今、話題のワード “Attack Surface Management”とは？

～サプライチェーンリスクへの備え～

Soliton®

Attack Surface
＝攻撃対象領域とは

悪意あるハッカーによるサイバー攻撃の足掛かりとなりうる、IT資産や侵入経路は“Attack Surface”と呼ばれ「攻撃対象領域」と訳されます。

Attack Surface の中でも特に外部インターネットに公開されているIT資産は、External Attack Surface（外部攻撃対象領域）とも呼ばれます。

急速に進んだクラウド利用やテレワークの普及、システムの多様化などにより、Attack Surfaceは増え続けています。

※各組織より公開された情報を元に弊社にて整理

実際に狙われた “Attack Surface”

2022年 2月　製造業

子会社が取引先との接続 に利用していたリモート接続機器経由で侵入されランサム感染。
製造業の取引先である、**大手企業も影響確認のため業務停止。**

2022年 4月　飲料メーカー

インターネット回線に接続したネットワーク機器の脆弱性経由で侵入され、ランサム感染。
個人情報を情報漏洩の可能性が否定できない状況となった。

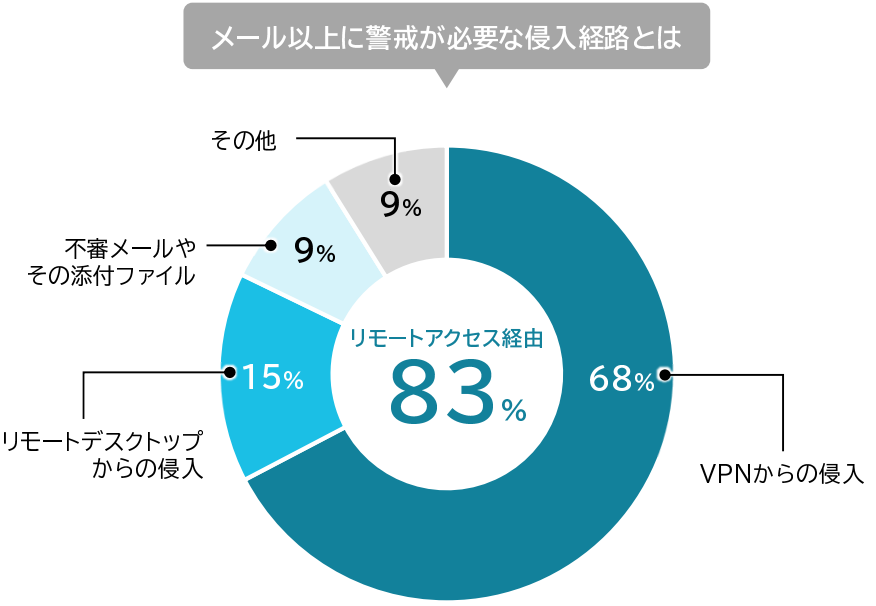
2022年 10月　医療機関

取引先のソフトウェア未更新VPN機器から侵入され、医療機関もランサム感染。
電子カルテシステムが利用できず、**数千人の患者に影響。完全復旧まで約2ヶ月を要した。**

Attack Surfaceを狙う侵入型ランサムウェア被害

現在主流のランサムウェアは、日本では「侵入型ランサムウェア」と言われています。 別名、二重恐喝型、暴露型、標的型などとも呼ばれるもので、従来のランサムウェアと異なり、企業や組織を狙い、侵入後に情報を盗みだしたうえでデータを暗号化します。 復号化のために金銭を要求するとともに、応じなければ盗み出したデータをリークサイトで暴露する二重の恐喝をする攻撃手法です。

警察庁のデータでは、この侵入型ランサムウェアの被害が急増しており、**侵入経路の83%が外部インターネットに公開されたリモートアクセス**からの侵入となっています。



ランサムウェアの感染経路 （令和4年9月15日 警察庁）

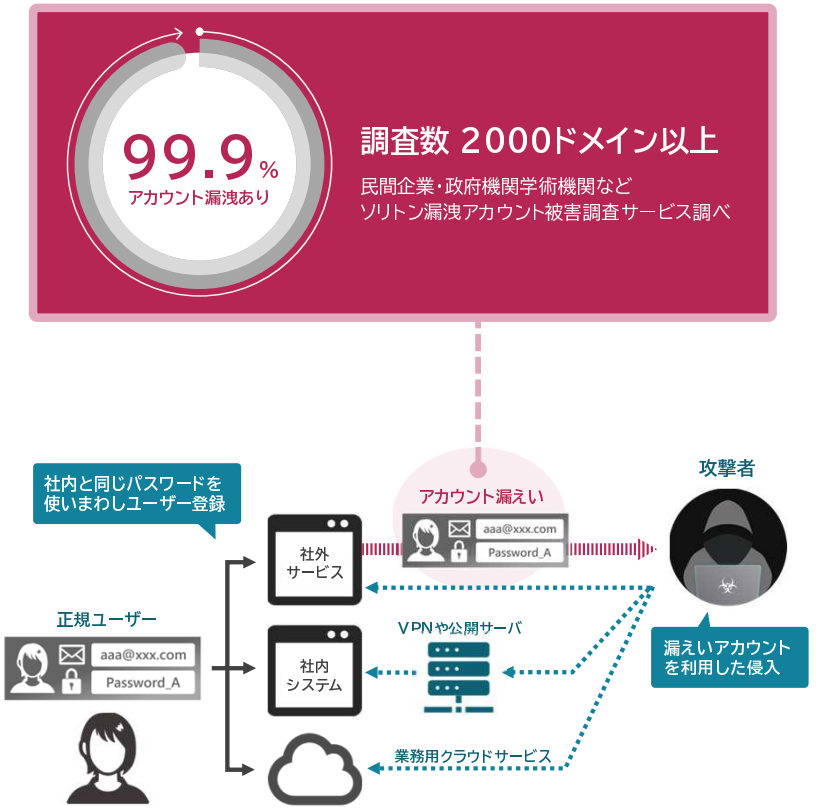
令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和4年9月15日 警察庁）
図表7：感染経路（注 図中の割合は小数第1位以下四捨五入しているため、総計が必ずしも100にならない。）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

Attack Surfaceへの侵入に使われる、漏えいアカウント

社員が業務利用目的で登録したユーザーIDやパスワードが漏えいした場合、Attack Surfaceへの侵入リスクが高まります。

過去に漏えいしたパスワードは攻撃者によってリスト化されており、不正アクセスのための“総当たり攻撃”に使われる危険もあります。

ソリトンシステムズがこれまでに行った「漏えいアカウント被害調査」のうち、全体の **99.9%の企業・団体で、現職職員のパスワードを含むアカウント情報の漏えい**が確認されました。



Attack Surface Management の必要性

Attack Surfaceを把握し適切に管理する

2022年の重大なインシデントは、Attack Surfaceを把握できていなかったり、その脆弱性を放置したことに起因しています。

悪意ある攻撃を予防するには、海外拠点やサプライチェーンを含めたAttack Surfaceを把握し、脆弱性対策や不正侵入対策を実施するなど、適切に管理することが重要です。

今、企業にはDXを推進するとともに、サイバー攻撃から自社のIT資産を守るために、**攻撃対象領域の管理＝Attack Surface Management** が求められています。

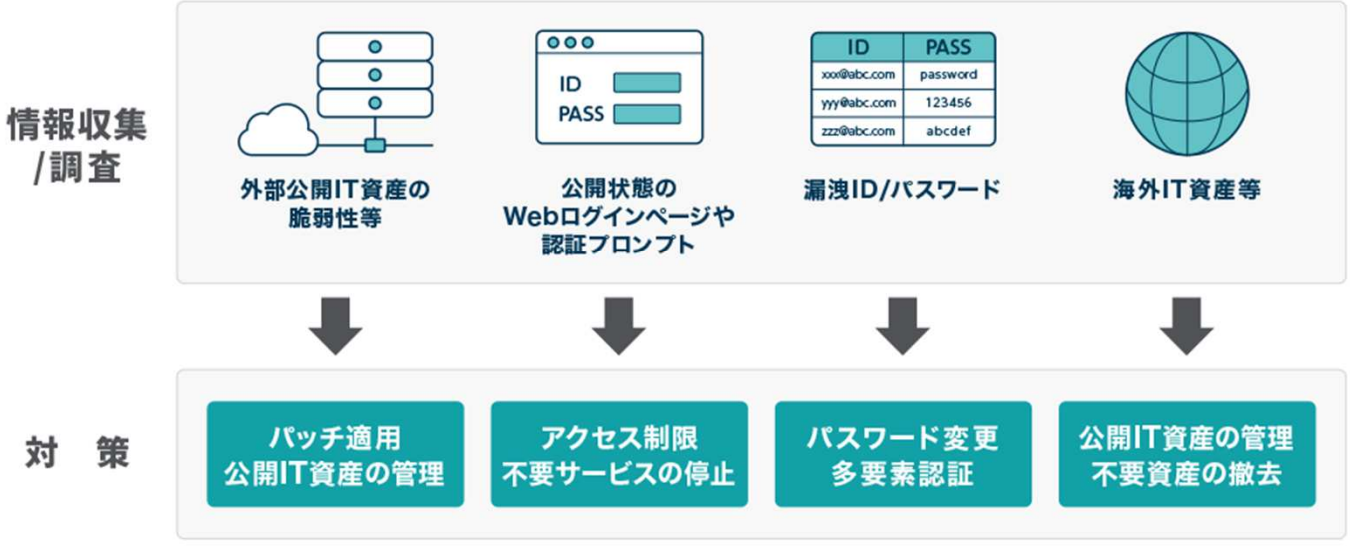
情シス応援価格で提供中

攻撃者目線で企業ネットワークへの侵入口を調査

インターネットに直接接続された外部公開IT資産や、インターネット上に漏洩したユーザーID・パスワードなどのクレデンシャル情報を、攻撃者がターゲット組織を調べる際に用いるものと同じ OSINT※ 手法で調査します。

攻撃者目線で、侵入口やなりすましによるセキュリティリスクを調査することにより、緊急性の高いものから効率的に対策を行うことを支援します。調査に必要な情報は調査対象のドメイン名だけなので、自社のセキュリティリスクだけでなく、海外拠点、グループ企業や取引先といったサプライチェーン全体を調査することができます。

※ Open Source INTelligence



調査報告書のサンプル -1

VPNやリモートデスクトップ、SSH、WEBアプリケーションなど、外部からログインの試行が可能な状態になっているIT資産と漏洩事件などから流出したアカウント、脆弱性のあるIT資産とその脆弱性の内容を報告し、対策を提言します。

侵入口となりうる外部公開IT資産

■ 検出されたエクスポージャー

調査の結果、下記のサービスが公開されております。これらのサービスは攻撃者に頻繁に狙われています。
公開が必要なサービスなのか、いま一度ご確認ください。

IT資産名	IPアドレス	国	サービス名	プロトコル	ポート番号
www.abc.com	x.x.x.x	ドイツ	SSH	TCP	22

```
                    :~$ ssh root@ www.abc.com
root@          www.abc.com          's password:
```

アクセスを許可するIPアドレスを制限するか、制限できなければ認証方式をパスワード認証を禁止し、公開鍵証明書認証を利用することをお勧めします。これにより悪意のある第三者にアカウントが漏れても、アカウントだけではログインが出来なくなります。

www.abc.com	x.x.x.x	ドイツ	FTP	TCP	21

```
                ~$ ftp  www.abc.com
Connected to  www.abc.com
220 Welcome to         ABC Company's        FTP service.
Name (         www.abc.com         : User ):
```

FTPは通信が暗号化されません。認証の通信も平文で行われます。SSHサーバーも動いているようなので、代わりにSCPを使うなど、検討することをお勧めします。

ソフトウェア脆弱性

■ 攻撃リスクの高い脆弱性

攻撃が観測されている脆弱性や、リモートから攻撃可能な攻撃コードが公開されている脆弱性があります。
攻撃が観測されている脆弱性
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
攻撃コードが公開されている脆弱性
https://www.exploit-db.com/

下記はサイバー攻撃を受けるリスクの高い脆弱性となりますので、「対策(JVN)」列のリンク先をご確認の上、対策をご検討ください。
これ以外の脆弱性については別添のエクセルファイルをご参照ください。

No.	CVE-ID	CVSS	タイトル	ホスト名	攻撃観測	攻撃コードの公開	対策 (JVN)
1	CVE-2015-1635	10	複数の Microsoft Windows 製品の HTTP.sys における任意のコードを実行される脆弱性	www.xyz-company.co.jp	有	有	リンク
2	CVE-2018-7584	7.5	PHP におけるバッファエラーの脆弱性	www.xyz-service1.jp	無	有	リンク
3	CVE-2019-0211	7.2	Apache HTTP Server における認可・権限・アクセス制御に関する脆弱性	www.xyz-service1.jp	有	有	リンク
4	CVE-2021-40438	6.8	Apache HTTP Server におけるリモートユーザが選択したオリジンサーバにリクエストを転送される脆弱性	www.xyz-service2.jp	有	無	リンク
5	CVE-2014-0160	5	OpenSSL の heartbeat 拡張に情報漏えいの脆弱性	www.xyz-service2.jp	有	有	リンク

調査報告書のサンプル -2

VPNやリモートデスクトップ、SSH、WEBアプリケーションなど、外部からログインの試行が可能な状態になっているIT資産と漏洩事件などから流出したアカウント、脆弱性のあるIT資産とその脆弱性の内容を報告し、対策を提言します。

発見されたWEB認証画面

■ 検出されたIT資産

調査の結果、下記の認証画面が公開されております。WEBメールの認証画面が公開されています。漏洩アカウントも確認されているので、多要素認証、アクセス元の制限、証明書認証を導入して認証画面を出さないなど、対応を検討される事をお勧めいたします。

IT資産名	IPアドレス	国
vpn.abc.com	x.x.x.x	ドイツ

IT資産名	IPアドレス	国
mail.abc.com	x.x.x.x	日本

発見されたWEB認証画面

■ 検出されたIT資産

調査の結果、下記の認証画面が公開されております。ホスト名や認証画面から、SSL-VPNやリモートデスクトップ環境であることが推測され、攻撃者から特に狙われる可能性があります。漏洩アカウントも確認されているので、多要素認証、アクセス元の制限、証明書認証を導入して認証画面を出さないなど、対応を検討される事をお勧めいたします。

IT資産名	IPアドレス	国
www.abc.com	x.x.x.x	イギリス

IT資産名	IPアドレス	国
desktop.abc.com	x.x.x.x	アメリカ

調査報告書のサンプル -3

VPNやリモートデスクトップ、SSH、WEBアプリケーションなど、外部からログインの試行が可能な状態になっているIT資産と漏洩事件などから流出したアカウント、脆弱性のあるIT資産とその脆弱性の内容を報告し、対策を提言します。

漏えいアカウントのサンプル

推測されるユーザー名	メールアドレス	漏洩事件	ID情報漏えい	パスワード漏えい			その他漏えい情報
				平文	暗号化	ヒント	
あいず mh	mh.aizu@sample.co.jp	Dropbox			●		
あいはら ひろき	hiroki.aihara@sample.co.jp	Adobe	●		●		
いとう しげお	Shigeo.ito@sample.co.jp	Adobe	●		●	●	
		Facebook	●				
		Linkedin			●		
うさみ ようじ	youji.usami@sample.co.jp	Antipublic		●			
おかだ a	a.okada@sample.co.jp	Last.FM		●			
かとう y	y.kato@sample.co.jp	Adobe	●				
		badoo	●		●		生年月日
かとう ひでお	hideo.kato@sample.co.jp	Dropbox			●		
きくち ゆか	yuka.kikuchi@sample.co.jp	Stratfor	●				クレジットカード番号

【ご参考】 漏えいアカウントデータベース

Solitonがインターネット上から収集した漏えいアカウントは **234億件**

漏えい元・リスト名		件数	DB登録済アカウント数
サイバー攻撃でWEBサービスから漏えいしたもの	Twitter facebook YAHOO! Adobe Dropbox LinkedIn etc.	国内 618件 世界 562件	234億
漏えいしたアカウントをもとに攻撃者が不正アクセス用に作成したアカウントのリスト	FORTINET※ Onliner Spambot Exploit.In Phorpiex Phorpiex C2 Anti Public Collection# arkei Stealer etc.	31種類	

※ Fortinet製VPNのログイン情報リスト

【ご参考】 Fortinet の漏えいログイン情報リストも登録済み

2021年9月 インターネット上の捜索で発見した**29万件**のデータもDB登録済みです。

事案NO	ハッキング被害者	国籍	発覚年月	全漏洩数	.JP属性	漏洩内容
G204	FORTINET	米国	2021年9月	29万	140	メールアドレス 平文パスワード
G205	afaqs!	インド	2018年1月	29万	28	メールアドレス 平文パスワード 暗号パスワード
G206	GoogleEarthHacks.com	不明	2019年9月	28万	282	メールアドレス 暗号パスワード
G207	遊戲戰紀	台湾	2017年10月	27万	714	メールアドレス 暗号パスワード
G208	ANN LANDERS	米国	2019年9月	26万	1,067	メールアドレス 平文パスワード

サイバー攻撃リスクを調査

情シス応援価格で提供中

ゼロトラスト時代の多要素認証サービス

認証強化には多要素認証を

お問い合せはこちら bdr@list.soliton.co.jp