ID・パスワードだけに頼らない

ネットワークセキュリティ強化策

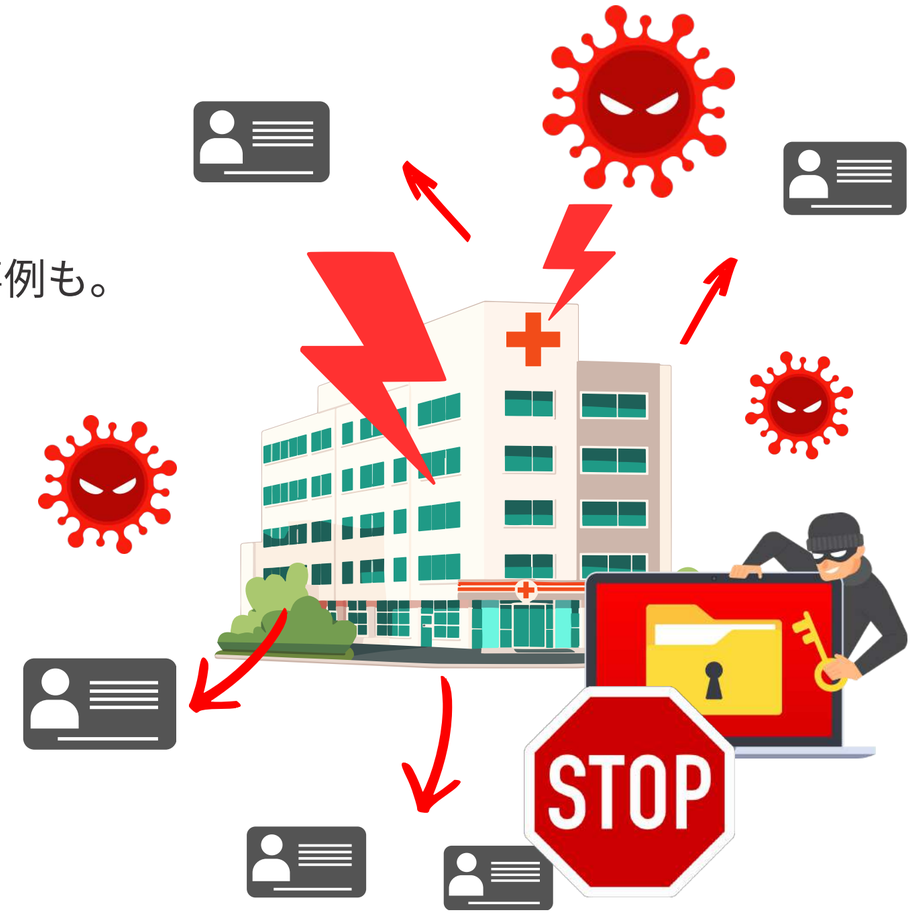
BCC株式会社

もくじ

01 はじめに：巧妙化するサイバー攻撃の現状

リモートアクセスの普及により、
かつての「社内は安全」という境界型防御は崩壊しています。
2024年、国内のとある医療機関が大規模なランサムウェア攻撃を受け、
4万人分以上の個人情報漏洩の懸念とシステム全停止という事態に陥った事例も。

IDとパスワードだけの認証、管理しきれないVPN装置の脆弱性――。
今、情シス担当者に求められているのは、
「利便性を維持しながら、
どうやってゼロトラスト（何も信頼しない）環境へ移行するか」
という視点です。



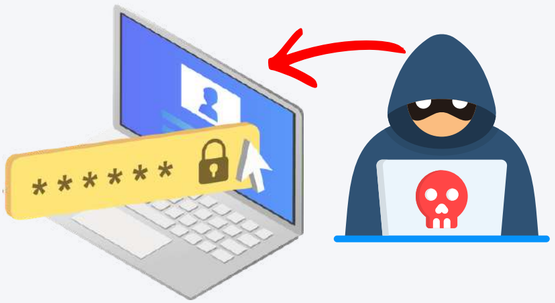
02 【Case Study】国内医療センターが受けた「魔の1週間」

ある医療センターでは、外部接点となるUTM（統合脅威管理）装置の脆弱性を突かれ、侵入を許しました。

攻撃者はわずか1週間の間に、下記の手順で組織を壊滅させました。　※パートナー企業等からの情報を元にした事例です。

初期侵入

ID/PWへの
「辞書攻撃」により
内部へ潜入



検索と破壊

AD（Active Directory）から情報を窃取、
バックアップデータを破壊。
ウイルス対策ソフトすら停止・削除。

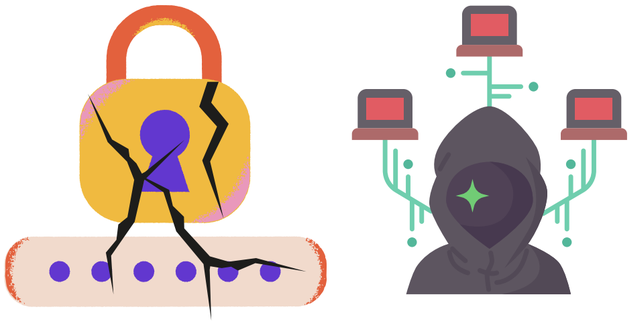
本攻撃

仮想基盤を暗号化。
電子カルテをはじめ
とする全システムが
停止。

03 事例から学ぶ教訓と対策とは

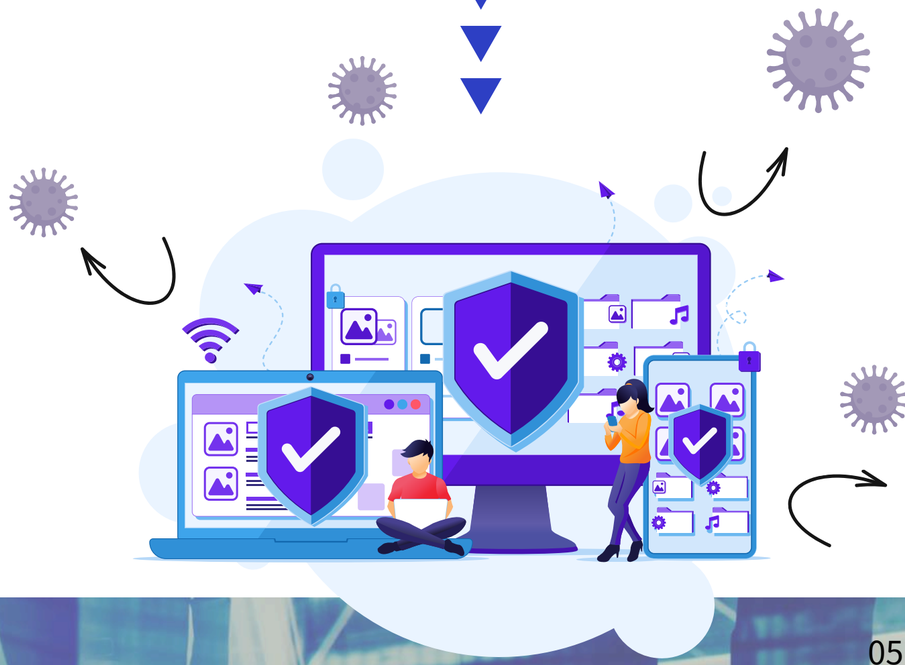
教訓

「入り口」の認証がID/PWのみであったこと、
そして**「侵入後」に自由に動けるネットワーク構造**
であったことで被害が拡大。



対策

毎日の監視と、侵入を前提とした多層防御が不可欠



04 ネットワークの「詰まり」と「死角」を解消するSD-WAN

セキュリティを強固にしても、業務が遅くなっては意味がありません。

「Microsoft 365などのクラウドが重い」「拠点の状況がブラックボックス化している」といった課題を解決するのがSD-WANです。なお、弊社で提供している「Cisco Meraki」（SD-WAN）は、UTMの自動アップデート機能が搭載されており、利便性を確保しつつも攻撃者の初期侵入を許さないネットワークを構築できます。

ローカルブレイクアウト

各拠点からクラウドへ直接接続。SaaSなどの通信はインターネットに流し、輻輳（渋滞）を解消。

可視化と一元管理

ブラウザーつで全拠点のネットワークを把握。属人化を防ぎ、運用工数を大幅に削減。

05 認証の「質」を根本から変える多要素認証（MFA）

SD-WANとの組み合わせでさらに強力なセキュリティとなる多要素認証。
しかし、多くの人が**「二段階認証」**と**「多要素認証」**を混同しています。
同じ要素（例：パスワード＋秘密の質問）を重ねるだけでは、
辞書攻撃やフィッシングを防げません。

これらから**「2つ以上」の異なる要素を組み合わせる**
多要素認証（MFA）こそが、現代の最低ライン。
（例：パスワード＋デジタル証明書）

特に「デジタル証明書」による端末特定は、
ID/PWの漏洩を無効化する極めて有効な手段です。

多要素認証　3つの認証要素

知識	パスワード	生年月日、秘密の質問
所持	デジタル証明書	スマホ、ICカード
生体		指紋、顔認証

二段階認証の要素は一つだけ

06 解決策は　BM X Security plus　～Cisco Meraki × Soliton OneGate～

そこで当社では、世界シェアの高い「**Cisco Meraki**」（**SD-WAN**）に、国産IDaaS初のISMAP認証を取得した
ソリトンシステムズ「**OneGate**」（**多要素認証**）を組み合わせたパッケージをご提供します。

BMX BCC managed cross　Security plus

SD-WAN

全ての通信を
可視化/一元管理

「デジタル証明書」対応　/　クラウド型認証サービス

クラウドをまとめて
多要素認証（MFA）

社内AD等と連携
ID管理の自動化

社内システムも
スマホもSSO

Wi-Fi / VPNの認証も
一元管理

07 専用アプリで手間なく安全なデジタル証明書の配布・運用

「デジタル証明書でのセキュリティの運用は難しそう、手間が増えそう。。。」そんな心配はご無用です。
One Gate専用のデジタル証明書導入・運用アプリをご用意しており、管理者様のお悩みを解決します。

マルチOS対応

全OS同じ手順で
デジタル証明書を取得

利用者も管理者も低負担

ブラウザの設定や
ActiveXは不要
ヘルプデスク工数ほぼゼロ

不正コピーが一切できない

不正接続を許さない仕組みで
リモートワークを促進

社外ユーザーへ

MDMで管理していない、
協力会社・取引先の
端末・ユーザーもOK

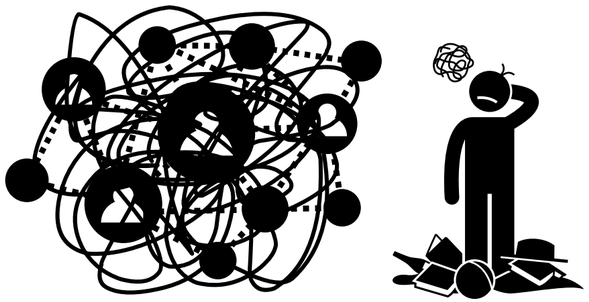
ワンタッチ証明書配布

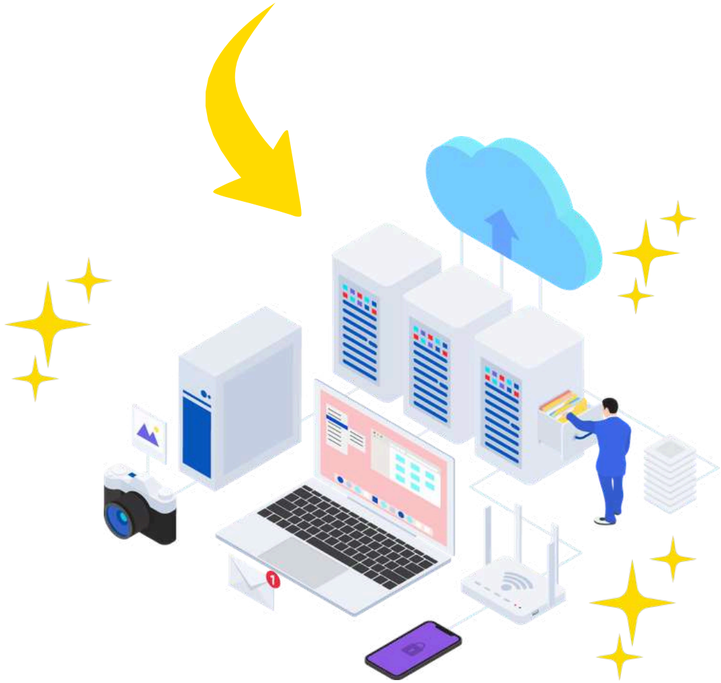
ユーザー操作を
最小限に

◆オンプレもクラウドも対応
◆AD/Entra ID、Intune連携対応
etc...

08 BCCが選ばれる理由：ブラックボックス化したネットワークを「見える化」

「運用はできるかもしれないけど、自社のネットワーク構成がどうなっているか、実は誰も把握できていない……」 実は、多くのお客様からいただくご相談です。
そんなお悩みを当社はお客様と共に解決してきました。





現状の紐解きから伴走

構成が不明確な状態からでも、複雑に絡み合ったネットワークを一つひとつ紐解きます。

ブラックボックスの解消

「どこに、何が、どう繋がっているか」をオープン化し、属人化を排除。

「お任せ」できる安心感

可視化されたネットワークを基盤に、日々の監視からトラブル対応まで、専門チームがまるごとサポート。

09 まとめ：セキュリティ強化を、まるっとお任せ

セキュリティ対策は、個別の製品を導入するだけでは不十分です。
「どのような攻撃に対し、どの範囲をカバーするか」を俯瞰し、貴社の要件に合わせて最適化する必要があります。

「リモートアクセスを安全にしたい」
「自宅のセキュリティ環境を底上げしたい」
「まずは自社のネットワーク構成を整理したい」

その悩み、まるごと弊社にて引き受けます。
まずはお気軽に貴社の現在の状況をお聞かせください！

お問い合わせはこちらから

会社概要

商号	ＢＣＣ株式会社		
事業所	東京本社 ：東京都千代田区外神田６-15-９ 明治安田生命末広町ビル９Ｆ 大阪本社 ：大阪市中央区今橋2-5-8 トレードピア淀屋橋9Ｆ		
代表取締役社長	伊藤一彦		
創立	2002年3月	主要部門	・営業アウトソーシング ・ソリューション
カンパニー名	IT営業アウトソーシングカンパニー	カンパニー長	松村健太
許認可	一般労働者派遣事業（派27-302361） 有料職業紹介事業（27-ユ-302045） プライバシーマーク認定（第10861424(07)号） 電気通信事業（E-28-03972)		
主要取引先	株式会社インターネットイニシアティブ(IIJ) 日鉄ソリューションズ株式会社 ダイワボウ情報システム株式会社 日本電気株式会社(NEC) 富士ソフト株式会社		