

IDS/IPSログ解析サービス

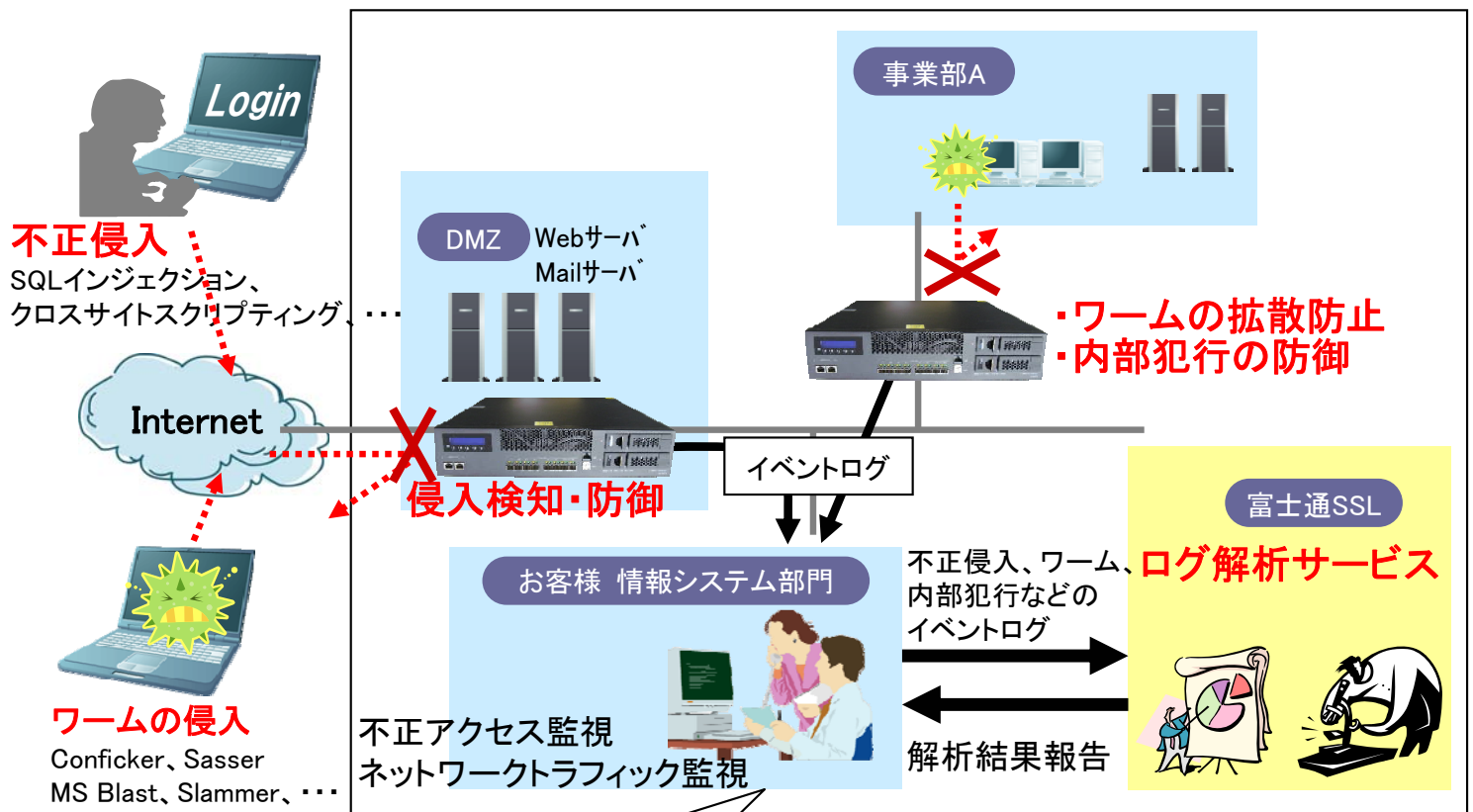


IDS/IPSのログをお客さまに代わって解析し、ご報告いたします。

ネットワークの不正アクセスを監視するためにIDS(不正アクセス監視システム)／IPS(不正侵入防御システム)を設置しても、適切に対処しなくては、セキュリティを保つことはできません。IDS/IPSを効果的に使用するためには、検知したイベントをセキュリティの専門家による解析を実施し、現状のセキュリティ運用へのフィードバックを行う必要があります。

サービスの特長

- ◇IDS／IPSが出力する大量のログをセキュリティの専門家が解析し、ひと目でシステムに対する影響の有無がわかる形式の報告書を作成します。
- ◇システムに影響を与えるイベントが含まれていた場合、対策についてアドバイスします。
- ◇個々のイベントの詳細な解析、それぞれのイベントの関連性、最新の攻撃のトレンドとの関係、過去の検出傾向との差異など、様々な観点から総合的な解析を行ないます。
- ◇セキュリティ強化のための予防策や改善策をアドバイスします。



- ・セキュリティ強化のためにIDS／IPSを導入したが、イベントが大量に通知され、何が起きているのかがよくわからない。
- ・大量のログの中から影響があるものだけを知りたい。
- ・通知されるイベントの傾向を知りたい。
- ・ポリシーを見直すために、イベントを詳しく解析したい。

ログ解析対象製品

IBM社製IPS IBM Security IPS
(旧:Proventia)

IBM社製IDS Server Sensor®

分析結果レポートサンプル

1. 概要

1.1 今月の傾向

表1 優先度 検出回数別 検出イベント数一覧

優先度	有	無	2000	3444
High				
Medium	有	40,000	2,000	3,444
Low	無	100,000	300,000	2,000,000

(1) イベントの優先度別 イベントのシステムへの影響有無や、増減の想定される原因を把握していただけるような報告をしております。

「High」
イベントの優先度を「High」としているイベントの検出件数の増加は、DNS系イベントの増加によるものです。
具体的なイベントとしては、「DNS_Spoof_Success」となっております。
今回の検出は、単独の検出であるため、DNSのなりすましを狙った攻撃でないと判断できるため、特に問題ありません。
詳細は、『2.1.2 DNS系のイベントについて』をご参照ください。

「Medium」
イベントの優先度を「Medium」としているイベントの検出件数の増加は、ICMP系イベントの増加によるものです。
具体的なイベントとしては、「ICMP_Redirect」となっております。
該当アクセスについては、FWにてDropする設定となっているため、特に問題ありません。
詳細は、『2.1.5 ICMP系のイベントについて』をご参照ください。

「Low」
イベントの優先度を「Low」としているイベントの検出件数の増加は、HTTP系イベント「HTTP_Authentication」が増加したためです。
イベントについては、HTTP Basic認証を用いた際の検出であり、通常のHTTPアクセスによるものと想定されるため、特に問題ありません。
詳細は、『2.1.4 HTTP系のイベントについて』をご参照ください。

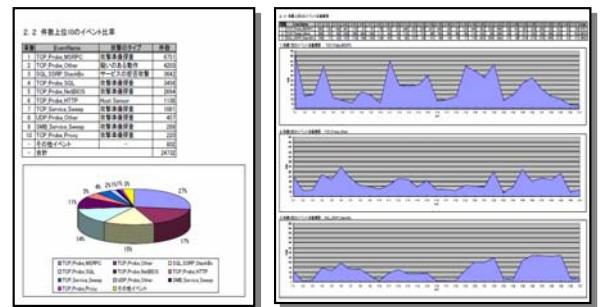
(2) Proventia 関連作業(監視センタ側で実施した作業)について記載しています。その月に実施された作業を把握するのに役立ちます。

a. XPU 適用作業
作業実施日時：
作業内容：Proventia XPU 30.050 適用作業
備考：特に問題無く完了しております。

1.2 危険な攻撃

(1) 特に危険と思われる Dos攻撃やシステムに存在する脆弱性を突くような攻撃の有無を把握していただけるような報告をしております。

- ・報告書は、イベントの説明と影響の有無を簡潔に記載します。
- ・影響があるものについては、処置や対策のアドバイスを記載します。
- ・報告書および報告の形式については、ご要望・ご予算にあわせてカスタマイズ可能です。
- ・最新のセキュリティ情報も報告書に記載し提供します。
- ・解析対象ログは、月／週／日のいずれの単位でも対応いたします。



サービスラインナップ

■IDS/IPSログ解析サービス(ライト)

検知・防御したログを、当社セキュリティスタッフがお客さまに代わり解析し、解析結果のサマリーのご報告と改善策のアドバイスを発行いたします。

■IDS/IPSログ解析サービス(スタンダード)

ログ解析サービス(ライト)に加え、検知・防御したログの詳細な解析結果も報告書に記載し、ご提供します。

■不正アクセス監視/防御サービス(ライト、スタンダード、アドバンスド)

お客様のネットワークシステム環境に合わせ、IDS/IPSの機能を最大限に引き出し、セキュリティパッチ対策、ワームの拡散防止や不正侵入を防御します。

※記載の会社名、商品名は、各社の商標または登録商標です。
※記載された情報は、予告なく変更することがあります。
※記載の内容は、2010年10月現在のものです。

SafetyValueとは、安心・安全・信頼・事業継続分野における富士通株式会社のブランドです。
サービス素材の一部は、SafetyValueの一環としてご提供しております。
PoweredSolutionは、富士通SSLのソリューション商品体型の名称です。

●当社ホームページ <http://www.ssl.fujitsu.com>

株式会社富士通ソーシャルサイエンスラボラトリ
(富士通SSL)

お問い合わせ先

お問い合わせ総合窓口
〒211-0063 川崎市中原区小杉町1-403 武蔵小杉タワープレイス
E-mail: ssl-info@cs.jp.fujitsu.com
TEL 044-739-1251