\Orchestrating a brighter world NEC

企業の経営に多大なダメージを与える新たな脅威

ビジネスメール詐欺（BEC）への対策

国内でも3.8億円の被害事例
対策を行わなければ、どの企業でも被害が起こりうる

新たな脅威
ビジネスメール詐欺

今、注目すべき脅威

■2017年に発生した社会的に影響が大きい情報セキュリティに対する脅威をランク付けした「情報セキュリティ10大脅威 2018」に新たにビジネスメール詐欺がランクイン

NEW ：初めてランクインした脅威

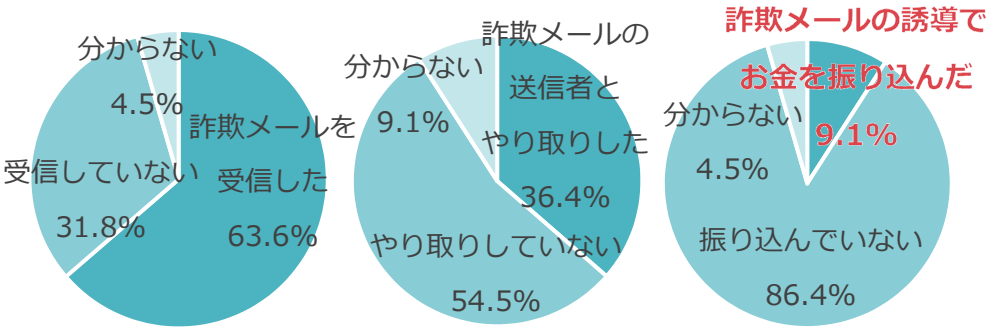
順位	「組織」の10大脅威	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位
3位	**ビジネスメール詐欺** NEW	ランク外
4位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
5位	セキュリティ人材の不足 NEW	ランク外
6位	ウェブサービスからの個人情報の窃取	3位
7位	IoT機器の脆弱性の顕在化	8位
8位	内部不正による情報漏えい	5位
9位	サービス妨害攻撃によるサービス停止	4位
10位	攻撃のビジネス化(アンダーグラウンドサービス)	9位

出典：情報セキュリティ10大脅威 2018
IPA 独立行政法人 情報処理推進機構（2018年1月30日発表）

急増するビジネスメール詐欺被害

■ 国内上場企業の売上高上位50社の被害調査

10%近くの企業が被害を受ける



2017年1月以降のビジネスメール詐欺の被害を教えてください　(n=22)

出展：「日経 xTECH」2018年3月12日掲載「ニュース解説」より
http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00128/

■ 国内の2016年以降に報道されたビジネスメール詐欺

大企業から中小企業まで経営に影響する被害が発生

時期	被害企業	被害額	概要
2016年 3月	不動産管理会社	2,000万円	外国人オーナーを装った犯人に、ペンションの宿泊代などをだまし取られる
2016年11月	貿易会社	見積書	サウジアラビアの取引先に成りすまし、ライバル会社から見積りを不正に入手、逮捕
2017年 2月	農耕具販売会社	300万円	海外取引先に農機具を発注。代金を騙し取られる
2017年 2月	貿易会社	580万円	フィリピンの農業用肥料販売会社から貿易会社への取引代金が別会社に送金、逮捕
2017年 3月	農耕具販売会社	500万円	海外取引先に農機具を発注、代金を騙し取られる
2017年12月	航空会社	3億8,000万円	取引先を装った犯人に代金を騙し取られる

各プレス発表内容より

ビジネスメール詐欺とは

■ ビジネスメール詐欺の概要

ビジネスメール詐欺（Business E-mail Compromise：BEC）とは、巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させたり情報を搾取する詐欺の手口です。

ビジネスメール詐欺「５つのタイプ」

- 現在の被害のほとんどは「タイプ１」ですが、２社間の商談の成り行きに影響されず、社内完結で実施しやすい「タイプ２」の攻撃が急速に拡大しています。

タイプ１：取引先との請求書の偽装

（例）取引のメールの最中に割り込み、偽の請求書（振込先）を送る

タイプ２：経営者等へのなりすまし

（例）経営者を騙り、偽の振込先に振り込ませる

タイプ３：窃取メールアカウントの悪用

（例）メールアカウントを乗っ取り、取引先に対して詐欺を行う

タイプ４：社外の権威ある第三者へのなりすまし

（例）社長から指示を受けた弁護士といった人物になりすまし、
振り込ませる

タイプ５：詐欺の準備行為と思われる情報の詐取

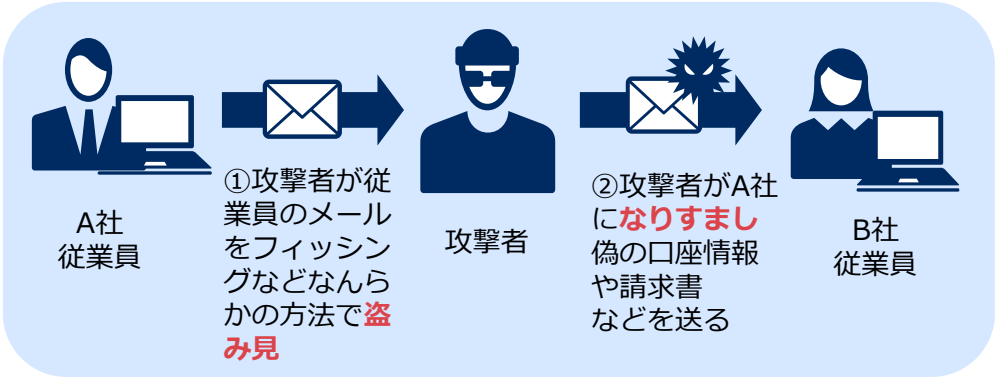
（例）経営層や人事部になりすまし、今後の詐欺に利用するため、
社内の従業員の情報を窃取する

引用：独立行政法人情報処理推進機構 「ビジネスメール詐欺「BEC」に関する事例と注意喚起 要約版」

代表的な攻撃手法

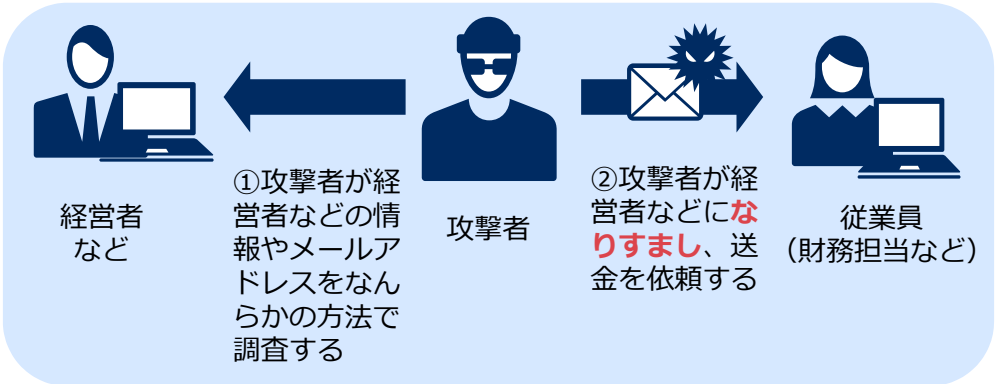
■ 「取引先との請求書の偽装」の例（タイプ１）

勤務している会社は海外の取引先から調達を行っています。取引先から事業拡大に伴い取引銀行の変更を知らせるメールが届きました。今後の支払いはすべて新しい銀行に入金してほしいという内容で、口座情報も一緒に送られてきました。取引先担当者の名前は本物で、メール送信者も実在します。



■ 「経営者等へのなりすまし」の例（タイプ２）

過去に何度か企業買収を行っている大企業で、支払業務を担当しています。ある朝、海外出張中のCEOからメールが届き、企業買収に必要な費用を電信送金するように依頼され、契約が成立するまで口外しないように指示を受けました。CEOからメールで電子送金を依頼されるのは珍しいことではなく、情報漏れを警戒し口外しない指示があるのも当然のことです。



なりすましメールに
人間が気づくのは非常に困難

■ 高度に偽装されたメールは本物と見分けがつかない
怪しいメールには注意をするなどの社内ルールだけでは防げません。
セキュリティシステムによる検査が必要です。

送信日時：2018年4月2日（月） 22:30
差出人：CEO<suzuki@example.com>
宛先：CFO<yamada@example.com>
件名：至急対応願います

本物

To:　CFO　山田一郎さん
お疲れ様です。

検討中のX社の買収の件ですが、緊急で進めることになりました。
本日中に極秘で先方が指定する海外の口座に送金を完了する
必要があるため、対応をお願いできないでしょうか？
必要な情報は後ほど送付します。

よろしくお願いします。

Chief Executive Officer
鈴木　太郎

攻撃者はメールの本文や差出人など
表示上怪しいところが一切ない、
見た目では本物と全く区別がつかない
なりすましメールを送信できます。

送信日時：2018年4月2日（月） 22:30
差出人：CEO<suzuki@example.com>
宛先：CFO<yamada@example.com>
件名：至急対応願います

偽物

To:　CFO　山田一郎さん
お疲れ様です。

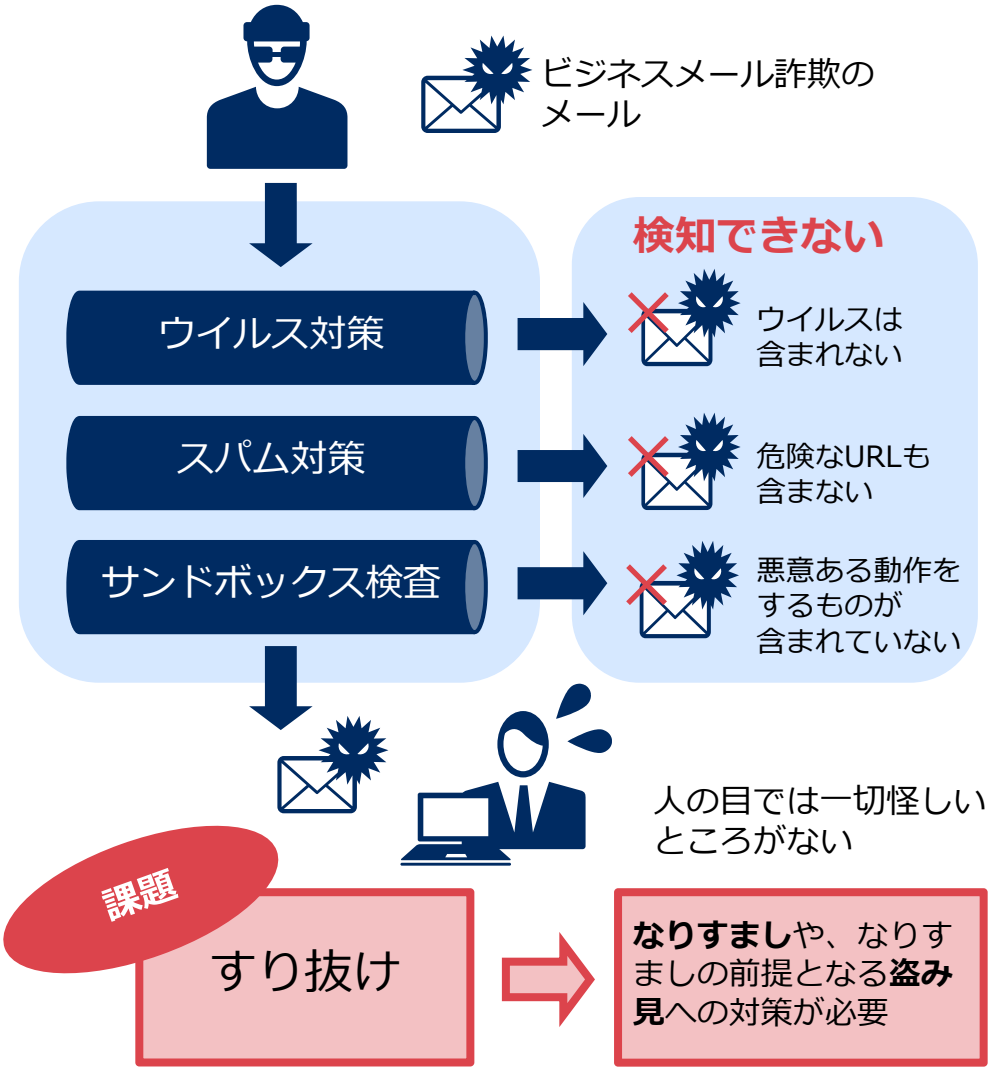
検討中のX社の買収の件ですが、緊急で進めることになりました。
本日中に極秘で先方が指定する海外の口座に送金を完了する
必要があるため、対応をお願いできないでしょうか？
必要な情報は後ほど送付します。

よろしくお願いします。

Chief Executive Officer
鈴木　太郎

一般的な攻撃対策では検知できない
ビジネスメール詐欺

■ ビジネスメール詐欺は、ウイルスも危険なURLも含まない**標的型攻撃メールの一種**です。
従来のセキュリティ対策では検知できません。



NECのビジネスメール詐欺対策ソリューション

■ ビジネスメール詐欺には、なりすましとなりすましの前提となる盗み見の2つの観点で対策が必要です。

対策レベル	概要	なりすまし対策	盗み見対策（フィッシング対策）
レベル1	一般的な攻撃者に対する対策	既知の攻撃元からのメールの受信を防止	既知の危険なURL、悪意あるURLへのアクセス禁止
レベル2	専門知識や設備を持つ攻撃者からの、**最も多く一般的に実施されている攻撃手法**に対する対策	送信ドメイン認証を用い正規のサーバから送信されていないなりすましメールを防御	有害サイトや業務に無関係な禁止カテゴリのURLへのアクセス禁止
レベル3	高度な専門知識や高度な設備を持つ攻撃者からの、**新たな攻撃手法**に対する最高強度の対策	送信ドメイン認証を回避するなりすましメール攻撃を検知･防御	攻撃者が新規に準備した本物と誤認する未知のURLのフィッシングサイトへのアクセスを禁止

■ NECはビジネスメール詐欺対策ソリューションとして、提供形態と対策攻撃手法毎にそれぞれ最適な製品・サービスをご用意しています。

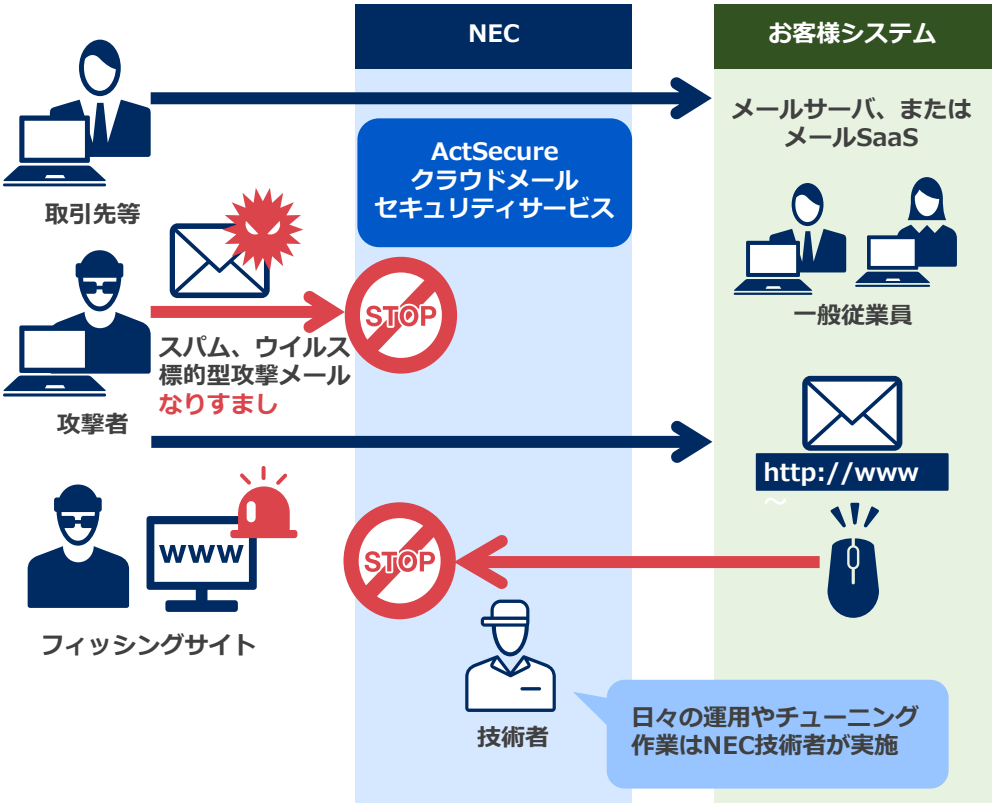
対策攻撃手法	提供形態：クラウド	提供形態：自社運用
なりすまし	対策1 → P.9 ActSecure クラウドメールセキュリティサービス 対策レベル2	対策2 → P.10 Mission Critical Mail Filter 対策レベル3
盗み見		対策3 → P.11 InterSafe WebFilter 対策レベル3

対策 1 クラウド

対策レベル2

ActSecure
クラウドメールセキュリティサービス

- メールセキュリティをクラウド型のサービスとして提供し、なりすましによるビジネスメール詐欺や標的型攻撃メールを検知･防御します。
- メールに記載されたURLをユーザがクリックする際に安全性を検査、危険だった場合はブロックし、フィッシングによる盗み見を防ぎます。



https://jpn.nec.com/act/acts_cloudmailsec.html

すぐに使え、安心、簡単、手間なし

- お客様環境はメール配送経路を変更するだけで導入が可能です。(最短7営業日でご用意)
- ビジネスメール詐欺･標的型攻撃メールだけでなく、スパム・ウイルスチェック、誤送信対策等も含めメールセキュリティをトータルにご提供します。

対策 2 自社運用

対策レベル3

Mission Critical Mail Filter

■ 最先端セキュリティ技術を製品化したメールフィルタリング製品
送信ドメイン認証を回避する攻撃についても検知し、ビジネスメール詐欺や標的型攻撃に対して一歩先を行く対策が可能です。

なりすまし対策機能

エンベロープ偽装対策	送信ドメイン認証（SPF、DMARC）
ヘッダ偽装対策	送信ドメイン認証（DKIM、DMARC、SenderID）
表示名偽装対策（Mailsploit脆弱性攻撃など）	特許出願中 表示名偽装チェック
送信ドメイン認証回避攻撃対策（近似ドメイン利用攻撃など）	特許出願中 インタラクションチェック
詐欺メール常套句チェック（件名、本文チェック）	コンテンツチェック·無害化 URLレピュテーション
新たなりすまし手法	プラグインアーキテクチャ AIエンジンなどをアドオン可能

https://jpn.nec.com/mcmail/bec-sl.html

高度で充実したなりすまし対策

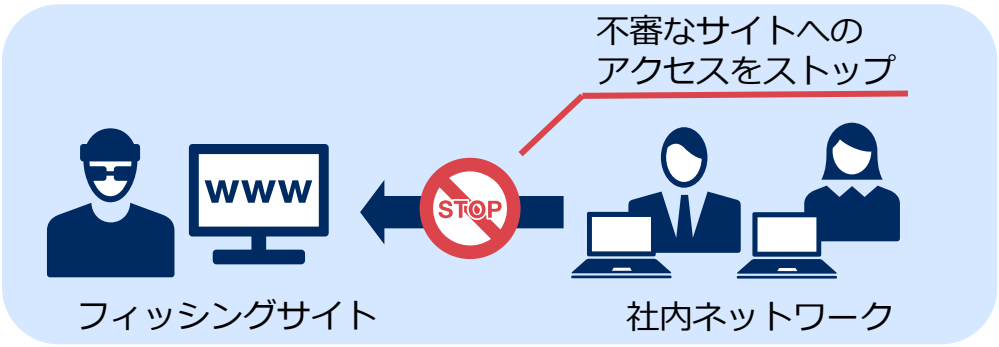
- 攻撃者から正規のメールサーバ以外から送信されたなりすましメールは送信ドメイン認証で検出できます。しかし、送信ドメイン認証だけでは、攻撃者が準備したよく似たメールドメイン名から送信されたメールについては防御できません。
- インタラクションチェックとは、これまでやりとりのないメールサーバやメールアカウントからの受信メールを検知し、危険度に応じて注意喚起や隔離などの対策を行うことができます。これにより、これまで検知できなかった攻撃者が新規に準備したメールドメインから送信されたメールについても検知することができるようになります。
- さらに、送信国の通知やAIエンジンのアドオンなど、多様なセキュリティ機能をアドオンできるアーキテクチャにより将来の攻撃の変化にも対応できる発展性を備えます。

対策3 自社運用

対策レベル3

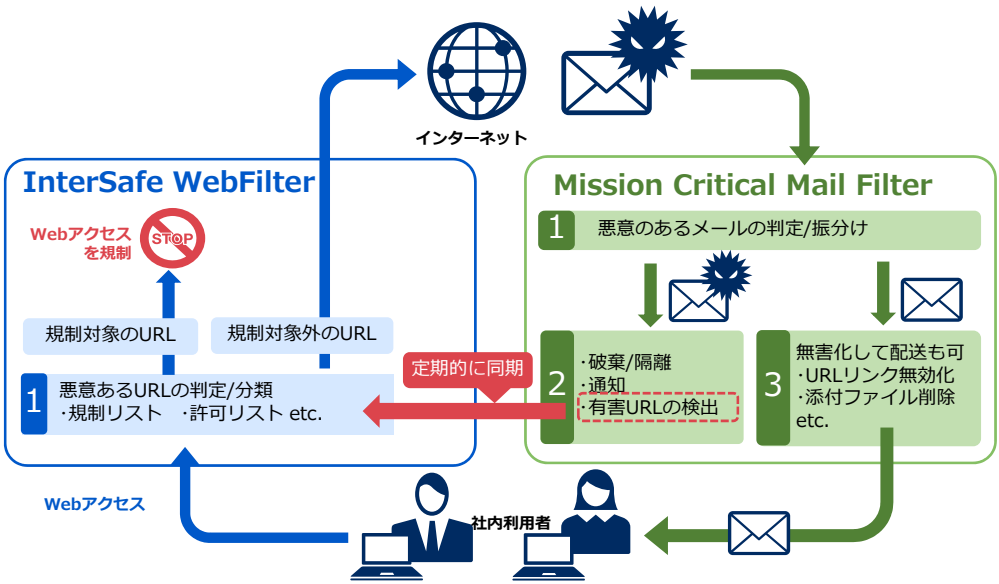
InterSafe WebFilter

■ 大手携帯キャリア3社が採用
網羅率98%を越える高精度URLデータベースにより、フィッシングサイトへのアクセスを防ぎ盗み見やアカウント乗っ取りを防ぎます。



http://www.nec.co.jp/middle/InterSafe

■ 悪意あるメールを**”検知”＋”即時対応（ブロック）”**
Mission Critical Mailと連携してリアルタイムで対策

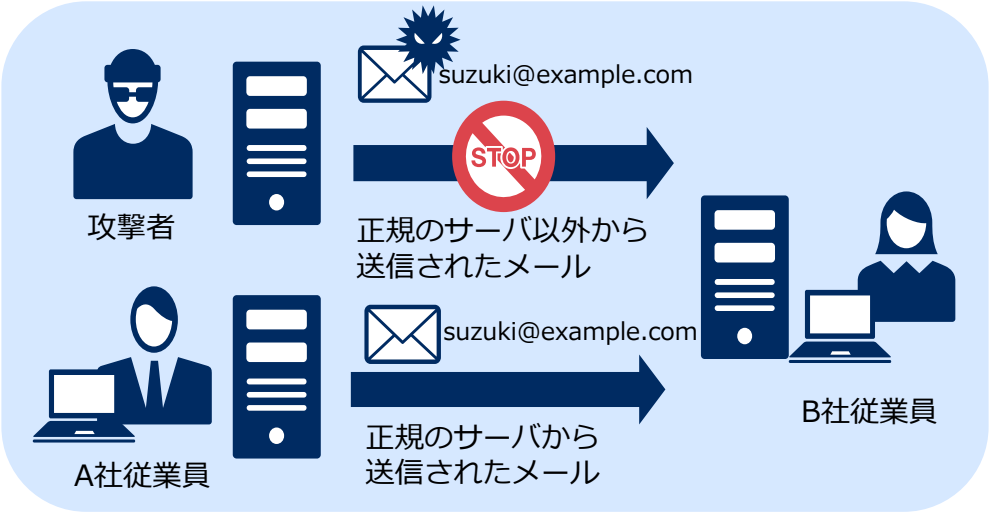


https://jpn.nec.com/mcmail/intersafesol.html

付録：なりすましへの対策①

ActSecure　MCMail

■ 送信ドメイン認証技術による対策
差出人や本文、件名などが完全に同一のメールであっても攻撃者により正規のメールサーバ以外から送信されたメールを識別して防御



MCMail

■ Mailsploit脆弱性攻撃に対する対策
Mailsploit脆弱性攻撃とは、メーラが差出人の表示の処理の際に　制御コード　「¥0」　以降は表示することができないことを利用した攻撃
制御コードが含まれるかを検知するなどで防御

送信日時：2018年4月2日（月） 22:30
差出人：CEO<suzuki@example.com>¥0**@invader.com**
宛先：CFO<yamada@example.com>
件名：至急対応願います

To:　CFO　山田一郎さん
お疲れ様です。

攻撃者の実際のメールアドレスは
メーラには表示されない
メールは～@invader.comの攻撃者の
正規のメールサーバから送信されるため
送信ドメイン認証では防御できない

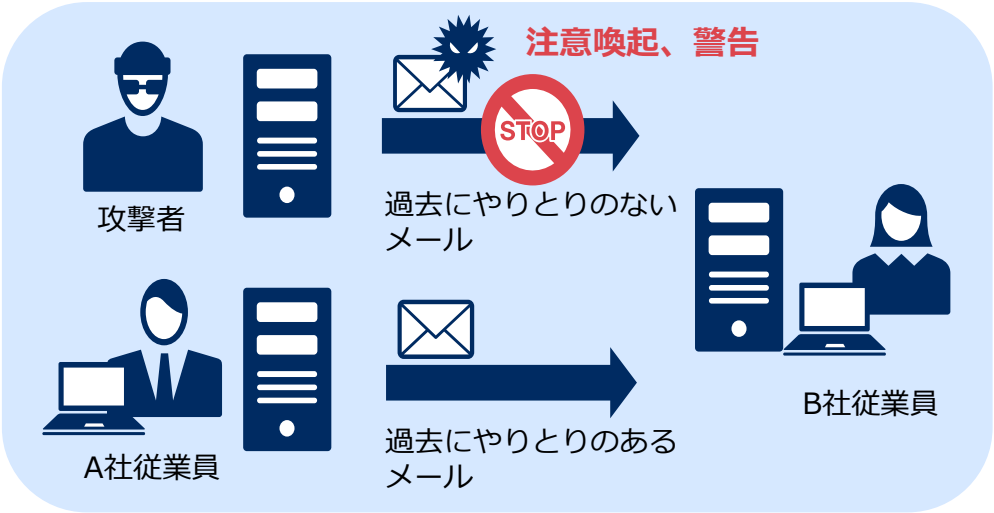
付録：なりすましへの対策②

MCMail

■ 近似ドメイン名からの送信の対策
視覚的に本物によく似た偽のメールアドレスやドメインを用意した攻撃
攻撃者のメールサーバは偽のメールアドレスに対しては正規のものになるため送信ドメイン認証では防御できない。

■本物		alice@campany.com
■偽物	①	alice@campnay.com
	②	alice@campanys.com
		aalice@campany.com
	③	alice@campny.com
	④	alice@carnpany.com
	⑤	alice-campany-a@freemail.com

過去にやりとりのないメールアドレスやメールサーバからのメールについては注意喚起、警告を行うことで利用者に気づきを与え被害を防ぎます。



付録：盗み見への対策

InterSafe

■ 業務に必要で安全と確認された分類カテゴリのWEBサイトのみのアクセスを許可することで、攻撃者が新規に用意したフィッシングサイトなどからの攻撃を防止し、盗み見やアカウント乗っ取りを防ぎます。

ビジネス･経済
ニュース
学術･教育

業務関連

マルウェア
DBD攻撃
フィッシング詐欺・
ワンクリック詐欺

既知のマルウェア関連

未分類

新規フィッシングサイト

画面の表示上は本物と区別がつかない
攻撃者が新規に用意したフィッシングサイトなど

価格

■1000ユーザ

導入形態	製品名	価格
クラウド	ActSecure クラウドメールセキュリティ	¥300,000円/月～
自社運用	Mission Critical Mail Filter	¥2,070,000円～ （1年間保守つき）
自社運用	InterSafe WebFilter	¥1,018,800円～ （１年あたり）

■3000ユーザ

導入形態	製品名	価格
クラウド	ActSecure クラウドメールセキュリティ	¥900,000円/月～
自社運用	Mission Critical Mail Filter	¥3,450,000円～ （1年間保守つき）
自社運用	InterSafe WebFilter	¥1,798,800円～ （１年あたり）

■5000ユーザ

導入形態	製品名	価格
クラウド	ActSecure クラウドメールセキュリティ	¥1,500,000円/月～
自社運用	Mission Critical Mail Filter	¥4,370,000円～ （1年間保守つき）
自社運用	InterSafe WebFilter	¥2,880,000円～ （１年あたり）

Futureproof Security
安心の先へ。

日本電気株式会社
〒108-8001　東京都港区芝五丁目７－１（NEC本社ビル）
URL：https://jpn.nec.com/mcmail/bec-sl.html

2018年5月(V1) EX-301933