NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA　2013年度活動報告会

「中小企業向け情報セキュリティチェックシート」で現状把握の解説

情報セキュリティチェックシートWG
嶋倉　文裕
富士通関西中部ネットテック㈱

2014 年　6月　10日（火）　ベルサール神田

情報セキュリティチェックシートの利用目的

- 現状における対策レベルを確認
- リスク度に応じた適切な対策を導く

認識した業務における起こりうるリスクを念頭に、現状の対策状況を確認

情報セキュリティチェックシート　2008年に第１版を公開
http://www.jnsa.org/seminar/2008/1217nsf2008/data/1217-C2-01checksheetA3.xls

9to5、ソリューションガイドとの関連付け、内容の見直し、構成の見直し、公開
http://www.jnsa.org/seminar/nsf/2014kansai/

情報セキュリティチェックシートの構成①

２つの階層　上位層（９項目）と下位層（１８項目）

－上位層　　９項目

リスクとは関係なく、情報セキュリティ対策を持続的に行うためのフレームワーク

9to5では前提条件

- 体制（役割、責任）
- ルール
- 文書化
- 実施状況の確認　など

情報セキュリティ特有なことではない！
何かをするさい、必然なもの

情報セキュリティチェックシートの構成②

－上位層　　9項目

1.情報セキュリティ基本方針
2.責任の明確化
3.職務の分離
4.委託先の管理
5.情報資産管理台帳
6.規程の文書化とレビュー
7.法令順守
8.秘密保持
9.情報セキュリティの確認

情報セキュリティチェックシートの構成③

－下位層　　１８項目

リスクに応じた情報セキュリティ対策とシステム管理

ISO27001管理策、システム管理基準(一部)ベース

1.セキュリティ境界と入退出管理	10.スマートデバイス　*New!*
2.クラウドサービスの利用　*New!*	11.電子メールの利用
3.障害・事故管理	12.Webの開発管理
4.IT継続性	13.ログの取得
5.認証と権限	14.バックアップ
6.ネットワークのアクセス制限	15.容量・能力の管理
7.パッチの適用	16.変更管理
8.ウイルス及び悪意のあるプログラムに対する対策	17.構成管理
9.記憶媒体の管理	18.SNSの利用　*New!*

上位層の利用ポイント①

No.	キーワード	管理目的	持続可能な計画に必要なフレームワークが確立されていないことのリスク	判断基準	確認内容	対策の参考となるサービス/製品 JNSAソリューションガイド
1	情報セキュリティ基本方針	経営陣の情報セキュリティへの取り組み、方向性を明確化し全組織がそれを共有し同じレベルで情報セキュリティに取り組むため	・組織としての情報セキュリティの取り組みがないため、取引先からの信頼を失う ・個人毎に情報セキュリティ対策の遵守が異なり、対策が不十分なところで事故を起こしてしまう	・経営陣の情報セキュリティの取り組み方針を含む情報セキュリティ対策指針、基準の有無 ・情報セキュリティ対策指針、基準の組織内、組織外への明示の有無 ・組織を取り巻く環境に合わせた情報セキュリティ基本方針の見直し有無	①経営方針の中に情報セキュリティに関する記載が無い ②経営方針の中に記載しており、社内にしか明示していない ③経営方針の中に記載しており、社外にも明示している ④経営方針の中に記載し、社内外に明示しており、環境の変化に合わせて方針を見直している	・セキュリティ基本方針の立案・維持(管理項目)

キーワード
対策項目を一言で…
管理目的
対策の目的を明記

No.	キーワード	管理目的	持続可能な計画に必要なフレームワークが確立されていないことのリスク
1	情報セキュリティ基本方針	経営陣の情報セキュリティへの取り組み、方向性を明確化し全組織がそれを共有し同じレベルで情報セキュリティに取り組むため	・組織としての情報セキュリティの取り組みがないため、取引先からの信頼を失う ・個人毎に情報セキュリティ対策の遵守が異なり、対策が不十分なところで事故を起こしてしまう

フレームワークがないことによる情報セキュリティ対策推進への弊害を解説

上位層の利用ポイント②

No.	キーワード	管理目的	持続可能な計画に必要なフレームワークが確立されていないことのリスク	判断基準	確認内容	対策の参考となるサービス/製品 JNSAソリューションガイド
1	情報セキュリティ基本方針	経営陣の情報セキュリティへの取り組み、方向性を明確化し全組織がそれを共有し同じレベルで情報セキュリティに取り組むため	・組織としての情報セキュリティの取り組みがないため、取引先からの信頼を失う ・個人毎に情報セキュリティ対策の遵守が異なり、対策が不十分なところで事故を起こしてしまう	・経営陣の情報セキュリティの取り組み方針を含む情報セキュリティ対策指針、基準の有無 ・情報セキュリティ対策指針、基準の組織内、組織外への明示の有無 ・組織を取り巻く環境に合わせた情報セキュリティ基本方針の見直し有無	①経営方針の中に情報セキュリティに関する記載が無い ②経営方針の中に記載しており、社内にしか明示していない ③経営方針の中に記載しており、社外にも明示している ④経営方針の中に記載し、社内外に明示しており、環境の変化に合わせて方針を見直している	・セキュリティ基本方針の立案・維持(管理項目)

判断基準	確認内容	対策の参考となるサービス/製品 JNSAソリューションガイド
・経営陣の情報セキュリティの取り組み方針を含む情報セキュリティ対策指針、基準の有無 ・情報セキュリティ対策指針、基準の組織内、組織外への明示の有無 ・組織を取り巻く環境に合わせた情報セキュリティ基本方針の見直し有無	①経営方針の中に情報セキュリティに関する記載が無い ②経営方針の中に記載しており、社内にしか明示していない ③経営方針の中に記載しており、社外にも明示している ④経営方針の中に記載し、社内外に明示しており、環境の変化に合わせて方針を見直している	・セキュリティ基本方針の立案・維持(管理項目)

現状評価の基準を明記

4段階での成熟度モデルで現状確認内容を明記

具体的に対策を検討するさいの参照先

下位層の利用ポイント①

No.	キーワード	管理目的	対策をしていないことによるトラブル事象例	判断基準	確認内容	9-5紐付け	対策の参考となるサービス/製品 JNSAソリューションガイド
	セキュリティ境界と入退室管理	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	・従業員以外が従業員になりすまし入館する ・重要な情報を扱うエリア(室)への入退室記録が無く、情報漏えい発生時、誰がいつエリア(室)に入退したのかわからない ・許可されていない者がセキュリティエリアに入り権限のない情報を閲覧する ・共有サーバーにアクセス権限を持たない者が直接サーバーにログインし、情報を閲覧する ・訪問者が重要な情報を閲覧する ・ホワイトボードの消し忘れにより、重要な情報を訪問者が閲覧する ・会議室に置き忘れた書類を訪問者が社外に持ち出す	・社内におけるセキュリティ境界の識別、アクセスコントロールポリシーの有無 ・セキュリティ領域の設定有無 例)執務エリアと一般人立ち入り可能な場所の分離 サーバールームと執務エリアの分離 ・定期的なポリシー、セキュリティ境界の見直しの有無	①セキュリティ設計・ゾーン管理をしていない ②セキュリティ設計・ゾーン管理はしているが、アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理ではない ③アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしている ④アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしており、定期的にポリシー、設計・ゾーン管理を見直している	2 セキュリティエリアへのアクセス1【エリア分け】 3 セキュリティエリアへのアクセス2【入退出記録】 22 共有サーバーの利用2【物理的アクセス】 30 訪問者との打ち合わせ1【訪問者の識別】 31 訪問者との打ち合わせ2【会議室の使用】	情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション(サービス)
				・入の入退館、入退室の確認の有無 ・入退館、入退室のログ・記録の有無 ・定期的な入退館、入退室対策の見直しの有無	①個人を識別した入退管理をしていない ②個人を識別した入退管理をしているが、入退に関するログ・記録は残していない ③個人を識別した入退管理をしており、入退に関するログ・記録も残している ④個人を識別した入退管理をしており、入退に関するログ・記録も残している。さらに定期的に入退管理方法を見直している	1 入館 22 共有サーバーの利用2【物理的アクセス】 30 訪問者との打ち合わせ1【訪問者の識別】	入退出管理を行いたい(利用シーン)

No.	キーワード	管理目的	対策をしていないことによるトラブル事象例
1	セキュリティ境界と入退室管理	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	・従業員以外が従業員になりすまし入館する ・重要な情報を扱うエリア(室)への入退室記録が無く、情報漏えい発生時、誰がいつエリア(室)に入退したのかわからない ・許可されていない者がセキュリティエリアに入り権限のない情報を閲覧する ・共有サーバーにアクセス権限を持たない者が直接サーバーにログインし、情報を閲覧する ・訪問者が重要な情報を閲覧する ・ホワイトボードの消し[illegible]問者が閲覧する ・会議室に置き忘れた[illegible]出す

キーワード
対策項目を一言で…
管理目的
対策の目的を明記
9to5の第1部の各管理項目と同じ

対策をしていないことにより、おこりうる情報セキュリティ上のトラブル、インシデントを解説

下位層の利用ポイント②

No.	キーワード	管理目的	対策をしていないことによるトラブル事象例	判断基準	確認内容	9-5紐付け	対策の参考となるサービス/製品 JNSAソリューションガイド
1	セキュリティ境界と入退室管理	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	・従業員以外が従業員になりすまし入館する ・重要な情報を扱うエリア(室)への入退室記録が無く、情報漏えい発生時、誰がいつエリア(室)に入退したのかわからない ・許可されていない者がセキュリティエリアに入り権限のない情報を閲覧する ・共有サーバーにアクセス権限を持たない者が直接サーバーにログインし、情報を閲覧する ・訪問者が重要な情報を閲覧する ・ホワイトボードの消し忘れにより、重要な情報を訪問者が閲覧する ・会議室に置き忘れた書類を訪問者が社外に持ち出す	・社内におけるセキュリティ境界の識別、アクセスコントロールポリシーの有無 ・セキュリティ領域の設定有無 例）執務エリアと一般人立ち入り可能な場所の分離 サーバールームと執務エリアの分離 ・定期的なポリシー、セキュリティ境界の見直しの有無	①セキュリティ設計・ゾーン管理をしていない ②セキュリティ設計・ゾーン管理はしているが、アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理ではない ③アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしている ④アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしており、定期的にポリシー、設計・ゾーン管理を見直している	2 セキュリティエリアへのアクセス1【エリア分け】 3 セキュリティエリアへのアクセス2【入退出記録】 2 共有サーバーの利用2【物理的アクセス】 3 訪問者との打ち合わせ1【訪問者の識別】 3 訪問者との打ち合わせ2【会議室の使用】	情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション(サービス)
				・人の入退館、入退室の確認の有無 ・入退館、入退室のログ・記録の有無 ・定期的な入退館、入退室対策の見直しの有無	①個人を識別した入退管理をしていない ②個人を識別した入退管理をしているが、入退に関するログ・記録は残していない ③個人を識別した入退管理をしており、入退に関するログ・記録も残している ④個人を識別した入退管理をしており、入退に関するログ・記録も残している。さらに定期的に入退管理方法を見直している	1 入館 2 共有サーバーの利用2【物理的アクセス】 3 訪問者との打ち合わせ1【訪問者の識別】	入退出管理を行いたい(利用シーン)

判断基準	確認内容
・社内におけるセキュリティ境界の識別、アクセスコントロールポリシーの有無 ・セキュリティ領域の設定有無 例）執務エリアと一般人立ち入り可能な場所の分離 サーバールームと執務エリアの分離 ・定期的なポリシー、セキュリティ境界の見直しの有無	①セキュリティ設計・ゾーン管理をしていない ②セキュリティ設計・ゾーン管理はしているが、アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理ではない ③アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしている ④アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしており、定期的にポリシー、設計・ゾーン管理を見直している
・人の入退館、入退室の確認の有無 ・入 ・定	①個人を ②個人を ③個人を ④個人を に定期的

現状評価の基準を明記

4段階での成熟度モデルで現状確認内容を明記

下位層の利用ポイント③

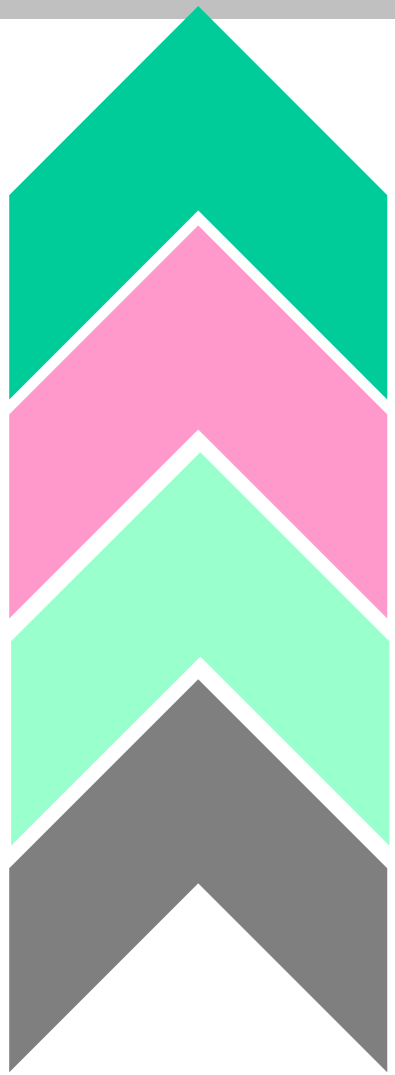
No.	キーワード	管理目的	対策をしていないことによる トラブル事象例	判断基準	確認内容	9-5紐付け	対策の参考となる サービス/製品 JNSAソリューションガイド
1	セキュリティ境界と入退室管理	情報と情報機器への許可されていないアクセスを防止するため	・従業員以外が従業員になりすまし入館する ・重要な情報を扱うエリア(室)への入退室記録が無く、情報漏えい発生時、誰がいつエリア(室)に入退したのかわからない ・許可されていない者がセキュリティエリアに入り権限のない情報を閲覧する ・共有サーバーにアクセス権限を持たない者が直接サーバーにログインし、情報を閲覧する ・訪問者が重要な情報を閲覧する ・ホワイトボードの消し忘れにより、重要な情報を訪問者が閲覧する ・会議室に置き忘れた書類を訪問者が社外に持ち出す	・社内におけるセキュリティ境界の識別、アクセスコントロールポリシーの有無 ・セキュリティ領域の設定有無 例）執務エリアと一般人立ち入り可能な場所の分離 サーバールームと執務エリアの分離 ・定期的なポリシー、セキュリティ境界の見直しの有無	①セキュリティ設計・ゾーン管理をしていない ②セキュリティ設計・ゾーン管理はしているが、アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理ではない ③アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしている ④アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしており、定期的にポリシー、設計・ゾーン管理を見直している	2 セキュリティエリアへのアクセス1【エリア分け】 3 セキュリティエリアへのアクセス2【入退出記録】 22 共有サーバーの利用2【物理的アクセス】 30 訪問者との打ち合わせ1【訪問者の識別】 31 訪問者との打ち合わせ2【会議室の使用】	情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション(サービス)
				・人の入退館、入退室の確認の有無 ・入退館、入退室のログ・記録の有無 ・定期的な入退館、入退室対策の見直しの有無	①個人を識別した入退管理をしていない ②個人を識別した入退管理をしているが、入退に関するログ・記録は残していない ③個人を識別した入退管理をしており、入退に関するログ・記録も残している ④個人を識別した入退管理をしており、入退に関するログ・記録も残している。さらに定期的に入退管理方法を見直している	1 入館 22 共有サーバーの利用2【物理的アクセス】 30 訪問者との打ち合わせ1【訪問者の識別】	入退出管理を行いたい(利用シーン)

9-5紐付け	対策の参考となる サービス/製品 JNSAソリューションガイド
2 セキュリティエリアへのアクセス1【エリア分け】 3 セキュリティエリアへのアクセス2【入退出記録】 22 共有サーバーの利用2【物理的アクセス】 30 訪問者との打ち合わせ1【訪問者の識別】 31 訪問者との打ち合わせ2【会議室の使用】	情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション(サービス)

9to5の第2部と関連を明記
本対策が不十分なとき、具体的な業務に潜むリスクの確認先

具体的に対策を検討するさいの参照先

判断基準、成熟度モデル



レベル４　対策が有効か、確認を行う

レベル３　リスクを鑑み、ルールに基づき
対策に取り組む、より確実に
対策に取り組む

レベル２　とりあえず手をうった

レベル１　なにもしていない

対策立案時の参照先

JNSA

成熟度モデルで現状把握、対策はどうすれば？

今回の変更で、参照先を明記

- **JNSAソリューションガイド**
  http://www.jnsa.org/JNSASolutionGuide/IndexAction.do

- **JNSAすぐに使える情報セキュリティ　お役立ちツール**
  http://www.jnsa.org/ikusei/form/05_00.html
  中小企業情報セキュリティ対策促進事業にあわせて開設したサイト、基本的な解説もあり

情報セキュリティチェックシートから始める

PDCAサイクルのCで利用する
チェックシート

チェックシート

これまでの話

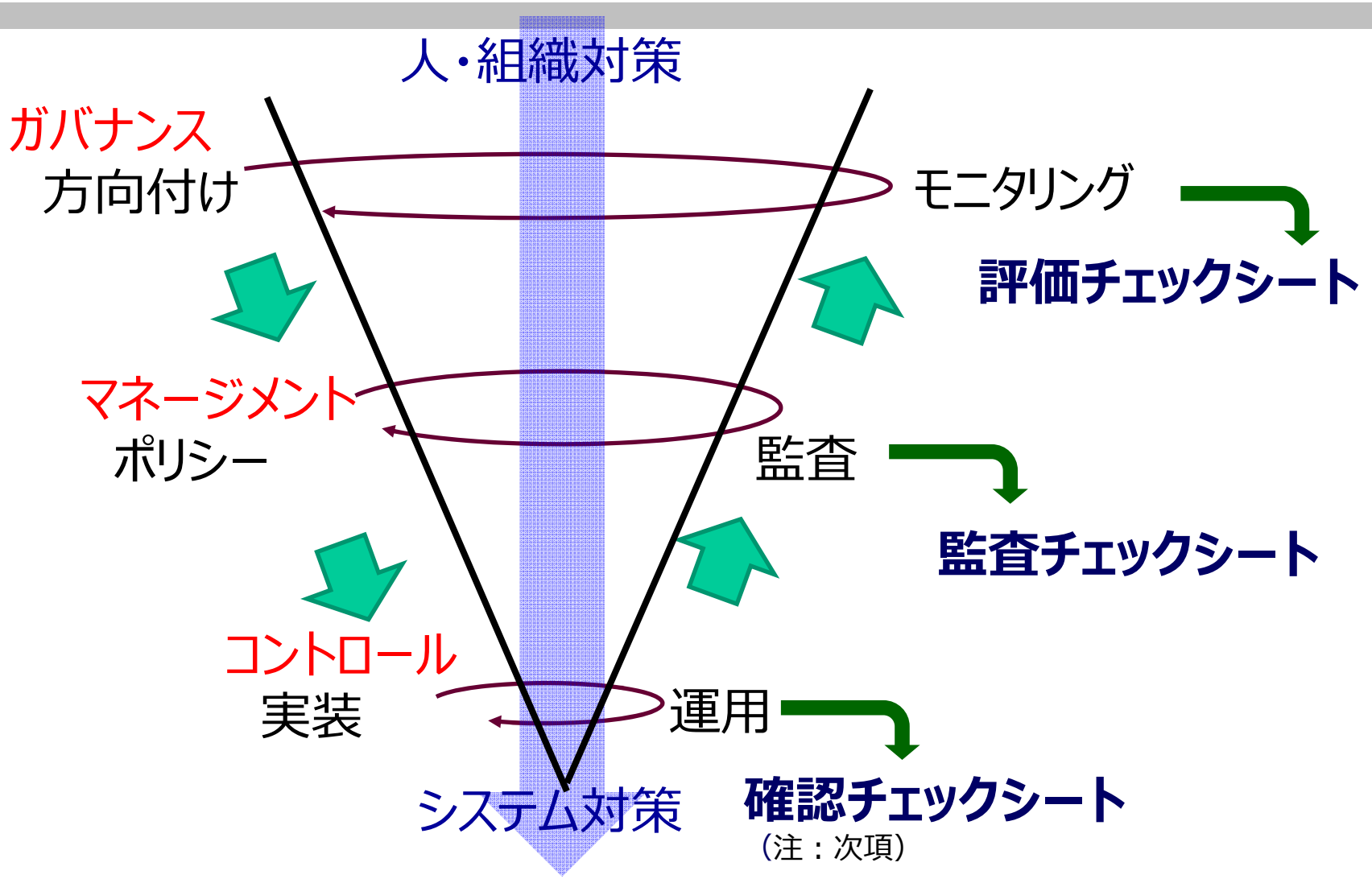
9to5から、自分たちの仕事のやり方に潜むリスクを認識、チェックシートで現状把握、対策検討

体系的にセキュリティ対策を行いたい方

チェックシート(27001簡略版)から起こりうる問題を把握、必要な対策を認識、検討

9to5を参考に、業務のリスクをイメージする

最後に　その他のチェックシートの考え方



最後に　確認チェックシート

	情報システム部門	業務部門
確認したいこと	・対策の定着 対策の停止、回避、無視の有無 ・対策の効果 インシデントの検知、抑止 ・対策の維持 対策の停止、回避、無視の有無	・情報ｾｷｭﾘﾃｨ関連手続きの適用 手続きの回避、無視の有無 ・情報ｾｷｭﾘﾃｨ関連手続きの維持 手続きの回避・無視の有無 ・対策の維持 対策の遵守状況
確認対象	・システムログ ネットワークログ、サーバログ、PCログ ・ダッシュボード 管理画面 ・人（対象：部門管理者） ヒアリング	・人（対象：自部門） 業務手順書＆チェックシート ヒアリング ・ダッシュボード 管理画面
確認契機	・定期的 毎日、毎週、毎月 ・不定期 イベント時 （アップデート、キャンペーン） インシデント時	・業務内でのイベント ・定期的 毎日、毎週、毎月 ・不定期 イベント時（業務監査前）