



報道資料

平成 23 年 10 月 14 日
内閣官房情報セキュリティセンター (NISC)

情報セキュリティ対策推進会議第 3 回会合の開催について

－官民連携の強化のための分科会の設置等について－

本日、「情報セキュリティ対策推進会議」(議長:内閣官房副長官(事務))の第3回会合が開催されました。

その概要は、以下のとおり。

官民連携の強化のための分科会の設置

10月7日に開催された情報セキュリティ政策会議の審議を踏まえ、情報セキュリティ対策における官民連携の強化に向けた検討を行うため情報セキュリティ対策推進会議(以下「CISO等連絡会議」という。)に「官民連携の強化のための分科会」を設置。CISO等連絡会議に引き続き、第1回の分科会を開催。

政府機関における主な取組

- ・内閣官房等12の政府機関約5万人を対象とした「標的型不審メール訓練」の実施。
- ・電子メールの送信元について、なりすましを防止するための対策の一環として「DNSサーバへのSPFレコードの記録」を推進。

(別添) CISO 等連絡会議第3回資料一式

※ 本日の会議資料は、内閣官房情報セキュリティセンターのホームページにおいても公表する。
(<http://www.nisc.go.jp/conference/seisaku/index.html>)

情報セキュリティ対策推進会議（CISO等連絡会議）第3回

平成23年10月14日(金) 15時00分～15時30分
於：総理大臣官邸2階大ホール

<議事次第>

1 開会

2 議事

- (1) 官民連携の強化のための分科会の設置について
- (2) 政府機関における主な取組について
- (3) 情報セキュリティ対策推進会議幹事会の設置規程の改正について

3 閉会

<配布資料>

資料1 官民連携の強化のための分科会の設置

資料1-1 官民連携の強化のための分科会について(案)
(設置規程)

資料2-1 政府機関における標的型不審メール訓練について

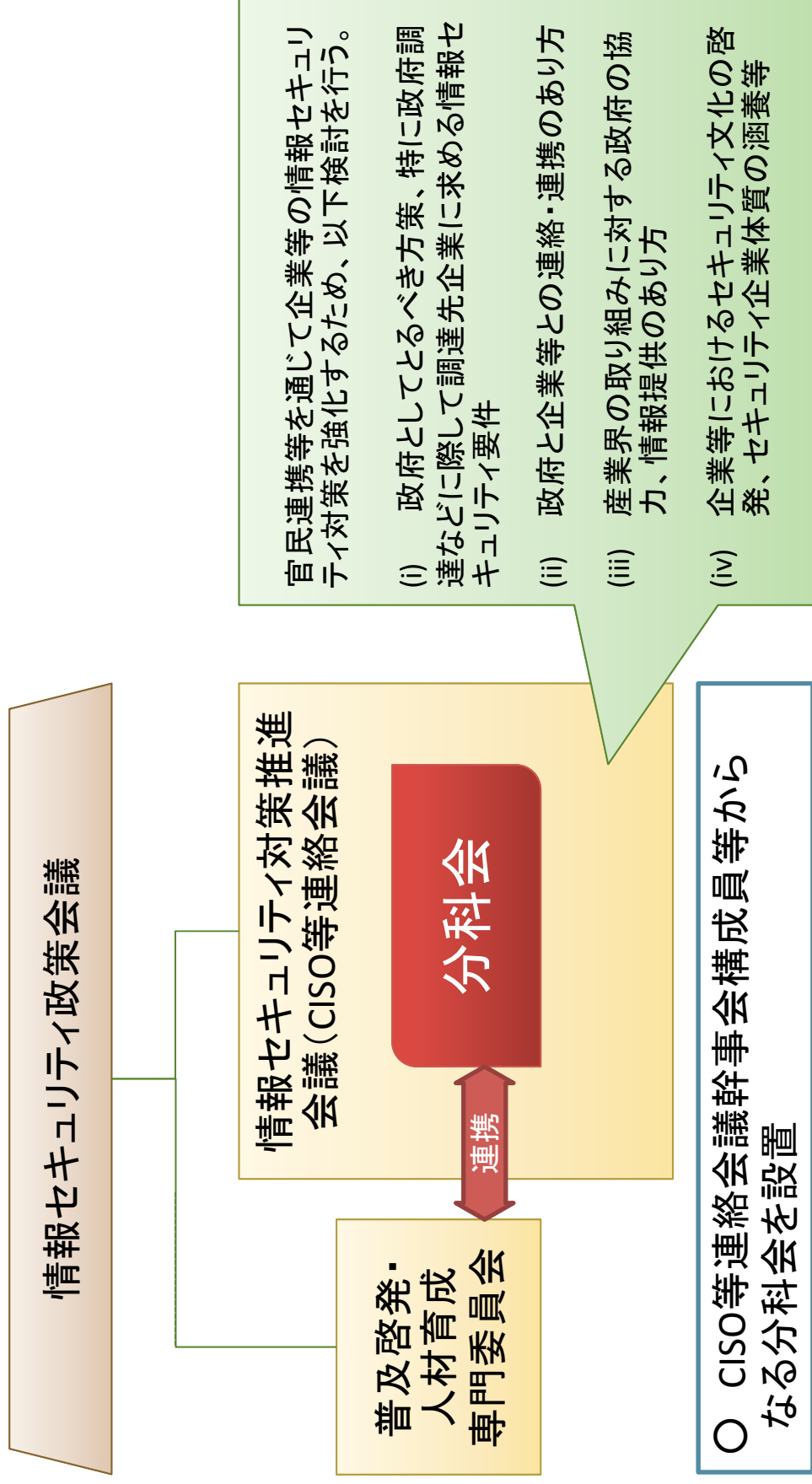
資料2-2 政府のメールアドレスを詐称されないための対策について

資料3 情報セキュリティ対策推進会議幹事会について(案)
(設置規程の改正)

参考資料1 情報セキュリティ対策の強化について
(10月7日情報セキュリティ政策会議 官房長官メッセージ)

参考資料2 三菱重工業等に対するサイバー攻撃事案について(経緯等)

官民連携の強化のための分科会の設置



* CISO: Chief Information Security Officer (最高情報セキュリティ責任者)

官民連携の強化のための分科会の進め方（案）

会議は、原則非公開とし、検討結果については、推進会議等に報告

検討体制

今後の進め方

分科会長	内閣審議官（情報セキュリティセンター 副センター長）
構成員	危機管理審議官 内閣参事官（情報セキュリティセンター）
警察庁	生活安全局情報技術犯罪対策課長 警備局警備企画課長 情報通信局情報管理課長
総務省	大臣官房企画課長 情報流通行政局情報セキュリティ対策室長
経済産業省	大臣官房情報システム厚生課長 商務情報政策局情報経済情報セキュリティ政策室長
防衛省	運用企画局情報通信・研究課情報保証室長 経理装備局装備政策課開発・調達企画室長

○月1回程度開催予定

○必要に応じ、民間有識者から意見聴取。

○来年2月の情報セキュリティ月間を活用し、対策の強化を図る。

* 必要に応じて構成員以外の者を参加させることができる。

官民連携の強化のための分科会について（案）

平成23年 月 日
情報セキュリティ対策推進会議決定

1. 情報セキュリティ対策推進会議（以下「推進会議」という。）に、推進会議幹事会の関係省庁構成員等からなる「官民連携の強化のための分科会」（以下「官民連携分科会」という。）を置く。
2. 官民連携分科会は、重要な情報を扱う企業等における情報セキュリティ上の脅威が高まってきていることを踏まえ、普及啓発・人材育成専門委員会と連携して企業等における情報セキュリティ対策を強化するため、以下の検討を行う。
 - (i) 政府としてとるべき方策、特に政府調達などに際して調達先企業に求める情報セキュリティ要件
 - (ii) 政府と企業等との連絡・連携のあり方
 - (iii) 産業界の取り組みに対する政府の協力、情報提供のあり方
 - (iv) 企業等におけるセキュリティ文化の啓発、セキュリティ企業体質の涵養等
3. 検討結果については、推進会議等に報告する。

なお、重要インフラ部門については、すでに重要インフラの情報セキュリティ対策に係る行動計画等により対策を推進していることから、この取組を参考として官民連携分科会における検討の内容を充実させるものとする。
4. 官民連携分科会の構成は、次のとおりとする。

分科会長	内閣審議官（情報セキュリティセンター 副センター長）
構成員	危機管理審議官
	内閣参事官（情報セキュリティセンター 基本戦略立案担当）
	内閣参事官（情報セキュリティセンター 情報統括担当）
	内閣参事官（情報セキュリティセンター 政府機関総合対策促進担当）
	内閣参事官（情報セキュリティセンター 事案対処調整担当）
	警察庁生活安全局情報技術犯罪対策課長
	警察庁警備局警備企画課長
	警察庁情報通信局情報管理課長
	総務省大臣官房企画課長
	総務省情報流通行政局情報セキュリティ対策室長

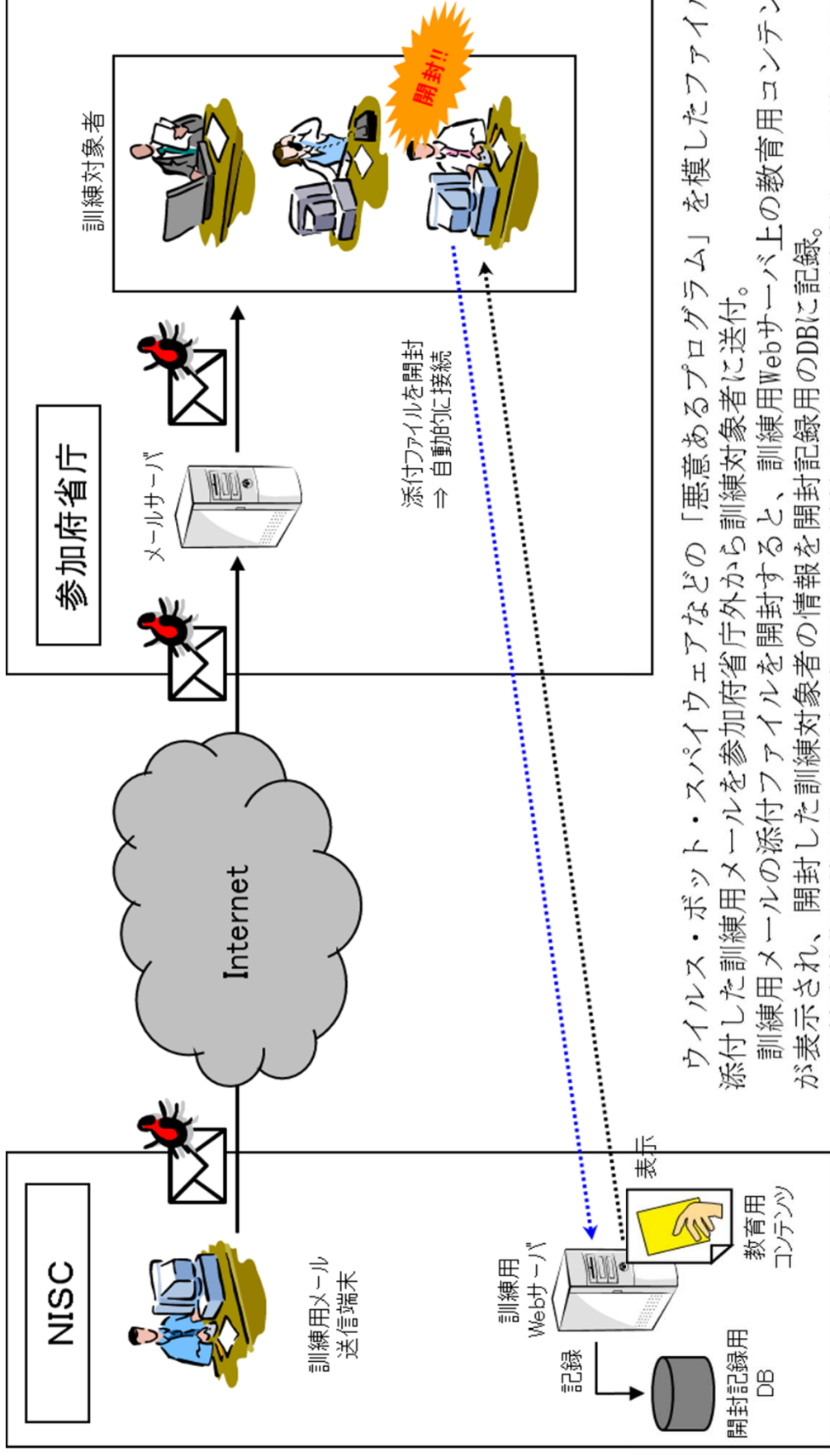
経済産業省大臣官房情報システム厚生課長
経済産業省商務情報政策局情報経済課情報セキュリティ政策室長
防衛省運用企画局情報通信・研究課情報保証室長
防衛省経理装備局装備政策課開発・調達企画室長

5. 分科会長は、必要に応じて構成員以外の者を参加させることができる。
6. 官民連携分科会の庶務は、内閣官房情報セキュリティセンターにおいて処理する。
7. 官民連携分科会の内容は原則として非公開とし、適宜、推進会議等に報告を行う。
8. 前各項に掲げるもののほか、官民連携分科会の運営に関する事項その他必要な事項は、分科会長が定める。

政府は、本年5月に情報セキュリティ対策推進会議(CISO等連絡会議)において決定した「政府機関における情報セキュリティに係る年次報告」において取り組みを推奨した「標的型不審メール訓練」を以下のとおり実施する。

1. 訓練期間 平成23年10月～12月
2. 訓練対象 内閣官房等12の政府機関約5万名
3. 訓練内容
 - ①訓練対象者に対して、標的型不審メールを模擬したメールを送付。
 - ②模擬メール中の添付ファイルを開封するなど不適切な扱いをした場合は、教育コンテンツに誘導。
 - ③参加府省庁のCISOに個別の訓練結果を通知し、府省庁内において適切な教育指導を実施。
 - ④CISO等連絡会議にて訓練結果の総評を報告。

参考（訓練の実施イメージ図）



ウイルス・ボット・スパイウェアなどの「悪意あるプログラム」を模したファイルを送付した訓練用メールを参加府省庁外から訓練対象者に送付。

訓練用メールの添付ファイルを開封すると、訓練用Webサーバ上の教育用コンテンツが表示され、開封した訓練対象者の情報を開封記録用のDBに記録。

訓練実施期間終了後、開封記録用DBから添付ファイルの開封者数や、開封した理由等の教育結果を集計。

◎ 標的型メールを見極めるポイント

1. 差出人欄に注意！！
(フリーメールアドレスや普段やりとりのない@ドメイン)
2. 件名に注意！！
(【至急】【重要】は罨キーワード)
3. 本文末の署名に注意！！
(差出人メールアドレスと署名のメールアドレスが違う)

◎ 不審なメールが送られて来た場合の対処方法

ヘルプデスクもしくは、情報システムセキュリティ管理者に連絡する

◎ 万が一不審なメールの添付ファイル等を開封してしまった場合の対処方法

1. LANケーブルを抜く
2. ヘルプデスクもしくは、情報システムセキュリティ管理者に連絡する

電子メールの送信元について、なりすましを防止するための対策の一環としてDNSサーバへのSPFレコードの記録を推進

これまでの主な取組

- ・ 本省、外局、地方支分部局、独立行政法人等において、送信側SPFの導入を推進
- ・ 本府省庁ドメインについて、送信側SPFの設定を完了（H22年7月）
 - * 外局等を含むDNSサーバ（送信側）におけるSPF設定状況（率）
H23年 7月末現在 37.4% → H23年10月13日現在 63.2%
- ・ 受信側においても、送信元を検証する機能を設定することを推進

具体的な取組内容

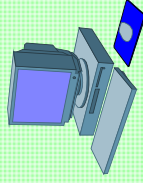
- ・ DNSサーバにSPFレコードを記載
- ・ 利用していないgo.jpドメインについては、廃止
- ・ メール送信を行わないgo.jpドメインについては、メール送信を行わない旨をSPFレコードに記述

* SPF (Sender Policy Framework) : メールを送信元アドレスの偽装を防止する技術

送信ドメイン認証について

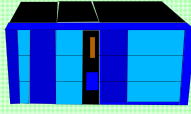
メールの送信手順

送信者のPC



送信側メールサーバ

IPアドレス 192.0.2.112
ドメイン名 smtp.xxx.go.jp



メールを作成・送信

送り先のドメイン名から受信側メールサーバのIPアドレスを確認して、送信者のメールアドレス (alice@xxx.go.jp) などを送信

送信側メールサーバのIPアドレスを頼りにメールを受け取る準備ができたことを

返信

メール本文を送信

受信側メールサーバ

IPアドレス 198.18.100.240
ドメイン名 smtp.example.co.jp



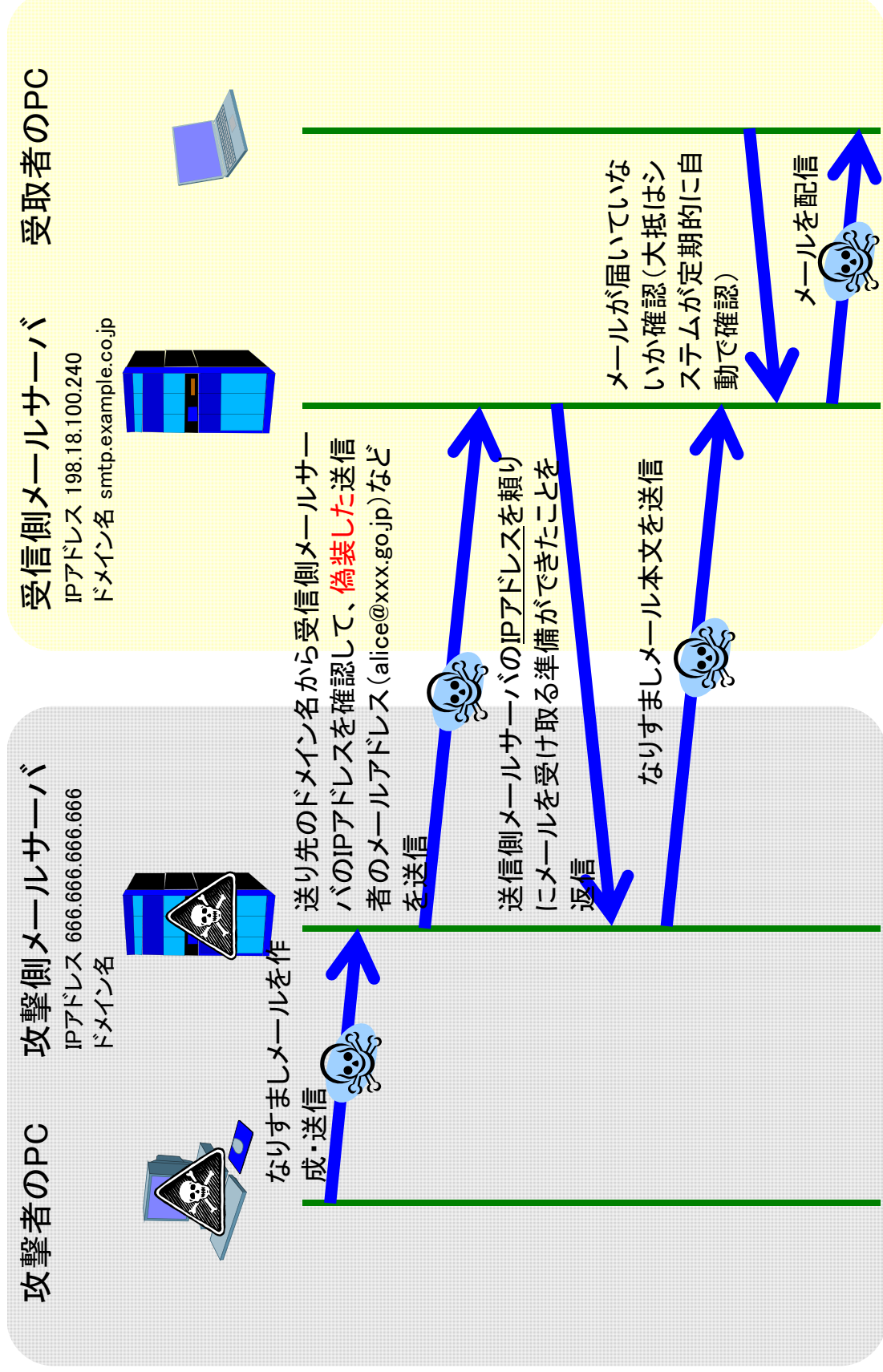
受取者のPC

メールが届いていないか確認(大抵はシステムが定期的に自動で確認)

メールを配信

送信ドメイン認証について

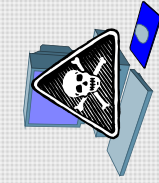
なりすましメールの場合



送信ドメイン認証について

SPFレコードの確認

攻撃者の
PC
攻撃側メールサーバ
IPアドレス 666.666.666.666
ドメイン名

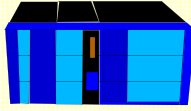


なりすましメールを作成・送信

偽装した送信者のメールアドレス (alice@xxx.go.jp) などを送信

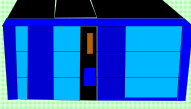


受信側メールサーバ
IPアドレス 198.18.100.240
ドメイン名 smtp.example.co.jp

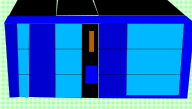


偽装したメールアドレスのドメイン名から、なりすまされた側のDNSサーバに正しいメールサーバのIPアドレスを問い合わせる

なりすまされたドメインのDNSサーバ



なりすまされたドメインのメールサーバ
IPアドレス 192.0.2.112
ドメイン名 smtp.xxx.go.jp



SPFレコードの形式で回答とIPアドレスが一致しなかったので送信を許可しない



正しいメールサーバのIPアドレスを回答

```
"v=spf1 +ip4:192.0.2.112 -all"
```

情報セキュリティ対策推進会議幹事会について（案）

平成22年12月27日

平成 年 月 日

情報セキュリティ対策推進会議決定

1 情報セキュリティ対策推進会議幹事会（以下「幹事会」という。）の構成は、次のとおりとする。

議長	内閣官房内閣審議官（情報セキュリティセンター）
構成員	内閣官房内閣参事官（内閣総務官室）
	内閣官房内閣参事官（安全保障・危機管理）
	内閣官房内閣参事官（情報セキュリティセンター）
	内閣官房内閣参事官（情報通信技術（IT）担当室）
	内閣官房内閣参事官（内閣広報室）
	内閣官房内閣参事官（内閣情報調査室）
	内閣法制局長官総務室総務課長
	人事院事務総局総務課広報情報室長
	内閣府大臣官房企画調整課長
	宮内庁長官官房秘書課長
	公正取引委員会事務総局官房総務課長
	警察庁生活安全局情報技術犯罪対策課長
	警察庁情報通信局情報管理課長
	金融庁総務企画局総務課長
	<u>消費者庁総務課長</u>
	総務省大臣官房企画課長
	法務省大臣官房秘書課長
	外務省大臣官房情報通信課長
	財務省大臣官房文書課業務企画室長
	文部科学省大臣官房政策課情報化推進室長
	厚生労働省大臣官房統計情報部企画課情報企画室長
	<u>農林水産省大臣官房評価改善課長</u>
	経済産業省大臣官房情報システム厚生課長
	経済産業省商務情報政策局情報経済課情報セキュリティ政策室長
	<u>国土交通省総合政策局情報政策課長</u>
	環境省大臣官房総務課環境情報室長
	防衛省運用企画局情報通信・研究課情報保証室長

オブザーバー 衆議院事務局庶務部会計課情報化推進室長

参議院事務局庶務部文書課情報化推進室長
国立国会図書館電子情報部電子情報企画課長
会計検査院事務総長官房上席情報処理調査官
最高裁判所事務総局情報政策課参事官
日本銀行システム情報局システム企画課情報セキュリティ・
SCCグループ長

- 2 幹事会は、特定の事項について専門的な検討を行うため、必要に応じて、ワーキンググループを設けることができる。
- 3 その他幹事会の運営に関し必要な事項は、幹事会において定める。

情報セキュリティ対策の強化について

平成 23 年 10 月 7 日

情報セキュリティ政策会議議長

内閣官房長官 藤村 修

情報通信技術の発展により、私たちは多大な経済的利益や生活の利便性を享受していますが、その一方で、情報セキュリティ上の脅威も日常のものとなっています。こうした中、国の重要な情報を扱う企業がサイバー攻撃の対象となり、不正なプログラムに感染するという事態が発生しました。

サイバー攻撃は、被害によっては国の安全や国民生活に深刻な事態をもたらす可能性があります。政府及び重要インフラ関連組織においては、これまで進めてきた情報セキュリティ対策を更に高めてまいります。国の重要な情報を扱い国の安全に深く係わる企業の皆様におかれても、今回の事態を契機に、企業の情報セキュリティの一層の強化に努めてください。

情報セキュリティの確保においては、とりわけ早期の情報共有が重要です。その観点に立ち、政府は今後、政府・民間双方向の情報共有等を通じた官民連携の強化を進めてまいりますので、関係する皆様のご理解とご協力をお願いいたします。

情報セキュリティ上のリスクは、被害者となる恐れがあることはもちろんのこと、不正なプログラムに感染することで意図せずに加害者になってしまうこともあります。情報セキュリティ対策を講じることは、今や社会的な責務ともいえるものになっています。

企業等におかれては、攻撃に強いシステムの導入と、職場一人一人の情報セキュリティ意識の向上等に努めるとともに、感染してしまった場合であっても、被害を最小限にとどめる対策の実施が必要です。国民の皆様におかれては、自分のパソコンやスマートフォン等について、そのセキュリティ関連ソフトウェアを常に最新の状態に維持するなどの対策に努めてください。

情報セキュリティの確保は、安全で安心な国民生活の実現と国際競争の中での継続的な発展に不可欠なものとなっています。官民の連携により世界最先端の情報セキュリティの実現に努めてまいります。

三菱重工業等に対するサイバー攻撃事案について（経緯等）

三菱重工業等に対する攻撃（標的型攻撃によるウィルス感染）

- 防衛装備品や原子カプラントを製造している三菱重工業のコンピュータがウィルスに感染し、情報が抜き取られた痕跡ありと報道（9/19 読売）。同社によると、本社、研究所等の約 80 台のサーバやパソコンが実際に感染し、一部のコンピュータのシステム情報が流出した可能性があるものの、製品や技術に関する情報の流出は確認されていない。
- I H I、川崎重工業、三菱電機に対しても同様の攻撃があったと報道（9/21 各紙）。関係省庁からのヒアリング調査に対し各社は、現時点で重要な情報の漏えいは確認されていない旨回答。
- 政府においては、内閣官房において全府省庁の担当課長等を集め、「政府内の迅速な情報共有」の徹底を指示（9/20）。
- 経済産業省及び防衛省において、引き続き情報収集を実施中。また、警察は三菱重工業からの被害届の提出（9/30）を受け、捜査中。

（参考）本年 9 月中旬の我が国政府機関等に対する攻撃（アクセス集中）

- 中国のチャットサイトに我が国へのサイバー攻撃の呼びかけが掲載されたことを受け、内閣官房から全府省庁に対し関連情報を提供するとともに、事態への警戒、事態発生の際の迅速な連絡を依頼（9/15）。
- また、在中国日本国大使館から中国政府に対し「攻撃が発生することのないよう、早急に適切な対策を講じることを求める」旨、申し入れを実施（9/15）。
- 9 月 17 日から 18 日にかけて、人事院 HP 及び内閣府 HP（政府インターネットテレビ等）が、アクセス集中により一時的に閲覧しづらい状態になった。システム侵入等の被害はなし。