●●●株式会社　御中

情報セキュリティ現状調査報告書
（サンプル）

2016 年●月●日

株式会社ディアイティ

目次

添付資料

・別紙 1 【ヒアリングシート】　情報セキュリティ現状調査（情報システム管理用）
・別紙 2-a～i 【ヒアリングシート】情報セキュリティ現状調査（情報システム管理用）
　Web サービス セキュリティチェックシート
・サンプル 1 クラウドサービス セキュリティチェックシート
・サンプル 2 情報管理規則

1　調査の目的等

1.1　情報セキュリティ現状調査概要

1.1.1 情報セキュリティ現状調査の目的

本調査は以下の目的で取り組みました。

- 貴社の情報システムおよびネットワークの情報セキュリティ管理の現状調査と、調査結果に基づく課題の洗い出しと課題の改善案の提案。
- クラウドサービス等アウトソーシング先の情報セキュリティ管理の現状調査と、調査結果に基づく課題の洗い出しと課題の改善案の提案。

1.1.2 情報セキュリティ現状調査の範囲

本調査は、図１の通り“社内システム”“クラウドサービス等アウトソースシステム環境”の２つの区分に関連する脅威（リスク要因）に対するセキュリティの取り組みを対象としました。

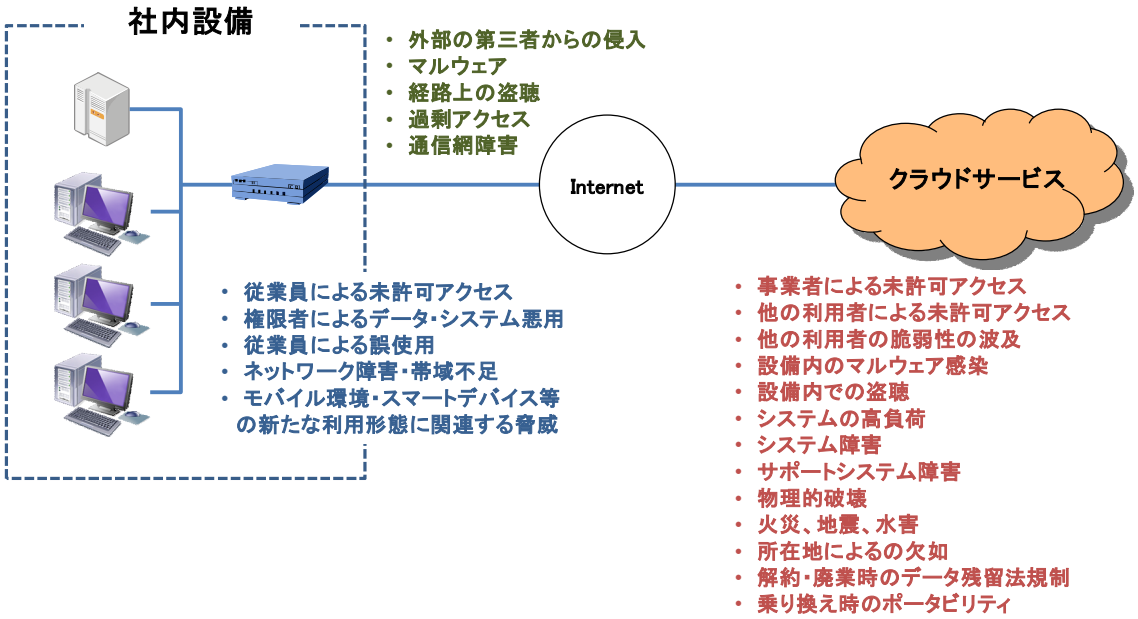

図１：　情報セキュリティ現状調査の範囲

1.1.3 情報セキュリティ現状調査の方法

調査は、以下の対象区分と方法で行いました。

評価対象	調査方法
貴社内システム	ヒアリングシートに基づく、システム管理部門担当者への聞き取り調査
クラウド等アウトソース環境	契約書、ホームページ等の公開情報の確認。 アウトソース先へのアンケート結果の確認

【評価基準】

評価は情報セキュリティの国際規格 ISO/IEC 27001（JIS Q 27001）と 27002（JIS Q 27002）に照らし、システム実装と維持・運用管理の両面で行いました。

【調査項目】

調査は、ISO/IEC 27001/27002 をベースに以下の項目について確認しました。

A. 共通
   1. 情報の識別
   2. 設備の物理的保護
   3. 脆弱性管理
   4. バックアップ
   5. アクセス制御
   6. モニタリング
   7. システム処理管理
   8. ネットワーク制御

B. Web サーバ
   1. 脆弱性管理
   2. バックアップ
   3. アクセス制御
   4. モニタリング
   5. ネットワーク制御

C. 社内サーバ
   1. 脆弱性管理
   2. バックアップ
   3. アクセス制御

D. PC 端末
   1. 情報の識別
   2. 設備の物理的保護
   3. 脆弱性管理
   4. モニタリング

E. スマートデバイス（スマートフォン、タブレット PC）
   1. 情報の識別
   2. 設備の物理的保護、アクセス制御
   3. 脆弱性管理

F. モバイル環境
   1. 情報の識別
   2. 設備の物理的保護、アクセス制御
   3. 脆弱性管理
   4. バックアップ
   5. モニタリング
   6. ネットワーク制御

G. 記憶媒体管理
   1. 情報の識別
   2. 設備の物理的保護
   3. アクセス制御
   4. システム処理管理

H. 私有デバイスの業務利用（BYOD： Bring Your Own Device）

1. 情報の識別
2. 設備の物理的保護
3. 脆弱性管理、バックアップ、アクセス制御、モニタリング、システム処理管理
4. システム処理管理
5. ネットワーク制御

I. 維持運用管理
1. システム構成管理
2. システムの障害管理
3. インシデント対応

J. システムの開発・変更
1. システムの開発・変更

K. アウトソーシング
1. アウトソーシングの管理

L. マネジメント
1. システム管理体制
2. 内部規定
3. 教育
4. 点検

【調査の限界】

今回は聞き取り調査およびアンケート調査による評価を行いました、客観的な証跡による評価ではありませんので監査のような厳格さを持つものではありません。また、特定の時点での評価ですので時間の経過による変化は考慮していません。したがって、本調査結果をもって何らかの安全性を保証するものではありません。

1.1.4 調査のスケジュール

ヒアリング調査およびアンケート調査は、事前に予備調査を行い業務内容やシステム構成の概要を把握した後、実情に合わせたヒアリングシートを作成し、それを基に本調査を実施し聞き取り調査を行いました。

クラウドサービス事業者やWebコンテンツ開発・運営事業者等アウトソース先には、アンケート方式で調査を行いました。

調査内容	調査部門	調査方法	調査日
予備調査	●●●部	ヒアリング	2014/●/●
本調査	●●●部	ヒアリング	2014/●/●
	アウトソーシング先	アンケート	2014/●/●～2014/●/●

2　調査結果要約（サマリー）

今回の調査における、社内システムのセキュリティ実装と維持・運用管理とクラウドサービス等アウトソース先のセキュリティレベルと、について評価した結果の要点を以下に記します。
調査結果の評価詳細については 3 章以降に解説します。

2.1　社内システムのセキュリティの評価

社内システムのセキュリティについては、○○対策が遅れていることが懸案となっています。
課題を整理し優先順位をつけて段階的に進められるように今回の結果を参考にしてください。詳細の評価結果と課題に対する対応案は「3.1 情報セキュリティ現状調査評価詳細」「3.2 情報セキュリティ現状調査リスク評価別対応案」を参照ください。

(1) 現行の手続きの正式化

現在、システム管理部門ではアクセス権管理やウイルス対策等を適切に実施されています。これら現行の○○○。
また、現在の管理体制で○○○可能性があります。

(2) 各部署および各社員に依存するセキュリティの強化

PC 端末の運用や○○○の観点から必要な処置を施すことが望まれます。
対策としては○○○。
各部署・各社員のセキュリティの整備が進んできたなら、○○○検討ください。

(3) 協業者の監督

アウトソース先や外部委託先等の協業者の監督を強化することが望まれます。○○○、以下のような対策強化を図ることが望まれます。

・○○○○○○○○○○
・○○○○○○○○○○
・○○○○○○○○○○

(4) サービス選定基準の整備

現在利用されているクラウドサービス等の導入に際し、○○評価することが望まれます。サンプル 2 のチェックシートを参考にしてください。

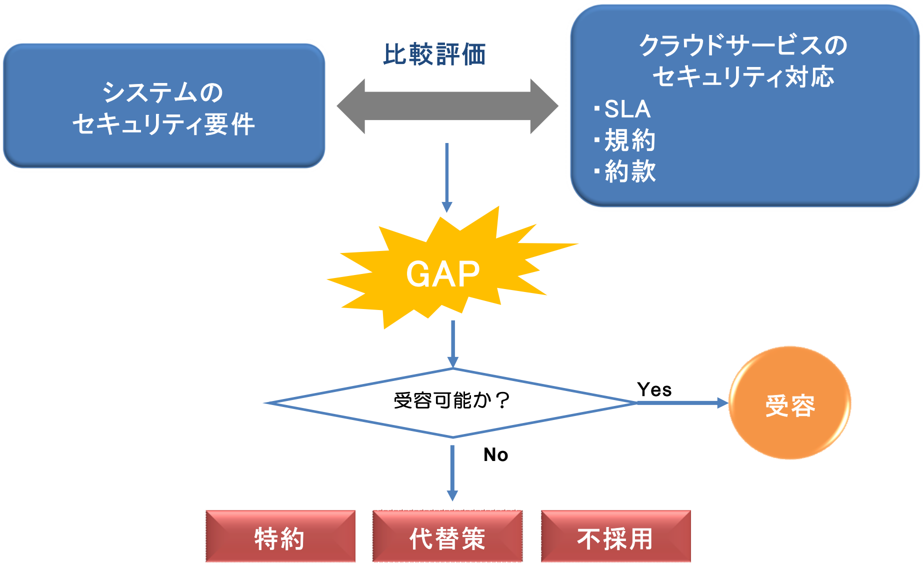

図２：　サービスの選定

2.2　クラウドサービス等のアウトソース先のセキュリティレベル評価

クラウドサービス等のアウトソース先のセキュリティについては、各ベンダーから回収した調査表の分析の結果、○○○経営的判断を交え具体的な対策を検討ください。

調査の詳細の評価結果と課題に対する対応案は「4.2 システムアウトソーシングのシステム管理状況調査の評価と対応案」「4.3 システムアウトソーシングのシステム管理状況調査の評価まとめ」を参照ください。

(1) ウイルス対策

想定されるウイルスの感染経路を十分に検証し○○○することが望まれます。

■ 対象：　（株）○○○○○○○○○○、（株）○○○○○○○○○○

(2) コンテンツ改ざん検知

Web サーバのコンテンツが改ざんされると、○○○の対策を強化することが望まれます。

■ 対象：　（株）○○○○○○○○○○、（株）○○○○○○○○○○

(3) Web サーバ脆弱性管理

特に Web サイトで個人情報等機密情報を収集○○、IPA「安全なウェブサイトの作り方」「ウェブ健康診断仕様」等[1]を用いて設計・構築・運用することが望まれます。

必要ならば、○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○検討ください。

■ 対象：　（株）○○○○○○○○○○、（株）○○○○○○○○○○

---

[1] IPA「安全なウェブサイトの作り方」「ウェブ健康診断仕様」等：　独立行政法人 情報処理推進機構（IPA）作成のガイドブック。https://www.ipa.go.jp/security/vuln/websecurity.html

3　社内システム環境調査結果詳細

個々の調査結果についてリスク度とコメントを記します。リスク度は高・中・低で表示しています。リスク度の判定は、その発生頻度と発生時の影響の大きさを考慮して決めています。ただし、当社の経験的判定であるため、目安程度に考えてください。コメントには、改善のヒントを記述しています。必ず実施しなければならない事項ではないので、改善するか否かおよび実施の具体的方法は貴社内で検討ください。

凡例

良：　今回調査した範囲ではリスクを招く要因は見られませんでした。

低：　今すぐ問題が顕在化するリスクではありませんが、今後クラウド利用範囲の拡大や情報の利用方法の変化や拡大があった場合に強化が必要と思われるリスクを表します。

中：　セキュリティ対策を実施されていますが、対策が属人的である、委託先等の自社で直接コントロールできないといった理由から、対策が徹底できない可能性があるリスクを表します。

高：　リスクが顕在化する可能性が高く、すぐに対策の許可が望まれるリスクを表します。(今回の調査では該当箇所は見つかりませんでした)

3.1　情報セキュリティ現状調査評価詳細

区分	管理分野		確認事項	回答	リスク対応案	リスク度評価
A. 共通	1. 情報の識別	a	業務継続や法令、契約上の要求に基づいて、特に保護すべき情報を識別し認識していますか。	○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	▼○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	低
		b	上記情報がどのシステムに存在するか認識していますか。	・○○○○○○○○○○○○○○○○○○○○○○。	▼ ○○○○○○○○○○○○○○○○○○○○○○	良
	2. 設備の物理的保護	a	社内設備は、入退室制限された区画に設置していますか。	・○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	▼ ○○○	良
		b	上記区画への入退室制限はどのような方法でされていますか。	・○○○	▼ ○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	中
		c	上記区画の入退室は記録されていますか。	・○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	▼ ○○○	中

区分	管理分野	確認事項		回答	リスク対応案	リスク度評価
		d	システムが正常稼働するよう、電源と空調を適切に保っていますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	▼ 〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	低
		e	電源ケーブルやネットワークケーブルは破損や抜けから保護していますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	▼〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	良
		f	サーバ等重要設備の設置場所では、災害等環境的脅威（地震、水害、火災、粉じん等）への対策はしていますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇		良
		g	サーバ等重要設備の設置場所へのデバイスや記憶媒体の持ち込みを制限していますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	▼ 〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	低
		h	サーバ等重要設備の設置場所からのデバイスや記憶媒体の持ち出しを制限していますか。	・〇〇〇〇〇〇〇〇〇〇	〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	低
	3. 脆弱性管理	a	OS、アプリケーションのアップデート、パッチ適用の方針を決めていますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	▼ 〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	中
		b	コンピュータにウイルス対策ソフトを実装していますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇		良
I						
B. Web サーバ	1. 脆弱性管理	a	サーバ群上の不要なサービスやを停止又は削除していますか。	・〇〇〇〇〇〇〇〇〇〇		良
		b	インターネットに公開しているWebサーバ等は改ざん、乗っ取りから保護し、サーバからの情報流出を防止する対策を施していますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇。	▼ 〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	高
		c	インターネットに公開しているWebサーバ等は、定期的および改修後に脆弱性検査（ペネトレーションテスト等）を実施し評価していますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	▼ 〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	中
	2. バックアップ	a	サーバ群は、最大許容停止時間に基づきシステム冗長化、または、バックアップシステムを設置していますか。	・〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	▼ 〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	中