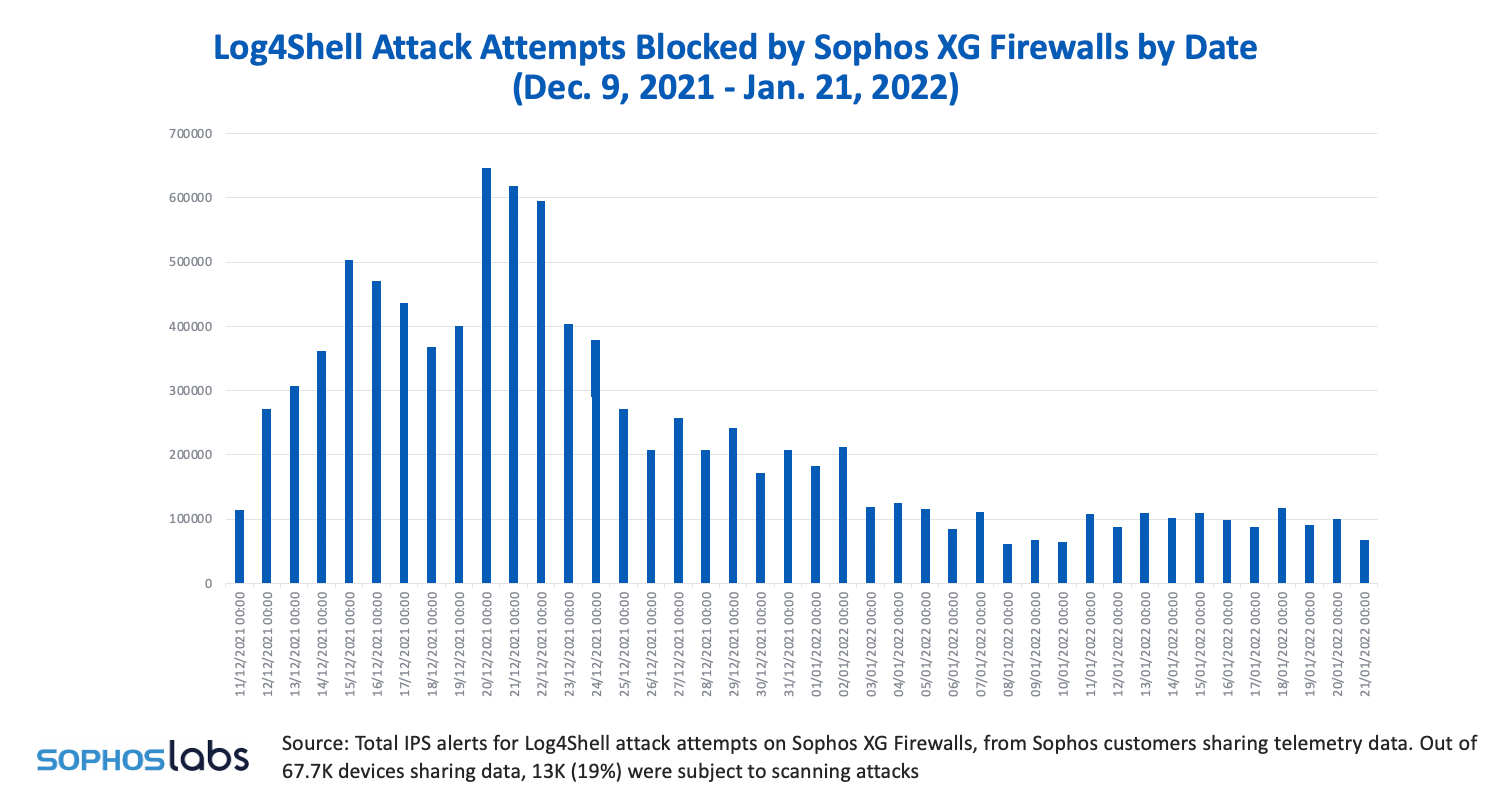
バラクーダのレポートによると、MiraiボットネットでLog4Shellが使用されているようです。

また、下記のようなものでもLog4Shellが使用されているようです。

* BillGates malware (DDoS)
* Kinsing (cryptominer)
* XMRig (cryptominer)
* Muhstik (DDoS)

また、TunnelVisionというイラン系のハッカーグループが、VMware Horizo​​nサーバー上のLog4jを悪用して、[中東と米国の企業ネットワークを侵害しているのが発見された](https://www.bleepingcomputer.com/news/security/iranian-hackers-target-vmware-horizon-servers-with-log4j-exploits/)という報告が上がっています。

[Sophos社のレポート](https://news.sophos.com/en-us/2022/01/24/log4shell-no-mass-abuse-but-no-respite-what-happened/)によると、現在Log4Shellをターゲットとした攻撃活動は減少しているようですが、ネット上には永く残っていくものと思われます。

[](https://news.sophos.com/wp-content/uploads/2022/01/Screenshot-2022-01-23-at-09.03.29.png)

参考情報)

[Spring Frameworkの脆弱性(Spring4Shell / SpringShell : CVE-2022-22965)](https://security.sios.com/vulnerability/spring4shell-vulnerability-20220401.html)

[MiraiボットネットマルウェアによるSpring4Shell脆弱性の悪用を確認](https://news.mynavi.jp/techplus/article/20220411-2319243/)

[Microsoft detects Spring4Shell attacks across its cloud services](https://www.bleepingcomputer.com/news/security/microsoft-detects-spring4shell-attacks-across-its-cloud-services/#.Yk2fJQvQ2EA.twitter)

[Linux Kernelの脆弱性(Important: CVE-2022-0847 (Dirty Pipe))](https://security.sios.com/vulnerability/kernel-security-vulnerability-20220309.html)

[Android端末のルート権限を一瞬で奪取するムービーが公開される、Linuxの脆弱性「Dirty Pipe」を用いた攻撃が現実的に](https://gigazine.net/news/20220316-dirty-pipe-android-root/)

[QNAP warns severe Linux bug affects most of its NAS devices](https://www.bleepingcomputer.com/news/security/qnap-warns-severe-linux-bug-affects-most-of-its-nas-devices/)

[脅威に関する情報: CVE-2022-1388 BIG-IP製品のiControlRESTコンポーネントにおけるリモートコード実行の脆弱性](https://unit42.paloaltonetworks.jp/cve-2022-1388/)

[Finally #coinminer targeting F5 iControl REST RCE #CVE-2022-1388](https://twitter.com/0xrb/status/1523964137776496641)

[Threat Spotlight: Attacks on Log4Shell vulnerabilities](https://blog.barracuda.com/2022/03/02/threat-spotlight-attacks-on-log4shell-vulnerabilities/)

[Iranian hackers target VMware Horizon servers with Log4j exploits](https://www.bleepingcomputer.com/news/security/iranian-hackers-target-vmware-horizon-servers-with-log4j-exploits/)

[Log4Shell: No Mass Abuse, But No Respite, What Happened?](https://news.sophos.com/en-us/2022/01/24/log4shell-no-mass-abuse-but-no-respite-what-happened/)

[Belgian Defense Ministry confirms cyberattack through Log4j exploitation](https://www.zdnet.com/article/belgian-defense-ministry-confirms-cyberattack-through-log4j-exploitation/)

### III. 2022Q1での脆弱性を利用したインシデント

CISA(Cybersecurity & Infrastructure Security Agency)は、”[KNOWN-EXPLOITED-VULNERABILITIES-CATALOG](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)”として、悪用されていることが判明した脆弱性(CVE)のカタログを公開しています。

これによると、単純に”CVE-2022”で始まる脆弱性は2022/06/05時点で40個登録されています。

| CVE-2022-22587 | Apple | iOS and macOS | メモリ破損脆弱性 |
| --- | --- | --- | --- |
| CVE-2022-21882 | Microsoft | Win32k | Win32kの特権昇格 |
| CVE-2022-22620 | Apple | Webkit | Apple Webkitのリモートコード実行脆弱性 |
| CVE-2022-24086 | Adobe | Commerce and Magento Open Source | Adobe Commerce and Magento Open Sourceの不正な入力値チェック |
| CVE-2022-0609 | Google | Chrome | Google Chrome Use-After-Free 脆弱性 |
| CVE-2022-23131 | Zabbix | Frontend | Zabbix Frontend認証バイパス 脆弱性 |
| CVE-2022-23134 | Zabbix | Frontend | Zabbix Frontend 不正なアクセス制御 脆弱性 |
| CVE-2022-24682 | Zimbra | Webmail | Zimbra Webmail XSS 脆弱性 |
| CVE-2022-20708 | Cisco | Small Business RV160, RV260, RV340, and RV345 Series Routers | Cisco Small Business RV Series Routers スタックベースバッファーオーバーフロー 脆弱性 |
| CVE-2022-20703 | Cisco | Small Business RV160, RV260, RV340, and RV345 Series Routers | Cisco Small Business RV Series Routers スタックベースバッファーオーバーフロー 脆弱性 |
| CVE-2022-20701 | Cisco | Small Business RV160, RV260, RV340, and RV345 Series Routers | Cisco Small Business RV Series Routers スタックベースバッファーオーバーフロー 脆弱性 |
| CVE-2022-20700 | Cisco | Small Business RV160, RV260, RV340, and RV345 Series Routers | Cisco Small Business RV Series Routers スタックベースバッファーオーバーフロー 脆弱性 |
| CVE-2022-20699 | Cisco | Small Business RV160, RV260, RV340, and RV345 Series Routers | Cisco Small Business RV Series Routers スタックベースバッファーオーバーフロー 脆弱性 |
| CVE-2022-26486 | Mozilla | Firefox | Mozilla Firefox Use-After-Free 脆弱性 |
| CVE-2022-26485 | Mozilla | Firefox | Mozilla Firefox Use-After-Free 脆弱性 |
| CVE-2022-26318 | WatchGuard | Firebox and XTM Appliances | WatchGuard Firebox and XTM Appliances 任意のコード実行 |
| CVE-2022-26143 | Mitel | MiCollab, MiVoice Business Express | MiCollab, MiVoice Business Express アクセス制御 脆弱性 |
| CVE-2022-21999 | Microsoft | Windows | Microsoft Windows Print Spooler 特権昇格 脆弱性 |
| CVE-2022-1096 | Google | Chromium V8 | Google Chromium V8 Type Confusion 脆弱性 |
| CVE-2022-0543 | Redis | Debian-specific Redis Servers | Debian-specific Redis Server Lua サンドボックス脱出の脆弱性 |
| CVE-2022-26871 | Trend Micro | Apex Central | Trend Micro Apex Central 任意のファイルアップロード脆弱性 |
| CVE-2022-1040 | Sophos | Firewall | Sophos Firewall認証バイパス 脆弱性 |
| CVE-2022-22965 | VMware | Spring Framework | Spring Framework JDK 9+ リモートコード実行 脆弱性 |
| CVE-2022-22675 | Apple | macOS | Apple macOS 境界外書き込みの脆弱性 |
| CVE-2022-22674 | Apple | macOS | Apple macOS 境界外読み込みの脆弱性 |
| CVE-2022-23176 | WatchGuard | Firebox and XTM | WatchGuard Firebox and XTM 特権昇格 脆弱性 |
| CVE-2022-24521 | Microsoft | Windows | Microsoft Windows CLFS Driver 特権昇格 脆弱性 |
| CVE-2022-22954 | VMware | Workspace ONE Access and Identity Manager | VMware Workspace ONE Access and Identity Manager サーバサイドテンプレートインジェクションの脆弱性 |
| CVE-2022-22960 | VMware | Multiple Products | VMwareの複数製品の特権昇格脆弱性 |
| CVE-2022-1364 | Google | Chromium V8 Engine | Google Chromium V8 Type Confusion 脆弱性 |
| CVE-2022-22718 | Microsoft | Windows | Microsoft Windows Print Spooler 特権昇格 脆弱性 |
| CVE-2022-29464 | WSO2 | Multiple Products | WSO2 複数製品での制限のないファイルアップロード脆弱性 |
| CVE-2022-26904 | Microsoft | Windows | Microsoft Windows User Profile Service 特権昇格 脆弱性 |
| CVE-2022-21919 | Microsoft | Windows | Microsoft Windows User Profile Service 特権昇格 脆弱性 |
| CVE-2022-0847 | Linux | Kernel | Linux Kernel 特権昇格 脆弱性 |
| CVE-2022-1388 | F5 | BIG-IP | F5 BIG-IP 認証の欠落の脆弱性 |
| CVE-2022-30525 | Zyxel | Multiple Firewalls | Zyxel Multiple Firewalls OSコマンドインジェクション脆弱性 |
| CVE-2022-22947 | VMware | Spring Cloud Gateway | VMware Spring Cloud Gatewayコードインジェクション脆弱性 |
| CVE-2022-20821 | Cisco | IOS XR | Cisco IOS XR オープンポート脆弱性 |
| CVE-2022-26134 | Atlassian | Confluence Server/Data Center | Atlassian Confluence Server and Data Center リモートコード実行 脆弱性 |

これらのCVEに関しては、既に悪用していることが判明していることから、対象の製品はすぐに更新ないし迂回策を取る必要があります。

その他にも、下記のようなインシデントが発生している脆弱性があります。

1. “node-ipc”に意図的に仕組まれたコードによる脆弱性（CVE-2022-23812）

ウクライナ時間の2022年3月7日に、npmメンテナーであるRIAEvangelistことBrandon Nozaki Miller氏がNode.jsモジュール「[node-ipc](https://github.com/RIAEvangelist/node-ipc)」のバージョン10.1.1を公開しました。このバージョン10.1.1には[ロシア・ウクライナ紛争への抗議活動として”node-ipc”パッケージに意図的に脆弱性が仕込まれました。](https://gigazine.net/news/20220322-sabotage-code-to-node-ipc/)このパッケージをロシア・ベラルーシのIPアドレスを持つユーザが実行するとファイルの内容を消去してハートの絵文字に上書きしてしまいます。

ウェブアプリのUI構築用JavaScriptフレームワークであるVue.jsなどの多くのプロジェクトが”node-ipc”に依存しています。そのため、”node-ipc”を呼び出すシステムがロシアあるいはベラルーシからアクセスした場合、重大なセキュリティインシデントが発生する可能性があります。

GitHub上での議論をきっかけに、問題のコード部分はバージョン10.1.3ですべて削除されましたが、新たにMiller氏により”[peacenotwar](https://snyk.io/blog/peacenotwar-malicious-npm-node-ipc-package-vulnerability/)”というnpmパッケージが作成され、node-ipcと依存関係のリポジトリとして設定されました。

このnpmパッケージは、デスクトップとOneDriveに「WITH-LOVE-FROM-AMERICA.txt」というテキストファイルを作成します。これにより、node-ipcが呼び出されるたびにロシアとウクライナの戦況に関するコンテンツを含むファイルを、ユーザーのデスクトップディレクトリに配置する仕様になっています。

Miller氏はnode-ipcの他にも40種類以上のnpmパッケージのメンテナーを務めているため、これらすべてのパッケージを考慮しなくてはならないことになりました。

1. WPS(Kingsoft Office)の脆弱性（CVE-2022-24934）

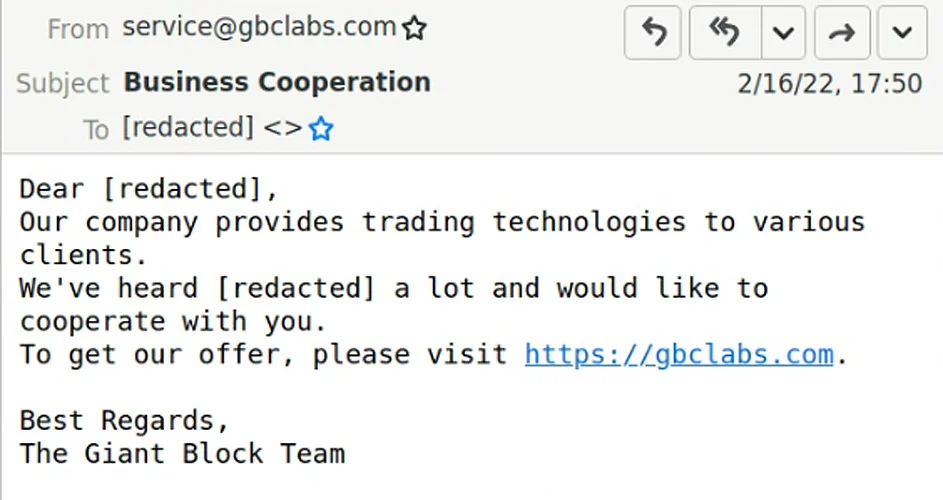
[AVASTによると、中国の攻撃者が台湾・香港・フィリピンの賭け会社を標的とした攻撃を行っています。これには、WPSOfficeアップデートユーティリティの脆弱性であるCVE-2022-24934が利用されています](https://www.bleepingcomputer.com/news/security/hackers-exploit-new-wps-office-flaw-to-breach-betting-firms/)。

WPS Officeの脆弱性を利用して、標的となるシステムにマルウェアを送り込みバックドアを仕掛けているようです。AVASTは既に製品開発元に連絡を行い、ユーザにパッケージの更新を促している様です。

1. 北朝鮮のハッカーによる[Google Chrome脆弱性を悪用したゼロデイ攻撃](https://www.bleepingcomputer.com/news/security/north-korean-hackers-exploit-chrome-zero-day-weeks-before-patch/)

Googleの脅威分析グループ（TAG）によると、2022/02/10にGoogle Chromeの脆弱性（その時点では未報告）を用いた攻撃キャンペーンを観測し、脆弱性に対処するために2022/02/14に緊急のGoogleChromeアップデートを実施しました。

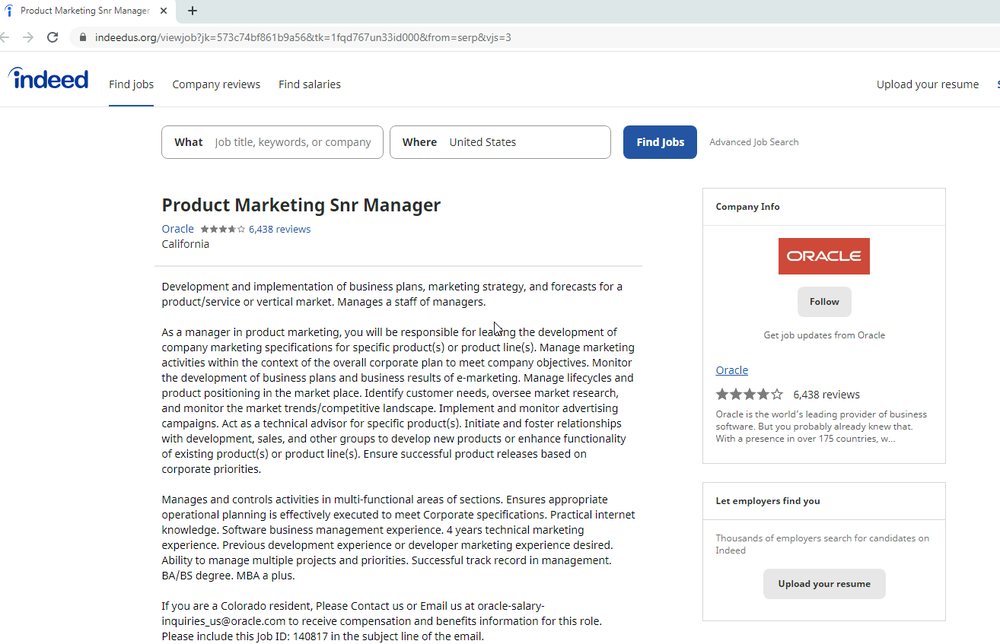
このCVE-2022-0609ですが、メールにエクスプロイトキットへのリンク（偽のWebサイトや侵害されたWebサイト）が仕込まれていました。



研究者によると、ゼロデイ脆弱性が積極的に悪用されている兆候は、2022年1月4日に発見されており、Lazarus Groupと呼ばれる北朝鮮政府が後援するハッカーグループとのつながりが指摘されています。

Google TAGは、この活動は、2020年8月に展開された北朝鮮のスパイ活動である[OperationDreamJob](https://www.gamingdeputy.com/jp/tech/%E5%8C%97%E6%9C%9D%E9%AE%AE%E3%81%AE%E3%83%8F%E3%83%83%E3%82%AB%E3%83%BC%E3%81%8C%E3%80%81%E7%B1%B3%E5%9B%BD%E3%81%AE%E4%BD%95%E7%99%BE%E3%82%82%E3%81%AE%E3%82%BF%E3%83%BC%E3%82%B2%E3%83%83%E3%83%88/)と一致していると述べています。 OperationDreamJobでは、ボーイング社、ダグラス社、BAE社など、米国の有名な防衛及び航空宇宙企業からの偽の求人を被害者に送りました。

Google TAGは、今回のキャンペーンでDisney、Google、およびOracleの採用担当者からの偽の求人情報を含むフィッシングメールを観測したと述べています。



(参考：[North Korean hackers exploit Chrome zero-day weeks before patch](https://www.bleepingcomputer.com/news/security/north-korean-hackers-exploit-chrome-zero-day-weeks-before-patch/)）

参考情報)

[CISA KNOWN EXPLOITED VULNERABILITIES CATALOG](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

[MiraiボットネットマルウェアによるSpring4Shell脆弱性の悪用を確認](https://news.mynavi.jp/techplus/article/20220411-2319243/)

[Linux Kernelの脆弱性(Important: CVE-2022-0847 (Dirty Pipe))](https://security.sios.com/vulnerability/kernel-security-vulnerability-20220309.html)

[Android端末のルート権限を一瞬で奪取するムービーが公開される、Linuxの脆弱性「Dirty Pipe」を用いた攻撃が現実的に](https://gigazine.net/news/20220316-dirty-pipe-android-root/)

[オープンソースのnpmパッケージ「node-ipc」にロシア在住の開発者を標的にした悪意のあるコードがメンテナーによって追加される](https://gigazine.net/news/20220322-sabotage-code-to-node-ipc/)

[Alert: peacenotwar module sabotages npm developers in the node-ipc package to protest the invasion of Ukraine](https://snyk.io/blog/peacenotwar-malicious-npm-node-ipc-package-vulnerability/)

[Hackers exploit new WPS Office flaw to breach betting firms](https://www.bleepingcomputer.com/news/security/hackers-exploit-new-wps-office-flaw-to-breach-betting-firms/)

[North Korean hackers exploit Chrome zero-day weeks before patch](https://www.bleepingcomputer.com/news/security/north-korean-hackers-exploit-chrome-zero-day-weeks-before-patch/)

## まとめ

2022Q1の脅威動向は、ロシア・ウクライナの紛争があったこと以外は、ほぼIPAの予想通りです。その中でも教訓となる所を下記に抜き出します。

1. 踏み台・攻撃に使われるのでテスト環境・IPだけの機器も適切なフィルタ・管理を
2. 「独自に外部企業との接続を行わない」。必要ならきちんと管理し更新を。
3. ランサムウェア対策（マルウェア対策）をちゃんと行う。
4. 「ソーシャルエンジニアリング」に気をつける
5. サポート端末と言えども保護し、データへのアクセス制御を。
6. 「サポートエンジニア」等の輪の弱い所が狙われる。
7. SWのサプライチェーンに気をつけよう
   1. 社内のIT資産を確認・整理する
   2. CI/CDパイプラインに脆弱性検査を組み込む
   3. SBOM(Software Bill of Materials: ソフトウェア部品表)の整備が重要