情報セキュリティ報告書

平成 24 年 5 月

宮　内　庁

目次

1　はじめに

宮内庁は，内閣総理大臣の管理の下にあって，皇室関係の国家事務を担い，御璽・国璽を保管しています。

皇室関係の国家事務には，天皇皇后両陛下を始め皇室の方々の宮中における行事や国内外へのお出まし，諸外国との親善などの御活動や御日常のお世話のほか，皇室に伝わる文化の継承，皇居や京都御所等の皇室関連施設の維持管理などがあり，業務で取り扱う情報や情報システムも多岐にわたっています。

また，昨今は政府機関等に向けられた「標的型メール」等の標的型サイバー攻撃が発生しており，これに適切に対処するためには，当庁の職員一人ひとりが情報セキュリティ対策についての正しい知識を持ち，意識を高く保つことが求められます。

このことを踏まえ，様々な情報資産や情報システムを適切に管理し，利用するためには，組織として情報セキュリティ対策に取り組む必要があります。

宮内庁は，これまで，次の点を中心に情報セキュリティ対策を推進してきました。

① 情報セキュリティ教育
② 職員を対象とした情報セキュリティ対策実施状況の自己点検と職員向けの注意喚起

本報告書は，平成 23 年度に宮内庁が実施した情報セキュリティ対策の具体的取組や監査結果に基づいて取りまとめたものです。現段階では重大な課題等は発見されておりませんが，リスク・脅威への対策や職員向け教育は，常に改善と努力が必要です。宮内庁は，今後も引き続き情報セキュリティの維持・向上に努めてまいります。

平成 24 年 3 月

宮内庁最高情報セキュリティ責任者
（長官官房審議官）
牧野　尊行

2　平成 23 年度の総括

(1) 平成 23 年度の評価

ア　平成 23 年度の重点事項

① 政府機関の情報セキュリティ対策のための統一基準（以下「統一基準」という。）の改定に伴い，宮内庁の規程体系を見直しました。（なお，この改定により，統一基準は，政府機関の情報セキュリティ対策のための統一管理基準（以下「統一管理基準」という。）と，政府機関の情報セキュリティ対策のための統一技術基準（以下「統一技術基準」という。）に分割されています。）

② 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の内容を職員に周知するとともに，仕様書作成時におけるセキュリティ要件策定手順の標準化を検討しました。

イ　情報セキュリティ対策の自己点検結果

宮内庁職員の情報セキュリティ対策実施状況について自己点検を行った結果，おおむね適切に実施していることが明らかとなりましたが，到達率が１００％に達していない事項も見られることから，なお改善の余地があるものと考えています。

ウ　情報システムごとの状況

宮内庁の各情報システムの情報セキュリティについては，重点検査を行った結果，ウェブサーバ，電子メールサーバ及び DNS サーバにおいて必要な対策が講じられています。

エ　教育・啓発

宮内庁では，毎年度，定期的に情報セキュリティ教育を実施するとともに，教育資料を職員用掲示板に掲載するなど，職員の情報セキュリティ対策に対する理解の浸透に努めています。

オ　調達・外部委託

宮内庁では，情報システムの調達や外部委託に当たっては，委託先の情報セキュリティ管理を適切に行っています。

カ　情報セキュリティに関する障害・事故等の報告

平成 23 年度において，宮内庁では情報セキュリティに関する重大

な障害・事故等はありませんでした。

(2) 平成 24 年度の目標

宮内庁で重点的に取り組む目標は，次のとおりとします。

① 情報セキュリティポリシーや関連規程の見直し

② 標的型メール等の標的型サイバー攻撃に適切に対処するため，研修教材を充実させ，職員研修，訓練を実施する。

3 報告の基本情報

(1) 宮内庁の概要

宮内庁は，内閣総理大臣の管理の下にあって，皇室関係の国家事務を担い，御璽・国璽を保管しています。

皇室関係の国家事務には，天皇皇后両陛下を始め皇室の方々の宮中における行事や国内外へのお出まし，諸外国との親善などの御活動や御日常のお世話のほか，皇室に伝わる文化の継承，皇居や京都御所等の皇室関連施設の維持管理などがあります。

宮内庁では，これら職務の遂行に当たって必要な情報システムを導入・運用し，効率的かつ着実な事務遂行に努めています。

現在，宮内庁で導入・運用している主な情報システムは次のとおりです。

- 宮内庁情報ネットワークシステム
- グループウェアシステム
- 宮内庁公開システム
- 正倉院宝物公開管理システム
- CAD システム
- 特定歴史公文書等ファイル検索システム
- 診療報酬（レセプト）オンライン請求システム

(2) 報告の対象とする期間

本報告書は，平成 23 年 4 月 1 日から平成 24 年 3 月 31 日までの情報セキュリティ対策に関する取組を対象としています。

(3) 報告の対象とする組織

本報告書が対象とする組織は，宮内庁の全ての組織（内部部局，施設等機関及び地方支分部局）としています。

(4) 報告の対象とする情報

本報告書が対象とする情報は，統一管理基準で対象とする情報（情報システム内部に記録された情報，情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記録された情報）としています。

(5) 本報告書の責任部署

宮内庁長官官房秘書課調査企画室

(6) 定員数

本報告の対象となる宮内庁の定員数は，1,023 人（平成 23 年度）です。

(7) 情報システム予算額

宮内庁で運用している情報システムに関する予算総額は，321,031 千円（平成 23 年度予算：宮内庁情報処理業務庁費及び通信専用料）です。

4 情報セキュリティ対策の枠組み

(1) 情報セキュリティ対策に関する文書体系

宮内庁では，政府機関の統一的な枠組みの中で，各府省庁が情報セキュリティ確保のために実施すべき対策の基準である統一基準に準拠した宮内庁情報セキュリティポリシー（以下「ポリシー」という。）を平成 18 年 3 月に制定し，その後，統一基準の改定に合わせてポリシーを見直し，改定してきました。平成 23 年度には，統一基準が統一管理基準と統一技術基準に分割されたのに伴い，ポリシーのうち，統一管理基準に準拠した部分のみを新しいポリシーとして改定し，統一技術基準に準拠した部分を「情報セキュリティ対策のための技術基準」（以下「技術基準」という。）として独立した規程にしています。

このポリシー及び技術基準は，宮内庁における情報セキュリティの確保に関する基本規範として位置付けられるものです。

また，ポリシー及び技術基準に規定された遵守事項についての具体的な実施手順を定めた下位規程として，「情報の格付け及び取扱制限に関する規程」，「情報処理及び情報システムについての対策規程」など，37 種の規程や手順を整備しています。

(2) 情報セキュリティ対策に係る組織体制

情報セキュリティ対策は，宮内庁職員全員が取り組むことはもちろんですが，主体ごとの権限と責任を明確化し，必要となる推進体制を確立して組織全体として取り組む必要があります。宮内庁では，情報セキュリティ対策を推進するために，統一管理基準及びポリシーに基づき，次のような体制を整備しています。

ア　最高情報セキュリティ責任者

情報セキュリティ対策に関する事務を総括しており，宮内庁では長官官房審議官が務めています。

イ　情報セキュリティ委員会

ポリシーの策定等を行う機能を持つ組織として，宮内庁次長を委員長とする情報セキュリティ委員会を設置しています。

なお，情報セキュリティ委員会は，宮内庁行政情報化推進委員会をもって充てることとしています。

ウ　情報セキュリティ監査責任者

情報セキュリティ監査に関する事務を統括しており，宮内庁では長官官房参事官のうち，最高情報セキュリティ責任者が指名する者１人が務めています。

エ　統括情報セキュリティ責任者

連絡体制や関係規程の整備及び情報セキュリティ教育の実施に関し，情報セキュリティ責任者を統括しています。宮内庁では長官官房秘書課長が務めています。

オ　情報セキュリティ責任者

部局内の情報セキュリティに係る事務を統括しており，宮内庁では，宮内庁文書管理規程により指定された文書管理者が情報セキュリティ責任者を務めています。

なお，宮内庁では，課室情報セキュリティ責任者を設置しておらず，その職務は，情報セキュリティ責任者が行うこととしています。

カ　情報システムセキュリティ責任者

所管する情報システムの情報セキュリティ対策の管理に関する事務

を統括しています。

キ　情報システムセキュリティ管理者

所管する情報システムの情報セキュリティ対策を実施しています。

ク　最高情報セキュリティアドバイザー

情報セキュリティに関する専門的な知識及び経験を有する外部の専門家を置き，情報セキュリティ対策に関する様々な事務への助言・支援を行っています。

また，宮内庁では，統一管理基準で規定された組織以外に，情報セキュリティ対策をより推進するため，次のような体制を設けています。

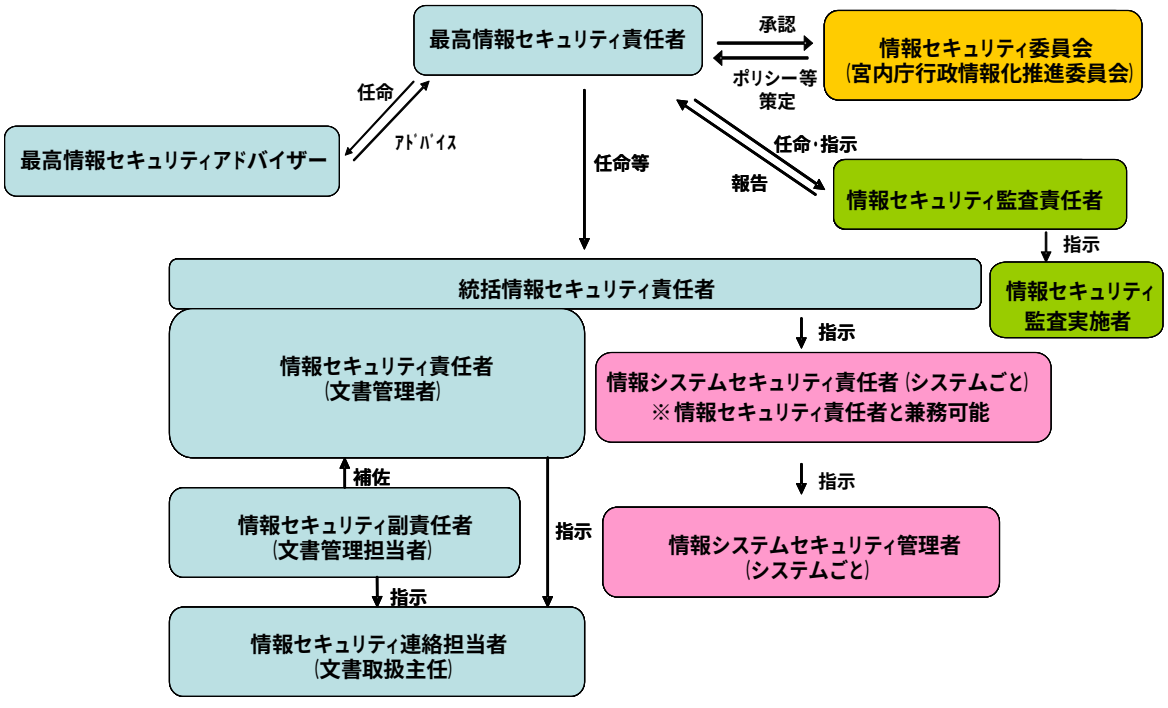
ケ　情報セキュリティ副責任者

情報セキュリティ責任者を補佐する者として，各課等の文書管理担当者が情報セキュリティ副責任者を務めています。

コ　情報セキュリティ連絡担当者

情報セキュリティ責任者及び情報セキュリティ副責任者の指示の下，部局の情報セキュリティに関する事務を行う者として，各課等の文書取扱主任が情報セキュリティ連絡担当者を務めています。

宮内庁情報セキュリティポリシーに係る体制図



(3) 情報セキュリティ監査の実施

宮内庁では，統一管理基準及びポリシーに基づき，毎年度，情報セキュリティ監査計画を策定の上，監査を実施しています。

監査の内容は，宮内庁の情報セキュリティ関連規程類の統一管理基準及び統一技術基準への準拠性や，情報セキュリティ対策自己点検に関する監査及び情報システムの情報セキュリティ対策の実施状況の監査です。

なお，監査の対象となる情報システムは，毎年度，情報システムのライフサイクルを考慮して実施しています。

平成 23 年度に実施した情報セキュリティ監査の内容は，次のとおりです。

ア　監査対象

(ｱ) ポリシーの統一管理基準との準拠性，技術基準の統一技術基準との準拠性並びに各実施規程・手順のポリシー及び技術基準との準拠性

(ｲ) 情報セキュリティ対策自己点検

(ｳ) 宮内庁情報ネットワークシステムのシステム設定

イ　監査時期及び監査体制

監査は，平成 23 年 11 月 16 日から平成 24 年 2 月 27 日の期間で，情報セキュリティ監査責任者及び同責任者から指名された監査担当者が主体となり，実施しました。

ウ　監査結果

(ｱ) ポリシーの統一管理基準との準拠性及び技術基準の統一技術基準との準拠性については，改善を必要とする指摘事項はありません。しかし，下位規程である，各実施規程・手順書類については，ポリシー及び技術基準との準拠性において，一部，改善を要するものが見受けられました。

(ｲ) 情報セキュリティ対策自己点検の監査

情報セキュリティ責任者等，情報システムセキュリティ責任者等及び職員に対して，自己点検における全項目の回答内容が正しいか確認し，自己点検が適正に実施されていることが確認されました。

しかし，若干ながら，ポリシーの趣旨の理解が不十分であることを示す事例も見受けられました。

(ｳ) 宮内庁情報ネットワークシステム

ポリシーに則った手順書どおりに利用できており，実際のシステム設定も手順書等と整合していることが確認されました。

エ　監査結果を踏まえた対応

今回監査対象とした職員のみならず，全職員に対し，ポリシーの規定の趣旨を更に浸透させるため，情報セキュリティ研修の充実など職員への教育・啓発を図ることとします。

(4) 情報セキュリティ対策に関する文書の見直し状況

政府において統一管理基準及び統一技術基準の改定が行われた際には，ポリシー及び技術基準に適切に反映させ，準拠性を確保することとしています。

5　平成 23 年度の重点事項

(1) 重点事項の目標，実績及び評価

ア　ポリシー及び関連規程の見直し

統一基準の改定に準拠し，宮内庁情報セキュリティポリシーの体系を以下のように改定しました。

「宮内庁における情報セキュリティの基本方針」（統一規範に対応）
「宮内庁情報セキュリティポリシー」（統一管理基準に対応）
「情報セキュリティ対策のための技術基準」（統一技術基準に対応）

イ　仕様書作成時におけるセキュリティ要件策定手順の標準化の検討

仕様書の作成過程で，「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を参考にして業務の特徴の整理等を行いました。

(2) 障害・事故等の再発防止策

平成 23 年度は，情報セキュリティに関する重大な障害・事故は発生していません。また，軽微な故障等についても，速やかに対処し，再発防止策を講じています。

6　平成 23 年度における情報セキュリティ対策の取組

(1) ポリシーに関する対策実施状況の自己点検

ポリシーに関する対策実施状況の自己点検（以下「自己点検」という。）は，ポリシーに規定された遵守事項についての　実施状況を全ての職員が自ら確認・点検するものです。

自己点検の実施は，各職員が情報セキュリティ対策の内容を理解し，情報セキュリティ対策に対する意識を向上させることにもつながるものと考えます。

宮内庁においては，平成 20 年度から，全職員を対象に自己点検を実施しています。

ア　平成 23 年度自己点検における課題と対策

平成 23 年度の自己点検では，把握率（全職員のうち自己点検を提出した者の割合）は 100%でした。

実施率（責務が生じた事項のうち，遵守された項目の割合）については，情報セキュリティ責任者，情報システムセキュリティ責任者等は 100%でしたが，職員については，前年度に実施率の低かった分野である「情報のライフサイクル（作成と入手，利用，保存，移送，提供，消去)」に対象を絞って実施したことから，実施率は 99.4%であり，改善の余地があります。

また，到達率（全対象者のうち一定の割合以上の者が対策を実施した遵守事項の割合）については，情報セキュリティ責任者，情報システムセキュリティ責任者等は前年度に引き続き 100%と高い水準でしたが，職員においては，上述の理由から「到達率 100%」の達成率が低い値となっています。

これらの結果を受け，各情報セキュリティ責任者に対し，最高情報セキュリティ責任者から改善指示をしたほか，職員向けの情報セキュリティ研修の中で，情報の格付を行うために必要な観点を重点的に解説し，職員の知識と意識の向上を図りました。

イ　平成 23 年度の自己点検結果の状況

(ｱ) 把握率

平成 23 年度の宮内庁全体の自己点検を提出した者の割合である把握率は 100%です。

把握率

対象年度	把握率
平成 23 年度	100%

(ｲ) 実施率

自己点検提出者のうち，対策を実施した者の割合である対策実施率の主体別の状況は次のとおりです。セキュリティ責任者等及びシステムセキュリティ責任者等では前年度に続き 100%, 職員については, 99. 4%でした。

実施率

対象年度	責任者等	システム責任者等	職　員
平成 23 年度	100%	100%	99.4%

(ｳ) 到達率

自己点検提出者のうち，全対象者のうち一定の割合（100%，95%，90%）以上の者が対策を実施した遵守事項の割合である到達率の主体別の状況は，以下のとおりです。

【到達率 100%】

対象年度	責任者等	システム責任者等	職　員
平成 23 年度	100%	100%	0%

【到達率 95%】

対象年度	責任者等	システム責任者等	職　員
平成 23 年度	100%	100%	100%

【到達率 90%】

対象年度	責任者等	システム責任者等	職　員
平成 23 年度	100%	100%	100%

ウ　自己点検結果の総評

平成 23 年度の自己点検は，上記イのとおり，把握率は 100%で，実施率も高い水準であるのに対し，到達率については，改善の余地があります。

エ　自己点検結果に基づく改善指示

自己点検の結果を踏まえ，今後は実施率の比較的低い遵守事項に焦点を絞った教材を整備するなど，情報セキュリティ教育研修の内容を見直すとともに，機会あるごとに職員に対する啓発を行っていくこととします。

(2) 情報システムのごとの状況

ア　課題と対策

情報システムのセキュリティ対策は，情報システムで取り扱う情報を守るという点から重要なものであり，また，情報システムは様々な脅威にさらされています。したがって，情報システムに対するセキュリティ対策は，システムを利用するユーザーの利便性との調整を図りながら，適切な対策を実施する必要があります。

宮内庁では，公開用ウェブサーバ，電子メールサーバ及びDNSサーバに対する情報セキュリティ対策について，統一管理基準及び統一技術基準で規定された遵守事項の実施状況について重点的な検査を実施しています。

検査は，宮内庁ホームページの公開用ウェブサーバ，電子メールサーバ及びDNSサーバを対象に，搭載しているOSなどソフトウェアのセキュリティ修正プログラムの適用状況や，不正アクセス対策及び不正プログラム対策などの情報セキュリティ対策実施状況について検査を実施し，確認を行っています。

平成23年度の検査結果は，公開用ウェブサーバにおいて一部改善の余地があるほかは，電子メールサーバ及びDNSサーバのいずれもおおむね問題なく対策を実施しています。

イ　平成23年度情報システムの対策実施状況

平成23年度の重点検査における情報システムの対策状況は，次のとおりです。

(ｱ) 公開用ウェブサーバ

公開用ウェブサーバの不正プログラム対策，不正アクセス対策，情報保護対策及びサーバ管理の対策事項については，おおむね対処されていますが，一部の項目については改善の余地があります。

(ｲ) 電子メールサーバ

電子メールサーバについては，不正プログラム対策，不正アクセス対策，情報保護対策及びサーバ管理の対策事項の実施率は， 100%を達成しています。

(ｳ) DNS サーバ

DNS サーバについては，DNSSEC 対応が実施されています。

ウ　総評

宮内庁では，情報システムのセキュリティ対策には万全を期するための対策を講じてきましたが，今回の検査結果を踏まえ，引き続き，より適切な情報セキュリティ対策の実施に努めます。

(3) 情報セキュリティ教育・啓発

ア　教育計画の策定及び教育の企画等

情報セキュリティ対策を着実に実施するためには，情報を取り扱う職員それぞれが情報セキュリティ関連規程に基づく具体的なセキュリティ対策を理解し，遵守することが肝要であり，そのためには，職員に対する教育，研修が重要なものと考えています。

宮内庁では，情報セキュリティ教育についての年度計画を策定し，集合教育や職員用電子掲示板を利用した自習教育を実施しています。集合研修については，初級及び中級の 2 つの段階に分けて，それぞれ 2 回ずつ，6 月と 3 月に実施する計画としました。

イ　対象者の知識レベルに応じた教育教材の整備

職員の情報セキュリティ対策についての知識，経験及び理解度に応じ，初級用と中級用の教育教材を作成しています。

また，教材には，情報のライフサイクルにおけるセキュリティ対策や，日常的に使われるインターネットやメールにおける対策を適宜記載しています。さらに，国内外で発生したセキュリティ事故の実例を紹介しながら，課題や取るべき対策を具体的に説明するようにしています。

特に今年度は，政府機関を標的とした「標的型サイバー攻撃」が多発したこと及び当庁においても「標的型メール攻撃訓練」を実施したことを踏まえ，「標的型メール」に焦点を当てた解説を行いました。

ウ　教育受講状況の管理

集合研修において出席状況を確認するとともに，自己点検の結果分析等を通じてセキュリティ教育の効果を確認しています。

エ　教育による効果等

定期研修のほか，自己点検の実施や「標的型メール攻撃訓練」の実施等が，職員の意識向上に寄与するものと推察します。今後も，充実した教育機会の提供や教材の整備に努めます。

(4) 調達・外部委託

情報システムの開発などの業務を外部に委託して実施する際には，宮内庁の求める情報セキュリティの水準が委託先において確保されている必要があります。

このため，宮内庁では，外部委託を行う際，委託元としての業務を行う情報システムセキュリティ責任者が遵守すべき事項を定め，外部委託により行う情報処理業務の遂行において必要な情報セキュリティ水準を確保するよう規定を整備しています。

7　情報セキュリティに関する障害・事故等報告

宮内庁では，情報セキュリティに関する重大な障害・事故等はありませんでした。

宮内庁では，万一，情報セキュリティに関する障害・事故等が発生した場合には，障害時の対応手順（障害等対応規程）や緊急連絡網により，発生箇所の責任者がその状況を把握し，関係者に連絡することになっており，障害・事故等に対応した後は，再発防止策を策定し，最高情報セキュリティ責任者に報告することになっています。

また，内閣官房情報セキュリティセンターから提供される不審メール情報等については，職員用電子掲示板に随時掲載し，常に注意喚起を行うとともに，職員が使用しているパソコンの OS やソフトウェアの脆弱性情報を常に収集し，全職員のパソコンにセキュリティ修正プログラムを随時配信しています。

8　情報セキュリティ対策に関する平成 24 年度の計画

平成 24 年度は，引き続き，情報セキュリティ対策に関する自己点検及び教育を実施するとともに，情報システムの重点検査を実施します。

また，内閣官房情報セキュリティセンターを中心として進められる統一管理基準及び統一技術基準の改定等の諸施策に対応し，宮内庁では，以下の取組を平成 24 年度も継続して実施します。

① ポリシー，技術基準及び関連規程の見直し

② 標的型サイバー攻撃等に適切に対処するため，職員が正しい判断基

準を持てるよう情報セキュリティ教材を充実するとともに，研修・訓練の機会の確保

9　おわりに

宮内庁は皇居，京都事務所，正倉院事務所，御料牧場など，広域かつ多数の拠点を有しており，それぞれを接続したネットワークを構成しております。その中で皇室関係の事務を担い，機密性の高い情報を取り扱うことから，情報セキュリティ対策を確実に実施することが求められます。

平成 23 年度は，情報セキュリティ事故等の発生はなく，公開サーバ等の検査においてもセキュリティ対策が施されている点は十分評価できると考えられます。ただし，自己点検においては，全ての職員に対するセキュリティ対策の徹底が必ずしも完全ではないことが課題であり，今後も情報セキュリティ教育研修等を通じて更なるポリシーの周知・徹底を行う必要があります。

特に，昨今問題となっている「標的型メール」等の標的型サイバー攻撃に対処するためには，職員一人ひとりが正しい判断基準を持つことが重要であり，そのために必要な知識を得る場としての研修，訓練等を充実させることが急務です。

情報セキュリティ対策には，物理的側面，技術的側面及び人的側面がありますが，人的対策として，職員が日常業務の中でルールを意識し，遵守する習慣ができることが非常に重要です。自己点検における課題を踏まえ，宮内庁の日常業務の遂行においても情報セキュリティに対する高い意識が維持できるよう，今後も取組を継続する必要があります。

宮内庁最高情報セキュリティアドバイザー
樋口勝彦