出社してから退社するまで中小企業の情報セキュリティ対策実践手引き

SAMPLE 版

2014 年 2 月 21 日版
NPO 日本ネットワークセキュリティ協会　西日本支部

目次

※SAMPLE 版のため目次のページと内容とは合っていません。

導入部

第１部　情報セキュリティ管理策

0.1.第 1 部と第 2 部との対応

第1部		第2部
本手引き管理項目	管理策	業務No.
1.セキュリティ境界と入退室管理	①	1,2,22,30,65
	②	1,2,22,30
	③	3
2.クラウドサービスの利用	①	25,26,28
	②	24,25,26,28
	③	
3.障害・事故管理	①	60
	②	59
	③	59
4.IT継続性	①	57
	②	
	③	
5.認証と権限	①	1,4,12,21,30,37,44,45,51
	②	4,21,24,45
	③	1,2,3,5,21,45
	④	1,2,21
	⑤	21
	⑥	6
6.ネットワークのアクセス制御	①	38,42,67,69
	②	67,69
	③	45,46
	④	67,69
	⑤	67,69
	⑥	33
	⑦	32,33,65
	⑧	27
7.パッチの適用	①	8,64,68
	②	
	③	68
8.ウイルス及び悪意のあるプログラムに対する対策	①	7
	②	7
	③	13,66
	④	13,66
	⑤	27
	⑥	27
	⑦	66
9.記憶媒体の管理	①	12,40,43
	②	34
	③	
	④	11
	⑤	

上付き(N)は参考資料の番号を示す

第1部		第2部
本手引き管理項目	管理策	業務No.
10.スマートデバイスの利用	①	
	②	49
	③	44,49
	④	48,49
	⑤	48,49
	⑥	
	⑦	42
	⑧	
	⑨	48,49
13.ログの取得	①	3,62
	②	61
	③	62
	④	62
	⑤	
14.バックアップ	①	9,23,57
	②	9,23,55,56,57
	③	23,57
15.容量・能力の管理	①	63
	②	63
16.変更管理	①	55
	②	55
	③	55
	④	55
	⑤	56
	⑥	56
17.構成管理	①	10,58
	②	58,64
	③	
18.SNSの利用	①	48,53,54
19.暗号化	①	14,16,20,37,40,43,47,51
	②	
	③	14,16,20
20.アプリケーションの利用	①	52
	②	52
	③	19
	④	39
	⑤	17
	⑥	17
	⑦	20
21.クリアデスク・クリアスクリーン	①	50
	②	29,35,36,50
	③	31
	④	18

上付き(N)は参考資料の番号を示す

0.2.凡例

(1) 管理目的

管理策を行う目的

(2) 管理策

中小企業が行うべき具体的な情報セキュリティ対策

大きな投資及び技術的・運用的に難しいものは“(参考)”として記述している

(3) 運用で心がけるポイント

セキュリティ対策を継続していくうえでの運用における注意点

(4) 関連する管理項目

関連する管理項目を列挙

2.クラウドサービスの利用

(1) 管理目的

クラウドサービスの利用に際し、組織の要求する情報セキュリティ及びサービスレベル[13]を確保し、維持するため

(2) 管理策

①クラウドサービスの利用に際し、組織の求めるセキュリティレベル(入退館・入退室管理、情報漏えい対策、認証強度、アクセス制御、ウイルス対策、障害・事故対策、災害対策等)、サービスレベル(対応時間、サービス可能時間、リソースの使用保証等)を明確にする。

②クラウドサービスの利用に際し、セキュリティレベル、サービスレベルの確認を実施する

③クラウドサービス提供者とセキュリティレベル、サービスレベルを取りきめ契約を締結する(参考)

(3) 運用で心がけるポイント

①クラウドサービスに要求するセキュリティレベル、サービスレベルを確認する

②クラウドサービスのユーザインターフェイスの変更、機能変更・追加に注意し、認証などセキュリティ強化に繋がる変更は使用して行く

③データセンターのロケーションにより適用される法律が違うことに注意する。

(4) 関連する管理項目

認証、SNS、スマートデバイス

上付き[N]は参考資料の番号を示す

3.障害･事故管理

(1) 管理目的

システム障害(システム・サービスの停止、誤動作、破損等)、セキュリティ事故(情報漏えい、改ざん、アクセス違反、ウイルス感染、外部からの攻撃等)が発生した場合、根本原因を取り除き、再発防止を行うため

(2) 管理策

①システム障害、セキュリティ事故の発生に備え、連絡網を整備し、障害・事故発生時は連絡網に従い報告する

②障害・事故が発生した場合は、いつ、誰が、何を、どのようにして、障害・事故を発生させ、その結果どうなったのかを記録する

③記録から障害・事故発生の根本原因を追及し、それを取り除き、再発防止を行う

(3) 運用で心がけるポイント

①障害・事故発生時の連絡網が組織の実情を反映しているか確認する

②障害・事故発生時の記録が保存されているか確認する

(4) 関連する管理項目

ウイルス及び悪意のあるプログラムに対する対策、バックアップ、変更管理、構成管理、容量・能力の管理

4.IT 継続性

(1) 管理目的

システムの重大な障害(システム・サービスの停止、誤動作、破損等)の影響からシステムを保護し、またシステムの中断に対応するとともに復旧を確実にするため

(2) 管理策

①システムに重大な障害が発生した場合の業務への影響範囲、被害及びリスクを明確にし、それらに基づいた、システムの保護対策(バックアップ、リプリケーション、冗長化等)あるいは障害への対応・復旧計画を策定する

②システム障害におけるシステムの保護対策、対応・復旧計画が有効であることを定期に確認、見直しする

③地震、火災、水害、大規模停電などの災害によるシステムへの影響を考慮し、システムの保護対策あるいは障害への対応・復旧計画を策定する(参考)

(3) 運用で心がけるポイント

①定期的に障害への対応・復旧訓練を行い対応・復旧計画を見直す

上付き(N)は参考資料の番号を示す

(4) 関連する管理項目

バックアップ、ウイルス及び悪意のあるプログラムに対する対策、変更管理、構成管理、障害・事故管理、容量・能力の管理

5.認証と権限

(1) 管理目的

情報と情報機器への許可されていないアクセスを防止するため

(2) 管理策

①入館・入室設備、PC(BIOS、OS)、サーバー、ネットワーク、アプリケーション、スマートデバイス（スマートフォン、タブレット)、携帯電話等にアクセスするための個人及びプログラムを認証する仕組みを構築・設定する

②認証には、ワンタイムパスワード、二段階、ID カード、デバイス(ハードウェアトークン、IC カード、USB キー等)、パスワード、バイオメトリックス(指紋認証、静脈認証等)等及びこれらの組み合わせ(複数要素認証)の第三者が簡単に悪用できない仕組みを用いる

③認証のためのユーザ ID は個人を特定できるように付与する

④ユーザ ID は職務権限に応じた、情報と情報機器へのアクセス権限を付与する

⑤特権は、システム管理者、業務の管理者等特別の職務権限を持った者だけに付与する

⑥パスワード[9]は例えば「12 文字以上に設定し、
大文字、小文字、数字、特殊文字の 4 つを組み合わせ、
3 カ月に 1 度変更する」
(以降「」をパスワードポリシーとする)とする。

(3) 運用で心がけるポイント

①退職、人事異動に伴う、ユーザ ID、アクセス権限の見直しを行う

②アクセスする情報の重要度、情報機器のある場所及び情報にアクセスする場所により認証の強度を検討する

(4) 関連する管理項目

セキュリティ境界と入退室管理、アプリケーションの利用、電子メールの利用、ネットワークのアクセス制御、Web の開発・管理、クラウドの利用、SNS、スマートデバイスの利用

6.ネットワークのアクセス制御

上付き[N]は参考資料の番号を示す

(1) 管理目的

ネットワークを経由した情報への許可されていないアクセスを防止するため

(2) 管理策

①インターネット等の外部ネットワークと組織のネットワークの境界には、ファイアーウォール、ルータなどのアクセス制御装置を設置しアクセス制御を行う

②公開用の Web サーバー、メールリレーサーバー等は内部ネットワークとはファイアーウォールで隔てた別のネットワーク(DMZ)に設置する

③外部から組織のネットワークに接続する場合、許可された者のみに接続を許すために、適切な認証を行い、安全な接続(SSL-VPN、IPsec、PPTP 等)を行う

④外部ネットワークと内部ネットワーク、外部ネットワークと DMZ 間の通信プロトコル(=サービス：HTTP、HTTPS、FTP、SMTP、POP 等)は必要最低限のもののみ許可する

⑤公開サーバー、内部サーバー共に不要なサービスは停止する

⑥無線 LAN を使用する場合は、WPA2 等の安全な暗号化方式を用い、暗号鍵を設定する

⑦特定の場所または特定の PC、端末からの接続のみ許可するために PC、端末の識別子(IP アドレス、MAC アドレス等)での認証を行う(参考)

⑧危険な Web サイトにアクセスできないように Web フィルタリングを導入する(参考)

(3) 運用で心がけるポイント

①通信に不要なプロトコル、ポートが使用できないことを確認する

②外部からの接続をする場合、認証が有効であることを確認する

③無線 LAN は外部ネットワーク扱いとしてネットワークを設計する

(4) 関連する管理項目

セキュリティ境界と入退室管理、認証と権限

9.記憶媒体の管理

(1) 管理目的

情報の漏えい、改ざん、消去、破壊を防止するため

(2) 管理策

①記憶媒体の数量、所在を管理する

②使用した記憶媒体(ハードディスク、テープ、USB メモリー、CD、DVD、スマートカード等)を廃棄する場合は、保存した情報が解読できないように、信頼できる方法で、記憶媒体の物理的破壊[10]、情報の磁気的な消去または上書き消去[11]を行う

③重要な情報を保存した記憶媒体は、製造者の仕様に従って、適切な環境(磁気、湿度、温度などの制限)及びセキュリティの確保(耐火金庫、施錠管理)できる場所に保存する

④許可されていない記憶媒体の使用ができないように、PC、サーバーのデバイス制御を

上付き[N]は参考資料の番号を示す

行う(参考)

⑤バックアップデータを記憶媒体に長期保管する場合は、記憶媒体の寿命を考慮し、定期的に、バックアップデータを新規記憶媒体に移動する等適切な処置を行う(参考)

(3) 運用で心がけるポイント

①定期的に記憶媒体の棚卸を実施し、数量、所在を確認する

②磁気的にデータ消去した場合は、廃棄前に情報が消去されていることを確認する

③USB メモリー、Flash SSD、SD カード、スマートフォン、タブレットの記憶装置として使用される NAND 型フラッシュメモリ[19][20]は、情報の磁気的な消去または上書き消去が出来ないことがあることに注意する

(4) 関連する管理項目

ウイルス及び悪意のあるプログラムに対する対策、バックアップ

10.スマートデバイスの利用

(1) 管理目的

スマートデバイス(スマートフォン、タブレット)の利用に伴う、情報の漏えい、改ざん、破壊を防止するため

(2) 管理策

①スマートデバイスの資産管理を行う

②ジェイルブレイク、ルート化を禁止する

③製造者及びキャリアの提供するパスコードロック、自動ロック、パスコード入力に失敗した場合のデータ消去、リモートワイプ、暗号化、ウイルス及び悪意のあるプログラムに対する対策機能は有効にしておく

④有償、無償を問わず組織が許可したアプリケーション(ソフトウェア)のみ使用を許可する

⑤有償、無償を問わず組織が許可したクラウドサービスのみ使用を許可する

⑥スマートデバイス、アプリケーションの脆弱性情報を入手し、リリースされたセキュリティパッチは必ず適用する

⑦社外で Wi-Fi、赤外線、Bluetooth ネットワークに接続する場合は、信頼できるネットワークのみ利用する

⑧重要な情報をスマートデバイス以外にバックアップする手順を備える

⑨スマートデバイスの使用ガイドライン[21][22][23]を定める。

(3) 運用で心がけるポイント

①位置情報とアプリケーション、スマートデバイスとクラウドサービス及び SNS との自動連携機能の設定を確認し、意図しない連携を防止する

上付き[N]は参考資料の番号を示す

②定期的にスマートデバイスの棚卸しを実施すると共に設定状況を確認し、セキュリティパッチの適応状況、許可アプリケーション以外使用されていないことを確認する

(4) 関連する管理項目

認証と権限、パッチの適用、記憶媒体の管理、暗号化、バックアップ、クラウドサービスの利用、SNS の利用

12.Web の開発・管理

(1) 管理目的

情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため

(2) 管理策

①Web に公開する情報は改ざんから保護するため、必要なアクセス制御(ルータ、ファイアーウォール、OS、Web サーバー、アプリケーション等での制御)を行う

②顧客の個人情報等、第三者の情報を保存する場合は、「安全な Web アプリケーション構築の手引き」[14][15]に従い、Web システムを開発・構築する(参考)

③組織の外部から、公開している Web サイトに悪意のある攻撃が無いか、WAF、IPS、IDS、外部の監視サービス等を用い監視を行う(参考)

④定期的に Web サイトの強度、運用、管理方法に関して、第三者機関の検査または監査を実施する(参考)

(3) 運用で心がけるポイント

①公開されている Web サイトが改ざんされていないか定期的に確認する

②改ざん、漏えい事故が発生した場合の、対処方法(リカバリー方法、届け出等)を確認する

(4) 関連する管理項目

認証と権限、バックアップ、ネットワークのアクセス制御、変更管理、構成管理、障害・事故管理

18.SNS の利用

(1) 管理目的

従業員が SNS を私的利用するに際し、企業情報の漏えいを防止すると共に、企業の信用失墜を防止するため。

(2) 管理策

上付き[N]は参考資料の番号を示す

①従業員が SNS を利用する場合の、勤務先名の記載可否、企業が持つ公開情報についての記載可否または記載範囲・記載条件、SNS 上での顧客、取引先社員との交友方法、私的情報の記載内容、利用方法について、SNS 使用ガイドライン(24)を定める

(3) 運用で心がけるポイント

①使用デバイス(PC、スマートフォン、タブレット)と SNS の設定により、使用デバイス上のデータ、写真、位置情報と SNS が自動連携されることに注意する

②SNS の設定変更、機能追加による情報漏えいに注意する

③従業員の法律、公序良俗に違反する SNS の記載により、企業の信用失墜の可能性があることに注意する

④SNS セキュリティ設定の問題により、SNS のアカウントが乗っ取られ、悪用される可能性のあることに注意する

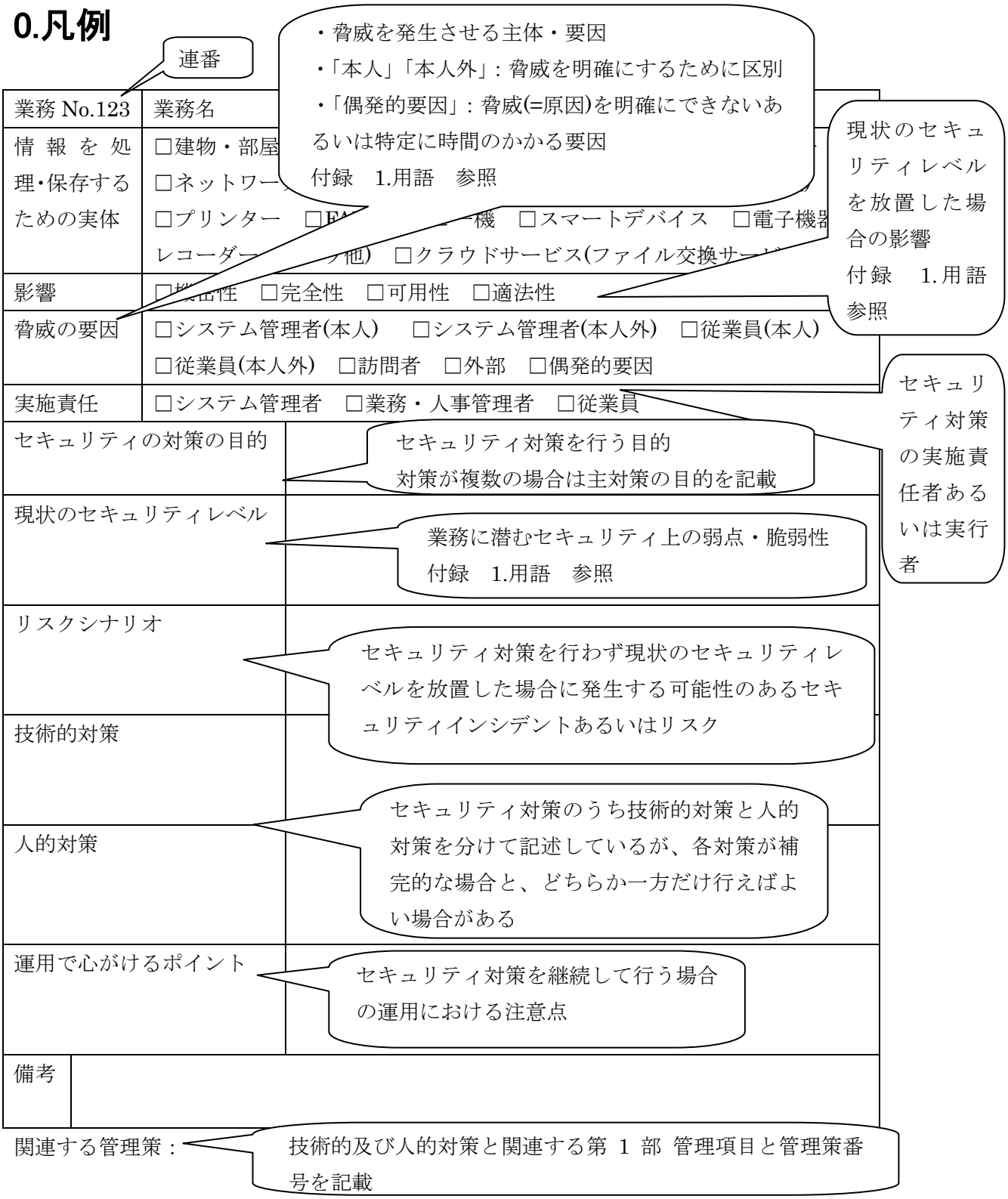
(4) 関連する管理項目

認証、クラウドサービスの利用

上付き(N)は参考資料の番号を示す

第 2 部　業務に基づく情報セキュリティ対策

0.凡例



業務 No.123	業務名
情報を処理･保存するための実体	□建物・部屋 □ネットワー □プリンター　□FA　ー機　□スマートデバイス　□電子機器 レコーダー　ー他)　□クラウドサービス(ファイル交換サー
影響	□機密性　□完全性　□可用性　□適法性
脅威の要因	□システム管理者(本人)　□システム管理者(本人外)　□従業員(本人) □従業員(本人外)　□訪問者　□外部　□偶発的要因
実施責任	□システム管理者　□業務・人事管理者　□従業員
セキュリティの対策の目的	
現状のセキュリティレベル	
リスクシナリオ	
技術的対策	
人的対策	
運用で心がけるポイント	
備考	

関連する管理策：

上付き(N)は参考資料の番号を示す

1.出社

業務 No.1	入館
情報を処理･保存するための実体	■建物・部屋・エリア　□キャビネット　□机上　□PC　□サーバー □ネットワーク　□アプリケーション　□記憶媒体(USB メモリー他) □プリンター　□FAX　□コピー機　□スマートデバイス　□電子機器(IC レコーダー、カメラ他)　□クラウドサービス(ファイル交換サービス等)
影響	■機密性　■完全性　■可用性　□適法性
脅威の要因	□システム管理者(本人)　□システム管理者(本人外)　□従業員(本人) □従業員(本人外)　□訪問者　■外部　□偶発的要因
実施責任	□システム管理者　■業務・人事管理者　□従業員

セキュリティの対策の目的	情報と情報機器への許可されていないアクセスを防止するため
現状のセキュリティレベル	従業員かどうかを識別、認証する仕組みが無い
リスクシナリオ	従業員以外が従業員になりすまし入館する
技術的対策	従業員に個人を特定できる社員証を与え、入館システムでチェックする
人的対策	従業員に個人を特定できる社員証を与え、人(守衛)がチェックする
運用で心がけるポイント	退職、人事異動した従業員の社員証の棚卸を定期的に行う

備考	従業員には、正社員の他、契約社員、派遣社員、パート・アルバイトなど非正規の社員も含んでいる

関連する管理策：1.セキュリティ境界と入退室管理 ①,② 5.認証と権限 ①,③,④

上付き(N)は参考資料の番号を示す

2.社内業務

業務 No.6	PC の起動・ログイン 3 【パスワードポリシーの使用】
情報を処理･保存するための実体	□建物・部屋・エリア　□キャビネット　□机上　■PC　□サーバー □ネットワーク　□アプリケーション　□記憶媒体(USB メモリー他) □プリンター　□FAX　□コピー機　□スマートデバイス　□電子機器(IC レコーダー、カメラ他)　□クラウドサービス(ファイル交換サービス等)
影響	■機密性　□完全性　□可用性　□適法性
脅威の要因	□システム管理者(本人)　□システム管理者(本人外)　□従業員(本人) ■従業員(本人外)　□訪問者　□外部　□偶発的要因
実施責任	■システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	情報と情報機器への許可されていないアクセスを防止するため
現状のセキュリティレベル	簡単なパスワード(数字 4 桁など)を使用している
リスクシナリオ	簡単なパスワードを使用しているためログオン時の覗き見によりパスワードが漏えいし、情報にアクセスされる
技術的対策	認証システムのパスワードポリシーを設定(複雑なパスワード、定期的パスワードの変更)し、ユーザに強制的にパスワードポリシーを使用させる
人的対策	パスワードの文字数、文字列の組み合わせ、変更の周期等についてのパスワードポリシーをルール化しユーザに周知徹底する
運用で心がけるポイント	・認証システムのパスワードポリシーを確認する ・パスワードルールが周知徹底されているかユーザに確認する
備考	

関連する管理策：5.認証と権限 ⑥

上付き(N)は参考資料の番号を示す

3.社外業務

業務 No.48	スマートデバイスを利用した業務【OS・アプリケーションの設定】
情報を処理･保存するための実体	□建物・部屋・エリア　□キャビネット　□机上　□PC　□サーバー □ネットワーク　□アプリケーション　□記憶媒体(USB メモリー他) □プリンター　□FAX　□コピー機　■スマートデバイス　□電子機器(IC レコーダー、カメラ他)　■外部のサービス(ファイル交換サービス等)
影響	■機密性　□完全性　□可用性　□適法性
脅威の要因	□システム管理者(本人)　□システム管理者(本人外)　■従業員(本人) □従業員(本人外)　□訪問者　□外部　□偶発的要因
実施責任	■システム管理者　■業務・人事管理者　□従業員

セキュリティの対策の目的	スマートデバイスの利用に伴う、情報の漏えい、改ざん、破壊を防止するため
現状のセキュリティレベル	スマートデバイスの使用に関するガイドラインが無い
リスクシナリオ	顧客・パートナー情報を含んだスマートデバイスのアドレス帳と SNS が自動同期になっており、さらに SNS 招待メール機能が有効になっていたため、SNS から顧客・パートナーへ招待メールが送信されてしまった
技術的対策	デバイス管理ツールを利用しスマートデバイスの管理を行う
人的対策	・スマートデバイス使用に関するガイドラインを策定する ・SNS 使用に関するガイドラインを策定する
運用で心がけるポイント	スマートデバイスの OS、アプリケーションのバージョンアップに伴う設定変更に注意する
備考	

関連する管理策：10.スマートデバイスの利用 ④,⑤,⑨ 18.SNS の利用 ①

上付き(N)は参考資料の番号を示す

業務 No.49	スマートデバイスを利用した業務【ルート化、Jailbreak の禁止】
情報を処理･保存するための実体	□建物・部屋・エリア　□キャビネット　□机上　□PC　□サーバー □ネットワーク　■アプリケーション　□記憶媒体(USB メモリー他) □プリンター　□FAX　□コピー機　■スマートデバイス　□電子機器(IC レコーダー、カメラ他)　□外部のサービス(ファイル交換サービス等)
影響	■機密性　■完全性　■可用性　■適法性
脅威の要因	□システム管理者(本人)　□システム管理者(本人外)　■従業員(本人) □従業員(本人外)　□訪問者　■外部　□偶発的要因
実施責任	■システム管理者　■業務・人事管理者　□従業員

セキュリティの対策の目的	スマートデバイスの利用に伴う、情報の漏えい、改ざん、破壊を防止するため
現状のセキュリティレベル	ルート化、Jailbreak 禁止のルールが無い
リスクシナリオ	スマートデバイスをルート化・Jailbreak して使用し、さらに悪意のあるアプリケーションダウンロードしてしまい、そのアプリケーションがスマートデバイスにある情報を漏えいする
技術的対策	デバイス管理ツールを使用し、ルート化・Jailbreak の禁止、アプリケーションの無断使用を禁止する
人的対策	スマートデバイス使用に関するガイドラインを策定する
運用で心がけるポイント	ルート化・Jailbreak をしていない事、無許可アプリケーションを使用していない事を定期的に確認する
備考	

関連する管理策：10.スマートデバイスの利用 ②,③,④,⑤,⑨

上付き(N)は参考資料の番号を示す

5.帰宅

業務 No.53	SNS の利用【OS・アプリケーションの設定】
情報を処理･保存するための実体	□建物・部屋・エリア　□キャビネット　□机上　□PC　□サーバー □ネットワーク　□アプリケーション　□記憶媒体(USB メモリー他) □プリンター　□FAX　□コピー機　■スマートデバイス　□電子機器(IC レコーダー、カメラ他)　■外部のサービス(ファイル交換サービス等)
影響	■機密性　□完全性　□可用性　□適法性
脅威の要因	□システム管理者(本人)　□システム管理者(本人外)　■従業員(本人) □従業員(本人外)　□訪問者　□外部　□偶発的要因
実施責任	■システム管理者　■業務・人事管理者　□従業員

セキュリティの対策の目的	従業員が SNS を私的利用するに際し、企業情報の漏えいを防止すると共に、企業の信用失墜を防止するため。
現状のセキュリティレベル	SNS 利用についてのルールが無い
リスクシナリオ	位置情報の付いた取引先に関連する写真を知らずに SNS にアップし、位置情報より取引先名が判明してしまう
技術的対策	SNS に写真をアップする前に、位置情報を削除しておく
人的対策	SNS の使用ガイドラインを策定する
運用で心がけるポイント	どのアプリケーションと位置情報との連携設定がされているか、どのアプリケーションと SNS との連携設定がされているかを認識しておく
備考	

関連する管理策：18.SNS の利用 ①

上付き(N)は参考資料の番号を示す