（報告事項２）

情報セキュリティ対策について

区　分	報　告	対象範囲	法人全体及び業務委託先等

エグゼクティブサマリー

- 「政府機関の情報セキュリティ対策のための統一規範及び統一基準群」に準拠した規程類、体制を整備
- 情報セキュリティ強化に向けて、人的対策・技術的対策の面からPDCAサイクルを継続実施
- NISC、厚生労働省、民間業者による監査、セキュリティ診断等の第三者評価を実施し、特段の問題なしとの評価
- 2017年度：情報セキュリティインシデント※の発生なし

※定義：望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（JIS Q 27000:2014）

バックグランド

高度化・巧妙化するサイバー攻撃等に対応するため、情報セキュリティ対策の総合的な推進が求められる。

フィードバック期間及び検証方法

年度毎の業務実績評価における定性・定量評価

便益

情報セキュリティ対策の実効性向上・情報漏えい防止

人的対策

・最高情報セキュリティアドバイザーの設置（平成30年度より）
・情報通信技術等に関する情報提供サービスの利用（平成30年度より）
・eラーニングの実施
・標的型攻撃メール訓練の実施
・運用受託機関等のセキュリティ管理体制を評価　等

技術的対策

・入口：インテリジェント・ファイアウォール 等
・内部：仮想PCにおけるウィルス防御 等
・出口：外部送信メール添付ファイルの暗号化 等

（詳細は別紙参照）

（報告事項２）

情報セキュリティ関係規程 概念図

政府統一基準群

政府機関の情報セキュリティ対策のための統一規範

政府機関等の情報セキュリティ対策の運用等に関する指針

政府機関の情報セキュリティ対策のための統一基準

府省庁対策基準策定のためのガイドライン

【参考】

厚生労働省情報セキュリティポリシー

GPIF 情報セキュリティ関係規程

情報セキュリティポリシー（基本方針）
«法人の情報セキュリティ対策の全体概要について対外公表を前提に定めたもの»

情報セキュリティ管理規程
«統一規範における規定内容等を法人規程として読み替えたもの»

情報セキュリティ体制の整備に関する規程
«情報セキュリティ委員会及び責任者等の分掌を規定したもの»

運用受託機関等における情報セキュリティ対策実施規程
«運用受託機関等に対する情報セキュリティ対策を規定したもの»

【手順書等】

要管理対策区域における情報セキュリティ対策基準

政府機関の情報セキュリティ対策のための統一基準
情報取扱手順書
組織・体制の管理に関する手順書
例外措置手順書
自己点検手順書
情報セキュリティインシデント対応手順書
運用受託機関等のセキュリティ評価等に関する手順書
USBメモリ等取扱手順書
情報システム利用手順書
管理運用法人支給外ＰＣによる情報処理手順書

情報セキュリティ管理体制

最高情報セキュリティ責任者（CISO）
（理事：総務・企画担当）

最高情報セキュリティアドバイザー
（TIS(株) シニアエキスパート）

統括情報セキュリティ責任者
（情報管理部長）

各部室毎に設置

- 情報セキュリティ責任者
- 情報セキュリティ管理者
- 情報セキュリティ管理補助者

情報セキュリティ監査責任者
（監査室長）

ＣＳＩＲＴ体制
（Computer Security Incident Response Team）

最高情報セキュリティ責任者（CISO）
（理事：総務・企画担当）

ＣＳＩＲＴ責任者
（統括情報セキュリティ責任者）

業務統括者
（システム管理課長）

ＣＳＩＲＴ事務局
（情報管理セキュリティ対策課長他）

システム管理課職員

広報担当
企画部企画課長
企画部広報担当

情報セキュリティ委員会

- 対策推進計画の策定
- 関係規程の整備
- 情報セキュリティインシデントへの対応 等

情報セキュリティ対策

情報セキュリティポリシー → 情報セキュリティ強化に向けてＰＤＣＡサイクルの継続実施により法人のセキュリティレベルを引き上げる → 情報セキュリティインシデント：発生なし

Plan

平成29年度情報セキュリティ対策を総合的に推進するための計画（対策推進計画）

Do

人的対策

- 厚生労働省 最高情報セキュリティアドバイザーからの支援（ 2017年1月-2018年3月）
- eﾗｰﾆﾝｸﾞの実施（2018年1月-2月）
  集合研修を実施（2017年6月、7月）
- 自己点検を1回実施（ 2017年9月）
- 標的型攻撃メール訓練の実施（年度中 5回）
- メールや会議等を通じた注意喚起（年度実績：18件）
- 運用受託機関等のセキュリティ管理体制の評価

技術的対策

- 要機密情報をNWシステム（インターネットに接続した環境）で保管しない運用を継続
- 不正アクセスに対する多層防御機能（入口・内部・出口）追加
  →未許可機器の不正接続防止、ファイル操作ログ等の収集、未登録プログラムの実行制限等を目的とした仕組みを導入
- 第三者によるセキュリティ診断（ペネトレーションテスト等含む）の継続実施（2017年7月、2018年2月）及び対応
- 標的型メール攻撃等への対応
  →フリーメールやなりすましメールの隔離機能の導入等

Check

対策推進計画の実施状況・評価について情報セキュリティ委員会においてマネジメントレビューし有効性を確認

- ✓ 全役職員が受講済、新入職員も着任後速やかに受講済
  ⇒ 組織全体のセキュリティ意識を維持・向上
- ✓ 標的型攻撃メールの手口巧妙化に対応するため、訓練効果の向上を図る
  （訓練の分散実施、送信者アドレス偽装、初回開封者に対し再訓練の実施等）
- ✓ インシデント発生時の対応手順を繰り返し周知

【適切に対応した者】
2017年度：96.4%（2016年度：98.6%）

- ✓ 要機密情報を保管するシステムについて、インターネットから分離し、外部サイバー攻撃から防御
- ✓ セキュリティ診断結果によりNWシステムにおける「多層防御機能の有効性」を確認済み
- ✓ 不正アクセス等を常時監視/検知/防御、不正プログラムによる感染の未然防止
- ✓ セキュリティインシデント発生時、収集したログ活用で調査分析を円滑に実施できる環境を整備
- ✓ 各種フィルタリング機能の導入により隔離される受信メールを日次で点検 （感染の未然防御）

Act

マネジメントレビューを踏まえ「平成30年度対策推進計画」へ反映

＜法人独自の取組＞

法人全体システムに係るセキュリティ上の課題及びリスク評価（H28年10月）	リスク評価の結果、優先的に対応を要するとしたものは以下の6項目→全て対応済み。 ①ＵＳＢメモリ等の紛失による情報漏洩リスク ②許可されていないＵＳＢメモリ等の接続によるデータの不正持ち出しリスク ③データの不正持出し、改竄等が発生した場合、証跡による調査・トレースができないリスク ④ＧＰＤＲネットワークにおける印刷物の残置、紛失リスク ⑤許可されていないＰＣ等の接続によるデータ不正持ち出しリスク ⑥秘文解除者等によるメール送信時の誤送信等リスク

＜第三者による外部監査等＞

公的機関	ＮＩＳＣ（ＩＰＡに委託）による情報セキュリティマネジメント監査（H29年1月～4月）	指摘・推奨事項37項目→うち35項目は対応済み、残り２項目は今年度対応。
	ＮＩＳＣ（ＩＰＡに委託）によるペネトレーションテスト（H29年9月）	評価結果はＡＡＡ（最高）。
	厚生労働省によるペネトレーションテスト（H28年11月）	ランクＡ なお、検出事項はレベル「低」の事項が1件のみで対応済みである。
	厚生労働省による情報セキュリティ監査（H28年12月）	監査の結果、検出された不適合は７項目→全て対応済み。
民間	（株）ファイブドライブによるセキュリティ診断（ペネトレーションテストを含む）（H29年2月、H30年2月）	インターネット（外部）からシステム内部への不正侵入や、情報漏洩等のセキュリティ事象が発生する状況にないことが確認された。
	中電技術コンサルタント（株）によるマネジメント監査（H28年12月）	監査の結果、検出された事象は４項目→全て対応済み。
	（株）ブレインワークスによるマネジメント監査（H29年12月）	監査の結果、指摘事項は検出されていない。

＜運用受託機関等の委託先に対するセキュリティ評価＞

各室課が銀行、証券会社、信託銀行、投資顧問、システム開発・運用委託会社、コンサルタント、給与計算、広報支援、翻訳業務等194社に対し評価を実施。結果、契約継続に支障の及ぶ「評価基準3点未満」となった運用受託機関等は、該当無であった。（H30年3月）

別紙：技術的対策

	入口	内部	出口	機能	概要	導入済
1	○			ISPメールフィルター	一般的に脅威になる内容を含んでいると推定されるメールをプロバイダー時点で遮断する。	
2	○		○	インテリジェント・ファイアウォール	ポート制御だけでなく、通信分析防御・フィルタリングを行う。	
3	○			インターネットサーバーにおける防御	DMZにあるインターネットサーバーについてウィルス・スパイウェア等への感染を防御する。	
4	○	○		各仮想サーバーにおける防御	各仮想サーバーについてウィルス・スパイウェア等への感染を防御する。	
5	○	○	○	仮想PCにおけるウィルス防御	仮想PCのウィルス・スパイウェア等への感染を防御する。	
6		○		アクセス権限制御による防御	ユーザーIDのファイルアクセス権を特定範囲に限定する。	
7	○			業務に関係のないWEBページ閲覧制限	ユーザがアクセスできるWEBページを限定し、業務に関係のないWEBページ閲覧を制限する。	
8	○		○	外部機器持込みにおける対策	登録されていないUSBデバイス等の使用禁止及び利用ユーザを制限する。	
9			○	オフラインによるデータ移動における対策	移動用メディア紛失・盗難時の情報漏えいを防止する。	・暗号化機能付USBメモリー
10		○	○	NWシステム、GPDRシステム間のデータ移動における対策	システム間のデータ移動に際し、物理的隔離により、情報漏えいを防止する。	
11			○	外部送信メール添付ファイルの漏えい対策	外部へ送信したメールを傍受された場合でも情報の漏えいを防止する。	
12		○		複数ソフトウェアがネットワーク内で連携した異常な動きへの対策	ネットワークシステム内での複数機器をまたがった異常な動きを検知する。	
13	○			仮想PCへのアプリケーションインストールの制限	各ユーザー・アプリケーションプログラムが、勝手にソフトウェアをインストール出来ないようにする。	・管理者権限ユーザー以外のインストールを制限済
14		○		異常な通信の検知・遮断	スパイウィア等による外部との不審な通信を検知し遮断する。	・IPS装置＋SOC（ セキュリティ・オペレーション・センタ）