

【ご参考】 HDE One フィルターレシピ集

株式会社HDE
HDE One サポートチーム



戦略的セキュリティを考えるための3つの「セキュリティスコープ」

Gmail

Office365

1. フィルタリングの対象者

特定の人や組織、事象を対象に限定した対策か、広く全社へむけた対策か。

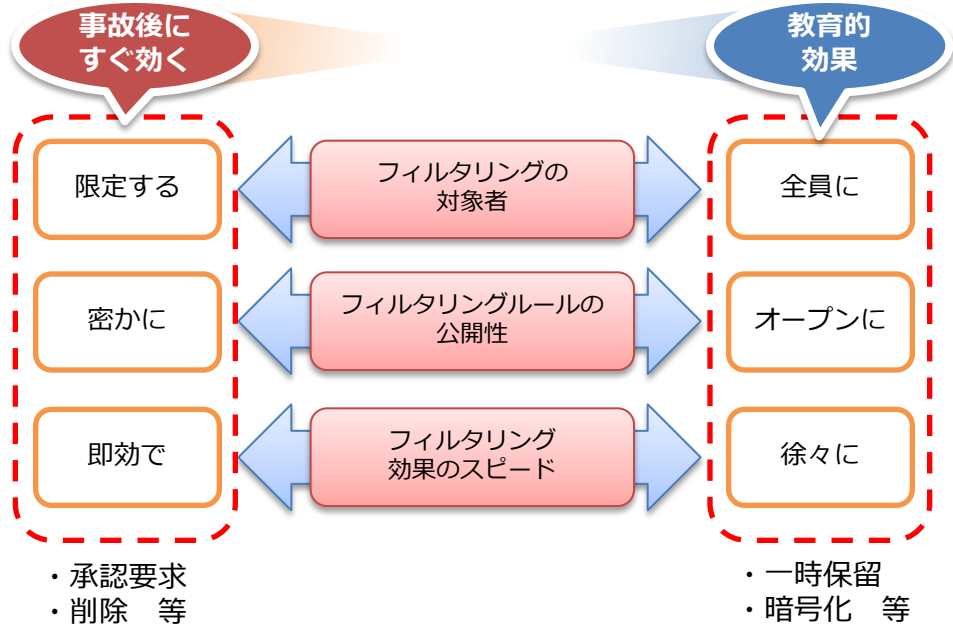
2. フィルタリングルールの公開性

社員に対して隠密に進めるのか、教育的効果を期待して公開して進めるのか。

3. フィルタリング効果のスピード

じわじわと浸透していく対策か、設定してすぐに効果が見られる即効性のある対策か。

3つの「セキュリティスコープ」



事故前：「全員に」「オープンに」「徐々に」効果が出るセキュリティ対策が有効。

⇒一時保留等でセキュリティ意識を高める

事故後：「限定する」「即効で」効果が出るセキュリティ対策が有効

⇒承認要求などの懲罰的な対応

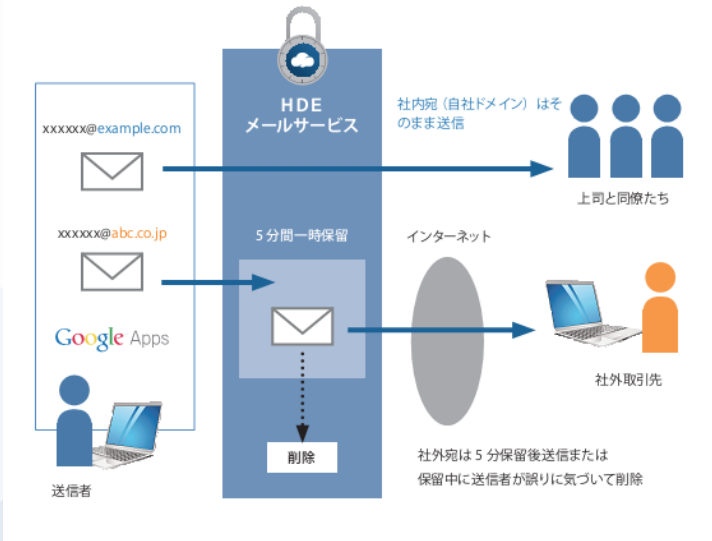
(1) チームワークで誤送信を防止する(一時保留+ZIP暗号化)



社外宛メールに対して一時保留を適用すると、社内宛のメールが先に届くので、同僚や上司がメールの誤りを見つけて送信者に知らせることで、保留時間内であればそのメールをストップすることができます。
 「自分が間違いに気づくことで、仲間の誤送信が防げる」という意識が高まり、チームワークで誤送信を防止しようという企業風土が生まれます。

○セキュリティスコープ

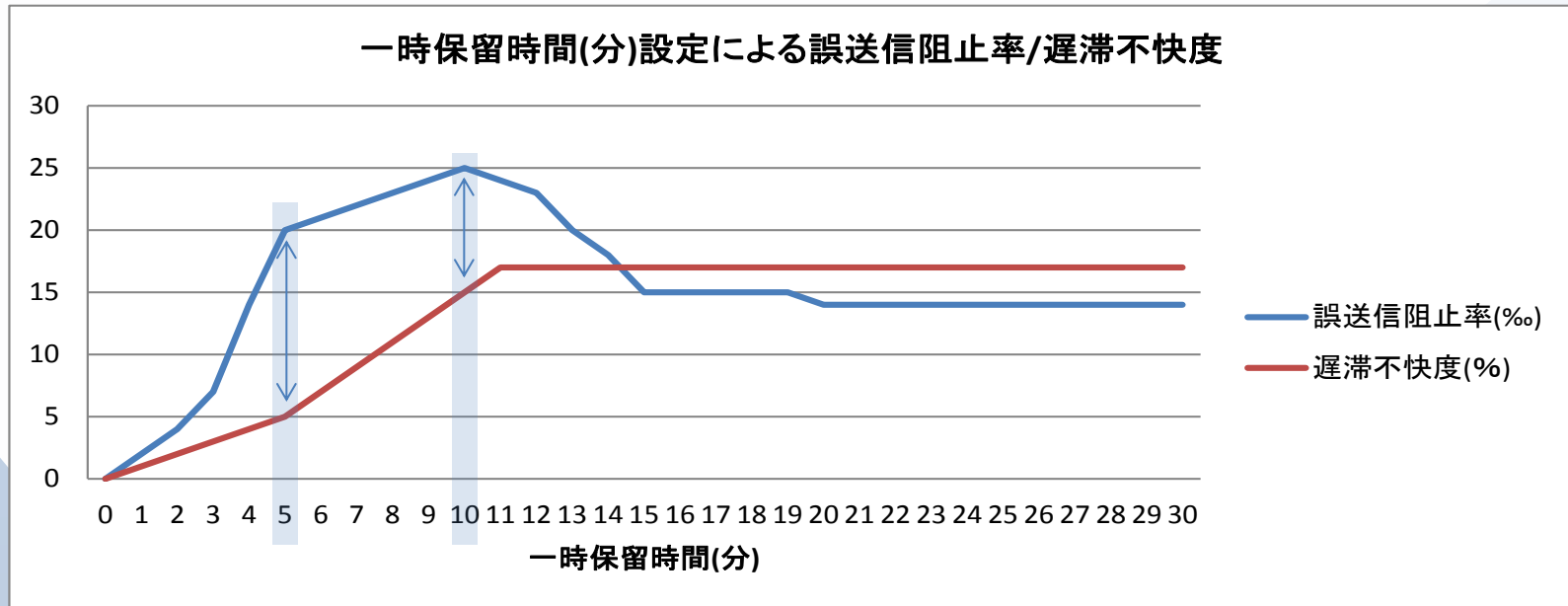
対象者は?	限定する		全員に
公開性は?	密かに		オープンに
効果は?	即効で		徐々に



○フィルターの設定例

優先度	送信元メールグループ		送信先メールグループ	ルールグループ
(100)	すべて	→	すべて	最初のチェック)
110	社内ドメイン	→	社内ドメイン	社内宛ルールグループ └全て：送信
120	社内ドメイン	→	すべて	社外宛ルールグループ └全て：一時保留(5分)+ZIP暗号化

【参考情報】 一時保留時間の目安



弊社のお客様の代表的な例をヒアリングし、数値化したグラフです。

【誤送信阻止率】

- ・ 一時保留3分未満では、阻止率が著しく低い
- ・ 一時保留5～10分は、阻止率が高いレベルで推移
- ・ 一時保留10分を超えると、一時保留画面で保留解除をルーティンワーク的にやってしまうケースが出てくるため、誤送信阻止率は逆に落ちてくる

【遅滞不快感】

- ・ 5分以下であれば、それほど不快感は高くない
- ・ 5～10分で徐々に不快感が高くなり、10分を超えると高止まりする

HDEの推奨値は、誤送信防止率が高く、遅滞の不快感が低い**5分**を推奨とさせていただきます。もう少し誤送信防止率を高くしたい場合は、最大10分までとさせていただくのがよいと思われます。

(2)特定のファイル流出を防ぐ(削除+本人通知)

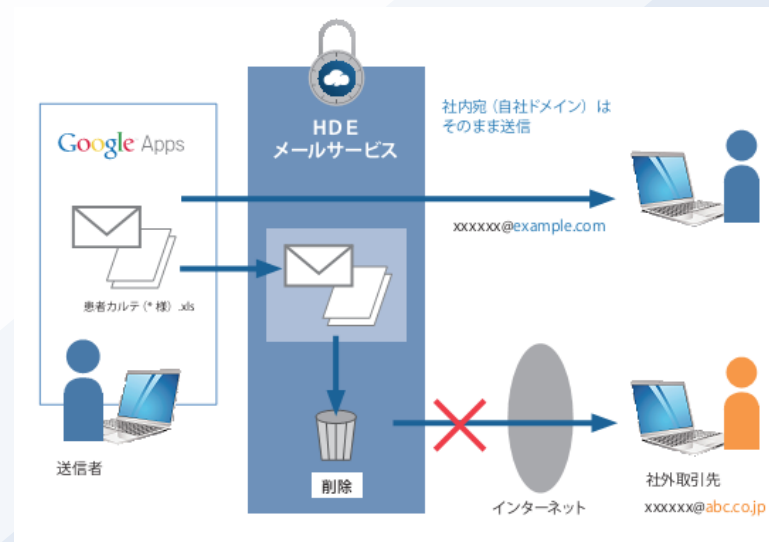
Gmail

Office365

HDEメールサービスでは、ファイル名やファイルの内容に含まれる特定の文言をチェックして、メール送信をストップすることが可能です。ファイル名(「患者カルテ(*様).xls」など)の検査や、ファイルの中の含まれる文字列(正規表現で「顧客番号:[A-Z]{2}[0-9]{6}」といった指定も可能)を検査することが可能です。

○セキュリティスコープ

対象者は?	限定する		全員に
公開性は?	密かに		オープンに
効果は?	即効で		徐々に



○フィルターの設定例

優先度	送信元メールグループ		送信先メールグループ	ルールグループ
(100	すべて	→	すべて	最初のチェック)
110	社内ドメイン	→	社内ドメイン	社内宛ルールグループ ↳全て:送信
120	社内ドメイン	→	すべて	社外宛ルールグループ ↳ファイル名が「患者カルテ(*様).xls」に一致:削除+送信者通知 ↳全て:送信(※一時保留+ZIP暗号化等でも可)

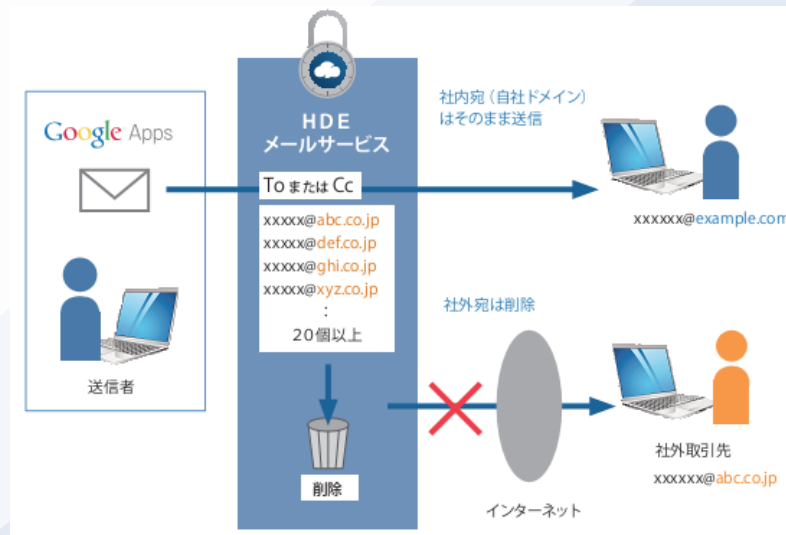
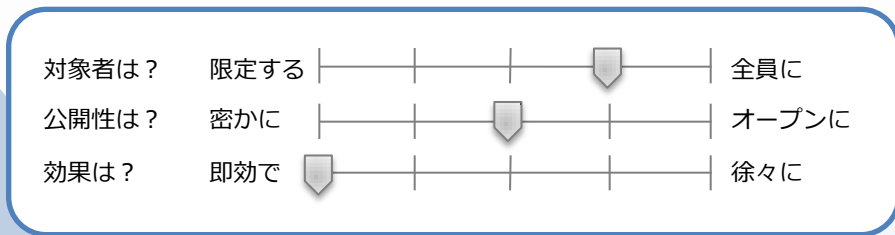
(3)大量誤配信を防止する(削除+本人通知)

Gmail

Office365

メルマガや会員へのお知らせなど多数の宛先に一齐送信をする場合、アドレスのリストをコピーしてメールソフトの宛先欄にペーストするような手作業を行っている企業も多く、誤って To や CC にペーストして、宛先の全員にメールアドレスを公開してしまう事故が発生しています。

○セキュリティスコープ



○フィルターの設定例

優先度	送信元メールグループ		送信先メールグループ	ルールグループ
(100)	すべて	→	すべて	最初のチェック)
110	社内ドメイン	→	社内ドメイン	社内宛ルールグループ └全て：送信
120	社内ドメイン	→	すべて	社外宛ルールグループ └Toに「@」が20件以上ある：削除+送信者通知 └CCに「@」が20件以上ある：削除+送信者通知 └全て：送信

(4) 事故を起こしたユーザーのメールを期間限定で承認制にする(承認要求)

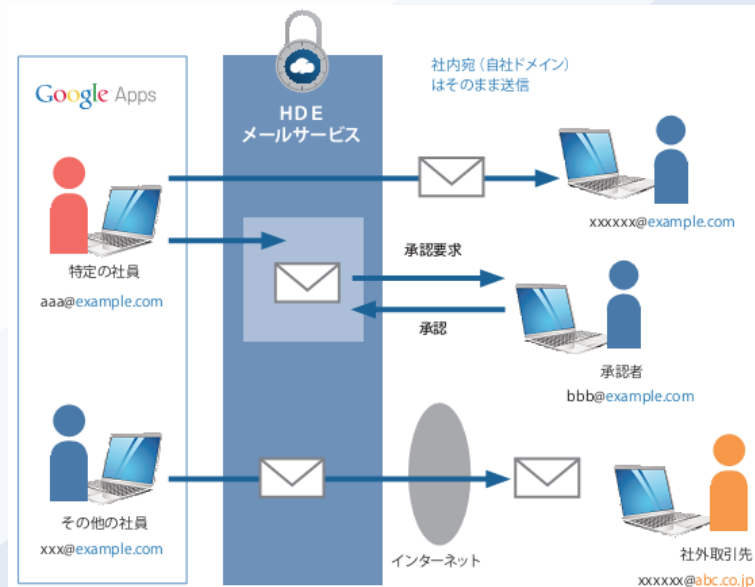
Gmail

Office365

情報漏洩事故を起こした社員については、再発防止のために何らかの対策と教育が必要です。厳重注意で終わり、始末書を出して終わりということでは、また同じ失敗を犯すリスクがあります。業務を停滞させることなく、本人のセキュリティに対する意識を高め、同じ失敗を繰り返さないようにしなければなりません。

○セキュリティスコープ

対象者は?	限定する		全員に
公開性は?	密かに		オープンに
効果は?	即効で		徐々に



○フィルターの設定例

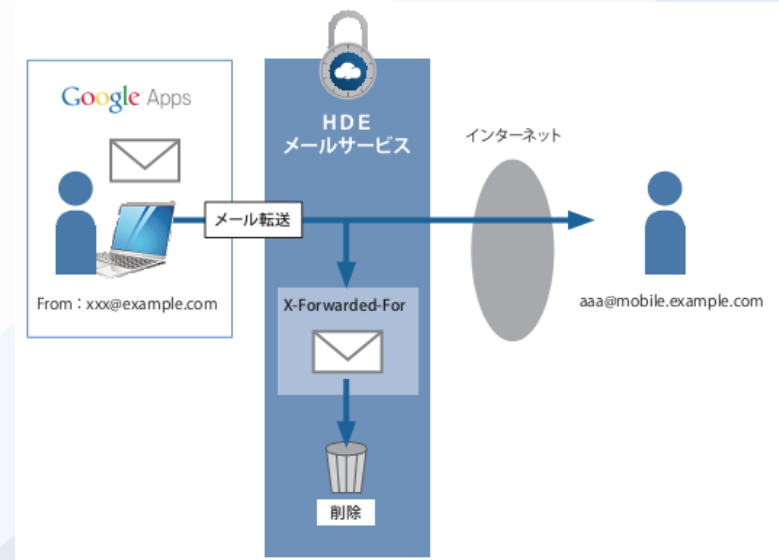
優先度	送信元メールグループ		送信先メールグループ	ルールグループ
(100	すべて	→	すべて	最初のチェック)
100	社内ドメイン	→	社内ドメイン	社内宛ルールグループ └全て：送信
110	承認要求ユーザー	→	すべて	承認要求ルールグループ └全て：承認要求
120	社内ドメイン	→	すべて	社外宛ルールグループ └全て：送信

(5) 携帯電話へのメール自動転送を一部のスタッフに許可する(転送制御)

Google Apps では、受信メールを指定した宛先へ自動転送するように、各自で設定することができます。しかし、メール転送を社員の自由に任せていると、セキュリティ対策が不十分な自宅のパソコンへ転送したり、携帯電話へ転送したりするため、セキュリティ事故のリスクが生じます。

○セキュリティスコープ

対象者は？	限定する		全員に
公開性は？	密かに		オープンに
効果は？	即効で		徐々に



○フィルターの設定例

優先度	送信元メールグループ		送信先メールグループ	ルールグループ
100	社内ドメイン	→	自動転送許可アドレス	転送許可ルールグループ └自動転送メールである(※)：送信
110	社内ドメイン	→	すべて	転送禁止ルールグループ └自動転送メールである(※)：削除
(120	すべて	→	すべて	最初のチェック)
130	社内ドメイン	→	すべて	通常メール送信ルールグループ └全て：送信

※Google Appsの場合、自動転送メールはヘッダーに「X-Forwarded-For」が存在。


HDE One 初期設定フィルター

HDE Oneでは下記の初期設定フィルターを提供いたします。
運用に合わせて、対象者や検知キーワードをご調整下さい。

	優先度	送信元メールグループ		送信先メールグループ	ルールグループ
	(100)	すべて	→	すべて	最初のチェック)
社内系	110	社内ドメイン	→	社内ドメイン	社内宛ルールグループ ↳全て：送信
削除系	120	社内ドメイン	→	すべて	送信禁止ルールグループ ↳Toに「@」が20件以上ある：削除+送信者通知 ↳CCに「@」が20件以上ある：削除+送信者通知 ↳件名/本文に「極秘」キーワードが含まれる：削除+送信者通知 ↳パスワード付きファイルが含まれる：削除+送信者通知 ↳ZIPファイルが含まれる：削除+送信者通知
送信系	130	社内ドメイン	→	すべて	通常メール送信ルールグループ ↳全て：一時保留5分+添付ファイル自動暗号化

運用を考慮して適切な閾値や
キーワードを設定いただく

暗号化を除外する宛先を
個別に設定することも可能

※  部分はお客様側でメンテナンスいただく