WebALARM™

Data Integrity Monitoring & Automatic Recovery System

～Webサイト改ざん防止のセキュリティパッケージ～

2014年1月

イーロックジャパン株式会社

WebALARM™

I. 会社案内

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

I. 会社案内：イーロックジャパン株式会社

上：ペルモダラン・
ナショナル有限会社
右：イーロック
コーポレーション有限会社

【会社情報】 **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
エイチティーズビル　6F
本　社：マレーシア　クアラルンプール
1996年設立

【事業内容】

- セキュリティ製品の販売
- 脆弱性診断
- 日本企業のASEAN進出支援

【受　賞】
2011年　WebALARM：PCI DSS 要件10.5.5、要件11.5
NECより推奨
2012年　TheGRID　：日本にて特許取得

【実　績】
国内では500サイト以上、11年間の実績と信頼があります。
銀行、生保、大学、官公庁等その他実績多数有り。

【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

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

会社案内：e-Lock Corporation Sdn Bhd.（マレーシア本社）

【会社情報】 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
株　主：　ペルモダラン・ナショナル
　　マレーシア最大の国営投資会社
　　UMW ホールディングス

【事業内容】

- 脆弱性診断
- セキュリティコンサルティング
- システムインテグレータ
- セキュリティ製品の開発

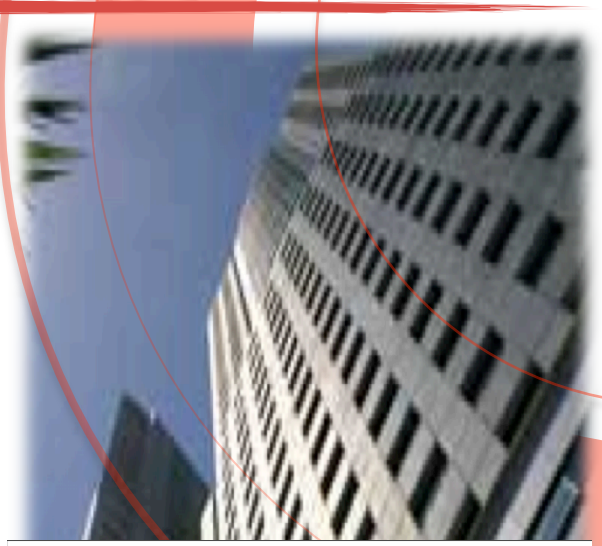
【 受　賞 】

2000年　WebALARM：　PIKOM ICT Awardを受賞

2007年　TheGRID　　：　PIKOM ICT Awardを受賞

【 実　績 】

案件実績：1,852件
マレーシアでは中央銀行を始め多くの金融機関、大手企業のITセキュリティコンサルタントとして、高いセキュリティ技術を提供し、マレーシア発のITセキュリティにおけるリーディングカンパニーとして、ワールドワイドに事業展開をおこなっております。



E-Community... and its story

ICT industry pays tribute to USJ Subang Jaya e-Community

www.USJ.com.my was announced "Community Website of The Year" in the PIKOM-Computimes IT Awards 2000 Thursday night. The Team thanks communities from within and outside Subang Jaya for making it happen. Chief Secretary Halim Ali gave away the awards.

Posted on 02.14am Nov 03, 2000

- BREAKING NEWS -

By usjXpress Team
Email:
edteam@usj.com.my

BANDAR SUNWAY - www.USJ.com.my was pronounced the "Community Website of The Year" in the PIKOM-Computimes IT Awards 2000 presentation ceremony held at a hotel here Thursday night.

Tan Sri Abdul Halim Ali, Chief Secretary to the Government, gave away the awards.

Jeff Ooi, who received the award on behalf of the Web and Editorial Teams, said

PIKOM ICT Award受賞式

PIKON ICT Award授賞式 2000年

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

I. ワールドワイドのビジネスを展開

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。

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

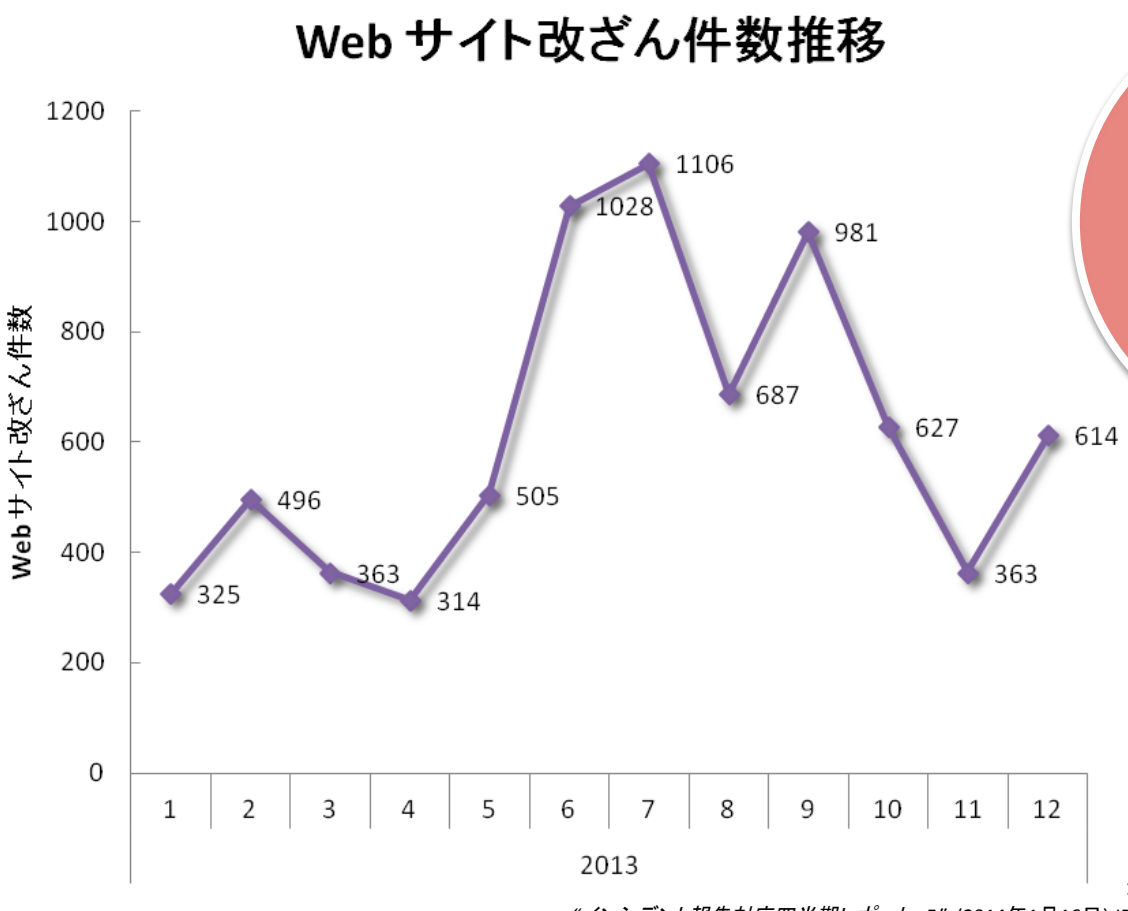
WebALARM™

II. 昨今のセキュリティにおける現状と必要環境

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II. 昨今のセキュリティにおける現状ー”Webサイト改ざん被害件数”

JPCERTコーディネーションセンターの2014年1月16日報告書によると、2013年1月~12月に報告されたWebサイト改ざん件数は計7,409件。 月平均617件の改ざん被害が確認されている。



1ヶ月平均
617件

“インシデント報告対応四半期レポートp.5”, (2014年1月16日) JPCERT/CC <http://www.jpcert.or.jp/ir/report.html>

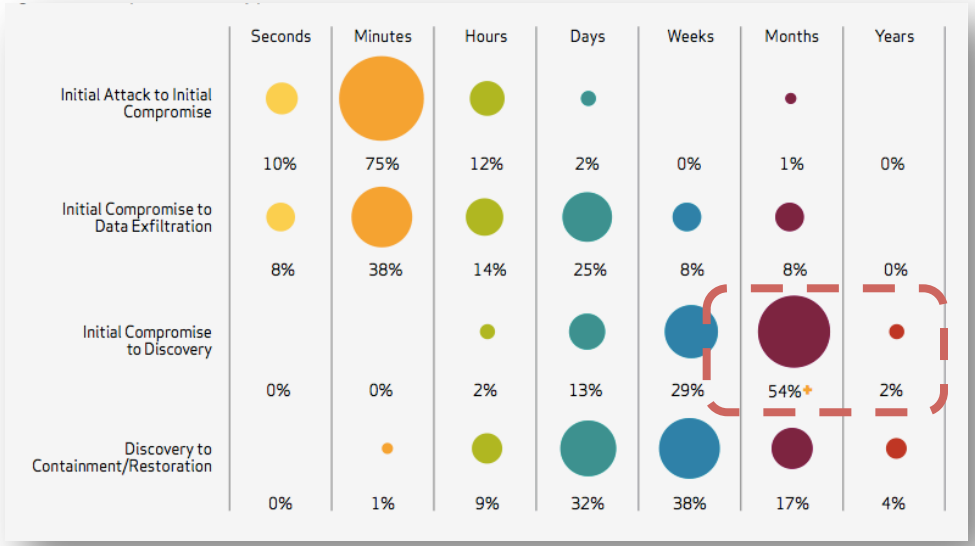
Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II. 昨今のセキュリティにおける現状ー”攻撃から発見までの期間”

サイバー攻撃によりWebサイトが改ざんされた場合、早急に復旧する必要があります。
なぜならば、マルウェアやトロイの木馬等ウイルスをWebサイトへ仕込まれた場合、閲覧者への感染の被害につながり、Webサイト運営者は「**被害者**」から「**加害者**」へなりうるからです。

Verizonの調査によると、サイバー攻撃をうけた場合、50%以上の被害を受けた団体・企業が、攻撃を受けたことに気付く迄に**1ヶ月以上の期間**を要し、その「発見の9割以上が**第三者**による発見」で多くの場合運営者は気付かない傾向にあります。

<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

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II. 昨今のセキュリティにおける現状―”被害総額：○○○円”

「1件あたりの想定損害賠償額は 1億2810万円 」

NPO　日本ネットワークセキュリティ協会　2012年9月20日発表の報告書によると
2011年度の1件のインシデントにかかる損害賠償額は前年に比べほぼ2倍に

表 3-1：2010 年 個人情報漏えいインシデント 概要データ

漏えい人数	557 万 9316 人
インシデント件数	1679 件
想定損害賠償総額	1215 億 7600 万円
一件あたりの漏えい人数※1	3468 人
一件あたり平均想定損害賠償額※1	7556 万円
一人あたり平均想定損害賠償額※2	4 万 3306 円

表 3-1：2011 年 個人情報漏えいインシデント 概要データ

漏えい人数	628 万 4363 人
インシデント件数	1551 件
想定損害賠償総額	1899 億 7379 万円
一件あたりの漏えい人数※1	4238 人
一件あたり平均想定損害賠償額※1	1 億 2810 万円
一人あたり平均想定損害賠償額※2	4 万 8533 円

NPO　日本ネットワークセキュリティ協会　2012年9月20日、2011年7月1日発行 「2011年情報セキュリティインシデントに関する調査報告書」

狙われる業種分別トップ5

1位　公務
2位　金融業、保険業
3位　教育、学習支援
4位　医療、福祉
5位　情報通信業

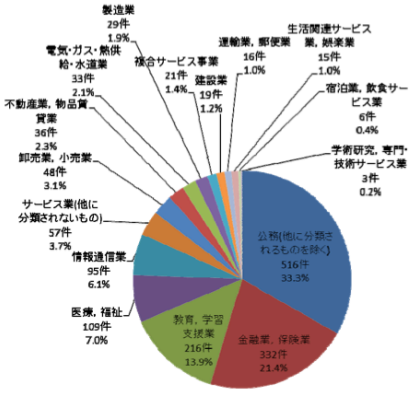


図 3-1：業種別比率（件数）

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II. 昨今のセキュリティにおける現状ー”狙われているのは「Webアプリケーション」”

Gartnerの報告によると、ほとんどのWebアプリケーションに脆弱性がみられ、サイバー攻撃の **75 %は アプリケーション 層**で発見されています。

そして多くのWebサイト改ざんは、そのWebアプリケーションの脆弱性が原因とされています。

(*ここでいう「Webサイトの改ざん」は、データの内容についての改ざんだけではなく、目に見えないガンブラー・トロイの木馬・SQLインジェクション・マルウェア等を「Webサイトに埋め込む行為」も示しています。)

下記の資料は、東京SOC調べによる昨今のサイバー攻撃に関する詳細です。

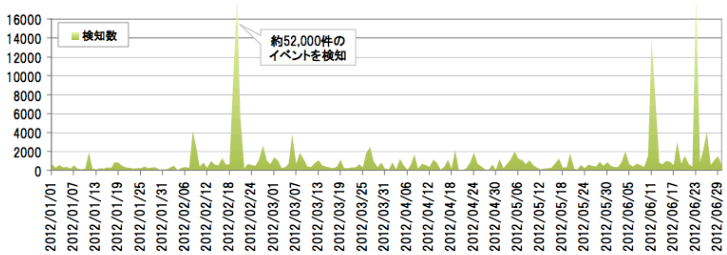


図 15 SQL インジェクション攻撃の検知件数推移(東京 SOC 調べ:2012 年 1 月 1 日~6 月 30 日)

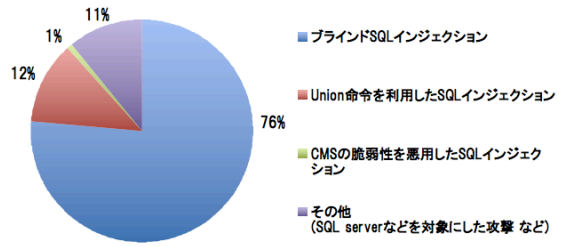


図 16 SQL インジェクション攻撃の種類別割合(東京 SOC 調べ:2012 年 1 月 1 日~6 月 30 日)

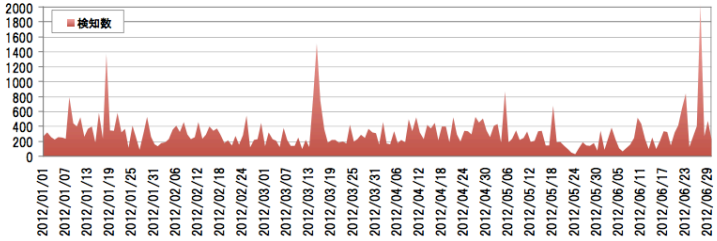


図 17 SQL インジェクション攻撃以外の Web アプリケーションへの攻撃検知件数推移
(東京 SOC 調べ:2012 年 1 月 1 日~6 月 30 日)

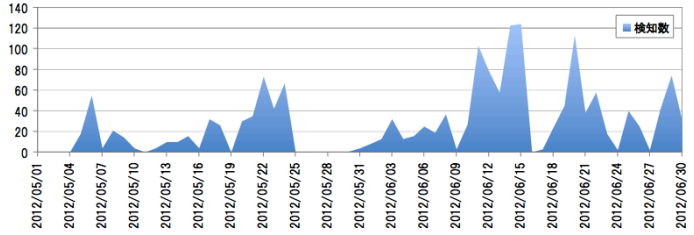


図 18 PHP の脆弱性を悪用する攻撃検知件数推移(東京 SOC 調べ:2012 年 5 月 1 日~6 月 30 日)

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II.昨今のセキュリティにおける現状ー”「入り口対策」が中心”

従前の「入口対策」と呼ばれるセキュリティは
「完全」に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」だけ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。

Hacker → Firewall → IDS/IPS → Web Server

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。

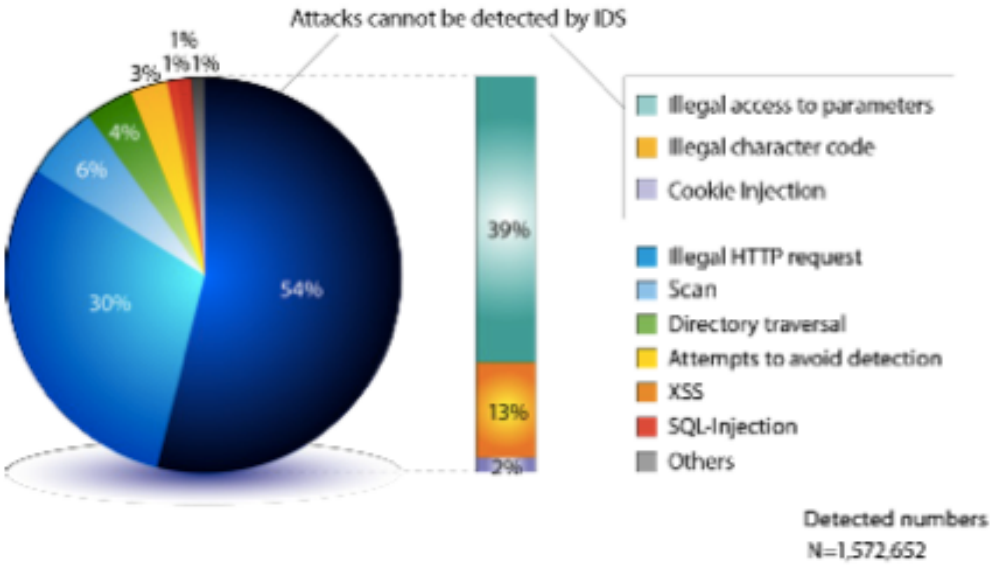
従来の「入口対策」と呼ばれるセキュリティは必然とされ
認知度も高く、対策をとられている企業・団体も多い

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II.昨今のセキュリティにおける現状ー”IDS/IPSは？”

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.

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II.昨今のセキュリティにおける現状ー ”WAFは？”

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>

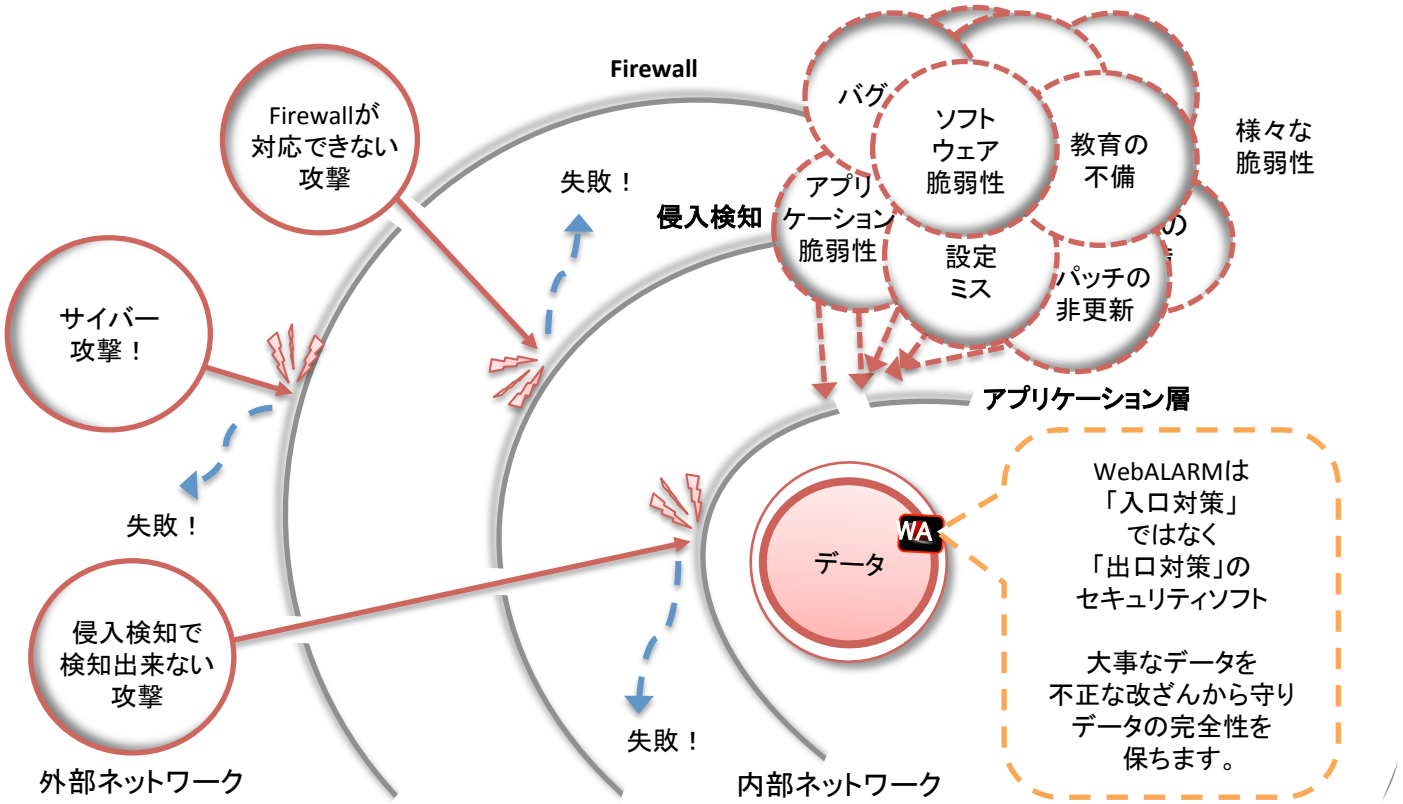
1) ヨーロッパ非営利組織OWASP (Open Web Application Security Project)

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II. 昨今のセキュリティにおける現状 ー ”必要なのは「出口対策」”

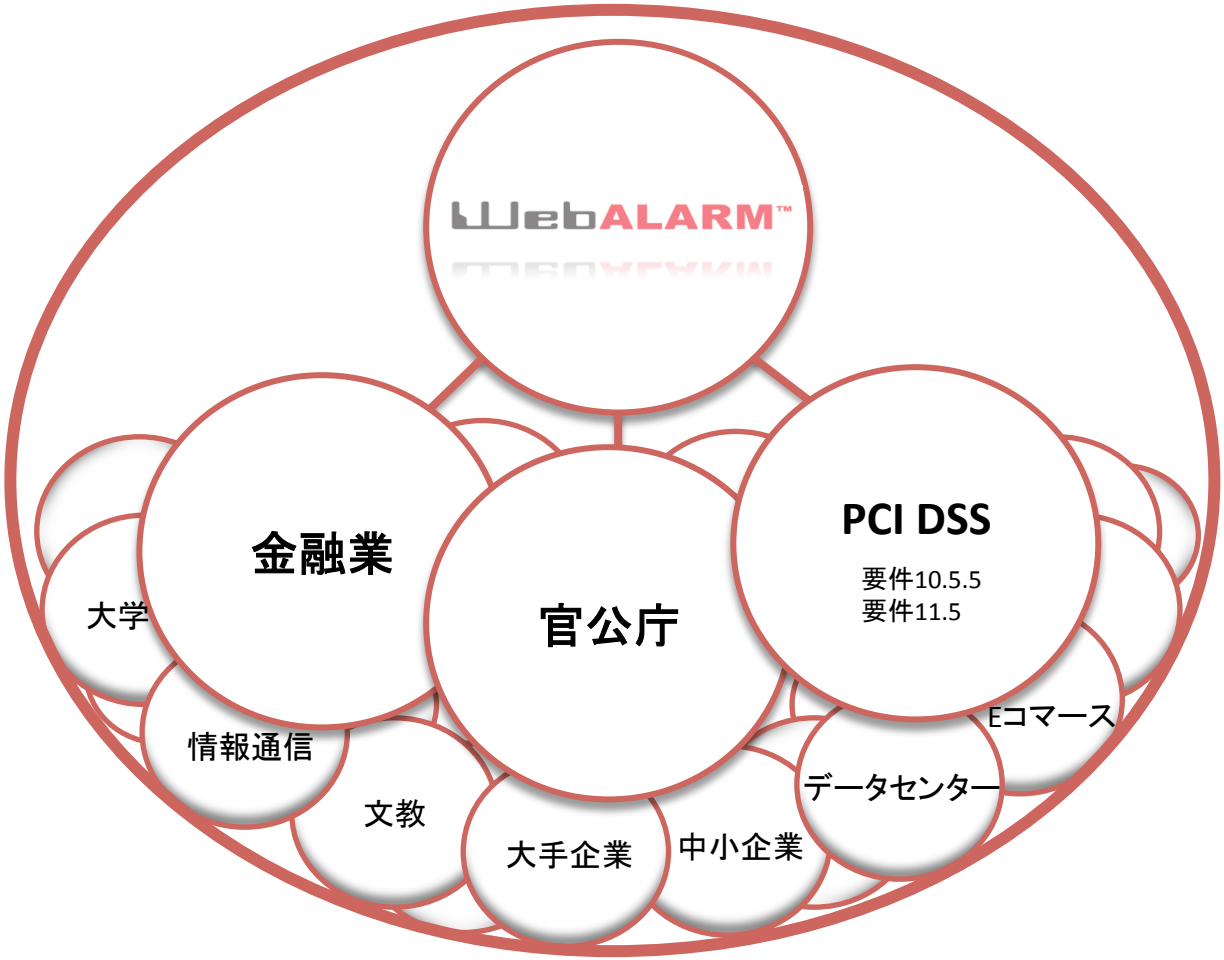
「入り口対策」だけでなく、「出口対策」におけるセキュリティ強化を早急に

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」）



Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

II.「WebALARMの必要環境」＝「サーバのある環境」



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は日本で初めてPCI DSSを取得したシルバーレイクジャパン株式会社に採用されました。
- 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。

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

WebALARM™

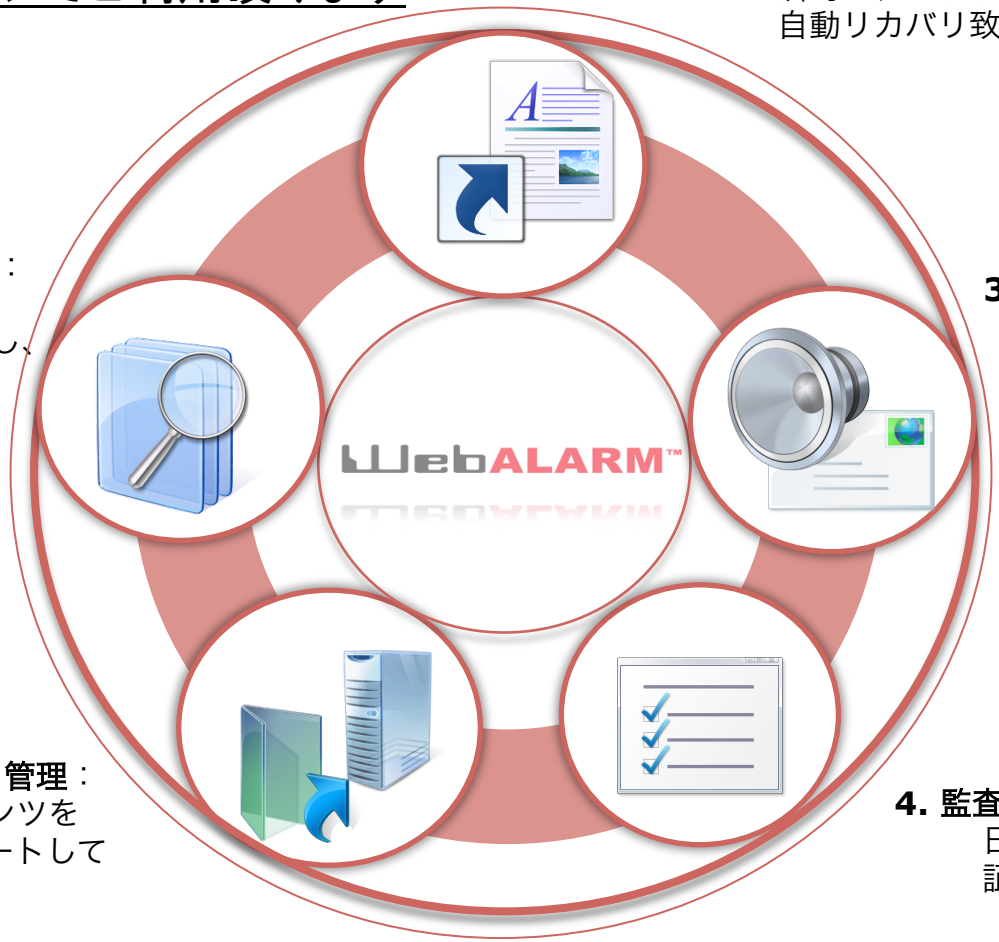
III. WebALARM 一“製品概要”

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

III. WebALARM ー“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。

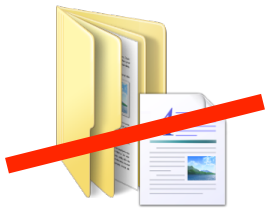
Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

III. WebALARM ー“製品概要：モニタリング(監視)”

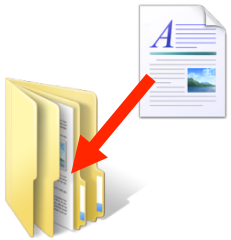
SHA1の暗号化アルゴリズムを使用し、「1bit」の改ざんも検知致します。

正確なデータ保全の監視

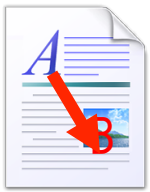
- ファイルとフォルダーの削除
- コンテンツの改ざん
- 新しいファイルの追加
- 権限の変更



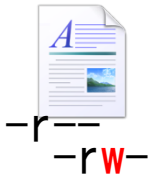
削除



追加



改ざん



属性の変更

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

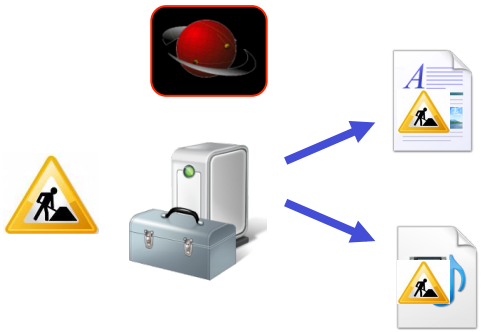
III. WebALARM ―“製品概要：自動リカバリ”

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。

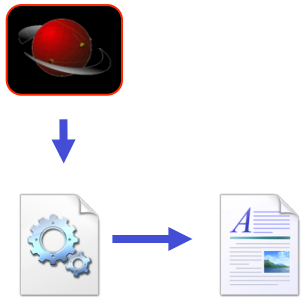
不測の事態にも、即リカバリー

- 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

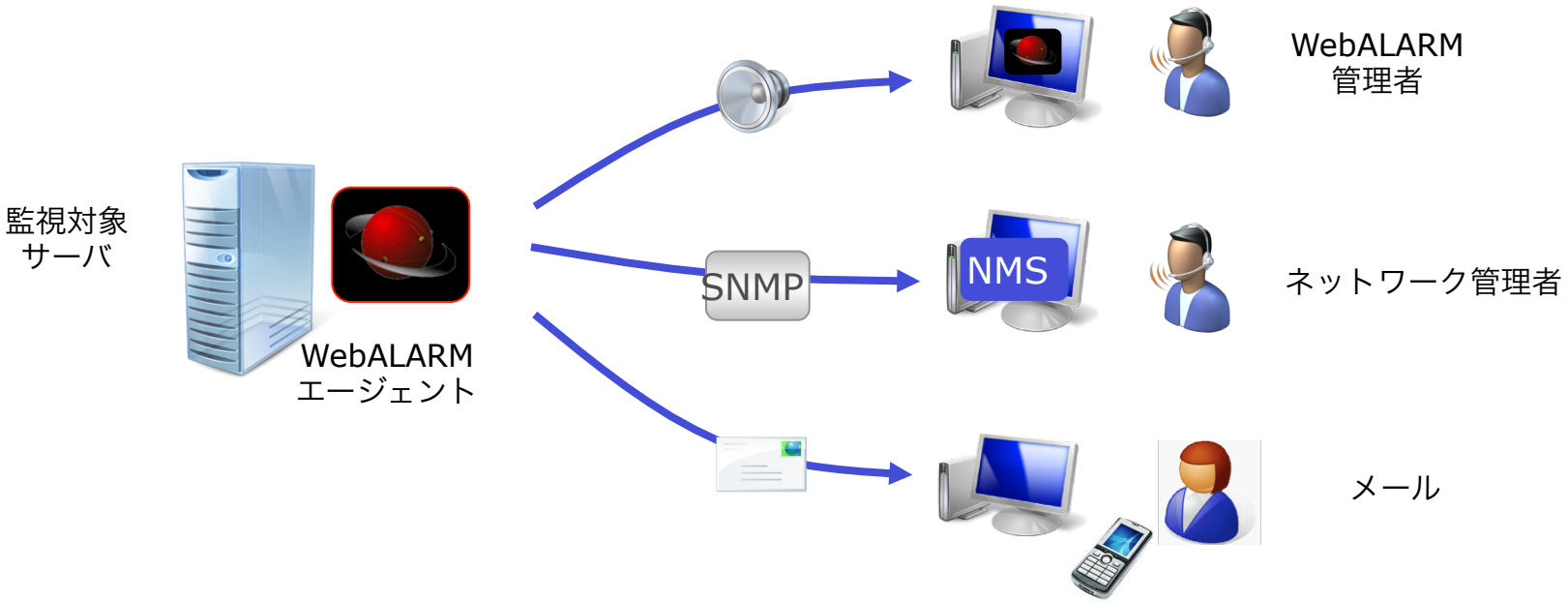
Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

III. WebALARM ―“製品概要：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)
- Email での警告(複数の宛先設定可能)
- SNMP にも対応



Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

III. WebALARM ―“製品概要：監査と証拠保全”

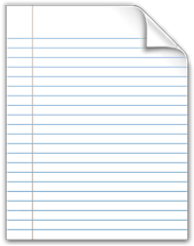
日毎、イベント毎のログを証拠として残します。

<u>下記について監視出来ます。</u>

- データの改ざん
- 勝手なアップデート
- 管理者の動向

<u>調査のための証拠保全</u>

- 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)

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

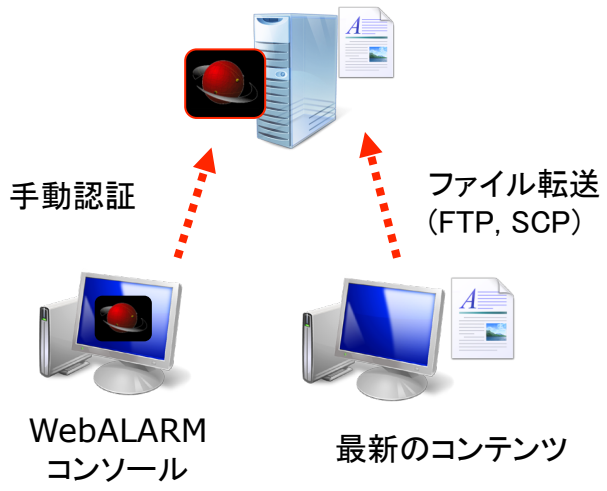
III. WebALARM ー“製品概要：データアップデート管理”

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

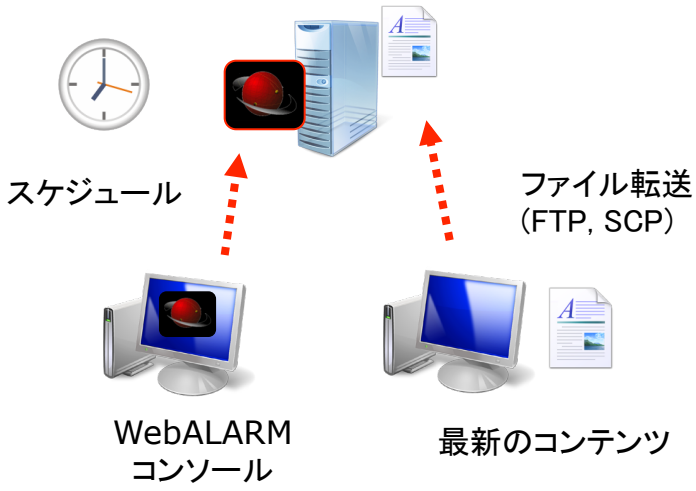
最新のコンテンツを、WebALARM管理者によって

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

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

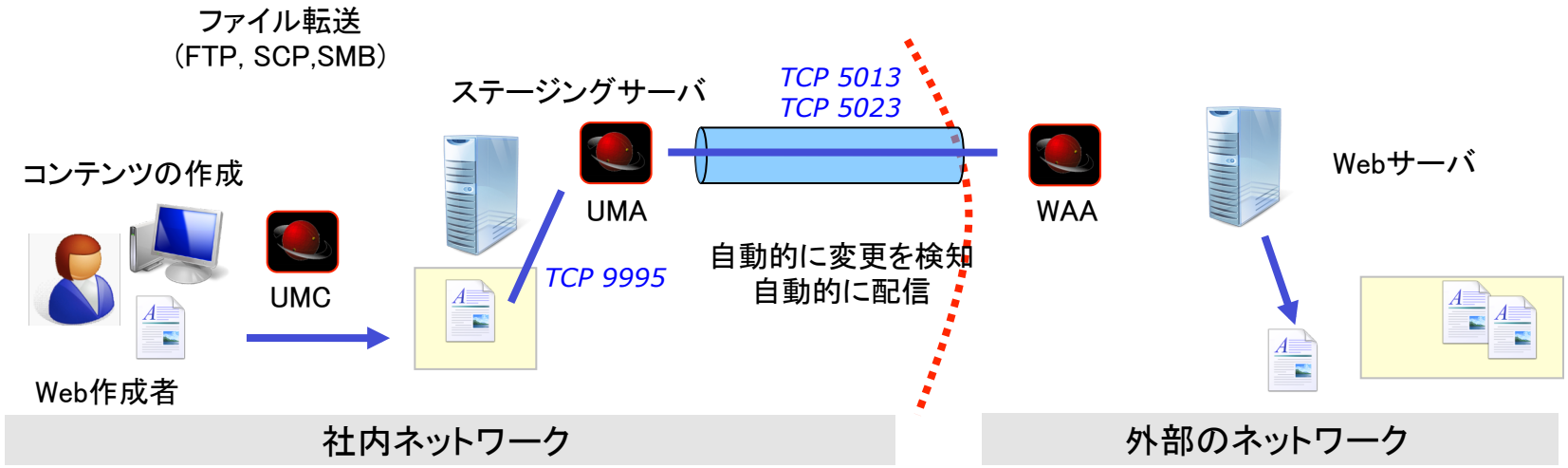
III. WebALARM ー“製品概要：データアップデート管理”

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:

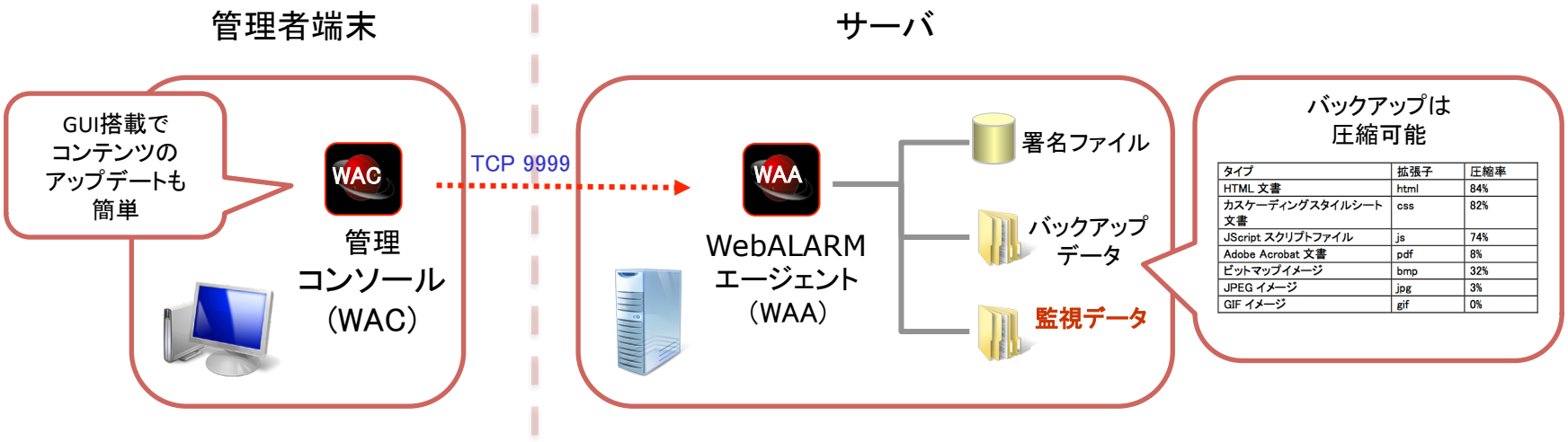
- ステージングフォルダの**変化を監視**します。
- ステージングフォルダに変化があれば、**ライブフォルダへコピー**します。



Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

III. WebALARM ー“構成例1：Standard/Premiumパッケージ”

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

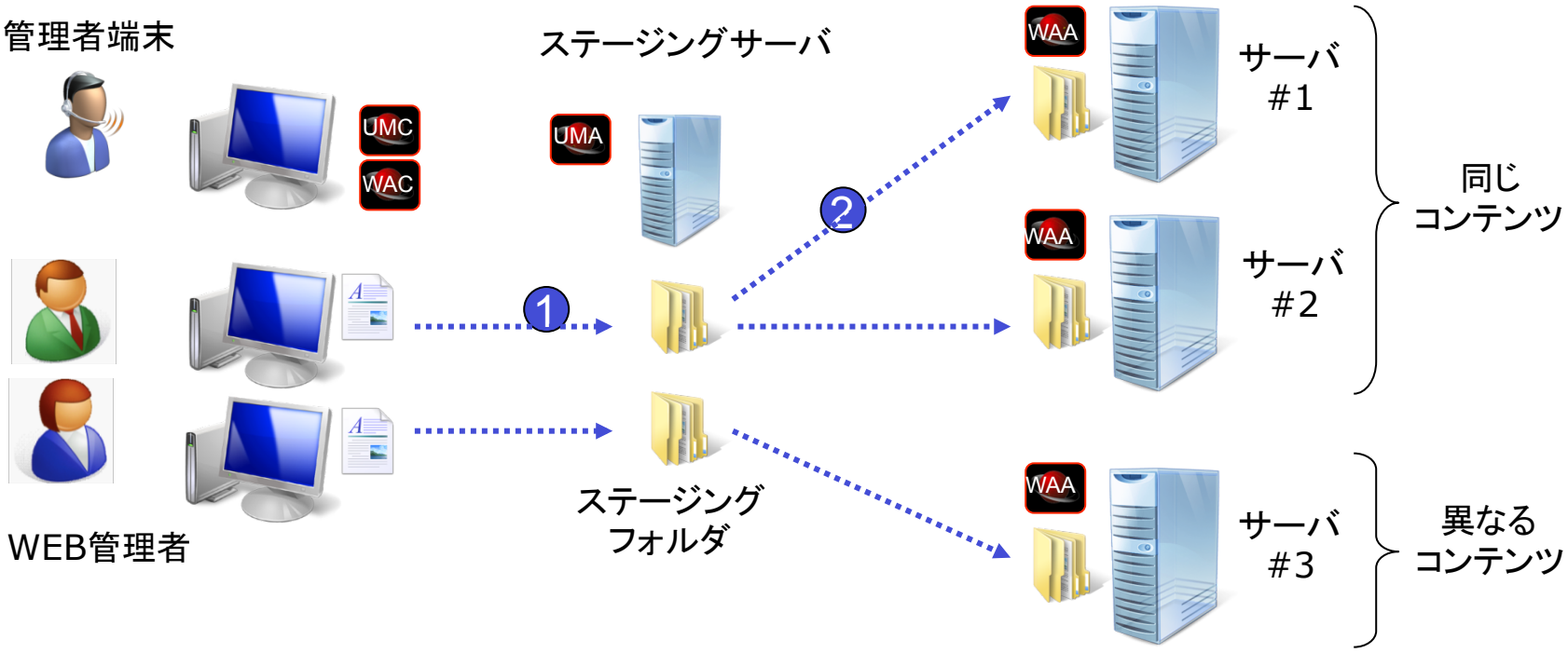
配信用モジュール

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

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

III. WebALARM ー“構成例2：Professionalパッケージ”

自動アップデート機能は、エージェントを止めることなくコンテンツを複数サーバへ更新することが可能です。



- 一つのステージングフォルダから複数のサーバへの配信が可能

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

WebALARM™

IV. 価格と対象OS

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

IV. WebALARM ー“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	o	o	o
アラートの通知	o	o	o
リカバリ	o	o	o
GUIの搭載	o	o	o
レポーティング機能	–	o	o
通常のアップデート機能	o	o	o
自動アップデート機能	–	–	o
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

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

IV. WebALARM ー “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。

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.

IV. お問い合わせ先

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>

イーロックジャパン株式会社
<www.elock.co.jp>

TEL: 03-3265-1169
FAX: 03-6272-9878

営業時間：平日　9:00～17:00 (祝日を除く)

東京都千代田区麹町3-12-7
エイチティーズビル　6F

Copyright © e-Lock Corporation Sdn Bhd. All Rights Reserved.