

クラウドサービス活用によるセキュリティラボの構築

会員名：株式会社トインクス（東北支部）

会社概要

名称：株式会社トインクス
所在地：宮城県仙台市青葉区中央二丁目 9 番 10 号
設立年月日：2001 年 7 月 1 日（合併）
代表者：取締役社長 八代 浩久
資本金：9,680 万円
従業員数：757 名（2023 年 4 月現在）
事業内容：情報システムおよび情報ネットワークに関するコンサルティング、開発および運用業務

執筆者



開発運用本部
基盤技術部
サイバーセキュリティ
センター
主査

大久保 孝毅
(代表執筆者)

要旨

当社では、2017 年度より情報セキュリティの監視および調査分析の運用検討を実施し、Security Operation Center を運用し、東北電力および東北電力グループ企業のセキュリティ監視業務を実施している。

セキュリティ業務を担うセキュリティ人財のスキル向上を目的として、外部団体にて開催されるセキュリティ演習へ参加していたが、2020 年初めからのコロナ感染拡大により、セキュリティ演習も含め集合教育が中止されるケースが増加し教育受講の機会が失われていた。

このことを契機にセキュリティ人財のスキル向上を目的とした自社環境を検討し、セキュリティ新技術の検証および実践に近い訓練ができる疑似環境としてセキュリティラボの検討および構築を実施した。

セキュリティラボの構築にあたっては、オンプレミスおよびクラウドサービスでの構築による費用面、機能面での比較を行った。機能差は許容範囲であり費用面ではオンプレミスに比べ低コストで実現可能であることから、クラウドサービス活用による構築を選択した。

一般的には同等環境を構築する場合にはオンプレミスよりも高コストとなるクラウドサービスについて、セキュリティラボの運用形態によりクラウドサービスを活用することにより安価に環境維持を実現することが出来た。

目次

1 序論	1
2 セキュリティラボ検討の流れ	1
2.1 セキュリティラボ構築スケジュール	1
2.2 セキュリティラボ要件の整理	2
2.3 セキュリティラボ整備の目的の設定	3
2.4 セキュリティラボの構成	3
2.4.1 全体構成イメージ	3
2.4.2 設備構成の検討	4
2.4.3 当初の構築範囲	7
3 セキュリティラボの構築および利用	8
3.1 セキュリティラボの構築	8
3.2 セキュリティラボの活用	8
4 今後の見通し	10
4.1 セキュリティラボ環境の拡充	11
4.2 クラウドサービスの利用検討	11
4.3 サービスの提供拡大に向けた検証	11
5 結論	11

1 序論

株式会社トインクスは、東北電力グループの一員として東北電力および東北電力グループ企業を中心に東北地方の企業をIT面から支える企業として、情報システムの企画・コンサルティングから開発、運用、保守までの一貫した情報システムサービスの提供を行っている。

筆者の所属するサイバーセキュリティセンターでは、セキュリティ対策製品の導入および維持管理、セキュリティ監視業務を担当している。

近年、社会インフラに被害を与えるサイバー攻撃の脅威が増加していることに加え、東京オリンピック・パラリンピックの開催によりサイバーセキュリティリスクの増加が予測されたことから、電力インフラのセキュリティ体制の強化が求められた。

当社では、2017年度より情報セキュリティの監視および調査分析の運用検討を実施し、Security Operation Center（以下、SOCと略す）の運用を開始し、東北電力および東北電力グループ企業のセキュリティ監視業務を実施している。

セキュリティ業務を担うセキュリティ人財のスキル向上を目的として、日立製作所 大みか事業所などの外部団体にて開催されるセキュリティ演習への参加を行ってきたが、2020年初めからのコロナ感染拡大により、セキュリティ演習も含め集合教育が中止されるケースが増加し教育受講の機会が失われていた。

このことを契機にセキュリティ人財のスキル向上を目的とした自社環境を検討し、セキュリティ新技術の検証および実践に近い訓練ができる疑似環境としてセキュリティラボの構築を実施した。

本論文では、セキュリティラボ環境の実現について、オンプレミスおよびクラウドサービスでの比較検討を行い、クラウドサービスを活用することで用途に応じた検証環境を柔軟に構築できるラボ環境を低コストで実現した事例を紹介する。

2 セキュリティラボ検討の流れ

2. 1 セキュリティラボ構築スケジュール

セキュリティラボの構築スケジュールは図1の通りである。

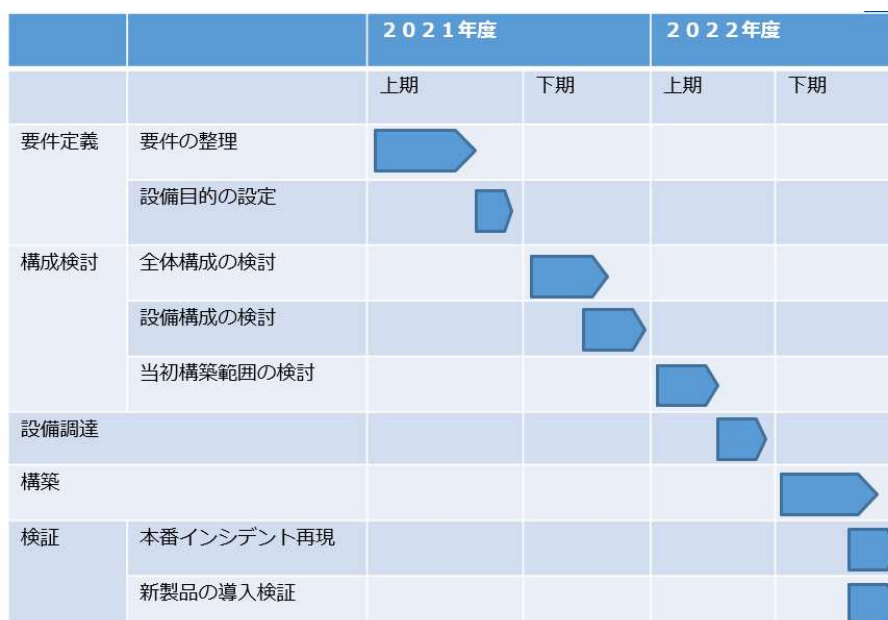


図1 構築スケジュール

2021年度よりセキュリティラボの検討を開始し、2021年度は要件定義としてSOC運用の実務者および過去に外部団体のセキュリティ演習を受講したメンバーを中心にセキュリティラボの活用方法についての検討および整備目的を設定、セキュリティラボの全体構成イメージを作成、要件を実現するために必要となる設備構成の検討を実施し設備構成の検討の結果、オンプレミスより低コストでの実現が可能であったためク

クラウドサービスを活用することとなった。

2022 年度上期にはクラウドサービスを利用することにより機能拡張を容易に行える環境となったことから、全体構成イメージから当初必要となる構築範囲を選定し設備調達を実施した。2022 年度下期よりセキュリティラボ環境の構築を開始し、本番インシデントの再現および新製品の導入検証の場として利用を開始した。

2. 2 セキュリティラボ要件の整理

セキュリティ演習など外部教育等による教育機会が失われたことを契機として、セキュリティラボの検討を開始した。当初は図2のような過去に参加したセキュリティ演習の環境を基本として、モノづくり、新技術検証、訓練など自由に利用できる環境を目指した。

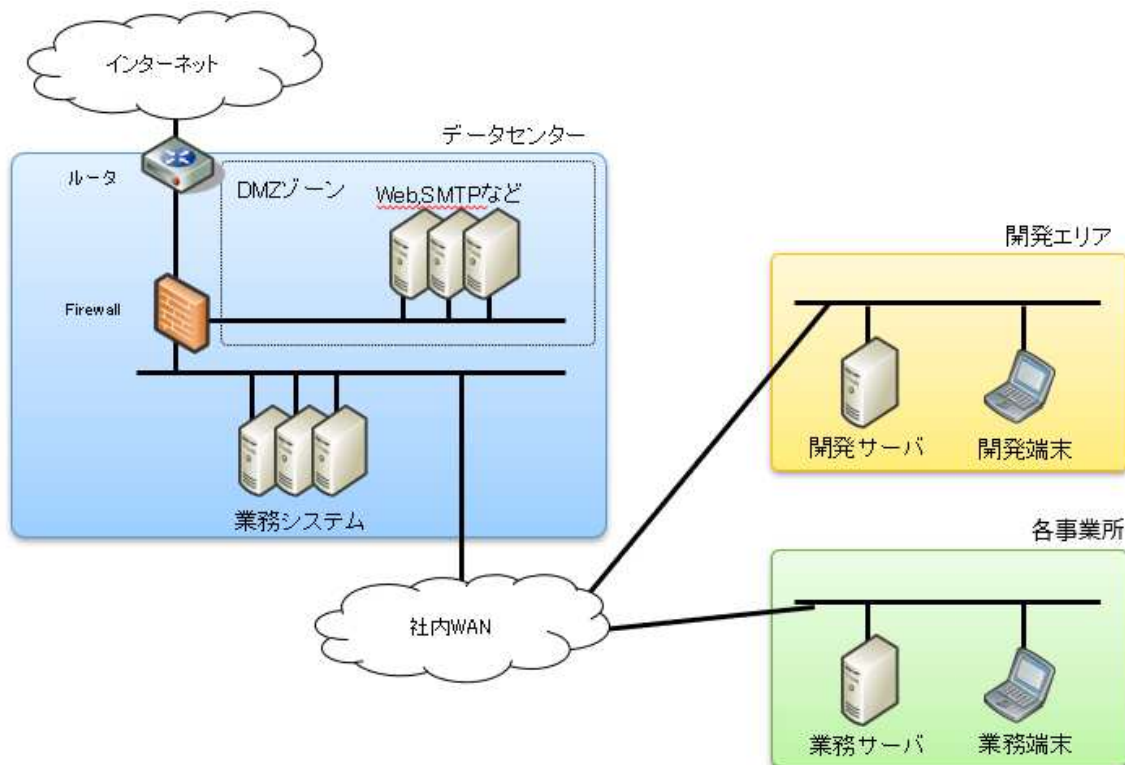


図2 セキュリティ演習をベースとした構成イメージ

セキュリティ運用を担う SOC 運用の実務者および過去に外部団体のセキュリティ演習を受講したメンバーを中心に、セキュリティラボの活用方法について意見集約を行い、以下の通り要件を整理した。

- ・疑似攻撃者環境（レッドチーム）を有すること
- ・疑似攻撃やウイルスの挙動確認など本番環境で実施出来ないことを検証可能であること
- ・顧客の本番環境に影響を与えない安全で独立した環境であること
- ・本番環境で使用している技術・製品を出来るだけ採用し本番環境でのインシデントを再現できること
- ・被攻撃機器について、攻撃後容易に復旧できること
- ・新製品のトライアル、PoC などを受け入れ可能であること
- ・新規受け入れ要員に対して、教育の場として利用できること

自社内に環境構築を行うことから、外部教育のような汎用的なセキュリティ教育の環境ではなく実運用に近い環境を整備する方針とした。

2. 3 セキュリティラボ整備の目的の設定

要件整理の結果からセキュリティラボ整備にあたりセキュリティ業務従事者のスキル向上を主目的として、顧客疑似環境での本番インシデントの再現およびセキュリティ新技術の検証といった2つ目的を設定した。

(1) 顧客疑似環境での本番インシデントの再現

顧客環境にて利用している技術および製品をできるだけ多く採用した顧客疑似環境を構築することで、実践に近い訓練や転入者などに対して実機操作を通じてより実践に近い導入教育を行うことを可能とする。

セキュリティラボは本番環境から安全で独立した環境として構築することで、顧客の本番環境に影響を与えずに疑似攻撃者環境からの疑似攻撃によるインシデント再現を可能とする。

本番環境における重大インシデントの発生頻度が少ないことからセキュリティラボにて過去のインシデントを再現し、本番環境と同じ製品を利用していることにより、本番環境でのインシデント発生時と同等のエラーログなど同等の挙動を再現し、インシデント対応を実施することで SOC 要員のスキルアップを目指す。

(2) セキュリティ新技術の検証

セキュリティラボにて検証を行うことにより、各種メーカの最新セキュリティ技術ソリューションを顧客の本番環境に近い状況で検証することを可能とする。疑似攻撃者環境からの疑似攻撃による新技術の有効性の確認などの検証を通じ、最新のセキュリティノウハウを身に付けることを期待できる。

新技術検証によるスキルアップだけではなく、セキュリティラボで検証した結果から顧客への導入提案、他の自社サービスと連携した新たなセキュリティビジネスの検討に繋げる。

2. 4 セキュリティラボの構成

2. 4. 1 全体構成イメージ

本番インシデントの再現および新技術の検証として設定したセキュリティラボの目的から、実際に SOC にて監視している顧客環境を基本として全体構成を検討した。

疑似顧客環境として DMZ/社内サーバ/開発エリア/運転監視を配置した環境に、疑似攻撃を実施するレッドチームと疑似インターネットとして疑似企業を配置した環境を全体構成イメージとして図3に示す。

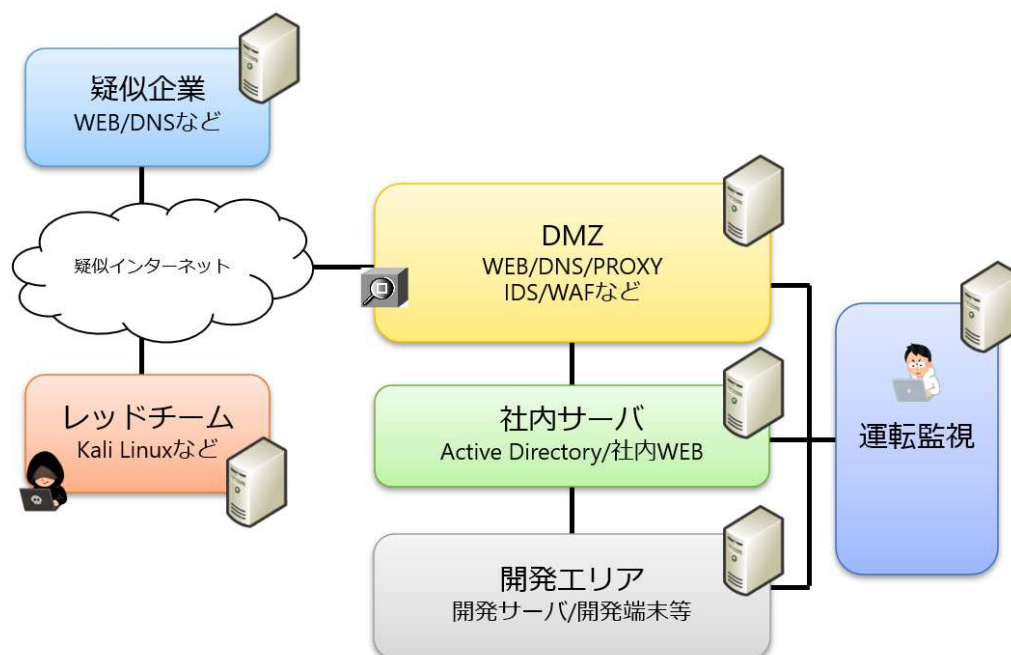


図3 全体構成イメージ

2. 4. 2 設備構成の検討

本番環境に影響を与えずに疑似攻撃により本番インシデントを再現し、疑似攻撃後に容易に復旧可能であるという要件より、復旧容易性から仮想環境での構築を実施するものとし設備構成の検討を実施した。

環境の設定にあたってはオンプレミスとクラウドサービスの利用での環境構築を想定し、費用面および機能面での検討を実施した。

比較の結果としてクラウドサービスを利用してセキュリティラボを構築することとし、検討内容については以下に記載する。

(1) 費用比較

ミドルウェアについては環境間で利用製品および費用差は少ないものと考え OS/ネットワークといったハードウェア観点での費用比較を実施した。同条件での費用比較を行うため全体構成イメージより図4に示すベース構成を設定し、5年間のランニングコストを考慮して費用算出を実施した。

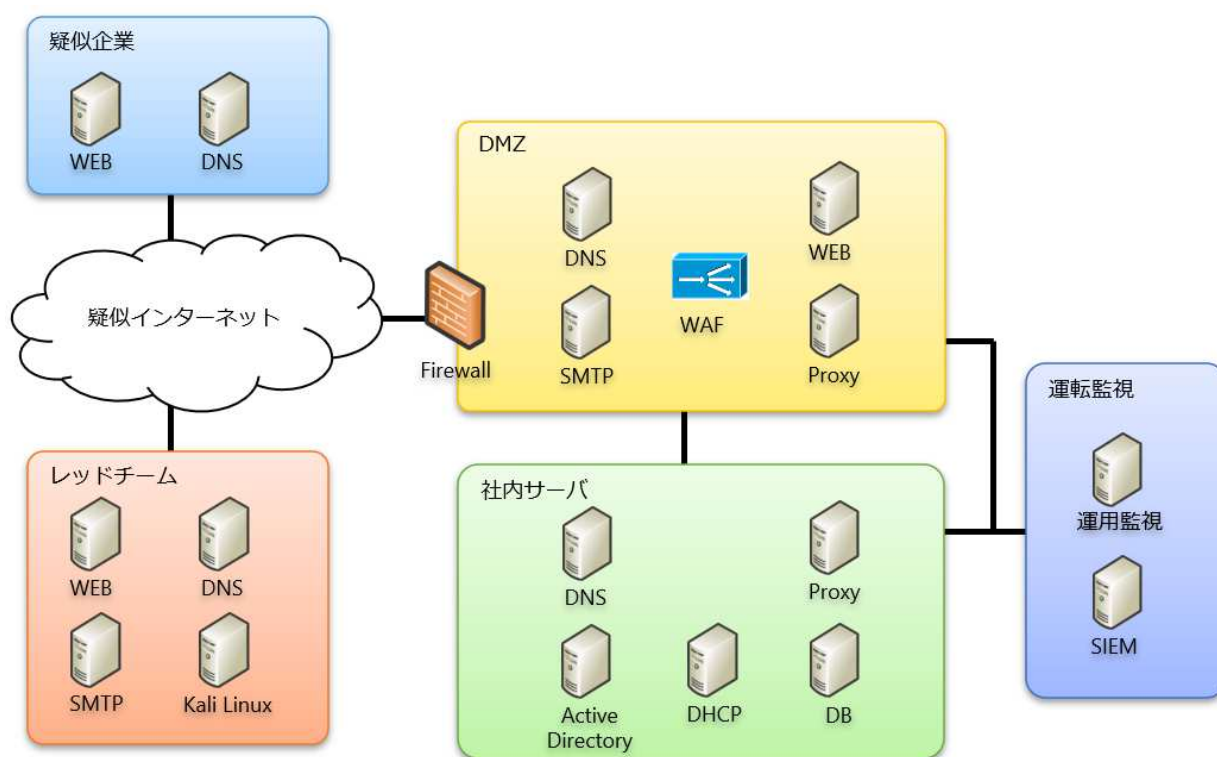


図4 セキュリティラボ ベース構成案

オンプレミスはVMware vSphereによる仮想化環境を利用するものとし、サーバ構成よりLinuxサーバが主体となることから物理サーバはLinux用2台、Windows用1台の構成で試算した。

オンプレミスでは物理リソースが拡張上限となるため将来的な拡張を見越した余剰リソースを考慮した構成とし、柔軟な機能拡張が行える環境を確保する。

本条件での試算結果を表1に記載する。

表1 オンプレミス構成 試算結果

単位：千円

品目		数量	導入費	保守費(5年)
ハードウェア	サーバ CPU:Xeon Gold 12core メモリ:256GB	3	6,458	1,088
	ストレージ(15TB)	1	2,705	441
	SAN-SW	2	1,831	157
	L3SW	1	516	405
	ラック一式	1	669	0
ソフトウェア	VMware 一式	1	1,032	1,786
	Red Hat Linux Virtual Datacenters	2	544	2,718
	Windows Server Datacenter	1	805	0
合計			21,155	

クラウドサービスは Amazon Web Service(以下、AWS と略す)を利用して構築するものとし、サーバ台数(インスタンス数)にて費用試算を行う。AWS は利用時間による課金となるため平日日中の利用を想定し月160 時間(20 営業日×8 時間)にて費用試算を実施した。AWS 料金単価は\$ 単位となるため、昨今のレートより150 円/\$ で試算した。また、参考として月720 時間(30 営業日×24 時間)での試算結果も掲載する。

本条件での試算結果を表2 に記載する。

表2 クラウドサービス 試算結果

単位：千円

品目		数量	160 時間/月 ×5 年間	720 時間/月 ×5 年間
疑似企業	Linux サーバ	2	790	3,141
レッドチーム	Linux サーバ	4	1,581	6,282
DMZ	Linux サーバ	4	1,581	6,282
	Network 機器(Firewall/WAF)	2	1,053	4,612
社内	Linux サーバ	2	790	3,141
	Windows サーバ	3	1,338	5,396
運用監視	Linux サーバ	2	790	3,141
合計			7,923	31,995

費用比較においては試算結果の通り、クラウドサービス利用の方が低コストでセキュリティラボの実現が可能である。また、セキュリティラボにおいては検証に必要なサーバのみ起動すればよいため今回の試算条件のように全サーバを同時稼働させる必要性はなく、実際には試算値より低コストでの運用が可能であると考ええる。

常設時の試算結果の通り同等構成にてクラウド環境にサーバ構築をする場合は、一般的にはオンプレミスより費用が高くなり、オンプレミスからの単純なクラウドシフトにはコストメリットは無いが、常設が求められず今回のように検証目的の環境のように必要に応じて稼働停止が出来る環境においてはコスト面でのクラウド利用も選択肢となりうると考える。

(2) 機能面・各構成のメリットデメリット

機能面でのオンプレミスおよびクラウドサービスの比較としては、セキュリティラボの要件から本番インシデントの再現、攻撃後の復旧の容易性、新技術の検証の3点を重点として比較を実施した。

比較結果を以下の分類で表3に記載する。比較結果の詳細は後述する。

- (a) 本番インシデントの再現
- (b) 攻撃後の復旧の容易性
- (c) 新技術の検証

表3 メリットデメリット比較結果

比較項目	メリット	デメリット
オンプレミス	(a) 詳細なバージョン選択が可能であり、本番と同バージョンでの環境構築が可能 (b) 復旧要件に応じて柔軟な手段の選択が可能	(c) 評価製品のライセンス購入、評価ライセンスの取得が必要
クラウドサービス	(c) 利用期間に応じてライセンス方式を選択することで安価に製品利用が可能	(a) 製品バージョンが定期的に最新化されるため古いバージョンの確保が難しい (b) オンプレミスに比べると柔軟性が低い

本番インシデントの再現、攻撃後の復旧の容易性についてはオンプレミスが優位となるが、クラウドサービスでも許容範囲である。新技術の検証についてはクラウドサービスの利用により柔軟な対応が可能であると考ええる。

(a) 本番インシデントの再現

本番インシデントの再現のためには本番環境に近い環境を構築する必要がある。

オンプレミスではVMware vSphereでのサポートバージョンの範囲内にはなるが、詳細なバージョン選択が可能であり、本番と同バージョンでの環境構築が可能である。

クラウドサービスでは製品ごとにバージョンが決まっており定期的に最新化され、古いバージョンの確保が難しい。セキュリティ演習のような意図的に脆弱性の持つバージョン構成のソフトウェアを確保することは難しいが、疑似本番環境として本番インシデントを再現する環境を構築する際はマイナーバージョンの違いに留まるため許容範囲である。

(b) 攻撃後の復旧の容易性

被攻撃機器について攻撃後容易に復旧できることについては、オンプレミスについてはVMware vSphereにてスナップショット機能およびRed Hat Enterprise LinuxのrearなどのOS標準のバックアップ機能を利用したバックアップリストアが利用可能であり、復旧ポイントや復旧対象数・リカバリ時間など復旧要件に応じて柔軟な手段の選択が可能となる。

クラウドサービスについてはEC2インスタンスに割り当てられたボリュームのスナップショットを活用し、ボリューム再作成からの再割り当て、新規インスタンスでの再生成などの手段により攻撃前の状態に復旧することは可能であるが、オンプレミスに比べると柔軟性が低いものと考ええる。

(c) 新技術の検証

新技術および新製品の検証については、OS 上で稼働するミドルウェアについては、仮想化製品/クラウドサービスでの利用制限等が無い限りはオンプレミス/クラウドサービスどちらでも同等と考えられる。

アプライアンス製品については、オンプレミスでは VMware vSphere に対応した仮想アプライアンスであればライセンス購入や評価ライセンスの取得により導入および評価が可能である。

クラウドサービスにおいては AWS Marketplace にて VMware vSphere 等の仮想化製品に対応した仮想アプライアンスは利用できる製品が多く、利用可能な製品についてはオンプレミスと同等となる。ライセンスについては自己所有ライセンス方式、従量課金方式の利用が可能であり、利用期間に応じてライセンス方式を選択することにより安価に製品利用が可能である。オンプレミスと同様に評価ライセンスを取得して自己所有ライセンス方式で利用することも可能であるが、従量課金方式を利用することによって期間制限のある評価ライセンスよりも長い期間の利用、正規ライセンス購入より安価で利用などの対応が可能となる。

今回の対応例として Firewall 製品で Cisco ASA と FortiGate を利用したが、機能評価を目的とした FortiGate については従量課金方式で利用し、長期利用予定であった Cisco ASA については自己保有ライセンス方式での利用を選択した。

2. 4. 3 当初の構築範囲

クラウドサービスを利用する方針としたため、機能要件に応じて後から柔軟に環境拡張が可能となることから、初期構築範囲は SOC 運用にて主要な監視範囲となる DMZ を中心として、図 5 に記載した疑似インターネットから DMZ までを範囲を当初の構築範囲として設定し、2022 年度の構築作業を行った。

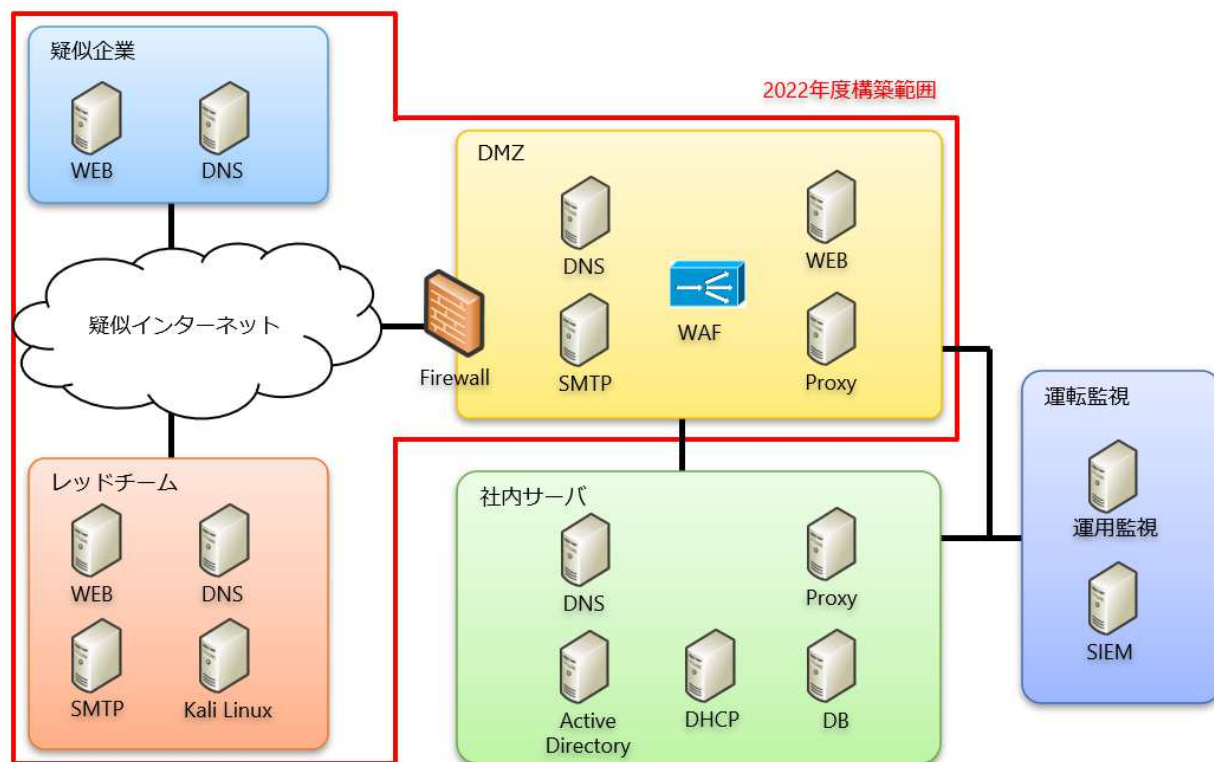


図 5 当初の構築範囲

3 セキュリティラボの構築および利用

3. 1 セキュリティラボの構築

AWS にて構築したセキュリティラボの構成を図 6 に示す。

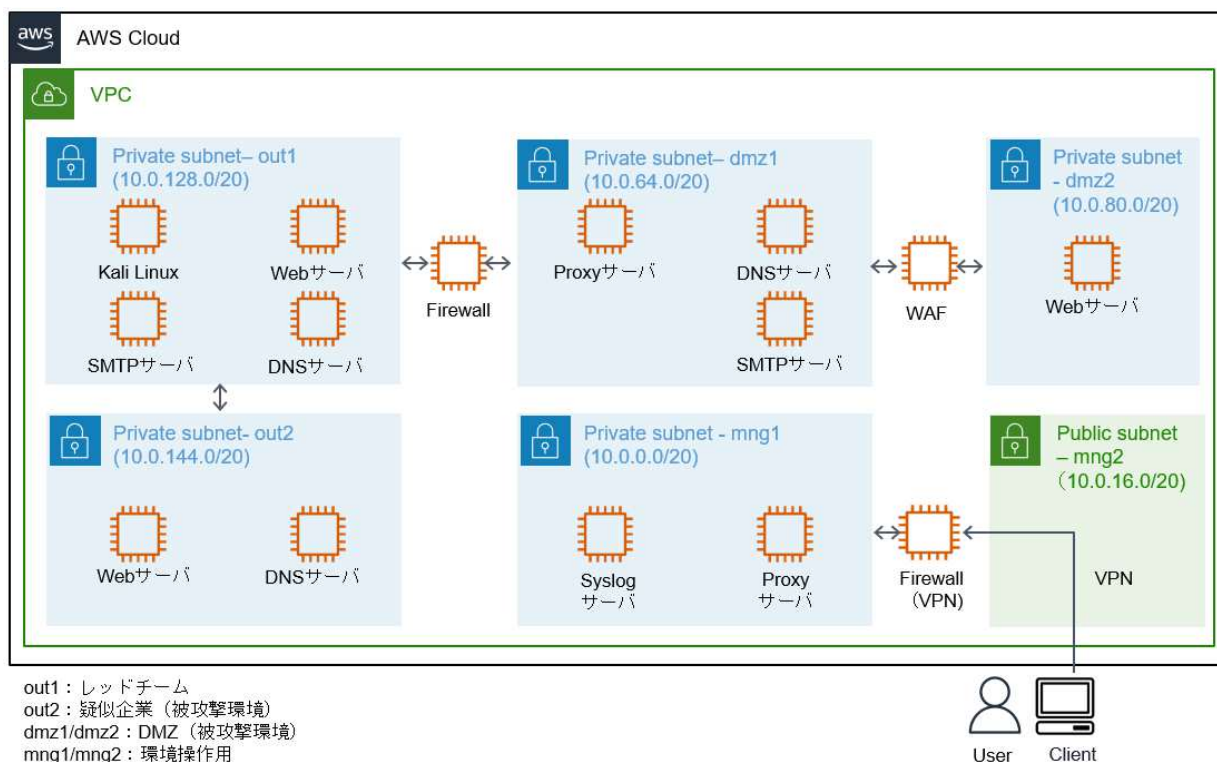


図 6 セキュリティラボ構成図

セキュリティラボは疑似攻撃などのセキュリティインシデントの再現を行うという性質から、誤操作等による外部への攻撃を防止する必要がある、セキュリティラボ内から直接インターネットへの接続は出来ないようにする必要があった。

セキュリティラボ内のネットワーク (VPC) 構築にあたり、内部通信のみ可能とする Private subnet とインターネット接続可能な Public subnet とサブネット単位でインターネットアクセス可否について定義を行った。セキュリティラボの各エリアは Private subnet とし、Private subnet と Public subnet の境界には管理エリアを設置した。セキュリティラボとインターネットとの通信は管理エリア経由で実施する。

セキュリティラボとインターネットの通信としては、環境の構築維持とユーザからのセキュリティラボの操作を想定している。

環境構築時にパッケージ導入や仮想アプライアンスのライセンス認証などインターネット接続が必要なものは管理エリアに設置した Proxy サーバを経由で行うものとし、宛先ドメイン名にて最低限必要なアクセス制限を実施する。ユーザからのセキュリティラボの操作については、管理エリアに設置された Firewall に VPN 接続することで利用可能とした。

3. 2 セキュリティラボの活用

2022 年度下期にはセキュリティラボの利用目的である疑似顧客環境での本番インシデントの再現および新製品の導入検証を実施した。

(1) 本番インシデントの再現

本番インシデントの再現例として、ホームページへの DDoS 攻撃について記載する。当該インシデントはホームページサーバに対して SYN Flooding より DDoS 攻撃が行われホームページへのアクセス不可となっ

た事象である。

疑似攻撃としてはレッドチームの Kali Linux から Firewall 経由で DMZ Web サーバに SYN Flooding 攻撃を実施することで再現した。具体的には hping3 ツールにて送信元 IP をランダム生成して SYN パケットのみ送信を繰り返すことで実施した。

当初実行時は送信元 IP をランダムで実施した際には、Firewall まで疑似攻撃が到達せずインシデントが制限出来なかった。送信元 IP を Kali Linux の実 IP からとした場合には SYN Flooding は再現するが本番インシデント以外の挙動も確認され、本番インシデントの再現とは言い難い結果となった。

原因としては AWS ではデフォルト設定により、図7のようにネットワークインターフェイスにて送信元/送信先のチェックを行っており、インスタンス自身が保持していない IP アドレスではトラフィックを送信できない仕組みとなっているためであった。

本機能を無効化することにより、Firewall にて本番インシデントと同様のログが出力されることを確認し当該インシデントの再現が可能であることを確認した。

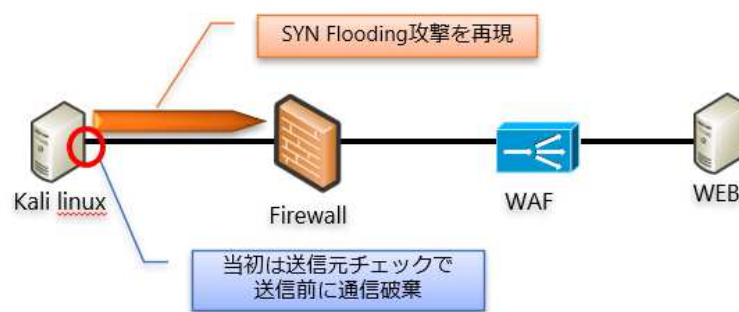


図7 AWSの通信チェック

本件のように意図的に不正通信を実施する際にはクラウドサービス自身のセキュリティ機能との競合について考慮が必要である。

(2) 新製品の導入検証

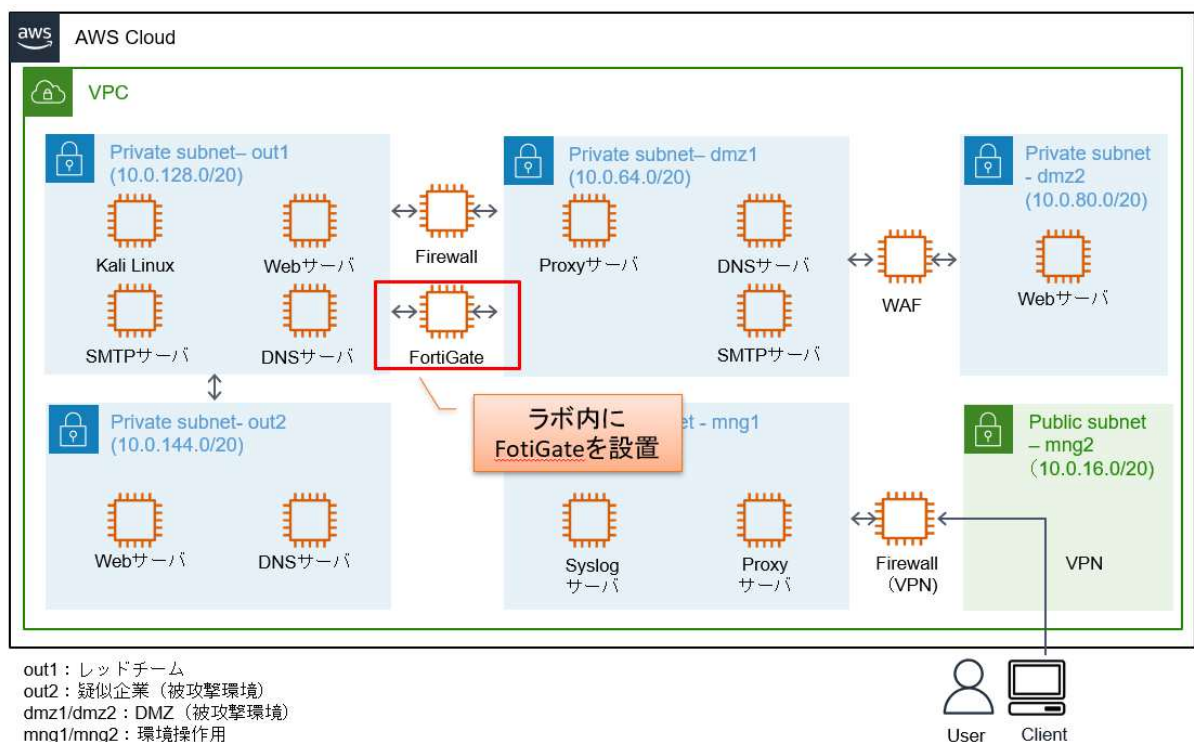


図8 セキュリティラボ内への FortiGate の設置

セキュリティラボの構築期間中に FortiGate の UTM 機能の導入の引き合いがあり、設備調達から運用開始までの期間が短く、設備調達後の機能検証、構築期間の確保が難しかった。このことから新製品の導入検証としてセキュリティラボを活用し、FortiGate の機能検証および構築手順の整備を実施した。

FortiGate については AWS Marketplace にて従量課金方式での利用が可能であったため、図 8 のようにセキュリティラボの環境内に設置し事前検証を実施した。

セキュリティラボを活用して事前に機能検証を行いつつ、ユーザが想定していた導入機能と利用目的から実際に必要となる機能の差異があることを確認し、要件確定に繋げることが出来た。

セキュリティラボを用いての製品検証を行うことが出来たため、必要ライセンスの事前確認、構築手順の整備などを行うことが出来、図 9 のようにユーザへの設備導入期間の短縮に繋がった。



図 9 UTM 導入スケジュール

4 今後の見通し

今後の見通しとしては図 10 の通り当初構築で見送った社内サーバゾーン、運転監視についてセキュリティラボの機能拡張を行うことを想定している。また新規製品検証の観点では AWS のセキュリティサービスの検証および新たな SIEM 製品の検証を予定している。

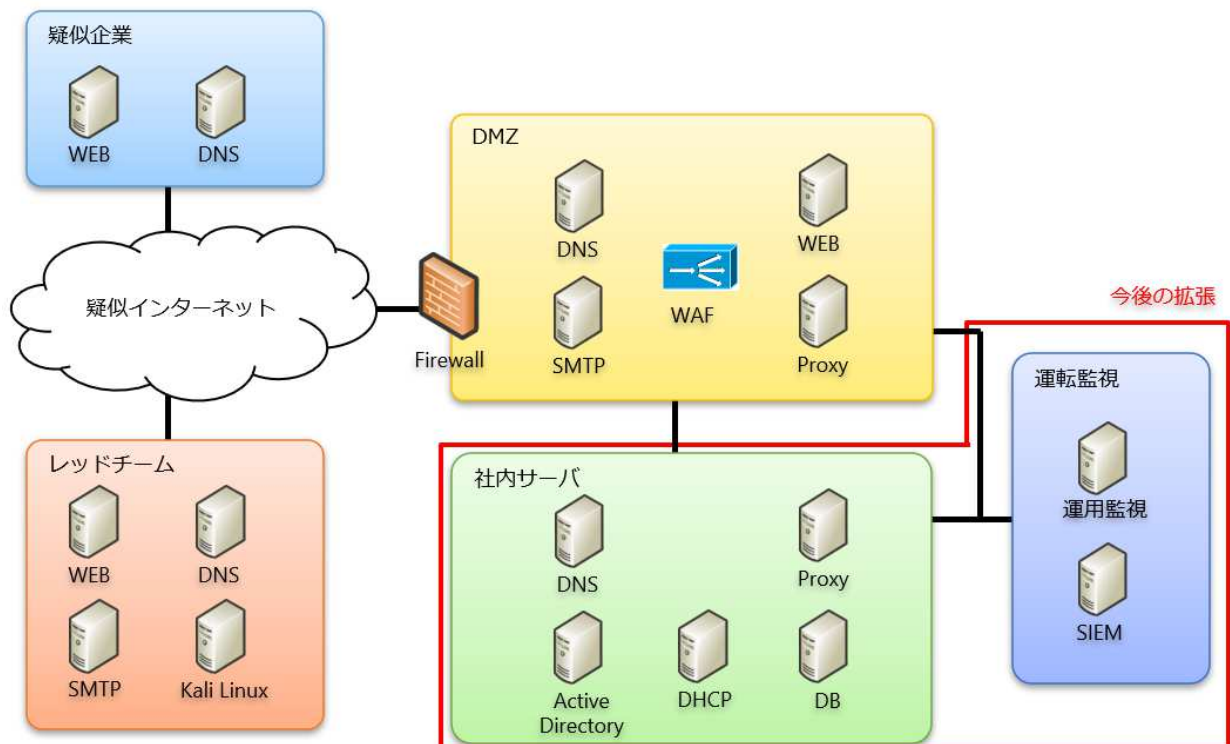


図 10 今後の拡張

4. 1 セキュリティラボ環境の拡充

当初構築では外部攻撃によるインシデント対応を想定して、DMZ 環境を中心として構築を行いホームページへの DDoS 攻撃の再現などインターネット接続環境からの攻撃を想定したインシデント対応環境を構築した。

近年はウイルス感染等による内部からの社内システムの攻撃事例も増加していることから、社内システム特に Active Directory を中心とした Windows サーバに対するセキュリティ機能に対する検証を目的としてセキュリティラボ環境の機能拡張を実施する。

4. 2 クラウドサービスの利用検討

当部署では SOC 運用以外にもセキュリティ製品の構築および維持管理も実施している。AWS を中心にクラウドサービスを活用したシステム構築が増加しており、AWS でのセキュリティサービスの活用について対応が求められてる。新規案件への適用を想定してセキュリティラボにてセキュリティ設定、サービス活用について機能検証を行い、システム構築案件への活用につなげたい。

4. 3 サービスの提供拡大に向けた検証

運転監視として弊社の SOC では Security Information and Event Management (以下、SIEM と略す) 製品として Splunk Enterprise を活用してログ監視およびログ検索機能を用いてインシデント調査を実施している。

現在 SOC 監視を実施している企業グループ以外への SOC サービスの提供拡大のため、コストやユーザ環境構成に応じて柔軟なサービス環境の提供を行うため、SIEM on Amazon OpenSearch Service など Splunk Enterprise 以外の SIEM 製品の検証を行う場としてセキュリティラボを活用する。

5 結論

クラウドサービスを利用したセキュリティラボの構築によって、OS バージョンなど利用製品が定期的に最新化されることにより、製品バージョンが選択しにくいという制約はあるがサーバ数の増減や機能追加などを柔軟に実施出来る検証環境を構築することが出来た。

クラウドサービスではオンプレミスと同等構成のサーバ環境を構築する場合は、オンプレミスに比べて高コストになるため、クラウドサービスでコストメリットを出すためにはサーバレス機能を活用するなどオンプレミスとは異なるインフラ設計が必要であるが、本件のように常時稼働が求められない環境であれば、ストレージなど固定費用となる部分もあるが、サーバインスタンスなど利用時間に応じた従量課金となる部分が大きいため、検証ごとに必要な機能(インスタンス)のみを起動するといった運用により安価に環境を維持することが出来ると考える。

新製品の活用については、オンプレであれば検証目的で一時的に利用する場合、メーカーから検証機の借用や評価ライセンスの取得をしたうえで期間限定での利用となる。Firewall、UTM などのセキュリティアプライアンスについては仮想化対応している製品も多く、クラウドサービスでは AWS Marketplace のように従量課金で利用可能な製品も多く、利用期間や台数、構成など柔軟な対応が可能であった。

今後の見通しに記載した通り、当初のセキュリティラボの構築目的であったセキュリティ人材育成の場として活用を進めるとともに、新製品の検証の一環としてクラウドサービス自体を活用した機能の検証および部門内の他サービスへの展開を進めていきたい。

参考文献

IPUSIRON

ハッキング・ラボのつくりかた 仮想環境におけるハッカー体験学習

2018 年 12 月 7 日 株式会社 翔泳社

商標

Amazon Web Services、AWS Marketplace、Amazon OpenSearch Service は米国およびその他の国における Amazon Web Services, Inc. の商標または登録商標です。

VMware vSphere、VMware vCenter は米国およびその他の国における VMware, Inc. の商標または登録商標です。

Linux は Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

Red Hat Enterprise Linux は米国およびその他の国における Red Hat, Inc. の商標または登録商標です。

Windows は米国およびその他の国における Microsoft Corporation の商標または登録商標です。

Cisco ASA は米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。

FortiGate は米国およびその他の国における Fortinet Corporation の商標または登録商標です。

Splunk は米国およびその他の国における Splunk Inc. の商標または登録商標です。