WebALARM™

～Webサイト改ざん防止のセキュリティパッケージのご紹介～

2013年7月10日

イーロックジャパン株式会社

35分間

本日の目的。それはWebALARMを知る

1.会社案内
2.製品紹介& FAQ

Who is e-Lock?

マレーシア発のセキュリティ会社

e-Lock Corporation Sdn Bhd

CEO: Dr.Ken Leong
設　立：　1996年設立
所在地：　マレーシア　クアラルンプール
資本金：　2億円

イーロックジャパン株式会社

代表取締役社長：秦　基嘉
設　立：　2006年設立
所在地：　102-0083東京都千代田区麹町 3-12-7

マレーシア発のセキュリティ会社

e-Lock Corporation Sdn Bhd

CEO: Dr Kep Leong
設　立　1996年設立
所在地　マレーシア　クアラルンプール
資本金　非公開

Solution Development & Customization
セキュリティ製品の開発

Security Consulting & Training
セキュリティコンサルティング

Penetration/ Security Testing
脆弱性診断

Enterprise Solution Integration
システムインテグレータ

イーロックジャパン(株)

代表取締役社長　茅　嘉泉
設　立　2006年設立
所在地　102-0083東京都千代田区
麹町 3-12-7

Permodalan Nasional Berhad

国営投資会社 *ペルモダラン・ナショナル*「PNB」
1978年3月17日設立

創設者：Tengku Razaleigh Hamzah (称号：Tan Sri)

1976~1984	：元マレーシア財務大臣
1984~1987	：元経済産業大臣
世界銀行	：元会長
アジア開発銀行	：元会長
イスラム開発銀行	：元会長
ペトロナス（石油会社）	：元会長

Permodalan Nasional Berhad

<http://www.pnb.com.my/>

"In year 2000, Permodalan Nasional Berhad (PNB) invested in e-Lock with their strong confidence in e-Lock's R&D achievements and global growth potential."

Sigmaline Technologies Sdn. Bhd.

2003年　物理セキュリティ専門の子会社
シグマライン･テクノロジーズを設立

<Business Focus>

- Building Automation & Energy Management System
- About Automation & Networking System
- CCTV Application & Video Surveillance Security System
- Access Control System & Management
- Vehicle Parking System & Cash Collection Management
- Structured Cabling & Media Management System
- Public Addressable System & Acoustical Design
- Intrusion Alarm System & Security Monitoring Services
- Perimeter Protection & Compound Security
- Radio Frequency Identification & Tracking System
- Satellite Master Antenna Television

2001年、日本へ

◆日本進出のきっかけ

2000年 PIKON ICTアワードを受賞

2000年　WebALARM

2007年　TheGRID

ビジネスパートナー

◆ビジネスパートナー

IIJ Internet Initiative Japan

Next IT Inc.

NISSHO CLOUD INITIATIVE

SoftBank ソフトバンクBB株式会社

Networld

VALUE Drivers

ENERGIZE

Suzuyo shinwart

SBI Trade Win Tech

S-CUBE CAPITAL ADVISORS エスキューブ・キャピタル・アドバイザーズ株式会社

◆参加・加盟団体

JAPAN CARD DATA SECURITY CONSORTIUM 日本カード情報セキュリティ協議会 安全なカード社会の実現をめざして

JNSA Japan Network Security Association

一般社団法人 日本CISO協会 Japan CISO Association

順不同

ASEAN地域から世界へ

イーロック社は、マレーシア・クアラルンプールの本社を中心に、日本・中国・東南アジア・南アフリカ・ アメリカ合衆国と、その高いITセキュリティ技術とビジネスを世界的に展開しています。

イーロック社は、ワンストッププロバイダーとして、セキュリティに対するコンサルティングやサポートサービスを提供することにより、デジタル環境の分野で真の可能性を拡大・追求しております。

なぜ今WebALARMが必要とされているのか

なぜ今WebALARMが必要とされているのか

約 1000 件

2 ヶ月

JP Certコーディネーション6/7発表

質問
あなたはサイバー攻撃を受けた時どれぐらいで気付きますか？

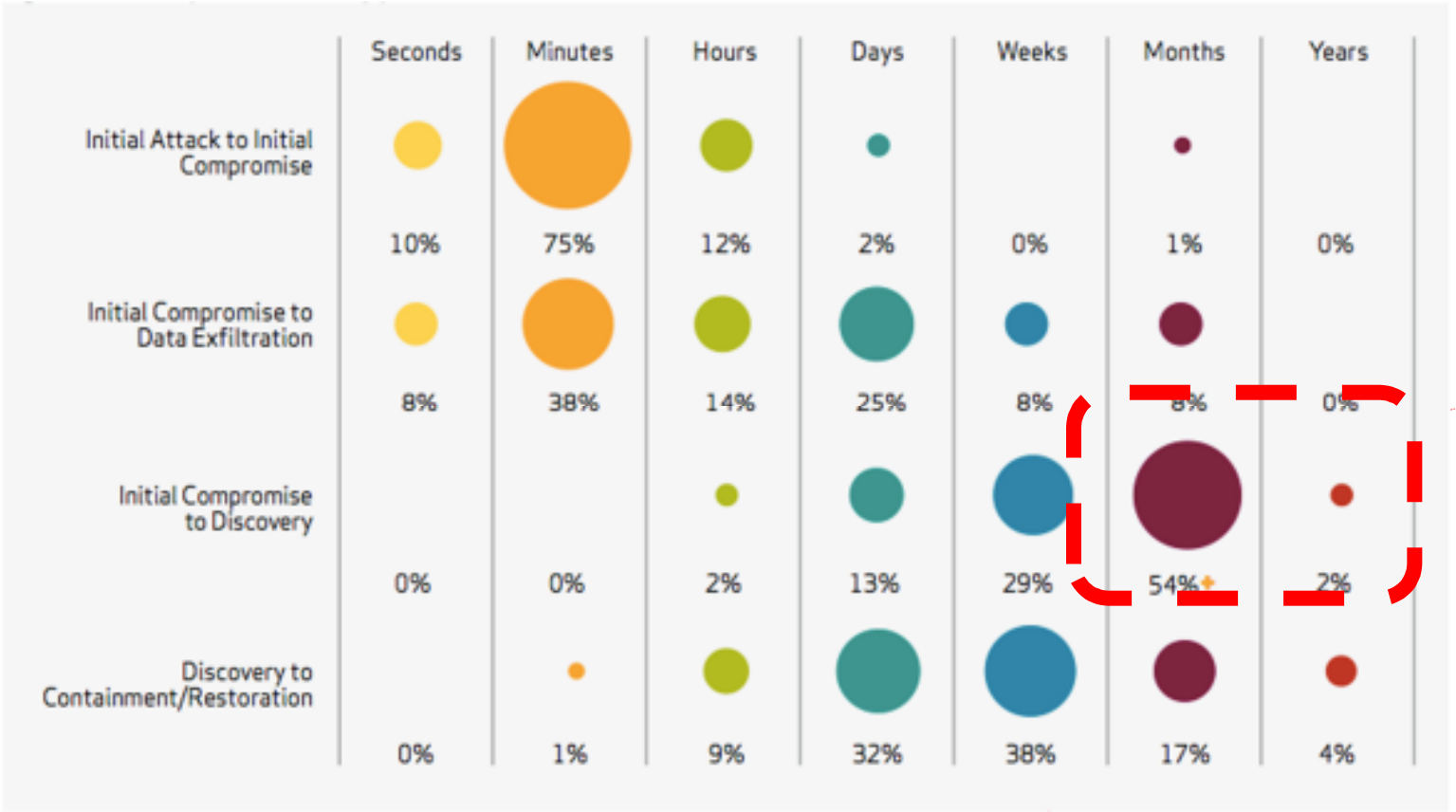
WebALARMの必要性と悲しい現実

悲しい現実：
担当者が気付くまでに
意外に時間がかかること

担当者が気付くまでに意外に時間がかかること

5割以上の担当者が、攻撃を「受けていた」ことに気付くのに1ヶ月以上の期間を要した。
その9割が、第三者による発見と報告されている。

<発見に至るまでの期間>

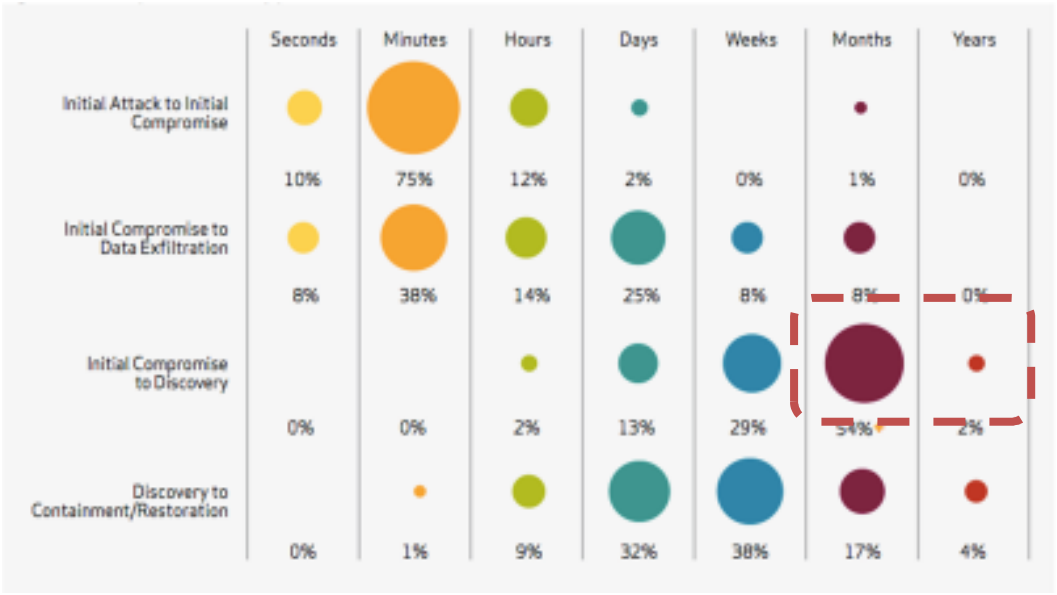


Verizon, 2012, *"Timespan of Events"*, 2012 DATA BREACH INVESTIGATIONS REPORT p.63

担当者が気付くまでに意外に時間がかかること

5割以上の担当者が、攻撃を「受けていた」ことに気付くのに1ヶ月以上の期間を要した。
その9割が、第三者による発見と報告されている。

<発見に至るまでの期間>



Verizon, 2012, *"Timespan of Events"*, 2012 DATA BREACH INVESTIGATIONS REPORT p.63

＜2012年に報道された実例の一部＞

30日間
2012/6/7　発表
某県民参加型地域情報発信サイトが
約1ヶ月間もの間改ざん被害

23日間
2012/5/17報道(Security Next)
某大手企業がウェブサイト改ざん、閲覧でマルウェア感染のおそれ」 23日間ものあいだ改ざんされる
「被害者」から「加害者」へ

18日間
2012/5/29　報道 (Scan NetSecurity)
某テレビ通販サイトで会員情報が
不具合により表示(テレビ東京ダイレクト)

1ヶ月間
2012/4/18　報道 (Scan NetSecurity)
某大一サイトの一部が改ざん、閲覧でウイルス感染のおそれ　復旧までに1ヶ月

2日間
2012/7/13報道 (西日本新聞)
某カードゲームWebサイトが改ざん
～閲覧者にウイルスが送りつけられる状態に

2日間
2012/5/18　報道 (Security Next)
某埋蔵文化センターのサイトが改ざん
～閲覧でウイルス感染のおそれ

1.5日間
2012/5/23　報道 (Security Next)
某市のサイトが2度にわたり改ざん

とりかえしのつかない企業の信用失墜

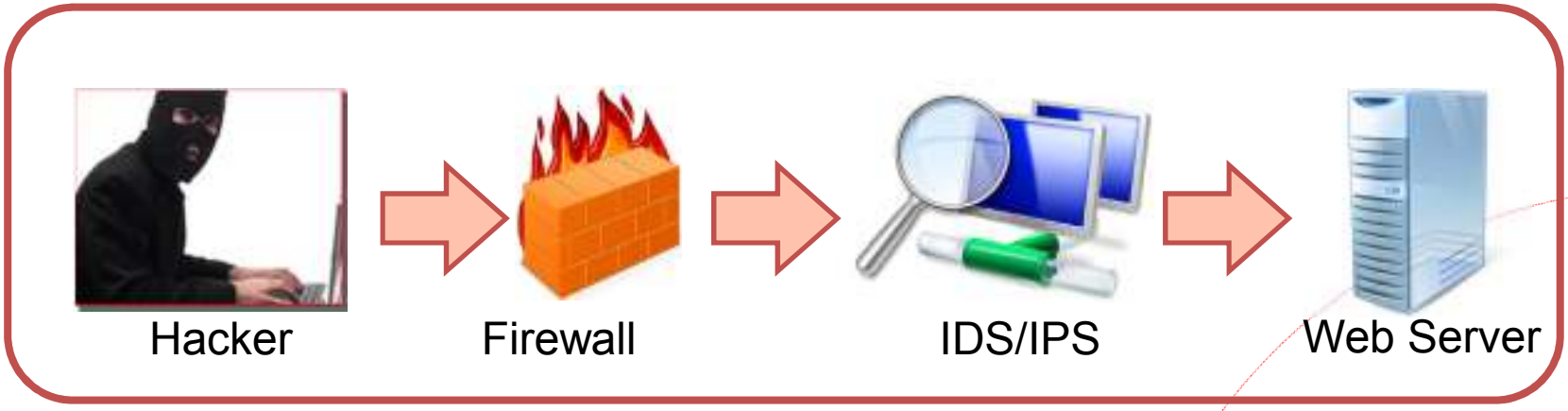
悲しい現実:

どんなにセキュリティ対策しても100%は防げない

どんなにセキュリティ対策しても100%は防げない

ご存知の通り、セキュリティは「100%」
サイバー攻撃を防げるわけではありません。

セキュリティ対策としてFirewall、侵入検知、Webフィルタリング、Proxyサーバ等、
「入り口対策」のセキュリティ強化をしている団体・企業が、実際にWebサイト改ざん被害をうけています。



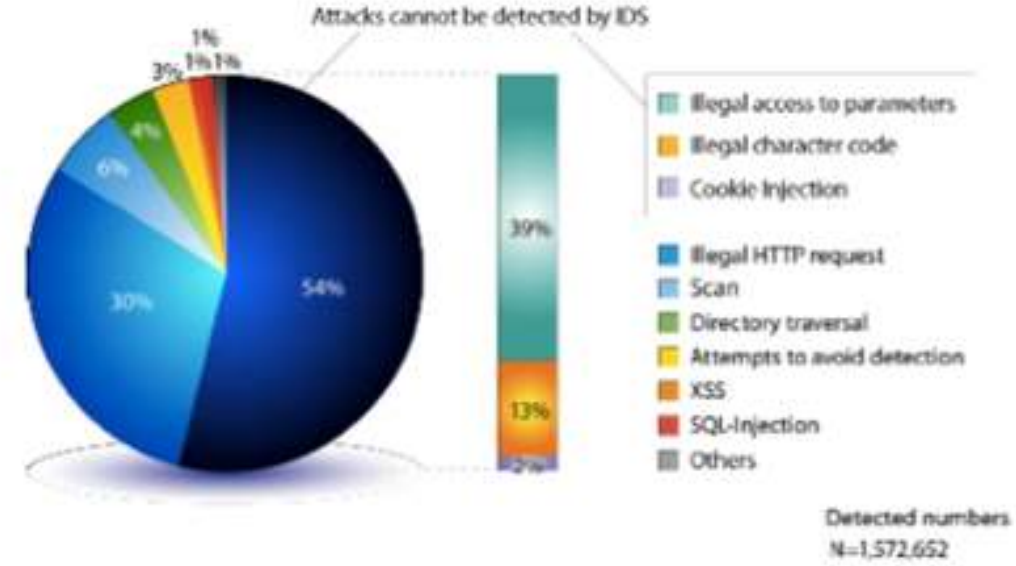
Verizonの調査によると、昨今のサイバー攻撃は、全体で約9割以上、
大手企業団体においては約9割弱が外部からの攻撃です。

従来の「入口対策」と呼ばれるセキュリティは必然とされ
認知度も高く、対策をとられている企業・団体も多い

どんなにセキュリティ対策しても100%は防げない

IDS/IPSで、アプリケーション層への全ての攻撃を防ぐのは不可能。

NRIテクノロジー社は、1,572,652件のサイバー攻撃を調査し、IDS/IPSはその54%である約 **849,230件** を検知できなかったと報告しています。



"Cyber Security Trend –Annual Review 2011", 2012, NRI SecureTechnologies, Ltd.

どんなにセキュリティ対策しても100%は防げない

WAFですら防げないサイバー攻撃がある。

WAF=Web Application Firewallの略

ヨーロッパ非営利組織OWASP[1]の発表によると独自の二つの攻撃ツール(WafW00f・WafFun)を使用することにより、多くのWAF製品のホワイトリスト・ブラックリストモードの動作を悪用し、WAFのブロックを回避することを証明した。

Researchers Hack Web Application Firewalls

OWASP Europe presentation demonstrates tools that fingerprint the brand of WAF, as well as bypass it altogether

May 13, 2009 | 03:24 PM | 0 Comments

By Kelly Jackson Higgins

A pair of researchers at the OWASP Europe 2009 conference on Wednesday showed how some Web application firewalls (WAFs) are prone to attack.

Wendel Henrique, a member of SpiderLabs (Trustwave's advanced security team), and Sandro Gauci, founder and CSO for EnableSecurity, also found some WAFs vulnerable to the same types of exploits they are supposed to protect Web apps from, such as cross-site scripting (XSS) attacks.

The researchers used a tool they developed, called WafW00f, to detect and fingerprint the presence -- and in some cases, the brand -- of a WAF running in front of a Web application. A second tool created by Henrique and Gauci, called WafFun, let them exploit and bypass WAFs running in blacklisting and whitelisting modes. With a combination of WafW00f and WafFun, the researchers are able to execute attacks on the WAF invisibly so they can successfully hack the Web-facing application sitting behind it.

"If an attacker knows what product and version, it's easy to exploit it. One of the things [WAF] vendors claim is that they [operate] in stealth [mode]," Henrique says. "But in practice, they have a lot of different behaviors that they create...and you can use those behaviors to identify what WAF is in place."

Other researchers previously have demonstrated fingerprinting and bypassing intrusion-detection systems/intrusion-prevention systems, as well as how signature-based WAFs are susceptible to SQL injection attacks.

Mark Kraynak, vice president of marketing for Imperva, says Henrique and Gauci's research is not all that new, including their work on signature evasion, which Imperva has researched. "A lot of what they are saying is not new," he says. "Part of the founding premise of why you need a WAF versus a signature engine...is that you can evade a weak signature engine."

Products that use only signatures -- without other features like normalization and encoding/decoding -- are not true WAFs, he says. "Signature-only WAFs are not going to do it," he says.

Meanwhile, Henrique says he and Gauci are working with several WAF vendors to fix vulnerabilities in their products, including Armorlogic, which has since patched for its WAF bug. They also will release WafW00F, which detects more than 20 different WAFs, by Friday, and WafFun within two weeks.

"A WAF can help, for sure," Henrique says. But even more importantly, he says, organizations must protect their Web apps by writing better code and regularly testing their applications. "Training developers, doing code certification review, and testing Web apps are much more useful," he says. "The problem is we found so many WAF products have really bad design flaws that allowed us to directly compromise [them]."

And while adding a whitelisting Web traffic is a stronger model than a blacklist/signature-only approach, he says, it's not necessarily realistic for large Websites. "It's not easy to put in place a WAF with a positive [whitelisting] model at a company with huge Websites," he says. "In general, companies will use a negative [blacklisting] model," which can leave their WAF open to attack.

"Researchers Hack Web Application Firewalls" May 13, 2009 by Kelly Jackson Higgins
<http://www.darkreading.com/security/application-security/217400819/index.html>

1) ヨーロッパ非営利組織OWASP (Open Web Application Security Project)

結果

入り口対策セキュリティ製品

だけではなく

＋

最後の砦として

WebALARMが

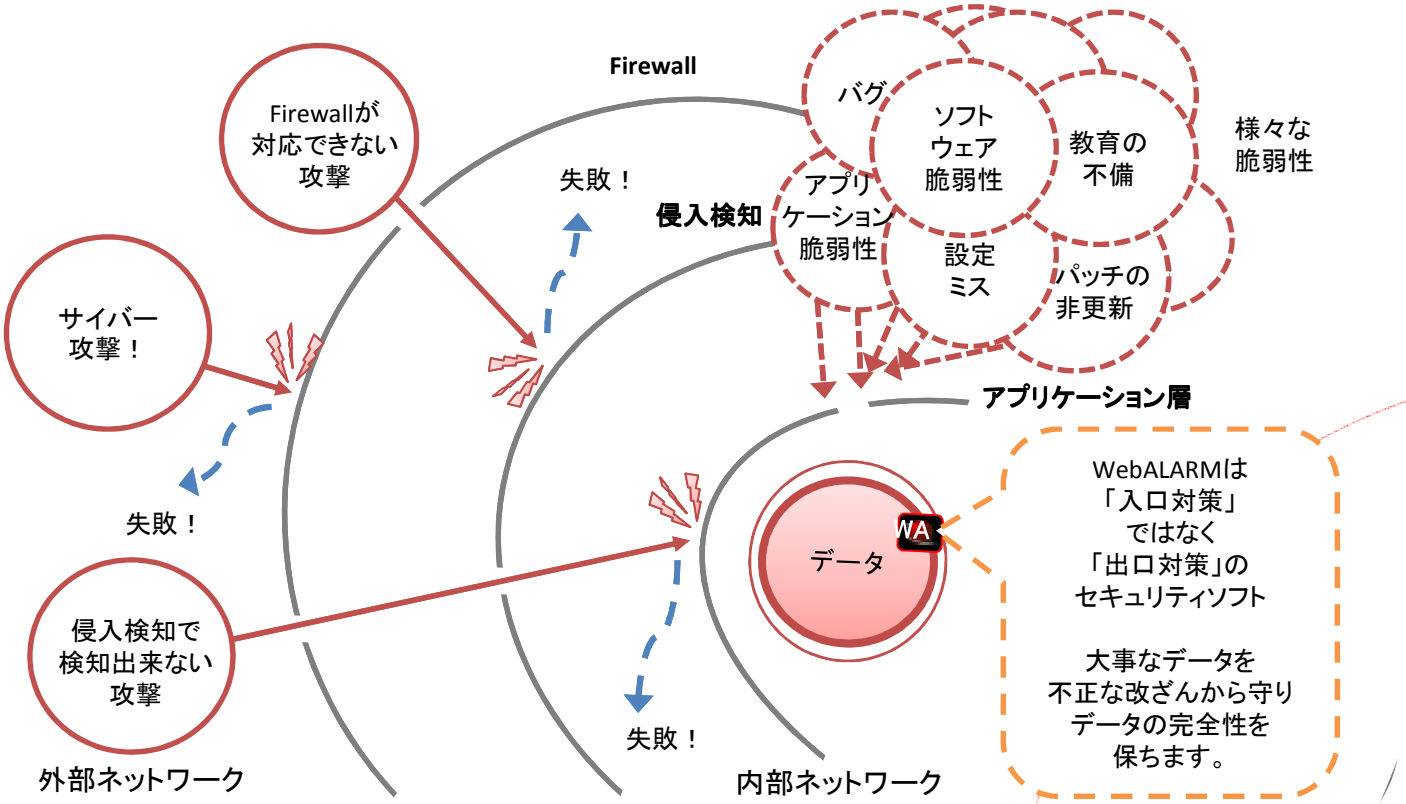
必要になってきている

WebALARMの必要性

「入り口対策」だけでなく、「出口対策」におけるセキュリティ強化を早急に

WebALARMはサーバ上にある重要なデータを改ざんから防ぎます。

（IPA 2011年11月発表「新しいタイプの攻撃」）



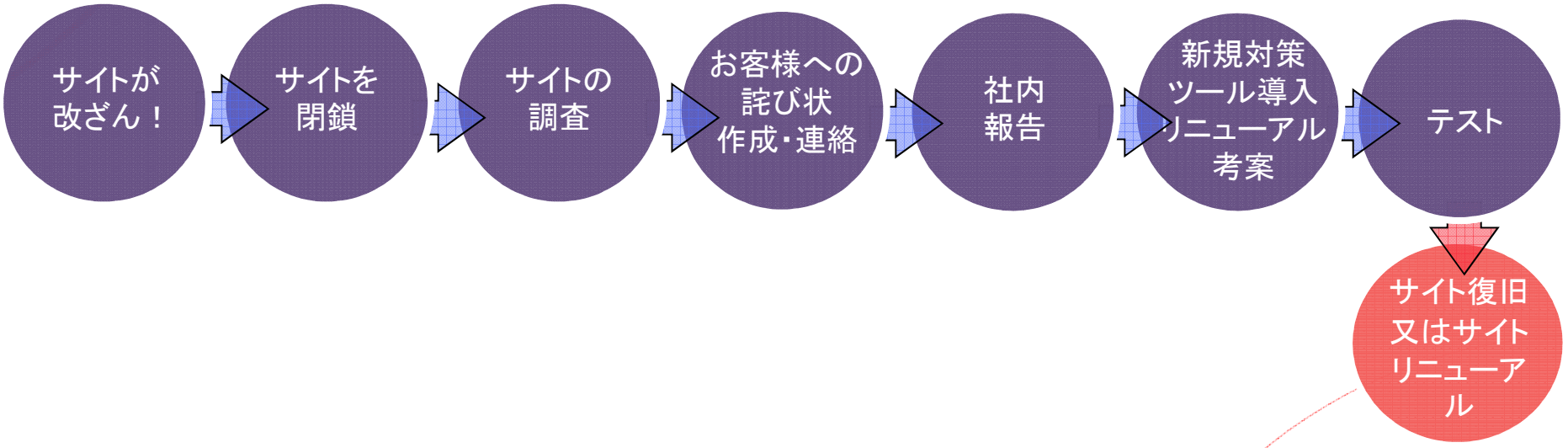
WebALARMのメリット。

自動復帰機能。

マニュアルによる復帰作業がいらない。

WebALARMのメリット

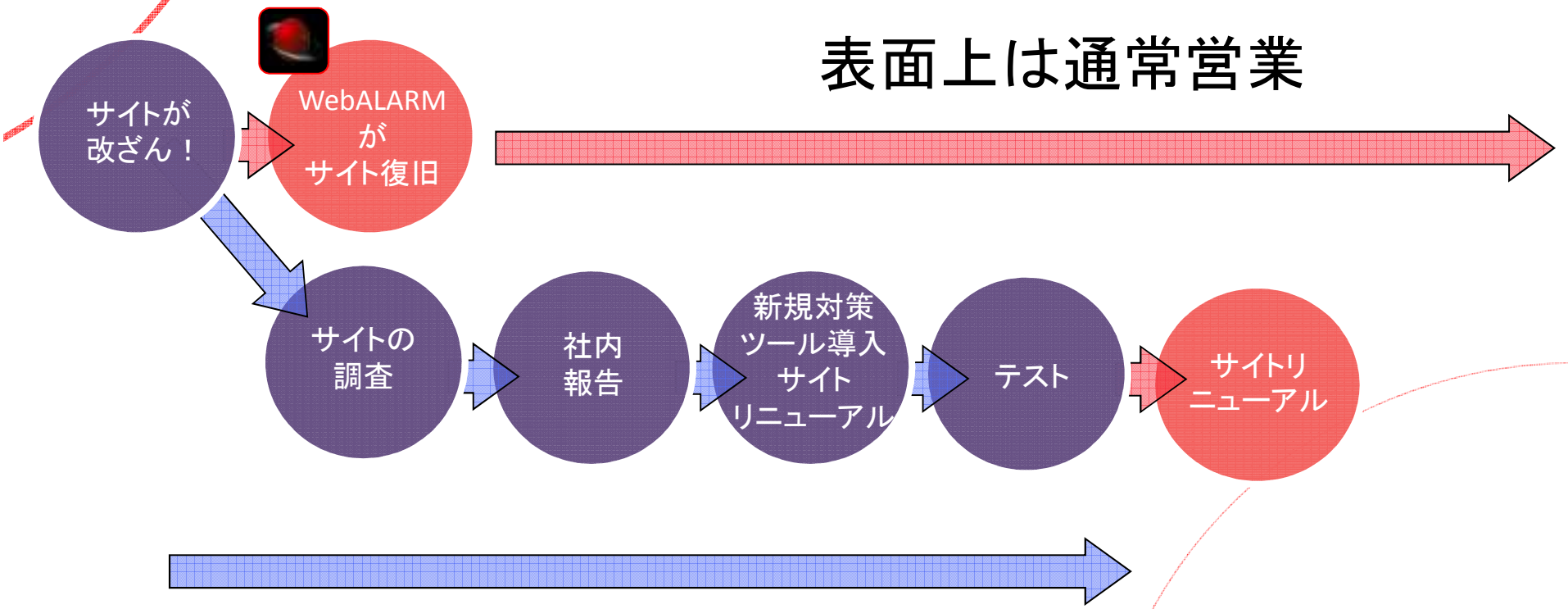
通常の対策



改ざんされて、復旧までの時間

WebALARMのメリット

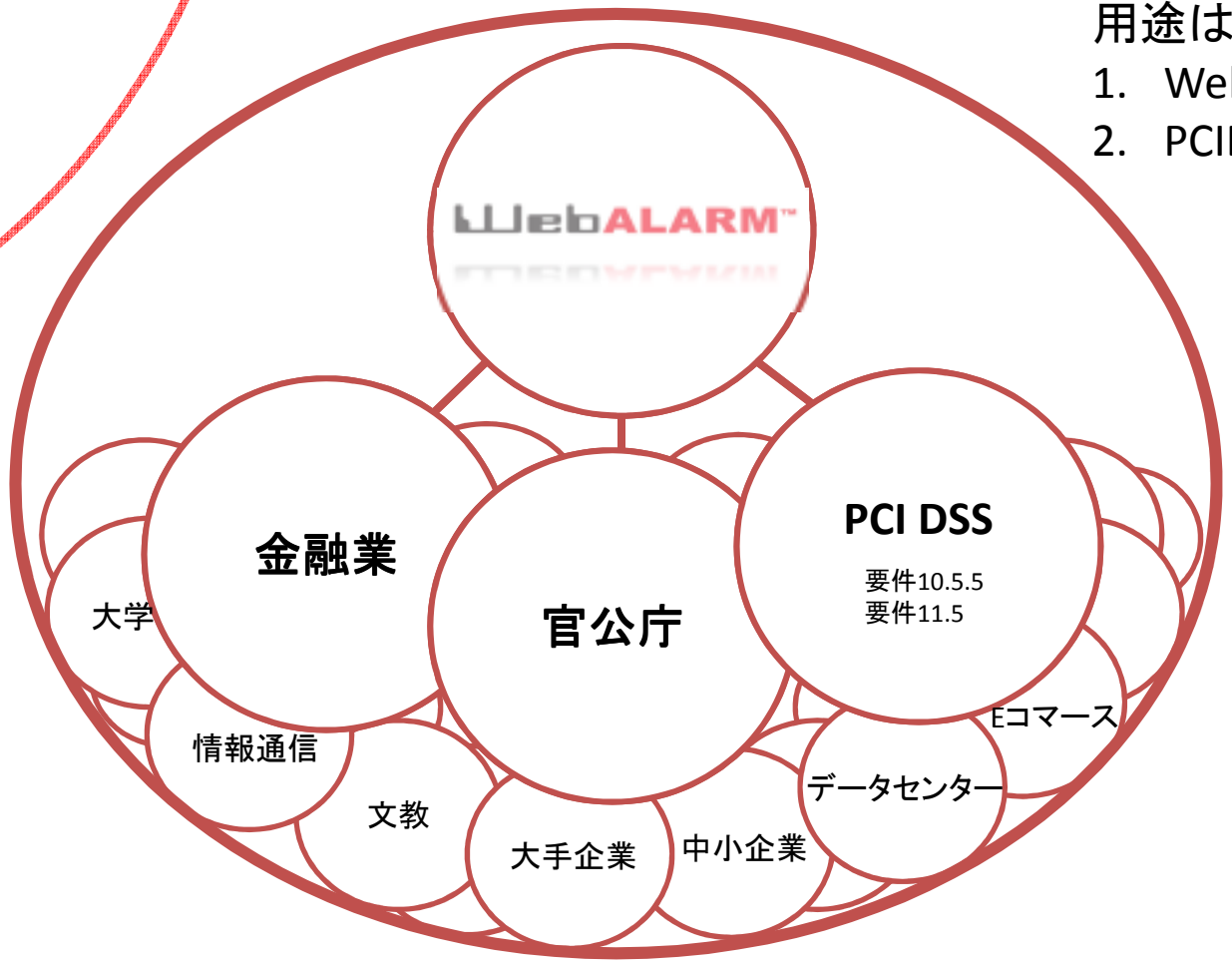
WebALARMがあった場合



改ざんされて、復旧までの時間

WebALARMの
利用と用途の事例

WebALARM利用と用途の事例



用途は大きく分けて2つ

1. Webサイト改ざん対策
2. PCIDSS　ファイル整合性の確保

PCI DSS

日本カード情報セキュリティ協議会
2012年5月31日

2013年3月末　ネット通販企業
2018年3月末　対面加盟店企業
(デパート等)

JCA「クレジットカード情報セキュリティフォーラム」にてクレジット協会へPCI DSSへの準拠を公式に要請

- WebALARMは日本でPCI DSSを取得したシルバーレイクジャパン株式会社にご利用頂いております。
- 国内では12年間の実績があり、導入したほぼ100%のお客様に継続してご利用頂いております。

WebALARM利用と用途の事例

下記2点の要件に対応しております。

要件10.5.5	**ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータを追加する場合は警告を発生させない）。**
要件11.5	ファイル整合性監視ツールを導入して重要なシステムファイル、構成ファイル、またはコンテンツファイルの不正な変更を担当者に警告し、重要なファイルの比較を少なくとも週に一度実行するようにソフトウェアを構成する。

WebALARMを活用したPCI DSSコンプライアンスへの取り組み
シルバーレイクジャパン株式会社　様

Case Study 1

「PCI DSSを準拠するために」

今回は、シルバーレイクジャパン株式会社、代表取締役執行役員CEOである根田　秀人志氏にWebALARM導入の経緯、またクレジットカードシステムアウトソーシングをする上で必要不可欠である「セキュリティ」にかける想いをインタビューさせて頂きました。

「決めては中央銀行のセキュリティ監査を努めていたこと」

PCI DSS 要件10.5.5及び要件11.5へWebALARMを選定した理由について根田氏は、WebALARMを選定した理由として、下記の3点を挙げている。

◆金融業界での実績

「一つ目の大きな理由は、シルバーレイク本社のあるマレーシアの中央銀行のセキュリティ監査を受け持っているのが、このWebALARMを開発したイーロック社であったこと。」 イーロック社は、マレーシアの中央銀行を始めとする、多くの金融業界のセキュリティ監査及び、WebALARMの導入実績があり、また日本国内でも官公庁、銀行等金融業界での導入実績があったことが、クレジットカードシステムアウトソーシングサービスを行うシルバーレイクジャパンのお客様に「安心」して頂ける製品だと確信したからだという。

◆優れた機能

「二つ目の理由は、機能が優れていたこと。」 WebALARMは優れた検知機能をもっている製品です。日本国内をみても、検知のみを行う他製品とは違い、改ざんや人為的ミスの更新があった場合、元の状態へ瞬時に戻すリカバリ機能もついています。

◆リーズナブルな価格

「三つ目の理由は価格が機能に対しリーズナブルであること。」を挙げた。上記の機能ををを踏まえた上での、この価格は他社製品と比べて一桁違う値段であることは大きな魅力であると語る。

シルバーレイクジャパン株式会社
東京都中央区新川1-17-24
新川中央ビル5F
設立：平成9年5月26日
Tel: 03-3523-2309
<http://www.silverlake.co.jp/>

<導入製品>
WebALARM Professional
<導入時期>
2009年
<導入用途>
PCI DSS 要件10.5.5及び要件11.5への対応

クレジットカード企業向けにシステム・業務の殆どを一括して受託できる本格的なサードパーティプロフェッサです。

シルバーレイクジャパン株式会社
代表取締役
執行役員兼CEO
根田　秀人志　氏

「お客様の情報が漏洩することはあってはならないこと」

2008年当時、米国で顧客情報漏洩大型事件が多発し、PCI DSSに準拠することが迅速に広がった。米国系銀行に長年勤めてきた根田氏には、今後、日本の銀行・クレジットカード会社がターゲットにされることは目に見えていたと当時を語る。「お客様の情報が漏洩することは、あってはならない」 このお客様を第一に思う信念から、PCI DSSの準拠を目指し、わずか半年間でQSAであるBSIグループジャパン株式会社（英国規格協会）[1]の審査を受け完全準拠を達成したのである。

WebALARMの製品紹介

- 製品機能概要
- 管理画面
- 機能
- 構成
- 製品ラインナップと価格
- FAQ
- 製品・見積のお問い合わせ先

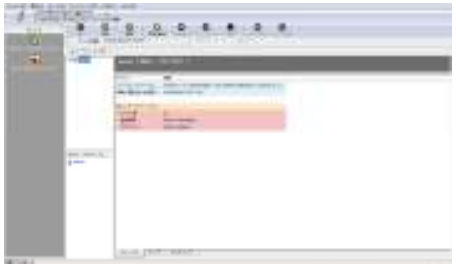
WebALARM製品概要

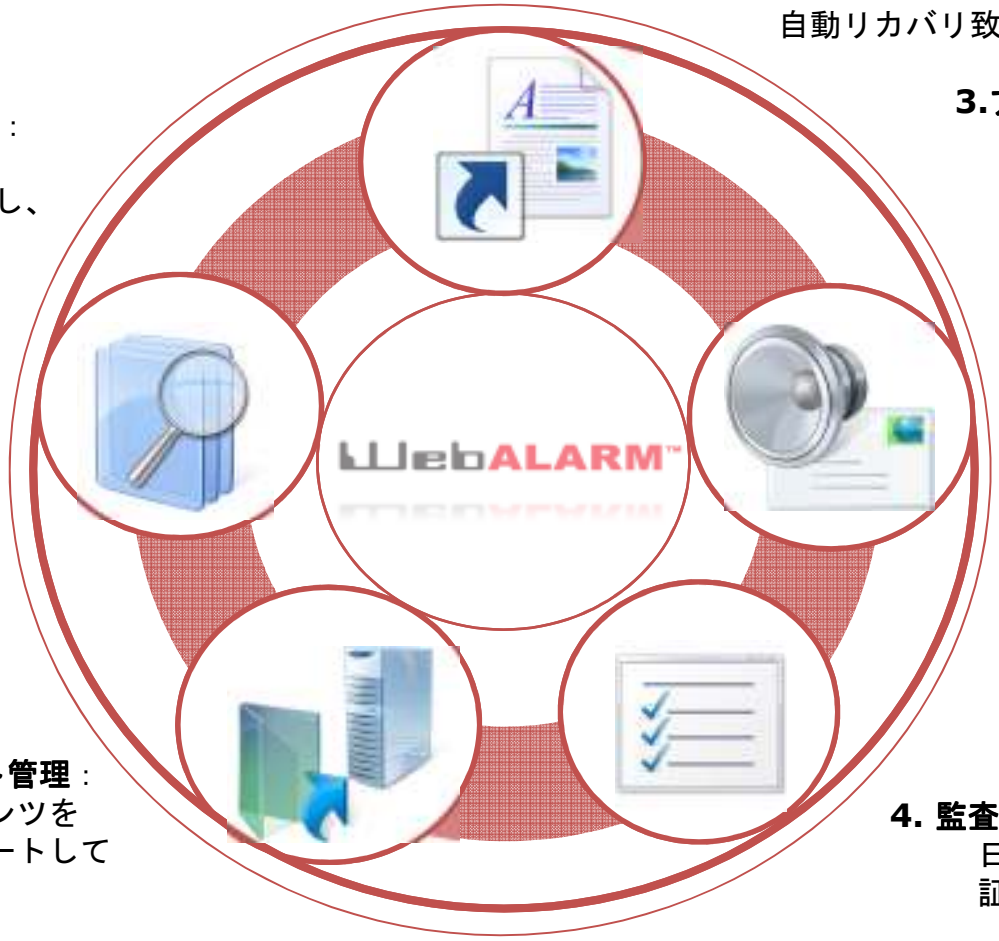
WebALARMは一覧の機能が
一つのパッケージでご利用頂けます！

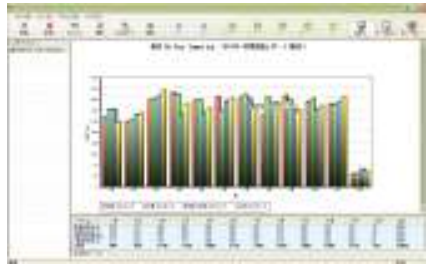
2.自動リカバリ: 改ざんがあった場合
瞬時に、バックアップより
自動リカバリ致します。

1.モニタリング(監視)：
SHA1の暗号化
アルゴリズムを使用し、
「1bit」の改ざんも
検知致します。

3.アラート機能：
3つのアラート機能を
ご利用頂けます。
・メール
・管理画面でのアラート
・SNMP







5. データアップデート管理：
データ・コンテンツを
簡単にアップデートして
頂ける機能です。

4. 監査と証拠保全：
日毎、イベント毎のログを
証拠として残します。

管理画面

機能:モニタリング(監視)

SHA1の暗号化アルゴリズムを使用し、「1bit」の改ざんも検知致します。

正確なデータ保全の監視

- ファイルとフォルダーの削除
- 新しいファイルの追加
- コンテンツの改ざん
- 権限の変更

削除

追加

改ざん

属性の変更

機能:自動リカバリ

改ざんがあった場合瞬時に、バックアップより自動リカバリ致します。

不測の事態にも、即リカバリ

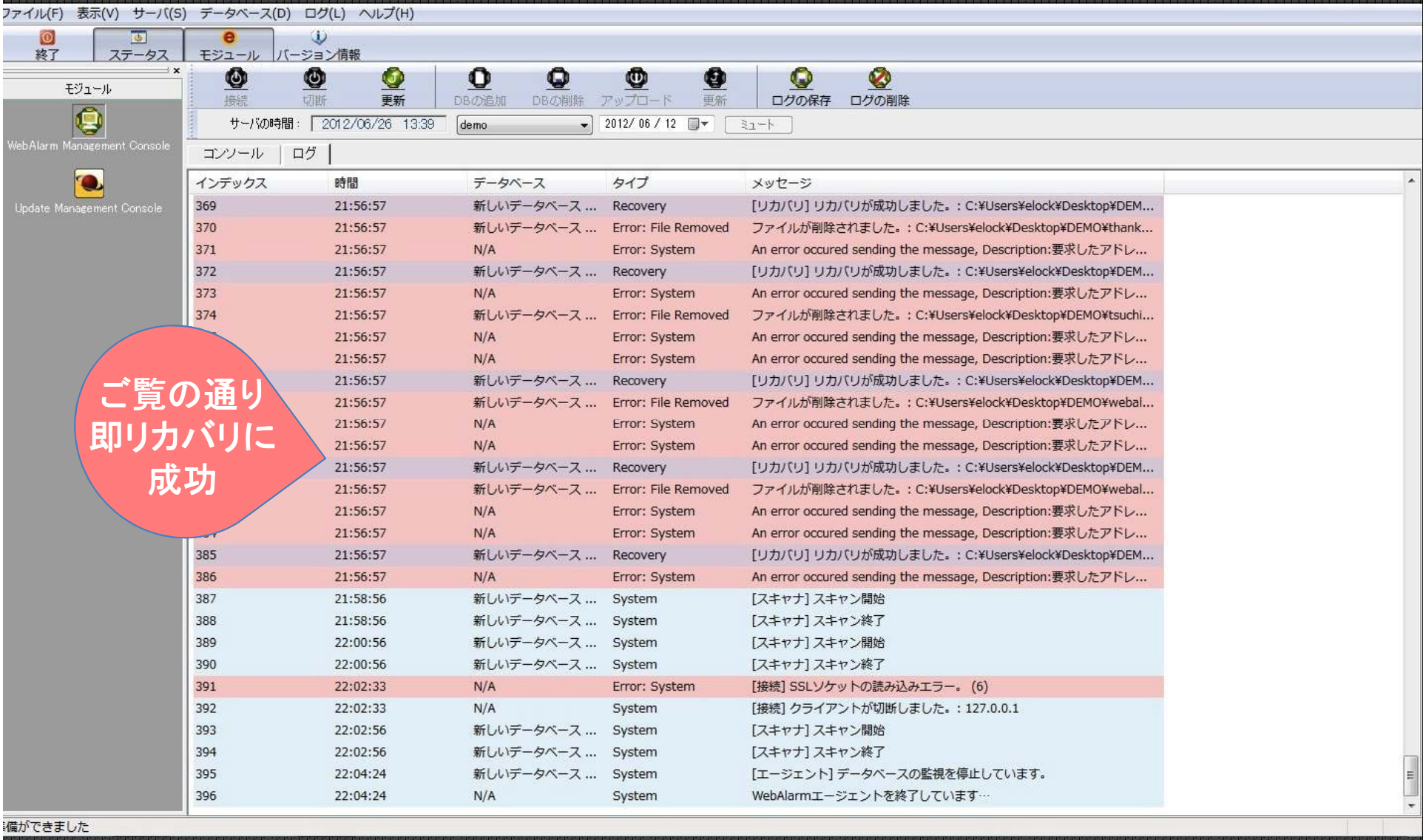
- 全自動でバックアップからリカバリ
  (automatic backup during setup and updates)
- 別のテンプレートに差し替え （工事中など）
- カスタムプログラムなどの実行
  (e.g. custom recovery script, anti-virus scan)

全自動リカバリ

代替ページ表示

カスタムリカバリ

機能：自動リカバリ



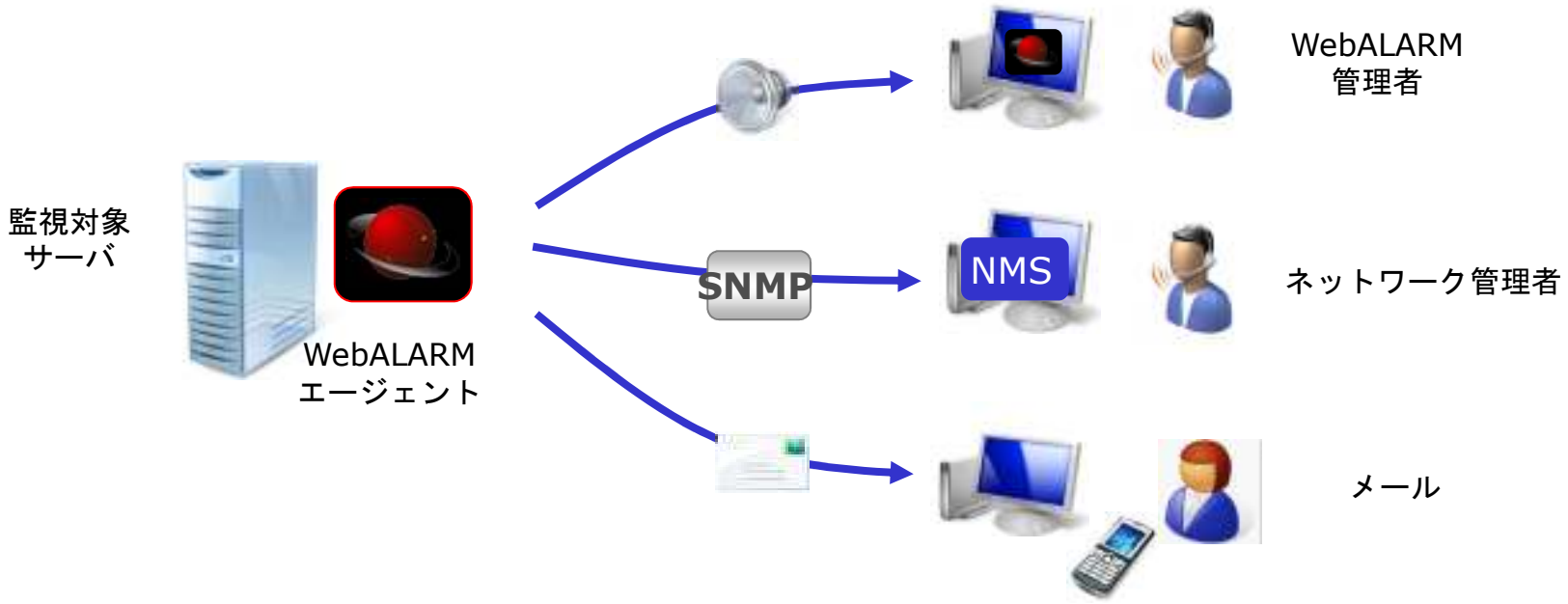
ご覧の通り
即リカバリに
成功

機能:アラート機能

3つのアラート機能をご利用頂けます。

データを改変されたときは、管理者へ即時警報を送ります。

- コンソールアラート(画面上と音)
- SNMP にも対応
- Email での警告(複数の宛先設定可能)



機能:ログ　監査と証拠保全

日毎、イベント毎のログを証拠として残します。

下記について監視出来ます。

- データの改ざん
- 勝手なアップデート
- 管理者の動向

調査のための証拠保全

- 改ざんされたファイルを隔離・保存

日ごとのレポート &時間単位のレポート

イベントごと

対象ファイルのファイルパス

日付毎に検索可能なログ

不正に追加されたファイルはコピーを保存
(Windows対応)

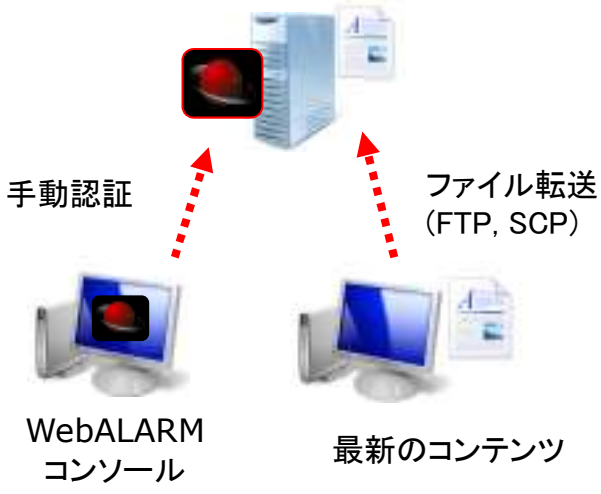
機能：データアップデート管理

データ・コンテンツを簡単にアップデートして頂ける機能です

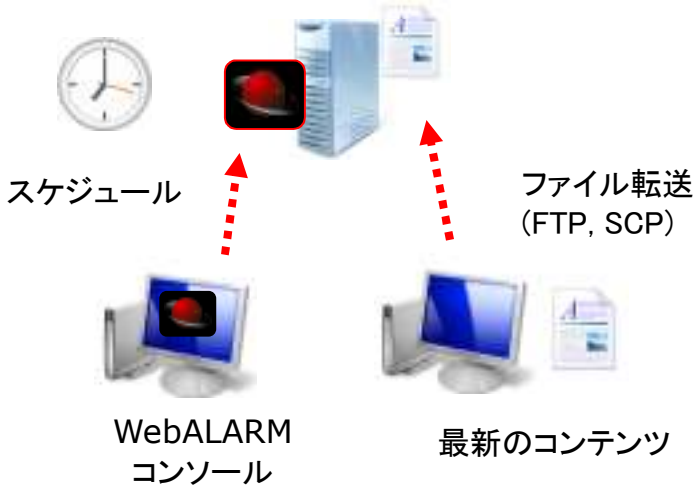
最新のコンテンツを、WebALARM管理者によって

許可された時間にアップデートを行う方法です。

管理端末にて**アップロードボタンを押下**する必要があります。



手動でのアップデート



スケジュール機能もあります

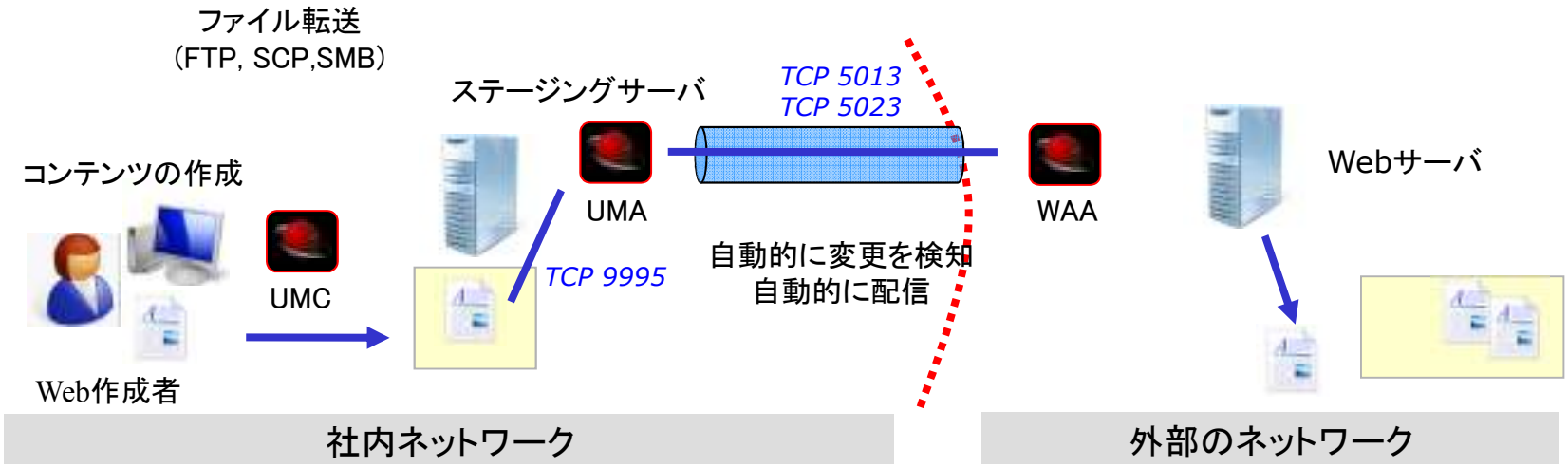
機能：データアップデート管理

UMAという配信用サーバを利用した運用が可能です。

WebALARM AgentはUpdate Management Agent (UMA)からの
変更のみ受け入れます。

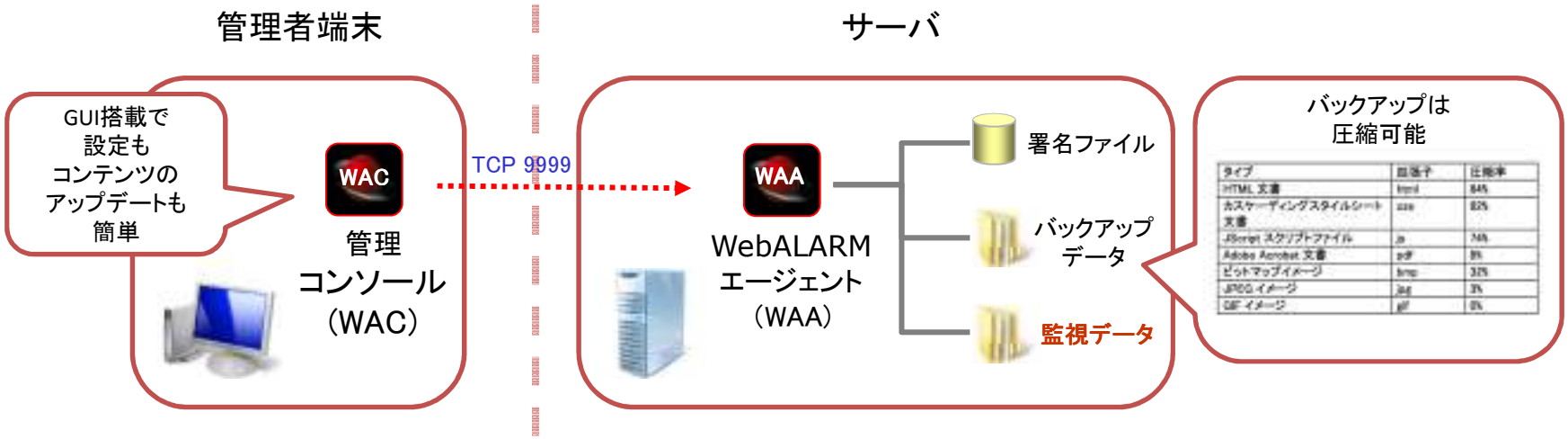
The WebALARM UMA の動き:

- ステージングフォルダの**変化を監視**します。
- ステージングフォルダに変化があれば、**ライブフォルダへコピー**します。



構成

WebALARMはたった2つのモジュールで構成されています。(Standard及びPremium)



WAC

- WAA を管理するグラフィック管理インターフェース(GUI)は日本語化済み

WAA

- Windows とUNIX・Linux に対応
- モニタリングと回復、アラート機能
- バックアップを作成します

さらに！

UMC UMA

配信用モジュール

配信用モジュールをご利用頂くことで、自動アップデート(ミラーリング)機能をお使い頂くことができます。(Professional) →25ページを参照

監視可能なファイル及び対象OS

監視可能なファイル

- ウェブコンテンツ: HTML, XML, CSS, ...
- マルチメディア: JPG, GIF, PNG, WMV, MPG, AVI, SWF, ...
- ウェブアプリ: PHP, JSP, ASP, CGI, PL, C++, ...
- プログラムのバイナリ: EXE, DLL, BIN, OCX, LIB, ...
- スクリプト: BAT, SH, SQL, ...
- ドキュメント: DOC, XLS, PPT, PDF, TXT, CSV, ...
- 設定: CFG, INF, CF, ...
- UNIX 特殊ファイル: デバイスノード, シンボリックリンク
- 共有ネットワークファイル: Windows 共有, Samba, NFS, ...

監視出来ないファイル

- OSスワップファイル／仮想記憶
- データベース(インデックス及びデータファイル)

対象OS

WebALARM Agent (WAA)

- Windows 2000, XP, Server 2003, Vista, 7, Server 2008/R2, Windows 7, Windows Server 2012
- Red Hat Linux 7, 8, 9, Enterprise Linux WS/AS/ES 3, 4, 5,6 (6.1~6.3) on i686/x86_64
- All Fedora/Centos versions on i686/x86_64
- Linux (kernel 2.2, 2.4, 2.6)
- HP-UX 11.0, 11i on PA-RISC 1.1/2.0 & 11iv2 on IPF
- Solaris 2.6, 7, 8, 9 on SPARC, Solaris 10 on both SPARC and x86

Update Management Agent (UMA) **

- Windows 2000, XP, Server 2003, Vista, Server 2008, Windows 7, Server 2012
- Red Hat Linux 7, 8, 9, Enterprise Linux WS/AS/ES 3, 4, 5, 6 on i686/x86_64
- All Fedora/Centos versions on i686/x86_64
- Linux (kernel 2.2, 2.4, 2.6)

WebALARM Console (WAC) / Update Management Console (UMC)

- Windows 2000, XP, Server 2003, Vista, 7 Server 2008/R2, Server 2012

** 備考:
- Windows版WAAは、Windows版UMAとのみ連携します。
- UNIX/Linux版WAAは、Linux版UMAとのみ連携します。

製品ラインナップ・定価価格

WebALARMにはStandard、Premium、Professionalの三つのラインナップを用意しております。

	WebALARM Standard	WebALARM Premium	WebALARM Professional
主要な機能			
モニタリング	○	○	○
アラートの通知	○	○	○
リカバリ	○	○	○
GUIの搭載	○	○	○
レポーティング機能	–	○	○
通常のアップデート機能	○	○	○
自動アップデート機能	–	–	○
価格			
基本パッケージ (1コンソール+1サーバ)	188,000円	498,000円	778,000円
追加サーバ1台分	188,000円	198,000円	208,000円
追加 コンソール1台分	48,000円	48,000円	48,000円
次年度保守(追加メンテナンス費1年分)	37,600円	99,600円	155,600円

情シスさん向け。
WebALARM FAQ TOP5

情シスさん向け。FAQ TOP1：
改ざん検知方法とその周期

監視：WindowsとUNIX/LINUX版　検知方法の違い

1）Windowsの場合：リアルタイム検知

Windows基盤をしようする場合、WebALARMはWindowsのイベントトリガーを使用することにより、改ざんをリアルタイムに検知します。

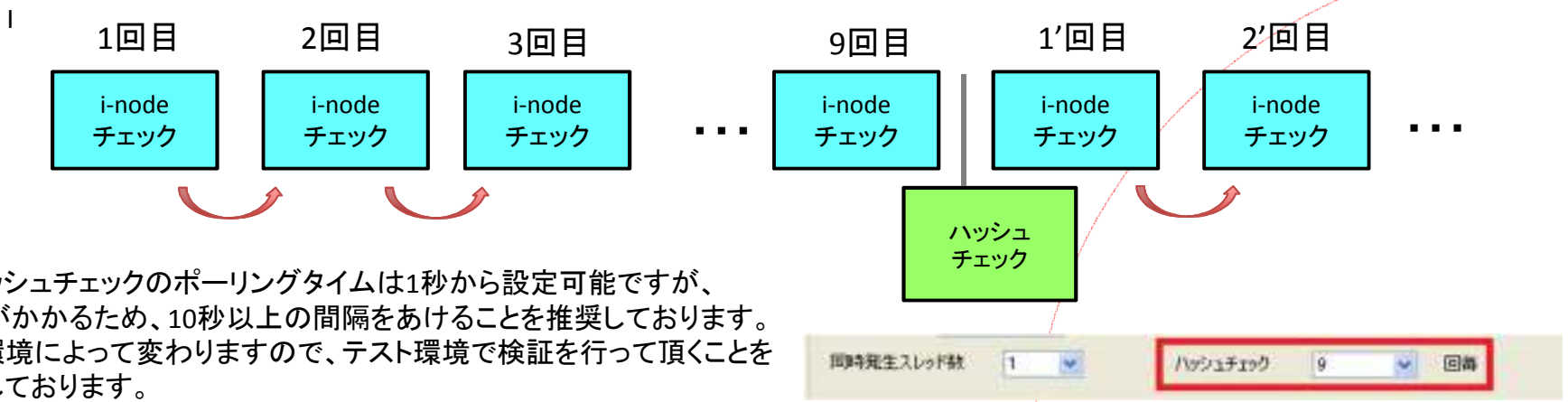
- WebALARMの必要な動作として、OSが、ファイル生成や消去、改変のイベントを検知したものと連携しています。
- このモニタリング方法はシステムに負荷をかけることがありません。

2）UNIX/LINUXの場合：検知方法

UNIX/LINUX系OSを基盤として使用する場合、WebALARMは、i-nodeモニタリングプロセスを使用することにより、ほぼリアルタイムに検知することが可能です。

①i-nodeチェックは99%の改ざんを下記項目によって検知します。
- ・ファイルのサイズ
- ・タイムスタンプ
- ・権限
- ・ファイル形式

②ハッシュチェック
- ・100%の改ざんを検知
- ・負荷がかかる



※ハッシュチェックのポーリングタイムは1秒から設定可能ですが、負荷がかかるため、10秒以上の間隔をあけることを推奨しております。また環境によって変わりますので、テスト環境で検証を行って頂くことを推奨しております。

情シスさん向け。FAQ TOP2：
ハッシュチェックスピードとCPU使用率

ハッシュチェックスピードはどれぐらいかかるか？

FAQ TOP2

下記に以前にベンチマークしたものを参照してください。
＜テスト環境＞

OS : CentOS 5.1
CPU: Intel Quad Core Xeon Pro X3210 2.13GHz
メモリRAM: 4GB
ハードディスク容量HDD: 7200rpm SATA II

テスト 1

ファイルの数	: 1
トータルサイズ	: 895MB
ハッシュチェックスピード	: ～4秒
スレッドの数	: 1

テスト2

ファイルの数	: 90,000 (~30KB毎)
トータルサイズ	: 2.7GB
ハッシュチェックスピード	: ～5秒
スレッドの数	: 4

・検知中にかかるCPU使用率は　30%～50%

※ファイル数が多い場合、CPUの使用率を下げるためには、
監視周期を長くすることを推奨致します。

速度・負荷：CPU使用率を下げる方法

FAQ TOP2

1. 【環視周期】ポーリング毎のハッシュチェック回数を減らす

1. 【コネクションとパフォーマンス】「CPU負荷を抑える」を選択する

情シスさん向け。FAQ TOP3：
UMAのコンテンツ速度と注意点

UMAから更新されたデータの配信速度はどれぐらいか

「配信は即時に反映されますが、数秒の遅延がかかります。
またミラーリングされるデータが多ければ、複製される時間が長くなります。」

【評価環境】

		WAA	UMA
OS	:	CentOS 5.3	CentOS 3.9
CPU	:	Intel(R) Pentium(R) Dual CPU E2180 @2.00GHz	
Memory RAM	:	2GB	256MB
HDD	:	7200rpm SATA II	

	テスト1	テスト2
ファイル数	1	1000
ファイルサイズ	1GB	1GB
所要時間	4分25秒	4分55秒

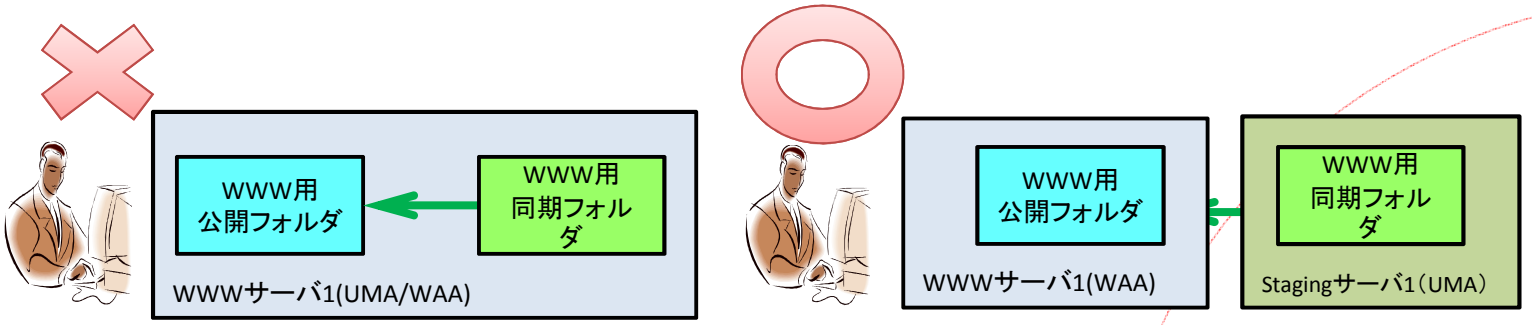
UMA導入時の注意点について

FAQ TOP3

<UMAインストール先について >

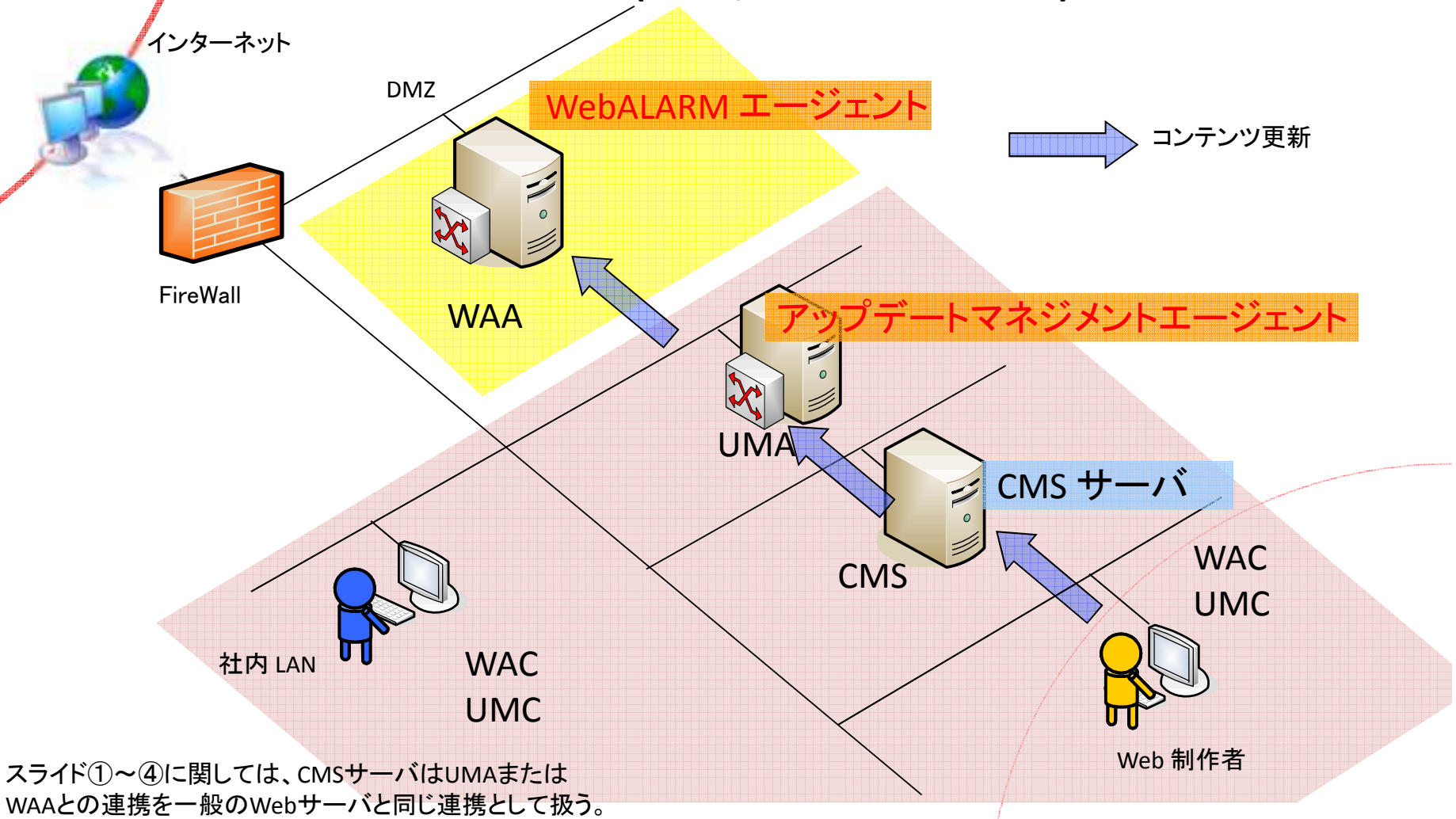
通常UMAは、常にインターネットからのアクセスが禁止されている環境である内部LAN環境内にインストールすることを推奨しております。
通常WAAは、DMZセグメント内に配置されているWebサーバにインストールされています。

※DMZセグメントとは、外部（インターネット）から見ることができるに対して、内部LANセグメントは外部から見ることができません。



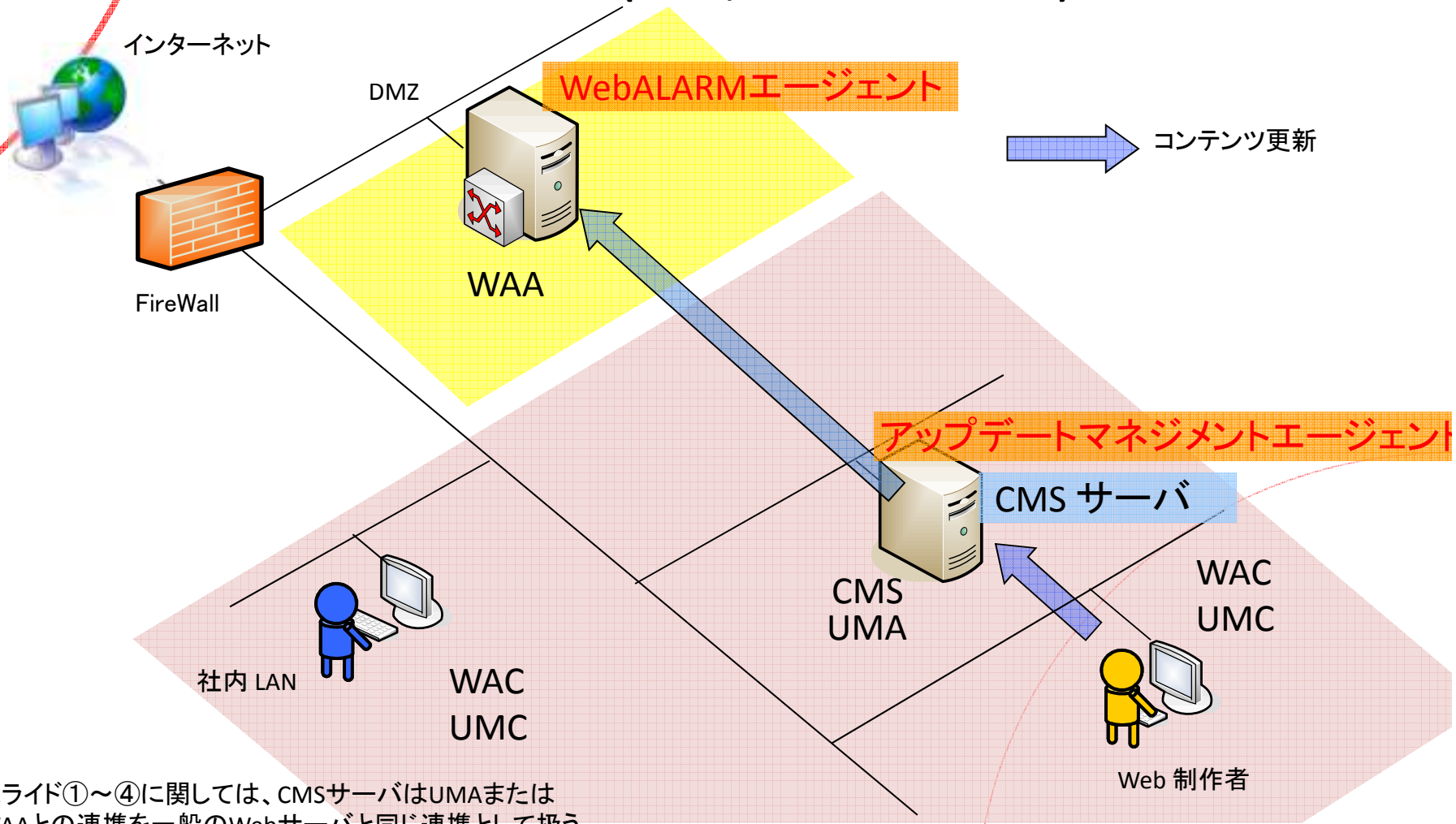
情シスさん向け。FAQ TOP4：
CMS環境への導入：3種類

方法 1: WebALARM Professional (UMA, CMS 別居の場合)



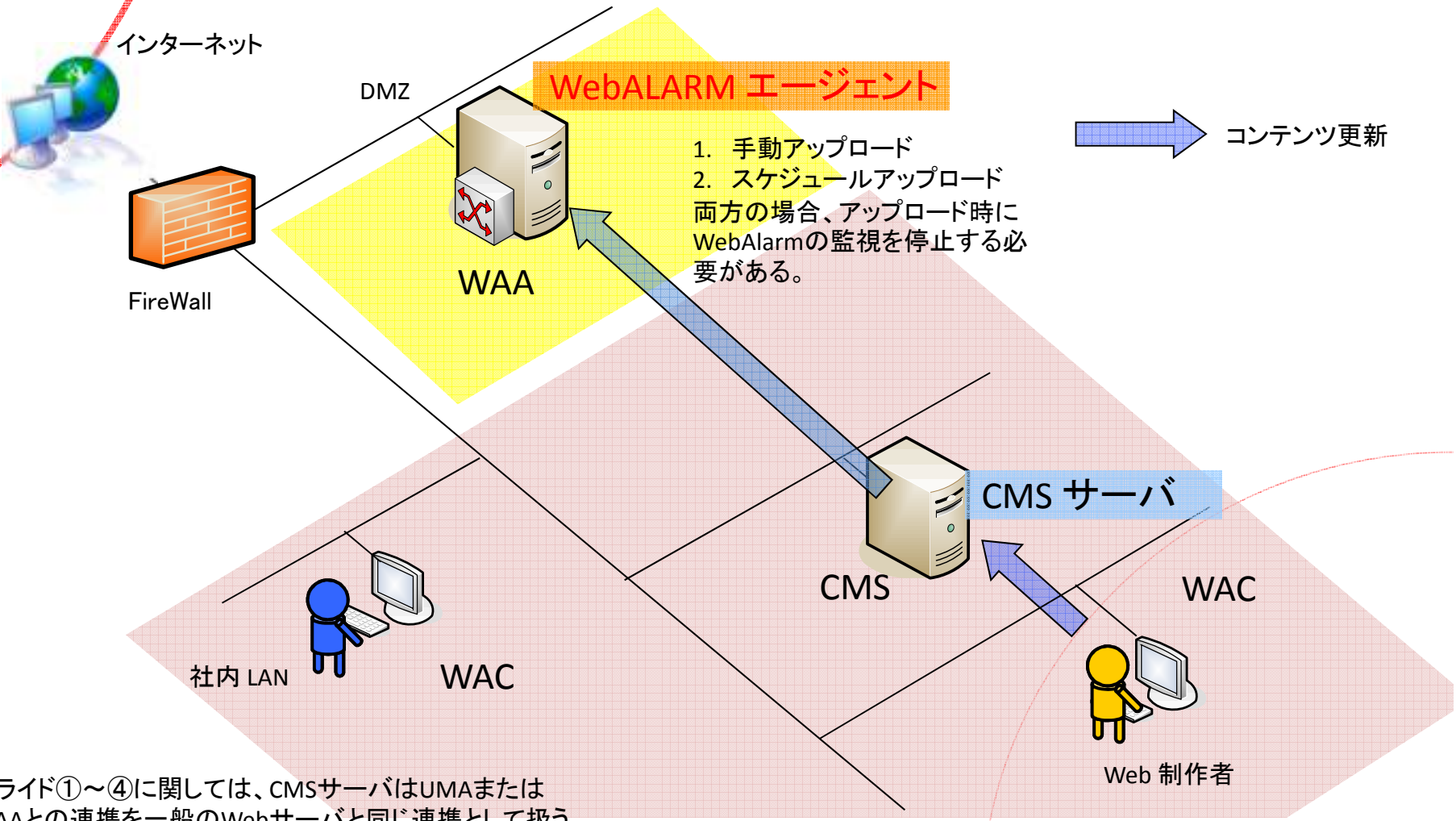
スライド①～④に関しては、CMSサーバはUMAまたは
WAAとの連携を一般のWebサーバと同じ連携として扱う。

方法 2: WebALARM Professional (UMA, CMS 同居の場合)



スライド①～④に関しては、CMSサーバはUMAまたは
WAAとの連携を一般のWebサーバと同じ連携として扱う。

方法 3: WebALARM Standard (手動アップロードまたはスケジュールアップロード)



スライド①～④に関しては、CMSサーバはUMAまたは
WAAとの連携を一般のWebサーバと同じ連携として扱う。

情シスさん向け。FAQ TOP5:
評価版ライセンスから正規ライセンスへの移行

FAQ TOP5

<評価版から正規ライセンスに変更手順>

方法①

評価版をアンインストール後、正規版を新しくインストー ル。

方法②

評価版をアンインストールせずに、ライセンスキーのみ入れ替える。
※対象OSによって入れ替え方法が異なります。

対象OSがWindowsの場合

1. 「スタート」ー「コントロールパ ネル」ー「管理ツール」ー「サービス」「WebAlarm Server」を停止。
2. 「スタート」ー「コントロールパ ネル」ー「管理ツール」ー「サービス「System Service IV」を停止。
3. 正規版のライセンスキーを入れ替 える。
4. 「スタート」ー「コントロールパ ネル」ー「管理ツール」ー「サービス」「WebAlarm Server」を開始。

対象OSがLinux/Unixの場合

1. ライセンスキー（wa.p12）を入れ替える。 # mv wa.p12 /usr/local/wa4/wa.p12
2. waプロセスを開始。 # kill -15 <wa process id>

情シスさん向け。
その他の注意事項

その他

ログのサイズ

・通常一日のログサイズは、平均20KB

（作成されたグループ（データベース)の数にも影響されます）

1	1 データベース、監視間隔1分の場合	約255KB／日
2	10 データベース、監視間隔1分の場合	約2.5MB／日
3	1 データベース、監視間隔30分の場合	約8.5KB／日

FAQ

ある一定量に達すると、過去のログは自動的に削除されるか？

回答:「自動的に削除されない。」

その他

<インストール時、サーバに必要な最小スペックは下記の通りです>

WebAlarmエージェント(WAA)

CPU : 速度 500 MHz以上のプロセッサ
メモリ : 最小 256MBのRAM
ディスク容量 : (最小 10MB ⇒インストールファイル用)とコンテンツのバックアップ及びログファイル用の追加収納容量を含む。

WebAlarmコンソール(WAC)

CPU : 速度 500 MHz以上のプロセッサ
メモリ : 最小 128MBのRAM
ディスク容量 : (最小 10MB ⇒インストールファイル用)

アップデートマネジメントエージェント(UMA)

CPU : 速度 500 MHz以上のプロセッサ
メモリ : 最小 256MBのRAM
ディスク容量 : (最小 10MB ⇒インストールファイル用)とコンテンツのバックアップ及びログファイル用の追加収納容量を含む。

アップデートマネジメントコンソール(UMC)

CPU : 速度 500 MHz以上のプロセッサ
メモリ : 最小 128MBのRAM
ディスク容量 : (最小 10MB ⇒インストールファイル用)

<バッティングする製品はあるか？>

今迄、他セキュリティ製品とのバッティングされた報告はありません。

しかしながら、WebALARM以外の改ざん検知ツールをご利用のサーバにインストールする場合、WebALARMをインストールする前に、検知ツールをアンインストールしサーバの再起動を行うことを推奨しております。

製品に対するお問い合わせ

WebALARMお問い合わせ

テクニカル
サポート

評価版ライセンス

WebALARM 評価版ライセンスを下記URLよりダウンロードして頂けます。
<www.elock.co.jp/download.php>

トレーニングビデオ

インストール・設定手順のトレーニングビデオを下記URLにてご用意しております。
<www.elock.co.jp/webalarm/documentation5.html>

FAQ

WebALARMに関するよくあるご質問(FAQ)を下記URLにてご紹介しております。
<www.elock.co.jp/webalarm/documentation1.html>

製品説明
お見積

IIJ Internet Initiative Japan
Next IT Inc.
NEC | NISSHO CLOUD INITIATIVE
SoftBank ソフトバンクBB株式会社
Networld
Suzuyo shinwart
SBI Trade Win Tech

テレマカセ！