Cisco Firepower Management Center バージョン 6.6 から収集される Cisco Success Network テレメトリデータ

初版：2022 年 5 月 31 日

最終更新：2023 年 8 月 16 日

Cisco Secure Firewall Management Center から収集される Cisco Success Network テレメトリデータ

Cisco Success Network では、登録済み FMC はリアルタイムの設定と動作の状態に関する情報を Cisco Success Network Cloud に継続的にストリーミングすることができます。このドキュメントでは、収集およびモニターされるデータのリストを示します。

登録済みデバイス データ

Cisco Success Network に FMC を登録したら、登録済みの FMC デバイスに関する選択したテレメトリデータが Cisco Cloud へストリーミングされます。次の表に、登録済みのデバイスに関して収集し、監視しているデータを示します。このデータには、侵入ポリシー（システムが提供するポリシーとカスタムポリシーの両方）および登録済みの FMC のマルウェア検出に関する機能に固有の情報が含まれます。

表 *1*：登録済みデバイスのテレメトリ データ

データ ポイント	値の例
デバイス名（Device Name）	Management Center East
デバイス UUID	24fd0ccf-1464- 491f-a503- d241317bb327
デバイス モデル	Cisco Firepower Management Center 4000 Cisco Firepower Management Center for VMWare
シリアル番号（Serial Number）	9AMDESQP6UN
システム稼動時間（System Uptime）	99700000
製品 ID（Product Identifier）	FS-VMW-SW-K9
スマート ライセンス PIID	24fd0ccf-1464- 491f-a503- d241317bb327

データ ポイント	値の例
仮想アカウント識別子	CiscoSVStemp
スマートライセンスバーチャルアカウント名	FTD-ENG-SJC

ソフトウェア バージョン データ

Cisco Success Network は、ソフトウェアのバージョン、ルールの更新バージョン、地理位置情報データベースのバージョン、脆弱性データベースのバージョン情報など、登録済みの FMC デバイスに関連するソフトウェア情報を収集します。次の表に、登録済みのデバイスに関して収集し、監視しているソフトウェア情報を示します。

表 *2:* ソフトウェア バージョンのテレメトリ データ

データ ポイント	値の例
FMC ソフトウェアバージョン	{ type: "SOFTWARE", version: "x.x.x.x" }
ルールの更新バージョン	{version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }
脆弱性データベース（VDB）のバージョン	{version: "271", lastUpdated: 1468606837000 }
地理的位置情報データベースのバージョン	{version: "850" }

管理対象デバイス データ

Cisco Success Network は、登録済み FMC に関連付けられているすべての管理対象デバイスに関する情報を収集します。次の表に、管理対象デバイスに関して収集し、監視している情報を示します。これには、管理対象デバイスの URL フィルタリング、侵略防御、およびマルウェア 検出など、機能に固有のポリシーおよびライセンス情報が含まれます。

表 *3:* 管理対象デバイスのテレメトリ データ

データ ポイント	値の例
管理対象デバイス名。	firepower
管理対象デバイスバージョン。	6.2.3-10616
管理対象デバイスマネージャ。	FMC
管理対象デバイスモデル。	Cisco Firepower 2130 NGFW アプライアンス Cisco FTD VMware
管理対象デバイスのシリアル番号。	9AMDESQP6UN

データ ポイント	値の例
管理対象デバイスの PID。	FPR2130-NGFW-K9 NGFWv
デバイスにURLフィルタリング ライセンスを使用しているか	True
デバイスごとにURLフィルタリングを使用する AC ルール。	10
URL フィルタリングライセンスを使用する URL フィルタリングでの AC ルールの数。	3
脅威ライセンスを使用するURLフィルタリングでの AC ルールの数。	3
デバイスに脅威ライセンスを使用しているか	True
AC ポリシーに侵略ルールを追加しているか	True
侵入ポリシーを使用する AC ルールの数。	10
デバイスにマルウェア ライセンスを使用しているか	True
マルウェアポリシーを使用する AC ルールの数。	10
マルウェアライセンスを使用するマルウェアポリシーでの AC ルールの数。	5
デバイスに Threat Intelligence Director (TID) を使用しているか	True
静的ルートの数。	4
VRF 数。	0
ローカル URL 項目の数。	{"url": "/api/local/fmc_config/v1/domain/{domainUUID}/object/networks", "count": 10}, {"url": "/api/local/fmc_platform/v1/info/serverversion", "count": 2}

導入情報

展開を設定した後、影響を受けるデバイスにその変更を展開する必要があります。次の表に、影響を受けるデバイスの数と成功か失敗かの情報を含む展開のステータスなど、設定の展開に関して収集し、モニターするデータを示します。

表 *4:* 導入情報

データ ポイント	値の例
ジョブ ID（Job ID）	8589936079
展開用に選択したデバイスの数	3
展開に失敗したデバイスの数	1
展開に成功したデバイスの数	2
終了時間（End Time）	1523993913001
開始時間(Start Time)	1523993840445
ステータス	SUCCEEDED
ターゲット デバイスの UUID	4f14f644-41e0 -11e8-9354- cf32315d7095
展開したポリシー タイプ	NetworkDiscovery NGFWPolicy DeviceConfiguration
現在の実行で収集した最後の展開ジョブの ID	8589936079
コンテナ タイプ（スタンドアロンまたは HA ペア）	STANDALONE HAPAIR
コンテナの UUID	5e006633-30fe-11e9-8a70-cd88086eeac0
デバイス モデル	Cisco FTD for VMWare
デバイスバージョン	6.4.0
ポリシー バンドルのサイズ	3588153

TLS/SSL インスペクション イベント データ

Firepower システムは、デフォルトではセキュア ソケット レイヤ（SSL）プロトコルまたはその後継である Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。TLS/SSLインスペクションを使用すると、暗号化トラフィックをインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセス コントロールを使用して検査したりできます。次の各表では、暗号化されたトラフィックについて Cisco Success Network と共有する統計情報について説明します。

ハンドシェイク プロセス

システムで TCP 接続での TLS/SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうかが判定されます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。

表 *5 : TLS/SSL* インスペクション : ハンドシェイクのテレメトリ データ

データ ポイント	値の例
システムは、トラフィックが**復号できず**次の状態となった場合、適用されたアクションを報告します。 • ブロック • TCP リセットによるブロック • 復号されない	0 以上の整数値
システムは、トラフィックが次の方法で**復号できた**場合、適用されたアクションを報告します。 • 既知の秘密キーを使用する。 • 置換キーのみを使用する。 • 自己署名証明書へ再署名する。 • サーバー証明書へ再署名する。	0 以上の整数値

キャッシュ データ

TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッションデータをキャッシュに保存し、それによりフルハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバー証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

表 *6 : TLS/SSL* インスペクション：キャッシュのテレメトリ データ

データ ポイント	値の例
	0 以上の整数値

データ ポイント	値の例
システムは暗号化されたセッションデータおよびサーバ証明書データをキャッシュし、**キャッシュ**について SSL 接続ごとにレポートします。具体的な内容は次のとおりです。 • SSLセッション情報がキャッシュされた回数。 • SSL証明書検証キャッシュがヒットした回数。 • SSL 証明書検証キャッシュのルックアップが失敗した回数。 • SSL 元証明書キャッシュがヒットした回数。 • SSL 元証明書キャッシュのルックアップが失敗した回数。 • SSL 再署名証明書キャッシュがヒットした回数。 • SSL 再署名証明書キャッシュのルックアップが失敗した回数。 • Client Hello ダイジェスト キャッシュ エントリの回数。 • Client Hello ダイジェストキャッシュが削除された回数。 • Client Hello ダイジェストキャッシュがヒットした回数。 • Client Hello ダイジェスト キャッシュ メモリが使用された回数。 • Client Hello ダイジェストキャッシュがヒットしなかった回数。 • エンドポイント証明書キャッシュエントリの回数。 • エンドポイント証明書キャッシュメモリが使用された回数。 • 外部証明書キャッシュエントリの回数。 • 外部証明書キャッシュメモリが使用された回数。 • 内部 CA キャッシュエントリ。 • 内部CAキャッシュメモリが使用された回数。	

データ ポイント	値の例
• オブジェクト リスト キャッシュ エントリの回数。 • オブジェクト リスト キャッシュ メモリが使用された回数。 • 元の証明書キャッシュエントリの回数。 • 元の証明書キャッシュエントリのメモリが使用された回数。 • 元の証明書キャッシュが削除された回数。 • 元の証明書キャッシュがヒットした回数。 • 元の証明書キャッシュメモリが使用された回数。 • 元の証明書キャッシュがヒットしなかった回数。 • 再署名された証明書キャッシュエントリの回数。 • 再署名された証明書キャッシュエントリのメモリが使用された回数。 • 再署名された証明書キャッシュが削除された回数。 • 再署名された証明書キャッシュがヒットした回数。 • 再署名された証明書キャッシュメモリが使用された回数。 • 再署名された証明書キャッシュがヒットしなかった回数。 • サーバー名キャッシュエントリの回数。 • サーバー名キャッシュが削除された回数。 • サーバー名キャッシュがヒットした回数。 • サーバー名キャッシュメモリが使用された回数。 • サーバー名キャッシュがヒットしなかった回数。 • セッション ID キャッシュエントリの回数。	

データ ポイント	値の例
• セッションIDキャッシュが削除された回数。 • セッションIDキャッシュがヒットした回数。 • セッションIDキャッシュメモリが使用された回数。 • セッションIDキャッシュがヒットしなかった回数 • セッション チケット キャッシュ エントリの回数。 • セッションチケットキャッシュが削除された回数。 • セッションチケットキャッシュがヒットした回数。 • セッション チケット キャッシュ メモリが使用された回数。 • セッションチケットキャッシュがヒットしなかった回数。 • SSL キャッシュ合計メモリの回数。 • SSLキャッシュ合計メモリが使用された回数。 • URL 再試行キャッシュエントリの回数。 • URL 再試行キャッシュが削除された回数。 • URL 再試行キャッシュがヒットした回数。 • URL 再試行キャッシュメモリが使用された回数。 • URL 再試行キャッシュがヒットしなかった回数。	
FMCでSSLの使用が有効になっているかどうか。	はい（True）

証明書のステータス

システムは暗号化されたトラフィックを評価し、暗号化サーバーの証明書のステータスを報告します。

表 *7: TLS/SSL* インスペクション：証明書ステータスのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたトラフィックを暗号化サーバーの**証明書ステータス**に基づいて評価し、報告します。 • SSL 証明書が有効な接続の数。 • SSL 証明書の有効期限が切れている接続の数。 • SSL 証明書の発行者が無効な接続の数。 • SSL 証明書に無効な署名が含まれている接続の数。 • SSL証明書がチェックされない接続の数。 • SSL 証明書がまだ有効になっていない接続の数。 • SSL 証明書が取り消された接続の数。 • SSL 証明書が自己署名されている接続の数。 • SSL 証明書が不明な接続の数。	0 以上の整数値

失敗の理由

システムは暗号化されたトラフィックを評価し、システムがトラフィックの復号化に失敗している場合は失敗の理由を報告します。

表 *8 : TLS/SSL* インスペクション：失敗のテレメトリデータ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、システムが次の理由のためにトラフィックの復号化に失敗している場合は**失敗の理由**を報告します。 • 復号エラー。 • ハンドシェイク中のポリシー判定の実行。 • ハンドシェイク前のポリシー判定の実行。 • 圧縮がネゴシエートされている。 • キャッシュされていないセッション。 • インターフェイスがパッシブモード。 • 不明な暗号スイート。 • サポートされていない暗号スイート。	0 以上の整数値

バージョン（Version）

システムは暗号化されたトラフィックを評価し、ネゴシエートされた TLS/SSL バージョンを接続ごとに報告します。

表 *9 : TLS/SSL* インスペクション：バージョンのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、次のようなネゴシエートされた**バージョン**を SSL 接続ごとに報告します。 • SSLv2 のネゴシエート。 • SSLv3 のネゴシエート。 • 不明なバージョンのネゴシエート。 • TLSv1.0 のネゴシエート。 • TLSv1.1 のネゴシエート。 • TLSv1.2 のネゴシエート。 • TLSv1.3 のネゴシエート。	0 以上の整数値

Snort 再起動データ

管理対象デバイス上のSnortプロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。ユーザー定義のアプリケーションの作成/削除を行うか、システムまたはカスタム アプリケーション ディテクタを有効化/無効化すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snort プロセスの再起動が続行されていることが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内の任意の管理対象デバイスで発生します。

表 *10 : Snort* 再起動のテレメトリ データ

データ ポイント	値の例
カスタムアプリケーションディテクタを有効または無効にした場合の Snort 再起動の数。	0 以上の整数値
カスタムアプリケーションディテクタを作成または変更した場合の Snort 再起動の数。	0 以上の整数値

コンテキスト クロス起動データ

コンテキストクロス起動機能を使用すると、FMC の外部の Web ベースのリソースにおける潜在的な脅威に関する詳細情報をすばやく検索できます。FMC のイベントビューアまたはダッシュボードのイベントから、外部リソースの関連情報を直接クリックできます。これにより、その IP アドレス、ポート、プロトコル、ドメイン、または SHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

表 *11 :* コンテキスト クロス起動のテレメトリ データ

データ ポイント	値の例
FMC 上に設定されているコンテキストクロス起動リソースの数。	0 以上の整数値
FMC 上で有効になっているコンテキストクロス起動リソースの数。	0 以上の整数値
ドメイン変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
IP 変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
SHA 256 変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
テーマのレガシーの数。	0 以上の整数値

テレメトリ ファイルの例

次に、FMC とその管理対象デバイスに関してポリシーと展開の情報をストリーミングするための Cisco Success Network テレメトリファイルの例を示します。


```
{
  "version" : "1.0",
  "metadata" : {
    "topic" : "fmc.telemetry",
    "contentType" : "application/json"
  },
  "payload" : {
    "recordType" : "CST_FMC",
    "recordVersion" : "6.6.0",
    "recordedAt" : 1568961395861,
    "fmc" : {
      "deviceInfo" : {
        "deviceModel" : "Cisco Firepower Management Center for VMWare",
        "deviceName" : "liverpool",
        "deviceUuid" : "c9a7877c-da65-11e9-956f-cc1767fe73df",
        "serialNumber" : "None",
       "smartLicenseProductInstanceIdentifier" : "1077ac5d-619f-49eb-a6a9-6ad61c30a481",

        "smartLicenseVirtualAccountName" : "FTD-ENG-SJC",
        "systemUptime" : 114808000,
        "udiProductIdentifier" : "FS-VMW-SW-K9"
      },
      "versions" : {
        "items" : [
          {
            "type" : "SOFTWARE",
            "version" : "6.6.0-1034"
          },
          {
            "lastUpdated" : 0,
            "type" : "SNORT_RULES_DB",
            "version" : "2019-08-12-001-vrt"
          },
          {
            "lastUpdated" : 1568847127000,
            "type" : "VULNERABILITY_DB",
            "version" : "309"
          },
          {
            "type" : "GEOLOCATION_DB",
            "version" : "None"
          }
        ]
      }
    },
    "managedDevices" : {
      "items" : [
        {
          "deviceInfo" : {
            "deviceManager" : "FMC",
            "deviceModel" : "Cisco Firepower 4125 Threat Defense",
            "deviceName" : "192.168.1.165",
            "deviceVersion" : "6.6.0-1034",
            "serialNumber" : "FCH22197RU0"
          },
          "malware" : {
            "malwareLicenseUsed" : true,
            "numberOfACRulesNeedMalwareLicense" : 0,
```

```
    "numberOfACRulesWithMalware" : 0
  },
  "sslCacheStats" : {
    "clientHelloDigestCacheEntries" : 3,
    "clientHelloDigestCacheEvicted" : 0,
    "clientHelloDigestCacheHit" : 7,
    "clientHelloDigestCacheMemoryUsed" : 720460,
    "clientHelloDigestCacheMiss" : 7,
    "endpointCertCacheEntries" : 0,
    "endpointCertCacheMemoryUsed" : 960,
    "externalCertCacheEntries" : 0,
    "externalCertCacheMemoryUsed" : 960,
    "internalCACacheEntries" : 1,
    "internalCACacheMemoryUsed" : 1049,
    "objectListCacheEntries" : 2,
    "objectListCacheMemoryUsed" : 1278,
    "originalCertCacheEntries" : 3,
    "originalCertCacheEntriesMemoryUsed" : 9120,
    "originalCertCacheEvicted" : 0,
    "originalCertCacheHit" : 7,
    "originalCertCacheMemoryUsed" : 80460,
    "originalCertCacheMiss" : 0,
    "resignedCertCacheEntries" : 3,
    "resignedCertCacheEntriesMemoryUsed" : 4270,
    "resignedCertCacheEvicted" : 0,
    "resignedCertCacheHit" : 14,
    "resignedCertCacheMemoryUsed" : 720484,
    "resignedCertCacheMistt" : 2,
    "serverNameCacheEntries" : 6,
    "serverNameCacheEvicted" : 0,
    "serverNameCacheHit" : 14,
    "serverNameCacheMemoryUsed" : 16731,
    "serverNameCacheMiss" : 0,
    "sessionIDCacheEntries" : 1,
    "sessionIDCacheEvicted" : 0,
    "sessionIDCacheHit" : 0,
    "sessionIDCacheMemoryUsed" : 720428,
    "sessionIDCacheMiss" : 14,
    "sessionTicketCacheEntries" : 1,
    "sessionTicketCacheEvicted" : 0,
    "sessionTicketCacheHit" : 0,
    "sessionTicketCacheMemoryUsed" : 720393,
    "sessionTicketCacheMiss" : 0,
    "sslCachesTotalMemory" : 14000000,
    "sslCachesTotalMemoryUsed" : 2999399,
    "urlRetryCacheEntries" : 0,
    "urlRetryCacheEvicted" : 0,
    "urlRetryCacheHit" : 0,
    "urlRetryCacheMemoryUsed" : 16176,
    "urlRetryCacheMiss" : 0
  },
  "sslUsage" : {
    "isSSLEnabled" : true
  },
  "threat" : {
    "acPolicyHasIntrusion" : false,
    "acRulesWithIntrusion" : 0,
    "isTIDEnabled" : true,
    "numberOfACRulesNeedThreatLicense" : 0,
    "threatLicenseUsed" : true
  },
  "urlFiltering" : {
    "acRulesWithURLFiltering" : 0,
    "numberOfACRulesNeedThreatLicense" : 0,
```

```
        "numberOfACRulesNeedURLLicense" : 0,
        "urlFilteringLicenseUsed" : true
      },
      "vrfInfo": {
        "literal": false,
        "numberOfStaticRoutes": 4,
        "vrfCount": 0
      }
    }
  ]
},
"deploymentData" : { },
"analysis" : {
  "crossLaunchInfo" : {
    "count" : 28,
    "enabledCount" : 28,
    "iocInfo" : [
      {
        "domain" : 10,
        "ip" : 9,
        "sha256" : 9
      }
    ]
  }
},
"theme" : {
  "legacy" : 1
},
"SSLStats" : {
  "action" : {
    "block" : 0,
    "block_with_reset" : 0,
    "decrypt_resign_self_signed" : 0,
    "decrypt_resign_self_signed_replace_key_only" : 0,
    "decrypt_resign_signed_cert" : 887,
    "decrypt_with_known_key" : 0,
    "do_not_decrypt" : 0
  },
  "cache_status" : {
    "cached_session" : 60,
    "cert_validation_cache_hit" : 0,
    "cert_validation_cache_miss" : 887,
    "orig_cert_cache_hit" : 771,
    "orig_cert_cache_miss" : 0,
    "resigned_cert_cache_hit" : 887,
    "resigned_cert_cache_miss" : 17,
    "session_cache_hit" : 0,
    "session_cache_miss" : 700
  },
  "cert_status" : {
    "cert_expired" : 0,
    "cert_invalid_issuer" : 1,
    "cert_invalid_signature" : 0,
    "cert_not_checked" : 0,
    "cert_not_yet_valid" : 0,
    "cert_revoked" : 0,
    "cert_self_signed" : 0,
    "cert_unknown" : 0,
    "cert_valid" : 886
  },
  "failure_reason" : {
    "decryption_error" : 0,
    "handshake_error_before_verdict" : 0,
    "handshake_error_during_verdict" : 0,
```

```
          "ssl_compression" : 0,
          "uncached_session" : 0,
          "undecryptable_in_passive_mode" : 0,
          "unknown_cipher_suite" : 0,
          "unsupported_cipher_suite" : 0
        },
        "version" : {
          "ssl_v20" : 0,
          "ssl_v30" : 0,
          "ssl_version_unknown" : 0,
          "tls_v10" : 0,
          "tls_v11" : 0,
          "tls_v12" : 887,
          "tls_v13" : 0
        }
      },
      "snortRestart" : {
        "appDetectorSnortRestartCnt" : 0,
        "appSnortRestartCnt" : 0
      }
    }
  }
```

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。