忙しい人のための統合型SASEソリューション
Cisco Secure Connect

2024年3月27日

シスコシステムズ合同会社
セキュリティ事業部
セキュリティセールススペシャリスト　藤田 佑未子
ソリューションズエンジニア　谷 裕一朗

Agenda

- セキュリティ最新動向と中小企業を取り巻く環境
- SASEとは
- Ciscoが提供する統合SASEとは
- Cisco Secure Connectがお客様の課題を解決
- デモンストレーション
- ライセンス
- Q&A

セキュリティ最新動向と中小企業を取り巻く環境

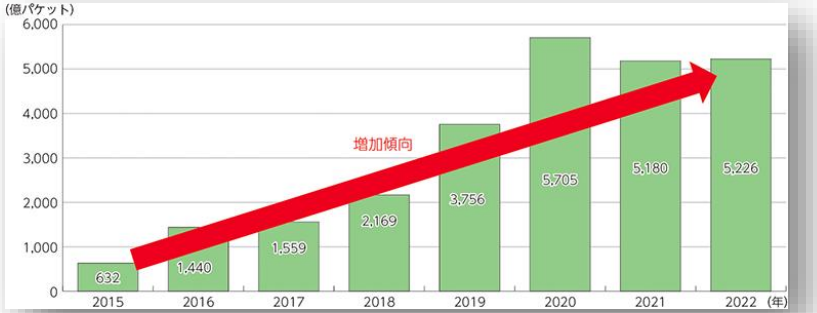
ルータなどIoT機器を狙ったサイバー攻撃が増加

情報セキュリティ10大脅威　2024

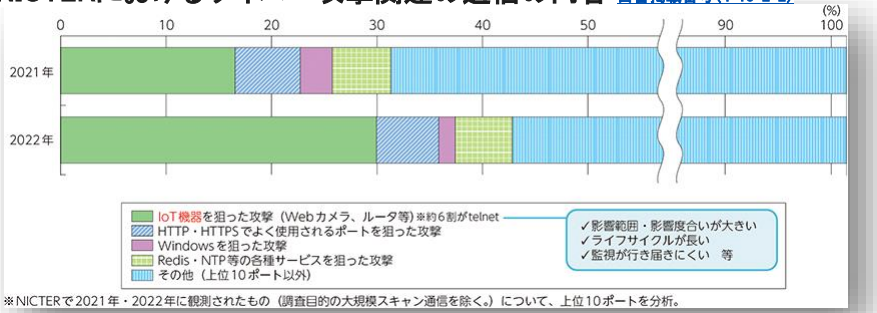
順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

出典：「情報セキュリティ10大脅威 2024」（IPA 独立行政法人　情報処理推進機構）
https://www.ipa.go.jp/security/10threats/10threats2024.html

NICTERにおけるサイバー攻撃関連の通信数の推移 白書掲載番号(4-10-2-1)

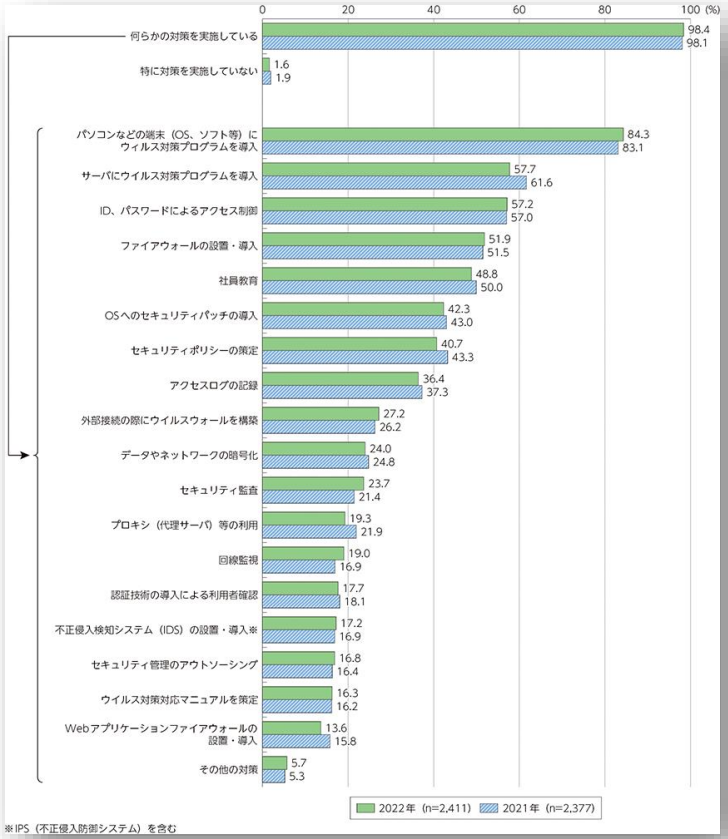


NICTERにおけるサイバー攻撃関連の通信の内容 白書掲載番号(4-10-2-2)



出典：「令和5年版情報通信白書」（総務省）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00262

企業における情報セキュリティ対策の実施状況



- 何らかの対策を実施していると回答している企業が98.4％だが、ウィルス対策プログラムによる対策が中心
- ファイアウォールの設置でも51.9％
- トラブル時に必要となるアクセスログの記録は36.4％
- クラウド利用が進む中で求められるプロキシやWebアプリのセキュリティ対策は20％以下

まだまだセキュリティ対策不足！

出典：「令和5年版情報通信白書」（総務省）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00262

業界ごとに様々セキュリティガイドラインを策定

厚労省「医療機関等におけるサイバーセキュリティ対策の強化について」

1　サプライチェーンリスク全体の確認

上記の通り、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

2　リスク低減のための措置

○パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。

○IoT 機器を含む情報資産の保有状況を把握する。

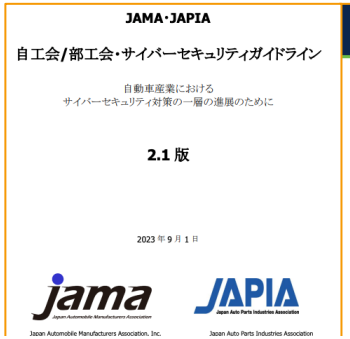
○VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

○悪用が既に報告されている脆弱性に関連する攻撃の痕跡の有無を確認するなど、開発元が推奨する対策が全て行われていることを確認する。

○VPN 機器に対する管理インターフェースへのアクセスは、必要最小限の通信制限を実施する。

○メールの添付ファイルを不用意に開かない訓練を行う。不審メールは、連絡・相談を迅速に

自工会サイバーセキュリティガイドライン


JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

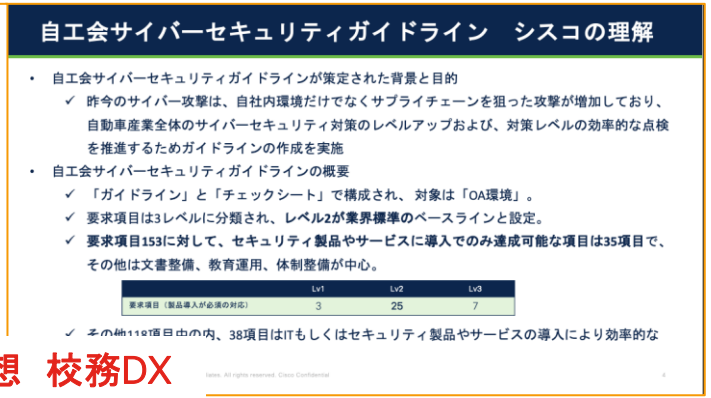
自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.1 版

2023 年 9 月 1 日

jama Japan Automobile Manufacturers Association, Inc.

JAPIA Japan Auto Parts Industries Association


自工会サイバーセキュリティガイドライン　シスコの理解

- 自工会サイバーセキュリティガイドラインが策定された背景と目的
  - ✓ 昨今のサイバー攻撃は、自社内環境だけでなくサプライチェーンを狙った攻撃が増加しており、自動車産業全体のサイバーセキュリティ対策のレベルアップおよび、対策レベルの効率的な点検を推進するためガイドラインの作成を実施
- 自工会サイバーセキュリティガイドラインの概要
  - ✓ 「ガイドライン」と「チェックシート」で構成され、対象は「OA環境」。
  - ✓ 要求項目は3レベルに分類され、**レベル2が業界標準のベースラインと設定。**
  - ✓ **要求項目153に対して、セキュリティ製品やサービスに導入でのみ達成可能な項目は35項目で、**その他は文書整備、教育運用、体制整備が中心。

	Lv1	Lv2	Lv3
要求項目（製品導入が必須の対応）	3	25	7

- ✓ その他118項目中の内、38項目はITもしくはセキュリティ製品やサービスの導入により効率的な

教育委員会　GIGAスクール構想　校務DX

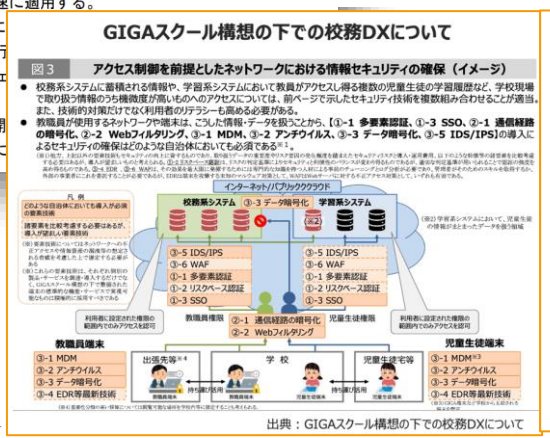

GIGAスクール構想の下での校務DXについて

図３　アクセス制御を前提としたネットワークにおける情報セキュリティの確保（イメージ）

- 校務系システムに蓄積される情報や、学習系システムにおいて教員がアクセスし得る複数の児童生徒の学習履歴など、学校現場で取り扱う情報のうち機微度が高いものへのアクセスについては、前ページで示したセキュリティ技術を複数組み合わせることが適当。また、技術的対策だけでなく利用者のリテラシーも高める必要がある。
- 教職員が使用するネットワークや端末は、こうした情報・データを扱うことから、【①-1 多要素認証、①-3 SSO、②-1 通信経路の暗号化、②-2 Webフィルタリング、③-1 MDM、③-2 アンチウイルス、③-3 データ暗号化、③-5 IDS/IPS】の導入によるセキュリティの確保はどのような自治体においても必須である※1。

インターネット/パブリッククラウド

校務系システム　③-3 データ暗号化　学習系システム

③-5 IDS/IPS　③-6 WAF　①-1 多要素認証　①-2 リスクベース認証　①-3 SSO

②-1 通信経路の暗号化　②-2 Webフィルタリング

教職員端末　③-1 MDM　③-2 アンチウイルス　③-3 データ暗号化　③-4 EDR等最新技術

児童生徒端末　③-1 MDM※3　③-2 アンチウイルス　③-3 データ暗号化　③-4 EDR等最新技術

出張先等※4　学校　児童生徒宅

出典：GIGAスクール構想の下での校務DXについて


ガイドライン対応に必要な製品

必要な製品	ガイドライン対応	Microsoft製品	Cisco製品
認証基盤	●	Azure AD(A3ライセンス) A3ライセンス	なし
MDM	●	Intune(A3ライセンス)	なし
端末の2要素認証	●	Windows Hello for business (A3ライセンス)	Cisco Duo おすすめ
SaaSの2要素認証	●	Azure AD 多要素認証(A3ライセンス)	Cisco Duo
Identity Aware Proxy (完全なゼロトラストを目指す場合)	●	Application Proxy(A3ライセンス)	Cisco Duo / Cisco+ Secure Connect
EDR	●	Microsoft Defender for Endpoint P2(A5ライセンス)	Cisco Secure Endpoint
リモートアクセスVPN (校務支援システムがオンプレの場合)	●	なし Microsoft不足分	Cisco+ Secure Connect
クラウドFW	●	なし	Umbrella SIG / Cisco+ Secure Connect
クラウドプロキシ	●	なし	Umbrella SIG / Cisco+ Secure Connect
CASB(SaaSセキュリティ)	△	Cloud Apps ©Microsoft 365 Defender (旧)Microsoft Cloud App Security(A5ライセンス)	Umbrella SIG / Cisco+ Secure Connect
メールセキュリティ	●	Exchange Online Protection (EOP) Microsoft Defender for Office 365 P2 (A5ライセンス)	Email Threat Defense
SaaS通信の可視化	△	なし	Thousand Eyes
SIEM、XDR etc	△	Azure Sentinel(別途従量課金※特典あり)	SecureX

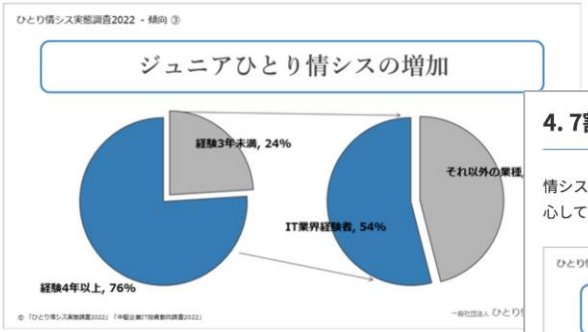
Microsoft A3 + Cisco Securityの、
必要な対策のみを選ぶ、アラカルトをおすすめします

価格メリットあり！
シスコでまとめることでのボリュームディスカウントも

中小企業のひとり情シスでは負担が増加

3. 経験3年未満のひとり情シスの増加

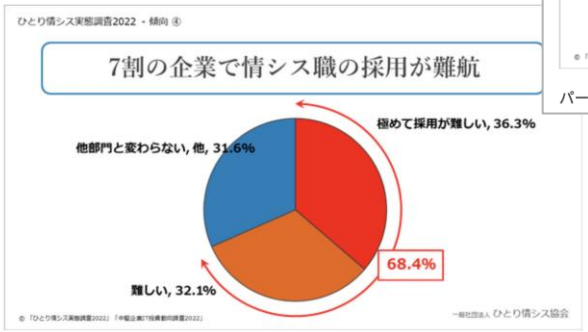
ベテランひとり情シスの定年退職や転職などの後任として情シス経験の浅いひとり情シスが増加している。ひとり情シスの24%が3年未満の経験であることが判明。社内の管理部門や技術部門から異動して着任する場合と、IT業界の勤務経験者の転職が54%を占めた。



経験3年未満の情シスの増加

4. 7割の企業で情シス職の採用が難航

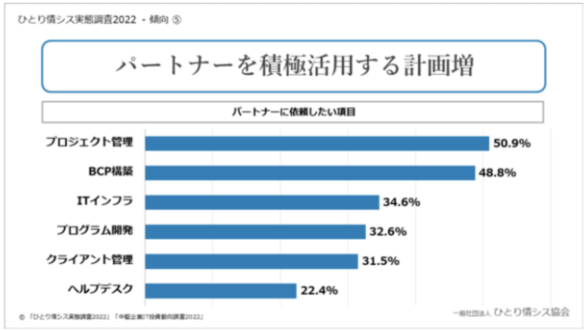
情シスの採用に積極的になる反面、極めて採用が難しいと感じる企業が36%な
心している姿が報告された。主な理由は給与面、必要とスキルのアンマッチ。



情シス職の採用を難しく感じる

5. 半数以上の企業がパートナーを今後積極活用

ひとり情シスの業務量増大に伴い外部パートナーの積極活用の方針が強まっている。比較的軽度なPCクライアント管理やヘルプデスクなどのアウトソーシング活用よりも、プロジェクト管理やBCP環境構築などのプロフェッショナルワークの外部委託意向が鮮明になった。



パートナーを積極活用する計画増

出典:「ひとり情シス実態調査2022年」(一般社団法人　ひとり情シス協会)
https://promit.gr.jp/2022/01/26/476/

SASEとは

これまでのセキュリティ対策はパッチワーク

データ漏洩

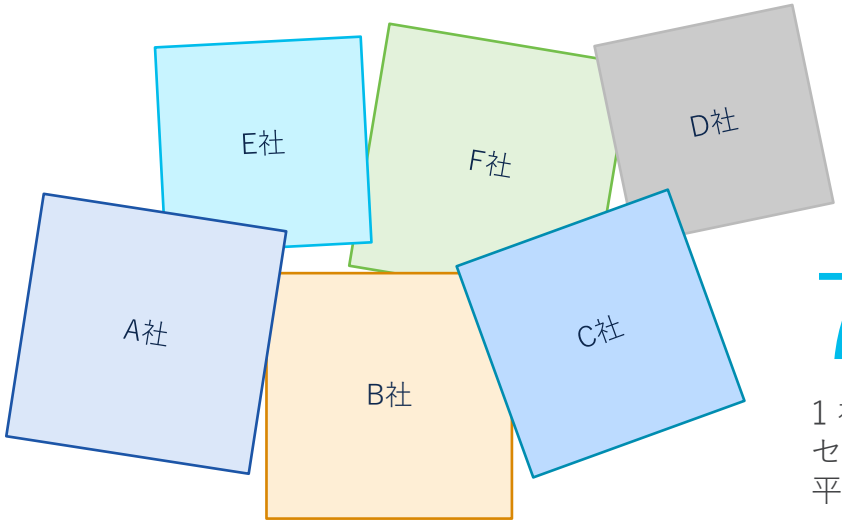
ランサムウェア

ラテラルムーブメント

Web の脅威

クレデンシャルの盗用

スパム



バラバラなポリシー管理

76

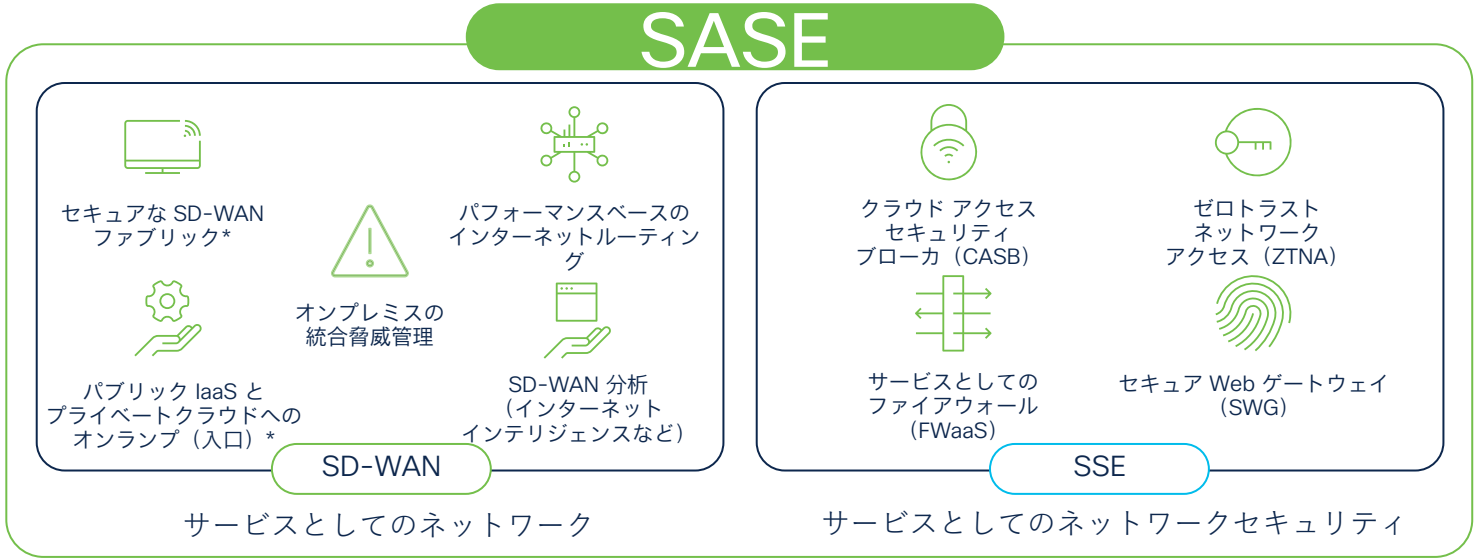
1 社で使われている
セキュリティツールの
平均数

新たな脅威が新たなベンダーを生み、顧客に重荷を負わせている

SASE (Secure Access Service Edge)とは

ネットワークとネットワークセキュリティを**統合**し、クラウドサービスとして提供するセキュリティフレームワーク（2019年にアメリカIT調査企業のガートナー社が提唱）

→クラウド利用の増加、リモートワークの浸透、新たな脅威の出現に対応する



Ciscoが提供する統合SASEとは

Cisco Secure Connectの嬉しいポイント

1. 実績のあるCiscoの MerakiとUmbrellaの統合で安心
   - Ciscoセキュリティの導入実績が多数ある既存サービスがベースで安心
2. 単一ベンダー統合SASEにより管理負荷軽減
   - Meraki管理画面から設定、変更、ログ確認が可能
   - 拠点側、クラウド側かかわらず問い合わせ窓口が統合され、迅速に問題解決
3. 簡単な設定、障害対応機能で運用工数削減
   - AutoVPNで拠点から数クリックでSecure ConnectにTunnel接続
   - 障害時も自動フェールオーバーで安心
4. シンプルなライセンス体系でスモールスタート可能
   - 1ライセンスからのユーザライセンスで、拠点数やデバイス数による課金は無く管理がシンプル

セキュリティはシスコの最重要戦略 ～売上世界3位～

1995年からセキュリティ関連企業を
32社買収し、業界で最も広範囲な
セキュリティーポートフォリオを保有

VALTIX　Lightspin

ORT　PINACL

ISOVALENT　Armorblox

splunk>

売上世界第3位

Palo Alto Networks	8.7%
Fortinet	7.0%
Cisco	**6.1%**
CrowdStrike	3.6%
Check Point	3.5%
Okta	3.2%
Microsoft	3.2%
IBM	2.9%
Symantec	2.9%
Trellix	2.7%
Zscaler	2.4%
Trend Micro	2.3%
Others	51.4%
All vendors	100.0%

参考:Canalys Cybersecurity Market Pulse: Q1 2023

世界最大規模の民間セキュリティ
研究機関であるCisco Talosを
保有し、約500名の分析官が
毎日5,500億件のイベントを観測

Talos

主なアライアンス先

NISC 内閣サイバーセキュリティセンター

NATO OTAN

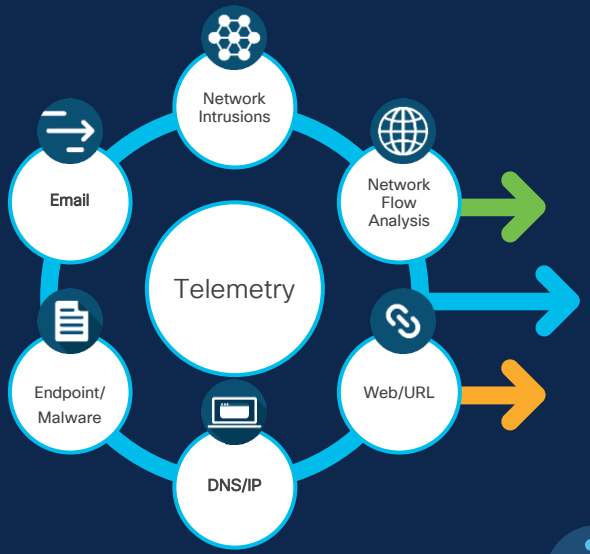
JPCERT CC®

INTERPOL

cisco SECURE

Cisco Talos

世界最大規模のセキュリティインテリジェンス&リサーチチーム



Cloud – Public, Private

TALOS

200億
1日の脅威ブロック数

200以上のゼロデイ脆弱性
1年間の検出数（全く新しい脅威）

圧倒的なデータ量

6000億
1日あたりの電子メールメッセージ数

280万
1日あたりのマルウェアのサンプル

160億
1日に監視されるWebリクエスト

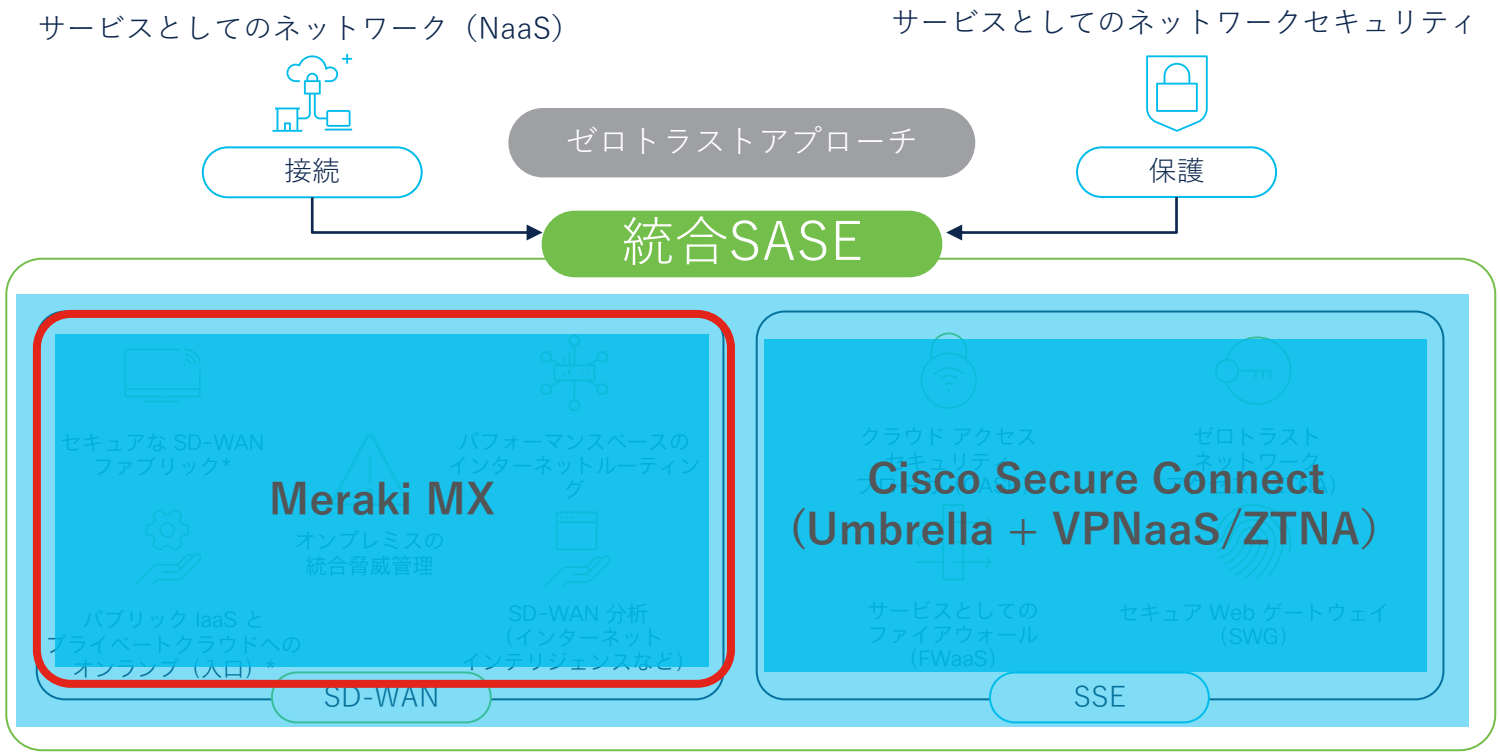
5500億
1日あたりの観測されるセキュリティイベント

世界最大規模の組織

500人以上
フルタイムの脅威インテリジェンス担当者

100社以上
脅威インテリジェンスパートナー

シスコが提供する統合SASE Cisco Secure Connect



*リモートワーカーに対応

クラウド管理型ネットワークのCisco Meraki

クラウドからアクセスポイントを管理して18年

MV
スマートカメラ

MT
IoT センサー

SM
MDM

MR
アクセスポイント

MS
（PoE）スイッチ

MX
UTM/
SD-WAN ルータ

MG
セルラー
ゲートウェイ

77万4,000以上
顧客数

400万以上
顧客ネットワーク数

1,200万以上
オンラインのMeraki デバイス数

190以上
ネットワークが位置する国数

99.99%
クラウド SLA

60億以上
1 か月あたりの外部 API 呼び出し数

1億9,000万以上
1 日あたりのエンドユーザデバイス接続数

2億5,000万以上
1 日あたりのスプラッシュページ利用数

cisco SECURE

Meraki MXとは？

3つの機能を1 Boxで提供

① SD-WAN（WANの制御）

自動 VPN

高可用性 / フェールオーバー

② UTM（セキュリティ）

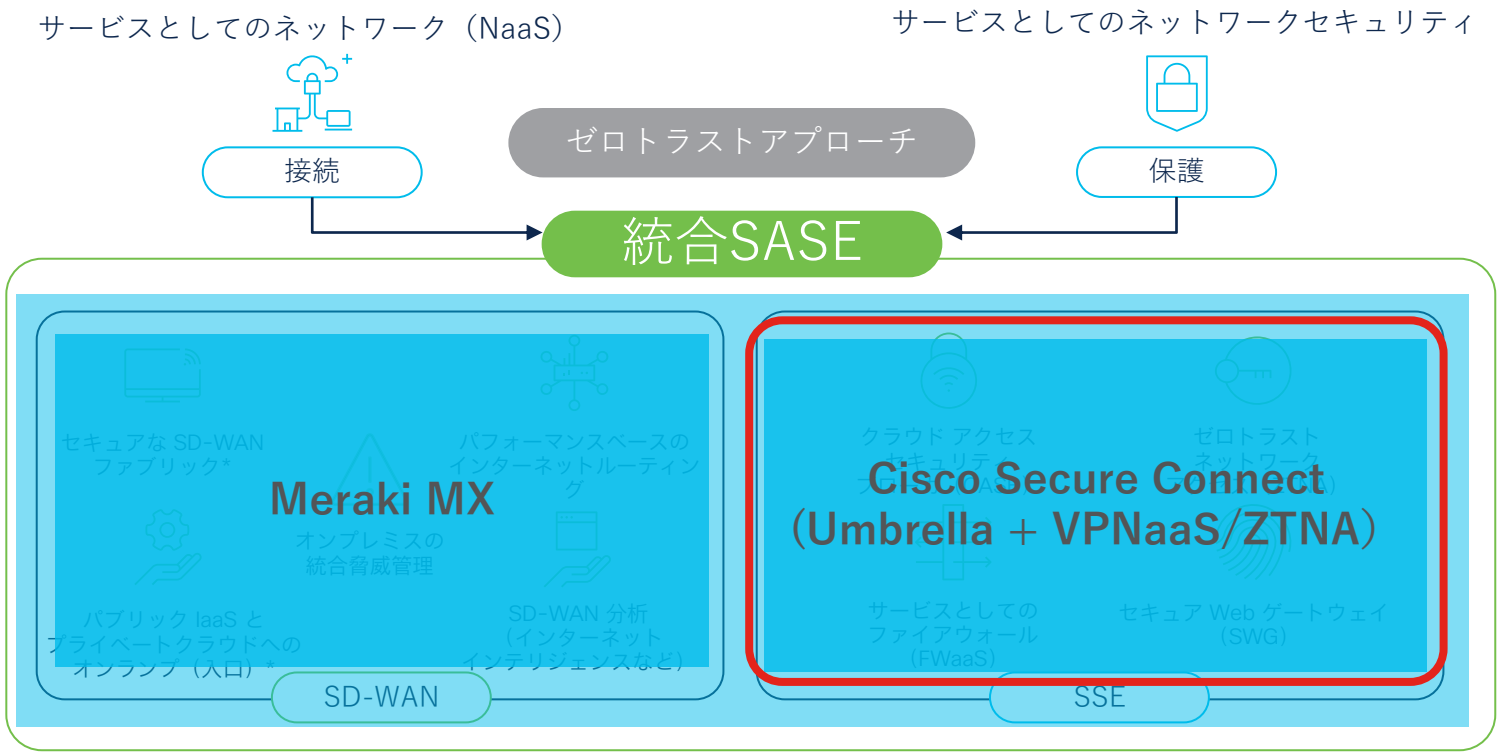
侵入防御システム

高度なマルウェア防御

③ Visibility（可視性）

アプリの可視化と制御

シスコが提供する統合SASE Cisco Secure Connect



*リモートワーカーに対応

インターネットアクセスセキュリティ　Umbrella

クラウド提供型の境界セキュリティ

- DNS レイヤ セキュリティ
- セキュア ウェブ ゲートウェイ
- URLフィルタリング
- HTTPS復号
- フルアクセスログ
- クラウド提供型 ファイアウォール (L3-4, L7)
- クラウド提供型 IPS
- 情報漏えい 防止 (DLP)
- ウェブ分離 (RBI)
- インタラクティブ 脅威インテリジェンス
- クラウド セキュリティ アクセス ブローカ (CASB)
- アプリケーション制御
- SaaSテナント制御
- マルウェア対策 (Sandbox)
- クラウドマルウェア検知

ロードマップ

HTTPS復号のクラウド化

- サイジング不要なクラウド化
- 機器更改の負担を最小化

SaaS利用の可視化

- 使用したアプリを可視化
- 重要情報のアップロードを検知

不正コンテンツ阻止

- マルウェアなど不正なコンテンツの防御
- Web閲覧に組織のポリシーを適用

Umbrella導入実績

グローバルで26,000社以上で実績があり、国内でも様々な業種で幅広くご採用いただいています。

導入事例：株式会社 日立製作所

日立製作所がゼロトラスト実装に向けたSASEを導入

日立製作所は、働き方の多様化やデジタル活用の進展によって、人やモノ、システム、データが社内外に分散してしまった現在、ゼロトラストに基づき、人とモノの信用を担保するための仕組を実現するためにシスコのSASEを活用し、セキュリティの再構築を進めています。

ビデオを観る (1:54)　事例を読む

武蔵野赤十字病院

クラウド型セキュリティソリューション Cisco Umbrella を導入し、インターネット通信そのものを監視。初期費用を抑え、シンプルで安全なネットワーク環境を実現。

Cisco Start 事例を読む（PDF - 1.2 MB）

株式会社北國銀行

全拠点からのローカルブレイクアウトとエンドポイントセキュリティ強化によりクラウド時代のワークスタイル環境を実現

事例を読む(PDF - 952KB)

日本郵便株式会社

全国 2 万以上の郵便局業務を支えるタブレットでの安全な Web アクセスを確保

事例を読む(PDF - 1.64 MB)

奈良市教育委員会

GIGA スクール構想、1 人 1 台端末時代に即したセキュリティとして Cisco Umbrella を導入

事例を読む(PDF - 1.45 MB)

高いセキュリティ検知率

SWGセキュリティ AV-TEST による検証結果 2022

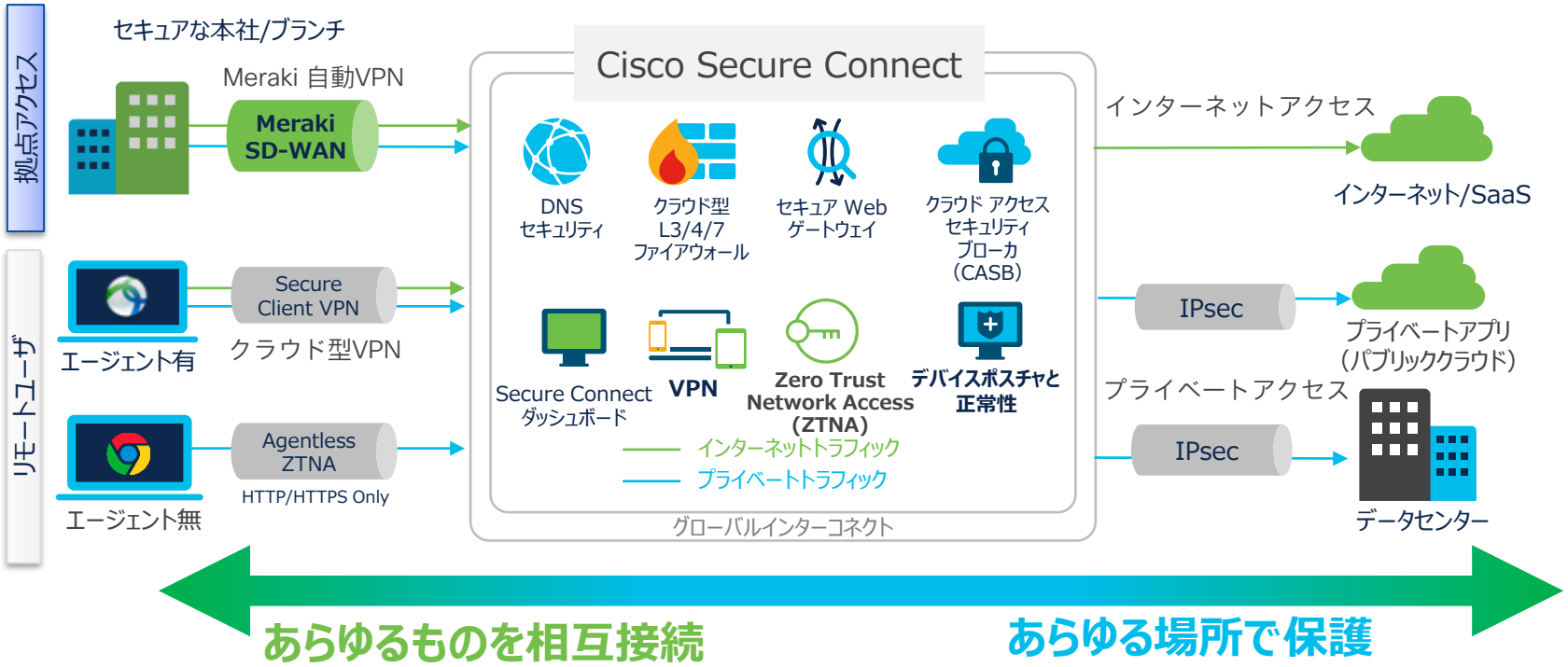
- AV-TESTが6月～9月に同社のサンプルを使用して取得したデータ（Ciscoには不明）
- 最高レベルの保護を提供するように設定された製品
- アンブレラSWGもDNSセキュリティポリシーを適用

Type of test	Umbrella	Netskope	Zscaler	PAN	Skyhigh (McAfee)	Iboss
Malicious PE files (Portable executables)	85.89	86.21	76.80	90.07	65.83	60.29
Malicious destinations	98.04	94.46	87.90	73.77	62.61	32.05
Phishing links	84.83	58.43	71.91	77.69	64.13	47.43
Total detection rate	90.41	80.12	79.60	79.33	63.96	44.60

% Detected (higher is better)

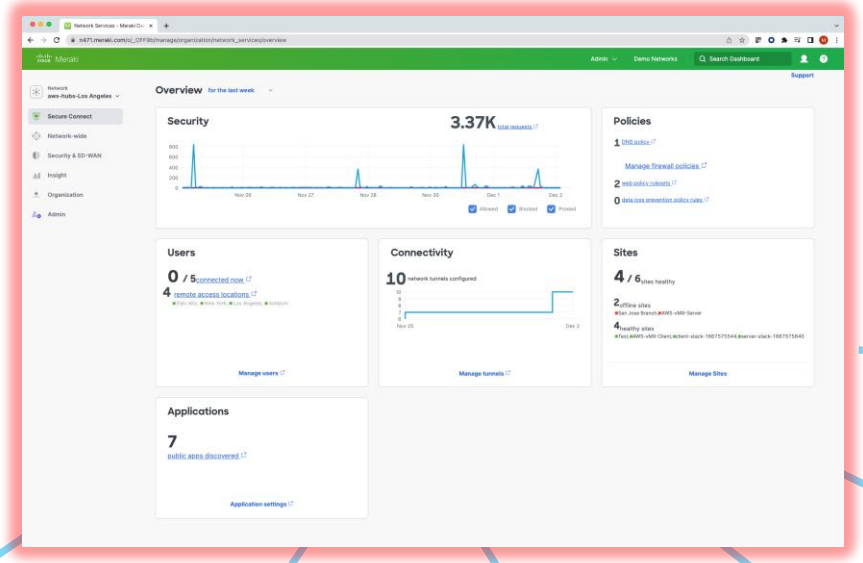
Cisco Secure Connect

Meraki MX連携 や リモートアクセス要件にも対応した SASEソリューション



ネットワークとセキュリティの統合ダッシュボード

すべてのデバイスとネットワーク/セキュリティ設定を 1 つのダッシュボードで管理



スマートカメラ
（MV）

センサー
（MT）

モバイルデバイス
管理（SM）

ワイヤレス（MR）

セルラー（MG）

セキュリティと
SD-WAN（MX）

スイッチ
（MS）

セキュリティと
SD-WAN（MX）

Secure Client

Secure Connect

cisco SECURE

Ciscoの考えるSASE /ゼロトラストへのステップ

一気にZTNAへ移行しようとすると
利用アプリの把握や非対応アプリなどにより
失敗する例が多い

よくある課題

- ネットワーク集中による負荷増大
- ネットワーク機器管理の手間
- 脆弱性対策、セキュリティ維持運用

解決できること

- VPN機器管理不要
- クラウド型VPN Head-endが処理を行うため、**サイジング不要**
- デバイスポスチャ機能でアクセス時のセキュリティ強化

利用者への影響

- **利用者はVPN接続先が変わるのみ**

＋解決できる課題

- 外部の人のアクセスや最重要なアプリから**無理なくZTNA化可能**

利用者への影響

- ZTNA化したアプリの接続先が変更になるのみ

cisco SECURE

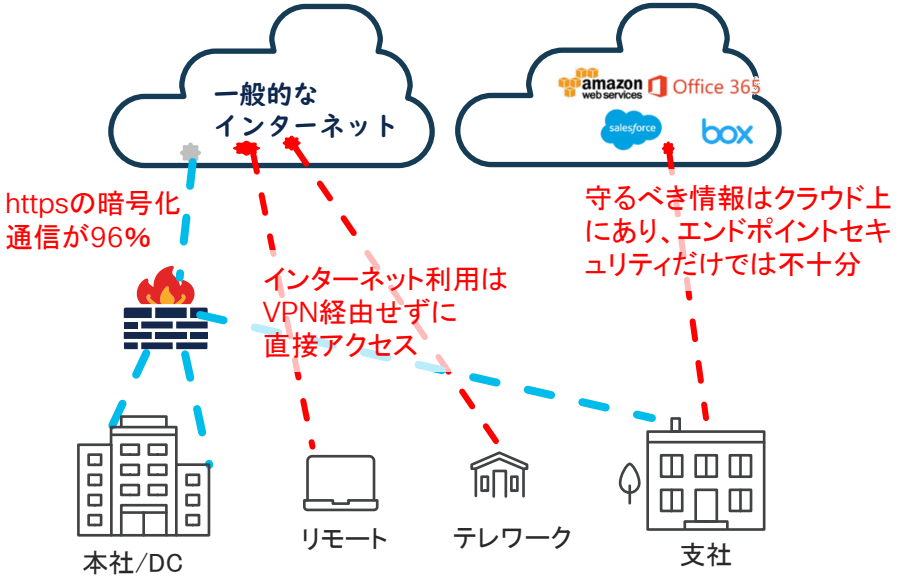
Cisco Secure Connectがお客様の課題を解決

cisco SECURE

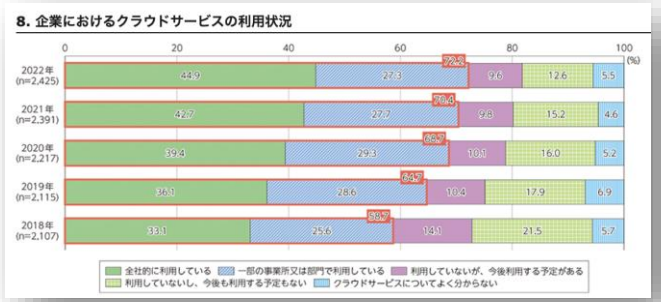
課題1　リモートワーク/クラウド活用の拡大への対応

守るべき対象がクラウドに変わりつつあり、UTMやエンドポイントセキュリティだけでは不十分

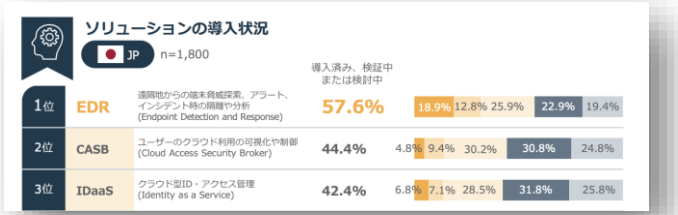
クラウドサービス利用の拡大に対して、クラウドアプリの利用の可視化や制御の対策は遅れている

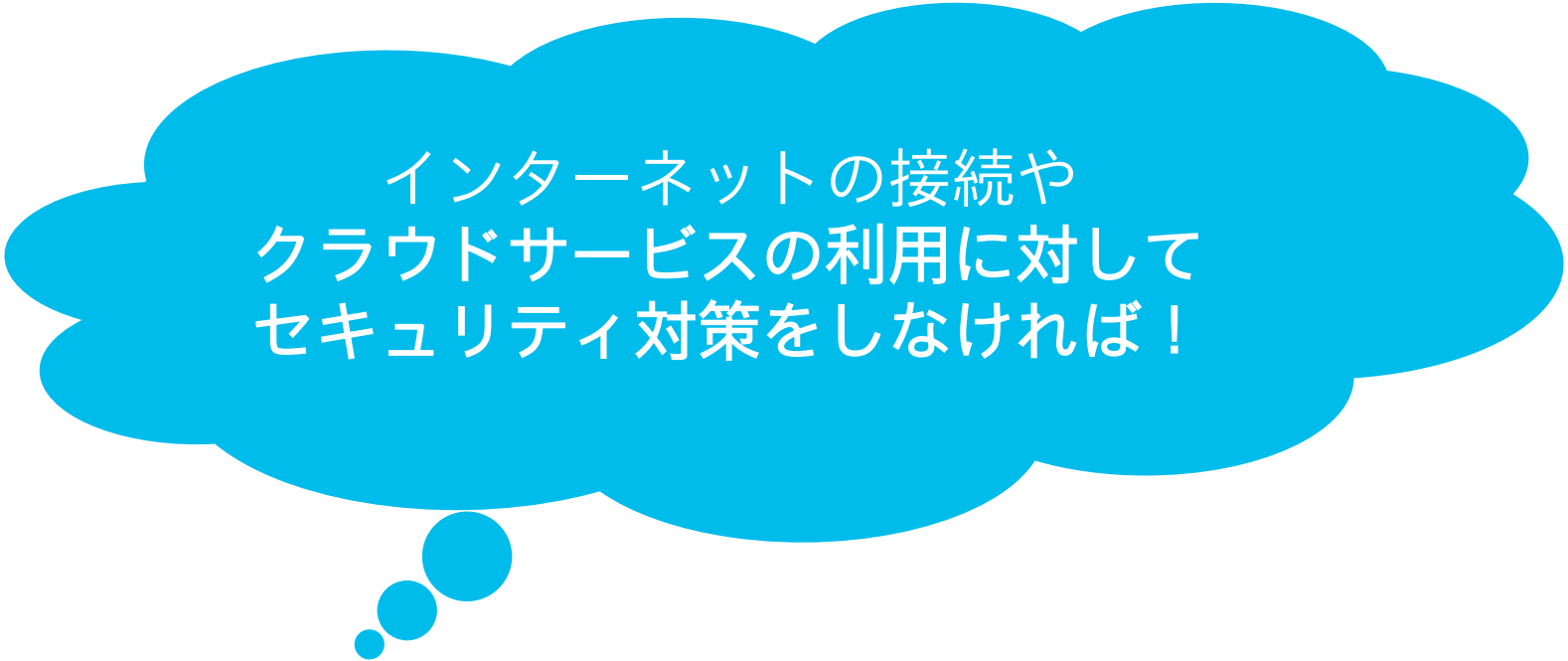


総務省「情報通信統計白書」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html



NRIセキュア「企業における情報セキュリティ実態調査」
https://www.nri-secure.co.jp/download/insight2022-report





インターネットアクセスセキュリティ

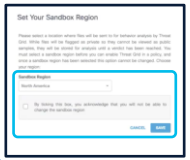
インターネットやクラウドアプリを利用する際に必要となるセキュリティ機能を統合して提供

①危険なサイトへのアクセスをブロック

- DNS レイヤ セキュリティ
- セキュア ウェブ ゲートウェイ
- URL フィルタリング
- HTTPS復号
- クラウド提供型 ファイアウォール (L3-4, L7)
- クラウド提供型 IPS

②Webサイトやクラウドストレージから マルウェアをブロック

- マルウェア対策 (Sandbox)
- クラウドマルウェア 検知

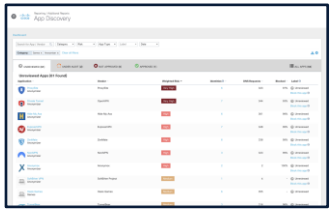


ダウンロードされるファイルに隠された脅威を検出し、アラートを表示

クラウドリポジトリをスキャンし、保存されたファイルをリアルタイムでスキャン

③クラウドアプリの利用の可視化・制御

- クラウド セキュリティ アクセス ブローカ (CASB)
- アプリケーション 制御
- SaaSテナント 制御
- 情報漏えい防止 (DLP)



④すべてのアクセスログを一元管理

- フルアクセスログ

定期的にS3にログを出力。
お客様環境のS3への出力も可能

cisco SECURE

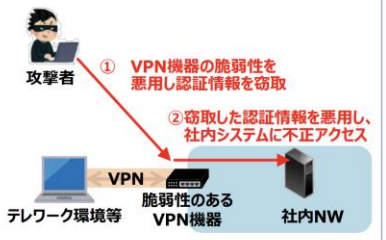
課題②　VPN機器の脆弱性対応

経済産業省「サイバーセキュリティに関連する海外の動き」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/008_04_00.pdf

VPN機器の認証情報流出

- **VPN機器の脆弱性**が相次いで報告され、そうした脆弱性を**悪用するコードが公開**されるなど深刻な状況が発生。**攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入**し、攻撃を展開。
- 2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、**国内外900以上の事業者からVPNの認証情報が流出**。2020年11月、Fortinet製品の**VPN機能の脆弱性の影響を受ける約5万台の機器に関する情報が公開**。**認証情報等が悪用されることで容易に侵入されるおそれ**。
- **どちらのケースも既に悪用されている可能性**があるため、**機器のアップデートや多要素認証の導入といった事前対策**に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

VPN機器に対する不正アクセス



Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	国内外900社（国内は38社）の認証情報が公開

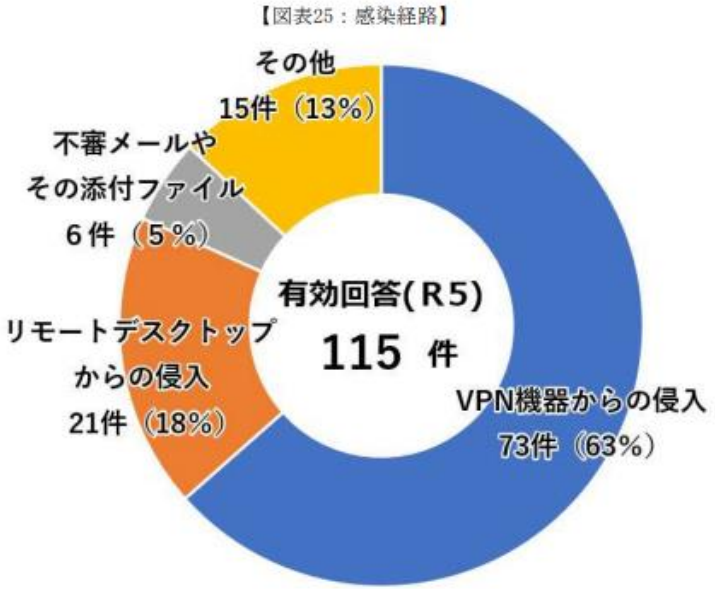
Fortinet製FortiOSの脆弱性

2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

12

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」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf



VPN機器の脆弱性対策をIPAからアナウンス

Fortinet 製 FortiOS SSL VPN の脆弱性対策について

https://www.ipa.go.jp/security/security-alert/2023/alert20240209.html

Ivanti Connect Secure（旧Pulse Connect Secure）および
Ivanti Policy Secure Gateways の脆弱性対策について

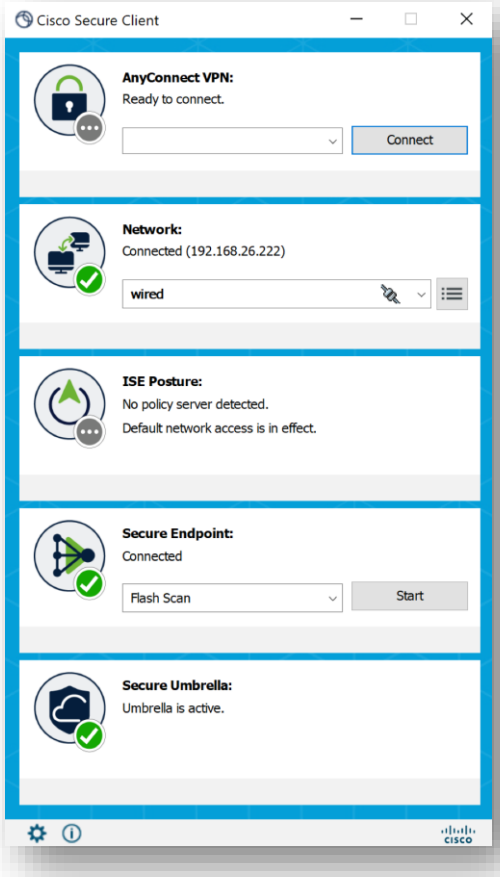
https://www.ipa.go.jp/security/security-alert/2023/20240111.html

VPN機器の脆弱性対策をしなければ
いけないけれど、機器のメンテナンスを
続けるのは負担・・・
オンプレのVPNから
クラウド型のVPNに変えたい！

クラウド型VPNを実績のある 旧AnyConnect(Cisco Secure Client)で利用

- VPN機器管理不要
- クラウド型VPN Head-endが処理を行うため、サイジング不要
- デバイスポスチャ機能でアクセス時のセキュリティ強化
- Ciscoセキュリティの統合エージェントで他商品の機能追加にも対応し、管理者とユーザーの運用負担を低減

AnyConnect VPN やその他の統合機能の導入例では、個別のライセンスが必要です。



課題③ 保守業者の接続に対する管理の必要性

大阪急性期・総合医療センター
情報セキュリティインシデント調査報告書 概要
https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf

「情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入」

大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要 2023.3.28 調査委員会

本書は、2022年10月31日(月)に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害が発生した情報セキュリティインシデントについて、調査委員会として調査した結果をまとめた報告書の概要である。電子カルテシステムが暗号化された影響で長期間、診療制限をせざるを得なかったが、同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧した。

◆調査結果から推定される攻撃者の手順 (調査報告書11～12頁)

No	項目	攻撃者の手順
1	給食事業者に侵入	給食事業者が設置・運営する給食システムに、情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入(漏洩され公開されていたID・パスワード情報を用いて侵入された可能性もある)。
2	給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報(IPアドレスやパスワード情報など)を窃取されたため給食事業者内での攻撃拡大。
3	病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入。ウイルス対策ソフトのアンインストールも実施。
4	病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。
5	他サーバー侵入	病院給食サーバーで窃取した他サーバー認証情報により、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入。
6	クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性。
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート(身代金要求文書)を表示

◆被害状況 (調査報告書11)

No	項目	
1	電子カルテを含む総合情報システム	基幹 ⇒
2	診療制限	202 新 初
3	被害額	現

技術的発生要因と再発防止策 (調査報告書18～19頁)

①外部接続(リモートメンテナンス)の管理不備

VPN機器の管理やRDP接続の運用などが適切になされていれば被害を免れた可能性がある。

No	発生原因	発生要因	再発防止策
1	サプライチェーンのVPN機器の脆弱性が放置されていた。	VPN機器やファイアウォールなど外部通信機器の保守や脆弱性管理など役割分担が曖昧だった。	機器毎に管理者と設置者が互いに保守の範囲や脆弱性管理の役割分担等について文書により確認を行う。
2	リモートデスクトップ通信(RDP)接続が常時接続となっていた。	リモート保守を許可するための基準が曖昧で、またリモート保守を行う側のセキュリティ環境の確認が不十分だった。	外部接続やリモート保守を許可する場合の基準を定めるとともに、許可申請を受ける場合には、通信元のセキュリティ環境を確認する運用を構築する。
		外部接続(リモート保守)を許可した後に、その利用状況を確認していなかった。	外部接続やリモート保守を行う場合は、相手よりその目的や時間を確認し、通信ログの確認を行い、他の不正なアクセスなどの記録が残されていないかを確認する運用を構築する。

②内部のセキュリティが脆弱

侵入を許した場合でも初期設定が適切であれば、大規模に横展開されることはなかった可能性がある。

No	横展開を許した初期設定	再発防止策
1	ユーザーすべてに管理者権限を与えていたため、攻撃者に管理者権限を利用され、ウイルス対策ソフトをアンインストールされた。	ユーザーは管理者権限のない標準ユーザーアカウントに設定。ユーザーアクセス制御を適用させ、管理者権限を要する重要な操作が意図せずに自動実行されることを防ぐ。
2	Windowsのパスワードが、サーバー、端末毎にすべて共通であり、一つのパスワードが窃取されると、他のすべてのサーバー(端末)が乗っ取り可能な状態。	Windows のパスワードを、サーバー、端末毎にすべて個別化(ユニーク化)。
3	アカウントロックアウトの設定が無く、パスワード総当たり攻撃や辞書攻撃によりパスワードを数多く試行されログオンが成功した。	アカウントロックアウトの設定を有効化。
4	電子カルテシステムサーバーにウイルス対策ソフト未設定のため、容易に侵入され、ランサムウェアを実行された(他のサーバーや端末にはウイルス対策インストール済み)。	電子カルテシステムサーバーにもウイルス対策ソフトをインストールする。

Copyright (C) 2023 Osaka General Medical Center. All rights reserved.

厚労省
「医療機関等におけるサイバーセキュリティ対策の強化について(注意喚起)」
https://www.mhlw.go.jp/content/10808000/001024395.pdf

「関係事業者とのネットワーク接続点(特にインターネットとの接続点)をすべて管理下におき、脆弱性対策を実施する」

1　サプライチェーンリスク全体の確認

上記の通り、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点(特にインターネットとの接続点)をすべて管理下におき、脆弱性対策を実施する。

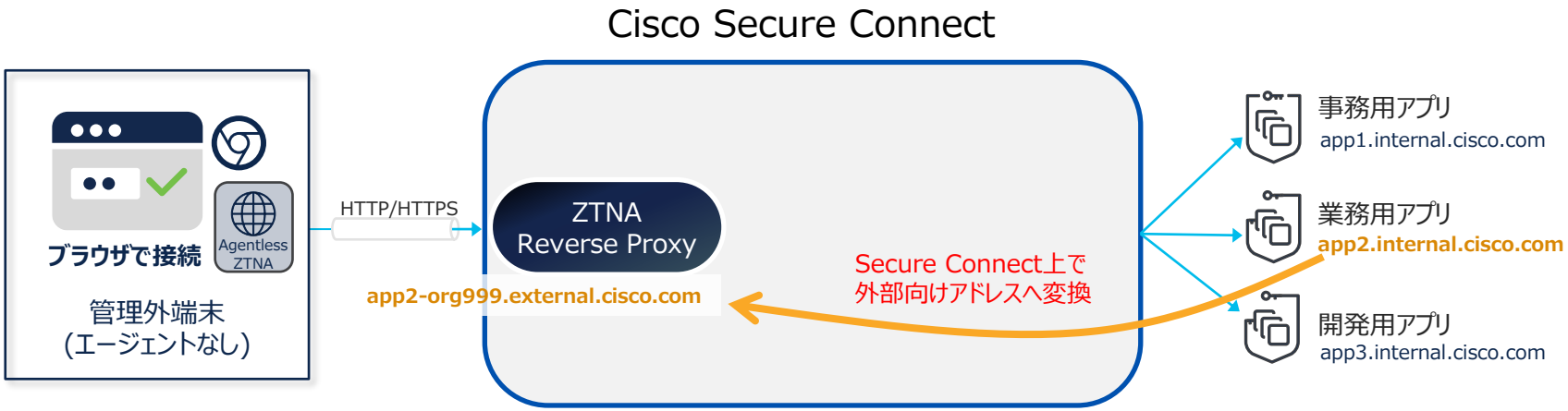
2　リスク低減のための措置

○パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。
○IoT 機器を含む情報資産の保有状況を把握する。
○VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるので、セキュリティパッチ(最新のファームウェアや更新プログラム等)を迅速に適用する。
○悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。
○VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。
○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

保守業者にVPN接続させたくない...
最小アクセス権限で
必要なアプリにだけ接続させたい！
あまりコストはかけたくない！

対象アプリのみ最小アクセス権限で公開可能　ZTNA

エージェント配布ができない利用者にも、ブラウザベースの内部アプリへのリモートアクセスをセキュアに提供可能に



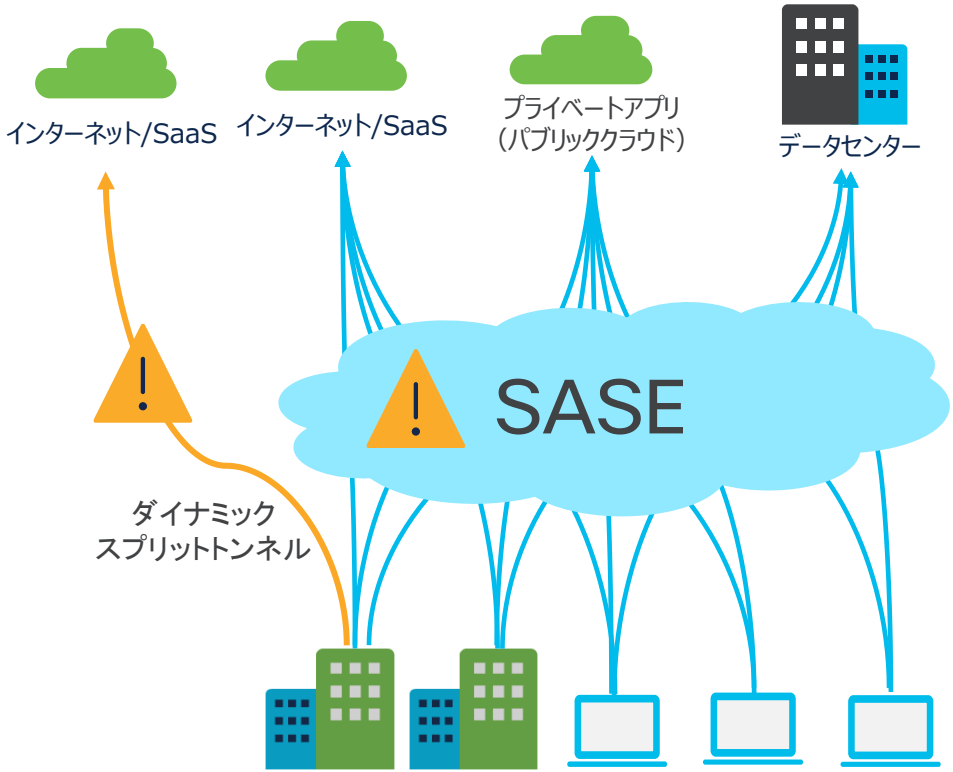
非正規社員・BYOD

- セキュアにBYODを実現
- 管理外端末でも内部システム利用可
- 内部システム利用までの期間を縮小

保守業者

- 保守端末へエージェント導入不要
  (終了後のアンインストールも不要)
- ポータルなどでURLを公開するだけ

課題④ 障害時の対応

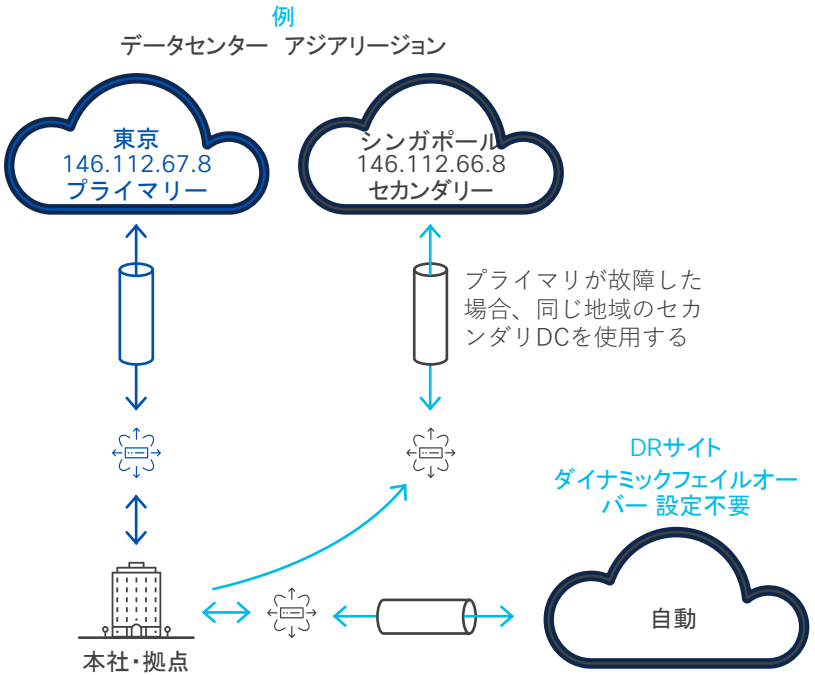


全ての通信を集約すると
障害時は業務停止の
リスクが・・・

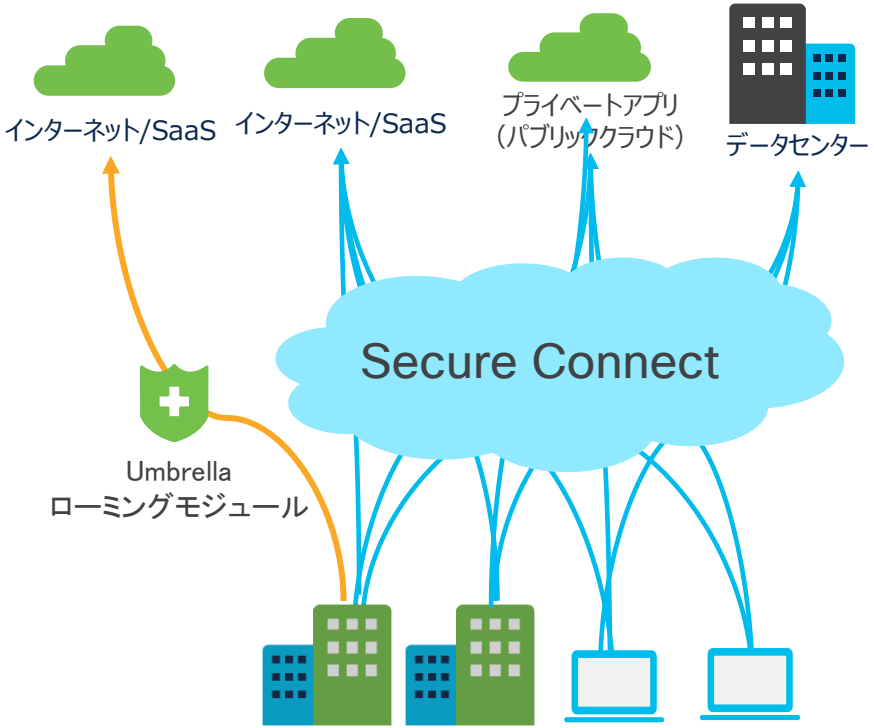
障害時用のトンネルにも
コストがかかる・・・

スプリットするとセキュ
リティがかからない

除外通信も障害時も安心



障害時は自動フェールオーバーで接続するため、障害時用に別途IPSECトンネルを用意する必要がない



SASEを経由しない通信も、Umbrellaローミングモジュールが保護

ライセンス

統合型SASEを実現するには？

Meraki MX

UTM/SD-WAN ルータおよびその使用ライセンス

Secure Connect

ライセンス

シンプルでスモールスタートしやすいライセンス形態

社内のみで利用

Foundation

- Essentials
- Advantage
  - アドバンスドセキュリティ
    L7 CDFW、IPS、DLP

インターネットアクセス　基本セキュリティ
DNS、SWG、CASB、マルウェア検知、サンドボックスなど
＊サンドボックスとクラウドマルウェア検知はEssentialsでは数に制限あり

リモートワークもあり

Complete

- Essentials
- Advantage
  - アドバンスドセキュリティ
    L7 CDFW、IPS、DLP

インターネットアクセス　基本セキュリティ
DNS、SWG、CASB、マルウェア検知、サンドボックスなど
＊サンドボックスとクラウドマルウェア検知はEssentialsでは数に制限あり

リモートアクセス(プライベートアクセス)
クラウド型VPN、ZTNA
＊ZTNAはEssentialsでは数に制限あり

- ✓ ユーザライセンスで1ユーザから契約可能（デバイス数や拠点数に制限なし）
- ✓ リモートワークの有無とセキュリティ機能でエディションを選択。混在も可能

参考）パッケージ詳細比較：Foundation vs Complete

	Foundation		Complete	
	Essentials	Advantage	Essentials	Advantage
Security				
セキュア Web ゲートウェイ （SWG）	✔	✔	✔	✔
URL フィルタリング	✔	✔	✔	✔
セキュア マルウェア アナリティクス	✔	✔	✔	✔
サンドボックス	500サンプル／1日	無制限	500サンプル／1日	無制限
CASB	✔	✔	✔	✔
クラウドマルウェア検知	2 アプリ	無制限	2 アプリ	無制限
DNSセキュリティ	✔	✔	✔	✔
L3/L4 クラウドファイアウォール	✔	✔	✔	✔
L7 クラウドファイアウォール		✔		✔
侵入検知システム (IPS)		✔		✔
データ ロス プリベンション (DLP)		✔		✔
Remote Access				
クライアントベースのアクセス（リモートアクセスVPN）			✔	✔
クライアントレスのアクセス（ブラウザベース）			10 アプリ	300 アプリ
ユーザーおよびアプリベースのきめ細かいアクセスポリシー			✔	✔
SAML 認証			✔	✔
組み込み IdP			✔	✔
ポスチャおよびコンテキストに応じたアクセス制御			✔	✔
リモートアクセスのレポート			✔	✔
Add Ons				
RBI	roadmap	roadmap	roadmap	roadmap
Reserve IP	✔	✔	✔	✔
Multi-org	✔	✔	✔	✔
24時間x7日サポート（平日日本語対応）	✔	✔	✔	✔
ファブリックインターコネクト	✔	✔	✔	✔

Cisco Secure Connectまとめ

① クラウドネイティブ アーキテクチャ

② SASEを通さない ネットワーク設計可能

③ VPNaaS(VPN as a Service) を提供

④ 1ユーザから利用可能

国内で導入実績豊富なMerakiとUmbrellaが基盤

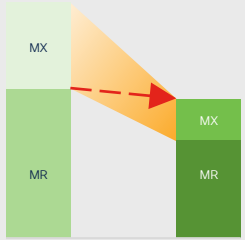
セキュアネットワークを実現する
今だけのキャンペーン

第1弾

Meraki MR & MX バンドル を特価でご提供

対象製品: MR36/44, MX67/MX75 および3年/5年のライセンス (適用台数の条件有り)

主な対象: Cisco Meraki でネットワーク環境を構築されるお客様　※2024年7月26日まで



第2弾

Meraki MX とそのライセンスを特価でご提供

対象製品: MX 67/68/75/85 ハードウェア + ライセンス (Advanced Security 3年~, SD-WAN 3年~)

主な対象: Meraki MX を中心に SD-WANやセキュリティ環境を整えたいお客様　※2024年7月26日まで

第3弾

Cisco Secure Connect を特価でご提供

詳細はお問い合わせください。

詳細はウェブサイトをご覧ください： https://www.cisco.com/jp/go/secure-smb

統合型SASEを体感！

まずは

30日間無料トライアル

Meraki MXの検証機器も貸与可能

お問い合わせ先

アンケート または

www.cisco.com/jp/go/secure-smbまで

Cisco セキュリティウェビナー
次回予告

- 4月 Cisco Duo
- 5月 Network Security
- 6月 Cisco Secure Access
- 7月 Cisco Multicloud Defense

※予定は予告なく変更されることがあります。

The bridge to possible