特集論文

SaaS型セキュリティ診断サービス

今川大輔* 藤井誠司***
河内清人**
佐伯保晴***

SaaS Security Assessment Service

Daisuke Imagawa, Kiyoto Kawauchi, Yasuharu Saeki, Seiji Fujii

要 旨

企業活動にインターネットが不可欠である一方，不正アクセスによるセキュリティ事故が後を絶たない。その対策としてセキュリティ診断の必要性が叫ばれて久しいが，従来の診断は技術者が専用ツールを駆使する必要があり，広く利用されていないのが現状である。

この課題を解決するため三菱電機情報ネットワーク㈱(MIND)は，SaaS(Software as a Service)(注1)型セキュリティ診断サービスを開発した。このサービスでは，MINDの診断ノウハウを反映した診断ツールによる自動診断機能が提供される。ユーザーはポータルサイトを通じて簡単な設定を行うだけで，この機能をいつでも利用でき，“所有から利用へ”を実現したサービスとなっている。

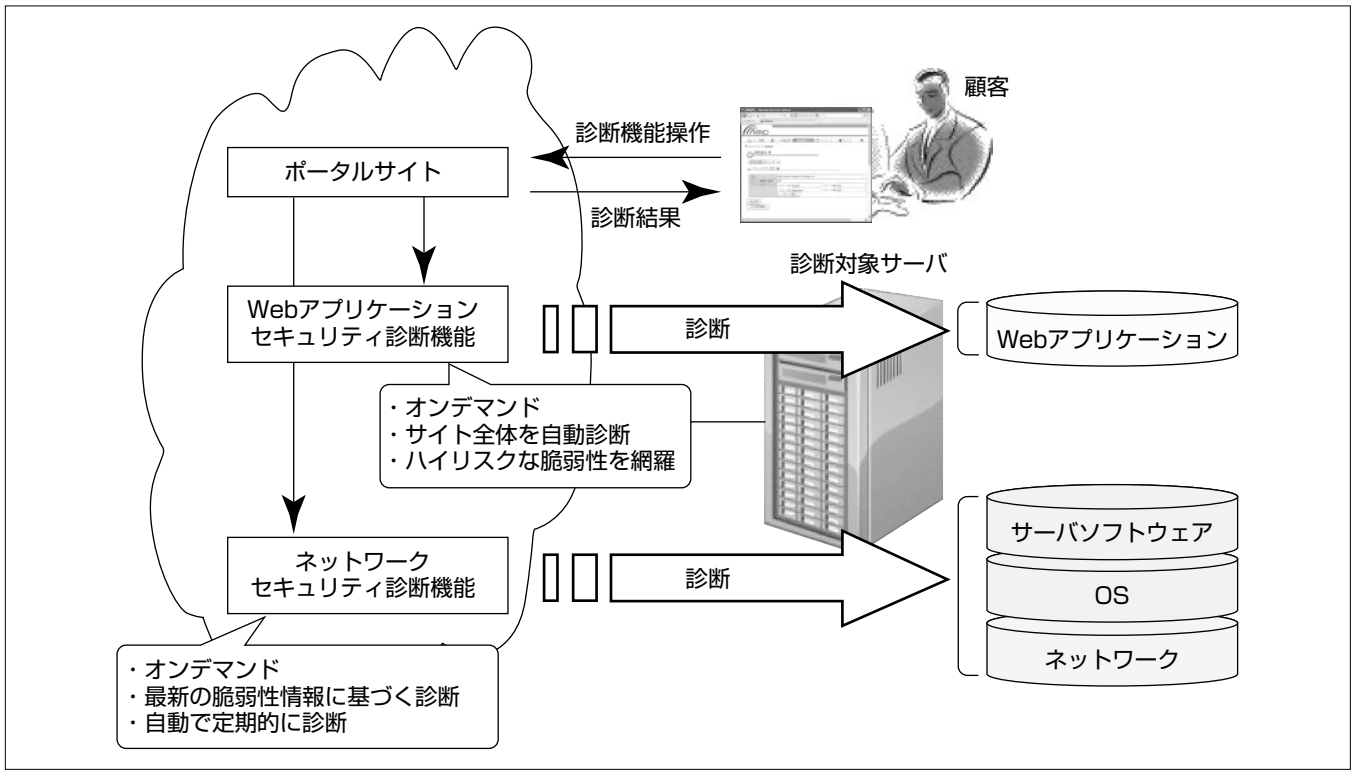
MINDは現在，SaaS型セキュリティ診断サービスとして，Webアプリケーションセキュリティ診断とネットワークセキュリティ診断を提供している。

SaaS型Webアプリケーションセキュリティ診断サービスは，①必要に応じユーザー自ら診断が可能，②診断開始ページの指定だけでサイト全体を診断，③再現診断機能によって脆弱(ぜいじゃく)性修正後の確認が容易，④従来は技術者が実施していた，OWASPが公開している高リスクな脆弱性を自動診断，という特長がある。

一方SaaS型ネットワークセキュリティ診断サービスは，サーバのOSやサーバソフトウェアに対する脆弱性診断を行う。SaaS型Webアプリケーションセキュリティ診断サービスと組み合わせることで，OSからWebアプリケーションまでサーバ全体に対する診断を提供可能である。

MINDは今後，SaaS型Webアプリケーションセキュリティ診断サービスの高精度化と，脆弱性管理機能の強化に取り組み，企業のセキュリティ事故防止に役立つサービスを提供する予定である。

(注1) ユーザーが必要とするソフトウェア機能をサービスとして提供する形態。



SaaS型セキュリティ診断サービスの概念図

MINDは，セキュリティ診断機能をサービスとして提供するSaaS型セキュリティ診断サービスを提供している。現在MINDでは，Webアプリケーションセキュリティ診断サービスとネットワークセキュリティ診断サービスをSaaS型サービスとして提供しており，ユーザーのサーバの脆弱性をOSからWebアプリケーションまで診断可能である。

*三菱電機情報ネットワーク㈱(理博) **三菱電機㈱ 情報技術総合研究所 ***三菱電機情報ネットワーク㈱

1. まえがき

サーバやWebアプリケーションへのセキュリティ対策の必要性が叫ばれて久しいが，不正アクセスによるセキュリティ事故は後を絶たない。さらに昨今は，情報漏えいやWebサイトの改ざんによるウイルス配布サイトへのリンク埋め込みなど，Webサイト管理者が加害者として責任を問われる場合も多く，そのため，自社のサーバやWebアプリケーションが最新の脆弱性に対し対策ができているかを確認するセキュリティ診断の必要性はますます高まりつつある。

しかし従来のセキュリティ診断は，専門的な技術を身につけた診断技術者による作業が必要であった。そのため，必要性は認識されつつも，セキュリティ診断の普及がなかなか進んでいないのが現状である。

そこで，MINDはセキュリティ事故の防止に貢献することを目指し，だれでも簡単に使える診断サービスとしてSaaS型セキュリティ診断サービスの開発に取り組んでいる。現在MINDでは，SaaS型Webアプリケーションセキュリティ診断サービスとSaaS型ネットワークセキュリティ診断サービスを提供している。

SaaS型セキュリティ診断サービスでは，だれでも使えるようにMINDの診断ノウハウが反映された診断ツールが自動診断を行う。ユーザーはポータルサイトを通じて，診断ツールに簡単な設定を行うだけで，必要なときにいつでも簡単に診断を行うことができる。

本稿では，これらMINDのSaaS型セキュリティ診断サービスと，それらを実現する技術について述べる。

2. SaaS型セキュリティ診断サービス

ここでは，現在MINDが提供しているSaaS型Webアプリケーションセキュリティ診断サービスとSaaS型ネットワークセキュリティ診断サービスについて述べる。

2.1 SaaS型Webアプリケーションセキュリティ診断サービス

このサービスは，インターネット上に公開されたユーザーのWebアプリケーションの脆弱性を自動診断するサービスである(**図1**)。このサービスは，SaaS型セキュリティ診断サービスの“ユーザーが必要なときにいつでも簡単に診断を行うことができる”という特長に加え，次の特長がある。

(1) サイト全体をスピーディに診断

サイト全体を巡回して各ページを自動で診断する。1ページ当たり約30秒で診断可能である。さらに，診断結果は利用者向けポータルサイト上で即時確認可能である。

(2) 検出された脆弱性への再現診断

診断で検出された脆弱性が正しく修正されたか，再度診断を行いたいというニーズは多い。そこで，過去に検出された脆弱性が，正しく修正されたかを容易に確認できる再現診断機能を提供している。

(3) 主要な脆弱性をカバー

他社に先駆け，Webアプリケーションが必ず対策すべき脆弱性として広く認知されているOWASP Top 10[(1)]脆弱性に対応した診断を実施可能である。

OWASP Top 10とはWebアプリケーションセキュリティ向上のために活動する非営利団体OWASPが公開している，Webアプリケーション上で知られるハイリスクな脆弱性の上位10項目である。OWASP Top 10はクレジットカード業界のセキュリティ対策基準であるPCI-DSS[(2)]でも，Webアプリケーションに対する診断項目として採用されており，対策が不可欠の脆弱性として世の中に広く認知されている。

表1にOWASP Top 10(2010年版)に記載されている脆弱性の一覧を示す。このサービスは，ストレージ暗号化に関する脆弱性(表中網掛け)を除き，全項目を診断する。

2.2 SaaS型ネットワークセキュリティ診断サービス

SaaS型ネットワークセキュリティ診断サービスは，ユーザーがインターネット上に公開しているサーバやネットワーク機器に対し，OSやサーバソフトウェアにおけるセキュリティ上の問題点を検査する。

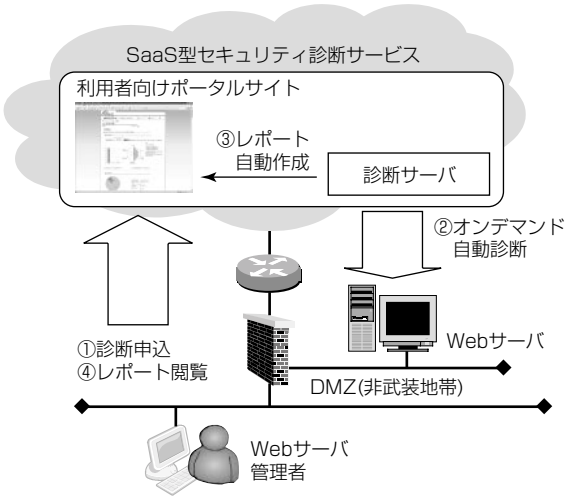


図1．SaaS型Webアプリケーションセキュリティ診断サービス

表1．OWASP Top 10の脆弱性

順位	脆弱性の名称
1	インジェクションの不具合(SQLインジェクション等)
2	クロスサイトスクリプティング
3	不完全な認証管理とセッション管理
4	安全でないオブジェクトの直接参照
5	クロスサイトリクエストフォージェリ
6	セキュリティ設定の不備
7	安全でない暗号化保存
8	URLアクセスの制限失敗
9	トランスポート層の不十分な保護
10	未チェックのリダイレクト・フォワード

URL：Uniform Resource Locator

この診断サービスは，日々発見される最新の脆弱性情報に基づき，一日一回など，高い頻度で繰り返しネットワーク診断を自動実施可能な点が特長である。

このサービスを利用することで，ユーザーは新たな脆弱性に対しても被害を受ける前に対処することが可能となる。

この診断サービスとSaaS型Webアプリケーションセキュリティ診断サービスによって，OSからWebアプリケーションまですべての階層をSaaS型でカバー可能である。

3. SaaS型セキュリティ診断を支える基盤技術

ここでは，MIND SaaS型セキュリティ診断サービスを実現する技術であるWebアプリケーションセキュリティ自動診断技術とMINDクラウド技術基盤について述べる。

3.1 Webアプリケーションセキュリティ自動診断技術

OWASP Top 10のうち，“不完全な認証管理とセッション管理”“クロスサイトリクエストフォージェリ”及び“URLアクセスの制限失敗”といった脆弱性は，MINDが他社SaaS型Webアプリケーション診断サービスに先駆けて自動診断を実現している。この診断を実現するために，MINDと三菱電機が共同で診断方式の開発を行った。

SaaS型Webアプリケーションセキュリティ診断サービスでは，実際の攻撃を模擬した診断用データをWebアプリケーションに入力し，それに対するWebアプリケーションの応答の中に脆弱性を示す特徴が現れているかを調べることで，脆弱性の有無を判定する。

脆弱性を診断するためには，擬似攻撃を実施した結果として，Webアプリケーション機能を不正に呼び出せたことを確認する必要がある。しかし，応答を分析し，擬似攻撃に成功したかを自動で判断することは従来困難であった。

この課題を解決するため，正当な権限のもとアクセスしたときに返されるページの内容と，擬似攻撃によって不正にアクセスしたときのページの内容とを比較し，同じ内容が返されていた場合に擬似攻撃に成功したと判定する方式を開発した。

しかし，単純なページ比較では，広告等，診断とは無関係にページ内容が変化する場合に判定誤りを起こす可能性がある。そこで，ページ間の類似度を定量評価する方式を開発し，類似度に基づいてページ内容が同一かどうかを判定することで，コンテンツの多少の変化に対して影響を受けないようにしている。

3.2 MINDクラウド技術基盤

このサービスを提供するため，診断サーバ，Webポータルサーバ，及び管理サーバで構成されている。各サーバは，**図2**に示すとおり，MIND iDC(internet Data Center)のクラウド技術基盤上の仮想マシンとして動作する。各仮想マシンには，SAN（Storage Area Network)で接続されたストレージが仮想ハードディスクとして割り当てられ，仮想L2スイッチを経由して，ファイアウォールなどの外部ネットワーク機器と接続されている。

クラウド技術基盤を利用することで，システムの構築に当たり，次の効果を得ることができた。

⑴ 短期間でシステム構築ができる

クラウド技術基盤では，ハイパーバイザーに要求するだけで，必要な性能を持った仮想マシンが生成される。ネットワークも既設ケーブルを仮想化して共有するため，物理的に新たなケーブルを配線する必要がない。そのため，ハードウェア調達や施設工事にかかる時間が不要となり，従来の約半分の期間(2か月)で必要なシステムを構築できた。

⑵ 顧客数の増加に対し，柔軟に対応できる

システムを仮想マシン上で構築することで，ハードウェアのリプレースなく，柔軟にサーバの処理性能を向上させていくことができる。そのため，サービス初期は少ないコンピュータ資源のみを使用するスモールスタートとし，顧客数の増加に応じて，段階的に使用するコンピュータ資源を増加させていくという運用を容易に行えるようになった。

4. SaaS型セキュリティ診断サービスの今後

最後に，MIND SaaS型セキュリティ診断サービスの今後の計画として，Webアプリケーションセキュリティ診断サービスの高精度化，及び脆弱性管理機能の強化について述べる。

4.1 SaaS型Webアプリケーションセキュリティ診断サービスの高精度化

SaaS型Webアプリケーションセキュリティ診断サービスが検出できる脆弱性の数は，Webアプリケーション内で診断ツールが巡回できる画面数と診断項目数に左右される。MINDは，より高い精度でWebアプリケーションの脆弱性を検出できるよう，①巡回できる画面数の増加，②診断項目数の拡充に取り組んでいく。

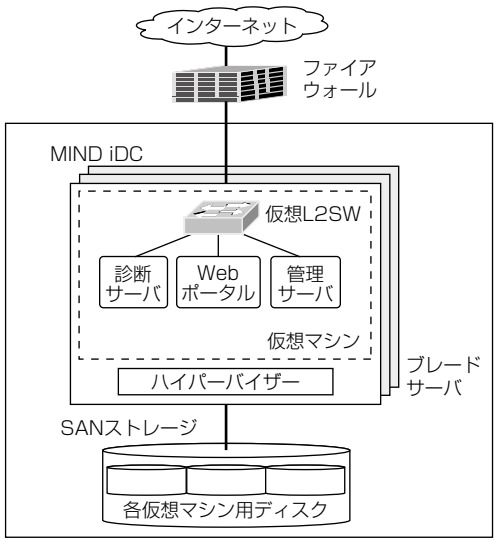


図2．MINDクラウド技術基盤

4.1.1 巡回できる画面数の増加

SaaS型Webアプリケーションセキュリティ診断サービスでは，診断対象サイトを自動巡回し，到達できた各ページを診断するため，到達できないページは診断対象から漏れてしまう。このようなページが発生する主な原因として，JavaScript(注2)によるページ移動が挙げられる。

JavaScriptによるページ移動は，ページ内のJavaScriptがブラウザを操作することで行われるページ移動を指す。このようなページ移動に対し，現在の診断システムでは，静的にJavaScriptを解析して移動先URLを推測するが，連結や置換等の文字列操作で生成されるURLまで認識することはできていない。

この課題を解決するため，今後は，従来の静的な解析に加え，動的な解析，すなわち，診断ツール内でJavaScriptを実際に動作させることで，移動先ページのURLを取得する方式についても検討を進めていく予定である。

自動巡回機能を継続的に改良する一方，ユーザーが必要に応じ，診断対象ページURLを追加できるよう，自動巡回できた範囲を簡単に確認できるようにする仕組みも必要である。例えば，巡回中にWebアプリケーションから返されたエラー画面などを自動認識し，エラーによって巡回が中断したページをユーザーに提示する機能などが有効と考えている。

(注2) JavaScriptは，Sun Microsystems, Inc. の登録商標である。

4.1.2 診断項目数の一層の拡充

2.1節で述べたとおり，現在のSaaS型Webアプリケーションセキュリティ診断サービスでは，OWASP Top 10で示されるハイリスクなWebアプリケーションの脆弱性に対応した診断サービスを提供している。

より高いセキュリティを求めるユーザーに対応するため，今後も継続して診断項目の拡充に努めていく予定である。それと並行し，既存の診断項目に対しても，診断アルゴリズムの改良に取り組んでいく。

4.2 脆弱性管理機能の強化

現状のSaaS型セキュリティ診断サービスは，Webアプリケーションやサーバ機器の“現在”の脆弱性の状況を報告する。しかし，セキュリティレベルを維持し続けるためには，日々の運用にセキュリティ診断を組み込み，脆弱性を早期に発見して，被害が発生する前に必要な対策を完了させる必要がある。このように管理サイクルとして診断と対策を継続的に行う“脆弱性管理”の考え方が重要となる。

脆弱性管理業務の中では，SaaS型サービスを使ったセキュリティ診断は単なる1ステップにすぎない。例えば，診断実施後には，検出された脆弱性に対するリスク評価や取るべき対策(パッチ適用，アプリケーション修正等)の決定，及び対策の実施が必要である。さらに，スケジュールや作業要員の管理といった業務全体の管理も行わなければならない。

これら脆弱性管理業務は，管理サイクルを早めれば早めるほど，またユーザーのネットワークが大規模になればなるほどユーザーにかかる負担は増大していく。

SaaS型ネットワーク診断サービスでは，診断システムが，検出された脆弱性の修正状況の表示など，脆弱性管理の支援機能を一部提供している。今後はSaaS型Webアプリケーションセキュリティ診断でもこれらの機能を提供するとともに，両者を統合して管理できるようにしていく予定である。

5. むすび

昨今のセキュリティ診断のニーズの高まりを受け，だれでも容易に利用可能なセキュリティ診断としてMINDが開発したSaaS型セキュリティ診断サービスについて述べた。

SaaS型セキュリティ診断サービスでは，診断ツールの機能がサービスとしてユーザーに提供される。ユーザーは，Webポータルを通じて簡単な設定を行うだけで，必要なときにいつでも診断を実施可能である。

今後MINDは，SaaS型Webアプリケーションセキュリティ診断の高精度化に取り組むとともに，脆弱性管理機能の強化に取り組み，企業のセキュリティ事故防止に役立つサービスを提供する予定である。

参考文献

(1) OWASP：OWASP Top 10-2010
http://www.owasp.org/index.php/Category : OWASP_Top_Ten_Project
(2) PCI Security Standards Council：PCI DSS-PCI Security Standards Council,
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml