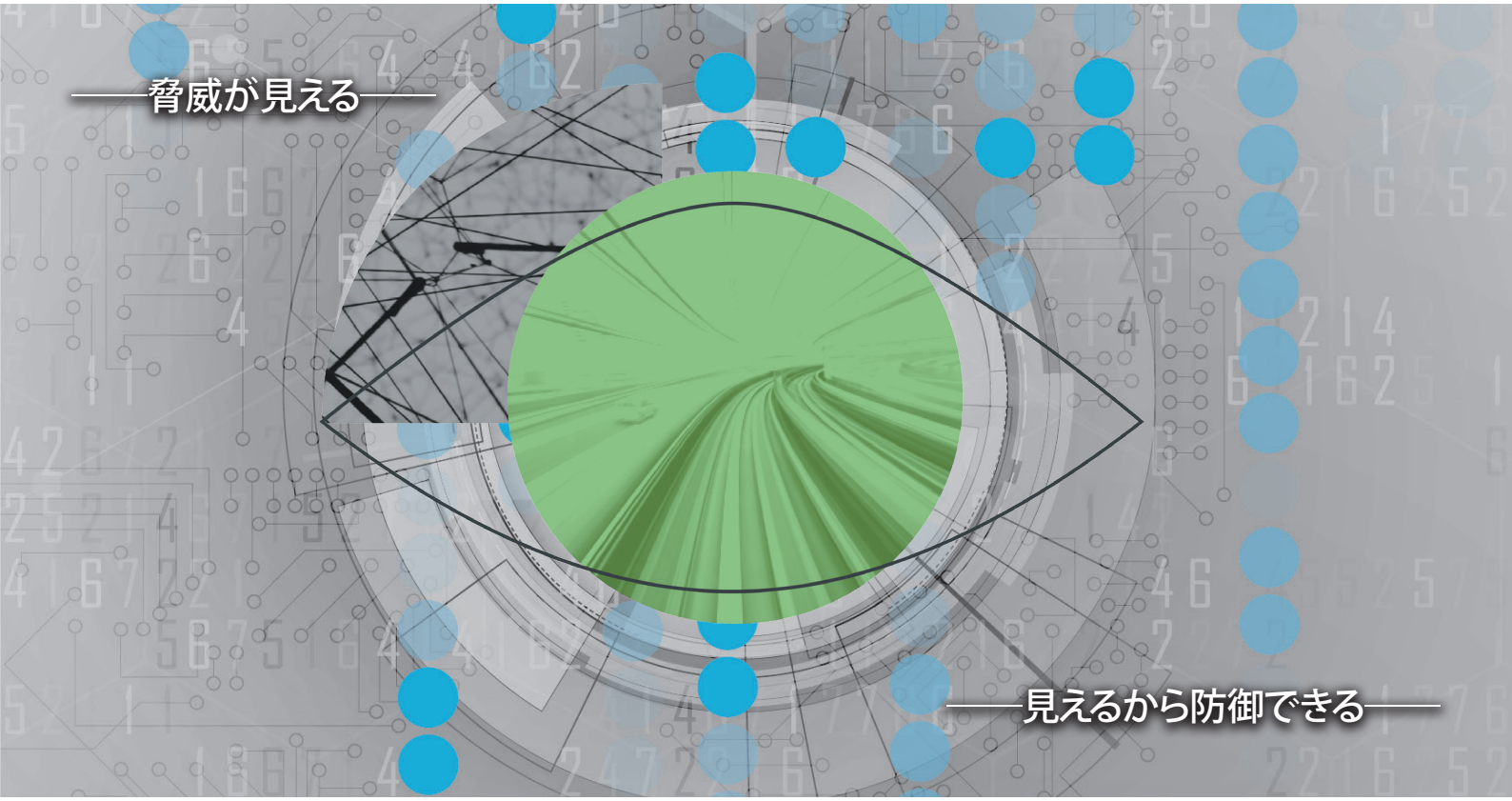
シスコの**ネットワーク可視化**および**セキュリティ分析**ソリューション

Cisco Secure Network Analytics

旧 Cisco Stealthwatch



Cisco Secure Network Analytics は、包括的なネットワーク可視化およびセキュリティ分析ソリューションです。
既存のネットワークインフラからテレメトリデータを収集、可視化して、
業界をリードする機械学習およびビヘイビアモデルで分析、脅威を検出します。
このソリューションによって、次のような課題を解決できます。

追いつかない解析

207 日 *1

感染から検出 / 修復までの平均日数
（一般的な企業）

莫大な経済的損失

4.4 億円 *1

インシデント修復にかかる
平均総費用

暗号化トラフィックに潜む脅威

76% *2

暗号化を利用するハイリスクな脅威
（ESG 社の例）

*1　出典：Ponemon Institute, 2020. Cost of a Data Breach Report 2020.　*2　出典：Enterprise Strategy Group, 2020. Network Traffic Analysis (NTA): A Cybersecurity 'Quick Win.'

ネットワークの可視化とセキュリティ分析で克服すべき、今日の課題

巧妙化を続けるサイバー攻撃

マルウェアの高度化、攻撃者が検出を回避する技術の向上、Internet of Things（IoT）やクラウドサービスの拡大に伴って発生する脆弱性の悪用など、サイバー攻撃が巧妙化を続けています。たとえば、IPA が『**情報セキュリティ 10 大脅威 2021［組織編］**』で選出したランキングでは、「ランサムウェアによる被害」とともに「サプライチェーンの弱点を悪用した攻撃」や「脆弱性対策情報の公開に伴う悪用増加」がランクインしていますが、これらがまさに、巧妙化を続ける攻撃の典型例です。

厄介なことに、これらの攻撃は、従来のファイアウォールや侵入防御システムなど「**境界セキュリティ**」で防御しきれるものではありません。従来のセキュリティを巧みにすり抜けて、内部に侵入し、感染活動を広げてゆくのです。

そのため、従来のように境界セキュリティで侵入を防止する対策はもちろんのこと、PC などエンドポイントで感染を防止する対策も求められますが、いち早く侵入や感染を察知して対応することで侵入後および感染後の被害の拡大を抑止するための対策が、ますます重要になっています。

情報セキュリティ 10 大脅威 2021 脅威ランキング（「組織」向け脅威）ライセンス *1

順位	「組織」向け脅威	昨年順位
1 位	ランサムウェアによる被害	5 位
2 位	標的型攻撃による機密情報の窃取	1 位
3 位	テレワークなどのニューノーマルな働き方を狙った攻撃	
4 位	サプライチェーンの弱点を悪用した攻撃	4 位
5 位	ビジネスメール詐欺による金銭被害	3 位
6 位	内部不正による情報漏洩	2 位
7 位	予期せぬ IT 基盤の障害に伴う業務停止	6 位
8 位	インターネット上のサービスへの不正ログイン	16 位
9 位	不注意による情報漏洩などの被害	7 位
10 位	脆弱性対策情報の公開に伴う悪用増加	14 位

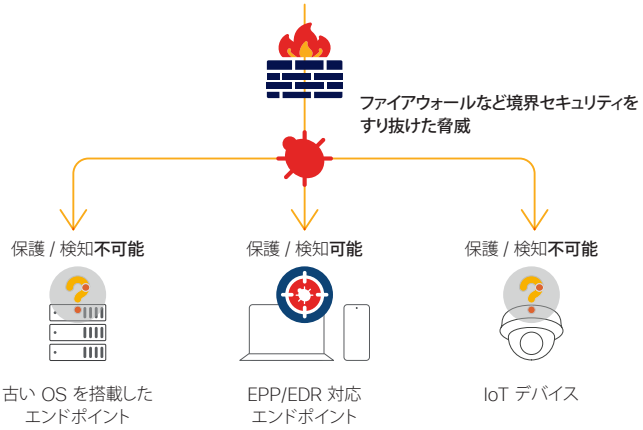
*1　出典：IPA『**情報セキュリティ 10 大脅威 2021［組織編］**』。

EPP や EDR では保護できない古い OS や IoT デバイス

境界セキュリティをすり抜ける攻撃への対策として、すでに多くの企業が導入しているソリューションが、いわゆるウイルス対策ソフトのように脅威をブロックして保護する「**EPP（Endpoint Protection Platform）**」です。さらに近年は EPP に加えて、脅威を可視化して検知および対応を支援する「**EDR（Endpoint Detection and Response）**」を導入する企業も増えてきました。

EPP や EDR は、PC やスマートフォンなどエンドポイントを個別に保護する観点では有効ですが、各エンドポイントに「エージェント」と呼ばれるプログラムを実装することが不可欠であるため、エージェントをインストールすることができないエンドポイントは保護できません。たとえば、Windows XP や Windows 7 のようにサポートが終了した古い OS や、セキュリティカメラやセンサーのような IoT デバイスには、ほとんどの EPP や EDR ではエージェントをインストールできません。

一方で、古い OS や IoT デバイスを標的とした攻撃はリスクが高く、たとえばアメリカでは FBI が Windows 7 のサポート終了を受けて民間企業に注意を喚起したほか、日本でも総務省が IoT デバイスの脆弱性を悪用した攻撃が増加していると注意を喚起しています。したがって、EPP や EDR に加えて、これらのソリューションのセキュリティ上の盲点を補完するソリューションが必要です。



さまざまな業界で根強く残る古い OS ベースのシステムや増加する一方の IoT デバイスが境界セキュリティや EPP/EDR に頼る企業ネットワークのセキュリティ上の盲点となっている

暗号化されたトラフィックに潜む脅威

近年、情報保護の主要な手段として、多くのサービスやアプリケーションで暗号化が使用されています。たとえば『**Google 透明性レポート**』では Google Chrome を使用して HTTPS 経由で読み込んだ Web ページの割合を確認できますが、ほとんどのプラットフォームで 90% 以上の Web ページが HTTPS 経由で読み込まれていることがわかります。

一方で、攻撃者もまた、悪意のあるアクティビティを検出されないようにするための手段として暗号化を活用しています。たとえばシスコの顧客である ESG 社の例では、ハイリスクな脅威の 76% が暗号化されたトラフィックから検出されました。*1

したがって、暗号化されたトラフィックを解析して、そこに潜む脅威を検出できる対策が必要ですが、一般的な対策では主として 3 つの問題があります。

1 つ目は、暗号化されたトラフィックを解析する前段階として、復号するための専用ハードウェアが必要になること、2 つ目は、解析そのものに非常に高度な技術が必要になること、最後に 3 つ目は、暗号化されたトラフィックを復号、解析、および再暗号化することで不可避的に発生するネットワークパフォーマンスの低下です。セキュリティとユーザエクスペリエンスを両立させるためには、これらの問題を回避できるソリューションが必要になります。

HTTPS で読み込まれた Web ページの割合（Google Chrome プラットフォーム別） *2

プラットフォーム	2015 年 3 月 14 日	2021 年 12 月 4 日
Windows	39%	91%
Mac	43%	96%
Android	29%	95%
Chrome	44%	98%
Linux	44%	80%

*1　出典：Enterprise Strategy Group, 2020. Network Traffic Analysis (NTA): A Cybersecurity 'Quick Win'.
*2　出典：「**ウェブ上での HTTPS 暗号化**」（transparencyreport.google.com/https/overview）『**Google 透明性レポート**』。

Cisco Secure Network Analytics がもたらすメリット

ネットワークを包括的に可視化、業界最先端の機械学習とビヘイビアモデルで脅威を分析

Cisco Secure Network Analytics は、包括的なネットワーク可視化およびセキュリティ分析ソリューションです。既存のネットワークインフラからテレメトリデータを収集、可視化して、業界最先端の機械学習、ビヘイビアモデル、およびグローバルな脅威インテリジェンスで分析、脅威を検出します。

ネットワークインフラが Cisco Catalyst 9000 シリーズ スイッチなど最新のシスコ デバイスで構成される場合は、**暗号化トラフィック分析**（Encrypted Traffic Analytics；ETA）によって暗号化されたトラフィックも可視化および分析できます。

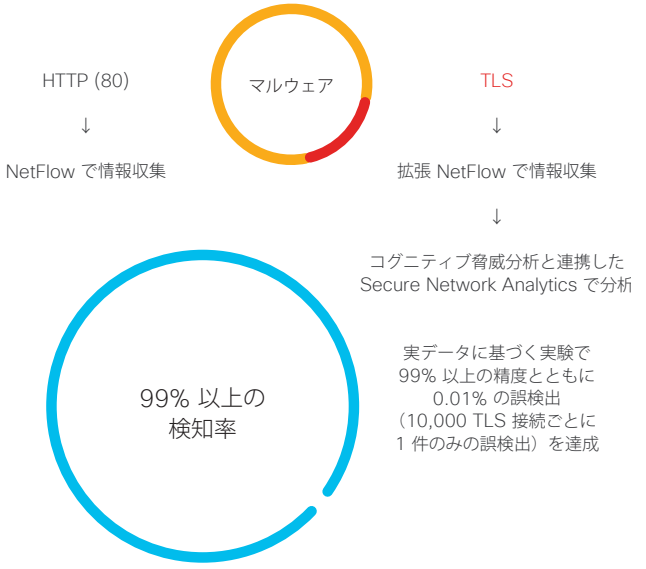
Cisco Secure Network Analytics は、セキュリティポリシーを集中管理する **Cisco Identity Services Engine**（ISE）と連携することで、ユーザ情報など、より豊富なテレメトリ情報を活用できるだけでなく、検出した脅威を迅速に封じ込めることができるようになります。これらは、Cisco ISE の管理画面を操作することなく可能です。

Cisco Secure Network Analytics
www.cisco.com/jp/go/stealthwatch

暗号化トラフィック分析（ETA）

暗号化トラフィック分析（Encrypted Traffic Analytics；ETA）は、Transport Layer Security（TLS）で暗号化されたトラフィックからマルウェアを特定できる、シスコの独自機能です。

ETA では、復号専用のハードウェアを必要としないだけでなく、TLS 通信を復号せずに解析できるため、復号および再暗号化に伴うネットワークパフォーマンスの低下がありません。さらに、クラウドサービスの **Cisco コグニティブ脅威分析**と連携した Cisco Secure Network Analytics では、実データに基づく実験で 99% 以上の検知率を達成しました。



暗号化トラフィック分析（ETA）
www.cisco.com/jp/go/eta

Cisco Secure Network Analytics 製品コンポーネント

Cisco Secure Network Analytics セキュリティバンドル

製品型番	製品説明
ST-SEC-BUN	セキュリティバンドル（ダイレクトセールス用）
ST-SEC-BUN-DIST	セキュリティバンドル（ディストリビュータまたは T2 パートナー用）

TIP バンドルについて

Secure Network Analytics 製品は、フローレート ライセンスの数量に応じてディスカウント価格が適用される、セキュリティバンドル（ST-SEC-BUN または ST-SEC-BUN-DIST）による購入を推奨します。

Cisco Secure Network Analytics フローレート ライセンス

製品型番	製品説明
ST-FR-100-LIC	フローレート ライセンス 100 fps パック *1

*1　1 ～ 5 年間のサブスクリプション。

Cisco Secure Network Analytics マネージャ

製品型番		フローコレクタ管理数	データストレージ		メモリ	CPU		イーサネットポート		仮想マシン構成	
			容量	RAID		コア	クロック	10GE RJ45	10GE SFP+	仮想 CPU	仮想メモリ
物理 *1	ST-SMC2210-K9	25	4 TB	6	512 GB	2 × 20	2.1 GHz	2	2		
仮想 *2	L-ST-SMC-VE-K9	5								4	32 GB
		25								8	64 GB

*1　ハードウェア構成の詳細はスペックシートを参照。　*2　システム要件の詳細はインストールガイド（データストアなし / データストアあり）を参照。

Cisco Secure Network Analytics フローコレクタ

製品型番		ノード	フロー数 / 秒（fps）	インターフェイス	エクスポータ	フローストレージ		メモリ	CPU		イーサネットポート		仮想マシン構成	
						容量	RAID		コア	クロック	10GE RJ45	10GE SFP+	仮想 CPU	仮想メモリ
物理 *1	ST-FC4210-K9		200,000 *3	65,535	4,096	4 TB	6	512 GB	2 × 20	2.1 GHz	2	2		
	ST-FC5210-K9	エンジン	300,000	65,535	4,096			256 GB	2 × 20	2.1 GHz	2	2		
		データベース				6 TB	10	512 GB	2 × 20	2.1 GHz	2	2		
仮想 *2	L-ST-FC-VE-K9		10,000	65,535	1,024								2	24 GB
			30,000	65,535	1,024								6	32 GB
			60,000	65,535	2,048								8	64 GB
			120,000	65,535	4,096								12	128 GB

*1　ハードウェア構成の詳細はスペックシート（ST-FC4210-K9/ST-FC5210-K9）を参照。　*2　数値はデータストアなしの場合。システム要件の詳細はインストールガイド（データストアなし / データストアあり）を参照。
*3　データストアなしの場合。データストアありの場合は 250,000 ～ 500,000。

Cisco Secure Network Analytics データストア

製品型番		データノード数	フロー数 / 秒（fps）	データ保持期間	データストレージ *1		メモリ *1	CPU *1		コミュニケーションポート *1	仮想マシン構成	
					容量	RAID		コア	クロック	10GE SFP+	仮想 CPU	仮想メモリ
物理 *2	ST-DS6200-K9	3	500,000	90 日 *4	15.8 TB	6	384 GB	2 × 12	3.3 GHz	4		
仮想 *3	L-ST-DS-VE-K9	3	50,000	30 日 *5							6	32 GB
		3	120,000	30 日 *6							12	32 GB
		3	220,000	30 日 *7							16	64 GB

*1　ノードあたりの仕様。　*2　ハードウェア構成の詳細はスペックシートを参照。　*3　システム要件の詳細はインストールガイドを参照。　*4　ノードあたり 500,000 FPS の場合。
*4　1 日あたり平均 50,000 FPS、ノードあたり 800 GB データストレージの場合。　*5　1 日あたり平均 120,000 FPS、ノードあたり 1.92 TB データストレージの場合。
*6　1 日あたり平均 220,000 FPS、ノードあたり 3.52 TB データストレージの場合。

Cisco Secure Network Analytics フローセンサー

製品型番		モニタリングパフォーマンス	メモリ	CPU		モニタリングポート				仮想マシン構成	
				コア	クロック	1GE RJ45	10GE RJ45	10GE SFP+	40GE QSFP+	仮想 CPU	仮想メモリ
物理 *1	ST-FS1210-K9	3 Gbps	16 GB	1 × 8	2.1 GHz	4	1				
	ST-FS3210-K9	4.5 Gbps	256 GB	2 × 16	2.3 GHz	4	1				
		6 Gbps						2			
	ST-FS4240-K9	40 Gbps	384 GB	2 × 18	3.1 GHz			4			
		80 Gbps							2		
仮想 *2	L-ST-FS-VE-K9	850 Mbps								2	4 GB
		1,850 Mbps								4	8 GB
		3,700 Mbps								8	16 GB
		8 Gbps								12	24 GB
		16 Gbps								22	40 GB

*1　ハードウェア構成の詳細はスペックシート（ST-FS1210-K9/ST-FS3210-K9/ST-FS4240-K9）を参照。　*2　システム要件の詳細はインストールガイド（データストアなし / データストアあり）を参照。

Cisco Secure Network Analytics オプション ライセンス *1

製品型番	製品説明
ST-EP-LIC	エンドポイント ライセンス（1 エンドポイント～） *2
TB-ESS-100GB	Telemetry Broker Essential ライセンス 100 GB/ 日パック

*1　1 ～ 5 年間のサブスクリプション。　*2　Cisco AnyConnect Secure Mobility Client が必要。

製品型番	製品説明
L-LC-TI-FC1K=	フローコレクタ 1000 用 Threat Feed ライセンス
L-LC-TI-FC2K=	フローコレクタ 2000 用 Threat Feed ライセンス
L-LC-TI-FC4K=	フローコレクタ 4000 用 Threat Feed ライセンス
L-LC-TI-FC5K=	フローコレクタ 5000 用 Threat Feed ライセンス

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日10:00-12:00, 13:00-17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

2291-2112-000-TO