NRI SECURE

Web分離・無害化によるセキュリティ対策
～Menlo Securityのご紹介～

2019年12月19日

NRIセキュアテクノロジーズ株式会社
DXセキュリティ事業本部
セキュリティインテグレーション一部

弊社ご紹介

NRIセキュアテクノロジーズ 会社概要

野村総合研究所（NRI）グループにおける情報セキュリティ専門の中核企業

社　　名	**NRIセキュアテクノロジーズ株式会社**（略称：NRIセキュア）		
会社所在地	本社　　：東京都千代田区大手町 東京サンケイビル 横浜テクニカルセンター　：神奈川県横浜市保土ケ谷区 NRIタワー 北米支社　　：米国カリフォルニア州アーバイン		
設立年月日	2000年8月1日　※サービス提供開始：1995年		
資　本　金	4.5億円		
株　　主	株式会社野村総合研究所		
代表取締役社長	小田島 潤		
取　締　役	池田 泰徳、榊原 大史、竹本 具城、山口 隆夫	監査役	原田 豊
社　員　数	連結：493名、単体：401名　（2019年10月1日現在）		
NRIセキュアグループ会社	株式会社ユービーセキュア：東京都港区 株式会社NDIAS　　：東京都港区		
提　供　実　績	官公庁、金融機関（銀行、証券、資産運用、保険、信販、消費者金融） 流通、製造、製薬、通信、マスコミ など		
認　証　取　得	ISO/IEC 27001認証取得		

IS 75215 / ISO 27001

NRIセキュアテクノロジーズ 事業概要

4事業のシナジーにより、企業の情報セキュリティ課題をワンストップ解決

4つの主要事業

コンサルティング
高い専門性による
オーダーメイドの課題解決支援

DXセキュリティ
デジタルトランスフォーメーション
を支えるセキュリティ

マネージドセキュリティサービス
24時間365日で
世界トップレベルのMDRとSOC

ソフトウェア
高品質で利便性の高い
自社開発ソリューション

4事業で提供する5つのサービスカテゴリ

セキュリティ コンサルティング	専門のコンサルタントによる セキュリティ対策のPDCA支援
人材育成・研修	セキュリティ人材の育成と資格（GIAC、CISSP）の取得支援
セキュリティ診断・ ペネトレーションテスト	攻撃者の視点・技術による ITシステムの脆弱性チェック
セキュリティ監視・ SOCサービス	サイバー攻撃からITシステムを防御する、24時間×365日の監視・管理サービス
セキュリティ ソリューション	自社開発を中心とした、高品質で利便性の高い各種セキュリティ対策ソリューション

ナビゲーション活動

国内外で政策提言と標準化活動、独自調査分析の公開を行い、業界の発展に貢献

加盟団体

- 金融情報システムセンター (FISC)
- 日本セキュリティ監査協会 (JASA)
- 日本ネットワークセキュリティ協会 (JNSA)
- Forum of Incident Response and Security Teams (FIRST)
- 日本シーサート協議会
- 日本カード情報セキュリティ協議会 (JCDSC)
- 日本公認不正検査士協会 (ACFE JAPAN)
- ICT-ISAC (ICT-ISAC-J)
- 技術研究組合制御システムセキュリティセンター (CSSC)
- 日本スマートフォンセキュリティ協議会 (JSSEC)
- デジタル・フォレンジック研究会
- 日本セキュリティオペレーション事業者協議会 (ISOG-J)
- 金融ISAC
- AWS パートナーネットワーク (APN)
- 日本文書情報マネジメント協会 (JIIMA)
- 日本サイバー犯罪対策センター (JC3)
- 自治体情報セキュリティ支援協議会
- 情報処理学会 情報規格調査会 (ITSCJ)
- Fintech協会
- 重要生活機器連携セキュリティ協議会 (CCDS)

情報発信

NRI Secure Insight
企業における情報セキュリティ実態調査

：NRIセキュアテクノロジーズ 発行

Cyber Security Trend Annual Review
サイバーセキュリティ傾向分析レポート

：NRIセキュアテクノロジーズ 発行

ITロードマップ

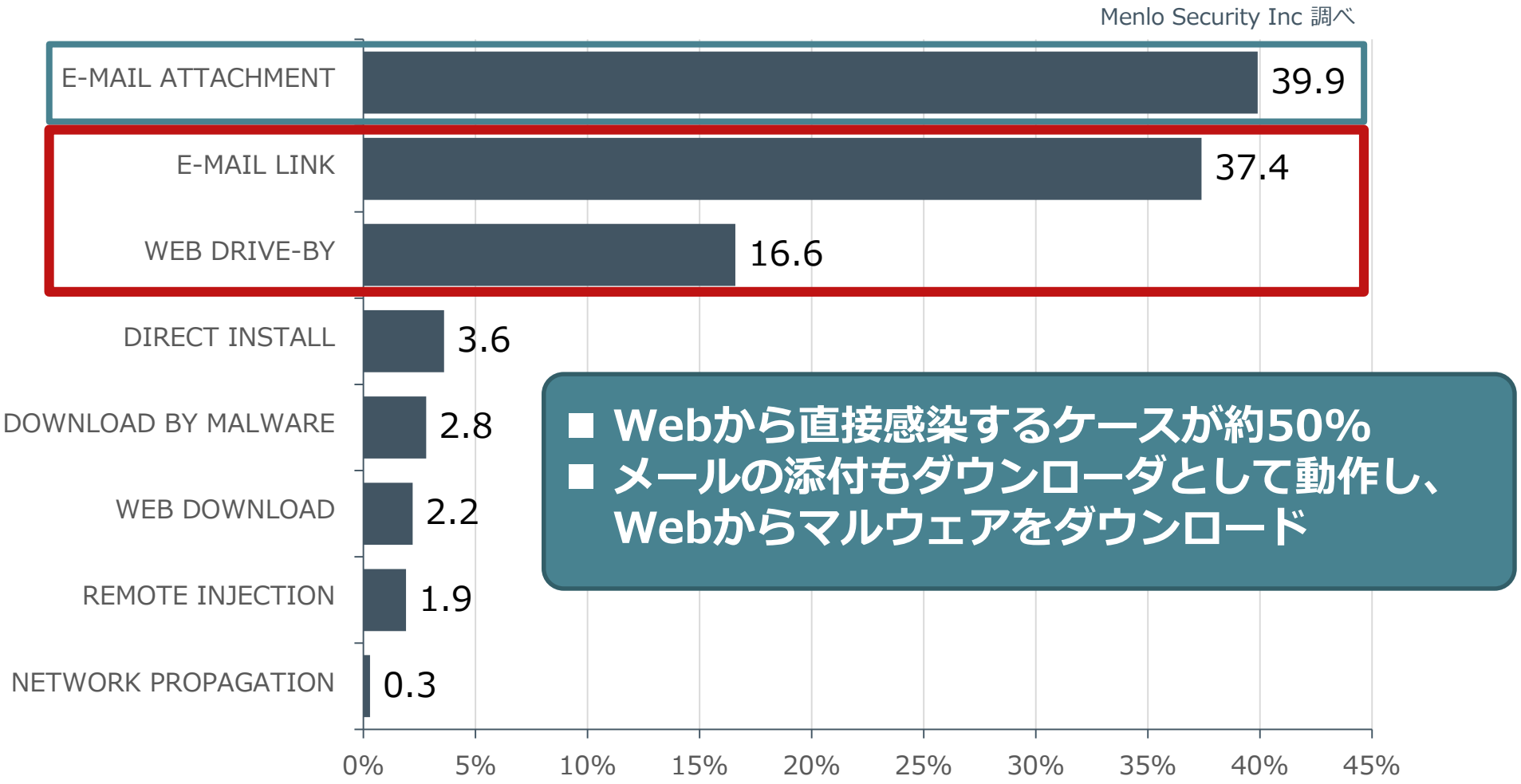
：東洋経済新報社 発行
NRIセキュアテクノロジーズ、
野村総合研究所デジタル基盤開発部　共著

目　次

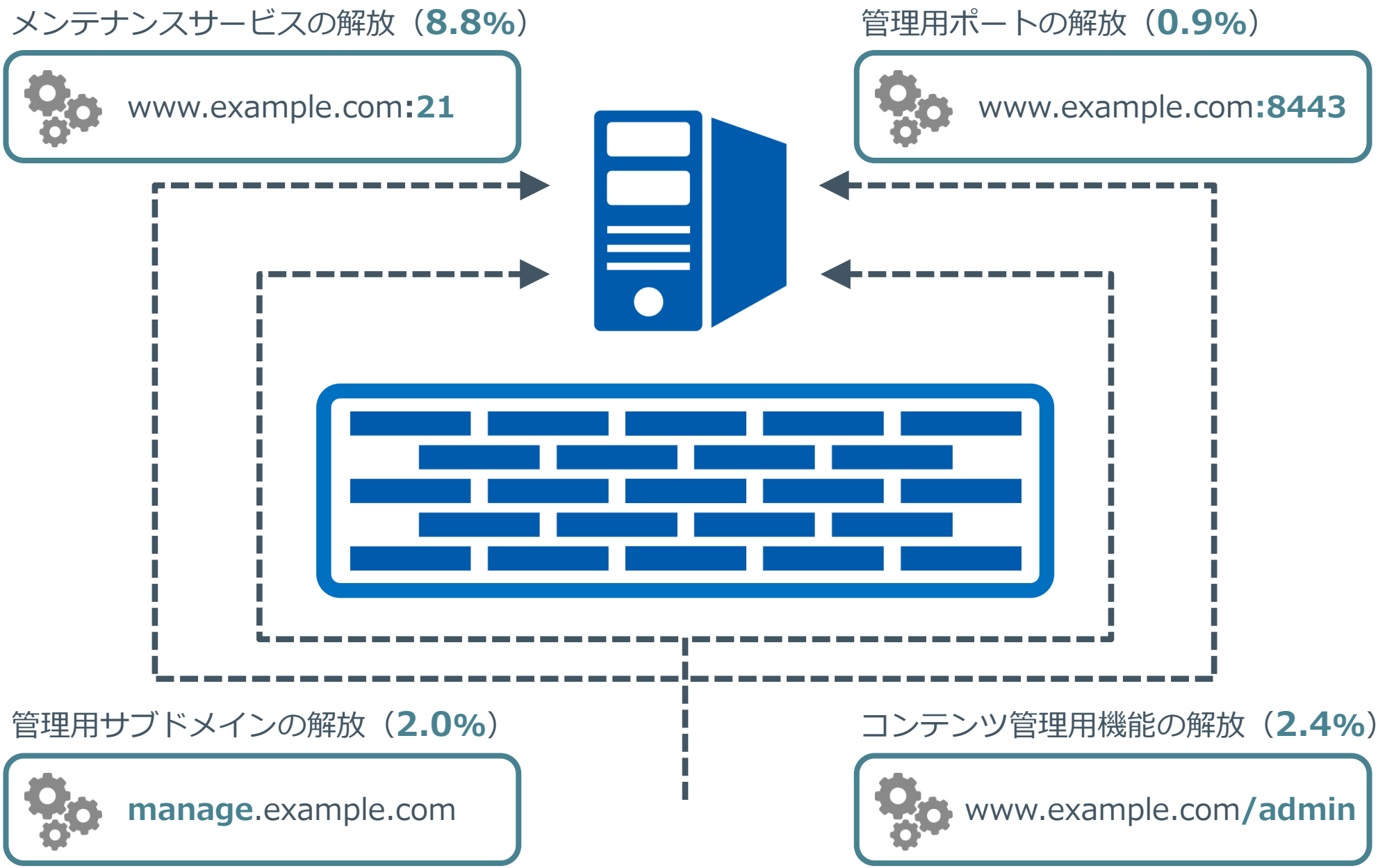
目　次

マルウェアの侵入経路

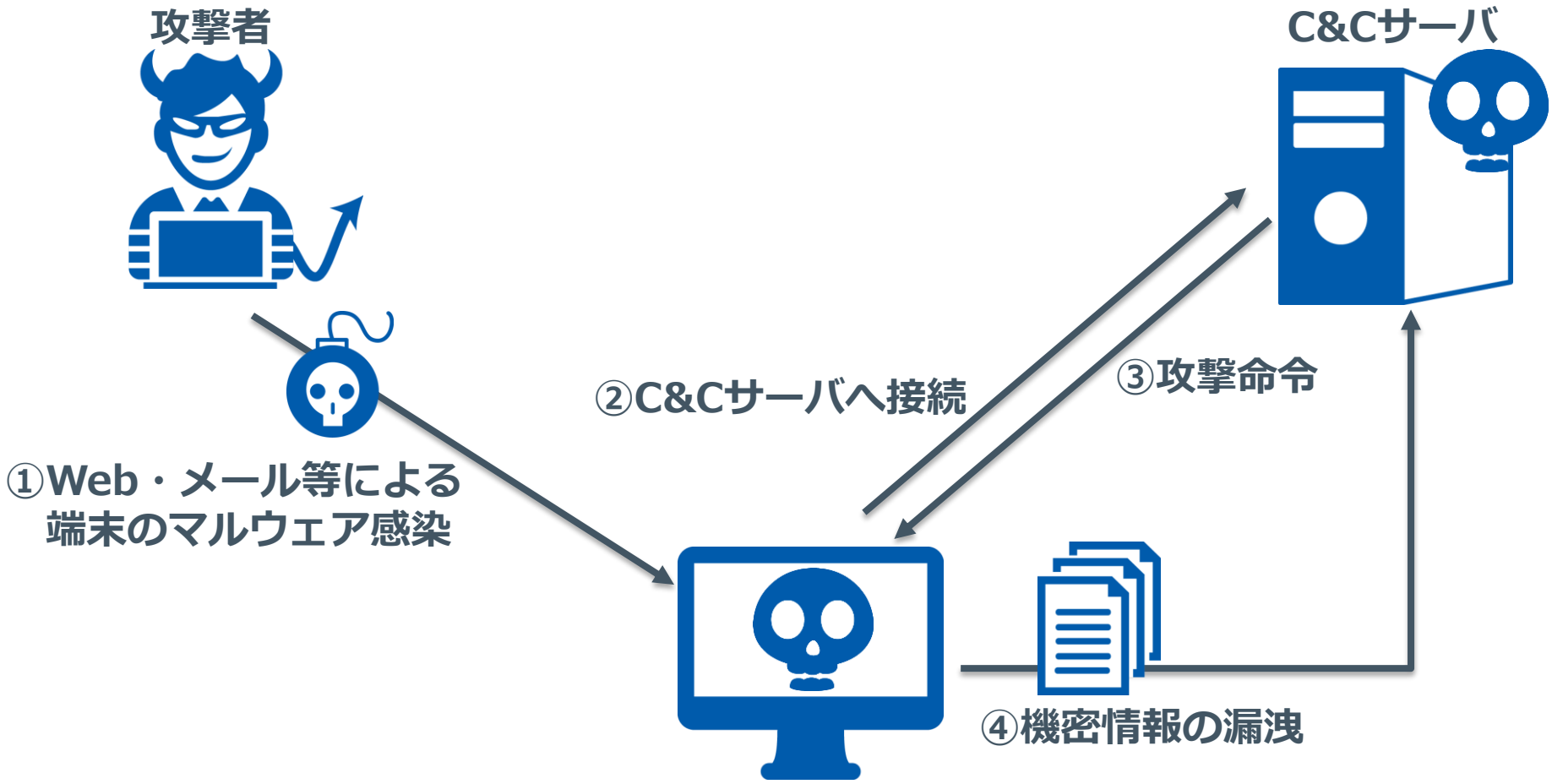
■Vector of malware installation



企業のサイトでも安心はできない

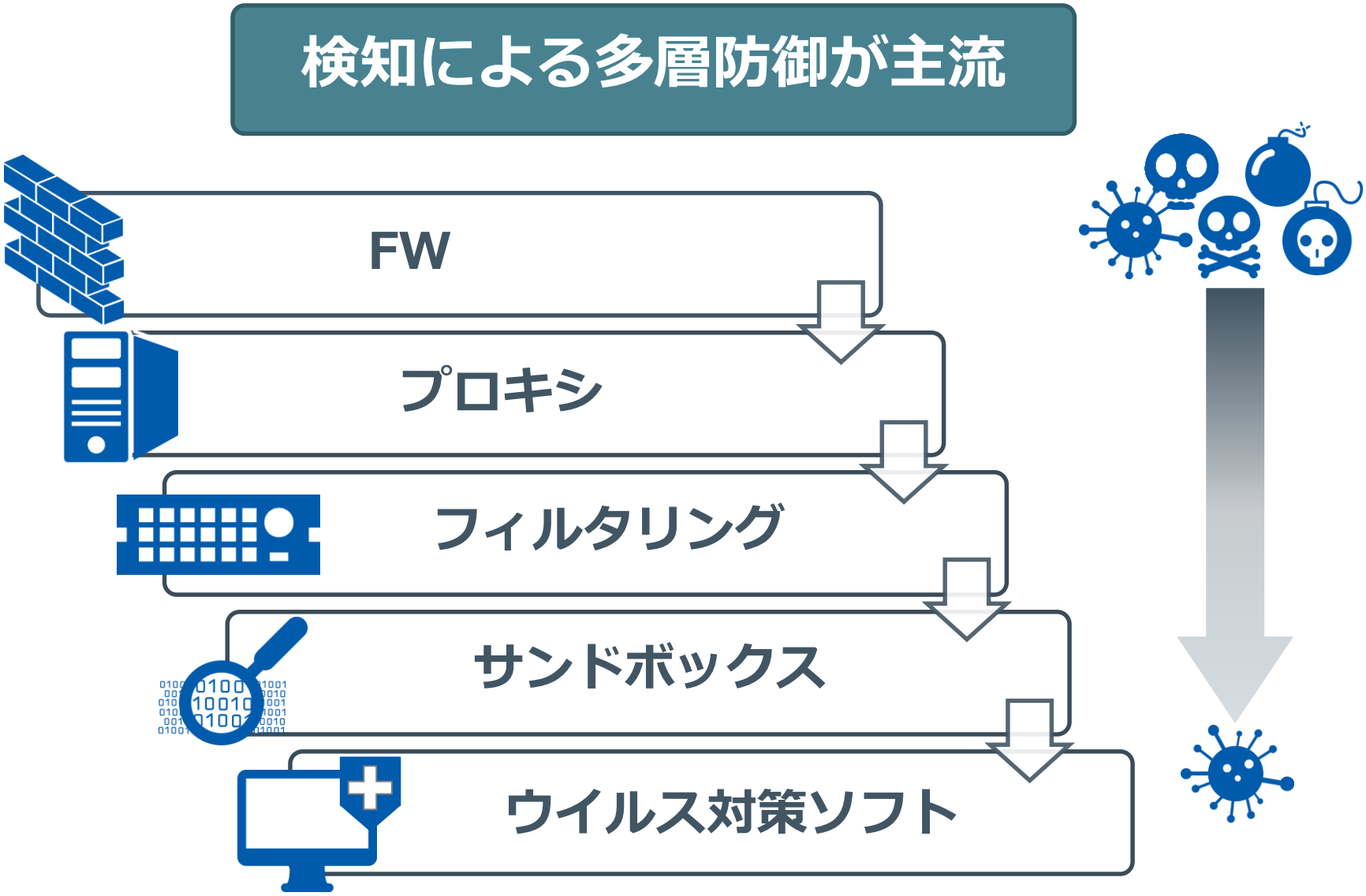


マルウェア感染による攻撃フロー

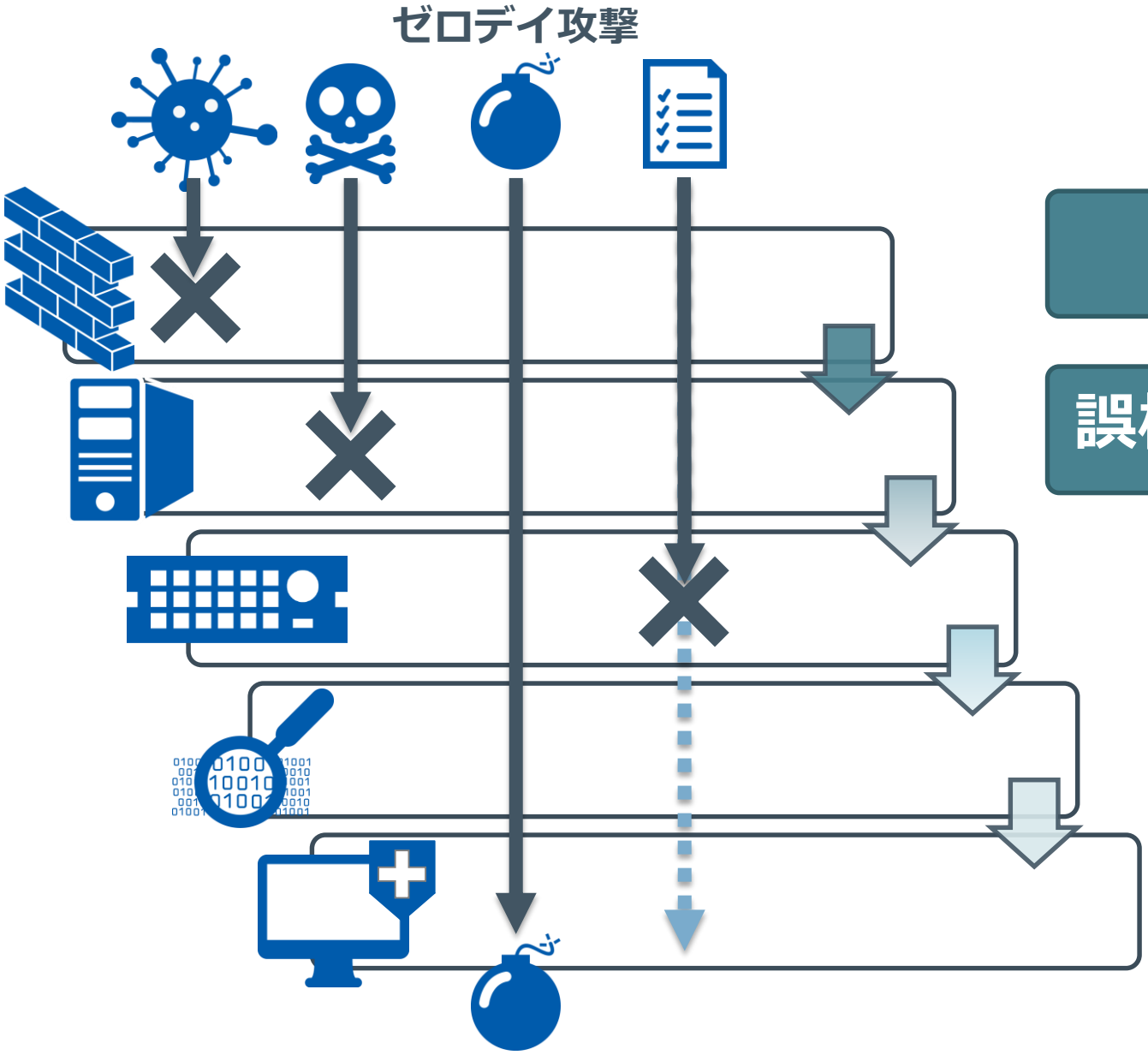


C&Cサーバとの通信の多くはhttp/httpsで行われる

従来のセキュリティ対策



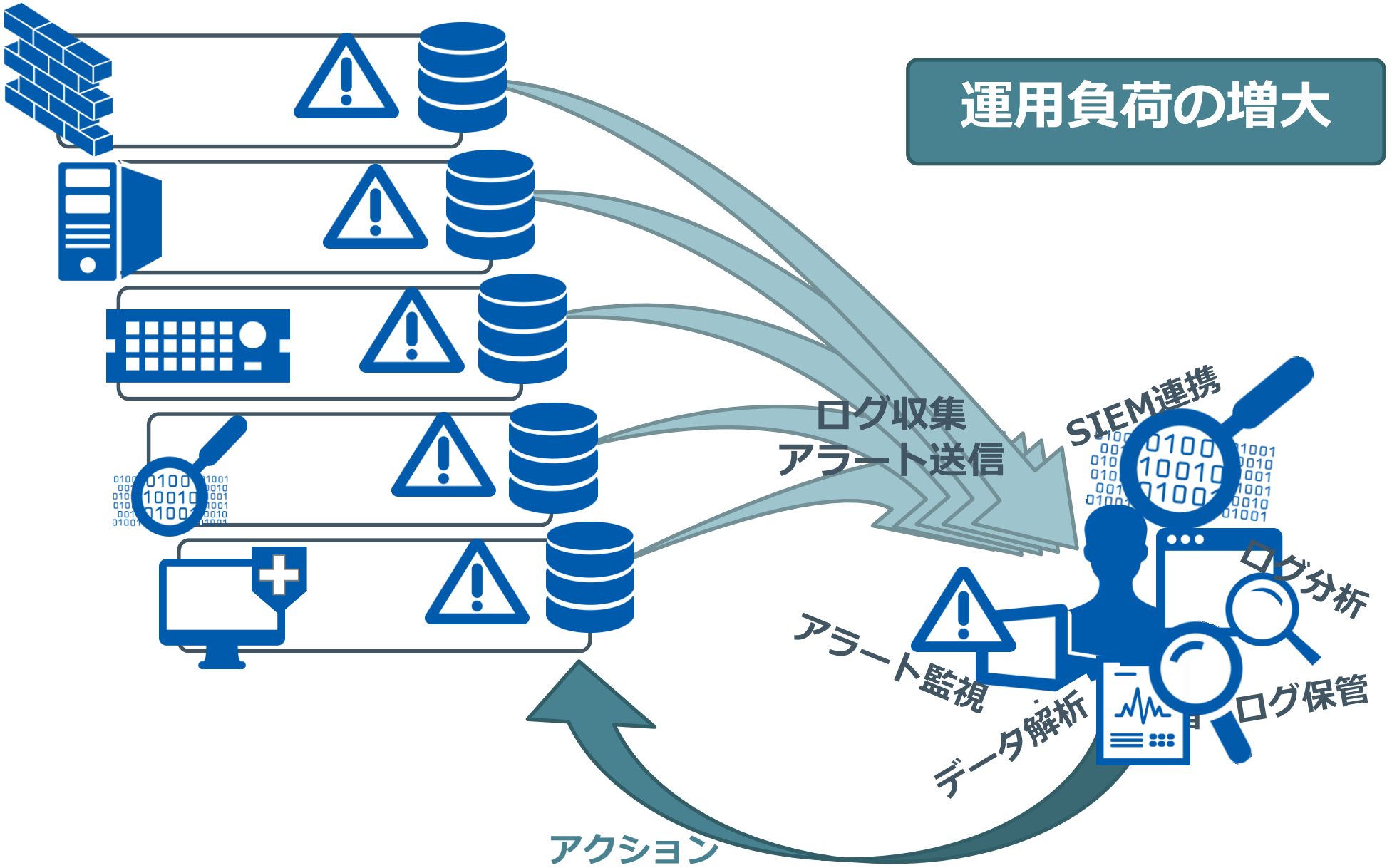
検知ベースの対策における課題



すり抜けの可能性

誤検知・過検知の可能性

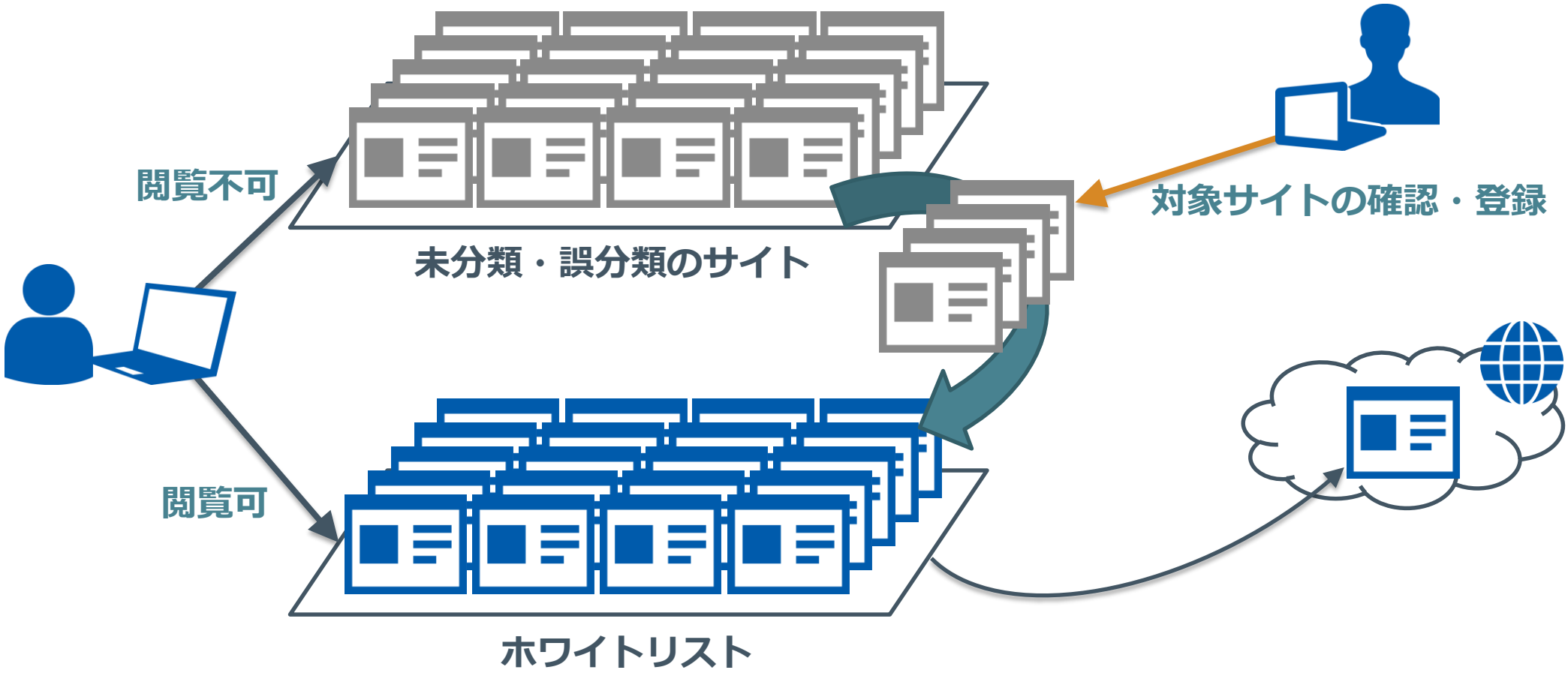
アラート検知に頼る対策における課題



URLフィルタリング（ホワイトリスト運用）の課題

利便性・業務効率の低下

非効率な運用



ここまでのまとめ

- マルウェア対策にはWebの対策が必須
- 検知・判断するアプローチではすり抜けのリスクが残る
- 誤検知・過検知が業務へ大きな影響を与える
- 対策を強化すると利便性の低下、運用負荷増大が起こる

目　次

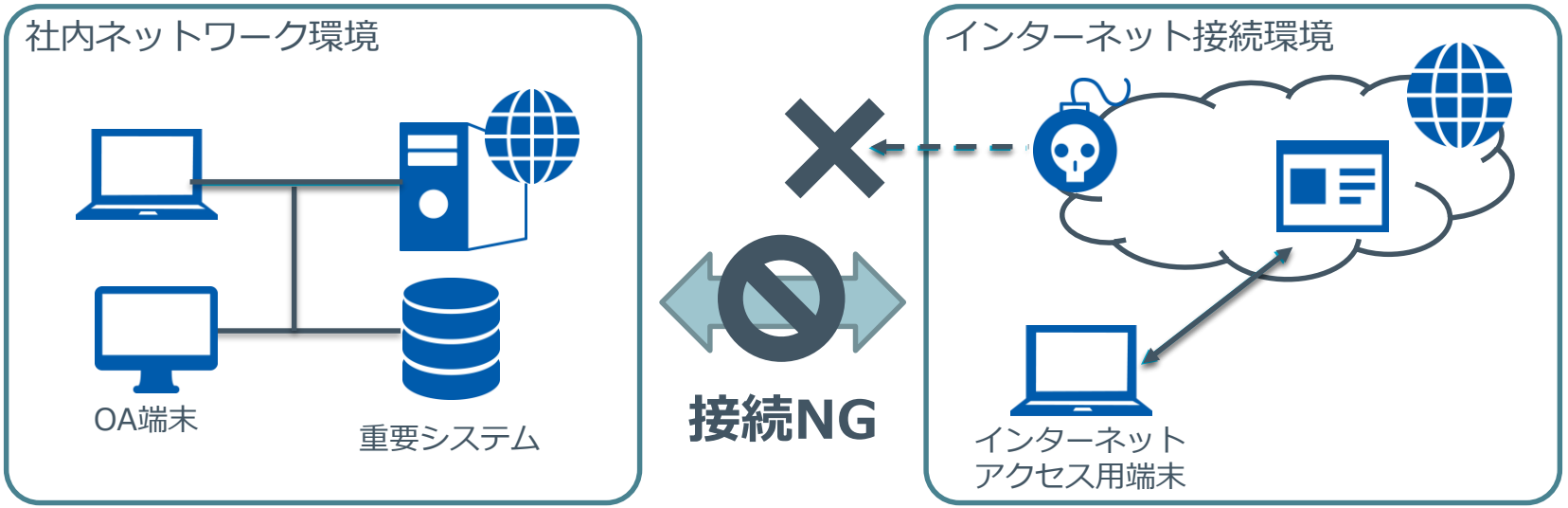
Web分離とは

ネットワーク分離とは

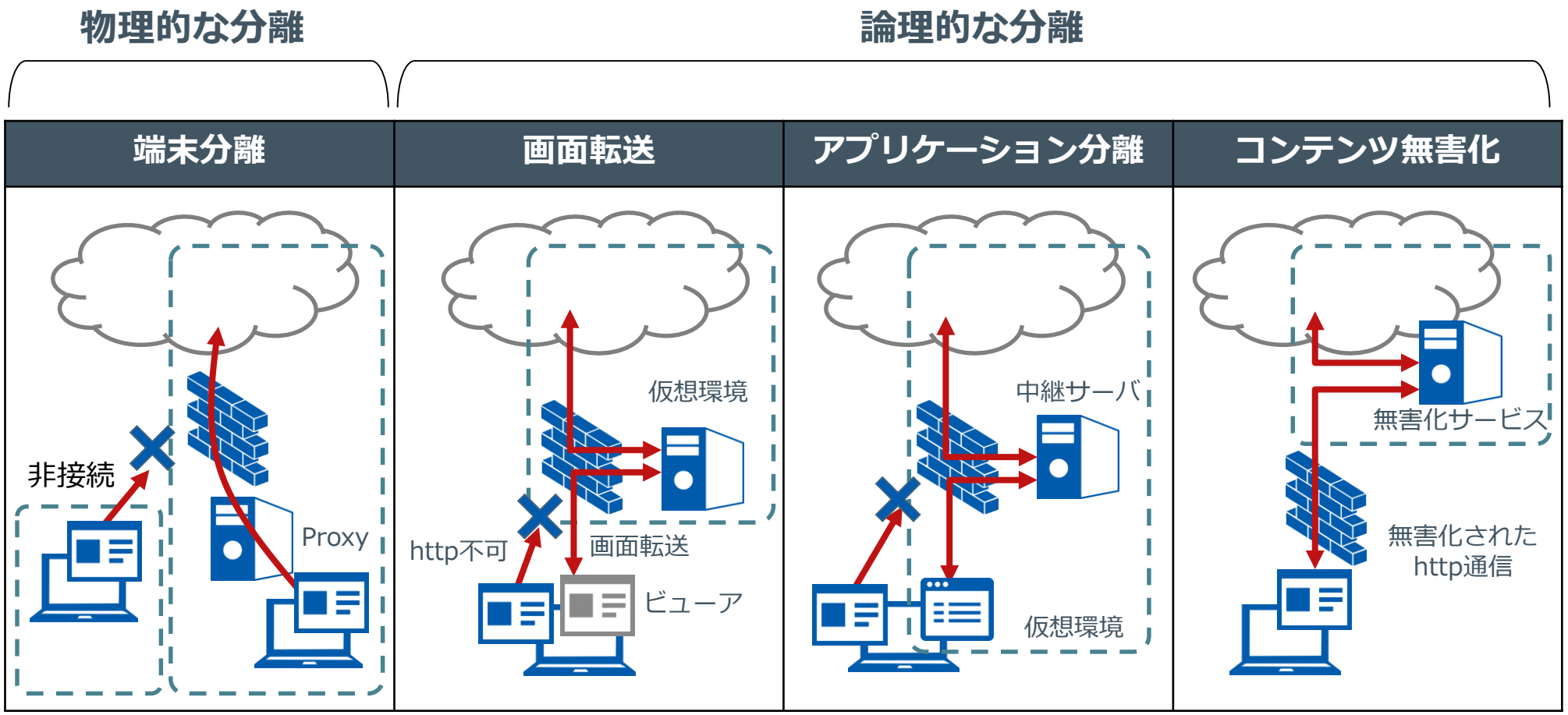
個人情報などの重要情報を扱うシステム（重要システム）と直接的、間接的問わずインターネットへ接続する業務端末やシステムをネットワーク的に切り離す仕組みです。

ネットワーク分離に期待する効果

- インターネットと繋がらないため、マルウェア等への感染リスクが大幅に減る
- 万が一、マルウェア等へ感染してもインターネット経由での情報漏洩が発生しない



ネットワーク分離の方式



Web分離推進の動き

■改めて注目される「 Web（ネットワーク）分離」

	発表元	内容
2015年　6月	IPA	多層防御における有効な対策としてネットワーク分離を推奨。
2015年　6月	FISC	「安全対策基準」の技術基準の検討項目としてネットワーク分離について記載。
2015年　7月	NISC	「サイバーセキュリティ戦略」の中で、業務の内容や取り扱う情報の性質・量に応じた情報システムの分離を進め、セキュリティ強化を行うことを明記。
2015年 8月	総務省	日本年金機構の個人情報流出問題を踏まえ、マイナンバー制度が施行されるまでに、各自治体の住民基本台帳システムをインターネットから分離することを要望。 ⇒ 2015年10月5日までに全自治体で対応完了。
2015年12月	経済産業省	「サイバーセキュリティ経営ガイドライン」の中で、サイバー攻撃の脅威への対策としてネットワーク分離の検討を記載。
2016年　7月	観光庁	相次ぐ旅行業者からの個人情報漏えい事案の発生を受け、再発防止策として、個人情報にアクセスするシステムをインターネット環境から分離させることを提言。
2017年10月	文部科学省	「教育情報セキュリティポシーに関するガイドラン」の中で、インターネットリスクからの対策としてネットワーク分離を記載。

目　次

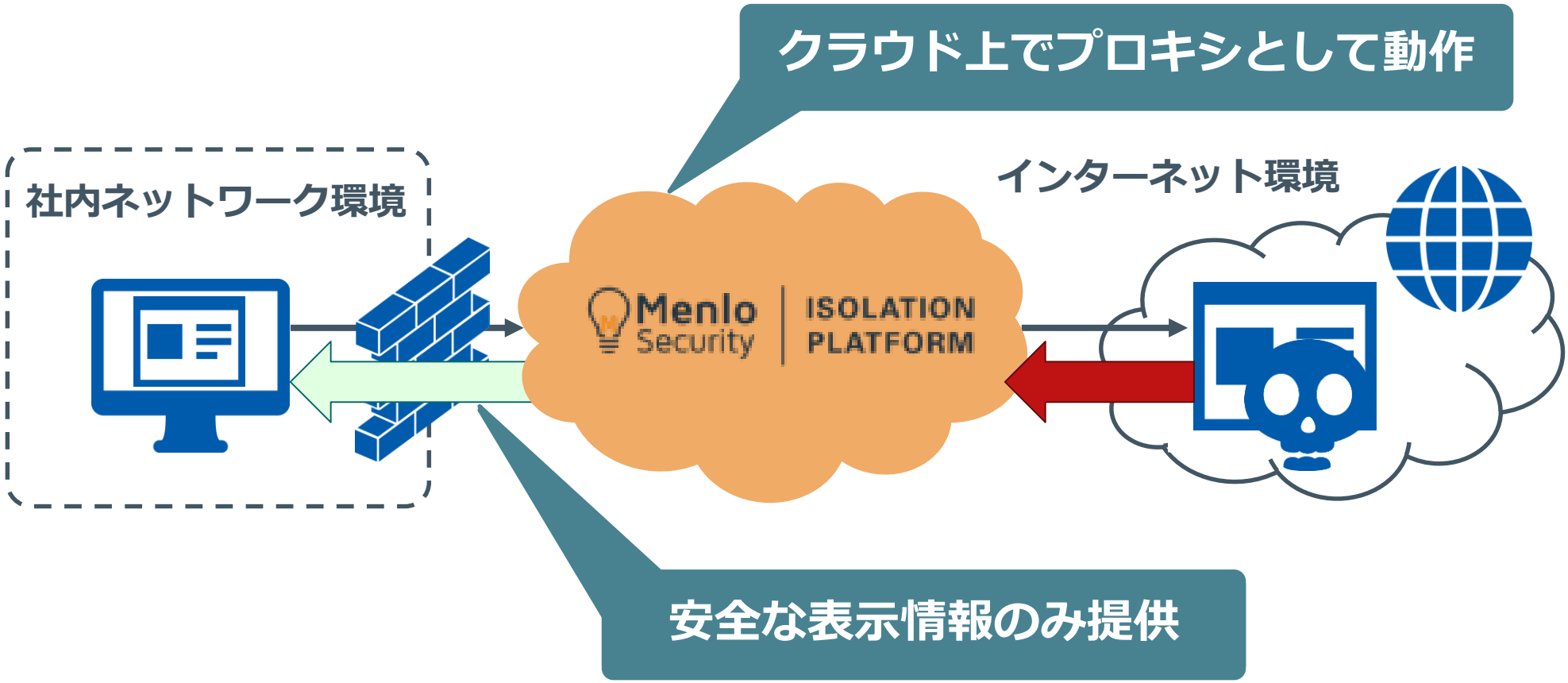
最新のIsolationテクノロジーによるWeb分離・無害化アプローチ

- 2013年 4月 米国カリフォルニア州メンロパークに創業
- 2016年 2月 日本でソリューションの販売を開始
- 2016年 独自レンダリング技術の特許取得
  (ACR：Adaptive Clientless Rendering)

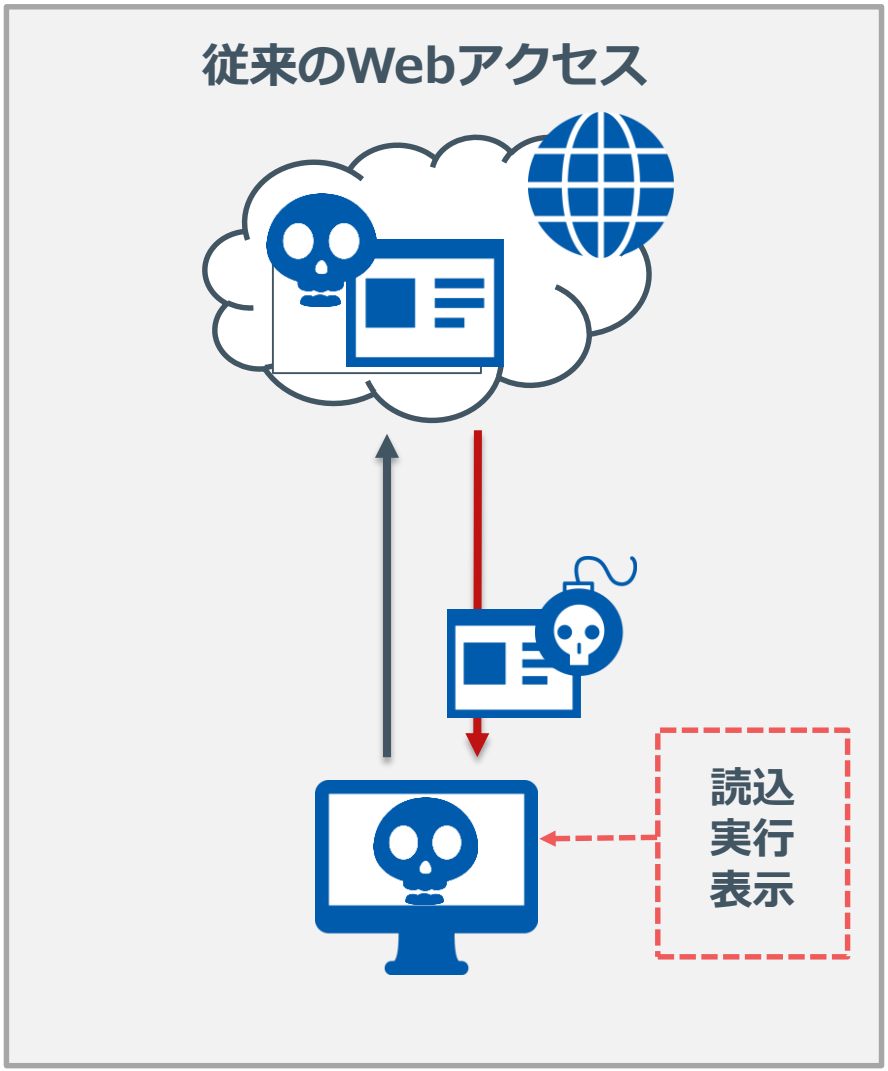
受賞歴

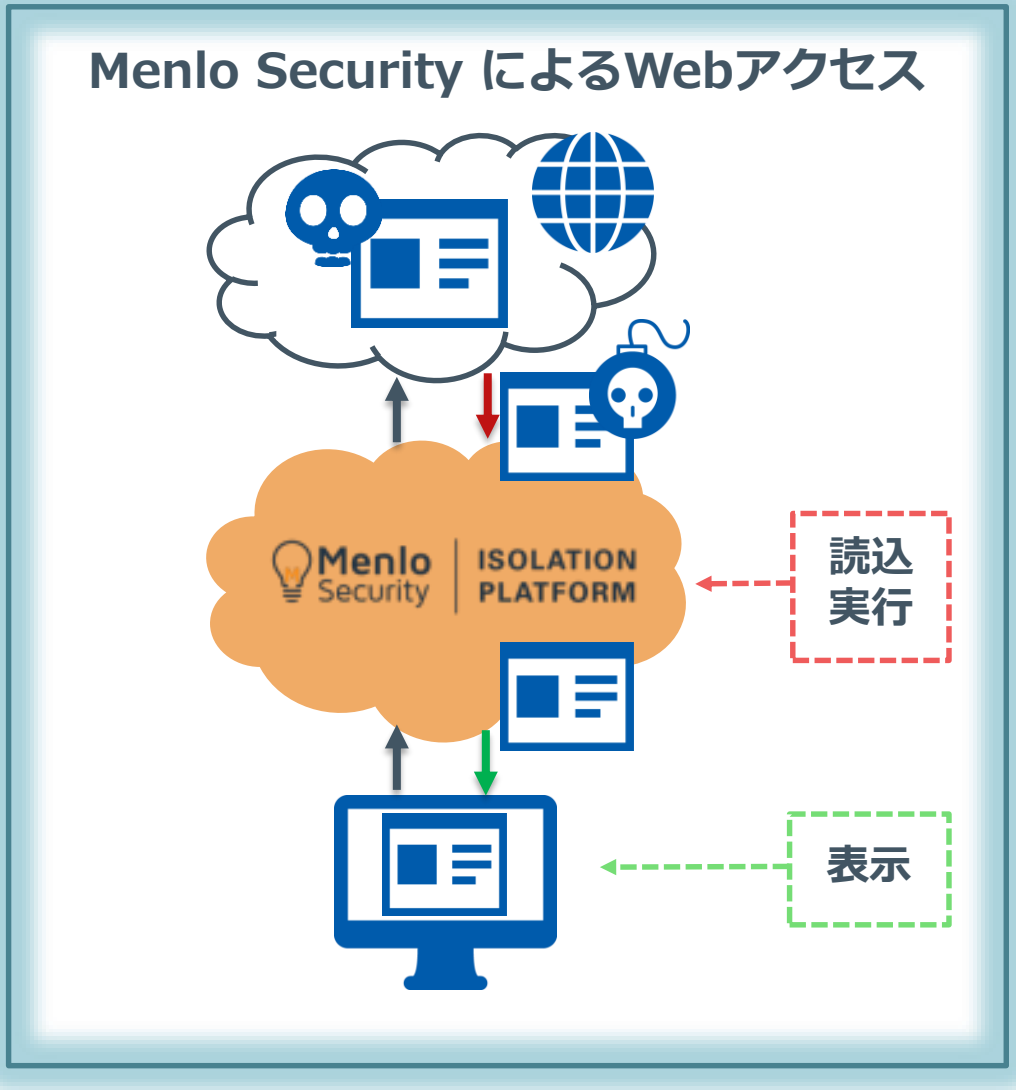
- **Silicon Review誌「2018年最も急成長したセキュリティ企業10社」**
- **CRN誌「2018年最もすばらしいWeb、Eメール、アプリケーションのセキュリティ企業20社」**
- **Interop Tokyo 2016 Best show award グランプリ獲得(クラウドサービス部門)**

Menlo Security Web Isolation Service による分離・無害化



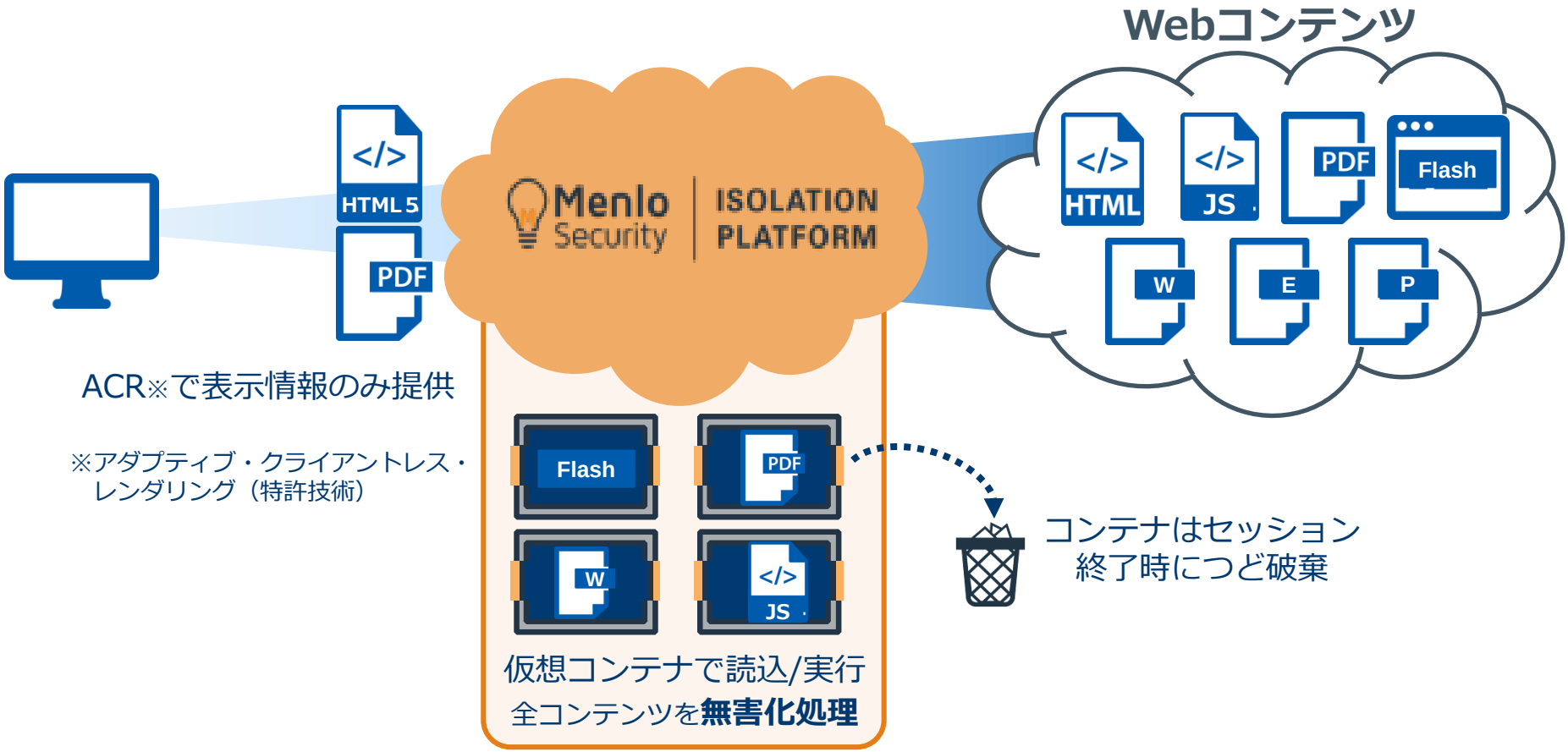
従来のWebアクセスとの比較





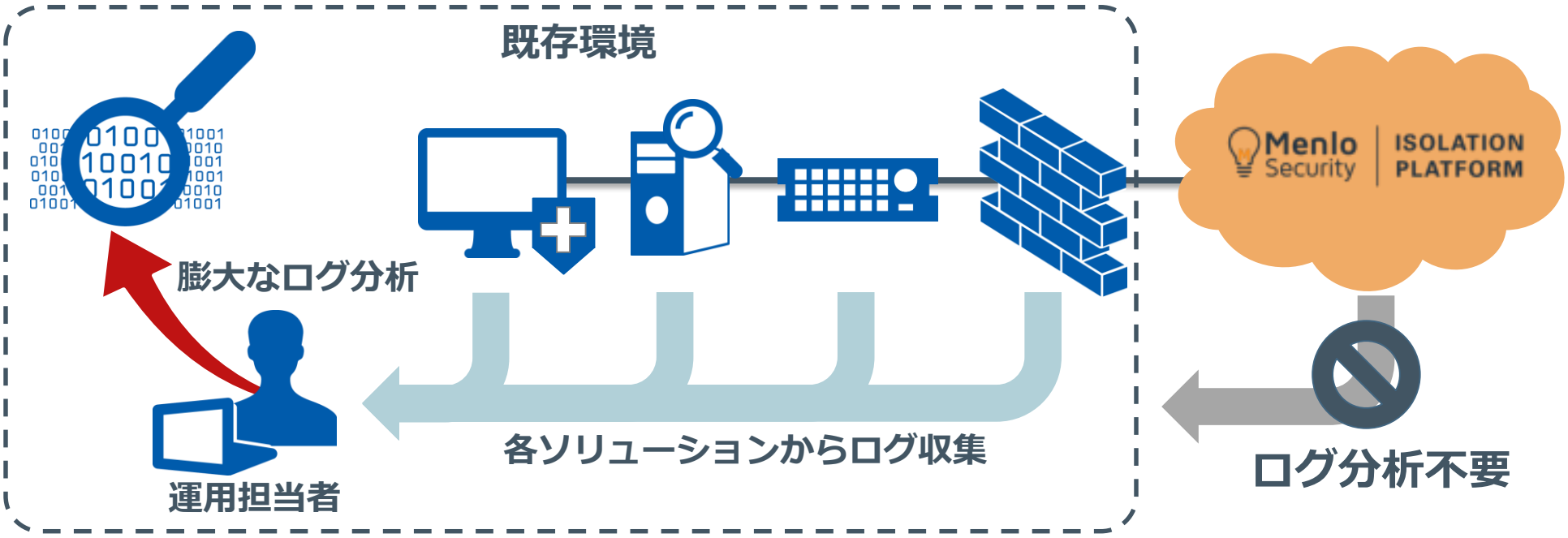
マルウェア排除のしくみ（すり抜け、誤検知・過検知への対策）

すり抜け、誤検知・過検知が発生しない



新しいアプローチによる運用負荷の軽減（運用負荷増大への対策）

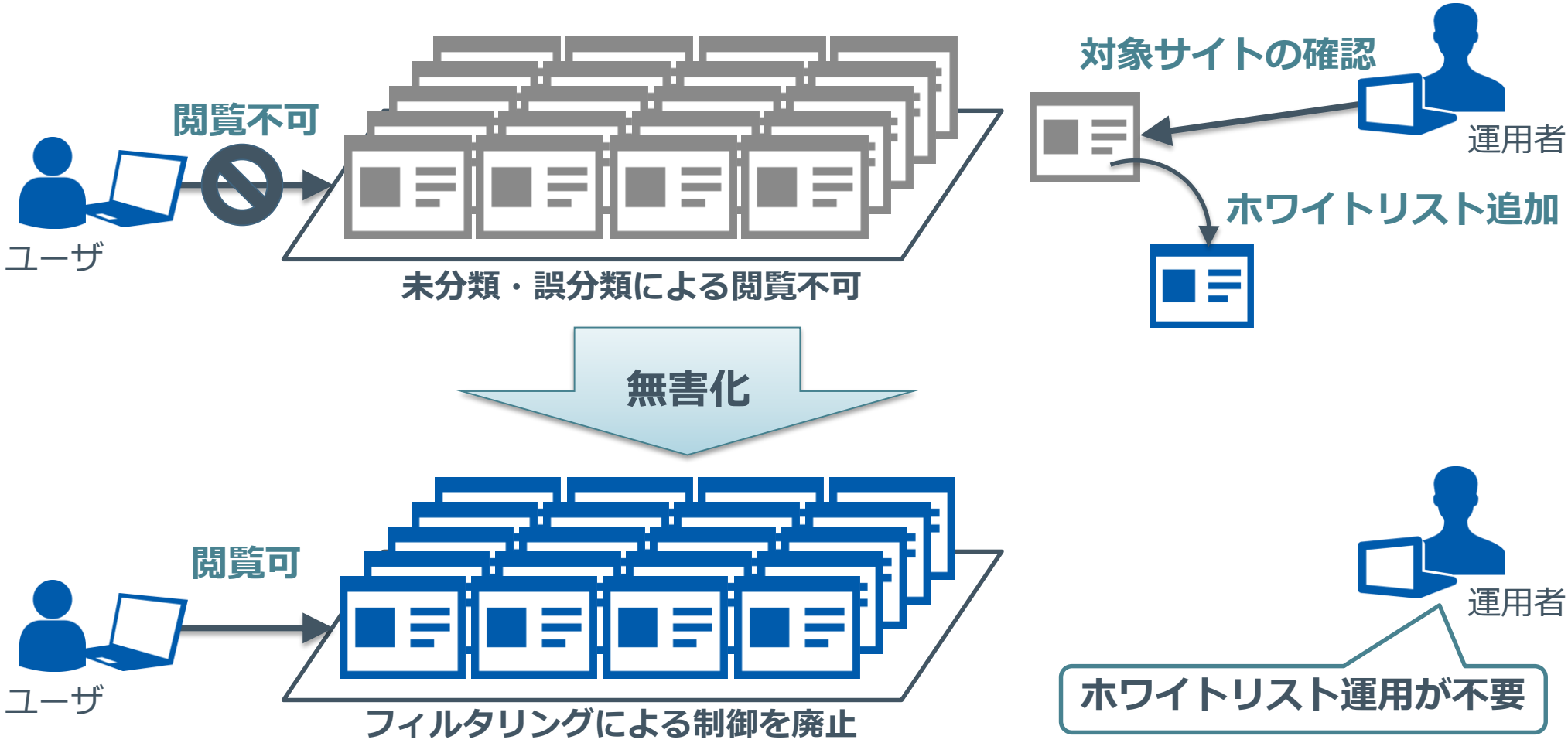
運用負荷、オペレーションコストを大幅に低減



URLフィルタリング（ホワイトリスト運用）の課題

ユーザの利便性向上

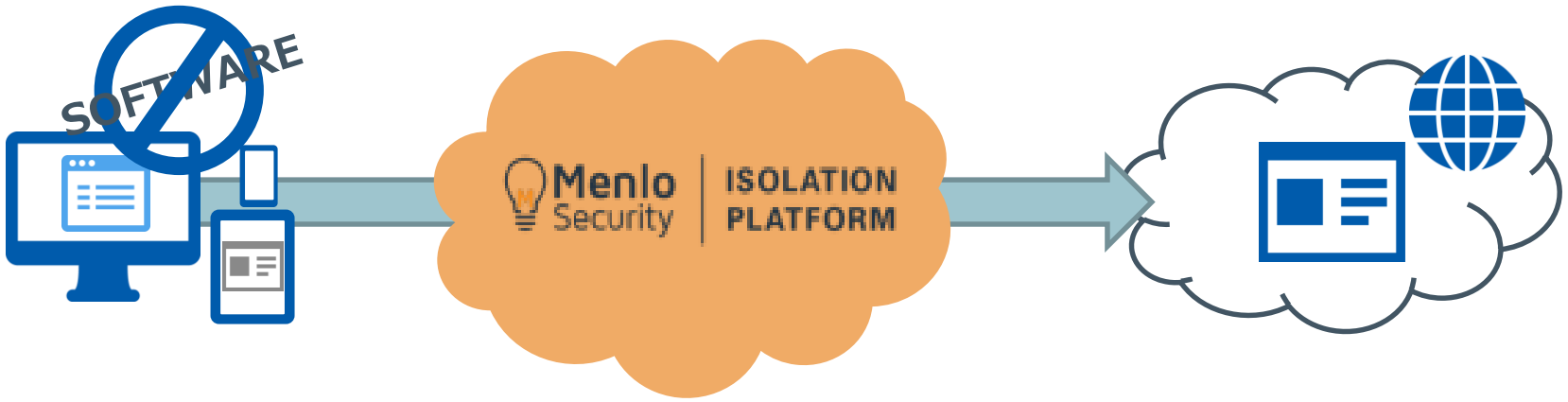
運用者の業務を効率化



導入のしやすさ

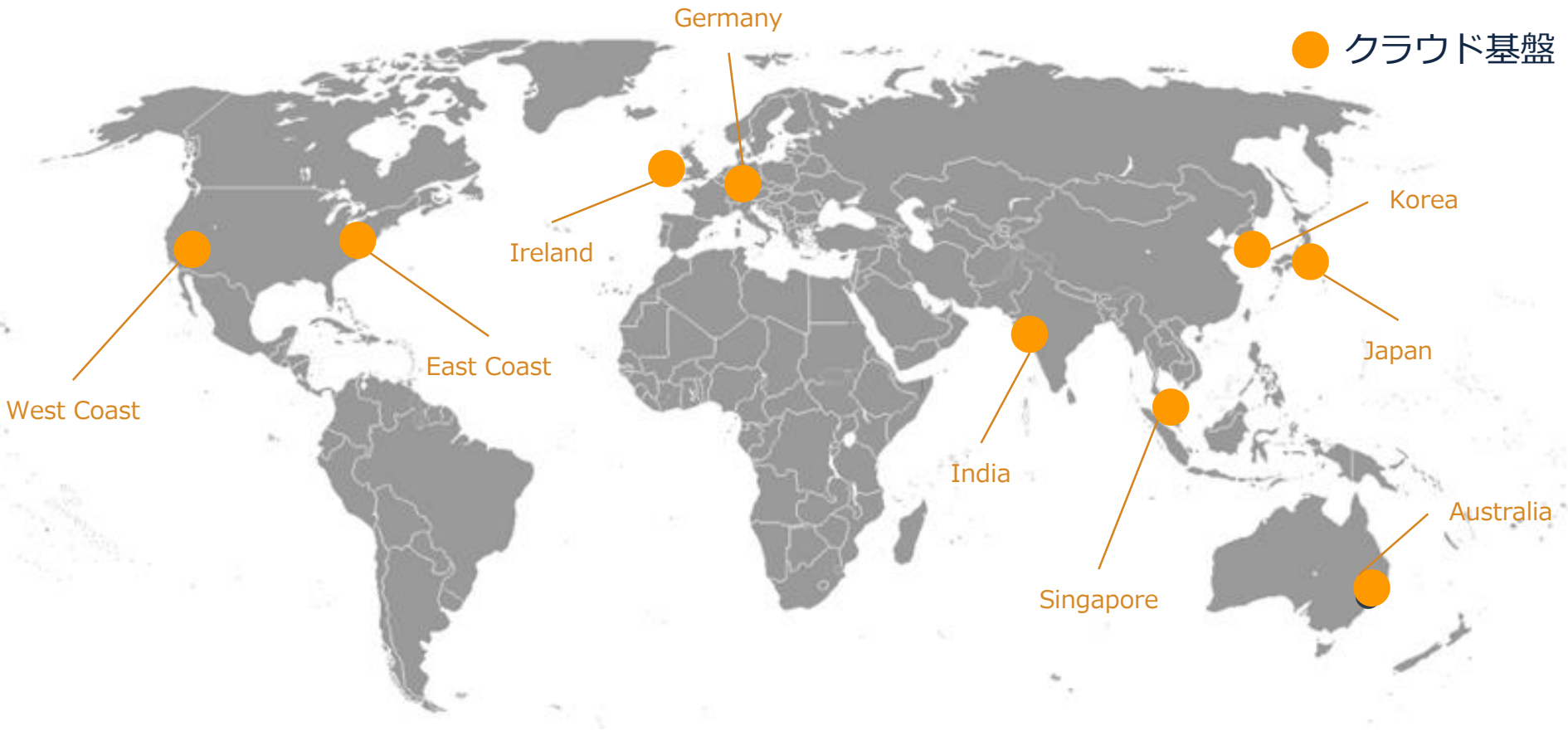
■ **管理者の視点**
- クラウド型サービスのため環境構築不要
- サービスアップデート作業不要（Menlo社が全て実施）
- プロキシとして動作するため、既存の設定変更も容易

■ **ユーザの視点**
- クライアントソフトが不要（SSL通信に対応するため証明書のインポートは必要）
- マルチOS、マルチブラウザに対応
- 使用感は従来のWebブラウジングとほとんど変わらない



システムのスケーラビリティ

- グローバルスケールのフェイルオーバー機能
- サービスアップデート時のゼロダウンタイム保証
- ユーザ数・トラフィック量に応じたオートスケール機能
- トラフィックのバーストに対応（全リージョン）



その他の機能

機能	概要
ドキュメントファイル無害化	Word、Excel、PowerPoint、Ichitaro、PDF等のドキュメントを無害化し、ブラウザ上でファイルの内容を表示します。無害化した表示情報をPDFに変換し、ダウンロードすることも可能です。 （オリジナルファイルのダウンロードも可）
フィルタリング	Menlo社が保有する辞書にもとづくWebサイトのカテゴリや接続先ドメインの情報を指定しアクセスをブロックします。
出口対策	アウトバウンドの通信に対して、許可するアプリケーションを限定することで、マルウェアとC&Cサーバとの通信をブロックします。
フィッシング対策	Menlo社が保有する辞書にもとづくWebサイトのカテゴリや接続先ドメインを指定することでフォームを無効化し、Webサイトからの情報アップロードを制御します。
ファイルダウンロード制御	Word等のドキュメントファイルをはじめ、実行形式のファイルや圧縮ファイルをファイルタイプごとにダウンロード制御が可能です。
ファイルアップロード制御	ファイル選択ダイアログの表示を制限することでファイルアップロードを制御します。
ウイルス対策(オプション)	シグネチャベース、サンドボックスによるウイルスチェックを行いブロックします。（本オプションは別途費用が発生します）

まとめ

課題	Menlo Securityの対応
すり抜け、誤検知・過検知	検知・判断をせず、全てのコンテンツを無害化することで安全なWebアクセスを実現
運用負荷の増大	検知をしないという新しいアプローチにより従来のログやアラートに頼った運用を軽減
利便性、業務効率の低下	無害化によりWeb閲覧におけるマルウェア感染リスクを排除し、URLフィルタリングによる必要以上の制限を緩和

目　次

NRI SECURE

NRI SecureTechnologies, Ltd.

www.nri-secure.co.jp