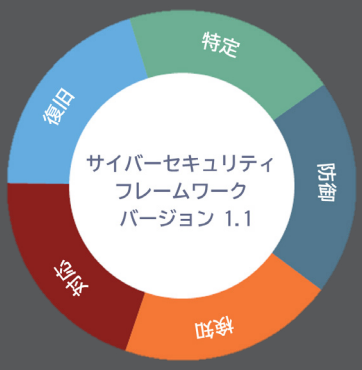
proofpoint.

ホワイトペーパー

NIST サイバーセキュリティ ガイドラインへの準拠

はじめに



セキュリティ脅威に対抗するには強固な防御策が必要であり、それに対応するために米国国立標準研究所（NIST）は、サイバーセキュリティ フレームワーク 1.1 を発行しました。これはセキュリティプログラムを構築する際に不可欠なガイドラインです。これを基にしてサイバーセキュリティ体制を評価したり、または自社特有の要件に合うようにカスタマイズして使うことも可能です。

プルーフポイントのソリューションはこのフレームワークと調和し、以下の主要な NIST 要件に準拠しています。

- リスクアセスメント (ID.RA)
- 意識向上およびトレーニング (PR.AT)
- データセキュリティ (PR.DS)
- 異常とイベント (DE.AE)
- セキュリティの継続的なモニタリング (DE.CM)
- 検知プロセス (DE.DP)
- 分析 (RS.AN)
- 低減 (RS.MI)

本文書は、プルーフポイントのソリューションでどのように NIST ガイドラインに準拠し、セキュリティ目標を達成できるかを説明します。

プルーフポイントが支援できること

Proofpoint Browser Isolationを使えば、悪意のあるコンテンツによる会社支給デバイスの被害を防ぎ、ユーザーが安全にインターネットを使用できる環境を提供できます。

Proofpoint Email Protection はゲートウェイで詐欺メールを特定してユーザーに届かないようブロックします。

Proofpoint Premium Threat Intelligence Service (PTIS) は詳細な脅威レポートやアナリストの見解、そして脅威エキスパートによる Q&A を提供します。

Proofpoint Threat Response Auto-Pull (TRAP) は悪意のあるメールをユーザーの受信箱から自動的に（または管理者による手動で）隔離します。

Proofpoint Cloud App Security Broker (CASB) はユーザー/組織の行動を監視します。

Proofpoint Enterprise Archive は、eディスカバリ、規制へのコンプライアンス、そしてエンドユーザーのデータアクセスをシンプルにします。

Proofpoint Security Awareness Trainingは、脅威とはどういうもので、どのように対処すべきかをユーザーに教育します。

Proofpoint Insider Threat Management (ITM)は、インサイダー（内部関係者）の悪意、怠慢、または事故によるデータ損失、犯罪、およびブランド価値の毀損などの内部脅威から組織を守ります。

Proofpoint Targeted Attack Protection (TAP) は組織に侵入する脅威を詳細に可視化してリスク評価をします。

目次

プルーフポイントを用いた NIST CSF 要件への準拠

資産管理 (ID.AM)

目標:「自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている。」

NIST CSF 要件 ID.AM-1

「自組織内の物理デバイスとシステムが、目録作成されている。」

参照:

- CIS CSC V7.1 1
- COBIT 5 BAI09.01, BAI09.02
- ISA 62443-2-1:2009 4.2.3.4
- ISA 62443-2-1:2013 SR 7.8
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
- NIST SP 800-53 Rev. 4 CM-8, PM-5
- NIST SP 800-53 Rev. 5 CM-8, PM-5

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM はシステムからハードウェアおよびソフトウェアの仕様の一覧を入手し、OS のバージョン、ハードウェアの詳細、IP アドレス、ハードウェアのドメインなどの目録を作成します。この情報を報告し、システムアセットの監査に活用できるようにします。

NIST CSF 要件 ID.AM-2

「自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。」

参照:

- CIS CSC V7.1 2
- COBIT 5 BAI09.01, BAI09.02, BAI09.05
- ISA 62443-2-1:2009 4.2.3.4
- ISA 62443-2-1:2013 SR 7.8
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
- NIST SP 800-53 Rev. 4 CM-8, PM-5
- NIST SP 800-53 Rev. 5 CM-8, PM-5

本要件に対応する製品:

- CASB
- Insider Threat Management (ITM)

CASB はファイアウォールやプロキシサーバーなどの企業セキュリティデバイスと統合し、シャドー IT を検知します。

ITM はデスクトップ、サーバー、アプリケーションなど、従業員が使用する資産の詳細アクティビティログを提供します。こういった情報は ID 管理や資産管理システムのレポートや補足情報から収集できます。さらに PDF レポートが提供されるため、自社事業に特有のリスクや該当するリスクの特定や対処に活用できます。

NIST CSF 要件 ID.AM-5

「リソース(例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア)が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。」

参照:

- CIS CSC V7.1 2
- COBIT 5 BAI09.01, BAI09.02, BAI09.05
- ISA 62443-2-1:2009 4.2.3.4
- ISA 62443-2-1:2013 SR 7.8
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
- NIST SP 800-53 Rev. 4 CM-8, PM-5
- NIST SP 800-53 Rev. 5 CM-8, PM-5

本要件に対応する製品:

- Enterprise Archive
- Insider Threat Management (ITM)

Enterprise Archive を利用すると、グローバルポリシーまたは詳細ポリシーに基づいてメッセージを分類し保持することができます。

ITM のアクティブ タイムマッピングとユーザー アクティビティ プロファイルを用いれば、アプリケーションの重要度と事業上の価値(最も使用されているものと、最もアクセスの少ないもの)を特定できます。PDF レポートも提供されます。管理者が定義したアラートに抵触したユーザーとそのリスクを関連付けて管理します。

ビジネス環境 (ID.BE)

目標:「自組織のミッション、目標、利害関係者、活動が、理解され、優先順位付けが行われている。この情報は、サイバーセキュリティ上の役割、責任、リスクマネジメント上の意思決定を伝えるために使用されている。」

NIST CSF 要件 ID.BE-1

「サプライチェーンにおける自組織の役割が、識別され、周知されている。」

参照:

- COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
- ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
- NIST SP 800-53 Rev. 4 CP-2, SA-12
- NIST SP 800-53 Rev. 5 CP-2, SR-1, SR-8

本要件に対応する製品:

- Proofpoint Premium Threat Intelligence Service (PTIS)

PTIS は脅威の最新ランドスケープとその中における自組織のポジションを明確にし、セキュリティ上の意思決定の優先順位付けを容易にします。

NIST CSF 要件 ID.BE-2

「重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。」

参照:

- COBIT 5 APO02.06, APO03.01
- ISO/IEC 27001:2013 4.1 節
- NIST SP 800-53 Rev. 4 PM-8
- NIST SP 800-53 Rev. 5 PM-8

本要件に対応する製品:

- Proofpoint Premium Threat Intelligence Service (PTIS)

PTIS は、同業他社との比較や、誰が組織を狙い、組織内の誰が狙われているかを明らかにするために、パーソナライズされたレポートを提供します。

NIST CSF 要件 ID.BE-3

「組織のミッション、目標、活動の優先順位が、定められ、周知されている。」

参照:

- COBIT 5 APO02.01, APO02.06, APO03.01
- ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6
- NIST SP 800-53 Rev. 4 PM-11, SA-14
- NIST SP 800-53 Rev. 5 PM-11, RA-9

本要件に対応する製品:

- Proofpoint Premium Threat Intelligence Service (PTIS)

PTIS は、サイバーセキュリティ対策を優先順位付けするためのリスク評価用にインテリジェンスを提供します。

ガバナンス (ID.GV)

目標:「自組織に対する規制、法律、リスク、環境、運用上の要求事項を、管理し、モニタリングするためのポリシー、手順、プロセスが理解されており、経営層にサイバーセキュリティリスクについて伝えている。」

NIST CSF 要件 ID.GV-1

「組織のサイバーセキュリティポリシーが、定められ、周知されている。」

参照:

- CIS CSC V7.1 19
- COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02
- ISA 62443-2-1:2009 4.3.2.6
- ISO/IEC 27001:2013 A.5.1.1
- NIST SP 800-53 Rev. 4 全セキュリティ コントロール ファミリーからのコントロール
- NIST SP 800-53 Rev. 5 全セキュリティ コントロール ファミリーからのコントロール

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM は管理ポリシー文書を配布する技術的手段として利用できます。こういった通知は利用規定メッセージとして静的に掲示するか、またはアクションが取られたときにリアルタイムに送ることができます。例えば大量のファイルが印刷またはコピーされるなど、異常なアクションが行われたときに利用規定が表示されます。

リスク評価 (ID.RA)

目標:「自組織は、(ミッション、機能、イメージ、評判を含む)組織の業務、組織の資産、個人に対するサイバーセキュリティリスクを把握している。」

NIST CSF 要件 ID.RA-1

「資産の脆弱性が、識別され、文書化されている。」

参照:

- CIS CSC V7.1 4
- COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02
- ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
- ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
- NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
- NIST SP 800-53 Rev. 5 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

本要件に対応する製品:

- Security Awareness Training

Security Awareness Trainingにはネットワーク上での脆弱性をチェックするオプションがあり、ブラウザの脆弱性検知に利用できます。またエンドユーザー PC 上のサードパーティ プラグインが最新化されていない (潜在的な脆弱性) 場合に警告します。

NIST CSF 要件 ID.RA-2

「サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。」

参照:

- CIS CSC V7.1 4
- COBIT 5 BAI08.01
- ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
- ISO/IEC 27001:2013 A.6.1.4
- NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
- NIST SP 800-53 Rev. 5 SI-5, PM-15, PM-16

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Proofpoint Premium Threat Intelligence Service (PTIS)
- Security Awareness Training
- TAP

Browser Isolation は、プルーフポイント エコシステムや会社メールを保護する脅威インテリジェンスと同じインテリジェンスを使用しています。

CASB はプルーフポイントの脅威インテリジェンスと、サイバー脅威に関する外部ソースを活用します。

Email Protection はアンチウイルス、悪意のあるファイルシグネチャ、悪意のある URL、およびスパム防御に関する共有脅威インテリジェンスを、内部および外部リソースから入手します。

PTISでは人による作業でフォーラムやソースから情報を収集し、他の機能の情報ソースとなります。

Security Awareness Training コミュニティでは情報共有のフォーラムが準備されています。マネージド Security Awareness Trainingには、顧客とのやり取りや業界ソースからの知識がプールされています。

共有脅威インテリジェンスは、悪意のあるファイルシグネチャと悪意のある URL の情報を扱う TAP 内の内部および外部ソースから受け取られます。

NIST CSF 要件 ID.RA-3

「内部および外部からの脅威が、識別され、文書化されている。」

参照:

- CIS CSC V7.1 4
- COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
- ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
- ISO/IEC 27001:2013 6.1.2 項
- NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
- NIST SP 800-53 Rev. 5 RA-3, SI-5, PM-12, PM-16

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Insider Threat Management (ITM)
- Proofpoint Premium Threat Intelligence Service (PTIS)

- Security Awareness Training
- TAP

Browser Isolation のポリシーにより、危険が疑われる URL を特定して、隔離された環境でアクセスされるようにします。

CASB はプルーフポイントの豊富なクロスチャネル（メール、SaaS、ソーシャル）脅威インサイトおよびユーザーの振る舞いをもとに、不審な行動を検知します。

Email Protection アンチウイルスでは、新種および既知のウイルスや、シグネチャベースおよび高度な技術を用いたその他の悪意あるコードを防御します。統合 DLP アプローチを活用することで、一般的なリスクインジケーターを可視化します。ここでは、機密ファイルのダウンロード、機密コードの移動、不審なソフトウェアのインストール、信頼できないクラウドストレージへの顧客リストのアップロード、リストに記載のないリムーバブルメディアへのファイルのコピーなどを誰が行ったかを特定して追跡します。

ITM はインサイダー脅威ライブラリを使って内部脅威を特定します。システム上のアクティビティは、アクセスレベルやロケーションに関係なくすべて文書化されます。ユーザーアクションから発生する外部および内部脅威は監視、文書化され、精査できる状態で提供されます。

PTISは詳細脅威レポートやアナリストの見解、そして脅威エキスパートによる Q&A を提供します。

Security Awareness Training、フィッシング シミュレーション、Cyberstrength アセスメントを用いると、潜在的な内部脅威を特定できます。

TAP Threat Dashboard は組織に入り込む脅威を詳細に可視化します。これにより誰がどのように、何を目的として攻撃してきており、どのユーザーが狙われているかがわかります。データは組織、脅威、ユーザー別に提供されます。これによってアラートの優先順位を明らかにし、それに沿って行動を起こすことができるようになります。

NIST CSF 要件 ID.RA-4

「ビジネスに対する潜在的な影響とその発生可能性が、識別されている。」

参照:

- CIS CSC V7.1 4
- COBIT 5 DSS04.02
- ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
- ISO/IEC 27001:2013 A.16.1.6, 6.1.2 節
- NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11
- NIST SP 800-53 Rev. 5 RA-2, RA-3, RA-9, PM-9, PM-11

本要件に対応する製品:

- CASB
- Email Protection
- Insider Threat Management (ITM)
- Proofpoint Premium Threat Intelligence Service (PTIS)
- TAP

CASB はサードパーティ アプリを自動管理し、ベンダーのレピュテーションとデータアクセスに基づいてスコア付けします。

Email Protection、TAP、PTIS は、その脅威が大勢を狙ったものかそれとも標的を絞ったものかという知見を提供するため、セキュリティ管理者がリスクを判断するときの材料として利用できます。Email DLP はユーザーの利用規定違反を検知して優先順位付けします。

ITM は、ユーザーの役割、機能、性質、そして脅威の深刻さを基に各脅威のリスクスコアとビジネスへの影響を判断します。

PTIS はご利用中のすべてのプルーフポイントのツール (TAP、CASB、Digital Risk など) から脅威データを入手して活用します。

TAP Threat Dashboard を利用すると、感染が疑われるユーザー (ターゲットとしての価値の高いユーザーを含む) を可視化できます。この知見を用いれば影響の大きさを理解でき、修復作業を優先順位付けできます。

NIST CSF 要件 ID.RA-5

「脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。」

参照:

- CIS CSC V7.1 3
- COBIT 5 APO12.02
- ISO/IEC 27001:2013 A.12.6.1
- NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
- NIST SP 800-53 Rev. 5 RA-2, RA-3, PM-16

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Insider Threat Management (ITM)
- PTIS
- TAP
- TRAP

Browser Isolation では、最もよく狙われるユーザーに注目し彼ら宛てのメールに含まれている URL の中で最もリスクの高いものを特定します。

CASBサンドボックスとアナリティクスはクラウド環境内の SaaS アプリの潜在的リスクを検知します。

Email Protection、TAP、PTIS は、その脅威が大勢を狙ったものかそれとも標的を絞ったものかという知見を提供するため、セキュリティ管理者がリスクを判断するときの材料として利用できます。Email DLP ルールは、組織が管理するデータへの脅威に基づいて導入できます。

ITM は各内部脅威のリスクスコアを提供します。このスコア付けではアクションの深刻さ、ユーザーの役割上のリスク、内部脅威による事業への影響が考慮されます。

TRAPを用いると、メール/セキュリティ管理者はメールを分析でき、悪意あるまたは望ましくないメールを配信後に隔離できるようになります。

NIST CSF 要件 ID.RA-6

「リスク対応が、識別され、優先順位付けされている。」

参照:

- CIS CSC V7.1 3
- COBIT 5 APO12.05, APO13.02
- ISO/IEC 27001:2013 6.1.3 節
- NIST SP 800-53 Rev. 4 PM-4, PM-9
- NIST SP 800-53 Rev. 5 PM-4, PM-9

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Insider Threat Management (ITM)
- PTIS
- TAP
- TRAP

Browser Isolation は不審な URL を、(最も脆弱で頻繁に攻撃される特権ユーザー向けに送られたものに特に注目して) 自動的に隔離します。

CASB は広範囲にわたるインシデント検知とアラート機能を提供し、リスク対応方法の特定と優先順位付けを容易にします。これらの情報は API を通して外部ソースにも取り込めます。

Email Protection、PTIS、TAP は、その脅威が大勢を狙ったものかそれとも標的を絞ったものかという知見を提供するため、セキュリティ管理者がリスクを判断するときの材料として利用できます。Email DLP は、セキュリティや開示ポリシーの決定が属人的にならないようにします。

ITM を用いれば、オペレーターはイベントの深刻さと重要性に基づいて様々なリスク対応からアクションを選定できます。このソリューションでは通知を自動化したりアクションを自動的に阻止できるよう設定できます。例えばリアルタイムに警告する、アプリケーションを閉じる、セッションからユーザーをログアウトさせる、などができます。

PTIS には脅威研究者による Q&A、調査、レスポンスが含まれます。

TAPは感染したユーザーや狙われやすいユーザーを特定するので、レスポンスの優先順位付けやリスク管理が可能になります。

TRAP を使えば、メール及びセキュリティ管理者はメールを分析でき、悪意のあるまたは望ましくないメールを配信後に隔離できるようになります。

リスクマネジメント戦略 (ID.RM)

目標:「自組織の優先順位、制約、リスク許容度、想定が、定められ、運用リスクに対する意思決定を支援するために利用されている。」

NIST CSF 要件 ID.RM-2

「組織のリスク許容度が、決定され、明確に表現されている。」

参照:

- COBIT 5 APO12.06
- ISA 6243-2-1 2009 4.3.2.6.5
- ISO/IEC 27001:2013 6.1.3 項、8.3 項
- NIST SP 800-53 Rev. 4 PM-9
- NIST SP 800-53 Rev. 5 PM-9

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM は組織上のリスクを集計してダッシュボードに表示し、全体リスクポリシーに基づいて閾値を設定します。

サプライチェーンリスクマネジメント (ID.SC)

目標:「自組織の優先順位、制約、リスク許容度、想定が、定められ、サプライチェーンリスクマネジメントに関連するリスクに対する意思決定を支援するために利用されている。自組織は、サプライチェーンリスクを識別し、分析・評価し、管理するためのプロセスを定め、実装している。」

NIST CSF 要件 ID.SC-4

「サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。」

参照:

- COBIT 5 APO12.05, APO13.02
- ISA 62443-2-1:2009 4.3.2.6.7
- ISA 62443-3-3:2013 SR 6.1
- ISO/IEC 27001:2013 A.15.2.1, A.15.2.2
- NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA 9, SA-12
- NIST SP 800-53 Rev. 5 AU-2, AU-6, AU-12, AU-16, PS-7, SA 9, SR-6

本要件に対応する製品:

- Enterprise Archive
- Insider Threat Management (ITM)

Enterprise Archive の Intelligent Supervision の監視システムを用いれば、送受信メール、IM、ブルームバーグ、音声、SMS、エンタープライズコラボレーション、ソーシャルメディアによるコミュニケーションを特定、レビュー、対処できます。また、監査証跡と監査レビューの記録の保持、コンプライアンス用の監督手順のモニタリングおよび評価、そして SEA 17a-4(b) で求められる内部コミュニケーションおよび通信内容の保管 (保管機関:3年および6年) への対応も可能になります。

ITM はユーザー アクティビティ レポートを提供します。これは契約上の義務が果たされているかを確認するために毎日または毎週ダウンロードできます。

アイデンティティ管理、認証／アクセス制御 (PR.AC)

目標:「物理的・論理的資産および関連施設へのアクセスが、認可されたユーザ、プロセス、デバイスに限定されている。また、これらのアクセスは、認可された活動およびトランザクションに対する不正アクセスのリスクアセスメントと一致して、管理されている。」

NIST CSF 要件 PR.AC-1

「認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。」

参照:

- CIS CSC V7.1 1, 4, 15, 16
- COBIT 5 DSS05.04, DSS06.03
- ISA 62443-2-1:2009 4.3.3.5.1
- ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
- ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
- NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
- NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

本要件に対応する製品:

- Enterprise Archive
- Insider Threat Management (ITM)

Enterprise Archive では検索、メッセージの閲覧、エクスポート、取得、監督アクティビティをトラッキングし、監査証跡と包括的レポートを作成します。これにより誰がいつ、どのコンプライアンスタスクを実行したかが可視化できます。保管された情報はインデックス付けされます。インデックス付けされた情報はデータが保管された場所で複製されます。データはどのような形式にもエクスポートできます。

ITM をデバイスにインストールすると、サービスデスクとの統合や二次認証を用いて、デバイスへのユーザーアクセスの監視やアクセス制御ができます。

NIST CSF 要件 PR.AC-3

「リモートアクセスが、管理されている。」

参照:

- CIS CSC V7.1 12
- COBIT 5 APO13.01, DSS01.04, DSS05.03
- ISA 62443-2-1:2009 4.3.3.6.6
- ISA 62443-3-3:2013 SR 1.13, SR 2.6
- ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1
- NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
- NIST SP 800-53 Rev. 5 AC-1, AC-17, AC-19, AC-20, SC-15

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM はターミナルサービス、ジャンプサーバー/ボックス、踏み台サーバー、および境界サーバーに配備され、ハードウェアのアクセス制御リストに基づいてアクセスを制限します。

NIST CSF 要件 PR.AC-4

「アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。」

参照:

- CIS CSC V7.1 3, 5, 12, 14, 15, 16, 18
- COBIT 5 DSS05.04
- ISA 62443-2-1:2009 4.3.3.7.3
- ISA 62443-3-3:2013 SR 2.1
- ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
- NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
- NIST SP 800-53 Rev. 5 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24

本要件に対応する製品:

- CASB
- Insider Threat Management (ITM)

CASB では保護対象の SaaS アプリケーション内のファイルへのアクセス許可をアップデートできるため、最小権限の原則を適用できます。

ITM は職務の分離のポリシー違反があった場合に警告します。例えば Salesforce の IT 管理者が見積もりを承認するということはポリシー違反です。ServiceNow や Remedy などとチケットを統合することで、チケット ID を持つユーザーのみにサーバーへのアクセスを許可できます。

NIST CSF 要件 PR.AC-5

「ネットワークの完全性が、保護されている(例:ネットワークの分離、ネットワークのセグメント化)。」

参照:

- CIS CSC V7.1 9, 12, 13, 14, 15, 18
- COBIT 5 DSS01.05, DSS05.02
- ISA 62443-2-1:2009 4.3.3.4
- ISA 62443-3-3:2013 SR 3.1, SR 3.8
- ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
- NIST SP 800-53 Rev. 5 AC-4, AC-10, SC-7

本要件に対応する製品:

- Browser Isolation

Browser Isolation は、通常プライベートで閲覧されるような URL カテゴリを企業ネットワークから分離できます。

NIST CSF 要件 PR.AC-6

「IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。」

参照:

- CIS CSC V7.1 6
- COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03
- ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4
- ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1
- ISO/IEC 27001:2013 A.7.1.1, A.9.2.1
- NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
- NIST SP 800-53 Rev. 5 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

本要件に対応する製品:

- Insider Threat Management (ITM)

ITMはアクセス制御にディレクトリサービスを使用します。多くの組織では Kerberos を用いた認証および追加制御が用いられるようになっており、これらは認証情報の証明として使われ、それに紐づけられ、相互に確認されます。

NIST CSF 要件 PR.AC-7

「ユーザ、デバイス、その他の資産は、トランザクションのリスク(例:個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク)の度合いに応じた認証(例:一要素、多要素)が行われている。」

参照:

- CIS CSC V7.1 1, 12, 15, 16
- COBIT 5 DSS05.04, DSS05.10, DSS06.10
- ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
- ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10
- ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4
- NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
- NIST SP 800-53 Rev. 5 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

本要件に対応する製品:

- CASB
- Insider Threat Management (ITM)

CASB はアイデンティティ プロバイダーと統合して Adaptive Access Control 機能を提供し、アクセス制御イベントに対してリスクに基づいた対応を実行できるようにします。

ITM では役割に基づいたアクセス制御ができるので、閲覧者、管理者、構成管理者に分類できます。機密データや個人特定が可能なユーザーデータの閲覧には二次認証を求めることができます。

意識向上およびトレーニング (PR.AT)

目標:「自組織の人員およびパートナーは、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育とトレーニングが実施されている。」

NIST CSF 要件 PR.AT-1

「すべてのユーザは、情報が周知され、トレーニングが実施されている。」

参照:

- CIS CSC V7.1 17, 18
- COBIT 5 APO07.03, BAI05.07
- ISA 62443-2-1:2009 4.3.2.4.2
- ISO/IEC 27001:2013 A.7.2.2
- NIST SP 800-53 Rev. 4 AT-2, PM-13
- NIST SP 800-53 Rev. 5 AT-2, PM-13

本要件に対応する製品:

- Insider Threat Management (ITM)
- Security Awareness Training

ITMは、ユーザーがログインしようとしているワークステーションに関するセキュリティポリシーを提示し、ユーザーがそのポリシーに同意しない限りアクセスを許可しません。

Security Awareness Trainingは様々なセキュリティトピックに関する包括的なエンドユーザー トレーニングを提供します。

NIST CSF 要件 PR.AT-2

「権限を持つユーザが、自身の役割と責任を理解している。」

参照:

- CIS CSC V7.1 4, 17, 18
- COBIT 5 APO07.02, DSS05.04, DSS06.03
- ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
- NIST SP 800-53 Rev. 4 AT-3, PM-13
- NIST SP 800-53 Rev. 5 AT-3, PM-13

本要件に対応する製品:

- Insider Threat Management (ITM)
- Security Awareness Training

ITM では役割に基づいたアクセス制御ができるので、閲覧者、管理者、構成管理者に分類できます。特権アカウントを使用してユーザーがログインする際には、その責任について説明するメッセージが表示されます。特権アカウントは、セキュリティおよび IT ベストプラクティスに基づいて高リスクとして位置付けられ、トラッキングされます。

Security Awareness Trainingでは、特権ユーザーや狙われやすいユーザー向けにカスタマイズしたトレーニングモジュールを提供できます。

NIST CSF 要件 PR.AT-3

「第三者である利害関係者(例:サプライヤー、顧客、パートナー)が、自身の役割と責任を理解している。」

参照:

- CIS CSC V7.1 17
- COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05
- ISA 62443-2-1:2009 4.3.2.4.2
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2
- NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16

本要件に対応する製品:

- Insider Threat Management (ITM)
- Security Awareness Training

ITM は、第三者である利害関係者が会社のアプリケーションやデバイスを使用する際に、その責任について知らせるための警告通知を表示します。

外部ベンダーやパートナーはSecurity Awareness Trainingを使って脅威対策を学習できます。

NIST CSF 要件 PR.AT-4

「上級役員(セキュリティ担当役員)が、自身の役割と責任を理解している。」

参照:

- CIS CSC V7.1 17, 19
- COBIT 5 APO07.03
- ISA 62443-2-1:2009 4.3.2.4.2
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,
- NIST SP 800-53 Rev. 4 AT-3, PM-13
- NIST SP 800-53 Rev. 5 AT-3, PM-13

本要件に対応する製品:

- Insider Threat Management (ITM)
- Security Awareness Training

ITM は、会社のアプリケーションやデバイスを使用するユーザーに利用規定を通知します。

Security Awareness Trainingは幹部社員に対して、彼らを標的とする脅威について教育します。

NIST CSF 要件 PR.AT-5

「物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。」

参照:

- CIS CSC V7.1 17
- COBIT 5 APO07.03
- ISA 62443-2-1:2009 4.3.2.4.2
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,
- NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
- NIST SP 800-53 Rev. 5 IR-2, PM-13, PM-15

本要件に対応する製品:

- Insider Threat Management (ITM)
- Security Awareness Training

ITM は、会社のアプリケーションやデバイスを使用するユーザーに利用規定を通知します。

Security Awareness Trainingではセキュリティ担当者向けのトレーニングモジュール提供しています。

データセキュリティ (PR.DS)

目標:「情報と記録(データ)が、情報の機密性、完全性、可用性を保護するための自組織のリスク戦略に従って管理されている。」

NIST CSF 要件 PR.AT-1

「保存されているデータが、保護されている。」

参照:

- CIS CSC v. 7.1 10, 13, 14
- COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06
- ISA 62443-3-3:2013 SR 3.4, SR 4.1
- ISO/IEC 27001:2013 A.8.2.3
- NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
- NIST SP 800-53 Rev. 5 AC-16, MP-8, SC-12, SC-28

本要件に対応する製品:

- Browser Isolation
- CASB
- Enterprise Archive
- Insider Threat Management (ITM)

Browser Isolation を用いれば、ポリシーを設定して、ダウンロード、アップロード、コピー&ペースト、キー入力など、リスクの高いアクションを管理できます。

CASB はメール、保存されたデータ、サポート対象のクラウドアプリケーションに DLP 検知を導入します。

Enterprise Archiveに含まれるProofpoint DoubleBlind™ Key Architecture では、すべてのメッセージ、ファイル、その他のコンテンツのアーカイブデータを、プルーフポイントデータセンターに届く前に任意のキーで暗号化できます。

ITMは、非構造化データやアプリケーション内のデータへのアクセスを監視して、データの誤用を警告し、データ閲覧者の情報を提供します。

NIST CSF 要件 PR.DS-2

「伝送中のデータが、保護されている。」

参照:

- CIS CSC V7.1 10, 13, 14
- COBIT 5 APO01.06, DSS05.02, DSS06.06
- ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2
- ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
- NIST SP 800-53 Rev. 5 AC-16, SC-8, SC-11, SC-12

本要件に対応する製品:

- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- TAP

CASB のポリシーベースのルールとブラウザ分離技術の統合により、伝送中のデータの持つリスクに則した対応を自動的に実施できます。

Email Protection は自動的にメールと添付ファイルを暗号化します。統合 DLP アプローチを活用することで、信頼できないクラウドストレージ、ネットワーク、リムーバブルメディアへの機密データのダウンロードを特定して保護します。また送信メールにおけるデータ漏洩のリスクを低減するための機能も提供します。

伝送中の Enterprise Archive データはプルーフポイント クラウドに保存されるまでは TLS で保護されます

デスクトップに ITM をインストールすると、アプリケーション、ファイル共有、Web サイトとの間で伝送されるデータをキャプチャできます。これにより情報伝送ポリシーおよび手順を効果的に執行できます。

伝送中の TAP データは FIPS 140-2 対応の暗号化技術で保護されます。

NIST CSF 要件 PR.DS-4

「可用性を確保するのに十分な容量が、維持されている。」

参照:

- CIS CSC V7.1 6, 10, 13
- COBIT 5 APO13.01, BAI04.04
- ISA 62443-3-3:2013 SR 7.1, SR 7.2
- ISO/IEC 27001:2013 A.12.1.3, A.17.2.1
- NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
- NIST SP 800-53 Rev. 5 AU-4, CP-2, SC-5

本要件に対応する製品:

- Enterprise Archive

Enterprise Archive を用いれば、メール基盤がオフラインになった場合でもアーカイブされたメールにアクセスできます。またディザスタリカバリにも対応しています。

NIST CSF 要件 PR.DS-5

「データ漏えいに対する防御対策が、実装されている。」

参照:

- CIS CSC V7.1 13
- COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02
- ISA 62443-3-3:2013 SR 5.2
- ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
- NIST SP 800-53 Rev. 5 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

本要件に対応する製品:

- Browser Isolation
- CASB
- Insider Threat Management (ITM)

Browser Isolation ポリシーでは、アップロード、ダウンロード、コピー&ペースト、およびキー入力を制限できます。

CASB はスマート識別子と辞書を用いた高精度な検知および防御

機能を提供し、クラウド SaaS アプリケーション内の個人情報や機密情報の漏洩を防ぎます。機密データが検知された場合はポリシーを執行し、本来の受信者以外にはアクセスや共有ができないようにします。

ITM　ライブラリを用いれば、データ損失や破壊行為を検知できます。このソリューションは非構造化データやアプリケーション内のデータへのアクセスを監視します。またデータにアクセス、またはデータを閲覧したユーザーの情報を提供します。

NIST CSF 要件 PR.DS-6

「完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。」

参照:

- CIS CSC V7.1 2, 5
- COBIT 5 APO01.06, BAI06.01, DSS06.02
- ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8
- ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
- NIST SP 800-53 Rev. 4 SC-16, SI-7
- NIST SP 800-53 Rev. 5 SC-16, SI-7

本要件に対応する製品:

- Enterprise Archive

デジタル フィンガープリンティング プロセスで完全性を維持し、アーカイブ時に MD5 バリューが合致することを確認します。

NIST CSF 要件 PR.DS-7

「開発・テスト環境が、実稼働環境から分離されている。」

参照:

- CIS CSC v. 7.1 18, 20
- COBIT 5 BAI03.08, BAI07.04
- ISO/IEC 27001:2013 A.12.1.4
- NIST SP 800-53 Rev. 4 CM-2
- NIST SP 800-53 Rev. 5 CM-2

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- TAP
- TRAP

プルーフポイントのソリューションは実稼働環境、開発環境、テスト環境などに別々に配備できます。

ITM によるチケッティングの統合で、承認されたユーザーのみにアクセスを許可できます。実稼働システムへのログインが許可されていない開発者は、実稼働システムにはアクセスできません。ジャンプサーバーに ITM をインストールすると実稼働環境へのアクセスを監視できます。これはユーザー毎にアクセス権を制限できると同時に、メンテナンスやトラブルシューティングの場合にのみアクセスを許可することもできます。

情報を保護するための プロセスおよび手順 (PR.IP)

目標:「(目的、範囲、役割、責任、経営コミットメント、組織間の調整について記した)セキュリティポリシー、プロセス、手順が、維持され、情報システムと資産の防御の管理に使用されている。」

NIST CSF 要件 PR.IP-1

「情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則(例:最低限の機能性の概念)を組み入れて、定められ、維持されている。」

参照:

- CIS CSC V7.1 3, 9, 11
- COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05
- ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
- ISA 62443-3-3:2013 SR 7.6
- ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
- NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
- NIST SP 800-53 Rev. 5 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

本要件に対応する製品:

- Browser Isolation
- Insider Threat Management (ITM)

Browser Isolation はブラウザセッションが終了された時点でブラウザを破壊します。そして新たにブラウザセッションを始めるときには基礎構成に沿った新しいブラウザを作成します。

ITM は、Remedy や ServiceNow などのサービス管理ツールと統合し、ユーザーがシステムにアクセスする前に承認チケットを要求します。ITM アプリケーションは管理上の変更、ヘルスイベント、エージェントの改ざんの試みをすべて監査します。特定の構成ファイルに対して ITM アラートを設定すると、それらのファイルへの変更を通知し記録します。

NIST CSF 要件 PR.IP-3

「構成変更管理プロセスは、策定されている。」

参照:

- CIS CSC v. 7.1 3, 11
- COBIT 5 BAI01.06, BAI06.01
- ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
- ISA 62443-3-3:2013 SR 7.6
- ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
- NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
- NIST SP 800-53 Rev. 5 CM-3, CM-4, SA-10

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM レポートは構成変更をトラッキングし、変更管理プロセスが効力を持ち管理されていることを確認します。

NIST CSF 要件 PR.IP-4

「情報のバックアップが、実施され、維持され、テストされている。」

参照:

- CIS CSC v. 7.1 10
- COBIT 5 APO13.01, DSS01.01, DSS04.07
- ISA 62443-2-1:2009 4.3.4.3.9
- ISA 62443-3-3:2013 SR 7.3, SR 7.4
- ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
- NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
- NIST SP 800-53 Rev. 5 CP-4, CP-6, CP-9

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Enterprise Archive
- Insider Threat
- Security Awareness Training
- TAP
- TRAP

自動バックアップシステムでは、プルーフポイントにホスティングされた実稼働システムおよびデータを、事前定義した間隔でバックアップするよう設定できます。

NIST CSF 要件 PR.IP-6

「データは、ポリシーに従って破壊されている。」

参照:

- COBIT 5 BAI09.03, DSS05.06
- ISA 62443-2-1:2009 4.3.4.4.4
- ISA 62443-3-3:2013 SR 4.2
- ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
- NIST SP 800-53 Rev. 4 MP-6
- NIST SP 800-53 Rev. 5 MP-6

本要件に対応する製品:

- Enterprise Archive

Enterprise Archive はコンプライアンス維持ポリシーに沿ってすべてのメッセージとコンテンツをアーカイブし、規制要件への対応をサポートします。

NIST CSF 要件 PR.IP-7

「防御プロセスは、改善されている。」

参照:

- COBIT 5 BAI09.03, DSS05.06
- ISA 62443-2-1:2009 4.3.4.4.4
- ISA 62443-3-3:2013 SR 4.2
- ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
- NIST SP 800-53 Rev. 4 MP-6
- NIST SP 800-53 Rev. 5 MP-6

本要件に対応する製品:

- Browser Isolation
- Email Protection

Browser Isolation は web ブラウザ経由で届くフィッシングやマルウェア攻撃からユーザーを保護します。

Email Protection はユーザーのメールに対するアクションの情報を活用して、今後の検知および分類精度を向上させます。

NIST CSF 要件 PR.IP-11

「サイバーセキュリティには、人事に関わるプラクティス(例:アクセス権限の無効化、人員のスクリーニング)が含まれている。」

参照:

- CIS CSC V7.1 5, 16
- COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
- ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
- ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4
- NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
- NIST SP 800-53 Rev. 5 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

本要件に対応する製品:

- Security Awareness Training

Security Awareness Trainingは人事のトレーニング (特に新入社員のオンボーディングや、継続的なトレーニングおよびアセスメント) と統合できます。

保護技術 (PR.PT)

目標:「技術的なセキュリティソリューションが、関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンスを確保するために管理されている。」

NIST CSF 要件 PR.PT-1

「監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。」

参照:

- CIS CSC V7.1 1, 3, 5, 6, 14, 15, 16
- COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01
- ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
- ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
- NIST SP 800-53 Rev. 4 AU Family
- NIST SP 800-53 Rev. 5 AU Family

本要件に対応する製品:

- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- TAP

CASB は、ユーザー、ロケーション、デバイス、ネットワーク、ログイン時間などのコンテキストログ記録データを提供します。また振る舞い分析を行って、異常または不審な利用を監視します。

Email Protection ログファイルを SIEM ツールにエクスポートします。異常なアクティビティがないかネットワークを監視します。

Enterprise Archive では検索、メッセージの閲覧、エクスポート、取得、監督アクティビティをトラッキングし、監査証跡と包括的レポートを作成します。

Enterprise Archive の Intelligent Supervision の監視システムを用いれば、送受信メール、IM、ブルームバーグ、音声、SMS、エンタープライズコラボレーション、ソーシャルメディアによるコミュニケーションを特定、レビュー、対処できます。また監査証跡と監査レビューの記録の保持、コンプライアンス用の監督手順のモニタリングおよび評価、そして SEA 17a-4(b) で求められる内部コミュニケーションおよび通信内容の保管 (保管機関:3年および6年) への対応も可能になります。

ITM はデスクトップ、アプリケーション、サーバー上のすべてのユーザーアクティビティを記録します。ログを生成しないアプリケーションもまた監査されます。

TAP システムログファイル (ネットワーク アクティビティを含む) は、不審なアクティビティを監視する SIEM ツールにエクスポートされます。

NIST CSF 要件 PR.PT-2

「リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。」

参照:

- CIS CSC V7.1 8, 13
- COBIT 5 APO13.01, DSS05.02, DSS05.06
- ISA 62443-3-3:2013 SR 2.3
- ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
- NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
- NIST SP 800-53 Rev. 5 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8

本要件に対応する製品:

- Email Protection
- Insider Threat Management (ITM)

Email Protection は DLP および暗号化ルールを用いて、メール内の機密データを暗号化し、リムーバブルメディアにダウンロードしたとしても判読できないようにします。

ITM はリムーバブルメディアの使用を検知し、ポリシーに沿ってその使用を制限します。

NIST CSF 要件 PR.PT-3

「最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。」

参照:

- CIS CSC V7.1 3, 11, 14
- COBIT 5 DSS05.02, DSS05.05, DSS06.06
- ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4

- ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
- ISO/IEC 27001:2013 A.9.1.2
- NIST SP 800-53 Rev. 4 AC-3, CM-7
- NIST SP 800-53 Rev. 5 AC-3, CM-7

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- TAP

Browser Isolation は、コーポレートメール内の URL をユーザーがクリックした場合に、そのリスクに基づいて処理を分離します。

CASB はポリシーおよび振る舞い分析に基づいてユーザー機能を無効化します。

Email Protection は、制限対象となっているタイプのファイルの送信/受信ができないようアクセスを制限します。

Enterprise Archive は会社のポリシーに従って、適切な権限を持ったユーザーにのみメールと監視データへのアクセスを許可します。

ITM はチケッティングシステムに統合し、アクティブな承認済みサービスチケットに基づいてアクセスを制限します。二次認証およびメッセージのブロック機能で、ネットワーク上でのアクセス制御を強化できます。また ITM をジャンプサーバーに導入すると、ジャンプサーバーを経由しなければネットワークデバイスにアクセスできないように設定できます。すべてのアクセスは記録されます。

TAP は URL の書き直しをかけることにより、悪意のあるサイトへのアクセスを制限します。

NIST CSF 要件 PR.PT-4

「通信(情報)ネットワークと制御ネットワークが、保護されている。」

参照:

- CIS CSC V7.1 8, 12, 15
- COBIT 5 DSS05.02, APO13.01
- ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
- ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC 36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
- NIST SP 800-53 Rev. 5 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC 36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM はシステム、ICA、RDP、VPN、SSH、および Telnet プロトコル上のすべてのアクティビティを記録します (SFTP 通信とコマンドの詳細記録を含む)。これにより情報伝送ポリシーおよび手順を効果的に執行できます。

NIST CSF 要件 PR.PT-5

「メカニズム(例:フェールセーフ、ロードバランシング、ホットスワップ)が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。」

参照:

- COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
- ISA 62443-2-1:2009 4.3.2.5.2
- ISA 62443-3-3:2013 SR 7.1, SR 7.2
- ISO/IEC 27001:2013 A.17.1.2, A.17.2.1
- NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
- NIST SP 800-53 Rev. 5 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

本要件に対応する製品:

- CASB
- Browser Isolation
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- Security Awareness Training
- TAP
- TRAP

プルーフポイントのソリューションは必要な場合、米国、カナダ、オランダ、ドイツに地理的に分散した複数のデータセンターを介して、管轄上問題のないクラウドアーキテクチャを使用します。

異常とイベント (DE.AE)

目標:「異常な活動は、検知されており、イベントがもたらす潜在的な影響が、把握されている。」

NIST CSF 要件 DE.AE-1

「ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。」

参照:

- CIS CSC V7.1 1, 4, 6, 12, 13, 15, 16
- COBIT 5 DSS03.01
- ISA 62443-2-1:2009 4.4.3.3
- ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2
- NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
- NIST SP 800-53 Rev. 5 AC-4, CA-3, CM-2, SI-4

本要件に対応する製品:

- CASB
- Email Protection
- Insider Threat Management (ITM)
- Security Awareness Training

CASB および Email Protection DLP 機能は、伝送中、保存中、使用中の機密データを可視化し保護します。例えば、ユーザーが機密データをクラウドアプリケーションや SharePoint サイトにアップロードしようとしたり、データを抜き出してメールで送ろうとしているときに警告をします。

ITM はエンドポイント (アプリケーション IT インフラストラクチャ) からデータを収集して、インデックス付きの検索可能なアクティビティログを作成し、セッションを記録します。これは「ユーザーモード」エージェントを介してベースラインを確立するために利用できます。このソリューションでは面倒なアラート設定をすることなく、ユーザーがファイル、システム、アプリケーションをどのように使用しているかを可視化できます。このデータは詳細分析をするために SIEM やその他のツールに送信することができます。

Security Awareness Trainingは、誰がフィッシングに騙されやすいかを特定します。

NIST CSF 要件 DE.AE-2

「検知したイベントは、攻撃の標的と手法を理解するために分析されている。」

参照:

- CIS CSC V7.1 13, 14
- COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06
- ISA 62443-3-3:2013 SR 3.4, SR 4.1
- ISO/IEC 27001:2013 A.8.2.3
- NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
- NIST SP 800-53 Rev. 5 MP-8, SC-12, SC-28

本要件に対応する製品:

- CASB
- Email Protection
- PTIS
- Security Awareness Training
- TAP

CASB は脅威インテリジェンスを用いて攻撃対象と手法を検知します。

Email Protection はメール本文と添付ファイルを検査して既知のマルウェアを検知し、メールやファイルを隔離します。Email DLP 機能では機密データの伝送を検知し防止します。

ITM アラートは、アラートを引き起こしたユーザーアクションに関係するアプリケーション、ファイル、サーバーを明示します。さらに、攻撃手法と標的を検知するようアラートを設定できます。例えば、SU および SUDO の誤用、不審な FTP、RDP、SSH 接続などのアラートです。

PTIS では、特定の標的型攻撃について、セキュリティアナリストが詳細な個別コンテキストを提供します。

Security Awareness Trainingは、特定の攻撃タイプに騙されやすいユーザーを特定して報告します。

TAPはファイルシグネチャ、ファイルサンドボックス、URL 分析でメール本文と添付ファイルを調べ、既知のゼロデイ脅威を検知します。

NIST CSF 要件 DE.AE-3

「イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。」

参照:

- CIS CSC V7.1 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16
- COBIT 5 BAI08.02
- ISA 62443-3-3:2013 SR 6.1
- ISO/IEC 27001:2013 A.12.4.1, A.16.1.7
- NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
- NIST SP 800-53 Rev. 5 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

本要件に対応する製品:

- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- PTIS
- Security Awareness Training
- TAP

Email Protection はEメールファイアウォール、アンチウイルス、スパムモジュールからイベントを収集します。

Enterprise Archive は電子的なコミュニケーション (メール、IM、ブルームバーグ、音声、SMS、エンタープライズコラボレーション、ソーシャルメディア コンテンツなど) への、単一の統合インターフェースを提供します。

ITM は Windows、Macintosh、Linux / UNIX マシンを含むさまざまなエンドポイントのセンサーからイベントデータ(ユーザーアクティビティ)を収集します。この情報はまた、SIEM や UBA ツールなどのアグリゲーターツールにエクスポートできます。

PTIS では、特定の標的型攻撃について、セキュリティアナリストが詳細な個別コンテキストを提供します。

Security Awareness Trainingでは、トレーニング結果やフィッシング攻撃シミュレーションについてのレポートを提供します。

TAPイベントは、ファイルシグネチャ、ファイルサンドボックス、URL分析モジュールから収集されます。

NIST CSF 要件 DE.AE-4

「イベントの影響が、判断されている。」

参照:

- CIS CSC V7.1 6
- COBIT 5 APO12.06, DSS03.01
- ISO/IEC 27001:2013 A.16.1.4
- NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
- NIST SP 800-53 Rev. 5 CP-2, IR-4, RA-3, SI-4

本要件に対応する製品:

- Email Protection
- Insider Threat Management (ITM)
- PTIS
- TAP

Email Protection はTAP を用いて、コンテンツや URL が安全か、または悪意があるかをフィルタリングします。

ITM は容易に設定可能なアラートルールに基づいて、イベントをスコア付け (影響と必要な対処の詳細を含む) します。これは環境にあわせてカスタマイズもできます。

PTIS では、検出した脅威、そして対策がされていない脅威について、システム、ネットワーク、および運用上のリスクを顧客と話し合います。

NIST CSF 要件 DE.AE-5

「インシデント警告の閾値が、定められている。」

参照:

- CIS CSC V7.1 6, 19
- COBIT 5 APO12.06, DSS03.01
- ISA 62443-2-1:2009 4.2.3.10
- ISO/IEC 27001:2013 A.16.1.4
- NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
- NIST SP 800-53 Rev. 5 IR-4, IR-5, IR-8

本要件に対応する製品:

- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- TAP

CASB では、例えば DLP ポリシー違反が規定数を超えた時など、アラートの閾値を適宜変更できます。

悪意のある、または無害なコンテンツをどのように処理するかといったメールポリシーを設定できます。

Enterprise Archive は以下の場合に警告を出します。

- 特定の時間内にメールが一通もアーカイブまたは受信されなかった場合。
- メールが適切にアーカイブされなかった場合。
- アーカイブのキューの数が多くなりすぎた場合。

ITM ではアラートの閾値が最初から設定されています。管理者はユーザー単位、グループ単位、アプリケーション単位およびアラート単位に閾値を変更できます。ユーザーアクティビティプロファイルはユーザーアクティビティの基準となり、アプリケーションの使用、Web アクセス、アカウント/マシンの使用についての知見と閾値を提供します。

TAP は潜在的脅威を発見した場合管理者にアラートを送ります。

セキュリティの継続的なモニタリング (DE.CM)

目標:「情報システムと資産は、サイバーセキュリティイベントを識別し、保護対策の有効性を検証するために、モニタリングされている。」

NIST CSF 要件 DE.CM-1

「ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。」

参照:

- CIS CSC V7.1 1, 7, 8, 12, 13, 15, 16
- COBIT 5 DSS01.03, DSS03.05, DSS05.07
- ISA 62443-3-3:2013 SR 6.2
- NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
- NIST SP 800-53 Rev. 5 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- TAP

Browser Isolation は、コーポレートメール内の URL をユーザーがクリックした場合に、そのリスクに基づいて処理を分離します。

CASB はお客様のクラウド SaaS 環境上で、不審なログイン、マルウェア、異常なアクティビティなどのサイバーセキュリティイベントが発生していないかを監視します。

Email Protection および TAP はメールを監視して、異常なメールアクティビティを発見します。

NIST CSF 要件 DE.CM-2

「物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。」

参照:

- COBIT 5 A.11.1.1, A.11.1.2
- ISA 62443-2-1:2009 4.3.3.3.8
- ISO/IEC 27001:2013 A.11.1.1, A.11.1.2
- NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
- NIST SP 800-53 Rev. 5 CA-7, PE-3, PE-6, PE-20

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM はユーザーがアクセスする物理および仮想プラットフォームに関してホストベースのインテリジェンスを提供します。

NIST CSF 要件 DE.CM-3

「人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。」

参照:

- CIS CSC V7.1 1, 7, 8, 12, 13, 15, 16
- COBIT 5 DSS01.03, DSS03.05, DSS05.07
- ISA 62443-3-3:2013 SR 6.2
- NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
- NIST SP 800-53 Rev. 5 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Insider Threat Management (ITM)
- Security Awareness Training
- TAP

Browser Isolation はプライバシー要件に対応するため匿名モードで実行したり、ユーザーのアクティビティを監視したりできます。

CASB は SaaS アプリケーション内でのユーザーのアクティビティを監視します。侵害したアカウントを使った内部攻撃などのサイバーセキュリティイベントを検知できます。

Email Protection および TAP は管理作業をログしアーカイブします。

ITM はエンドポイントでのユーザーアクティビティを監視し、内部脅威アラートに基づいて高リスクのアクティビティを検知します。エンドポイントにはデスクトップ、サーバー、アプリケーションが含まれます。

Security Awareness Trainingのフィッシング シミュレーション データを用いれば、実際に起こり得るイベントを想定できます。

NIST CSF 要件 DE.CM-4

「悪質なコードは、検知されている。」

参照:

- CIS CSC V7.1 5, 7, 14, 16
- COBIT 5 DSS01.04, DSS01.05
- ISA 62443-2-1:2009 4.3.3.3.8
- ISO/IEC 27001:2013 A.11.1.1, A.11.1.2
- NIST SP 800-53 Rev. 4 4 CA-7, PE-3, PE-6, PE-20
- NIST SP 800-53 Rev. 5 4 CA-7, PE-3, PE-6, PE-20

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- TAP

Browser Isolation はメールや Web アプリケーション内の悪意のあるコードを特定します。

CASB は TAP サンドボックス技術と統合してマルウェアを検知します。

Email Protection は、ファイル シグネチャ分析とファイルサンドボックスを用いたアンチウイルスソフトウェアで、メール内の悪意のあるコードを検知します。

NIST CSF 要件 DE.CM-5

「不正なモバイルコードは、検知されている。」

参照:

- CIS CSC V7.1 7, 8
- COBIT 5 DSS05.01
- ISA 62443-2-1:2013 SR 2.4
- ISO/IEC 27001:2013 A.12.5.1, A.12.6.2
- NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
- NIST SP 800-53 Rev. 5 SC-18, SI-4, SC-44

本要件に対応する製品:

- CASB
- Email Protection
- TAP

CASB は、Oauth トークンを使って保護された SaaS アプリケー

ションへアクセスするサードパーティ アプリケーションを検知します。Oauth トークンはたいていのモバイルデバイスにインストールされています。

Email Protection および TAP は、ファイル シグネチャ分析とファイルサンドボックスを用いたアンチウイルスソフトウェアで、メール内の悪意のあるコードを検知します。

NIST CSF 要件 DE.CM-6

「外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。」

参照:

- COBIT 5 DSS05.01
- ISO/IEC 27001:2013 A.14.2.7, A.15.2.1
- NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
- NIST SP 800-53 Rev. 5 CA-7, PS-7, SA-4, SA-9, SI-4

本要件に対応する製品:

- CASB
- Email Protection
- Insider Threat Management (ITM)

CASB および Email Protection の DLP 機能は、機密データの伝送を可視化し保護します。

ITM は、組織が提供したエンドポイントや仮想環境を使用する第三者のアクティビティを監視します。このソリューションでは内部脅威アラートに基づいて高リスクなアクティビティを検知します。これは通常、入力マシンまたは出力サービスを通じて外部サービスプロバイダーのマシンを監視することで検知します。

NIST CSF 要件 DE.CM-7

「権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。」

参照:

- CIS CSC V7.1 1, 2, 3, 5, 9, 12, 13, 15, 16
- COBIT 5 DSS05.02, DSS05.05
- ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1
- NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
- NIST SP 800-53 Rev. 5 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4

本要件に対応する製品:

- Email Protection
- Insider Threat Management (ITM)

Email Protection は無効または未知の受信者へのメール、またはそれらからのメールをブロックできます。

ITM は未承認のソフトウェア、特権の付与や誤用に焦点を当てた内部脅威アラートを送ることができます。これにより未承認および承認済みのユーザー、アクセス、ソフトウェアを可視化できます。

NIST CSF 要件 DE.CM-8

「脆弱性スキャンが、実施されている。」

参照:

- CIS CSC V7.1 4, 20
- COBIT 5 BAI03.10, DSS05.01
- ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7
- ISO/IEC 27001:2013 A.12.6.1
- NIST SP 800-53 Rev. 4 RA-5
- NIST SP 800-53 Rev. 5 RA-5

本要件に対応する製品:

- Security Awareness Training
- TAP

Security Awareness Trainingではフィッシングシミュレーションを行って脆弱性を検知できます。プラグイン検知には、Java、Silverlight、QuickTime、Adobe Flash、Windows Media Player、Adobe PDF、RealPlayer のスキャンを実行するオプションがあります。

TAP は添付ファイルと URL を分析して既知および未知の脆弱性を検知します。

検知プロセス (DE.DP)

目標:「検知プロセスおよび手順が、異常なイベントに確実に気付くために維持され、テストされている。」

NIST CSF 要件 DE.DP-2

「検知活動は、該当するすべての要求事項を準拠している。」

参照:

- COBIT 5 DSS06.01, MEA03.03, MEA03.04
- ISA 62443-2-1:2009 4.4.3.2
- ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3
- NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
- NIST SP 800-53 Rev. 5 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Insider Threat Management (ITM)
- PTIS
- Security Awareness Training
- TAP
- TRAP

プルーフポイント ソリューションでは事業要件に沿うよう構成をカスタマイズできます。

NIST CSF 要件 DE.DP-3

「検知プロセスが、テストされている。」

参照:

- COBIT 5 APO13.02, DSS05.02
- ISA 62443-2-1:2009 4.4.3.2
- ISA 62443-3-3:2013 SR 3.3
- ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3
- NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
- NIST SP 800-53 Rev. 5 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- Security Awareness Training
- TAP
- TRAP

Proofpoint Professional Service は配備フェーズにおいて、検知シナリオが想定通りに機能するよう設定を確認します。

NIST CSF 要件 DE.DP-4

「イベント検知情報が、周知されている。」

参照:

- CIS CSC V7.119
- COBIT 5 APO08.04, APO12.06, DSS02.05
- ISA 62443-2-1:2009 4.3.4.5.9
- ISA 62443-3-3:2013 SR 6.1
- ISO/IEC 27001:2013 A.16.1.2, A.16.1.3
- NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
- NIST SP 800-53 Rev. 5 AU-6, CA-2, CA-7, RA-5, SI-4

本要件に対応する製品:

- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- TAP

CASB は自動生成レポートや API フィードを用いてイベント検知情報を提供します。

Email Protection のイベントは TAP ダッシュボードおよびログファイルに送られます。これは SIEM ツールにエクスポートできます。

Enterprise Archive の Intelligent Supervision は、メールインフラストラクチャ内で発生している詐欺行為やその他のアクティビティを検知します。

違反があった場合、ITM は違反したユーザーに代替手段を提案し、これによりセキュリティポリシーへの意識を向上させます。

NIST CSF 要件 DE.DP-5

「検知プロセスが、継続的に改善されている。」

参照:

- COBIT 5 APO12.06, DSS04.05
- ISA 62443-2-1:2009 4.4.3.4
- ISO/IEC 27001:2013 A.16.1.6
- NIST SP 800-53 Rev. 4 CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
- NIST SP 800-53 Rev. 5 CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

本要件に対応する製品:

- CASB
- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- TAP

CASB を継続的に使用することで、自動修正を用いて成熟度を高め、リスクに則した対応を提供できるようになります。

Email Protection のアンチウイルスとスパムシグネチャは継続的に改善され更新されています。

Enterprise Archive の Intelligent Supervision は検知した情報をレビューして、トレーニングを向上させます。

ITM はオペレーターが検出結果を向上できるよう、内部脅威アナリストによる追加サービスを提供します。

TAP は悪意のあるファイルを新たに特定した場合、共有ファイル レピュテーション データベースに追加します。

分析 (RS.AN)

目標:「分析は、効果的な対応を確実にし、復旧活動を支援するために実施されている。」

NIST CSF 要件 RS.AN-1

「検知システムからの通知は、調査されている。」

参照:

- CIS CSC V7.1 4, 6, 8, 19
- COBIT 5 DSS02.04, DSS02.07
- ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
- ISA 62443-3-3:2013 SR 6.1
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5
- NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
- NIST SP 800-53 Rev. 5 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

本要件に対応する製品:

- CASB
- Email Protection
- Insider Threat Management (ITM)
- TAP
- TRAP

CASB は、クラウド SaaS アプリケーション内で検知したインシデントを管理し調査します。

Email Protection を用いると、TAP ダッシュボードや SIEM ログファイルでアラートを受け取ることができます。セキュリティ管理者はこれらのイベント通知をインシデント対応プロセスに活用できます。

ITM のアラートは管理者または SIEM に送られます。管理者はこれを用いてファイル移動のタイムライン、メール送受信、ユーザーアクティビティを調査できます。調査に必要なレポートは自動作成できます。

TRAP アラートには調査に役立つ関連脅威情報が書かれています。

NIST CSF 要件 RS.AN-2

「インシデントがもたらす影響は、把握されている。」

参照:

- COBIT 5 DSS02.02
- ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
- ISO/IEC 27001:2013 A.16.1.4, A.16.1.6
- NIST SP 800-53 Rev. 4 CP-2, IR-4
- NIST SP 800-53 Rev. 5 CP-2, IR-4

本要件に対応する製品:

- CASB
- Email Protection
- Insider Threat Management (ITM)
- TAP
- TRAP

CASB はインシデント分析用に、ユーザー、ファイル、アラート、およびアクティビティの観点から複数の使いやすいビューを提供します。これによりイベントの影響がわかりやすくなり、分析のスピードアップができます。

Email Protection を用いると、TAP ダッシュボードや SIEM ログファイルでアラートを受け取ることができます。セキュリティ管理者はこれらのイベント通知をインシデント対応プロセスに活用できます。

ITM はユーザーアクションのコンテキストを提供します。アラートにはイベントの影響の詳細と必要な対応計画が含まれています。

TRAP アラートには調査に役立つ関連脅威情報が書かれています。

NIST CSF 要件 RS.AN-3

「フォレンジックが、実施されている。」

参照:

- COBIT 5 APO12.06, DSS03.02, DSS05.07
- ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
- ISO/IEC 27001:2013 A.16.1.7
- NIST SP 800-53 Rev. 4 AU-7, IR-4
- NIST SP 800-53 Rev. 5 AU-7, IR-4

本要件に対応する製品:

- Email Protection
- Enterprise Archive
- Insider Threat Management (ITM)
- PTIS
- TAP
- TRAP

Email Protection を用いると、TAP ダッシュボードや SIEM ログファイルでアラートを受け取ることができます。セキュリティ管理者はこれらのイベント通知をインシデント対応プロセスに活用できます。

Enterprise Archive では、問題調査に必要となる、コミュニケーションの検索ができます。

ITM のセッション記録とログは安全に保存されます。そしてインシデント中に発生した事象について正確なフォレンジック エビデンスを提供します。

PTIS はエンドポイントまたは SIEM と比較するためサンドボックスフォレンジックを提供します。

TRAP アラートには調査に役立つ関連脅威情報が書かれています。

NIST CSF 要件 RS.AN-4

「インシデントは、対応計画に従って分類されている。」

参照:

- CIS CSC VER.7.119
- COBIT 5 DSS02.02
- ISA 62443-2-1:2009 4.3.4.5.6
- ISO/IEC 27001:2013 A.16.1.7
- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
- NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-5, IR-8

本要件に対応する製品:

- CASB
- Email Protection
- Insider Threat Management (ITM)
- PTIS
- TAP
- TRAP

CASB ではインシデントを不審なログイン、不審なアクティビティ、データ、データ漏洩に分類します。

Email Protection を用いると、TAP ダッシュボードや SIEM ログファイルでアラートを受け取ることができます。セキュリティ管理者はこれらのイベント通知をインシデント対応プロセスに活用できます。

ITM を用いれば、高リスクユーザーのアクティビティとデータの移

動をすぐに把握できます。コンテキストを活用して誰が、何を、どこで、いつ、なぜアラートを引き起こしたかを理解することで、迅速なインシデント対応が可能になります。

PTIS はエンドポイントまたは SIEM と比較するためサンドボックスフォレンジックを提供します。また、危険な脅威を受信したユーザーには担当者が連絡します。

TRAP では、Proofpoint Threat Intelligence だけでなく、STIX/TAXII フィード、WHOIS、VirusTotal、Soltra、MaxMind などのサードパーティの脅威インテリジェンスも活用します。これらによって「誰が、何を、どこで」攻撃したかを理解でき、イベントを迅速に選別して優先順位付けでき、また単純な繰り返し作業を減らせます。

NIST CSF 要件 RS.AN-5

「プロセスは、内外のソース（例:内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。」

参照:

- CIS CSC VER.7.119
- COBIT 5 DSS02.02
- ISA 62443-2-1:2009 4.3.4.5.6
- ISO/IEC 27001:2013 A.16.1.7
- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
- NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-5, IR-8

本要件に対応する製品:

- Insider Threat Management (ITM)
- Security Awareness Training

アラートは、調査に役立つ情報（通知を含む）および ITM から提供されるコンテキストを含むよう設定できます。

Security Awareness Trainingのフィッシング シミュレーションレポートでは、フィッシングに対する脆弱性の確認に役立つ内部データを提供します。

低減 (RS.MI)

目標:「活動は、イベントの拡大を防ぎ、その影響を緩和し、インシデントを解決するために実施されている。」

NIST CSF 要件 RS.MI-1

「インシデントは、封じ込められている。」

参照:

- CIS CSC VER.7.119
- COBIT 5 APO12.06
- ISA 62443-2-1:2009 4.3.4.5.6
- ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4
- ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
- NIST SP 800-53 Rev. 4 IR-4
- NIST SP 800-53 Rev. 5 IR-4

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Insider Threat Management (ITM)
- TAP
- TRAP

Browser Isolation は分離プラットフォーム上のブラウザで、危険が疑われるコードを封じ込めます。危険な可能性のあるコードの実行はユーザーのコンピューターには到達しません。

CASBは、不審なログイン、不審なアクティビティ、データ漏洩インシデントを自動修復し、またマニュアルでの封じ込めも行います。

Email Protection はゲートウェイで脅威を特定して阻止します。

ITM を用いれば、オペレーターは様々なリスク対応オプションからアクションを選定できます。これらのオプションには、セキュリティチームへアラートを送る、リアルタイムに警告する、アプリケーションを閉じる、セッションからユーザーをログアウトさせる、などがあります。

TAP ではセキュリティ管理者が分析できるよう、悪意のあるメールは隔離環境に送られます。

悪意のあるメールが検知されると、TRAPはメールを分析して悪意のあるメールを自動的に除去します。TRAP はまた、ユーザーの受信箱に届いてしまった後でも、不要なメールを隔離できます。

NIST CSF 要件 RS.MI-2

「インシデントは、緩和されている。」

参照:

- CIS CSC VER.7.14, 19
- COBIT 5 APO12.06
- ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10
- ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
- NIST SP 800-53 Rev. 4 IR-4
- NIST SP 800-53 Rev. 5 IR-4

本要件に対応する製品:

- Browser Isolation
- CASB
- Email Protection
- Insider Threat Management (ITM)
- TAP
- TRAP

Browser Isolation はブラウザセッションが終了された時点でブラウザを破壊します。そして新たにブラウザセッションを始めるときには基礎構成に沿った新しいブラウザを作成します。

CASB では、不審なログイン、不審なアクティビティ、データ漏洩インシデントを自動および手動で対処します。

Email Protection はメールから脅威が検知された場合、そのメールが受信箱に到達することを防止します。オプションのメール暗号化機能を用いれば、機密データの書かれた外部送信メールをポリシーに基づいて自動的に暗号化できます。

ITM を用いれば、オペレーターは様々なリスク対応オプションからアクションを選定できます。これらのオプションには、セキュリティチームへアラートを送る、リアルタイムに警告する、アプリケーションを閉じる、セッションからユーザーをログアウトさせる、などがあります。監査レポートにはデフォルトでアクティビティ、アラート、対応が含まれ、リスク緩和やコンプライアンスの対応に活用できます。

TAP はメールが転送される前に悪意のあるコンテンツを取り除いて隔離します。

TRAP はメールを分析して、悪意のあるメールを自動的に除去します。TRAP はまた、ユーザーの受信箱に届いてしまった後でも、不要なメールを隔離できます。

NIST CSF 要件 RS.MI-3

「新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。」

参照:

- CIS CSC VER.7.14
- COBIT 5 APO12.06
- ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10
- ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
- NIST SP 800-53 Rev. 4 IR-4
- NIST SP 800-53 Rev. 5 IR-4

本要件に対応する製品:

- Insider Threat Management (ITM)
- TAP

ITM には（アラートのアップデートの一環として）新たに発見された脆弱性やソーシャル エンジニアリング パターンがアップデートされます。これらはアラートのアップデートにも活用できます。

TAP は悪意のあるファイルを新たに特定した場合、共有ファイル レピュテーション データベースに追加します。

復旧計画 (RC.RP)

目標:「復旧プロセスおよび手順は、サイバーセキュリティインシデントによる影響を受けたシステムや資産を復旧できるよう実行され、維持されている。」

NIST CSF 要件 RC.RP-1

「復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。」

参照:

- CIS CSC VER.7.1 10
- COBIT 5 APO12.06, DSS02.05, DSS03.04
- ISO/IEC 27001:2013 A.16.1.5
- NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
- NIST SP 800-53 Rev. 5 CP-10, IR-4, IR-8

本要件に対応する製品:

- Insider Threat Management (ITM)

ITM の統合機能 (ServiceDesk など) は、アラートをトリガーにして復旧計画を始動することができます。

クイックリファレンス

以下の表で、プルーフポイント製品が NIST フレームワーク コア機能にどのように当てはまるかを説明します。識別、防御、検知、対応、復旧。

識別

「システム、人、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深める。「識別」機能における対策は、フレームワークを効果的に使用する上で基本となる。組織はビジネスを取り巻く状況、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを理解することで、組織のリスクマネジメント戦略とビジネスニーズに適合するように取り組みの対象を絞って、優先順位付けを行うことが可能になる。「識別」機能の成果カテゴリーには、「資産管理」、「ビジネス環境」、「ガバナンス」、「リスクアセスメント」、「リスクマネジメント戦略」などがある。」

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。	—	—	—	—	○	—	—	—	—
ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。	—	○	—	—	○	—	—	—	—
ID.AM-3: 組織内の通信とデータフロー図が、作成されている。	—	—	—	—	—	—	—	—	—
ID.AM-4: 外部情報システムが、カタログ作成されている。	—	—	—	—	—	—	—	—	—
ID.AM-5: リソース(例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア)が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。	—	—	—	○	○	—	—	—	—
ID.AM-6: 全労働力と利害関係にある第三者(例:サプライヤー、顧客、パートナー)に対してのサイバーセキュリティ上の役割と責任が、定められている。	—	—	—	—	—	—	—	—	—
ID.BE-1: サプライチェーンにおける自組織の役割が、識別され、周知されている。	—	—	—	—	○	○	—	—	—
ID.BE-2: 重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。	—	—	—	—	—	○	—	—	—
ID.BE-3: 組織のミッション、目標、活動の優先順位が、定められ、周知されている。	—	—	—	—	—	○	—	—	—

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
ID.BE-4: 重要サービスを提供する上での依存関係と重要な機能が、定められている。	—	—	—	—	—	—	—	—	—
ID.BE-5: 重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況(例:脅迫・攻撃下、復旧時、通常時等)について定められている。	—	—	—	—	—	—	—	—	—
ID.GV-1: 組織のサイバーセキュリティポリシーが、定められ、周知されている。	—	—	—	—	○	—	—	—	—
ID.GV-2: サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。	—	—	—	—	—	—	—	—	—
ID.GV-3: プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。	—	—	—	○	—	—	—	—	—
ID.GV-4: ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している。	—	—	—	—	—	—	—	—	—
ID.RA-1: 資産の脆弱性が、識別され、文書化されている。	—	—	—	—	—	—	○	—	—
ID.RA-2: サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。	○	○	○	—	—	○	○	○	—
ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。	○	○	○	—	○	○	○	○	—
ID.RA-4: ビジネスに対する潜在的な影響とその発生可能性が、識別されている。	—	○	○	—	○	○	—	○	—
ID.RA-5: 脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。	○	○	○	—	○	○	—	○	○
ID.RA-6: リスク対応が、識別され、優先順位付けされている。	○	○	○	—	○	○	—	○	○
ID.RM-1: リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。	—	—	—	—	—	—	—	—	—
ID.RM-2: 組織のリスク許容度が、決定され、明確に表現されている。	—	—	—	—	○	—	—	—	—

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
ID.RM-3: 自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。	—	—	—	—	—	—	—	—	—
ID.SC-1: サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。	—	—	—	—	—	—	—	—	—
ID.SC-2: 情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。	—	—	—	—	—	—	—	—	—
ID.SC-3: サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。	—	—	—	—	—	—	—	—	—
ID.SC-4: サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。	—	—	—	○	○	—	—	—	—
ID.SC-5: 対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーと共に行なわれている。	—	—	—	—	—	—	—	—	—

防御

「重要サービスの提供を確実にするための適切な保護対策を検討し、実施する。「防御」機能は、発生する可能性のあるサイバーセキュリティイベントがもたらす影響を抑制するのを支援する。「防御」機能の成果カテゴリーには、例えば「アイデンティティ管理とアクセス制御」、「意識向上およびトレーニング」、「データセキュリティ」、「情報を保護するためのプロセス及び手順」、「保守」、「保護技術」などがある。」

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
PR.AC-1: 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。	—	—	—	○	○	—	—	—	—
PR.AC-2: 資産に対する物理アクセスが、管理され、保護されている。	—	—	—	—	—	—	—	—	—
PR.AC-3: リモートアクセスが、管理されている。	—	—	—	—	○	—	—	—	—
PR.AC-4: アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。	—	○	—	—	○	—	—	—	—
PR.AC-5: ネットワークの完全性が、保護されている(例:ネットワークの分離、ネットワークのセグメント化)。	○	—	—	—	—	—	—	—	—
PR.AC-6: IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。	—	—	—	—	○	—	—	—	—
PR.AC-7: ユーザ、デバイス、その他の資産は、トランザクションのリスク(例:個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク)の度合いに応じた認証(例:一要素、多要素)が行われている。	—	○	—	—	○	—	—	—	—
PR.AT-1: すべてのユーザは、情報が周知され、トレーニングが実施されている。	—	—	—	—	○	—	○	—	—
PR.AT-2: 権限を持つユーザが、自身の役割と責任を理解している。	—	—	—	—	○	—	○	—	—
PR.AT-3: 第三者である利害関係者(例:サプライヤー、顧客、パートナー)が、自身の役割と責任を理解している。	—	—	—	—	○	—	○	—	—
PR.AT-4: 上級役員(セキュリティ担当役員)が、自身の役割と責任を理解している。	—	—	—	—	○	—	○	—	—
PR.AT-5: 物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。	—	—	—	—	○	—	○	—	—

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
PR.DS-1: 保存されているデータが、保護されている。	○	○	–	○	○	–	–	–	–
PR.DS-2: 伝送中のデータが、保護されている。	–	○	○	○	○	–	–	–	–
PR.DS-3: 資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。	–	–	–	–	–	–	–	–	–
PR.DS-4: 可用性を確保するのに十分な容量が、維持されている。	–	–	–	○	–	–	–	–	–
PR.DS-5: データ漏えいに対する防御対策が、実装されている。	○	○	–	–	○	–	–	–	–
PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。	–	–	–	○	–	–	–	–	–
PR.DS-7: 開発・テスト環境が、実稼働環境から分離されている。	–	–	–	○	○	–	–	–	–
PR.DS-8: 完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。	–	–	–	–	–	–	–	–	–
PR.IP-1: 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則(例:最低限の機能性の概念)を組み入れて、定められ、維持されている。	○	–	–	–	○	–	–	–	–
PR.IP-2: システムを管理するためのシステム開発ライフサイクルが、実装されている。	–	–	–	–	–	–	–	–	–
PR.IP-3: 構成変更管理プロセスは、策定されている。	–	–	–	–	○	–	–	–	–
PR.IP-4: 情報のバックアップが、実施され、維持され、テストされている。	○	○	○	○	○	–	–	○	○
PR.IP-5: 組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。	–	–	–	–	–	–	–	–	–
PR.IP-6: データは、ポリシーに従って破壊されている。	–	–	–	○	–	–	–	–	–
PR.IP-7: 防御プロセスは、改善されている。	○	–	○	–	–	–	–	–	–
PR.IP-8: 防御技術の有効性に関する情報が、共有されている。	–	–	–	–	–	–	–	–	–

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
PR.IP-9: (インシデント対応および事業継続)対応計画と(インシデントからの復旧および災害復旧)復旧計画が、策定され、管理されている。	—	—	—	—	—	—	—	—	—
PR.IP-10: 対応計画と復旧計画が、テストされている。	—	—	—	—	—	—	—	—	—
PR.IP-11: サイバーセキュリティには、人事に関わるプラクティス(例:アクセス権限の無効化、人員のスクリーニング)が含まれている。	—	—	—	—	—	—	○	—	—
PR.IP-12: 脆弱性管理計画が、作成され、実装されている。	—	—	—	—	—	—	—	—	—
PR.MA-1: 組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。	—	—	—	—	—	—	—	—	—
PR.MA-2: 組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。	—	—	—	—	—	—	—	—	—
PR.PT-1: 監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。	—	○	○	○	○	—	—	○	—
PR.PT-2: リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。	—	—	—	—	○	—	—	—	—
PR.PT-3: 最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。	○	○	○	○	○	—	—	○	—
PR.PT-4: 通信(情報)ネットワークと制御ネットワークが、保護されている。	—	—	—	—	○	—	—	—	—
PR.PT-5: メカニズム(例:フェールセーフ、ロードバランシング、ホットスワップ)が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。	○	○	○	○	○	—	○	○	○

検知

「サイバーセキュリティイベントの発生を識別するのに適した対策を検討し、実施する。「検知」機能はサイバーセキュリティイベントのタイムリーな発見を可能にする。「検知」機能の成果カテゴリーには、例えば「異常とイベント」、「セキュリティの継続的なモニタリング」、「検知プロセス」などがある。」

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
DE.AE-1: ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。	–	○	○	–	○	–	○	–	–
DE.AE-2: 検知したイベントは、攻撃の標的と手法を理解するために分析されている。	–	○	○	–	○	○	○	○	–
DE.AE-3: イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。	–	–	○	○	○	○	○	○	–
DE.AE-4: イベントがもたらす影響が、判断されている。	–	–	○	–	○	○	–	○	–
DE.AE-5: インシデント警告の閾値が、定められている。	–	○	○	○	○	–	–	○	–
DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	○	○	○	–	○	–	–	○	–
DE.CM-2: 物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	–	–	–	–	○	–	–	–	–
DE.CM-3: 人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	○	○	○	–	○	–	○	○	–
DE.CM-4: 悪質なコードは、検知されている。	○	○	○	–	–	–	–	○	–
DE.CM-5: 不正なモバイルコードは、検知されている。	–	○	○	–	–	–	–	○	–
DE.CM-6: 外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。	–	–	–	–	○	–	–	–	–
DE.CM-7: 権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。	–	–	○	–	○	–	–	–	–

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
DE.CM-8: 弱性スキャンが、実施されている。	—	—	—	—	—	—	○	○	—
DE.DP-1:　検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。	—	—	—	—	—	—	—	—	—
DE.DP-2:　検知活動は、該当するすべての要求事項を準拠している。	○	○	○	○	○	○	○	○	○
DE.DP-3: 検知プロセスが、テストされている。	—	○	○	○	○	—	○	—	—
DE.DP-4: イベント検知情報が、周知されている。	○	○	○	○	○	—	—	○	—
DE.DP-5: 検知プロセスが、継続的に改善されている。	—	○	○	○	○	—	—	○	—

対応

「検知されたサイバーセキュリティインシデントに対処するための適切な対策を検討し、実施する。「対応」機能は、発生する可能性のあるサイバーセキュリティインシデントがもたらす影響を封じ込めるのを支援する。「対応」機能の成果カテゴリーには、例えば「対応計画の作成」、「コミュニケーション」、「分析」、「低減」、「改善」などがある。

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
RS.RP-1: 対応計画が、インシデントの発生中または発生後に実行されている。	—	—	—	—	—	—	—	—	—
RS.CO-1: 人員は、対応が必要になった時の自身の役割と行動の順序を認識している。	—	—	—	—	—	—	—	—	—
RS.CO-2: インシデントが、定められた基準に沿って報告されている。	—	—	—	—	—	—	—	—	—
RS.CO-3: 対応計画に従って、情報が共有されている	—	—	—	—	—	—	—	—	—
RS.CO-4: 利害関係者との間で調整が、対応計画に従って行なわれている。	—	—	—	—	—	—	—	—	—
RS.CO-5: サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。	—	—	—	—	—	—	—	—	—
RS.AN-1: 検知システムからの通知は、調査されている。	—	○	○	—	○	—	—	○	○
RS.AN-2: インシデントがもたらす影響は、把握されている。	—	○	○	—	○	—	—	○	○
RS.AN-3: フォレンジックが、実施されている。	—	—	○	○	○	○	—	○	○
RS.AN-4: インシデントは、対応計画に従って分類されている。	—	○	○	—	○	○	—	○	○
RS.AN-5: プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。	—	—	—	—	○	—	○	—	—
RS.MI-1: インシデントは、封じ込められている。	○	○	○	—	○	—	—	○	○
RS.MI-2: インシデントは、緩和されている。	○	○	○	—	○	—	—	○	○
RS.MI-3: 新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。	—	—	—	—	○	—	—	○	—
RS.IM-1: 対応計画は、学んだ教訓を取り入れられている。	—	—	—	—	—	—	—	—	—
RS.IM-2: 対応戦略は、更新されている。	—	—	—	—	—	—	—	—	—

復旧

「レジリエンスを実現させるための計画を策定・維持し、サイバーセキュリティインシデントによって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施する。「復旧」機能は、サイバーセキュリティインシデントがもたらす影響を軽減するために、通常の運用状態へタイムリーに復旧するのを支援する。「復旧」機能の成果カテゴリーには、「復旧計画の作成」、「改善」、「コミュニケーション」などがある。」

サブカテゴリ	BROWSER ISOLATION	CASB	EMAIL PROTECTION	ENTERPRISE ARCHIVE	INSIDER THREAT	PTIS	SECURITY AWARENESS TRAINING	TAP	TRAP
RC.RP-1: 復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。	—	—	—	—	○	—	—	—	—
RC.IM-1: 復旧計画は、学んだ教訓を取り入れている。	—	—	—	—	—	—	—	—	—
RC.IM-2: 復旧戦略は、更新されている。	—	—	—	—	—	—	—	—	—
RC.CO-1: 広報活動が、管理されている。	—	—	—	—	—	—	—	—	—
RC.CO-2: 評判は、インシデント発生後に回復されている。	—	—	—	—	—	—	—	—	—
RC.CO-3: 復旧活動は、内外の利害関係者だけでなく役員と経営陣にも周知されている。	—	—	—	—	—	—	—	—	—

詳細

プルーフポイントは NIST サイバーセキュリティ フレームワークへの準拠をサポートします。
詳細は proofpoint.com/jpでご覧ください。

プルーフポイントについて

Proofpoint, Inc.(NASDAQ:PFPT)は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点をあてています。Proofpointは、クラウドベースの統合ソリューションによって、世界中の企業が標的型攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を 持てるよう支援しています。また、Fortune 1000の過半数を超える企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web関連のセキュ リティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は www.proofpoint.com/jp にてご確認ください。