Security Report

May 25, 2012
Toshio Nishihara, CCIE R&S, Security
Consulting Systems Engineer
Borderless Network Systems Engineering
Cisco Systems G.K.

Agenda

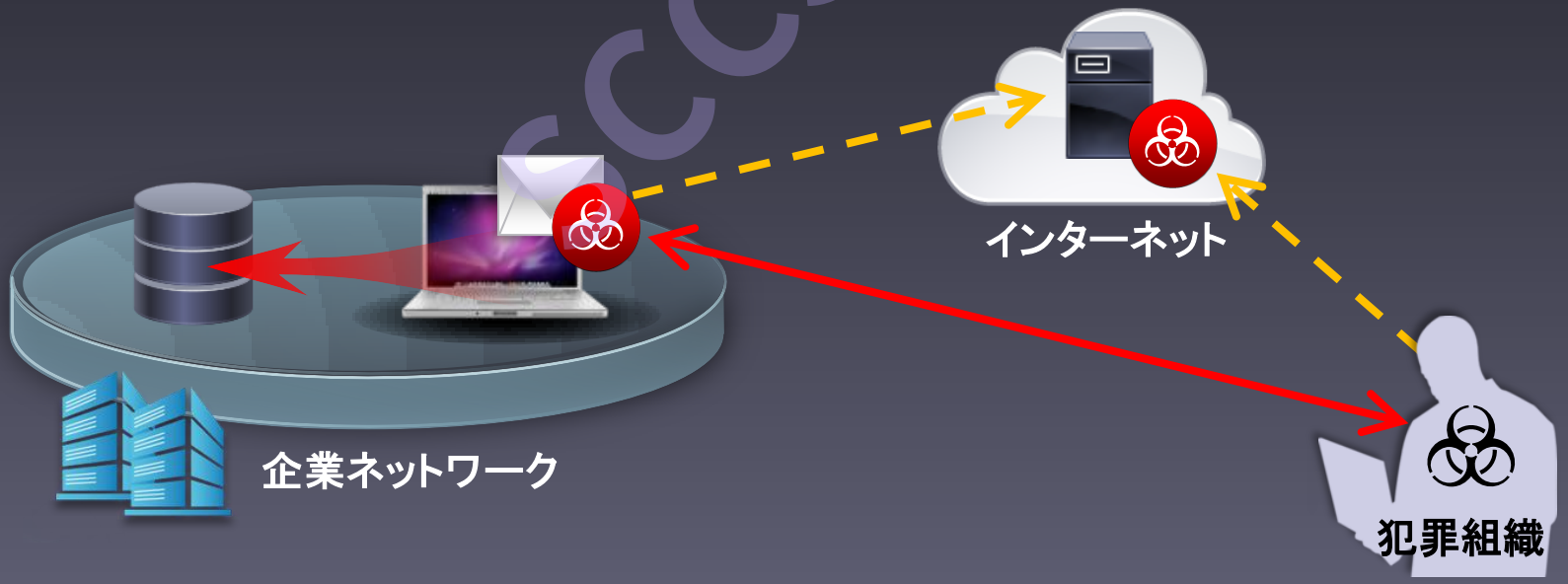
- Guess Number
- Advanced Persistent Threat (APT)
- Security Architecture
- Action Item

Advanced Persistent Threat

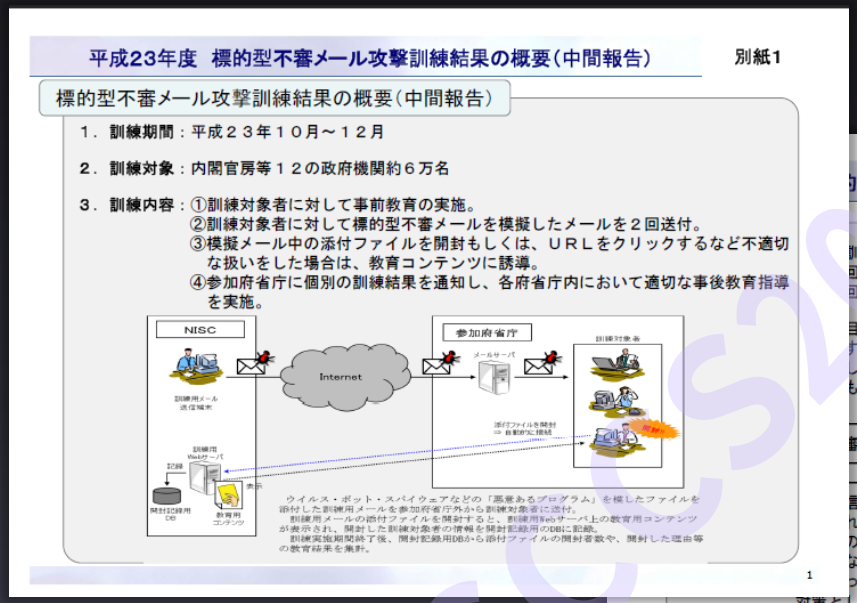
従来の対処法における内在された課題

現状の起きている問題は、以下のような仕組みで情報が流出しています。

1. 犯罪組織が主にソーシャルエンジニアリングで情報収集し、ターゲットを定める
2. 犯罪組織がターゲットにエクセルなどの添付ファイル付きのメールを送信する
3. ターゲットがメールを受信し、添付ファイル(例：エクセル)を開く
4. 添付ファイルのエクセルには、エクセルの脆弱性を突く不正プログラムが仕組まれている
5. 不正プログラムが省庁・企業内から犯罪組織へアクセスし、PCを遠隔操作するための不正ツールをダウンロードする
6. 犯罪組織が不正ツールを利用し、遠隔からPC/サーバの情報を盗み続ける



政府の標的型不審メール攻撃訓練の結果


平成23年度　標的型不審メール攻撃訓練結果の概要（中間報告）

別紙1

標的型不審メール攻撃訓練結果の概要（中間報告）

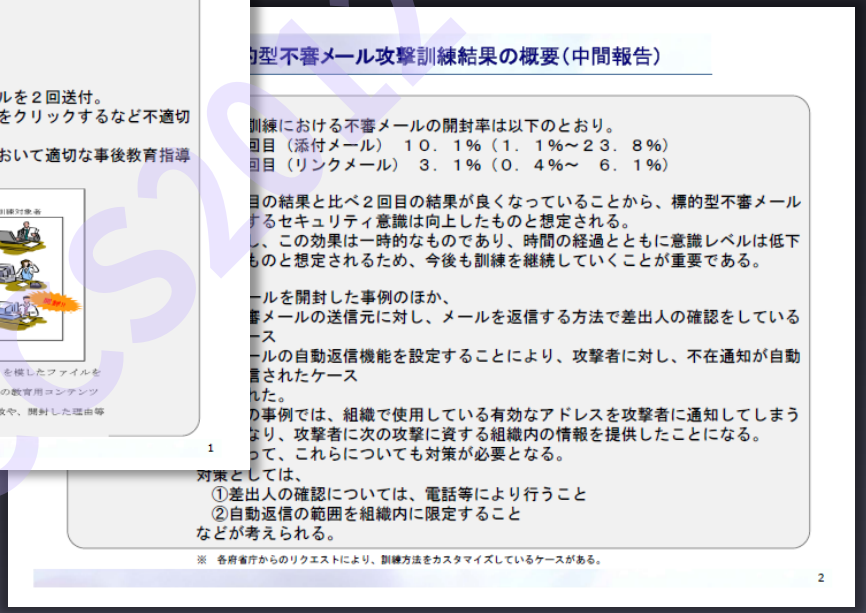
1．訓練期間：平成２３年１０月～１２月

2．訓練対象：内閣官房等１２の政府機関約６万名

3．訓練内容：①訓練対象者に対して事前教育の実施。
②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２回送付。
③模擬メール中の添付ファイルを開封もしくは、ＵＲＬをクリック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。
④参加府省庁に個別の訓練結果を通知し、各府省庁内において適切な事後教育指導を実施。

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添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。

1


型不審メール攻撃訓練結果の概要（中間報告）

訓練における不審メールの開封率は以下のとおり。
回目（添付メール）　１０．１%（１．１%～２３．８%）
回目（リンクメール）　３．１%（０．４%～　６．１%）

目の結果と比べ２回目の結果が良くなっていることから、標的型不審メールするセキュリティ意識は向上したものと想定される。
し、この効果は一時的なものであり、時間の経過とともに意識レベルは低下ものと想定されるため、今後も訓練を継続していくことが重要である。

ールを開封した事例のほか、
審メールの送信元に対し、メールを返信する方法で差出人の確認をしている
ース
ールの自動返信機能を設定することにより、攻撃者に対し、不在通知が自動信されたケース
れた。
の事例では、組織で使用している有効なアドレスを攻撃者に通知してしまうなり、攻撃者に次の攻撃に資する組織内の情報を提供したことになる。
って、これらについても対策が必要となる。

対策としては、
①差出人の確認については、電話等により行うこと
②自動返信の範囲を組織内に限定すること
などが考えられる。

※　各府省庁からのリクエストにより、訓練方法をカスタマイズしているケースがある。

2

例え「1通」の開封でも標的型攻撃は成立する事実を踏まえると、旧来の予防（入口）のみならず発見（出口）と予防 & 発見（真ん中）の防衛ラインを考慮が必要

出典：政府機関における情報セキュリティ対策の取り組み状況について
http://www.nisc.go.jp/press/pdf/torikumi_press.pdf

APT攻撃のターゲットと対策のポイント

予防的防御
（入口対策）

発見的防御
（出口対策）

事故発生の未然予防

事故発生後の局所化

APT攻撃のターゲットと対策のポイント

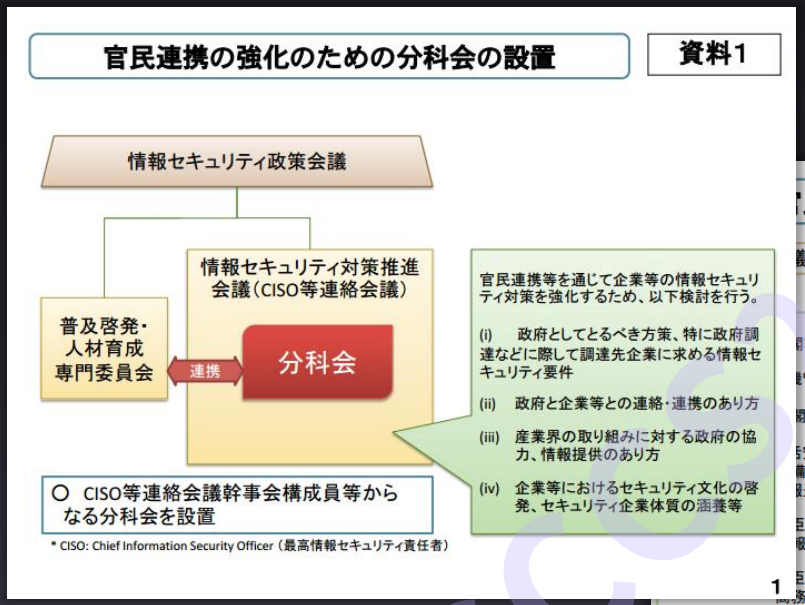
発見的防御
（出口対策）

事故発生後の局所化

発見的防御 （出口対策）

- ドメイン詐称されるような標的型メールを簡単に閲覧をしない為に定期的な訓練
- ドメイン詐称(フィッシング攻撃)を前提としたSPFやDKIMによる送信者認証による規制
- スパム対策やSMTP/HTTP/FTPウイルス対策並びにURLアクセスコントロール
- 標的型メールに含まれる犯罪サイトへのアクセスを統合型Eメールセキュリティで防御
- ウイルス感染後の犯罪サイトアクセスをウェブレピュテーションで規制
- インラインFirewall & IPSとリアルタイムログ監視による未知のウイルス感染の早期把握

情報セキュリティ対策に関する官民連携の在り方に関して


官民連携の強化のための分科会の設置

資料1

情報セキュリティ政策会議

情報セキュリティ対策推進会議（CISO等連絡会議）

普及啓発・人材育成専門委員会

連携

分科会

官民連携等を通じて企業等の情報セキュリティ対策を強化するため、以下検討を行う。

(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

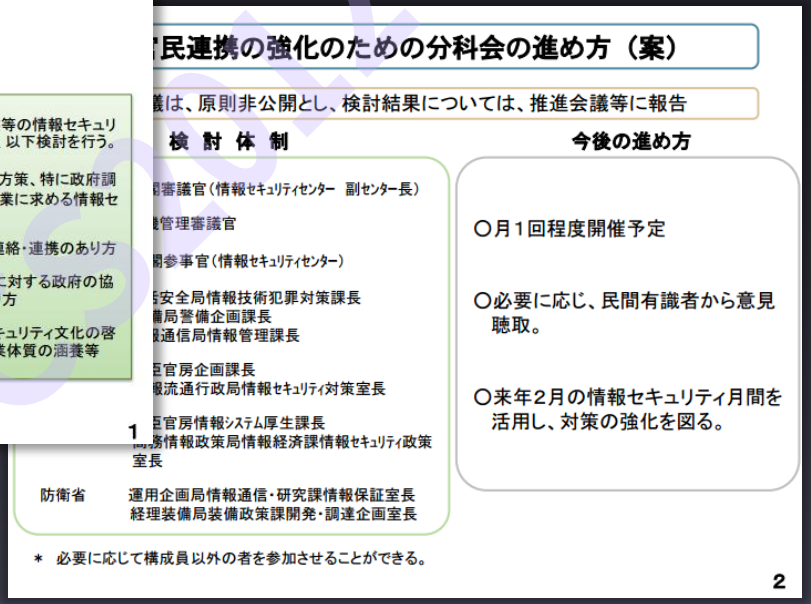
(ii) 政府と企業等との連絡・連携のあり方

(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

○ CISO等連絡会議幹事会構成員等からなる分科会を設置

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


民連携の強化のための分科会の進め方（案）

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

審議官（情報セキュリティセンター 副センター長）

管理審議官

参事官（情報セキュリティセンター）

安全局情報技術犯罪対策課長

局警備企画課長

通信局情報管理課長

官房企画課長

流通行政局情報セキュリティ対策室長

官房情報システム厚生課長

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
経理装備局装備政策課開発・調達企画室長

＊ 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。

○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。

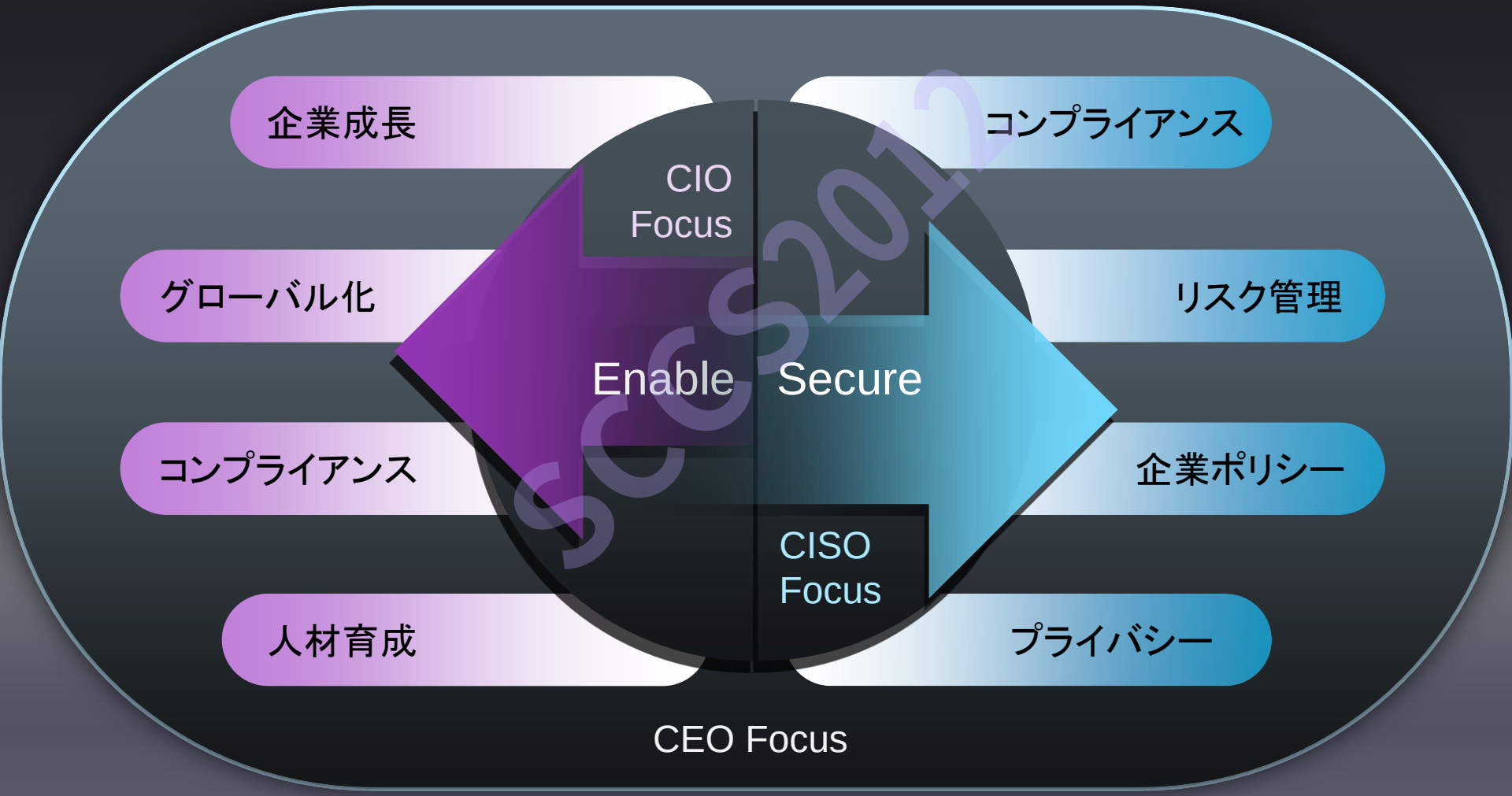
1

2

昨今のサイバー攻撃（テロ）に対応すべく企業/行政共に情報共有を促進し、
それらを実現する基盤として「CSIRT」と「CISO」設置の必要性が強化される

出典：2012年1月　政府の情報セキュリティ対策推進会議の官民連携の強化のための分科会資料より
http://www.nisc.go.jp/conference/suishin/ciso/dai3/pdf/1.pdf

CISOの役割



Security Architecture

(Cisco SecureX)

ネットワーク

ネットワーク ＝ セキュリティ

コンテキスト アウェア セキュリティの必要性

だれが	なにを	どこで	いつ	どのように
社員	ウェブサイト	@会社	月曜12:00PM	会社支給PC
契約社員	ウェブアプリ	@自宅	水曜16:00PM	会社支給スマートフォン
ゲスト	サービス	街中	日曜20:00PM	個人所有タブレット
	ソーシャル			
	ストレージ			

企業内 無線LAN

公衆 無線LAN

モバイル 3G/4G

ローカル ネットワーク

ポリシー、抑止力、インテリジェンス

サイバー攻撃に対応するフレームワーク

Action Item

組織における
セキュリティアクションアイテム

- ✓ ネットワーク全体の評価
- ✓ 受け入れられる使用ポリシーと行動規範の再評価
- ✓ 保護する必要のあるデータの決定
- ✓ データがある場所、データの保護方法を把握する
- ✓ ユーザ教育の方法を評価する
- ✓ 出口監視を行う
- ✓ BYODの必然性に備える
- ✓ インシデント対応計画の作成
- ✓ ソーシャルネットワークに関するセキュリティ対策の導入
- ✓ リスクの動的な現状を監視し、ユーザに情報を提供する