

今、気になる

『アタックサーフェス管理』の実際

～サプライチェーンリスクへの備え～

Soliton®

アタックサーフェス ＝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「アタックサーフェス」と呼ばれ「攻撃対象領域」と訳されます。

アタックサーフェス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、アタックサーフェスは増え続けています。

Attack Surface



IPアドレス、ドメイン、
DNSレコード、証明書、
オープンポート
VPN、RDP、GW
バージョン情報、脆弱性
etc...

公開されている
IT資産



海外拠点やサプライチェーンを含めた、管理不十分な公開IT資産がハッカーによるサイバー攻撃の足掛かりになっている

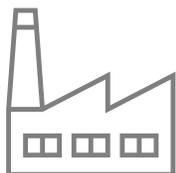
実際に狙われた、アタックサーフェス

2024年 5月 小売業



リモートアクセス装置経由でグループ会社のサーバーに侵入され、ランサムウェアに感染。
被害拡大防止のため、**グループの全サーバーの停止と社内外ネットワークの遮断を実施した。**

2024年 3月 製造業



海外の事業所でネットワークの異常が起き、サイバー攻撃が発覚。工場のネットワークや受注システムが停止し、**サプライチェーンにおいても納期遅延が発生した。**

2024年 5月 住宅メーカー

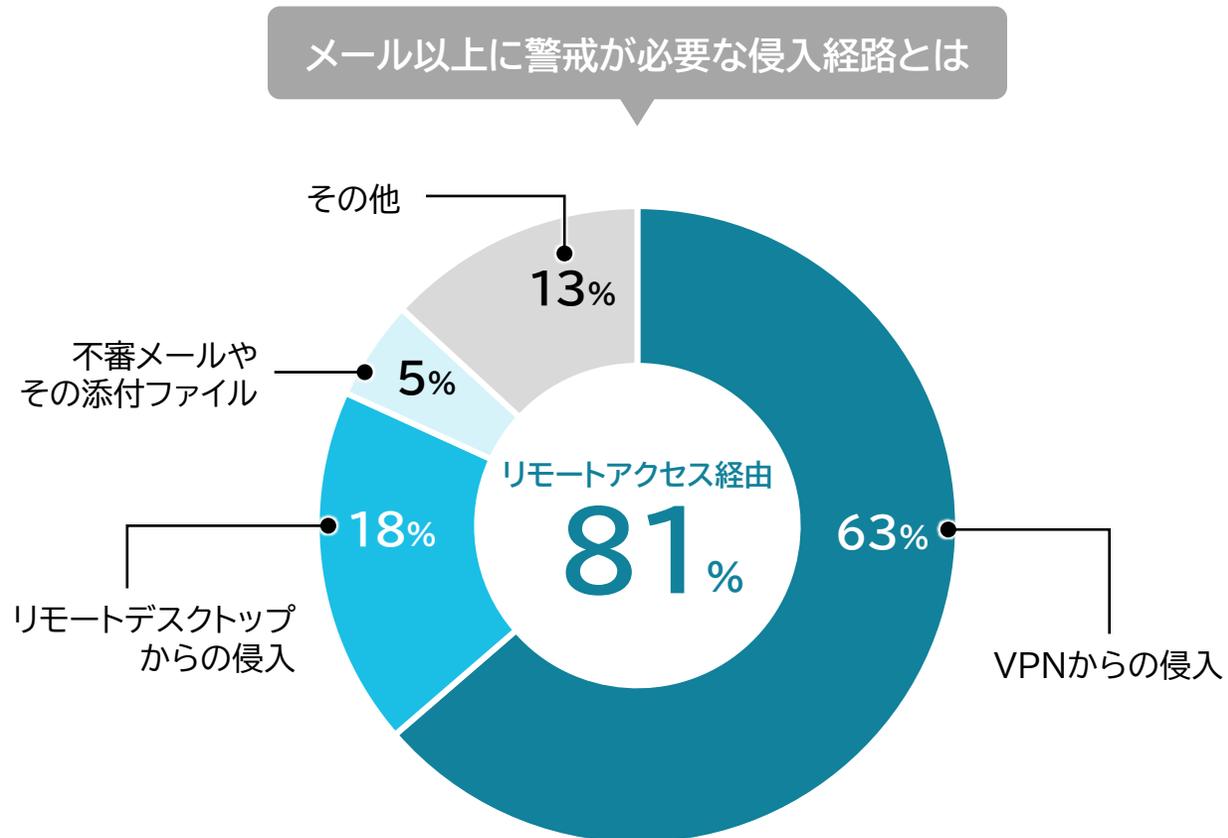


会員制サイトの、現在は運用されていないページ経由で侵入され、顧客情報が流出。
登録されたメールアドレス・ID・パスワードの漏洩が確認され運用を停止した。

アタックサーフェスを狙う 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81%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6年3月14日 警察庁）

令和5年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6年3月14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。)

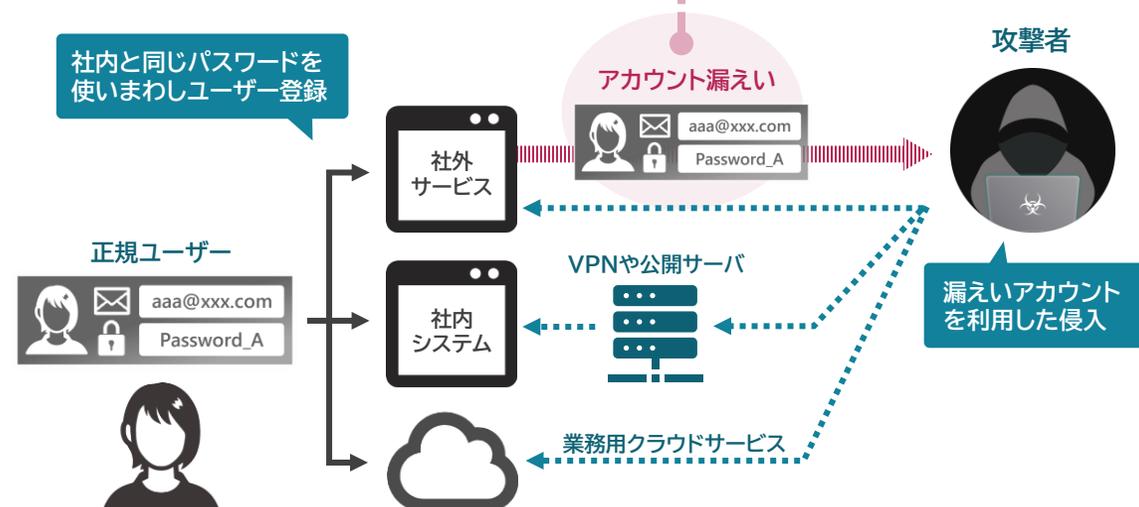
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

アタックサーフェス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、アタックサーフェス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。



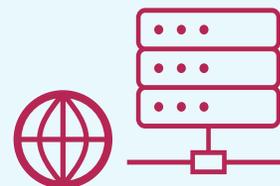
アタックサーフェスを把握し 適切に管理する

近年の重大なインシデントは、自社のアタックサーフェス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アタックサーフェスを把握し、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＝アタックサーフェス管理**が求められています。

外部公開されている
IT資産の脆弱性等



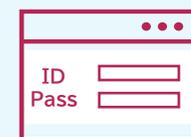
パッチ適用
公開IT資産の管理

漏洩ID/パスワード

ID	パスワード
xxx@abc.com	password
yyy@abc.com	123456
zzz@abc.com	abcdef

パスワード変更
多要素認証

公開状態の
Webログインページや
認証プロンプト



アクセス制限
不要サービスの停止

海外拠点の
IT資産等



公開IT資産の管理
不要資産の撤去

Attack Surface を把握して管理する

攻撃の侵入口を調査し、サイバー攻撃リスクを低減

Soliton®

Attack Surface Management サービス

緊急点検パッケージ

- 基本ドメイン+追加5ドメイン
- 特別価格 70万円(税別)
- 申込後10営業日で納品
- 2024年9月末までの特別パッケージ

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

情報収集 / 調査



外部公開IT資産の
脆弱性等



公開状態の
Webログインページや
認証プロンプト

ID	PASS
xxx@abc.com	password
yyy@abc.com	123456
zzz@abc.com	abcdef

漏洩ID/パスワード



海外IT資産等

対 策

パッチ適用
公開IT資産の管理

アクセス制限
不要サービスの停止

パスワード変更
多要素認証

公開IT資産の管理
不要資産の撤去

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

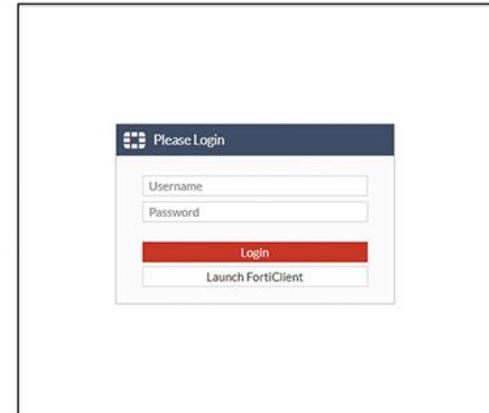


発見されたWEB認証画面

■ 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



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

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	

サイバー攻撃リスクを調査



攻撃の侵入口を調査し、サイバー攻撃リスクを低減

Attack Surface Management サービス

Soliton

45.69 64.78 82.43 9.4 3.6 65

SECURITY

PASSWORD

A person in a suit is holding a smartphone, with a futuristic digital interface overlaid on the screen showing a padlock and various data points.

緊急点検パック提供中

ゼロトラスト時代の多要素認証サービス



Soliton OneGate

企業の情報資産を不正アクセスから守る

多要素認証サービス

<https://www.soliton.co.jp/onegate/>

A blue shield icon is visible on the right side of the advertisement.

認証強化には MFA

お問い合わせはこちら



bdr@list.soliton.co.jp