CSS MDRサービスのご紹介

V70

株式会社セントラルソフトサービス

会社概要　1/2

株式会社セントラルソフトサービス

設立　　1979年5月15日
本社所在　　愛知県岡崎市明大寺町字河原25-1
名古屋オフィス　愛知県名古屋市中村区名駅1-1-1
　　JPタワー名古屋21階 2117号室
静岡オフィス　　静岡県静岡市葵区紺屋町17-1葵タワー1F
資本金　　5,000万円
年商　　6.1億円
代表者　　代表取締役社長　清川高史
社員数　　27名
日本IBM Gold Partner
サイボーズ公式パートナー

主要取引先：
愛知県庁
朝日インテック株式会社
岡崎市役所
岡谷システム株式会社
春日井市役所
カリモク皆栄株式会社
蒲郡市役所
静岡県庁
名古屋市役所　等

取扱品

IBM Cloud
HCL BigFix
Box
CrowdStrike
Cybozu kintone
WithSecure

JQA-IM1695　JQA-IC0044

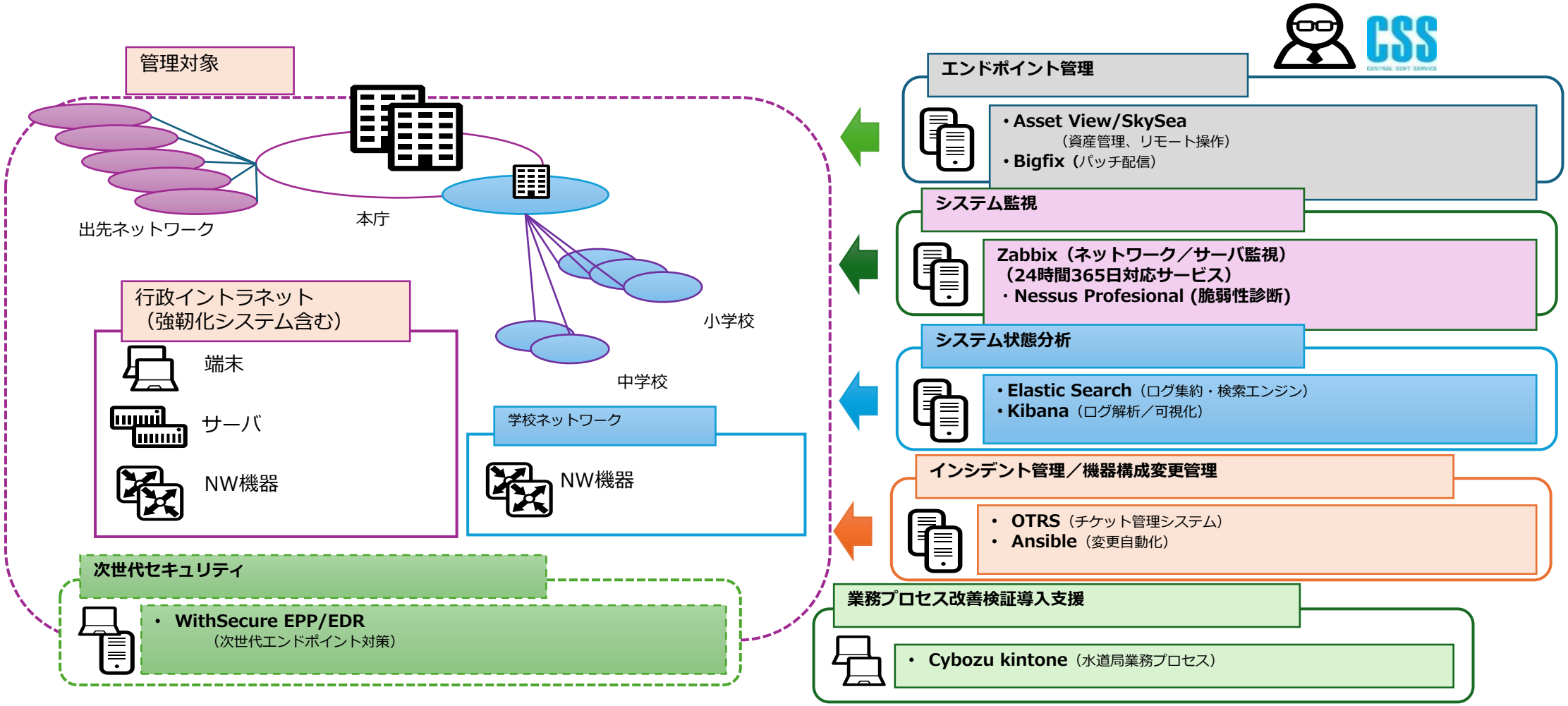
Japan Special Award 2024

ISO/IEC27001
ISO/IEC27017
経済産業省 情報セキュリティサービス審査登録制度適合事業者
(https://www.ipa.go.jp/security/ug65p90000019fc0-att/20241219_4.pdf)
CrowdStrike認定パートナー

会社概要　2/2

提供しているサービス

- エンドポイント／サーバ／ネットワーク機器にいたるまでのあらゆる情報機器を一括管理
- ヘルプデスクからインシデント管理／変更管理／問題管理／パフォーマンス管理／セキュリティ等包括的な運用サービスを提供



ランサムウエアの侵攻パターン

戦術	概要
初期アクセス(Initial Access)	攻撃者がネットワークに侵入しようとしている。
実行(Execution)	攻撃者が悪意のあるコードを実行しようとしている。
永続化(Persistence)	攻撃者が不正アクセスする環境を確保しようとしている。
権限昇格(Privilege Escalation)	攻撃者がより高いレベルの権限を取得しようとしている。
防衛回避(Defense Evasion)	攻撃者が検知されないようにしようとしている。
認証情報アクセス(Credential Access)	攻撃者がアカウント名とパスワードを盗もうとしている。
探索(Discovery)	攻撃者がアクセス先の環境を理解しようとしている。
水平展開(Lateral Movement)	攻撃者がアクセス先の環境を移動しようとしている。
収集(Collection)	攻撃者が目標に関心のあるデータを収集しようとしている。
C&C（Command and Control）	攻撃者が侵害されたシステムと通信して制御しようとしている。
持ち出し(Exfiltration)	攻撃者がデータを盗もうとしている。
影響(Impact)	攻撃者がシステムとデータを操作、中断、または破壊しようとしている。

ランサム被害が進行しています

https://www.security-next.com/158090

ランサム被害が発生、個人情報流出の可能性も - 情報処理会社

金融機関や公共機関向けに情報処理サービスを提供しているイセトーは、サイバー攻撃を受け、ランサムウェアによる被害が発生したことを明らかにした。

同社によれば、5月26日に一部サーバやパソコン内のデータをランサムウェアによって暗号化される被害を確認したもの。

外部における情報の流通などは確認されていないが、一部取引先に関しては、個人情報が流出した可能性があることが判明し、報告を行ったという。

同社では内部ネットワークや感染が疑われるサーバ、端末を停止。外部協力のもと、引き続き調査や復旧に向けた対応を進めている。

（Security NEXT - 2024/06/07 ）

顧客の個人情報の漏洩となる

パナソニック健康保険組合	13,150名
公文教育研究会	4,678名
クボタクレジット	61,424件
豊田市	約42万人
京都商工会議所	41,819件
徳島県	132,503名
和歌山市	151,421件
・	
・	

豊田市の漏洩情報内容
市県民税、軽自動車税、固定資産税、都市計画税、国民健康保険税などの納税通知書のほか、市営住宅使用料の納付通知書、介護保険料納入通知書、後期高齢者医療保険料納入通知書、新型コロナ予防接種券、非課税世帯等給付金確認書、子育て世帯臨時特別給付金申請書などが漏洩

氏名、住所、税額、生年月日、保険料、口座情報などの情報が含まれる。

海外の地方自治体のランサムウエアによる被害の事例

ChatGPTに聞いてみました

海外の自治体事例は件数が多いので、代表的なものを、被害内容・影響・復旧/費用が分かる形で絞って整理します。

年	自治体	国	概要	主な影響	
2018	アトランタ市	米国	SamSam ランサムウェア被害。身代金要求は約5万ドル規模だったが、復旧対応費が大きく膨らんだ事例	市民サービス、裁判所、警察関連システムなどに影響。復旧費用は数百万ドル規模と報道	
2019	ボルチモア市	米国	RobbinHood ランサムウェア被害。市の多くのシステムが停止	不動産取引、料金支払い、メール、各種行政システムに影響。復旧コストは約1,800万ドル規模と報道 CBS News	約28億円
2023	ダラス市	米国	Royal ランサムウェア被害。攻撃者は暗号化前に約1か月ネットワーク内に潜伏していたとされる	市議会は復旧・封じ込め・復元対応に850万ドルの予算を承認 ダラス市役所 +1	約16億円
2023	オークランド市	米国	ランサムウェア被害により市が非常事態宣言	市のネットワーク停止、行政サービスに影響。非常事態宣言を出すレベルの混乱 インフォセキュリティマガジン +1	
2024	レスター市議会	英国	ランサムウェアグループによる攻撃。市議会は2024年3月7日にITネットワークを停止	電話・ITシステム停止。盗まれたデータが公開され、機密文書漏えいも確認 レスター市ニュース +1	
2025	セントポール市	米国	市の重要バックアップサーバー関連アカウントの不審活動を検知。市はシステムを隔離し、外部IRベンダーを起用	市のオンラインサービスや庁内システムに影響。州兵のサイバー部隊支援まで動員された事例 Saint Paul Minnesota +1	

サプライチェーンのセキュリティー対策　業界団体や経産省の動き

日本自動車工業会(JAMA)、日本自動車部品工業会(JAPIA)が、共同でセキュリティガイドラインを2022年3月にV2を策定

サプライチェーンの保護に動く

自工会/部工会・サイバーセキュリティガイドラインV2.3の公開について

自動車産業界はCASE(Connected、Autonomous、Shared & Services、Electric)に代表されるように100年に一度の技術的大変革期を迎えており、業界全体がモビリティ社会の実現に向けてITの利活用を推進しています。
そして次世代のモビリティビジネスへの構造変化に伴い、サプライヤーは拡大し、取り扱う機密情報のデータ量も増加傾向にあります。
また、自社内環境だけでなくサプライチェーンを狙ったサイバー攻撃も増加しており、自動車産業界を取り巻くサイバーセキュリティリスクは深刻化しています。

このような環境の中で安全・安心で豊かなモビリティ社会と自動車産業界の持続可能な発展を実現するためには、業界を取り巻くサイバーセキュリティリスクを正確に理解しながら業界全体でサイバーセキュリティリスクに適切な対処を行うことが必要不可欠です。

そのため、自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業界固有のサイバーセキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業界全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的として、JAMA（一般社団法人日本自動車工業会）、JAPIA（弊会・サイバーセキュリティ部会）が協業して共同でセキュリティガイドライン（対策項目、基準）を2020年3月31日に初版を策定しました。

その後、初版で策定した項目に加え、更なるレベルアップ項目を追加したセキュリティガイドライン（v2.0）を2022年3月31日に改訂しました。

また、自己評価結果の提出方法のシステム化に伴う入力項目追加と誤記修正を実施したセキュリティガイドライン（v2.1）を2023年9月1日に改訂しました。（最新版はv2.3）

以下の自工会様のサイトで公開されておりますので、是非、ダウンロードのうえご確認下さい。

https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

セキュリティー対応状況の可視化

経済産業省は、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業のセキュリティ対策を提示しつつ、その対策状況を可視化する仕組みの構築に向けた検討を進め、本日、現時点での検討の概要を「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」として公表しました。
今後、2026年度の制度開始を目指し、実証事業や制度運営基盤の整備、利用促進に向けた各種施策の実行等を進めていく予定です。

https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

情報システム等の適切な管理、管理区域の適切な管理、電気通信回線の適切な管理、職員の利用する通信端末機器及び電磁的記録媒体の適切な管理その他の物理的なサイバーセキュリティに関する対策の適切な実施

職員の遵守事項の遵守等のための適切な措置の実施、研修及び訓練の実施、サイバーセキュリティに関するインシデントの報告、不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号の適切な管理その他の人的なサイバーセキュリティに関する対策の適切な実施

情報資産の適切な管理、不正アクセス行為の禁止等に関する法律第二条第三項に規定するアクセス制御機能の適切な整備、同法同条第四項に規定する不正アクセス行為を防止するための適切な対策の実施、刑法（明治四十年法律第四十五号）第百六十八条の二第一項各号に掲げる電磁的記録その他の記録を通じた電子計算機に対する不正な活動による被害の防止のための適切な対策の実施、情報システム等の開発、導入及び保守の適切な実施、サイバーセキュリティに関する情報の収集その他の技術的なサイバーセキュリティに関する対策の適切な実施

情報システムに対する監視の適切な実施、サイバーセキュリティに関する方針等のサイバーセキュリティに関する規程の遵守状況の確認、情報資産に対するサイバーセキュリティに関するインシデントへの適切な対応その他のサイバーセキュリティに関する対策の適切な運用の実施

適切な業務委託（情報システム等に関するものを含む。）の実施及びインターネットその他の高度情報通信ネットワークを通じて電子計算機を他人の情報処理の用に供する役務の適切な利用

監査及び自己点検の実施、サイバーセキュリティに関する方針等のサイバーセキュリティに関する規程の見直しその他のサイバーセキュリティに関する対策の適切な評価及び見直しの実施

ランサムウェア対策 ～ EDRの導入(従来のセキュリティ対策の限界)

- ランサムウェア対策として、最近注目を浴びているのがEDR(Endpoint Detection and Response)です。
- 近年、ランサムウェアの攻撃が巧妙化し、これまでのアンチウイルス製品のような対策では対処しきれなくなっています。

ファイルレス攻撃の常態化

- 一般的なWindowsコマンド(PowerShell*など)を悪用しての侵入行為を行う「ファイルレス攻撃」が、猛威を奮っている
- PowerShellは正規ソフトウェアのため、従来のマルウェア*対策製品では検知することが難しい
- 攻撃の77%がファイルレス攻撃といわれており、エンドポイントの対策が急務

ネットワーク型セキュリティ製品の効果低下

- Web全通信の95%以上がSSL*通信で暗号化されている(2025年2月時点 日本)
- ゲートウェイ型*のサンドボックス*もSSL復号をしないと分析ができない
- ウィルスファイルも「パスワード設定」されてメールに添付される攻撃が常態化している

エンドポイントで攻撃の“ふるまい”自体を検知・防御するEDRへの移行が必須

CSS MDRサービスの概要

ご提供するサービスの構成

CSS MDRサービスにて以下の内容を一本化してご提供します

脆弱性診断
- Total　年2回
- Internetからアクセスが可能な機器Daily

日本語ポータルの提供

24/365の
運用代行

チューニング

隔離・復旧

脅威ハンティング

WithSecure Elements EPP/EDRライセンス

年間利用料金に全て込み込みでのご提供となります

WithSecure（旧エフセキュア）について

✓エフセキュアから社名を変更
✓1988年創業、本社フィンランド
✓世界中で100,000を超える法人顧客と数千万の個人顧客

総合セキュリティベンダー

アンチウイルス製品
・クラウド型
・Windows、Mac、PC
・Winサーバ、Linuxサーバ

次世代型/異常動作の検知
・EDR

クラウドセキュリティ
・CPSM
クラウドコラボレーション保護
・セールスフォース
・MS Office 365

- **法人展開:** 世界29地域
- **ビジネス展開:** 100ヵ国以上
- **オペレータ数:** 200以上
- **リセラー数:** 1000以上
- **法人顧客数:** 世界10万社以上
- **欧州のサイバー犯罪における調査機関として最多の依頼数**
- **厳格なセキュリティ条件下でのコンサルティングサービス**

英銀行トップ 5/5 行

米銀行トップ 3/5 行

北欧銀行トップ 5/5 行

航空、電力、船舶

ドイツ4大自動車メーカー

セキュリティコンサルティング
・Web
・ITプラットフォーム
・アプリケーション
・自動車
・航空機/管制
・組み込み系

1.34
億ユーロの売上

40+
Fortune500企業のユーザ

35
年以上に渡る経験

72
ヶ国からの社員

毎月のランサムウエアの検知数
250万

毎月のソフトウエアの更新
150万

日本での実績
700以上の公共機関
（中央省庁/地方自治体）

特徴的な機能　ランサム被害からのロールバック機能

暗号化されたファイルやレジストリーの更新を復元

WithSecure
セキュリティクラウド

1. ユーザーがアプリケーションを起動すると、Elements EPP はまずアプリケーションが Security Cloud によって認識されているかどうかを確認します。

オプション 1:アプリケーションが既知であり、有害であると考えられる場合は、すぐにブロックされます。

オプション 2:アプリケーションが既知であり、安全であるとみなされる場合は、起動が許可され、アクティビティ監視は開始されません。

オプション 3: アプリケーションが Security Cloud に知られていない場合、または有害または安全であると評価されていない場合、アクティビティ監視が開始されます。

2 . アプリケーションは正常に実行され、Elements EPP も通常どおりに動作しますが、アクティビティ モニターがファイル システムとレジストリに対するすべての変更を追跡している点が異なります。

アプリケーションが EPP が有害とみなすアクションを実行した場合:

1. アプリケーションはデバイス上で終了します。
2. アプリケーションによってファイル システムに加えられた変更はすべてロールバックされ、元のコンテンツが復元されます。
3. Windows レジストリへの変更もロールバックされます。
4. データは隔離にも保存されるため、誤検知の場合でも変更を復元できます。

13

脆弱性診断を無償提供（年2回/台数制限なし）

EDR運用サービスをご提供しているお客様にIT資産の脆弱性診断を提供します。

■ 基本サービス
① ネットワーク脆弱性診断の実施
② 診断レポートの提供

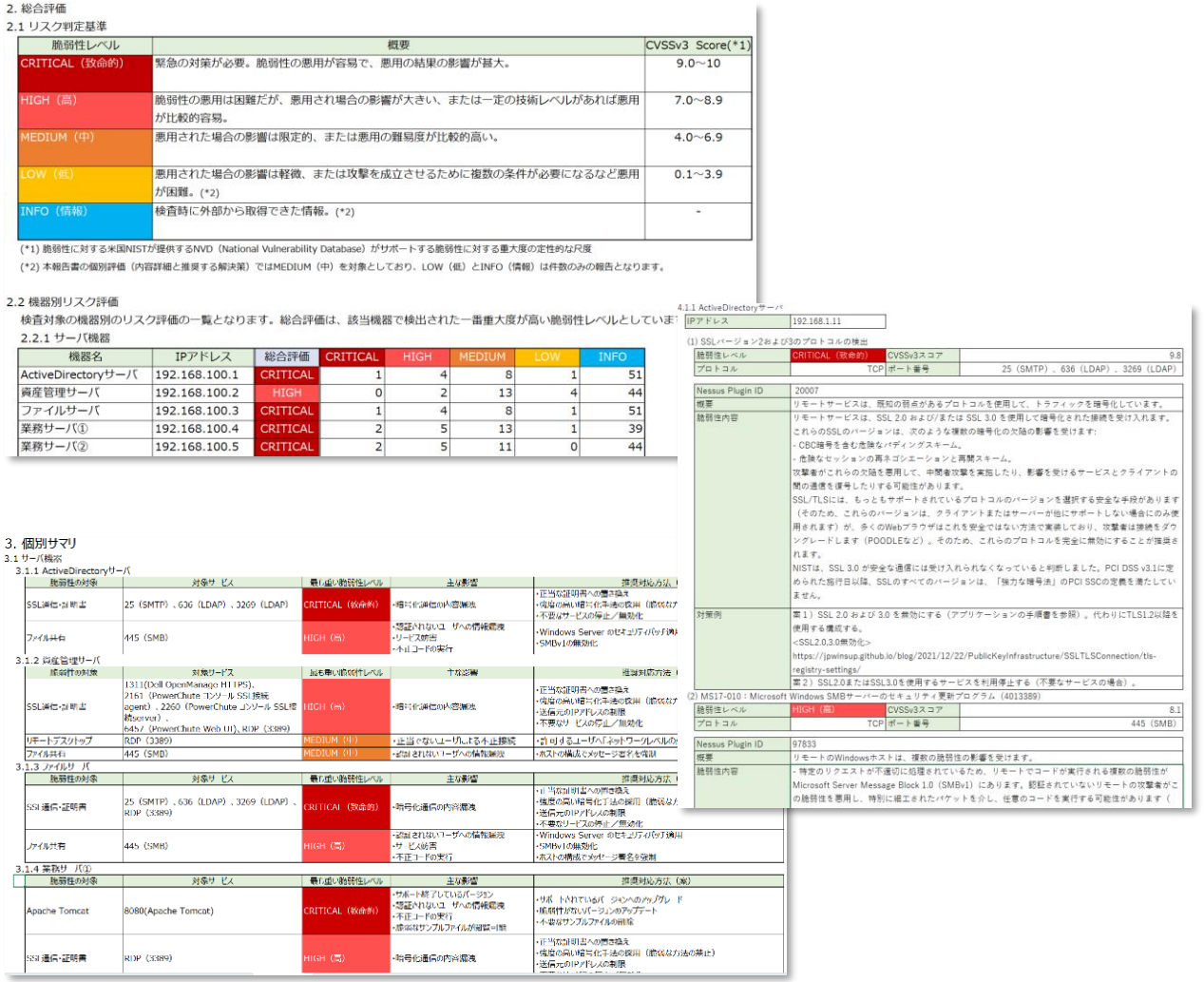
＜診断対象＞
サーバ、ネットワーク機器、NAS装置などアプライアンス機器

＜診断内容＞
デバイスおよびアプリケーションにおけるソフトウェアの
弱点、パッチの不足、構成ミスを網羅的に診断

＜診断方法＞
インターネット側からの診断
社内ネットワーク側からの診断

＜診断レポート＞
総合評価
機器別評価
機器別脆弱性詳細
重大な脆弱性に対する推奨対応策の提示

※診断レポートは、実機への検査を実施後、約１ヵ月後に提供



2. 総合評価
2.1 リスク判定基準

脆弱性レベル	概要	CVSSv3 Score(*1)
CRITICAL（致命的）	緊急の対策が必要。脆弱性の悪用が容易で、悪用の結果の影響が甚大。	9.0～10
HIGH（高）	脆弱性の悪用は困難だが、悪用され場合の影響が大きい、または一定の技術レベルがあれば悪用が比較的容易。	7.0～8.9
MEDIUM（中）	悪用された場合の影響は限定的、または悪用の難易度が比較的高い。	4.0～6.9
LOW（低）	悪用された場合の影響は軽微、または攻撃を成立させるために複数の条件が必要になるなど悪用が困難。(*2)	0.1～3.9
INFO（情報）	検査時に外部から取得できた情報。(*2)	-

(*1) 脆弱性に対する米国NISTが提供するNVD（National Vulnerability Database）がサポートする脆弱性に対する重大度の定性的な尺度
(*2) 本報告書の個別評価（内容詳細と推奨する解決策）ではMEDIUM（中）を対象としており、LOW（低）とINFO（情報）は件数のみの報告となります。

2.2 機器別リスク評価
検査対象の機器別のリスク評価の一覧となります。総合評価は、該当機器で検出された一番重大度が高い脆弱性レベルとしています
2.2.1 サーバ機器

機器名	IPアドレス	総合評価	CRITICAL	HIGH	MEDIUM	LOW	INFO
ActiveDirectoryサーバ	192.168.100.1	CRITICAL	1	4	8	1	51
資産管理サーバ	192.168.100.2	HIGH	0	2	13	4	44
ファイルサーバ	192.168.100.3	CRITICAL	1	4	8	1	51
業務サーバ①	192.168.100.4	CRITICAL	2	5	13	1	39
業務サーバ②	192.168.100.5	CRITICAL	2	5	11	0	44

3. 個別サマリ
3.1 サーバ機器
3.1.1 ActiveDirectoryサーバ

脆弱性の対象	対象サービス	最も重い脆弱性レベル	主な影響	推奨対応方法
SSL通信・証明書	25（SMTP）、636（LDAP）、3269（LDAP）	CRITICAL（致命的）	・暗号化通信の内容漏洩	・正当な証明書への置き換え ・強度の高い暗号化手法の採用（脆弱な方 ・不要なサービスの停止／無効化
ファイル共有	445（SMB）	HIGH（高）	・認証されないユーザへの情報漏洩 ・サービス断念 ・不正コードの実行	・Windows Server のセキュリティパッチ適 ・SMBv1の無効化

3.1.2 資産管理サーバ

脆弱性の対象	対象サービス	最も重い脆弱性レベル	主な影響	推奨対応方法
SSL通信・証明書	1311(Dell OpenManage HTTPS)、2161（PowerChute コンソール SSL接続 agent）、2260（PowerChute コンソール SSL接続server）、6457（PowerChute Web UI）、RDP（3389）	HIGH（高）	・暗号化通信の内容漏洩	・正当な証明書への置き換え ・強度の高い暗号化手法の採用（脆弱な方 ・送信元のIPアドレスの制限 ・不要なサービスの停止／無効化
リモートデスクトップ	RDP（3389）	MEDIUM（中）	・正当でないユーザによる不正接続	・許可するユーザへ「ネットワークレベルの
ファイル共有	445（SMB）	MEDIUM（中）	・認証されないユーザへの情報漏洩	・ホストの構成でメッセージ署名を強制

3.1.3 ファイルサーバ

脆弱性の対象	対象サービス	最も重い脆弱性レベル	主な影響	推奨対応方法
SSL通信・証明書	25（SMTP）、636（LDAP）、3269（LDAP）、RDP（3389）	CRITICAL（致命的）	・暗号化通信の内容漏洩	・正当な証明書への置き換え ・強度の高い暗号化手法の採用（脆弱な方 ・送信元のIPアドレスの制限 ・不要なサービスの停止／無効化
ファイル共有	445（SMB）	HIGH（高）	・認証されないユーザへの情報漏洩 ・サービス断念 ・不正コードの実行	・Windows Server のセキュリティパッチ適用 ・SMBv1の無効化 ・ホストの構成でメッセージ署名を強制

3.1.4 業務サーバ①

脆弱性の対象	対象サービス	最も重い脆弱性レベル	主な影響	推奨対応方法（案）
Apache Tomcat	8080(Apache Tomcat)	CRITICAL（致命的）	・サポート終了しているバージョン ・認証されないユーザへの情報漏洩 ・不正コードの実行 ・脆弱なサンプルファイルが確認=脆	・サポートされているバージョンへのアップグレード ・脆弱性がないバージョンのアップデート ・不要なサンプルファイルの削除
SSL通信・証明書	RDP（3389）	HIGH（高）	・暗号化通信の内容漏洩	・正当な証明書への置き換え ・強度の高い暗号化手法の採用（脆弱な方法の禁止） ・送信元のIPアドレスの制限

4.1.1 ActiveDirectoryサーバ

IPアドレス	192.168.1.11

(1) SSLバージョン2および3のプロトコルの検出

脆弱性レベル	CRITICAL（致命的）	CVSSv3スコア	9.8
プロトコル	TCP	ポート番号	25（SMTP）、636（LDAP）、3269（LDAP）

Nessus Plugin ID	20007
概要	リモートサービスは、既知の弱点があるプロトコルを使用して、トラフィックを暗号化しています。
脆弱性内容	リモートサービスは、SSL 2.0 および/または SSL 3.0 を使用して暗号化された接続を受け入れます。 これらのSSLのバージョンは、次のような複数の暗号化の欠陥の影響を受けます: - CBC暗号を含む危険なパディングスキーム。 - 危険なセッションの再ネゴシエーションと再開スキーム。 攻撃者がこれらの欠陥を悪用して、中間者攻撃を実施したり、影響を受けるサービスとクライアントの間の通信を復号したりする可能性があります。 SSL/TLSには、もっともサポートされているプロトコルのバージョンを選択する安全な手段があります（そのため、これらのバージョンは、クライアントまたはサーバーが他にサポートしない場合にのみ使用されます）が、多くのWebブラウザはこれを安全ではない方法で実装しており、攻撃者は接続をダウングレードします（POODLEなど）。そのため、これらのプロトコルを完全に無効にすることが推奨されます。 NISTは、SSL 3.0 が安全な通信には受け入れられなくなっていると判断しました。PCI DSS v3.1に定められた施行日以降、SSLのすべてのバージョンは、「強力な暗号法」のPCI SSCの定義を満たしていません。
対策例	要1）SSL 2.0 および 3.0 を無効にする（アプリケーションの手順書を参照）。代わりにTLS1.2以降を使用する構成する。 <SSL2.0,3.0無効化> https://jpwinsup.github.io/blog/2021/12/22/PublicKeyInfrastructure/SSLTLSConnection/tls-registry-settings/ 要2）SSL2.0またはSSL3.0を使用するサービスを利用停止する（不要なサービスの場合）。

(2) MS17-010：Microsoft Windows SMBサーバーのセキュリティ更新プログラム（4013389）

脆弱性レベル	HIGH（高）	CVSSv3スコア	8.1
プロトコル	TCP	ポート番号	445（SMB）

Nessus Plugin ID	97833
概要	リモートのWindowsホストは、複数の脆弱性の影響を受けます。
脆弱性内容	- 特定のリクエストが不適切に処理されているため、リモートでコードが実行される複数の脆弱性がMicrosoft Server Message Block 1.0（SMBv1）にあります。認証されていないリモートの攻撃者がこの脆弱性を悪用し、特別に細工されたパケットを介し、任意のコードを実行する可能性があります（

Internetからアクセス可能な機器に対して Daily/Monthlyに脆弱性のチェックを実施

問題があった場合　チケット管理システムよりメールにてご案内いたします。

対象機器　(サポート対象機器か個別に確認いたします)
・ネットワーク機器
　FortiGate，Ivanti，SonicWall，Cisco，F5，Juniper，Palo Alto
　CheckPoint，FireEye，Sophos
・Web Server

攻撃対象領域対策として以下のチェックを実施します （月報に含みます）

-グローバルアドレス一覧と使用ポート一覧
-メール向けDNS設定の評価
-お客様グローバルアドレスのリピュテーション
-パッチ適用状況の報告

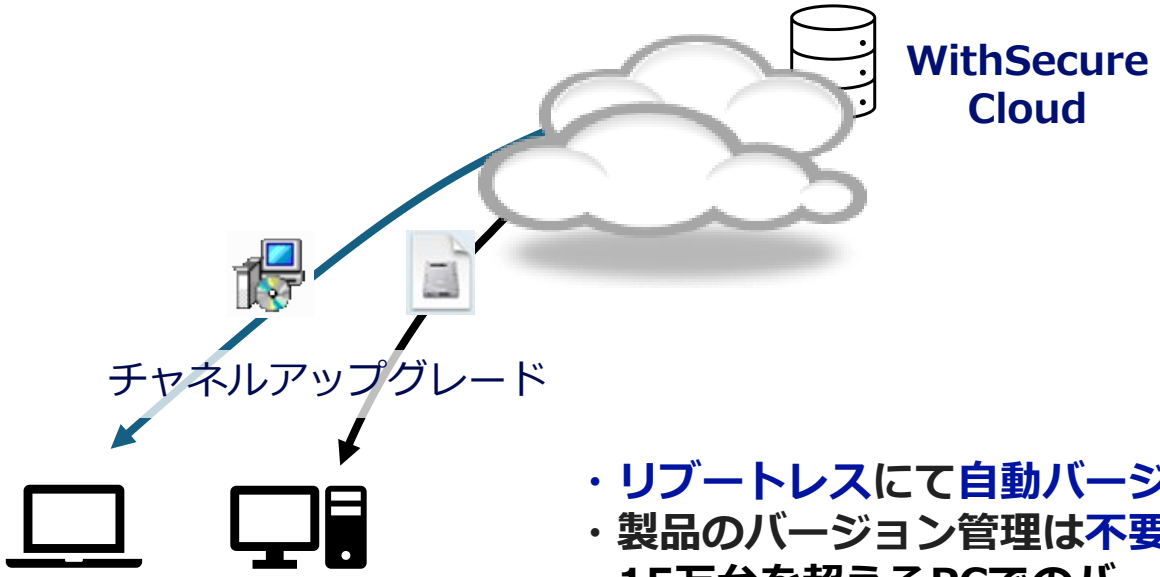
WithSecure機能概要

WithSecure機能概要 エージェントの再起動無しでの自動更新

バージョンアップに伴う工数はゼロ

QRadarEDRは、コンソールからのキックが必要

新バージョンのプログラムが**自動で配信！**



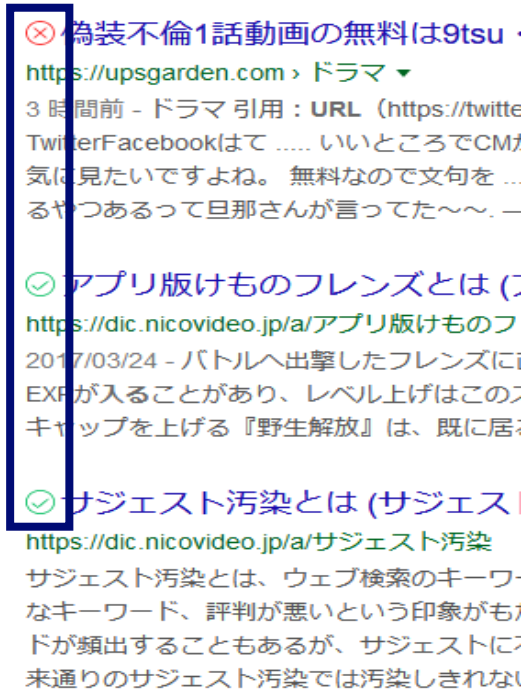
- **リブートレス**にて**自動バージョンアップ**
- 製品のバージョン管理は**不要**
- 15万台を超えるPCでのバージョンアップ実施の実績

WithSecure機能概要 ブラウザー保護機能

HTTP/HTTPSのURLサイトの安全性評価を**「安全」「危険」「不審」「禁止」**の４つ段階で振り分ける。

各WEBブラウザソフトの検索結果でもアイコンで表示可能。

＊HTTPSのWEBサーバとの通信は暗号化されている為、URLフィルタリングはWEBブラウザを用いた対策が有効



危険：
有害なサイトへのアクセスをブロックします 。
(サイトにマルウェアが含まれている場合など)

不審：
疑わしいコンテンツを含むサイトへのアクセスをブロックします
(サイトが偽のサイトまたはスパム サイトである可能性がある場合など)。

禁止：
侵害コンテンツまたは禁止コンテンツを含むサイトへのアクセスをブロックします
(不正なコンテンツを含むサイトなど)。

WithSecure機能概要 デバイス制御機能

大容量記憶装置、USB カメラ、プリンタなどの USB デバイスへのアクセス制限を設定できます。
特定USBデバイスのみの使用許可やUSB ストレージ デバイスへの書き込みのみを禁止なども設定可能。
実行中の実行ファイルを禁止したり、デバイス グループに基づいて制限を設定することができます。

対象デバイス
- **USBストレージデバイス**
- カードリーダ
- CD/DVD/FDドライブ
- プリンター
- **カメラ・スキャナー（画像デバイス）**
- **Bluetooth**
- 無線デバイス
- COM(シリアルポート)、LPT(パラレルポート)

WithSecure機能概要 パッチ適用状況のリポート

MSのOS・Office,その他のAPLのSecurityパッチの適用状況を
確認するためのバッチプログラムを提供します

アウトプットイメージ

デバイス名	ベンダ名	ソフトウェア名	パッチ名	現行バージョン	アップデートバージョン	カテゴリ	重大度
PC1	Microsoft Corporation	Microsoft Teams classic	Microsoft Teams 1.7.00.33761	1.5.00.17656	1.7.00.33761	security	important
PC1	Google Inc.	Google Chrome	Google Chrome 132.0.6834.84	131.0.6778.265	132.0.6834.84	security	important
PC1	Zoom Video Communications, Inc.	Zoom	Zoom 6.3.6	6.2.7	6.3.6	nonSecurity	unclassified
PC1	Microsoft Corporation	Microsoft Visual C++ Redistributable 2012 (x86)	Microsoft Visual C++ Redistributable 2012 11.0.61030.0	11.0.60610.1	11.0.61030.0	nonSecurity	unclassified
PC1	Microsoft Corporation	Microsoft Visual C++ Redistributable 2012 (x64)	Microsoft Visual C++ Redistributable 2012 11.0.61030.0	11.0.60610.1	11.0.61030.0	nonSecurity	unclassified
PC1	Microsoft Corporation	Microsoft Visual C++ 2015-2019 Redistributable (x86)	Microsoft Visual C++ Redistributable 14.42.34433.0	14.27.29112.0	14.42.34433.0	nonSecurity	unclassified
PC1	Microsoft Corporation	Microsoft Visual C++ 2015-2019 Redistributable (x64)	Microsoft Visual C++ Redistributable 14.42.34433.0	14.27.29112.0	14.42.34433.0	nonSecurity	unclassified
PC1	Microsoft Corporation	Microsoft Teams (work or school)	Microsoft Teams 24335.208.3315.1951	24295.605.3225.8804	24335.208.3315.1951	nonSecurity	unclassified
PC2	Google Inc.	Google Chrome	Google Chrome 132.0.6834.84	131.0.6778.265	132.0.6834.84	security	important
PC2	Zoom Video Communications, Inc.	Zoom	Zoom 6.3.6	6.2.7	6.3.6	nonSecurity	unclassified
PC2	Microsoft Corporation	Microsoft Visual C++ Redistributable 2012 (x86)	Microsoft Visual C++ Redistributable 2012 11.0.61030.0	11.0.60610.1	11.0.61030.0	nonSecurity	unclassified
PC2	Microsoft Corporation	Microsoft Visual C++ Redistributable 2012 (x64)	Microsoft Visual C++ Redistributable 2012 11.0.61030.0	11.0.60610.1	11.0.61030.0	nonSecurity	unclassified
PC2	Microsoft Corporation	Microsoft Visual C++ 2015-2019 Redistributable (x86)	Microsoft Visual C++ Redistributable 14.42.34433.0	14.27.29112.0	14.42.34433.0	nonSecurity	unclassified
PC2	Microsoft Corporation	Microsoft Visual C++ 2015-2019 Redistributable (x64)	Microsoft Visual C++ Redistributable 14.42.34433.0	14.27.29112.0	14.42.34433.0	nonSecurity	unclassified
PC2	Microsoft Corporation	Microsoft Teams (work or school)	Microsoft Teams 24335.208.3315.1951	24295.605.3225.8804	24335.208.3315.1951	nonSecurity	unclassified
PC3	Microsoft Corporation	Windows Update Agent	2024-10 .NET 6.0.35 Security Update for x64 Client (KB5045998)	1309.2410.30012.0	10.0.26100	security	important
PC3	Google Inc.	Google Chrome	Google Chrome 132.0.6834.84	131.0.6778.265	132.0.6834.84	security	important
PC3	Igor Pavlov	7-Zip exe (x64)	7-Zip 24.09	22	24.09	security	moderate
PC3	Zoom Video Communications, Inc.	Zoom	Zoom 6.3.6	6.2.7	6.3.6	nonSecurity	unclassified
PC3	Microsoft Corporation	Microsoft Visual C++ 2015-2022 Redistributable (x86)	Microsoft Visual C++ 2015-2022 Redistributable 14.42.34433.0	14.30.30708.0	14.42.34433.0	nonSecurity	unclassified

WSUSでのパッチ適用を行なっていない場合
WithSecureよりSecurity関連のパッチに対して定期的な適用が可能です

＊一度適用したパッチのアンインストールはできませんのでご留意願います

＊お客様ポータルよりパッチ適用のタイミングのセットが必要です

更新可能なソフトウエア

最新情報はこちらを参照願います

https://www2.withsecure.com/en/solutions/software-and-services/business-suite/software-updater?utm_source=chatgpt.com

Adobe Acrobat Reader **Google Chrome** Google Drive

Mozilla Firefox Thunderbird Java VirtualBox **WinZip** RealPlayer

PuTTY Notepad++ TeamViewerWireshark Skype Evernote **Open Office**

iTunes GIMP Dropbox **Zoom**

MS Office **Microsoft Office 365** Microsoft OneDrive Microsoft Teams

Microsoft Edge Microsoft Visual C++ Redistributable

Citrix Workspace Winamp Node.js LTS Node.js Current OpenVPN

Cisco Jabber VNC Server VNC Viewer Webex Jabra Direct VMware Workstation VMware Player VMware Horizon Client Git

Amazon CorrettoGlobalProtect **Zabbix Agent** WatchGuard Mobile VPN with SSL

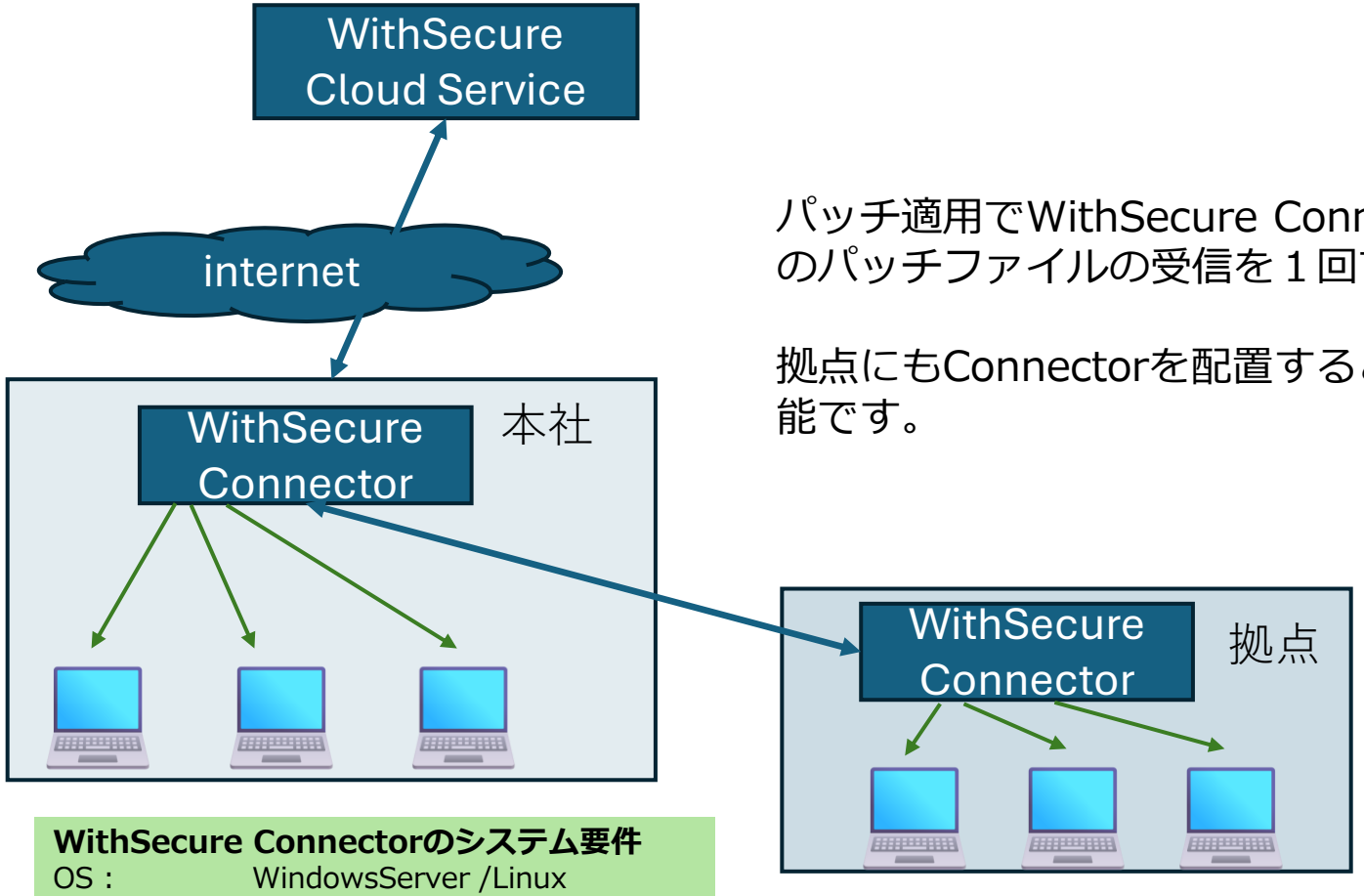
Dell SupportAssist ExpressVPN Slack

Windows OSのパッチはQUまで適用可能　FU対象外となります

WithSecure Connectorを利用したパッチ適用

WithSecure Connectorとは

無償で提供可能なWithSecure専用のProxyです
WithSecureのCloudサービスとの接続のみ仲介します



パッチ適用でWithSecure Connectorを利用すると、Internetからのパッチファイルの受信を１回で済ますことが可能となります。

拠点にもConnectorを配置することにより、多段構成を築こともできます。

WithSecure Connectorのシステム要件

OS：	WindowsServer /Linux
プロセッサー:	デュアルコア2GHzCPU以上
メモリ:	4 GB RAM
• ディスク容量:	10GBの空きディスク容量
• ネットワーク:	100Mビットネットワーク

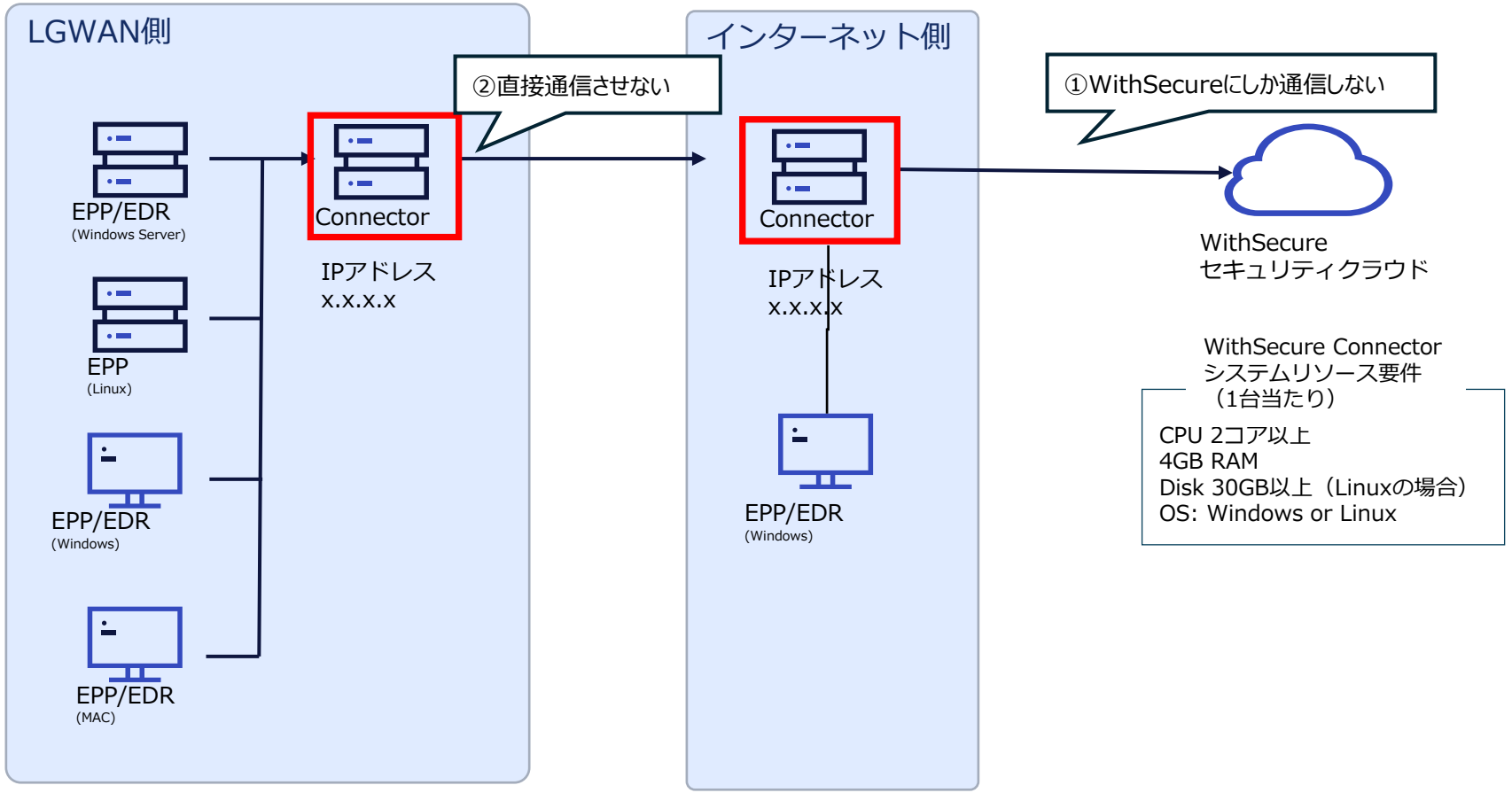
某自治体での利用例

WithSecure Connector（ベンダ提供の専用プロキシ）によるインターネットへの接続

① Connector は、WithSecureセキュリティクラウドにしか接続できない

② LGWAN端末からの直接通信させないために多段構成を採用

アクセス先をWithSecure のみに限定



WithSecure Connector
システムリソース要件
（1台当たり）

CPU 2コア以上
4GB RAM
Disk 30GB以上（Linuxの場合）
OS: Windows or Linux

WithSecure機能概要　PCの設定情報の提供

- Windowsの自動更新の状況
- パスワードの最小文字数
- アカウントロックアウトの閾値
- システムドライブの空き容量
- ディスクの暗号化ステータス
- BitLocker回復キーの収集
- リモートデスクトップの利用状況
- ローカルディスクの共有状況

WithSecureによる機密データ保護機能　　＊Premium版

Windows Serverではデータガード機能とアプリケーション制御が提供されます

＊Windows PC版ではPremiumライセンス（追加料金発生）が必要

-データガード機能

不明なアプリケーションがフォルダにアクセスするのを防ぐことで、
フォルダをランサムウェア (暗号化による恐喝) から保護します。

-アプリケーション制御

アプリケーションの実行とインストールを防ぎ、スクリプトの実行を阻止します。
悪意のある、違法な、不正なソフトウェアが安定稼働にもたらすリスクを軽減します。

悪用される正規ツールの事前ブロック／アプリケーション制御　*Premium版

通常業務で使われない管理用ツールを アプリケーション制御 で先回りブロック
― 攻撃の連鎖を未然に断つ

考え方 ／ 正規ツールは「使う前提か／使わない前提か」で判断する

攻撃で使われるツールは**マルウェアとは限らず、システム管理用の正規ツール**（LOLBins／Living off the Land）であることが多い。通常業務でこれらを使わない端末では、**使用された時点で危険な兆候**。あらかじめ Application Control でブロックしておくことで、防御の網をすり抜けた攻撃でも次フェーズに進めなくする。

ATTACK PHASES ／ 各フェーズで悪用される代表的な正規ツール

PHASE 1 初期侵入	PHASE 2 遠隔操作・接続性維持	PHASE 3 権限昇格	PHASE 4 隠蔽・無効化	PHASE 5 資格情報の窃取・悪用	PHASE 6 環境探索・調査	PHASE 7 情報窃取・データ流出	PHASE 8 横展開・ランサム配布
以下のルートで侵入 • 脆弱性 • 漏洩したパスワード • ソーシャルエンジニアリング etc.	• TightVNC • AnyDesk • TeamViewer • tera(WebCatalog) • Metasploit etc.	• PAExec • PsExec • CSExec • Empire • cmstp etc.	• AdvancedRun • sc.exe • wevtutil • vssadmin • HRSword etc.	• Mimikatz • Cobalt Strike • procdump • ntdsutil • Kerbrute etc.	• AdFind • BloodHound • net view • nltest • Nmap etc.	• **Cyberduck** • **MEGAsync** • **WinSCP** • **FileZilla** • **FreeFileSync** etc.	• CSExec • PAExec • PSExec • winexe • PDQ Deploy etc.

―― 準備段階（足場固め）　　**最終目的（実被害）** ――

適用例 ／ PHASE 7「情報窃取・データ流出」の事前ブロック

最も「気付きにくく」かつ「実害が大きい」フェーズ

Rclone・MEGAsync・WinSCP などは**正規のファイル転送ツール**で、シグネチャベース検知では止めにくい。通常業務で利用しない場合は Application Control で**あらかじめ実行をブロック**しておくことで、内部からの**情報漏洩リスクを大きく低減**できる。

※ 検知後の対応では手遅れになりやすい流出フェーズを、実行前に断つ

HOW TO DEPLOY ／ 段階的に導入する 3 ステップ

1. **PRE-REGISTER ／ 事前登録**
   悪用の可能性がある**約 130 種類のツール**をあらかじめ Application Control に登録
2. **OBSERVE ／ 検知のみで経過観察**
   一定期間は**ブロックせず検知のみ**。業務利用が確認されたツールは**例外登録**し誤検知を排除
3. **ENFORCE ／ ブロックへ移行**
   誤検知収束後、**未然に攻撃を防ぐ**モードへ

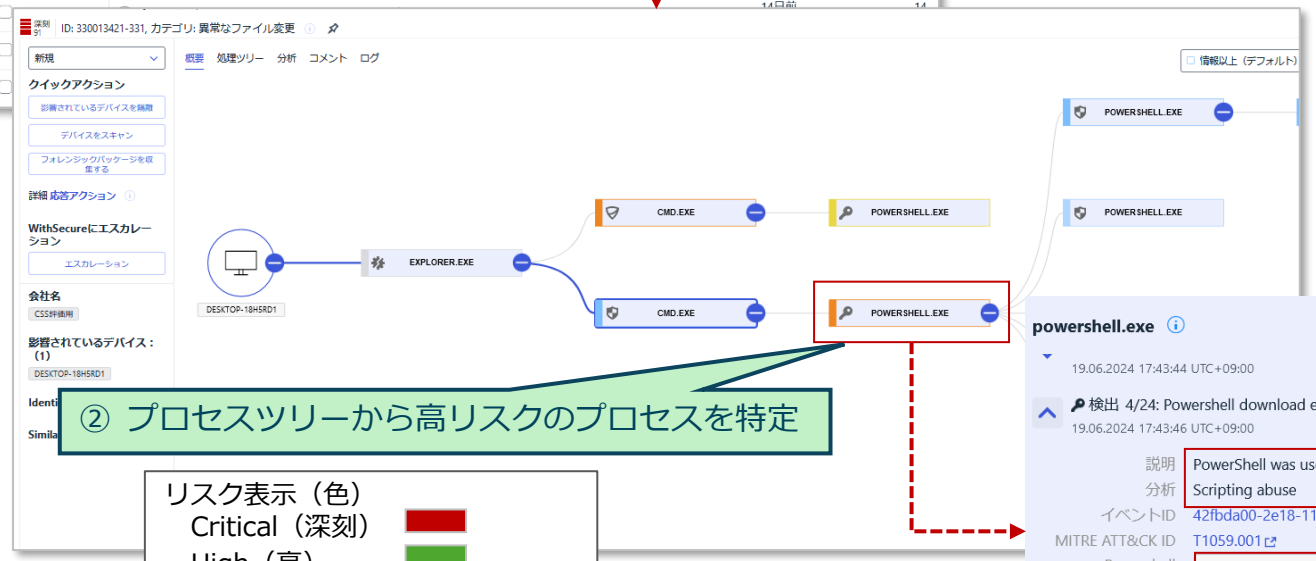
■ インシデントの可視化

～ 数クリックでインシデントを素早く攻撃詳細を把握することができます ～

① EDRアラート一覧画面

① アラート検知時に一覧画面から対象のアラートIDを選択

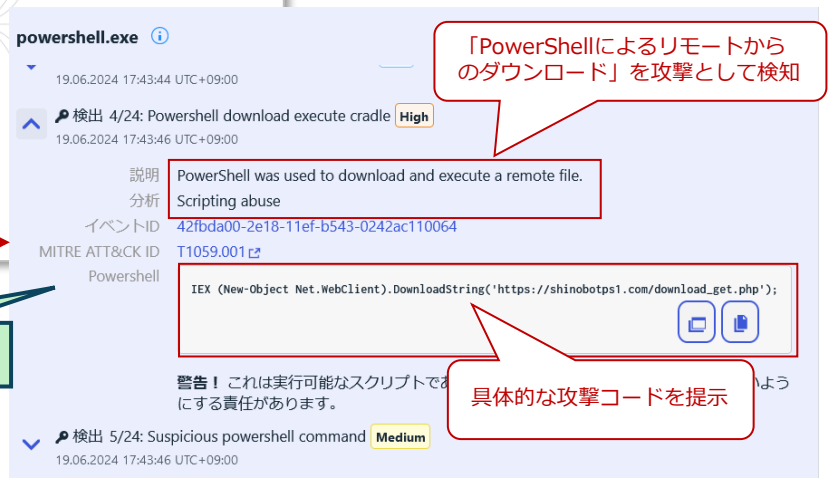
② 関連プロセスのプロセスツリー



② プロセスツリーから高リスクのプロセスを特定

リスク表示（色）
- Critical（深刻）
- High（高）
- Medium（中）
- Low（低）
- Info（情報）

③ 攻撃処理の詳細



「PowerShellによるリモートからのダウンロード」を攻撃として検知

具体的な攻撃コードを提示

③ 攻撃詳細を確認

サービスの流れ
インシデント対応サービス

■ 基本的なサービス内容

- アラート一次受付
- 一次切り分け（トリアージ）
- お客様への連絡
- ネットワーク隔離
- 端末復旧処置
- 対応報告

■ 重大度別／端末種別による対応（例）

<Highの場合>
ネットワーク隔離後、お客様（情報システム課）へメールで連絡し、その後、復旧作業を行う
<Middleの場合>
お客様へ連絡（情報システム課）へ電話し、承認を得たうえでネットワーク隔離し、その後、復旧作業を行う
<Lowの場合>
基本的に対応しない。上記対応時に必要に応じて参考情報として確認する