ALog

テレワークを狙う サイバー攻撃

あなたのPCはWeb上から 攻撃者に丸見え

～始業80秒後から13,850回の攻撃を実測～

AMIYA

目次

■ はじめに
- テレワークが、想像を越えるほど攻撃の餌食になっている

■ 1. グローバル IP アドレスを持つ PC を狙った攻撃とは？
- グローバル IP アドレスを PC に割り当てるとなぜ危険なのか？
- グローバル IP アドレスが割り当てられる構成とは
- 特に多い攻撃方法

■ 2. 実際に攻撃が来るの？
- 開始数分で攻撃を観測
- RDP ポートをスキャン後、RDP への総当たり攻撃が開始
- 2 日間でトータル 13,850 回のログオンチャレンジ（総当たり攻撃）
- パスワードを破られたユーザー名とパスワード
- 攻撃元の国と地域

■ 3. Active Directory の監視が要に
- 4,800 社以上が利用している
  統合ログ製品『ALog シリーズ』でサイバー攻撃を自動検知

はじめに

テレワークが、想像を越えるほど攻撃の餌食になっている

コロナ禍の影響により、テレワークが大幅に浸透し、今や出勤の大半を在宅で過ごす人も少なくない世の中になった。
同時に、もともと脆弱であった家庭のPC/インターネット環境は攻撃者にとってはまさにご馳走の餌場（えさば）といっても過言ではない。
当社の実証実験の結果は、NHKのクローズアップ現代+でも取り上げられたが、多くの攻撃パターンやその脅威の蔓延性が白日の下にさらされることになった。
一般の方々だけでなく、IT業界に精通している者にとっても、サイバー攻撃はおよそEMOTETのようなメール添付型で襲われるか、脆弱なWebサイトが攻撃の踏み台にされる程度でしか起こり得ないと信じて疑わない。

しかし、実態は大きく異なり、想像を絶するほど広範囲に、多くの人々がテレワークを行ったせいで、いとも簡単に侵入を許している。
今回は、その攻撃の手口を具体的に見ていきながら、それに対処すべき方法も合わせてご紹介する。

NHK クローズアップ現代＋
2020年11月12日(木)放送
コロナ禍 あなたを狙うサイバー攻撃　　番組HPより

1. グローバルIPアドレスを持つPCを狙った攻撃とは？

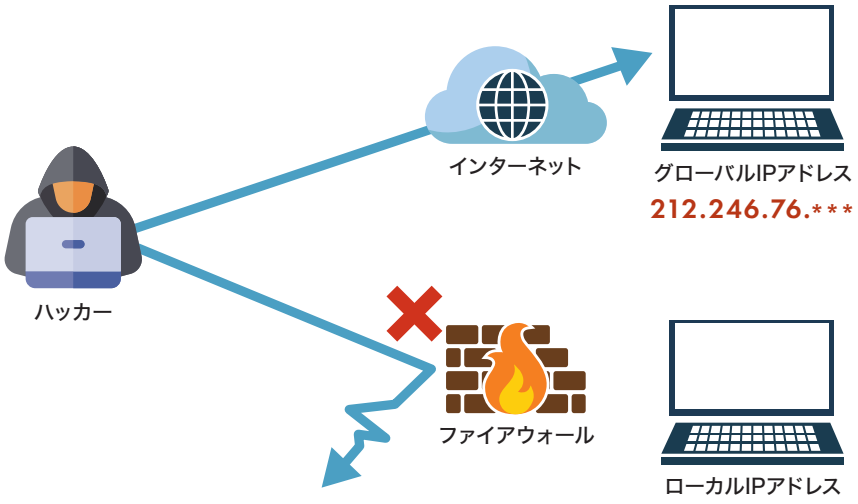
テレワークの浸透により、今や日常となった社外でのインターネット利用。そのインターネット環境が、非常に危険な状態であることをご存じでしょうか。
通常、PCはローカルIPアドレスというアドレスを持ちます。ローカルIPアドレスはルータを通すことでグローバルIPアドレスに変換され、インターネットへとアクセスするのが一般的ですが、最近ではルータを介さない（=PCがグローバルIPアドレスを直接持つ）状態で行われる非常に危険な通信が急増しています。

グローバルIPアドレスを直接持ったまま通信を行うということは、そのPCが「裸のまま」、つまり丸見えの状態であることを意味します。攻撃者からすれば格好の餌食となるわけですが、弊社の調べでは、テレワーク端末の約6%(※)がこの「裸のまま」の状態であることがわかりました。一見少ない数字に思えますが、一台のPCが感染すると社内ネットワーク全体に影響を及ぼすため、決して楽観視してはいけません。

※リモートアクセスVPNサービス「Verona」を利用しているユーザー端末のうち、
グローバルIPアドレスを割り当てられた端末のパーセンテージ

グローバルIPアドレスをPCに割り当てるとなぜ危険なのか？

グローバルIPアドレスを割り当てられたPCには、インターネット上のどこからでもアクセスでき、世界中の攻撃者（ハッカー）が自由に攻撃することも可能です。攻撃者は、脆弱性を抱えたデバイスが存在しないか常に探索（スキャン）しており、もし見つかれば、その脆弱性をついた攻撃を仕掛けてきます。特にファイル共有やRDPを利用している場合は注意が必要です。
片や、ローカルIPアドレスであれば、攻撃者からの攻撃が到達することはないため、比較的安全と言えます。



グローバルIPアドレスが割り当てられる構成とは

グローバルIPアドレスをPCが持つケースとして多いのは2つです。

- **「ルータ機能」を持たないUSBモデム + 直接「グローバルIPアドレス」を割り当てるSIM経由での接続**
- **古いVDSLやCATVのインターネット回線モデム経由での接続**

1つ目のケースは以下の理由から多くのテレワーク環境で採用されています。

- **比較的安価に導入できること**
- **簡単であること（PCにUSBモデムを接続するだけで利用できるため）**

他にも「自宅のインターネット回線を利用する際、古いVDSLやCATVのインターネット回線モデムに直接PCを接続することで、グローバルIPアドレスが割り当てられてしまう」といったケースもあります。
一般ユーザーは、プライベートアドレス環境かグローバルアドレス環境かは意識しません。危険な状態を放置したまま利用している可能性が高いです。

特に多い攻撃方法

RDP総当たり攻撃

＜攻撃内容＞	リモートデスクトッププロトコル（RDP）に対して、 ID／パスワードのリストを使った総当たり攻撃。 一般的によく利用されるパスワードは破られる可能性大。
＜感染すると＞	・ランサムウェア感染や機密情報漏えい ・ボット化し、次のターゲットにRDP総当たり攻撃を実施
＜条件＞	・RDPポートが開いている
＜対策＞	・強固なパスワードを設定 ・ログオンフェイラーを検知できるログ取得環境を整備 ・ビルトイン管理者アカウントを無効化

SMBの脆弱性を狙った攻撃

事例：脆弱性攻撃ツール「EternalBlue」を悪用し、ランサムウェア「WannaCry」を世界中に拡散

＜攻撃内容＞	WindowsOSにおけるサーバメッセージブロック(SMB)プロトコルの脆弱性をついた攻撃
＜脆弱性情報＞	・EternalBlue（Microsoft Server Message Block 1.0 (SMBv1)の脆弱性） ・SMBGhost（Microsoft Server Message Block 3.1.1 (SMBv3)の脆弱性） ・SMBleed（Microsoft Server Message Block 3.1.1 (SMBv3)の脆弱性）
＜感染すると＞	・ランサムウェア感染や機密情報漏えい
＜条件＞	・SMBの古いバージョンを利用している ・SMBポートが開いている
＜対策＞	・最新のパッチを適用する

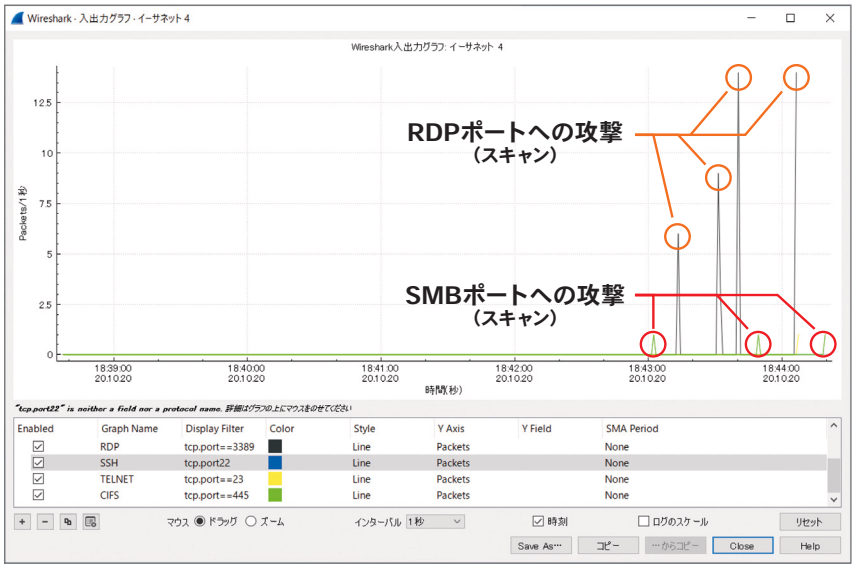
2. 実際に攻撃が来るの？

実際にグローバルIPアドレスが割り当てられるUSBモデムとSIM回線をPCに接続し、2日間に発生した攻撃を観測します。結果として、開始数分で攻撃を受け、2日間でトータル13,850回のログオンチャレンジを観測しています。

知らないうちにグローバルIPアドレスを割り当てられた場合、非常に危険であるということがわかります。

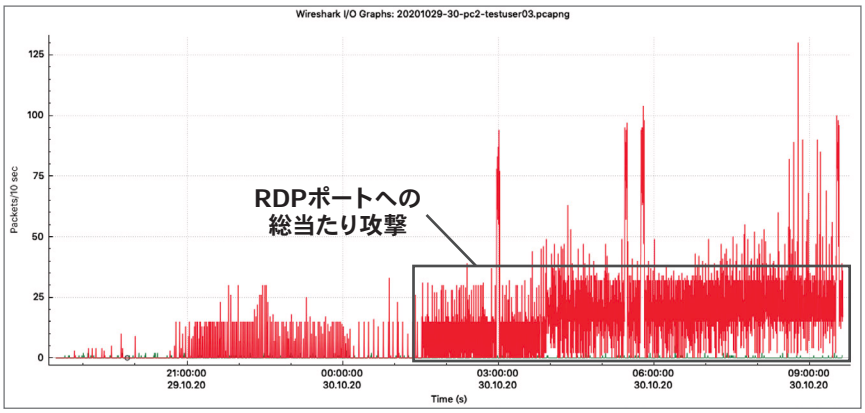
開始数分で攻撃を観測

特定のポートが開いているか、脆弱性が存在しているかをスキャンされています。



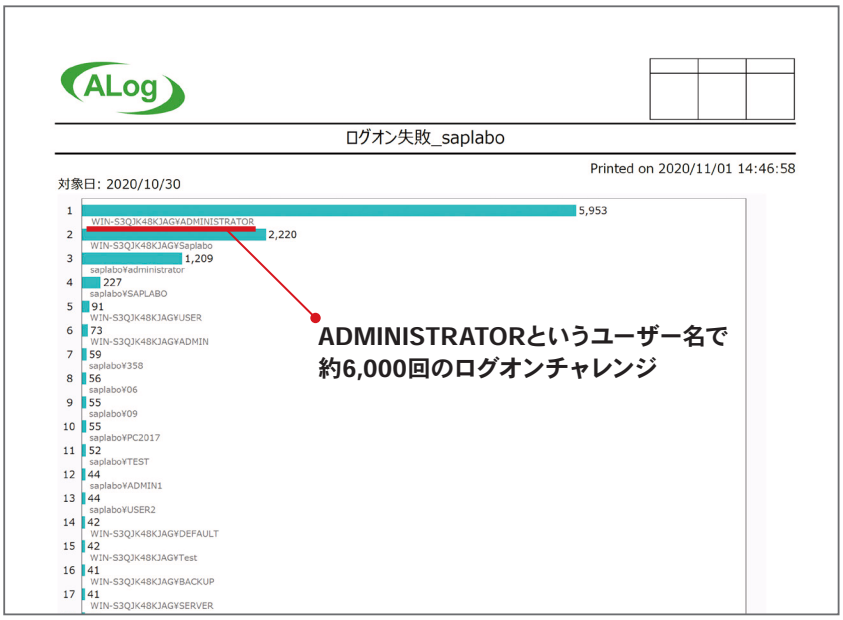
RDPポートをスキャン後、RDPへの総当たり攻撃開始

RDPポートが開いていることを攻撃者に確認された後、パスワードリスト を使った総当たり攻撃を観測。複数の攻撃者を確認しています。



2日間でトータル13,850回のログオンチャレンジ（総当たり攻撃）

「ADMINISTRATOR」や「USER」、「ADMIN」などよく使われるユーザー名に対して、パスワードリストを使ったログオンチャレンジをトータル13,850回観測。
内、いくつか簡単なパスワードを設定していたユーザーはパスワードを破られています。



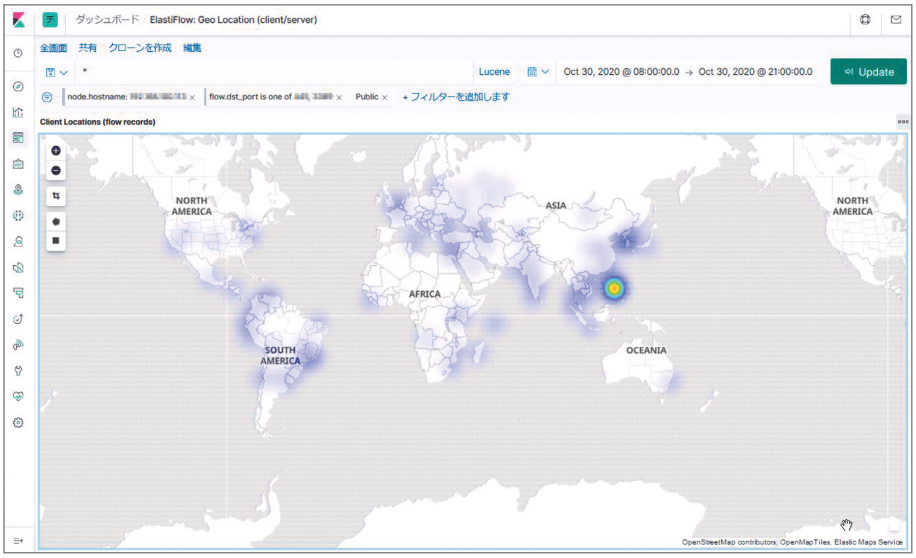
パスワードを破られたユーザー名とパスワード

今回破られたパスワードは、ID：admin、Password：adminと非常に簡単なものでしたが、もしこのようなIDとパスワードを利用されている場合は直ちにパスワードを変更しましょう。

No	ID	Password
1	admin	admin
2	user	user
3	default	default

攻撃元の国と地域

フィリピンや韓国を中心に世界中からの攻撃を観測。また、RDPとSMBポートへの攻撃が最多になります。



国別ランキング

No	Country	Flow Records
1	Philippines	1,968
2	South Korea	855
3	Eswatini	234
4	Latvia	193
5	Republic of Moldova	87
6	Netherlands	84
7	Turkey	76
8	China	71
9	United States	39
10	Russia	31
11	Vietnam	25
12	Venezuela	19
13	Brazil	17
14	India	13
15	Indonesia	13
16	Egypt	7
17	Ukraine	7
18	Romania	6
19	Taiwan	6
20	Japan	5

サービス名（通信プロトコル/ポート）

No	Service	Flow Records
1	ms-wbt-server (TCP/3389)	7,116
2	microsoft-ds (TCP/445)	204
3	telnet (TCP/23)	174
4	netbios-ns (UDP/137)	86
5	ms-sql-s (TCP/1433)	73
6	https (TCP/443)	41
7	ssh (TCP/22)	36
8	http (TCP/80)	34
9	http-alt (TCP/8080)	30
10	personal-agent (TCP/5555)	29
11	http-alt (TCP/81)	27
12	ntp (UDP/123)	24
13	fcp-addr-srvr2 (TCP/5501)	19
14	sip (UDP/5060)	19
15	netbios-ssn (TCP/139)	17
16	3d-nfsd (TCP/2323)	11
17	redis (TCP/6379)	11
18	ssdp (UDP/1900)	11
19	ldap (UDP/389)	10
20	dsc (TCP/3390)	9

3. Active Directory の監視が要に

テレワークPCが丸裸にならないために、以下の対策が効果的です。

- **グローバルIPが割り振られるUSBドングル、SIMは利用しない**
- **最新のパッチを適用する**
- **不必要なポートを開放しない**
- **ID/パスワードは強固なものを利用**

そして、今回の調査では侵入された後については省略していますが、もしPCを乗っ取られた場合、権限昇格、システムの中枢となるActive Directoryの掌握、重要データの奪取と攻撃対象を広げていきます。

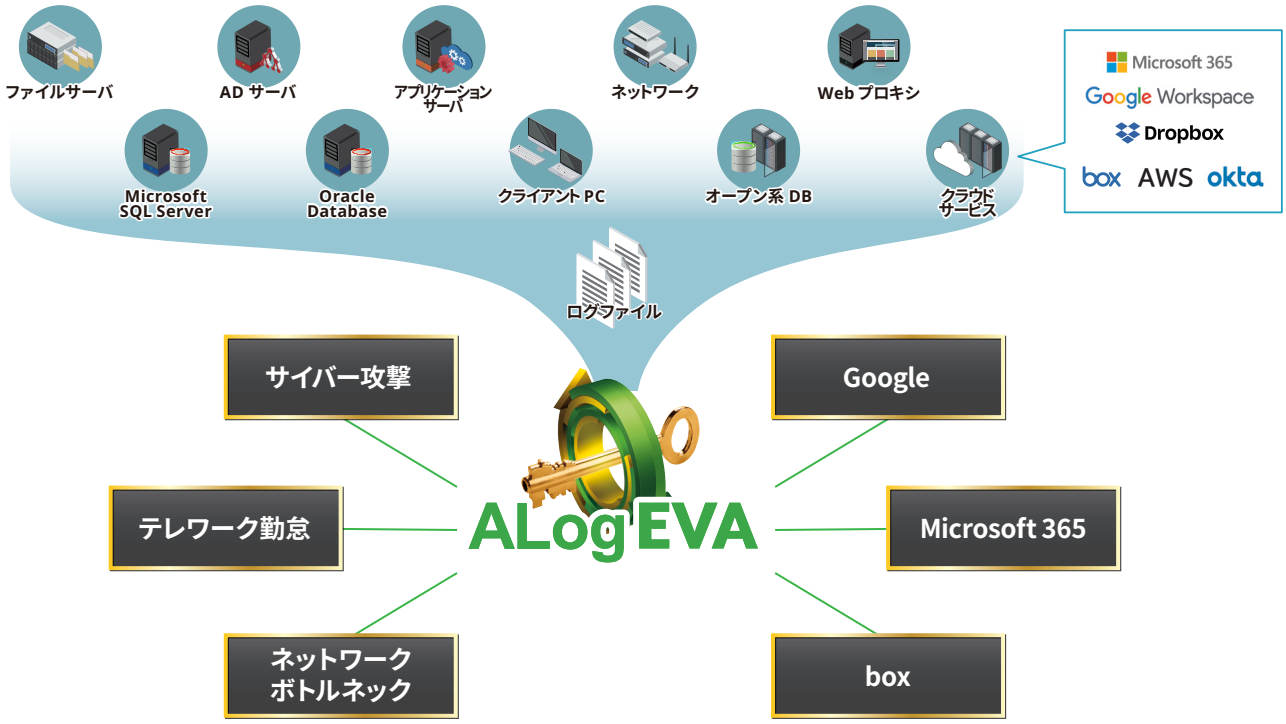
そこで、これらの攻撃から重要データを守るためには、侵入されることを前提に、**侵入されたことを検知できる仕組みを導入しておくことが非常に重要**です。
特に、システムの中枢となるActive Directory（AD）は狙われる可能性が高く、ADは必ず監視しておく必要があります。

よくあるADへの攻撃

- 大量のログオン失敗
- 新規ユーザーの作成
- イベントログの削除
- 管理権限に昇格させる行為

etc...

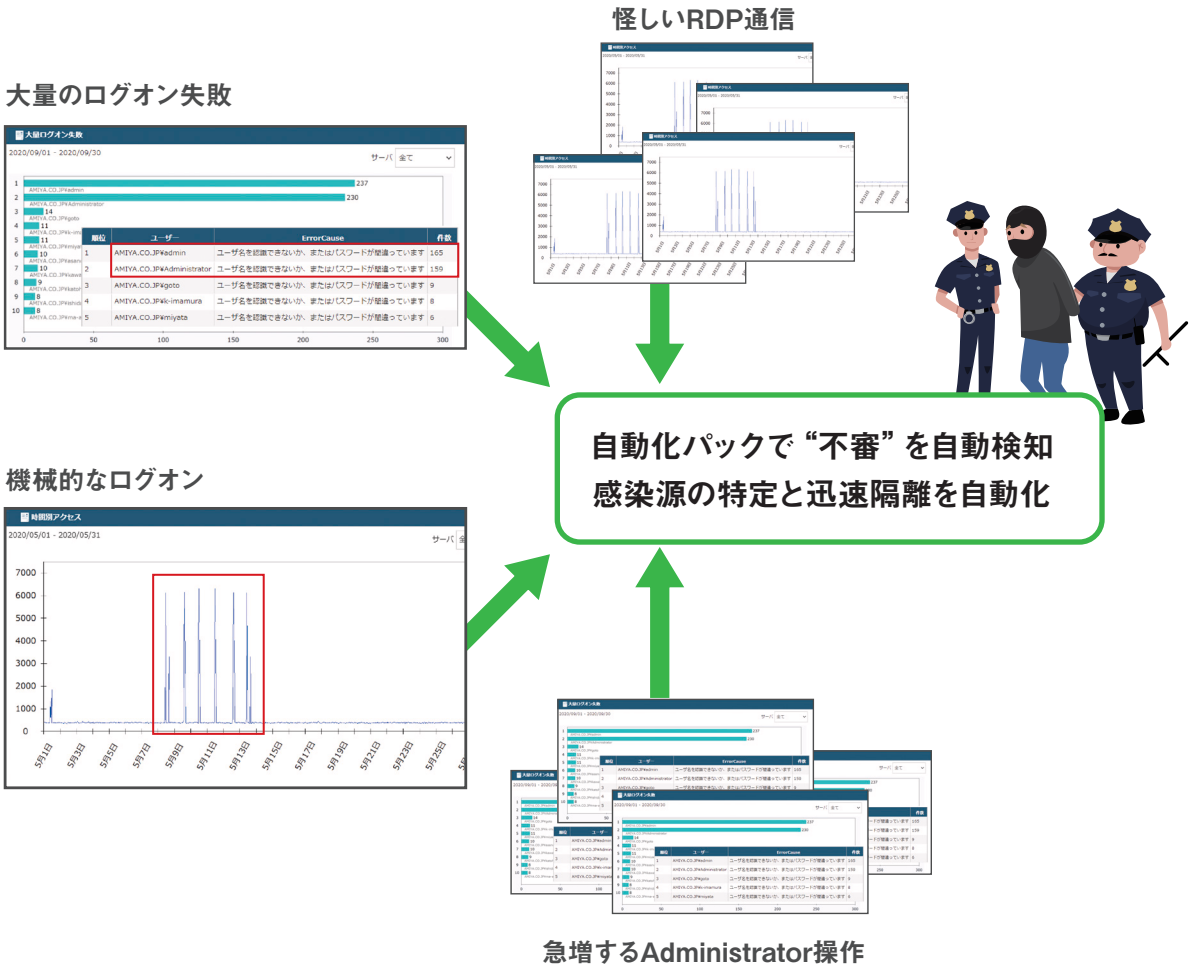
4,800契約以上の導入実績を誇る『ALogシリーズ』でサイバー攻撃を自動検知



ALog EVA
サイバー攻撃自動検知パック

典型的な攻撃パターンは各所にセンサーを埋め込んでおくことで素早く察知可能です。
このパックでは、IPA※やJPCERT※のガイドラインに沿って最も有効性のある対処を実施します。

※ IPA：独立行政法人 情報処理推進機構
※ JPCERT ：Japan Computer Emergency Response Team



サーバアクセスログ
ALog ConVerter®

ALog ConVerter は、重要データへのアクセス記録をエージェントレスで取得する製品です。重要データが格納されるサーバ側からログを取得することにより、ストレスのない効率的なログ管理を実現します。

統合ログ
ALog EVA

ALog EVA は、ALog シリーズの守備範囲を飛躍的に拡張します。
高度な専門技術を要求する従来の統合ログ製品から一線を画した手軽さと柔軟さを備えた新しい統合データマネジメントツールです。

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

お問い合わせ先

株式会社網屋
データセキュリティ事業部

TEL：03-6822-9996　E-mail bv-sales@amiya.co.jp

詳しい製品概要資料はこちら ＞

開発元

AMIYA 株式会社 網屋
〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998
https://www.amiya.co.jp/

販売元

ALog ConVerterは株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、著作権の侵害になります。