国立大学法人　長岡技術科学大学様

情報セキュリティ監査業務
セキュアドサーバ外部監査実施結果報告

平成30年3月1日（木）

株式会社ＩＴスクエア
〒950-0088　新潟市中央区万代３－１－１

１．情報セキュリティ監査の概要

目的

情報システムの運用や設定が本学の情報セキュリティポリシー及び情報セキュリティに関する諸規定に準拠して行われているか確認し、その結果を元に改善を行い、情報セキュリティレベルの向上、維持を図ることを目的とする。

手法

情報システム機器及びセキュアドサーバを対象に、インターネットから脆弱性スキャンを実施。公開ポートに対して擬似的な攻撃パケットを送信し、そのレスポンスからサーバ上で稼働している各種サービスに脆弱性が存在するかの確認を行う脆弱性検査方式。

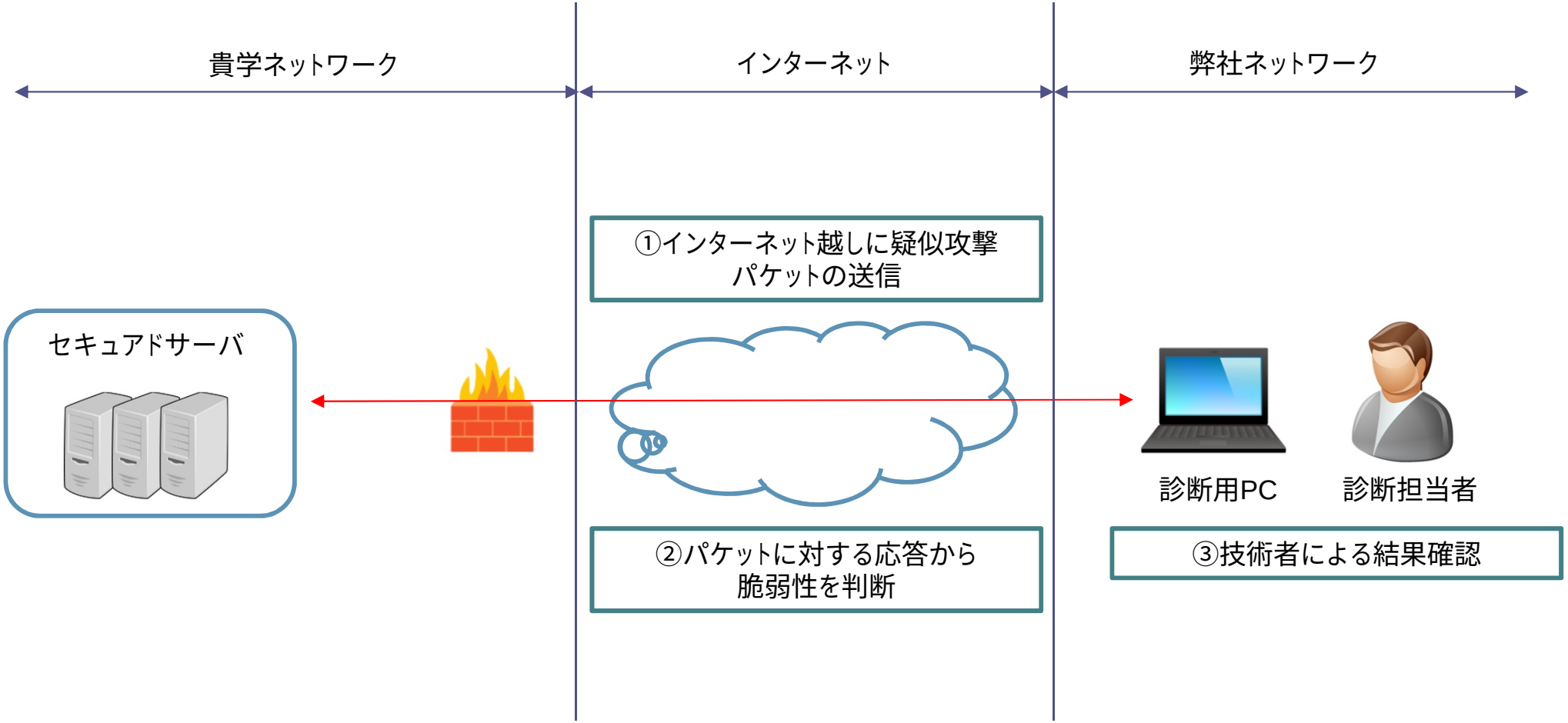
対象

セキュアドサーバ：35台

検査実施期間

2017年9月12日～19日

２．イメージ


貴学ネットワーク
インターネット
弊社ネットワーク
①インターネット越しに疑似攻撃
パケットの送信
セキュアドサーバ
診断用PC
診断担当者
②パケットに対する応答から
脆弱性を判断
③技術者による結果確認

３．検査手順

- ポートスキャン

  Nmapを用い、対象機器上でインターネットに公開されているTCP/UDPポートを洗い出す。公開されているポートのバナー情報を取得などを試みる。

- 脆弱性スキャン

  Retina Network Scannerを用い、公開ポートに対して疑似攻撃パケットを送信。4万以上の項目を検査。

- 手動確認

  脆弱性スキャンの結果、誤報がないかを技術者による手動でのコマンド入力等で確認。

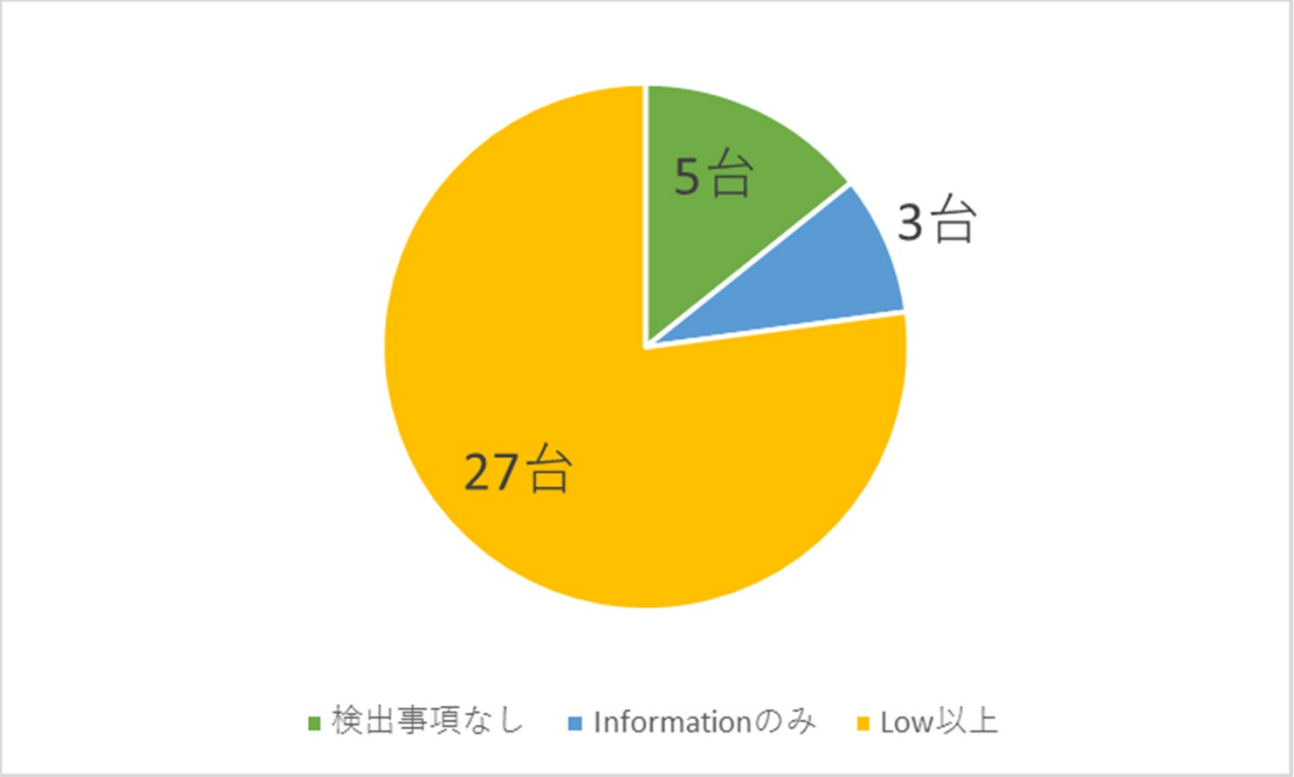
３．指摘事項に対する評価基準

項番	ﾘｽｸﾚﾍﾞﾙ	脆弱性の内容	緊急度	対策の必要性
1	High	・脆弱性をついて攻撃されると個人情報や機密情報が漏洩する可能性がある。 ・脆弱性により侵入されデータの破壊、漏洩、改竄の可能性がある。	緊急に対応を行う必要がある。	即座に対策が取れない場合、サービス停止等、暫定対処が必要
2	Medium	・脆弱性情報が一般に公開されており、影響度が高い。 ・脆弱性をついて攻撃された場合、深刻な影響を受ける。	早い対応が必要。（概ね1ヶ月以内、定期保守等での対応など）	対策を行うことを強く推奨。
3	Low	・脆弱性情報が一般に公開されているが、影響度が低い。 ・攻撃者にとってかなり有用な情報を与えてしまう	出来るだけ早い対応が必要。（概ね3ヶ月以内、他のメンテナンスと同時での対応など）	対策を行うことを推奨。
4	Information	・攻撃者に有用な情報を与えてしまう。 ・他の脆弱性と組み合わされる事により重大な脆弱性に繋がる可能性がある。	対応を行うか検討する必要がある。 （概ね6ヶ月以内）	運用上等、問題が無いようであれば対策を行うことを推奨。

4．結果

対象	指摘件数			
	High	Medium	Low	Information
セキュアドサーバ	0件	4件	62件	55件

- 35台中指摘件数0件のサーバは5台。
- 対応が求められるLow以上の指摘が検出されたサーバは27台（うちMediumが指摘されたサーバ4台）



5．総評

- 今回の監査では、直ちに侵入や情報漏えいに繋がる、リスクレベル「High」の脆弱性は検出されなかった。一部のサーバでクロスサイトスクリプティングの脆弱性、内部情報を含んでいると思われるコンテンツの公開、アプリケーションが最新でないことに起因する脆弱性、暗号化の強度に関する脆弱性等が検出された。

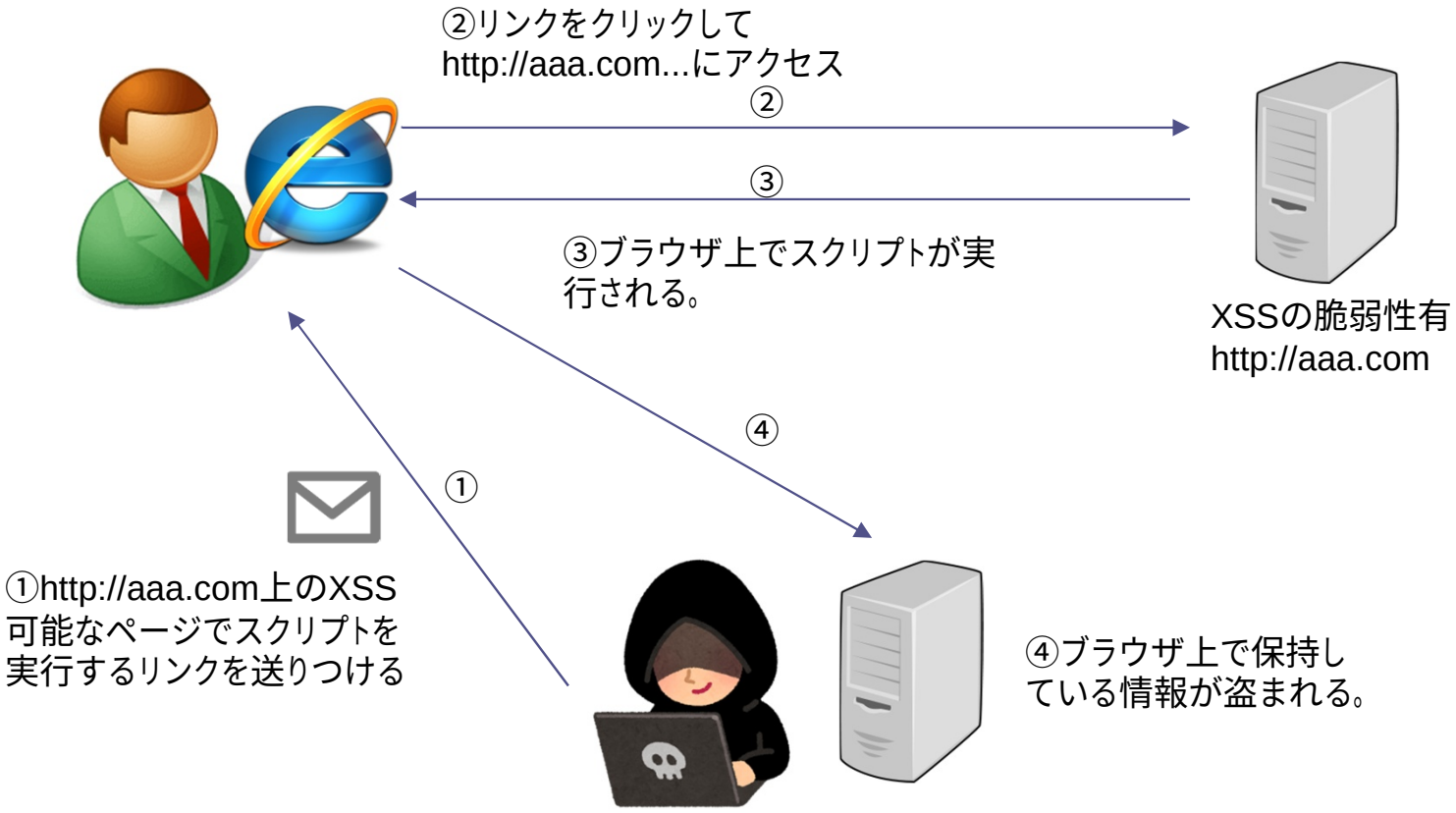
- 本監査の対象とならなかったネットワーク機器、サーバ機器についても以下の点を確認することを推奨。

・定期的にアプリケーションのバージョンアップを行っているか
・定期的にセキュリティパッチを適用しているか
・不要なサービス、ポートは公開していないか
・Webアプリケーションの入力値チェックを厳密に行っているか

６．クロスサイトスクリプティングの脆弱性（Medium）

- Webアプリケーション上で動的にページを生成するような画面（例：検索画面、問い合わせフォーム等）において、ブラウザから渡される入力値のチェックが不十分なために不正なスクリプトの実行が可能となってしまう脆弱性。偽HPへの誘導やブラウザが保持しているCookie等の情報の窃取が可能。

クロスサイトスクリプティングの一例



7．その他の脆弱性(1)

- 内部情報が含まれたコンテンツがインターネットに公開（Medium）

→不要なコンテンツを削除した上でどうしても共有したい情報がある場合は、IPアドレスによるアクセス制限を設けるか、FTPSサーバなどセキュアな方式で公開を行うこと。

- サポートが終了したOSの使用（Medium）

→Microsoft Windows Server 2003 (2015年7月15日サポート終了)の使用が確認された。サポートが終了したOSについては特別な事情を除いてセキュリティパッチがリリースされないことから、脆弱性への対応が非常に困難である。

参考：Microsoft 製品のライフサイクルの検索

https://support.microsoft.com/ja-jp/lifecycle/search/

7．その他の脆弱性(2)

■脆弱な暗号化方式をサポートするSSLサービス（Low）

→https（TCP/443)などSSL通信を行うサービスにおいて使用が推奨されない脆弱な暗号化方式を使用しているサーバが見られた。

プロトコル：SSLv2,SSLv3　アルゴリズム：RC4,128bit未満のビット安全性

参考：SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～　https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

■古いソフトウェアのバージョンに起因する脆弱性（Low）

→バナー情報（バージョン情報）を外部に公開しているサーバが見られた。公開されているバージョン情報＝実際のバージョン情報とは限らないが、古いバージョン情報を公開している場合に攻撃者に目をつけられる可能性があるため、隠蔽する必要がある。

→定期的なバージョンアップ、セキュリティパッチの適用を推奨。

8．フォローアップ診断

- 前述の診断結果を各サーバ管理者に送付し、2017年12月20日を期限として今後の対応について是正計画書の記載を依頼した。

①対応完了→OK

②対応中、又は対応予定→対応期限の記載があればOK。

③対応しない→予算等の都合により対応しない、リスクを承知の上で未対応とする等…

- 全35台の是正計画書について対応内容に問題ないかの確認を実施した。

検査結果兼是正計画書

No.	確認事項	リスクレベル	検出対象	確認事項説明 (想定される影響)	推奨対応方法	対応状況	対応内容	ITS確認
1	検出されたポート一覧	-	【検出されたポート】 80/tcp	検出対象に記載のポートが開放されています。 不要なポートが開放されている場合、攻撃者に悪用される可能性があり、セキュリティリスクが高まります。	開放されているポートが必要か確認し、必要最低限のポートのみ開放するようにしてください。	対応しない	80/tcpは学外向けWebサーバとして開放しており、今後も運用を継続する。	問題なしと判断します。

No.	脆弱性名称	リスクレベル	検出対象	脆弱性説明 (想定される影響)	推奨対応方法	対応状況	対応内容	ITS確認
1	バージョン情報の表示	Information	【検出されたポート】 80/tcp 【得られたバージョン情報】 Apache httpd/2.2.X (FREEBSD)	HTTPリクエストを送った際のレスポンスヘッダにサーバの詳細なバージョン情報が表示されています。 バージョン情報の公開は、攻撃者にとって有用な情報を与えてしまう可能性があります。	【Apache】 Apacheの「httpd.conf」に下記の設定を行うことで、レスポンスヘッダにApacheのバージョン情報が表示されなくなります。 ①httpd.confを編集し下記の設定を行います。 ServerTokens ProductOnly ②設定変更後、httpd.confを保存し、Apacheを再起動します。	対応完了	2017/11/17に対応完了、学術情報誌へ報告済み。	問題なしと判断します。

参考：JVN iPediaによる脆弱性情報収集

- JVN iPedia(https://jvndb.jvn.jp/index.html）では製品名やベンダ名、ソフトウェア名などで検索が可能な脆弱性情報データベースを公開しています。