北海道におけるサイバーセキュリティ対策と新法や協議会への期待

セキュリティ対策

Ⅰ　地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）

道においては、総務省から示される「地方公共団体における情報セキュリティポリシーに関するガイドライン」」を踏まえ、道のポリシーを適宜見直しを行っています。

Ⅱ　情報システムセキュリティ強靭化（三層の対策）平成29年～

マイナンバー制度導入に伴う国からの要請に基づき、情報セキュリティ対策の抜本強化を実施

三層分離	対策内容
インターネット接続系	インターネット接続口を集約し、自治体情報セキュリティクラウドの構築による高度なセキュリティ対策
LGWAN接続系	インターネット接続と分割、無害化通信
マイナンバー利用事務系	インターネット完全分離、データ持出不可、二要素認証

Ⅲ　自治体情報セキュリティクラウド

○道と市町村がWebサーバ等を集約し、監視及びログ分析・解析をはじめ高度なセキュリティ対策を実施
○北海道においては、道・道内市町村（179）・一部広域連合（6）の186団体が利用

項目	内容
技術的対策	ファイアウォール、IPS/IDS、振る舞い検知、マルウェア対策、URLフィルタリングなど

セキュリティ対策

Ⅳ　β’へ移行（令和4年～）

職員が時間や空間に制約されない多様で柔軟な働き方を実現するため、テレワーク環境を導入するとともに、主要なシステムをLGWAN接続系で利用する「αモデル」からインターネット接続系で利用する「β’モデル」へ移行

また、全職員（警察官・教員を除く）に公用スマートフォン（16,500台）を配付し、内線電話やPCをネットワークに特定通信で庁内ネットワークに接続するためのテザリングなどで利用。

モデル	モデルの特徴
αモデル	これまでの「三層の対策」による強靱化モデル
α’モデル	LGWAN接続系から特定のクラウドサービスへの直接接続が可能
βモデル	業務システムをLGWAN接続系に残しつつ、業務端末をインターネット接続系（重要な情報資産の配置なし）に移行し、画面転送によりLGWAN接続系業務システムを利用
β’モデル	βモデルに加え、文書管理、人事給与、財務会計等の業務システム（マイナンバー利用事務系を除く）をインターネット接続系（重要な情報資産の配置あり）に移行し、業務の効率化を改善

セキュリティ対策

Ⅴ　セキュリティ対策のポイント

項目		守るべき情報		対策
技術的対策	インターネット接続系	業務システム	人事給与等、職員情報	F/W、EDR、EPP、NDR、標的型攻撃対策（異常通信）
		ファイルサーバ	業務データ	F/W、EDR、EPP、NDR、ランサムウェア対策、・標的型攻撃対策（異常通信）
		パソコン 公用スマートフォン	ローカルディスクに保存される情報	MDM、Webフィルタ、ディスクの暗号化、標的型攻撃対策（異常通信）
	LGWAN接続系	税、福祉関係		・インターネット接続系対策と同様 ・無害化通信、LGWAN画面転送（RDS・VDI）
	マイナンバー利用事務系	マイナンバーなど住民の個人情報		・ネットワーク接続制限（分離） ・二要素認証
人的対策		―		研修・訓練等の強化、外部監査など

新法や協議会への期待

Ⅵ　サイバー対処能力強化法及び同整備法への期待

サイバー攻撃がますます巧妙化・高度化するなか、システムの安定運用や重要なデータを守るため、新法の整備には次のようなことを期待します。

※セキュリティを所管する担当者としての考え

期待する効果	内　容
サイバー攻撃の未然防止・迅速対応	基幹インフラ事業者からの、インシデント報告や脆弱性情報の報告が義務化されることにより、国や自治体間に情報共有が図られ、早期に脅威を把握し被害拡大防止につながる。
攻撃サーバの無害化	警察などが重大な危害を防止するために、攻撃関係サーバに対する・無害化措置の実施が可能になれば、被害拡大や未然防止につながる。
国の体制強化	内閣サイバー官による強力な総合調整により、サイバー安全保障分野を一元的に調整する体制の整備により、インフラ等の安全確保の向上が図られる。

新法や協議会への期待

Ⅶ　情報共有・対策のための協議会への期待

協議会には、関係行政機関や基幹インフラ事業者、電子計算機等のベンダー等が参加し、専門的な見地から、被害防止に資する情報を共有していただくことを期待します。特に、サイバーセキュリティの確保に当たって普段から注意すべき事項や、設備等の具体的な脆弱性に関する情報、サイバー攻撃を受けた際の対処のマニュアルや実例など、サイバーセキュリティの向上に資する情報が、自治体の担当者の実務に役立つような形で共有され、未然防止や早期対処が図られ、被害防止につながることを期待します。