ウクライナ侵攻における戦闘活動と連動型サイバー攻撃

新井 悠 ●NTTデータ サイバーセキュリティ技術部 Executive Security Analyst

ロシアによるウクライナ侵攻では、軍事攻撃と連動してサイバー攻撃も盛んに行われている。ロシア側の事例を中心に、攻撃組織の実態や攻撃手法、ハクティビストグループによる関与の可能性について解説する。

■ハイブリッド戦とAPT

2022年2月24日から始まったロシアによるウクライナ侵攻は、従来の通常兵器に加えてサイバー攻撃の影響力が増しており、「ハイブリッド戦」と呼ばれている。本稿では、このサイバー攻撃に焦点を当て、その実態を解説する。

今回のウクライナ侵攻におけるサイバー攻撃の要点は、次の3つに大別される。

① 戦闘活動と連動型のサイバー攻撃
② 戦闘活動と非連動型のサイバー攻撃
③ 連動型に加担するハクティビストの存在

●APT攻撃とパブリックアトリビューション

戦争で実施されるサイバー攻撃は特定の相手（国家や組織）を狙う標的型攻撃となるが、特に持続的かつ執拗に行われるものを「APT（Advanced Persistent Threat：高度標的型）攻撃」と呼ぶ。「高度」と付くのは、「ゼロデイ攻撃」（修正プログラムが用意される前にソフトウエア脆弱性を攻撃すること）のような高度で洗練された手法を用いるからだ。

例えば、iPhoneを遠隔攻撃して侵入できるような脆弱性の情報は、1件で1億円以上もの市場価値があるとされている。そのような脆弱性の情報や攻撃手法を市場から買うのではなく、自分たちで研究開発している集団が存在する。一般にソフトウエアの脆弱性を発見する能力やマルウエアを独自開発できる技術力は経験と才能に大きく依存しており、こうした組織は非常に高いものを備えていると推察される。このような活動を維持するには、相当な規模の組織体制や資金力が必要であり、その点から政府機関レベルの支援や関与が疑われている。実際、APTの攻撃元となる国の属性が「パブリックアトリビューション（属性判定）」として広く示されている。

パブリックアトリビューションとは、サイバー攻撃などの攻撃元の国名を名指しし、その手口を公表することで、攻撃の抑止と被害拡大防止につなげる手法である。

日本でも、2021年に警察庁が「ティック（Tick）」と呼ばれる中国組織のAPT事例をパブリックアトリビューションとして公表している。この事例では、JAXAなど国内約200の組織が攻撃され、これに関与していた男を警視庁が書類送検した。背後には中国軍の関与があったと見られている。

また、2022年10月には、「ラザルス（Lazarus）」と呼ばれる北朝鮮関連組織の動静が公表された。

この事例の場合は、諜報活動ではなく外貨獲得が目的である点が他国のAPTと異なる。警察庁とともに金融庁や内閣サイバーセキュリティセンターからも注意勧告がなされた。

■ロシアのサイバー攻撃部隊

世界的には米国がパブリックアトリビューションに積極的で、ロシア軍関係機関のサイバー部隊も情報セキュリティベンダーによるアトリビューションがある（資料4-1-6）。

ロシア政府の関連機関として、大きく分けると「ロシア連邦軍参謀本部情報総局（GRU）」「ロシア連邦保安局（FSB）」「ロシア対外情報庁（SVR）」の3つがある。それぞれの配下にサイバー攻撃部隊が無数に存在するが、ここでは主要な4つを紹介する。

●APT28

APT28は、GRU配下の26165部隊が実態とされており、「ファンシーベア（Fancy Bear）」や「ストロンチウム（STRONTIUM）」「ポーンストーム（Pawn Storm）」などの別呼称もある。

APT28関連で有名な事例は、2016年の米国大統領選挙だ。民主党のヒラリー・クリントン候補の選対本部長を務めたジョン・ポデスタ氏のGメールアカウントが乗っ取られ、内情が暴露サイトのウィキリークスにアップロードされた。その活動に関与したと言われているのがAPT28だ。米国司法省は、大統領選に対して積極的な関与を行ったと名指ししており、APT28関係者の起訴事実がウェブで公開されている。14年ほど前から攻撃を繰り返しており、2020年の米国大統領選挙にも介入したとされている。

●サンドワーム

「サンドワーム（SandWorm）」もGRU配下で74455部隊が実態とされており、「イリジウム（IRIDIUM）」などの別呼称がある。一説によると、2014年のクリミア半島併合をきっかけに生まれたとされている。ウクライナ侵攻以前での事例としては、2015年12月にウクライナの電力会社3社のシステムに侵入し、23万人の市民を停電被害に遭わせたことで知られている。この攻撃ではワイパー型のマルウエアが使われた。

米国連邦大陪審によって、74455部隊の幹部とされるロシア国籍の6人が起訴されている。サンドワームは、ウクライナ侵攻に伴うサイバー攻撃を仕掛けた可能性が高いとして、しばしば名指しされている。

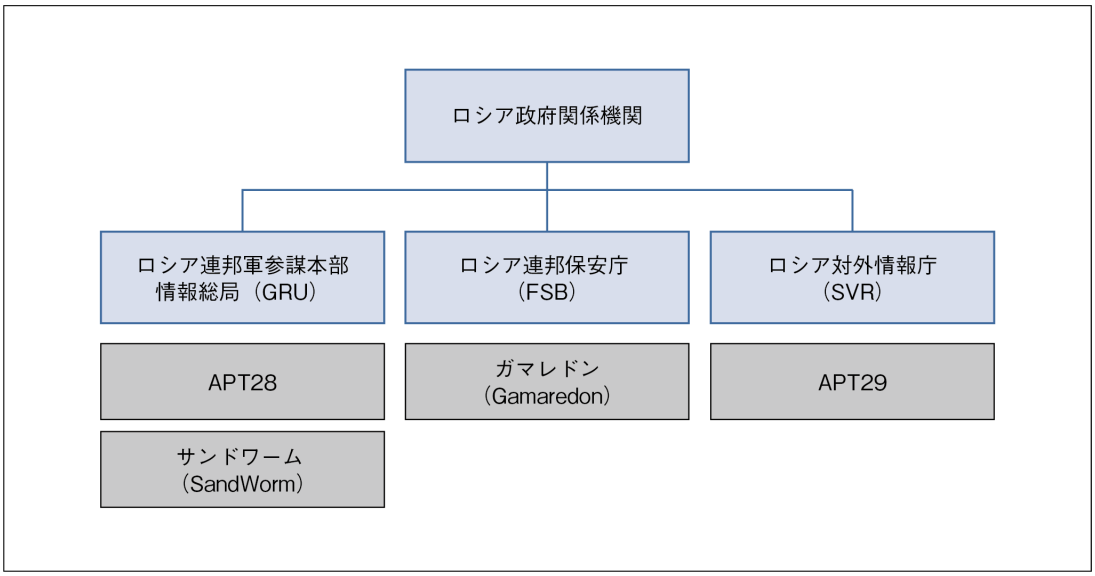
●APT29

SVRに帰属すると言われているのがAPT29で、「コージーベア（Cozy Bear）」や「ノベリウム（NOBELIUM）」などの別呼称がある。ウクライナ侵攻とはほとんど関係なく、事例としては2021年に発生した米国政府機関への攻撃「サンバースト」が有名だ。

米国政府機関で使用されているソフトウエア「Orion Platform」の開発元であるソーラーウィンズに侵入し、ユーザーに提供する更新ファイルをマルウエアに置き換えることで、公式アップデートを通してマルウエアを拡散した。

このように更新ファイルやファームウエアを置き換えて侵入経路を作る手口は、「サプライチェーン攻撃」と呼ばれる。従来は主にハードウエア製品の製造・流通過程において、問題のある部品が混入することをサプライチェーンリスクと呼んでいた。ソフトウエアも部品の集合であり、攻撃者が意図して不正なものを忍ばせることで、情報の抜き取りなど目的を達成できる。情報産業におけるサプライチェーンリスクとして、今後は対策が重要となる。

資料4-1-6　情報セキュリティベンダーによるロシア軍関連機関のサイバー部隊アトリビューション（属性判定）結果



出所：NTTデータ

●ガマレドン

「ガマレドン（Gamaredon）」はあまり表に出てこないが、ウクライナ保安庁（SSU）の調査によるとFSB配下にあるとされる攻撃グループだ。これもクリミア半島併合の後から、ウクライナの国家機関に対してメールでマルウエアを添付して送る標的型メール攻撃を繰り返している。

このようなグループがロシア政府の配下にいて、攻撃に加担しているとされている。マイクロソフトの調査によると、ウクライナの国土で実際の軍事作戦とサイバー攻撃が連動しているケースも多いと報告されている（資料4-1-7）。

■ワイパー攻撃の脅威が増大

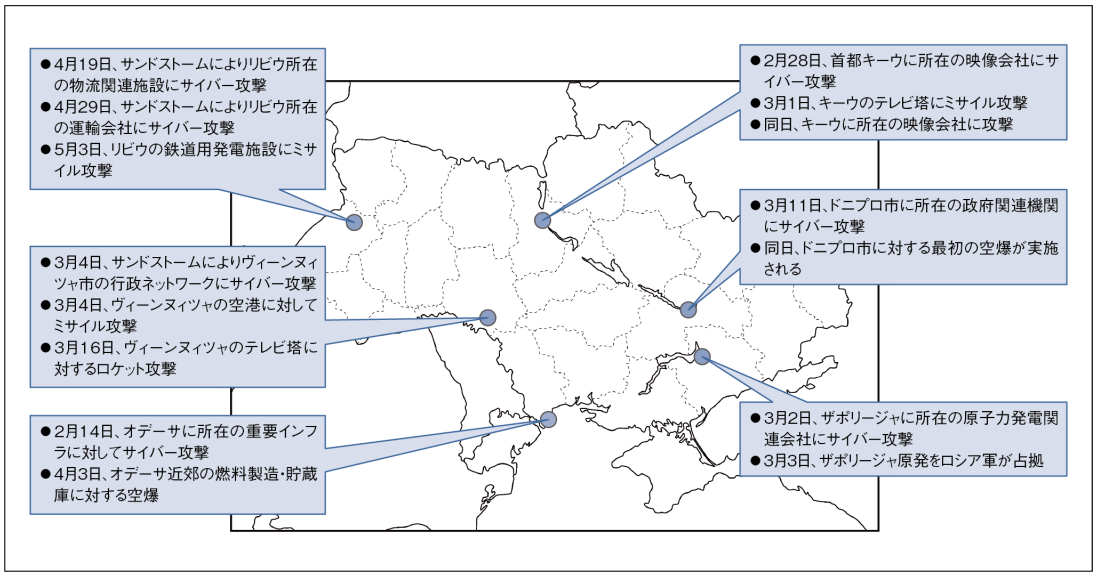
ウクライナ侵攻で発生したサイバー攻撃では、セキュリティベンダーによってさまざまなマルウエアの検体が発見されているが、そのほとんどはワイパー型だ（資料4-1-8）。

ワイパーとはマルウエアの種類で、システムを破壊する目的でストレージ内のファイルを削除して機能不全を発生させるというもの。ウクライナ侵攻以前で知られた事例として、2013年の韓国サイバー事件がある。韓国の放送局や金融機関のシステムに対する攻撃で、ワイパー型マルウエアによって多くのATMやモバイル決済が停止し、社会的に大きな影響を及ぼした。

また、ソニーピクチャーズが北朝鮮の指導者を皮肉るような映画を作った際、同社の社内に対してワイパー型のマルウエアがばらまかれ、システムが止まった事例もある。

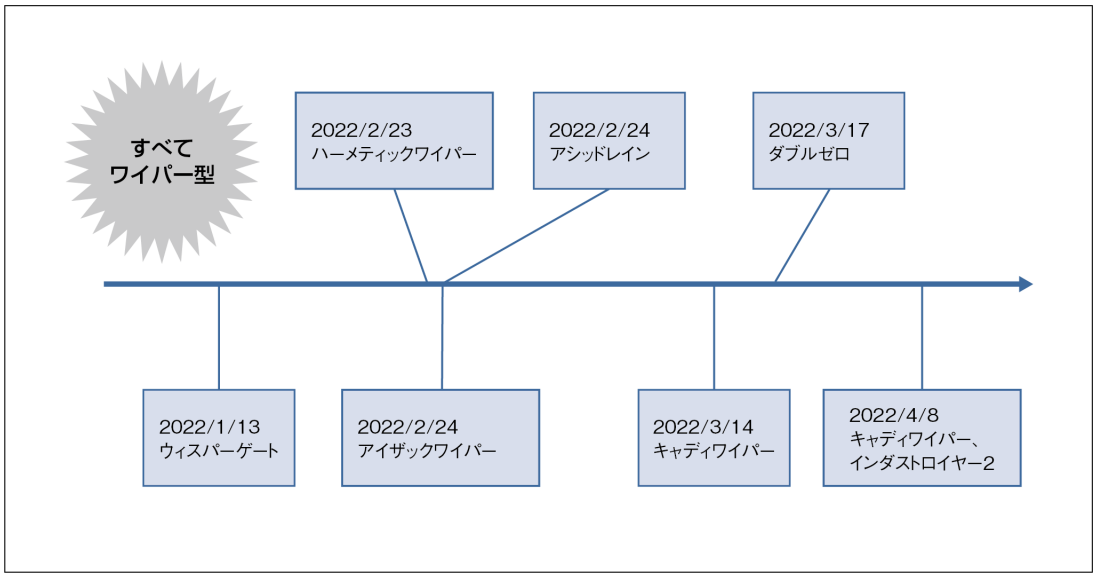
ワイパーによる被害はそれほど深刻なものではなく、バックアップがあれば復旧できるものだ。単純なワイパーに対してはOS標準のバックアップ機能で十分対策できるので、実は脅威としてそれほど大きくはない。むしろ、一般的な諜報活動――相手に活動を知られずに密かに情報を抜き取る――の方が脅威としては深刻だという評価が一般的だった。ところが、戦争のような有事においてはワイパーの脅威は増大する。復旧のためのIT

資料4-1-7　ウクライナに対するロシアの軍事攻撃とサイバー攻撃の連動例



出所：マイクロソフト「ウクライナを守る:サイバー戦争の初期の教訓」をもとに筆者が作成

資料4-1-8　ウクライナ侵攻で悪用されたとされるコンピュータウイルスの検出状況



出所：NTT データ

スキルを持った人材が不足している場合、システム復旧に非常に時間がかかってしまうため、より大きなダメージを受けてしまうからだ。影響が長期化する恐れもあるとして、ウクライナ侵攻以降はワイパーに対する評価が変わりつつある。

次に主なワイパー型マルウエアについて説明する。

●事例：ハーメティックワイパー

「ハーメティックワイパー（HarmeticWiper）」は、システムの起動に必要なストレージ内の領域を破壊するワイパーだ。キプロスにあるハーメティカデジタルの製品のデジタル署名を盗み、正規のプログラムになりすますことでマルウエア対策ソフトの検出を回避する。Windows標準のバックアップと復旧の機能も無効化することで、復旧を混乱させる機能も備えている。破壊終了後は、強制的にシステムが再起動して止まるので、被害に遭ったことが一目で分かる。

ワイパーは自ら標的を探して動き回り、感染を広げるようなことはしない。平時からサイバー攻撃の実行者が諜報・偵察活動を行い、何らかの形で標的となるネットワークシステムに侵入してワイパーを侵入させ、時限爆弾のように起動時間を設定することで、標的となるネットワークシステムに被害をもたらす。

●事例：アシッドレイン

ウクライナ侵攻当初に最も報道されたのが「アシッドレイン（AcidRain）」というワイパーだ。セキュリティ会社のセンチネルワンによる調査では、衛星通信会社のバイアサット製モデムを動作不能にしたサイバー攻撃が2022年2月にあったとされる。これにより、当該モデムを採用していたドイツのエネルギー会社エネルコムが管理する発電用風力タービン5800台の誤動作を引き起こした。実際の被害は、発電機の回転数や動作の観測ができなくなったことと言われている。

アシッドレインの特徴は、モデムというIoT機器が狙われた点にある。一般的なパソコンに比べるとハードウエアやOSが特殊な製品であり、事前調査や動作検証もした上でなければ実現できない攻撃だった。バイアサットの報告によると、脆弱性を突かれてVPN経由で管理ネットワークに侵入されたとしている。

●事例：インダストロイヤー2

「インダストロイヤー2（Industroyer2）」は、ワイパーにもう1つ攻撃手法を加えたマルウエアだ。2016年にウクライナの首都キーウで発生した停電は、変電所に対するサイバー攻撃が原因とされているが、そこで使われたのがインダストロイヤー1だった。インダストロイヤー2はその後継で、2022年にウクライナの高圧変電所への攻撃に使われた。

産業機器用の通信プロトコルを使って偽の信号を電力プラントに送信したとされている。さらに、同じタイミングで「キャディワイパー（CaddyWiper）」という別のマルウエアも使われ、電力システムとその関連システムを同時に攻撃した。

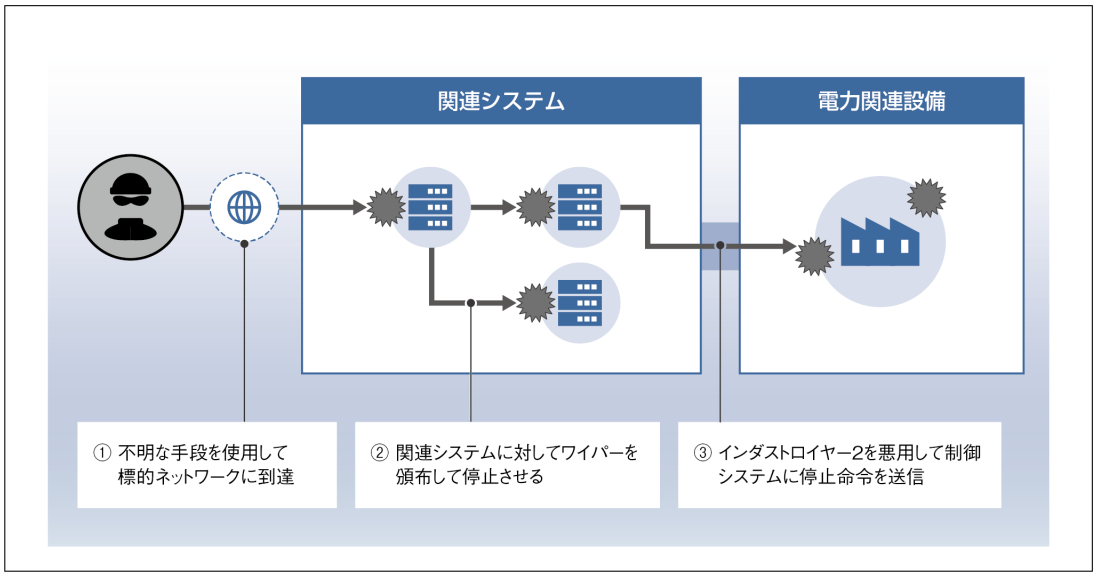
具体的な侵入方法は明らかになっていないが、攻撃の概要は資料4-1-9に示すとおり。関連システムはワイパーによる攻撃で停止させ、それを踏み台にしてインダストロイヤー2から電力関連設備に対して出力を低下もしくは停止するように信号を送る。これは電力プラントの仕組みを熟知していないと達成できない手法だ。

■ハクティビストによる攻撃

ハクティビズム（Hactivism）とは、アクティビズム（積極行動主義）とハックを組み合わせた言葉で、政治的な意思や目的を達成するためにハッキングを手段として使うグループをハクティビストと呼ぶ。

ハクティビストで有名なのはアノニマスだ。本来は情報の自由や共通理念に賛同するという社会的な運動をインターネット上で展開するもので、グループとしては緩いつながりで分散した集団だった。しかし、アノニマスが一人歩きして細か

資料4-1-9　インダストロイヤー2の攻撃概略図



出所：NTT データ

く分裂した結果、非常に政治色の強いサブグループが点在するようになった。それにともない、それまでアノニマスが持っていた社会運動的な意義は薄れてしまった。

ウクライナ侵攻においても、親ロシア派と親ウクライナ派それぞれにハクティビストのグループが結成されており、テレグラム（強力な暗号機能を備えたチャットツール）上で次々にグループが生まれて積極的に活動している。

●キルネット

「キルネット（Killnet）」は、主要なハクティビストグループの1つで、2022年2月に活動を開始した親ロシア派の集まりだ。テレグラム上で活動しており、NATO加盟国の政府機関や民間企業に対してDDoS攻撃を繰り返している。

2022年9月には、日本政府機関の4省庁や民間企業のウェブにDDoS攻撃を行い、通信不全を発生させたとの声明をテレグラムで発表した。キルネットにはいくつものサブグループがあり、目的ごとに分散してOSINT[1]などでウクライナの組織を調査している。

キルネットは、実は開戦前の2022年1月時点で、サイバー犯罪者に向けてDDoS攻撃代行サービスの広告をネットの闇掲示板やYouTubeに出していた。その時点では特に政治的な活動ではなかったが、ウクライナ侵攻をきっかけに親ロシア派のハクティビストグループに変貌した。

●APTとハクティビストが連携した事例

APTとハクティビストが連携した事例もある。キルネットとは別のハクティビストグループに「ザックネット（XakNet）」がある。2022年2月から活動しており、ウクライナの主要機関にDDoS攻撃をしたり、ウクライナ外務省に侵入して内部文章などを盗み出したりしている。また、キルネットと連携して、DDoS攻撃やウクライナ軍機材の攻撃を行っているとも主張している。

ザックネットのメンバーとされる者がロシア国内のメディアに登場し、インタビューも受けている。その中で、ロシア軍関係者からザックネットに接触があり、攻撃を依頼されたと答えている。

さらに、ウクライナ軍の指揮統制システムに対するDDoS攻撃を成功させ、それによりウクライナ東部のドネツク州クラスニー・リマン地区の開放に貢献したとして、ロシア政府から感謝状を受け取ったと語っている。ただし、自分たちはロシア政府関係者ではなく、社会で生活している一般の技術者であり、サイバー攻撃はあくまでもロシア軍兵士の命を守るためにやったとしている。

DDoS攻撃代行サービスの広告の件からも分かるように、少なくともウクライナ侵攻以前は、単に金銭目的で活動していたことは確かで、必ずしもロシア政府とつながりがあるとは断言できない。しかし、APTのようにロシア政府配下の組織ではないものの、情報提供など何らかの形で政府機関と連携していることは明らかだ。

これまでハクティビストについては、政府や軍とはそれほど関係していないとの見方が強かった。しかしザックネットの例からは、ハクティビストの活動や攻撃能力を政府機関が取り込む実態も見えてきた。これらが、ウクライナ侵攻で新たに認識された脅威だといえる。ハクティビストたちの活動や主義主張が盛り上がり、その矛先が日本や日本企業に向いてしまう兆候もあるため十分な注意が必要だ。

■日本政府や企業がすべき対策

ワイパーによる攻撃は、偵察活動やOSINT、ネットワーク探索など、事前の準備活動を丹念に行ったうえで実行されていると考えられる。被害を防ぐには、その予兆や端緒をしっかりと発見し、駆除・排除しなければならない。今後は、脆弱性調査にAIが使われるなど、手口はますます高度化すると予測されており、危険性は高まる一方だ。

日本政府は、2022年12月20日に治安・テロ対策の総合指針として「『世界一安全な日本』創造戦略の変更について」を公表した。2013年以来9年ぶりの改定となるが、引き続きサイバーセキュリティの取り組みを戦略の筆頭に挙げている。

実際に日本国内でも、ランサムウエアを使うグループが活発に活動している。攻撃手法はどれも似ているので、基本的な対策で多くの攻撃から身を守ることができる。修正プログラムの適用といった基本レベルからでかまわないので、セキュリティ対策をしっかりと行うこと。攻撃は執拗に継続して行われるので、対策も平時から継続的に行うことが必須となる。実際にサイバー攻撃を受けてから対応しようとしても、止めることは非常に難しい。

近年ではセキュリティ対策の一環として、「レッドチーム」と呼ばれる企業システムの脆弱性や欠陥を探して攻撃する組織が注目されている。ほかにもアタックサーフェスマネジメント（ASM）とも呼ばれる企業向けのサービスも新たに提供されるようになっており、実際の攻撃者と同じ視点や方法で調査することで、侵入につながる穴を見つけ出せる。

1. Open Source Intelligenceの略語で「オシント」と読む。ネット上など一般でもアクセス可能な公開情報を使った調査活動のこと。

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2023年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp